# Diretrizes de Segurança do Oracle® Solaris 11

Número do Item: E36476–05
Setembro de 2013

ORACLE®

130926@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`.<br>Use `ls -a` para listar todos os arquivos.<br>`machine_name%, você tem e-mail.` |
| **`AaBbCc123`** | O que você digita, em comparação com a saída do computador na tela | `machine_name%` **`su`**<br>`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*.<br>Um *cache* é uma cópia que é armazenada localmente.<br>*Não* salve o arquivo.<br>**Nota:** alguns itens enfatizados aparecem on-line em negrito. |

# Prompts do shell em exemplos de comando

A tabela a seguir mostra os prompts do sistema UNIX e os prompts de superusuário para shells incluídos no SO Oracle Solaris. Nos exemplos de comando, o prompt de shell indica se o comando deve ser executado por um usuário comum ou por um usuário com privilégios.

**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 | `machine_name%` |
| Shell C para superusuário | `machine_name#` |

◆ ◆ ◆ CAPÍTULO 1

# 1 Visão geral da segurança do Oracle Solaris

O Oracle Solaris 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 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

O Oracle Solaris fornece uma base sólida para dados e aplicativos corporativos protegendo os dados em disco e em trânsito. O gerenciamento de recursos do Oracle Solaris e as Zonas do Oracle Solaris Zones 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 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 da memória – O layout do espaço de endereço é randomizado para processos userland.
- 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

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.

## Layout aleatório do espaço de endereço

A ASLR (Address Space Layout Randomization) randomiza os endereços usados por um binário. A ASLR pode impedir determinados tipos de ataque com base no conhecimento da localização exata de alguns intervalos de memória, e pode detectar a tentativa no momento em que o executável é interrompido. Para obter mais informações, consulte "Address Space Layout Randomization" no *Oracle Solaris 11.1 Administration: Security Services*.

## 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 11.1 Administration: Security Services*.
- Para obter diretrizes, consulte "Como auditar eventos significativos além de login/logout" na página 36 e as páginas man.
- Para obter uma visão geral da auditoria, consulte o Capítulo 26, "Auditing (Overview)," no *Oracle Solaris 11.1 Administration: Security Services* .
- Para obter informações sobre tarefas de auditoria, consulte o Capítulo 28, "Managing Auditing (Tasks)," no *Oracle Solaris 11.1 Administration: Security Services*.

## Verificação de arquivos BART

O recurso BART 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 47, "Verificação da integridade do arquivo usando o BART" na página 49 e as páginas man.
- Para obter uma visão geral do BART, consulte o Capítulo 6, "Verifying File Integrity by Using BART (Tasks)," no *Oracle Solaris 11.1 Administration: Security Services*.
- Para obter exemplos do uso do recurso BART, consulte "Using BART (Tasks)" no *Oracle Solaris 11.1 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 11.1 Administration: Security Services* e o Capítulo 13, "Key Management Framework," no *Oracle Solaris 11.1 Administration: Security Services*.
- Para obter exemplos de uso da Estrutura criptográfica, consulte o Capítulo 12, "Cryptographic Framework (Tasks)," no *Oracle Solaris 11.1 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 11.1 Administration: Security Services*.
- Para obter uma visão geral e exemplos de proteção de arquivos ZFS, consulte o Capítulo 7, "Using ACLs and Attributes to Protect Oracle Solaris ZFS Files," no *Oracle Solaris 11.1 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 4, "IP Filter in Oracle Solaris (Overview)," no *Securing the Network in Oracle Solaris 11.1*.
- Para obter exemplos de uso do Filtro de IP, consulte o Capítulo 5, "IP Filter (Tasks)," no *Securing the Network in Oracle Solaris 11.1* 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 `proftpd` 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 TCP wrappers, consulte "How to Use TCP Wrappers to Control Access to TCP Services" no *Configuring and Administering Oracle Solaris 11.1 Networks*.
- 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 11.1 Administration: Security Services*
- "Securing Logins and Passwords (Tasks)" no *Oracle Solaris 11.1 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 Pluggable Authentication Modules," no *Oracle Solaris 11.1 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 11.1 Administration: Security Services*
- "Using Privileges (Tasks)" no *Oracle Solaris 11.1 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 6, "IP Security Architecture (Overview)," no *Securing the Network in Oracle Solaris 11.1*
- Capítulo 7, "Configuring IPsec (Tasks)," no *Securing the Network in Oracle Solaris 11.1*
- Capítulo 9, "Internet Key Exchange (Overview)," no *Securing the Network in Oracle Solaris 11.1*
- Capítulo 10, "Configuring IKE (Tasks)," no *Securing the Network in Oracle Solaris 11.1*
- 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 11.1 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 11.1 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 11.1 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 1, "Managing Services (Overview)," no *Managing Services and Faults in Oracle Solaris 11.1*
- Capítulo 2, "Managing Services (Tasks)," no *Managing Services and Faults in Oracle Solaris 11.1*
- 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 arquivos de proteção ACE, e é possível criptografar todo o conjunto de dados na criação. 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 11.1 Administration: ZFS File Systems*
- "Oracle Solaris ZFS and Traditional File System Differences" no *Oracle Solaris 11.1 Administration: ZFS File Systems*
- Capítulo 5, "Managing Oracle Solaris ZFS File Systems," no *Oracle Solaris 11.1 Administration: ZFS File Systems*
- "How to Remotely Administer ZFS With Secure Shell" no *Oracle Solaris 11.1 Administration: Security Services*
- 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. No Oracle Solaris 11, é possível configurar uma raiz de zona somente para leitura.

