Guia de Segurança do Oracle® ZFS Storage Appliance

ORACLE®

Visão Geral da Segurança do Oracle ZFS Storage Appliance

Este guia explora, examina e destaca as considerações de segurança necessárias para criar um sistema de armazenamento seguro e ajudar a equipe como um todo a entender suas metas específicas de segurança. Recomendamos que você leia este guia antes de configurar seu appliance a fim de utilizar os recursos de segurança disponíveis e criar os níveis de segurança necessários.

Você também pode usar este guia como referência para obter informações mais detalhadas sobre as considerações de segurança dos diversos recursos do Oracle ZFSSA (ZFS Storage Appliance). Para conhecer os procedimentos de configuração do produto, consulte o Oracle ZFS Storage System Administration Guide.

As seções a seguir fornecem uma descrição dos recursos de segurança do ZFSSA:

- **Instalação inicial** - Descreve como configurar o acesso administrativo, como a conta com a função root é estabelecida e os efeitos de uma redefinição de fábrica do ZFSSA.
- **Segurança Física** - Descreve o ambiente de segurança física do ZFSSA.
- **Modelo Administrativo** - Descreve a restrição de acesso à CLI e à BUI, o modelo de aplicação de patches do sistema, atualizações diferidas, pacotes de suporte e backup de configuração.
- **Usuários do ZFSSA** - Descreve as funções administrativas, quem pode administrar o ZFSSA e o gerenciamento de autorizações do usuário.
- **ACLs (Listas de Controle de Acesso)** - Descreve o mecanismo que permite ou nega acesso a arquivos e diretórios.
- **SAN (Storage Area Network)** - Descreve os LUNs (números de unidades lógicas) e os grupos de iniciadores associados, bem como as opções e os padrões de autenticação do iniciador.
- **Serviços de Dados** - Descreve os serviços de dados aos quais o ZFSSA oferece suporte e a segurança oferecida pelos diferentes serviços.
- **Serviços de Diretório** - Descreve os serviços de diretório que podem ser configurados no ZFSSA e as respectivas ramificações de segurança.
- **Configurações do Sistema** - Descreve as configurações do sistema; Phone Home, Service Tags, SMTP, SNMP, Syslog, System Identity, Disk Scrubbing e Preventing Destruction.
- Acesso Administrativo Remoto - Descreve o acesso remoto via BUI e CLI. · Logs - Descreve os tipos de log relacionados à segurança.

Instalação inicial

O ZFSSA é fornecido aos clientes com o respectivo software pré-instalado. Nenhuma instalação de software é necessária e nenhuma mídia é fornecida.

A instalação inicial é realizada com o nome de conta e a senha padrão; a senha root padrão deve ser alterada após a instalação. Se o ZFSSA for redefinido para os padrões de fábrica, a senha root do ZFSSA e do processador de serviço também será redefinida para o valor padrão.

Durante a instalação inicial de um ZFSSA, há um nome de conta e uma senha padrão associados ao Processador de Serviço do sistema. Essa é a conta padrão que permite ao administrador do sistema acessar pela primeira vez o ZFSSA e, em seguida, executar as etapas necessárias de instalação inicial do sistema. Uma das etapas necessárias é definir uma nova senha administrativa do ZFSSA, o que, por sua vez, também redefinirá a senha padrão do Processador de Serviço como o mesmo valor.

Segurança Física

Para controlar o acesso ao sistema, você deve manter a segurança física do seu ambiente de computação. Por exemplo, um sistema conectado e deixado desassistido é vulnerável a acesso não autorizado. O ambiente e o hardware do computador devem ser sempre protegidos fisicamente contra acesso não autorizado.

O acesso ao ZFSSA deve ser restrito e controlado por mecanismos de segurança (por exemplo, chave, trava, ferramenta, autorização por crachá eletrônico), e o pessoal com acesso autorizado deve estar ciente dos motivos das restrições e de todas as precauções necessárias.

Modelo Administrativo

Esta seção descreve a segurança dos modelos administrativos do ZFSSA.

Acesso Restrito (CLI e BUI)

O acesso administrativo à BUI (Browser User Interface) e à CLI (Command Line Interface) é limitado ao usuário com a função root, aos administradores locais definidos com os privilégios relevantes e àqueles autorizados por meio de servidores de identidade como LDAP (Lightweight Directory Access Protocol) e NIS (Network Information Service).

A administração é realizada por meio de uma sessão de login de linha de comandos SSL (Secure Sockets Layer) ou de uma sessão HTTP segura (HTTPS) do navegador. As sessões HTTPS são criptografadas com um certificado autoassinado que é gerado exclusivamente para cada ZFSSA durante a instalação inicial. As sessões HTTPS têm um tempo-limite padrão definido pelo usuário de 15 minutos.

Atualizações do Sistema

As atualizações do sistema são aplicadas como substituições de binários inteiros do software do sistema. Antes da atualização, é obtido um instantâneo do pool do sistema em execução. Isso permite que o administrador faça rollback para a versão anterior, se necessário.

Atualizações Diferidas

Uma atualização diferida é um recurso ou uma funcionalidade que faz parte de uma atualização do sistema a qual não é ativada quando a atualização é executada. Cabe ao administrador decidir quando ou se essas atualizações devem ser aplicadas. As atualizações não aplicadas durante uma atualização do sistema permanecem disponíveis durante atualizações sucessivas do sistema. Não é possível selecionar atualizações individuais para serem aplicadas. Ao aplicar atualizações diferidas, você só poderá aplicar todas ou nenhuma delas. Uma vez aplicada uma atualização, não será possível fazer rollback para uma versão anterior do software do sistema.

Pacotes de Suporte

Quando o sistema é registrado para suportar o serviço Phone Home, e ocorre uma falha grave nele, o seu status é enviado ao My Oracle Support, onde poderá ser examinado pelo pessoal de suporte de engenharia, e um pacote de suporte poderá ser criado. As informações de status do sistema enviadas ao My Oracle Support não contêm dados do usuário; somente as informações de configuração são enviadas.

