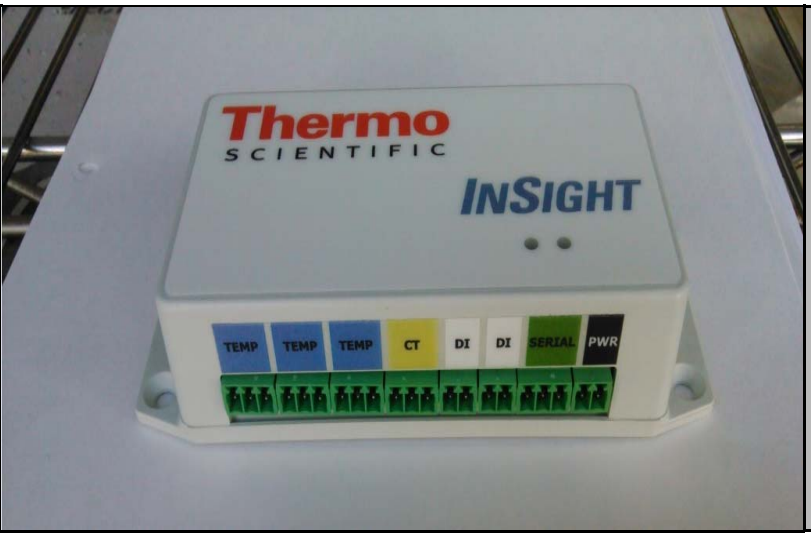


Thermo Scientific InSight

Architecture and Security Manual

327573H03 Rev. A September 2015

Visit us online to register your warranty
www.thermoscientific.com/labwarranty

IMPORTANT Read this instruction manual. Failure to follow the instructions in this manual can result in damage to the unit, injury to operating personnel, and poor equipment performance.

CAUTION All internal adjustments and maintenance must be performed by qualified service personnel.

Material in this manual is for informational purposes only. The contents and the product it describes are subject to change without notice. Thermo Fisher Scientific makes no representations or warranties with respect to this manual. In no event shall Thermo be held liable for any damages, direct or incidental, arising from or related to the use of this manual.

Version Control

Version	Date	Author	Description
1.0	5/16/15	Chris Exline	Creation of the intial document.
1.1	9/22/15	Chris Exline	Updated documentation to adjust for migration from Rackspace to AWS.

Table of Contents

1 Architecture & Security

The InSight data storage is based on a NOSQL technology is a decentralized fault tolerance system designed to scale to up to pedebytes of data storage. Currently InSight is processing over 2 million data points every day.

1.1 Proven Technology

The database is in use at Constant Contact, CERN, Comcast, eBay, GitHub, GoDaddy, Hulu, Instagram, Intuit, Netflix, The Weather Channel, and over 1500 more companies that have large, active data sets. One of the largest production deployments is Apple's, with over 75,000 nodes storing over 10 PB of data. Other large installations include Netflix (2,500 nodes, 420 TB, over 1 trillion requests per day), Chinese search engine Easou (270 nodes, 300 TB, over 800 million requests per day), and eBay (over 100 nodes, 250 TB). InSight currently runs on a 3 node deployment. There is ample room for growth using the current technology for years to come.