Para obter mais informações, consulte:

- "Configuring Read-Only Zones" no *Oracle Solaris 11.1 Administration: Oracle Solaris Zones, Oracle Solaris 10 Zones, and Resource Management*
- Parte II, "Oracle Solaris Zones," no *Oracle Solaris 11.1 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 de usuário devem ter pelo menos seis caracteres, sendo dois caracteres alfabéticos e um caractere não alfabético. As senhas são hash, usando o algoritmo `SHA256`. Ao alterarem a senha, todos os usuários, inclusive a função `root`, devem atender a esses requisitos de senha.

**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.

# Avaliação de segurança do Oracle Solaris 11

Atualmente, o Oracle Solaris 11 está *em avaliação* pelo Canadian Common Criteria Scheme para EAL4 (Evaluation Assurance Level 4) e EAL4+ (aprimorado com remediação de falhas). O EAL4+ representa o mais alto nível de avaliação para software comercial. O EAL4 é também o nível mais alto de avaliação mutuamente reconhecido por 26 países no CCRA (Common Criteria Recognition Arrangement).

A avaliação está sendo conduzida pelo OS PP (Operating System Protection Profile) e inclui os seguintes quatro pacotes estendidos opcionais:

- AM (Advanced Management)
- EIA (Extended Identification and Authentication)
- LS (Labeled Security)
- VIRT (Virtualization)

**Observação –** Estar em processo de *avaliação* não garante que o certificado de segurança será obtido.

Para obter mais informações sobre a avaliação, consulte:

- Oracle Security Evaluations (`http://www.oracle.com/technetwork/topics/security/security-evaluations-099357.html`)
- The Common Criteria Recognition Arrangement (`http://www.commoncriteriaportal.org/ccra/`)
- Products in Evaluation (`http://www.cse-cst.gc.ca/its-sti/services/cc/oe-pece-eng.html`)
- Operating System Protection Profile (`http://www.commoncriteriaportal.org/files/ppfiles/pp0067b_pdf.pdf`)

# 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. Se você estiver desenvolvendo programas ou instalando programas de terceiros, deverá desenvolver e instalar esses programas de forma segura.

Para obter mais informações, consulte o que se segue:

- Apêndice A, "Secure Coding Guidelines for Developers," no *Developer's Guide to Oracle Solaris 11 Security*
- 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

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, da seguinte maneira:

- **Servidor de grande porte do Oracle Solaris –** 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 de grande porte Oracle Solaris.
- **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` ao servidor de área de trabalho. 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 11.1 Systems*.