Backup de Configuração

As configurações do sistema podem ser salvas localmente para restauração posterior. Esses backups não contêm dados do usuário; somente as configurações são salvas.

Usuários do ZFSSA

Há dois tipos de usuários do ZFSSA:

- **Usuários de Serviços de Dados** – Clientes que acessam recursos de arquivo e de bloco utilizando os protocolos suportados, como NFS, SMB, Fibre Channel, iSCSI, http e FTP.
- **Usuários Administrativos** - Os usuários que gerenciarão a configuração e os serviços no ZFSSA. Esta seção se aplica somente aos usuários administrativos.

Funções de Usuário Administrativo

É possível conceder privilégios aos administradores atribuindo funções personalizadas a eles. Uma função é um conjunto de privilégios que podem ser atribuídos a um administrador. É possível criar diversas funções de administrador e operador, com diferentes níveis de autorização. Os membros da equipe devem receber a função adequada às suas necessidades, sem a atribuição de privilégios desnecessários.

O uso de funções é mais seguro do que usar senhas de administrador de acesso completo compartilhado, como, por exemplo, conceder a todos os usuários a senha root. As funções restringem os usuários a conjuntos definidos de autorizações. Além disso, as funções de usuário podem ser rastreadas para nomes de usuário individuais nos logs de auditoria. Por padrão, existe uma função chamada "Administração básica", que contém o mínimo de autorizações.

Os usuários administrativos podem ser:

- Usuários locais – Onde todas as informações sobre as contas são salvas no ZFSSA.
- Usuários de diretório – Onde as contas NIS ou LDAP existentes são usadas e configurações de autorização complementares são salvas no ZFSSA. Isso permite que os usuários NIS/LDAP existentes façam login e administrem o ZFSSA. No entanto, esses usuários não podem fazer login no ZFSSA por padrão. O acesso ao ZFSSA deve ser concedido explicitamente.

Escopos administrativos

As autorizações permitem que os usuários executem tarefas específicas, como criar compartilhamentos, reinicializar o ZFSSA e atualizar o software do sistema. Os grupos de autorizações são chamados escopos. Cada escopo pode conter um conjunto de filtros opcionais que limitam o número de autorizações. Por exemplo, é possível usar um filtro a fim de permitir que uma autorização reinicie apenas o serviço HTTP, em vez de reiniciar todos os serviços.

ACLs (Listas de Controle de Acesso)

O ZFSSA fornece controle de acesso a arquivos por meio de listas de controle de acesso (ACLs). Essas listas são um mecanismo que permite ou nega acesso a determinado arquivo ou diretório.

O modelo de ACL fornecido pelo ZFSSA se baseia no modelo de ACL do NFSv4, o qual é derivado da semântica da ACL do Windows. Ele é um modelo sofisticado de ACL que permite o acesso refinado a arquivos e diretórios. Todos os arquivos e diretórios contidos no ZFSSA de armazenamento têm uma ACL

e todas as decisões de controle de acesso relativas ao SMB e ao NFS passam pelos mesmos algoritmos para determinar quem tem ou não permissão de acessar esses arquivos e diretórios.

Uma ACL é composta de uma ou mais ACEs (Entradas de Controle de Acesso). Cada ACE contém uma entrada para as permissões concedidas ou negadas por ela, uma entrada para as pessoas às quais ela se aplica e outra para os sinalizadores de nível de herança usados.

Herança da ACL

As ACLs do NFSv4 permitem que ACEs individuais sejam herdadas por arquivos e diretórios recém-criados. A herança de ACEs é controlada por diversos sinalizadores de nível de herança definidos pelo administrador na ACL durante sua configuração inicial.

Determinando o Acesso à ACL

As ACLs do NFSv4 se baseiam em ordem e são processadas de cima para baixo. Uma vez concedida uma permissão, uma ACE subsequente não poderá negá-la. Uma vez negada uma permissão, uma ACE subsequente não poderá concedê-la.

ACL de Nível de Compartilhamento do SMB

Uma ACL de nível de compartilhamento do SMB é uma ACL combinada com uma ACL de arquivo ou de diretório no compartilhamento para determinar as permissões efetivas do arquivo. A ACL de nível de compartilhamento proporciona uma camada de controle de acesso acima das ACLs de arquivo e fornece configurações de controle de acesso mais sofisticadas. Elas são definidas quando o sistema de arquivos é exportado com o protocolo SMB. Se o sistema de arquivos não for exportado com o protocolo SMB, a definição da ACL de nível de compartilhamento não terá efeito. Por padrão, as ACLs de nível de compartilhamento concedem controle total a todos os usuários.

Propriedades da ACL do ZFS

As propriedades de comportamento e herança de ACLs se aplicam somente aos clientes NFS. Os clientes SMB utilizam a semântica estrita do Windows e têm precedência sobre as propriedades do ZFS. A diferença é que o NFS utiliza a semântica POSIX, e os clientes SMB, não. As propriedades são compatíveis principalmente com POSIX.

SAN (Storage Area Network)

Em uma SAN, os grupos de destinos e de iniciadores definem conjuntos de destinos e de iniciadores que podem estar associados a um LUN (Número de Unidade Lógica). Um LUN associado a um grupo de destinos só poderá ser acessado por meio dos destinos desse grupo. Um LUN associado a um grupo de iniciadores só poderá ser acessado pelos iniciadores desse grupo. Os grupos de iniciadores e de destinos são aplicados a um LUN quando ele é criado. Não será possível criar um LUN com êxito sem definir pelo menos um grupo de destinos e outro de iniciadores.

Além da autenticação CHAP (Challenge-Handshake Authentication Protocol), que só pode ser selecionada para acesso de iniciadores iSCSI/iSER, nenhuma autenticação é executada.