1.2 Fault Tolerant

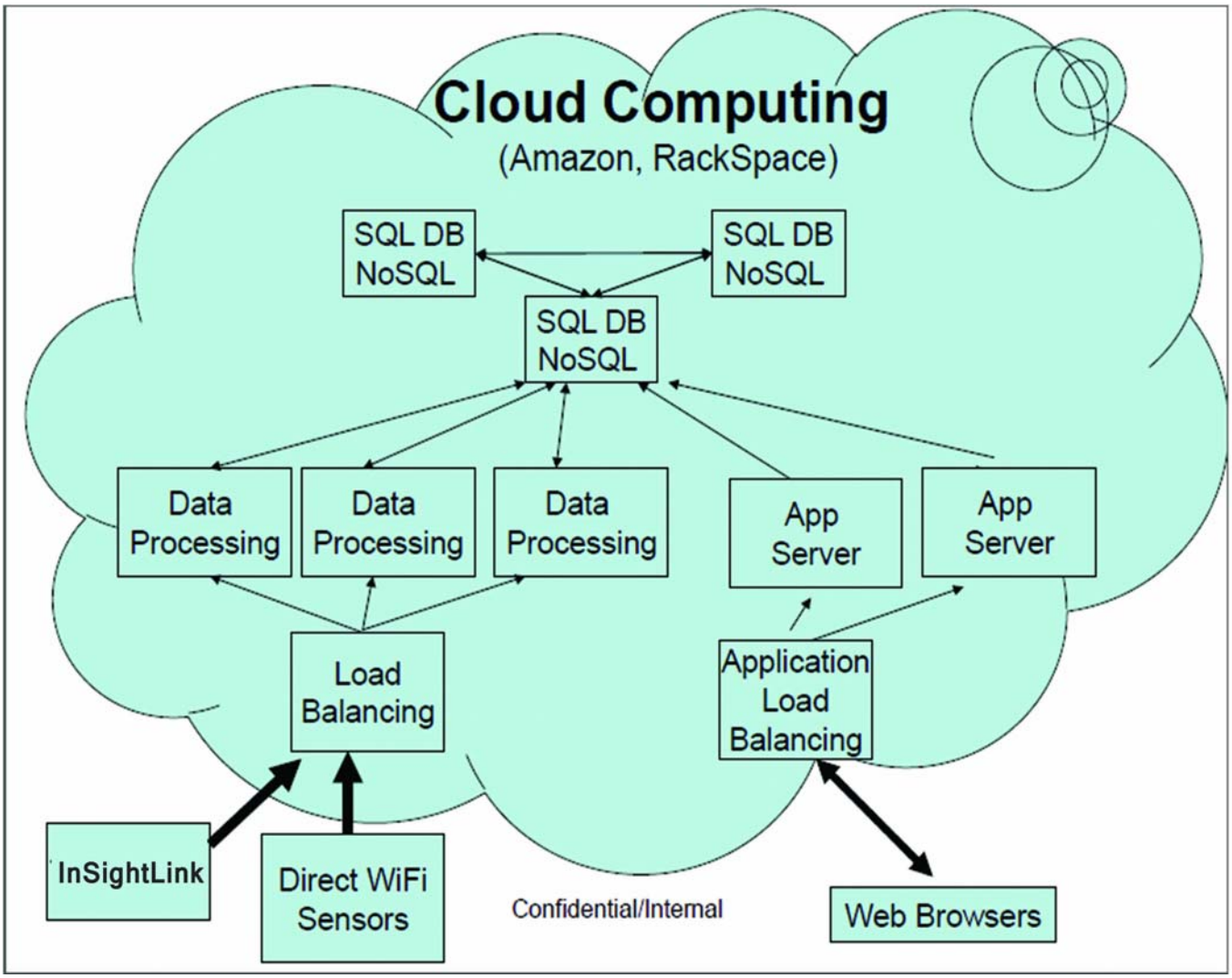
Data is automatically replicated to multiple nodes for fault-tolerance. Replication across multiple data centers is supported. Failed nodes can be replaced with no downtime.

1.3 Decentralized

There are no single points of failure. There are no network bottlenecks. Every node in the cluster is identical.

1.4 Durable

Durability is the property that writes, once completed, will survive permanently, even if the server is killed or crashes or loses power. This requires calling fsync to tell the OS to flush its write-behind cache to disk. The naive way to provide durability is to fsync your data files with each write, but this is prohibitively slow in practice because the disk needs to do random seeks to write the data to the write location on the physical platters. (Remember that each seek costs 5-10ms on rotational media.) Instead, like other modern systems, the system provides durability by appending writes to a commitlog first. This means that only the commitlog needs to be fsync'd, which, if the commitlog is on its own volume, obviates the need for seeking since the commitlog is append-only.


Cloud Computing
(Amazon, RackSpace)
SQL DB NoSQL
SQL DB NoSQL
SQL DB NoSQL
Data Processing
Data Processing
Data Processing
App Server
App Server
Load Balancing
Application Load Balancing
InSightLink
Direct WiFi Sensors
Confidential/Internal
Web Browsers

2 Amazon Web Services (AWS) Security Standards

2.1 ISO 27001

Amazon Web Services (AWS) is **ISO 27001** certified (**published certificate**) under the International Organization for Standardization (ISO) 27001 standard. ISO 27001 is a widely-adopted global security standard that outlines the requirements for information security management systems. It provides a systematic approach to managing company and customer information that's based on periodic risk assessments. In order to achieve the certification, a company must show it has a systematic and ongoing approach to managing information security risks that affect the confidentiality, integrity, and availability of company and customer information.

AWS has established a formal program to maintain the certification. This certification reinforces our commitment to providing transparency into our security controls and practices. The AWS ISO 27001 certification includes AWS data centers in the US East (Northern Virginia), US West (Oregon), US West (Northern California), AWS GovCloud (US) (Oregon), EU (Ireland), Asia Pacific (Singapore), Asia Pacific (Tokyo), Asia Pacific (Sydney), and South America (Sao Paulo) that support in-scope services.

2.2 SOC 1 / ISAE 3402

Amazon Web Services publishes a **Service Organization Controls 1 (SOC 1), Type II report**. The audit for this report is conducted in accordance with AICPA: AT 801 (formerly SSAE 16) and the International Standards for Assurance Engagements No. 3402 (ISAE 3402).

