Servidores da Série SPARC T7

Guia de Segurança

Número do Item: E63379-01
Outubro de 2015

Conteúdo

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, registrar todos os números de série ajuda a impedir roubo, revenda ou risco à cadeia de fornecimento (ou seja, injeção de componentes falsificados ou comprometidos na cadeia de fornecimento da sua organização).

Estas seções fornecem diretrizes gerais de segurança de hardware para os servidores SPARC T7-1, T7-2 e T7-4.

Restrições de Acesso

- Instale servidores e equipamentos relacionados em um local trancado e 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 (field-replaceable units, unidades substituíveis no campo) e CRUs (customer-replaceable units, unidades substituíveis pelo cliente) em um armário trancado. Restrinja o acesso ao armário trancado a pessoas autorizadas.
- Periodicamente, verifique o status e a integridade dos bloqueios no rack e no gabinete de peças sobressalentes para protegê-los ou para detectar falsificação ou portas deixadas acidentalmente 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 (power distribution units, unidades de distribuição de energia) e switches 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 hardware.
- Faça uma marca de segurança em todos os itens relevantes do 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 emergência. Os documentos impressos podem ser sua única prova de propriedade.

Os leitores de RFID (radio frequency identification, identificação por radiofrequência) sem fio podem 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

Unidades de Disco Rígido

Em geral, unidades de disco rígido são usadas para armazenar informações confidenciais. Para proteger essas informações contra a divulgação não autorizada, esvazie as unidades de disco rígido antes de reutilizá-las, descontinuá-las ou descartá-las.

- Use ferramentas de limpeza de disco como o comando format (1M) do Oracle Solaris para apagar completamente todos os dados do disco rígido.
- As organizações devem consultar suas políticas de proteção de dados para determinar o método mais apropriado de limpeza das unidades de disco rígido.
- Se necessário, utilize o Serviço de Dados do Cliente e de Retenção de Dispositivos da Oracle

  http://www.oracle.com/us/support/library/data-retention-ds-405152.pdf

Noções Básicas de Segurança de Software

A maior parte da segurança do hardware é implementada por meio de medidas de software. Estas seções fornecem diretrizes gerais de segurança de software para os servidores SPARC T7-1, T7-2 e SPARC T7-4.

▼ Impedir o Acesso Não Autorizado (Sistema Operacional Oracle Solaris)

- **Use os comandos do Sistema Operacional Oracle Solaris para restringir o acesso ao software do Oracle Solaris, proteger o Sistema Operacional, usar funcionalidades de segurança e proteger aplicativos.**

  Obtenha o documento *Oracle Solaris Security Guidelines* referente à versão que você está usando em:

  - `http://www.oracle.com/goto/solaris11/docs`
  - `http://www.oracle.com/goto/solaris10/docs`

▼ Impedir o Acesso Não Autorizado (Oracle ILOM)

- **Use os comandos do Oracle ILOM para restringir o acesso ao software Oracle ILOM, alterar a senha definida na fábrica, limitar o uso da conta de superusuário root e proteger a rede privada do processador de serviços.**

  Obtenha o *Oracle ILOM Security Guide* em:

  `http://www.oracle.com/goto/ilom/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 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)

Estes tópicos descrevem como restringir o acesso ao prompt do OpenBoot.

- Implementar a Proteção por Senha [8]
- Ativar o Modo de Segurança [9]
- Desativar o Modo de Segurança [9]
- Verificar Falhas de Log-in [10]
- Fornecer um Power-On Banner [10]

Para obter informações sobre como definir as variáveis de segurança do OpenBoot, consulte a documentação do OpenBoot em:

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

▼ Implementar a Proteção por Senha

- **Caso você não ainda tenha definido uma senha, execute esta etapa.**

```
{0} ok password
New password (8 characters max):
Retype new password: password
```

A senha pode ter de um a oito caracteres. Se você informar mais de oito caracteres, apenas os oito primeiros caracteres serão usados. Todos os caracteres imprimíveis são aceitos. Caracteres de controle não são aceitos.

Observação - Definir a senha como zero caractere desliga a segurança e trata o parâmetro `security-mode` como se tivesse sido definido como `none`. No entanto, não altera a definição.

▼ Ativar o Modo de Segurança

1. **Defina o parâmetro de `security-mode` como `full` ou `command`.**

   Quando definida como `full`, uma senha é solicitada para executar qualquer ação, incluindo operações normais, como `boot`. 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 `security-mode` como `command`, como no exemplo a seguir.

   ```
   {0} ok setenv security-mode command
   {0} ok
   ```

2. **Obtenha o prompt de modo de segurança.**

   Após você definir o modo de segurança conforme descrito acima, há duas maneiras de obter o prompt de modo de segurança.

   - **Use as palavras `logout` e `login`.**

     ```
     {0} ok logout
     Type boot , go (continue), or login (command mode)
     >
     > login
     Firmware Password: password
     Type help for more information
     {0} ok
     ```

     Para sair do modo de segurança, use os nomes `logout` e `login`, conforme mostrado no exemplo.

   - **Use a palavra `reset-all`.**

     ```
     {0} ok reset-all
     ```

     Esta palavra redefine o sistema. Quando o sistema voltar, o OpenBoot mostrará o prompt de modo de segurança. Para efetuar log-in novamente no prompt de log-in (ou fazer log-out do modo de segurança), use os nomes `logout` e `login`, e insira a senha, conforme descrito acima.

▼ Desativar o Modo de Segurança

1. **Defina o parâmetro de `security-mode` como `none`.**

   ```
   {0} ok setenv security-mode none
   ```

2. **Defina a senha com um tamanho zero digitando Return após os dois prompts de senha.**

▼ Verificar Falhas de Log-in

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

```
{0} ok printenv security-#badlogins
```

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

2. **Redefina o parâmetro digitando este comando.**

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

▼ Fornecer um Power-On Banner

Embora não seja um controle detetive ou preventivo direto, um banner pode ser usado por estes motivos:

- Convir propriedade.
- Advertir os usuários a respeito do uso aceitável do servidor.
- Indicar que o acesso ou modificações no parâmetro OpenBoot estão restritos ao pessoal autorizado.

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

```
{0} ok setenv oem-banner banner-message
{0} ok setenv oem-banner? true
```

A mensagem de banner pode ter até 68 caracteres. Todos os caracteres imprimíveis são aceitos.

Oracle System Firmware

O Oracle System Firmware usa um processo de atualização de firmware controlado para impedir modificações não autorizadas. Somente o superusuário ou um usuário autenticado com a devida autorização pode usar o processo de atualização.

Para obter informações sobre como obter as atualizações ou os patches mais recentes, consulte as notas do produto do seu servidor.

Inicialização Segura de WAN

A inicialização de WAN suporta diversos níveis de segurança. É possível utilizar uma combinação de funcionalidades de segurança suportadas na inicialização da WAN para atender as necessidades da rede. Uma configuração mais segura requer mais administração, mas também protege os dados do sistema mais amplamente.

- Para o Sistema Operacional Oracle Solaris 10, consulte as informações sobre como proteger a configuração da instalação de inicialização no manual *Oracle Solaris Installation Guide: Network-Based Installations*.
- Para o Sistema Operacional Oracle Solaris 11, consulte *Securing the Network in Oracle Solaris 11.1*.