Guía de seguridad de Oracle® ZFS Storage Appliance

ORACLE®

Descripción general de la 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 (ZFSSA). Para conocer los procedimientos de configuración del dispositivo, consulte la guía de administración del sistema de Oracle ZFS Storage Appliance.

Las siguientes secciones brindan una descripción de las características de seguridad del dispositivo ZFSSA:

- **Instalación inicial**: Describe cómo configurar el acceso administrativo, cómo establecer la cuenta root y los efectos del restablecimiento de fábrica del dispositivo ZFSSA.
- **Seguridad física**: Describe el entorno de seguridad física para el dispositivo ZFSSA.
- **Modelo administrativo**: Describe cómo restringir el acceso a la CLI y la BUI, 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 ZFSSA**: Describe los roles administrativos, quién puede administrar el dispositivo ZFSSA y la gestión de autorizaciones de usuario.
- **Listas de control de acceso (ACL)**: Describe el mecanismo que autoriza o deniega el acceso a archivos y directorios.
- **Red de área de almacenamiento (SAN)**: Describe los números de unidad lógica (LUN) y los grupos de iniciadores asociados, al igual que las opciones de autenticación de iniciadores y los valores predeterminados.
- **Servicios de datos**: Describe los servicios de datos que admite el dispositivo ZFSSA 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 ZFSSA y sus ramificaciones de seguridad.
- **Ajustes del sistema**: Describe la configuración del sistema, la asistencia técnica remota, las etiquetas de servicio, SMTP, SNMP, Syslog, la identidad del sistema, el limpiado de discos y la destrucción preventiva.
- **Acceso administrativo remoto**: Describe el acceso remoto mediante la BUI y la CLI.
- **Logs**: Describe los tipos de log que son pertinentes a la seguridad.

Instalación inicial

El dispositivo ZFSSA se entrega a los clientes con el software de ZFSSA 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 el dispositivo ZFSSA se restablece a los valores de fábrica, la contraseña root también se restablece al valor predeterminado en el dispositivo ZFSSA y en el procesador de servicio.

Durante la instalación inicial de un dispositivo ZFSSA, 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 ZFSSA, donde luego debe realizar los pasos de instalación inicial del sistema. Uno de los pasos requeridos es configurar una nueva contraseña administrativa del dispositivo ZFSSA, 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.

El dispositivo ZFSSA se ha concebido para un acceso restringido y, por lo tanto, éste se controla mediante mecanismos de seguridad (p. ej., acceso con clave, bloqueo, herramienta y tarjeta de identificación). Las personas con acceso autorizado están al corriente de los motivos de esta restricción y de las precauciones que se deben tomar.

Modelo administrativo

En esta sección, se describen los modelos administrativos del dispositivo ZFSSA.

Acceso restringido (CLI y BUI)

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

La administración es llevada a cabo mediante un inicio de sesión de línea de comandos de capa de conexión segura (SSL) o una sesión de explorador de HTTP segura (HTTPS). Las sesiones HTTPS están cifradas con un certificado de firma automática que se genera de manera exclusiva para cada dispositivo ZFSSA 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.

Actualizaciones del sistema

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 es parte de una actualización del sistema 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 o ninguna de las actualizaciones. Después de aplicar una actualización, no puede anularla y volver a una versión anterior del software del sistema.

Paquetes de asistencia

Cuando 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; sólo se envía información de configuración.

Copia de seguridad de la configuración

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

Usuarios de dispositivos ZFSSA

Existen dos tipos de usuarios de ZFSSA.

- **Usuarios de servicios de datos**: Clientes que acceden a los recursos de archivo y bloqueo mediante los protocolos admitidos, como NFS, SMB, canal de fibra, iSCSI, http y FTP.
- **Usuarios administrativos**: Usuarios que gestionarán la configuración y los servicios en el dispositivo ZFSSA. Esta sección sólo se aplica a los usuarios administrativos.

Roles del usuario administrativo

Los administradores pueden obtener privilegios si se les asignan 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 la cuenta se guarda en el dispositivo ZFSSA.
- 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 ZFSSA. Esto permite que los usuarios existentes de NIS/LDAP inicien sesión y administren el dispositivo ZFSSA, pero que los usuarios existentes de NIS/LDAP no puedan iniciar sesión en el dispositivo ZFSSA de forma predeterminada. Debe otorgarse acceso al dispositivo ZFSSA explícitamente.

