



AWS Splunk Environments:

A step by step guide to empowering collaborative community learning



Your Presenters



Aleem Cummins

Community Enablement Warrior

Independent

@aleemcummins

<https://www.linkedin.com/in/aleemcummins>

SplunkTrust
Splunk User Group London
Splunk Study Club



<http://slack.splunkstudy.club>



Suman Gajavelly

CTO / Co-founder

BitsIO Inc

@sumangajavelly

<https://www.linkedin.com/in/sumangajavelly>

Fort Worth Splunk User Group



<https://github.com/SplunkStudyClub>



splunk>

Session Agenda

AWS

- Sign Up
- Security
- Instances
- Access

Splunk

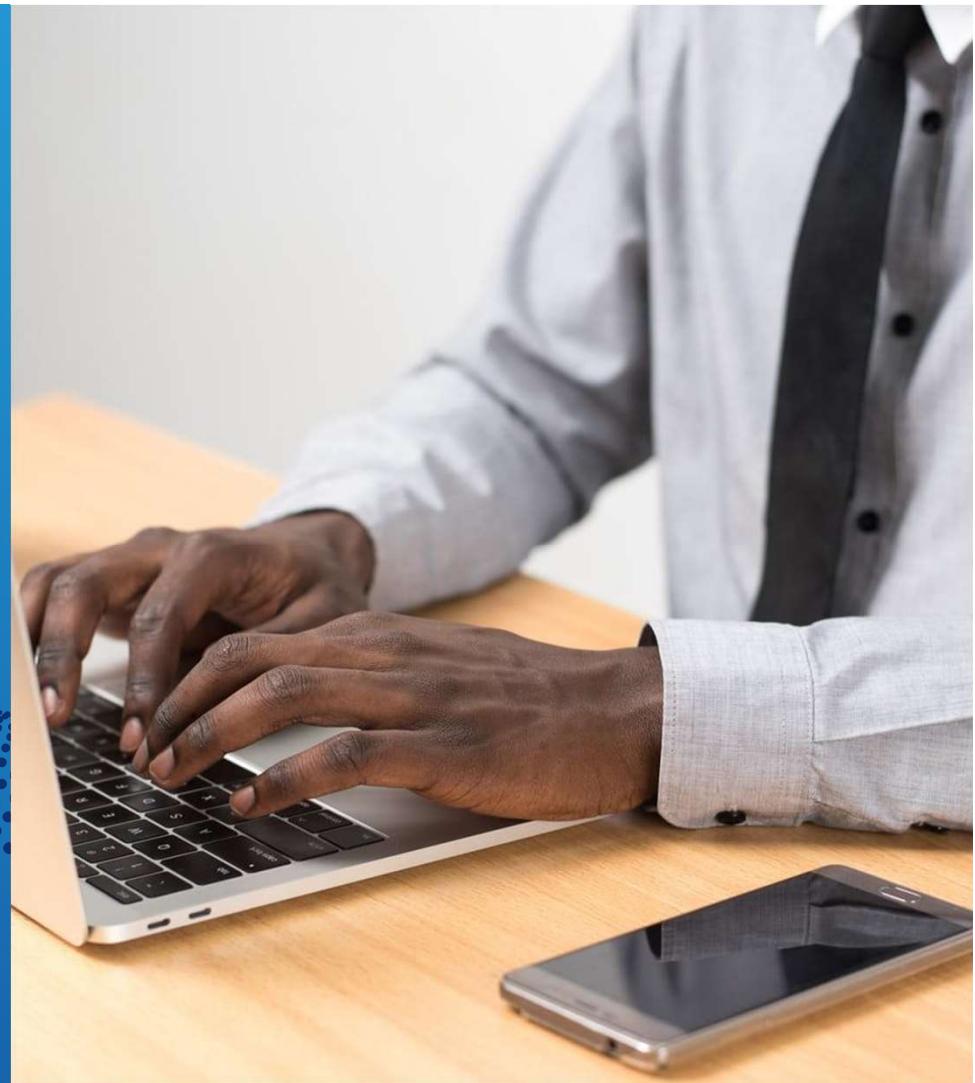
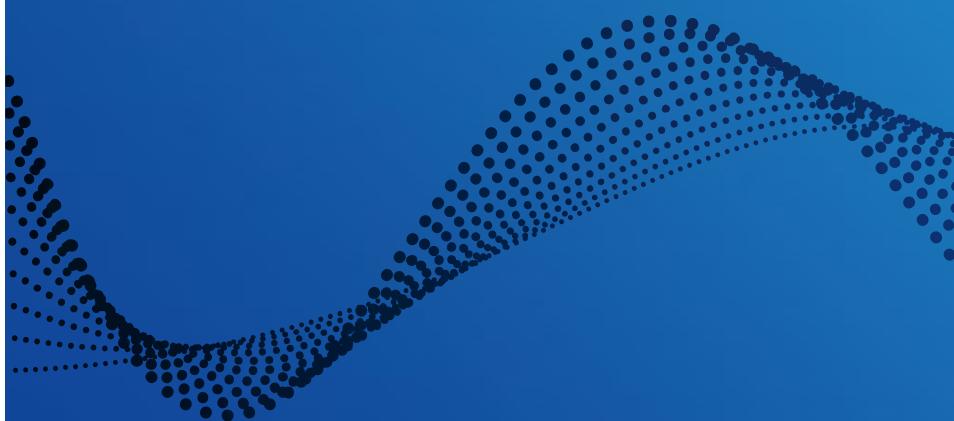
- Deployment
- Growth
- Study Club

Keeping Lights On

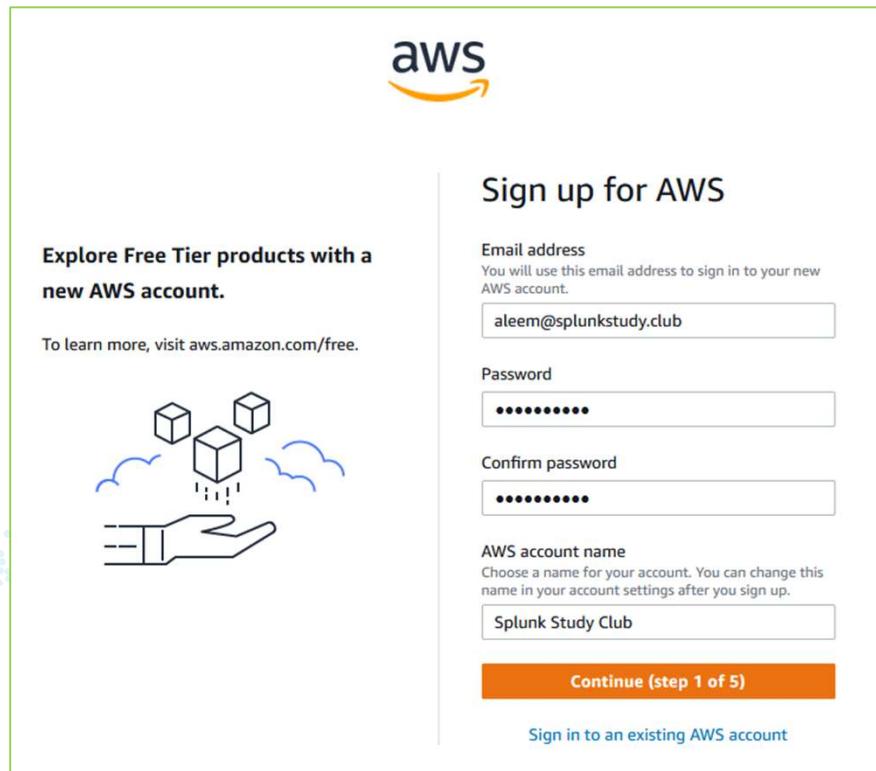
- DNS Scripts
- Splunking DNS Logs
- Lambda Functions

AWS

Sign Up



<https://aws.amazon.com>



The image shows the AWS sign-up form. At the top right is the AWS logo. Below it, the heading "Sign up for AWS" is displayed. The form consists of several input fields:

- Email address:** aleem@splunkstudy.club
- Password:** [REDACTED]
- Confirm password:** [REDACTED]
- AWS account name:** Splunk Study Club

At the bottom of the form are two buttons: "Continue (step 1 of 5)" in orange and "Sign in to an existing AWS account" in blue.

aws

Sign up for AWS

Contact Information

How do you plan to use AWS?

Business - for your work, school, or organization
 Personal - for your own projects

Who should we contact about this account?

Full Name

Phone Number

Country or Region

Address

Apartment, suite, unit, building, floor, etc.

City

State, Province, or Region

Postal Code

I have read and agree to the terms of the AWS Customer Agreement [\[?\]](#).

Continue (step 2 of 5)

aws

Sign up for AWS

Billing Information

Credit or Debit card number

VISA    

AWS accepts all major credit and debit cards. To learn more about payment options, review our [FAQ](#).

Expiration date

Cardholder's name

Billing address

Use my contact address

Use a new address

Verify and Continue (step 3 of 5)

You might be redirected to your bank's website to authorize the verification charge.

aws

Sign up for AWS

Confirm your identity

Before you can use your AWS account, you must verify your phone number. When you continue, the AWS automated system will contact you with a verification code.

Country or region code

Mobile phone number

Security check

Type the characters as shown above

Send SMS (step 4 of 5)

aws

Sign up for AWS

Confirm your identity

Verify code

Continue (step 4 of 5)

Having trouble? Sometimes it takes up to 10 minutes to retrieve a verification code. If it's been longer than that, [return to the previous page](#) and try again.

aws

Sign up for AWS

Select a support plan

Choose a support plan for your business or personal account. [Compare plans and pricing examples](#)
[You can change your plan anytime in the AWS Management Console.](#)

<input checked="" type="radio"/> Basic support - Free <ul style="list-style-type: none">Recommended for new users just getting started with AWS24x7 self-service access to AWS resourcesFor account and billing issues onlyAccess to Personal Health Dashboard & Trusted Advisor 	<input type="radio"/> Developer support - From \$29/month <ul style="list-style-type: none">Recommended for developers experimenting with AWSEmail access to AWS Support during business hours12 (business)-hour response times 	<input type="radio"/> Business support - From \$100/month <ul style="list-style-type: none">Recommended for running production workloads on AWS24x7 tech support via email, phone, and chat1-hour response timesFull set of Trusted Advisor best-practice recommendations 
--	--	---

Need Enterprise level support?
From \$15,000 a month you will receive 15-minute response times and concierge-style experience with an assigned Technical Account Manager. [Learn more](#)

Complete sign up

aws

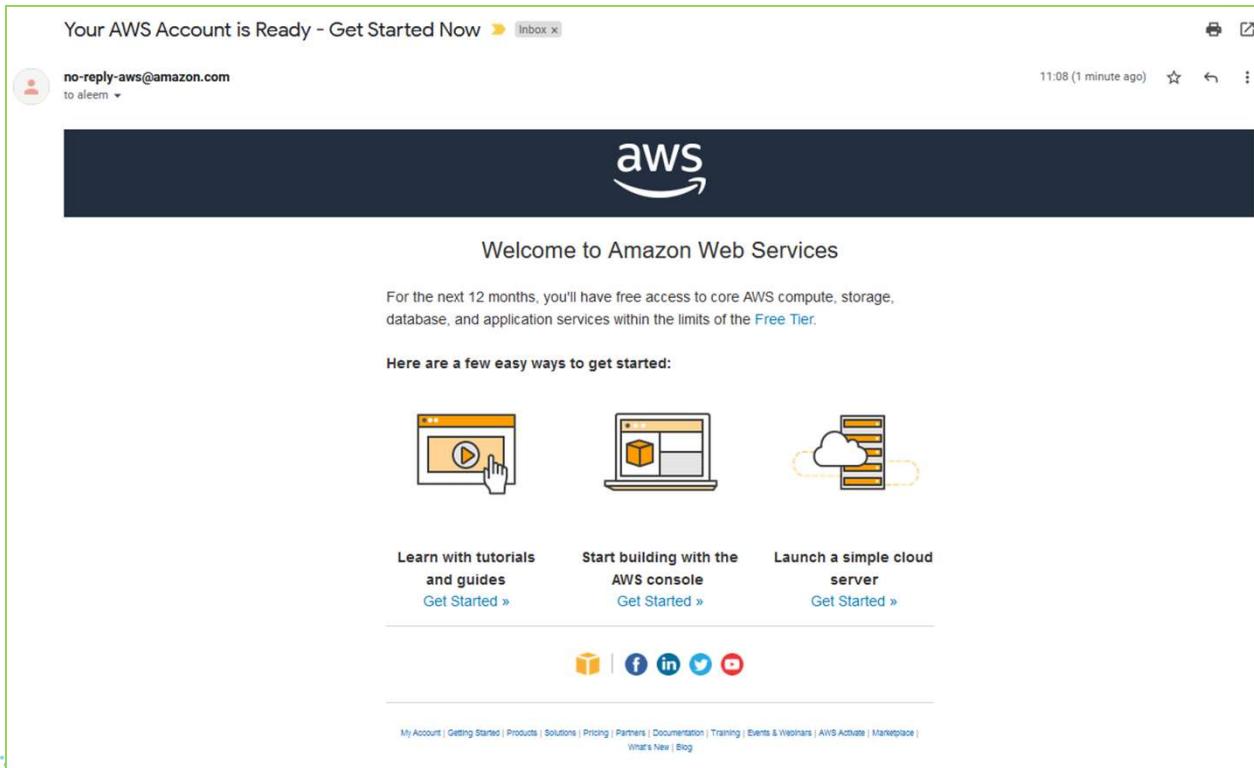


Congratulations

Thank you for signing up for AWS.
We are activating your account, which should only take a few minutes. You will receive an email when this is complete.

Go to the AWS Management Console

[Sign up for another account](#) or [contact sales](#).



Wait for this email to come through



<https://signin.aws.amazon.com/>

aws

Sign in

Root user
Account owner that performs tasks requiring unrestricted access. [Learn more](#)

IAM user
User within an account that performs daily tasks. [Learn more](#)

Root user email address

Next

By continuing, you agree to the [AWS Customer Agreement](#) or other agreement for AWS services, and the [Privacy Notice](#). This site uses essential cookies. See our [Cookie Notice](#) for more information.

New to AWS? [Create a new AWS account](#)

aws

Security check

For security reasons, we need to verify that account holders are real people.

