StorageTek Enterprise Library Software

보안 설명서

E63469-01

2015년 3월

ORACLE

StorageTek Enterprise Library Software
보안 설명서

E63469-01

차례

머리말

이 문서는 Oracle StorageTek ELS(Enterprise Library Software)의 보안 기능에 대해 설명합니다.

대상

이 설명서는 StorageTek ELS(Enterprise Library Software)의 보안 설치와 구성 및 보안 기능과 관련이 있는 모든 사람을 대상으로 합니다.

설명서 접근성

오라클의 접근성 개선 노력에 대한 자세한 내용은 http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc에서 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=info를 참조하거나, 청각 장애가 있는 경우 http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs를 방문하십시오.

1

개요

이 절에서는 ELS 소프트웨어 제품군의 개요를 살펴보고 응용 프로그램 보안의 일반적인 원칙에 대해 설명합니다.

1.1. 제품 개요

ELS는 다음 플랫폼에 대해 Oracle StorageTek 메인프레임 테이프 환경의 테이프 자동화를 지원합니다.

- IBM z/OS플랫폼. ELS는 TCP/IP 클라이언트/서버 테이프 자동화 구조를 지원하므로 하나의 z/OS LPAR에서 실행 중인 SMC 클라이언트 소프트웨어가 다른 z/OS LPAR에서 실행 중인 HSC/VTCS 서버 소프트웨어와 통신할 수 있습니다.
- IBM z/VM 플랫폼. z/VM 시스템용 ELS VM 클라이언트 소프트웨어는 z/OS LPAR에서 실행 중인 HSC/VTCS 서버 소프트웨어와 통신하여 z/VM에 대한 가상 및 실제 테이프 처리를 자동화합니다.
- Fujitsu MSP/EX 플랫폼. SMC는 테이프 처리가 발생하는 모든 호스트에서 실행되어야 합니다. ELS 서버 구성 요소(HSC/VTCS)는 SMC와 동일한 MSP/EX 호스트에서도 실행될 수 있고, 별도의 원격 호스트에서도 실행될 수 있습니다. SMC와 HSC/VTCS가 서로 다른 MSP/EX 호스트에 있는 경우 TCP/IP를 사용하여 클라이언트 호스트에서 서버 호스트로 요청이 전송됩니다. 원격 SMC 클라이언트에서 HTTP 요청을 받으려면 서버 호스트에서 실행 중인 SMC에서 HTTP 구성 요소를 활성화해야 합니다.

ELS 클라이언트/서버 통신은 가상 및 물리적 테이프 볼륨에 대해 제어 경로 요청(주로 마운트/마운트 해제 요청)을 실행하는 데 사용됩니다. 이러한 제어 경로 요청에 포함된 정보는 TapePlex 구성 및 정책 정보, 가상/물리적 테이프 전송 단위 주소 및 가상/물리적 테이프 볼륨 일련 번호로 구성됩니다. ELS 클라이언트/서버 통신은 고객 데이터를 전혀 포함하고 있지 않으며, 항상 호스트 LPAR을 Oracle StorageTek 테이프 전송 또는 VSM 가상 테이프 장치로 연결하는 IBM FICON/ESCON 데이터 경로 인터페이스를 통해 이동합니다.

이 보안 설명서의 정보는 모든 ELS 릴리스에 적용됩니다. 이 설명서의 파트 3에서 설명되었듯이 보호가 필요한 경우 ELS 클라이언트/서버 제어 경로 통신을 보안할 수 있습니다. 이 문서는 다양한 ELS 설치 및 사후 설치 작업의 보안 측면에 대해서도 설명합니다.

1.2. 일반 보안 원칙

다음 원칙은 제품을 안전하게 사용하는 데 반드시 필요한 사항입니다.

1.2.1. 소프트웨어를 최신 상태로 유지

올바른 보안 실행 원칙 중 하나는 모든 소프트웨어 버전 및 패치를 최신 상태로 유지하는 것입니다. 최신 ELS 누적 유지 관리 번들과 개별 PTF 및 HOLDDATA는 모두 MOS(My Oracle Support)에서 제공됩니다. 누적 유지 관리 번들은 최신 ELS 월별 회귀 테스트 주기에서 발생하는 모든 PTF를 포함하도록 매월 업데이트됩니다. 누적 번들의 모든 PTF는 하나의 완전한 패키지로 함께 테스트되었습니다. HIPER PTF 전자 메일 통지는 ELS 제품에 대한 MOS Hot Topics Alert 문서에 가입하면 제공됩니다. 고객은 현재 유지 관리 레벨을 지키고, HOLDDATA를 최신 상태로 유지하고, Hot Topics Alert에 가입하여 HIPER 통지를 받도록 권장됩니다.

