Netra Server X3-2 (antigo Sun Netra X4270 M3 Server)

Security Guide

Número do Item: E35615–01
Julho de 2012

ORACLE

130429@25097

Conteúdo

Guia de Segurança do Netra Server X3-2 5
Visão Geral do Sistema 5
Princípios de Segurança 5
Usando Ferramentas de Configuração e Gerenciamento do Servidor 7
Planejando um Ambiente Seguro 9
Mantendo um Ambiente Protegido 11

Guia de Segurança do Netra Server X3-2

Este documento contém diretrizes gerais de segurança que ajudam a proteger o Oracle Netra Server X3-2 (antigo Sun Netra X4270 M3 Server), suas interfaces de rede e os switches de rede aos quais ele está conectado.

Este capítulo contém as seguintes seções:

- "Visão Geral do Sistema" na página 5
- "Princípios de Segurança" na página 5
- "Usando Ferramentas de Configuração e Gerenciamento do Servidor" na página 7
- "Planejando um Ambiente Seguro" na página 9
- "Mantendo um Ambiente Protegido" na página 11

Visão Geral do Sistema

O Netra Server X3-2 é um servidor 2U de classe empresarial, em conformidade com o NEBS, que tem dois processadores e oferece suporte a dezesseis DDR3 DIMMs (oito por processador), seis slots PCIe Gen3 e oito ou seis unidades de armazenamento do SAS/SATA. O modelo de seis unidades também fornece um DVD.

O servidor inclui um processador de serviço (SP) Oracle Integrated Lights Out Manager (Oracle ILOM) inserido. Uma ferramenta de configuração do servidor chamada Oracle System Assistant é também incorporada em uma unidade USB pré-instalada como parte da sua configuração do servidor.

Princípios de Segurança

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

- **Acesso**

  Acesso refere-se ao acesso físico ao hardware ou o acesso físico ou virtual ao software.

  - Use controles físicos e de software para proteger seu hardware e dados de intrusão.
  - Consulte a documentação que veio com seu software para habilitar quaisquer recursos de segurança disponíveis para o software.

- Instale servidores e equipamentos relacionados em um local bloqueado e com acesso restrito.
- Se o equipamento for instalado em um rack com uma porta de bloqueio, mantenha a porta bloqueada, exceto quando você tiver componentes de serviço no rack.
- Restrinja o acesso aos conectores e portas que possam fornecer um acesso mais vigoroso do que as conexões SSH. Dispositivos como controladores de sistema, unidades de distribuição de energia e comutadores de rede fornecem conectores e portas.
- Restrinja o acesso a dispositivos de hot-plug ou hot-swap em especial porque eles podem ser facilmente removidos.
- Armazene unidades substituíveis de campo sobressalentes e unidades substituíveis do cliente em um gabinete bloqueado. Restrinja o acesso ao gabinete bloqueado para a equipe autorizada.

- **Autenticação**

  A autenticação se refere à certificação de que os usuários de hardware ou software são quem eles dizem que são.

  - Configure recursos de autenticação como um sistema de senha em seus sistemas operacionais de plataforma para garantir que os usuários são quem eles dizem que são.
  - Certifique-se de que sua equipe usa crachás adequadamente para entrar na sala de computadores.
  - Para contas de usuário, use listas de controle de acesso onde forem apropriadas. Defina tempos limite para sessões estendidas e defina níveis de privilégio para os usuários.

- **Autorização**

  Autorização refere-se às restrições impostas para a equipe trabalhar com hardware e software.

  - Permitir que a equipe trabalhe somente com hardware e software que eles estejam treinados e qualificados para usar.
  - Configure um sistema de permissões de leitura, gravação e execução para controlar acesso de usuários aos comandos, espaço de disco, dispositivos e aplicativos.

- **Contabilidade**

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

  - Use logs do sistema para monitorar log-in de usuário. Monitore o administrador do sistema e contas de serviço em especial porque essas contas podem acessar comandos poderosos do sistema.
  - Mantenha um registro dos números em sério de todo o seu hardware. Use números de componentes em série para rastrear ativos do sistema. Os números de peças Oracle são registros eletronicamente em cartões, módulos e placas mães.

