Intel hardware delivers scalable, cost-effective performance for the Splunk Data-to-Everything Platform.

Learn about the Business Story >
Learn more about the Reference Configuration >

Authors

Intel
Murali Madhanagopal
Solutions Architect for Analytics & AI, Solutions Development Group
Merritte Stidston
Technical Solution Specialist, Data Platforms Group
Shibani Singh
Cloud Solutions Engineer for Analytics & AI, Solutions Development Group
Sandeep Togrikar
Solutions Architect for Analytics & AI, Data Platforms Group

Splunk
Francisco Casas
Director of Core Product Management
Jason Beyer
Senior Performance Engineer
Brian Wooden
Director of Partner Integrations
Splunk Solution Benefits

Splunk provides visibility into security, IT operations, application development, and business operations data and processes to deliver the following business value:

- **Continuous threat remediation.** Splunk can identify potential incidents, compromised systems, or both by monitoring for vulnerabilities that can lead to breaches. Splunk can find threats, determine security posture, and report on compliance through continuous security monitoring.

- **Reduced downtime.** Using Splunk to collect, analyze, and report on machine data from thousands of Internet of Things (IoT) devices can lead to improved equipment uptime and increased customer satisfaction.

- **Observability.** Splunk can provide visibility into security, IT operations, and business data and processes.

- **Application uptime.** Competitive advantage and customer experience are driven by the development speed and quality of your applications. Splunk provides real-time insights across the application development lifecycle.

- **Smarter production insight.** Real-time monitoring and predictive analytics unleash the power of machine learning to understand performance baselines, predict deviations, and provide intelligent recommendations that relate to production, asset maintenance, and supply chain management.

- **Faster, easier, more intuitive analytics.** Drive business outcomes with visual context, collaboration, and automation.

- **Management of at-scale operations.** Architect robust data strategies for a scalable, ever-changing data market.

Executive Summary

The Splunk Data-to-Everything Platform built in an optimized environment delivers scalable, high-performance data analytics, empowering enterprises and service providers to turn data into insights and bring the power of data analytics to users across the enterprise. Combining the industry-leading Splunk product set with a reference configuration of Intel® technologies helps organizations accelerate and scale their Splunk on-premises or private cloud deployments, converting raw data into operational, business, and security intelligence.

The power of Splunk lies in its ability to handle any structure, any source, or any time scale of data. Organizations can bring the data together to investigate, monitor, analyze, and act on it across a myriad of use cases. The resulting insights can help them identify security threats, optimize application performance, understand customer behavior, and more.

To get the most out of aSplunk deployment, no matter the use case, IT organizations need to understand their Splunk workloads and optimize their infrastructure so that Splunk runs as efficiently as possible—low search runtimes, high data ingestion rates, and high numbers of concurrent searches. Splunk and Intel worked together to develop and benchmark various Splunk workloads using the latest Intel® compute and storage hardware. This document provides a business-level overview of how to build an optimized environment for the Splunk Data-to-Everything Platform. It describes a reference configuration for Splunk on-premises or private cloud deployments of different business sizes and types, and documents the resulting environment’s performance and scalability.

**Figure 1.** The Splunk Data-to-Everything Platform ingests and analyzes data from diverse sources to help maximize the value of event and machine data.
Terms to Know

**Indexing** is the gathering of relevant data in Splunk, categorizing it, and preparing it for search.

**Searching** is the primary way users navigate data in Splunk Enterprise. You can write a search to retrieve events from an index, use statistical commands to calculate metrics and generate reports, search for specific conditions within a rolling time range window, identify patterns in your data, predict future trends, and so on.

Business Challenge: Efficiently Exploit the Power of Machine Data

A significant amount of event and machine data is generated by applications, the OS, network, security software, client devices, the Internet of Things (IoT), and other technologies. Monitoring and analyzing machine data can help organizations solve many problems, like analyzing Web traffic, understanding customer behavior, streamlining financial analysis, improving customer experience, and more. But machine data is complex, and enterprises face significant challenges in converting it into timely insights.

Splunk Enterprise can help solve these challenges by enabling enterprises to investigate machine and event data in its raw form; monitor it as it streams through the IT, security, and IoT business systems; analyze trends; and take action. But as with any technology, efficiency is paramount to maximizing total cost of ownership and return on investment. Efficiently deploying Splunk Enterprise requires understanding the characteristics of a Splunk workload and how the components of Splunk work together. Some workloads require more indexing of data, other workloads focus on running searches, and still other workloads have a more balanced amount of data indexing and search queries.

Without understanding the workload and then configuring Splunk infrastructure specifically for that workload, organizations will struggle to obtain maximum performance and scalability from Splunk—meaning it’s more difficult to obtain timely analyses of their enormous and fast-growing data volumes.

