
BSIDES
splunk>
AWS Splunk Environments:
A step by step guide to empowering collaborative community learning
aws | Free Tier
Cloud Compute
BSIDES
splunk>

Your Presenters

Aleem Cummins
Community Enablement Warrior
Independent

@aleemcummins
https://www.linkedin.com/in/aleemcummins

SplunkTrust
Splunk User Group London
Splunk Study Club

Suman Gajavelly
CTO / Co-founder
BitsIO Inc

@sumangajavelly
https://www.linkedin.com/in/sumangajavelly

Fort Worth Splunk User Group

http://slack.splunkstudy.club

GitHub https://github.com/SplunkStudyClub

BSIDES splunk>

Session Agenda

AWS

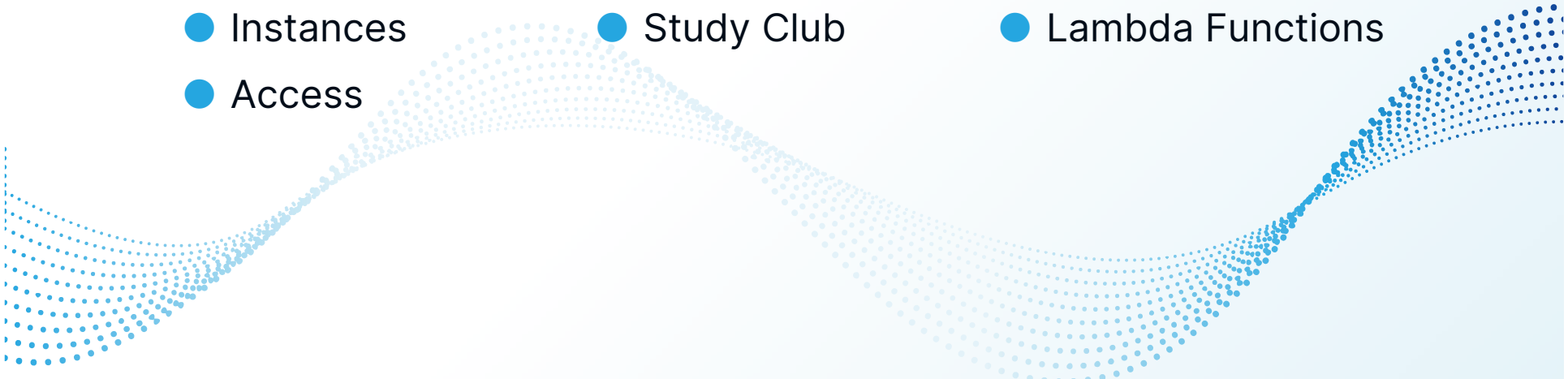
- Sign Up
- Security
- Instances
- Access

Splunk

- Deployment
- Growth
- Study Club

Keeping Lights On

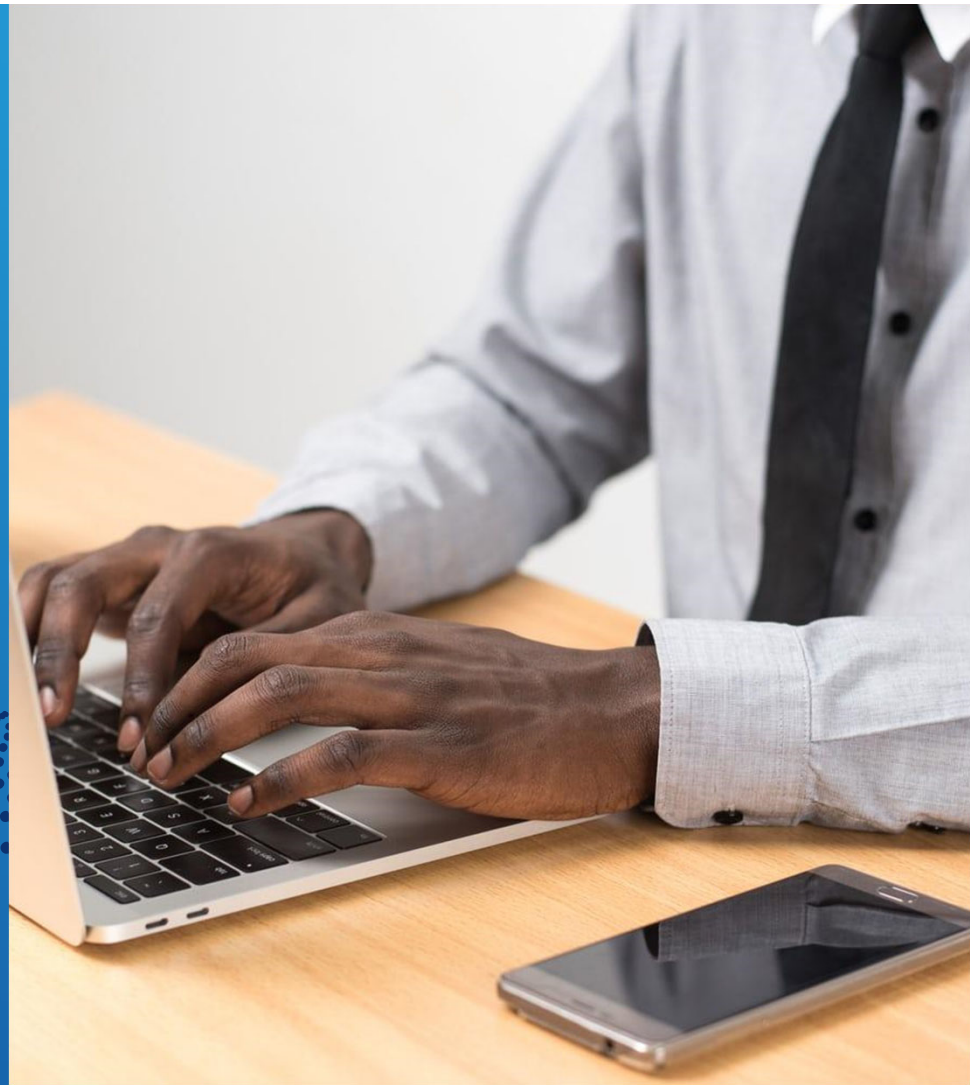
- DNS Scripts
- Splunking DNS Logs
- Lambda Functions



