Guía de seguridad de Oracle® ZFS Storage Appliance (versión OS8.7.0)

Referencia: E81239-01
Marzo de 2017

Referencia: E81239-01

Accesibilidad a la documentación

Para obtener información acerca del compromiso de Oracle con la accesibilidad, visite el sitio web del Programa de Accesibilidad de Oracle en `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc`.

Acceso a Oracle Support

Los clientes de Oracle que hayan adquirido servicios de soporte disponen de acceso a soporte electrónico a través de My Oracle Support.. Para obtener información, visite `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` o `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs` si tiene problemas de audición.

Contenido

Guía de seguridad de Oracle ZFS Storage Appliance

En esta guía, se exploran, revisan y destacan las consideraciones de seguridad necesarias para crear un sistema de almacenamiento seguro y una comprensión de todo el equipo sobre los objetivos de seguridad específicos. Recomendamos que lea esta guía antes de configurar el dispositivo de modo que pueda aprovechar las características de seguridad disponibles y crear los niveles de seguridad que necesite.

También puede usar esta guía como referencia para encontrar información más detallada sobre las consideraciones de seguridad de las distintas características y funciones del dispositivo Oracle ZFS Storage Appliance. Para conocer los procedimientos de configuración del dispositivo, consulte la *Guía de administración de Oracle ZFS Storage Appliance*.

En las siguientes secciones, se brinda una descripción de las recomendaciones y funciones de seguridad de Oracle ZFS Storage Appliance:

- **Primeros pasos**: describe la seguridad de inicio de sesión durante la instalación inicial del dispositivo y recomendaciones para la seguridad física del sistema.
- **Modelo administrativo**: describe cómo acceder de forma remota mediante la BUI y la CLI, cómo restringir el acceso a la BUI y la CLI, el modelo de aplicación de parches del sistema, las actualizaciones diferidas, los paquetes de asistencia y cómo realizar la copia de seguridad de la configuración.
- **Usuarios del dispositivo**: describe los roles administrativos, quién puede administrar el dispositivo y la gestión de autorizaciones de usuario.
- **Listas de control de acceso**: describe el mecanismo que autoriza o deniega el acceso a archivos y directorios.
- **Servicios de datos**: describe los servicios de datos que admite el dispositivo y la seguridad que ofrecen los distintos servicios de datos.
- **Servicios de directorio**: describe los servicios de directorio que se pueden configurar en el dispositivo y sus ramificaciones de seguridad.
- **Ajustes del sistema**: describe la configuración del sistema, es decir, la asistencia técnica remota, las etiquetas de servicio, Kerberos, SMTP, SNMP, Syslog, la identidad del sistema, la limpieza de discos y la prevención de la destrucción.
- **Logs de seguridad**: describe los tipos de log que son pertinentes a la seguridad.

Primeros pasos

En esta sección, se describe la seguridad de inicio de sesión durante la instalación inicial del dispositivo y recomendaciones para la seguridad física del sistema.

Instalación inicial

Oracle ZFS Storage Appliance se proporciona con el software del dispositivo preinstalado. No se requiere ninguna instalación de software y no se envía ningún medio.

La instalación inicial se realiza con el nombre de cuenta y la contraseña predeterminados; la contraseña root predeterminada debe cambiarse después de la instalación. Si Oracle ZFS Storage Appliance se restablece a los valores de fábrica, la contraseña root también se restablece al valor predeterminado en el dispositivo y en el procesador de servicio.

Durante la instalación inicial de un dispositivo Oracle ZFS Storage Appliance, se cuenta con un nombre de cuenta y una contraseña predeterminados que están asociados con el procesador de servicio del sistema. Esta cuenta predeterminada permite que el administrador del sistema obtenga acceso inicial al dispositivo, donde luego debe realizar los pasos de instalación inicial. Uno de los pasos requeridos es configurar una nueva contraseña administrativa del dispositivo, que, a su vez, restablece con el mismo valor la contraseña predeterminada del procesador de servicio.

Seguridad física

Para controlar el acceso al sistema, debe mantener la seguridad física del entorno informático. Por ejemplo, un sistema cuya sesión está iniciada pero desatendida es vulnerable al acceso no autorizado. El entorno y el hardware del equipo deben estar físicamente protegidos contra el acceso no autorizado en todo momento.

Oracle ZFS Storage Appliance se ha diseñado para obtener acceso restringido, y, por lo tanto, dicho acceso se controla mediante mecanismos de seguridad (p. ej., acceso con clave, bloqueo, herramienta y tarjeta de identificación). Las personas con acceso autorizado conocen los motivos de esta restricción y de las precauciones que se deben tomar.

Modelo administrativo

En esta sección, se describe la seguridad del modelo administrativo de Oracle ZFS Storage Appliance.

Acceso administrativo remoto

En esta sección, se describe la seguridad de acceso remoto de Oracle ZFS Storage Appliance.

Interfaz de usuario basada en explorador

La interfaz de usuario basada en explorador (BUI) se usa para la administración general del dispositivo. Las pantallas de servicios de la BUI se utilizan para ver y modificar los servicios y los parámetros de configuración de acceso remoto.

La administración se realiza por medio de una sesión HTTP segura (HTTPS) del explorador. Las sesiones HTTPS están cifradas con un certificado de firma automática que se genera de manera exclusiva para cada dispositivo Oracle ZFS Storage Appliance en el momento de la instalación inicial. Las sesiones de HTTPS tienen un timeout de sesión predeterminado de 15 minutos que el usuario puede definir.

Interfaz de línea de comandos

La interfaz de línea de comandos (CLI) se puede utilizar para realizar la mayoría de las acciones administrativas que pueden realizarse en la BUI.

El shell seguro (SSH) permite a los usuarios iniciar sesión en Oracle ZFS Storage Appliance mediante una conexión de capa de conexión segura (SSL) a la CLI. SSH también se puede usar como medio para ejecutar secuencias de comandos automatizadas desde un host remoto, por ejemplo, para recuperar logs diarios o estadísticas de análisis.

Autorización de usuario restringida

El acceso administrativo está limitado al usuario root, a los administradores locales definidos con los privilegios relevantes y a aquellos usuarios autorizados mediante servidores de identidad, como el protocolo ligero de acceso a directorios (LDAP) y el servicio de información de red (NIS).

Además, el dispositivo puede usar Kerberos para autenticar usuarios para el inicio de sesión administrativo por medio de la BUI, de la CLI y de la API RESTful. y para el acceso a servicios, incluidos NFS, HTTP, FTP, SFTP y SSH. Kerberos también se puede usar para configurar valores de seguridad para recursos compartidos individuales que usan el protocolo NFS, como se describe en “Opciones de cifrado y autenticación de NFS” [15].

API de RESTful de Oracle ZFS Storage Appliance

La API de RESTful de Oracle ZFS Storage Appliance se puede usar para gestionar Oracle ZFS Storage Appliance. La arquitectura RESTful está basada en un modelo cliente-servidor por capas que permite que los servicios se puedan redireccionar de manera transparente a través de concentradores, enrutadores y otros sistemas de red estándares sin necesidad de configuración de los clientes.