1.2.2. 네트워크 액세스 제한

성능 및 보안을 위해 ELS 제어 경로 통신을 방화벽 뒤의 격리된 네트워크로 경로를 지정합니다. 방화벽을 사용하면 ELS 시스템에 대한 액세스가 필요한 경우 모니터하고 제한할 수 있는 알려진 네트워크로 제한됩니다. ELS 클라이언트/서버 통신에 전용 네트워크를 사용하면 다른 응용 프로그램과의 네트워크 경합이 없어지고 테이프 시스템 성능이 개선됩니다.

1.2.3. 최신 보안 정보 적용

오라클은 지속적으로 소프트웨어 및 설명서를 개선하고 있습니다. 이 보안 설명서 및 다른 모든 ELS 제품 설명서에 개정된 내용이 있는지 정기적으로 확인하십시오. 이 문서에 참조된 모든 ELS 설명서는 Oracle Technical Network의 Tape Storage Products 섹션에서 확인할 수 있습니다.

2

보안 설치

IBM z/OS SAF(System Authorization Facility)는 ELS 보안 사항 대부분에 대해 필수적인 보호 기능을 제공합니다. SAF는 대개 IBM RACF 패키지 또는 이에 상응하는 패키지로 구현됩니다. 이 절에서는 RACF 기반 SAF 환경을 사용하여 보안 ELS를 설치 및 구성하는 방법에 대해 간략히 설명합니다.

2.1. ELS 설치

오라클 문서 *StorageTek Enterprise Library Software: Installing ELS*에서는 RACF 보호를 사용하여 사용자 버전의 ELS를 설치 및 구성하는 방법에 대해 설명합니다. 다음 보안 관련 설치 항목에 대한 자세한 내용은 이 문서를 참조하십시오.

- 기본 소프트웨어 및 최신 누적 유지 관리 번들 설치
- ELS 로드 라이브러리 APF 권한 부여
- HSC User Exit 라이브러리 APF 권한 부여
- SMC JES3 로드 라이브러리 APF 권한 부여

2.2. ELS 사후 설치 구성

다음 오라클 문서는 사용자 버전의 ELS에 대한 사후 설치 구성 작업에 대해 설명합니다.

- *StorageTek Enterprise Library Software: Configuring HSC and VTCS*
- *StorageTek Enterprise Library Software: Configuring and Managing SMC*
- *StorageTek Enterprise Library Software: ELS Programming Reference*

다음 보안 관련 사후 설치 항목에 대한 자세한 내용은 이 문서를 참조하십시오.

- CDS 데이터 세트 보안에 대한 RACF 보호 정의
- HSC User Exit SLSUX15를 사용하여 명령 권한 및 프로그램 인터페이스 권한 정의
- HSC User Exit SLSUX14를 사용하여 볼륨 마운트 및 꺼내기에 대한 볼륨 액세스 권한 정의
- MVC 풀 및 스크래치 하위 풀 volser 권한 정의
- 원격 HSC 부속 시스템과 통신하기 위한 SMC OMVS RACF 세그먼트 정의
- VLE 어플라이언스와 통신하기 위한 SMC OMVS RACF 세그먼트 정의

3

보안 기능

이 장에서는 ELS에서 제공하는 구체적인 보안 메커니즘을 설명합니다.

3.1. AT-TLS를 사용한 ELS 보안 - z/OS만 해당

IBM z/OS AT-TLS(Application Transparent Transport Layer Security) 기능에서는 SSL 데이터 암호화를 사용하여 z/OS TCP/IP 응용 프로그램을 보안합니다. AT-TLS에 대한 자세한 내용은 *IBM publication z/OS Communications Server: IP Configuration Guide* 및 *IBM publication z/OS Communications Server: IP Configuration Reference*의 AT-TLS 정책 에이전트 정보를 참조하십시오.

SMC와 HSC/VTCS 간 ELS 클라이언트/서버 통신 보안은 오라클 백서 *Using AT-TLS with HSC/SMC Client/Server z/OS Solution: Implementation Example*에 설명되어 있습니다. 이 백서는 Oracle Technical Network의 Tape Storage Products 섹션에 게시되어 있습니다. 자세한 구성 정보는 이 게시물을 참조하십시오.

오라클에서는 AT-TLS로 ELS를 보안할 때 다음 SSL 암호화 알고리즘 중 하나를 사용하도록 권장합니다.