OBS.: O uso do grupo de iniciadores padrão poderá resultar na exposição do LUN a iniciadores indesejados ou conflitantes.

Serviços de Dados

TABELA 1 Serviços de Dados

SERVIÇO	DESCRIÇÃO	PORTAS USADAS
NFS	Acesso ao sistema de arquivos por meio dos protocolos NFSv3 e NFSv4	111 e 2049
iSCSI	Acesso ao LUN por meio do protocolo iSCSI	3260 e 3205
SMB	Acesso ao sistema de arquivos por meio do protocolo SMB	SMB-over-NetBIOS 139
		SMB-over-TCP 445
		NetBIOS Datagram 138
		NetBIOS Name Service 137
FTP	Acesso ao sistema de arquivos por meio do protocolo FTP	21
HTTP	Acesso ao sistema de arquivos por meio do protocolo HTTP	80
NDMP	Serviço de host NDMP	10000
Replicação Remota	Replicação remota	216
Migração Shadow	Migração de dados shadow	
SFTP	Acesso ao sistema de arquivos por meio do protocolo SFTP	218
SRP	Bloquear acesso por meio do protocolo SRP	
TFTP	Acesso ao sistema de arquivos por meio do protocolo TFTP	
Verificação de Vírus	Verificação de vírus no sistema de arquivos	

Mínimo de Portas Necessárias:

Para fornecer segurança em uma rede, você pode criar firewalls. Os números de porta são usados para criar firewalls e identificar, de forma exclusiva, uma transação em uma rede, especificando o host e o serviço.

A seguinte lista mostra o mínimo de portas necessárias para a criação de firewalls:

Portas de Entrada

- icmp/0-65535 (PING)
- tcp/1920 (EM)
- tcp/215 (BUI)
- tcp/22 (SSH)
- udp/161 (SNMP)

Portas de entrada adicionais se o compartilhamento de arquivos http for usado (normalmente não é)

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

Portas de Saída

- tcp/80 (WEB)

Obs.: Para replicação, use o tunelamento GRE (Generic Routing Encapsulation) onde possível. Ele permite que o tráfego seja direcionado para as interfaces back-end e evita o firewall em locais onde o tráfego

poderia se tornar lento. Se os túneis GRE não estiverem disponíveis no NFS principal, você deverá executar a replicação na interface externa (front-end). Nesse caso, a porta 216 também deve ser aberta.

Opções de Criptografia e Autenticação NFS

Por padrão, os compartilhamentos NFS são alocados com a autenticação AUTH_SYS RPC. Também é possível configurá-los para serem compartilhados com a segurança Kerberos. Com a autenticação AUTH_SYS, o uid e o gid UNIX do cliente são enviados não autenticados pelo servidor NFS na rede. Como esse mecanismo de autenticação é facilmente violado por qualquer pessoa com acesso de root em um cliente, é preferível usar um dos outros modos de segurança disponíveis.

Controles de acesso adicionais podem ser especificados para cada compartilhamento a fim de permitir ou negar acesso aos compartilhamentos em redes, domínios DNS ou hosts específicos.

Modos de Segurança

Os modos de segurança são definidos por compartilhamento. A lista a seguir descreve as configurações de segurança Kerberos disponíveis.

- krb5 - Autenticação do usuário final por meio do Kerberos V5
- krb5i - krb5 mais proteção de integridade (os pacotes de dados são à prova de adulteração)
- krb5p - krb5i mais proteção de privacidade (os pacotes de dados são à prova de adulteração e criptografados)

Combinações de tipos de Kerberos também podem ser especificadas na configuração do modo de segurança. A combinação dos modos de segurança permite que os clientes usem todos os tipos de Kerberos listados.

Tipos de Kerberos

- sys - Autenticação do Sistema
- krb5 - Somente Kerberos v5, os clientes devem usar este tipo na combinação selecionada.
- krb5:krb5i - Kerberos v5, com integridade; os clientes devem usar qualquer tipo listado na combinação selecionada.
- krb5i - Kerberos v5, somente integridade; os clientes devem usar este tipo na combinação selecionada.
- krb5:krb5i:krb5p - Kerberos v5, com integridade ou privacidade; os clientes podem usar qualquer tipo listado na combinação selecionada.
- krb5p - Kerberos v5, somente privacidade, os clientes devem usar este tipo na combinação selecionada.

iSCSI

Ao configurar um LUN no ZFSSA, você poderá exportar esse volume por meio de um destino iSCSI (Internet Small Computer System Interface). O serviço iSCSI permite que os iniciadores iSCSI acessem destinos usando o protocolo iSCSI.

Esse serviço suporta a descoberta, o gerenciamento e a configuração com o protocolo iSNS. O serviço iSCSI suporta a autenticação unidirecional (o destino autentica o iniciador) e bidirecional (o destino e o iniciador autenticam um o outro) usando CHAP. Além disso, ele suporta o gerenciamento de dados de autenticação CHAP em um banco de dados RADIUS.

Primeiro, o sistema executa a autenticação e, em seguida, a autorização, em duas etapas independentes. Se o iniciador local tiver um nome e um segredo CHAP, o sistema executará a autenticação. Se o iniciador

local não tiver propriedades CHAP, o sistema não executará a autenticação e, portanto, todos os iniciadores estarão qualificados para autorização.

O serviço iSCSI permite especificar uma lista global de iniciadores que pode ser usada nos grupos de iniciadores. Quando a autenticação iSCSI ou CHAP é usada, o RADIUS pode ser utilizado como o protocolo iSCSI que transfere todas as autenticações CHAP para o servidor RADIUS selecionado.

Suporte ao RADIUS

O RADIUS (Remote Authentication Dial-In User Service) é um sistema que permite utilizar um servidor centralizado para executar a autenticação CHAP dos nós de armazenamento. Ao usar a autenticação iSCSI e CHAP, você poderá selecionar o RADIUS para o protocolo iSCSI, que aplicará o iSCSI e o iSER (iSCSI Extensions for RDMA) e enviará todas as autenticações CHAP para o servidor RADIUS selecionado.

