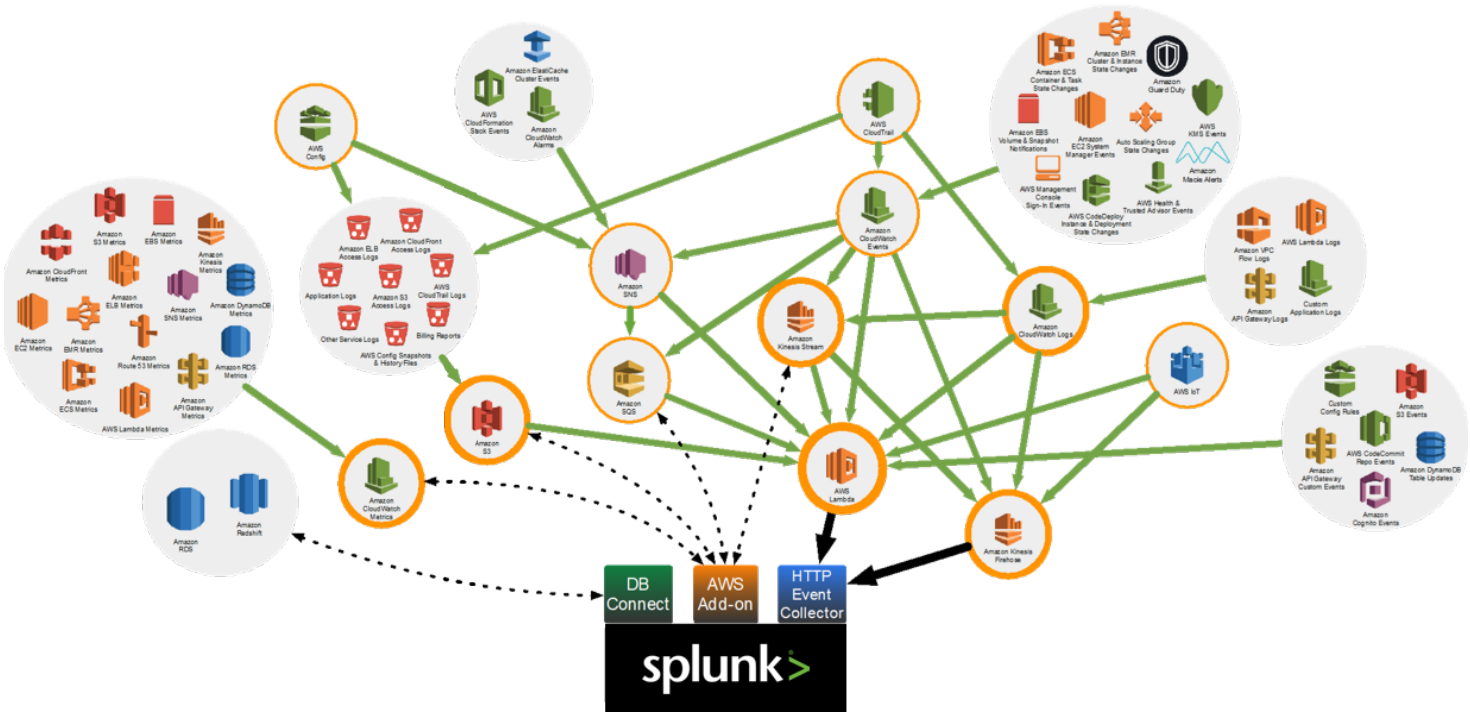


The Ultimate Guide

to Migrating Your Splunk On-Prem to Amazon Web Services

TekStream

Experts in Business & Digital Transformation

aws

splunk>

turn data into doing™

Contents

A Common Struggle

Maintaining physical, On-Premise (On-Prem) servers can be expensive. Between the hard cost of the On-Prem equipment and the soft labor cost to maintain these systems, it's no wonder that more businesses are taking their holistic digital ecosystem to the cloud.

This migration trend includes installing critical third-party applications like Splunk onto their cloud-based environment. This is a trend that Splunk themselves is supporting through a significant investment in its platform as well as an integrated partnership with industry-leading cloud-based platforms – specifically Amazon Web Services (AWS).

This is excellent news for companies that are already utilizing Splunk within their On-Prem environment but want to enjoy the benefits of a cloud-based platform like AWS. To further support the varied needs of its customer base, Splunk also offers Splunk Cloud, a cloud service layered onto AWS backed by a 100% uptime service level agreement.