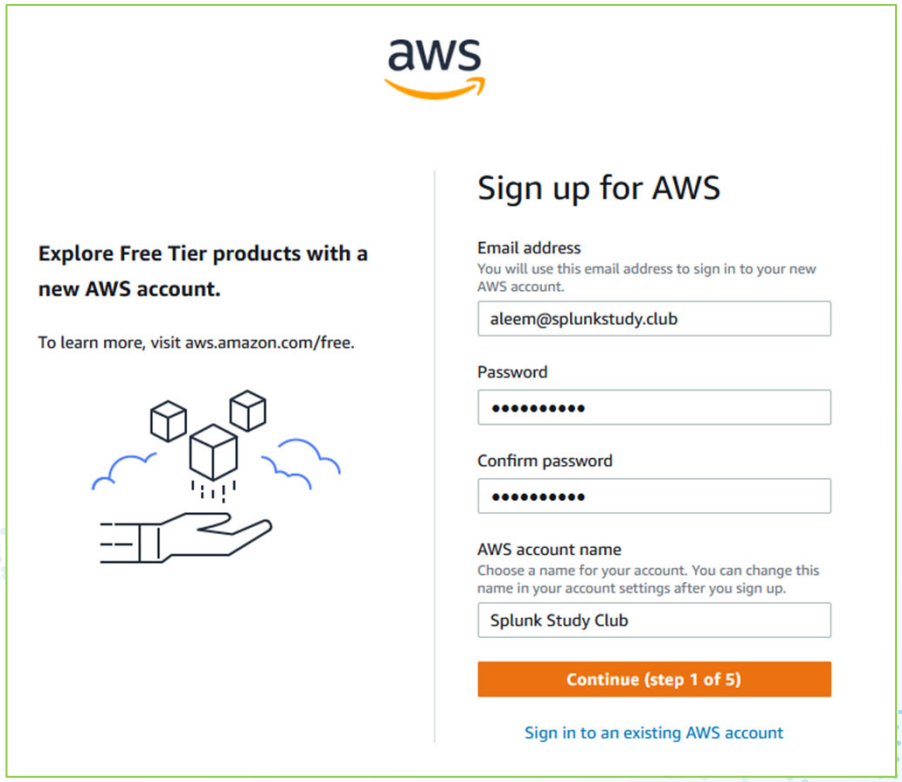
BSIDES splunk>

AWS

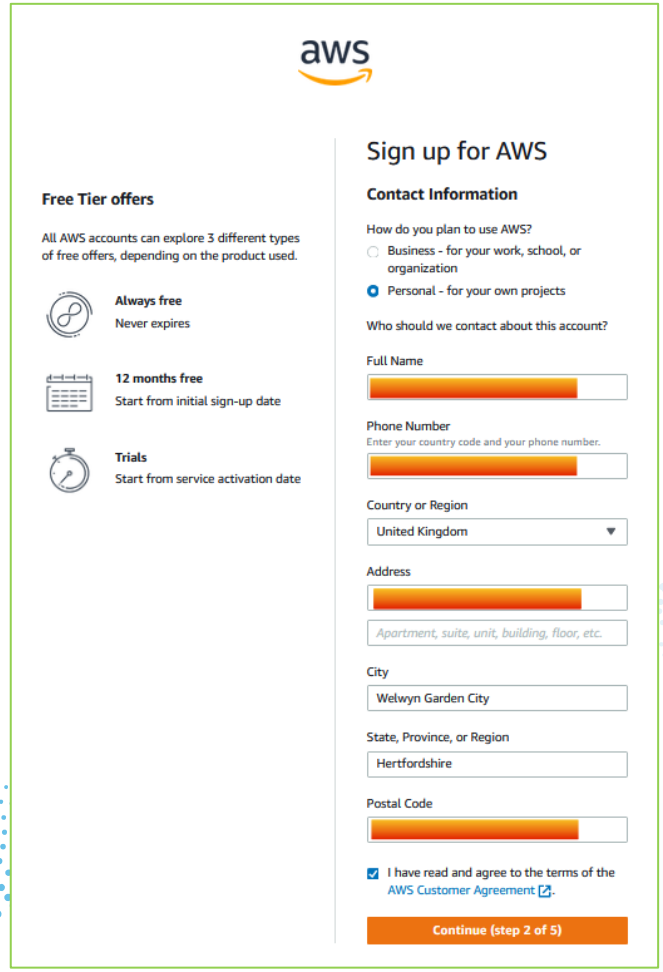
Sign Up

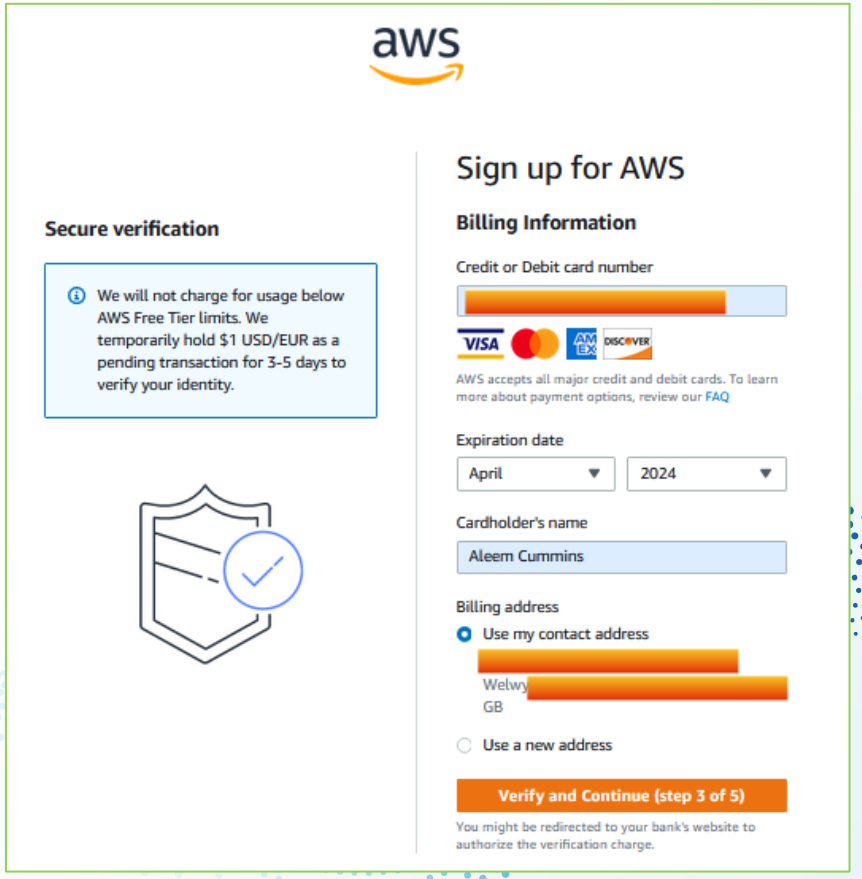


https://aws.amazon.com

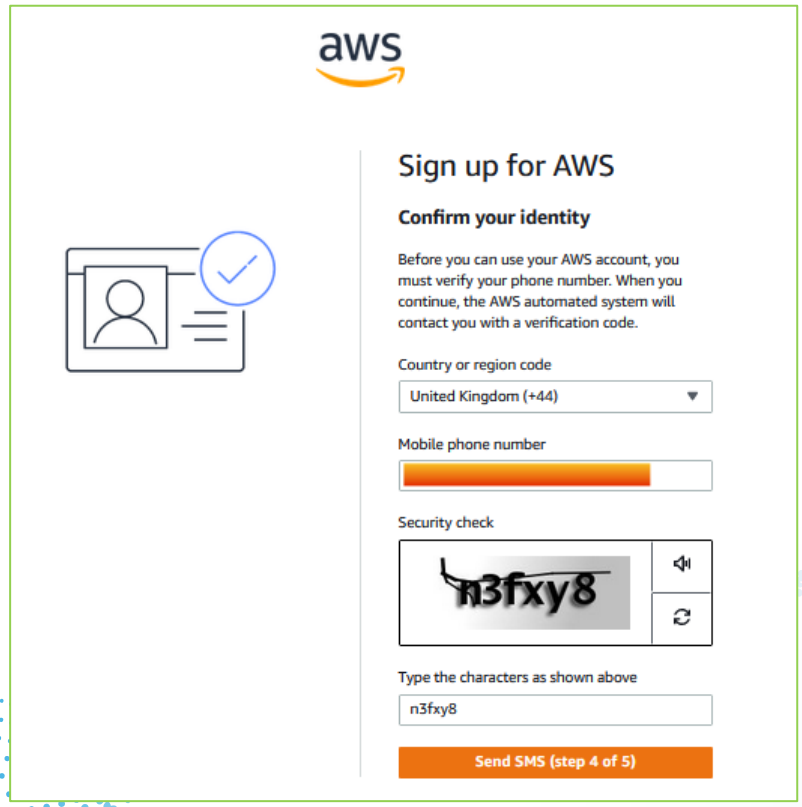


BSIDES splunk>

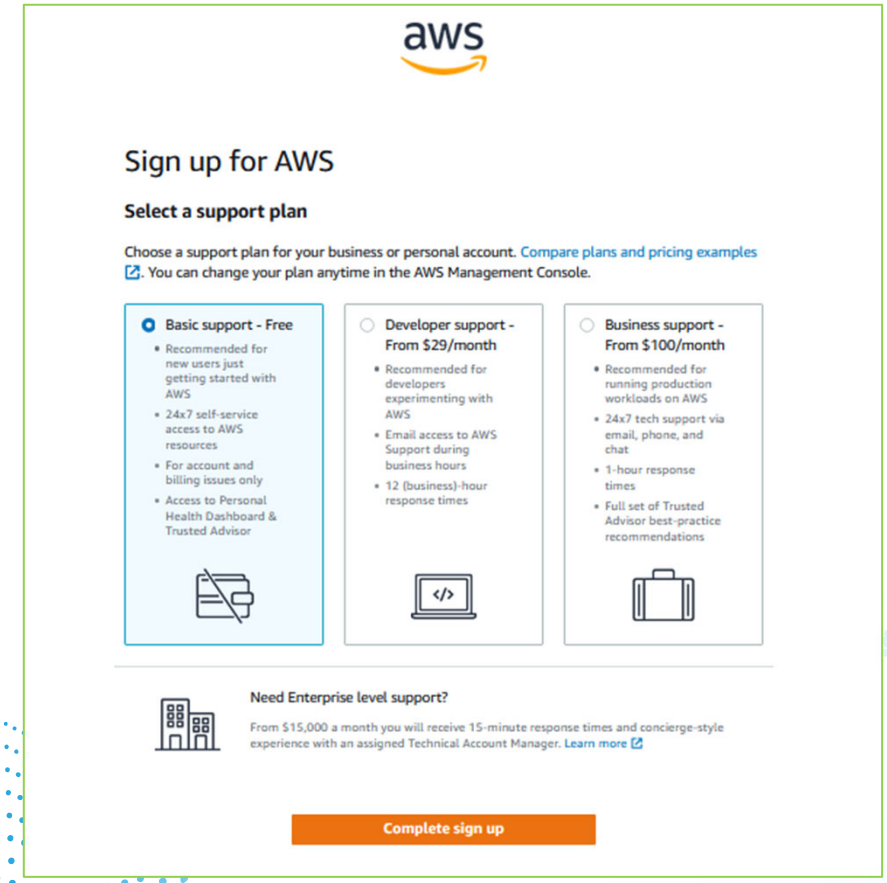


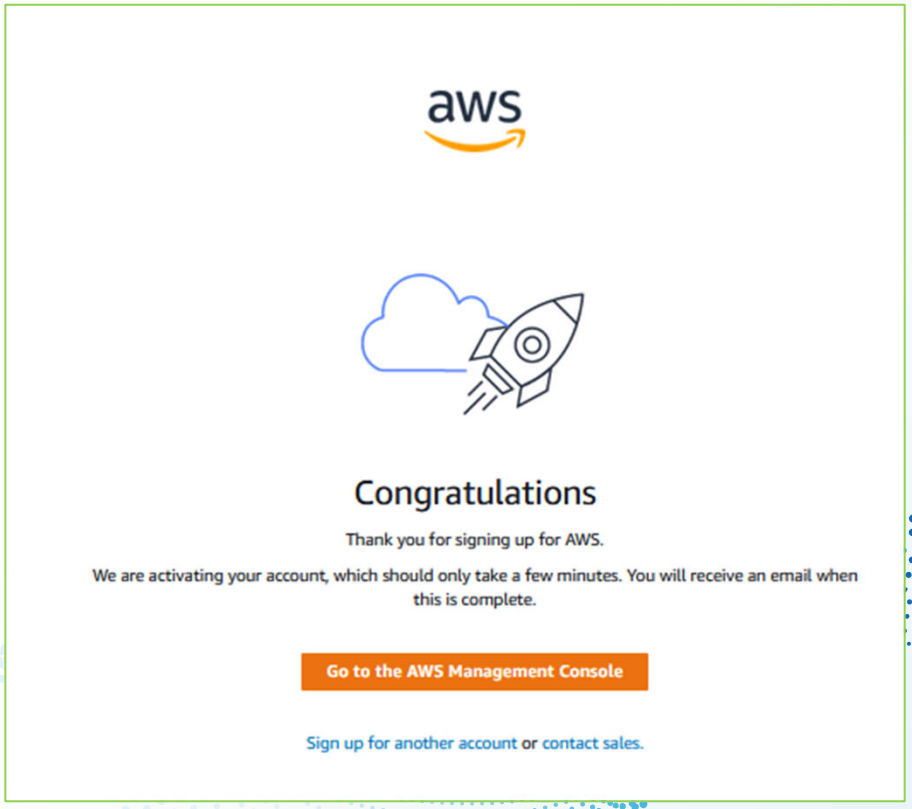


