Guia de Segurança do Oracle® Hardware Management Pack

Número do Item: E39916-02
Outubro de 2015

Número do Item: E39916-02

Acessibilidade da Documentação

Para obter informações sobre o compromisso da Oracle com a acessibilidade, visite o Web site do Programa de Acessibilidade da Oracle em `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc`.

Acceso ao Oracle Support

Os clientes da Oracle que adquiriram serviços de suporte têm 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 `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs` caso tenha deficiência de audição.

Conteúdo

Visão Geral 7
Visão Geral do Produto 7
Sobre Este Guia de Segurança 8
Princípios de Segurança Básicos 8
Resumo de Segurança do Oracle Hardware Management Pack 9

Pré-instalação do Oracle Hardware Management Pack 11
Componentes do Oracle Hardware Management Pack 11
Configurações de Segurança do Plug-in SNMP Baseado no Agent 12
Escolhendo uma Versão do Protocolo SNMP do SNMP Agent 12

Instalação do Oracle Hardware Management Pack 13
Executando o Instalador do Oracle Hardware Management Pack 13
Optando pela Ativação da Interconexão Host-to-ILOM 13
Optando por Salvar Credenciais em um Arquivo 14

Pós-instalação do Oracle Hardware Management Pack 17
Desinstalação do Oracle Hardware Management Pack 17

Visão Geral

Esta seção contém uma visão geral do produto Oracle Hardware Management Pack, com informações sobre o guia de segurança e explicações sobre os princípios gerais da segurança de aplicativos.

Os seguintes tópicos são abordados:

- "Visão Geral do Produto" [7]
- "Sobre Este Guia de Segurança" [8]
- "Princípios de Segurança Básicos" [8]
- "Resumo de Segurança do Oracle Hardware Management Pack" [9]

Visão Geral do Produto

O Oracle Hardware Management Pack está disponível para muitos servidores x86 e alguns servidores 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. Para obter informações sobre o Hardware Management Agent, consulte o *Guia do Usuário do Oracle Server Management Agents.*.

É possível usar as Ferramentas CLI do Oracle Server para configurar os servidores Oracle. As CLI Tools são compatíveis com os sistemas operacionais Oracle Solaris, Oracle Linux, Oracle VM, outras variações do Linux e Microsoft Windows. Para obter uma lista de ferramentas, consulte o *Guia do Usuário do Oracle Server CLI Tools.*

Consulte a documentação do Oracle Hardware Management Pack para Oracle Solaris para obter mais informações sobre recursos e uso.

- Biblioteca de Documentação do Oracle Hardware Management Pack em: `http://www.oracle.com/goto/ohmp/docs`
- Para obter informações gerais sobre o Oracle ILOM, consulte: `http://www.oracle.com/goto/ilom/docs`

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:

- Pré-instalação do Oracle Hardware Management Pack [11]
- Instalação do Oracle Hardware Management Pack [13]
- Pós-instalação do Oracle Hardware Management Pack [17]

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, limites de acesso em geral significam meios físicos e virtuais.
  - Não é possível alterar o firmware, exceto pelo processo de atualização da Oracle.
- Autenticação

  Configure 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 os colaboradores 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 peças Oracle são gravados eletronicamente em todos os cartões, módulos e placas-mãe.

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 raiz inicializável, é possível ter acesso ao Oracle ILOM, ao Oracle System Assistant e ao disco rígido.
- *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.

Pré-instalação do Oracle Hardware Management Pack

Durante a instalação e configuração iniciais, 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" [11]
- "Configurações de Segurança do Plug-in SNMP Baseado no Agent" [12]
- "Escolhendo uma Versão do Protocolo SNMP do SNMP Agent" [12]

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.

Para obter mais informações sobre os recursos do Oracle Hardware Management Pack, consulte estas bibliotecas de documentação:

- Oracle Hardware Management Pack Documentation Library (`http://www.oracle.com/goto/ohmp/docs`)
- Biblioteca de Documentação do Oracle ILOM (`http://www.oracle.com/goto/ilom/docs`)

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. Consulte também as instruções no *Guia do Usuário do Oracle Server Management Agents* no link abaixo:

- Oracle Hardware Management Pack Documentation Library (`http://www.oracle.com/goto/ohmp/docs`)

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 SNMP nativo. Consulte a documentação sobre net-snmp (Oracle Solaris e Linux) ou o serviço SNMP do Windows para obter instruções sobre como configurar o SNMPv3.