Thinking about migrating your Splunk application to the cloud? Here are of the most common questions we hear from our client base on this subject. Do they sound familiar?

- **How do we handle licensing in this new environment? What new models should we consider?**
- **How much will this cost?**
- **Who will oversee the migration? What are the decisions that need to be made?**
- **How do we ensure that we don't have any downtime in Splunk monitoring?**
- **What pitfalls should we aim to avoid?**
- **What new capabilities and benefits will we gain from moving to a cloud-based environment?**
- **Where do we even start?**

In this eBook, we'll walk through some of key benefits and considerations for migrating your Splunk On-Prem installation to an AWS environment. We'll also detail out our step-by-step approach to ensuring your migration happens on-time and under budget.

Why AWS?

AWS is the world's most comprehensive cloud platform and serves the IT needs of companies across the globe. From Fortune 1,000 enterprise companies to small businesses and entrepreneurial startups, AWS is one of the most broadly adopted cloud platforms available in the market.

More and more enterprise companies are migrating their critical workloads away from an On-Prem infrastructure to an AWS environment. Why?

Key Benefits of AWS

While several distinct factors work together to determine whether or not a migration to AWS is ideal for your specific needs, the list below outlines the most common and compelling reasons why companies are making the switch to AWS for their infrastructure needs.

Security

As unfortunate as it is, it appears data breaches are becoming more of a common occurrence. Every week it seems there's another breaking headline announcing that there has been another company or organization that has had their data breached by a third-party.

Data breaches are expensive. Not only in terms of capital costs (fees/penalties) but also in terms of the loss of consumer/vendor trust that comes as a consequence of a security breach.

To that end, AWS has built a best-of-breed security platform for their cloud product. This includes:

- 24x7 staffed data centers with privileged access
- Tracked activity by different users through IAM and CloudTrail
- Multi-factor authentication
- Built-in firewall rules that can be custom configured based on your data protection needs

More and more enterprise companies are migrating their critical workloads away from an On-Prem infrastructure to an AWS environment.

Cost-Effective

With AWS, you pay based on your actual usage. No more fixed server cost or On-Prem monitoring fees. Your cost structure scales as your business scales, providing your company with an affordable option that correlates with its current needs.

Procurement and Scale

With AWS, you can spin-up a new server within a matter of minutes compared to the time it takes (hours to days) to procure a new traditional server.