Making Data Accessible, Usable, and Valuable

The Splunk Data-to-Everything Platform provides powerful capabilities for storing, organizing, analyzing, and gaining insights from a welter of data sources. Splunk’s platform helps organizations to address critical use cases, such as:

- **Infrastructure and IT services.** Splunk provides real-time monitoring, proactive alerting, and visibility into the health of infrastructure and services, to help prevent downtime.
- **Security and compliance.** Splunk speeds security investigations through real-time monitoring, historical analysis, and visualization of massive data sets. Security teams can perform comprehensive incident investigations and create ad hoc reports in minutes. Common security use cases include fraud analytics and detection, insider threat, incident investigation and forensics, advanced threat detection, incident response, compliance, data privacy, and automation and orchestration of a security operations center.
- **Application delivery.** Splunk offers real-time visibility across the application stack, with end-to-end views into application performance, transactions, and user activity. IT can quickly deliver releases and optimize application quality, performance, and costs.
- **Business analytics.** Splunk opens a window into complex business processes, customer behavior, product usage, and digital marketing campaigns. Businesses seeking to drive more revenue through their websites or mobile apps can gain timely and relevant business insights.
- **IoT and industrial data.** Splunk provides the ability to monitor operations, analyze usage, and integrate insights into an end-to-end view of business operations by leveraging data generated by connected devices, control systems, sensors, SCADA systems, and more.

About Splunk

Splunk helps organizations ask questions, get answers, take actions, and achieve business outcomes from their data. Organizations use Splunk solutions with machine learning to monitor, investigate, and act on all forms of business, IT, security, and IoT data. Founded in 2003 and headquartered in San Francisco, Splunk has been named a leader in the Gartner Magic Quadrant for SIEM for six consecutive years and was ranked Number 1 in worldwide IT analytics software by IDC.  

Solution Value: Simplified Deployment, Fast Answers, Smooth Scaling

With an optimized environment for Splunk, organizations can speed and strengthen data analytics while enjoying the advantages of an integrated, flexible product suite. Splunk Enterprise releases event and machine data from its silos and doesn't require the data to be formatted before asking questions.²

Splunk workloads are being optimized by the latest Intel® technologies, including 2nd Generation Intel® Xeon® Scalable processors, Intel® Optane™ SSDs, and Intel® 3D NAND SSDs. Architects and engineers from Splunk and Intel worked together to develop a reference configuration and benchmark its performance and scalability. They focused on the critical Splunk Enterprise tasks of indexing and searching.

In particular, the benchmarking explored how to best optimize the Splunk Data-to-Everything Platform for three use cases: balanced, indexing-intensive, and search-intensive workloads. These recommendations can help organizations scale their Splunk Enterprise deployments and get optimal performance for different use cases.
The following is a summary of the primary findings:

- The aggregate indexing rate and the number of searches for Splunk Enterprise scale almost linearly, to accommodate more users and data.
- Using Intel 3D NAND SSDs instead of Intel® SATA SSDs for server-attached storage on indexer nodes, the optimized solution provides a six-fold throughput increase.
- Using Intel Optane SSDs for server-attached storage on the search heads, the platform provides lower latency, faster random-read performance, and enhanced endurance (tested drive endurance of up to 60 full-span drive writes per day), compared to 3D NAND SSD capabilities in the market.
- The reference configuration for the Splunk Data-to-Everything (such as DevOps, Utilities, or Security) or by technology. The community through SplunkBase. You can browse by category available from Splunk, its partners, and the broader Splunk applications. In fact, over 1,000 apps and add-ons are the use of additional Splunk products and third-party Enterprise, the software suite can be expanded through benchmark testing was limited to Splunk premises, in the cloud, or accessible through a hybrid cloud. Although the benchmark testing was limited to Splunk Enterprise, the software suite can be expanded through the use of additional Splunk products and third-party applications. In fact, over 1,000 apps and add-ons are available from Splunk, its partners, and the broader Splunk community through SplunkBase. You can browse by category (such as DevOps, Utilities, or Security) or by technology.

**Solution Architecture: Scalable and Flexible Splunk Enterprise Infrastructure**

Splunk Enterprise can be deployed on-premises, as a service, through a managed cloud, or in a hybrid cloud environment. Splunk software can connect to and receive data from devices, applications, and other data sources, whether they are on-premises, in the cloud, or accessible through a hybrid cloud.

Although the benchmark testing was limited to Splunk Enterprise, the software suite can be expanded through the use of additional Splunk products and third-party applications. In fact, over 1,000 apps and add-ons are available from Splunk, its partners, and the broader Splunk community through SplunkBase. You can browse by category (such as DevOps, Utilities, or Security) or by technology.

The reference configuration for the Splunk Data-to-Everything Platform (Figure 2) incorporates the following Intel technologies:

- **2nd Generation Intel Xeon Scalable processors.** The 2nd Generation Intel Xeon Scalable processors are optimized for big data analytics workloads like Splunk. These processors incorporate architecture improvements and enhancements for compute-intensive and data-intensive workloads, making them well suited to the work of ingesting and analyzing massive quantities of real-time and near-real-time machine data.
- **Intel Optane SSDs.** Revolutionary Intel Optane SSDs provide high throughput for data caching and low latency for rapid responses under load. With high endurance and predictably fast service along with their outstanding performance, these SSDs help optimize Splunk search heads.
- **Intel 3D NAND SSDs.** These PCIe/NVMe-based SSDs deliver scalable, cost-effective performance and low latency for Splunk Enterprise indexers. The SSDs also offer outstanding quality, reliability, advanced manageability, and serviceability to minimize service disruptions.
- **Intel® Ethernet network connection.** Intel® Ethernet network controllers, adapters, and accessories enable agility in the data center to deliver services efficiently and cost-effectively. Compatible with the Open Compute Platform, these high-performance connectors support high throughput, reliability, and compatibility for Splunk computing.

See Test Results and Recommendations for detailed data and benchmark results; Appendix A: Test Environment describes the testing process and bill of materials.

