Servidores SPARC M5-32 e SPARC M6-32

Guia de Segurança

Parte No: E49765-02
Julho de 2014

Índice

• • • Capítulo 1

Noções Básicas de Segurança de Hardware

O isolamento físico e o controle do acesso compõem a base da arquitetura de segurança. Garantir que o servidor físico esteja instalado em um ambiente seguro o protege contra o acesso não autorizado. Da mesma forma, a gravação de todos os números de série ajuda a evitar roubo, revenda ou risco à cadeia de fornecimento (ou seja, injeção de componentes falsificados ou comprometidos na cadeia de fornecimento da sua organização).

Este capítulo fornece diretrizes gerais de segurança de hardware para os servidores SPARC M5-32 e M6-32.

As seguintes seções estão incluídas neste capítulo:

Restrições de Acesso

- Instale servidores e equipamentos relacionados em um local trancado com acesso restrito.
- Se o equipamento for instalado em um rack com uma porta com trava, sempre tranque a porta do rack até que seja feita manutenção dos componentes no rack. O travamento das portas também restringe o acesso aos dispositivos hot-plug ou hot-swap.
- Guarde FRUs (unidades substituíveis no campo) e CRUs (unidade substituíveis pelo cliente) sobressalentes em um gabinete trancado. Restrinja o acesso ao gabinete ao pessoal autorizado.
- Periodicamente, verifique o status e a integridade dos bloqueios no rack e no gabinete de peças para protegê-los contra, ou detectar, falsificação ou portas destravadas.
- Guarde as chaves do gabinete em um local seguro com acesso limitado.
- Restrinja o acesso aos consoles USB. Dispositivos como controladores de sistema, PDUs (unidades de distribuição de energia) e comutadores de rede podem ter conexões USB. O acesso físico é um método mais seguro de acessar um componente já que ele não é suscetível a ataques baseados na rede.
- Conecte a console a um KVM externo para permitir o acesso remoto à console. Em geral, os dispositivos KVM suportam autenticação de dois fatores, controle de acesso centralizado e auditoria. Para obter mais informações sobre as diretrizes de segurança e as melhores práticas para KVMs, consulte a documentação que acompanha o dispositivo KVM.

Números de Série

- Mantenha um registro dos números de série de todo o equipamento de hardware.
- Faça uma marca de segurança em todos os itens relevantes de hardware do computador, como peças de reposição. Use canetas especiais ultravioletas ou etiquetas em alto-relevo.
- Mantenha as chaves de ativação e as licenças do hardware em um local seguro e de fácil acesso ao gerente do sistema em caso de emergências. Os documentos impressos podem ser sua única prova de propriedade.

Leitores RFID sem fio podem simplificar ainda mais o controle de ativos. Para obter mais informações, leia *How to Track Your Oracle Sun System Assets by Using RFID* em:

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

Discos rígidos

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, devido à maneira como gerenciam o acesso aos dados.

• • • Capítulo 2

Noções Básicas de Segurança de Software

A maior parte da segurança de hardware é implementada por medidas de software. Este capítulo fornece diretrizes gerais de segurança de software para servidores SPARC M5-32 e SPARC M6-32.

As seguintes seções estão incluídas neste capítulo:

▼ Impedir o Acesso Não Autorizado (SO Oracle Solaris)

- Use os comandos do SO Oracle Solaris para restringir o acesso ao software do Oracle Solaris, fortalecer o SO, usar recursos de segurança e proteger aplicativos.
  Obtenha o documento de diretrizes de segurança do Oracle Solaris referente à versão do SO que você está usando:
  http://www.oracle.com/goto/Solaris11/docs
  http://www.oracle.com/goto/Solaris10/docs

▼ Impedir o Acesso Não Autorizado (Oracle ILOM)

1. Use os comandos do Oracle ILOM para restringir o acesso do usuário ao software do Oracle ILOM, alterar a senha definida de fábrica, limitar o uso da conta de superusuário root e proteger a rede privada para o processador de serviço.
   Obtenha o *Oracle ILOM Security Guide* em:
   http://www.oracle.com/goto/ILOM/docs
2. Use os comandos específicos da plataforma Oracle ILOM para proteger domínios individuais, criando contas de usuário com funções que se aplicam a um domínio físico específico.
   Quando você atribui funções de usuário a um domínio físico, os recursos desse domínio se espelham nas funções de usuário atribuídas à plataforma, mas estão restritos aos comandos executados no componente especificado.