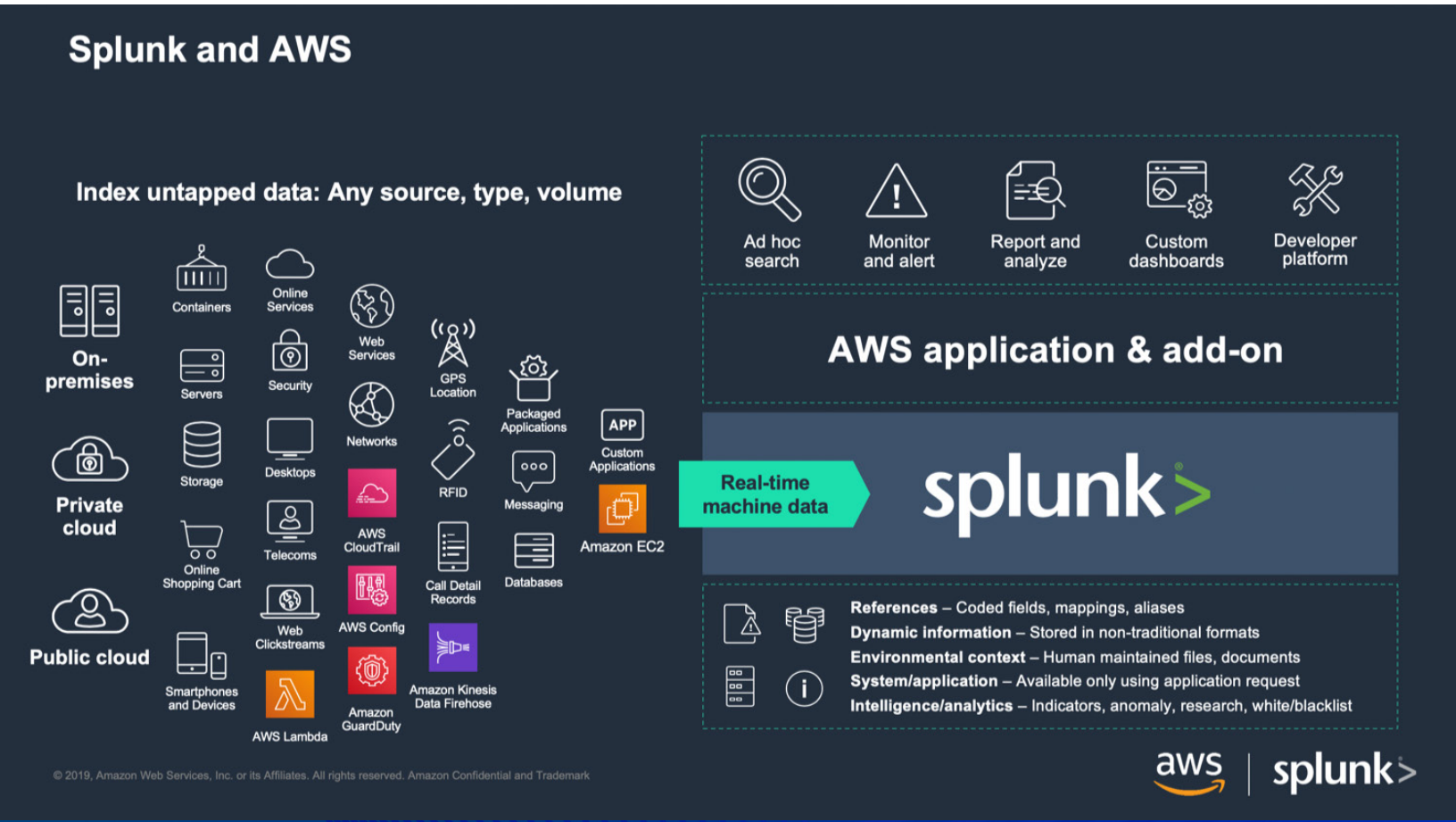
Flexibility

AWS allows its users to select their preferred operating system, programming language, database, and other vital preferences. Users have the flexibility they need to create their preferred environment, easing the migration process while preserving opportunities for future growth.

Multiple Migration Options

Depending on your unique business and tech stack needs AWS offers companies multiple options for realizing its host of benefits. For Splunk those options include:

1. Migrate your Splunk On-Prem directly to AWS
2. Migrate your Splunk On-Prem to Splunk Cloud (which sits on AWS)



Benefits and Features of Migrating Splunk to AWS

If you're a Splunk Enterprise user, you're no doubt already familiar with many of the core benefits and features of the Splunk platform. From world-class monitoring to in-depth visibility, thousands of companies across the globe utilize Splunk to support their digital ecosystem. Now you can take that critical workload to your AWS environment.

Key Benefits of Migrating Splunk On-Prem to AWS

Whether you choose to migrate your Splunk On-Prem directly to AWS or to Splunk Cloud, here are just a few benefits to deploying and migrating Splunk onto AWS.

Comprehensive Visibility

Splunk offers a series of pre-built integrations and add-ons that layer perfectly with the AWS environment. Anyone familiar with AWS will know that to ensure full visibility, it's critical to have a fundamental understanding of Amazon CloudWatch, AWS CloudTrail, VPC Flow Logs, and other essential AWS systems, events and logs.

Through the Splunk Add-On for Amazon Web Services, you can pull data from across your AWS system directly into Splunk through a single tool. Which, in turn, makes it easier for you to monitor and manage your AWS ecosystem. The Splunk App for AWS also provides dashboards and reports *on* the data that the Splunk Add-On for Amazon Web Services pulls in.

Troubleshooting/Triage

Splunk's machine learning capabilities make it an ideal tool for troubleshooting and investigation. Through Splunk, teams can more quickly analyze logs, events, and alerts to help troubleshoot complex issues.

Splunk can analyze your AWS environment in real-time to help identify and triage errors and issues as they occur. This can add up to huge savings as your team no longer has to spend hours (or even days) manually reviewing logs and reports.

Security and Compliance

Cloud migration can add new challenges to an organization's ability to maintain security and compliance including adding operational complexity and increasing the attack surface to help mitigate threat actors. Splunk offers its users a variety of tools including Splunk Security Essentials and Splunk ES Content Updates.

Further, Splunk integrates with more than 500 security sources and products, including several common AWS services and data types like Amazon GuardDuty, AWS Security Hub, and others. These integrations can help protect your data both during and after the migration process.

Splunk integrates with more than 500 security sources and products

Scalability

Unlike deployment onto an On-Prem device, your Splunk implementation can automatically scale as your needs scale. Not only does this help to ensure consistent monitoring and analysis across your growing ecosystem, but it also saves time and energy by removing the need to manually configure your Splunk environment to account for new On-Prem servers and data streams.

