Servidores SPARC e Netra SPARC Série T5

Security Guide

Parte No: E40478-01
Abril de 2013

Índice

• • • Capítulo 1

Segurança de Servidores SPARC e Netra SPARC Série T5

Este documento oferece diretrizes gerais de segurança dos servidores SPARC T5-1B, T5-2, T5-4, T5-8 e Netra SPARC T5-1B. Este guia tem o objetivo de ajudá-lo com a segurança durante o uso desses servidores com outros produtos de hardware Oracle, como switches de rede e placas de interface de rede.

As seguintes seções estão neste capítulo:

Noções Básicas dos Princípios de Segurança

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

- **Acesso**

  Os controles físicos e de software protegem o hardware ou os dados contra invasão.
  - No caso de hardware, os limites de acesso geralmente significam limites de acesso *físico*.
  - No caso de software, o acesso é limitado através de meios físicos e virtuais.
  - O firmware só pode ser alterado por meio do processo de atualização da Oracle.
- **Autenticação**

  Todos os sistemas operacionais da plataforma fornecem recursos de autenticação que podem ser configurados para garantir que os usuários sejam quem eles dizem ser.

  A autenticação oferece diversos graus de segurança por meio de medidas como crachás e senhas.
- **Autorização**

  A autorização permite que funcionários da empresa trabalhem somente com hardware e software nos quais foram treinados e estejam qualificados para usar. Configure um sistema de permissões de Leitura, Gravação e Execução para controlar o acesso de usuários a comandos, espaço em disco, dispositivos e aplicativos.

- **Contabilidade**

  Use os recursos de contabilidade de software e hardware da Oracle para monitorar a atividade de log-in e manter os inventários de hardware.

  - Os log-ins de usuários podem ser monitorados através de logs do sistema. As contas de Administrador do Sistema e de Serviço têm, em particular, acesso a comandos avançados e devem ser cuidadosamente monitoradas através de logs do sistema. Normalmente, os logs são mantidos por um longo período, por isso é essencial remover periodicamente os arquivos de log quando ultrapassar um tamanho razoável, de acordo com a política da empresa do cliente.
  - Geralmente, os ativos de TI do Cliente são controlados através de números de série. Os números de peça da Oracle são gravados eletronicamente em todos os cartões, módulos e placas-mãe, e podem ser usados para fins de inventário.

Planejando um Ambiente Seguro

Use as notas a seguir antes e durante a instalação e a configuração de um servidor e equipamento relacionado.

Segurança do Hardware

O hardware físico pode ser protegido de forma bastante simples, limitando o acesso ao hardware e gravando números de série.

- **Restringir o 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.
  - Restrinja o acesso a consoles de USB, que podem fornecer um acesso mais eficaz do que as conexões SSH. Dispositivos como controladores de sistema, PDUs (unidades de distribuição de energia) e switches de rede podem ter conexões USB.
  - Restrinja o acesso a dispositivos hot-plug ou hot-swap, pois eles são removidos facilmente.
  - Guarde unidades substituíveis no campo (FRUs) e unidade substituíveis pelo cliente (CRUs) sobressalentes em um armário trancado. Restrinja o acesso ao armário trancado a pessoas autorizadas.
- **Registrar os números de série**
  - Mantenha um registro dos números de série de todo o 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.

Segurança do Software

A maior parte da segurança do hardware é implementada por meio de medidas de software.

- Altere todas as senhas padrão quando um novo sistema for instalado. A maioria dos tipos de equipamento utiliza senhas padrão, como **changeme**, que são amplamente conhecidas e que permitiriam acesso não autorizado ao equipamento. Além disso, dispositivos como switches de rede podem ter várias contas de usuário por padrão. Certifique-se de alterar todas as senhas da conta.

