



Uso de los servicios de directorio

SANtricity 11.8

NetApp
April 05, 2024

Tabla de contenidos

- Uso de los servicios de directorio 1
 - Añadir servidor de directorio 1
 - Editar ajustes y asignaciones de roles del servidor de directorios 7
 - Quitar un servidor de directorio 10

Uso de los servicios de directorio

Añadir servidor de directorio

Para configurar la autenticación de Access Management, se debe establecer la comunicación entre un servidor LDAP y el host donde se ejecuta el proxy de servicios web para Unified Manager. A continuación, se deben asignar los grupos de usuarios LDAP a los roles de usuario local.

Antes de empezar

- Debe iniciar sesión con un perfil de usuario que cuente con permisos de administración de seguridad. De lo contrario, no se mostrarán las funciones de Access Management.
- Debe haber grupos de usuarios definidos en el servicio de directorio.
- Deben estar disponibles las credenciales del servidor LDAP, incluidos el nombre de dominio y la URL del servidor y, de manera opcional, el nombre de usuario y la contraseña de la cuenta de enlace.
- En el caso de los servidores LDAPS que utilizan un protocolo seguro, se debe instalar la cadena de certificados del servidor LDAP en la máquina local.

Acerca de esta tarea

La adición de un servidor de directorio es un proceso que consta de dos pasos. Primero, se debe introducir la URL y el nombre de dominio. Si el servidor utiliza un protocolo seguro, se debe cargar también un certificado de CA para autenticación si no se encuentra firmado por una entidad de firma estándar. Si se poseen credenciales de una cuenta de enlace, es posible introducir también el nombre de cuenta de usuario y la contraseña. Luego, se deben asignar los grupos de usuarios del servidor LDAP a los roles de usuario local.

Pasos


1. Seleccione **Access Management**.
2. En la ficha **Servicios de directorio**, seleccione **Agregar servidor de directorio**.


Se abre el cuadro de diálogo Añadir servidor de directorio.

3. En la ficha **Configuración del servidor**, introduzca las credenciales del servidor LDAP.

Detalles del campo

Ajuste	Descripción
Ajustes de configuración	Dominios
Introduzca el nombre de dominio del servidor LDAP. Si desea introducir varios dominios, escríbalos en una lista separada por comas. El nombre de dominio se utiliza en el inicio de sesión (<i>username@domain</i>) para especificar con qué servidor de directorio debe realizarse la autenticación.	URL del servidor
Introduzca la URL para acceder al servidor LDAP con el formato de <code>ldap[s]://host:*port*</code> .	Cargar certificado (opcional)

Ajuste	Descripción
<div data-bbox="245 363 302 417"></div> <p data-bbox="358 170 480 611">Este campo aparece solo si se especifica a un protocolo LDAPS en el campo URL del servidor arriba.</p> <p data-bbox="212 659 509 961">Haga clic en examinar y seleccione un certificado de CA para cargar. Este es el certificado o la cadena de certificados de confianza utilizado para autenticar el servidor LDAP.</p>	<p data-bbox="529 159 846 191">Enlazar cuenta (opcional)</p>
<p data-bbox="212 1014 505 1598">Introduzca una cuenta de usuario de solo lectura para realizar consultas de búsqueda en el servidor LDAP y para buscar dentro de los grupos. Introduzca el nombre de cuenta con formato tipo LDAP. Por ejemplo, si el usuario de enlace se denomina "bindacct", es posible introducir un valor como el siguiente <code>CN=bindacct,CN=Users,DC=cpoc,DC=local</code>.</p>	<p data-bbox="529 1014 899 1045">Enlazar contraseña (opcional)</p>

Ajuste		Descripción
 <p>Este campo se muestra cuando se introduce una cuenta de enlace.</p> <p>Introduzca la contraseña de la cuenta de enlace.</p>		Probar conexión del servidor antes de añadir
	<p>Seleccione esta casilla de comprobación si desea asegurarse de que el sistema pueda comunicarse con la configuración de servidor LDAP que introdujo. La prueba se produce después de hacer clic en Agregar en la parte inferior del cuadro de diálogo.</p> <p>Si esta casilla de comprobación está seleccionada y la prueba falla, no se añadirá la configuración. Debe resolver el error o anular la selección de la casilla de comprobación para omitir la comprobación y añadir la configuración.</p>	Configuración de privilegios
DN base de búsqueda		Introduzca el contexto de LDAP para buscar usuarios, generalmente con el formato de CN=Users, DC=cpoc, DC=local.
Atributo de nombre de usuario		Introduzca el atributo vinculado al ID de usuario para los fines de autenticación. Por ejemplo: sAMAccountName.

Ajuste	Descripción
Atributos de grupo	Introduzca una lista de atributos de grupo en el usuario, que se utilizará para la asignación de grupos a roles. Por ejemplo: <code>memberOf</code> , <code>managedObjects</code> .

4. Haga clic en la ficha **asignación de roles**.
5. Asigne grupos LDAP a los roles predefinidos. Un grupo puede tener varios roles asignados.