The combination of Splunk and Intel technologies provides a feature-rich, high-performance, future-ready, and industry-leading solution that can scale well beyond most needs. Speed and quality of information are the two most important elements of a data analytics solution, and running your Splunk deployment in an optimized environment provides both.

---

**SATA Versus NVMe: A Primer**

Today, SATA SSDs are quite common in many data centers. However, modern data centers are replacing SATA drives with newer drives based on improved technology.

SATA was initially designed for slower spinning HDDs; the SATA specification has not been significantly improved since 2008. As a result, SATA transfer rates have not kept up with innovations in storage technology and cannot move the volumes of data at the speeds modern applications and use cases require.

In 2004, Intel led the industry to create a new standard interface: Peripheral Component Interconnect Express (PCIe), which has a higher number of data-transfer channels (roughly 10 for SATA and 25 for PCIe). Unlike the SATA specification, PCIe has continued to evolve to support storage and processor innovation and is currently in its fourth generation. Beyond its leadership role in developing PCIe, in 2011 Intel led an open industry consortium that created a standardized high-performance host-controller interface for PCIe SSDs: Nonvolatile Memory Express (NVMe), which is specifically designed for nonvolatile memory to overcome the SATA bottleneck and to deliver the throughput for high-bandwidth storage applications.

How does NVMe work? Imagine a shuttle bus, driving from destination A to B, with a speed limit of 15 miles per hour. Now imagine there are four buses and the new speed limit is 70. You can now increase the speed at which passengers can go from A to B. This is how NVMe utilizes PCIe. NVMe can send data in parallel on up to four PCIe lanes.

**Ready to learn more?** Turn the page for the detailed Reference Configuration discussion.
Overview of Splunk Enterprise

Splunk Enterprise software brings a new value proposition to the field of data collection and analytics. Traditional extract, transform, and load (ETL) systems require all the data to be structured before insights can be gleaned from it, slowing down the analytics process. But Splunk Enterprise is different. It is an extract, load, and transform (ELT) platform. That is, it supports schema-on-demand (also known as "schema-on-read," "schema-on-need," and "schema-on-use"), which allows data to be ingested first and structure to be imposed on the data later. With Splunk Enterprise, new raw data sources can be added at any time.

Splunk Enterprise is a software product for enabling enterprises to collect, search, organize, analyze, and visualize data gathered from various system components. Splunk Enterprise ingests log and streaming data from a wide variety of sources, including websites, applications, sensors, and devices. From each data source, Splunk Enterprise indexes the data stream and parses it into a series of individual events that you can view and search. Splunk's web interface can be used to analyze the data further. Splunk's search language, lookups, macros, and sub searches reduce hours of tedium to seconds of simplicity, and its tags, saved searches, and dashboards offer both operational insights and collaborative vehicles. Figure 3 illustrates the Splunk Enterprise Core.

Key conclusions from validation on Intel® architecture are:

### Storage Optimization (Table 2)

For indexer node attached storage, Intel® 3D NAND SSDs provide volume storage at a reasonable cost and up to 6x throughput improvement over SATA-based SSDs. For search heads, Intel® Optane™ SSDs provide smaller capacity storage with lower latency, better random read performance, and enhanced endurance.

### Workload Optimization

For balanced workloads, Splunk Enterprise scales well on Intel® architecture. Using scalability testing on one-, three-, five-, and 10-node clusters, we observed that the aggregate ingestion rate and the number of searches can be scaled almost linearly to accommodate more Splunk Enterprise users and higher data ingestion rates.

For indexing-intensive workloads, follow Splunk parallel pipeline setting guidelines to increase the throughput, and increasing DRAM capacity can improve ingestion rates by up to 1.3x.

For search-intensive workloads, more concurrent search users can be supported by increasing the number of search heads. Also, disabling hyper-threading can improve search runtimes by up to 2x, but indexing throughput will be negatively impacted by about 30 percent. In addition, increasing DRAM capacity improves search runtimes—in our tests, doubling the amount of DRAM improved search times by up to 14x.

### Equipment and Methodology

The tests were conducted to gauge the amount and type of Intel® equipment needed to execute certain workloads, in addition to getting a perspective of Splunk performance. It’s important to note that the tests used oversized equipment and only a small fraction of the capacity was utilized during the tests.

---

[Figure 3. Splunk Enterprise Core for parsing, indexing, and searching data. Source: docs.splunk.com/Documentation/Splunk/7.3.3/Installation/Splunksarchitectureandwhatgetsinstalled]
Splunk Enterprise can be used for many use cases where data is streaming in from hundreds of sources, and both ad hoc and scheduled searches and indexing tasks are required. Organizations use Splunk solutions with machine learning to monitor, investigate, and act on all forms of business, IT, security, and Internet of Things (IoT) data (see “Making Data Accessible, Usable, and Valuable” earlier in this document for a further discussion of Splunk use cases).

Characterizing Splunk Enterprise Performance

The performance of Splunk Enterprise is heavily influenced by the underlying compute, storage, and network infrastructure. Working together, Splunk and Intel identified opportunities for improved performance and integrated the latest Intel® technology into an optimized environment for the Splunk Data-to-Everything Platform. The solution was tested with a Splunk-provided test tool that approximates real industry data and workloads to verify that adequate performance was achieved.