Type the characters seen in the image below



Submit

aws

Root user sign in [e](#)

Email: aleem@splunkstudy.club

Password [Forgot password?](#)

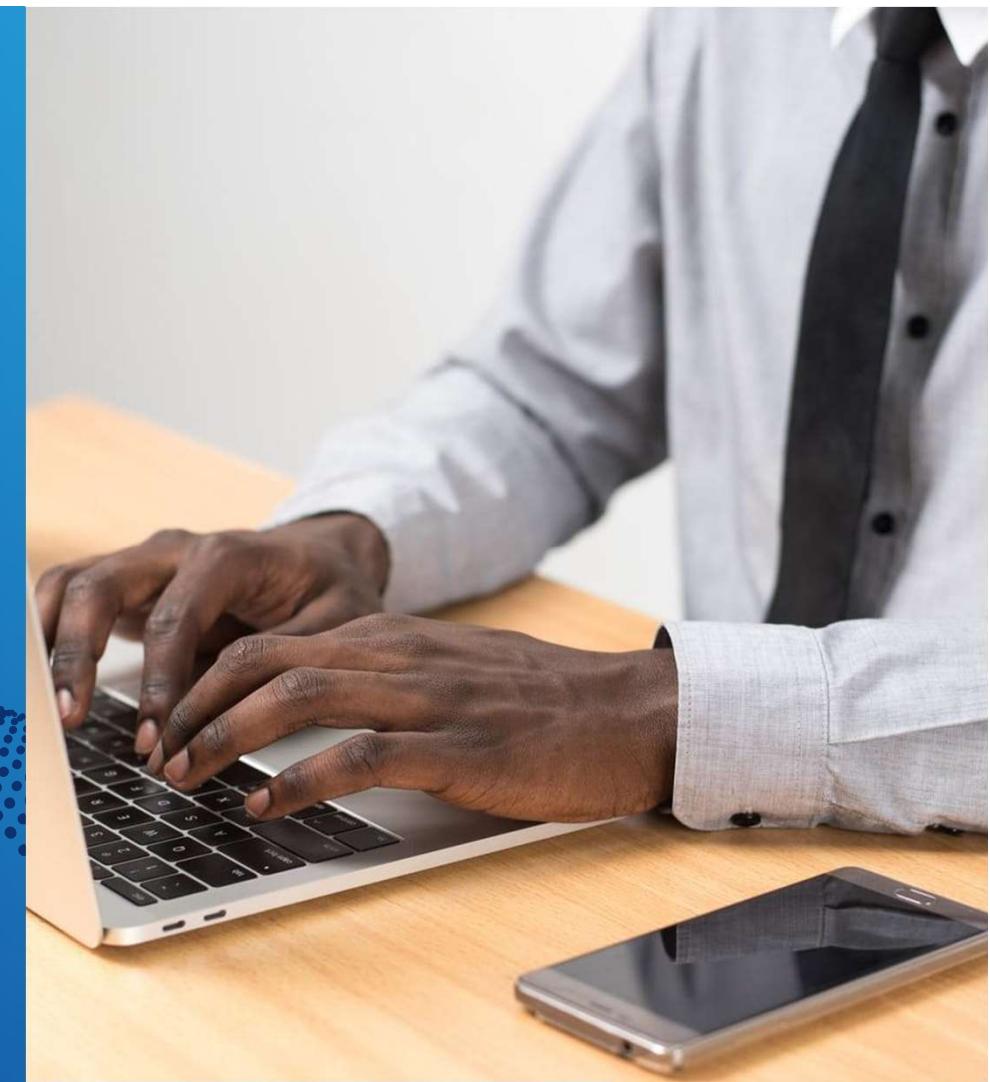
Sign in

[Sign in to a different account](#)

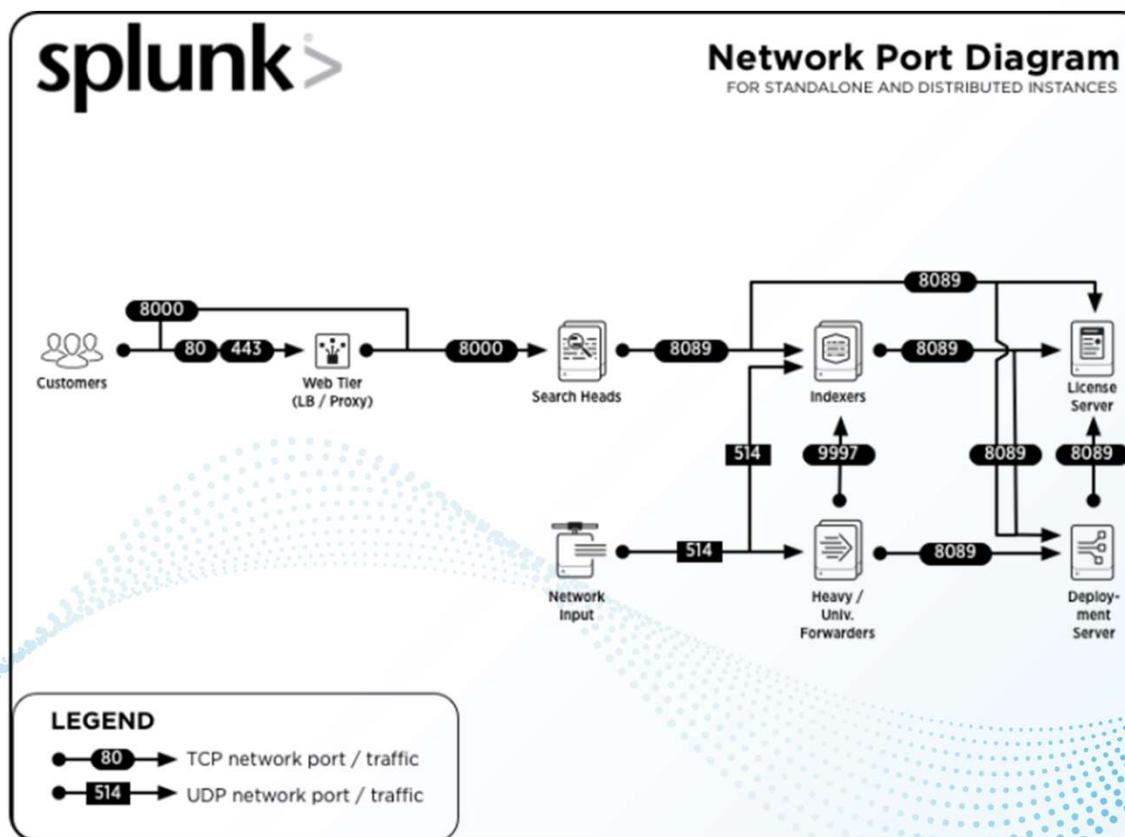
[Create a new AWS account](#)

AWS: Security

SecurityGroups



Splunk Enterprise Components: Network Connectivity



<https://docs.splunk.com/Documentation/Splunk/8.1.3/InheritedDeployment/Ports>

BSIDES

splunk>

Splunk Enterprise Components: Network Connectivity

Component	Purpose	Communicates on	Listens on
All components*	Management / REST API	N/A	TCP/8089
Search head / Indexer	Splunk Web access	Any	TCP/8000
Search head	App Key Value Store	Any	TCP/8065, TCP/8191
Indexer	Receiving data from forwarders	N/A	TCP/9997
Search head cluster member	Cluster replication	N/A	TCP/8081, TCP/9887, TCP/8181
Indexer cluster peer node	Cluster replication	N/A	TCP/8080, TCP/9887
Heavy Forwarder or Indexer	Receiving data over HTTP Event Collector (HEC)	N/A	TCP/8088

<https://docs.splunk.com/Documentation/Splunk/8.1.3/InheritedDeployment/Ports>



AWS SecurityGroup

Splunk Enterprise-8-1-3-AutogenByAWSMP

Default AWS Marketplace SecurityGroup based on recommended settings for Splunk Enterprise version 8.1.3 provided by Splunk

Inbound Rules

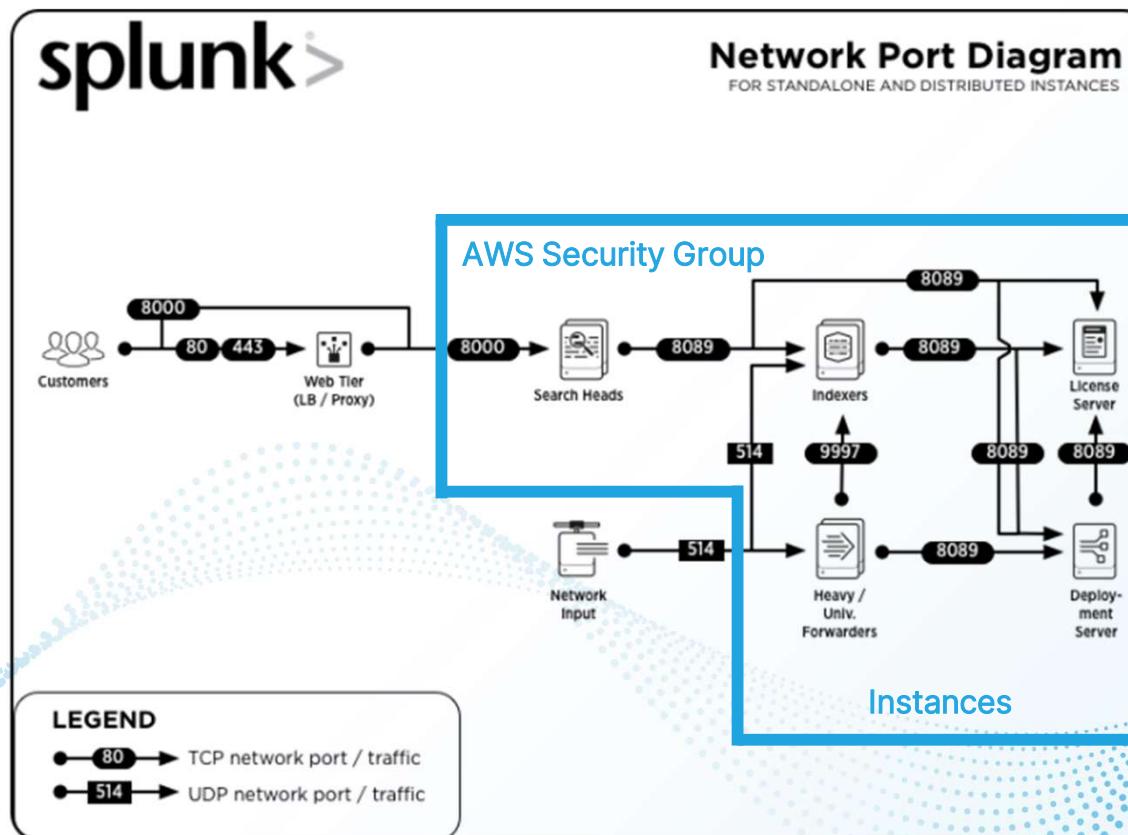
Type	Protocol	Port Range	Source
Custom TCP	TCP	8000	0.0.0.0/0
Custom TCP	TCP	554	0.0.0.0/0
SSH	TCP	22	0.0.0.0/0
Custom TCP	TCP	8089	0.0.0.0/0
Custom TCP	TCP	9997	0.0.0.0/0
HTTPS	TCP	443	0.0.0.0/0

Outbound Rules

Type	Protocol	Port Range	Destination
All Traffic	All	All	0.0.0.0/0



All Splunk instances should be in same Security Group



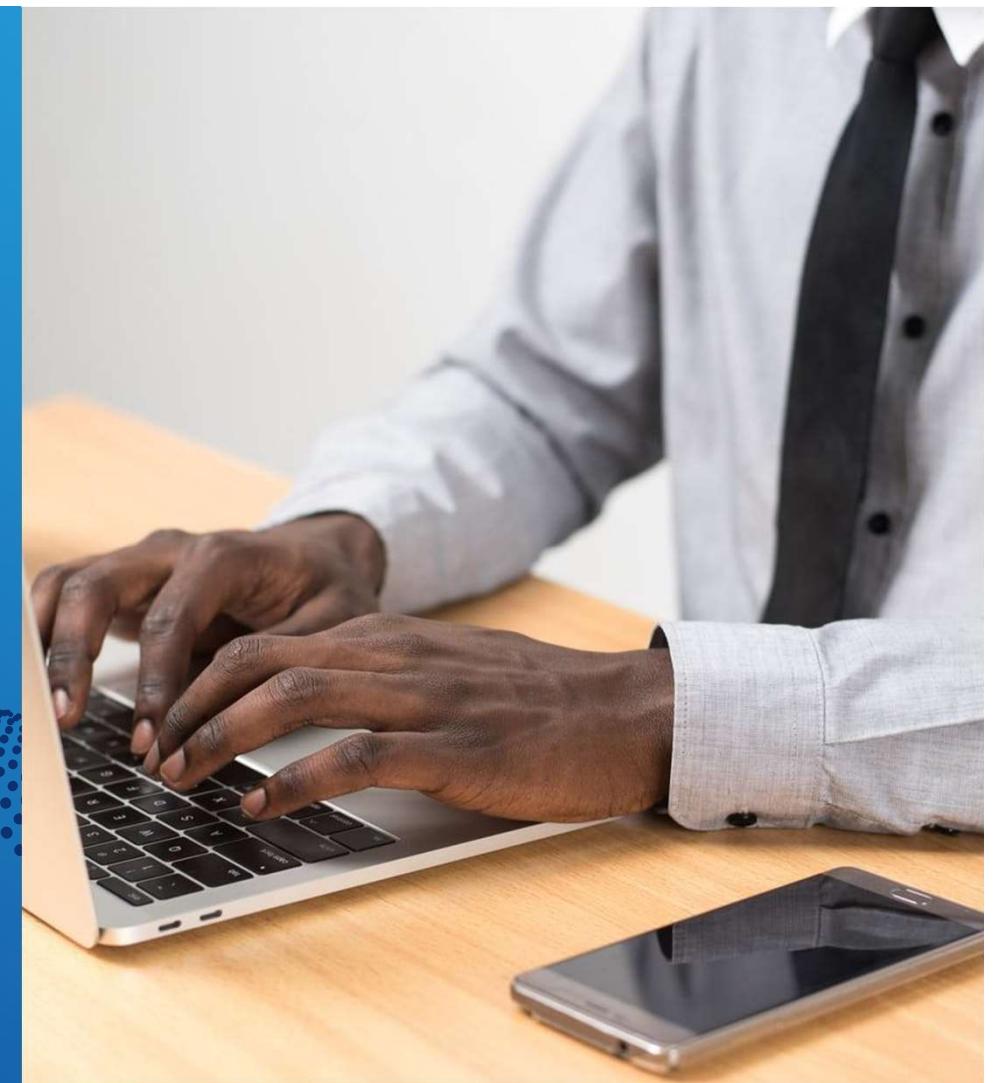
<https://docs.splunk.com/Documentation/Splunk/8.1.3/InheritedDeployment/Ports>

BSIDES

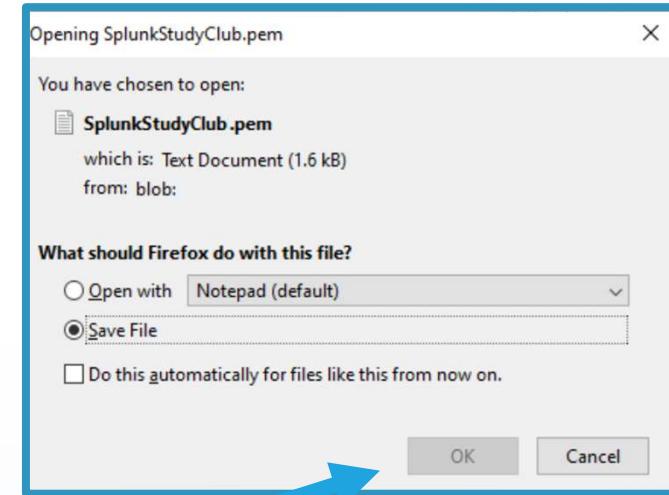
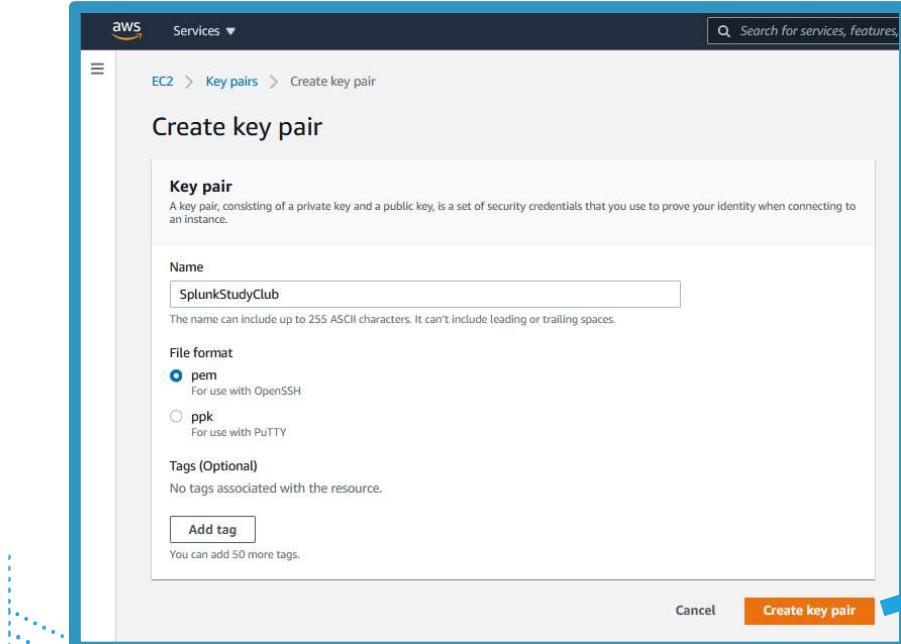
splunk>

AWS: Security

Keys



Create Key Pair



Only downloadable on creation. Keep safe!