La API de RESTful de Oracle ZFS Storage Appliance utiliza las mismas credenciales de autenticación que la BUI y la CLI. Todas las solicitudes de clientes externos se autentican de forma individual utilizando las credenciales de dispositivo y se realizan mediante una conexión HTTPS en el puerto 215. La API de RESTful admite sesiones de HTTPS que tienen un timeout de 15 minutos predeterminado que el usuario puede definir.

Para obtener información acerca de la administración del dispositivo Oracle ZFS Storage Appliance con la API de RESTful, consulte la *Guía de la API de RESTful del dispositivo Oracle ZFS Storage Appliance*.

Actualizaciones del sistema

Para aprovechar las mejoras de seguridad más recientes, Oracle recomienda mantener el software del sistema actualizado.

Las actualizaciones del sistema se aplican como reemplazos binarios completos del software del sistema. Antes de la actualización, se toma una instantánea de la agrupación del sistema en ejecución. Esto permite que el usuario anule la actualización y vuelva a la versión anterior en caso de que sea necesario.

Actualizaciones diferidas

Una actualización diferida es una característica o función que forma parte de una actualización del sistema, pero que no se activa cuando se realiza una actualización del sistema. El administrador decide si se deben aplicar actualizaciones diferidas y cuándo hacerlo. Las actualizaciones que no se aplican durante una actualización del sistema siguen estando disponibles en las sucesivas actualizaciones del sistema. No puede seleccionar que se apliquen actualizaciones individuales; cuando selecciona aplicar actualizaciones diferidas, puede aplicar todas las actualizaciones o ninguna de ellas. Después de aplicar una actualización, no puede anularla y volver a una versión anterior del software del sistema.

Paquetes de asistencia

Si el sistema está registrado para la asistencia telefónica remota y sufre un fallo grave, el estado del sistema se envía a My Oracle Support, donde personal de asistencia de ingeniería lo examina y se puede crear un paquete de asistencia. La información del estado del sistema que se envía a My Oracle Support no contiene datos del usuario; solo se envía información de configuración.

Copia de seguridad de la configuración

Las configuraciones del sistema se pueden guardar localmente para una restauración posterior. Estas copias de seguridad no contienen datos del usuario; solo se guardan los valores de configuración.

Usuarios del dispositivo

Hay dos tipos de usuarios de Oracle ZFS Storage Appliance:

- **Usuarios de servicios de datos**: clientes que acceden a recursos de bloques y archivos utilizando los protocolos admitidos, como el sistema de archivos de red (NFS), el bloque de mensajes de servidor (SMB), el canal de fibra, la interfaz estándar de equipos pequeños de Internet (iSCSI), el protocolo de transferencia de hipertexto (HTTP) y el protocolo de transferencia de archivos (FTP).
- **Usuarios administrativos**: usuarios que gestionarán la configuración y los servicios en el dispositivo.

Esta sección solo se aplica a los usuarios administrativos.

Roles del usuario administrativo

Puede otorgar privilegios a los administradores asignándoles roles personalizados. Un rol es una recopilación de privilegios que puede asignar a un administrador. Es posible que quiera crear distintos roles de administrador y operador, con diferentes niveles de autorización. Los integrantes del personal deben recibir un rol que sea adecuado para sus necesidades, sin tener que asignarles privilegios innecesarios.

El uso de roles es más seguro que el uso de contraseñas de administrador de acceso completo compartidas, como asignar a todos la contraseña root. Los roles restringen a los usuarios a un

conjunto definido de autorizaciones. Además, los roles de usuario pueden rastrearse hasta los nombres de usuarios individuales en los logs de auditoría. De forma predeterminada, existe un rol llamado "Basic administration" (Administración básica) que contiene un mínimo de autorizaciones.

Los usuarios administrativos pueden ser:

- **Usuarios locales**: toda la información de cuenta se guarda en Oracle ZFS Storage Appliance.
- **Usuarios de directorio**: se usan las cuentas de NIS o LDAP existentes, y los valores de configuración de autorización complementaria se guardan en el dispositivo. El acceso al dispositivo se debe otorgar de forma explícita a los usuarios NIS o LDAP existentes, quienes luego pueden iniciar sesión en el dispositivo y administrarlo. No se puede otorgar acceso de forma predeterminada.

Ámbitos administrativos

Las autorizaciones permiten a los usuarios realizar tareas específicas, por ejemplo, crear recursos compartidos, reiniciar el dispositivo y actualizar el software del sistema. Los grupos de autorizaciones se denominan ámbitos. Cada ámbito puede tener un juego de filtros opcionales que limitan la cantidad de autorizaciones. Por ejemplo, en lugar de otorgar una autorización para reiniciar todos los servicios, se puede usar un filtro para permitir reiniciar solo el servicio HTTP.

Listas de control de acceso

Oracle ZFS Storage Appliance proporciona control de acceso a archivos por medio de listas de control de acceso (ACL, Access Control List). Una ACL es un mecanismo que permite o deniega el acceso a un archivo o directorio en particular.

El modelo de ACL proporcionado por Oracle ZFS Storage Appliance se basa en el modelo de ACL de NFSv4, que deriva de la semántica de ACL de Windows. Es un modelo de ACL enriquecido que proporciona acceso específico a los archivos y directorios. Cada archivo y directorio dentro del dispositivo de almacenamiento tiene una ACL, y todas las decisiones de control de acceso de SMB y NFS atraviesan los mismos algoritmos para determinar quién tiene permitido o denegado acceder a los archivos y directorios.

Una ACL se compone de una o más entradas de control de acceso (ACE, Access Control Entry). Cada ACE contiene una entrada para los permisos que ACE otorga o deniega, a quién se aplica la ACE y los indicadores de nivel de herencia usados.

Herencia de ACL

Las ACL de NFSv4 permiten que las ACE sean heredadas por los archivos y los directorios recientemente creados. La herencia de ACE se controla mediante varios indicadores de nivel de herencia que el administrador configura en las ACL durante la configuración inicial.

Determinación de acceso de la ACL

Las ACL de NFSv4 dependen del orden y se procesan de arriba abajo. Una vez que se otorga un permiso, una ACE subsiguiente no lo puede revocar. Una vez que se deniega un permiso, una ACE subsiguiente no lo puede otorgar.

ACL de nivel de recurso compartido de SMB

Una ACL de nivel de recurso compartido de SMB es una ACL que está combinada con una ACL de un archivo o directorio en el recurso compartido para determinar los permisos vigentes del archivo. La ACL de nivel de recurso compartido proporciona otra capa de control de acceso superior a las ACL de archivo y permite realizar configuraciones de control de acceso más sofisticadas. Las ACL de nivel de recurso compartido se configuran cuando el sistema de archivos se exporta mediante el protocolo SMB. Si el sistema de archivos no se exporta mediante el protocolo SMB, la configuración de la ACL de nivel de recurso compartido no se aplicará. De manera predeterminada, las ACL de nivel de recurso compartido otorgan control total a todos.

Propiedades de la ACL de ZFS

El comportamiento de la ACL y las propiedades de herencia son aplicables solo para los clientes NFS. Los clientes SMB usan semántica de Windows estricta y tienen prioridad por sobre las propiedades de ZFS. La diferencia es que NFS utiliza semántica POSIX y los clientes SMB no. Las propiedades son principalmente compatibles con POSIX.

