Gain Operational Intelligence at Scale with Cisco UCS Integrated Infrastructure for Big Data and Splunk Enterprise

Cisco and Splunk deliver a scalable unified infrastructure platform for operational intelligence.

**Highlights**

**Proven platform for operational intelligence**
- Based on the fifth-generation of the converged infrastructure for operational intelligence
- Deployed across major industry-specific environments

**Cisco UCS Integrated Infrastructure for Big Data**
- Provides industry-leading performance, capacity, and scalability for Splunk Enterprise deployments
- Designed to scale linearly to handle multiple petabytes (PB) of storage

**Real-time operational intelligence with Splunk Enterprise**
- Monitors and analyzes data from any source, including customer click streams and transactions, network activity, and call records, turning machine-generated data into business insight
- Powerful search, analysis, and visualization capabilities with Splunk Enterprise
- Provides an easy, fast, and secure way to analyze massive streams of data generated by IT systems, security devices, and technical infrastructure

**Cisco Unified Computing System foundation**
- Provides unified fabric, unified management, and advanced monitoring capabilities
- Using service profiles, delivers consistent and rapid deployment for out-of-the-box performance

**Fast deployment using Cisco UCS Director Express for Big Data**
- Delivers a highly extensible and customizable management platform that efficiently creates, manages, and monitors Splunk clusters at scale
Today's data center has evolved into a complex mix of layered and interconnected systems with blended boundaries to support modern applications. When problems arise, finding the root cause and gaining visibility across the infrastructure to proactively identify and prevent outages is a huge challenge. Meanwhile, virtualization and cloud infrastructures introduce additional complexity and create an environment that is more difficult to control and manage.

Traditional tools for managing and monitoring IT and security infrastructure are out of step with the environments they are meant to control because the environment is constantly changing. These tools are inflexible, costly, usually not scalable, and not consciously designed for the complexity of today's environments and application demands. Designed for individual specific IT functions, traditional tools do not work across multiple data center technologies to help solve problems. When problems arise, these tools typically lack the capability to provide targeted, detailed analysis of IT and security data. Traditional monitoring tools built on relational databases cannot handle the complexity or massive scale of today's machine data.

The Splunk Enterprise Advantage

Machine data is one of the fastest-growing and most complex varieties of big data. It is also one of the most valuable, containing a definitive record of user transactions, customer activity, sensor readings, machine behavior, security threats, and fraudulent activity. Splunk Enterprise is the industry-leading platform for machine data.

With Splunk Enterprise, you can troubleshoot problems and investigate security incidents in minutes, not hours or days. Splunk Enterprise scales linearly to collect and index petabytes of machine data generated across your entire data center, including physical, virtual, and cloud environments. It enables you to search, monitor, and analyze your data from one place in real time. Monitor your end-to-end infrastructure to avoid service degradation and outages. Gain operational intelligence with real-time visibility and critical insights into the customer experience, transactions, and other key business metrics.

Table 1 shows major use cases for Splunk Enterprise.

<table>
<thead>
<tr>
<th>Industry</th>
<th>Use cases</th>
</tr>
</thead>
</table>
| Aerospace and defense | • Monitor asset health, reliability, and system integrity and protect critical infrastructure from cybersecurity threats.  
                           • Comply with Defense Federal Acquisition Regulation Supplement (DFARS) and Risk Management Framework (RMF).  
                           • Gain real-time insights from sensors, devices, supervisory control and data acquisition (SCADA), incident command systems (ICS), and the core IT infrastructure. |
| Service providers  | • Accelerate service provisioning, improve customer experiences, accelerate delivery of new products, improve overall security posture, and reduce fraud. |
| Energy and utilities | • Monitor the asset health, reliability, and system integrity and protect critical infrastructure from cybersecurity threats.  
                           • Comply with North American Electric Reliability Corporation (NERC) reporting requirements.  
                           • Gain real-time insights from sensors, devices, SCADA, ICS, and the core IT infrastructure. |
Industry | Use cases
--- | ---
Financial services | • Protect against cyber threats and fraud.  
• Gain IT operational efficiency, bring order to unstructured data, and derive deep customer insights using machine learning and advanced analytics.

Healthcare | • Gain insights into system performance and interact with the broader healthcare ecosystem.  
• Protect patient records and comply with regulatory requirements.  
• Deliver better information access to patients, payers, and providers.

