

# **StorageTek SL150 Modular Tape Library**

Guia de Segurança

**E41029-03**

**Junho de 2015**

---

## StorageTek SL150 Modular Tape Library

### Guia de Segurança

#### E41029-03

Copyright © 2012, 2015, 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
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
Contra quem os recursos estão sendo protegidos? .....	11
O que acontecerá se as proteções dos recursos estratégicos falharem? .....	11
Protegendo a Biblioteca .....	11
Configuração da Instalação .....	12
Atribuir a senha (admin) do usuário .....	12
Impor o gerenciamento de senhas .....	13
Autenticação da Interface do Usuário do Browser .....	13
<b>3. Recursos de Segurança</b> .....	15
<b>4. Reimplantação</b> .....	17
<b>A. Lista de Verificação para uma Implantação Segura</b> .....	19
<b>B. Referências</b> .....	21



# Lista de Tabelas

2.1. Portas de Rede SL150 .....	11
---------------------------------	----



# Prefácio

---

Este documento descreve os recursos de segurança do StorageTek SL150 Modular Tape Library da Oracle.

## **Público-alvo**

Este guia destina-se aos envolvidos com a instalação e configuração seguras do StorageTek SL150 Modular Tape Library da Oracle e com o uso de seus recursos de segurança.

## **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.





## Visão Geral

Esta seção fornece uma visão geral do StorageTek SL150 Modular Tape Library da Oracle e explica os princípios gerais da segurança da biblioteca de fitas.

### Visão Geral do Produto

O StorageTek SL150 Modular Tape Library é uma biblioteca de fitas automatizada modular montada em rack de 3U a 21U 19" da Oracle Corporation. Oferece capacidade de armazenamento para 30 a 300 cartuchos LTO, 1 a 20 unidades de fita SAS (Serial Attached SCSI) ou FC (Fibre Channel) LTO ou um caminho de controle de porta SAS ou FC de unidade com ponte, por meio de uma das unidades de fita instaladas.

### Segurança

Todos os produtos da biblioteca de fitas foram projetados e documentados para uso em um ambiente de servidor controlado sem acesso à rede geral ou acesso do usuário. Isso oferece a melhor relação de funcionalidade e proteção, tanto do ponto de vista da Internet em geral como da entidade interna que opera a biblioteca.

### Princípios Gerais de Segurança

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

#### Manter o Software Atualizado

Um dos princípios da boa prática de segurança é manter todas as versões e patches do software atualizados. As versões do Firmware SL150 lançadas desde abril de 2015 são estas:

Junho de 2012 v1.00 (RTA 0.1.0.0.0)  
Setembro de 2012 v1.03 (RTA 0.1.0.3.0)  
Outubro de 2012 v1.50 (RTA 0.1.5.0.0)  
Janeiro de 2013 v1.82 (RTA 0.1.8.2.0)  
Agosto de 2013 v2.0 (RTA 0.2.0.0.0)  
Outubro de 2013 v2.01 (RTA 0.2.0.1.0)  
Abril de 2014 v2.25 (RTA 0.2.2.5.0)  
Junho de 2015 v2.50 (RTA 0.2.5.0.0)

## **Restringir o Acesso à Rede**

Mantenha a biblioteca protegida por um firewall de centro de dados. O firewall garante que o acesso a esses sistemas seja restrito a uma 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 se conectar à biblioteca 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.

---

---

## Instalação Segura

Esta seção aborda o processo de planejamento de uma instalação segura, descreve várias topologias de implantação recomendadas para os sistemas e explica como proteger a biblioteca.

### Compreender seu Ambiente

Para compreender melhor suas necessidades de segurança, as perguntas a seguir devem ser feitas.

#### Quais recursos precisam ser protegidos?

Vários recursos do ambiente de produção podem ser protegidos. Considere os recursos que necessitam de proteção ao decidir o nível de segurança que você deve fornecer.

#### Contra quem os recursos estão sendo protegidos?

A biblioteca deverá ser protegida contra todos na Internet e contra usuários não autorizados na intranet.

#### 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, uma falha poderá causar danos a empresas ou a clientes individuais que utilizam a biblioteca. Compreender as implicações de segurança de cada recurso ajudará a protegê-los adequadamente.

### Protegendo a Biblioteca

Por padrão, a biblioteca utiliza as portas listadas em [Tabela 2.1, “Portas de Rede SL150”](#). O firewall deve estar configurado para permitir que o tráfego use essas portas e que qualquer porta não utilizada seja bloqueada.

**Tabela 2.1. Portas de Rede SL150**

Porta	Tipo	Descrição
22	TCP	Acesso CLI SSH – com monitoramento do estado de entrada

Porta	Tipo	Descrição
		Apenas para teste de desenvolvimento e depuração, não disponível no campo
25	TCP	SMTP sem autenticação
67	DHCP	cliente - saída
68	DHCP	cliente - entrada
80	HTTP	Porta do WebLogic para interface do usuário remota
123	NTP	Network Time Protocol (se ativado)
161	UDP	Solicitações do agente de biblioteca SNMP - com monitoramento do estado de entrada
162	UDP	Traps de biblioteca SNMP e notificações informativas - sem monitoramento do estado de saída para traps, com monitoramento do estado de saída para informações
465	TCP	SMTP com autenticação SSL ou TLS
443	HTTPS	Porta do WebLogic para interface do usuário remota para HTTPS
546	DHCPv6	IPv6 - cliente DHCP - saída
547	DHCPv6	IPv6 - cliente DHCP - entrada
33200-33500	TRACEROUTE	Uso no desenvolvimento de software

A seleção dos números de porta válidos para uso da biblioteca é reservada ou recomendada de acordo com a lista da tabela anterior. Os números de porta válidos começam com o número 1, uma vez que zero não é um número de porta válido.