Servicios de datos

En la siguiente tabla, se proporcionan descripciones y los puertos que se utilizan para cada servicio de datos.

TABLA 1 Servicios de datos

SERVICIO	DESCRIPCIÓN	PUERTOS USADOS
NFS	Acceso al sistema de archivos mediante los protocolos NFSv3 y NFSv4	111 y 2049
iSCSI	Acceso al LUN mediante el protocolo iSCSI	3260 y 3205
SMB	Acceso al sistema de archivos mediante el protocolo SMB	SMB mediante NetBIOS 139 SMB mediante TCP 445 Datagrama NetBIOS 138 Servicio de nombres NetBIOS 137
Análisis de virus	Análisis de virus del sistema de archivos	
FTP	Acceso al sistema de archivos mediante el protocolo FTP	21
HTTP	Acceso al sistema de archivos mediante el protocolo HTTP	80
HTTPS	Para conexiones entrantes seguras	443
NDMP	Servicio de host NDMP	10000
Replicación remota	Replicación remota	216 y 217
Cifrado	Cifrado transparente para sistemas de archivos y LUN	
Migración shadow	Migración shadow de datos	
SFTP	Acceso al sistema de archivos mediante el protocolo SFTP	218
TFTP	Acceso al sistema de archivos mediante el protocolo TFTP	
Red de área de almacenamiento	Grupos de iniciadores y de destino de red de área de almacenamiento	

Cantidad mínima de puertos necesaria

Para proporcionar seguridad en una red, puede crear firewalls. Los números de puerto se usan para crear firewalls e identificar de manera unívoca cada transacción realizada por la red mediante la especificación del host y el servicio.

En la siguiente lista, se muestra la cantidad mínima de puertos necesaria para crear firewalls:

Puertos de entrada

- icmp/0-65535 (PING)
- tcp/1920 (EM)
- tcp/215 (BUI)

- tcp/22 (SSH)
- udp/161 (SNMP)

Puertos de entrada adicionales si se usa la función de uso compartido de archivos por HTTP (normalmente no se la usa):

- tcp/443 (SSL WEB)
- tcp/80 (WEB)

Puertos de salida

- tcp/80 (WEB)

Nota - Para la replicación, de ser posible, use túneles de encapsulación de enrutamiento genérico (GRE). De esta manera, el tráfico circula por las interfaces de back-end y evita el firewall, que podría ralentizarlo. Si no hay túneles GRE disponibles en el núcleo NFS, debe ejecutar la replicación por la interfaz de front-end. En este caso, el puerto 216 y el puerto 217 también deben estar abiertos.

Opciones de cifrado y autenticación de NFS

Además de la capacidad del dispositivo para usar Kerberos para autenticar usuarios para el inicio de sesión administrativo y para el acceso a servicios, Kerberos también se puede usar para configurar la seguridad de recursos compartidos individuales que usan el protocolo NFS.

Por defecto, los recursos compartidos NFS se asignan mediante la autenticación AUTH_SYS RPC. También puede configurarlos para que se compartan con la seguridad de Kerberos. Mediante el uso de la autenticación AUTH_SYS, el ID de usuario (UID) y el ID de grupo (GID) UNIX del cliente pasan sin autenticación en la red por el servidor NFS. Este mecanismo de autenticación puede ser fácilmente derrotado por cualquier usuario con acceso root en un cliente; por lo tanto, es mejor usar cualquiera de los otros modos de seguridad disponibles.

Es posible especificar controles de acceso adicionales por recurso compartido para permitir o denegar el acceso a los recursos compartidos de hosts, dominios DNS o redes específicos.

Modos de seguridad

Los modos de seguridad se configuran por recurso compartido. En la siguiente lista, se describe la configuración de seguridad de Kerberos disponible:

- **krb5**: autenticación de usuario final mediante Kerberos V5.

- **krb5i**: krb5 más protección de integridad (los paquetes de datos están protegidos contra alteraciones).
- **krb5p**: krb5i más protección de privacidad (los paquetes de datos están protegidos contra alteraciones y cifrados).

Al definir los modos de seguridad, se pueden especificar combinaciones de tipos de Kerberos. La combinación de modos de seguridad permite que los clientes realicen el montaje con cualquiera de los tipos de Kerberos mostrados.

Tipos de Kerberos

- **sys**: autenticación del sistema
- **krb5**: Kerberos v5 únicamente; los clientes deben realizar el montaje con este tipo.
- **krb5:krb5i**: Kerberos v5 con integridad; los clientes pueden realizar el montaje con cualquier tipo de la lista.
- **krb5i**: Kerberos v5 con integridad únicamente; los clientes deben realizar el montaje con este tipo.
- **krb5:krb5i:krb5p**: Kerberos v5 con integridad o privacidad; los clientes pueden realizar el montaje con cualquiera de los tipos de la lista.
- **krb5p**: Kerberos v5 con privacidad únicamente; los clientes deben realizar el montaje con este tipo.

Servicio de datos iSCSI

Al configurar un LUN en Oracle ZFS Storage Appliance, puede exportar ese volumen por medio de un destino iSCSI. El servicio iSCSI permite a los iniciadores iSCSI utilizar el protocolo iSCSI para tener acceso a los destinos deseados.

El servicio admite realizar tareas de detección, gestión y configuración con el protocolo iSNS. El servicio iSCSI admite autenticación unidireccional (el destino autentica al iniciador) y bidireccional (el destino y el iniciador se autentican mutuamente) con el protocolo de autenticación por desafío mutuo (CHAP). Asimismo, el servicio admite la gestión de datos de autenticación de CHAP en una base de datos de servicio de autenticación remota telefónica de usuario (RADIUS).

El sistema realiza primero la autenticación y después la autorización, en dos pasos independientes. Si el iniciador local tiene un nombre CHAP y un secreto CHAP, el sistema realiza la autenticación. Si el iniciador local no tiene propiedades CHAP, el sistema no realiza ninguna autenticación, y, por lo tanto, todos los iniciadores son elegibles para autorización.

El servicio iSCSI le permite especificar una lista global de iniciadores que se pueden utilizar en grupos de iniciadores. Cuando use iSCSI y autenticación CHAP, RADIUS puede usarse como protocolo iSCSI que difiere todas las autenticaciones CHAP al servidor RADIUS seleccionado.

Compatibilidad con RADIUS

RADIUS es un sistema para usar un servidor centralizado con el fin de realizar la autenticación CHAP en nombre de los nodos de almacenamiento. Cuando usa iSCSI y autenticación CHAP, puede seleccionar RADIUS para el protocolo iSCSI, que se aplica a iSCSI y a extensiones de iSCSI para RDMA (iSER), y envía todas las autenticaciones CHAP al servidor RADIUS seleccionado.