Ámbitos administrativos

Las autorizaciones permiten a los usuarios realizar tareas específicas, por ejemplo, crear recursos compartidos, reiniciar el dispositivo ZFSSA y actualizar el software del sistema. Los grupos de autorizaciones se denominan ámbitos. Cada ámbito puede tener un conjunto 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 que la autorización permita reiniciar el servicio HTTP solamente.

Listas de Control de Acceso (ACL)

El dispositivo ZFSSA proporciona control de acceso a archivos mediante listas de control de acceso (ACL). Una lista de control de acceso es un mecanismo que permite o deniega el acceso a un archivo o directorio en particular.

El modelo de ACL proporcionado por el dispositivo ZFSSA se basa en el modelo de ACL de NFSv4 que deriva de la semántica de ACL de Windows. Es un modelo ACL enriquecido que proporciona acceso granular a los archivos y directorios. Cada archivo y directorio dentro del dispositivo de almacenamiento ZFSSA 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). 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 utilizados.

Herencia de ACL

Las ACL de NFSv4 permiten que las ACE sean heredades por los archivos y 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 hacia 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 sólo 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.

Red de área de almacenamiento (SAN)

En una SAN, los grupos de destinos e iniciadores definen conjuntos de destinos e iniciadores que se pueden asociar con un número de unidad lógica (LUN). Sólo puede accederse a un LUN asociado con un grupo

de destinos mediante esos destinos del grupo. Sólo 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 sólo para el acceso de iniciador iSCSI/iSER, no se realiza ninguna otra autenticación.

NOTA: El uso del grupo de iniciadores predeterminado puede generar una exposición de los LUN a iniciadores no deseados o en conflicto.

Servicios 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
FTP	Acceso al sistema de archivos mediante el protocolo FTP	21
HTTP	Acceso al sistema de archivos mediante el protocolo HTTP	80
Protocolo de administración de datos de redes (NDMP)	Servicio de host NDMP	10000
Replicación remota	Replicación remota	216
Migración shadow	Migración shadow de datos	
SFTP	Acceso al sistema de archivos mediante el protocolo SFTP	218
SRP	Acceso de bloque mediante el protocolo SRP	
TFTP (servidor TFTP)	Acceso al sistema de archivos mediante el protocolo TFTP	
Análisis de virus	Análisis de virus del sistema de archivos	

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 GRE (Generic Routing Encapsulation, encapsulado de enrutamiento genérico). De esta manera, el tráfico circula por las interfaces de back end y se evita el firewall, que podría ralentizar el tráfico. 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 también debe estar abierto.

Opciones de cifrado y autenticación de NFS

De forma predeterminada, 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 UID y el 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 y, 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 están 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 deben 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.

iSCSI

Al configurar un LUN en el dispositivo ZFSSA, puede exportar ese volumen por medio de un destino de interfaz estándar de equipos pequeños de Internet (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 CHAP. Asimismo, el servicio admite la gestión de datos de autenticación de CHAP en una base de datos 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

El servicio de autenticación remota telefónica de usuario (RADIUS) es un sistema para usar un servidor centralizado a fin de realizar la autenticación de 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 el dispositivo ZFSSA realice autenticación de CHAP con RADIUS, los siguientes parámetros deben coincidir:

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

Bloque de mensajes de servidor (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:

- **Restrict Anonymous Access to share list** (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.
- **SMB Signing Enabled** (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.
- **SMB Signing Required** (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 se encuentra desactivada de forma predeterminada.
- **Enable Access-based Enumeration** (Activar enumeración basada en acceso): Si se configura esta opción, se filtran las entradas del directorio en función de las credenciales del cliente. Cuando el cliente no tiene acceso a un archivo o directorio, ese archivo no se incluye en la lista de entradas devueltas al cliente. Esta opción está desactivada de forma predeterminada.

Autenticación de modo de dominio de Active Directory (AD)

En el modo de dominio, los usuarios se definen en Active Directory. Los clientes SMB pueden conectarse a ZFSSA mediante Kerberos o autenticación NTLM.

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

Cuando un cliente SMB usa autenticación NTLM para conectarse al dispositivo ZFSSA, 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 a ZFSSA mediante un nombre de host completo. Para obtener más información, consulte este artículo de MSDN: 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 ZFSSA. Cuando un cliente SMB se conecta a un dispositivo ZFSSA en el modo de grupo de trabajo, el nombre de usuario de ese usuario y su 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 ZFSSA está en el modo de grupo de trabajo.

