Diretrizes de segurança do Oracle® Solaris 11

Número do Item: E25821–03
Março de 2012

ORACLE

120424@25097

Conteúdo

Prefácio

Este guia apresenta as diretrizes de segurança para o Sistema operacional Oracle Solaris (SO Oracle Solaris). Primeiro, o guia descreve os problemas de segurança que um sistema operacional corporativo deve abordar. Em seguida, descreve os recursos de segurança padrão do SO Oracle Solaris. Finalmente, o guia fornece etapas específicas a serem executadas para aprimorar o sistema e usar os recursos de segurança do Oracle Solaris a fim de proteger seus dados e aplicativos. Você pode personalizar as recomendações contidas neste guia de acordo com a política de segurança de sua empresa.

Público-alvo

O *Diretrizes de segurança do Oracle Solaris 11* é destinado a administradores de segurança e outros administradores que executam as seguintes tarefas:

- Analisar requisitos de segurança
- Implementar a política de segurança da empresa no software
- Instalar e configurar o SO Oracle Solaris
- Manter a segurança do sistema e da rede

Para usar este guia, você deve ter conhecimento geral de administração do UNIX, uma boa formação de segurança de software e conhecimento da política de segurança da sua empresa.

Acesso ao suporte Oracle

Os clientes Oracle possuem acesso a suporte eletrônico por meio do My Oracle Support. Para obter informações, visite `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` ou visite `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs` se você é portador de deficiência auditiva.

Convenções tipográficas

A tabela a seguir descreve as convenções tipográficas usadas neste livro.

TABELA P–1 Convenções tipográficas

Fonte	Descrição	Exemplo
`AaBbCc123`	Nomes de comandos, arquivos, diretórios e saídas do computador na tela	Edite seu arquivo `.login`. Use `ls -a` para listar todos os arquivos. `machine_name%, você tem e-mail.`
`AaBbCc123`	O que você digita, em comparação com a saída do computador na tela	`machine_name%` **`su`** `Senha:`
aabbcc123	Espaço reservado: substitua, aplicando um nome ou valor real	O comando para remover um arquivo é `rm` *nome do arquivo*.
AaBbCc123	Títulos de manuais, termos novos e termos a serem enfatizados	Consulte o Capítulo 6 do *Guia do Usuário*. Um *cache* é uma cópia que é armazenada localmente. *Não* salve o arquivo. **Nota:** alguns itens enfatizados aparecem on-line em negrito.

Prompts do shell em exemplos de comando

A tabela a seguir mostra o prompt de sistema UNIX padrão e o prompt do superusuário para shells, que estão incluídos no SO Oracle Solaris. Note que o prompt do sistema padrão que é exibido em exemplos de comando varia dependendo da versão do Oracle Solaris.

TABELA P–2 Prompts de shell

Shell	Prompt
Bash shell, Korn shell e Bourne shell	`$`
Bash shell, Korn shell e Bourne shell para o superusuário	`#`
Shell C	`nome_da_máquina%`
Shell C para superusuário	`nome_da_máquina#`

◆ ◆ ◆ CAPÍTULO 1

Visão geral da segurança do Oracle Solaris 11

O Oracle Solaris 11 é um sistema operacional empresarial avançado e pioneiro que oferece recursos de segurança comprovados. Com um sofisticado sistema de segurança de toda a rede que controla a forma como os usuários acessam arquivos, protegem bancos de dados do sistema e usam recursos do sistema, o Oracle Solaris 11 atende aos requisitos de segurança em cada camada. Embora sistemas operacionais tradicionais possam apresentar debilidade de segurança inerente, a flexibilidade do Oracle Solaris 11 permite que ele atenda a diversos objetivos de segurança, desde servidores corporativos até clientes de desktop. O Oracle Solaris 11 foi completamente testado e possui suporte em uma variedade de sistemas baseados em SPARC e x86 de Oracle e em outras plataformas de hardware de fornecedores terceiros.

Proteções de segurança do Oracle Solaris 11

O Oracle Solaris fornece uma base sólida para dados e aplicativos corporativos, protegendo os dados em disco e em trânsito. O Oracle Solaris Resource Manager, denominado *gerenciamento de recursos*, e as Zonas do Oracle Solaris fornecem recursos que separam e protegem aplicativos contra o mau uso. Esse confinamento, juntamente com o privilégio mínimo implementado por meio de privilégios e o recurso de controle de acesso baseado em função (RBAC) do Oracle Solaris, reduzem o risco de segurança das ações de invasores ou de usuários regulares. Os protocolos autenticados e criptografados, como a segurança de IP (IPsec), fornecem redes privadas virtuais (VPNs) por meio da Internet, bem como túneis dentro de uma LAN ou WAN para entrega de dados seguros. Além disso, o recurso de auditoria do Oracle Solaris garante que registros de qualquer atividade de interesse sejam mantidos.

Os serviços de segurança do Oracle Solaris 11 fornecem defesa em profundidade, oferecendo camadas de proteção para o sistema e a rede. O Oracle Solaris protege o kernel, limitando,

dentro de seus utilitários, quais ações privilegiadas o utilitário pode executar. A configuração de rede padrão fornece proteção de dados no sistema e remotamente. A IPsec, o recurso Filtro de IP do Oracle Solaris e o Kerberos podem fornecer proteções adicionais.

Os serviços de segurança do Oracle Solaris incluem:

- Proteção do kernel – os daemons do Kernel e dispositivos são protegidos por permissões de arquivo e privilégios.
- Proteção de logins – os logins requerem senhas. As senhas têm criptografia forte. Os logins remotos são inicialmente limitados a um canal criptografado e autenticados por meio do recurso Secure Shell do Oracle Solaris. A conta `root` não pode fazer login diretamente.
- Proteção de dados - os dados no disco são protegidos por permissões de arquivo. É possível configurar as camadas adicionais de proteção. Por exemplo, é possível usar listas de controle de acesso (ACLs), colocar dados em uma zona, criptografar um arquivo, criptografar um conjunto de dados ZFS do Oracle Solaris, criar um conjunto de dados ZFS de somente leitura e montar sistemas de arquivos para impedir a execução de programas `setuid` e de arquivos executáveis.

Tecnologias de segurança do Oracle Solaris 11

Os recursos de segurança do Oracle Solaris podem ser configurados para implementar a política de segurança da sua empresa.

As seções a seguir fornecem uma breve introdução aos recursos de segurança do Oracle Solaris. As descrições incluem referências a explicações mais detalhadas e a procedimentos contidos neste manual e em outros guias de administração do sistema do Oracle Solaris que demonstram esses recursos.

Serviço de auditoria

A auditoria é a coleta de dados sobre o uso dos recursos do sistema. Os dados de auditoria fornecem um registro de eventos do sistema relacionados à segurança. Em seguida, é possível usar esses dados para atribuir responsabilidade por ações ocorridas em um sistema.

A auditoria é um requisito básico para empresas de avaliação de segurança, validação e certificação. A auditoria também pode deter invasores potenciais.

Para obter mais informações, consulte:

- Para obter uma lista de páginas man relacionadas a auditoria, consulte o Capítulo 29, "Auditing (Reference)," no *Oracle Solaris Administration: Security Services*.
- Para obter diretrizes, consulte "Auditar eventos significativos além de login/logout" na página 35 e as páginas man.

- Para obter uma visão geral da auditoria, consulte o Capítulo 26, "Auditing (Overview)," no *Oracle Solaris Administration: Security Services*.
- Para obter informações sobre tarefas de auditoria, consulte o Capítulo 28, "Managing Auditing (Tasks)," no *Oracle Solaris Administration: Security Services*.

BART (Basic Audit Reporting Tool)

O recurso BART (Basic Audit Reporting Tool) do Oracle Solaris permite validar sistemas de forma abrangente, executando verificações de cinco níveis de um sistema com o decorrer do tempo. Ao criar manifestos BART, é possível reunir informações, com facilidade e de forma confiável, sobre os componentes da pilha de software instalada em sistemas implantados.

BART é uma ferramenta útil para gerenciamento de integridade em um sistema ou em uma rede de sistemas.

Para obter mais informações, consulte:

- As páginas man selecionadas incluem `bart(1M)`, `bart_rules(4)` e `bart_manifest(4)`.
- Para obter diretrizes, consulte "Criação de um instantâneo BART do sistema" na página 49, "Uso da Basic Audit Reporting Tool" na página 51 e as páginas man.
- Para obter uma visão geral de BART, consulte o Capítulo 6, "Verifying File Integrity by Using BART," no *Oracle Solaris Administration: Security Services*.
- Para obter exemplos de uso da BART, consulte "Using BART (Tasks)" no *Oracle Solaris Administration: Security Services* e as páginas man.

Serviços criptográficos

Os recursos Estrutura criptográfica e KMF (Estrutura de gerenciamento de chaves) do Oracle Solaris fornecem repositórios centrais para serviços criptográficos e gerenciamento de chaves. Usuários de hardware, software e finais têm acesso contínuo a algoritmos otimizados. Os diferentes mecanismos de armazenamento, utilitários administrativos e interfaces de programação para várias infraestruturas de chave pública (PKIs) podem usar uma interface unificada ao adotarem interfaces KMF.

A Estrutura criptográfica fornece serviços criptográficos a usuários e aplicativos por meio de comandos individuais, uma interface de programação de nível do usuário, uma interface de programação de kernel e estruturas de nível do kernel e do usuário. A Estrutura criptográfica fornece esses serviços criptográficos a aplicativos e módulos de kernel de forma contínua ao usuário final. Ela também traz serviços criptográficos diretos, como criptografia e descriptografia de arquivos, ao usuário final.

A KMF fornece ferramentas e interfaces de programação para gerenciamento centralizado de objetos de chave pública, como certificados X.509 e pares de chave pública/privada. Os formatos para armazenar esses objetos podem variar. A KMF também fornece uma ferramenta para gerenciamento de políticas que definem o uso de certificados X.509 por aplicativos. A KMF oferece suporte a plugins de terceiros.

Para obter mais informações, consulte:

- As páginas man selecionadas incluem `cryptoadm(1M)`, `encrypt(1)`, `mac(1)`, `pktool(1)` e `kmfcfg(1)`.
- Para obter uma visão geral dos serviços criptografados, consulte o Capítulo 11, "Cryptographic Framework (Overview)," no *Oracle Solaris Administration: Security Services* e o Capítulo 13, "Key Management Framework," no *Oracle Solaris Administration: Security Services*.
- Para obter exemplos de uso da Estrutura criptográfica, consulte o Capítulo 12, "Cryptographic Framework (Tasks)," no *Oracle Solaris Administration: Security Services* e as páginas man.

Permissões de arquivos e entradas de controle de acesso

A primeira linha de defesa para proteger objetos em um sistema de arquivos são as permissões UNIX padrão atribuídas a cada objeto do sistema de arquivos. As permissões UNIX oferecem suporte à atribuição de direitos de acesso exclusivos ao proprietário do objeto, a um grupo atribuído ao objeto e a qualquer outra pessoa. Além disso, a ZFS oferece suporte a listas de controle de acesso (ACLs), também denominadas entradas de controle de acesso (ACEs), que controlam com mais precisão o acesso a objetos individuais ou grupos de objetos do sistema de arquivos.