Para permitir que Oracle ZFS Storage Appliance realice la autenticación CHAP con RADIUS, los siguientes parámetros deben coincidir:

- El dispositivo debe especificar la dirección del servidor RADIUS y un secreto para usar al comunicarse con el servidor RADIUS.
- El servidor RADIUS debe tener una entrada (por ejemplo, en su archivo de cliente) que proporcione la dirección del dispositivo y especifique el mismo secreto antes mencionado.
- El servidor RADIUS debe tener una entrada (por ejemplo, en su archivo de usuario) que proporcione el nombre CHAP y el secreto CHAP coincidente para cada iniciador.
- Si el iniciador utiliza su nombre IQN como nombre CHAP (configuración recomendada) y el dispositivo no necesita una entrada de iniciador independiente para cada cuadro de iniciador, el servidor RADIUS puede realizar todos los pasos de autenticación.
- Si el iniciador usa un nombre CHAP independiente, el dispositivo tiene que tener una entrada de iniciador para ese iniciador que especifique la asignación del nombre IQN al nombre CHAP. No es necesario que esta entrada de iniciador especifique el secreto CHAP del iniciador.

Servicio de datos de SMB

El protocolo SMB, también conocido como sistema de archivos de Internet común (CIFS), brinda principalmente acceso compartido a todos los archivos de la red de Microsoft Windows. También proporciona autenticación.

Las siguientes opciones de SMB tienen implicancias de seguridad:

- **Restringir el acceso anónimo a la lista de recursos compartidos**: esta opción requiere que los clientes se autentifiquen mediante SMB antes de recibir una lista de recursos compartidos. Si esta opción está desactivada, los clientes anónimos pueden acceder a la lista de recursos compartidos. Esta opción está desactivada de forma predeterminada.

- **Firma de SMB activada**: esta opción permite la interoperabilidad con clientes SMB mediante la característica de firma de SMB. Si la opción está activada, se verificará la firma de un paquete firmado. Si la opción está desactivada, un paquete no firmado se aceptará sin verificación de firma. Esta opción está desactivada de forma predeterminada.
- **Firma de SMB requerida**: esta opción puede usarse cuando se requiere firma de SMB. Cuando la opción está activada, todos los paquetes de SMB deben estar firmados o se rechazarán. Los clientes que no admitan la firma de SMB no pueden conectarse con el servidor. Esta opción está desactivada por defecto.
- **Activar enumeración basada en acceso**: si se configura esta opción, se filtran las entradas del directorio en función de las credenciales del cliente. Enable Access-based Enumeration Esta opción está desactivada de forma predeterminada.

Autenticación de modo de dominio de Active Directory

En el modo de dominio, los usuarios se definen en Active Directory (AD) de Microsoft. Los clientes SMB pueden conectarse a Oracle ZFS Storage Appliance mediante la autenticación NTLM o Kerberos.

Cuando un usuario se conecta mediante un nombre de host de Oracle ZFS Storage Appliance completo, los clientes de Windows en el mismo dominio o un dominio de confianza usan la autenticación Kerberos; de lo contrario, usan la autenticación NTLM.

Cuando un cliente SMB usa la autenticación NTLM para conectarse al dispositivo, las credenciales del usuario son reenviadas al controlador de dominio AD para autenticación. Esto se denomina autenticación cruzada.

Si se definen políticas de seguridad de Windows que restringen la autenticación NTLM, los clientes de Windows deben conectarse al dispositivo mediante un nombre de host completo. Para obtener más información, consulte el siguiente artículo de Microsoft Developer Network:

`http://technet.microsoft.com/en-us/library/jj865668%28v=ws.10%29.aspx`

Después de la autenticación, se establece un "contexto de seguridad" para la sesión de SMB del usuario. El usuario representado por el contexto de seguridad tiene un descriptor de seguridad único (SID). El SID denota la propiedad del archivo y se usa para determinar los privilegios de acceso del archivo.

Autenticación en modo de grupo de trabajo

En el modo de grupo de trabajo, los usuarios se definen localmente en el dispositivo Oracle ZFS Storage Appliance. Cuando un cliente SMB se conecta a un dispositivo en modo de grupo

de trabajo, sus algoritmos hash de nombre de usuario y contraseña se usan para autenticar al usuario localmente.

El nivel de compatibilidad del gestor LAN (LM) se usa para especificar el protocolo usado para la autenticación cuando el dispositivo está en el modo de grupo de trabajo.

En la siguiente lista, se muestra el comportamiento de Oracle ZFS Storage Appliance para cada nivel de compatibilidad de LM:

- Nivel 2: acepta autenticación LM, NTLM y NTLMv2
- Nivel 3: acepta autenticación LM, NTLM y NTLMv2
- Nivel 4: acepta autenticación NTLM y NTLMv2
- Nivel 5: acepta solo autenticación NTLMv2

Una vez que el usuario de grupo de trabajo se autentica correctamente, se establece un contexto de seguridad. Se crea un SID único para los usuarios definidos en el dispositivo mediante una combinación del SID de la máquina y el UID del usuario. Todos los usuarios locales se definen como usuarios UNIX.

Grupos locales y privilegios

Los grupos locales son grupos de usuarios del dominio que confieren privilegios adicionales a esos usuarios. Los administradores pueden pasar por alto permisos de archivos para cambiar la propiedad de los archivos. Los operadores de copia de seguridad pueden pasar por alto los controles de acceso de los archivos para hacer copias de seguridad de los archivos y restaurarlos.

Operaciones administrativas mediante Microsoft Management Console

Para garantizar que solo los usuarios apropiados tengan acceso a las operaciones administrativas, existen restricciones de acceso para las operaciones que se realizan de manera remota mediante Microsoft Management Console (MMC).

La siguiente lista muestra los usuarios y sus operaciones permitidas:

- **Usuarios regulares**: generan listas de recursos compartidos.
- **Miembros del grupo de administradores**: generan listas de archivos abiertos y cerrados, desconectan conexiones de usuarios y ven logs de servicios y eventos. Los miembros del grupo de administradores también pueden establecer y modificar las ACL de nivel de recurso compartido.

Análisis de virus

El servicio de análisis de virus analiza en busca de virus en el nivel del sistema de archivos. Cuando se accede a un archivo desde cualquier protocolo, el servicio de análisis de virus primero analiza el archivo y, si encuentra algún virus, deniega el acceso y pone el archivo en cuarentena. El análisis es realizado por un motor externo que Oracle ZFS Storage Appliance contacta. El motor externo no está incluido en el software del dispositivo.

Una vez que el archivo ha sido analizado con las definiciones de virus más recientes, no se lo vuelve a analizar hasta la siguiente modificación. El análisis de virus se proporciona principalmente para los clientes SMB que pueden llegar a introducir virus. Los clientes NFS también pueden usar el análisis de virus, pero debido a la manera en la que trabaja el protocolo NFS, es posible que un virus no se detecte tan rápido como con el cliente SMB.

Motor de retraso para ataques de temporización

SMB no implementa ningún motor de retraso para evitar los ataques de temporización. Se basa en la estructura criptográfica de Oracle Solaris.

Cifrado de datos durante la conexión

El servicio SMB usa la versión 1 del protocolo SMB, que no admite el cifrado de datos durante la conexión.

Servicio de datos FTP

FTP permite el acceso al sistema de archivos de clientes FTP. El servicio FTP no permite los inicios de sesión anónimos, y los usuarios deben autenticarse con el servicio de nombres configurado.