Para permitir que o ZFSSA execute a autenticação CHAP usando RADIUS, as seguintes informações devem estar corretas:

- O ZFSSA deve especificar o endereço do servidor RADIUS e um segredo para ser usado durante a comunicação com esse servidor.
- O servidor RADIUS (por exemplo, no arquivo do cliente) deve ter uma entrada que forneça o endereço do ZFSSA e especifique o mesmo segredo especificado anteriormente.
- O servidor RADIUS (por exemplo, no arquivo do usuário) deve ter uma entrada que forneça o nome CHAP e o segredo CHAP correspondente de cada iniciador.
- Se o iniciador usar o seu nome IQN como o seu nome CHAP (a configuração recomendada), e o ZFSSA não precisar de uma entrada Initiator separada para cada caixa Initiator, o servidor RADIUS poderá executar todas as etapas de autenticação.
- Se o iniciador usar um nome CHAP diferente, o ZFSSA deverá ter uma entrada Initiator para o iniciador que especifique o mapeamento de um nome IQN para o nome CHAP. Essa entrada Initiator NÃO precisa especificar o segredo CHAP do iniciador.

SMB (Server Message Block)

O protocolo SMB (também conhecido como CIFS (Common Internet File System)) fornece principalmente acesso compartilhado a arquivos em uma rede do Microsoft Windows. Ele também fornece autenticação.

As seguintes opções do SMB têm implicações de segurança:

- **Restrict Anonymous Access to share list** - Esta opção exige que os clientes façam a autenticação usando o SMB para receberem uma lista de compartilhamentos. Se esta opção estiver desativada, os clientes anônimos poderão acessar a lista de compartilhamentos. Por padrão, esta opção está desativada.
- **SMB Signing Enabled** - Esta opção ativa a interoperabilidade com clientes SMB utilizando o recurso de assinatura SMB. Se a opção estiver ativada, um pacote assinado terá a assinatura verificada. Se ela estiver desativada, um pacote não assinado será aceito sem a verificação de assinatura. Por padrão, esta opção está desativada.
- **SMB Signing Required** - Esta opção pode ser usada quando a assinatura SMB é obrigatória. Quando esta opção estiver ativada, todos os pacotes SMB deverão ser assinados, caso contrário, eles serão rejeitados. Os clientes que não oferecem suporte ao recurso de assinatura SMB não podem se conectar ao servidor. Por padrão, esta opção está desativada.
- **Enable Access-based Enumeration** - Quando esta opção é definida, as entradas de diretório são filtradas com base nas credenciais do cliente. Quando o cliente não tiver acesso a um arquivo ou diretório, esse arquivo será omitido da lista de entradas retornadas para esse cliente. Por padrão, esta opção está desativada.

Autenticação no Modo de Domínio do AD (Active Directory)

No Modo de Domínio, os usuários são definidos no Active Directory. Os clientes SMB podem se conectar ao ZFSSA usando a autenticação Kerberos ou NTLM.

Quando o usuário se conecta com um nome de host ZFSSA totalmente qualificado, os clientes Windows do mesmo domínio ou de um domínio confiável utilizam a autenticação Kerberos; caso contrário, eles usarão a autenticação NTLM.

Quando um cliente SMB usa a autenticação NTLM para se conectar ao ZFSSA, as credenciais do usuário são encaminhados ao Controlador de Domínio do AD para autenticação. Isso é denominado autenticação de passagem.

Se forem definidas políticas de segurança do Windows restringindo a autenticação NTLM, os clientes Windows deverão se conectar ao ZFSSA usando um nome de host totalmente qualificado. Para obter mais informações, consulte este artigo do MSDN: http://technet.microsoft.com/en-us/library/jj865668%28v=ws.10%29.aspx.

Após a autenticação, um "contexto de segurança" é estabelecido para a sessão SMB do usuário. O usuário representado pelo contexto de segurança tem um SID (Security Descriptor) exclusivo. O SID denota a propriedade do arquivo e é usado para determinar os privilégios de acesso ao arquivo.

Autenticação no Modo de Grupo de Trabalho

No Modo de Grupo de Trabalho, os usuários são definidos localmente no ZFSSA. Quando um cliente SMB se conecta ao ZFSSA no Modo de Grupo de Trabalho, os hashes de nome de usuário e senha desse usuário são usados para autenticá-lo localmente.

O nível de compatibilidade do LM (LAN Manager) é usado para especificar o protocolo usado para autenticação quando o ZFSSA está no modo de grupo de trabalho.

A lista a seguir mostra o comportamento do ZFSSA para cada nível de compatibilidade do LM:

- Nível 2: Aceita a autenticação LM, NTLM e NTLMv2
- Nível 3: Aceita a autenticação LM, NTLM e NTLMv2
- Nível 4: Aceita a autenticação NTLM e NTLMv2
- Nível 5: Aceita somente a autenticação NTLMv2.

Quando o usuário do Grupo de Trabalho é autenticado com êxito, um contexto de segurança é estabelecido. Um SID exclusivo é criado para os usuários definidos no ZFSSA utilizando uma combinação do SID da máquina e do UID do usuário. Todos os usuários locais são definidos como usuários UNIX.

Grupos Locais e Privilégios

Os grupos locais são grupos de usuários do domínio que concedem privilégios adicionais a esses usuários. Os administradores podem ignorar as permissões de arquivo para alterar a propriedade dos arquivos. Os operadores de backup podem ignorar os controles de acesso a arquivos para fazer backup e restaurar arquivos.

Operações Administrativas por meio do MMC (Console de Gerenciamento Microsoft)

Para garantir que somente os usuários adequados tenham acesso às operações administrativas, algumas restrições de acesso se aplicam às operações executadas remotamente com o MMC.