La siguiente lista muestra el comportamiento del dispositivo ZFSSA 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 autenticación NTLMv2 únicamente

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 ZFSSA 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 (MMC)

Para garantizar que sólo los usuarios apropiados tengan acceso a las operaciones administrativas, existen algunas restricciones de acceso para las operaciones que se realizan de manera remota mediante MMC.

La siguiente lista muestra los usuarios y sus operaciones permitidas:

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

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 el dispositivo ZFSSA contacta. El motor externo no está incluido en el software de ZFSSA.

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 detecten tan rápido como con el cliente SMB.

Activación del motor de retraso para prevenir ataques de temporización

SMB no implementa ningún motor de retraso para evitar los ataques de temporización. Se basa en el entorno criptográfico de 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.

Protocolo de transferencia de archivos (FTP)

FTP permite el acceso al sistema de archivo 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 para los que se permite el acceso de protocolo FTP:

- Enable SSL/TLS (Activar SSL/TLS): Permite las conexiones de FTP cifradas SSL/TLS y se asegura de que la transacción de FTP esté cifrada. De forma predeterminada, esta opción está desactivada.
- Permit root login (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 es de texto sin formato, lo que representa un riesgo de seguridad por ataques de examen de red.
- Maximum number of allowable login attempts (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.
- Logging level (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.

Protocolo de transferencia de hipertexto (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 que los clientes accedan a sistemas de archivos compartidos mediante un explorador web o un sistema de archivos local si el software del cliente lo admite. El servidor HTTPS utiliza un certificado de seguridad de firma automática.

Están disponibles las siguientes propiedades:

- Require client login (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 creen. Si no se define esta opción, el propietario de los archivos creados será el servicio HTTP, con usuario "nobody" (nadie).
- Protocols (Protocolos): Seleccione los métodos de acceso que admiten HTTP, HTTPS o ambos.
- HTTP Port (for incoming connections) (Puerto HTTP [para conexiones entrantes]): Puerto HTTP, el puerto predeterminado es el 80.
- HTTPS Port (for incoming secure connections) (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, el dispositivo 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. Sólo 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, ZFSSA no intentar realizar la autenticación.

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.

Protocolo de gestión de datos de red (NDMP)

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

Replicación remota

La replicación remota de ZFSSA facilita la replicación de proyectos y recursos compartidos. Este servicio permite ver dispositivos ZFSSA que han replicados datos en este ZFSSA y configurar los ZFSSA a los que este ZFSSA se puede replicar.

Cuando se activa este servicio, el dispositivo ZFSSA recibe actualizaciones de replicación de otros ZFSSA 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 root para el dispositivo ZFSSA remoto para configurar los destinos de replicación remota para ZFSSA. Estos destinos se usan para configurar una conexión de par de replicación que permite que los dispositivos ZFSSA se comuniquen.

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

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

Migración shadow

La migración shadow permite la migración de datos automáticos de 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.

NFS se monta en un origen NFS y no están bajo el control del usuario de ZFSSA. La migración shadow no se puede asegurar y, por lo tanto, si el servidor espera una solicitud Kerberos o similar, el montaje de origen se rechaza.

Protocolo de transferencia de archivo SSH (SFTP)

SFTP permite el acceso de sistema de archivos de 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.

Protocolo trivial de transferencia de archivos (TFTP)

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 un FTP regular. 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.

Servicios de directorio

Servicio de información de red (NIS)

NIS es un servicio de nombre para la gestión de directorio centralizada. El dispositivo ZFSSA puede actuar como un cliente NIS para los usuarios y los grupos de modo que los usuarios NIS pueden iniciar sesión en el FTP y HTTP/WebDAV. Los usuarios de NIS también puedan recibir privilegios para la administración de ZFSSA. El dispositivo ZFSSA complementa la información de NIS con su propia configuración de privilegios.