FTP admite la siguiente configuración de seguridad. Esta configuración se comparte para todos los sistemas de archivos en los que se permite el acceso de protocolo FTP:

- **Activar SSL/TLS**: permite las conexiones de FTP cifradas con SSL/TLS y se asegura de que la transacción de FTP esté cifrada. De forma predeterminada, esta opción está desactivada. El servidor FTP utiliza un certificado de seguridad autofirmado o un certificado proporcionado por el cliente.
- **Permitir inicio de sesión root**: permite los inicios de sesión de FTP del usuario root. Está desactivada de forma predeterminada porque la autenticación de FTP usa texto sin formato, lo que representa un riesgo de seguridad por ataques de examen de red.

- **Cantidad máxima de intentos de inicio de sesión permitidos**: cantidad de intentos de inicio de sesión incorrectos antes de que se desconecte la conexión de FTP y el usuario tenga que volver a conectarse para intentarlo de nuevo. El valor predeterminado es 3.
- **Nivel de log**: el nivel de detalle del log.

El servicio FTP admite los siguientes logs:

- **proftpd**: eventos de FTP, incluidos los inicios de sesión correctos y los intentos de inicio de sesión fallidos.
- **proftpd_xfer**: log de transferencia de archivos.
- **proftpd_tls**: eventos de FTP relacionados con el cifrado SSL/TLS.

Servicio de datos HTTP

HTTP proporciona acceso a los sistemas de archivos mediante los protocolos HTTP y HTTPS (WebDAV) y mediante el sistema distribuido de creación y control de versiones web de la extensión HTTP (WebDAV). Esto permite a los clientes acceder a los sistemas de archivos compartidos mediante un explorador web o como sistema de archivos local si el software del cliente lo admite.

El servidor HTTPS utiliza un certificado de seguridad autofirmado o un certificado proporcionado por el cliente. Para obtener un certificado proporcionado por el cliente, debe generar una solicitud de firma de certificado (CSR) y enviársela a la autoridad de certificación (CA) para que la firme. Cuando la CA devuelve el certificado firmado, se lo puede instalar en el dispositivo. Si un certificado está firmado por una CA que no es una CA raíz, debe obtener también certificados de las CA de segundo nivel y niveles superiores. Para obtener más información acerca de la gestión de certificados, consulte la *Guía de administración de Oracle ZFS Storage Appliance*.

Están disponibles las siguientes propiedades:

- **Requerir inicio de sesión de cliente**: los clientes deben autenticarse antes de que se permita el acceso a los recursos compartidos y son propietarios de los archivos que crean. Si no se configura, el propietario de los archivos creados será el servicio HTTP, con usuario "nobody" (nadie).
- **Protocolos**: seleccione los métodos de acceso que admiten HTTP, HTTPS o ambos.
- **Puerto HTTP (para conexiones entrantes)**: puerto HTTP; el puerto predeterminado es el 80.
- **Puerto HTTPS (para conexiones entrantes seguras)**: puerto HTTPS; el puerto predeterminado es el 443.

Si la opción Require client login (Requerir inicio de sesión de cliente) está activada, Oracle ZFS Storage Appliance denegará el acceso a los clientes que no proporcionen las credenciales

de autenticación válidas correspondientes a un usuario local, un usuario de NIS o un usuario de LDAP. No se admite la autenticación de Active Directory. Solo se admite la autenticación HTTP básica. A menos que se esté usando HTTPS, durante esta operación se transmiten el nombre de usuario y la contraseña sin cifrar, lo que puede no ser apropiado para todos los entornos. Si la opción Require client login (Requerir inicio de sesión de cliente) está desactivada, el dispositivo no intentará autenticar las credenciales.

Independientemente de la autenticación, no hay ningún permiso enmascarado en los archivos y los directorios creados. Los nuevos archivos creados tienen permisos de lectura y escritura para todos. Los nuevos archivos creados tienen permisos de lectura, escritura y ejecución para todos.

Servicio de datos NDMP

El protocolo simple de administración de redes (NDMP) permite que Oracle ZFS Storage Appliance participe en operaciones de copia de seguridad y restauración basadas en NDMP controladas por un cliente NDMP remoto denominado aplicación de gestión de datos (DMA). Con NDMP, los datos de usuario del dispositivo (es decir, los datos almacenados en recursos compartidos creados por el administrador en el dispositivo) se pueden incluir en copias de seguridad y se pueden restaurar tanto con dispositivos conectados localmente, como unidades de cinta, como con sistemas remotos. Los dispositivos conectados localmente también se pueden copiar y restaurar mediante DMA.

Servicio de datos de replicación remota

La replicación remota de Oracle ZFS Storage Appliance facilita la replicación de proyectos y recursos compartidos. Este servicio permite ver los dispositivos que han replicado datos en un dispositivo específico y controlar en qué dispositivos un dispositivo específico puede replicar.

Cuando se activa este servicio, el dispositivo recibe actualizaciones de replicación de otros dispositivos y envía actualizaciones de replicación para los proyectos y los recursos compartidos locales en función de las acciones que tenga configuradas. Cuando el servicio está desactivado, las actualizaciones de replicación entrantes fallan y no se replica ningún proyecto ni recurso compartido local.

Se requiere la contraseña de usuario root para el dispositivo remoto para configurar los destinos de replicación remota para el dispositivo. Estos destinos se usan para configurar una conexión de par de replicación que permite que los dispositivos se comuniquen.

Durante la creación de destinos, la contraseña de usuario root se usa para confirmar la autenticidad de la solicitud y producir e intercambiar claves de seguridad que se usarán para identificar los dispositivos en comunicaciones posteriores.

Las claves generadas se almacenan permanentemente como parte de la configuración del dispositivo. La contraseña de usuario root nunca se almacena de manera permanente ni se transmite sin cifrar. Todas las comunicaciones del dispositivo, incluido este intercambio de identidad inicial, se protegen con SSL.

La función de replicación fuera de línea del dispositivo Oracle ZFS Storage Appliance reduce el tiempo, los recursos y los errores potenciales de datos al replicar juegos de datos voluminosos mediante una red que tiene un ancho de banda limitado. Durante la replicación fuera de línea, el flujo de replicación se exporta a un archivo que está en un servidor NFS, el cual se puede transportar físicamente a la ubicación de destino remota o, de manera opcional, se puede copiar en un medio externo para su envío. En el sitio de destino, el administrador importa al dispositivo de destino el archivo que contiene el flujo de replicación.

Para limitar el acceso al flujo de replicación exportado, exponga el recurso compartido de NFS solo a la dirección IP de los dispositivos de origen y destino. Para cifrar los datos, active el cifrado en disco para el recurso compartido de NFS en el servidor NFS. Consulte la documentación del servidor NFS para obtener más información. Tenga en cuenta que el flujo de replicación exportado nunca es cifrado por el dispositivo.

Cómo trabajar con cifrado de datos

AVISO DE LICENCIAS: *La función de cifrado se puede evaluar sin cargo, pero para poder usarla en producción se debe adquirir una licencia independiente por separado. El cifrado solo está disponible para licencia en Oracle ZFS Storage ZS5-4, Oracle ZFS Storage ZS5-2, Oracle ZFS Storage ZS4-4 y Oracle ZFS Storage ZS3-4. Después del periodo de evaluación, se debe adquirir la licencia correspondiente para esta función o se la debe desactivar. Oracle se reserva el derecho de realizar auditorías en cualquier momento para controlar la existencia de las licencias necesarias. Para obtener información detallada, consulte "Acuerdo de licencia de software (SLA)" de Oracle y derecho de sistemas de hardware con opciones de software integrado".*

Oracle ZFS Storage Appliance ofrece cifrado transparente de los datos para recursos compartidos individuales (sistemas de archivos y LUN) y recursos compartidos creados dentro de proyectos.