- Limite o uso da conta de superusuário `root`. Perfis de usuário do Oracle ILOM (Oracle Integrated Lights Out Manager), como `operador` e `administrador` devem ser usados sempre que possível.
- Use uma rede dedicada para processadores de serviço para separá-los da rede geral.
- Consulte a documentação que veio com seu software para habilitar quaisquer recursos de segurança disponíveis para o software.
- Um servidor pode ser inicializado de forma segura com a Inicialização WAN ou iSCSI.
  - No caso de uma versão do Oracle Solaris 10, consulte a documentação *Oracle Solaris Installation Guide: Network-Based Installations*
  - No caso de uma versão do Oracle Solaris 11, consulte a documentação *Installing Oracle Solaris 11 Systems* para obter informações sobre a Inicialização WAN e a documentação *System Administration Guide: Basic Administration* para obter informações sobre a inicialização iSCSI.

O documento *Oracle Solaris Security Guidelines* fornece informações sobre:

- Como proteger o Oracle Solaris
- Como usar os recursos de segurança do Oracle Solaris ao configurar seus sistemas
- Como operar com segurança quando você adiciona aplicativos e usuários a um sistema
- Como proteger aplicativos baseados em rede

O documento *Oracle Solaris Security Guidelines* da versão que você está usando está em:

- http://www.oracle.com/goto/Solaris11/docs
- http://www.oracle.com/goto/Solaris10/docs

Segurança do Firmware

Todos os subcomponentes do Oracle System Firmware só podem ser atualizados juntos. O Oracle System Firmware usa um processo de atualização do firmware controlado para evitar modificações não autorizadas no firmware. Somente o superusuário ou um usuário autenticado com a devida autorização pode usar o processo de atualização.

Segurança do Oracle OpenBoot

O acesso à interface de linha de comando do Oracle OpenBoot Firmware pode ser protegido por senha através do uso de variáveis de segurança do OpenBoot.

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

Oracle ILOM Firmware

O Oracle ILOM (Oracle Integrated Lights Out Manager) é o firmware de gerenciamento de sistema que vem pré-instalado no servidor, no módulo de servidor, no sistema modular e em outro hardware Oracle. O Oracle ILOM permite o gerenciamento e o monitoramento ativos dos componentes instalados no sistema. A maneira como você usa o Oracle ILOM afeta a segurança do sistema. Para saber mais sobre como usar esse firmware durante a configuração de senhas, o gerenciamento de usuários e a aplicação de recursos relacionados a segurança, incluindo autenticação SSH (Secure Shell), SSL (Secure Socket Layer) e RADIUS, consulte a documentação do Oracle ILOM:

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

Mantendo um Ambiente Seguro

Após a instalação e a configuração iniciais, use os recursos de segurança de software e hardware da Oracle para continuar controlando o hardware e rastreando os ativos do sistema.

Controles de Hardware

Alguns sistemas Oracle podem ser configurados para ligar e desligar através de comandos de software. Além disso, as unidades de distribuição de energia (PDUs) de alguns gabinetes de sistema podem ser habilitadas e desabilitadas remotamente, através de comandos de software. Geralmente, a autorização a esses comandos é configurada durante a configuração do sistema e normalmente limitada a administradores de sistema e equipes de serviços. Consulte a documentação referente ao seu sistema ou gabinete para obter mais informações.

Rastreamento de Ativo

Os números de série da Oracle são incorporados no firmware localizado em placas opcionais e placas-mãe do sistema. Esses números de série podem ser lidos através de conexões de rede local para controle de inventário.

Os leitores de identificação por radiofrequência (RFID) sem fio podem simplificar ainda mais o rastreamento de ativo. 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

- Verifique regularmente se há atualizações.
- Sempre instale a última versão lançada do software ou firmware no seu equipamento.
- Instale todos os patches de segurança necessários para o software.
- Lembre-se de que os dispositivos, como switches de rede, também contêm firmware e podem necessitar de atualizações de patches e firmware.

Acesso Local e Remoto

Siga estas diretrizes para garantir a segurança do acesso local e remoto aos seus sistemas:

- Crie um aviso para informar a proibição do acesso não autorizado.
- Use listas de controle de acesso quando apropriado.
- Defina tempos limite para sessões estendidas e defina níveis de privilégio.
- Use recursos de AAA (autenticação, autorização e contabilidade) para acesso local e remoto a um switch.
- Se possível, use os protocolos de segurança RADIUS e TACACS+:
  - O RADIUS (Remote Authentication Dial In User Service) é um protocolo de cliente/servidor que protege as redes de acesso não autorizado.
  - O TACACS+ (Terminal Access Controller Access-Control System) é um protocolo que permite a um servidor de acesso remoto a comunicação com um servidor de autenticação para determinar se um usuário tem acesso à rede.
- Use o recurso de espelhamento de portas do switch para acesso IDS (sistema de detecção de invasões).