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

- *Installing Oracle Solaris 11.1 Systems*
- *Creating a Custom Oracle Solaris 11.1 Installation Image*
- *Adding and Updating Oracle Solaris 11.1 Software Packages*

# Proteção do sistema

As tarefas a seguir têm melhores resultados quando executadas em ordem sequencial. Nesse ponto, o SO do Oracle Solaris já está instalado e apenas o usuário inicial, que pode assumir a função `root`, possui 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. | "Como verificar pacotes" na página 27 |
| 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 11.1 Administration: Security Services* |
| 3. Desativar os serviços desnecessários. | Impede a execução de processos que não fazem parte das funções necessárias do sistema. | "Como desativar serviços desnecessários" na página 27 |

| Tarefa | Descrição | Instruções |
|---|---|---|
| 5. Impedir que o proprietário da estação de trabalho desligue o sistema. | Impede que o usuário do console desligue ou suspenda o sistema. | "Como remover a capacidade de gerenciamento de energia dos usuários" na página 28 |
| 6. Criar 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. | "Como colocar uma mensagem de segurança em arquivos de banner" na página 29<br>"Como colocar uma mensagem de segurança na tela de login da área de trabalho" na página 29 |

## ▼ Como verificar pacotes

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

**Antes de começar** Você deve assumir a função `root`. Para obter mais informações, consulte "How to Use Your Assigned Administrative Rights" no *Oracle Solaris 11.1 Administration: Security Services*.

**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`.

## ▼ Como desativar serviços desnecessários

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

**Antes de começar** Você deve assumir a função `root`. Para obter mais informações, consulte "How to Use Your Assigned Administrative Rights" no *Oracle Solaris 11.1 Administration: Security Services*.

**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 Capítulo 1, "Managing Services (Overview)," no *Managing Services and Faults in Oracle Solaris 11.1* e a página man `svcs`(1).

## ▼ Como 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** Você deve assumir a função `root`. Para obter mais informações, consulte "How to Use Your Assigned Administrative Rights" no *Oracle Solaris 11.1 Administration: Security Services*.

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 a Rights Profile" no *Oracle Solaris 11.1 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 "policy.conf File" no *Oracle Solaris 11.1 Administration: Security Services* e as páginas man `policy.conf`(4) e `usermod`(1M).

## ▼ Como colocar uma mensagem de segurança em arquivos de banner

Siga esse procedimento para criar mensagens de segurança em dois arquivos de banner que reflitam a política de segurança do seu site. O conteúdo desses arquivos de banner 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. A prática recomendada é consultar o conselho jurídico da sua empresa sobre o conteúdo da mensagem de segurança.

---

**Antes de começar** Você deverá se tornar um administrador com o perfil de direitos para Editar mensagens do administrador. Para obter mais informações, consulte "How to Use Your Assigned Administrative Rights" no *Oracle Solaris 11.1 Administration: Security Services*.

**1 Adicione uma mensagem de segurança ao arquivo `/etc/issue`.**

```
$ pfedit /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.
```

O comando `login` exibe o conteúdo de `/etc/issue` antes da autenticação, da mesma forma que os serviços `telnet` e FTP. Para permitir que outros aplicativos usem esse arquivo, consulte "Como exibir uma mensagem de segurança para usuários `ssh` " na página 40 e "Como colocar uma mensagem de segurança na tela de login da área de trabalho" na página 29.

Para obter mais informações, consulte as páginas man `issue(4)` e `pfedit(1M)`.

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

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

No Oracle Solaris, o shell inicial do usuário exibe o conteúdo do arquivo `/etc/motd`.

## ▼ Como colocar uma 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. A prática recomendada é consultar o conselho jurídico da sua empresa sobre o conteúdo da mensagem de segurança.

---

**Antes de começar** Para criar um arquivo, você deverá assumir a função `root`. Para modificar um arquivo existente, você deverá se tornar um administrador com a autorização `solaris.admin.edit/`*path-to-existing-file*.

- **Coloque uma mensagem de segurança na tela de login da área de trabalho usando uma destas três opções:**

  As opções que criam uma caixa de diálogo podem usar a mensagem de segurança no arquivo `/etc/issue` da Etapa 1 de "Como colocar uma mensagem de segurança em arquivos de banner" na página 29.

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

    ```
    # pfedit /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.**

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

Para obter informações sobre a edição de arquivos do sistema como um usuário não `root`, consulte a página man `pfedit(1M)`.

