

StorageTek T10000D

보안 설명서

E50323-04

2016년 8월

StorageTek T1000D

보안 설명서

E50323-04

Copyright © 2014, 2016, 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
T10000D 용량 및 성능	9
보안	9
일반 보안 원칙	9
소프트웨어를 최신 상태로 유지	9
네트워크 액세스 제한	10
최신 보안 정보 유지	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
테이프 드라이브 보안	11
VOP(Virtual Operator Panel) 응용 프로그램 설치	12
설치 후 구성	12
사용자(관리자) 암호 지정	12
암호 관리 적용	12
3. 보안 기능	15
A. 보안 배치 점검 목록	17
B. 참조	19

표 목 록

2.1. 사용되는 네트워크 포트	11
-------------------------	----

머리말

이 문서에서는 Oracle StorageTek T10000D의 보안 기능에 대해 설명합니다.

대상

이 설명서는 StorageTek T10000D의 보안 설치/구성 및 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.

1장. 개요

이 절에서는 StorageTek T10000D 테이프 드라이브의 개요를 살펴보고, 테이프 드라이브 보안의 일반적인 원칙에 대해 설명합니다.

제품 개요

T10000D 엔터프라이즈 테이프 드라이브는 광 섬유 채널 프로토콜을 통해 개방형 시스템 SCSI에 연결되고 FICON 프로토콜을 통해 메인프레임에 연결됩니다. T10000D 테이프 드라이브는 호스트와 데이터를 주고 받으며 이동식 자기 매체에 데이터를 저장합니다. T10000D 테이프 드라이브는 주로 사용률이 높고 안정성이 필요한 엔터프라이즈 고객에 매우 안정적인 고용량 백업, 아카이브 및 데이터 처리 기능을 제공하는 데 사용됩니다. 이 제품은 데이터 암호화를 선택사항으로 제공합니다. 고객은 필요에 따라 암호화 기능을 사용으로 설정할 수 있습니다. 테이프 드라이브 제품의 용량 및 고유 테이프 속도가 향상되었습니다. 또한 데이터 관리 기능도 추가되었습니다.

T10000D 용량 및 성능

T10000D 테이프 드라이브는 최대 8.5TB 용량 및 초당 252MB 고유 테이프 속도를 제공합니다.

보안

T10000D 테이프 드라이브는 제어된 하드웨어 환경에서 사용하도록 설계되고 문서화되었습니다. 테이프 드라이브는 항상 제어된 데이터 센터 내부에 있으며 대개 테이프 라이브러리 내부에 배치됩니다. 드물게 고객이 랙 마운트 버전을 사용하는 경우도 있습니다. 제어된 데이터 센터는 또한 고객의 자체 보안 정책에 의해 보호되는 방화벽 내부에 있습니다. 따라서 인터넷 전반 및 테이프 드라이브를 운영하는 내부 엔티티 모두로부터 테이프 드라이브가 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. 이 문서 전체에서 다음 소프트웨어 레벨이라고 가정합니다.

T10000D 4.XX.1XX

네트워크 액세스 제한

테이프 드라이브를 데이터 센터 방화벽으로 보호합니다. 방화벽으로 보호하면 시스템에 대한 액세스가 필요한 경우 모니터링하고 제한할 수 있는 알려진 네트워크 경로로 제한됩니다. 또는 방화벽 라우터가 여러 개의 독립된 방화벽을 대체할 수 있습니다. 테이프 드라이브에 대한 연결이 허용되는 호스트를 식별하고 가능한 한 다른 모든 호스트를 차단하는 것이 권장됩니다.

최신 보안 정보 유지

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

2장. 보안 설치

이 절에서는 보안 설치 및 구성에 대한 계획 및 구현 프로세스의 개요를 살펴보고, 권장되는 몇 가지 시스템 배치 토폴로지에 대해 설명하고, 테이프 라이브러리를 보호하는 방법을 살펴봅니다.

사용자 환경 이해

보안 요구사항을 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?

테이프 드라이브는 인터넷의 모든 사용자로부터 보호되어야 합니다. 테이프 드라이브를 회사의 인트라넷에 있는 직원들로부터 보호해야 할지도 고려해야 합니다.

전략적 리소스에 대한 보호를 실패할 경우 어떤 일이 발생합니까?

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

테이프 드라이브 보안

기본적으로 테이프 드라이브는 다음 표에 나열된 포트를 사용합니다. 이러한 포트를 사용하는 트래픽은 허용하고 사용되지 않는 포트는 차단되도록 방화벽을 구성해야 합니다. 테이프 드라이브는 IPv6 및 IPv4를 지원합니다.