BSIDES splunk>

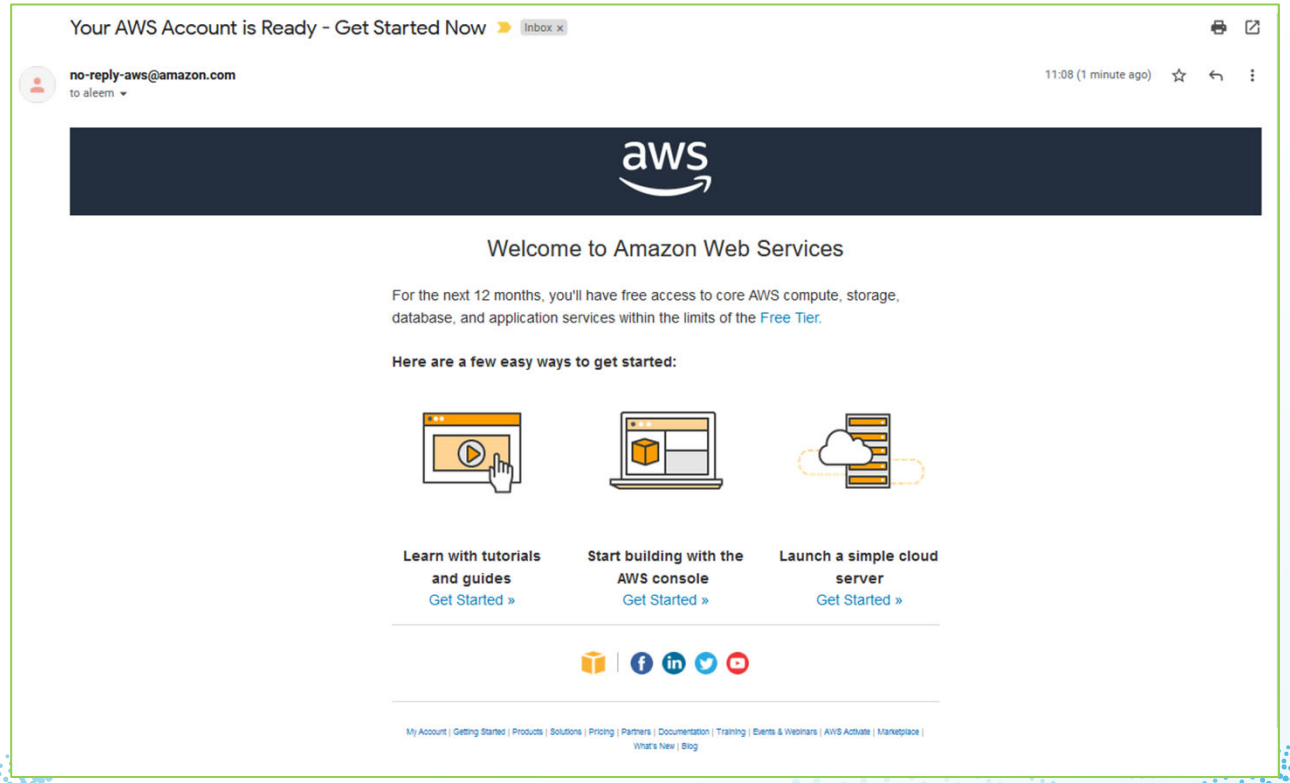


BSIDES splunk>



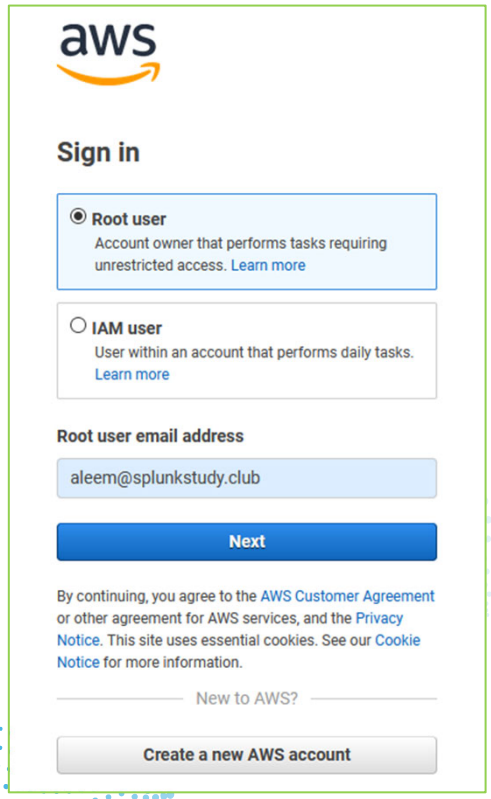


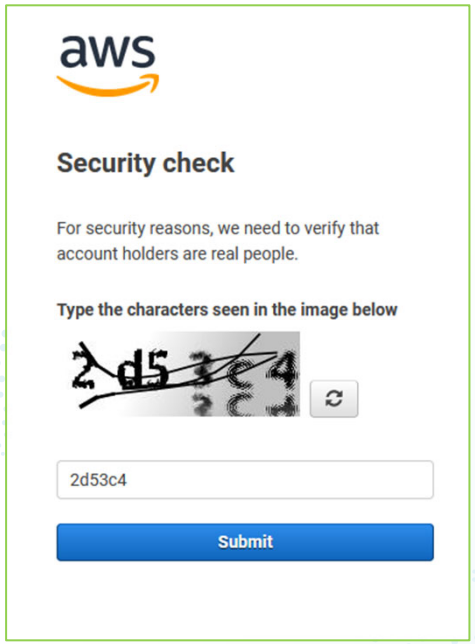
BSIDES splunk>

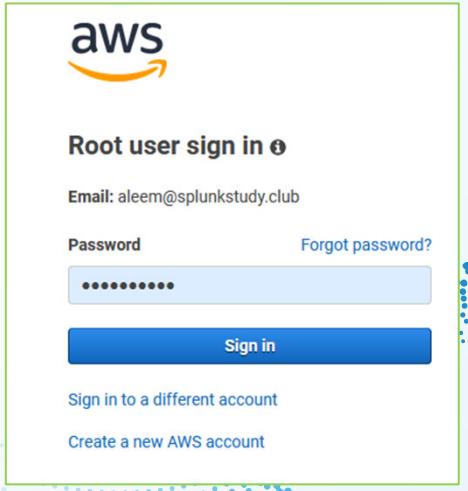


Wait for this email to come through

