

# **StorageTek T10000D**

Guia de Segurança

**E50328-04**

**Agosto de 2016**

---

## **StorageTek T1000D**

### Guia de Segurança

#### **E50328-04**

Copyright © 2014, 2016, Oracle e/ou suas empresas afiliadas. Todos os direitos reservados.

Este programa de computador e sua documentação são fornecidos sob um contrato de licença que contém restrições sobre seu uso e divulgação, sendo também protegidos pela legislação de propriedade intelectual. Exceto em situações expressamente permitidas no contrato de licença ou por lei, não é permitido usar, reproduzir, traduzir, divulgar, modificar, licenciar, transmitir, distribuir, expor, executar, publicar ou exibir qualquer parte deste programa de computador e de sua documentação, de qualquer forma ou através de qualquer meio. Não é permitida a engenharia reversa, a desmontagem ou a descompilação deste programa de computador, exceto se exigido por lei para obter interoperabilidade.

As informações contidas neste documento estão sujeitas a alteração sem aviso prévio. A Oracle Corporation não garante que tais informações estejam isentas de erros. Se você encontrar algum erro, por favor, envie-nos uma descrição de tal problema por escrito.

Se este programa de computador, ou sua documentação, for entregue/distribuído(a) ao Governo dos Estados Unidos ou a qualquer outra parte que licencie os Programas em nome daquele Governo, a seguinte nota será aplicável:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

Este programa de computador foi desenvolvido para uso em diversas aplicações de gerenciamento de informações. Ele não foi desenvolvido nem projetado para uso em aplicações inerentemente perigosas, incluindo aquelas que possam criar risco de lesões físicas. Se utilizar este programa em aplicações perigosas, você será responsável por tomar todas e quaisquer medidas apropriadas em termos de segurança, backup e redundância para garantir o uso seguro de tais programas de computador. A Oracle Corporation e suas afiliadas se isentam de qualquer responsabilidade por quaisquer danos causados pela utilização deste programa de computador em aplicações perigosas.

Oracle e Java são marcas comerciais registradas da Oracle Corporation e/ou de suas empresas afiliadas. Outros nomes podem ser marcas comerciais de seus respectivos proprietários.

Intel e Intel Xeon são marcas comerciais ou marcas comerciais registradas da Intel Corporation. Todas as marcas comerciais da SPARC são usadas sob licença e são marcas comerciais registradas da SPARC International, Inc. AMD, Opteron, a logomarca da AMD e a logomarca da AMD Opteron são marcas comerciais ou marcas comerciais registradas da Advanced Micro Devices. UNIX é uma marca comercial registrada do The Open Group.

Este programa ou hardware e sua documentação podem oferecer acesso ou informações relativas a conteúdos, produtos e serviços de terceiros. A Oracle Corporation e suas empresas afiliadas não fornecem quaisquer garantias relacionadas a conteúdos, produtos e serviços de terceiros e estão isentas de quaisquer responsabilidades associadas a eles, a menos que isso tenha sido estabelecido entre você e a Oracle em um contrato vigente. A Oracle Corporation e suas empresas afiliadas não são responsáveis por quaisquer tipos de perdas, despesas ou danos incorridos em consequência do acesso ou da utilização de conteúdos, produtos ou serviços de terceiros, a menos que isso tenha sido estabelecido entre você e a Oracle em um contrato vigente.

---

# Índice

---

<b>Prefácio</b> .....	7
Público-alvo .....	7
Acessibilidade da Documentação .....	7
<b>1. Visão geral</b> .....	9
Visão Geral do Produto .....	9
Capacidade e Desempenho do T10000D .....	9
Segurança .....	9
Princípios Gerais de Segurança .....	9
Manter o Software Atualizado .....	9
Restringir o Acesso à Rede .....	10
Manter-se Atualizado com as Informações Mais Recentes de Segurança .....	10
<b>2. Instalação Segura</b> .....	11
Compreender seu Ambiente .....	11
Quais recursos precisam ser protegidos? .....	11
De quem os recursos precisam ser protegidos? .....	11
O que acontecerá se as proteções dos recursos estratégicos falharem? .....	11
Protegendo a Unidade de Fita .....	11
Instalando o aplicativo do Virtual Operator Panel (VOP) .....	12
Configuração Pós-Instalação .....	12
Atribuir a senha (admin) do usuário. ....	12
Impor o gerenciamento de senhas .....	13
<b>3. Recursos de Segurança</b> .....	15
<b>A. Lista de Verificação para uma Implantação Segura</b> .....	17
<b>B. Referências</b> .....	19



# Lista de Tabelas

2.1. Portas de rede usadas ..... 11



# Prefácio

---

Este documento descreve os recursos de segurança do StorageTek T10000D da Oracle.