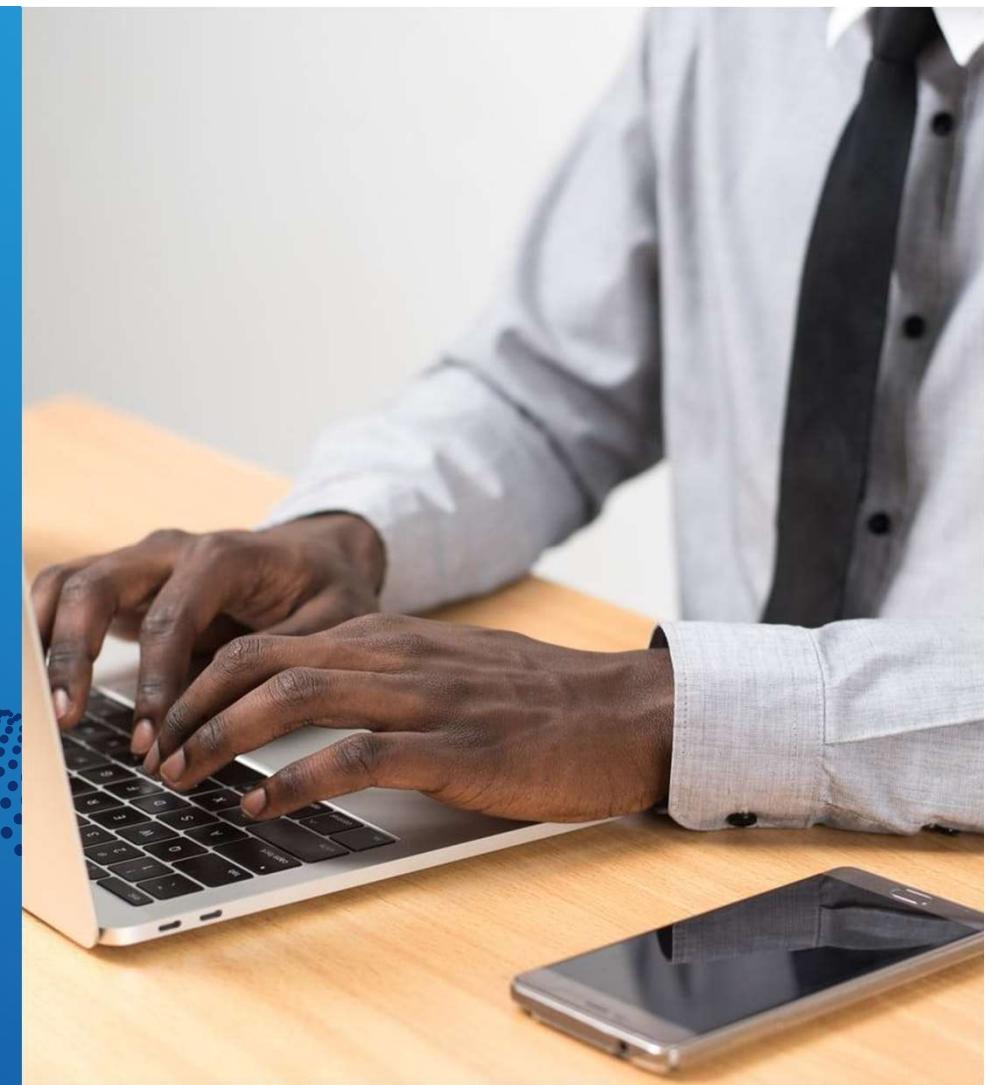
Permissions on download

Permissions required



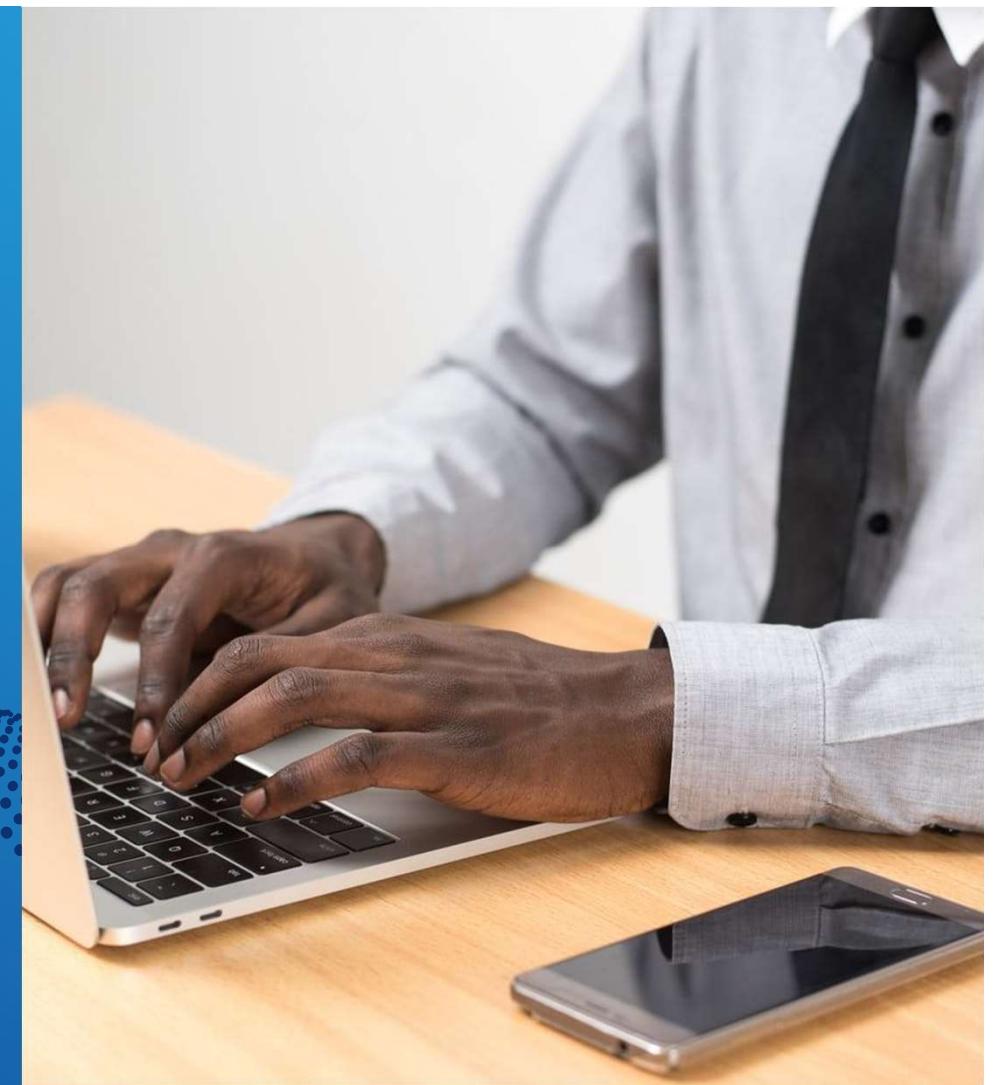
Create an Instance

Demo



AWS: Security

Access



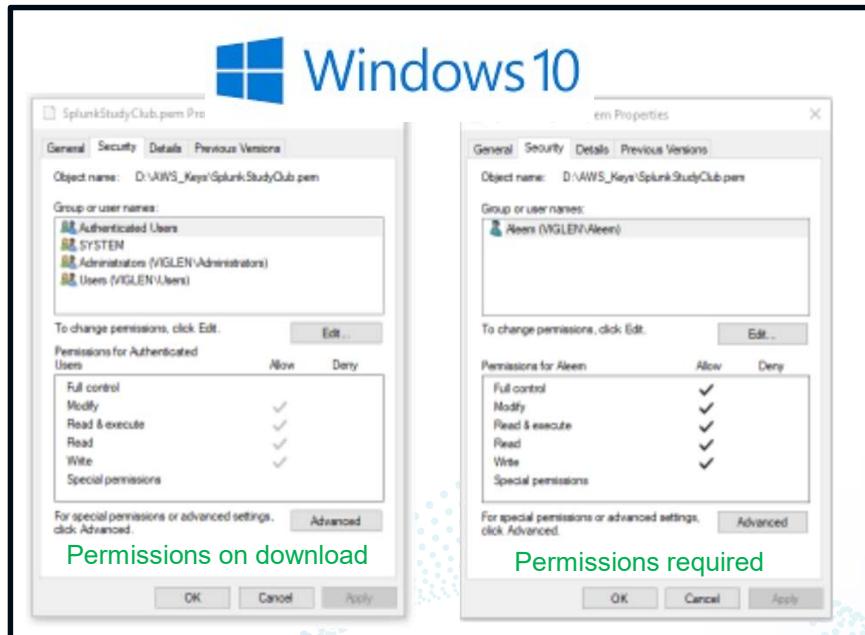
Accessing an AWS Instance

This will require an SSH client. Free examples include:

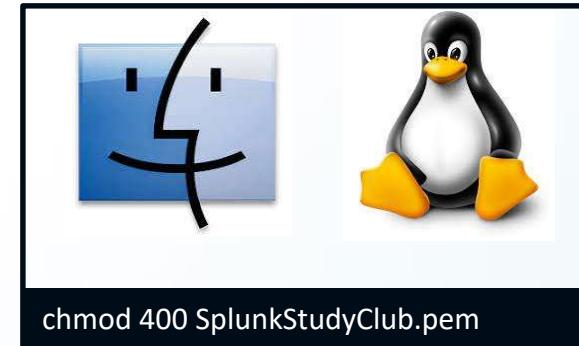
Name	OS	Download
PuTTY	Windows	https://www.putty.org
MobaXterm	Windows	https://mobaxterm.mobatek.net
Terminal	Mac	Built into Mac OS
iTerm2	Mac	https://iterm2.com

Set Key Permissions

Permissions must be made restrictive to work with AWS via a SSH client

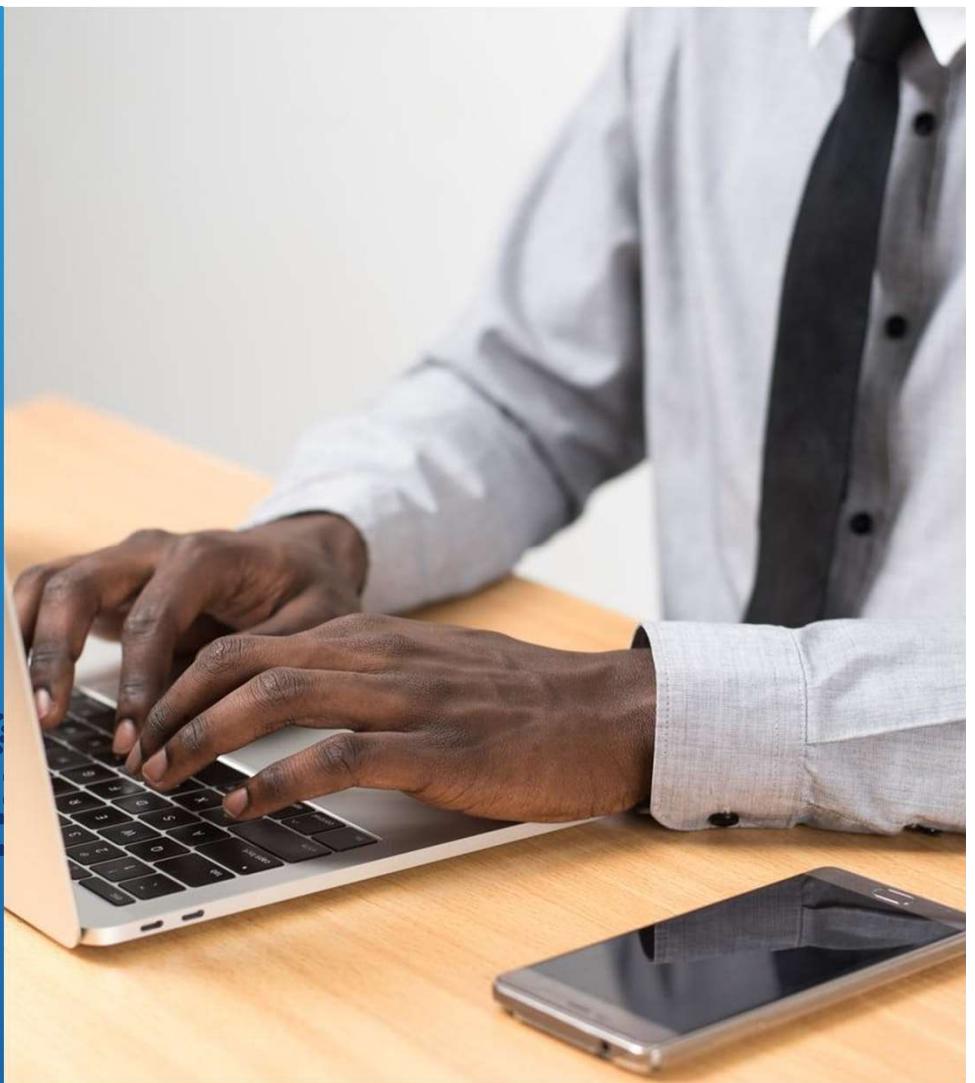
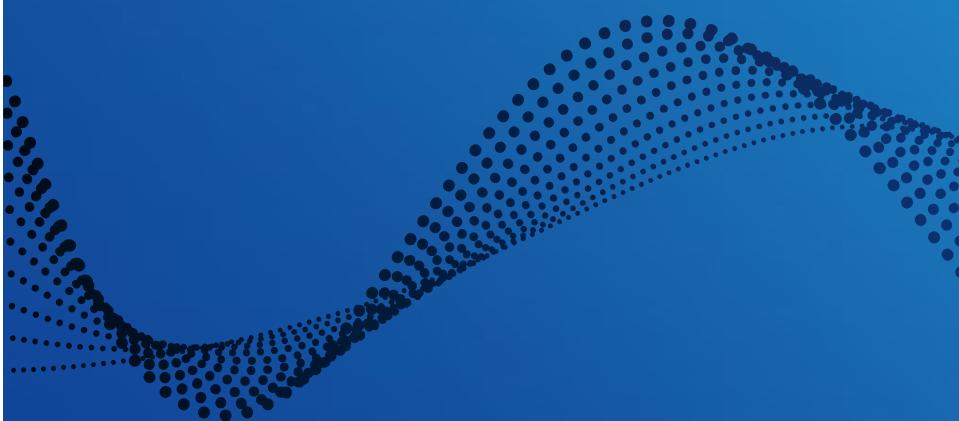


```
C:\restrict_pem_key.bat "c:\SplunkStudyClub.pem" "aleem"
```