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

```
$ pfedit /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) Salve uma cópia da Interface de Usuário da janela de login modificada.**

```
# 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.

```
# pfedit /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. | "Como definir restrições de senha mais fortes" na página 33 |
| Configurar permissões de arquivo restritivas para usuários regulares. | Define um valor mais restritivo do que `022` para as permissões de arquivo de usuários regulares. | "Como definir um valor `umask` mais restritivo para usuários regulares" na página 35. |
| 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. | "Como definir o bloqueio de contas para usuários regulares" na página 34 |
| Pré-selecionar classes de auditoria adicionais. | Fornece melhores formas de monitoramento e registro de ameaças potenciais ao sistema. | "Como auditar eventos significativos além de login/logout" na página 36 |
| 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. | "Como monitorar os eventos `lo` em tempo real" na página 37 |

| Tarefa | Descrição | Instruções |
|---|---|---|
| Criar funções. | Distribui tarefas administrativas distintas para alguns usuários confiáveis, de forma que ninguém possa danificar o sistema. | "Setting Up and Managing User Accounts by Using the CLI" no *Managing User Accounts and User Environments in Oracle Solaris 11.1*<br>"How to Create a Role" no *Oracle Solaris 11.1 Administration: Security Services*<br>"How to Assign a Role" no *Oracle Solaris 11.1 Administration: Security Services*. |
| Reduza o número de aplicativos visíveis na área de trabalho do GNOME. | Impede que os usuários usem aplicativos da área de trabalho que possam afetar a segurança. | Consulte o Capítulo 11, "Disabling Features in the Oracle Solaris Desktop System," no *Oracle Solaris 11.1 Desktop Administrator's Guide*. |
| Limitar os privilégios de um usuário. | Remove os privilégios básicos que não são necessários aos usuários. | "Como remover privilégios básicos desnecessários de usuários" na página 38 |

## ▼ Como 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.

Você deve assumir a função `root`. Para obter mais informações, consulte "How to Use Your Assigned Administrative Rights" no *Oracle Solaris 11.1 Administration: Security Services*.

- **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)`

## ▼ Como 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** Não defina essa proteção em todo o sistema usado para atividades administrativas.

Você deve assumir a função `root`. Para obter mais informações, consulte "How to Use Your Assigned Administrative Rights" no *Oracle Solaris 11.1 Administration: Security Services*.

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

- **Defina em todo o sistema.**

```
# pfedit /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`.**

```
# pfedit /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 11.1 Administration: Security Services*.
- As páginas man selecionadas incluem `policy.conf`(4) e `user_attr`(4).

## ▼ Como 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** Você deve assumir a função `root`. Para obter mais informações, consulte "How to Use Your Assigned Administrative Rights" no *Oracle Solaris 11.1 Administration: Security Services*.

- **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 026` – fornece proteção de arquivos moderada

    (`741`) – `r` para grupo, `x` para outros
  - `umask 027` – fornece proteção de arquivos severa

    (`740`) – `r` para grupo, nenhum acesso 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 and Managing User Accounts by Using the CLI" no *Managing User Accounts and User Environments in Oracle Solaris 11.1*
- "Default umask Value" no *Oracle Solaris 11.1 Administration: Security Services*
- As páginas man selecionadas incluem `usermod`(1M) e `umask`(1).

## ▼ Como 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** Você deve assumir a função `root`. Para obter mais informações, consulte "How to Use Your Assigned Administrative Rights" no *Oracle Solaris 11.1 Administration: Security Services*.

**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 11.1 Administration: Security Services*.
- Para obter exemplos de definição de sinalizadores de auditoria, consulte "Configuring the Audit Service (Tasks)" no *Oracle Solaris 11.1 Administration: Security Services* e "Troubleshooting the Audit Service (Tasks)" no *Oracle Solaris 11.1 Administration: Security Services*.
- Para configurar a auditoria, consulte a página man `auditconfig`(1M).

## ▼ Como 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 assumir a função `root` para modificar o arquivo `syslog.conf` . Outras etapas requerem que seja atribuído a você o perfil de direitos Configuração de auditoria. Para obter mais informações, consulte "How to Use Your Assigned Administrative Rights" no *Oracle Solaris 11.1 Administration: Security Services*.

1. **Envie a classe `lo` para o plug-in `audit_syslog` e torne o plug-in ativo.**

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

2. **Determine qual instância de serviço `system-log` está on-line.**

   ```
   # svcs system-log
   STATE          STIME    FMRI
   disabled       13:11:55 svc:/system/system-log:rsyslog
   online         13:13:27 svc:/system/system-log:default
   ```

   **Dica** – Se a instância de serviço `rsyslog` estiver on-line, modifique o arquivo `rsyslog.conf`.

3. **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
   ```

4. **Crie o arquivo de log.**

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

5. **Atualize as informações de configuração para o serviço `system-log`.**

   ```
   # svcadm refresh system-log:default
   ```

   **Observação** – Atualize a instância de serviço `system-log:rsyslog` se o serviço `rsyslog` estiver on-line.

6. **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 11.1 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 51.