A lista a seguir mostra os usuários e as operações que eles têm permissão de executar:

- Usuários regulares - Listar compartilhamentos
- Membros do grupo Administradores - Listar arquivos abertos e fechar arquivos, desconectar conexões de usuários, exibir serviços e log de eventos
- Os membros do grupo Administradores também podem definir/modificar ACLs de nível de compartilhamento
- Membros do grupo Administradores - Listar arquivos abertos e fechar arquivos, desconectar conexões de usuários, exibir serviços e log de eventos

Verificação de Vírus

Este serviço verifica se há vírus no nível do sistema de arquivos. Quando um arquivo é acessado em um protocolo, o serviço de Verificação de Vírus verifica o arquivo e, caso seja encontrado um vírus, ele negará o acesso ao arquivo e o colocará em quarentena. A verificação é realizada por um mecanismo externo contatado pelo ZFSSA. Esse mecanismo não é fornecido no software do ZFSSA.

Após a verificação de um arquivo com as definições de vírus mais recentes, ele não será verificado novamente até ser modificado. A verificação de vírus é fornecida sobretudo para clientes SMB que têm maior probabilidade de introduzir vírus. Os clientes NFS também podem usar esse tipo de verificação, porém, devido ao modo como o protocolo NFS funciona, é possível que um vírus não seja detectado de forma tão rápida como ocorre em um cliente SMB.

Mecanismo de Atraso para Ataques Baseados em Tempo

O SMB não implementa qualquer mecanismo de atraso para impedir ataques baseados em tempo. Ele utiliza a estrutura criptográfica do Solaris.

Criptografia de Dados Durante a Transmissão

O serviço SMB usa a versão 1 do protocolo SMB, a qual não oferece suporte à criptografia de dados durante a transmissão.

FTP (File Transfer Protocol)

O FTP permite o acesso de clientes FTP ao sistema de arquivos. O serviço FTP não permite logins anônimos, e os usuários devem autenticar-se com o serviço de nomes configurado.

O FTP oferece suporte às seguintes configurações de segurança. Essas configurações são compartilhadas por todos os sistemas de arquivos para os quais o acesso do protocolo FTP está ativado:

- Enable SSL/TLS - Permite conexões FTP criptografadas com SSL/TLS e garante que a transação FTP seja criptografada. Por padrão, esta opção está desativada.
- Permit root login - Permite logins FTP do usuário com a função root. Por padrão, esta opção está desativada porque a autenticação FTP é feita com texto sem formatação, o que coloca em risco a segurança devido a ataques de sniffing na rede.
- Maximum number of allowable login attempts - O número de tentativas de login que falharam antes de uma conexão FTP ser desconectada, e o usuário precisar se conectar novamente para fazer uma nova tentativa. O valor padrão é 3.
- Logging level - O nível de detalhamento do log.

O FTP oferece suporte aos seguintes logs:

- proftpd - Eventos FTP, incluindo tentativas de login com e sem êxito
- proftpd_xfer - Log de transferência de arquivos
- proftpd_tls - Eventos FTP relacionados à criptografia SSL/TLS

HTTP (Hypertext Transfer Protocol)

O HTTP fornece acesso a sistemas de arquivos por meio dos protocolos HTTP e HTTPS e da extensão HTTP WebDAV (Web based Distributed Authoring and Versioning). Isso permite que os clientes acessem sistemas de arquivos compartilhados usando um navegador da Web ou como um sistema de arquivos local caso o software cliente ofereça suporte a ele. O servidor HTTPS usa um certificado de segurança autoassinado.

As seguintes propriedades estão disponíveis:

- Require client login - Os clientes devem autenticar-se para terem acesso a um compartilhamento, e os arquivos criados por eles serão de sua propriedade. Se esta propriedade não estiver definida, os arquivos criados pertencerão ao serviço HTTP com o usuário "nobody”.
- Protocols - Selecione os métodos de acesso que deverão ser suportados: HTTP, HTTPS ou ambos.
- HTTP Port (for incoming connections) - Porta HTTP, a porta padrão é a 80.
- HTTPS Port (for incoming secure connections) - Porta HTTP, a porta padrão é a 443.

Quando a propriedade Require Client Login está ativada, o ZFSSA nega acesso aos clientes que não fornecem credenciais de autenticação válidas para um usuário local, NIS ou LDAP. Não há suporte para a autenticação do Active Directory. Somente a autenticação HTTP básica é suportada. A menos que o HTTPS seja usado, o nome de usuário e a senha serão transmitidos não criptografados, o que poderá não ser adequado para todos os ambientes. Se a propriedade Require Client Login estiver desativada, o ZFSSA não tentará fazer a autenticação.

Independentemente da autenticação, as permissões não são mascaradas nos arquivos e nos diretórios criados. Todos os usuários têm permissões de leitura e gravação nos arquivos criados recentemente Todos os usuários têm permissões de leitura, gravação e execução nos diretórios criados recentemente.

NDMP (Network Data Management Protocol)

O NDMP permite que o ZFSSA participe de operações de backup e restauração baseadas em NDMP controladas por um cliente NDMP remoto chamado DMA (Data Management Application). Usando o NDMP, os dados de usuários do ZFSSA (por exemplo, os dados armazenados em compartilhamentos criados pelo administrador no ZFSSA) podem ser salvos em um backup e restaurados para dispositivos conectados localmente, como unidades de fita e sistemas remotos. Também é possível fazer backup de dispositivos conectados localmente e restaurá-los via DMA.

Replicação Remota

A replicação remota do ZFSSA facilita a replicação de projetos e compartilhamentos. Esse serviço permite exibir os ZFSSAs que têm dados replicados nesse ZFSSA e configurar os ZFSSAs nos quais esse ZFSSA poderá fazer a replicação.

Quando esse serviço está ativado, o ZFSSA recebe atualizações de replicação de outros ZFSSAs, bem como envia atualizações de replicação relativas a projetos e compartilhamentos locais de acordo com as ações configuradas para eles. Quando o serviço está desativado, as atualizações de replicação recebidas falham, e os projetos e os compartilhamento locais não são replicados.