Higher education | • Gain end-to-end situational awareness.  
• Gain visibility into IT operations, regulations, and mandates.  
• Monitor security and regulatory compliance.  
• Perform real-time monitoring of security incidents and mitigation processes.

Manufacturing | • Gain visibility into IT and manufacturing operations.  
• Monitor the performance and uptime of systems and applications.  
• Improve security posture.  
• Gain insights into device, sensor, and equipment performance.

Online services | • Improve website performance and uptime.  
• Strengthen security posture.  
• Improve the customer experience.  
• Manage cloud, on-premises, and hybrid environments.  
• Monitor DevOps processes.

Public sector | • Address use cases in all three branches of government and four branches of the military.  
• Achieve rapid time to value.  
• Address cybersecurity use cases.  
• Comply with National Information Assurance Partnership (NIAP) Common Criteria certification requirements.

Retail | • Gain operational visibility across systems and applications across sales channels.  
• Track orders, inventory, and processes.  
• Gain real-time insights into cross-channel customer behavior.

Table 1. Splunk Enterprise is widely deployed across major industry-specific environments
Cisco UCS Integrated Infrastructure for Splunk Enterprise

Cisco UCS® Integrated Infrastructure for Splunk Enterprise is based on the fifth generation of industry-leading architectures known as Cisco UCS Integrated Infrastructure for Big Data and Analytics. We designed these solutions to meet a variety of scale-out application demands such as support for high performance, high capacity, high availability, massive scalability, ease of management, and integration capabilities.

Cisco UCS 6300 Series Fabric Interconnects
Cisco UCS fabric interconnects establish a single point of connectivity and management for the entire system. They provide high-bandwidth, low-latency connectivity for Cisco UCS servers, with integrated, unified management for all connected devices provided by Cisco UCS Manager, which is embedded within each fabric interconnect. Deployed in redundant pairs, Cisco UCS fabric interconnects offer full active-active redundancy, high performance, and the exceptional scalability needed to support the large number of servers that are typical in clusters serving big data applications. Cisco UCS Manager enables rapid and consistent server configuration using Cisco UCS service profiles, advanced health monitoring, and automation of ongoing system maintenance activities across the entire cluster as a single operation.

Cisco UCS Rack and Storage Servers
The Cisco UCS C240 M5 Rack Server is a dual-socket, 2-rack-unit (2RU) server offering industry-leading performance and expandability for a wide range of storage and I/O-intensive infrastructure workloads, from big data analytics to collaboration. This server uses the new Intel® Xeon® Processor Scalable Family with up to 28 cores per socket. It supports up to 24 DDR4 DIMMs for improved performance and lower power consumption. The DIMM slots are also 3D XPoint ready, supporting next-generation nonvolatile memory technology. The server offers a range of storage options, with up to 24 small-form-factor (SFF) 2.5-inch drives (with support for up to 10 Non-Volatile Memory Express [NVMe] PCIe solid-state disks [SSDs] on the NVMe-optimized chassis version) with a Cisco® 12-Gbps SAS Module RAID Controller. Additionally, it has two modular M.2 cards that can be used for boot. A modular LAN-on-motherboard (mLOM) slot supports the Cisco UCS Virtual Interface Card (VIC) 1387 with dual 40-Gbps network connectivity.

The Cisco UCS S3260 Storage Server is a high-density modular storage server designed to deliver efficient, industry-leading storage for data-intensive workloads. The Cisco UCS S3260 is a modular chassis with dual server nodes (two servers per chassis) and up to 60 large-form-factor (LFF) drives in a 4RU form factor. The server uses dual Intel® Xeon® processor E5-2600 v4 series CPUs and supports up to 512 GB of main memory and a range of hard-disk-drive (HDD) and solid-state disk (SSD) options.

The Cisco UCS S3260 chassis has 56 top-load LFF HDDs with a maximum capacity of 10 TB per HDD and can be mixed with up to 28 SSDs with maximum capacity of 3.2 TB per SSD. The modular Cisco UCS S3260 chassis offers flexibility with more computing, storage, and PCIe expansion on the second slot in the chassis. This second slot can be used for:

- An additional server node
- Four additional LFF HDDs with up to 10 TB capacity per HDD
- New PCIe expansion tray with up to two x8 half-height, half-width PCIe slots that can use any industry-standard PCIe card including Fibre Channel and Ethernet cards

The Cisco UCS S3260 chassis includes a Cisco UCS Virtual Interface Card (VIC) 1300 platform chip onboard the system I/O controller, offering high-performance bandwidth with dual-port 40 Gigabit Ethernet and FCoE interfaces per system I/O controller.
Reference Architecture

The reference architectures for the solution include server configurations such as CPU, memory, and I/O subsystems settings configured appropriately to address the specific resource requirements of Splunk Enterprise. Cisco and Splunk together have created reference architectures to accelerate deployment and reduce risk. Figure 1 shows the configurations available.