- SHA-2 유형(SHA-256, SHA-384, SHA-512)
- AES >= 128비트
- RSA >= 2048비트
- DH(Diffie-Hellman) >= 2048비트
- ECC >= 256비트

다른 모든 SSL 암호화 알고리즘은 보호 수준이 낮으므로 ELS에서 사용하지 않아야 합니다.

주:

VSM에 대한 StorageTek VLE(Virtual Library Extension) 어플라이언스는 현재 AT-TLS 통신을 지원하지 않습니다. AT-TLS를 사용하여 ELS VLE 통신을 보안하지 마십시오.

3.2. ELS XAPI 보안 기능 사용

ELS 7.3에서는 클라이언트 서버 간 통신에 새로운 XAPI 보안 기능이 도입되었습니다. 이 기능은 SMC HTTP에서 기본적으로 사용으로 설정됩니다. XAPI 보안 기능은 XAPI 프로토콜의 일부로 추가적인 사용자 인증 기능을 제공합니다. 이 기능은 ELS에 완전히 포함된 ELS 내부 기능입니다. XAPI 보안 기능을 사용하려면 ELS 클라이언트 및 서버에 대한 보안 자격 증명(사용자 ID 및 암호)을 정의해야 합니다. ELS 7.3 TapePlex 작업은 이 보안 자격

증명을 사용하여 XAPI 트랜잭션(마운트, 마운트 해제, 볼륨 조회, 스크래치 등)을 보안합니다. XAPI 보안 자격 증명 사용은 완전히 투명하며, 추가적인 사용자 또는 운영자 개입이 필요하지 않습니다. XAPI 보안 기능 구성에 대한 자세한 내용은 *Configuring and Managing SMC 7.3*을 참조하십시오.

ELS 클라이언트 응용 프로그램(SMC 및 VM 클라이언트)만 호스트하는 TapePlex에 대해 XAPI 트랜잭션을 보안하는 가장 좋은 방법은 3.1절. “AT-TLS를 사용한 ELS 보안 - z/OS만 해당”에 설명된 대로 AT/TLS 기능을 사용하는 것입니다. AT/TLS는 ELS 외부에 있으며 ELS에 투명한 전송 계층 기능입니다.

ELS 이외의 클라이언트(개방형 시스템 클라이언트) 또는 ELS 클라이언트(SMC 및 VM 클라이언트)와 ELS 이외 클라이언트의 조합을 호스트하는 TapePlex를 보안하려면 ELS 7.3 XAPI 보안 기능을 사용하십시오. 이러한 환경에서 ELS 7.3 XAPI 보안 기능에 추가하여 AT-TLS를 사용할 수는 있지만 AT-TLS는 ELS 이외의 클라이언트에 대해 XAPI 트랜잭션을 보안하지 않습니다.

4

개발자용 보안 고려 사항

오라클 문서 *StorageTek Enterprise Library Software: ELS Programming Reference*에서는 응용 프로그램 개발자가 사용할 수 있는 ELS API에 대해 설명합니다. ELS에 대한 프로그램 인터페이스는 UUI(Unified User Interface)를 사용하는데, 이 인터페이스는 HSC 명령 보안 출구 SLSUX15를 통해 RACF 권한 부여(또는 이와 동등한 권한 부여)를 기준으로 해당 함수에 대한 액세스를 관리합니다. RACF로 SLSUX15를 보안하는 방법은 2.2절. “ELS 사후 설치 구성”을 참조하십시오.

부록 A

보안 배치 점검 목록

1. 이 보안 설명서에 설명된 대로 RACF 보호(또는 이와 동일한 기능)를 사용합니다.
2. 네트워크 액세스를 제한합니다. ELS 및 ELS에서 관리하는 테이프 라이브러리를 회사 방화벽 뒤에 두어야 합니다.
3. 필요한 경우 IBM AT-TLS 기능 또는 ELS XAPI 보안 기능을 사용하여 ELS 네트워크 트래픽을 보안합니다.
4. 모든 ELS PTF 및 HOLDDATA를 적용합니다.
5. Oracle ELS 소프트웨어에 취약점이 발견된 경우 오라클 소프트웨어 지원 센터 (http://www.myoraclesupport.com/)로 문의하십시오.

부록 B

참조

ELS 설명서는 ELS 릴리스별로 구성된 라이브러리에 저장됩니다. Tape Storage Documentation 페이지에서 액세스할 수 있습니다.

http://www.oracle.com/technetwork/documentation/tape-storage-curr-187744.html