A senha root do ZFSSA remoto é necessária para configurar os destinos de replicação remota do ZFSSA. Esses destinos são usados para configurar uma conexão de mesmo nível para replicação a qual permite que os ZFSSAs se comuniquem.

Durante a criação dos destinos, a senha root é usada para confirmar a autenticidade da solicitação, bem como produzir e trocar as chaves de segurança que serão usadas para identificar os ZFSSAs nas comunicações subsequentes.

As chaves geradas são armazenadas de maneira persistente como parte da configuração do ZFSSA. A senha root nunca é armazenada de maneira persistente. A senha root nunca é transmitida sem proteção. Todas as comunicações do ZFSSA, incluindo essa troca inicial de identidades, são protegidas com SSL.

Migração Shadow

A migração shadow permite a migração automática de dados de origens externas ou internas e controla a migração automática em segundo plano. Independentemente de o serviço estar ou não ativado, os dados são migrados de forma síncrona para solicitações em banda. O principal objetivo do serviço é permitir o ajuste do número de threads dedicados à migração em segundo plano.

As montagens NFs em uma origem NFS não são controladas pelo usuário do ZFSSA. Portanto, as montagens da migração shadow não podem ser seguras; se o servidor esperar uma solicitação Kerberos ou semelhante, a montagem de origem será rejeitada.

SFTP (SSH File Transfer Protocol)

O SFTP permite o acesso de clientes SFTP a sistemas de arquivos. Como não são permitidos logins anônimos, os usuários devem autenticar-se com o serviço de nomes configurado.

Ao criar uma chave SFTP, você deve incluir a propriedade do usuário com uma atribuição de usuário válida. As chaves SFTP são agrupadas por usuário e autenticadas por meio do SFTP com o nome do usuário.

OBSERVAÇÃO: Para fins de segurança, você deverá criar novamente as chaves SFTP existentes que não incluem a propriedade do usuário, mesmo que elas sejam autenticadas.

TFTP (Trivial File Transfer Protocol)

O TFTP é um protocolo simples para transferência de arquivos. Ele foi projetado como um protocolo pequeno e de fácil implementação, mas não possui a maioria dos recursos de segurança do FTP. O TFTP apenas lê e grava arquivos de/em um servidor remoto. Ele não pode listar diretórios e, no momento, não contém provisões para autenticação de usuários.

Serviços de Diretório

NIS (Network Information Service)

NIS é um serviço de nomes para o gerenciamento centralizado de diretórios. O ZFSSA pode atuar como um cliente NIS para usuários e grupos. Isso permite que os usuários NIS façam login no FTP e no HTTP/WebDAV. Esses usuários também podem receber privilégios de administração do ZFSSA. O ZFSSA complementa as informações do NIS com suas próprias configurações de privilégios.

LDAP (Lightweight Directory Access Protocol)

O ZFSSA usa o LDAP para autenticar tanto usuários administrativos como alguns usuários de serviços de dados (ftp, http). A segurança do LDAP via SSL é suportada pelo ZFSSA. O LDAP é usado para recuperar informações sobre usuários e grupos das seguintes maneiras:

- Fornece interfaces de usuário que aceitam e exibem nomes de usuários e grupos.
- Mapeia nomes para/de usuários e grupos, no caso de protocolos de dados como o NFSv4 que utilizam nomes. · Define associações de grupo para uso no controle de acesso.
- Opcionalmente, para transportar dados usados para autenticação administrativa e de acesso a dados.

Conexões LDAP podem ser usadas como um mecanismo de autenticação. Por exemplo, quando o usuário tentar autenticar-se no ZFSSA, o ZFSSA poderá tentar fazer a autenticação no servidor LDAP como esse usuário como um mecanismo para verificar a autenticação.

Há vários controles de segurança de conexões LDAP:

- Autenticação do appliance para o servidor:
  - O appliance é anônimo
  - O appliance faz a autenticação usando as credenciais Kerberos do usuário
  - O appliance faz a autenticação usando a senha e o usuário do "proxy" especificados
- Autenticação do servidor para o appliance (verifica se o servidor correto foi contatado):
  1. Não segura
  2. O servidor é autenticado usando Kerberos
  3. O servidor é autenticado usando um certificado TLS

Os dados transportados por uma conexão LDAP serão criptografados se o Kerberos ou o TLS for usado; caso contrário, eles não serão criptografados. Quando o TLS é usado, a primeira conexão durante a configuração não é segura. O certificado do servidor é obtido nesse momento e é usado para autenticar conexões de produção posteriores.

Não será possível importar um certificado de uma Autoridade de Certificação para usá-lo na autenticação de vários servidores LDAP nem importar manualmente um certificado de determinado servidor LDAP.

Somente o TLS (LDAPS) bruto é suportado. Conexões STARTTLS, iniciadas em uma conexão LDAP não segura e, depois, alteradas para uma conexão segura, não são suportadas. Os servidores LDAP que exigem um certificado de cliente não são suportados.

Mapeamento de Identidades

Os clientes podem acessar recursos de arquivo no ZFSSA usando o SMB ou o NFS, e cada um deles tem um identificador de usuário exclusivo. Os usuários do SMB/Windows têm Descritores de Segurança (SIDs) e os usuários do UNIX/Linux têm IDs de Usuário (UIDs). Os usuários também podem ser membros de grupos identificados por SIDs de Grupo (no caso de usuários do Windows) ou IDs de Grupo (GID), no caso de usuários do UNIX/Linux.

Nos ambientes em que os recursos de arquivo são acessados por meio dos dois protocolos, geralmente convém estabelecer equivalências de identidade em que, por exemplo, um usuário do UNIX é equivalente a um usuário do Active Directory. Isso é importante para determinar os direitos de acesso a recursos de arquivo no ZFSSA.