The three Cisco Unified Computing System™ (Cisco UCS) reference architectures for Splunk are based on Cisco UCS Integrated Infrastructure for Big Data and Analytics. The architectures vary in CPU, memory, disk capacity, and performance. All configurations are fully supported by Cisco UCS Director Express for Big Data for complete end-to-end deployment of Splunk Enterprise with an indexer cluster, search head cluster, and Splunk Monitoring Console. Table 2 shows the reference architectures.

Configuration tips

Note the following tips when configuring a solution:

- Three or more servers are required for search-head clusters.
- Splunk Enterprise Security applications require a dedicated search head (or cluster).
- Storage capacity and retention are inversely related, and a smaller indexing volume enables a greater retention capacity.
- The indexer configurations in Table 2 are specified for an ingest rate of up to 300 GB per day while supporting a search load. The number of search peers and search head machines that you need to index and search data in Splunk Enterprise depends on the number of concurrent users and the amount of data that the instance indexes.
- Splunk premium solutions (such as Splunk Enterprise Security and Splunk IT Service Intelligence) can require greater hardware resources than a reference configuration. Before designing a deployment for a Splunk premium solution, you should adjust the configuration accordingly.
### Table 2. Reference architectures

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Starter</th>
<th>Performance and capacity balanced</th>
<th>High capacity and performance</th>
</tr>
</thead>
</table>
| **Search heads** | 1 to 3 Cisco UCS C220 M5 Rack Servers, each with:  
- 2 Intel Xeon Processor Scalable Family 4110 CPUs (20 cores) at 2.1 GHz  
- 12 x 16 GB 2666 MHz (192 GB)  
- 2 x 480-GB Enterprise Value SSDs  
- Cisco 12-Gbps RAID Controller with 2-GB flash-based write cache (FBWC)  
- Cisco UCS VIC 1387 | 1 to 3 Cisco UCS C220 M5 Rack Servers, each with:  
- 2 Intel Xeon Processor Scalable Family 6132 CPUs (28 cores) at 2.6 GHz  
- 12 x 16 GB 2666 MHz (192 GB)  
- 2 x 480-GB Enterprise Value SSDs  
- Cisco 12-Gbps RAID Controller with 2-GB FBWC  
- Cisco UCS VIC 1387 |  |
| **Syslog-ng servers and heavy forwarders (optional)** | 2 Cisco UCS C220 M5 Rack Servers, each with:  
- 2 Intel Xeon Processor Scalable Family 6132 CPUs (28 cores) at 2.6 GHz  
- 12 x 16 GB 2666 MHz (192 GB)  
- 2 480 GB SSD-EV  
- 4 x 1.2 TB 10K SAS HDD (optional)  
- 12-Gbps RAID controller with 2-GB flash-based write cache (FBWC)  
- Cisco UCS VIC 1387 |  |
| **Indexers** | 8 Cisco UCS C220 M5 Rack Servers¹, each with:  
- 2 Intel Xeon Processor Scalable Family 4110 CPUs (20 cores) at 2.1 GHz  
- 12 x 16 GB 2666 MHz (192 GB)  
- M.2 with 2 x 480-GB SSDs  
- 2 x 1.6-TB solid state drives (SSDs) configured as RAID1  
- 8 x 1.8-TB 10,000-rpm SAS hard-disk drives (HDDs) configured as RAID10  
- Cisco 12-Gbps RAID Controller with 4-GB FBWC  
- Cisco UCS VIC 1387 | 8 Cisco UCS C240 M5 Rack Servers¹, each with:  
- 2 Intel Xeon Processor Scalable Family 6132 CPUs (28 cores) at 2.6 GHz  
- 12 x 16 GB 2666 MHz (192 GB)  
- M.2 with 2 x 480-GB SSDs  
- 26 x 960-GB SSDs configured as RAID5  
- Cisco 12-Gbps RAID Controller with 4-GB FBWC  
- Cisco UCS VIC 1387 | 4 Cisco UCS S3260 Storage Servers with 2 processing nodes, each with:  
- 2 Intel Xeon processor E5-2680 v4 CPUs (28 cores) at 2.4 GHz  
- 8 x 32 GB 2400 MHz (256 GB)  
- 2 x 480-GB SSDs for boot  
- 8 x 1.6-TB SSDs configured as RAID5  
- 20 x 10-TB 7200-rpm HDDs configured as RAID10  
- Cisco 12-Gbps RAID Controller with 4-GB FBWC  
- Cisco UCS VIC 1300 |
## Configuration

