# Guia de Segurança do Oracle® Server X5-2L

**Número do Item: E58231-01**
Outubro de 2014

**Número do Item: E58231-01**

# Conteúdo

# Segurança Básica

Este documento contém diretrizes gerais de segurança para ajudar a proteger o servidor Oracle, as interfaces de rede do servidor e os comutadores de rede conectados.

Entre em contato com o Oficial de Segurança de TI para obter requisitos de segurança adicionais específicos para o seu sistema e ambiente.

Existem quatro princípios básicos de segurança que você deve seguir ao usar qualquer tipo de hardware e software. Esta seção aborda os quatro princípios básicos de segurança:



## Acesso

O acesso se refere ao acesso físico ao hardware ou ao acesso físico ou virtual ao software.

- Use os controles físicos e de software para proteger seu hardware e seus dados contra invasão.
- Altere todas as senha padrão ao instalar um novo sistema. A maioria dos tipos de equipamento utiliza senhas padrão, como `changeme`, que são amplamente conhecidas e que permitiriam acesso não autorizado ao hardware ou software.
- Consulte a documentação que acompanha o software para ativar todos os recursos de segurança disponíveis para o software.
- Instale servidores e equipamentos relacionados em um local trancado com acesso restrito.
- Se o equipamento for instalado em um rack com uma porta com fechadura, mantenha a porta trancada, exceto durante os períodos de manutenção nos componentes do rack.
- Restrinja o acesso às portas e aos consoles USB. Dispositivos como controladores de sistema, unidades de distribuição de energia (PDUs) e comutadores de rede podem ter conexões USB, que podem oferecer acesso direto ao sistema. O acesso físico é um método mais seguro de acessar componentes já que ele não é suscetível a ataques baseados na rede.
- Restrinja a capacidade de reiniciar o sistema na rede.

- Restrinja o acesso especificamente a dispositivos hot-plug ou hot-swap porque podem ser facilmente removidos.
- Guarde unidades substituíveis no campo (FRUs) e unidade substituíveis pelo cliente (CRUs) sobressalentes em um gabinete fechado. Restrinja o acesso ao gabinete trancado a pessoas autorizadas.

# Autenticação

A autenticação é como um usuário é identificado, normalmente por meio de informações confidenciais, como nome de usuário e senha. A autenticação se refere a garantir que os usuários do hardware ou software são quem eles dizem que são.

- Configure recursos de autenticação, como um sistema de senhas nos sistemas operacionais da plataforma, para garantir que os usuários são realmente quem eles dizem ser.
- Certifique-se de que sua equipe use crachás para entrar na sala do computador.
- Para contas de usuário: use listas de controle de acesso onde apropriado; defina tempos limite para sessões estendidas; defina níveis de privilégios para usuários.

# Autorização

A autorização permite que os administradores controlem quais tarefas ou privilégios um usuário pode executar ou usar. Sua equipe só pode executar as tarefas e usar os privilégios que foram atribuídos a ela. A autorização se refere a restrições impostas à equipe para trabalhar com hardware ou software.

- Permita que sua equipe trabalhe somente com hardware e software nos quais foi treinada e esteja qualificada para usar.
- Configure um sistema de permissões de Leitura/Gravação/Execução para controlar o acesso de usuários a comandos, espaço em disco, dispositivos e aplicativos.

# Contabilidade e Auditoria

A contabilidade e a auditoria se referem à manutenção de um registro das atividades do usuário no sistema. Os servidores Oracle possuem recursos de software e hardware que permitem que os administradores monitorem atividades de login e mantenham inventários de hardware.

- Use logs do sistema para monitorar logins de usuários. Monitore as contas de administrador do sistema e de serviço em particular porque essas contas têm acesso aos comandos que, se usados incorretamente, poderiam prejudicar o sistema ou resultar em perda de dados. O acesso e os comandos devem ser cuidadosamente monitorados por meio de logs do sistema.

