Sun Server X4-2

Guia de Segurança

Parte No: E49390-01
Setembro de 2013

Índice

• • • Capítulo 1

Sun Server X4-2 Guia de Segurança

Este documento fornece diretrizes gerais de segurança que ajudam a proteger o Oracle Sun Server X4-2, suas interfaces de rede e os switches de rede aos quais ele está conectado.

As seguintes seções estão incluídas neste capítulo:

Visão Geral do Sistema

O Sun Server X4-2 é um servidor de classe empresarial, de um rack (1U). Ele oferece suporte aos seguintes componentes:

- Até dois processadores Intel. Processadores com os seguintes recursos são suportados:
  - 2.5 GHz, 4-Core, 80W
  - 2.6 GHz, 6-core, 80W
  - 2.6 GHz, 8-core, 95W
  - 3.0 GHz, 10-core, 130W
  - 2.7 GHz, 12-core, 130W
- Até 8 DIMMs por processador para um máximo de 16 DIMMs DDR3 e 512 GB de memória em sistemas de processador duplo. DIMMs de 8 GB, 16 GB e 32 GB são suportados.

Observação

Um máximo de 8 DIMMs para um máximo de 256 GB são suportados em sistemas de processador simples.

- Quatro slots PCIe Gen3 em sistemas de processador duplo, três slots externos e um interno. O slot PCIe 1, que é um slot externo, não funciona em sistemas de processador simples.

- As configurações da unidade de armazenamento podem incluir unidades de disco rígido (HDDs) ou unidades de disco de estado sólido (SSD). As configurações de unidade de armazenamento suportadas incluem:
  - Até quatro HDDs SAS/SSDs SATA hot-plug de 2,5 pol com DVD
  - Até oito HDDs SAS/SSDs SATA hot-plug de 2,5 pol
- Duas fontes de alimentação redundantes hot-plug.
- Um processador de serviço (SP) Oracle ILOM (Oracle Integrated Lights Out Manager) on-board baseado no chip AST2300 que fornece gerenciamento seguro local e remoto.
- A ferramenta de configuração de servidor Oracle System Assistant, que está inserida em uma unidade flash USB pré-instalada.

Princípios de Segurança

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

- **Acesso**

  O acesso se refere ao acesso físico ao hardware ou ao acesso físico ou virtual ao software.
  - Use os controles físicos e de software para proteger seu hardware e seus dados contra invasão.
  - Consulte a documentação que acompanha o software para ativar todos os recursos de segurança disponíveis para o software.
  - Instale servidores e equipamentos relacionados em um local trancado com acesso restrito.
  - Se o equipamento for instalado em um rack com uma porta com fechadura, mantenha a porta trancada, exceto durante os períodos de manutenção nos componentes do rack.
  - Restrinja o acesso a conectores ou portas, os quais podem fornecer um acesso mais fácil do que os conectores SSH. Dispositivos como controladores de sistema, unidades de distribuição de força (PDUs) e switches de rede apresentam conectores e portas.
  - Restrinja o acesso especificamente a dispositivos hot-plug ou hot-swap porque podem ser facilmente removidos.
  - Guarde unidades substituíveis no campo (FRUs) e unidade substituíveis pelo cliente (CRUs) sobressalentes em um gabinete fechado. Restrinja o acesso ao gabinete trancado a pessoas autorizadas.
- **Autenticação**

  Autenticação refere-se a garantir que os usuários do hardware ou software são quem eles dizem que são.
  - Configure recursos de autenticação, como um sistema de senhas nos sistemas operacionais da plataforma, para garantir que os usuários são realmente quem eles dizem ser.
  - Certifique-se de que sua equipe use crachás para entrar na sala do computador.
  - Para contas de usuário: use listas de controle de acesso onde apropriado; defina tempos limite para sessões estendidas; defina níveis de privilégios para usuários.
- **Autorização**

  Autorização refere-se a restrições impostas à equipe para trabalhar com hardware ou software.
  - Permita que sua equipe trabalhe somente com hardware e software nos quais foi treinada e esteja qualificada para usar.
  - Configure um sistema de permissões de Leitura/Gravação/Execução para controlar o acesso de usuários a comandos, espaço em disco, dispositivos e aplicativos.
- **Contabilidade**

Contabilidade refere-se aos recursos de software e hardware usados para monitorar a atividade de login e a manutenção de inventários de hardware.