Instalação do Oracle Hardware Management Pack

Os seguintes tópicos são abordados:

- “Executando o Instalador do Oracle Hardware Management Pack” [13]
- “Optando pela Ativação da Interconexão Host-to-ILOM” [13]
- “Optando por Salvar Credenciais em um Arquivo” [14]

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. Para obter mais informações, consulte o *Guia de Instalação do Oracle Hardware Management Pack* no link abaixo:

- Oracle Hardware Management Pack Documentation Library (`http://www.oracle.com/goto/ohmp/docs`)

Optando pela Ativação da Interconexão Host-to-ILOM

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. O Oracle Hardware Management Pack refere-se a este recurso como Interconexão Host-to-ILOM. A interface do Oracle ILOM refere-se a este recurso como Interconexão de Host Local. 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 da interconexão Host-to-ILOM (Interconexão de Host Local) requer autenticação, como se a conexão fosse realizada através da rede com a porta de gerenciamento do Oracle ILOM. Todos os serviços ou protocolos expostos na rede de gerenciamento ficam disponíveis através da interconexão Host-to-ILOM com o host. Por exemplo, é possível usar um navegador Web no host para acessar a interface Web do Oracle ILOM ou usar um cliente SSH (Secure Shell) para estabelecer conexão com a CLI (interface de linha de comando) do Oracle ILOM. Em todos os casos, é preciso informar um nome de usuário e uma senha válidos para usar a interconexão Host-to-ILOM.

O instalador do Oracle Hardware Management Pack tem a opção de ativar a interconexão Host-to-ILOM. A Oracle recomenda ativar a interconexão Host-to-ILOM somente se a instrução de rede for compatível com RFC 3927 e aceitar a presença de 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. Para obter mais informações, consulte o *Guia de Instalação do Oracle Hardware Management Pack* no link abaixo:

- Oracle Hardware Management Pack Documentation Library (`http://www.oracle.com/goto/ohmp/docs`)

Optando por Salvar Credenciais em um Arquivo

O recurso foi desativado depois do Oracle Hardware Management Pack 2.3.3.

As ferramentas `ilomconfig` e `fwupdate`, que fazem parte do Oracle Hardware Management Pack para Oracle Solaris, podem se conectar ao Oracle ILOM por meio da interconexão Host-to-ILOM de alta velocidade. Como a interconexão Host-to-ILOM requer autenticação, é necessário autenticar no Oracle ILOM toda vez que essas ferramentas forem chamadas. Como conveniência, é possível armazenar as credenciais em um arquivo em cache, de forma que as ferramentas as usem automaticamente. Esse procedimento evita 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 a 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 criar uma senha exclusiva em cada Oracle ILOM para impedir o uso de senhas comprometidas em outros sistemas Oracle ILOM.

Para obter instruções sobre como salvar as credenciais em um arquivo, consulte o *Guia do Usuário do Oracle CLI Tools para Oracle Solaris* no link abaixo.

- Oracle Hardware Management Pack Documentation Library (`http://www.oracle.com/goto/ohmp/docs`)

Pós-instalação do Oracle Hardware Management Pack

Os seguintes tópicos são abordados:

- "Desinstalação do Oracle Hardware Management Pack" [17]

Desinstalação do Oracle Hardware Management Pack

É possível desinstalar os pacotes do 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 do pacote nativo é usado para remover pacotes, se você tiver salvado um arquivo em cache com as credenciais do host usando o Oracle Hardware Management Pack para facilitar o acesso ao Oracle ILOM usando a interconexão Host-to-ILOM, o arquivo não será excluído. Nesse caso, antes de desinstalar os pacotes do Oracle Hardware Management Pack, execute o comando `ilomconfig delete credential` para excluir o arquivo.

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. Para obter mais informações, consulte o *Guia de Instalação do Oracle Hardware Management Pack* no link abaixo:

- Oracle Hardware Management Pack Documentation Library (`http://www.oracle.com/goto/ohmp/docs`)