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

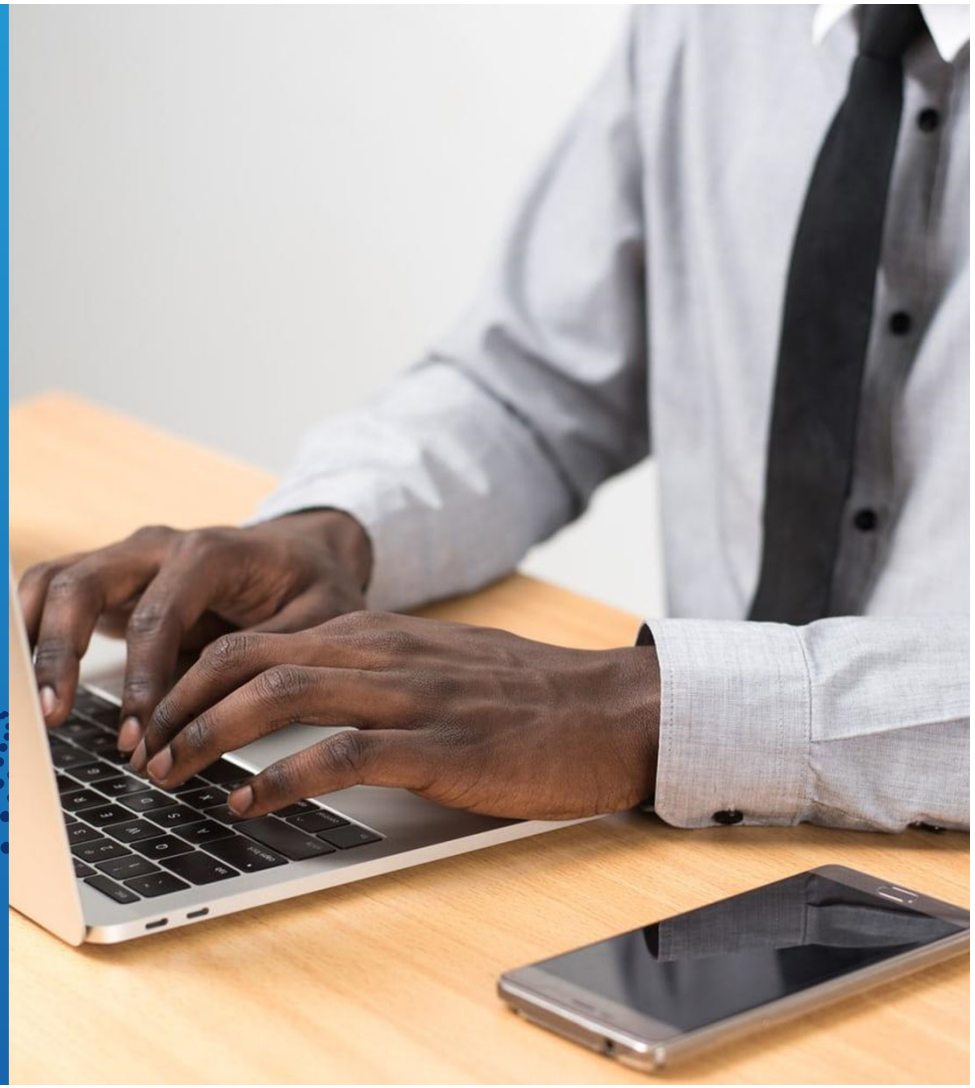




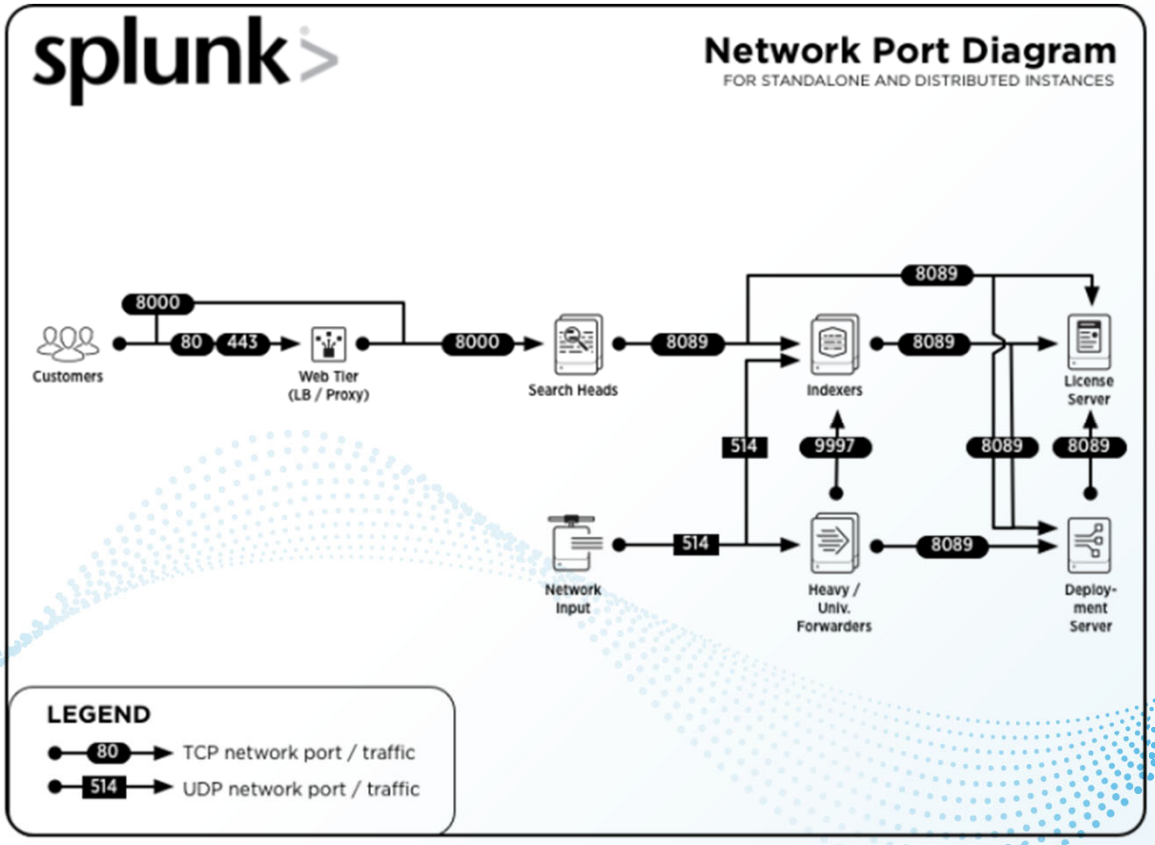


AWS: Security

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

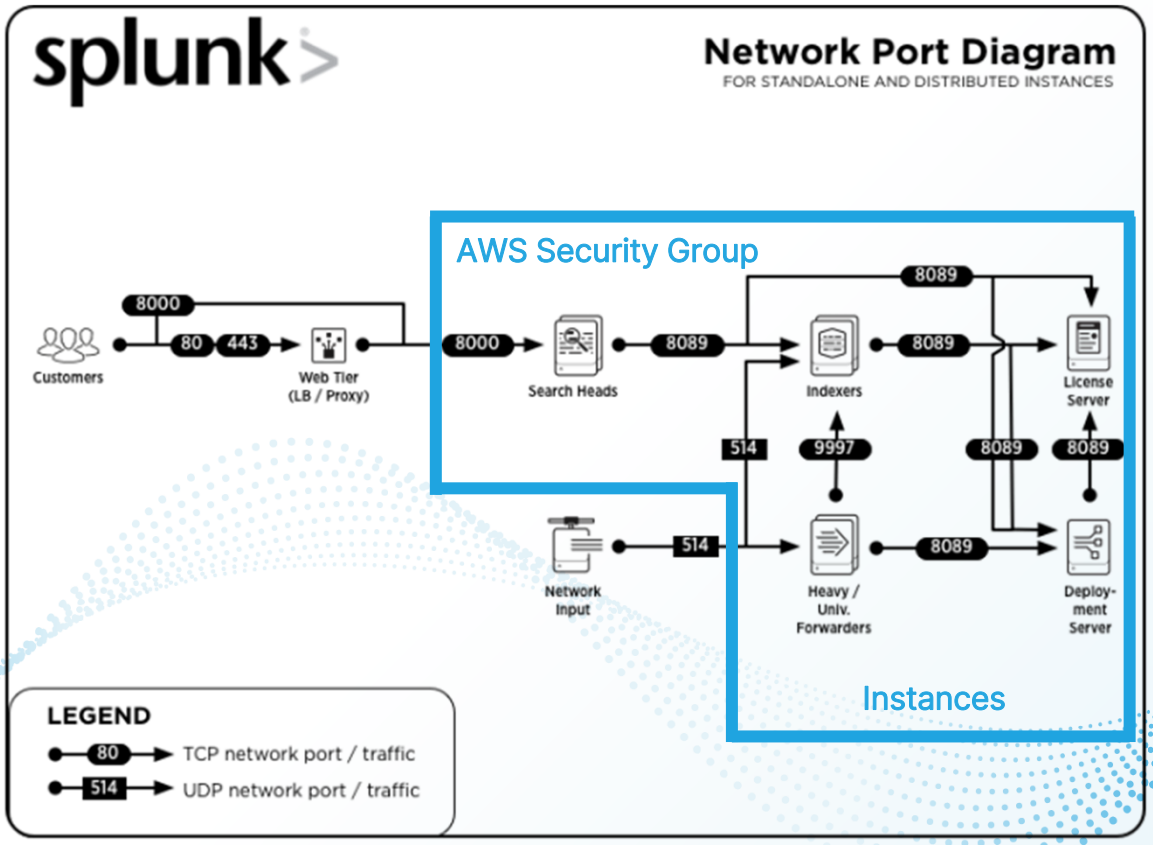
`Inbound Rules`

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

