

StorageTek SL150 Modular Tape Library

보안 설명서

E40926-03

2015년 6월

StorageTek SL150 Modular Tape Library

보안 설명서

E40926-03

Copyright © 2012, 2015, Oracle and/or its affiliates. All rights reserved.

본 소프트웨어와 관련 문서는 사용 제한 및 기밀 유지 규정을 포함하는 라이선스 합의서에 의거해 제공되며, 지적 재산법에 의해 보호됩니다. 라이선스 합의서 상에 명시적으로 허용되어 있는 경우나 법규에 의해 허용된 경우를 제외하고, 어떠한 부분도 복사, 재생, 번역, 방송, 수정, 라이선스, 전송, 배포, 진열, 실행, 발행, 또는 전시될 수 없습니다. 본 소프트웨어를 리버스 엔지니어링, 디스어셈블리 또는 디컴파일하는 것은 상호 운용에 대한 법규에 의해 명시된 경우를 제외하고는 금지되어 있습니다.

이 안의 내용은 사전 공지 없이 변경될 수 있으며 오류가 존재하지 않음을 보증하지 않습니다. 만일 오류를 발견하면 서면으로 통지해 주시기 바랍니다.

만일 본 소프트웨어나 관련 문서를 미국 정부나 또는 미국 정부를 대신하여 라이선스한 개인이나 법인에게 배송하는 경우, 다음 공지 사항이 적용됩니다.

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.

본 소프트웨어 혹은 하드웨어는 다양한 정보 관리 애플리케이션의 일반적인 사용을 목적으로 개발되었습니다. 본 소프트웨어 혹은 하드웨어는 개인적인 상해를 초래할 수 있는 애플리케이션을 포함한 본질적으로 위험한 애플리케이션에서 사용할 목적으로 개발되거나 그 용도로 사용될 수 없습니다. 만일 본 소프트웨어 혹은 하드웨어를 위험한 애플리케이션에서 사용할 경우, 라이선스 사용자는 해당 애플리케이션의 안전한 사용을 위해 모든 적절한 비상-안전, 백업, 대비 및 기타 조치를 반드시 취해야 합니다. Oracle Corporation과 그 자회사는 본 소프트웨어 혹은 하드웨어를 위험한 애플리케이션에서의 사용으로 인해 발생하는 어떠한 손해에 대해서도 책임지지 않습니다.

Oracle과 Java는 Oracle Corporation 및/또는 그 자회사의 등록 상표입니다. 기타의 명칭들은 각 해당 명칭을 소유한 회사의 상표일 수 있습니다.

Intel 및 Intel Xeon은 Intel Corporation의 상표 내지는 등록 상표입니다. SPARC 상표 일체는 라이선스에 의거하여 사용되며 SPARC International, Inc.의 상표 내지는 등록 상표입니다. AMD, Opteron, AMD 로고, 및 AMD Opteron 로고는 Advanced Micro Devices의 상표 내지는 등록 상표입니다. UNIX는 The Open Group의 등록상표입니다.

본 소프트웨어 혹은 하드웨어와 관련문서(설명서)는 제3자로부터 제공되는 콘텐츠, 제품 및 서비스에 접속할 수 있거나 정보를 제공합니다. 사용자와 오라클 간의 합의서에 별도로 규정되어 있지 않는 한 Oracle Corporation과 그 자회사는 제3자의 콘텐츠, 제품 및 서비스와 관련하여 어떠한 책임도 지지 않으며 명시적으로 모든 보증에 대해서도 책임을 지지 않습니다. Oracle Corporation과 그 자회사는 제3자의 콘텐츠, 제품 및 서비스에 접속하거나 사용으로 인해 초래되는 어떠한 손실, 비용 또는 손해에 대해 어떠한 책임도 지지 않습니다. 단, 사용자와 오라클 간의 합의서에 규정되어 있는 경우는 예외입니다.