Para obter mais informações, consulte:

- Para obter instruções sobre a definição de ACLs em arquivos ZFS, consulte a página man `chmod(1)`.
- Para obter uma visão geral das permissões de arquivo, consulte "Using UNIX Permissions to Protect Files" no *Oracle Solaris Administration: Security Services*.
- Para obter uma visão geral e exemplos de proteção de arquivos ZFS, consulte o Capítulo 8, "Using ACLs and Attributes to Protect Oracle Solaris ZFS Files," no *Oracle Solaris Administration: ZFS File Systems* e as páginas man.

Filtragem de pacotes

A filtragem de pacotes fornece proteção básica contra ataques baseados na rede. O Oracle Solaris inclui o recurso Filtro de IP e wrappers TCP.

Filtro de IP

O recurso Filtro de IP do Oracle Solaris cria um firewall para impedir ataques baseados na rede.

Especificamente, o recurso Filtro de IP fornece recursos de filtragem de pacotes com monitoração de estado e pode filtrar pacotes pelo endereço IP ou rede, porta, protocolo, interface de rede e direção do tráfego. Também inclui filtragem de pacotes sem monitoramento de estado e a capacidade de criar e gerenciar pools de endereços. Além disso, o Filtro de IP também tem a capacidade de executar tradução de endereço de rede (NAT) e tradução de endereço de porta (PAT).

Para obter mais informações, consulte:

- As páginas man selecionadas incluem `ipfilter`(5), `ipf`(1M), `ipnat`(1M), `svc.ipfd`(1M) e `ipf`(4).
- Para obter uma visão geral do Filtro de IP, consulte o Capítulo 20, "IP Filter in Oracle Solaris (Overview)," no *Oracle Solaris Administration: IP Services*.
- Para obter exemplos de uso do Filtro de IP, consulte o Capítulo 21, "IP Filter (Tasks)," no *Oracle Solaris Administration: IP Services* e as páginas man.
- Para obter informações e exemplos sobre a sintaxe da linguagem da política do Filtro de IP, consulte a página man `ipnat`(4).

Wrappers TCP

Os wrappers TCP proporcionam uma forma de implementar controles de acesso, com a verificação do endereço de um host que solicita um serviço de rede específico em relação a uma ACL. As solicitações são concedidas ou negadas, conforme o caso. Os wrappers TCP também registram solicitações de host para serviços de rede, o que é uma função de monitoramento útil. Os recursos Secure Shell e `sendmail` do Oracle Solaris são configurados para usar wrappers TCP. Os serviços de rede que podem ser colocados sob controle de acesso incluem `ftpd` e `rpcbind`.

Os wrappers TCP oferecem suporte a uma rica linguagem de política de configuração que permite às empresas especificar uma política de segurança globalmente e com base em serviço. É possível permitir ou restringir acesso adicional a serviços com base no nome do host, endereço IPv4 ou IPv6, nome do grupo de rede, rede e até domínio DNS.

Para obter mais informações, consulte:

- Para obter informações sobre wrappers TCP, consulte "How to Use TCP Wrappers to Control Access to TCP Services" no *Oracle Solaris Administration: IP Services*.
- Para obter informações e exemplos da sintaxe da linguagem de controle de acesso para wrappers TCP, consulte a página man `hosts_access`(4).

Senhas e restrições de senha

Senhas de usuário fortes ajudam na proteção contra ataques envolvendo adivinhação por força bruta.

O Oracle Solaris tem vários recursos que podem ser usados na criação de senhas fortes para os usuários. É possível definir os requisitos de tamanho, de conteúdo, de frequência de alteração e de modificação da senha e manter um histórico de senhas. É fornecido um dicionário de senhas a serem evitadas. Vários algoritmos de senha possíveis estão disponíveis.

Para obter mais informações, consulte:

- "Maintaining Login Control" no *Oracle Solaris Administration: Security Services*
- "Securing Logins and Passwords (Tasks)" no *Oracle Solaris Administration: Security Services*
- As páginas man selecionadas incluem `passwd(1)` e `crypt.conf(4)`.

Módulo de autenticação conectável

A estrutura do PAM (Módulo de autenticação conectável) permite coordenar e configurar requisitos de autenticação de usuários para contas, credenciais, sessões e senhas.

A estrutura do PAM permite que as organizações personalizem a experiência de autenticação de usuários, bem como a funcionalidade de gerenciamento de contas, sessões e senhas. Os serviços de entrada do sistema, como `login` e `ftp` usam a estrutura do PAM para garantir que todos os pontos de entrada do sistema sejam protegidos. Essa arquitetura permite a substituição ou a modificação de módulos de autenticação no campo para proteger o sistema contra todas as vulnerabilidades recém-localizadas, sem exigir alterações em nenhum serviço do sistema que use a estrutura do PAM.

Para obter mais informações, consulte:

- Capítulo 14, "Using PAM," no *Oracle Solaris Administration: Security Services*
- Página man `pam.conf(4)`

Privilégios do Oracle Solaris

Os privilégios são direitos refinados e discretos em processos reforçados no kernel. O Oracle Solaris define mais de 80 privilégios, desde básicos como `file_read` a mais especializados como `proc_clock_highres`. É possível conceder privilégios a um comando, usuário, função ou sistema. Muitos comandos e daemons do Oracle Solaris são executados com apenas os privilégios necessários à execução de sua tarefa. O uso de privilégios também é chamado de *gerenciamento de direitos de processo*.

Programas habilitados para privilégios podem evitar que invasores obtenham mais privilégios do que os usados pelo próprio programa. Além disso, os privilégios permitem que as empresas limitem quais privilégios são concedidos a serviços e processos executados em seus sistemas.

Para obter mais informações, consulte:

- "Privileges (Overview)" no *Oracle Solaris Administration: Security Services*
- "Using Privileges (Tasks)" no *Oracle Solaris Administration: Security Services*
- Capítulo 2, "Developing Privileged Applications," no *Developer's Guide to Oracle Solaris 11 Security*
- As páginas man selecionadas incluem `ppriv(1)` e `privileges(5)`.

Acesso remoto

Os ataques de acesso remoto podem danificar sistemas e redes. A proteção do acesso de rede é necessária no ambiente de Internet atual e é útil mesmo em ambientes WAN e LAN.

IPsec e IKE

A segurança de IP (IPsec) protege os pacotes de IPs autenticando e/ou criptografando esses pacotes. O Oracle Solaris oferece suporte à IPsec para IPv4 e IPv6. Como a IPsec é implementada bem abaixo da camada de aplicativos, os aplicativos da Internet podem utilizar a IPsec sem exigir modificações no código.

A IPsec e seu protocolo de troca de chaves, o IKE, usam algoritmos da Estrutura criptográfica. Além disso, a Estrutura criptográfica fornece um armazenamento de chaves softtoken para aplicativos que usam o metaslot. Quando o IKE é configurado para usar o metaslot, as empresas têm a opção de armazenar as chaves em disco, em um armazenamento de chaves de hardware conectado ou no armazenamento de chaves softtoken.

Quando administrada de forma correta, a IPsec é uma ferramenta eficaz para proteger o tráfego de rede.

Para obter mais informações, consulte:

- Capítulo 14, "IP Security Architecture (Overview)," no *Oracle Solaris Administration: IP Services*
- Capítulo 15, "Configuring IPsec (Tasks)," no *Oracle Solaris Administration: IP Services*
- Capítulo 17, "Internet Key Exchange (Overview)," no *Oracle Solaris Administration: IP Services*
- Capítulo 18, "Configuring IKE (Tasks)," no *Oracle Solaris Administration: IP Services*
- As páginas man selecionadas incluem `ipsecconf`(1M) e `in.iked`(1M).

Secure Shell

O recurso Secure Shell do Oracle Solaris permite que usuários ou serviços acessem ou transfiram arquivos entre sistemas remotos por um canal de comunicações criptografadas. No Secure Shell, todo o tráfego de rede é criptografado. O Secure Shell também pode ser usado como uma rede privada virtual sob demanda (VPN) que pode encaminhar tráfego do sistema X Window ou conectar números de portas individuais entre sistemas remotos por um link de rede autenticado e criptografado.

Dessa forma, o Secure Shell evita que um possível invasor leia uma comunicação interceptada e que um concorrente falsifique o sistema. Por padrão, o Secure Shell é o único mecanismo de acesso remoto ativo em um sistema recém-instalado.

Para obter mais informações, consulte:

- Capítulo 15, "Using Secure Shell," no *Oracle Solaris Administration: Security Services*
- As páginas man selecionadas incluem `ssh(1)`, `sshd(1M)`, `sshd_config(4)` e `ssh_config(4)`.

Serviço Kerberos

O recurso Kerberos do Oracle Solaris permite logon único e transações seguras, mesmo em redes heterogêneas que executam o serviço Kerberos.

O Kerberos é baseado no protocolo de autenticação de rede Kerberos V5 desenvolvido no Massachusetts Institute of Technology (MIT). O serviço Kerberos é uma arquitetura cliente-servidor que fornece transações seguras em redes. O serviço oferece autenticação forte de usuário, bem como integridade e privacidade. Usando o serviço Kerberos, é possível fazer login uma vez e acessar outros sistemas, executar comandos, trocar dados e transferir arquivos com segurança. Além disso, o serviço permite que os administradores restrinjam o acesso a serviços e sistemas.

Para obter mais informações, consulte:

- Parte VI, "Kerberos Service," no *Oracle Solaris Administration: Security Services*
- As páginas man selecionadas incluem `kerberos(5)` e `kinit(1)`.

Controle de acesso baseado em função

O RBAC aplica o princípio de segurança de privilégio mínimo, permitindo que as empresas concedam, de forma seletiva, direitos a usuários ou funções de acordo com as necessidades e requisitos exclusivos.

O recurso RBAC (controle de acesso baseado em função) do Oracle Solaris controla o acesso do usuário a tarefas que, normalmente, estariam restritas à função `root`. Ao aplicar atributos de segurança a processos e usuários, o RBAC pode distribuir direitos administrativos entre vários administradores. O RBAC também é denominado *gerenciamento de direitos de usuário*.

Para obter mais informações, consulte:

- Parte III, "Roles, Rights Profiles, and Privileges," no *Oracle Solaris Administration: Security Services*
- As páginas man selecionadas incluem `rbac`(5), `roleadd`(1M), `profiles`(1) e `user_attr`(4).

SMF (Service Management Facility)

O recurso SMF (Service Management Facility) do Oracle Solaris é usado para adicionar, remover, configurar e gerenciar serviços. O SMF usa o RBAC para controlar o acesso a funções de gerenciamento de serviços do sistema. Especificamente, o SMF usa autorizações para determinar quem pode gerenciar um serviço e quais funções essa pessoa pode executar.