- Implemente a segurança de porta para limitar o acesso com base em um endereço MAC. Desabilite o entroncamento automático em todas as portas.
- 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 quase todos no segmento de LAN vejam as credenciais de log-in. Defina uma senha forte para SSH.
- As versões anteriores do SNMP não são seguras e transmitem dados de autenticação em texto não criptografado. Somente a versão 3 do SNMP pode oferecer transmissões de segurança.
- Alguns produtos são fornecidos com a definição PUBLIC como string padrão da comunidade SNMP. Invasores podem consultar uma comunidade para desenhar um mapa de rede completo e possivelmente modificar valores de base de informações (MIB) de gerenciamento. Se o SNMP for necessário, altere a string padrão da comunidade SNMP para uma string de comunidade forte.
- Habilite o registro em log e envie os logs para um host de log protegido dedicado.
- Configure o registro em log para incluir informações precisas de tempo, usando NTP e registros de hora e data.
- Verifique possíveis incidentes nos logs e arquive-os de acordo com uma política de segurança.
- Se seu controlador de sistema usar uma interface de browser, faça log-out sempre que usá-lo.

Segurança de Dados

Siga estas diretrizes para maximizar a segurança dos dados:

- Faça o backup de dados importantes usando dispositivos como discos rígidos externos, pen drives ou cartões de memória. Armazene os dados submetidos a backup em outro 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 na unidade. A exclusão de todos os arquivos ou reformatação da unidade removerá apenas as tabelas de endereços da unidade; as informações ainda poderão ser recuperadas de uma unidade depois da exclusão de dados ou de sua reformatação. (Use um software de limpeza de disco para apagar completamente todos os dados em uma unidade.)

Segurança de Rede

Siga estas diretrizes para maximizar a segurança de sua rede:

- A maioria dos switches permitem que você defina redes locais virtuais (VLANs). Se você usar seu switch para definir VLANs, separe clusters de sistemas confidenciais do restante da rede. Isso reduz a probabilidade de os usuários obterem acesso às informações sobre esses clientes e servidores.
- Gerenciar switches fora de banda (separados do tráfego de dados). Se o gerenciamento fora de banda não for viável, dedique um número de VLAN separado para o gerenciamento na banda.
- Mantenha hosts Infiniband protegidos. Uma malha InfiniBand é tão segura quanto seu host Infiniband menos seguro.
- Observe que o particionamento não protege uma malha Infiniband. O particionamento só fornece isolamento de tráfego Infiniband entre máquinas virtuais em um host.
- Mantenha um arquivo de configuração de switch off-line e limite o acesso somente a administradores autorizados. O arquivo de configuração deve conter comentários descritivos para cada configuração.
- Use configuração VLAN estática, quando possível.
- Desabilite as portas de switch não utilizadas e as atribua a um número de VLAN não utilizado.
- 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 remoção. Em seguida, defina o VTP no modo transparente.
- Desabilite os serviços desnecessários, como pequenos servidores TCP ou HTTP. Habilite os serviços de rede necessários e configure esses serviços de maneira segura.
- Switches diferentes oferecerão níveis diferentes de recursos de segurança de porta. Use estes recursos de segurança de porta se estiverem disponíveis no seu switch:
  - MAC Locking: Envolve a associação com um endereço MAC (Media Access Control) de um ou mais dispositivos conectados a um switch. Se você bloquear uma porta de switch para um endereço MAC específico, os superusuários não poderão criar portas traseiras na sua rede com pontos de acesso nocivos.
  - MAC Lockout: Desabilita um endereço MAC especificado de estabelecer conexão com um switch.
  - MAC Learning: Utiliza o conhecimento sobre cada conexão direta da porta de switch de modo que o switch de rede possa definir a segurança com base nas conexões atuais.