

Guia de Segurança do Oracle Hardware Management Pack

Este programa de computador e sua documentação são fornecidos sob um contrato de licença que contém restrições sobre seu uso e divulgação, sendo também protegidos pela legislação de propriedade intelectual. Exceto em situações expressamente permitidas no contrato de licença ou por lei, não é permitido usar, reproduzir, traduzir, divulgar, modificar, licenciar, transmitir, distribuir, expor, executar, publicar ou exibir qualquer parte deste programa de computador e de sua documentação, de qualquer forma ou através de qualquer meio. Não é permitida a engenharia reversa, a desmontagem ou a descompilação deste programa de computador, exceto se exigido por lei para obter interoperabilidade.

As informações contidas neste documento estão sujeitas a alteração sem aviso prévio. A Oracle Corporation não garante que tais informações estejam isentas de erros. Se você encontrar algum erro, por favor, nos envie uma descrição de tal problema por escrito.

Se este programa de computador, ou sua documentação, for entregue / distribuído(a) ao Governo dos Estados Unidos ou a qualquer outra parte que licencie os Programas em nome daquele Governo, a seguinte nota será aplicável:

U.S. GOVERNMENT END USERS:

Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

Este programa de computador foi desenvolvido para uso em diversas aplicações de gerenciamento de informações. Ele não foi desenvolvido nem projetado para uso em aplicações inerentemente perigosas, incluindo aquelas que possam criar risco de lesões físicas. Se utilizar este programa em aplicações perigosas, você será responsável por tomar todas e quaisquer medidas apropriadas em termos de segurança, backup e redundância para garantir o uso seguro de tais programas de computador. A Oracle Corporation e suas afiliadas se isentam de qualquer responsabilidade por quaisquer danos causados pela utilização deste programa de computador em aplicações perigosas.

Oracle e Java são marcas comerciais registradas da Oracle Corporation e/ou de suas empresas afiliadas. Outros nomes podem ser marcas comerciais de seus respectivos proprietários.

Intel e Intel Xeon são marcas comerciais ou marcas comerciais registradas da Intel Corporation. Todas as marcas comerciais SPARC são usadas sob licença e são marcas comerciais ou marcas comerciais registradas da SPARC International, Inc. AMD, Opteron, o logotipo da AMD e o logotipo do AMD Opteron são marcas comerciais ou marcas comerciais registradas da Advanced Micro Devices. UNIX é uma marca comercial registrada licenciada por meio do consórcio The Open Group.

Este programa e sua documentação podem oferecer acesso ou informações relativas a conteúdos, produtos e serviços de terceiros. A Oracle Corporation e suas empresas afiliadas não fornecem quaisquer garantias relacionadas a conteúdos, produtos e serviços de terceiros e estão isentas de quaisquer responsabilidades associadas a eles. A Oracle Corporation e suas empresas afiliadas não são responsáveis por quaisquer tipos de perdas, despesas ou danos incorridos em consequência do acesso ou da utilização de conteúdos, produtos ou serviços de terceiros.

Conteúdo

Visão Geral	5
Visão Geral do Produto	5
Sobre Este Guia de Segurança	6
Princípios de Segurança Básicos	6
Resumo de Segurança do Oracle Hardware Management Pack	7
Pré-instalação do Oracle Hardware Management	9
Componentes do Oracle Hardware Management Pack	9
Configurações de Segurança do Plug-in SNMP Baseado no Agent	10
Escolhendo uma Versão do Protocolo SNMP do SNMP Agent	10
Instalação do Oracle Hardware Management Pack	11
Executando o Instalador do Oracle Hardware Management Pack	11
Optando pela Ativação da Interconexão de LAN	11
Optando por Salvar Credenciais em um Arquivo	12
Pós-instalação do Oracle Hardware Management Pack	13
Desinstalação do Oracle Hardware Management Pack	13

Visão Geral

Esta seção oferece uma visão geral do produto Oracle Hardware Management Pack (HMP), incluindo informações do guia de segurança, e explica os princípios gerais da segurança do aplicativo.