Gestión de claves de cifrado

El dispositivo incluye un almacén de claves LOCAL integrado y la capacidad de conectarlo con el sistema Oracle Key Manager (OKM). Cada proyecto o recurso compartido cifrado requiere una clave de encapsulado del almacén de claves LOCAL o de OKM. Las claves de cifrado de datos se gestionan mediante el dispositivo de almacenamiento y se almacenan cifradas de forma persistente mediante la clave de encapsulado desde el almacén de claves LOCAL u OKM.

OKM es un sistema de gestión de claves (KMS) integral que aborda la necesidad creciente de cifrado de datos basado en almacenamiento que tienen las empresas. Desarrollada para cumplir con los estándares abiertos, esta función proporciona la capacidad, escalabilidad e interoperabilidad para gestionar centralmente las claves de cifrado en infraestructuras de almacenamiento ampliamente distribuidas y heterogéneas.

OKM aborda los desafíos únicos de la gestión de claves de almacenamiento, entre los que se incluyen los siguientes:

- **Retención de claves a largo plazo**: OKM garantiza que los datos archivados estén siempre disponibles y retiene de manera segura las claves de cifrado durante todo el ciclo de vida de los datos.
- **Interoperabilidad**: OKM proporciona la interoperabilidad necesaria para admitir una amplia variedad de dispositivos de almacenamiento conectados a plataformas de sistemas abiertos o mainframe en un único servicio de gestión de claves de almacenamiento.
- **Alta disponibilidad**: con agrupación en clusters de N nodos activa, el equilibro de carga dinámico y el failover automatizado, OKM proporciona alta disponibilidad, sin importar si los dispositivos están juntos o distribuidos por todo el mundo.
- **Alta capacidad**: OKM gestiona una gran cantidad de dispositivos de almacenamiento y una cantidad aún mayor de claves de almacenamiento. Un único dispositivo en cluster puede proporcionar servicios de gestión de claves para miles de dispositivos de almacenamiento y millones de claves de almacenamiento.
- **Configuración de clave flexible**: por cluster de OKM, las claves se pueden generar de forma automática o individualmente para un almacén de claves LOCAL o de OKM. Los administradores de seguridad son responsables de proporcionar los nombres de clave que, al combinarse con el almacén de claves, asocian una clave de ajuste con un proyecto o recurso compartido.

Mantenimiento de claves

Los recursos compartidos y los proyectos que usan claves OKM en estado desactivado permanecen accesibles. Para evitar que se use una clave OKM, el administrador de OKM debe suprimir explícitamente la clave.

Para garantizar que pueda accederse a los recursos compartidos y los proyectos cifrados, realice una copia de seguridad de las configuraciones y de los valores de claves del almacén de claves LOCAL del dispositivo. Si una clave se vuelve inaccesible, los proyectos o los recursos compartidos que usan esa clave se vuelven inaccesibles. Si la clave del proyecto no está disponible, no se pueden crear nuevos recursos compartidos en el proyecto.

Las claves se pueden volver no disponibles de las siguientes maneras:

- Se suprimen las claves.

- Se revierte la versión a una que no admite cifrado.
- Se revierte la versión a una que no tiene configuradas las claves.
- Se efectúa un restablecimiento de la configuración predeterminada.
- El servidor OKM no está disponible.

Ciclo de vida de clave de cifrado

El ciclo de vida de la clave de cifrado es flexible porque puede cambiar las claves en cualquier momento sin poner fuera de línea los servicios de datos.

Cuando se suprime una clave del almacén de claves, todos los recursos compartidos que la usan se desmontan y sus datos se vuelven inaccesibles. Las copias de seguridad de claves en el almacén de claves de OKM se deben realizar utilizando los servicios de copia de seguridad de OKM. Las copias de seguridad de claves en el almacén de claves LOCAL se incluyen como parte de la copia de seguridad de la configuración del sistema. Para el almacén de claves es LOCAL, también se puede proporcionar la clave por valor en el momento de la creación para permitir que sea custodiada en un sistema externo, lo cual proporciona una alternativa de copia de seguridad/restauración.

Servicio de datos de migración shadow

La migración shadow permite la migración de datos automática desde fuentes externas o internas, y controla la migración automática en segundo plano. Independientemente de si el servicio está activado o no, los datos se migrarán sincrónicamente para solicitudes en banda. La finalidad principal de este servicio consiste en permitir el ajuste de la cantidad de subprocesos dedicados a la migración en segundo plano.

Los montajes NFS en una fuente NFS no están bajo el control del usuario de Oracle ZFS Storage Appliance. No se pueden asegurar los montajes de migración shadow; por lo tanto, si el servidor espera una solicitud Kerberos o similar, el montaje de origen se rechaza.

Servicio de datos SFTP

El protocolo de transferencia de archivos SSH (SFTP) permite tener acceso al sistema de archivos desde clientes SFTP. Los inicios de sesión anónimos no se permiten, y, por lo tanto, los usuarios deben autenticarse con el servicio de nombres configurado.

Al crear una clave SFTP, debe incluir la propiedad "user" (usuario) con una asignación de usuario válida. Las claves SFTP se agrupan por usuario y se autentican mediante SFTP con el nombre del usuario.

Nota - Por motivos de seguridad, aunque se autenticarán, debe volver a crear las claves SFTP existentes que no incluyan la propiedad de usuario.

Servicio de datos TFTP

El protocolo trivial de transferencia de archivos (TFTP) es un protocolo simple para transferir archivos. Está diseñado para ser pequeño y fácil de implementar; por lo tanto, carece de la mayoría de las funciones de seguridad de un FTP. TFTP únicamente lee y escribe archivos desde/hacia un servidor remoto. No puede mostrar directorios y, en la actualidad, no ofrece la autenticación de usuarios.

Red de área de almacenamiento

En una red de área de almacenamiento (SAN), los grupos de destinos e iniciadores definen conjuntos de destinos e iniciadores que se pueden asociar con un número de unidad lógica (LUN). Solo puede accederse a un LUN asociado con un grupo de destinos mediante esos destinos del grupo. Solo puede accederse a un LUN asociado con un grupo de iniciadores mediante esos iniciadores del grupo. Los grupos de iniciadores y destinos se aplican a un LUN cuando crea un LUN. La creación de un LUN no se puede completar correctamente sin definir por lo menos un grupo de destinos y un grupo de iniciadores.

Aparte del protocolo de autenticación por desafío mutuo (CHAP), que puede seleccionarse solo para el acceso de iniciador iSCSI/iSER, no se realiza ninguna otra autenticación.

Nota - El uso del grupo de iniciadores predeterminado tiene como consecuencia iniciadores LUN no deseados o en conflicto.

Servicios de directorio

En esta sección, se describen los servicios de directorio que se pueden configurar en el dispositivo y sus ramificaciones de seguridad.