These best practices use Splunk benchmarks that rely on generated event data and process it through Splunk Enterprise (indexing and searching) to exhibit the performance enhancements that can be achieved by using high-performance 2nd Generation Intel® Xeon® Platinum processors, Intel® 3D NAND SSDs, and Intel® Optane™ SSDs.

Performance tuning is often problematic for big-data workloads. Typical Splunk workloads fall into three categories:

- **Indexing-intensive.** Some customer workloads focus on better ingestion rates and making more data available for indexing, instead of focusing on the number of queries that will run for searches. Ingestion rates can be boosted by:
  - Increasing the number of parallel ingestion pipelines on the indexer
  - Increasing DRAM capacity

- **Search-intensive.** Other workloads are search-centric, where most of the work involves querying and reporting. For these workloads, the number of concurrent search users and search runtimes are more significant than ingestion rates. These workloads can be scaled in three ways:
  - Adding more search heads, which will lower search runtimes
  - Adding more computing power on the indexers
  - Increasing DRAM capacity on indexers

- **Balanced.** These are workloads with a balance of data ingestion, indexing, and searches. Ingestion rates scale linearly with an increase in the number of indexers, and search rates improve as well.

How Splunk Enterprise Works

Splunk Enterprise installs the splunkd process on the host. splunkd is a distributed C/C++ service that accesses, processes, and indexes streaming data. It also handles search requests. splunkd processes and indexes data by streaming it through a series of pipelines, each inclusive of a series of processing steps.

The Splunk Data-to-Everything Platform is optimized for the semi-structured time series data generated by machines. The Splunk deployment architecture that we refer to as Splunk Enterprise is comprised of forwards, indexers, and search heads, as shown in Figure 4.

The roles are briefly described below:

- **Indexers** are Splunk Enterprise instances that index data, transform raw data into events, and place the results into an index. Indexes are stored in mutually exclusive and jointly exhaustive partitions. Indexers also search the indexed data in response to search requests.

- **Search heads** form the interface to the user; this is where searches can be spawned, and responses are aggregated and visualized. Search heads service users’ interactive search requests and execute scheduled reports and alerts.

- **Forwarders** run in production end nodes, and collect, forward, and load balance the data to the indexing tier. The forwards shard the data before sending it to the indexer.

When a user submits a search to the search head, the search is distributed across all the indexers to retrieve relevant events and synthesize intermediate results. Upon receiving results from the indexers, the search head can synthesize or reduce results to provide the final report or search results.
The data stream processed by Splunk Enterprise is time-series data. Data is indexed based on timestamps and is organized into temporally coherent and minimally overlapping chunks in the indexers. Splunk sorts this data by age into “buckets” as shown in Figure 5. Each bucket has its own index file that maps the parsed keywords to their location in the raw data file within the respective bucket.

![Figure 5. Splunk Enterprise sorts time-series data into buckets, based on the age of the data. Source: learnsplunk.com/splunk-indexer-configuration.html](image)

One unit of work in Splunk Enterprise is referred to as a search. Splunk’s MapReduce-like architecture enables searches by allowing the search to be distributed across all indexers. The search is performed on subsets of the data simultaneously and results are aggregated at the reduce step. The compute cost of a search cannot be inferred by examining the search string alone as it depends on the data, its cardinality, sparseness, and other factors. Searches in Splunk Enterprise are categorized into dense, sparse, super-sparse, and rare, each respectively reducing in number of events that are returned per search. It may be possible to estimate whether a search is CPU-heavy or I/O-heavy based on previous runs of the same search or heuristics on the data and operations being performed. However, the same search can convert from being CPU-heavy to being I/O-heavy based on what other searches are being serviced simultaneously.

The types of searches are described below:

- **Dense.** Searches that scan through and report on many events. Dense searches usually tax a server’s CPU first, because of the overhead required to decompress the raw data stored in a Splunk Enterprise index. Some examples of these searches include counting the number of errors that occurred or finding all events from a specific host. Indexer Throughput: Up to 50,000 matching events per second. Performance Impact: CPU-based.

- **Sparse.** Searches that look for a single event or an event that occurs infrequently within a large set of data. This type of search is often referred to informally as a “needle in a haystack” or “rare term” search. Some examples include searching for a specific and unique IP address or error code. Indexer Throughput: Up to 5,000 matching events per second. Performance Impact: CPU-bound. The tests documented in this reference configuration did not use sparse searches—only dense and super-sparse.

- **Super-sparse.** Returns a small number of results from each index bucket that matches the search. A super-sparse search is I/O-intensive because the indexer must look through all of the buckets of an index to find the results. Indexer Throughput: Up to 2 seconds per index bucket. Performance Impact: I/O-bound.

In most customer environments, there are several concurrent users writing searches and running reports in Splunk Enterprise. Concurrent users pose an additional layer of complexity for workload management. The factors controlling the number of concurrent searches are typically tied to available hardware resources such as core speed, core count, and available memory. Although it may seem a bit counterintuitive, having more cores is not always going to allow more concurrent searches. Instead, core speed is often a more important factor. For example, if 100 similar queries are waiting to run sequentially, and the server’s cores operate 25 percent faster than a slower system, then it is potentially possible to run 25 more queries (of equal size) in the same amount of time.

**Test Results and Recommendations**

In this section, we first discuss our recommendations for which type of SSD to use for indexers and search heads. Then, we present our test findings based on the three kinds of customer workloads discussed previously: balanced, indexing-intensive, and search-intensive. Each of these three tests was configured with an ingestion rate of 5 TB/day/indexer. We focused on hot and warm data storage; requirements were calculated based on two days’ retention and replication by a factor of three at a daily ingestion rate of about 30 TB.