Os seguintes tópicos são abordados:

- [“Visão Geral do Produto” na página 5](#)
- [“Sobre Este Guia de Segurança” na página 6](#)
- [“Princípios de Segurança Básicos” na página 6](#)
- [“Resumo de Segurança do Oracle Hardware Management Pack” na página 7](#)

Visão Geral do Produto

O Oracle Hardware Management Pack está disponível para o seu servidor e para muitos outros servidores 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 linha de comando entre sistemas operacionais (CLI Tools) para o gerenciamento de seus servidores.

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

Os Plug-ins SNMP do Hardware Management Agent são executados no sistema operacional host dos servidores Oracle. Os Plug-ins SNMP usam as Bibliotecas de Acesso de Armazenamento do Oracle Hardware para se comunicarem com o processador de serviços. O Hardware Management Agent busca automaticamente informações sobre o estado atual do servidor.

É possível usar as CLI Tools do Oracle Server para configurar servidores Oracle. As CLI Tools são compatíveis com os sistemas operacionais Oracle Solaris, Oracle Linux, Oracle VM, outras variações do Linux e Microsoft Windows. A tabela a seguir descreve as tarefas que podem ser executadas com o uso das CLI Tools.

Tarefa de Gerenciamento de Sistema do SO Host	CLI Tool
Defina as configurações de BIOS, a ordem de inicialização do dispositivo e algumas configurações do processador de serviços.	ubiosconfig biosconfig
Atualize o Oracle ILOM e a BIOS.	fwupdate
Consulte, atualize e valide versões de firmware em dispositivos de armazenamento SAS compatíveis, controladores de armazenamento SAS incorporados, expansores de armazenamento SAS e unidades de armazenamento.	
Restaurar, defina e exiba configurações do Oracle ILOM e exiba e configure propriedades do Oracle ILOM associadas com o gerenciamento de rede, configuração de relógio e gerenciamento de usuário.	ilomconfig
Exiba ou crie volumes RAID em unidades de armazenamento anexadas a controladores RAID, incluindo matrizes de armazenamento.	raidconfig
Monitore a integridade do sistema.	hwmgmt

Sobre Este Guia de Segurança

Este documento oferece diretrizes gerais de segurança para o Oracle Hardware Management Pack. Este guia tem o objetivo de ajudá-lo a garantir a segurança ao usar o software com outros produtos de hardware da Oracle, como switches de rede e placas de interface de rede.

Os seguintes tópicos são abordados:

- [“Visão Geral” na página 5](#)
- [“Pré-instalação do Oracle Hardware Management” na página 9](#)
- [“Instalação do Oracle Hardware Management Pack” na página 11](#)
- [“Pós-instalação do Oracle Hardware Management Pack” na página 13](#)

Princípios de Segurança Básicos

Existem quatro princípios básicos de segurança: acesso, autenticação, autorização e contabilidade.

- **Acesso**
Use os controles físicos e de software para proteger seu hardware ou seus dados contra invasão.
 - Para hardware, os limites de acesso geralmente significam limites de acesso físico.
 - Para software, os limites de acesso geralmente significam meios físicos e virtuais.
 - Não é possível alterar o firmware, exceto por meio do processo de atualização da Oracle.
- **Autenticação**

Configure todos os recursos de autenticação, como um sistema de senhas nos sistemas operacionais da plataforma, para verificar se os usuários são realmente quem eles dizem ser.

A autenticação oferece diversos graus de segurança por meio de medidas como crachás e senhas. Por exemplo, verifique se sua equipe usa adequadamente os crachás para entrar em uma sala de computadores.

- **Autorização**

A autorização permite que funcionários da empresa trabalhem somente com hardware e software nos quais foram treinados e estejam qualificados para usar.