O SMF permite que as empresas controlem o acesso a serviços e como os serviços são iniciados, parados ou atualizados.

Para obter mais informações, consulte:

- Capítulo 6, "Managing Services (Overview)," no *Oracle Solaris Administration: Common Tasks*
- Capítulo 7, "Managing Services (Tasks)," no *Oracle Solaris Administration: Common Tasks*
- As páginas man selecionadas incluem `svcadm`(1M), `svcs`(1) e `smf`(5).

Sistema de arquivos ZFS do Oracle Solaris

O ZFS é o sistema de arquivos padrão do Oracle Solaris 11. O sistema de arquivos ZFS basicamente altera a forma como os sistemas de arquivos do Oracle Solaris são administrados. O ZFS é robusto, dimensionável e fácil de administrar. Como a criação do sistema de arquivos em ZFS é leve, é possível estabelecer cotas e espaço reservado com facilidade. Permissões UNIX e ACE protegem arquivos, e o RBAC oferece suporte à administração delegada de conjuntos de dados ZFS.

Para obter mais informações, consulte:

- Capítulo 1, "Oracle Solaris ZFS File System (Introduction)," no *Oracle Solaris Administration: ZFS File Systems*
- Capítulo 3, "Oracle Solaris ZFS and Traditional File System Differences," no *Oracle Solaris Administration: ZFS File Systems*
- Capítulo 6, "Managing Oracle Solaris ZFS File Systems," no *Oracle Solaris Administration: ZFS File Systems*
- As páginas man selecionadas incluem `zfs`(1M) e `zfs`(7FS).

Zonas do Oracle Solaris

A tecnologia de particionamento de software em zonas do Oracle Solaris permite manter o modelo de implantação de um aplicativo por servidor e compartilhar, simultaneamente, recursos do hardware.

Zonas são ambientes operacionais virtualizados que permitem a execução de vários aplicativos isoladamente no mesmo hardware físico. Esse isolamento evita que os processos executados em uma zona monitorem ou afetem processos executados em outras zonas, visualizem dados uns dos outros ou manipulem o hardware subjacente. As zonas também fornecem uma camada de abstração que separa aplicativos de atributos físicos do sistema no qual eles estão implantados, como caminhos de dispositivos físicos e nomes de interfaces de rede.

Para obter mais informações, consulte:

- Parte II, "Oracle Solaris Zones," no *Oracle Solaris Administration: Oracle Solaris Zones, Oracle Solaris 10 Zones, and Resource Management*
- As páginas man selecionadas incluem `brands(5)`, `zoneadm(1M)` e `zonecfg(1M)`.

Trusted Extensions

O recurso Trusted Extensions do Oracle Solaris é uma camada opcionalmente ativada de tecnologia de rotulamento seguro que permite que políticas de segurança de dados sejam separadas da propriedade dos dados. O Trusted Extensions oferece suporte a políticas de controle de acesso condicional tradicional (DAC) baseadas em propriedade, bem como políticas de controle de acesso obrigatório baseado em rótulo (MAC). A menos que a camada de Trusted Extensions seja ativada, todos os rótulos são iguais, dessa forma, o kernel não é configurado para reforçar as políticas MAC. Quando as políticas MAC baseadas em rótulo são ativadas, todos os fluxos de dados são restritos com base em uma comparação dos rótulos associados aos processos (sujeitos) que solicitam acesso e objetos que contêm os dados. Diferentemente da maioria dos outros sistemas operacionais, o Trusted Extensions inclui uma área de trabalho multinível.

O Trusted Extensions atende aos requisitos do LSPP (Common Criteria Labeled Security Protection Profile), do RBACPP (Role-Based Access Protection Profile) e do CAPP (Controlled Access Protection Profile). No entanto, a implementação do Trusted Extensions é exclusiva em sua capacidade de fornecer alta garantia, maximizando, ao mesmo tempo, a compatibilidade e minimizando a sobrecarga.

Para obter mais informações, consulte:

- Para obter informações sobre a configuração e a manutenção do Trusted Extensions, consulte *Trusted Extensions Configuration and Administration* .
- Para obter informações sobre o uso da área de trabalho multinível, consulte o *Trusted Extensions User's Guide* .

- As páginas man selecionadas incluem `trusted_extensions(5)` e `labeld(1M)`.

Padrões de segurança do Oracle Solaris 11

Após a instalação, o Oracle Solaris protege o sistema contra invasões e monitora tentativas de login, entre outros recursos de segurança.

O acesso ao sistema é limitado e monitorado

Contas de usuário inicial e da função `root` – a conta de usuário final pode fazer login a partir do console. É atribuída a essa conta a função `root`. As senhas para as duas contas são inicialmente idênticas.

- Após o login, o usuário inicial pode assumir a função `root` para definir mais configurações do sistema. Ao assumir a função, o usuário é solicitado a alterar a senha `root`. Observe que nenhuma função pode fazer login diretamente, nem a função `root`.
- São atribuídos padrões do arquivo `/etc/security/policy.conf` ao usuário inicial. Os padrões incluem os perfis de direitos Usuário do Solaris básico e Usuário do console. Esses perfis de direitos permitem que os usuários leiam e gravem em um CD ou DVD, executem qualquer comando no sistema sem privilégio e parem e reiniciem o sistema a partir do console.
- A conta de usuário inicial também recebe o perfil de direitos Administrador do sistema. Dessa forma, sem assumir a função `root`, o usuário final tem alguns direitos administrativos, como o de instalar software e gerenciar o serviço de cadastramento.

Requisitos de senha – as senhas dos usuários devem ter, pelo menos, seis caracteres e um caractere alfabético e um numérico. As senhas são hash, usando o algoritmo `SHA256` . Ao alterarem a senha, todos os usuários, inclusive a função `root`, devem atender a esses requisitos.

Acesso de rede limitado – após a instalação, o sistema é protegido contra invasões pela rede. O login remoto feito pelo usuário inicial é permitido por uma conexão autenticada e criptografada com o protocolo `ssh`. Esse é o único protocolo de rede que aceita pacotes de entrada. A chave `ssh` é encapsulada pelo algoritmo `AES128`. Com a criptografia e autenticação ativadas, o usuário pode acessar o sistema sem intercepção, modificação nem falsificação.

Tentativas de login registradas – o serviço de auditoria é ativado para todos os eventos de `login/logoff` (login, logoff, troca de usuário, início e interrupção de uma sessão `ssh` e bloqueio de telas) e para todos os logins não atribuíveis (com falha). Como a função `root` não pode fazer login, o nome do usuário que está agindo como `root` pode ser rastreado na trilha de auditoria. O usuário inicial pode revisar os logs de auditoria por um direito concedido pelo perfil Administrador do sistema.

Proteções ativadas para kernel, arquivos e área de trabalho

Depois que o usuário inicial faz login, o kernel, os sistemas de arquivos e os aplicativos da área de trabalho são protegidos pelo privilégio mínimo, pelas permissões e pelo RBAC (controle de acesso baseado em função).

Proteções do kernel – muitos daemons e comandos administrativos recebem apenas os privilégios que lhes permitem operar com êxito. Muitos daemons são executados em contas administrativas especiais que não têm privilégios `root` (`UID=0`), portanto, eles não podem ser forçados a executar outras tarefas. Essas contas administrativas especiais não podem fazer login. Os dispositivos são protegidos por privilégios.

Sistemas de arquivos – por padrão, todos os sistemas de arquivos são ZFS. O `umask` do usuário é `022`, dessa forma, quando um usuário cria um novo arquivo ou diretório, apenas o usuário pode modificá-lo. Os membros do grupo do usuário podem ler e pesquisar o diretório, bem como ler o arquivo. Os logins externos ao grupo do usuário podem listar o diretório e ler o arquivo. As permissões de diretório são `drwxr-xr-x` (`755`). As permissões de arquivo são `-rw-r--r--` (`644`).

Miniaplicativos de área de trabalho – os miniaplicativos de área de trabalho são protegidos pelo RBAC. Por exemplo, apenas o usuário inicial ou a função `root` pode usar o miniaplicativo Package Manager para instalar novos pacotes. O Package Manager não é exibido para usuários regulares que não têm os direitos para usá-lo.

Recursos de segurança adicionais ativados

O Oracle Solaris 11 fornece recursos de segurança que podem ser usados para configurar seus sistemas e usuários para atender aos requisitos de segurança da empresa.

- **RBAC (controle de acesso baseado em função) –** o Oracle Solaris fornece várias autorizações, privilégios e perfis de direitos. `root` é a única função definida. Os perfis de direitos são uma boa base para as funções criadas. Além disso, alguns comandos administrativos requerem autorizações RBAC para operar com êxito. Os usuários sem autorizações não podem executar os comandos, mesmo que os usuários tenham os privilégios necessários.
- **Direitos de usuários –** os usuários recebem um conjunto básico de privilégios, perfis de direitos e autorizações do arquivo `/etc/security/policy.conf`, como o usuário inicial, conforme descrito em "O acesso ao sistema é limitado e monitorado" na página 21. As tentativas de login do usuário não são limitadas, mas todos os logins malsucedidos são registrados pelo serviço de auditoria.
- **Proteção de arquivos do sistema –** os arquivos do sistema são protegidos por permissões de arquivo. Somente a função `root` pode modificar os arquivos de configuração do sistema.

Prática e política de segurança da empresa

Para obter um sistema seguro ou uma rede de sistemas segura, a sua empresa deve ter uma política de segurança em vigor, com práticas de segurança que apoiem a política.

Para obter mais informações, consulte o que se segue:

- Apêndice A, "Site Security Policy," no *Trusted Extensions Configuration and Administration*
- "Security Requirements Enforcement" no *Trusted Extensions Configuration and Administration*
- Mantendo Seu Código Seguro (`http://blogs.oracle.com/maryanndavidson/entry/those_who_can_t_do`)

◆ ◆ ◆ CAPÍTULO 2

Configuração da segurança do Oracle Solaris 11

Este capítulo descreve as ações a serem executadas para configurar a segurança do sistema. O capítulo aborda a instalação de pacotes, a configuração do sistema em si, a configuração de vários subsistemas e aplicativos adicionais que possam ser necessários, como a IPsec.

Instalando o SO Oracle Solaris

Ao instalar o SO Oracle Solaris, escolha a mídia que instala o pacote de *grupos* apropriado:

- **Oracle Solaris Servidor de Grande Porte –** O manifesto padrão em uma instalação do AI (Automated Installer) e o instalador de texto instalam o grupo `group/system/solaris-large-server`, que fornece um ambiente de servidor Oracle Solaris de grande porte.
- **Oracle Solaris Área de Trabalho –** O Live Media instala o grupo `group/system/solaris-desktop`, o qual fornece um ambiente de área de trabalho Oracle Solaris 11.

  Para criar um sistema de área de trabalho para uso centralizado, adicione o grupo `group/feature/multi-user-desktop` a um servidor Oracle Solaris. Para obter mais informações, consulte o artigo Optimizing the Oracle Solaris 11 Desktop for a Multiuser Environment.