This audit is the replacement of the Statement on Auditing Standards No. 70 (SAS 70) Type II report. This dual-standard report can meet a broad range of auditing requirements for the U.S. and international auditing bodies.

The SOC 1 report audit attests that the AWS control objectives are appropriately designed and that the controls safeguarding customer data are operating effectively. The AWS SOC 1 report includes AWS data centers in the US East (Northern Virginia), US West (Oregon), US West (Northern California), AWS GovCloud (US) (Oregon), EU (Dublin), EU (Frankfurt), Asia Pacific (Singapore), Asia Pacific (Sydney), Asia Pacific (Tokyo), and South America (Sao Paulo) that support in-scope services.

2.3 SOC 2

In addition to the SOC 1 report, AWS publishes a **Service Organization Controls 2 (SOC 2), Type II report**. Similar to the SOC 1 in the evaluation of controls, the SOC 2 report is an attestation report that expands the evaluation of controls to the criteria set forth by the **American Institute of Certified Public Accountants (AICPA)** Trust Services Principles. These principles define leading practice controls relevant to security, availability, processing integrity, confidentiality, and privacy applicable to service organizations such as AWS.

The AWS SOC 2 is an evaluation of the design and operating effectiveness of controls that meet the criteria for the security principle set forth in the AICPA's Trust Services Principles criteria. This report provides additional transparency into AWS security and availability based on a defined industry standard and further demonstrates AWS' commitment to protecting customer data. The AWS SOC 2 report includes AWS data centers in the US East (Northern Virginia), US West (Oregon), US West (Northern California), AWS GovCloud (US) (Oregon), EU (Dublin), EU (Frankfurt), Asia Pacific (Singapore), Asia Pacific (Sydney), Asia Pacific (Tokyo), and South America (Sao Paulo) that support in-scope services.

2.4 SOC 3

AWS publishes a **Service Organization Controls 3 (SOC 3)** report. The SOC 3 report is a publicly available summary of the AWS SOC 2 report.

The report includes the external auditor's opinion of the operation of controls (based on the **AICPA's Security Trust Principles** included in the SOC 2 report), the assertion from AWS management regarding the effectiveness of controls, and an overview of AWS Infrastructure and Services. The AWS SOC 3 report includes AWS data centers in the US East (Northern Virginia), US West (Oregon), US West (Northern California), AWS GovCloud (US) (Oregon), EU (Dublin), EU (Frankfurt), Asia Pacific (Singapore), Asia Pacific (Sydney), Asia Pacific (Tokyo), and South America (Sao Paulo) that support in-scope services. This is a great resource for customers to validate that AWS has obtained the external auditor assurance without going through the process to request a SOC 2 report.

2.5 MTCS Tier 3 Certification

The **Multi-Tier Cloud Security (MTCS)** is an operational Singapore security management Standard (SPRING SS 584:2013), based on ISO 27001/02 Information Security Management System (ISMS) standards. The certification assessment requires us to:

- Systematically evaluate our information security risks, taking into account the impact of company threats and vulnerabilities
- Design and implement a comprehensive suite of information security controls and other forms of risk management to address company and architecture security risks

- Adopt an overarching management process to ensure that the information security controls meet our information security needs on an ongoing basis

2.6 ISO 9001

ISO 9001:2008 is a global standard (**published certificate**) for managing the quality of products and services. The 9001 standard outlines a quality management system based on eight principles defined by the International Organization for Standardization (ISO) Technical Committee for Quality Management and Quality Assurance. They include:

- Customer focus
- Leadership
- Involvement of people
- Process approach
- System approach to management
- Continual Improvement
- Factual approach to decision-making
- Mutually beneficial supplier relationships

The key to the ongoing certification under this standard is establishing, maintaining and improving the organizational structure, responsibilities, procedures, processes, and resources in a manner where AWS products and services consistently satisfy ISO 9001 quality requirements.

3 Security Operations

The AWS cloud infrastructure is housed in AWS's data centers, designed to satisfy the requirements of our most security-sensitive customers. The AWS infrastructure has been designed to provide the highest availability while putting strong safeguards in place regarding customer privacy and segregation. When deploying systems in the AWS Cloud, AWS helps by sharing the security responsibilities with you. AWS manages the underlying infrastructure, and you can secure anything you deploy in AWS.

The AWS infrastructure is protected by extensive network and security monitoring systems. In addition, AWS infrastructure components are continuously scanned and tested. The AWS production network is segregated from the Amazon corporate network, and access to this network is monitored and reviewed on a daily basis by AWS security managers. The AWS production network is segregated from the Amazon corporate network and requires a separate set of credentials for access, consisting of SSH public-key authentication through a bastion host using an MFA token. This access is monitored and reviewed on a daily basis by AWS security managers.