- Registre os números de série de todo o hardware. Use números de série de componente para rastrear ativos do sistema. Os números de peça da Oracle são gravados eletronicamente em cartões, módulos e placas-mãe, e podem ser usados para fins de inventário.
- Para detectar e rastrear componentes, faça uma marca de segurança em todos os itens importantes do hardware do computador, como FRUs e CRUs. Use canetas especiais ultravioletas ou etiquetas em alto-relevo.
- Mantenha as chaves de ativação de hardware e as licenças em um local seguro de fácil acesso ao administrador do sistema, principalmente durante situações de emergência do sistema. Os documentos impressos talvez sejam o seu único comprovante de propriedade.

# Como Usar as Ferramentas de Configuração e Gerenciamento do Servidor de Forma Segura

Siga as diretrizes de segurança destas seções ao usar ferramentas de software e firmware para configurar e gerenciar o servidor:

- “Segurança do Oracle System Assistant” [11]
- “Segurança do Oracle ILOM” [12]
- “Segurança do Oracle Hardware Management Pack” [14]

Entre em contato com o Oficial de Segurança de TI para obter requisitos de segurança adicionais específicos para o seu sistema e ambiente.

## Segurança do Oracle System Assistant

O Oracle System Assistant é uma ferramenta pré-instalada que ajuda a configurar e atualizar o hardware do servidor e a instalar sistemas operacionais compatíveis. Para obter informações sobre como usar o Oracle System Assistant, consulte o *Oracle X5 Series Servers Administration Guide* em:

`http://www.oracle.com/goto/x86AdminDiag/docs`

As informações a seguir descrevem informações de segurança relacionadas ao Oracle System Assistant.

- **O Oracle System Assistant contém um ambiente root inicializável.**

  O Oracle System Assistant é um aplicativo executado em uma unidade flash USB interna e pré-instalada. O Oracle System Assistant contém um ambiente root inicializável. O Oracle System Assistant também fornece a capacidade de acessar sua shell root subjacente. Os usuários com acesso físico ao sistema ou os que têm acesso KVMS remoto (teclado, vídeo, mouse e armazenamento) ao sistema por meio do Oracle ILOM, poderão acessar o Oracle System Assistant e a shell root.

  Um ambiente root pode ser usado para alterar a configuração e as políticas do sistema, assim como acessar dados em outros discos. Para aumentar a segurança, proteja o acesso físico ao servidor e atribua privilégios de administrador e console aos usuários do Oracle ILOM com moderação.

A shell do Oracle System Assistant foi criada para permitir que os usuários com privilégios apropriados usem as ferramentas CLI T do Oracle Hardware Management Pack para fins de gerenciamento do sistema. A shell não foi criada para fornecer serviços de rede. Os serviços de rede são desabilitados por padrão para garantir o nível mais alto de segurança e não devem ser habilitados.

- **O Oracle System Assistant monta um dispositivo de armazenamento USB que é acessível ao sistema operacional.**

  Além de ser um ambiente inicializável, o Oracle System Assistant também é montado como um dispositivo de armazenamento USB (unidade flash) que é acessível ao sistema operacional do host após a instalação. Isso é útil para o acesso a ferramentas e drivers durante operações de manutenção e reconfiguração. O dispositivo de armazenamento USB do Oracle System Assistant é legível e gravável, podendo ser potencialmente explorado por vírus.

  Para mais segurança, aplique ao dispositivo de armazenamento do Oracle System Assistant os mesmos métodos usados para a proteção de discos, incluindo verificações regulares de vírus e verificação de integridade.

- **O Oracle System Assistant pode ser desabilitado.**

  O Oracle System Assistant é uma ferramenta útil que auxilia na configuração do servidor, atualização e configuração de firmware e instalação do sistema operacional do host. No entanto, se as implicações de segurança descritas acima forem inaceitáveis ou se a ferramenta não for necessária, o Oracle System Assistant poderá ser desativado. Após desabilitar o Oracle System Assistant, o dispositivo de armazenamento USB não fica mais acessível para o sistema operacional host e os usuários não conseguirão inicializar no Oracle System Assistant.