Table 1 provides the basic unit of testing—the configuration of indexers and search heads. In various tests, we simply varied the number of indexers and search heads. For a full bill of materials, see Appendix A: Test Environment.

<table>
<thead>
<tr>
<th>Capacity Tier</th>
<th>1x Intel® Optane™ SSD DC P4800X 375 GB PCIe x4 U.2 or 1x Intel SSD DC P4510 1 TB 2.5&quot; NVMe U.2</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>2x Intel® Xeon® Platinum 8260 processor (24 cores, 2.4 GHz)</td>
</tr>
<tr>
<td>Memory</td>
<td>12x RDIMM 32 GB DDR4-2933</td>
</tr>
<tr>
<td>Indexer</td>
<td>2x Intel® SSD DC P4510 8 TB 2.5&quot; NVMe U.2</td>
</tr>
<tr>
<td>SEARCH HEAD</td>
<td>2x Intel® Xeon® Platinum 8260 processor (24 cores, 2.4 GHz)</td>
</tr>
<tr>
<td>Memory</td>
<td>12x RDIMM 32 GB DDR4-2933</td>
</tr>
<tr>
<td>Capacity Tier</td>
<td>1x Intel® Optane™ SSD DC P4800X 375 GB PCIe x4 U.2 or 1x Intel SSD DC P4510 1 TB 2.5&quot; NVMe U.2</td>
</tr>
</tbody>
</table>

[Table 1. Basic Bill of Materials for Indexers and Search Heads](#)
**Storage Recommendations**

To identify the optimal storage device for the indexers and search heads, we ran I/O-intensive tests (super-sparse searches) on various media, and measured indexing throughput and search performance on each media. We recommend using Intel 3D NAND SSDs on the indexers and Intel Optane SSDs for the search heads, based on the results in Table 2.

In summary, here are our findings:

- Intel SATA-based SSDs provide compact form factor with high reliability, lower power, lower service time, and higher IOPS (300x) compared to hard disk drives (HDDs).
- Intel 3D NAND SSDs are NVMe-based and offer better sequential read/write performance and lower disk service times compared to SATA SSDs. This makes **3D NAND SSDs an ideal choice for indexers**, which perform the bulk of the work and require high-volume storage.
- Intel Optane SSDs are also NVMe-based but use a technology with performance that is more similar to memory than other types of SSDs. With lower latency and higher random write performance compared to 3D NAND SSDs, **Intel Optane SSDs are ideal for search heads**, because search heads must aggregate data and provide fast results for ad hoc and scheduled searches.

**Balanced Workload Performance**

We verified the performance for a workload with a balance of indexing, searches, and data ingestion, as shown in Table 3. As shown in Figure 6, the ingestion rate scales linearly with the number of indexers.

**Balanced Workload Conclusion**

The Splunk Enterprise Core architecture scales well on Intel architecture. Using scalability testing on one-, three-, five-, and 10-node clusters, we estimate that the aggregate ingestion rate and the number of searches can be scaled almost linearly to accommodate more Splunk Enterprise users and data.

---

### Table 2. Storage Test Results

<table>
<thead>
<tr>
<th>Model/Size</th>
<th>COMMODITY HDD</th>
<th>INTEL® SATA SSD</th>
<th>INTEL® 3D NAND SSD</th>
<th>INTEL® OPTANE™ SSD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ingestion Rate per Indexer (TB/day)</td>
<td>2.09</td>
<td>2.77</td>
<td>4.13</td>
<td>4.09</td>
</tr>
<tr>
<td>Disk Service Time (milliseconds)</td>
<td>1.98</td>
<td>0.74</td>
<td>0.04</td>
<td>0.05</td>
</tr>
<tr>
<td>Search Run Time (seconds)</td>
<td>5.1</td>
<td>1.3</td>
<td>0.2</td>
<td>0.2</td>
</tr>
</tbody>
</table>

*www.storagereview.com/node/4038


---

### Table 3. Verified Configurations for a Balanced Ingestion/Indexing/Search Workload

<table>
<thead>
<tr>
<th>Description</th>
<th>DEPARTMENTAL</th>
<th>SMALL</th>
<th>MEDIUM</th>
<th>LARGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aggregate Data Ingestion per day</td>
<td>4.5 TB</td>
<td>13 TB</td>
<td>19.5 TB</td>
<td>34.3 TB</td>
</tr>
<tr>
<td>Successful Concurrent Searches per Minute</td>
<td>20</td>
<td>30</td>
<td>50</td>
<td>96</td>
</tr>
<tr>
<td>Average Search Runtime (seconds)</td>
<td>26.34</td>
<td>15.47</td>
<td>9.18*</td>
<td>24*</td>
</tr>
</tbody>
</table>

* The five-indexer configuration shows lower average runtime (9.18 seconds) than the 10-indexer configuration (24 seconds) because the ratio of search heads to indexers is greater in the Medium configuration. That is, although the number of indexers increased, the number of search heads remained the same; since the 10-indexer configuration indexes more data (34 TB) than the five-indexer configuration, the searches take longer to complete. We plan to add a fourth search head to the 10-indexer cluster, to assess continued scale and effect on search time.
Indexing-Intensive Workloads

For indexing-intensive workloads, we recommend using a ratio of five indexers and two search heads. You can use two easily accessible tuning knobs to adjust indexing-intensive performance. One is to scale the number of parallel pipelines, and the other is to scale the amount of available DRAM.