Para uma instalação automatizada usando o AI (Automated Installer), consulte a Parte III, "Installing Using an Install Server," no *Installing Oracle Solaris 11 Systems*.

Para orientar sua escolha de mídia, consulte os seguintes guias de instalação:

- *Installing Oracle Solaris 11 Systems*
- *Creating a Custom Oracle Solaris 11 Installation Image*
- *Adding and Updating Oracle Solaris 11 Software Packages*

Proteção do sistema

As tarefas a seguir têm melhores resultados quando executadas em ordem sequencial. Nesse ponto, o SO Oracle Solaris 11 já está instalado, e apenas o usuário inicial, que pode assumir a função `root`, tem acesso ao sistema.

Tarefa	Descrição	Instruções
1. Verificar os pacotes no sistema.	Verifica se os pacotes da mídia de instalação são idênticos aos pacotes instalados.	"Verificar os pacotes" na página 26
2. Proteger as configurações de hardware no sistema.	Protege o hardware exigindo uma senha para alterar as configurações de hardware.	"Controlling Access to System Hardware (Tasks)" no *Oracle Solaris Administration: Security Services*
3. Desativar os serviços desnecessários.	Impede a execução de processos que não fazem parte das funções necessárias do sistema.	"Desativar serviços desnecessários" na página 27
4. Exigir alocação de dispositivos.	Impede o uso de mídia removível sem autorização explícita. Dispositivos incluem microfones, unidades USB e CDs.	"How to Enable Device Allocation" no *Oracle Solaris Administration: Security Services*
5. Impedir que o proprietário da estação de trabalho desligue o sistema.	Impede que o usuário do console desligue ou suspenda o sistema.	"Remover a capacidade de gerenciamento de energia dos usuários" na página 27
6. Crie uma mensagem de aviso de login que reflita a política de segurança do seu site.	Notifica os usuários e possíveis invasores de que o sistema é monitorado.	"Colocar uma Mensagem de Segurança em Arquivos de Banner" na página 28 "Colocar Mensagem de Segurança na Tela de Login da Área de Trabalho" na página 29

▼ Verificar os pacotes

Logo após a instalação, valide a instalação verificando os pacotes.

Antes de começar É necessário estar na função `root`.

1. **Execute o comando `pkg verify`.**

   Para manter um registro, envie a saída do comando para um arquivo.

   ```
   # pkg verify > /var/pkgverifylog
   ```

2. **Verifique se há erros no registro.**

3. **Se encontrar erros, reinstale a partir da mídia ou corrija-os.**

Consulte também Para obter mais informações, consulte as páginas man `pkg`(1) e `pkg`(5). As páginas man contêm exemplos de uso do comando `pkg verify`.

▼ Desativar serviços desnecessários

Siga este procedimento para desativar serviços desnecessários, levando em conta a finalidade do sistema.

Antes de começar É necessário estar na função `root`.

1. **Liste os serviços on-line.**

   ```
   # svcs | grep network
   online         Sep_07   svc:/network/loopback:default
   ...
   online         Sep_07   svc:/network/ssh:default
   ```

2. **Desative os serviços que não são necessários ao sistema.**

   Por exemplo, se o sistema não for um servidor NFS nem um servidor Web e os serviços estiverem on-line, desative-os.

   ```
   # svcadm disable svc:/network/nfs/server:default
   # svcadm disable svc:/network/http:apache22
   ```

Consulte também Para obter mais informações, consulte o Capítulo 6, "Managing Services (Overview)," no *Oracle Solaris Administration: Common Tasks* e a página man `svcs`(1).

▼ Remover a capacidade de gerenciamento de energia dos usuários

Siga este procedimento para impedir que os usuários desse sistema o suspendam ou desliguem.

Antes de começar É necessário estar na função `root`.

1. **Revise o conteúdo do perfil de direitos Usuário do console.**

```
% getent prof_attr | grep Console
Console User:RO::Manage System as the Console User:
profiles=Desktop Removable Media User,Suspend To RAM,Suspend To Disk,
Brightness,CPU Power Management,Network Autoconf User;
auths=solaris.system.shutdown;help=RtConsUser.html
```

2. **Crie um perfil de direitos que inclua todos os direitos contidos no perfil Usuário do console que os usuários deverão manter.**

   Para obter instruções, consulte "How to Create or Change a Rights Profile" no *Oracle Solaris Administration: Security Services*.

3. **Comente o perfil de direitos Usuário do console no arquivo `/etc/security/policy.conf`.**

```
#CONSOLE_USER=Console User
```

4. **Atribua aos usuários o perfil de direitos criado na Etapa 2.**

```
# usermod -P +new-profile username
```

Consulte também Para obter mais informações, consulte as páginas man "policy.conf File" no *Oracle Solaris Administration: Security Services* e `policy.conf`(4) e `usermod`(1M).

▼ Colocar uma Mensagem de Segurança em Arquivos de Banner

Siga este procedimento para criar mensagens de aviso que reflitam a política de segurança da sua empresa. O conteúdo desses arquivos é exibido no login local e remoto.

Observação – As mensagens de exemplo contidas neste procedimento não atendem aos requisitos do governo dos Estados Unidos e, provavelmente, não atenderão à sua política de segurança.

Antes de começar É necessário estar na função `root`. A prática recomendada é consultar o conselho jurídico da sua empresa sobre o conteúdo da mensagem de segurança.

1. **Digite uma mensagem de segurança no arquivo `/etc/issue`.**

```
# vi /etc/issue
      ALERT   ALERT   ALERT   ALERT   ALERT

This machine is available to authorized users only.

If you are an authorized user, continue.

Your actions are monitored, and can be recorded.
```

Para obter mais informações, consulte a página man `issue(4)`.

O programa `telnet` exibe o conteúdo do arquivo `/etc/issue` como sua mensagem de login. Para usar esse arquivo com outros aplicativos, consulte "Exibir Mensagem de Segurança para Usuários `ssh` e `ftp`" na página 39 e "Colocar Mensagem de Segurança na Tela de Login da Área de Trabalho" na página 29.

2 Adicione uma mensagem de segurança ao arquivo `/etc/motd`.

```
# vi /etc/motd
This system serves authorized users only. Activity is monitored and reported.
```

▼ Colocar Mensagem de Segurança na Tela de Login da Área de Trabalho

Escolha um método para criar uma mensagem de segurança a ser exibida aos usuários durante o login.

Para obter mais informações, clique em Sistema > menu Ajuda na área de trabalho para acessar o Navegador da Ajuda do GNOME. Você também pode usar o comando `yelp`. Os scripts de login da área de trabalho são discutidos na seção `GDM Login Scripts and Session Files` da página man `gdm`(1M).

Observação – A mensagem de exemplo contida neste procedimento não atende aos requisitos do governo dos Estados Unidos e, provavelmente, não atenderá à sua política de segurança.

Antes de começar É necessário estar na função `root`. A prática recomendada é consultar o conselho jurídico da sua empresa sobre o conteúdo da mensagem de segurança.

- **Coloque uma mensagem de segurança na tela de login da área de trabalho**

  Você tem várias opções. As opções que criam uma caixa de diálogo podem usar o arquivo `/etc/issue` da Etapa 1 de "Colocar uma Mensagem de Segurança em Arquivos de Banner" na página 28.

  - **OPÇÃO 1: Crie um arquivo de área de trabalho que exiba a mensagem de segurança em uma caixa de diálogo durante o login.**

    ```
    # vi /usr/share/gdm/autostart/LoginWindow/banner.desktop
    [Desktop Entry]
    Type=Application
    Name=Banner Dialog
    Exec=/usr/bin/zenity --text-info --width=800 --height=300 \
    --title="Security Message" \
    --filename=/etc/issue
    OnlyShowIn=GNOME;
    X-GNOME-Autostart-Phase=Application
    ```

Depois de ser autenticado na janela de login, o usuário deverá fechar a caixa de diálogo para acessar o espaço de trabalho. Para obter opções para o comando `zenity`, consulte a página man `zenity`(1).

- **OPÇÃO 2: Modifique um script de inicialização GDM para exibir a mensagem de segurança em uma caixa de diálogo.**

  O diretório `/etc/gdm` contém três scripts de inicialização que exibem a mensagem de segurança antes, durante ou imediatamente após o login na área de trabalho. Esses scripts também estão disponíveis na release Oracle Solaris 10.

  - **Exiba a mensagem de segurança antes que a tela de login apareça.**

    ```
    # vi /etc/gdm/Init/Default
    /usr/bin/zenity --text-info --width=800 --height=300 \
    --title="Security Message" \
    --filename=/etc/issue
    ```

  - **Exiba a mensagem de segurança na tela de login após a autenticação.**

    Este script é executado antes da exibição do espaço de trabalho do usuário. Você modifica o script `Default.sample` para criar este script.

    ```
    # vi /etc/gdm/PostLogin/Default
    /usr/bin/zenity --text-info --width=800 --height=300 \
    --title="Security Message" \
    --filename=/etc/issue
    ```

  - **Exiba a mensagem de segurança no espaço de trabalho inicial do usuário após a autenticação.**

    ```
    # vi /etc/gdm/PreSession/Default
    /usr/bin/zenity --text-info --width=800 --height=300 \
    --title="Security Message" \
    --filename=/etc/issue
    ```

    Observação – A caixa de diálogo pode ser coberta por janelas no espaço de trabalho do usuário.

- **OPÇÃO 3: Modifique a janela de login para exibir a mensagem de segurança acima do campo de entrada.**

  A janela de login expande para ajustar sua mensagem. Este método não aponta para o arquivo `/etc/issue`. Você deve digitar o texto na GUI.

Observação – A janela de login, `gdm-greeter-login-window.ui`, é sobregravada pelos comandos `pkg fix` e `pkg update`. Para preservar suas alterações, copie o arquivo para um diretório de arquivos de configuração e mescle suas alterações com o novo arquivo após fazer upgrade do sistema. Para obter mais informações, consulte a página man `pkg`(5).

a. Altere o diretório para a interface de usuário da janela de login.

```
# cd /usr/share/gdm
```

b. (Opcional) Salve uma cópia da Interface de Usuário da janela de login original.

```
# cp gdm-greeter-login-window.ui /etc/gdm/gdm-greeter-login-window.ui.orig
```

c. Adicione um rótulo à janela de login usando o designer de interface do GNOME Toolkit.