- Use logs do sistema para monitorar logins de usuários. Monitore administradores de sistema e contas de serviço em particular porque essas contas têm acesso a comandos avançados.
- Mantenha um registro dos números de série de todo o equipamento de hardware. Use números de série de componente para rastrear ativos do sistema. Os números de peça da Oracle são gravados eletronicamente em cartões, módulos e placas-mãe, e podem ser usados para fins de inventário.
- Para detectar e rastrear componentes, faça uma marca de segurança em todos os itens importantes do hardware do computador, como FRUs. Use canetas especiais ultravioletas ou etiquetas em alto-relevo.

Usando as Ferramentas de Configuração e Gerenciamento do Servidor

Siga essas diretrizes de segurança ao usar ferramentas de software e firmware para configurar e gerenciar o servidor.

- "Segurança do Oracle System Assistant" [7]
- "Segurança do Oracle ILOM" [8]
- "Segurança do Oracle Hardware Management Pack" [9]

Segurança do Oracle System Assistant

O Oracle System Assistant é uma ferramenta pré-instalada que ajuda a configurar e atualizar, de forma local ou remota, o hardware do servidor e a instalar sistemas operacionais compatíveis. Para obter informações sobre como usar o Oracle System Assistant, consulte o *Oracle X4 Series Servers Administration Guide* em:

http://www.oracle.com/goto/x86AdminDiag/docs

As informações a seguir ajudarão a compreender problemas de segurança relacionados ao Oracle System Assistant.

- **O Oracle System Assistant contém um ambiente root inicializável**

O Oracle System Assistant é um aplicativo executado em uma unidade flash USB interna e pré-instalada. Foi desenvolvido para um ambiente root Linux inicializável. O Oracle System Assistant também fornece a capacidade de acessar sua shell root subjacente. Os usuários com acesso físico ao sistema ou os que têm acesso KVMS remoto (teclado, vídeo, mouse e armazenamento) ao sistema por meio do Oracle ILOM, poderão acessar o Oracle System Assistant e a shell root.

Um ambiente root pode ser usado para alterar a configuração e as políticas do sistema, assim como acessar dados em outros discos. É recomendável que o acesso físico ao servidor seja protegido e que os privilégios de administrador e console para os usuários do Oracle ILOM sejam atribuídos com moderação.

- **O Oracle System Assistant monta um dispositivo de armazenamento USB que é acessível ao sistema operacional**

Além de ser um ambiente inicializável, o Oracle System Assistant também é montado como um dispositivo de armazenamento USB (unidade flash) que é acessível ao sistema operacional do host após a instalação. Isso é útil para o acesso a ferramentas e drivers durante operações de manutenção e

reconfiguração. O dispositivo de armazenamento USB do Oracle System Assistant é legível e gravável e pode potencialmente ser explorado por vírus.

É recomendável que os mesmos métodos de proteção de disco sejam aplicados ao dispositivo de armazenamento do Oracle System Assistant, incluindo varreduras regulares de vírus e verificações de integridade.

- **O Oracle System Assistant pode ser desativado**

O Oracle System Assistant é uma ferramenta útil que auxilia na configuração do servidor, atualização e configuração de firmware e instalação do sistema operacional do host. No entanto, se as implicações de segurança descritas acima forem inaceitáveis ou se a ferramenta não for necessária, o Oracle System Assistant poderá ser desativado. Desativar o Oracle System Assistant significa que o dispositivo de armazenamento USB não estará mais acessível para o sistema operacional do host. Além disso, não será possível inicializar o Oracle System Assistant.

Você pode desativar o Oracle System Assistant na própria ferramenta ou no BIOS. Depois de desativado, o Oracle System Assistant só poderá ser ativado novamente com o BIOS Setup Utility. É recomendável que o BIOS Setup seja protegido por senha para que somente os usuários autorizados possam ativar o Oracle System Assistant novamente. Para obter informações sobre como desativar e reativar o Oracle System Assistant, consulte o *Oracle X4 Series Servers Administration Guide* em:

http://www.oracle.com/goto/x86AdminDiag/docs

Segurança do Oracle ILOM

É possível proteger, gerenciar e monitorar ativamente os componentes do sistema usando o firmware de gerenciamento Oracle ILOM (Integrated Lights Out Manager), o qual é pré-instalado no Sun Server X4-2, em outros sistemas baseados no Oracle x86 e em alguns servidores baseados no Oracle SPARC.

