Cloud services

Thermo Scientific Watson LIMS software deployments in AWS

Overview

Thermo Scientific™ Watson LIMS™ software can be deployed on-premises or in the Amazon Web Services (AWS) cloud. On-premises deployments or deployments to a customer's own cloud hosting service are managed by the customer based on their infrastructure standards

Customers who contract with Thermo Fisher Scientific to manage their cloud deployment in AWS receive end-to-end support. Thermo Fisher provisions the cloud services, installs Watson LIMS software and maintains the deployment.

The following are some of the features and benefits of deploying Watson LIMS software to AWS:

- Fully managed deployment available across the globe in select AWS Regions.
- Physical access to the AWS data centers and networks is strictly controlled, monitored, and audited.
- Your data is segregated with dedicated servers and logically isolated networks.
- Your data is secured in motion and at rest with industry standard encryption.
- Your data is protected from unauthorized access or compromise with tight controls at the firewall and policy/procedure level.
- Your data is backed up and retained on a 30 day sliding window.
- Systems are managed with integrated auto-recovery from hardware failures.
- 99.5% service availability.
- Realtime intrusion detection and prevention.
- Infrastructure and user activity logging and monitoring.
- Data backup snapshots occur at least hourly.
- 2 hour response time for all critical issues with continuous effort until service is restored.
- The following sections provide an overview of the security policies and procedures applied to Watson LIMS software. Please also refer to the AWS Cloud Security site for information on the security provided by AWS.

thermo scientific

Facility security

Deployments of Watson LIMS software utilize AWS for all customer systems; there are no systems located onsite in Thermo Fisher offices. Access to the Thermo Fisher facilities is strictly controlled.

System security

Watson LIMS software customer systems are deployed and managed on AWS in line with the security policies outlined in the AWS Cloud Security site. Access to systems – corporate and customer – is controlled and limited to specific identified employees. The Technical Operations team at Thermo Fisher utilizes multi-factor authentication to secure access to systems.

Network security

Customer systems are configured and managed in a customer-dedicated Virtual Private Cloud (VPC). The VPC provides fine grained control and monitoring of all network interactions between the outside world and your managed instance, as well as internally between infrastructure components. Security policies are implemented for each customer, defining all the rules for how data flows and who has access to the systems.

The network in which Watson LIMS software is hosted is secured with an Intrusion Detection and Prevention System. It provides a high level of security, with active monitoring and intrusion detection and prevention. The IDS is configured to alert appropriate personnel to malicious activity detected and automatically update the IDS signatures.

Watson LIMS software has a dedicated highly controlled Virtual Private Network (VPN) for access to the Watson LIMS software network. The VPN is for employee use only and is actively monitored to ensure proper usage.

Data security

Watson LIMS software employs the industry standard AES-256 encryption algorithm to encrypt your data at rest. All data residing in the database or on file systems are encrypted.

Watson LIMS software encrypts data in transit, ensuring that all communication with the managed instance is secure using industry standard 256-bit encryption with a 2048 bit public key. Direct access to data stored in customer databases is restricted.

Application access

Watson LIMS managed cloud service utilizes robust Authentication, Authorization, and Accounting (AAA) capabilities. Thermo Fisher recommends the use of AAA policies that provide for the highest level of security.

Watson LIMS software customers are provided with the option of limiting access to their application instance by IP restriction or allowing access from the internet.

Secure coding practices

Watson LIMS manage cloud service is reviewed based on best practices prescribed by the Open Web Application Security Project (OWASP).

Watson LIMS software leverages tools to assess the security of the code and employs a secure coding audit as part of code reviews.

Logging

Watson LIMS software utilizes a log management system which logs IT infrastructure activity as well as user activity, including successful and failed user authentication attempts. The log management system is used to review the logged activity and alert the Technical Operations team on the detection of suspicious activity. Log data is retained for up to one year.

Monitoring

Thermo Fisher software actively monitors all systems, networks, applications, and supporting infrastructure using multiple commercial tools. AWS CloudWatch, AWS GuardDuty, AWS CloudTrail, Intrusion Prevention/Detection services, Cloud Governance and Alerting tools are used for monitoring, logging and alerting Technical Operations team members for security and health of managed services.

The Technical Operations team performs vulnerability assessments on Watson LIMS software. Thermo Fisher's Corporate Information Security (CIS) program provides guidance, oversight and continuous review and improvement of security controls for cloud deployments of Watson LIMS software managed by Thermo Fisher.

Change management

Thermo Fisher employs a Change Management Policy to record changes to systems and infrastructure. Changes are reviewed to mitigate risk and recorded for accounting purposes. Thermo Fisher utilizes CloudTrail to log all activities related to infrastructure on AWS including actions taken through the AWS Management Console, AWS SDKs, command line tools, and other AWS services.

Disaster recovery

Watson LIMS software has a standardized deployment architecture and associated procedures. This standardization allows the Technical Operations team to easily stand up new environments as needed.

Thermo Fisher manages services for customers across multiple AWS Regions and availability zones (refer to Regions and Availability Zones).

Thermo Fisher maintains backups of all customer services separate from the deployed environment (refer to “Backup and Recovery” section of this document).

In the event of a disaster scenario, Thermo Fisher will evaluate the risk and impact of the event and contact affected customers. The Technical Operations team will develop a plan to restore services, focusing on risk and impact to the customer. The customer will be notified of the plan. The Technical Operations team will execute the plan to restore services.

Backup and recovery

Watson LIMS software leverages Amazon’s comprehensive infrastructure to execute a backup and restoration process in order to maintain system availability for all hosted systems.

- Systems and data are backed up and backups are retained to meet the recovery targets.
- The backed up image is stored separate from the system using Amazon Simple Storage Service (Amazon S3). This provides a highly durable (99.999999999% durability) storage infrastructure designed for mission-critical data storage. Amazon S3 redundantly stores objects on multiple devices across a minimum of three Availability Zones (AZs) in an Amazon Region.
- All backups are encrypted using industry-standard encryption algorithms.
- Restoration due to data or system corruption or loss is deemed an incident and is managed under the Incident Management Policy.
- The Technical Operations team will restore systems and data to address unrecoverable system failure, data corruption, or data loss.
- Customer stakeholders are notified prior to a planned execution of a system or data restore.
- Thermo Fisher will verify restored systems and data. The customer is required to verify that the restoration meets their expectations.
- All restoration procedures will be executed.

Thermo Fisher has been using AWS’s services since 2008.

Learn more at **thermofisher.com/watson**