  Você pode desativar o Oracle System Assistant na própria ferramenta ou no BIOS. Depois de desabilitado, o Oracle System Assistant só poderá ser habilitado novamente com o BIOS Setup Utility. É recomendável que o BIOS Setup seja protegido por senha para que somente os usuários autorizados possam habilitar o Oracle System Assistant novamente.

- **Consulte a documentação do Oracle System Assistant.**

  Para obter informações sobre os recursos e funções do Oracle System Assistant, consulte o *Oracle X5 Series Servers Administration Guide* em:

  `http://www.oracle.com/goto/x86AdminDiag/docs`

# Segurança do Oracle ILOM

É possível proteger, gerenciar e monitorar ativamente os componentes do sistema usando o firmware de gerenciamento Oracle ILOM (Integrated Lights Out Manager), o qual é incorporado nos sistemas Oracle baseados em x86 e em alguns servidores baseados em SPARC. Dependendo do nível de autorização concedido aos administradores do sistema, essas funções podem incluir a capacidade de desativar o servidor, criar contas de usuário, montar dispositivos de armazenamento remoto e assim por diante.

- **Use uma rede interna confiável e segura.**

  Seja para estabelecer ou não uma conexão de gerenciamento físico com o Oracle ILOM através de porta local serial, porta de gerenciamento de rede dedicada ou porta de rede de dados padrão, será essencial que essa porta física no servidor esteja sempre conectada a uma rede confiável interna ou uma rede privada ou de gerenciamento seguro dedicado.

  Nunca conecte o processador de serviço (SP) do Oracle ILOM a uma rede pública, como a Internet. Você deve manter o tráfego de gerenciamento do Oracle ILOM SP em uma rede de gerenciamento separada e conceder acesso apenas a administradores de sistema.

- **Limite o uso da conta do Administrador padrão.**

  Limite o uso da conta padrão do Administrador (`root`) ao login inicial do Oracle ILOM. Essa conta padrão do Administrador é fornecida apenas para auxiliar a instalação inicial do servidor. Portanto, para garantir o ambiente mais seguro possível, é necessário alterar a senha padrão do Administrador (`changeme`) como parte da configuração inicial do sistema. O acesso à conta padrão do Administrador concede a um usuário acesso irrestrito a todos os recursos do Oracle ILOM. Além disso, estabeleça novas contas de usuário com senhas exclusivas e atribua níveis de autorização exclusivos (funções de usuário) a cada novo usuário do Oracle ILOM.

- **Analise com cuidado os riscos ao conectar a porta serial a um servidor de terminais.**

  Os dispositivos de terminais nem sempre fornecem os níveis apropriados de autenticação ou autorização de usuários necessários para proteger a rede contra invasões maliciosas. Para proteger o sistema contra invasões indesejadas na rede, não estabeleça uma conexão serial (porta serial) com o Oracle ILOM por qualquer tipo de dispositivo de redirecionamento de rede, como um servidor de terminais, a menos que o servidor tenha controles de acesso suficientes.

  Além disso, algumas funções do Oracle ILOM, como redefinição de senha e menu Preboot, só estarão disponíveis com a porta serial física. A conexão da porta serial com uma rede usando um servidor de terminais não autenticado elimina a necessidade do acesso físico, o que reduz a segurança associada a essas funções.

- **O acesso ao menu Preboot requer o acesso físico ao servidor.**

  O menu Preboot do Oracle ILOM é um utilitário avançado que fornece uma maneira de redefinir o Oracle ILOM aos valores padrão, e piscar o firmware se o Oracle ILOM não estiver respondendo. Depois que o Oracle ILOM tiver sido redefinido, o usuário será solicitado a pressionar um botão no servidor (o padrão) ou digitar uma senha. A propriedade de Presença Física do Oracle ILOM controla esse comportamento (`check_physical_presence=true`). Para obter segurança máxima ao acessar o menu Preboot, não altere a configuração padrão (`true`), para que o acesso ao menu Preboot sempre exija o acesso físico ao servidor.