Detalles del campo

Ajuste	Descripción
Asignaciones	DN de grupo
<p>Especifique el nombre distintivo (DN) del grupo correspondiente al grupo de usuarios LDAP que se asignará. Se admiten expresiones regulares. Estos caracteres especiales de expresión regular deben escaparse con una barra diagonal inversa (\) si no forman parte de un patrón de expresión regular:</p> <p>\.[]{}()<>*+.=?<\$</p>	
Funciones	<p>Haga clic en el campo y seleccione uno de los roles de usuario local que se asignará al DN del grupo. Debe seleccionar individualmente cada rol que desee incluir en este grupo. Se requiere el rol de supervisión junto con los demás roles para iniciar sesión en SANtricity Unified Manager. Los roles asignados incluyen los siguientes permisos:</p> <ul style="list-style-type: none"> • Storage admin — acceso completo de lectura/escritura a los objetos de almacenamiento de las matrices, pero sin acceso a la configuración de seguridad. • Security admin — acceso a la configuración de seguridad en Access Management y Certificate Management. • Support admin — acceso a todos los recursos de hardware en matrices de almacenamiento, datos de fallos y eventos MEL. No brinda acceso a los objetos de almacenamiento ni a la configuración de seguridad. • Monitor — acceso de sólo lectura a todos los objetos de almacenamiento, pero sin acceso a la configuración de seguridad.



El rol de supervisión se requiere para todos los usuarios, incluido el administrador.

- Si lo desea, haga clic en **Agregar otra asignación** para introducir más asignaciones de grupo a rol.
- Cuando termine de asignar, haga clic en **Agregar**.

El sistema realiza una validación y se asegura de que la cabina de almacenamiento y el servidor LDAP pueden comunicarse. Si aparece un mensaje de error, compruebe las credenciales que introdujo en el cuadro de diálogo y vuelva a introducir la información, de ser necesario.

Editar ajustes y asignaciones de roles del servidor de directorios

Si anteriormente configuró un servidor de directorio en Access Management, es posible cambiar sus ajustes en cualquier momento. Entre estos ajustes se encuentran la información de conexión del servidor y las asignaciones de grupos a roles.

Antes de empezar

- Debe iniciar sesión con un perfil de usuario que cuente con permisos de administración de seguridad. De lo contrario, no se mostrarán las funciones de Access Management.
- Debe definirse un servidor de directorio.

Pasos

1. Seleccione **Access Management**.
2. Seleccione la ficha **Servicios de directorio**.
3. Si se define más de un servidor, seleccione el servidor que desea editar en la tabla.
4. Seleccione **Ver/editar configuración**.

Se abre el cuadro de diálogo Configuración del servidor de directorio.

5. En la ficha **Configuración del servidor**, cambie la configuración deseada.

Detalles del campo

Ajuste	Descripción
Ajustes de configuración	Dominios
Los nombres de dominio de los servidores LDAP. Si desea introducir varios dominios, escríbalos en una lista separada por comas. El nombre de dominio se utiliza en el inicio de sesión (<i>username@domain</i>) para especificar con qué servidor de directorio debe realizarse la autenticación.	URL del servidor
La URL para acceder al servidor LDAP con el formato de <code>ldap[s]://host:port</code> .	Enlazar cuenta (opcional)
La cuenta de usuario de solo lectura para realizar consultas en el servidor LDAP y buscar dentro de grupo.	Enlazar contraseña (opcional)
La contraseña de la cuenta vinculada. (Este campo se muestra cuando se introduce una cuenta vinculada.)	Probar conexión del servidor antes de guardar

Ajuste	Descripción
Comprueba que el sistema pueda comunicarse con la configuración del servidor LDAP. La prueba se produce después de hacer clic en Guardar . Si se selecciona esta casilla de comprobación y la prueba falla, no se modifica la configuración. Debe resolver el error o desmarcar la casilla de comprobación para omitir la prueba y volver a editar la configuración.	Configuración de privilegios
DN base de búsqueda	El contexto de LDAP para buscar usuarios, normalmente en la forma de CN=Users, DC=cpoc, DC=local.
Atributo de nombre de usuario	El atributo que está vinculado al ID de usuario para la autenticación. Por ejemplo: sAMAccountName.
Atributos de grupo	Lista de atributos de grupo en el usuario, que se utiliza para la asignación de grupos a roles. Por ejemplo:memberOf, managedObjects.

6. En la ficha **asignación de roles**, cambie la asignación deseada.

Detalles del campo

Ajuste	Descripción
Asignaciones	DN de grupo
El nombre de dominio para asignar el grupo de usuarios LDAP. Se admiten expresiones regulares. Estos caracteres especiales de expresión regular deben escaparse con una barra invertida (\) si no forman parte de un patrón de expresión regular: <code>\.[]{}()<>*+.=</code>	Funciones



El rol de supervisión se requiere para todos los usuarios, incluido el administrador.

- Si lo desea, haga clic en **Agregar otra asignación** para introducir más asignaciones de grupo a rol.
- Haga clic en **Guardar**.

Resultados

Una vez finalizada esta tarea, se finalizarán todas las sesiones de usuario activas. Solo se mantiene la sesión de usuario actual.

Quitar un servidor de directorio

Para interrumpir la conexión entre un servidor de directorio y el proxy de servicios web, es posible quitar la información del servidor de la página Access Management. Se recomienda ejecutar esta tarea si se configuró un servidor nuevo y se desea eliminar el anterior.

Antes de empezar

Debe iniciar sesión con un perfil de usuario que cuente con permisos de administración de seguridad. De lo contrario, no se mostrarán las funciones de Access Management.

Acerca de esta tarea

Una vez finalizada esta tarea, se finalizarán todas las sesiones de usuario activas. Solo se mantiene la sesión de usuario actual.

Pasos

- Seleccione **Access Management**.
- Seleccione la ficha **Servicios de directorio**.

3. Seleccione el servidor de directorio que desea eliminar de la lista.

4. Haga clic en **Quitar**.

Se abrirá el cuadro de diálogo Quitar servidor de directorio.

5. Tipo `remove` En el campo y, a continuación, haga clic en **Quitar**.

Se eliminará la configuración del servidor de directorio, la configuración de privilegios y las asignaciones de roles. Los usuarios ya no podrán iniciar sesión con las credenciales de este servidor.

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 INTERRUPCIÓN 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.