Servicio de información de red

El servicio de información de red (NIS) es un servicio de nombres para la gestión de directorio centralizada. Oracle ZFS Storage Appliance puede actuar como cliente NIS de usuarios y

grupos para que los usuarios de NIS puedan iniciar sesión en FTP y HTTP/WebDAV. Los usuarios de NIS también pueden recibir privilegios para la administración del dispositivo. El dispositivo complementa la información de NIS con su propia configuración de privilegios.

Protocolo ligero de acceso a directorios

Oracle ZFS Storage Appliance usa el protocolo ligero de acceso a directorios (LDAP) para autenticar usuarios administrativos y algunos usuarios de servicios de datos (FTP, HTTP). El dispositivo admite seguridad LDAP sobre SSL. LDAP se usa para recuperar información acerca de usuarios y grupos, y se usa de las siguientes maneras:

- Proporciona interfaces de usuario que aceptan y muestran nombres para usuarios y grupos.
- Asigna nombres a usuarios y grupos, y desde ellos, para protocolos de datos, como NFSv4, que usan nombres.
- Define la pertenencia al grupo para usarla en el control de acceso.
- Opcionalmente, transporta datos de autenticación usados para la autenticación de acceso de datos y administrativa.

Las conexiones LDAP pueden usarse como mecanismo de autenticación. Por ejemplo, cuando un usuario intenta realizar la autenticación con Oracle ZFS Storage Appliance, el dispositivo puede intentar realizar la autenticación con el servidor LDAP como ese usuario como un mecanismo para verificar la autenticación.

Existen una variedad de controles para la seguridad de la conexión de LDAP:

- Autenticación de dispositivo a servidor:
  - El dispositivo es anónimo.
  - El dispositivo realiza la autenticación usando las credenciales de Kerberos del usuario.
  - El dispositivo realiza la autenticación usando el usuario y la contraseña "proxy" especificados.
- Autenticación de servidor a dispositivo (garantiza que se haya contactado el servidor correcto):
  - No es segura.
  - El servidor se autentica usando Kerberos.
  - El servidor se autentica usando un certificado TLS.

Los datos transportados mediante una conexión LDAP se cifran si se usa Kerberos o TLS; de lo contrario, no se cifran. Cuando se usa TLS, la primera conexión en el tiempo de configuración no es segura. El certificado del servidor se recopila en ese momento y se usa para realizar la autenticación de conexiones de producción posteriores.

No es posible importar un certificado de autoridad de certificación para que se use a fin de realizar la autenticación de varios servidores LDAP ni importar un certificado de servidor LDAP particular manualmente.

Solo se admite TLS (LDAPS) sin procesar. Las conexiones STARTTLS, que comienzan con una conexión LDAP no segura y luego pasan a una conexión segura, no se admiten. Los servidores LDAP que requieren un certificado de cliente no se admiten.

Asignación de identidad

Los clientes pueden acceder a recursos de archivos en Oracle ZFS Storage Appliance mediante el uso de SMB o NFS, y cada uno tiene un identificador único de usuario. Los usuarios de SMB/Windows tienen descriptores de seguridad (SID) y los usuarios de UNIX/Linux tienen ID de usuario (UID). Los usuarios también pueden ser miembros de grupos que se identifican con SID de grupo para usuarios de Windows o ID de grupo (GID) para usuarios de UNIX/Linux.

En entornos en los que se accede a recursos de archivos con ambos protocolos, suele preferirse establecer equivalencias de identidad, donde, por ejemplo, un usuario de UNIX es equivalente a un usuario de Active Directory. Esto es importante para determinar derechos de acceso en los recursos de archivos del dispositivo.

Existen distintos tipos de asignaciones de identidad que involucran servicios de directorio, como Active Directory, LDAP y NIS. Debe tener cuidado y seguir las mejores prácticas de seguridad para el servicio de directorio que se utilice.

Gestión de identidades para UNIX

Microsoft ofrece una función denominada Gestión de identidades para Unix (IDMU). Este software está disponible para Windows Server 2003 y viene incluido con Windows Server 2003 R2 y versiones posteriores. Esta característica forma parte de lo que se denominaba Servicios para Unix en su forma independiente.

El uso principal de IDMU es permitir el uso de Windows como servidor NIS/NFS. IDMU permite al administrador especificar una serie de parámetros relacionados con UNIX: UID, GID, shell de inicio de sesión, directorio principal y similares para grupos. Estos parámetros están disponibles con AD mediante un esquema similar (pero no igual) al de RFC 2307 y mediante el servicio NIS.

Cuando se usa el modo de asignación IDMU, el servicio de asignación de identidad usa estos atributos de UNIX para establecer asignaciones entre identidades de Windows y UNIX. Este enfoque es muy similar al de la asignación basada en directorios, con la diferencia de que el

servicio de asignación de identidad consulta el esquema de propiedades establecido por el software IDMU en lugar de permitir un esquema personalizado. Cuando se utiliza este enfoque, no se puede utilizar ningún otro método de asignación basada en directorios.

Asignación basada en directorios

La asignación basada en directorios implica la anotación de un objeto de LDAP o Active Directory con información acerca de la manera en la que la identidad del objeto se asigna a una identidad equivalente en la plataforma opuesta. Estos atributos adicionales asociados con el objeto se deben configurar.

Asignación basada en nombres

La asignación basada en nombres requiere la creación de diversas reglas que asignan identidades por nombre. Estas reglas establecen equivalencias entre identidades de Windows e identidades de UNIX.

Asignación efímera

Si una regla de asignación basada en nombres no puede aplicarse a un usuario en particular, ese usuario recibe credenciales temporales mediante una asignación efímera, a menos que esté bloqueado por una asignación de denegación. Cuando un usuario de Windows que tiene un nombre de UNIX efímero crea un archivo en el sistema, los clientes de Windows que acceden al archivo mediante SMB ven que el propietario de ese archivo es la identidad de Windows. Sin embargo, los clientes NFS ven que el archivo es propiedad de "nobody" (nadie).

Configuración del sistema

En las siguientes secciones, se describe la configuración de seguridad disponible del sistema.

Asistencia técnica remota

El servicio de asistencia técnica remota se usa para gestionar el registro de Oracle ZFS Storage Appliance y el servicio de asistencia técnica remota. En estos mensajes, no se transmiten metadatos ni datos de usuario.

La operación de registro conecta Oracle ZFS Storage Appliance con el portal de inventario de Oracle, que le permite gestionar su equipo de Oracle. El registro es un requisito para poder usar el servicio de asistencia técnica remota.

El servicio de asistencia técnica remota se comunica con el servicio de asistencia técnica de Oracle para proporcionar lo siguiente:

- **Informe de fallos**: el sistema informa los problemas activos a Oracle para generar una respuesta de servicio automatizada. En función de la naturaleza del fallo, se puede abrir un caso de asistencia técnica.
- **Latidos**: se envían mensajes diarios de latidos a Oracle para indicar que el sistema esté en funcionamiento. El servicio de asistencia técnica de Oracle puede notificar al contacto técnico de una cuenta cuando uno de los sistemas activados tarda mucho en enviar un latido.
- **Configuración del sistema**: se envían mensajes periódicos a Oracle en los que se describen la configuración y las versiones actuales de software y hardware, y la configuración del almacenamiento.