O programa `glade-3` abre o designer de interface do GTK+. Você digita a mensagem de segurança em um rótulo exibido acima do campo de entrada do usuário.

```
# /usr/bin/glade-3 /usr/share/gdm/gdm-greeter-login-window.ui
```

Para verificar o guia do designer de interface, clique em Desenvolvimento no Navegador da Ajuda do GNOME. A página man `glade-3`(1) está listada em Aplicativos na Páginas Man.

d. (Opcional) Após modificar a GUI da janela de login, salve uma cópia.

```
# cp gdm-greeter-login-window.ui /etc/gdm/gdm-greeter-login-window.ui.site
```

Exemplo 2–1 Criando uma Mensagem de Aviso Curta no Login da Área de Trabalho

Neste exemplo, o administrador digita uma mensagem curta como um argumento para o comando `zenity` no arquivo de área de trabalho. O administrador também usa a opção `--warning`, que exibe um ícone de aviso com a mensagem.

```
# vi /usr/share/gdm/autostart/LoginWindow/bannershort.desktop
[Desktop Entry]
Type=Application
Name=Banner Dialog
Exec=/usr/bin/zenity --warning --width=800  --height=150 --title="Security Message" \
--text="This system serves authorized users only. Activity is monitored and reported."
OnlyShowIn=GNOME;
X-GNOME-Autostart-Phase=Application
```

Proteção dos usuários

Nesse ponto, somente o usuário inicial, que pode assumir a função `root`, tem acesso ao sistema. Para que os usuários regulares possam fazer login, execute as tarefas a seguir em ordem sequencial.

Tarefa	Descrição	Instruções
Exigir senhas fortes e alterações frequentes da senha.	Reforça as restrições de senha padrão em cada sistema.	"Definir restrições de senha mais fortes" na página 32
Configurar permissões de arquivo restritivas para usuários regulares.	Define um valor mais restritivo do que `022` para as permissões de arquivo de usuários regulares.	"Definir um valor `umask` mais restritivo para usuários regulares" na página 34.

Tarefa	Descrição	Instruções
Definir o bloqueio de contas para usuários regulares.	Em sistemas não usados para administração, define o bloqueio de contas em todo o sistema e reduz o número de logins que ativam o bloqueio.	"Definir o bloqueio de contas para usuários regulares" na página 33
Pré-selecionar classes de auditoria adicionais.	Fornece melhores formas de monitoramento e registro de ameaças potenciais ao sistema.	"Auditar eventos significativos além de login/logout" na página 35
Enviar resumos de texto dos eventos de auditoria ao utilitário `syslog`.	Fornece cobertura em tempo real de eventos de auditoria significativos, como logins e tentativas de login.	"Monitorar os eventos `lo` em tempo real" na página 36
Criar funções.	Distribui tarefas administrativas distintas para alguns usuários confiáveis, de forma que ninguém possa danificar o sistema.	"Setting Up User Accounts" no *Oracle Solaris Administration: Common Tasks* "How to Create a Role" no *Oracle Solaris Administration: Security Services* "How to Assign a Role" no *Oracle Solaris Administration: Security Services*.
Mostrar os aplicativos permitidos apenas na área de trabalho de um usuário.	Impede que os usuários vejam ou usem aplicativos que eles não tenham autorização para usar.	Consulte "How to Limit a User to Desktop Applications" no *Trusted Extensions Configuration and Administration*.
Limitar os privilégios de um usuário.	Remove os privilégios básicos que não são necessários aos usuários.	"Remover privilégios básicos desnecessários de usuários" na página 37

▼ Definir restrições de senha mais fortes

Siga este procedimento se os padrões não atenderem aos requisitos de segurança da sua empresa. As etapas seguem a lista de entradas no arquivo `/etc/default/passwd` .

Antes de começar Antes de alterar os padrões, verifique se as alterações permitem que todos os usuários façam a autenticação em seus aplicativos e em outros sistemas na rede.

É necessário estar na função `root`.

- **Edite o arquivo `/etc/default/passwd`.**

  a. **Exija que os usuários alterem as senhas todos os meses, mas não mais do que a cada três semanas.**

  ```
  ## /etc/default/passwd
  ##
  MAXWEEKS=
  MINWEEKS=
  ```

```
MAXWEEKS=4
MINWEEKS=3
```

b. Exija uma senha de, pelo menos, oito caracteres.

```
#PASSLENGTH=6
PASSLENGTH=8
```

c. Mantenha um histórico de senhas.

```
#HISTORY=0
HISTORY=10
```

d. Exija uma diferença mínima da última senha.

```
#MINDIFF=3
MINDIFF=4
```

e. Exija, pelo menos, uma letra maiúscula.

```
#MINUPPER=0
MINUPPER=1
```

f. Exija, pelo menos, um dígito.

```
#MINDIGIT=0
MINDIGIT=1
```

Consulte também

- Para obter a lista de variáveis que restringem a criação de senhas, consulte o arquivo `/etc/default/passwd`. Os padrões são indicados no arquivo.
- Para aplicar as restrições de senha após a instalação, consulte "O acesso ao sistema é limitado e monitorado" na página 21.
- Página man `passwd(1)`

▼ Definir o bloqueio de contas para usuários regulares

Siga este procedimento para bloquear contas de usuários regulares após determinado número de tentativas de login malsucedidas.

Observação – Não defina o bloqueio de contas para usuários que possam assumir funções, pois isso bloqueará a função.

Antes de começar É necessário estar na função `root`. Não defina essa proteção em todo o sistema usado para atividades administrativas.

1. **Defina o atributo de segurança `LOCK_AFTER_RETRIES` como `YES`.**

   - **Defina em todo o sistema.**

     ```
     # vi /etc/security/policy.conf
     ...
     #LOCK_AFTER_RETRIES=NO
     LOCK_AFTER_RETRIES=YES
     ...
     ```

   - **Defina por usuário.**

     ```
     # usermod -K lock_after_retries=yes username
     ```

2. **Defina o atributo de segurança `RETRIES` como `3` .**

   ```
   # vi /etc/default/login
   ...
   #RETRIES=5
   RETRIES=3
   ...
   ```

Consulte também

- Para ler uma discussão sobre atributos de segurança de usuário e função, consulte o Capítulo 10, "Security Attributes in Oracle Solaris (Reference)," no *Oracle Solaris Administration: Security Services*.
- As páginas man selecionadas incluem `policy.conf`(4) e `user_attr`(4).

▼ Definir um valor umask mais restritivo para usuários regulares

Se o valor `umask` padrão, `022`, não for restritivo o suficiente, defina uma máscara mais restritiva seguindo este procedimento.

Antes de começar É necessário estar na função `root`.

- **Modifique o valor umask nos perfis de login dos diretórios esqueleto para os diferentes shells.**

  Oracle Solaris fornece diretórios para que os administradores personalizem padrões de shell do usuário. Esses diretórios esqueleto incluem arquivos, como `.profile` , `.bashrc` e `.kshrc`.

  Escolha um dos seguintes valores:

  - `umask 027` – fornece proteção de arquivos moderada

    (`740`) – `w` para grupos, `rwx` para outros
  - `umask 026` – fornece uma proteção de arquivos um pouco mais rígida

    (`741`) – `w` para grupos, `rw` para outros
  - `umask 077` – fornece uma proteção de arquivos mais completa

(`700`) – nenhum acesso para grupos e para outros

Consulte também Para obter mais informações, consulte:

- "Setting Up User Accounts" no *Oracle Solaris Administration: Common Tasks*
- "Default umask Value" no *Oracle Solaris Administration: Security Services*
- As páginas man selecionadas incluem `usermod`(1M) e `umask`(1).

▼ Auditar eventos significativos além de login/logout

Siga este procedimento para auditar comandos administrativos, tentativas de invadir o sistema e outros eventos significativos, conforme especificado pela política de segurança da sua empresa.

Observação – Os exemplos neste procedimento podem não ser suficientes para atender à sua política de segurança.

Antes de começar É necessário estar na função `root`. Você está implementando a política de segurança da sua empresa em relação a auditoria.

1. **Audite todos os usos de comandos privilegiados por usuários e funções.**

   Para todos os usuários e funções, adicione o evento de auditoria `AUE_PFEXEC` à sua máscara de pré-seleção.

   ```
   # usermod -K audit_flags=lo,ps:no username

   # rolemod -K audit_flags=lo,ps:no rolename
   ```

2. **Registre os argumentos para comandos auditados.**

   ```
   # auditconfig -setpolicy +argv
   ```

3. **Registre o ambiente no qual os comandos auditados são executados.**

   ```
   # auditconfig -setpolicy +arge
   ```

Consulte também

- Para obter informações sobre política de auditoria, consulte "Audit Policy" no *Oracle Solaris Administration: Security Services*.
- Para obter exemplos de definição de sinalizadores de auditoria, consulte "Configuring the Audit Service (Tasks)" no *Oracle Solaris Administration: Security Services* e "Troubleshooting the Audit Service (Tasks)" no *Oracle Solaris Administration: Security Services*.
- Para configurar a auditoria, consulte a página man `auditconfig`(1M).

▼ Monitorar os eventos lo em tempo real

Siga este procedimento para ativar o plugin `audit_syslog` em relação a eventos que deseja monitorar à medida que eles ocorrem.

Antes de começar É necessário estar na função `root` para modificar o arquivo `syslog.conf` . Outras etapas requerem que seja atribuído a você o perfil de direitos Configuração de auditoria.

1. **Envie a classe `lo` para o plugin `audit_syslog` e ative o plugin.**

   ```
   # auditconfig -setplugin audit_syslog active p_flags=lo
   ```

2. **Adicione uma entrada `audit.notice` ao arquivo `syslog.conf`.**

   A entrada padrão inclui o local do arquivo de log.

   ```
   # cat /etc/syslog.conf
   ...
   audit.notice       /var/adm/auditlog
   ```

3. **Crie o arquivo de log.**

   ```
   # touch /var/adm/auditlog
   ```

4. **comando Atualize as informações do serviço `syslog`.**

   ```
   # svcadm refresh system/system-log
   ```

5. **Atualize o serviço de auditoria.**

   O serviço de auditoria lê as alterações feitas no plugin de auditoria na atualização.

   ```
   # audit -s
   ```

Consulte também

- Para enviar os resumos de auditoria a outro sistema, consulte o exemplo após "How to Configure syslog Audit Logs" no *Oracle Solaris Administration: Security Services*.
- O serviço de auditoria pode gerar uma saída extensiva. Para gerenciar os logs, consulte a página man `logadm(1M)`.
- Para monitorar a saída, consulte "Monitoramento de resumos de auditoria `audit_syslog`" na página 53.

▼ Remover privilégios básicos desnecessários de usuários

Em determinadas circunstâncias, um ou mais dos três privilégios básicos podem ser removidos do conjunto básico de um usuário regular.

- `file_link_any` – permite que um processo crie links físicos para arquivos pertencentes a um UID diferente do UID efetivo do processo.
- `proc_info` – permite que um processo examine o status de processos que não sejam aqueles para os quais ele pode enviar sinais. Processos que não é possível examinar não podem ser vistos em `/proc` e parecem não existir.
- `proc_session` – permite que um processo envie sinais ou rastreie processos fora de sua sessão.

Antes de começar É necessário estar na função `root`.