Use uma rede interna dedicada para o processador de serviço (SP) para separá-lo da rede geral. O Oracle ILOM fornece funções de controle e monitoramento de servidor para administradores de sistema. Dependendo do nível de autorização concedido aos administradores, essas funções podem incluir a capacidade de desligar o servidor, criar contas de usuários, montar dispositivos de armazenamento remoto, e assim por diante. Portanto, para manter o ambiente mais seguro e confiável possível para o Oracle ILOM, a porta de gerenciamento de rede dedicada ou a porta de gerenciamento de banda lateral do servidor deve estar sempre conectada a uma rede interna confiável ou a uma rede privada/de gerenciamento dedicada segura.

Limite o uso da conta de Administrador padrão (**root**) ao login inicial do Oracle ILOM. Essa conta de Administrador padrão só é fornecida para auxiliar a instalação inicial do servidor. Portanto, para garantir o ambiente mais seguro possível, você deve alterar a senha de Administrador padrão (**changeme**) como parte da configuração inicial do sistema. Além de alterar a senha da conta de Administrador padrão, novas contas de usuário com senhas exclusivas e níveis de autorização atribuídos devem ser estabelecidas para cada novo usuário do Oracle ILOM.

Consulte a documentação do Oracle ILOM para obter mais informações sobre 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. Para obter diretrizes de segurança específicas do Oracle ILOM, consulte o *Oracle Integrated Lights Out Manager (ILOM) 3 .1 Security Guide*, que faz parte da biblioteca de documentos do Oracle ILOM 3.1. Você encontra a documentação do Oracle ILOM 3.1 em:

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

Segurança do Oracle Hardware Management Pack

O Oracle Hardware Management Pack está disponível para o seu servidor e para muitos outros servidores baseados em 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 do servidor.

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 endereço IP do host) para monitorar vários servidores e módulos de servidor. Os Plug-ins SNMP são executados no sistema operacional do host de servidores Oracle.

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 com os sistemas operacionais Microsoft Windows.

Consulte a documentação do Oracle Hardware Management Pack para obter mais informações sobre esses recursos. Para obter as diretrizes de segurança específicas do Oracle Hardware Management Pack, consulte o *Oracle Hardware Management Pack (HMP) Security Guide*, que faz parte da biblioteca de documentos do Oracle Hardware Management Pack. Você encontra a documentação do Oracle Hardware Management Pack em:

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

Planejando um Ambiente Seguro

Use as informações a seguir ao instalar e configurar o servidor e equipamentos relacionados.

Diretrizes do Sistema Operacional Oracle

Consulte os documentos do sistema operacional Oracle para obter informações sobre:

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

Os documentos do Guia de Segurança para sistemas operacionais Oracle compatíveis fazem parte da biblioteca de documentos do sistema operacional. Para encontrar o documento do Guia de Segurança referente a um sistema operacional Oracle, vá para a biblioteca de documentos do sistema operacional Oracle:

- **Oracle Solaris 10 1/13** - http://www.oracle.com/goto/Solaris10/docs
- **Oracle Solaris 11.1** - http://www.oracle.com/goto/Solaris11/docs
- **Oracle Linux 6** - http://www.oracle.com/technetwork/documentation/ol-1-1861776.html
- **Oracle VM 3.2** - http://www.oracle.com/technetwork/documentation/vm-096300.html

Para obter informações sobre os sistemas operacionais de outros fornecedores, como o Red Hat Enterprise Linux, SUSE Linux Enterprise Server, Windows e VMware ESXi, consulte a documentação do fornecedor.