- Para detectar e rastrear componentes, forneça uma marca de segurança sobre todos os itens significativos do hardware do computador como FRUs. Use canetas ultravioleta especiais ou rótulos.

Usando Ferramentas de Configuração e Gerenciamento do Servidor

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

Segurança do Oracle System Assistant

O Oracle System Assistant é uma ferramenta pré-instalada que ajuda você a configurar e atualizar local ou remotamente o hardware do servidor e a instalar sistema operacionais suportados. Para obter informações sobre como usar a ferramenta Oracle System Assistant, consulte o *Guia de Administração* em:

`http://docs.oracle.com/cd/E27124_01`

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

- **O Oracle System Assistant contém um ambiente-raiz inicializável**.

O Oracle System Assistant é um aplicativo executado em uma unidade flash USB interna e pré-instalada. É criado na parte superior de um ambiente-raiz Linus inicializável. O Oracle System Assistant também fornece a capacidade de acessar seu shell-raiz subjacente. Os usuários que tiverem acesso físico ao sistema ou que tiverem acesso ao Remote KVMS (teclado, vídeo, mouse e armazenamento) para o sistema por meio do Oracle ILOM, estarão aptos a acessar o Oracle System Assistant e o shell-raiz.

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

- **O Oracle System Assistant monta um dispositivo de armazenamento USB acessível para o sistema operacional**.

Além de ser um ambiente inicializável, o Oracle System Assistant também é montado como um dispositivo de armazenamento USB (unidade flash) acessível para o sistema operacional do host após a instalação. Isso é útil ao acessar ferramentas e unidades para manutenção e configuração. O dispositivo USB do Oracle System Assistant é legível e gravável e pode potencialmente ser explorado por vírus.

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

- **O Oracle System Assistant pode ser desabilitado**.

O Oracle System Assistant é uma ferramenta útil para ajudar a configurar o sistema, atualizar e configurar o firmware e instalar o 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 não poderá ser desabilitado. Desabilitar o Oracle System Assistant significa que o dispositivo de armazenamento USB não ficará mais acessível para o sistema operacional do host. Além disso, não será possível inicializar o Oracle System Assistant.

É possível desabilitar o Oracle System Assistant por meio da própria ferramenta ou por meio do BIOS. Quando for desabilitado, o Oracle System Assistant só poderá ser reabilitado por meio do Utilitário de Configuração do BIOS. É recomendável que a Configuração do BIOS seja protegida por senha de modo que apenas usuários autorizados possam reabilitar o Oracle System Assistant. Para obter informações sobre como desativar e reativar a ferramenta Oracle System Assistant, consulte o *Guia de Administração*.

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 servidor, em outros sistemas baseados no Oracle x86 e em alguns servidores baseados no Oracle SPARC.

Use uma rede dedicada para o processador de serviço para separá-lo da rede geral. Limite o uso da conta de superusuário `root`. Em vez disso, atribua as contas do Oracle ILOM como `ilom-operator` e `ilom-admin` sempre que for possível. Altere todas as senhas padrão ao instalar um novo sistema. A maioria dos tipos de equipamento usam senhas padrão, como `changeme`, que são amplamente conhecidas e permitiriam acesso não autorizado ao equipamento.

Consulte a documentação do Oracle ILOM para obter noções básicas sobre como configurar senhas, gerenciar usuários e aplicar recursos relacionados à segurança, incluindo a autenticação Secure Shell (SSH), Secure Socket Layer (SSL) e RADIUS. Para diretrizes de segurança específicas para o Oracle ILOM, consulte o *Oracle Integrated Lights Out Manager (ILOM) 3.1 Security Guide*, aque faz parte da biblioteca de documentação do Oracle ILOM 3.1. É possível localizar a documentação do Oracle ILOM 3.1 em:

`http://docs.oracle.com/cd/E24707_01`

Segurança do Oracle Hardware Management Pack

O Oracle Hardware Management Pack está disponível para o seu servidor e para vários outros servidores com base no x86 e alguns servidores SPARC. O Oracle Hardware Management Pack

apresenta dois componentes: um agente de monitoramento SNMP e uma família de ferramentas de interface da linha de comando do sistema operacional cruzado (CLI Tools) para o gerenciamento do seu servidor.