Scaling the Number of Parallel Pipelines

Index parallelization is a feature that allows an indexer to maintain multiple pipeline sets. A pipeline set handles the processing of data from ingestion of raw data, through event processing, to writing the events to disk. If the underlying machine is under-utilized in terms of cores or I/O, by doubling the pipeline sets to two (default is one) we can double the indexing throughput capacity. Please follow Splunk guidelines on parallel pipelines. As shown in Figure 7, our testing revealed moving from one to two parallel pipelines increased indexing throughput significantly.

Scaling Memory on an Indexer

This is an indexing-only test; we did not enable search loads in this scenario. Scaling DRAM capacity also has a direct impact on the ingestion rate. With more DRAM available, write-through caching is enabled for the SSDs on all the nodes. Figure 9 illustrates our results when scaling DRAM on a system with five indexers and three search heads, performing a dense workload of 50 concurrent searches with pipelines set to one. Also shown in Figure 9, increasing DRAM from 192 GB to 384 GB can increase ingestion rate by up to 1.3x, while providing up to 14x improvement in search runtime.

![Image](Figure 7. Doubling the number of ingestion pipeline sets from one to two (parallel) provides the largest improvement in ingestion rates.)

![Image](Figure 8. The increase in aggregate data ingestion per day scales well across the Small, Medium, and Large test configurations when a parallel pipeline is added.)

Indexing-Intensive Workload Conclusion

- Two parallel pipelines increase indexing throughput by up to 73 percent. Adding extra pipelines beyond two contributes only a 20 percent increment in the ingestion rates.
- Scaling DRAM capacity also has a direct impact on the ingestion rates, resulting in up to 1.3x better indexing performance.
Search-Intensive Workloads

For workloads that mandate optimal search performance to maximize the number of concurrent search users, three of the tuning knobs available to enhance performance are:
- Increasing the ratio of search heads to indexers
- Increasing DRAM on the indexers (see Figure 9)
- Ability to turn hyper-threading on and off

Increasing the Number of Search Heads

Using a greater number of search heads (with search head clustering enabled), queries can be mapped onto more machines, thereby increasing the number of concurrent searches that can be performed. For the results shown in Figure 10, we used a 10-indexer configuration with the pipeline set to one and a data ingestion rate of 5 TB/day/indexer. In summary, adding just one more search head can support almost 2x more concurrent searches per minute.9

How Increasing the Number of Search Heads Affects Concurrent Search Performance

![Graph showing the impact of increasing the number of search heads on search rates.](image)

Figure 10. Impact of increasing the number of search heads on search rates.

Turning Hyper-Threading On or Off

Searches can take up to a physical core during execution time, and a higher core frequency can lead to faster searches. We performed a test by disabling hyper-threading on the indexers and search heads and measured search runtimes. As observed with other software products, hyper-threading enables about 30 percent more throughput (improved indexing rate); however, individual query response times are impacted (see Figure 11).

How Hyper-Threading Affects Search Runtimes

![Graph showing the impact of disabling hyper-threading on search runtimes.](image)

Figure 11. Disabling hyper-threading on the indexers and search heads can cut search times in half for compute-intensive dense searches.

Search-Intensive Workload Conclusion

- Adding an extra search head can support twice as many concurrent search users.
- Turning hyper-threading off can improve search runtimes by up to 2x.
- Turning hyper-threading on can improve search throughput by up to 30 percent.10
- Doubling DRAM capacity improves the search runtimes by 14x.

Learn More

Intel
- 2nd Generation Intel® Xeon® Scalable processors
- Intel® Optane™ SSDs
- Intel® SSD Data Center Family
- Intel® Ethernet Network Connection
- Transforming Intel’s Security Posture with Innovations in Data Intelligence White Paper

Splunk
- Splunk home page
- Splunk Enterprise
- Splunk savings calculator
- The Present and Future of Security Operations by the Splunk Enterprise Strategy Group

Contributors

These people helped in the engineering build by running tests and supplying hardware. Their contributions are greatly appreciated:

Data Platforms Group
- Rick Cnosson, Technical Program Manager
- Steve Richman, Engineer Manager
- Jason Stark, Technical Program Manager

Intel IT
- Victor Colvard, Infrastructure Engineer
- Jac Noel, Security Solutions Architect
- Elaine Rainbolt, Industry Engagement Manager

NAND Solutions
- Juan Fernandez, Solutions Specialist
- Frank Ober, Solution Architect
Appendix A: Test Environment

This appendix provides the details about the infrastructure setup for the validation runs and the testing bill of materials. We also elucidate details on how we configured the workload for Splunk Enterprise using the Splunk testing framework. Intel and Splunk jointly collaborate on these innovative architecture best practices.

The Splunk testing framework consists of a Test Controller, to which we specify user configurations, such as the number of searches to run, the type of search query, test execution time, and node configurations. The test controller, with the help of the cluster master, then deploys the workload on each of the test agents (search heads, indexers, and forwarders). This framework is shown in Figure A1.

Figure A1. Test suite setup.