차례

머리말	7
대상	7
설명서 접근성	7
1. 개요	9
제품 개요	9
보안	9
일반 보안 원칙	9
소프트웨어를 최신 상태로 유지	9
네트워크 액세스 제한	10
최신 보안 정보 적용	10
2. 보안 설치	11
사용자 환경 이해	11
어떤 리소스를 보호해야 합니까?	11
누구로부터 리소스를 보호합니까?	11
전략적 리소스에 대한 보호를 실패할 경우 어떤 일이 발생합니까?	11
라이브러리 보안	11
설치 구성	12
사용자(관리자) 암호 지정	12
암호 관리 적용	12
브라우저 UI 인증	13
3. 보안 기능	15
4. 재배포	17
A. 보안 배치 점검 목록	19
B. 참조	21

표 목 록

2.1. SL150 네트워크 포트	11
--------------------------	----

머리말

이 문서에서는 Oracle StorageTek SL150 Modular Tape Library의 보안 기능에 대해 설명합니다.

대상

이 설명서는 Oracle StorageTek SL150 Modular Tape Library의 보안 설치/구성 및 해당 보안 기능 사용과 관련된 모든 사람을 대상으로 합니다.

설명서 접근성

오라클의 접근성 개선 노력에 대한 자세한 내용은 <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>에서 Oracle Accessibility Program 웹 사이트를 방문하십시오.

오라클 고객지원센터 액세스

지원 서비스를 구매한 오라클 고객은 My Oracle Support를 통해 온라인 지원에 액세스할 수 있습니다. 자세한 내용은 <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info>를 참조하거나, 청각 장애가 있는 경우 <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs>를 방문하십시오.

이 절에서는 Oracle StorageTek SL150 Modular Tape Library의 개요를 살펴보고, 테이프 라이브러리 보안의 일반적인 원칙에 대해 설명합니다.

제품 개요

Oracle Corporation의 StorageTek SL150 Modular Tape Library는 3U~21U 19" 랙에 마운트된 자동화된 모듈식 테이프 라이브러리입니다. 이 라이브러리에서는 30~300 LTO 테이프 카트리지의 스토리지 용량, 1~20 LTO 광 섬유 채널 드라이브 또는 SAS 테이프 드라이브, 설치된 테이프 드라이브 중 하나를 통과하는 브리지 드라이브 광 섬유 또는 SAS 포트 제어 경로를 제공합니다.

보안

모든 테이프 라이브러리 제품은 일반적인 네트워크 또는 사용자 액세스가 없는 제어된 서버 환경 내부에서 사용하도록 설계되고 문서화되었습니다. 따라서 인터넷 전반 및 라이브러리를 운영하는 내부 엔티티 모두로부터 라이브러리가 손상되지 않도록 보호하고 최상의 기능을 제공할 수 있습니다.

일반 보안 원칙

다음 원칙은 제품을 안전하게 사용하는 데 반드시 필요한 사항입니다.

소프트웨어를 최신 상태로 유지

올바른 보안 실행 원칙 중 하나는 모든 소프트웨어 버전 및 패치를 최신 상태로 유지하는 것입니다. 2015년 4월 이후 릴리스된 SL150 펌웨어 버전은 다음과 같습니다.

2012년 6월 v1.00(RTA 0.1.0.0.0)
2012년 9월 v1.03(RTA 0.1.0.3.0)
2012년 10월 v1.50(RTA 0.1.5.0.0)
2013년 1월 v1.82(RTA 0.1.8.2.0)
2013년 8월 v2.0(RTA 0.2.0.0.0)
2013년 10월 v2.01(RTA 0.2.0.1.0)
2014년 4월 v2.25(RTA 0.2.2.5.0)
2015년 6월 v2.50(RTA 0.2.5.0.0)

네트워크 액세스 제한

라이브러리를 데이터 센터 방화벽으로 보호합니다. 방화벽으로 보호하면 시스템에 대한 액세스가 알려진 네트워크 경로로 제한되며 필요한 경우 모니터링하고 제한할 수 있습니다. 또는 방화벽 라우터가 여러 개의 독립된 방화벽을 대체할 수 있습니다. 라이브러리에 대한 연결이 허용되는 호스트를 식별하고 가능한 한 다른 모든 호스트를 차단하는 것이 좋습니다.

최신 보안 정보 적용

Oracle은 지속적으로 소프트웨어 및 설명서를 개선하고 있습니다. 개정이 릴리스될 때마다 문서를 확인하십시오.

보안 설치

이 절에서는 보안 설치에 대한 계획 프로세스의 개요를 살펴보고, 권장되는 몇 가지 시스템 배치 토폴로지에 대해 설명하고, 라이브러리를 보안하는 방법을 살펴봅니다.

사용자 환경 이해

보안 요구 사항을 더 잘 이해하려면 다음과 같은 질문을 해야 합니다.