AWS purpose-builds most of our security tools to tailor them for AWS's unique environment and scale requirements. These security tools are built to provide maximum protection for your data and applications. This means AWS security experts spend less time on routine tasks, and are able to focus more on proactive measures that can increase the security of your AWS Cloud environment.

A white paper providing an overview of the AWS Security Processes can be found here:
https://d0.awsstatic.com/whitepapers/Security/AWS%20Security%20Whitepaper.pdf

WEEE Compliance

WEEE Compliance. This product is required to comply with the European Union's Waste Electrical & Electronic Equipment (WEEE) Directive 2002/96EC. It is marked with the following symbol. Thermo Fisher Scientific has contracted with one or more recycling/disposal companies in each EU Member State, and this product should be disposed of or recycled through them. Further information on our compliance with these Directives, the recyclers in your country, and information on Thermo Scientific products which may assist the detection of substances subject to the RoHS Directive are available at www.thermo.com/

Great Britain

WEEE Konformittät. Dieses Produkt muss die EU Waste Electrical & Electronic Equipment (WEEE) Richtlinie 2002/96EC erfüllen. Das Produkt ist durch folgendes Symbol gekennzeichnet. Thermo Fisher Scientific hat Vereinbarungen getroffen mit Verwertungs-/Entsorgungsanlagen in allen EU-Mitgliederstaaten und dieses Produkt muss durch diese Firmen widerverwetet oder entsorgt werden. Mehr Informationen über die Einhaltung dieser Anweisungen durch Thermo Scientific, dieVerwerter und Hinweise die Ihnen nützlich sein können, die Thermo Fisher Scientific Produkte zu identizfizieren, die unter diese RoHS. Anweisungfallen, finden Sie unter www.thermo.com/

Deutschland

Conformità WEEE. Questo prodotto deve rispondere alla direttiva dell' Unione Europea 2002/96EC in merito ai Rifiuti degli Apparecchi Elettrici ed Elettronici (WEEE).
È marcato col seguente simbolo.Thermo Fischer Scientific ha stipulato contratti con una o diverse società di riciclaggio/smaltimento in ognuno degli Stati Membri Europei. Questo prodotto verrà smaltito o riciclato tramite queste medesime. Ulteriori informazioni sulla conformità di Thermo Fisher Scientific con queste Direttive, l'elenco delle ditte di riciclaggio nel Vostro paese e informazioni sui prodotti Thermo Scientific che possono essere utili alla rilevazione di sostanze soggette alla Direttiva RoHS sono disponibili sul sito www.thermo.com/

Italia

Conformité WEEE. Ce produit doit être conforme à la directive euro-péenne (2002/96EC) des Déchets d'Equipements Electriques et Electroniques (DEEE). Il est marqué par le symbole suivant. Thermo Fisher Scientific s'est associé avec une ou plusieurs compagnies de recyclage dans chaque état membre de l'union européenne et ce produit devraitêtre collecté ou recyclé par celles-ci. Davantage d'informations sur laconformité de Thermo Fisher Scientific à ces directives, les recycleurs dans votre pays et les informations sur les produits Thermo Fisher Scientific qui peuvent aider le détection des substances sujettes à la directive RoHS sont disponibles sur www.thermo.com/

France

Important

For your future reference and when contacting the factory, please have the following information readily available:

Model Number: _____

Serial Number: _____

Date Purchased: _____

The above information can be found on the dataplate attached to the equipment. If available, please provide the date purchased, the source of purchase (manufacturer or specific agent/rep organization), and purchase order number.

IF YOU NEED ASSISTANCE:

Thermo Scientific products are backed by a global technical support team ready to support your applications. We also offer cold storage accessories, including remote alarms, temperature recorders and validation services. Visit www.thermoscientific.com or call:

USA/Canada	+1 866 984 3766	**Germany international**	+49 6184 90 6000
India toll free	1800 22 8374	**Germany national toll free**	0800 1 536 376
India	+91 22 6716 2200	**Italy**	+32 02 95059 552
China	+800 810 5118 (or) +400 650 5118	**Netherlands**	+31 76 579 55 55
Japan	+81 3 5826 1616	**Nordic/Baltic/CIS countries**	+358 9 329 10200
Australia	+61 39757 4300	**Russia**	+7 812 703 42 15
Austria	+43 1 801 40 0	**Spain/Portugal**	+34 93 223 09 18
Belgium	+32 53 73 42 41	**Switzerland**	+41 44 454 12 22
France	+33 2 2803 2180	**UK/Ireland**	+44 870 609 9203
New Zealand	+64 9 980 6700	**Other Asian countries**	+852 2885 4613
		Countries not listed	+49 6184 90 6000

Thermo Fisher Scientific Inc.

275 Aiken Road
Asheville, NC 28804
United States
www.thermofisher.com

327573H03 Rev. A