Portas e Switches de Rede

Switches diferentes oferecem níveis diferentes de recursos de segurança de porta. Consulte a documentação sobre switches para aprender a:

- Use recursos de autenticação, autorização e contabilização para acesso local e remoto ao comutador.
- Alterar cada senha nos switches de rede que podem ter várias contas de usuários e senhas por padrão.
- Gerenciar switches fora de banda (separados do tráfego de dados). Se o gerenciamento Out-of-Band não for viável, dedique um número separado de VLAN (Virtual Local Area Network Number) para o gerenciamento In-Band.
- Use o recurso de espelhamento de portas do switch de rede para acesso ao sistema de detecção de intrusões (IDS).
- Mantenha um arquivo de configuração de switch off-line e restrinja o acesso somente a administradores autorizados. O arquivo de configuração deve conter comentários descritivos para cada definição.
- Implemente a segurança de porta para limitar o acesso com base nos endereços MAC. Desative o entroncamento automático em todas as portas.
- Use estes recursos de segurança de porta se eles estiverem disponíveis no seu switch:
  - **Bloqueio de MAC** envolve a associação de um endereço MAC (Media Access Control) de um ou mais dispositivos conectados a uma porta física em um switch. Se você bloquear uma porta de switch para um endereço MAC específico, os superusuários não poderão criar backdoors na rede com pontos de acesso rogue.
  - **Bloqueio de MAC** impede que um endereço MAC específico se conecte a 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.

Segurança de VLAN

Se você configurar uma VLAN (Virtual Local Area Network), lembre-se de que as VLANs compartilham largura de banda em uma rede e necessitam de medidas de segurança adicionais.

- Defina VLANs para separar clusters confidenciais de sistemas do restante da rede. Isso reduz a probabilidade de os usuários obterem acesso às informações sobre esses clientes e servidores.
- Atribua um número exclusivo de VLAN nativa para truncar portas.
- 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.

Segurança de Infiniband

Mantenha os hosts Infiniband seguros. Uma fábrica InfiniBand é tão segura quanto seu host Infiniband menos seguro.

- Observe que o particionamento não protege uma fábrica InfiniBand. O particionamento só oferece isolamento de tráfego para Infiniband entre máquinas virtuais em um host.
- Use configuração VLAN estática, quando possível.
- Desative portas de switch não utilizadas e as atribua a um número de VLAN não utilizado.

Segurança Física do Hardware

É possível proteger fisicamente o hardware de forma simples: limite o acesso aos números de série do hardware e do registro.

- **Restringir o 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 fechadura, mantenha a porta trancada, exceto durante os períodos de manutenção nos componentes do rack. Tranque a porta depois de trabalhar com o equipamento.
  - Restrinja o acesso a conexões USB, as quais podem fornecer um acesso mais fácil do que as conexões SSH. Dispositivos como controladores de sistema, PDUs (unidades de distribuição de energia) e comutadores de rede podem ter conexões USB, as quais fornecem um acesso mais fácil do que conexões SSH.
  - Restrinja o acesso especificamente a dispositivos hot-plug ou hot-swap porque podem ser facilmente removidos.
  - Guarde unidades substituíveis no campo (FRUs) e unidade substituíveis pelo cliente (CRUs) sobressalentes em um armário trancado. Restrinja o acesso ao gabinete trancado a pessoas autorizadas.

- **Gravar números de série**
  - Faça uma marca de segurança em todos os itens importantes do hardware do computador, como FRUs. Use canetas especiais ultravioletas ou etiquetas em alto-relevo.
  - Mantenha um registro dos números de série de todo o equipamento de hardware.
  - Mantenha as chaves de ativação e as licenças do hardware em um local seguro e de fácil acesso para o gerente do sistema em caso de emergência. Os documentos impressos talvez sejam o seu único comprovante de propriedade.

Segurança do Software

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

- Altere todas as senha padrão ao instalar um novo sistema. A maioria dos tipos de equipamento utiliza senhas padrão, como **changeme**, que são amplamente conhecidas e que permitiriam acesso não autorizado ao equipamento.
- Alterar cada senha nos switches de rede que podem ter várias contas de usuários e senhas por padrão.
- Limite o uso da conta de Administrador padrão (**root**) a um único usuário administrador. Sempre crie uma nova conta do Oracle ILOM para cada novo usuário. Verifique se uma senha exclusiva e um nível apropriado de privilégios de autorização (operador, administrador, e assim por diante) foram atribuídos a cada conta de usuário do Oracle ILOM.
- Use uma rede dedicada para os processadores de serviço a fim de separá-los da rede geral.
- Proteja o acesso a conexões USB. Dispositivos como controladores de sistema, PDUs (unidades de distribuição de energia) e comutadores de rede podem ter conexões USB, que podem oferecer mais acesso que conexões SSH.
- Consulte a documentação que acompanha o software para ativar todos os recursos de segurança disponíveis para o software.
- Implemente a segurança de porta para limitar o acesso com base nos endereços MAC. Desative o entroncamento automático em todas as portas.