AWS: Keeping lights on

Updating DNS



DNS Outcome

Domain: SplunkStudy.Club

Goal: Enable dns management of subdomain via scripting
Solve issue of non-static IP addressing for instances

Examples:

sh01-ext.bsides.dns.splunkstudy.club	34.213.206.70
sh01-int.bsides.dns.splunkstudy.club	172.31.43.187

Action: Add DNS ns record to existing nameserver to delegate
a subdomain to dynv6.com nameservers (dns.splunkstudy.club)

Type	Name	Value	TTL
NS	dns	ns1.dynv6.com	1 Hour
NS	dns	ns2.dynv6.com	1 Hour
NS	dns	ns3.dynv6.com	1 Hour



xpac

BSIDES splunk>

Subdomain Delegation

GoDaddy | Domain Manager

Domains ▾ Buy & Sell ▾ DNS ▾ Settings ▾ Help ▾

My Domains / Domain Settings

DNS Management

splunkstudy.club

NS	dns	ns1.dynv6.com	1 Hour
NS	dns	ns2.dynv6.com	1 Hour
NS	dns	ns3.dynv6.com	1 Hour

Delegated Domain Management

The screenshot shows the dynv6 web interface. At the top, there is a navigation bar with the dynv6 logo, Documentation, Community, My Zones, My Domains, and a user email aleem@cummins.me. The main content area has a heading "Add your delegated domain". On the left, there is a form with a "Domain" field containing "dns.splunkstudy.club" and a blue "Add domain" button. On the right, there is a "Instructions" box with the following steps:

1. Add your fully qualified domain name (FQDN) using the form below. You can either use the **root domain** itself (like `example.com`), or use a **subdomain** (like `dyn.example.com`).
2. You need **access** to your domain's **DNS settings** to **delegate** your domain to our nameservers:
 - `ns1.dynv6.com`.
 - `ns2.dynv6.com`.
 - `ns3.dynv6.com`.If you're using the root domain, setup the nameservers with your domain registrar. Otherwise, create `NS` records for the subdomain.
3. **Wait** for the changes to be propagated within the DNS (this might take up to 48 hours, depending on the `SOA` refresh timeout for your domain).
You will get an error, if the (sub-) domain is not setup properly.

Delegated Domain Management

The screenshot shows the dynv6 interface for managing delegated domains. The top navigation bar includes links for Documentation, Community, My Zones, My Domains, and a user account. The main content area is titled "dns.splunkstudy.club". It provides instructions for delegating the domain to dynv6's nameservers (ns1, ns2, ns3) and waits for DNS propagation. Below this is a "Delegation check" table:

Queried nameserver	Returned nameservers	Result
ns49.domaincontrol.com	ns1.dynv6.com. ns2.dynv6.com. ns3.dynv6.com.	✓ valid
ns50.domaincontrol.com	ns1.dynv6.com. ns2.dynv6.com. ns3.dynv6.com.	✓ valid

A "Restart check" button is located below the table. The "Danger Zone" section contains a warning about changing domain type and lists two options: "Multiple zones" (selected) and "Single zone". A "Change type" button is at the bottom of this section.

Adding DNS Zones

The screenshot shows the dynv6 website interface for creating a new DNS zone. The page has a light blue background with a decorative pattern of blue dots forming a wave-like shape at the bottom.

Header:

- Logo: **dynv6**
- Navigation links: Documentation ▾, Community, My Zones ▾, My Domains, aleem@splunkstudy.club ▾

Section Title: Create new Zone

Form Fields:

Name	bsides	dns.splunkstudy.club ▾
Only characters <code>a-z 0-9 -</code> are allowed, 5-20 characters. Do you have a short and fancy domain name to donate to us? Please let us know!		
New: Add your own domain		
IPv4 Address	<input type="text"/>	<input type="button" value="Set current address"/>
IPv6 prefix	<input type="text"/>	<input type="button" value="Set current address"/>

Buttons:

- Create Zone

Logos at the bottom:

- BSIDES
- splunk>

DNS Zone – Update Keys

dynv6 Documentation ▾ Community My Zones ▾ My Domains aleem@splunkstudy.club ▾

Add a new TSIG Key

Algorithm: hmac-md5
We strongly recommend using hmac-sha256 or sha512 and avoid md5 and sha1.

Zone: bsides.dns.splunkstudy.club
If chosen, the access of the key is limited to the zone. On removal of the zone this key will be automatically removed.

Generate TSIG Key **Cancel**

TSIG Keys

Name : tsig-227759.dynv6.com • Secret : 4ztzt3fDWn2Yv1A26P5YwnQV4dGQU07tN/fVM7QqBd0=	Details Edit Remove
Zone(s) : bsides.dns.splunkstudy.club Last used : never	Copy Regenerate

+ Add TSIG Key



DNS Update Commands

```
nsupdate
server ns1.dynv6.com
zone bsides.dns.splunkstudy.club
update delete sh100-int.bsides.dns.splunkstudy.club A
update add sh100-int.bsides.dns.splunkstudy.club 86400 A 172.31.8.205
update delete sh100-ext.bsides.dns.splunkstudy.club A
update add sh100-ext.bsides.dns.splunkstudy.club 86400 A 54.184.185.137
update delete i-0279ea465e401920f.bsides.dns.splunkstudy.club A
update add i-0279ea465e401920f.bsides.dns.splunkstudy.club 86400 A 54.184.185.137
key hmac-md5:tsig-227759.dynv6.com 4ztzt3fDWr2Yv1A26P5YWnQV4dGQUO7tN/fVM7QqBd0=
send
```



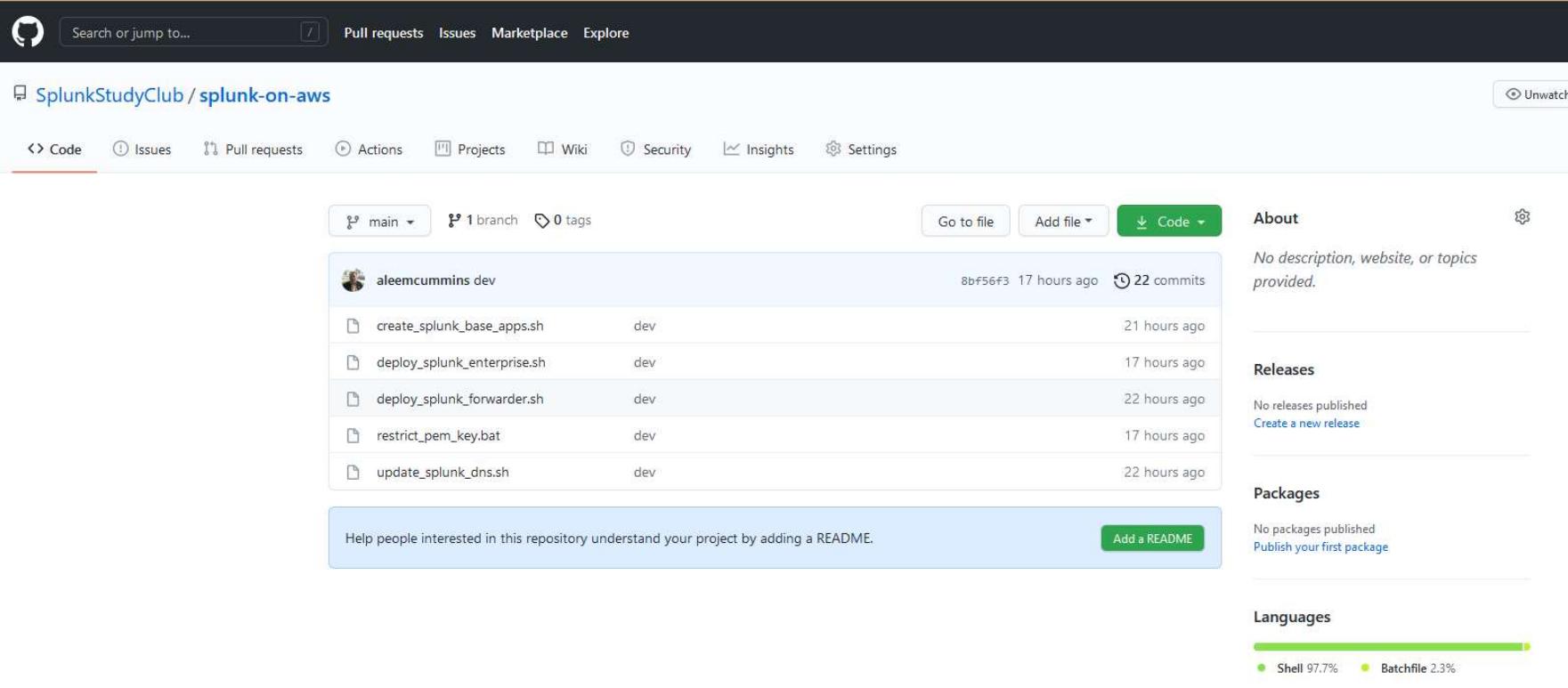
DNS Updates

The screenshot shows the dynv6 DNS management interface. At the top, there is a navigation bar with the dynv6 logo, Documentation, Community, My Zones, My Domains, and a user email aleem@splunkstudy.club. Below the navigation bar, the domain name `bsides.dns.splunkstudy.club` is displayed. Underneath the domain name, there are four tabs: Status, Records (which is selected), Hooks, and Instructions. The main content area is titled "Resource Records" and contains a table of records. The table has columns for Type, Name, and Data. There are four A-type records listed:

Type	Name	Data	Actions
A	sh01-ext.bsides.dns.splunkstudy.club	34.220.143.190	<button>edit</button> <button>delete</button>
A	sh01-int.bsides.dns.splunkstudy.club	172.31.29.130	<button>edit</button> <button>delete</button>
A	sh01-ext.bsides.dns.splunkstudy.club	34.213.206.70	<button>edit</button> <button>delete</button>
A	sh01-int.bsides.dns.splunkstudy.club	172.31.43.187	<button>edit</button> <button>delete</button>



DNS Scripting - GitHub



The screenshot shows a GitHub repository page for the user 'SplunkStudyClub' with the repository name 'splunk-on-aws'. The repository has 1 branch and 0 tags. The main branch was last updated 17 hours ago by aleemcummins dev with 22 commits. The commits listed are:

- create_splunk_base_apps.sh (dev, 21 hours ago)
- deploy_splunk_enterprise.sh (dev, 17 hours ago)
- deploy_splunk_forwarder.sh (dev, 22 hours ago)
- restrict_pem_key.bat (dev, 17 hours ago)
- update_splunk_dns.sh (dev, 22 hours ago)

The repository has no description, website, or topics provided. It also has no releases published, no packages published, and no languages used.

 <https://github.com/SplunkStudyClub>

DNS & Splunk Scripting

Getting host name for DNS updating

```
opt/splunk/etc/system/local/server.conf
```

```
[general]  
serverName = sh01
```

```
grep serverName /opt/splunk/etc/system/local/server.conf | sed 's/[ ]*[ ]*/g' | cut -c 12- | sed -e 's/\(\.*\)/\L\1/'
```

Getting internal server IP of instance for DNS updating

```
curl http://169.254.169.254/latest/meta-data/local-ipv4
```

Applying DNS settings

```
/opt/splunkforwarder/etc/system/local/deploymentclient.conf
```

```
[target-broker:deploymentServer]  
targetUri = sh01-int.bsides.dns.splunkstudy.club:8089
```

Applied using base apps via deployment server

Plan ahead for your naming convention and instances!!