1. **Impeça que um usuário se vincule a um arquivo que não lhe pertence.**

   ```
   # usermod -K defaultpriv=basic,!file_link_any user
   ```

2. **Impeça que um usuário examine processos que não lhe pertencem.**

   ```
   # usermod -K defaultpriv=basic,!proc_info user
   ```

3. **Impeça que um usuário inicie uma segunda sessão, como `ssh`, a partir da sessão atual do usuário.**

   ```
   # usermod -K defaultpriv=basic,!proc_session user
   ```

4. **Remova os três privilégios do conjunto básico de um usuário.**

   ```
   # usermod -K defaultpriv=basic,!file_link_any,!proc_info,!proc_session user
   ```

Consulte também Para obter mais informações, consulte o Capítulo 8, "Using Roles and Privileges (Overview)," no *Oracle Solaris Administration: Security Services* e a página man `privileges(5)`.

Proteção do kernel

Nesse ponto, talvez você já tenha criado usuários que possam assumir funções e criado as funções. Somente a função `root` pode modificar os arquivos do sistema.

Tarefa	Descrição	Instruções
Impeça que os programas explorem uma pilha executável.	Define uma variável do sistema que evita a exploração dos estouros de buffer que exploram a pilha executável.	"Protecting Executable Files From Compromising Security" no *Oracle Solaris Administration: Security Services*

Tarefa	Descrição	Instruções
Proteger os arquivos de núcleo que podem conter informações confidenciais.	Cria um diretório com acesso limitado, dedicado a arquivos de núcleo.	"How to Enable a Global Core File Path" no *Oracle Solaris Administration: Common Tasks* "Managing Core Files (Task Map)" no *Oracle Solaris Administration: Common Tasks*

Configuração da rede

Nesse ponto, talvez você já tenha criado usuários que possam assumir funções e criado as funções. Somente a função `root` pode modificar os arquivos do sistema.

Com base nas tarefas de rede a seguir, execute aquelas que fornecem segurança adicional de acordo com os requisitos da sua empresa. Essas tarefas de rede fortalecem os protocolos IP, ARP e TCP, e informam aos usuários conectados remotamente que o sistema está protegido.

Tarefa	Descrição	Instruções
Exiba mensagens de aviso que reflitam a política de segurança da sua empresa.	Notifica os usuários e possíveis invasores de que o sistema é monitorado.	"Exibir Mensagem de Segurança para Usuários `ssh` e `ftp`" na página 39
Desativar o daemon de roteamento de rede.	Limita o acesso de possíveis sniffers de rede aos sistemas.	"Desativar o daemon de roteamento de rede" na página 40
Impedir a disseminação das informações sobre a topologia de rede.	Impede a difusão de pacotes.	"Desativar o encaminhamento de pacotes de difusão" na página 41
	Impede a geração de respostas para solicitações de eco resultantes de operações de difusão e multicast.	"Desativar respostas para solicitações de eco" na página 41
Para sistemas que são gateways de outros domínios, como um firewall ou um nó VPN, ative a hospedagem múltipla estrita para origem e destino.	Impede que os pacotes que não tenham o endereço do gateway no cabeçalho ultrapassem o gateway.	"Definir hospedagem múltipla estrita" na página 42
Impedir ataques de negação de serviço controlando o número de conexões de sistema incompletas.	Limita o número permitido de conexões TCP incompletas para um listener TCP.	"Definir o número máximo de conexões TCP incompletas" na página 42
Impedir ataques de negação de serviço controlando o número de conexões recebidas permitidas.	Especifica o número máximo padrão de conexões TCP pendentes para uma escuta TCP.	"Definir o número máximo de conexões TCP pendentes" na página 43

Tarefa	Descrição	Instruções
Gerar números aleatórios fortes para conexões TCP iniciais.	É compatível com o valor de geração de número de sequência especificado pelo RFC 1948.	"Especificar um Número Aleatório Forte para a Conexão TCP Inicial" na página 43
Recuperar os valores padrão seguros dos parâmetros de rede.	Aumenta a segurança reduzida por ações administrativas.	"Redefinir os parâmetros de rede com valores seguros" na página 44
Adicionar wrappers TCP aos serviços de rede para limitar os aplicativos a usuários legítimos.	Especifica sistemas que podem acessar serviços de rede, como FTP. Por padrão, o aplicativo `sendmail` é protegido por wrappers TCP, como descrito em "Support for TCP Wrappers From Version 8.12 of sendmail" no *Oracle Solaris Administration: Network Services*.	Para ativar wrappers TCP para todos os serviços `inetd`, consulte "How to Use TCP Wrappers to Control Access to TCP Services" no *Oracle Solaris Administration: IP Services*. Para obter um exemplo de wrappers TCP protegendo o serviço de rede FTP, consulte "How to Start an FTP Server Using SMF" no *Oracle Solaris Administration: Network Services*.

▼ Exibir Mensagem de Segurança para Usuários ssh e ftp

Use este procedimento para exibir avisos no login remoto e na transferência de arquivos.

Antes de começar É necessário estar na função `root`. Você criou o arquivo `/etc/issue` na Etapa 1de "Colocar uma Mensagem de Segurança em Arquivos de Banner" na página 28.

1 Para exibir uma mensagem de segurança aos usuários que efetuaram login usando `ssh`, faça o seguinte:

a. Remova o comentário da diretiva Banner no arquivo `/etc/sshd_config`.

```
# vi /etc/ssh/sshd_config
# Banner to be printed before authentication starts.
Banner /etc/issue
```

b. Atualize o serviço `ssh`.

```
# svcadm refresh ssh
```

Para obter mais informações, consulte as páginas man `issue(4)` e `sshd_config(4)`.

2 Para exibir uma mensagem de segurança aos usuários que efetuaram login usando `ftp`, faça o seguinte:

a. Adicione a diretiva `DisplayConnect` ao arquivo `proftpd.conf`.

```
# vi /etc/proftpd.conf
# Banner to be printed before authentication starts.
DisplayConnect /etc/issue
```

b. Reinicie o serviço `ftp`.

```
# svcadm restart ftp
```

Para obter informações, consulte o site ProFTPD (`http://www.proftpd.org/`).

▼ Desativar o daemon de roteamento de rede

Siga este procedimento para impedir o roteamento de rede após a instalação, especificando um roteador padrão. Caso contrário, siga este procedimento depois de confirmar o roteamento manualmente.

Observação – Muitos procedimentos de configuração de rede requerem que o daemon de roteamento seja desativado. Dessa forma, você pode ter desativado esse daemon como parte de um procedimento de configuração mais abrangente.

Antes de começar É necessário ter o perfil de direitos Gerenciamento de rede.

1 Verifique se o daemon de roteamento está sendo executado.

```
# svcs -x svc:/network/routing/route:default
svc:/network/routing/route:default (in.routed network routing daemon)
 State: online since April 10, 2011 05:15:35 AM PDT
   See: in.routed(1M)
   See: /var/svc/log/network-routing-route:default.log
Impact: None.
```

Se o serviço não estiver em execução, você poderá parar aqui.

2 Desative o daemon de roteamento.

```
# routeadm -d ipv4-forwarding -d ipv6-forwarding
# routeadm -d ipv4-routing -d ipv6-routing
# routeadm -u
```

3 Verifique se o daemon de roteamento está desativado.

```
# svcs -x routing/route:default
svc:/network/routing/route:default (in.routed network routing daemon)
 State: disabled since April 11, 2011 10:10:10 AM PDT
Reason: Disabled by an administrator.
   See: http://sun.com/msg/SMF-8000-05
   See: in.routed(1M)
Impact: This service is not running.
```

Consulte também Página man `routeadm(1M)`

▼ Desativar o encaminhamento de pacotes de difusão

Por padrão, o Oracle Solaris encaminha pacotes de difusão. Se a política de segurança da sua empresa exigir a redução da possibilidade de inundação de difusão, altere o padrão com este procedimento.

Observação – Ao desativar a propriedade de rede `_forward_directed_broadcasts`, você também desativará os pings de difusão.

Antes de começar É necessário ter o perfil de direitos Gerenciamento de rede.

1 Defina a propriedade de encaminhamento de pacotes de difusão como 0 para pacotes IP.

```
# ipadm set-prop -p _forward_directed_broadcasts=0 ip
```

2 Verifique o valor atual.

```
# ipadm show-prop -p _forward_directed_broadcasts ip
PROTO  PROPERTY                   PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ip     _forward_directed_broadcasts  rw   0         --           0         0,1
```

Consulte também Página man `ipadm(1M)`

▼ Desativar respostas para solicitações de eco

Siga este procedimento para impedir a disseminação de informações sobre a topologia de rede.

Antes de começar É necessário ter o perfil de direitos Gerenciamento de rede.

1 Defina a propriedade de resposta para solicitações de eco de difusão como 0 para pacotes IP e, em seguida, confirme o valor atual.

```
# ipadm set-prop -p _respond_to_echo_broadcast=0 ip

# ipadm show-prop -p _respond_to_echo_broadcast ip
PROTO  PROPERTY                 PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ip     _respond_to_echo_broadcast rw   0         --           1         0,1
```

2 Defina a propriedade de resposta para solicitações de eco multicast como 0 para pacotes IP e, em seguida, confirme o valor atual.

```
# ipadm set-prop -p _respond_to_echo_multicast=0 ipv4
# ipadm set-prop -p _respond_to_echo_multicast=0 ipv6

# ipadm show-prop -p _respond_to_echo_multicast ipv4
PROTO  PROPERTY                 PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ipv4   _respond_to_echo_multicast rw   0         --           1         0,1
```

```
# ipadm show-prop -p _respond_to_echo_multicast ipv6
PROTO  PROPERTY                 PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ipv6   _respond_to_echo_multicast rw   0         --           1         0,1
```

Consulte também Para obter mais informações, consulte "_respond_to_echo_broadcast and _respond_to_echo_multicast (ipv4 or ipv6)" no *Oracle Solaris Tunable Parameters Reference Manual* e a página man `ipadm`(1M).

▼ Definir hospedagem múltipla estrita

Para sistemas que são gateways de outros domínios, como um firewall ou um nó VPN, siga este procedimento para ativar a hospedagem múltipla estrita.

A versão do Oracle Solaris 11 introduz uma nova propriedade, `hostmodel`, para IPv4 e IPv6. Essa propriedade controla o comportamento de envio e de recebimento de pacotes IP em um sistema de hospedagem múltipla.

Antes de começar É necessário ter o perfil de direitos Gerenciamento de rede.

1 Defina a propriedade `hostmodel` como `forte` para pacotes IP.

```
# ipadm set-prop -p hostmodel=strong ipv4
# ipadm set-prop -p hostmodel=strong ipv6
```

2 Verifique o valor atual e observe os valores possíveis.

```
# ipadm show-prop -p hostmodel ip
PROTO  PROPERTY    PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ipv6   hostmodel   rw   strong    strong       weak      strong,src-priority,weak
ipv4   hostmodel   rw   strong    strong       weak      strong,src-priority,weak
```

Consulte também Para obter mais informações, consulte"hostmodel (ipv4 or ipv6)" no *Oracle Solaris Tunable Parameters Reference Manual* e a página man `ipadm`(1M).

Para obter mais informações sobre o uso de hospedagem múltipla estrita, consulte "How to Protect a VPN With IPsec in Tunnel Mode" no *Oracle Solaris Administration: IP Services*.