The test suite consists of a set of tests that evaluate system performance. The performance numbers gathered with this suite are meant to serve as comparison points between different environments, workloads, or Splunk configurations. For example, this kit could be used to gauge how much of a performance boost can be achieved by moving from 12-core machines to 24-core machines, or by doubling the number of indexers.

The primary test case in this suite is a Longevity test, with a steady flow of data and a consistent scheduled search load. The Longevity test exposes the following parameters in the YAML files and/or on the command line, though this is not a comprehensive list:

- **test_duration_s.** The duration of the test specified in seconds.
- **indexer_gb_per_day.** Data volume per indexer, specified in GB/day.
- **indexers.** Number of indexers. If this is 3 or greater, then indexer clustering will be used.
- **search_heads.** Number of search heads. If this is 3 or greater, then search head clustering will be used.
- **forwarder_machines.** Number of machines used to handle data generation, and to run Splunk forwarders.
- **forwarders_per_machine.** Number of universal forwarders used to run on each forwarder machine, where data generation occurs.
- **scheduled_searches.** Includes the following parameters:
  - **max_searches.** Number of scheduled searches to create.
  - **search_string.** Search string for every scheduled search. This search string can be modified to run dense or super-sparse searches, as follows (sparse is also an option, but was not used in our testing):
    - Dense search (CPU-bound): “index=main every1 earliest=-1m | stats distinct _ count(id)”
    - Super-sparse search (I/O-bound): “index=main every100k earliest=-1h | stats distinct _ count(id)”
  - **cron_schedule.** Cron schedule of each scheduled search.

To measure the indexing and search performance, we used the following test metrics:

- Search runtime
- Ingestion rate
Test Configurations

We validated our solution on four configurations:

- **Departmental.** One indexer and one search head
- **Small.** Three indexers and two search heads
- **Medium.** Five indexers and three search heads
- **Large.** 10 indexers and three search heads

The benchmarking kit is composed of a module that generates log events on the forwarders. The forwarders used Intel® Xeon® processor E5-2699 v4 (22 cores per socket, two sockets) @ 2.2 GHz. The number of forwarders scales as we increase to larger configurations. To estimate the data generation rate, the event generation module can generate about 48 GB/sec of output on a 24-core system. We examined the different types of customer workloads and explored opportunities to tune configurations in accordance to resource requirements.

Table A1 details the reference configurations used in our typical enterprise environment.

**Table A1. Reference Configurations**

<table>
<thead>
<tr>
<th>ATTRIBUTE</th>
<th>DEPARTMENTAL-SCALE ENTERPRISE</th>
<th>SMALL-SCALE ENTERPRISE</th>
<th>MEDIUM-SCALE ENTERPRISE</th>
<th>LARGE-SCALE ENTERPRISE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incoming Data per Day (TB)</td>
<td>3–5</td>
<td>10–15</td>
<td>10–25</td>
<td>30–50</td>
</tr>
<tr>
<td>Maximum Concurrent Users</td>
<td>24</td>
<td>52</td>
<td>120</td>
<td>240</td>
</tr>
<tr>
<td>Indexer(s)</td>
<td>1</td>
<td>3</td>
<td>5</td>
<td>10</td>
</tr>
<tr>
<td>Search Head(s)</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>3</td>
</tr>
</tbody>
</table>

Bill of Materials

Table A2 provides the complete bill of materials used during our testing. We also recommend the following configuration settings:

- Enable a write cache for faster throughput and better ingestion rates.
- Use an ingestion rate of least 5 TB/day/indexer with search loads.
- Add more memory and compute to indexer heads helps to improve search and ingestion rates.
- Use a 10 GbE networking connection.
- Enable write-through caching for the disks on all the nodes.
- Disable Intel® Hyper-Threading Technology for search-intensive workloads.

**Table A2. Testing Bill of Materials**

<table>
<thead>
<tr>
<th>INDEXING TIER</th>
<th>QTY</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CPU</strong></td>
<td></td>
</tr>
<tr>
<td>Intel® Xeon® Platinum 8260 processor (24 cores, 2.4 GHz)</td>
<td>2</td>
</tr>
<tr>
<td>Memory</td>
<td></td>
</tr>
<tr>
<td>RDIMM 32 GB DDR4-2933</td>
<td>12</td>
</tr>
<tr>
<td><strong>Capacity Tier</strong></td>
<td></td>
</tr>
<tr>
<td>Intel® SSD DC P4510 8 TB 2.5&quot; NVMe U.2</td>
<td>2</td>
</tr>
<tr>
<td><strong>Boot Device</strong></td>
<td></td>
</tr>
<tr>
<td>Intel® SSD D3-S4510 Series 900 GB 2.5 SATA</td>
<td>1</td>
</tr>
<tr>
<td><strong>Network Interface Card (NIC)</strong></td>
<td></td>
</tr>
<tr>
<td>Intel® Ethernet Network Connection OCP X527-DA4 (10 GbE)</td>
<td>1</td>
</tr>
</tbody>
</table>

| SEARCH HEAD                          |     |
| **CPU**                              |     |
| Intel Xeon Platinum 8260 processor (24 cores, 2.4 GHz) | 2 |
| Memory                               |     |
| RDIMM 32 GB DDR4-2933                | 12  |
| **Capacity Tier**                    |     |
| Intel® Optane™ SSD DC P4800X 375 GB PCIe x4 U.2 | 1  |
| **Boot Device**                      |     |
| Intel SSD D3-S4510 Series 900 GB 2.5 SATA | 1  |
| **NIC**                              |     |
| Intel Ethernet Network Connection OCP X527-DA4 (10 GbE) | 1  |