- **Consulte a documentação do Oracle ILOM.**

  Consulte a documentação do Oracle ILOM para saber mais sobre a configuração de senhas, o gerenciamento de usuários e a aplicação de recursos relacionados a segurança. Para obter diretrizes de segurança específicas do Oracle ILOM, consulte o *Oracle ILOM Security Guide*, que faz parte da biblioteca de documentação do Oracle ILOM. Você encontra a documentação do Oracle ILOM em:

  `http://www.oracle.com/goto/ILOM/docs`

# Segurança do Oracle Hardware Management Pack

O Oracle Hardware Management Pack está disponível para o seu servidor e para muitos outros servidores Oracle baseados em x86 e alguns servidores baseados em SPARC. O Oracle Hardware Management Pack apresenta dois componentes: um agente de monitoramento SNMP e uma família de ferramentas de interface da linha de comando (CLI Tools) do sistema operacional cruzado para o gerenciamento do seu servidor.

- **Use Plugins SNMP do Hardware Management Agent.**

  O SNMP é um protocolo padrão usado para monitorar ou gerenciar um sistema. Com os Plug-ins SNMP do Hardware Management Agent, é possível usar o SNMP para monitorar servidores Oracle no seu centro de dados com a vantagem de não precisar se conectar a dois pontos de gerenciamento, o host e o Oracle ILOM. Essa funcionalidade permite usar um único endereço IP (o endereço IP do host) para monitorar vários servidores.

  Os Plug-ins SNMP são executados no sistema operacional do host de servidores Oracle. O módulo de Plug-in SNMP que estende o agente SNMP nativo no sistema operacional do host para fornecer outros recursos do Oracle MIB. O Oracle Hardware Management Pack não contém ele próprio um agente SNMP. Para o Linux, um módulo é adicionado ao agente net-snmp. Para o Oracle Solaris, um módulo é adicionado ao Oracle Solaris Management Agent. Para o Microsoft Windows, o Plug-in estende o serviço SNMP nativo. Todas as configurações de segurança relacionadas ao SNMP para o Oracle Hardware Management Pack são determinadas pelas configurações do agente ou serviço SNMP nativo, e não pelo Plug-in.

  O SNMPv1 e o SNMPv2c não fornecem criptografia e usam strings de comunidade como uma forma de autenticação. O SNMPv3 é mais seguro e é a versão recomendada porque usa a criptografia para fornecer um canal seguro, além de nomes de usuário e senha individuais.

- **Consulte a documentação do Oracle Hardware Management Pack.**

  Consulte a documentação do Oracle Hardware Management Pack para obter mais informações sobre esses recursos. Para obter as diretrizes de segurança específicas do Oracle Hardware Management Pack, consulte o *Oracle Hardware Management Pack (HMP) Security Guide*, que faz parte da biblioteca de documentos do Oracle Hardware Management Pack. Você encontra a documentação do Oracle Hardware Management Pack em:

  `http://www.oracle.com/goto/OHMP/docs`

# Planejamento de um Ambiente Seguro

As diretrizes de segurança devem estar implementadas antes da chegada do sistema. Após a chegada, as diretrizes de segurança devem ser revisadas e ajustadas periodicamente para ficarem atualizadas com os requisitos de segurança da sua organização.

Use as informações destas seções antes e durante a instalação e configuração de um servidor e equipamento relacionado:



Entre em contato com o Oficial de Segurança de TI para obter requisitos de segurança adicionais específicos para o seu sistema e ambiente.

## Proteção por Senha

As senhas são um aspecto importante da segurança, pois senhas mal escolhidas podem resultar em acesso não autorizado aos recursos da empresa. A implementação das melhores práticas de gerenciamento de senhas garante que os usuários sigam um conjunto de diretrizes para criação e proteção de suas senhas. Os componentes típicos de uma política de senha devem definir:

- Tamanho e força da senha
- Duração da senha
- Práticas comuns de senha

Imponha as seguintes práticas padrão para a criação de senhas fortes complexas:

- Não crie senhas que contenham o nome do usuário, o nome do funcionário ou nomes de familiares.
- Não escolha senhas fáceis de adivinhar.
- Não crie senhas que contenham uma sequência consecutiva de números como 12345.
- Não crie senhas que contenham uma palavra ou sequência de caracteres que seja facilmente descoberta por uma simples busca na Internet.