Even better, AWS also has automated scripts that can spin up new environments quickly and with minimum oversite.

Further, AWS also allows you to scale how you use Splunk by easing the time it takes to add additional capacities or nodes within your Splunk environment. This provides further flexibility to scale as your ingestion and search needs fluctuate.

Identify Cost Saving Opportunities

Splunk's in-depth topology view provides your team with a graphical representation of your current AWS deployment. Through this dashboard, your team can identify:

- Whether or not you have too many instances in a single VPC
- Whether or not you have too many security groups
- If your EC2 instances are secured in your private and public subnets
- If autoscaling is working as expected
- The relationships between your policies, groups, and IAM users
- Other vital data points

Having clear visibility into your AWS deployment can help to identify critical opportunities for resource redeployment and cost savings.

Additional Core Benefits

Cost-savings and scalability are important, but they don't represent all of the benefits of migrating your Splunk environment to AWS. Other core migration benefits include:

- AWS provides built-in fault tolerance and high availability, reducing the need to do that within Splunk (by utilizing AWS regions and Splunk SmartStore on AWS S3)
- You can reuse your existing Splunk Licenses (BYOL)
- Alternatively, you can explore new cost-effective license options

Key Considerations of Migrating Splunk to AWS

It's easy to get caught up in the benefits of migration. After all, who doesn't love efficiencies and cost savings? However, before you start exploring options, it's essential to note the key considerations that need to be thought through prior to beginning any AWS migration effort.

These key considerations include:

Lift-and Shift or Move-and-Improve

Before you begin to consider a migration, take an in-depth look at your system to determine whether you should choose to rebuild your Splunk environment on AWS in the same way as you had it setup On-Prem or take the opportunity to "build it better" by rearchitecting it first.

Migration Plan and Timeline

Always start with the end in mind, taking the time upfront to build out your migration plan and its correlating timeline. Consider any specific internal dates or key milestones that will affect your AWS deployment. You'll also need to determine whether or not you choose to migrate your Splunk environment directly to AWS or to Splunk Cloud (on AWS).

Key Aspects of the Lift-and-Shift Model

- It is easy to replicate On-Prem infrastructure within AWS.
- Your Splunk application can coexist with On-Prem during the migration (ensuring you can still actively monitor your systems during the migration).
- Of the two options, the lift-and-shift is the least time-intensive.

Key Aspects of the Move-and-Improve Model

- You'll upgrade to the latest version of Splunk.
- You can re-architect the environment from the ground up to take advantage of AWS capabilities.
- You can choose from several different instance sizes.
- You can leverage Splunk SmartStore to reduce storage requirements and costs (up to 75% or more).
- You can explore multi-site clusters across AWS regions.

Data Migration

In addition to developing your project management plan, you'll also need to put together a strategy for how you're going to manage and migrate any On-Prem data to AWS. Our experience shows that there are two common ways to handle data migration as it relates to Splunk.

Move the Data to Amazon Web Services

- Point forwarders to AWS indexers
- Decommission On-Prem indexers and search heads sooner
- The logistics of getting large amounts of data to AWS can be challenging (but there are several options)

Leave it On-Prem

- New data will go to AWS indexers
- Old data stays in existing On-Prem indexers
- Search heads set up as 'hybrid' to search both sets of indexers (may require inbound firewall rules)
- Requires leaving at least indexers (and maybe search heads) in service until 'old' data naturally ages out and is deleted
- Defers cost savings (and may temporarily increase costs)

Your Splunk Environment

As you build your migration plan, pay attention to how your Splunk environment is setup. Specifically, carefully consider your distributed and clustered Splunk environments. Here too, you'll want to consider whether your aim is to rebuild or recreate the same environment within AWS or Splunk Cloud.

Budget

Does your company have the budget to support an AWS migration? If so, at what level of investment? When determining your budgetary window, it's helpful to also consider the cost-savings of AWS versus your current legacy On-Prem system over time.

Employee Resourcing

Who on your team has the expertise, and the time, to see through the migration? Also, who on your team has the technical (AWS) experience to do the migration?

Any successful business initiative must have an owner assigned to it. Someone who has the direction, vision, and accountability to see the migration through to completion.

Unsure where to begin answering these questions? We can help. We've worked through hundreds of deployments and migrations and have the expertise and tribal knowledge needed to ensure a successful Splunk to AWS migration.

Who on your team has the expertise, and the time, to see through the migration?