<table>
<thead>
<tr>
<th>MANAGEMENT NODES (2 NODES): CLUSTER MASTER, TEST CONTROLLER</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CPU</strong></td>
<td></td>
</tr>
<tr>
<td>Intel® Xeon® Gold 6248 processor (20 cores, 2.5 GHz)</td>
<td>2</td>
</tr>
<tr>
<td>Memory</td>
<td></td>
</tr>
<tr>
<td>RDIMM 32 GB DDR4-2933</td>
<td>6</td>
</tr>
<tr>
<td><strong>Capacity Tier</strong></td>
<td></td>
</tr>
<tr>
<td>Intel SSD DC P4510 4 TB 2.5&quot; NVMe U.2</td>
<td>1</td>
</tr>
<tr>
<td><strong>Boot Device</strong></td>
<td></td>
</tr>
<tr>
<td>Intel SSD D3-S4510 Series 480 GB M.2 80mm</td>
<td>1</td>
</tr>
<tr>
<td><strong>NIC</strong></td>
<td></td>
</tr>
<tr>
<td>Intel Ethernet Network Connection OCP X527-DA4 (10 GbE)</td>
<td>1</td>
</tr>
</tbody>
</table>
1 Download the analyst reports: “Gartner 2018 Magic Quadrant for SIEM” and “Splunk Ranked No. 1 in IDC Worldwide SIEM Market Share 2018.”
3 For all performance claims: Testing by Intel as of August 1, 2019. Performance results are based on testing as of August 2019 and may not reflect all publicly available security updates. No product or component can be absolutely secure. See Table 1 for configuration information.

**Hardware Configuration:**
1x 2-socket Intel® Xeon® Platinum 8260 processor (24 cores, 48 threads) @ 2.4 GHz; 12 x 32 GB DDR4-2933 (total system memory 384 GB); Intel® Hyper-Threading Technology ON; Intel® Turbo Boost Technology ON; BIOS - SE5C620.86B.02.01.0008.031920191559; Microcode - OxS00001c; Storage Boot Drive - Intel® SATA SSD D3-S4510 480 GB, Cache Drive - Intel® Optane™ SSD P4800X 375 GB; Storage Application Drive - Intel® SSD DC P4510 Series 8 TB; NIC - 1x Intel® Ethernet Network Adapter X722.

**Software Configuration:**
OS - CentOS Linux release 7.6.1810 (Core); Kernel - 3.10.0-862.14.4.el7.x86_64; Splunk Enterprise Version - Splunk Core 7.2.5-088f.

**Benchmark:** SPLUNK Perf Kit/Longevity Test; Parameters - indexing_gb_per_day, test_duration_s, max_scheduled_searches; Output Column - Aggregate Data Ingestion/Day, # Successful Jobs/Min, Average Scheduled Search Run Time.

4 See endnote 3.
5 This number is an estimate derived from Intel’s experience testing other software applications.
6 See endnote 2.
7 Stearley, J., Corwell, S. and Lord, K., October 2010. “Bridging the Gaps: Joining Information Sources with Splunk.” In SLAML. pdfs.semanticscholar.org/3d7f/d06cc5c6e808330b1b0bb55c3568fd0914b.pdf
8 Splunk, “Turn data into answers with machine learning analytics,” splunk.com/en_us/software/splunk-enterprise.html
9 See endnote 3.
10 See endnote 5.

Software and workloads used in performance tests may have been optimized for performance only on Intel microprocessors. Performance tests, such as SYSmark and MobileMark, are measured using specific computer systems, components, software, operations and functions. Any change to any of those factors may cause the results to vary. You should consult other information and performance tests to assist you in fully evaluating your contemplated purchases, including the performance of that product when combined with other products. For more information go to intel.com/benchmarks.

Performance results are based on testing as of August 1, 2019 and may not reflect all publicly available security updates. No product or component can be absolutely secure.

Software and workloads used in performance tests may have been optimized for performance only on Intel microprocessors. Performance tests, such as SYSmark and MobileMark, are measured using specific computer systems, components, software, operations and functions. Any change to any of those factors may cause the results to vary. You should consult other information and performance tests to assist you in fully evaluating your contemplated purchases, including the performance of that product when combined with other products. For more information go to intel.com/benchmarks.

Performance results are based on testing as of August 1, 2019 and may not reflect all publicly available security updates. See configuration disclosure for details. No product or component can be absolutely secure.

Software and workloads used in performance tests may have been optimized for performance only on Intel microprocessors. Performance tests, such as SYSmark and MobileMark, are measured using specific computer systems, components, software, operations and functions. Any change to any of those factors may cause the results to vary. You should consult other information and performance tests to assist you in fully evaluating your contemplated purchases, including the performance of that product when combined with other products. For more information go to intel.com/benchmarks.

Intel processor numbers are not a measure of performance. Processor numbers differentiate features within each processor family, not across different processor families: Learn About Intel® Processor Numbers.

Cost reduction scenarios described are intended as examples of how a given Intel-based product, in the specified circumstances and configurations, may affect future costs and provide cost savings. Circumstances will vary. Intel does not guarantee any costs or cost reduction. Notice Revision #20110804

All information provided here is subject to change without notice. Contact your Intel representative to obtain the latest Intel product specifications and roadmaps.