# Cómo gestiona ONTAP la autenticación del cliente NFS

ONTAP 9

NetApp
April 24, 2024

# Tabla de contenidos

# Cómo gestiona ONTAP la autenticación del cliente NFS

## Cómo maneja ONTAP la información general sobre autenticación de clientes NFS

Los clientes de NFS deben autenticarse correctamente antes de poder acceder a los datos en la SVM. ONTAP autentica a los clientes al comprobar sus credenciales de UNIX con los servicios de nombres que se configuran.

Cuando un cliente NFS se conecta con la SVM, ONTAP obtiene las credenciales de UNIX del usuario comprobando diferentes servicios de nombre, en función de la configuración de los servicios de nombres de la SVM. ONTAP puede comprobar credenciales para cuentas UNIX locales, dominios NIS y dominios LDAP. Debe haber al menos uno de ellos configurado para que ONTAP pueda autenticar correctamente al usuario. Puede especificar varios servicios de nombres y el orden en el que ONTAP los busca.

En un entorno NFS puro con estilos de seguridad de volúmenes UNIX, esta configuración es suficiente para autenticar y proporcionar el acceso adecuado a los archivos para que los usuarios que se conecten desde un cliente NFS.

Si utiliza estilos de seguridad de volúmenes mixtos, NTFS o unificados, ONTAP debe obtener un nombre de usuario SMB para el usuario UNIX para la autenticación con un controlador de dominio de Windows. Esto puede suceder mediante la asignación de usuarios individuales mediante cuentas de UNIX locales o dominios LDAP, o bien mediante un usuario de SMB predeterminado. Puede especificar los servicios de nombres que ONTAP busca en qué orden, o bien especificar un usuario de SMB predeterminado.

## Cómo utiliza ONTAP los servicios de nombres

ONTAP utiliza los servicios de nombres para obtener información acerca de los usuarios y los clientes. ONTAP usa esta información para autenticar a los usuarios que acceden a los datos o administran el sistema de almacenamiento, y para asignar las credenciales de usuario en un entorno mixto.

Al configurar el sistema de almacenamiento, debe especificar los servicios de nombres que desea que ONTAP utilice para obtener credenciales de usuario con fines de autenticación. ONTAP admite los siguientes servicios de nombres:

- Usuarios locales (archivo)
- Dominios NIS externos (NIS)
- Dominios LDAP externos (LDAP)

Utilice la `vserver services name-service ns-switch` Familia de comandos de para configurar SVM con los orígenes para buscar información de red y el orden en el que realizar búsquedas. Estos comandos proporcionan la funcionalidad equivalente del `/etc/nsswitch.conf` Fichero de sistemas UNIX.

Cuando un cliente NFS se conecta a la SVM, ONTAP comprueba los servicios de nombre especificados para obtener las credenciales de UNIX del usuario. Si los servicios de nombres están configurados correctamente y ONTAP puede obtener las credenciales de UNIX, ONTAP autentica correctamente el usuario.

En un entorno con estilos de seguridad mixtos, es posible que ONTAP tenga que asignar credenciales de usuario. Debe configurar los servicios de nombres según sea necesario para el entorno de a fin de permitir que ONTAP asigne correctamente las credenciales de usuario.

ONTAP también utiliza servicios de nombres para autenticar cuentas de administrador de SVM. Debe tener esto en cuenta al configurar o modificar el switch del servicio de nombres para evitar deshabilitar accidentalmente la autenticación de las cuentas de administrador de SVM. Para obtener más información sobre los usuarios de administración de SVM, consulte "Autenticación de administrador y RBAC".

# Cómo ONTAP otorga acceso a archivos SMB desde los clientes NFS

ONTAP utiliza la semántica de seguridad del sistema de archivos de Windows NT (NTFS) para determinar si un usuario de UNIX, en un cliente NFS, tiene acceso a un archivo con permisos NTFS.

Para ello, ONTAP convierte el identificador de usuario de UNIX (UID) del usuario en una credencial de SMB y, a continuación, utiliza la credencial de SMB para verificar que el usuario tiene derechos de acceso al archivo. Una credencial SMB consta de un identificador de seguridad principal (SID), normalmente el nombre de usuario de Windows del usuario y uno o más SID de grupo que corresponden a los grupos Windows de los que el usuario es miembro.

El tiempo que tarda ONTAP en convertir el UID de UNIX en una credencial SMB puede ser de decenas de milisegundos a cientos de milisegundos, dado que el proceso implica contactar a un controlador de dominio. ONTAP asigna el UID a la credencial SMB e introduce la asignación en una caché de credenciales para reducir el tiempo de verificación debido a la conversión.

# Cómo funciona la caché de credenciales NFS

Cuando un usuario de NFS solicita acceso a exportaciones NFS en el sistema de almacenamiento de, ONTAP debe recuperar las credenciales de usuario desde servidores de nombres externos o desde archivos locales para autenticar el usuario. ONTAP después almacena estas credenciales en la caché de credenciales internas para futuras referencias. Comprender el funcionamiento de la caché de credenciales NFS le permite manejar los posibles problemas de rendimiento y acceso.

Sin la caché de credenciales, ONTAP tendría que consultar los servicios de nombres cada vez que un usuario NFS solicitara acceso. En un sistema de almacenamiento de mucha actividad al que acceden muchos usuarios, se pueden producir rápidamente problemas de rendimiento graves, que provocan retrasos no deseados o incluso la denegación del acceso del cliente NFS.

Con la caché de credenciales, ONTAP recupera las credenciales de usuario y las almacena durante un periodo predeterminado de tiempo para obtener un acceso rápido y sencillo en caso de que el cliente NFS envíe otra solicitud. Este método ofrece las siguientes ventajas:

- Facilita la carga en el sistema de almacenamiento al manejar menos solicitudes a servidores de nombres externos (como NIS o LDAP).
- Facilita la carga de los servidores de nombres externos enviando menos solicitudes.
- Acelera el acceso del usuario al eliminar el tiempo de espera para obtener credenciales de fuentes externas antes de que el usuario pueda autenticarse.

ONTAP almacena las credenciales positivas y negativas en la caché de credenciales. Las credenciales positivas significan que el usuario se ha autenticado y se le ha concedido acceso. Las credenciales negativas indican que el usuario no se ha autenticado y se le ha denegado el acceso.

De forma predeterminada, ONTAP almacena credenciales positivas durante 24 horas, es decir, tras autenticar inicialmente al usuario, ONTAP utiliza las credenciales en caché para cualquier solicitud de acceso por parte de ese usuario durante 24 horas. Si el usuario solicita acceso después de 24 horas, el ciclo se vuelve a iniciar: ONTAP descarta las credenciales en caché y obtiene de nuevo las credenciales del origen del servicio de nombres adecuado. Si las credenciales cambiaron en el servidor de nombres durante las 24 horas anteriores, ONTAP almacenará las credenciales actualizadas para utilizarlas en las próximas 24 horas.

De forma predeterminada, ONTAP almacena credenciales negativas durante dos horas; es decir, después de denegar inicialmente el acceso a un usuario, ONTAP continúa negando cualquier solicitud de acceso por ese usuario durante dos horas. Si el usuario solicita acceso después de 2 horas, el ciclo se inicia de nuevo: ONTAP obtiene las credenciales de nuevo del origen de servicio de nombres apropiado. Si las credenciales cambiaron en el servidor de nombres durante las dos horas anteriores, ONTAP almacena en caché las credenciales actualizadas para utilizarlas en las siguientes dos horas.