Com os Plug-ins SNMP do Agente de Gerenciamento de Hardware, é possível usar o SNMP para monitorar servidores Oracle e módulos do servidor no seu centro de dados com a vantagem de não ter que estabelecer conexão com 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 do SNMP são executados no sistema operacional do host dos servidores Oracle.

É possível usar as Ferramentas CLI do Oracle Server para configurar os servidores Oracle. As Ferramentas CLI funcionam com o Oracle Solaris, Oracle Linux, Oracle VM, outras variantes do Linux e sistemas operacionais do Microsoft Windows.

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

`http://docs.oracle.com/cd/E20451_01`

Planejando um Ambiente Seguro

Use as informações a seguir ao instalar e configurar o servidor e o equipamento relacionado.

Diretrizes do Sistema Operacional Oracle

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

- Como usar recursos de segurança ao configurar seus sistemas
- Como operar seguramente ao adicionar aplicativos e usuários a um sistema
- Como proteger aplicativos com base na rede

Os documentos do Security Guide para sistemas operacionais Oracle suportados fazem parte da biblioteca de documentação do sistema operacional. Para localizar a documentação do Security Guide para um sistema operacional Oracle, vá até a biblioteca de documentação do sistema operacional Oracle:

- **Oracle Solaris** - `http://docs.oracle.com/cd/E23824_01`
- **Oracle Linux** - `http://linux.oracle.com/documentation/`
- **Oracle VM** - `http://www.oracle.com/technetwork/documentation/vm-096300.html`

Portas e Comutadores de Rede

Comutadores diferentes oferecem níveis diferentes de recursos de segurança de porta. Consulte a documentação sobre comutadores para obter mais informações sobre como fazer o seguinte.

- Use recursos de autenticação, autorização e contabilidade para o acesso local e remoto para o comutador.
- Altere cada senha nos comutadores de rede que possam ter várias contas e senhas de usuário por padrão.
- Gerencie comutadores fora de faixa (separados do tráfego de dados). Se o gerenciamento fora de faixa não for viável, dedique um número de rede virtual de área local separada (VLAN) para o gerenciamento na faixa.
- Use os recursos de espelhamento de porta do comutador de rede para acesso ao sistema de detecção de intrusão (IDS).
- Mantenha um arquivo de configuração de comutador off-line e limite o acesso a somente administradores autorizados. O arquivo de configuração deve conter comentários descritivos para cada configuração.
- Implemente a segurança de porta para limitar o acesso com base nos endereços MAC. Desabilite o trunking automático em todas as portas.
- Use esses recursos de segurança de porta se eles estiverem disponíveis no seu comutador:
  - O **Bloqueio de MAC** envolve a associação com um endereço Media Access Control (MAC) de um ou mais dispositivos conectados em um comutador. Se você bloquear uma porta de comutador para um endereço MAC específico, os superusuários não poderão criar portas traseiras na sua rede com pontos de acesso nocivos.
  - O **Bloqueio de MAC** desabilita um endereço MAC especificado de estabelecer conexão com um comutador.
  - **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 VLAN

Se você configurar uma rede virtual de área local (VLAN), lembre-se de que VLANs compartilham largura de banda em uma rede e exigem medidas de segurança adicionais.

- Defina VLANs para separar cluster sensíveis de sistemas do resto da rede. Isso diminui a probabilidade de os usuários ganharem acesso a informações sobre esses clientes e servidores.
- Atribua um número de VLAN nativo exclusivo às portas de tronco.
- Limite as VLANs que podem ser transportadas sobre um tronco para apenas aquelas que forem estritamente exigidas.

- Desabilite o VLAN Trunking Protocol (VTP), se possível. Caso contrário, defina o seguinte para o VTP: domínio de gerenciamento, senha e abreviação. Em seguida, defina o VTP em um modo transparente.