- Não permita que os usuários reutilizem a mesma senha em vários sistemas.
- Não permita que usuários reutilizem senhas antigas.

Altere sua senha regularmente. Isso ajuda a impedir atividade maliciosa e garante que as senhas sigam as diretrizes de senha atuais.

# Diretrizes de Segurança do Sistema Operacional

Consulte os documentos do sistema operacional (SO) Oracle para obter informações sobre:

- Como usar recursos de segurança ao configurar sistemas
- Como operar com segurança ao adicionar aplicativos e usuários a um sistema
- Como proteger aplicativos baseados em rede

Os documentos do Guia de Segurança para sistemas operacionais Oracle compatíveis fazem parte da biblioteca de documentos do sistema operacional. Para encontrar o documento do Guia de Segurança referente a um sistema operacional Oracle, vá para a biblioteca de documentos do sistema operacional Oracle:

| Sistema Operacional | Link |
|---|---|
| SO Oracle Solaris | www.oracle.com/technetwork/documentation/solaris-11-192991.html |
| SO Oracle Linux | http://www.oracle.com/technetwork/documentation/ol-1-1861776.html |
| Oracle VM | http://www.oracle.com/technetwork/documentation/vm-096300.html |

Para obter informações sobre os sistemas operacionais de outros fornecedores, como o Red Hat Enterprise Linux, SUSE Linux Enterprise Server, Microsoft Windows e VMware ESXi, consulte a documentação do fornecedor.

# Portas e Comutadores de Rede

Os comutadores de rede oferecem níveis diferentes de recursos de segurança de porta. Consulte a documentação sobre comutadores para aprender a:

- Usar recursos de autenticação, autorização e contabilidade para acesso local e remoto ao comutador.
- Alterar todas as senhas nos comutadores de rede que podem ter várias contas de usuários e senhas por padrão.
- Gerenciar comutadores fora de banda (separados do tráfego de dados). Se o gerenciamento fora de banda (out-of-band) não for viável, dedique um número de rede local virtual (VLAN) separado para o gerenciamento dentro da banda (in-band).

- Use o recurso de espelhamento de portas do comutador de rede para acesso ao sistema de detecção de invasões (IDS).
- Mantenha um arquivo de configuração de comutador off-line e restrinja o acesso somente a administradores autorizados. O arquivo de configuração deve conter comentários descritivos para cada definição.
- Implemente a segurança de porta para limitar o acesso com base nos endereços MAC. Desative o entroncamento automático em todas as portas.
- Use estes recursos de segurança de porta se eles estiverem disponíveis no seu switch:
  - **Bloqueio de MAC** envolve a associação de um endereço MAC (Media Access Control) de um ou mais dispositivos conectados a uma porta física em um switch. Se você bloquear uma porta de switch para um endereço MAC específico, os superusuários não poderão criar backdoors na rede com pontos de acesso invasores (rogue).
  - **Bloqueio de MAC** impede que um endereço MAC específico se conecte a um switch.
  - **Conhecimento de MAC** utiliza o conhecimento sobre cada conexão direta da porta do comutador de modo que o comutador de rede possa definir a segurança com base nas conexões atuais.

# Segurança de VLAN

Se você configurar uma rede virtual de área local (VLAN), lembre-se de que as VLANs compartilham largura de banda em uma rede e exigem medidas de segurança adicionais.

- Separe cluster confidenciais do sistema do restante da rede ao usar VLANs. Isso reduz a probabilidade de os usuários obterem acesso às informações sobre esses clientes e servidores.
- Atribua um número de VLAN nativo exclusivo às portas de entroncamento.
- Limite as VLANs que podem ser transportadas em um entroncamento a apenas aquelas que forem estritamente necessárias.
- Desabilite o VTP (VLAN Trunking Protocol), se possível. Caso contrário, defina o seguinte para o VTP: domínio de gerenciamento, senha e abreviação. Em seguida, defina o VTP no modo transparente.
- Use as configurações de VLAN estática, quando possível.
- Desabilite portas de comutador não utilizadas e atribua a elas um número de VLAN não utilizado.