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Starter</th>
<th>Performance and capacity balanced</th>
<th>High capacity and performance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage capacity per indexer⁴</td>
<td>69 TB (12 TB hot and 57 TB cold)</td>
<td>184 TB</td>
<td>888 TB (88 TB hot and 800 TB cold)</td>
</tr>
<tr>
<td>Sample retention⁵ (IT operations analytics [ITOA]) per indexer</td>
<td>2.4 TB per day for 10 days hot and 45 days cold</td>
<td>2.4 TB per day for 5 months</td>
<td>2.4 TB per day for 70 days hot and 22 months cold</td>
</tr>
<tr>
<td>Sample retention⁵ (enterprise security) per indexer</td>
<td>800 GB per day for 30 days hot and 4.5 months cold</td>
<td>800 GB per day for 15 months</td>
<td>800 GB per day for 7 months of hot and over 5 years of cold</td>
</tr>
<tr>
<td>Administration nodes</td>
<td>1 to 3 Cisco UCS C220 M5 Rack Servers, each with:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 2 Intel Xeon Processor Scalable Family 4110 CPUs (20 cores) at 2.1 GHz</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 12 x 16 GB 2666 MHz (192 GB)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 2 x 480 GB Enterprise Value SSDs</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Cisco 12-Gbps RAID Controller with 2-GB FBWC</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Cisco UCS VIC 1387</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Connectivity</td>
<td>2 Cisco UCS 6332 Fabric Interconnects (40-Gbps ports)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rack space</td>
<td>15RU</td>
<td>35RU</td>
<td>21RU</td>
</tr>
<tr>
<td>Cisco UCS Director Express for Big Data</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

## Notes:

1. Other SSD and HDD options: 1.6-TB or 3.8-TB SSD, 1.8-TB 10,000-rpm SAS HDD, or a combination of SSD for hot and warm data and HDDs for cold data are supported.
2. The indexers can be used in standalone or distributed searches. In the distributed architecture, both the indexers and search heads can be configured as clustered or nonclustered. You can scale by adding search heads and indexers to the cluster.
3. The suggested maximum indexing capacities per indexer node are up to 300 GB per day for IT operational analytics, up to 200 GB per day for IT services intelligence (ITSI), and up to 100 GB per day for enterprise security.
4. The total storage capacity per server is the unformatted available storage space based on the parity used for the RAID group. The actual available storage space varies depending on the file system used.
5. Sample retention durations were calculated with the assumption of 50% compression of original data without any data replication.
Conclusion: A Solution for Massive Scalability

Splunk Enterprise delivers best in-class operational visibility and digital intelligence by monitoring all machine-generated data and making it accessible, usable, and valuable across your organization. Cisco UCS Integrated Infrastructure for Big Data, with its computing, storage, connectivity, and unified management features, simplifies deployment and offers a dependable, massively scalable integrated infrastructure that delivers predictable performance and high-availability for your Splunk Enterprise platform with reduced total cost of ownership (TCO).

Our reference architectures are carefully designed, optimized, and tested with Splunk Enterprise in a clustered distributed search environment to reduce risk and accelerate deployment. These architectures allow you to achieve a high-performance Splunk Enterprise deployment to meet your current needs, and they scale as your needs grow. You can deploy these configurations as is or use them as templates for building custom configurations. The Cisco UCS reference architectures for Splunk Enterprise support the massive scalability that Splunk deployments demand. The reference architectures described in this document can easily scale to thousands of servers through the use of Cisco Nexus® 9000 Series Switches.

Reference

For more information about Cisco UCS, visit https://www.cisco.com/go/ucs.
For more information about Splunk, visit http://www.splunk.com.
For more information about the Cisco UCS S3260 Storage Server, visit https://www.cisco.com/go/storage.
For more information about Cisco UCS Big Data Solutions, visit https://www.cisco.com/go/bigdata.
For more information on Cisco's big data validated designs, visit https://www.cisco.com/go/bigdata_design.