

StorageTek Linear Tape File System, Library Edition

보안 설명서

릴리스 1

E40932-02

2016년 7월

StorageTek Linear Tape File System, Library Edition

보안 설명서

E40932-02

Copyright © 2013, 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	5
대상	5
설명서 접근성	5
1. 개요	7
제품 개요	7
보안	7
물리적	7
네트워크	8
사용자 액세스	8
일반 보안 원칙	8
소프트웨어를 최신 상태로 유지	8
네트워크 액세스 제한	8
최신 보안 정보 유지	8
2. 보안 설치	9
사용자 환경 이해	9
어떤 리소스를 보호해야 합니까?	9
누구로부터 리소스를 보호합니까?	9
전략적 리소스에 대한 보호를 실패할 경우 어떤 일이 발생합니까?	9
LTFS-LE(Linear Tape File System – Library Edition) 설치	9
설치 후 구성	9
사용자(관리자) 암호 지정	10
암호 관리 적용	10
3. 보안 기능	11
A. 보안 배치 점검 목록	13
B. 참조	15

머리말

이 문서에서는 Oracle StorageTek Linear Tape File System, Library Edition(LTFS-LE)의 보안 기능에 대해 설명합니다.

대상

이 설명서는 LTFS-LE의 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 LTFS-LE의 개요를 살펴보고 해당 보안의 일반적인 원칙에 대해 설명합니다.

제품 개요

오늘날 고객이 사용 가능성 및 성능 문제를 해결하기 위해 니어라인 스토리지에 사용할 수 있는 효율적인 스토리지 플랫폼을 요구하고 있는 상황에서, 테이프 스토리지는 백업 및 아카이브 시장에 완전히 자리를 내어주는 위기에 직면하고 있습니다. 디스크 공급업체의 이러한 공격을 저지하기 위해 StorageTek과 Sun의 엔지니어들이 선구적으로 기초 작업을 수행한 결과 2010년 마침내 단일 테이프 드라이브용 LTFS(Linear Tape File System)가 출시되었습니다. IBM과 LTO 컨소시엄에 의한 개방형 소스 사양으로 처음 릴리스된 LTFS를 사용하면 하나의 드라이브를 썸 드라이브 또는 메모리 스틱으로 처리할 수 있습니다. 이러한 기능을 통해 테이프 스토리지 사용이 훨씬 더 쉬워졌습니다. 또한 휴대용 스토리지가 필요한 산업에서 이제 비용 효율적인 스토리지 플랫폼을 사용할 수 있으므로 테이프의 가치를 증가시킬 수 있는 새로운 가능성이 열렸습니다.

Oracle에서는 T10000C 테이프 드라이브에 이 사양을 채택했습니다. 하지만 고객에도 Oracle에도 단일 드라이브용 LTFS만으로는 부족합니다. LTFS를 전체 라이브러리로 확장하면 고객이 실질적으로 수천 개의 썸 드라이브를 사용할 수 있습니다. 고객은 기본적인 데스크탑 탐색기 인터페이스를 통해 페타바이트의 데이터를 관리할 수 있습니다. 이렇게 되면 테이프를 사용하기 쉬워질 뿐만 아니라 사용자의 모든 콘텐츠가 개방형 형식으로 작성되므로 안심하고 사용할 수 있습니다. 고객은 더 이상 백업 응용 프로그램 또는 독점적인 형식에 얽매이지 않아도 됩니다. 또한 휴대성도 현저하게 개선되었습니다. 마지막으로 LTFS-LE(LTFS – Library Edition)는 간단한 단일 액세스 지점을 제공하므로 향후 Oracle 응용 프로그램 또는 미들웨어에서 테이프를 스토리지 형식으로 사용할 수 있습니다.

보안

LTFS-LE 보안에는 물리적, 네트워크 및 사용자 액세스라는 3가지 측면이 있습니다.

물리적

LTFS-LE는 조직의 데이터 센터 내부에 있는 독립형 서버에 설치되어야 합니다. 서버에 대한 물리적 액세스는 고객 회사 정책을 따릅니다.

