

클라우드 서비스

Thermo Scientific SampleManager LIMS 소프트웨어의 AWS 내 배포

개요

Thermo Scientific™ SampleManager LIMS™ 소프트웨어는 온 프레미스 또는 Amazon Web Services(AWS) 클라우드에 배포할 수 있습니다. 온 프레미스 배포 또는 고객의 자체 클라우드 호스팅 서비스 배포는 고객의 인프라 표준에 기초하여 고객이 관리합니다.

AWS에서 클라우드 배포를 관리하기 위해 Thermo Fisher Scientific과 계약한 고객은 엔드-투-엔드(end-to-end) 지원을 받습니다. Thermo Fisher에서 클라우드 서비스를 공급하고 SampleManager LIMS 소프트웨어를 설치하며 배포를 유지 관리합니다.

다음은 SampleManager LIMS 소프트웨어를 AWS에 배포함으로써 확보할 수 있는 몇 가지 기능 및 이점입니다.

- 선택된 AWS 지역 내에서 전세계적으로 사용할 수 있는 완전 관리형 배포.
- AWS 데이터 센터 및 네트워크에 대한 물리적 액세스는 엄격하게 제어, 모니터링 및 감사됩니다.
- 다단계 인증이 - 신분 및 액세스 관리(IAM) 그리고 세분화된 권한과 함께 - 인프라에 액세스하는 데 사용됩니다.
- 데이터는 전용 서버와 논리적으로 독립된 네트워크로 분리됩니다.

- 데이터는 이동 중 및 저장되지 않은 상태에서 산업 표준 암호화를 통해 보호됩니다.
- 방화벽 및 정책/절차 수준에서 엄격한 제어를 통해 무단 액세스 또는 손상으로부터 데이터를 보호합니다.
- 데이터는 30일 슬라이딩 윈도우에 백업 및 보관됩니다.
- 시스템은 하드웨어 장애의 통합 자동 복구 기능에 의해 관리됩니다.
- 99.5% 서비스 가용성(고가용성 옵션과 함께 99.9% 가동 시간).
- 실시간 침입 감지 및 방지.
- 인프라와 사용자 활동 로깅 및 모니터링.
- 24시간 RTO(목표 복구 시간).
- 24시간 RPO(목표 복구 지점).

다음 섹션에서는 SampleManager LIMS 소프트웨어에 적용되는 보안 정책 및 절차의 개요가 제공됩니다. AWS에 의해 제공되는 보안에 대한 정보는 AWS 클라우드 보안 사이트를 참조하십시오.

설비 보안

SampleManager LIMS 소프트웨어 배포는 모든 고객 시스템에 대해 AWS를 활용합니다. Thermo Fisher 사무소 현장에 위치하는 시스템은 없습니다. Thermo Fisher 설비에 대한 접근은 엄격하게 통제됩니다.

시스템 보안

SampleManager LIMS 소프트웨어 고객 시스템은 AWS 클라우드 보안 사이트에 설명되어 있는 보안 정책에 의거하여 AWS에 배포 및 관리됩니다. 시스템 (기업 및 고객)에 대한 액세스는 통제되며 특정 직원으로 제한됩니다. Thermo Fisher의 기술 운영 팀에서는 다단계 인증을 통해 시스템에 대한 액세스를 보호합니다.

네트워크 보안

고객 시스템은 전용 VPC(가상 사설 클라우드)에서 구성 및 관리됩니다. VPC는 외부 세계와 관리형 인스턴스 간, 그리고 내부적으로 인프라 구성 요소 간의 모든 네트워크 상호 작용을 세밀하게 제어하고 모니터링합니다. 데이터 흐름 방식과 시스템 액세스 권한에 대한 모든 규칙을 정의하는 보안 정책이 각 고객에 대해 구현됩니다.

SampleManager LIMS 소프트웨어가 호스팅되는 네트워크는 침입 감지 및 방지 시스템에 의해 보호됩니다. 활발한 모니터링과 침입 감지 및 방지를 통해 높은 수준의 보안을 제공합니다. IDS는 감지된 악의적인 활동에 대해 담당 직원에게 경고하고, IDS 서명을 자동으로 업데이트하도록 구성됩니다.

SampleManager LIMS 소프트웨어에는 SampleManager LIMS 소프트웨어 네트워크에 액세스하기 위한 고도로 제어되는 전용 VPN(가상 사설 네트워크)이 있습니다. VPN은 직원 전용이며 적절한 사용을 위해 활발하게 모니터링됩니다.

데이터 보안

SampleManager LIMS 소프트웨어는 산업 표준 AES-256 암호화 알고리즘을 사용하여 저장되는 데이터를 암호화합니다. 데이터베이스 또는 파일 시스템 상의 모든 데이터는 암호화됩니다.

SampleManager LIMS 소프트웨어는 전송 중인 데이터를 암호화하고, 관리형 인스턴스와의 모든 통신은 2048비트 공개 키와 함께 산업 표준 256비트 암호화를 사용하여 안전하게 보호되도록 합니다. 고객 데이터베이스에 저장되어 있는 데이터에 대한 직접 액세스는 제한됩니다.