## ▼ Como 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** Você deve assumir a função `root`. Para obter mais informações, consulte "How to Use Your Assigned Administrative Rights" no *Oracle Solaris 11.1 Administration: Security Services*.

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 11.1 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 11.1 Administration: Security Services* |
| 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 *Troubleshooting Typical Issues in Oracle Solaris 11.1*<br>"Managing Core Files (Task Map)" no *Troubleshooting Typical Issues in Oracle Solaris 11.1* |

# 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. | "Como exibir uma mensagem de segurança para usuários `ssh` " na página 40 |
| Desativar o daemon de roteamento de rede. | Limita o acesso de possíveis sniffers de rede aos sistemas. | "How to Disable the Network Routing Daemon" no *Securing the Network in Oracle Solaris 11.1* |
| Impedir a disseminação das informações sobre a topologia de rede. | Impede a difusão de pacotes. | "How to Disable Broadcast Packet Forwarding" no *Securing the Network in Oracle Solaris 11.1* |
| | Impede a geração de respostas para solicitações de eco resultantes de operações de difusão e multicast. | "How to Disable Responses to Echo Requests" no *Securing the Network in Oracle Solaris 11.1* |

| Tarefa | Descrição | Instruções |
|---|---|---|
| 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. | "How to Set Strict Multihoming" no *Securing the Network in Oracle Solaris 11.1* |
| Impedir ataques de negação de serviço (DOS) controlando o número de conexões de sistema incompletas. | Limita o número permitido de conexões TCP incompletas para um listener TCP. | "How to Set Maximum Number of Incomplete TCP Connections" no *Securing the Network in Oracle Solaris 11.1* |
| 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. | "How to Set Maximum Number of Pending TCP Connections" no *Securing the Network in Oracle Solaris 11.1* |
| Gerar números aleatórios fortes para conexões TCP iniciais. | É compatível com o valor de geração de número de sequência especificado pelo RFC 6528. | "How to Specify a Strong Random Number for Initial TCP Connection" no *Securing the Network in Oracle Solaris 11.1* |
| Recuperar os valores padrão seguros dos parâmetros de rede. | Aumenta a segurança reduzida por ações administrativas. | "How to Reset Network Parameters to Secure Values" no *Securing the Network in Oracle Solaris 11.1* |
| Adicionar wrappers TCP aos serviços de rede para limitar os aplicativos a usuários legítimos. | Especifica sistemas que podem acessar serviços de rede, como FTP. | "Como Usar TCP Wrappers" na página 41. |

## ▼ Como exibir uma mensagem de segurança para usuários `ssh`

Use esse procedimento para exibir avisos ao efetuar login usando o protocolo `ssh` .

**Antes de começar**

Você criou o arquivo `/etc/issue` na Etapa 1 de "Como colocar uma mensagem de segurança em arquivos de banner" na página 29.

Você deve se tornar um administrador que recebeu a autorização `solaris.admin.edit/etc/ssh/sshd_config` e um dos perfis de direitos Rede. A função `root` possui todos esses direitos. Para obter mais informações, consulte "How to Use Your Assigned Administrative Rights" no *Oracle Solaris 11.1 Administration: Security Services*.