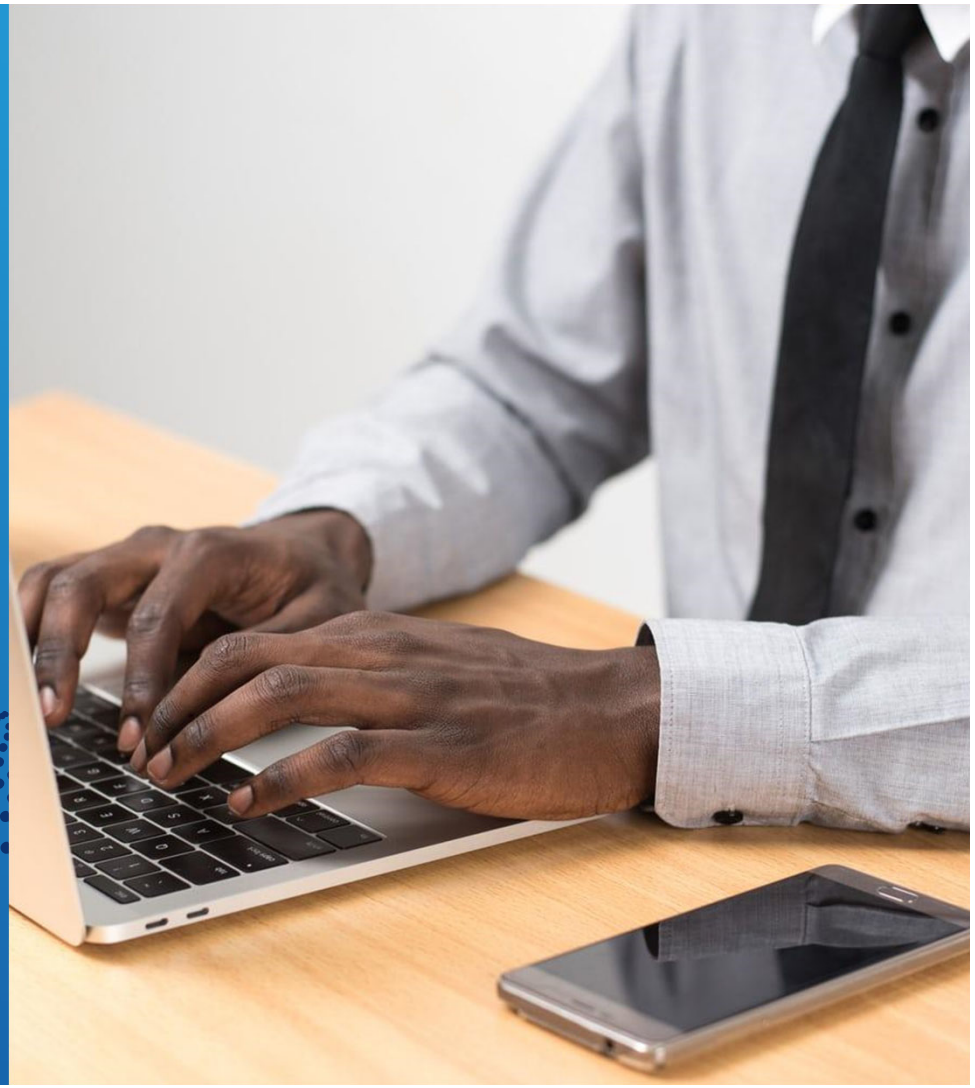


https://docs.splunk.com/Documentation/Splunk/8.1.3/InheritedDeployment/Ports

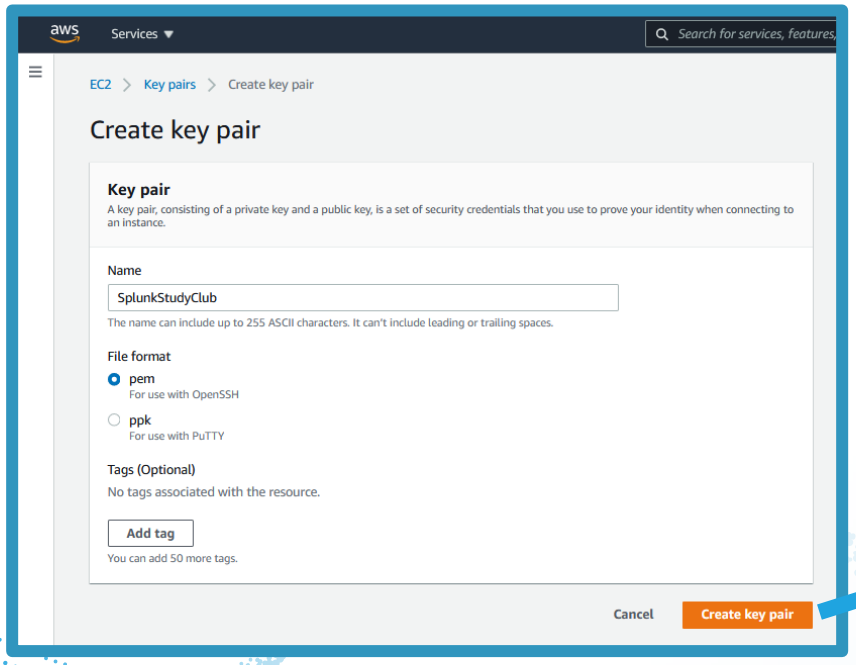
BSIDES splunk>

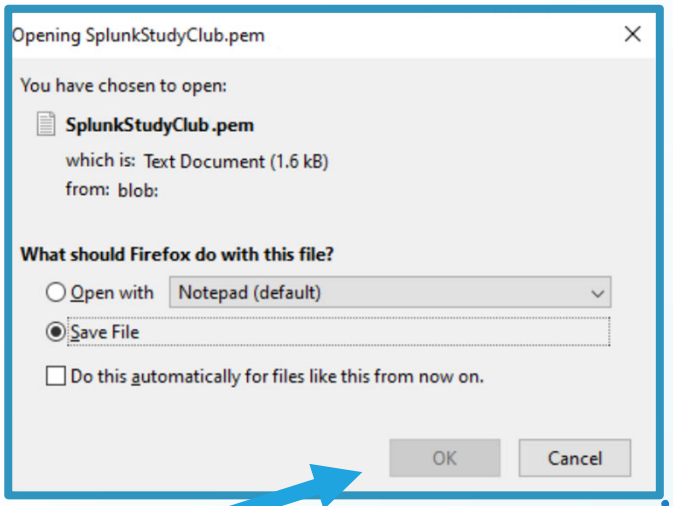
AWS: Security

Keys



Create Key Pair





Only downloadable on creation. Keep safe!