표 2.1. 사용되는 네트워크 포트

포트	T1000D
22 tcp - SSH VOP	X
22 tcp - SFTP	X

포트	T10000D
161 udp - SNMPV1 테이프 드라이브 에이전트 요청 - 인바운드 Stateful	X
162 udp - SNMPV1 테이프 드라이브 트랩 및 정보 알림 - 트랩의 경우 아웃바운드 Stateless, 정보의 경우 아웃바운드 Stateful	X
23 tcp - TELNET	
21 tcp - FTP	
9842 tcp - EPT	
3331 OKM - 챌린지 및 루트 CA 서비스	X
3332 OKM - 등록. Cyber strength(사이버 강도): AES256	X
3334 OKM - 암호화 키 교환. Cyber strength(사이버 강도): AES256	X
3335 OKM - 클러스터 검색. Cyber strength(사이버 강도): AES256	X

T10000D 고객의 경우 포트 21 및 23이 사용 안함으로 설정됩니다. 고객이 비보안 TELNET 또는 비보안 FTP(또는 둘 다)에 액세스하려면 VOP 구성 옵션을 사용할 수 있습니다.

VOP(Virtual Operator Panel) 응용 프로그램 설치

VOP는 테이프 드라이브와 동일한 보호된 네트워크 기반구조 내부에 있는 시스템에 설치되어야 합니다. VOP가 설치된 시스템에서는 테이프 드라이브에 대한 액세스가 제한되도록 고객 액세스 제어를 적용해야 합니다. VOP에서 사용하는 포트는 표 2.1. “사용되는 네트워크 포트”를 참조하십시오.

웹 실행 VOP 설치 지침은 다음 VOP 사용 설명서를 참조하십시오.

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

설치 후 구성

이 절에서는 설치 후 수행해야 하는 보안 구성 변경사항에 대해 설명합니다.

사용자(관리자) 암호 지정

고객 관리자 계정 암호는 고객이 소유하며 사이트에서 고객이 변경해야 합니다. 암호 보안은 Oracle 표준을 준수합니다. 테이프 드라이브의 수명 중 개수에 제한 없이 암호를 사용할 수 있습니다. 관리자 암호를 잊은 경우 재설정할 수 있습니다. 첫번째 암호는 테이프 드라이브와 함께 제공되는 기본 암호입니다.

암호 관리 적용

관리자 암호에는 암호 길이, 복잡성 등의 기본 암호 관리 규칙이 적용되어야 합니다.

암호 관리 규칙에 따르면 다음 각 규칙에 해당하는 항목이 하나 이상 있어야 합니다.

-
- 8자에서 16자 사이여야 합니다.
 - 소문자(a-z)
 - 대문자(A-Z)
 - 10진수(0-9)
 - 특수 문자(.,;:"{}[]!@#\$%&, ...)

3장. 보안 기능

이 절에서는 제품에서 제공하는 구체적인 보안 메커니즘의 개요를 살펴봅니다.

T10000D 테이프 드라이브는 보안 채널을 사용하여 Oracle Key Management System과 통신합니다. T10000D는 SSH 및 SFTP를 통해 Virtual Operator Panel과 통신하고 고객을 위해 TELNET 및 FTP가 사용 안함으로 설정됩니다. 이것이 테이프 드라이브를 보호하기 위한 보안의 전부는 아닙니다. 테이프 드라이브는 해당 기능을 사용하는 서버에만 액세스를 허용하는 보안된 네트워크 상의 물리적으로 보안된 데이터 센터에 두는 것이 권장됩니다. 라이브러리에서 실행되는 서버 및 응용 프로그램도 보안되어야 합니다. 또한 고객은 테이프 드라이브의 보안을 다른 레벨로 승격할 수 있습니다. 옵션 중 하나는 데이터를 암호화하는 것입니다.

부록 A

부록 A. 보안 배치 점검 목록

다음 보안 점검 목록에는 테이프 드라이브를 보안하는 데 도움이 되는 지침이 포함되어 있습니다.

1. 암호 관리를 적용합니다.
2. 액세스 제어를 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.
4. Oracle 테이프 드라이브에서 취약점이 발견되면 Oracle 서비스, Oracle 테이프 라이브러리 엔지니어링 또는 계정 담당자에게 문의합니다.

부록 B

부록 B. 참조

다음에서 VOP 사용 설명서에 액세스할 수 있습니다.

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