Ao configurar o SNMP, é altamente recomendável usar o SNMPv3, em vez do SNMPv2c, pelos seus recursos de confidencialidade, integridade e autenticação.

Ao configurar o SMTP, é altamente recomendável usar a autenticação TLS, em vez da autenticação SSL ou de nenhuma autenticação.

## Configuração da Instalação

Esta seção registra as alterações na configuração de segurança que devem ser feitas durante a instalação.

### Atribuir a senha (admin) do usuário

Na primeira inicialização, um assistente de configuração é executado automaticamente no painel de operador local para obter informações básicas de configuração. Isso inclui o nome de usuário e a senha da conta do administrador, as definições de rede e outras definições básicas.

A biblioteca não se tornará operacional até que o assistente de configuração seja concluído.

Uma conta de log-in é fornecida com a entrega do produto, a qual o instalador deverá fornecer como a primeira etapa na rotina do assistente de configuração. O usuário deverá informar uma nova senha antes da conclusão do assistente de configuração.

Quando o assistente de configuração inicial tiver sido concluído e a biblioteca estiver totalmente operacional, outras modificações poderão ser feitas em todas as definições da biblioteca por meio da BUI (Browser User Interface, Interface do Usuário do Browser).

## **Impor o gerenciamento de senhas**

As regras básicas de gerenciamento de senhas, como tamanho, histórico e complexidade da senha, devem ser aplicadas a todas as senhas. As senhas do SL150 devem ter entre 8 e 128 caracteres e conter pelo menos um caractere numérico ou especial. A senha padrão deve ser alterada durante a instalação e não pode ser reutilizada.

---

**Observação:**

O número de caracteres mostrados mascarados não indica o número exato de caracteres inseridos.

---

## **Autenticação da Interface do Usuário do Browser**

Limite as definições do browser usadas para acessar a interface do usuário remota de modo que permaneçam em TLS 1.0 ou em uma versão superior, a fim de reduzir a vulnerabilidade CVE-2014-3566 para os níveis de firmware abaixo da versão 2.50. O firmware da biblioteca não fará uma negociação automática para SSLv3 na versão 2.50.



---

---

## Recursos de Segurança

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

A biblioteca dispõe de um firewall interno para sua autoproteção. Esta não deve ser a única medida de segurança para proteger a biblioteca. É recomendável que a biblioteca esteja em um centro de dados protegido fisicamente em uma rede segura, permitindo acesso somente de servidores que utilizam sua funcionalidade. Os servidores e os aplicativos executados também devem estar protegidos.

As contas de usuário devem ser limitadas ao nível de atribuição *operador*, em vez de conceder a todos os usuários o nível de atribuição *Admin*. O uso adequado da atribuição de usuário *serviço* deve ser respeitado. Crie, ative ou desative as contas com a atribuição de usuário *serviço* conforme necessário. As atribuições de serviço têm privilégio maior do que a atribuição *operador*, com praticamente o mesmo nível de autorização que a atribuição *admin*.

Se um histórico da atividade da biblioteca for necessário para fins investigativos, o "Log de Atividade" poderá ser verificado e exportado para análise mais detalhada. O Log de Atividade na interface do usuário poderá mostrar ações iniciadas pela UI, pelo Host ou por log-ins do usuário para fins de rastreamento.





## Reimplantação

Esta seção descreve como a biblioteca é retornada ao estado padrão de fábrica para limpar todos os dados do cliente.

Caso o cliente precise encerrar uma biblioteca, será fornecido um procedimento para remover todas as informações de configuração do cliente e todos os arquivos de log, e retornar a biblioteca ao estado padrão de fábrica. Para chamar esse procedimento, coloque a biblioteca no modo "locate", em seguida, pressione simultaneamente os botões de localização frontal e traseiro por mais de 10 segundos e, depois, solte os dois botões.

Quando o botão Locate é pressionado por tempo suficiente, a velocidade de piscagem do LED muda de lenta para rápida.

---

---

# Apêndice A

---

## Lista de Verificação para uma Implantação Segura

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

1. Impor o gerenciamento de senhas para todas as contas de usuário.
2. Impor controles de acesso, tanto por proximidade física como por meio de interfaces, como SCSI, UI, SNMP etc.
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.
  - e. É possível que os serviços tenham ferramentas que necessitem de controles adequados de senha ou de acesso monitorados (por exemplo, SDP-2 para permitir o download automático de informações de log ou outro acesso)
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 Bibliotecas de Fitas da Oracle.
5. O SMTP deve usar o TLS em vez de protocolos inferiores, como SSL ou nenhum.
6. O SNMP deve ser configurado com o nível V3 em vez de com o nível V2C ou menos recursos.

---

---

# Apêndice B

---

## Referências

*SL150 User Guide* localizado em:

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

Toda a documentação relacionada ao produto SL150 está disponível no documento on-line definido com o número de componente E35103-07.