Etiquetas de servicio

Las etiquetas de servicio se usan para facilitar el inventario de productos y la asistencia técnica permitiendo que se hagan consultas de datos a Oracle ZFS Storage Appliance, por ejemplo:

- Número de serie del sistema
- Tipo de sistema
- Números de versión de software

Puede registrar las etiquetas de servicio con el servicio de asistencia técnica de Oracle, lo que le permite llevar un control de sus equipos de Oracle con facilidad y acelerar las llamadas de servicio. Las etiquetas de servicio están activadas de forma predeterminada.

Servicio Kerberos

El servicio Kerberos ofrece autenticación para el inicio de sesión administrativo del dispositivo y acceso a esos servicios como NFS, HTTP, FTP, SFTP y SSH cuando se usan en combinación con un entorno de Kerberos. Los usuarios del dispositivo deben tener un principal de Kerberos con el mismo nombre para poder usar la autenticación de Kerberos para estos servicios. Kerberos también se puede usar para configurar valores de seguridad para recursos compartidos individuales que usan el protocolo NFS, como se describe en “Opciones de cifrado y autenticación de NFS” [15].

Tanto Kerberos como Active Directory pueden estar activos al mismo tiempo porque tienen reinos y claves diferentes. Cuando ambos están activos, el reino Kerberos es el que se usa por defecto. Cuando solo está activo Active Directory, su reino es el que se usa por defecto.

Protocolo simple de transferencia de correo

El protocolo de simple transferencia de correo (SMTP) envía todos los mensajes generados por Oracle ZFS Storage Appliance, normalmente en respuesta a alertas configuradas. SMTP no acepta correo externo, solo envía correo generado automáticamente por el dispositivo.

Por defecto, el servicio SMTP usa DNS (registros MX) para determinar dónde se deben enviar los mensajes. Si el DNS no está configurado para el dominio del dispositivo o si el dominio de destino para correo saliente no tiene bien configurados los registros MX de DNS, el dispositivo se puede configurar para que reenvíe todos los mensajes de correo mediante un servidor de correo saliente.

Protocolo simple de administración de redes

El protocolo simple de administración de redes (SNMP) proporciona dos funciones en Oracle ZFS Storage Appliance: la información de estado del dispositivo puede ser proporcionada mediante SNMP, y las alertas pueden configurarse para enviar capturas SNMP. Cuando este servicio está activado, las versiones v1, v2c y v3 de SNMP están disponibles. El dispositivo admite un máximo de 128 interfaces de red físicas y lógicas.

Mensaje de Syslog

Un mensaje de Syslog es un mensaje de evento pequeño transmitido de Oracle ZFS Storage Appliance a uno o varios sistemas remotos. Syslog proporciona dos funciones del dispositivo:

- Se pueden configurar alertas para enviar mensajes de Syslog a uno o varios sistemas remotos.
- En el caso de los servicios del dispositivo capaces de utilizar Syslog, se pueden reenviar sus propios mensajes de Syslog a sistemas remotos.

El Syslog se puede configurar para utilizar el formato de salida clásico descrito por RFC 3164 o el formato de salida con versión más nuevo descrito por RFC 5424. Los mensajes de Syslog se transmiten como datagramas de UDP. Por lo tanto, es posible que sean rechazados por la red o que no puedan ser enviados si el sistema de envío no tiene suficiente memoria o la red está

suficientemente congestionada. Por consiguiente, los administradores deben asumir que, en caso de fallos complejos en la red, es posible que se pierdan o se rechacen algunos mensajes.

El mensaje contiene los siguientes elementos:

- Una utilidad que describe el tipo del componente del sistema que emitió el mensaje.
- Una gravedad que describe la gravedad de la condición relacionada con el mensaje.
- Un registro de hora que describe la hora del evento asociado en UTC.
- Un nombre de host que describe el nombre canónico del dispositivo.
- Una etiqueta que describe el nombre del componente del sistema que emitió el mensaje.
- Un mensaje que describe el evento en sí mismo.

Identidad de sistema

Este servicio permite configurar el nombre y la ubicación del sistema. Es posible que se deba cambiar el nombre y la ubicación del sistema si se traslada Oracle ZFS Storage Appliance a otra ubicación de la red o se cambia el fin para el que se utiliza.

Limpieza de discos

La limpieza de discos debe realizarse de manera regular para permitir que Oracle ZFS Storage Appliance detecte y corrija los datos dañados en el disco. La limpieza de disco es un proceso en segundo plano que lee los discos durante períodos de tiempo en espera a fin de detectar errores de lectura irremediables en sectores de acceso poco frecuente. La detección oportuna de esos errores en sectores latentes es importante para reducir la pérdida de datos.

Impedimento de destrucción

Cuando está activada la característica Prevent Destruction (Impedir destrucción), el recurso compartido o proyecto no se pueden destruir. Esto incluye destruir un recurso compartido mediante clones dependientes, destruir un recurso compartido dentro de un proyecto o destruir un paquete de replicación. Sin embargo, esta característica no afecta los recursos compartidos destruidos mediante actualizaciones de replicación. Si se destruye un recurso compartido en un dispositivo Oracle ZFS Storage Appliance que es el origen de la replicación, se destruirá el recurso compartido correspondiente en el destino, incluso si está configurada esta propiedad.

Para destruir el recurso compartido, primero se debe desactivar la propiedad de manera explícita como un paso aparte. Esta propiedad está desactivada de forma predeterminada.

Logs de seguridad

En esta sección, se describe la característica de logs relacionada con la seguridad.

Log de auditoría

El log de auditoría muestra los eventos de actividad de usuario, como el inicio y cierre de sesión en la BUI y la CLI, y acciones administrativas. En la siguiente tabla, se muestran ejemplos de entradas del log de auditoría como aparecen en la BUI.

TABLA 2 Registro de log de auditoría

Fecha y hora	Usuario	Host	Resumen	Anotación de sesión
2013-10-12 05:20:24	root	galaxy	Disabled ftp service	
2013-10-12 03:17:05	root	galaxy	User logged in	
2013-10-11 22:38:56	root	galaxy	Browser session timed out	
2013-10-11 21:13:35	root	<console>	Enabled ftp service	

Log del servicio de asistencia técnica remota

Si se utiliza el servicio de asistencia técnica remota, el log mostrará los eventos de comunicación con la asistencia técnica de Oracle. En la siguiente tabla, se muestra un ejemplo de entrada de la asistencia técnica remota como aparece en la BUI.

TABLA 3 Registro de log de asistencia técnica remota

Fecha y hora	Descripción	Resultado
2013-10-12 05:24:09	Uploaded file 'cores/ak.45e5ddd1-ce92-c16e-b5eb-9cb2a8091f1c.tar.gz' to Oracle support	OK (Correcto)

Información adicional

Puede encontrar la información completa del producto de Oracle ZFS Storage Appliance en la siguiente ubicación:

https://docs.oracle.com

Cuando utiliza la BUI para configurar el dispositivo Oracle ZFS Storage Appliance, puede hacer clic en el enlace de ayuda que aparece en la parte superior derecha de cualquier pantalla para mostrar la ayuda de esa pantalla.