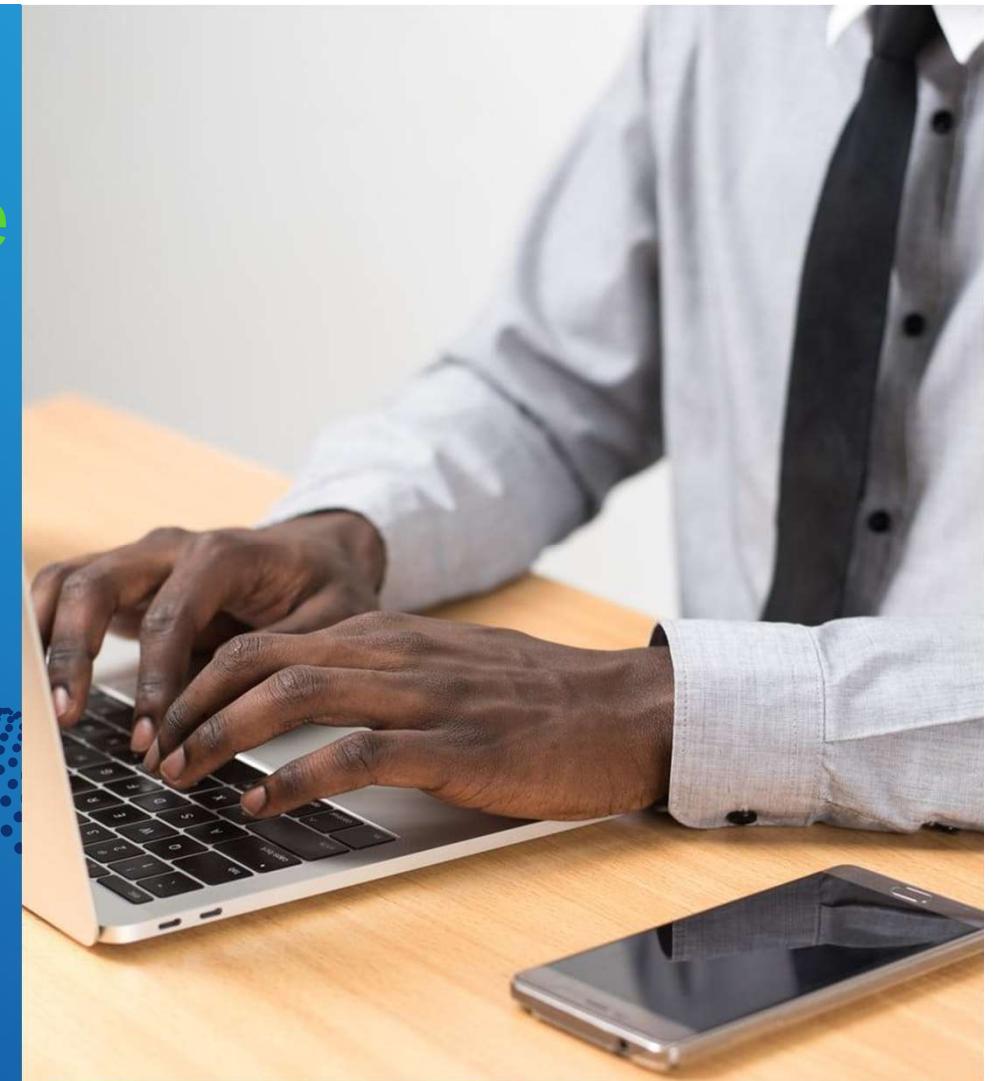


DNS Update Logs

```
UpdateTime=1618408851,AWS_INSTANCE_ID=i-0279ea465e401920f,DNS_SERVER=ns1.dynv6.com,Splunk_EXT_HOST=sh100-ext.bsides.dns.splunkstudy.club,Splunk_EXT_IP=34.221.89.29,Splunk_INT_HOST=sh100-int.bsides.dns.splunkstudy.club,Splunk_INT_IP=172.31.8.205,AWS_INSTANCE_ID_HOST=i-0279ea465e401920f.bsides.dns.splunkstudy.club,AWS_INSTANCE_ID_HOST_EXT_IP=34.221.89.29  
UpdateTime=1618409104,AWS_INSTANCE_ID=i-0279ea465e401920f,DNS_SERVER=ns1.dynv6.com,Splunk_EXT_HOST=sh100-ext.bsides.dns.splunkstudy.club,Splunk_EXT_IP=34.221.89.29,Splunk_INT_HOST=sh100-int.bsides.dns.splunkstudy.club,Splunk_INT_IP=172.31.8.205,AWS_INSTANCE_ID_HOST=i-0279ea465e401920f.bsides.dns.splunkstudy.club,AWS_INSTANCE_ID_HOST_EXT_IP=34.221.89.29  
UpdateTime=1618409405,AWS_INSTANCE_ID=i-0279ea465e401920f,DNS_SERVER=ns1.dynv6.com,Splunk_EXT_HOST=sh100-ext.bsides.dns.splunkstudy.club,Splunk_EXT_IP=34.221.89.29,Splunk_INT_HOST=sh100-int.bsides.dns.splunkstudy.club,Splunk_INT_IP=172.31.8.205,AWS_INSTANCE_ID_HOST=i-0279ea465e401920f.bsides.dns.splunkstudy.club,AWS_INSTANCE_ID_HOST_EXT_IP=34.221.89.29  
UpdateTime=1618409705,AWS_INSTANCE_ID=i-0279ea465e401920f,DNS_SERVER=ns1.dynv6.com,Splunk_EXT_HOST=sh100-ext.bsides.dns.splunkstudy.club,Splunk_EXT_IP=34.221.89.29,Splunk_INT_HOST=sh100-int.bsides.dns.splunkstudy.club,Splunk_INT_IP=172.31.8.205,AWS_INSTANCE_ID_HOST=i-0279ea465e401920f.bsides.dns.splunkstudy.club,AWS_INSTANCE_ID_HOST_EXT_IP=34.221.89.29  
UpdateTime=1618410005,AWS_INSTANCE_ID=i-0279ea465e401920f,DNS_SERVER=ns1.dynv6.com,Splunk_EXT_HOST=sh100-ext.bsides.dns.splunkstudy.club,Splunk_EXT_IP=34.221.89.29,Splunk_INT_HOST=sh100-int.bsides.dns.splunkstudy.club,Splunk_INT_IP=172.31.8.205,AWS_INSTANCE_ID_HOST=i-0279ea465e401920f.bsides.dns.splunkstudy.club,AWS_INSTANCE_ID_HOST_EXT_IP=34.221.89.29  
UpdateTime=1618410304,AWS_INSTANCE_ID=i-0279ea465e401920f,DNS_SERVER=ns1.dynv6.com,Splunk_EXT_HOST=sh100-ext.bsides.dns.splunkstudy.club,Splunk_EXT_IP=34.221.89.29,Splunk_INT_HOST=sh100-int.bsides.dns.splunkstudy.club,Splunk_INT_IP=172.31.8.205,AWS_INSTANCE_ID_HOST=i-0279ea465e401920f.bsides.dns.splunkstudy.club,AWS_INSTANCE_ID_HOST_EXT_IP=34.221.89.29  
UpdateTime=1618410607,AWS_INSTANCE_ID=i-0279ea465e401920f,DNS_SERVER=ns1.dynv6.com,Splunk_EXT_HOST=sh100-ext.bsides.dns.splunkstudy.club,Splunk_EXT_IP=34.221.89.29,Splunk_INT_HOST=sh100-int.bsides.dns.splunkstudy.club,Splunk_INT_IP=172.31.8.205,AWS_INSTANCE_ID_HOST=i-0279ea465e401920f.bsides.dns.splunkstudy.club,AWS_INSTANCE_ID_HOST_EXT_IP=34.221.89.29  
UpdateTime=1618410904,AWS_INSTANCE_ID=i-0279ea465e401920f,DNS_SERVER=ns1.dynv6.com,Splunk_EXT_HOST=sh100-ext.bsides.dns.splunkstudy.club,Splunk_EXT_IP=34.221.89.29,Splunk_INT_HOST=sh100-int.bsides.dns.splunkstudy.club,Splunk_INT_IP=172.31.8.205,AWS_INSTANCE_ID_HOST=i-0279ea465e401920f.bsides.dns.splunkstudy.club,AWS_INSTANCE_ID_HOST_EXT_IP=34.221.89.29
```

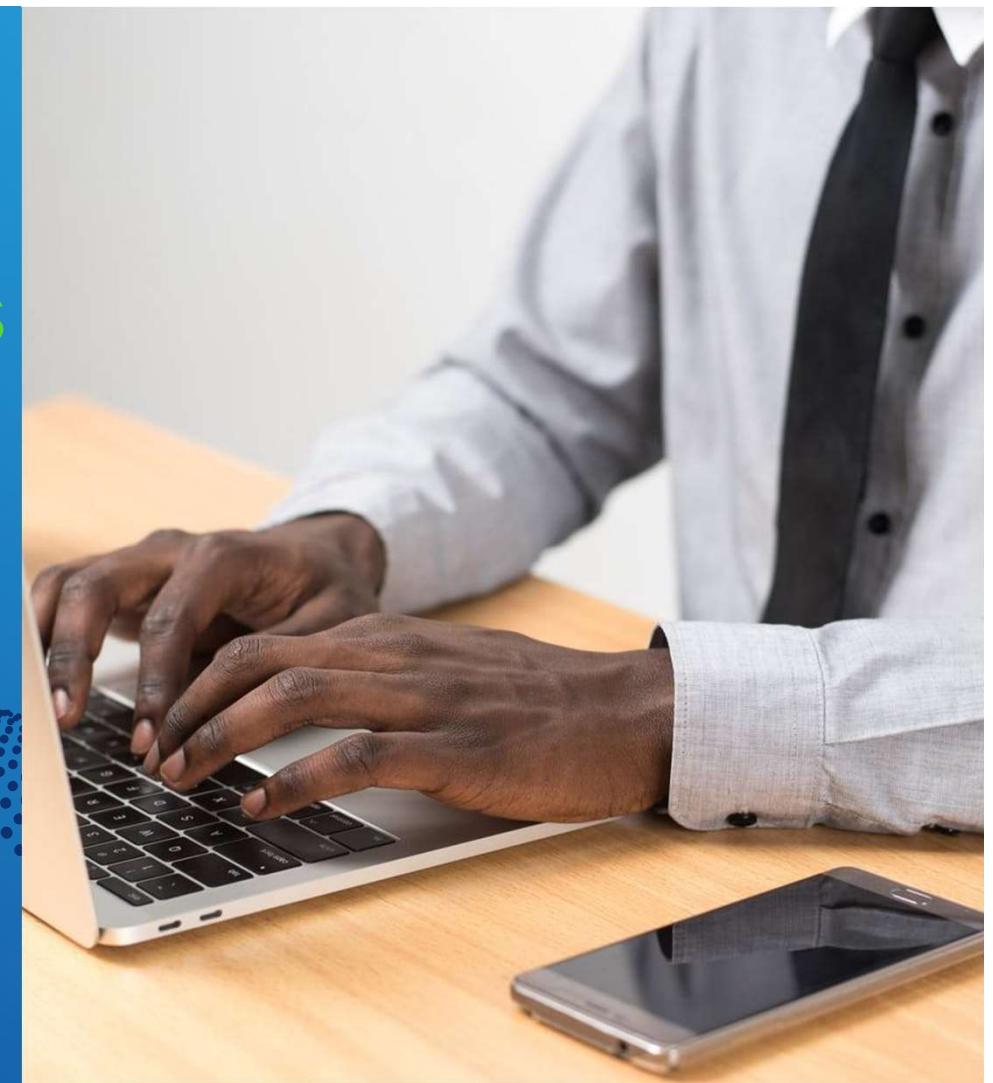
Accessing an Instance Deploying Splunk

Demo



Onboarding DNS Logs

Demo



Onboarding DNS Update Logs

```
UpdateTime=1618408851,AWS_INSTANCE_ID=i-0279ea465e401920f,DNS_SERVER=ns1.dynv6.com,Splunk_EXT_HOST=sh100-ext.bsides.dns.splunkstudy.club,Splunk_EXT_IP=34.221.89.29,Splunk_INT_HOST=sh100-int.bsides.dns.splunkstudy.club,Splunk_INT_IP=172.31.8.205,AWS_INSTANCE_ID_HOST=i-0279ea465e401920f.bsides.dns.splunkstudy.club,AWS_INSTANCE_ID_HOST_EXT_IP=34.221.89.29  
UpdateTime=1618409104,AWS_INSTANCE_ID=i-0279ea465e401920f,DNS_SERVER=ns1.dynv6.com,Splunk_EXT_HOST=sh100-ext.bsides.dns.splunkstudy.club,Splunk_EXT_IP=34.221.89.29,Splunk_INT_HOST=sh100-int.bsides.dns.splunkstudy.club,Splunk_INT_IP=172.31.8.205,AWS_INSTANCE_ID_HOST=i-0279ea465e401920f.bsides.dns.splunkstudy.club,AWS_INSTANCE_ID_HOST_EXT_IP=34.221.89.29  
UpdateTime=1618409405,AWS_INSTANCE_ID=i-0279ea465e401920f,DNS_SERVER=ns1.dynv6.com,Splunk_EXT_HOST=sh100-ext.bsides.dns.splunkstudy.club,Splunk_EXT_IP=34.221.89.29,Splunk_INT_HOST=sh100-int.bsides.dns.splunkstudy.club,Splunk_INT_IP=172.31.8.205,AWS_INSTANCE_ID_HOST=i-0279ea465e401920f.bsides.dns.splunkstudy.club,AWS_INSTANCE_ID_HOST_EXT_IP=34.221.89.29  
UpdateTime=1618409705,AWS_INSTANCE_ID=i-0279ea465e401920f,DNS_SERVER=ns1.dynv6.com,Splunk_EXT_HOST=sh100-ext.bsides.dns.splunkstudy.club,Splunk_EXT_IP=34.221.89.29,Splunk_INT_HOST=sh100-int.bsides.dns.splunkstudy.club,Splunk_INT_IP=172.31.8.205,AWS_INSTANCE_ID_HOST=i-0279ea465e401920f.bsides.dns.splunkstudy.club,AWS_INSTANCE_ID_HOST_EXT_IP=34.221.89.29  
UpdateTime=1618410005,AWS_INSTANCE_ID=i-0279ea465e401920f,DNS_SERVER=ns1.dynv6.com,Splunk_EXT_HOST=sh100-ext.bsides.dns.splunkstudy.club,Splunk_EXT_IP=34.221.89.29,Splunk_INT_HOST=sh100-int.bsides.dns.splunkstudy.club,Splunk_INT_IP=172.31.8.205,AWS_INSTANCE_ID_HOST=i-0279ea465e401920f.bsides.dns.splunkstudy.club,AWS_INSTANCE_ID_HOST_EXT_IP=34.221.89.29  
UpdateTime=1618410304,AWS_INSTANCE_ID=i-0279ea465e401920f,DNS_SERVER=ns1.dynv6.com,Splunk_EXT_HOST=sh100-ext.bsides.dns.splunkstudy.club,Splunk_EXT_IP=34.221.89.29,Splunk_INT_HOST=sh100-int.bsides.dns.splunkstudy.club,Splunk_INT_IP=172.31.8.205,AWS_INSTANCE_ID_HOST=i-0279ea465e401920f.bsides.dns.splunkstudy.club,AWS_INSTANCE_ID_HOST_EXT_IP=34.221.89.29  
UpdateTime=1618410607,AWS_INSTANCE_ID=i-0279ea465e401920f,DNS_SERVER=ns1.dynv6.com,Splunk_EXT_HOST=sh100-ext.bsides.dns.splunkstudy.club,Splunk_EXT_IP=34.221.89.29,Splunk_INT_HOST=sh100-int.bsides.dns.splunkstudy.club,Splunk_INT_IP=172.31.8.205,AWS_INSTANCE_ID_HOST=i-0279ea465e401920f.bsides.dns.splunkstudy.club,AWS_INSTANCE_ID_HOST_EXT_IP=34.221.89.29  
UpdateTime=1618410904,AWS_INSTANCE_ID=i-0279ea465e401920f,DNS_SERVER=ns1.dynv6.com,Splunk_EXT_HOST=sh100-ext.bsides.dns.splunkstudy.club,Splunk_EXT_IP=34.221.89.29,Splunk_INT_HOST=sh100-int.bsides.dns.splunkstudy.club,Splunk_INT_IP=172.31.8.205,AWS_INSTANCE_ID_HOST=i-0279ea465e401920f.bsides.dns.splunkstudy.club,AWS_INSTANCE_ID_HOST_EXT_IP=34.221.89.29
```



Onboarding DNS Update Logs

Add Data

Select Source Set Source Type Input Settings Review Done

< Back Next >

Files & Directories
Upload a file, index a local file, or monitor an entire directory.

HTTP Event Collector
Configure tokens that clients can use to send data over HTTP or HTTPS.

TCP / UDP
Configure the Splunk platform to listen on a network port.

Scripts
Get data from any API, service, or database with a script.

Systemd Journald Input for Splunk
This is the input that gets data from journald (systemd's logging component) into Splunk.

Configure this instance to monitor files and directories for data. To monitor all objects in a directory, select the directory. The Splunk platform monitors and assigns a single source type to all objects within the directory. This might cause problems if there are different object types or data sources in the directory. To assign multiple source types to objects in the same directory, configure individual data inputs for those objects. [Learn More](#)

File or Directory ? [Browse](#)

On Windows: c:\apache\apache.error.log or \\hostname\apache\apache.error.log. On Unix: /var/log or /mnt/www01/var/log.

Continuously Monitor Index Once

Whitelist ?

Blacklist ?