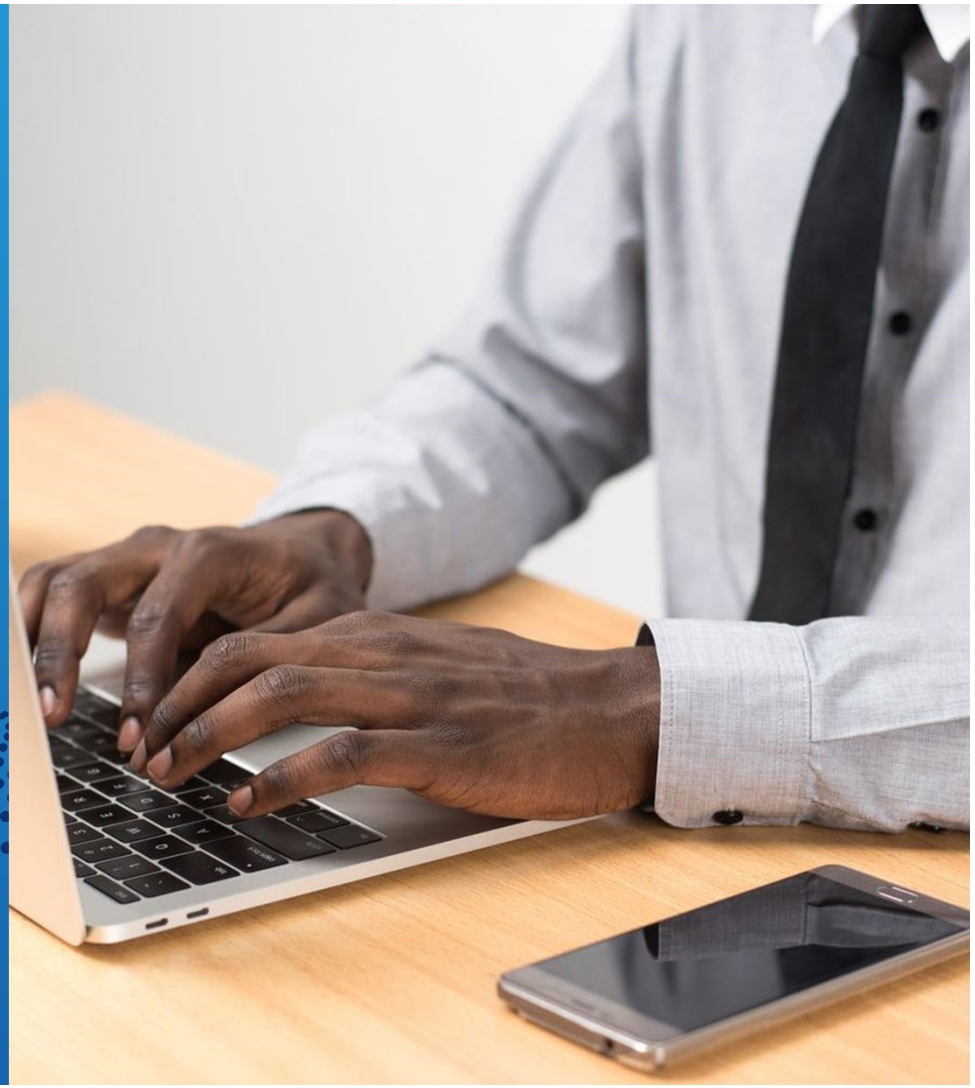
Permissions on download

Permissions required

BSIDES splunk>

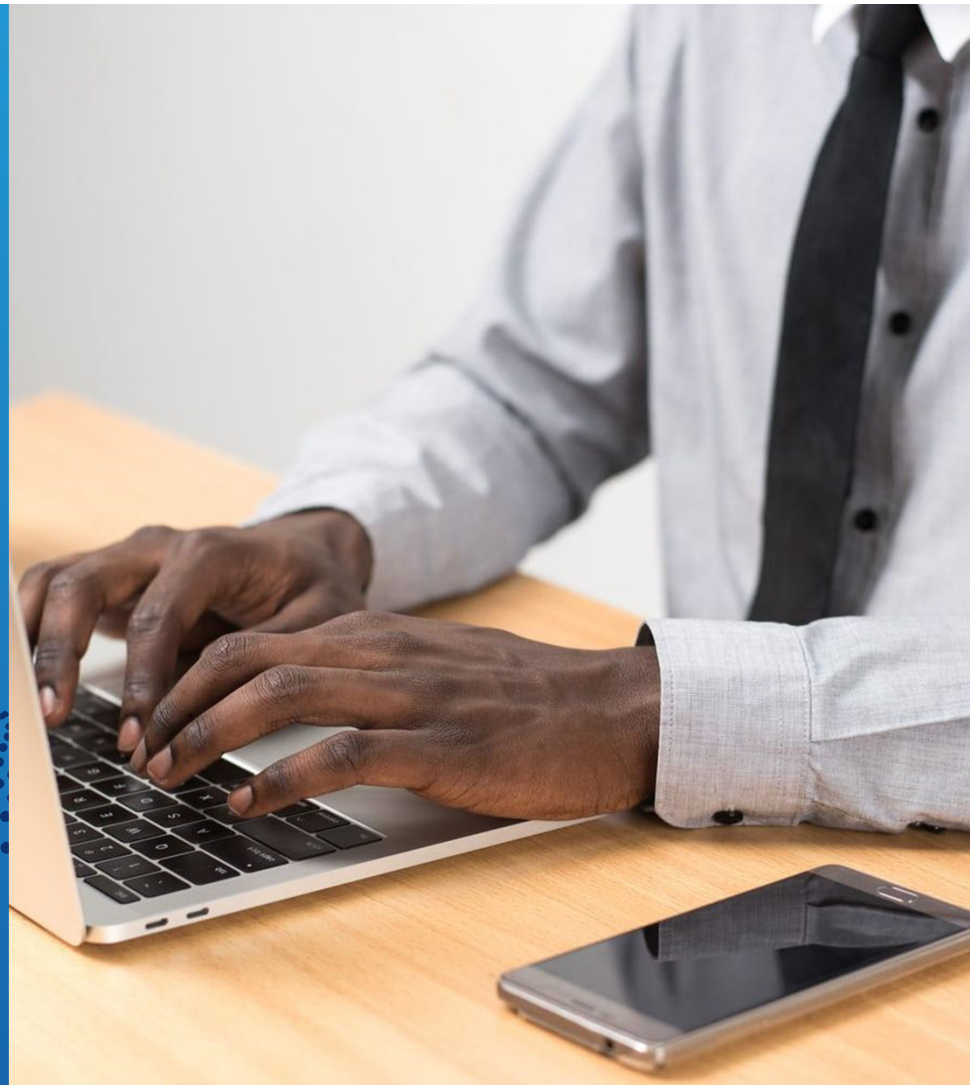
Create an Instance

Demo



AWS: Security

Access



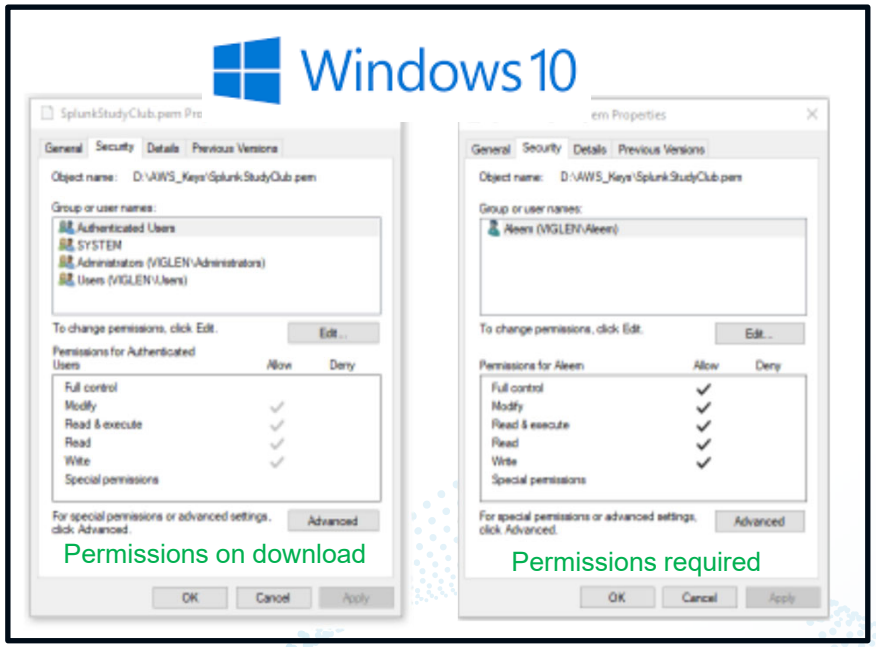
Accessing an AWS Instance

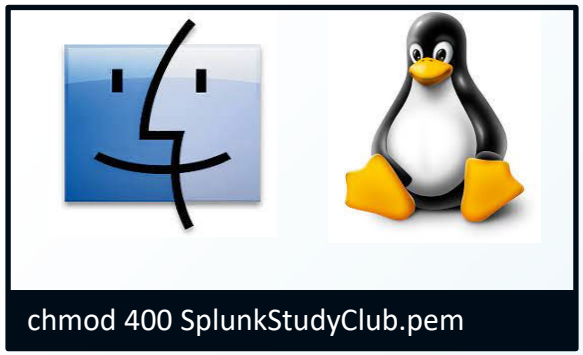
This will require an SSH client. Free examples include:

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





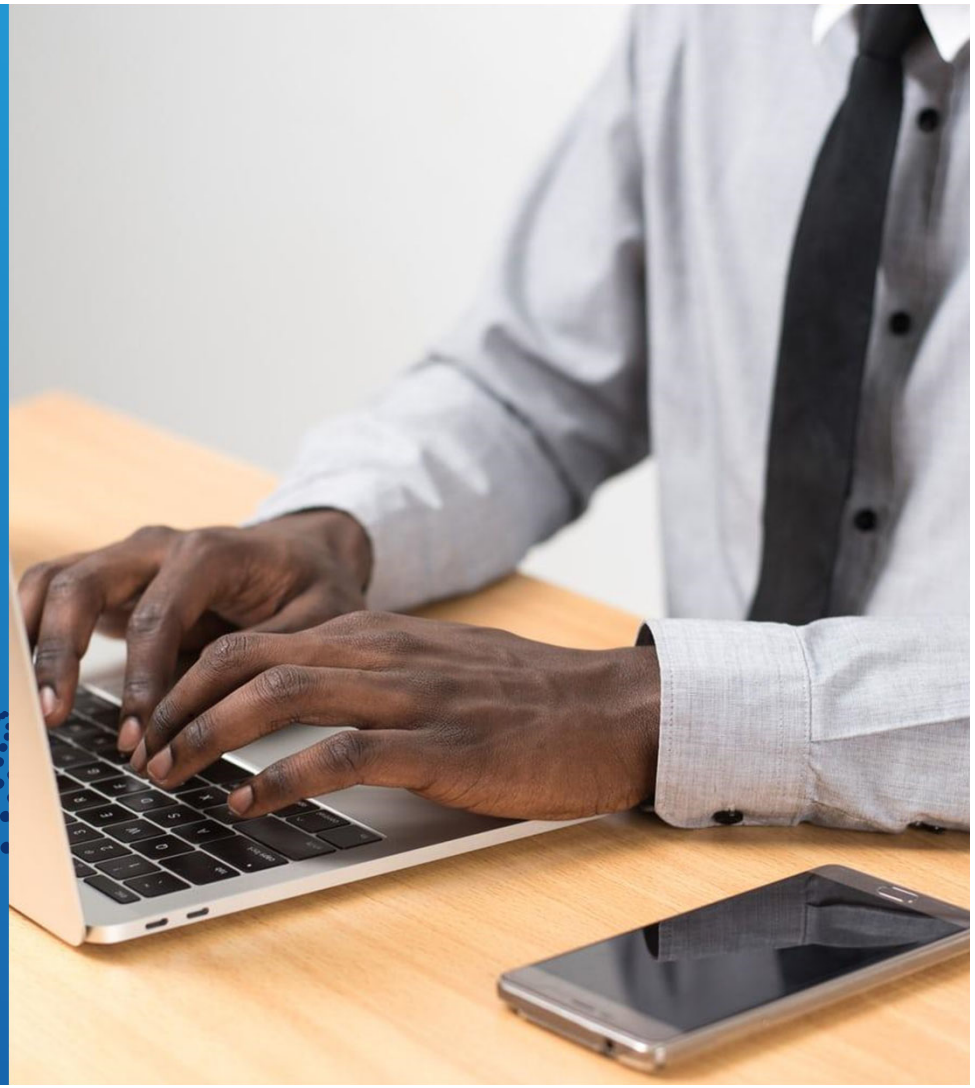

```
C:\restrict_pem_key.bat "c:\SplunkStudyClub.pem" "aleem"
```

GitHub

BSIDES splunk>

AWS:
Keeping lights on

Updating DNS



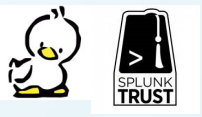
DNS Outcome

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)

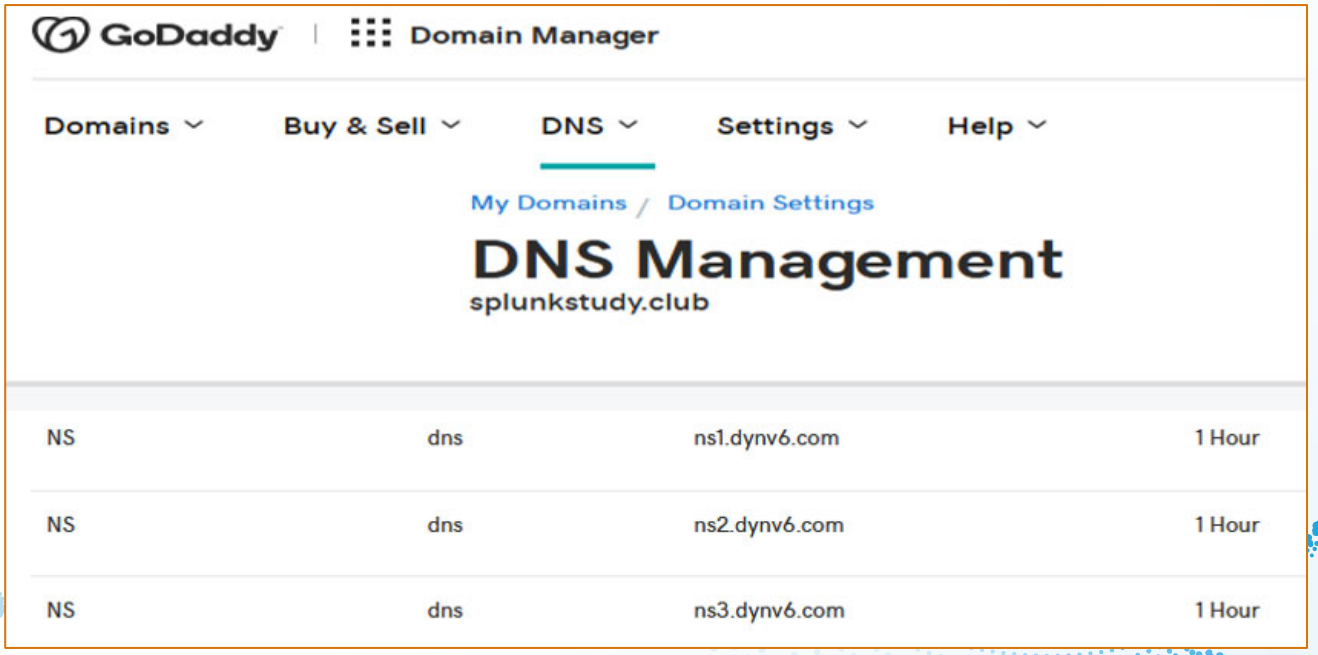
Type	Name	Value	TTL
NS	dns	ns1.dynv6.com	1 Hour
NS	dns	ns2.dynv6.com	1 Hour
NS	dns	ns3.dynv6.com	1 Hour