Por exemplo, configure um sistema de permissões de leitura/gravação/execução para controlar o acesso de usuários a comandos, espaço em disco, dispositivos e aplicativos.

- **Contabilidade**

A equipe de TI do cliente pode usar os recursos de software e hardware da Oracle para monitorar a atividade de login e manter os inventários de hardware.

- Use logs do sistema para monitorar logins de usuários. Especificamente, rastreie as contas do Administrador do Sistema e de Serviço por meio de logs do sistema, pois essas contas têm acesso a comandos avançados.
- Remova periodicamente arquivos de log quando excederem um tamanho considerável, de acordo com a política da empresa relacionada ao consumidor. Em geral, os logs são mantidos por um período longo, portanto é essencial guardá-los.
- Use números de série de componentes para rastrear os ativos do sistema para fins de estoque. Os números de peça da Oracle são gravados eletronicamente em cartões, módulos e placasmães.

Resumo de Segurança do Oracle Hardware Management Pack

Lembre-se destes importantes itens de segurança ao configurar todas as ferramentas de gerenciamento do sistema:

- *É possível usar produtos de gerenciamento do sistema para obter um ambiente root inicializável*

Com um ambiente root inicializável, é possível obter o acesso ao Oracle ILOM, Oracle System Assistant e discos rígidos.

- *Os produtos de gerenciamento do sistema incluem ferramentas avançadas que exigem privilégios de administrador ou root para serem executadas.*

Com este nível de acesso, é possível alterar configurações de hardware e apagar dados.

- **Biblioteca de Documentação do Oracle Hardware Management Pack**
(<http://www.oracle.com/pls/topic/lookup?ctx=ohmp>)

Pré-instalação do Oracle Hardware Management

Durante a instalação e configuração inicial, use os recursos de segurança de software da Oracle para controlar o hardware e rastrear ativos do sistema.

Os seguintes tópicos são abordados:

- “Componentes do Oracle Hardware Management Pack” na página 9
- “Configurações de Segurança do Plug-in SNMP Baseado no Agent” na página 10
- “Escolhendo uma Versão do Protocolo SNMP do SNMP Agent” na página 10

Componentes do Oracle Hardware Management Pack

O Oracle Hardware Management Pack contém um conjunto de ferramentas de linha de comando para gerenciamento de hardware destinado à configuração de RAID, BIOS e Oracle ILOM e para atualização do firmware. Ele contém também um plug-in SNMP para monitoramento. O Oracle Hardware Management Pack contém ainda um daemon ou serviço que se comunica com o Oracle ILOM por um canal interno para compartilhar informações de inventário e integridade do servidor.

Essas ferramentas e plug-ins são instalados no seu sistema operacional host para que você execute as tarefas de gerenciamento do sistema diretamente do host. Embora o Oracle Hardware Management Pack ofereça recursos úteis para o gerenciamento em um servidor Oracle, ele é totalmente opcional.

Consulte o Guia do Usuário do Sun Server Hardware Management Pack para obter mais informações sobre os recursos do Oracle Hardware Management Pack e ajudar a determinar se ele será usado e instalado.

- Biblioteca de Documentação do Oracle Hardware Management Pack (<http://www.oracle.com/pls/topic/lookup?ctx=ohmp>)
- Para obter informações gerais sobre o Oracle ILOM, consulte: <http://www.oracle.com/pls/topic/lookup?ctx=ilom31>

Configurações de Segurança do Plug-in SNMP Baseado no Agent

O Oracle Hardware Management Pack contém um módulo de Plug-in SNMP que estende o agente SNMP nativo no sistema operacional host para oferecer outros recursos do Oracle MIB. É particularmente importante observar que o Oracle Hardware Management Pack não contém, ele próprio, um agente SNMP. Para Linux, um módulo é adicionado ao agente net-snmp, que deve ser instalado previamente. Para o Solaris, um módulo é adicionado ao Solaris Management Agent. Para o Windows, o plug-in estende o serviço SNMP nativo.