▼ Definir o número máximo de conexões TCP incompletas

Siga este procedimento para impedir ataques de negação de serviço (DOS), controlando o número de conexões pendentes incompletas.

Antes de começar É necessário ter o perfil de direitos Gerenciamento de rede.

1. **Defina o número máximo de conexões de entrada.**

```
# ipadm set-prop -p _conn_req_max_q0=4096 tcp
```

2. **Verifique o valor atual.**

```
# ipadm show-prop -p _conn_req_max_q0 tcp
PROTO  PROPERTY         PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
tcp    _conn_req_max_q0 rw   4096      --           128       1-4294967295
```

Consulte também Para obter mais informações, consulte "_conn_req_max_q0" no *Oracle Solaris Tunable Parameters Reference Manual* e a página man `ipadm`(1M).

▼ Definir o número máximo de conexões TCP pendentes

Siga este procedimento para evitar ataques de negação de serviço, controlando o número de conexões de entrada permitidas.

Antes de começar É necessário ter o perfil de direitos Gerenciamento de rede.

1. **Defina o número máximo de conexões de entrada.**

```
# ipadm set-prop -p _conn_req_max_q=1024 tcp
```

2. **Verifique o valor atual.**

```
# ipadm show-prop -p _conn_req_max_q tcp
PROTO  PROPERTY         PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
tcp    _conn_req_max_q  rw   1024      --           128       1-4294967295
```

Consulte também Para obter mais informações, consulte "_conn_req_max_q" no *Oracle Solaris Tunable Parameters Reference Manual* e a página man `ipadm`(1M).

▼ Especificar um Número Aleatório Forte para a Conexão TCP Inicial

Este procedimento define o parâmetro de geração do número de sequência inicial TCP para que seja compatível com o RFC 1948 (`http://www.ietf.org/rfc/rfc1948.txt`).

Antes de começar É necessário estar na função `root` para modificar um arquivo do sistema.

- **Altere o valor padrão da variável `TCP_STRONG_ISS`.**

```
# vi /etc/default/inetinit
# TCP_STRONG_ISS=1
TCP_STRONG_ISS=2
```

▼ Redefinir os parâmetros de rede com valores seguros

Muitos parâmetros de rede, que são protegidos por padrão, são ajustáveis e, portanto, podem ser alterados. Se as condições da empresa permitirem, redefina os parâmetros ajustáveis a seguir com seus valores padrão.

Antes de começar É necessário ter o perfil de direitos Gerenciamento de rede. O valor atual do parâmetro é menos seguro que o valor padrão.

1 Defina a propriedade de encaminhamento de pacote de origem como 0 para pacotes IP e, em seguida, confirme o valor atual.

O valor padrão impede ataques de negação de serviço de pacotes falsificados.

```
# ipadm set-prop -p _forward_src_routed=0 ipv4
# ipadm set-prop -p _forward_src_routed=0 ipv6
# ipadm show-prop -p _forward_src_routed ipv4
PROTO  PROPERTY             PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ipv4   _forward_src_routed   rw   0         --           0         0,1
# ipadm show-prop -p _forward_src_routed ipv6
PROTO  PROPERTY             PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ipv6   _forward_src_routed   rw   0         --           0         0,1
```

Para obter mais informações, consulte "forwarding (ipv4 or ipv6)" no *Oracle Solaris Tunable Parameters Reference Manual*.

2 Defina a propriedade de resposta de máscara de rede como 0 para pacotes IP e, em seguida, verifique o valor atual.

O valor padrão impede a disseminação de informações sobre a topologia de rede.

```
# ipadm set-prop -p _respond_to_address_mask_broadcast=0 ip
# ipadm show-prop -p _respond_to_address_mask_broadcast ip
PROTO PROPERTY                          PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ip    _respond_to_address_mask_broadcast rw   0         --           0         0,1
```

3 Defina a propriedade de resposta de carimbo de data/hora como 0 para pacotes IP e, em seguida, verifique o valor atual.

O valor padrão remove demandas adicionais de CPU em sistemas e impede a disseminação de informações sobre a rede.

```
# ipadm set-prop -p _respond_to_timestamp=0 ip
# ipadm show-prop -p _respond_to_timestamp ip
PROTO  PROPERTY                       PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ip     _respond_to_timestamp          rw   0         --           0         0,1
```

4 Defina a propriedade de resposta de carimbo de data/hora de difusão como 0 para pacotes IP e, em seguida, verifique o valor atual.

O valor padrão remove demandas adicionais de CPU em sistemas e evita a disseminação de informações sobre a rede.

```
# ipadm set-prop -p _respond_to_timestamp_broadcast=0 ip
# ipadm show-prop -p _respond_to_timestamp_broadcast ip
```

```
PROTO  PROPERTY                        PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ip     _respond_to_timestamp_broadcast rw   0         --           0         0,1
```

5 Defina a propriedade ignorar redirecionamentos como 0 para pacotes IP e, em seguida, verifique o valor atual.

O valor padrão impede demandas adicionais de CPU em sistemas.

```
# ipadm set-prop -p _ignore_redirect=0 ipv4
# ipadm set-prop -p _ignore_redirect=0 ipv6
# ipadm show-prop -p _ignore_redirect ipv4
PROTO  PROPERTY         PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ipv4   _ignore_redirect  rw   0         --           0         0,1
# ipadm show-prop -p _ignore_redirect ipv6
PROTO  PROPERTY         PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ipv6   _ignore_redirect  rw   0         --           0         0,1
```

6 Impeça o roteamento de origem de IP.

Se você precisar de roteamento de origem de IP para fins de diagnóstico, não desative esse parâmetro de rede.

```
# ipadm set-prop -p _rev_src_routes=0 tcp
# ipadm show-prop -p _rev_src_routes tcp
PROTO  PROPERTY         PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
tcp    _rev_src_routes   rw   0         --           0         0,1
```

Para obter mais informações, consulte "_rev_src_routes" no *Oracle Solaris Tunable Parameters Reference Manual* .

7 Defina a propriedade ignorar redirecionamentos como 0 para pacotes IP e, em seguida, verifique o valor atual.

O valor padrão impede demandas adicionais de CPU em sistemas. Em geral, redirecionamentos não são necessários em uma rede bem projetada.

```
# ipadm set-prop -p _ignore_redirect=0 ipv4
# ipadm set-prop -p _ignore_redirect=0 ipv6
# ipadm show-prop -p _ignore_redirect ipv4
PROTO  PROPERTY           PERM  CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ipv4   _ignore_redirect   rw    0         --           0         0,1
# ipadm show-prop -p _ignore_redirect ipv6
PROTO  PROPERTY           PERM  CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ipv6   _ignore_redirect   rw    0         --           0         0,1
```

Consulte também Página man `ipadm(1M)`

Proteção dos sistemas de arquivos e arquivos

Os sistemas de arquivos ZFS são leves e podem ser criptografados, compactados e configurados com limites de espaço em disco e de espaço reservado.

As tarefas a seguir fornecem uma visão geral das proteções disponíveis no ZFS, o sistema de arquivos padrão do Oracle Solaris. Para obter informações adicionais, consulte "Setting ZFS Quotas and Reservations" no *Oracle Solaris Administration: ZFS File Systems* e a página man `zfs`(1M).

Tarefa	Descrição	Instruções
Impede ataques de negação de serviço gerenciando e reservando espaço em disco.	Especifica o uso do espaço em disco pelo sistema de arquivos, pelo usuário ou grupo ou pelo projeto.	"Setting ZFS Quotas and Reservations" no *Oracle Solaris Administration: ZFS File Systems*
Garantir um espaço em disco para um conjunto de dados e seus descendentes.	Garante espaço em disco pelo sistema de arquivos, pelo usuário ou grupo ou pelo projeto.	"Setting Reservations on ZFS File Systems" no *Oracle Solaris Administration: ZFS File Systems*
Criptografe dados em um sistema de arquivos.	Protege um conjunto de dados com criptografia e uma frase secreta para acessar o conjunto de dados na sua criação.	"Encrypting ZFS File Systems" no *Oracle Solaris Administration: ZFS File Systems* "Examples of Encrypting ZFS File Systems" no *Oracle Solaris Administration: ZFS File Systems*
Especifique ACLs para proteger arquivos em uma granularidade mais refinada do que as permissões de arquivos UNIX regulares.	Os atributos de segurança estendidos podem ser úteis para a proteção de arquivos. Para ler um aviso sobre o uso de ACLs, consulte Hiding Within the Trees (`http://www.usenix.org/publications/login/2004-02/pdfs/brunette.pdf`).	ZFS End-to-End Data Integrity (`http://blogs.oracle.com/bonwick/entry/zfs_end_to_end_data`)

Proteção e modificação de arquivos

Somente a função `root` pode modificar os arquivos do sistema.

Tarefa	Descrição	Instruções
Configurar permissões de arquivo restritivas para usuários regulares.	Define um valor mais restritivo do que `022` para as permissões de arquivo de usuários regulares.	"Definir um valor `umask` mais restritivo para usuários regulares" na página 34
Impedir a substituição de arquivos do sistema por arquivos invasores.	Localiza arquivos invasores por meio de script ou usando a BART.	"How to Find Files With Special File Permissions" no *Oracle Solaris Administration: Security Services*

Proteção de aplicativos e serviços

É possível configurar os recursos de segurança do Oracle Solaris para proteger seus aplicativos.

Criação de zonas para conter aplicativos críticos

Zonas são contêineres que isolam processos. São contêineres úteis para aplicativos e partes de aplicativos. Por exemplo, é possível usar zonas para fazer a separação entre o banco de dados e o servidor Web de um site.

Para obter informações e procedimentos, consulte:

- Capítulo 15, "Introduction to Oracle Solaris Zones," no *Oracle Solaris Administration: Oracle Solaris Zones, Oracle Solaris 10 Zones, and Resource Management*
- "Summary of Zones by Function" no *Oracle Solaris Administration: Oracle Solaris Zones, Oracle Solaris 10 Zones, and Resource Management*
- "Capabilities Provided by Non-Global Zones" no *Oracle Solaris Administration: Oracle Solaris Zones, Oracle Solaris 10 Zones, and Resource Management*
- "Setting Up Zones on Your System (Task Map)" no *Oracle Solaris Administration: Oracle Solaris Zones, Oracle Solaris 10 Zones, and Resource Management*.
- Capítulo 16, "Non-Global Zone Configuration (Overview)," no *Oracle Solaris Administration: Oracle Solaris Zones, Oracle Solaris 10 Zones, and Resource Management*.
- *Hardening Oracle Database with Oracle Solaris Security Technologies* (`http://www.oracle.com/technetwork/server-storage/solaris/solaris-security-hardening-db-167784.pdf`)

Gerenciamento de recursos em zonas

As zonas fornecem várias ferramentas para gerenciar seus recursos.