Segurança Infiniband

Mantenha hosts Infiniband protegidos. Uma malha Infiniband só é tão segura apenas quanto seu host Infiniband menos protegido.

- Observe que o particionamento não protege uma malha Infiniband. O particionamento fornece apenas isolamento de tráfego Infiniband entre máquinas virtuais em um host.
- Use a configuração de VLAN estática, quando for possível.
- Desabilite portas de comutador não utilizadas e atribua para elas um número de VLAN não utilizado.

Mantendo um Ambiente Protegido

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

Controle de Energia de Hardware

É possível usar software para ativar e desativar alguns sistemas Oracle. As unidades de distribuição de energia (PDUs) para alguns gabinetes de sistema podem ser habilitadas e desabilitadas remotamente. A autorização para esses comandos é geralmente configurada durante a configuração do sistema e geralmente é limitada a administradores de sistema e equipes de serviços. Consulte a documentação do sistema ou gabinete para obter mais informações.

Rastreamento de Ativo

Use número em série para rastrear o inventário. A Oracle incorpora números em série no firmware em cartões de opção e placas-mãe do sistema. É possível ler esses números em série através de conexões de rede de área local.

É possível também usar leitores de identificação de frequência de rádio sem fio (RFID) para simplificar mais o rastreamento do ativo. A documentação 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

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

- Procure regularmente por atualizações.
- Sempre instale a versão lançada mais recentemente do software ou do firmware.
- Instale qualquer patch de segurança necessário para o seu software.
- Lembre-se de que os dispositivos como comutadores de rede também contém firmware e podem exigir atualizações de paches e firmware.

Acesso de Rede

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

- Limite a configuração remota para endereços IP específicos usando o SSH em vez do Telnet. O Telnet informa nomes e senhas de usuário em texto claro, possivelmente permitindo que todos no segmento LAN possam visualizar as credenciais de log-in. Defina uma senha forte para o SSH.
- Use a versão 3 do Simple Network Management Protocol (SNMP) para fornecer transmissões protegidas. Versões anteriores do SNMP não são seguras e transmitem dados de autenticação em texto não criptografado.
- Altere a string da comunidade SNMP padrão para uma string de comunidade caso o SNMP seja necessário. Alguns produtos têm PUBLIC definido como a string de comunidade SNMP padrão. Invasores podem consultar uma comunidade para desenhar um mapa de rede completo e possivelmente modificar valores de base de informações (MIB) de gerenciamento.
- Sempre efetue log-out após usar o controlador do sistema, caso ele use uma interface de navegador.
- Desabilite serviços de rede desnecessários, como Transmission Control Protocol (TCP) ou Hypertext Transfer Protocol (HTTP). Habilite serviços de rede necessário e configure esses serviços seguramente.

Proteção de Dados

Siga essas diretrizes para maximizar a segurança de 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 uma segunda locação segura externa.
- Use o software de criptografia de dados para manter informações confidenciais em discos rígidos seguras.

- Ao descartar um disco rígido antigo, destrua fisicamente a unidade ou apague completamente todos os dados na unidade. As informações ainda podem ser recuperadas de uma unidade após a exclusão de arquivos ou após a unidade ser reformatada. A exclusão de arquivos ou a reformatação da unidade remove apenas as tabelas de endereços na unidade. Use o software de eliminação de disco para apagar completamente todos os dados em uma unidade.

Manutenção de Log

Inspecione e mantenha seus arquivos de log em uma programação regular. Use esses métodos para proteger arquivos de log.

- Habilite o log e envie logs do sistema para um host de log protegido dedicado.
- Configure o log para incluir informações de tempo precisas, usando o Network Time Protocol (NTP) e marcas de data/hora.
- Revise logs para possíveis incidentes e os arquive de acordo com uma política de segurança.
- Arquive periodicamente arquivos de log quando eles excederem um tamanho razoável e, em seguida, redefina os logs. É possível usar os arquivos armazenados para referência ou análise estatística.