Há diferentes tipos de mapeamento de identidade que envolvem Serviços de Diretório, como Active Directory, LDAP e NIS. É importante seguir as melhores práticas de segurança para o serviço de diretório que está sendo usado.

IDMU

A Microsoft oferece um recurso chamado IDMU (Identity Management for UNIX). Esse software está disponível para o Windows Server 2003 e é fornecido com o Windows Server 2003 R2 e versões posteriores. Ele faz parte de um recurso antes denominado Services for UNIX que era fornecido separadamente.

O IDMU é usado principalmente para suportar o Windows como um servidor NIS/NFS. O IDMU permite que o administrador especifique vários parâmetros relacionados ao UNIX: UID, GID, shell de login, diretório base e outros parâmetros semelhantes para grupos. Esses parâmetros são disponibilizados com o uso do AD por meio de um esquema semelhante, mas não idêntico ao da RFC2307, e por meio do serviço NIS.

Quando o modo de mapeamento do IDMU é usado, o serviço de mapeamento de identidades utiliza esses atributos UNIX para estabelecer mapeamentos entre identidades do Windows e do UNIX. Essa abordagem é muito semelhante ao mapeamento baseado em diretório; a única diferença é que o serviço de mapeamento de identidades consulta o esquema de propriedades estabelecido pelo software IDMU, em vez de permitir um esquema personalizado. Quando essa abordagem é usada, nenhum outro mapeamento baseado em diretório poderá ser usado.

Mapeamento Baseado em Diretório

No mapeamento baseado em diretório, informações sobre como a identidade é mapeada para outra equivalente na plataforma oposta são anotadas no objeto do Active Directory ou LDAP. Esses atributos extras associados ao objeto devem ser configurados.

Mapeamento Baseado em Nome

O mapeamento baseado em nome envolve a criação de várias regras que mapeiam as identidades por nome. Essas regras estabelecem equivalências entre as identidades do Windows e as do UNIX.

Mapeamento Efêmero

Se nenhuma regra de mapeamento baseado em nome se aplicar a determinado usuário, ele receberá credenciais temporárias por meio de um mapeamento efêmero, a menos que elas sejam bloqueadas por um mapeamento de negação. Quando um usuário do Windows com um nome UNIX efêmero cria um arquivo no sistema, os clientes Windows que acessam o arquivo usando o SMB veem que ele pertence a essa identidade do Windows. Entretanto, para os clientes NFS, esse arquivo aparece como pertencente ao usuário “nobody”.

Configurações do Sistema

As seções a seguir descrevem as configurações disponíveis de segurança do sistema.

Phone Home

O serviço Phone Home é usado para gerenciar o registro do ZFSSA, bem como o serviço de suporte remoto Phone Home. Nenhum dado ou metadado do usuário é transmitido nessas mensagens.

- O registro conecta o ZFSSA ao portal de inventário da Oracle, por meio do qual você poderá gerenciar seu equipamento Oracle. O registro é um pré-requisito para usar o serviço Phone Home.
- Esse serviço se comunica com o Oracle Support para fornecer:
  - Relatório de falhas - O sistema reporta problemas ativos à Oracle para obter uma resposta automatizada do serviço. Dependendo da natureza da falha, um caso de suporte poderá ser aberto.
  - Pulsações (Heartbeats) - Mensagens diárias de pulsação são enviadas à Oracle para indicar que o sistema está funcionando plenamente. O Oracle Support poderá notificar o contato técnico de uma conta quando um dos sistemas ativados não enviar uma mensagem de pulsação durante muito tempo.
  - Configuração do sistema - Mensagens periódicas são enviadas à Oracle descrevendo a configuração e as versões atuais de software e hardware, bem como a configuração de armazenamento.

Service Tags

Este recurso é usado para facilitar o suporte e o inventário de produtos, permitindo que os seguintes tipos de dados sejam consultados no ZFSSA:

- Número de série do sistema
- Tipo do sistema
- Números de versão do software

Você poderá registrar as tags de serviço no Oracle Support, o que tornará mais fácil manter o controle de seu equipamento Oracle, bem como agilizará as chamadas de serviço. As tags de serviço estão ativadas por padrão.

SMTP

O SMTP envia todos os e-mails gerados pelo ZFSSA, geralmente em resposta a alertas, conforme configurado. O SMTP não aceita e-mails externos; ele envia somente os e-mails gerados automaticamente pelo próprio ZFSSA.

Por padrão, o serviço SMTP usa o DNS (registros MX) a fim de determinar para onde os e-mails devem ser enviados. Se o DNS não estiver configurado para o domínio do ZFSSA ou se o domínio de destino dos e-mails de saída não contiver registros MX do DNS configurados de forma adequada, o ZFSSA poderá ser configurado para encaminhar todos os e-mails por meio de um servidor de e-mail de saída.

SNMP (Simple Network Management Protocol)

O SNMP fornece duas funções no ZFSSA; informações de status do ZFSSA podem ser fornecidas pelo SNMP e podem ser configurados alertas para enviar traps do SNMP. As versões 1 e 2c do SNMP estão disponíveis.

Syslog

Uma mensagem Syslog é uma pequena mensagem de evento transmitida do ZFSSA para um ou mais sistemas remotos. O Syslog fornece duas funções no ZFSSA:

- Podem ser configurados alertas para enviar mensagens Syslog para um ou mais sistemas remotos
- Os serviços habilitados para Syslog no ZFSSA podem ter suas mensagens Syslog encaminhadas para sistemas remotos

O Syslog pode ser configurado para usar o formato de saída clássico descrito na RFC 3164 ou o formato de saída mais recente controlado por versão descrito na RFC 5424. As mensagens Syslog são transmitidas como datagramas UDP. Portanto, elas estão sujeitas a serem descartadas pela rede ou simplesmente poderão não ser enviadas caso o sistema de envio tenha memória insuficiente ou se a rede estiver muito congestionada. Portanto, os administradores devem considerar que, em cenários complexos de falha na rede, é possível que algumas mensagens estejam ausentes e tenham sido descartadas.