TekStream's Holistic Approach to Migrating Splunk to AWS

As an AWS Partner Network Consulting Partner with Splunk Premiere status (an uncommon combination in the industry), TekStream has deep experience in executing complex data migrations (including Microsoft, Oracle, and Splunk) to AWS. We understand that the thought of digital change and transformation can be daunting. That's why we partner with our clients to guide them through a proven onboarding process from quote to migration execution, to ongoing support.

It's this commitment to our customer's experience that leads to 97% of our customers reengaging with us time and time again. As your technical advisor, we aim to help you make the best decision for your budget and goals.

Every digital transformation journey is challenging; TekStream gets you there.

Why TekStream?

Why should you choose TekStream to help guide your Splunk migration to AWS?

Licensing Expertise

TekStream has extensive experience navigating the ins and outs of complex license structures and contracts. We can help you analyze, review, and negotiate both current and new licenses and contracts.

As your advisory partner, TekStream will work with you to ensure that your Splunk and AWS licenses are in order.

The four most common licensing structures are:

- **Option 1:** Migrate Your Existing Perpetual or Term License to AWS
- **Option 2:** Convert Your Current License to Splunk Cloud (which would run on AWS)
- **Option 3:** Convert to a Term or Infrastructure License (if on a Perpetual License)
- **Option 4:** Pay-As-You-Go as part of a 3rd-Party Hosted MSP Solution

Through careful analysis of your current licensing structures and your desired future state, we will work with you to determine the optimal licensing structure.

Consulting Expertise

TekStream's deep experience overseeing complex data migrations empowers us to act as true consultative partners through all of our engagements. We have the experience needed to quickly scope challenges and present solutions for your unique situation

TekStream Guarantee

Take the risk out of your Splunk migration to AWS. We are confident in our battle-tested process and proven Splunk migration process. So much so, that we guarantee that your Splunk migration will be completed on-time and on-budget when using TekStream's Proven Process. We also guarantee optimal and cost-effective license and cloud subscriptions.

Single Contact Source

When you begin working with TekStream, we'll assign you to a single point of contact for your business consulting, migration, and Managed Services needs. This single contact source will act as your liaison and guide you through the migration process.

Analyze Your Existing Applications and Goals

As your advisory partner, TekStream will perform a detailed analysis of your current Splunk environment and what is available on the AWS cloud. We'll also work with you to identify your migration goals and desired future state. From there, we'll create a project roadmap to successfully and securely migrate your business to the cloud.

Create a Project Roadmap

Once the analysis is complete, we'll develop a detailed set of tasks and timelines to ensure that your AWS migration needs are met on-time and on-budget. Your project roadmap will also lay out the resources required (from both your team and ours) to ensure all tasks are completed as per the timeline.

Begin the Migration Processes

Once the roadmap has been approved, TekStream will begin completing the critical steps and prerequisites needed to begin the AWS migration process.

Migrate Data and Validate

Moving data and ensuring its accuracy requires experience, time, and patience. Once your AWS environment has been properly set up, TekStream will begin migrating your Splunk data and configurations to your new cloud.

As a note, many organizations use this opportunity to assess and cleanse their data to reduce bloat and move only the most essential data.

Test, Retest, and Test It Again

After moving your Splunk application to the cloud, our team of subject matter experts will run a series of QA, integration, and validation tests to ensure your application is working properly before allowing users to access it.

Go-Live Support and Beyond

From an end-user perspective, Splunk will work the same way on AWS as it does on your On-Prem hardware. However, moving to the cloud will change the back-end infrastructure of the system. As your long-term partner, TekStream is committed to ensuring your transition to the cloud is successful both at launch and beyond.

Ready to Get Started?

Whether you are brand new to AWS or have already migrated some of your digital ecosystem to the cloud, TekStream stands ready to ensure your Splunk migration to AWS is completed on-time and within your budget.

Contact us today to begin your migration assessment. Together, our certified Splunk and AWS experts will work with you to scope and analyze how best to migrate your specific Splunk environment to AWS.

TekStream accelerates your digital transformation by navigating complex technology environments. We guide your decisions, quickly implement the right technologies with the right people, and keep it running for sustainable growth.

To learn more about how TekStream can assist with your Splunk to AWS migration, contact us today.

Find Out More

TekStream continues to grow and bring innovative software solutions to our clients to meet new business demands. Stay up to date of new services, software, and support offerings:


www.tekstream.com


Info@tekstream.com


678-708-4900


Sales@tekstream.com