Mantendo um Ambiente Seguro

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

Controle de Energia de Hardware

É possível usar o software para ativar e desativar alguns sistemas Oracle. As PDUs (Power Distribution Units) de alguns gabinetes de sistema podem ser ativadas e desativadas remotamente. A autorização para esses comandos é normalmente configurada durante a configuração do sistema e, em geral, é limitada aos administradores do sistema e à equipe de manutenção. Consulte a documentação referente ao seu sistema ou gabinete para obter mais informações.

Rastreamento de Ativos

Use números de série para rastrear o estoque. A Oracle insere números de série em cartões de opção e em placas-mãe do sistema de firmware. É possível ler esses números de série por meio de conexões de rede local.

Também é possível usar leitores sem fio RFID (Radio Frequency Identification) para 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

Atualizações para Software e Firmware

Mantenha as versões de software e firmware atuais no equipamento do servidor.

- Verifique regularmente se há atualizações.
- Sempre instale a última versão lançada do software ou firmware.
- 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.

Segurança de Rede

Siga essas diretrizes para proteger o acesso local e remoto aos seus sistemas.

- 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 todos no segmento de LAN vejam as credenciais de login. Defina uma senha forte para SSH.
- Use a versão 3 do SNMP (Simple Network Management Protocol) para fornecer transmissões seguras. As versões anteriores do SNMP não são seguras e transmitem dados de autenticação em texto não criptografado.
- Altere a cadeia de caracteres de comunidade SNMP padrão para uma cadeia de caracteres de comunidade forte se o SNMP for necessário. Alguns produtos têm PUBLIC definido como a cadeia de caracteres de comunidade SNMP padrão. Os hackers podem consultar uma comunidade

para montar um mapa de rede completo e possivelmente modificar valores de MIB (Management Information Base).

- Sempre faça logout depois de usar o controlador do sistema se ele usa uma interface de navegador.
- Desabilite serviços de rede desnecessários, como Transmission Control Protocol (TCP) ou Hypertext Transfer Protocol (HTTP). Ative os serviços de rede necessários e configure esses serviços de forma segura.
- Siga as medidas de segurança de LDAP ao usar o LDAP para acessar o sistema. Consulte o *Oracle ILOM Security Guide* em: http://www.oracle.com/goto/ILOM/docs
- 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 contabilização) para acesso local e remoto a um comutador.
- 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 do 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 comutador para acesso ao IDS (sistema de detecção de intrusos).
- Implemente a segurança de porta para limitar o acesso com base em um endereço MAC. Desative o entroncamento automático em todas as portas.

Proteção de Dados e Segurança

Siga essas diretrizes para maximizar a segurança e a proteção dos dados.

- Faça backup de dados importantes usando dispositivos, como discos rígidos externos ou dispositivos de armazenamento USB. Armazene os dados submetidos a backup em um 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 contidos na unidade. Informações ainda podem ser recuperadas de uma unidade depois que os arquivos forem excluídos ou que a unidade tiver sido reformatada. Excluir os arquivos ou reformatar a unidade remove somente as tabelas de endereços na unidade. Use um software de limpeza de disco para apagar completamente todos os dados em uma unidade.

Manutenção de Logs

Inspecione e faça a manutenção de seus arquivos de log regularmente. Use esses métodos para proteger arquivos de log.

- Ative o registro em log e envie logs do sistema para um host de log dedicado seguro.
- Configure o registro em log para incluir informações de tempo precisas, usando NTP (Network Time Protocol) e registros de hora e data.
- Verifique possíveis incidentes nos logs e arquive-os de acordo com uma política de segurança.
- Remova periodicamente arquivos de log quando excederem um tamanho considerável. Mantenha cópias dos arquivos removidos para possíveis referências futuras ou análise estatística.