# Segurança de Infiniband

Mantenha os hosts Infiniband seguros. Uma malha InfiniBand é tão segura quanto seu host Infiniband menos seguro.

Observe que o particionamento não protege uma malha Infiniband. O particionamento só oferece isolamento de tráfego para Infiniband entre máquinas virtuais em um host.

# Manutenção de um Ambiente Seguro

Após a instalação e configuração iniciais, use os recursos de segurança de software e hardware da Oracle para continuar a controlar os ativos de hardware e software.

Use as informações nestas seções para manter um ambiente seguro:



Entre em contato com o Oficial de Segurança de TI para obter requisitos de segurança adicionais específicos para o seu sistema e ambiente.

## Controle de Energia

É possível usar o software para ativar e desativar alguns sistemas Oracle. As unidades de distribuição de energia (PDUs) de alguns gabinetes de sistema podem ser ativadas e desativadas remotamente. A autorização para esses comandos é normalmente configurada durante a configuração do sistema e, em geral, é limitada aos administradores do sistema e à equipe de manutenção.

Consulte a documentação do sistema ou gabinete para obter mais informações.

## Rastreamento de Ativos

Use números de série para rastrear o estoque. A Oracle insere números de série em cartões de opção e em placas-mãe do sistema de firmware. É possível ler esses números de série por meio de conexões de rede local (LAN).

Também é possível usar leitores sem fio RFID (Radio Frequency Identification) para simplificar ainda mais o rastreamento de ativos. Um white paper da Oracle, *How to Track Your Oracle Sun System Assets by Using RFID* está disponível em:

http://www.oracle.com/technetwork/articles/systems-hardware-architecture/o11-001-rfid-oracle-214567.pdf

# Atualizações de Software e Firmware

Aprimoramentos de segurança são incluídos nas novas versões e patches de software. O gerenciamento proativo e eficaz de patches é uma parte importante da segurança do sistema. Para obter as melhores práticas de segurança, atualize o sistema com a versão mais recente do software e todos os patches de segurança necessários.

- Verifique regularmente se há atualizações de software e patches de segurança.
- Sempre instale a última versão lançada do software ou firmware.
- Instale todos os patches de segurança necessários para o software.
- Lembre-se de que os dispositivos, como comutadores de rede, também contêm firmware e podem necessitar de atualizações de patches e firmware.

As atualizações de software e os patches de segurança podem ser encontrados no site do My Oracle Support em:

http://support.oracle.com

# Segurança de Rede

Depois que as redes são configuradas com base nos princípios de segurança, são necessárias uma revisão e manutenção regulares.

Siga estas diretrizes para proteger o acesso local e remoto aos seus sistemas:

- Limite a configuração remota a endereços IP específicos usando SSH em vez de Telnet. O Telnet transmite nomes de usuário e senhas em texto não criptografado, permitindo que todos no segmento de rede local (LAN) vejam as credenciais de login. Defina uma senha forte para o SSH.
- Use a versão 3 do SNMP (Simple Network Management Protocol) para fornecer transmissões seguras. As versões anteriores do SNMP não são seguras e transmitem dados de autenticação em texto não criptografado. O SNMPv3 usa a criptografia para fornecer um canal seguro, além de nomes de usuário e senha individuais.
- Altere a string de comunidade SNMP padrão para uma string de comunidade forte se o SNMPv1 ou o SNMPv2 for necessário. Alguns produtos têm PUBLIC definido como a cadeia de caracteres de comunidade SNMP padrão. Os hackers podem consultar uma comunidade para montar um mapa de rede completo e possivelmente modificar valores de MIB (Management Information Base).