A mensagem contém os seguintes elementos:

- Um recurso descrevendo o tipo de componente do sistema que emitiu a mensagem
- A severidade da condição associada à mensagem
- Um carimbo de data/hora descrevendo o horário do evento associado no UTC
- Um nome de host descrevendo o nome canônico do ZFSSA
- Uma tag descrevendo o nome do componente do sistema que emitiu a mensagem
- Uma mensagem descrevendo o próprio evento

System Identity

Este serviço fornece a configuração do nome e do local do sistema. Talvez seja necessário alterar essas informações caso o ZFSSA seja movido para outro local da rede ou seja redefinido.

Disk Scrubbing

Este serviço deve ser executado regularmente para que o ZFSSA possa detectar e corrigir os dados danificados no disco. Este é um processo em segundo plano que lê os discos durante os períodos ociosos para detectar erros de leitura irremediáveis em setores que não são acessados com frequência. A detecção desses erros latentes nos setores em tempo hábil é importante para reduzir a perda de dados.

Preventing Destruction

Quando este recurso está ativado, o compartilhamento ou o projeto não pode ser destruído. Isso inclui a destruição de um compartilhamento por meio de clones dependentes, a destruição de um compartilhamento em um projeto ou a destruição de um pacote de replicação. Entretanto, ele não afeta os compartilhamentos destruídos por atualizações de replicação. Se um compartilhamento for destruído em um ZFSSA que seja a origem da replicação, o compartilhamento correspondente no destino será destruído, mesmo que essa propriedade esteja ativada.

Para destruir o compartilhamento, será necessário primeiro desativar a propriedade explicitamente como uma etapa separada. Essa propriedade está desativada por padrão.

Acesso Administrativo Remoto

Esta seção descreve a segurança de acesso remoto do ZFSSA.

BUI (Browser User Interface)

Utilize as telas de Serviços da BUI (Browser User Interface) para exibir e modificar os serviços e as configurações de acesso remoto.

SSH (Secure Shell)

O SSH permite que os usuários façam login no ZFSSA por meio da CLI (Command Line Interface) e executem a maioria das ações administrativas que podem ser executadas na BUI. O SSH também pode ser usado para executar scripts automatizados em um host remoto, como, por exemplo, para recuperar logs diários ou estatísticas de análises.

Logs

Esta seção descreve os recursos de log relacionados à segurança.

Auditoria

O log de auditoria registra os eventos de atividades do usuário, incluindo login e logout na BUI e na CLI, além de ações administrativas. A seguinte tabela mostra um exemplo de entradas do log de auditoria exibidas na BUI:

TABELA 2 Registro de Log de Auditoria

Time	User	Host	Summary	Session Annotation
2009-10-12 05:20:24	root	galaxy	Disabled ftp service	
2009-10-12 03:17:05	root	galaxy	User logged in	
2009-10-11 22:38:56	root	galaxy	Browser session timed out	
2009-10-11 21:13:35	root	<console>	Enabled ftp service	

Phone Home

Se o serviço Phone Home for usado, este log mostrará os eventos de comunicação com o Oracle Support. A tabela a seguir fornece um exemplo de entrada do log Phone Home exibida na BUI:

TABELA 3 Phone Home Log Record

Time	Description	Result
2009-10-12 05:24:09	Uploaded file 'cores/ak.45e5ddd1-ce92-c16e-b5eb-9cb2a8091f1c.tar.gz' to Oracle support	OK

Mais Informações

Você pode obter ajuda on-line específica de contexto sobre cada página da BUI (Browser User Interface) do ZFSSA clicando no botão Help localizado no canto superior esquerdo de cada página.

Informações completas sobre o produto Oracle ZFS Storage Appliance podem ser obtidas no seguinte local:

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

Mapeamento da Documentação

Use as tabelas a seguir para localizar a documentação detalhada relativa a cada um dos serviços, configurações ou outros recursos do ZFSSA. Ao usar a BUI para configurar um ZFSSA, você poderá clicar no link HELP, no canto superior direito de qualquer tela, para exibir a ajuda referente a essa tela.

TABELA 4 Serviços

Serviço	Localização da Documentação
Active Directory	Services:Active_Directory
Identity Mapping	Services:Identity_Mapping
DNS	Services:DNS
Dynamic Routing	Services:Dynamic_Routing
IPMP	Services:IPMP
NTP	Services:NTP
Phone Home	Services:Phone_Home
Service Tags	Services:Service_Tags
SMTP	Services:SMTP
SNMP	Services:SNMP
Syslog	Services:Syslog
System Identity	Services:System_Identity
SSH	Services:SSH

TABELA 5 Configuração

Configuração	Localização da Documentação
SAN	Configuration:SAN
SAN:FC	Configuration:SAN:FC
SAN:iSCSI	Configuration:SAN:iSCSI
SAN:SRP	Configuration:SAN:SRP
Cluster	Configuration:Cluster
Users	Configuration:Users
Preferences	Configuration:Preferences
Alerts	Configuration:Alerts
Storage	Configuration:Storage

TABELA 6 Armazenamento

Armazenamento	Localização da Documentação
Shares	Shares
Concepts	Shares:Concepts
Shadow_Migration	Shares:Shadow_Migration

Armazenamento	Localização da Documentação
Space_Management	Shares:Space_Management
File system_Namespace	Shares:File system_Namespace
Shares	Shares:Shares
General	Shares:Shares:General
Protocols	Shares:Shares:Protocols
Access	Shares:Shares:Access
Snapshots	Shares:Shares:Snapshots
Projects	Shares:Projects
Projects:General	Shares:Projects:General
Projects:Protocols	Shares:Projects:Protocols
Projects:Replication	Shares:Projects:Replication
Schema	Shares:Schema