- **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`.**

  ```
  $ pfedit /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)`, `sshd_config(4)` e `pfedit(1M)`.

## ▼ Como Usar TCP Wrappers

As etapas a seguir mostram três formas como os TCP wrappers são usados ou podem ser usados no Oracle Solaris.

**Antes de começar** Você deve assumir a função `root` para modificar um programa para usar TCP wrappers.

1. **Você não precisa proteger o aplicativo `sendmail` com TCP wrappers.**

   Por padrão, ele é protegido por TCP wrappers, como descrito na seção "Support for TCP Wrappers From Version 8.12 of sendmail" no *Managing sendmail Services in Oracle Solaris 11.1*.

2. **Para ativar TCP wrappers para todos os serviços `inetd`, consulte "How to Use TCP Wrappers to Control Access to TCP Services" no *Configuring and Administering Oracle Solaris 11.1 Networks*.**

3. **Proteja o serviço de rede FTP com TCP wrappers.**

   a. **Siga as instruções no módulo `/usr/share/doc/proftpd/modules/mod_wrap.html`.**

   Como este módulo é dinâmico, você deve carregá-lo para usar TCP wrappers com FTP.

   b. **Carregue o módulo adicionando as seguintes instruções ao arquivo `/etc/proftpd.conf`:**

   ```
   <IfModule mod_dso.c>
       LoadModule mod_wrap.c
   </IfModule>
   ```

   c. **Reinicie o serviço FTP.**

   ```
   $ svcadm restart svc:/network/ftp
   ```

# 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.

O sistema de arquivos `tmpfs` pode crescer sem limite. Para impedir um ataque de negação de serviço (DOS), conclua "Como limitar o tamanho do sistema de arquivos `tmpfs`" na página 42.

As tarefas a seguir configuram um limite de tamanho para `tmpfs` e 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 11.1 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 11.1 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 11.1 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 11.1 Administration: ZFS File Systems*<br>"Examples of Encrypting ZFS File Systems" no *Oracle Solaris 11.1 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.<br>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`) |
| Limite o tamanho do sistema de arquivos `tmpfs`. | Impede que um usuário mal-intencionado crie arquivos grandes em `/tmp` para tornar o sistema mais lento. | "Como limitar o tamanho do sistema de arquivos `tmpfs`" na página 42 |

## ▼ Como limitar o tamanho do sistema de arquivos tmpfs

Por padrão, o tamanho do sistema de arquivos `tmpfs` não tem limite. Portanto, o `tmpfs` pode crescer a ponto de ocupar a memória disponível no sistema e o espaço de permuta (swap). Como o diretório `/tmp` é usado por todos os aplicativos e usuários, um aplicativo pode ocupar

toda a memória disponível do sistema. Da mesma forma, um usuário mal-intencionado sem privilégios pode prejudicar o desempenho do sistema criando arquivos grandes no diretório `/tmp`. Para evitar um impacto negativo no desempenho, limite o tamanho de cada montagem `tmpfs`.

Você pode tentar vários valores para obter o melhor desempenho do sistema.

**Antes de começar** Você deve assumir a função `root`. Para obter mais informações, consulte "How to Use Your Assigned Administrative Rights" no *Oracle Solaris 11.1 Administration: Security Services*.

**1 Determine a quantidade de memória do seu sistema.**

---

**Observação –** O sistema SPARC T3 series usado para o exemplo neste procedimento possui um disco de estado sólido (ssd) para operações de E/S mais rápidas e possui oito discos de 279,40 MB. O sistema possui cerca de 500 GB de memória.

---

```
# prtconf | head
System Configuration:  Oracle Corporation  sun4v
Memory size: 523776 Megabytes
System Peripherals (Software Nodes):

ORCL,SPARC-T3-4
    scsi_vhci, instance #0
        disk, instance #4
        disk, instance #5
        disk, instance #6
        disk, instance #8
```

**2 Calcule um limite de memória para o `tmpfs`.**

Dependendo do tamanho da memória do sistema, talvez você queira calcular um limite de memória de cerca de 20 por cento para sistemas de grande porte e 30 por cento para sistemas menores.

Assim, para um sistema menor, use `.30` como o multiplicador.

```
10240M x .30 ≈ 340M
```

Para um sistema maior, use `.20` como o multiplicador.

```
523776M x .20 ≈ 10475M
```

**3 Modifique a entrada de `swap` no arquivo `/etc/vfstab` com o limite de tamanho.**

```
# pfedit /etc/vfstab
#device       device       mount           FS      fsck    mount mount
#to mount     to fsck      point           type    pass    at boot options
#
/devices      -            /devices        devfs   -       no      -
/proc         -            /proc           proc    -       no      -
ctfs          -            /system/contract ctfs   -       no      -
```

```
objfs           -           /system/object  objfs   -       no      -
sharefs         -           /etc/dfs/sharetab  sharefs -    no      -
fd              -           /dev/fd         fd      -       no      -
swap            -           /tmp            tmpfs   -       yes     -
swap            -           tmpfs           -       yes     size=10400m
/dev/zvol/dsk/rpool/swap    -       -       swap    -       no      -
```

**4 Reinicialize o sistema.**

```
# reboot
```

**5 Verifique se o limite de tamanho está em vigor.**

```
# mount -v
swap on /system/volatile type tmpfs
read/write/setuid/devices/rstchown/xattr/dev=89c0006 on Fri Sep 7 14:07:27 2012
swap on /tmp type tmpfs
read/write/setuid/devices/rstchown/xattr/size=10400m/dev=89c0006 on Fri ...
```

**6 Monitore o uso da memória e ajuste-o aos requisitos do seu site.**

O comando `df` é útil. O comando `swap` fornece as estatísticas mais úteis.