Protocolo ligero de acceso a directorios (LDAP)

El dispositivo ZFSSA usa LDAP para autenticar usuarios administrativos y algunos servicios de datos de usuarios (ftp, http). El dispositivo ZFSSA 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 hacia y desde usuarios y grupos para protocolos de datos, como NFSv4, que usan nombres.
- Define la pertenencia a los grupos para usar en el control de acceso.
- Opcionalmente, para realizar la autenticación de datos usados para 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 el dispositivo ZFSSA, el dispositivo ZFSSA 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 credenciales de Kerberos
  - El dispositivo realiza la autenticación usando el usuario y la contraseña "proxy" especificados
- Autenticación de dispositivo a servidor (se asegura de que se haya contactado el servidor correcto):
  1. Sin seguridad
  2. El servidor se autentica usando Kerberos
  3. El servidor se autentica usando un certificado TLS

Los datos transportados mediante una conexión LDAP se cifran si Kerberos o TLS se usan, pero, 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 Certificate Authority para que se use a fin de realizar la autenticación de varios servidores LDAP; tampoco se puede importar un certificado de servidor LDAP manualmente.

Sólo 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 ZFSSA usando SMB o NFS, y cada uno tiene un identificador de usuario único. Los usuarios de SMB/Windows tienen descriptores de seguridad (SID) y los usuarios 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, el uso de ambos protocolos es a menudo deseable para establecer las equivalencias de identidad donde, por ejemplo, un usuario UNIX es equivalente a un usuario de Active Directory. Esto es importante para determinar los derechos de acceso en los recursos de archivos del dispositivo ZFSSA.

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

IDMU

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 posteriores. Esta característica es parte de lo que se denomina Servicios para Unix en su forma independiente.

El uso principal de IDMU es permitir el uso de Windows como servidor NIS/NFS. IDMU permite que el administrador especifique una cantidad de parámetros relacionados con UNIX: UID, GID, shell de inicio de sesión, directorio raíz y similares para grupos. Estos parámetros están disponibles por medio de AD mediante un esquema similar (pero no igual) al de RFC2307 y por medio del 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 no hay ninguna regla de asignación basada en nombres que pueda 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

La pantalla del servicio de Asistencia técnica remota se usa para gestionar el registro de ZFSSA y el servicio de asistencia técnica remota. En estos mensajes, no se transmiten metadatos ni datos de usuario.

- La operación de registro conecta el dispositivo ZFSSA 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 está encendido y 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 las versiones actuales de software y hardware, la configuración del dispositivo y la configuración del almacenamiento.

Etiquetas de servicio

Las etiquetas de servicio se usan para facilitar el inventario de productos y la asistencia técnica. Estas etiquetas permiten que se hagan consultas de datos del dispositivo ZFSSA, 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 Oracle con facilidad, además de acelerar las llamadas de servicio. Las etiquetas de servicio están activadas de forma predeterminada.

SMTP

SMTP envía todos los correos electrónicos generados por el dispositivo ZFSSA, en general como respuesta a las alertas según se configuren. SMTP no acepta correo externo, sólo envía correo generado automáticamente por ZFSSA.

De forma predeterminada, 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 ZFSSA o si el dominio de destino para correo saliente no tiene bien configurados los registros MX de DNS, el dispositivo ZFSSA se puede configurar para que reenvíe todos los mensajes de correo mediante un servidor de correo saliente.

Protocolo simple de administración de redes (SNMP)

SNMP brinda dos funciones en el dispositivo ZFSSA; la información de estado del ZFSSA puede servirse mediante SNMP y las alertas pueden configurarse para enviar trampas SNMP. Están disponibles las dos versiones de SNMP: 1 y 2c.

Syslog

Un mensaje de Syslog es un mensaje de evento pequeño desde el dispositivo ZFSSA a uno o más sistemas remotos. Syslog proporciona dos funciones del ZFSSA:

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

El Syslog se puede configurar para utilizar el formato de salida clásico descripto por RFC 3164, o el formato de salida nuevo, con versión, descripto por RFC 5424. Los mensajes 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 envíos no tiene suficiente memoria o la red está suficientemente congestionada. Por consiguiente, los administradores deben asumir que, en caso de fallas complejas 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 ZFSSA.
- Una etiqueta que describe el nombre del componente del sistema que emitió el mensaje.
- Un mensaje que describe el evento en sí mismo.

Identidad del sistema

Este servicio permite configurar el nombre y la ubicación del sistema. Si el dispositivo ZFSSA se traslada a otra ubicación de la red o se cambia el fin para el que se utiliza, es posible que sea necesario cambiar estos valores.