어떤 리소스를 보호해야 합니까?

프로덕션 환경의 다양한 리소스를 보호할 수 있습니다. 제공할 보안 레벨을 결정할 때는 보호가 필요한 리소스를 고려하십시오.

누구로부터 리소스를 보호합니까?

라이브러리는 모든 인터넷 사용자 및 허용되지 않은 인트라넷 사용자로부터 보호되어야 합니다.

전략적 리소스에 대한 보호를 실패할 경우 어떤 일이 발생합니까?

어떤 경우에는 보안 체계의 결함이 쉽게 감지되고 불편함 정도로만 간주됩니다. 경우에 따라서는 결함으로 인해 라이브러리를 사용하는 회사 또는 개별 클라이언트에 막대한 피해가 발생할 수 있습니다. 각 리소스의 보안이 미치는 영향을 이해하면 해당 리소스를 적절하게 보호할 수 있습니다.

라이브러리 보안

기본적으로 라이브러리는 표 2.1. "SL150 네트워크 포트"에 나열된 포트를 사용합니다. 이러한 포트를 사용하는 트래픽은 허용하고 사용되지 않는 포트는 차단되도록 방화벽을 구성해야 합니다.

표 2.1. SL150 네트워크 포트

포트	유형	설명
22	TCP	SSH CLI 액세스 – 인바운드 Stateful 개발 테스트 및 디버그용으로, 실제로는 사용할 수 없습니다.
25	TCP	인증 없는 SMTP
67	DHCP	클라이언트 - 아웃바운드

포트	유형	설명
68	DHCP	클라이언트 - 인바운드
80	HTTP	원격 사용자 인터페이스를 위한 WebLogic 포트
123	NTP	NTP(Network Time Protocol)(사용 가능한 경우)
161	UDP	SNMP 라이브러리 에이전트 요청 - 인바운드 Stateful
162	UDP	SNMP 라이브러리 트랩 및 정보 알림 - 트랩의 경우 아웃바운드 Stateless, 정보의 경우 아웃바운드 Stateful
465	TCP	SSL 또는 TLS 인증의 SMTP
443	HTTPS	HTTPS 원격 사용자 인터페이스를 위한 WebLogic 포트
546	DHCPv6	IPv6 DHCP 클라이언트 - 아웃바운드
547	DHCPv6	IPv6 DHCP 클라이언트 - 인바운드
33200-33500	TRACEROUTE	소프트웨어 개발용

위의 표 목록에 따라 라이브러리 사용을 위한 유효한 포트 번호 선택이 예약되거나 권장됩니다. 0은 올바른 포트 번호가 아닙니다. 올바른 포트 번호는 숫자 1부터 시작됩니다.

SNMP를 구성할 때는 기밀 유지, 무결성 및 인증 기능 때문에 SNMPv2c보다 SNMPv3을 사용할 것을 권장합니다.

SMTP를 구성할 때는 SSL 또는 인증 없음 옵션보다 TLS 인증을 사용할 것을 적극 권장합니다.

설치 구성

이 절에서는 설치 중 수행해야 하는 보안 구성 변경 사항에 대해 설명합니다.

사용자(관리자) 암호 지정

처음 전원을 켜면 로컬 운영자 패널에서 설치 마법사가 자동으로 실행되어 기본 구성 정보를 가져옵니다. 여기에는 관리자 계정 사용자 이름 및 암호, 네트워크 설정 및 기타 기본 설정이 포함되어 있습니다.

라이브러리는 설치 마법사가 완료될 때까지 작동하지 않습니다.

설치 프로그램이 설치 마법사 루틴의 첫번째 단계로 입력해야 하는 로그인 계정이 제품 출하시 제공됩니다. 사용자는 설치 마법사가 완료되기 전에 새 암호를 입력해야 합니다.

초기 설치 마법사가 완료되고 라이브러리의 전원이 완전히 켜지면 모든 라이브러리 설정에 대한 BUI(브라우저 사용자 인터페이스)를 통해 라이브러리 구성을 위한 추가 수정 작업을 수행할 수 있습니다.

암호 관리 적용

암호 길이, 내역, 복잡성 등의 기본 암호 관리 규칙이 모든 암호에 적용되어야 합니다. SL150 암호는 8자에서 128자 사이여야 하고 하나 이상의 숫자 또는 특수 문자를 포함해야 합니다. 기본 암호는 설치 중 변경되어야 하며 재사용할 수 없습니다.