Da mesma forma, todas as configurações de segurança relacionadas ao SNMP para o Plug-in SNMP do Oracle Hardware Management Pack são determinadas pelas configurações do agente ou serviço de SNMP nativo, e não pelo plug-in. Consulte a documentação do net-snmp ou serviço SNMP do Windows para obter instruções sobre como configurar o SNMP seguramente.

- [Biblioteca de Documentação do Oracle Hardware Management Pack](http://www.oracle.com/pls/topic/lookup?ctx=ohmp)
(<http://www.oracle.com/pls/topic/lookup?ctx=ohmp>)

Escolhendo uma Versão do Protocolo SNMP do SNMP Agent

O SNMP é um protocolo padrão usado para monitorar ou gerenciar um sistema. O SNMPv1/v2c não fornece criptografia e usa strings de comunicação como uma forma de autenticação. As strings de comunidade são enviadas em texto desprotegido pela rede e geralmente são compartilhadas por um grupo de indivíduos, em vez de serem privadas para um usuário individual. O SNMPv3, por outro lado, usa criptografia para oferecer um canal seguro e tem nomes de usuário e senhas específicos. As senhas de usuário do SNMPv3 estão localizadas de modo que elas possam ser armazenadas de modo seguro nas estações de gerenciamento.

A Oracle recomenda o uso do SNMPv3, se ele for suportado pelo agente do SNMP nativo. Consulte a documentação do net-snmp ou serviço SNMP do Windows para obter instruções sobre como configurar o SNMPv3.

- [Biblioteca de Documentação do Oracle Hardware Management Pack](http://www.oracle.com/pls/topic/lookup?ctx=ohmp)
(<http://www.oracle.com/pls/topic/lookup?ctx=ohmp>)

Instalação do Oracle Hardware Management Pack

Os seguintes tópicos são abordados:

- “Executando o Instalador do Oracle Hardware Management Pack” na página 11
- “Optando pela Ativação da Interconexão de LAN” na página 11
- “Optando por Salvar Credenciais em um Arquivo” na página 12

Executando o Instalador do Oracle Hardware Management Pack

O Oracle Hardware Management Pack consiste em um conjunto de pacotes de instalação nativos que podem ser instalados com o uso de ferramentas de instalação nativas de um sistema operacional, como RPM. Além disso, é possível usar um instalador com base em assistente para auxiliar a instalação. Além de adicionar os pacotes nativos, o instalador também ajuda a configurar o Oracle Hardware Management Pack para uso.

Como o instalador do Oracle Hardware Management Pack deve instalar pacotes nativos, ele deve ser executado com root ou administrador.

- [Biblioteca de Documentação do Oracle Hardware Management Pack](http://www.oracle.com/pls/topic/lookup?ctx=ohmp)
(<http://www.oracle.com/pls/topic/lookup?ctx=ohmp>)

Optando pela Ativação da Interconexão de LAN

Como uma alternativa mais rápida para a interface de KCS, os clientes no sistema operacional do host poderão estabelecer comunicação com o Oracle ILOM sobre uma interconexão interna de alta velocidade. Essa interconexão é implementada por uma conexão USB pela Ethernet interna, executando uma pilha IP. O Oracle ILOM e o host recebem endereços IP não roteáveis para comunicação por esse canal.

A conexão com o Oracle ILOM por meio de uma interconexão de LAN exige autenticação, quase como se a conexão estivesse em direção à rede para a porta de gerenciamento do Oracle ILOM. Todos os serviços ou protocolos expostos na rede de gerenciamento serão disponibilizadas pela interconexão de LAN para o host. Por exemplo, é possível usar um navegador Web no host para acessar a interface Web do Oracle ILOM ou usar um cliente shell

para estabelecer conexão com a interface a linha de comando do Oracle ILOM. Em todos os casos, um nome e senha de usuário válidos devem ser fornecidos para usar a interconexão de LAN.