## **Público-alvo**

Este guia destina-se aos envolvidos no uso de recursos de segurança e na instalação e configuração seguras do StorageTek T10000D.

## **Acessibilidade da Documentação**

Para obter informações sobre o comprometimento da Oracle com a acessibilidade, visite o site do Oracle Accessibility Program em <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

### **Acesso ao Oracle Support**

Os clientes da Oracle que adquiriram serviços de suporte têm acesso a suporte eletrônico por meio do My Oracle Support. Para obter informações, visite <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> ou <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> se você for portador de deficiência auditiva.





---

---

## Capítulo 1. Visão geral

Esta seção oferece uma visão geral da unidade de fita StorageTek T10000D e explica os princípios gerais de segurança de unidades de fita.

### Visão Geral do Produto

A unidade de fita empresarial T10000D anexa-se a sistemas abertos SCSI via protocolo Fibre Channel e mainframe via protocolo FICON. A unidade de fita T10000D transfere dados de entrada e saída para um host e os armazena em uma mídia magnética removível. A unidade de fita T10000D destina-se principalmente a fornecer alta confiabilidade, backup de alta capacidade, arquivamento e recursos de processamento de dados para clientes corporativos que exigem High duty cycle (HDC) e confiabilidade. O produto oferece criptografia de dados opcional. O cliente tem a opção de habilitar o recurso de criptografia. O produto de unidade de fita foi aprimorado para oferecer capacidade e velocidade de fita nativa. Além disso, os recursos de gerenciamento de dados também foram adicionados.

### Capacidade e Desempenho do T10000D

A unidade de fita T10000D possui 8,5 TB de capacidade e 252 MB por segundo de velocidade de fita nativa.

### Segurança

A unidade de fita T10000D foi projetada para ser usada em um ambiente de hardware controlado. As unidades de fita estão sempre localizadas em um centro de dados controlado e, normalmente, dentro de uma biblioteca de fitas. Em alguns casos, o cliente usará uma versão montada em rack, mas isso é raro. O centro de dados controlado também está dentro de um firewall protegido pelas políticas de segurança do próprio cliente. Isso oferece a melhor relação de funcionalidade e proteção, tanto para a internet em geral como para a entidade interna que opera a unidade de fita.

### Princípios Gerais de Segurança

Os princípios a seguir são essenciais para o uso seguro de qualquer produto.

#### Manter o Software Atualizado

Um dos princípios das boas práticas de segurança é manter todas as versões e patches do software atualizados. Em todo o documento, pressupomos o seguinte nível de software:

T10000D 4.XX.1XX

## **Restringir o Acesso à Rede**

Proteja a unidade de fita com um firewall de centro de dados. O firewall garante que o acesso a esses sistemas seja restrito à rota de rede conhecida, a qual poderá ser monitorada e restringida, se necessário. Como alternativa, um roteador de firewall substitui vários firewalls independentes. Identificar os hosts com permissão para anexar à unidade de fita e bloquear todos os outros hosts são práticas recomendadas sempre que possível.

## **Manter-se Atualizado com as Informações Mais Recentes de Segurança**

A Oracle aprimora continuamente seu software e documentações relacionadas. Verifique se há revisões em cada versão deste documento.

---

---

## Capítulo 2. Instalação Segura

Esta seção destaca o processo de planejamento e implementação de uma instalação e configuração seguras, descreve várias topologias de implantação recomendadas para o sistema e explica como proteger uma biblioteca de fitas.

### Compreender seu Ambiente

Para melhor compreender suas necessidades de segurança, as seguintes perguntas devem ser feitas:

#### Quais recursos precisam ser protegidos?

Muitos recursos no ambiente de produção podem ser protegidos. Considere os recursos que necessitam de proteção ao decidir o nível de segurança que você deve fornecer.

#### De quem os recursos precisam ser protegidos?

A unidade de fita deve ser protegida de todos na Internet. Mas a unidade de fita deve ser protegida dos funcionários na intranet da empresa?

#### O que acontecerá se as proteções dos recursos estratégicos falharem?

Em alguns casos, uma falha no esquema de segurança é facilmente detectada e considerada nada mais do que uma inconveniência. Em outros casos, uma falha poderia causar um grande dano às empresas ou aos clientes individuais que utilizam a unidade de fita. Compreender as ramificações de segurança de cada recurso ajudará a protegê-lo adequadamente.