Onboarding DNS Update Logs

The screenshot shows the 'Add Data' wizard in the 'Set Source Type' step. The progress bar indicates the current step is 'Set Source Type'. Below the progress bar, there is a message: "This page lets you see how the Splunk platform sees your data before indexing. If the events look correct and have the right timestamps, click 'Next' to proceed. If not, use the options below to define proper event breaks and timestamps. If you cannot find an appropriate source type for your data, create a new one by clicking 'Save As'." The table view shows four log entries:

	Time	Event
1	14/04/2021 14:00:51.000	UpdateTime=1618408851,AWS_INSTANCE_ID=i-0279ea465e401920f,DNS_SERVER=ns1.dynv6.com,Splunk_EXT_HOST=sh100-ext.bsides.dns.splunkstudy.club,Splunk_EXT_IP=34.221.89.29,Splunk_INT_HOST=sh100-int.bsides.dns.splunkstudy.club,Splunk_INT_IP=172.31.8.205,AWS_INSTANCE_ID_HOST=i-0279ea465e401920f.bsides.dns.splunkstudy.club,AWS_INSTANCE_ID_HOST_EXT_IP=34.221.89.29
2	14/04/2021 14:05:04.000	UpdateTime=1618409104,AWS_INSTANCE_ID=i-0279ea465e401920f,DNS_SERVER=ns1.dynv6.com,Splunk_EXT_HOST=sh100-ext.bsides.dns.splunkstudy.club,Splunk_EXT_IP=34.221.89.29,Splunk_INT_HOST=sh100-int.bsides.dns.splunkstudy.club,Splunk_INT_IP=172.31.8.205,AWS_INSTANCE_ID_HOST=i-0279ea465e401920f.bsides.dns.splunkstudy.club,AWS_INSTANCE_ID_HOST_EXT_IP=34.221.89.29
3	14/04/2021 14:10:05.000	UpdateTime=1618409405,AWS_INSTANCE_ID=i-0279ea465e401920f,DNS_SERVER=ns1.dynv6.com,Splunk_EXT_HOST=sh100-ext.bsides.dns.splunkstudy.club,Splunk_EXT_IP=34.221.89.29,Splunk_INT_HOST=sh100-int.bsides.dns.splunkstudy.club,Splunk_INT_IP=172.31.8.205,AWS_INSTANCE_ID_HOST=i-0279ea465e401920f.bsides.dns.splunkstudy.club,AWS_INSTANCE_ID_HOST_EXT_IP=34.221.89.29
4	14/04/2021 14:15:05.000	UpdateTime=1618409705,AWS_INSTANCE_ID=i-0279ea465e401920f,DNS_SERVER=ns1.dynv6.com,Splunk_EXT_HOST=sh100-ext.bsides.dns.splunkstudy.club,Splunk_EXT_IP=34.221.89.29,Splunk_INT_HOST=sh100-int.bsides.dns.splunkstudy.club,Splunk_INT_IP=172.31.8.205,AWS_INSTANCE_ID_HOST=i-0279ea465e401920f.bsides.dns.splunkstudy.club,AWS_INSTANCE_ID_HOST_EXT_IP=34.221.89.29

Onboarding DNS Update Logs

Add Data

Select Source Set Source Type Input Settings Review Done

< Back Review >

Input Settings

Optional set additional input parameters for this data input as follows:

App context

Application contexts are folders within a Splunk platform instance that contain configurations for a specific use case or domain of data. App contexts improve manageability of input and source type definitions. The Splunk platform loads all app contexts based on precedence rules. [Learn More](#)

App Context [Apps Browser \(appsbrowser\)](#)

Host

When the Splunk platform indexes data, each event receives a "host" value. The host value should be the name of the machine from which the event originates. The type of input you choose determines the available configuration options. [Learn More](#)

Host field value Constant value
 Regular expression on path
 Segment in path

Host field value

Index

The Splunk platform stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can always change this setting later. [Learn More](#)

Index [main](#) [Create a new index](#)

Onboarding DNS Update Logs

Add Data

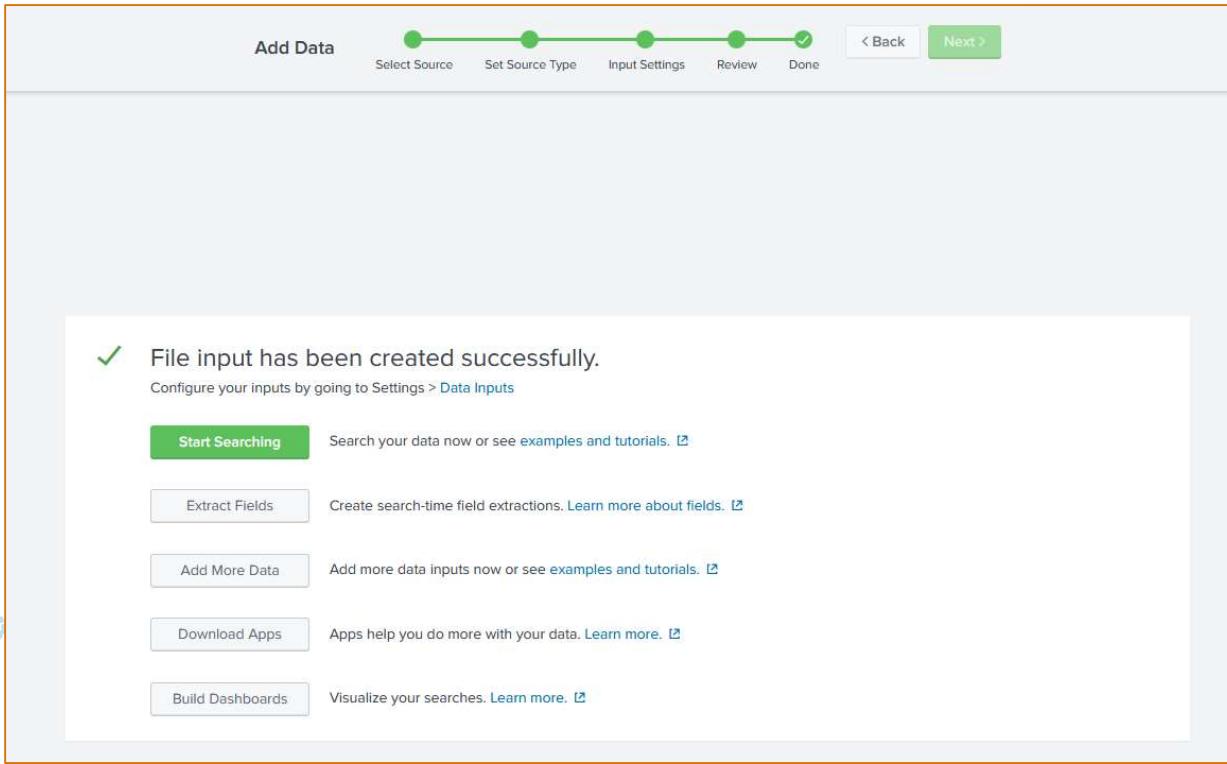
Select Source Set Source Type Input Settings Review Done

< Back Submit >

Review

Input Type File Monitor
Source Path /home/ubuntu/update_splunk_dns.log
Continuously Monitor Yes
Source Type splunkstudyclub_dns
App Context launcher
Host sh100
Index main

Onboarding DNS Update Logs



The screenshot shows the final step of the 'Add Data' wizard in Splunk, titled 'Done'. A green checkmark icon is displayed next to the 'File input has been created successfully.' message. Below this message, there is a link to 'Configure your inputs by going to Settings > Data Inputs'. The page also features several call-to-action buttons: 'Start Searching', 'Extract Fields', 'Add More Data', 'Download Apps', and 'Build Dashboards'. Each button has a corresponding description and a 'Learn more' link.

Add Data

File input has been created successfully.

Configure your inputs by going to Settings > [Data Inputs](#)

Start Searching Search your data now or see examples and tutorials. [Learn more](#)

Extract Fields Create search-time field extractions. [Learn more about fields](#).

Add More Data Add more data inputs now or see examples and tutorials. [Learn more](#)

Download Apps Apps help you do more with your data. [Learn more](#).

Build Dashboards Visualize your searches. [Learn more](#).



Working with DNS Update Logs

The screenshot shows the Splunk Enterprise search interface. The search bar contains the following command:

```
index=main sourcetype=splunkstudyclub_dns Splunk_EXT_HOST=sh100-ext.bsides.dns.splunkstudy.club | eval UpdateTime=strftime(UpdateTime,"%m/%d/%y %H:%M:%S") | table UpdateTime DNS_SERVER AWS_INSTANCE_ID Splunk_EXT_HOST Splunk_EXT_IP Splunk_INT_HOST Splunk_INT_IP | sort - UpdateTime | head 10
```

The results table displays 22 events from April 14, 2021, between 15:00:00.000 and 15:45:19.000. The table has columns: UpdateTime, DNS_SERVER, AWS_INSTANCE_ID, Splunk_EXT_HOST, Splunk_EXT_IP, Splunk_INT_HOST, and Splunk_INT_IP. An orange circle highlights the value "54.184.185.137" in the Splunk_EXT_IP column for the third event.

UpdateTime	DNS_SERVER	AWS_INSTANCE_ID	Splunk_EXT_HOST	Splunk_EXT_IP	Splunk_INT_HOST	Splunk_INT_IP
04/14/21 15:45:03	ns1.dynv6.com	i-0279ea465e401920f	sh100-ext.bsides.dns.splunkstudy.club	54.184.185.137	sh100-int.bsides.dns.splunkstudy.club	172.31.8.205
04/14/21 15:40:06	ns1.dynv6.com	i-0279ea465e401920f	sh100-ext.bsides.dns.splunkstudy.club	54.184.185.137	sh100-int.bsides.dns.splunkstudy.club	172.31.8.205
04/14/21 15:35:05	ns1.dynv6.com	i-0279ea465e401920f	sh100-ext.bsides.dns.splunkstudy.club	54.184.185.137	sh100-int.bsides.dns.splunkstudy.club	172.31.8.205
04/14/21 15:30:06	ns1.dynv6.com	i-0279ea465e401920f	sh100-ext.bsides.dns.splunkstudy.club	34.221.89.29	sh100-int.bsides.dns.splunkstudy.club	172.31.8.205
04/14/21 15:25:04	ns1.dynv6.com	i-0279ea465e401920f	sh100-ext.bsides.dns.splunkstudy.club	34.221.89.29	sh100-int.bsides.dns.splunkstudy.club	172.31.8.205
04/14/21 15:20:05	ns1.dynv6.com	i-0279ea465e401920f	sh100-ext.bsides.dns.splunkstudy.club	34.221.89.29	sh100-int.bsides.dns.splunkstudy.club	172.31.8.205
04/14/21 15:15:03	ns1.dynv6.com	i-0279ea465e401920f	sh100-ext.bsides.dns.splunkstudy.club	34.221.89.29	sh100-int.bsides.dns.splunkstudy.club	172.31.8.205
04/14/21 15:10:06	ns1.dynv6.com	i-0279ea465e401920f	sh100-ext.bsides.dns.splunkstudy.club	34.221.89.29	sh100-int.bsides.dns.splunkstudy.club	172.31.8.205
04/14/21 15:05:04	ns1.dynv6.com	i-0279ea465e401920f	sh100-ext.bsides.dns.splunkstudy.club	34.221.89.29	sh100-int.bsides.dns.splunkstudy.club	172.31.8.205
04/14/21 15:00:02	ns1.dynv6.com	i-0279ea465e401920f	sh100-ext.bsides.dns.splunkstudy.club	34.221.89.29	sh100-int.bsides.dns.splunkstudy.club	172.31.8.205

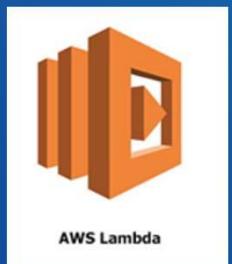
```
index=main sourcetype=splunkstudyclub_dns | eval UpdateTime=strftime(UpdateTime,"%m/%d/%y %H:%M:%S") | table UpdateTime DNS_SERVER AWS_INSTANCE_ID Splunk_EXT_HOST Splunk_EXT_IP Splunk_INT_HOST Splunk_INT_IP | sort - UpdateTime | head 10
```

```
index=main sourcetype=splunkstudyclub_dns | dedup AWS_INSTANCE_ID | eval UpdateTime=strftime(UpdateTime,"%m/%d/%y %H:%M:%S") | table UpdateTime DNS_SERVER AWS_INSTANCE_ID Splunk_EXT_HOST Splunk_EXT_IP Splunk_INT_HOST Splunk_INT_IP | sort - UpdateTime | head 10
```