주:

마스크되어 표시된 문자 수는 입력된 문자 수를 정확하게 나타내지 않습니다.

브라우저 UI 인증

버전 2.50 아래의 펌웨어 레벨에 대해 CVE-2014-3566을 완화하려면 원격 사용자 인터페이스에 액세스하는 데 사용되는 브라우저 설정을 TLS 1.0 이상으로 유지하도록 제한합니다. 버전 2.50에서 라이브러리 방화벽은 SSLv3로 아래로 자동 협상되지 않습니다.

보안 기능

이 절에서는 제품에서 제공하는 구체적인 보안 메커니즘의 개요를 살펴봅니다.

이 라이브러리는 자체 보호를 위한 내부 방화벽을 제공합니다. 라이브러리를 보호하기 위한 보안으로 방화벽만 있는 것은 아닙니다. 라이브러리는 해당 기능을 사용하는 서버에만 액세스를 허용하는 보안된 네트워크 상의 물리적으로 보안된 데이터 센터에 두는 것이 권장됩니다. 라이브러리에서 실행되는 서버 및 응용 프로그램도 보안되어야 합니다.

사용자 계정은 모든 사용자에게 관리자 역할 레벨을 부여하는 대신 운영자 역할 레벨로 제한되어야 합니다. 서비스 사용자 역할의 적절한 사용법을 알아 두어야 합니다. 필요한 대로 서비스 사용자 역할을 만들거나, 사용으로 설정하거나, 사용 안함으로 설정합니다. 서비스 역할은 관리자 역할과 거의 동일한 권한 부여 지점까지 운영자보다 큰 권한을 가집니다.

조사 용도로 라이브러리 활동의 내역이 필요한 경우 "Activity Log"를 검토하고 추가 분석을 위해 내보낼 수 있습니다. 사용자 인터페이스의 Activity Log는 사용자 로그인, 호스트 또는 추적을 위한 UI 시작 작업을 표시할 수 있습니다.

4

재배치

이 절에서는 고객 데이터를 지우기 위해 라이브러리를 출하 시 기본 상태로 되돌리는 방법에 대해 설명합니다.

고객이 라이브러리를 폐기해야 하는 경우 모든 고객 구성 정보 및 모든 로그 파일을 제거하고 라이브러리를 출하 시 기본 상태로 되돌리는 절차가 제공됩니다. 이 절차는 라이브러리를 "locate" 모드로 전환한 다음 전면과 후면의 위치 버튼을 10초 이상 동시에 눌렀다 놓으면 호출됩니다.

위치 버튼을 눌렀다 놓는 데 필요한 시간은 LED 표시등 깜빡임 속도(느림-빠름)가 변하는 것으로 알 수 있습니다.

부록 A

보안 배치 점검 목록

다음 보안 점검 목록에는 라이브러리를 보호하는 데 도움이 되는 지침이 포함되어 있습니다.

1. 모든 사용자 계정에 대한 암호 관리를 적용합니다.
2. 액세스 제어, 물리적 근접성과 SCSI, UI, SNMP 등의 통과 인터페이스를 모두 적용합니다.
3. 네트워크 액세스를 제한합니다.
 - a. 방화벽을 구현해야 합니다.
 - b. 방화벽이 손상되어서는 안 됩니다.
 - c. 시스템 액세스를 모니터링해야 합니다.
 - d. 네트워크 IP 주소를 확인해야 합니다.
 - e. 서비스에 적절한 암호 또는 모니터링 액세스 제어가 필요한 도구가 있을 수 있습니다 (예: 로그 정보의 자동 다운로드 또는 기타 액세스를 허용하는 SDP-2).
4. Oracle 테이프 라이브러리에서 취약점이 발견되면 Oracle 서비스, Oracle 테이프 라이브러리 엔지니어링 또는 계정 담당자에게 문의합니다.
5. SMTP는 SSL 또는 none과 같은 덜 중요한 프로토콜 대신 TLS를 사용해야 합니다.
6. SNMP는 V2C 또는 덜 중요한 기능 대신 V3 레벨로 설정되어야 합니다.

부록 B

참조

SL150 사용 설명서 위치:

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

SL150과 관련된 모든 설명서는 부품 번호가 E35103-07인 온라인 문서 세트에서 찾을 수 있습니다.