네트워크

LTFS-LE는 고객의 내부 방화벽으로 보호된 네트워크에 추가되거나 구성되어야 합니다. 이러한 네트워크에는 데이터가 액세스되는 라이브러리에 대한 SSH 및 SNMP 액세스가 필요합니다.

사용자 액세스

LTFS-LE 응용 프로그램 액세스는 사용자 이름 및 암호 인증에 의해 제어됩니다. 이러한 사항은 고객의 초기 설치 중 설정됩니다. 암호는 Oracle 표준 요구 사항을 충족해야 합니다.

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 문서는 다음 소프트웨어 레벨에 적용됩니다.

LTFS-LE 릴리스 1.0 이상

주:

라이브러리, 라이브러리 소프트웨어 및 드라이브도 LTFS-LE 응용 프로그램에 연결된 최소 펌웨어 버전 레벨을 충족해야 합니다. 이러한 펌웨어 레벨은 LTFS-LE 릴리스 노트에 지정되어 있습니다.

네트워크 액세스 제한

LTFS-LE 호스트 서버를 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. 라이브러리에 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 계획 프로세스의 개요를 살펴보고 권장되는 몇 가지 시스템 배치 토폴로지에 대해 설명합니다. 여기서는 LTFS-LE 응용 프로그램의 설치, 구성 및 관리에 대해 상세하게 설명하지 않습니다. 설치, 구성 및 관리는 LTFS-LE Installation and Administration Guide 1.0에서 설명합니다.

사용자 환경 이해

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

어떤 리소스를 보호해야 합니까?

LTFS-LE의 경우 허용되지 않은 액세스로부터 호스트 서버 및 연관된 네트워크를 보호해야 합니다.

누구로부터 리소스를 보호합니까?

LTFS-LE는 인터넷의 모든 사용자, 외부 사용자 및 허용되지 않은 내부 사용자로부터 보호되어야 합니다.

전략적 리소스에 대한 보호를 실패할 경우 어떤 일이 발생합니까?

허용되지 않은 사용자가 LTFS-LE에 악의적으로 액세스하여 테이프 스토리지의 데이터를 손상시킬 수 있습니다.

LTFS-LE(Linear Tape File System – Library Edition) 설치

LTFS-LE는 모니터링되는 장치와 동일한 보호된(방화벽 설치) 기반구조 내부에 있는 시스템에 설치되어야 합니다. LTFS-LE가 설치된 시스템에서는 응용 프로그램에 대한 액세스가 제한되도록 고객 액세스 제어를 적용해야 합니다.

설치 지침은 다음 LTFS-LE 사용 설명서를 참조하십시오.

Oracle LTFS-LE Planning and Installation

설치 후 구성

설치 후 구성 보안 변경 사항은 없습니다. 구성은 설치 중 고객에 의해 설정됩니다.

사용자(관리자) 암호 지정

고객 관리 계정 암호는 설치 중 고객에 의해 설정됩니다.

암호 관리 적용

관리자 암호에는 암호 길이, 내역, 복잡성 등의 고객 회사 암호 관리 규칙이 적용되어야 합니다.

3장. 보안 기능

이 절에서는 제품에서 제공하는 구체적인 보안 메커니즘의 개요를 살펴봅니다.

LTFS-LE 응용 프로그램에서는 사용자에게 암호화된 암호 역할을 제공합니다. 이것이 응용 프로그램을 보호하기 위한 보안의 전부는 아닙니다. 응용 프로그램은 권한이 부여된 사용자에게만 액세스를 허용하는 보안된 네트워크의 물리적으로 안전한 데이터 센터에 있어야 합니다.

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. LTFS-LE 또는 Oracle 테이프 라이브러리에서 의심되는 취약점이 발견되면 Oracle 서비스, Oracle 테이프 라이브러리 엔지니어링 또는 계정 담당자에게 문의합니다.

부록 B

부록 B. 참조

Oracle LTFS-LE Planning and Installation