- Sempre faça logout depois de usar o controlador do sistema se ele usa uma interface de navegador.
- Desabilite serviços de rede desnecessários, como TCP (Transmission Control Protocol) ou HTTP (Hypertext Transfer Protocol). Habilite os serviços de rede necessários e configure esses serviços de forma segura.
- Crie uma mensagem de banner que apareça no login para indicar que o acesso não autorizado é proibido. Você pode informar os usuários sobre regras ou políticas importantes. O banner pode ser usado para avisar usuários sobre restrições de acesso especiais para um sistema fornecido ou para lembrar aos usuários as políticas de senha e uso apropriado.
- Use listas de controle de acesso para aplicar restrições, quando apropriado.
- Defina tempos-limite para sessões estendidas e defina níveis de privilégio.
- Use recursos de autenticação, autorização e contabilidade para acesso local e remoto a um comutador.
- Use estes serviços em ambientes muito seguros, pois são protegidos por certificados e outras formas de criptografia forte para proteger o canal:
  - Active Directory
  - LDAP/SSL (Lightweight Directory Access Protocol/Secure Socket Layer)
- Use estes serviços em redes privadas e seguras onde não existam usuários maliciosos suspeitos:
  - RADIUS (Remote Authentication Dial In User Service)
  - TACACS+ (Terminal Access Controller Access-Control System)
- Use o recurso de espelhamento de portas do comutador para acesso ao IDS (sistema de detecção de intrusos).
- Implemente a segurança de porta para limitar o acesso com base em um endereço MAC. Desative o entroncamento automático em todas as portas.

Para obter mais informações sobre a segurança de rede, consulte o *Oracle ILOM Security Guide*, que faz parte da biblioteca de documentação do Oracle ILOM. Você encontra a documentação do Oracle ILOM em:

`http://www.oracle.com/goto/ILOM/docs`

# Proteção e Segurança de Dados

Siga estas diretrizes para maximizar a proteção e a segurança dos dados:

- Faça backup de dados importantes usando dispositivos, como discos rígidos externos ou dispositivos de armazenamento USB. Armazene os dados submetidos a backup em um local externo seguro.
- Use o software de criptografia de dados para manter as informações confidenciais em discos rígidos seguros.

- Ao descartar um disco rígido antigo, destrua fisicamente a unidade ou apague completamente todos os dados contidos na unidade. Informações ainda podem ser recuperadas de uma unidade depois que os arquivos forem excluídos ou que a unidade tiver sido reformatada. Excluir os arquivos ou reformatar a unidade remove somente as tabelas de endereços na unidade. Use um software de limpeza de disco para apagar completamente todos os dados em uma unidade.
- Discos rígidos são geralmente usados para armazenar informações confidenciais. Para proteger essas informações contra a divulgação não autorizada, os discos rígidos devem ser limpos antes de serem reutilizados, descontinuados ou descartados.
  - Use ferramentas de limpeza de disco como o comando `format(1M)` do Oracle Solaris para apagar completamente todos os dados do disco rígido. Como alternativa, é possível usar ferramentas de desmagnetização física, se apropriadas e disponíveis.
  - Em alguns casos, as informações contidas nos discos rígidos são tão confidenciais que o método de limpeza mais apropriado é a destruição física do disco rígido por meio de pulverização ou incineração.
  - É altamente recomendado que as organizações consultem suas políticas de proteção de dados para determinar o método mais apropriado de limpeza dos discos rígidos.

**Cuidado -** Talvez um software de limpeza de disco não consiga excluir alguns dados em discos rígidos modernos, principalmente os SSDs (Solid State Drives), devido à maneira como gerenciam o acesso aos dados.

# Manutenção de Logs

Inspecione e faça a manutenção de seus arquivos de log regularmente. Use estes métodos para proteger arquivos de log:

- Ative o registro em log e envie logs do sistema para um host de log dedicado seguro.
- Configure o registro em log para incluir informações de tempo precisas, usando NTP (Network Time Protocol) e registros de hora e data.
- Realize com frequência verificações agendadas nos logs de dispositivos da rede para detectar atividades de rede ou acessos incomuns.
- Verifique possíveis incidentes nos logs e arquive-os de acordo com uma política de segurança.
- Remova periodicamente arquivos de log quando excederem um tamanho considerável. Mantenha cópias dos arquivos removidos para possíveis referências futuras ou análise estatística.