```
# df -h /tmp
Filesystem Size Used Available Capacity Mounted on
swap          7.  4G     44M    7.4G 1%       /tmp

# swap -s
total: 190248k bytes allocated + 30348k reserved = 220596k used,
7743780k available
```

Para obter mais informações, consulte as páginas man `tmpfs`(7FS), `mount_tmpfs`(1M), `df`(1M) e `swap`(1M).

# 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. | "Como definir um valor `umask` mais restritivo para usuários regulares" na página 35 |
| 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 11.1 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*.

## 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 11.1 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 6, "IP Security Architecture (Overview)," no *Securing the Network in Oracle Solaris 11.1*
- Capítulo 9, "Internet Key Exchange (Overview)," no *Securing the Network in Oracle Solaris 11.1*
- Capítulo 7, "Configuring IPsec (Tasks)," no *Securing the Network in Oracle Solaris 11.1*
- Capítulo 10, "Configuring IKE (Tasks)," no *Securing the Network in Oracle Solaris 11.1*

## Configuração do recurso Filtro IP

O recurso Filtro IP fornece um firewall.

Para obter informações e procedimentos, consulte:

- Capítulo 4, "IP Filter in Oracle Solaris (Overview)," no *Securing the Network in Oracle Solaris 11.1*
- Capítulo 5, "IP Filter (Tasks)," no *Securing the Network in Oracle Solaris 11.1*

## 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 11.1 Administration: Security Services*
- Capítulo 21, "Configuring the Kerberos Service (Tasks)," no *Oracle Solaris 11.1 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 11.1 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 "Verificação da integridade do arquivo usando o BART" na página 49.

# 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 6, "IP Security Architecture (Overview)," no *Securing the Network in Oracle Solaris 11.1*
- "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

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



## Verificação da integridade do arquivo usando o BART

BART é uma ferramenta de relatórios e verificação de integridade de arquivos baseada em regras que utiliza somas de verificação de força criptográfica e metadados de sistema de arquivos para reportar alterações.

Para obter informações e procedimentos, consulte:

- "BART (Overview)" no *Oracle Solaris 11.1 Administration: Security Services*
- "Using BART (Tasks)" no *Oracle Solaris 11.1 Administration: Security Services*
- "BART Manifests, Rules Files, and Reports (Reference)" no *Oracle Solaris 11.1 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 11.1 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 11.1 Administration: Security Services*.

- Capítulo 26, "Auditing (Overview)," no *Oracle Solaris 11.1 Administration: Security Services*
- Capítulo 27, "Planning for Auditing," no *Oracle Solaris 11.1 Administration: Security Services*
- Capítulo 28, "Managing Auditing (Tasks)," no *Oracle Solaris 11.1 Administration: Security Services*
- Capítulo 29, "Auditing (Reference)," no *Oracle Solaris 11.1 Administration: Security Services*

  Para obter uma lista das páginas man e dos links para elas, consulte "Audit Service Man Pages" no *Oracle Solaris 11.1 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 11.1 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 11.1 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 11.1 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 11.1 Administration: Security Services*
- "How to Prevent Audit Trail Overflow" no *Oracle Solaris 11.1 Administration: Security Services*
- "Managing Audit Records on Local Systems (Tasks)" no *Oracle Solaris 11.1 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 11.1 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

O livro e os artigos a seguir contêm descrições de segurança dos sistemas Oracle Solaris 11.

- *Oracle Solaris 11.1 Administration: Security Services*

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

- *Security Configuration Benchmark For Solaris 11 11/11 Versão 1.0.0 11 de junho, 2012*

  Esse benchmark de segurança é publicado pelo CIS (Center for Internet Security) `http://cisecurity.org/` para a comunidade de segurança. Este documento recomenda as configurações de segurança para o SO Oracle Solaris. O público-alvo inclui administradores de sistemas e aplicativos, especialistas em segurança, auditores, engenheiros de suporte, e instaladores e desenvolvedores que desenvolvem, instalam, avaliam ou fornecem soluções de segurança para o Oracle Solaris. Para obter uma cópia, visite CIS Security Benchmarks (`http://benchmarks.cisecurity.org/`).

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