Observação

Somente as funções de usuário do tipo administrador (**a**), console (**c**) e redefinir (**r**) podem ser atribuídas a domínios físicos individuais.

Obtenha o *SPARC M5-32 and SPARC M6-32 Servers Administration Guide* em: http://www.oracle.com/goto/M6-32/docs

▼ Impedir o Acesso Não Autorizado (Oracle VM Server for SPARC)

- Use os comandos do Oracle VM for SPARC para restringir o acesso ao software do Oracle VM for SPARC.
  Obtenha o *Oracle VM for SPARC Security Guide* em: http://www.oracle.com/goto/VM-SPARC/docs

Restringindo o Acesso (OpenBoot)

Esses tópicos explicam como restringir o acesso ao prompt do OpenBoot.

- Implementar a Proteção de Senha (OpenBoot) [8]
- Verificar Falhas de Login (OpenBoot) [8]
- Fornecer um Power-On Banner (OpenBoot) [9]

Informações Relacionadas

- Para obter informações sobre como definir as variáveis de segurança do OpenBoot, consulte o*OpenBoot 4.x Command Reference Manual* em: http://download.oracle.com/docs/cd/E19455-01/816-1177-10/cfg-var.html#pgfId-17069

▼ Implementar a Proteção de Senha (OpenBoot)

- Defina o parâmetros de modo de segurança para **full** ou **command**.
  Quando definida como **full**, uma senha é solicitada para executar qualquer ação, incluindo operações normais, como inicialização. Quando definida como **command**, uma senha não é solicitada para os comandos **boot** ou **go**, mas todos os outros comandos exigem senha. Por razões de continuidade comercial, defina o parâmetro de modo de segurança como command, como no exemplo a seguir.

```
ok password
ok setenv security-mode command
ok password
```

▼ Verificar Falhas de Login (OpenBoot)

1. Determine se alguém tentou e não conseguiu acessar o ambiente do OpenBoot, usando o parâmetro **security-#badlogins**, como no exemplo a seguir.

```
ok printenv security-#badlogins
```

Se esse comando retornar um valor maior que zero, uma falha de tentativa de acessar o ambiente do OpenBoot foi registrada.

2. Redefina o parâmetro **security-#badlogins** digitando o comando a seguir.

```
ok setenv security-#badlogins 0
```

▼ Fornecer um Power-On Banner (OpenBoot)

- Use os comandos a seguir para ativar uma mensagem de advertência personalizada.

```
ok setenv oem-banner banner-message
ok setenv oem-banner? true
```

Oracle System Firmware

O Oracle System Firmware usa um processo de atualização do firmware controlado para impedir modificações não autorizadas no firmware. Somente o superusuário ou um usuário autenticado com a devida autorização pode usar o processo de atualização.

Para obter mais informações sobre como ter acesso às atualizações ou aos patches mais recentes, consulte as notas do produto do seu servidor.

Inicialização WAN Segura

A inicialização WAN suporta diversos níveis de segurança. É possível utilizar uma combinação de recursos de segurança que são suportados na inicialização WAN para atender as necessidades da rede. Uma configuração mais segura requer administração adicional, mas também protege os dados do sistema de forma mais abrangente.

- Para o SO Oracle Solaris 10, consulte “Secure WAN Boot Installation Configuration” em *Oracle Solaris Installation Guide: Network-Based Installations*.

  http://www.oracle.com/goto/Solaris10/docs
- Para o SO Oracle Solaris 11, consulte *Securing the Network in Oracle Solaris 11.1*.

  http://www.oracle.com/goto/Solaris11/docs