### Protegendo a Unidade de Fita

Por padrão, a unidade de fita utiliza as portas listadas na tabela a seguir. O firewall deve estar configurado para permitir que o tráfego use essas portas e que qualquer porta não utilizada seja bloqueada. As unidades de fita suportam IPv6 e IPv4.

**Tabela 2.1. Portas de rede usadas**

Porta	T10000D
22 tcp - SSH VOP	X

Porta	T10000D
22 tcp - SFTP	X
161 udp - Solicitações do agente da Unidade de Fita SNMPV1 - com monitoramento do estado de entrada	X
162 udp - Unidade de Fita SNMPV1 intercepta e informa notificações - sem monitoramento do estado de saída para traps, com monitoramento do estado de saída para informações	X
23 tcp - TELNET	
21 tcp - FTP	
9842 tcp - EPT	
3331 OKM - desafio e serviço da Root CA	X
3332 OKM – Inscrição. Cyber strength é AES256	X
3334 OKM – Troca de chaves de criptografia. Cyber strength é AES256	X
3335 OKM – Descoberta de cluster. Cyber strength é AES256	X

Nossos clientes terão as portas 21 e 23 desabilitadas para T10000D. Se um cliente solicitar acesso a um TELNET não seguro, ou FTP não seguro, ou ambos, uma opção de configuração do VOP estará disponível.

## Instalando o aplicativo do Virtual Operator Panel (VOP)

O VOP só deve ser instalado em sistemas que estão na mesma infraestrutura de rede protegida que a unidade de fita. Os controles de acesso do cliente devem ser reforçados nos sistemas onde o VOP está instalado para garantir acesso restrito à unidade de fita. Consulte [Tabela 2.1, “Portas de rede usadas”](#) para saber as portas usadas pelo VOP.

Consulte o guia do usuário do VOP a seguir para obter instruções de instalação do VOP pela Web.

<http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#vop>

## Configuração Pós-Instalação

Esta seção mostra as alterações na configuração de segurança que devem ser efetuadas após a instalação.

### Atribuir a senha (admin) do usuário.

A senha da conta de administração do cliente deve ser alterada pelo cliente no site e pertence ao cliente. A segurança da senha atende aos padrões da Oracle. Um número infinito de senhas está disponível para uso durante a vida útil da unidade de fita. Se a senha de administração for esquecida, ela poderá ser redefinida. A primeira senha é a senha padrão enviada com a unidade de fita.

## Impor o gerenciamento de senhas

As regras básicas de gerenciamento de senhas, como tamanho e complexidade da senha devem ser aplicadas à senha do administrador.

As regras de gerenciamento de senhas exigem pelo menos uma das regras a seguir.

- Deve ter entre 8 e 16 caracteres de extensão
- Letras minúsculas (a-z)
- Letras maiúsculas (A-Z)
- Dígito decimal (0-9)
- Caracteres especiais (.?;"'{}[]!@#\$%&, ...)



## Capítulo 3. Recursos de Segurança

Esta seção descreve os mecanismos de segurança específicos oferecidos pelo produto.

A unidade de fita T10000D se comunica em um canal seguro com o Oracle Key Management System. O T10000D estabelecerá a comunicação entre o SSH e SFTP com o Virtual Operator Panel, e o TELNET e o FTP serão desabilitados para nossos clientes. Esta não deverá ser a única medida de segurança para proteger a Unidade de Fita. De preferência, as Unidades de Fita devem estar em um centro de dados fisicamente protegido que também possui uma rede segura cujo acesso só é permitido de servidores que utilizam sua funcionalidade. Os servidores e aplicativos executados também devem estar protegidos. Além disso, o cliente tem a opção de aumentar a segurança da unidade de fita para outro nível. Uma das opções é criptografar os dados.





---

# Apêndice A

---

## Apêndice A. Lista de Verificação para uma Implantação Segura

A seguinte lista de verificação de segurança inclui diretrizes que ajudam a proteger a unidade de fita:

1. Impor o gerenciamento de senhas.
2. Impor controles de acesso.
3. Restringir o acesso à rede.
  - a. Um firewall deve ser implementado.
  - b. O firewall não deve estar comprometido.
  - c. O acesso ao sistema deve ser monitorado.
  - d. Os endereços IP de rede devem ser verificados.
4. Entre em contato com a equipe do Oracle Services, Oracle Tape Library Engineering ou com um representante de conta se você encontrar vulnerabilidades nas unidades de fita da Oracle.



---

# Apêndice B

---

## Apêndice B. Referências

É possível acessar o Guia do Usuário do VOP em:

<http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html#vop>