애플리케이션 액세스

SampleManager LIMS 소프트웨어는 강력한 AAA(Authentication, Authorization, and Accounting) 기능을 제공합니다. 고객에게는 구체적인 요구 사항에 따라 AAA 정책을 설정할 수 있는 기능이 제공됩니다. Thermo Fisher는 최고 수준의 보안을 제공하는 AAA 정책을 사용할 것을 권장합니다.

SampleManager LIMS 소프트웨어 고객에게는, IP 제한에 의해 애플리케이션 인스턴스에 대한 액세스를 제한하거나 인터넷에서의 액세스를 허용하는 옵션이 제공됩니다.

안전한 코딩 관행

SampleManager LIMS 소프트웨어는 OWASP(오픈 웹 애플리케이션 보안 프로젝트)에서 규정하고 있는 모범 사례에 기초한 보안 코딩 사례를 활용합니다.

SampleManager LIMS 소프트웨어는 도구를 활용하여 코드의 보안성을 평가하고 코드 검토의 일부로 보안 코딩 감사 기능을 채택합니다.

로깅

SampleManager LIMS 소프트웨어는 성공 및 실패한 사용자 인증 시도를 포함한 사용자 활동에 더해 IT 인프라 활동을 기록하는 로그 관리 시스템을 활용합니다. 기록된 활동을 검토하고 의심스러운 활동이 감지되었을 때 기술 운영 팀에 경고하는 데 로그 관리 시스템이 사용됩니다. 로그 데이터는 최대 1년 동안 보관됩니다.

모니터링

Thermo Fisher 소프트웨어는 여러 가지 상용 도구를 사용하여 모든 시스템, 네트워크, 애플리케이션 및 지원 인프라를 활발하게 모니터링합니다. AWS CloudWatch, AWS GuardDuty, AWS CloudTrail, 침입 방지/감지 서비스, 클라우드 거버넌스 및 경고 도구는 관리형 서비스의 보안 및 상태를 모니터링 및 로깅하고 기술 운영팀 구성원에게 경고하는 데 사용됩니다.

기술 운영 팀에서는 SampleManager LIMS 소프트웨어에 대한 취약성 평가를 수행합니다. Thermo Fisher의 기업 정보 보안(CIS) 프로그램은, Thermo Fisher에서 관리하는 SampleManager LIMS 소프트웨어의 클라우드 배포를 위한 보안 제어에 대해 지침, 감독 및 지속적인 검토와 개선을 제공합니다.

변화 관리

Thermo Fisher에서는 변경 관리 정책을 사용하여 시스템 및 인프라에 대한 변경 사항을 기록합니다. 변경 사항은 위험을 완화하기 위해 검토되고 회계를 위해 기록됩니다. Thermo Fisher는 CloudTrail을 사용하여 AWS Management Console, AWS SDK, 명령 줄 도구 및 기타 AWS 서비스를 통해 수행되는 작업을 포함하는, AWS의 인프라와 관련된 모든 활동을 기록합니다.

재난 복구

SampleManager LIMS 소프트웨어에는 표준화된 배포 아키텍처 및 관련 절차가 있습니다. 기술 운영 팀에서는 이 표준화를 통해 필요에 따라 새로운 환경을 쉽게 구축할 수 있습니다.

Thermo Fisher는 여러 AWS 지역 및 가용 영역 (지역 및 가용 영역 참조)에서 고객을 위한 서비스를 관리합니다.

Thermo Fisher는 AWS의 생명과학 역량 파트너 프로그램 내에서 유일한 LIMS 공급업체입니다. Thermo Fisher는 2008년부터 AWS 서비스를 사용하고 있습니다.

Thermo Fisher는 배포된 환경과 별도로 모든 고객 서비스의 백업을 유지합니다(본 문서의 "백업 및 복구" 섹션 참조).

재난 시나리오가 발생하는 경우, Thermo Fisher는 이벤트의 위험과 영향을 평가하고 영향을 받는 고객에게 연락합니다. 기술 운영 팀에서는 고객에 대한 위험과 영향에 초점을 맞춘 서비스 복원 계획을 수립합니다. 계획에 대한 알림이 고객에게 제공됩니다. 기술 운영 팀에서 서비스 복원 계획을 실행합니다.

백업 및 복구

SampleManager LIMS 소프트웨어는 모든 호스팅 시스템의 시스템 가용성을 유지하기 위해 Amazon의 전반적인 인프라를 활용하여 백업 및 복원 프로세스를 실행합니다.

- 시스템과 데이터는 표준 일정에 따라 백업되고 시스템과 분리되어 저장됩니다.
- 데이터 또는 시스템의 손상 또는 손실로 인한 복원은 사고로 간주되며 사고 관리 정책에 의거하여 관리됩니다.
- 복구할 수 없는 시스템 오류, 데이터 손상 또는 데이터 손실을 해결하기 위해 기술 운영 팀에서 시스템과 데이터를 복원합니다.
- 시스템 또는 데이터 복원의 계획된 실행에 앞서 고객 이해 관계자에게 알림이 전송됩니다.
- Thermo Fisher에서 복원된 시스템과 데이터를 확인합니다. 고객은 복구 내용이 기대치를 충족하는지 확인해야 합니다.
- 모든 복구 절차가 실행됩니다.



자세한 내용 알아보기: thermofisher.com/digitalscience

ThermoFisher
SCIENTIFIC