AWS: Keeping lights on

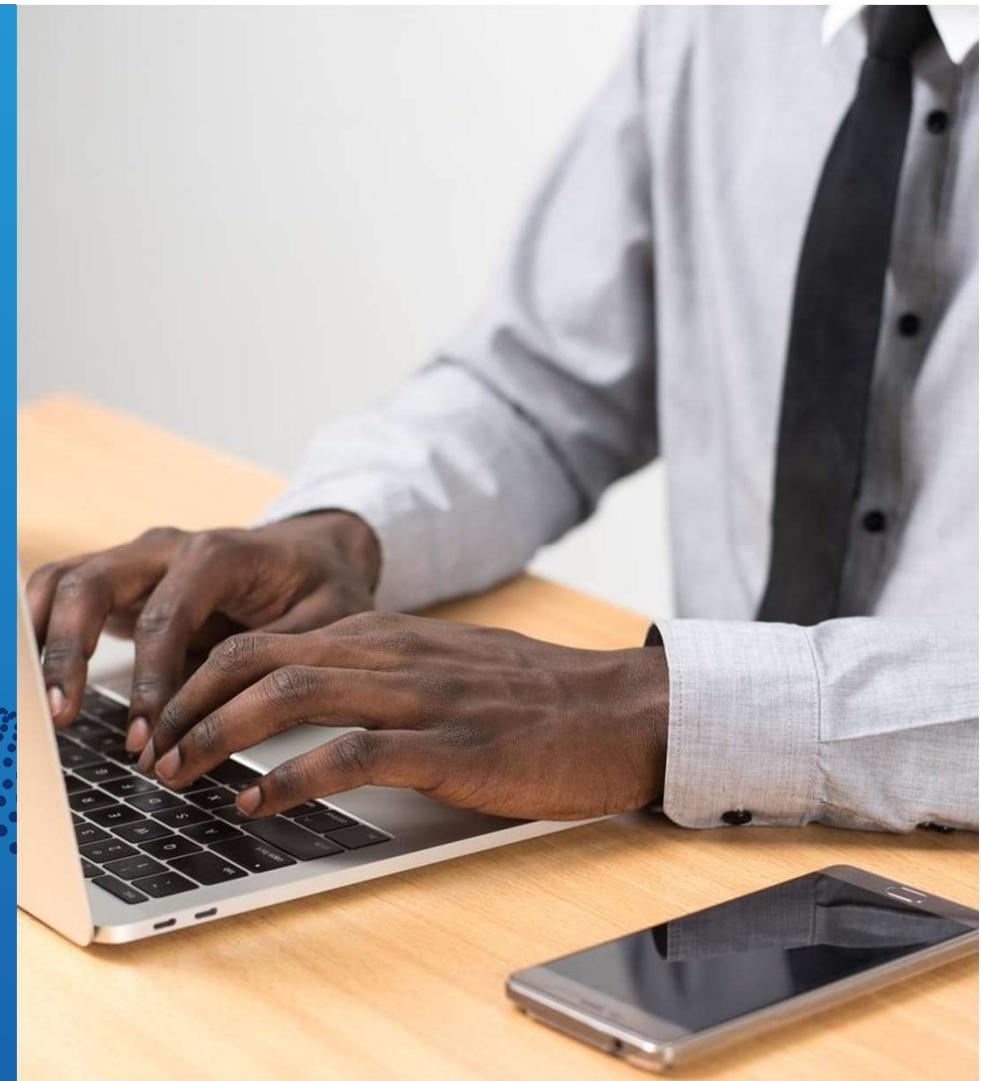
Minimising Costs



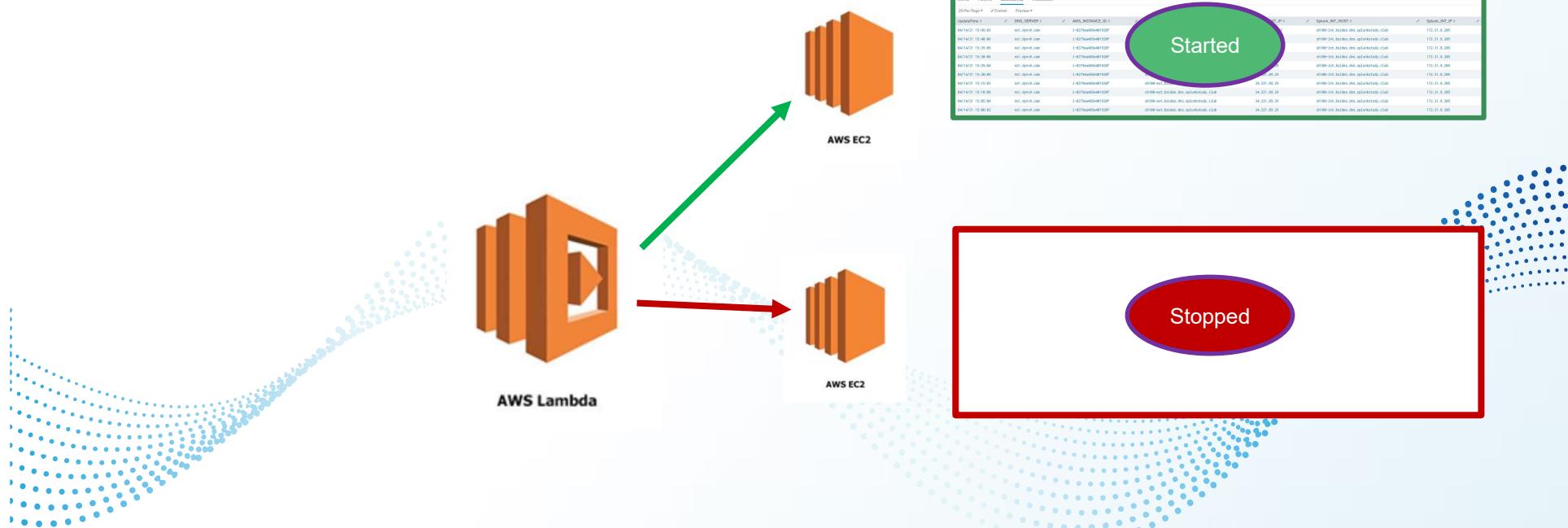
AWS Lambda



jkat54



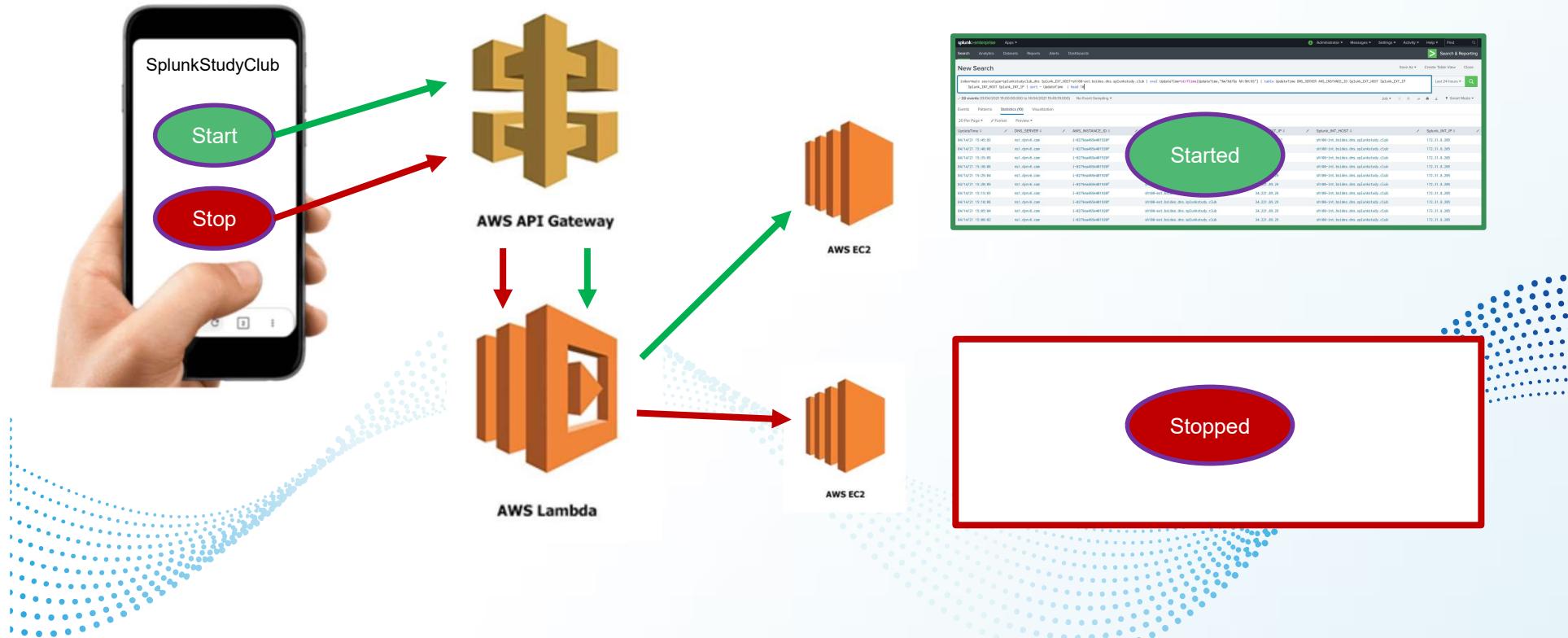
Lambda Functions - Concept



<https://aws.amazon.com/premiumsupport/knowledge-center/start-stop-lambda-cloudwatch/>



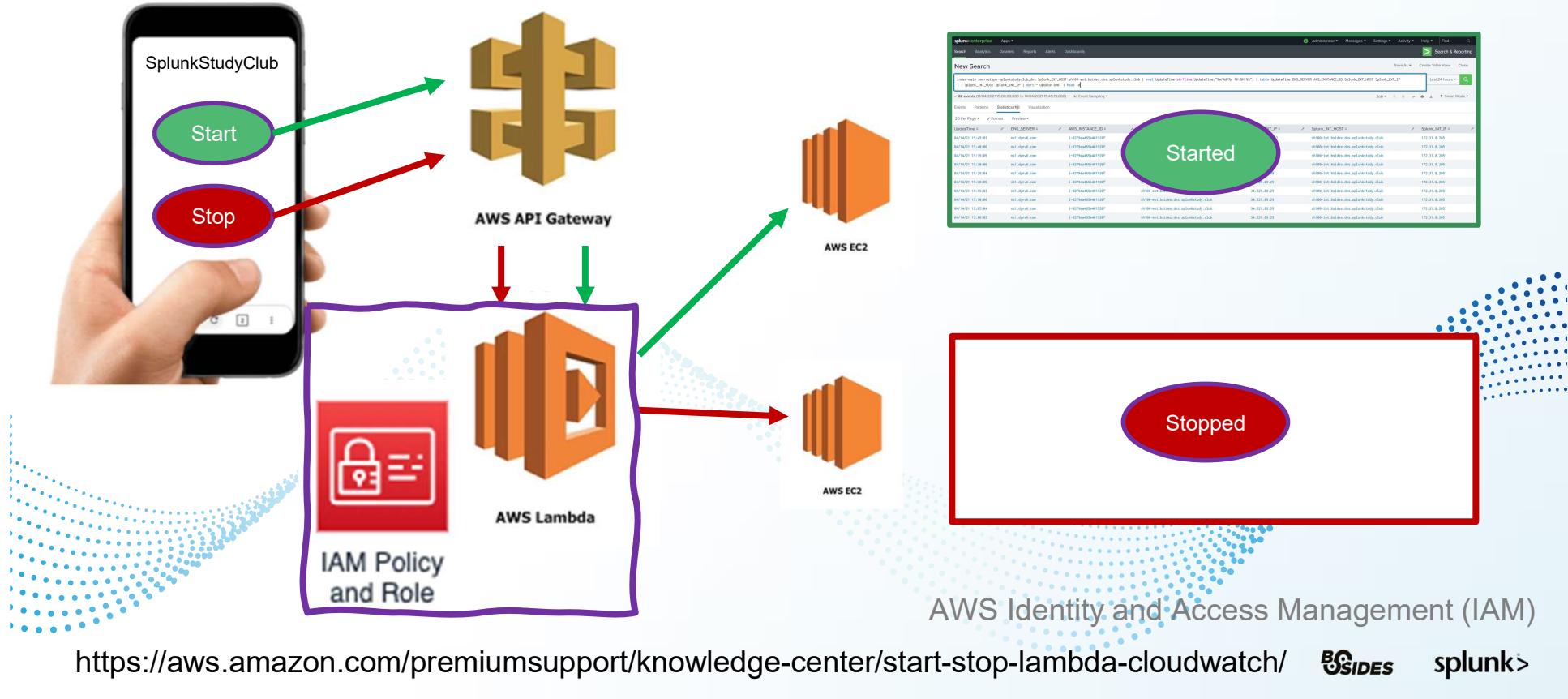
Lambda Functions - Serverless



<https://aws.amazon.com/premiumsupport/knowledge-center/start-stop-lambda-cloudwatch/>



Lambda Function - Permissions



To control AWS Instance state

- Create an AWS Identity and Access Management (IAM) policy and role
- Create Lambda function to stop EC2 instances using this new policy and role
- Create Lambda function to start EC2 instances using this new policy and role
- Expose Lambda functions via the AWS API Gateway



<https://aws.amazon.com/premiumsupport/knowledge-center/start-stop-lambda-cloudwatch/>

BSIDES

splunk>



IAM Policy
and Role

Create policy

1 2 3

A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. [Learn more](#)

Visual editor JSON

[Import managed policy](#)

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Effect": "Allow",  
6       "Action": [  
7         "logs:CreateLogGroup",  
8         "logs:CreateLogStream",  
9         "logs:PutLogEvents"  
10      ],  
11      "Resource": "arn:aws:logs:*:*:*"  
12    },  
13    {  
14      "Effect": "Allow",  
15      "Action": [  
16        "ec2:Start*",  
17        "ec2:Stop*"  
18      ],  
19      "Resource": "*"  
20    }  
21  ]  
22 }
```

🛡 Security: 0 ✎ Errors: 0 ⚠ Warnings: 0 💡 Suggestions: 0



IAM Policy
and Role

Create policy

1 2 3

Add tags (Optional)

Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

No tags associated with the resource.

Add tag

You can add up to 50 more tags



splunk>



IAM Policy
and Role

Create policy

1 2 3

Review policy

Name* SplunkStudyClub-InstanceControl

Use alphanumeric and '+,-,@-' characters. Maximum 128 characters.

Description Allowing for AW instances to be stopped or started to managed costs

Maximum 1000 characters. Use alphanumeric and '+,-,@-' characters.

Summary

Filter

Service	Access level	Resource	Request condition
Allow (2 of 277 services) Show remaining 275			
CloudWatch Logs	Limited: Write	arn:aws:logs:***	None
EC2	Limited: Write	All resources	None

Tags

Key	Value
No tags associated with the resource.	

BSIDES

splunk>



IAM Policy
and Role

Create role

1 2 3 4

Select type of trusted entity



AWS service
EC2, Lambda and others



Another AWS account
Belonging to you or 3rd party



Web identity
Cognito or any OpenID provider



SAML 2.0 federation
Your corporate directory

Allows AWS services to perform actions on your behalf. [Learn more](#)

Choose a use case

Common use cases

EC2

Allows EC2 instances to call AWS services on your behalf.

Lambda

Allows Lambda functions to call AWS services on your behalf.

Or select a service to view its use cases

API Gateway

CodeBuild

EMR

IoT SiteWise

RDS

AWS Backup

CodeDeploy

EMR Containers

IoT Things Graph

Redshift

AWS Chatbot

CodeGuru

ElastiCache

KMS

Rekognition

AWS Marketplace

CodeStar Notifications

Elastic Beanstalk

Kinesis

RoboMaker

AWS Support

Comprehend

Elastic Container Registry

Lake Formation

S3

Amplify

Config

Elastic Container Service

Lambda

SMS

AppStream 2.0

Connect

Elastic Transcoder

Lex

SNS

BSIDES

splunk>



IAM Policy
and Role

Create role

- 1
- 2
- 3
- 4

▼ Attach permissions policies

Choose one or more policies to attach to your new role.

[Create policy](#)



Filter policies		Q InstanceControl	Showing 2 results
	Policy name		Used as
<input checked="" type="checkbox"/>	▶ SplunkStudyClub-InstanceControl		None

▶ Set permissions boundary



splunk>



IAM Policy
and Role

Create role

- 1
- 2
- 3
- 4

Add tags (optional)

IAM tags are key-value pairs you can add to your role. Tags can include user information, such as an email address, or can be descriptive, such as a job title. You can use the tags to organize, track, or control access for this role. [Learn more](#)

Key	Value (optional)	Remove
<input type="text" value="Add new key"/>	<input type="text"/>	

You can add 50 more tags.



splunk>



IAM Policy
and Role

Create role

1 2 3 4

Review

Provide the required information below and review this role before you create it.

Role name* SplunkStudyClub-InstanceControl

Use alphanumeric and '+,-,@,_' characters. Maximum 64 characters.

Role description

Allows EC2 instances to call AWS services on your behalf.

Maximum 1000 characters. Use alphanumeric and '+,-,@,_' characters.

Trusted entities AWS service: ec2.amazonaws.com

Policies SplunkStudyClub-InstanceControl

Permissions boundary Permissions boundary is not set

No tags were added.

BSIDES

splunk>



IAM Policy
and Role

Create role

1 2 3 4

Review

Provide the required information below and review this role before you create it.

Role name* SplunkStudyClub-InstanceControl

Use alphanumeric and '+,-,@,_' characters. Maximum 64 characters.

Role description

Allows EC2 instances to call AWS services on your behalf.

Maximum 1000 characters. Use alphanumeric and '+,-,@,_' characters.

Trusted entities AWS service: ec2.amazonaws.com

Policies SplunkStudyClub-InstanceControl

Permissions boundary Permissions boundary is not set

No tags were added.

BSIDES

splunk>



Lambda Function

AWS Lambda X

Lambda > Functions

Functions (0)

Last fetched 50 seconds ago

Actions Create function

Filter by tags and attributes or search by keyword

Function name	Description	Package type	Runtime	Code size	Last modified
There is no data to display.					

Dashboard Applications Functions Additional resources Code signing configurations Layers Related AWS resources Step Functions state machines



The background features a large, abstract graphic composed of numerous small blue dots forming a wavy, undulating pattern across the bottom half of the screen.

BSIDES splunk>



Lambda Function

Search for services, features, marketplace products, and docs [Alt+S]

Splunk Study Club • Oregon • Support

Lambda > Functions > Create function

Create function Info

Choose one of the following options to create your function.

Author from scratch Start with a simple Hello World example.

Use a blueprint Build a Lambda application from sample code and configuration presets for common use cases.

Container image Select a container image to deploy for your function.

Browse serverless app repository Deploy a sample Lambda application from the AWS Serverless Application Repository.

Basic information

Function name
Enter a name that describes the purpose of your function.
SplunkStudyClub_StopInstances
Use only letters, numbers, hyphens, or underscores with no spaces.

Runtime Info
Choose the language to use for your function. Note that the console code editor supports only Node.js, Python, and Ruby.
Python 3.8

Permissions Info
By default, Lambda will create an execution role with permissions to upload logs to Amazon CloudWatch Logs. You can customize this default role later when adding triggers.

Change default execution role

Execution role
Choose a role that defines the permissions of your function. To create a custom role, go to the [IAM console](#).

Create a new role with basic Lambda permissions
 Use an existing role
 Create a new role from AWS policy templates

Existing role
Choose an existing role to use for your function. The role must have permission to upload logs to Amazon CloudWatch Logs.
service-role/SplunkStudyClub-StopInstancesFunction-role-0jtlttse



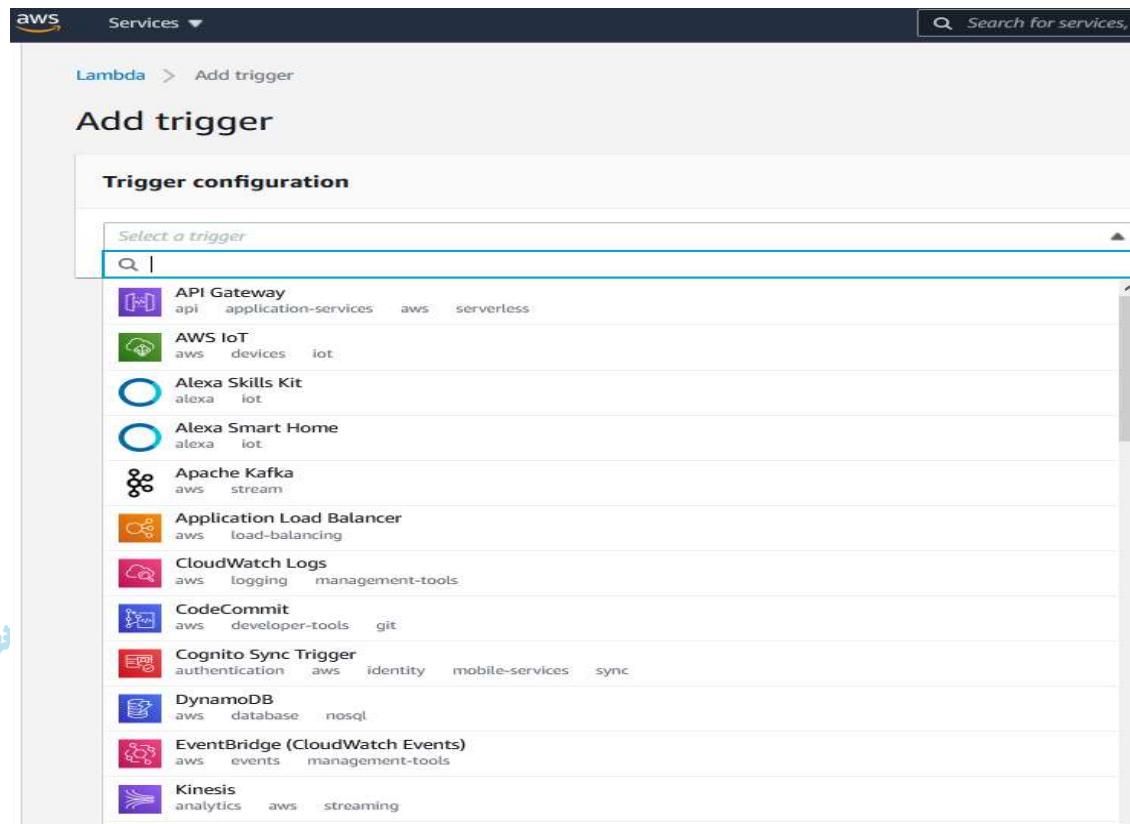
Lambda Function

The screenshot shows the AWS Lambda function configuration page for the function 'SplunkStudyClub_StopInstances'. The top navigation bar includes the AWS logo, 'Services ▾', a search bar ('Search for services, features, marketplace products, and docs [Alt+S]'), and a 'Throttle' button. The main content area displays the function overview, showing the function name 'SplunkStudyClub_StopInstances', its creation date ('4 hours ago'), and its ARN ('arn:aws:lambda:us-west-2:170417028123:function:SplunkStudyClub_StopInstances'). Below this, there are tabs for 'Code', 'Test', 'Monitor', 'Configuration', 'Aliases', and 'Versions'. The 'Code' tab is selected, showing the code source in a code editor. The code editor has tabs for 'File', 'Edit', 'Find', 'View', 'Go', 'Tools', 'Window', 'Test' (which is currently selected), 'Deploy', and 'Changes deployed'. The code itself is as follows:

```
1 import boto3
2 region = 'us-west-2'
3 instances = ['i-0279ea465e401920f']
4 ec2 = boto3.client('ec2', region_name=region)
5
6 def lambda_handler(event, context):
7     ec2.stop_instances(InstanceIds=instances)
8     print('stopped your instances: ' + str(instances))
```

<https://aws.amazon.com/premiumsupport/knowledge-center/start-stop-lambda-cloudwatch/>

Lambda Function - Triggers



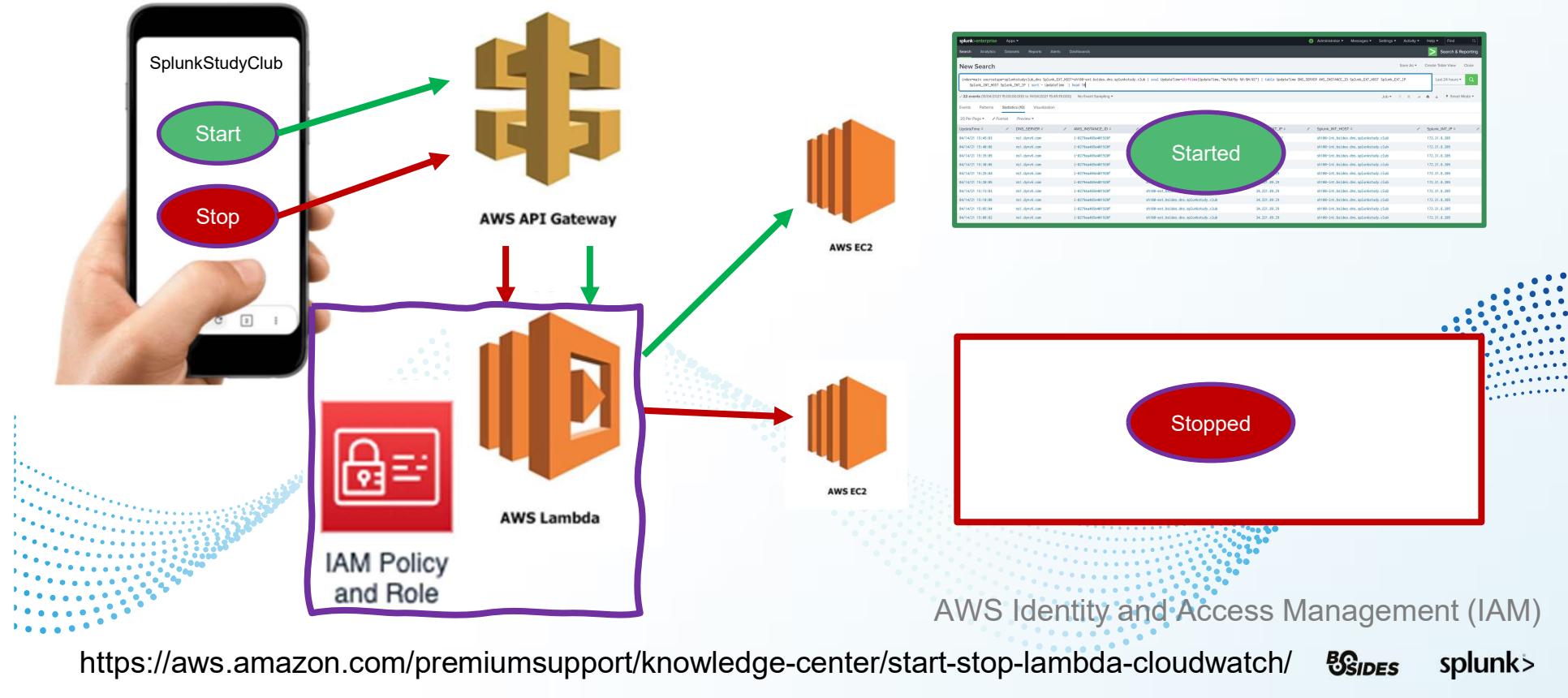
Lambda Function – API Gateway

The screenshot shows the AWS Lambda Function Overview page for the function 'SplunkStudyClub_StopInstances'. The function was last modified 13 minutes ago and has a Function ARN of `arn:aws:lambda:us-west-2:170417028123:function:SplunkStudyClub_StopInstances`. It has no layers and no triggers defined.

Configuration Tab: The Configuration tab is selected. Under General configuration, the Triggers section is expanded, showing one trigger named 'API Gateway: SplunkStudyClub_StopInstances-API'. The trigger details indicate it is an HTTP API endpoint at https://ksevpv3qf4.execute-api.us-west-2.amazonaws.com/default/SplunkStudyClub_StopInstances, using the NONE authorization type, and CORS is disabled. Detailed metrics are also disabled.

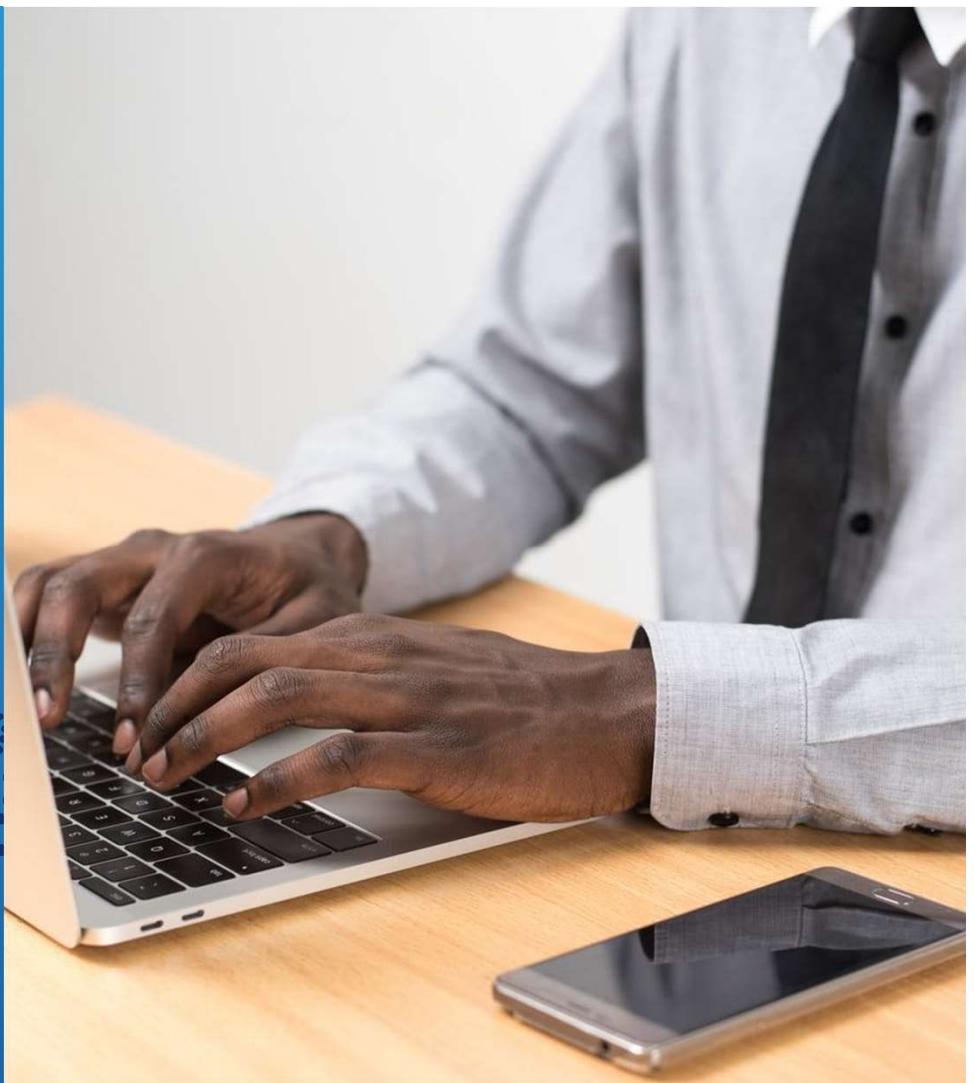
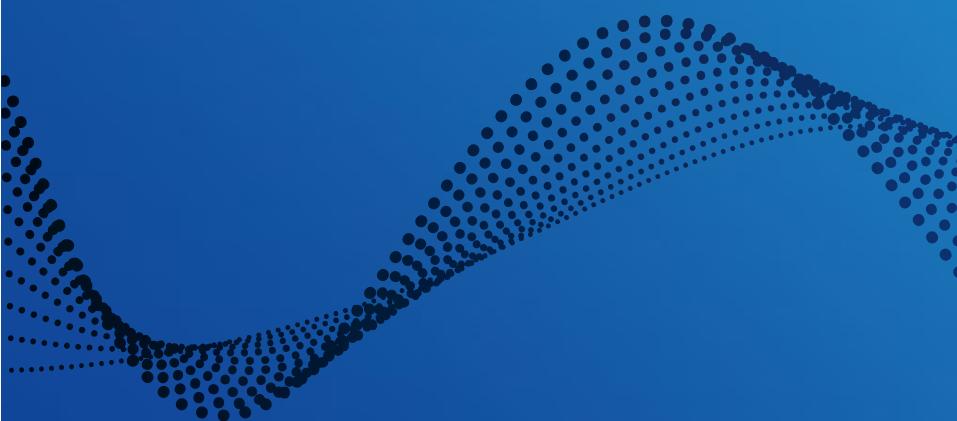
Red Annotation: A large red arrow points from the text 'https://ksevpv3qf4.execute-api.us-west-2.amazonaws.com/default/SplunkStudyClub_StopInstances' in the configuration details towards the URL in the browser's address bar.

AWS Instance Management



Growth

Splunk Licensing



Splunk Licenses

Splunk Enterprise Dev/Test license - 50GB

https://www.splunk.com/en_us/resources/personalized-dev-test-licenses.html

Splunk Developer License - 10GB

https://dev.splunk.com/enterprise/dev_license/

Splunk Enterprise License

https://www.splunk.com/en_us/software/splunk-enterprise.html

Splunk Study Club



aws | Free Tier
Cloud Compute



splunk>

Thanks!



Aleem Cummins

Community Enablement Warrior

Independent

@aleemcummins

<https://www.linkedin.com/in/aleemcummins>
aleem@splunkstudy.club

SplunkTrust
Splunk User Group London
Splunk Study Club

Any questions?



Suman Gajavelly

CTO / Co-founder

BitsIO Inc

@sumangajavelly

<https://www.linkedin.com/in/sumangajavelly>
suman.g@bitsioinc.com

Fort Worth Splunk User Group



<http://slack.splunkstudy.club>



<https://github.com/SplunkStudyClub>