Limpieza de discos

La limpieza de discos debe realizarse de manera regular para permitir que el dispositivo ZFSSA 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 ZFSSA que es la fuente de 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.

Acceso administrativo remoto

En esta sección, se describe la seguridad de acceso remoto del dispositivo ZFSSA.

Interfaz de usuario basada en explorador (BUI)

Las pantallas de servicios de la BUI se utilizan para ver y modificar los servicios y los parámetros de configuración de acceso remoto.

Shell seguro (SSH)

SSH permite que los usuarios inicien sesión en el dispositivo ZFSSA mediante la interfaz de línea de comandos (CLI) y realizar la mayoría de las mismas acciones administrativas que pueden realizarse en la BUI. 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.

Logs

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

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

Hora	Usuario	Host	Resumen	Anotación de sesión
2009-10-12 05:20:24	root	galaxy	Disabled ftp service	

Hora	Usuario	Host	Resumen	Anotación de sesión
2009-10-12 3:17:05	root	galaxy	User logged in	
11/10/2009 22:38:56	root	galaxy	Browser session timed out	
11/10/2009 21:13:35	root	<console>	Enabled ftp service	

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

Hora	Descripción	Resultado
2009-10-12 5:24:09	Uploaded file 'cores/ak.45e5ddd1-ce92-c16e-b5eb-9cb2a8091f1c.tar.gz' to Oracle support	OK

Más información

Puede encontrar ayuda en línea específica del contexto para cada página de la interfaz de usuario basada en explorador (BUI) del dispositivo ZFSSA si hace clic en el botón de Ayuda ubicado en la parte superior izquierda de cada página.

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

www.oracle.com/us/products/servers-storage/storage/nas/overview

Asignación de documentación

Use las tablas a continuación para ubicar la documentación detallada para cada uno de los servicios, las configuraciones u otras características en el dispositivo ZFSSA. Cuando utiliza la BUI para configurar un dispositivo ZFSSA, puede hacer clic en el enlace de ayuda en la parte superior derecha de la pantalla para mostrar la ayuda para esa pantalla.

TABLA 4 Servicios

Servicio	Ubicación de la documentación
Active Directory	Servicios:Active_Directory
Asignación de identidad	Servicios:Identity_Mapping
DNS	Servicios:DNS
Enrutamiento dinámico	Servicios:Dynamic_Routing
IPMP	Servicios:IPMP
NTP	Servicios:NTP

Servicio	Ubicación de la documentación
Asistencia técnica remota	Servicios:Phone_Home
Etiquetas de servicio	Servicios:Service_Tags
SMTP	Servicios:SMTP
SNMP	Servicios:SNMP
Syslog	Servicios:Syslog
Identidad del sistema	Servicios:System_Identity
SSH	Servicios:SSH

TABLA 5 Configuración

Configuración	Ubicación de la documentación
SAN	Configuración:SAN
SAN:FC	Configuración:SAN:FC
SAN:iSCSI	Configuración:SAN:iSCSI
SAN:SRP	Configuración:SAN:SRP
Cluster	Configuración:Cluster
Usuarios	Configuración:Usuarios
Preferencias	Configuración:Preferencias
Alertas	Configuración:Alertas
Almacenamiento	Configuración:Almacenamiento

TABLA 6 Almacenamiento

Almacenamiento	Ubicación de la documentación
Recursos compartidos	Recursos compartidos
Conceptos	Recursos compartidos:Conceptos
Shadow_Migration	Recursos compartidos:Shadow_Migration
Space_Management	Recursos compartidos:Space_Management
Archivo system_Namespace	Recursos compartidos:Archivo system_Namespace
Recursos compartidos	Recursos compartidos:Recursos compartidos
General	Recursos compartidos:Recursos compartidos:General
Protocolos	Recursos compartidos:Recursos compartidos:Protocolos
Acceso	Recursos compartidos:Recursos compartidos:Acceso
Instantáneas	Recursos compartidos:Recursos compartidos:Instantáneas
Proyectos	Recursos compartidos:Proyectos
Proyectos:General	Recursos compartidos:Proyectos:General
Proyectos:Protocolos	Recursos compartidos:Proyectos:Protocolos
Proyectos:Replicación	Recursos compartidos:Proyectos:Replicación
Esquema	Recursos compartidos:Esquema

ORACLE