O instalador do Oracle Hardware Management Pack apresenta a opção de permitir a interconexão com a LAN. A Oracle só recomenda a ativação da interconexão com a LAN se a instrução de rede suportar RFC 3927 e a capacidade de ter endereços IPv4 locais com link. Além disso, é necessário ter cuidado para garantir que o sistema operacional não atue como bridge ou roteador. Dessa forma, o tráfego de gerenciamento entre o host e o Oracle ILOM permanece privado.

- [Biblioteca de Documentação do Oracle Hardware Management Pack](http://www.oracle.com/pls/topic/lookup?ctx=ohmp)
(<http://www.oracle.com/pls/topic/lookup?ctx=ohmp>)

Optando por Salvar Credenciais em um Arquivo

As ferramentas `ilomconfig` e `fwupdate`, que fazem parte do Oracle Hardware Management Pack, podem se conectar ao Oracle ILOM por meio da interconexão de LAN de alta velocidade. O uso da interconexão de LAN em vez da interface KCS mais lenta pode aumentar significativamente o desempenho das principais operações, como atualizações de firmware do Oracle ILOM.

Como a interconexão de LAN exige autenticação, é necessário autenticar o Oracle ILOM em cada chamada dessas ferramentas. Como conveniência, é possível armazenar as credenciais em um arquivo em cache, de forma que as ferramentas as usem automaticamente. Esse procedimento impede a necessidade de incorporar senhas em texto sem formatação a scripts que usem as ferramentas do Oracle Hardware Management Pack.

É possível usar a ferramenta `ilomconfig` para armazenar o nome de usuário e a senha em um arquivo criptografado que seja somente leitura na raiz. Se esse arquivo for detectado quando `ilomconfig` ou `fwupdate` for usado para acessar o Oracle ILOM, as credenciais em cache serão usadas. Como alternativa, é possível especificar o nome de usuário e a senha na linha de comando para cada chamada da ferramenta.

O algoritmo de criptografia usado é exclusivo para cada sistema. Se a chave for descoberta, entretanto, o arquivo poderá ser descriptografado e expor o nome de usuário e a senha. A Oracle recomenda a criação de uma senha exclusiva em cada Oracle ILOM para essa finalidade, de forma que uma senha comprometida não seja usada contra outros sistemas Oracle ILOM.

Consulte o Guia do Usuário do Sun Server Hardware Management Pack para obter instruções sobre como salvar credenciais em um arquivo.

- [Biblioteca de Documentação do Oracle Hardware Management Pack](http://www.oracle.com/pls/topic/lookup?ctx=ohmp)
(<http://www.oracle.com/pls/topic/lookup?ctx=ohmp>)

Pós-instalação do Oracle Hardware Management Pack

Os seguintes tópicos são abordados:

- [“Desinstalação do Oracle Hardware Management Pack” na página 13](#)

Desinstalação do Oracle Hardware Management Pack

É possível desinstalar o Oracle Hardware Management Pack com ferramentas nativas do pacote, como RPM, ou com o desinstalador baseado em assistente fornecido com o Oracle Hardware Management Pack. Quando o método de pacote nativo é usado para remover pacotes, o arquivo criptografado que armazena o nome de usuário e a senha em cache para uso na LAN interconectada não é deletado. Ele deverá ser deletado manualmente.

O desinstalador baseado em assistente remove o arquivo de credenciais. Portanto, a Oracle recomenda o uso do instalador baseado em assistente para desinstalar o Oracle Hardware Management Pack.

- [Biblioteca de Documentação do Oracle Hardware Management Pack](http://www.oracle.com/pls/topic/lookup?ctx=ohmp)
(<http://www.oracle.com/pls/topic/lookup?ctx=ohmp>)