Para obter informações e procedimentos, consulte:

- Capítulo 14, "Resource Management Configuration Example," no *Oracle Solaris Administration: Oracle Solaris Zones, Oracle Solaris 10 Zones, and Resource Management*
- Parte I, "Oracle Solaris Resource Management," no *Oracle Solaris Administration: Oracle Solaris Zones, Oracle Solaris 10 Zones, and Resource Management*

Configuração de IPsec e IKE

IPsec e IKE protegem as transmissões de rede entre nós e redes que são configuradas em conjunto com IPsec e IKE.

Para obter informações e procedimentos, consulte:

- Capítulo 14, "IP Security Architecture (Overview)," no *Oracle Solaris Administration: IP Services*
- Capítulo 17, "Internet Key Exchange (Overview)," no *Oracle Solaris Administration: IP Services*
- Capítulo 15, "Configuring IPsec (Tasks)," no *Oracle Solaris Administration: IP Services*
- Capítulo 18, "Configuring IKE (Tasks)," no *Oracle Solaris Administration: IP Services*

Configuração do recurso Filtro IP

O recurso Filtro IP fornece um firewall.

Para obter informações e procedimentos, consulte:

- Capítulo 20, "IP Filter in Oracle Solaris (Overview)," no *Oracle Solaris Administration: IP Services*
- Capítulo 21, "IP Filter (Tasks)," no *Oracle Solaris Administration: IP Services*

Configuração do Kerberos

É possível proteger a rede com o serviço Kerberos. Essa arquitetura de servidor-cliente protege transações em redes. O serviço oferece autenticação forte de usuário, bem como integridade e privacidade. Usando o serviço Kerberos, é possível se conectar a outros sistemas, executar comandos, trocar dados e transferir arquivos com segurança. Além disso, o serviço permite que os administradores restrinjam o acesso a serviços e sistemas. Como usuário do Kerberos, você pode controlar o acesso de outras pessoas à sua conta.

Para obter informações e procedimentos, consulte:

- Capítulo 20, "Planning for the Kerberos Service," no *Oracle Solaris Administration: Security Services*
- Capítulo 21, "Configuring the Kerberos Service (Tasks)," no *Oracle Solaris Administration: Security Services*
- As páginas man selecionadas incluem `kadmin`(1M), `pam_krb5`(5) e `kclient`(1M).

Inclusão de SMF em um serviço herdado

É possível limitar a configuração de aplicativos a usuários confiáveis ou funções, adicionando o aplicativo ao recurso SMF (Service Management Facility) do Oracle Solaris.

Para obter informações e procedimentos, consulte:

- "How to Add RBAC Properties to Legacy Applications" no *Oracle Solaris Administration: Security Services*
- Securing MySQL using SMF - the Ultimate Manifest (`http://blogs.oracle.com/bobn/entry/securing_mysql_using_smf_the`).
- As páginas man selecionadas incluem `smf(5)`, `smf_security(5)`, `svcadm(1M)` e `svccfg(1M)`.

Criação de um instantâneo BART do sistema

Após a configuração do sistema, é possível criar um ou mais manifestos BART. Esses manifestos fornecem instantâneos do sistema. Em seguida, é possível programar instantâneos e comparações regulares. Para obter mais informações, consulte "Uso da Basic Audit Reporting Tool" na página 51.

Inclusão de segurança multinível (rotulada)

O Trusted Extensions amplia a segurança do Oracle Solaris reforçando uma política de controle de acesso obrigatório (MAC). Os rótulos de confidencialidade são automaticamente aplicados a todas as fontes de dados (redes, sistemas de arquivos e janelas) e consumidores de dados (usuário e processos). O acesso a todos os dados é restrito com base no relacionamento entre o rótulo dos dados (objeto) e o consumidor (sujeito). A funcionalidade sobreposta compreende um conjunto de serviços habilitados para rótulos.

Uma lista parcial de serviços do Trusted Extensions inclui:

- Rede rotulada
- Montagem e compartilhamento do sistema de arquivos habilitado para rótulos
- Área de trabalho rotulada
- Configuração e tradução de rótulos
- Ferramentas de gerenciamento de sistemas habilitados para rótulos
- Alocação de dispositivos habilitados para rótulos

Os pacotes `group/feature/trusted-desktop` fornecem o ambiente de área de trabalho confiável Oracle Solaris de vários níveis.

Configuração do Trusted Extensions

É necessário instalar os pacotes do Trusted Extensions e, em seguida, configurar o sistema. Após a instalação do pacote, o sistema poderá executar uma área de trabalho com um dispositivo de exibição de bitmap diretamente conectado, como um laptop ou uma estação de trabalho. É necessário que a configuração de rede se comunique com outros sistemas.

Para obter informações e procedimentos, consulte:

- Parte I, "Initial Configuration of Trusted Extensions," no *Trusted Extensions Configuration and Administration*
- Parte II, "Administration of Trusted Extensions," no *Trusted Extensions Configuration and Administration*

Configuração de IPsec rotulada

É possível proteger pacotes rotulados com a IPsec.

Para obter informações e procedimentos, consulte:

- Capítulo 14, "IP Security Architecture (Overview)," no *Oracle Solaris Administration: IP Services*
- "Administration of Labeled IPsec" no *Trusted Extensions Configuration and Administration*
- "Configuring Labeled IPsec (Task Map)" no *Trusted Extensions Configuration and Administration*

◆ ◆ ◆ CAPÍTULO 3

Monitoramento e manutenção da segurança do Oracle Solaris 11

O Oracle Solaris fornece duas ferramentas de sistema para monitorar a segurança, a Basic Audit Reporting Tool (BART) e o serviço de auditoria. Os programas e aplicativos individuais também podem criar registros de acesso e uso.

Uso da Basic Audit Reporting Tool

Os manifestos BART fornecem um registro estático do que está instalado no sistema. Com o decorrer do tempo e entre os sistemas, os manifestos BART podem ser comparados para rastrear alterações em sistemas instalados e diferenças entre eles.

Para obter informações e procedimentos, consulte:

- "BART (Overview)" no *Oracle Solaris Administration: Security Services*
- "Using BART (Tasks)" no *Oracle Solaris Administration: Security Services*
- "BART Manifests, Rules Files, and Reports (Reference)" no *Oracle Solaris Administration: Security Services*

Para obter instruções específicas sobre rastreamento de alterações em sistemas instalados, consulte "How to Compare Manifests for the Same System Over Time" no *Oracle Solaris Administration: Security Services*.

Uso do serviço de auditoria

A auditoria mantém um registro de como o sistema está sendo usado. O serviço de auditoria inclui ferramentas para auxiliar na análise dos dados da auditoria.

O serviço de auditoria é descrito na Parte VII, "Auditing in Oracle Solaris," no *Oracle Solaris Administration: Security Services*.

- Capítulo 26, "Auditing (Overview)," no *Oracle Solaris Administration: Security Services*
- Capítulo 27, "Planning for Auditing," no *Oracle Solaris Administration: Security Services*
- Capítulo 28, "Managing Auditing (Tasks)," no *Oracle Solaris Administration: Security Services*
- Capítulo 29, "Auditing (Reference)," no *Oracle Solaris Administration: Security Services*

  Para obter uma lista das páginas man e dos links para elas, consulte "Audit Service Man Pages" no *Oracle Solaris Administration: Security Services*.

Para atender aos requisitos da sua empresa, os seguintes procedimentos de serviço de auditoria poderão ser úteis:

- Crie funções separadas para configurar e analisar a auditoria e iniciar e parar o serviço de auditoria.

  Use os perfis de direitos Configuração de auditoria, Análise de auditoria e Controle de auditoria como a base para as suas funções.

  Para criar uma função, consulte "How to Create a Role" no *Oracle Solaris Administration: Security Services*.
- Monitore resumos de texto dos eventos auditados no utilitário `syslog`

  Ative o plugin `audit_syslog` e, em seguida, monitore os eventos relatados.

  Consulte "How to Configure syslog Audit Logs" no *Oracle Solaris Administration: Security Services*.
- Limite o tamanho dos arquivos de auditoria.

  Defina o atributo `p_fsize` para o plugin `audit_binfile` como um tamanho útil. Considere a sua programação de análise, o espaço em disco e a frequência do trabalho `cron`, entre outros fatores.

  Para obter exemplos, consulte "How to Assign Audit Space for the Audit Trail" no *Oracle Solaris Administration: Security Services*.
- Programe a transferência segura de arquivos de auditoria completos para um sistema de arquivos de análise de auditoria em um pool ZFS separado.
- Analise os arquivos de auditoria completos no sistema de arquivos de auditoria.

Monitoramento de resumos de auditoria audit_syslog

O plugin `audit_syslog` permite registrar resumos de eventos de auditoria pré-selecionados.

É possível exibir os resumos de auditoria em uma janela de terminal à medida que são gerados, executando um comando semelhante a este:

```
# tail -0f /var/adm/auditlog
```

Análise e arquivamento de logs de auditoria

É possível visualizar os registros de auditoria em formato de texto ou em um navegador no formato XML.

Para obter informações e procedimentos, consulte:

- "Audit Logs" no *Oracle Solaris Administration: Security Services*
- "How to Prevent Audit Trail Overflow" no *Oracle Solaris Administration: Security Services*
- "Managing Audit Records on Local Systems (Tasks)" no *Oracle Solaris Administration: Security Services*

Como localizar arquivos invasores

É possível localizar o uso potencialmente não autorizado das permissões `setuid` e `setgid` em programas. Um arquivo executável suspeito concede posse a um usuário em vez de concedê-la a uma conta de sistema, como `root` ou `bin`.

Para ler o procedimento e obter um exemplo, consulte "How to Find Files With Special File Permissions" no *Oracle Solaris Administration: Security Services*.

◆ ◆ ◆ APÊNDICE A

Bibliografia de segurança do Oracle Solaris

As referências a seguir contêm informações de segurança úteis para sistemas Oracle Solaris. As informações de segurança de releases anteriores do SO Oracle Solaris contêm algumas informações úteis e algumas desatualizadas.

Referências do Oracle Solaris 11

O manual e os artigos a seguir contêm descrições de segurança dos sistemas Oracle Solaris 11:

- *Oracle Solaris Administration: Security Services*

  Este guia de segurança é publicado pela Oracle para administradores do Oracle Solaris 11. Este guia descreve os recursos de segurança do Oracle Solaris e como usá-los ao configurar seus sistemas. O prefácio contém links para outros guias de administração do sistema Oracle Solaris que podem conter informações de segurança.

- *Oracle Solaris Security: Oracle Solaris Express* (`http://www.oracle.com/technetwork/articles/servers-storage-admin/os11esecurity-186797.pdf`)

  Esse artigo apresenta um panorama dos recursos de segurança do Oracle Solaris para a versão de novembro de 2010 desta release.

- ORACLE SOLARIS 11 EXPRESS 2010.11 (`http://www.oracle.com/technetwork/server-storage/solaris11/documentation/solaris-express-whatsnew-201011-175308.pdf`)

  Esse artigo apresenta um panorama dos recursos do Oracle Solaris para a versão de novembro de 2010 desta release.

Para obter referências do Oracle Solaris 10 que possam ser úteis, consulte *Oracle Solaris 10 Security Guidelines*.