xpac

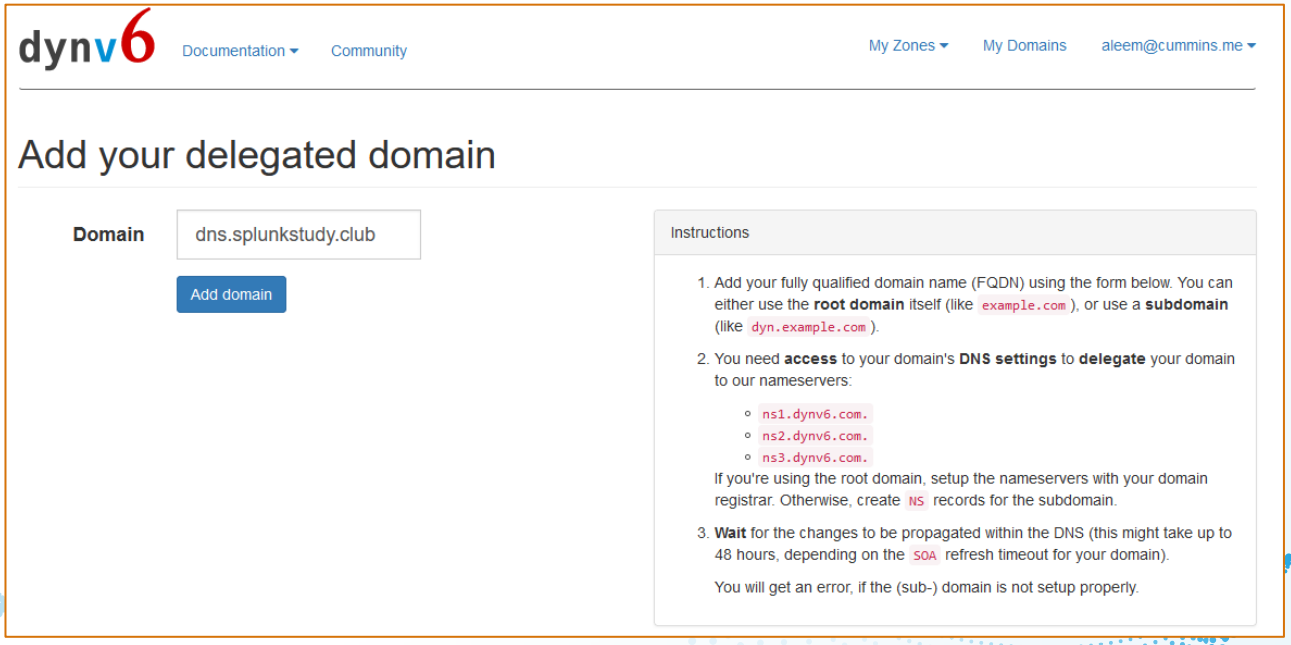
BSIDES splunk>

Subdomain Delegation



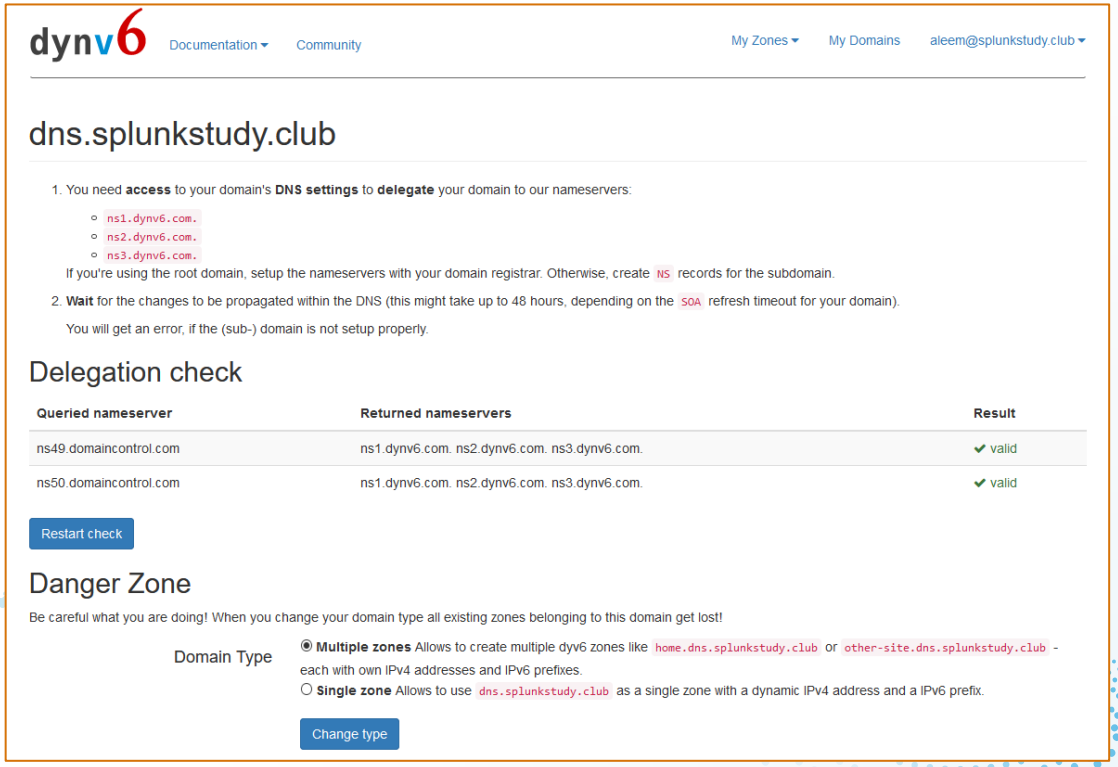
BSIDES splunk>

Delegated Domain Management

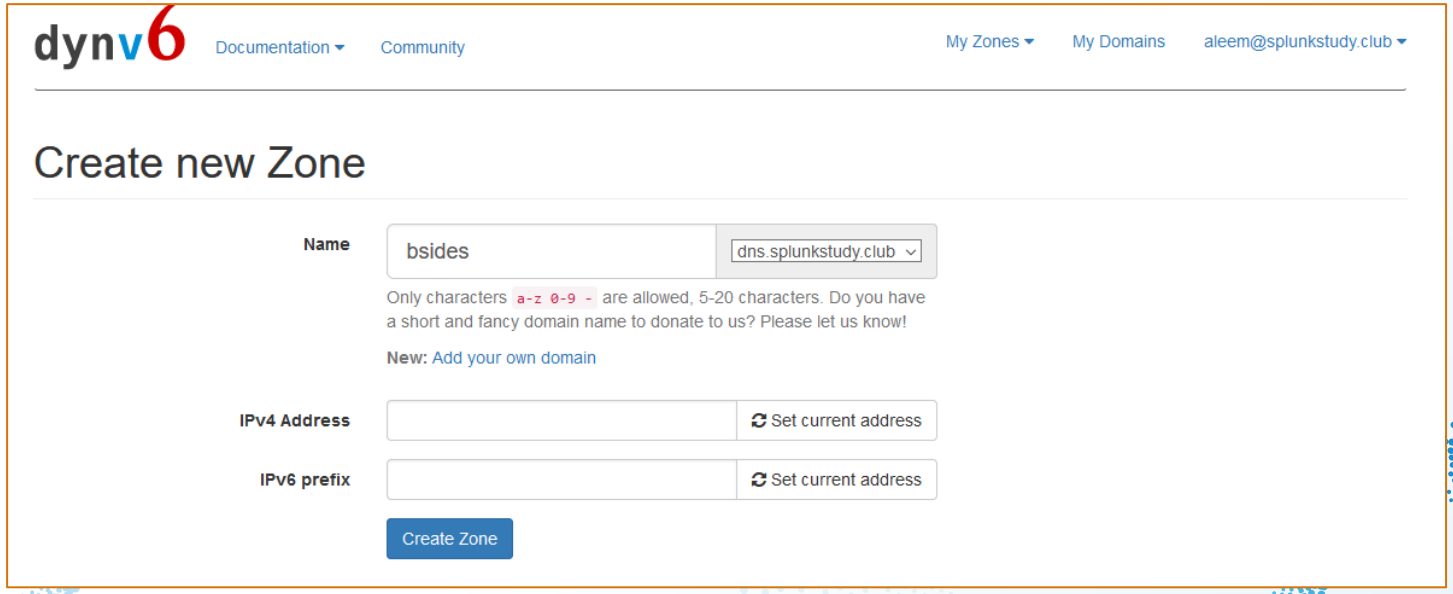


BSIDES splunk>

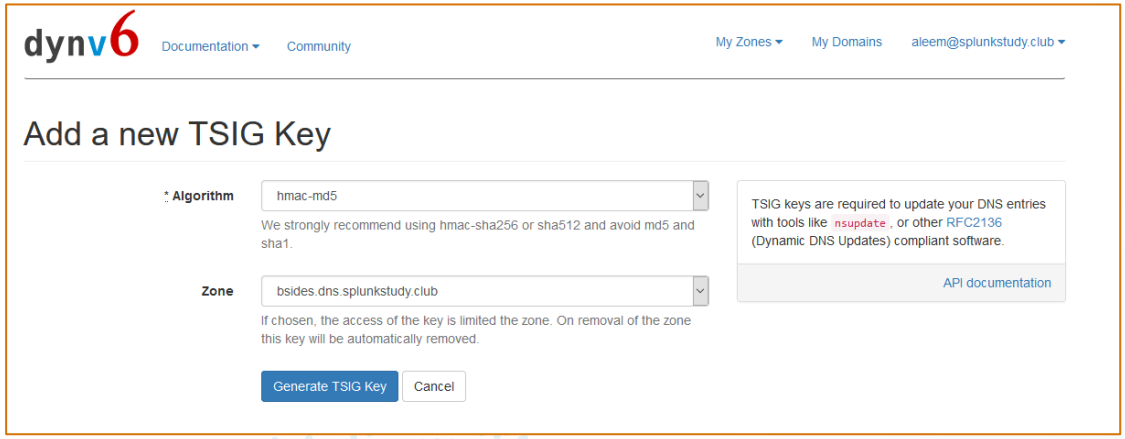
Delegated Domain Management

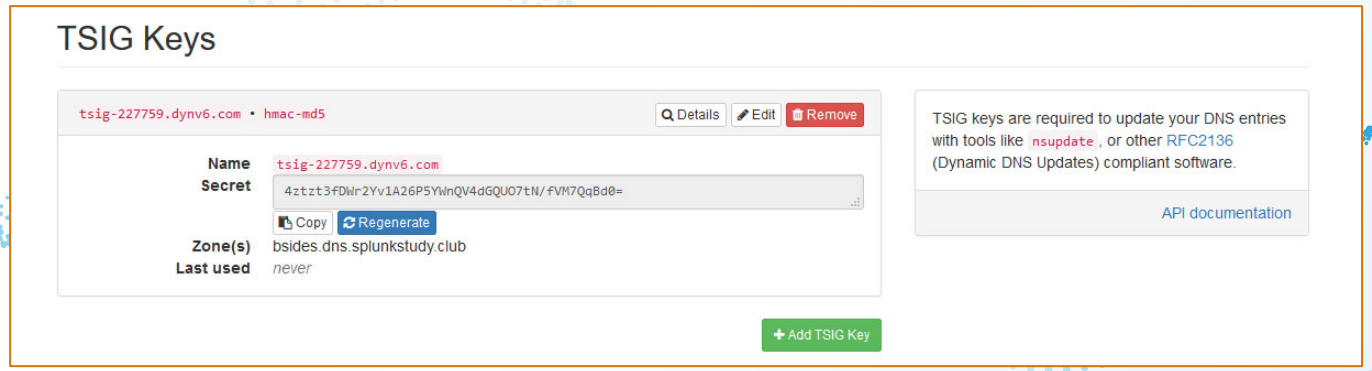


Adding DNS Zones



DNS Zone – Update Keys



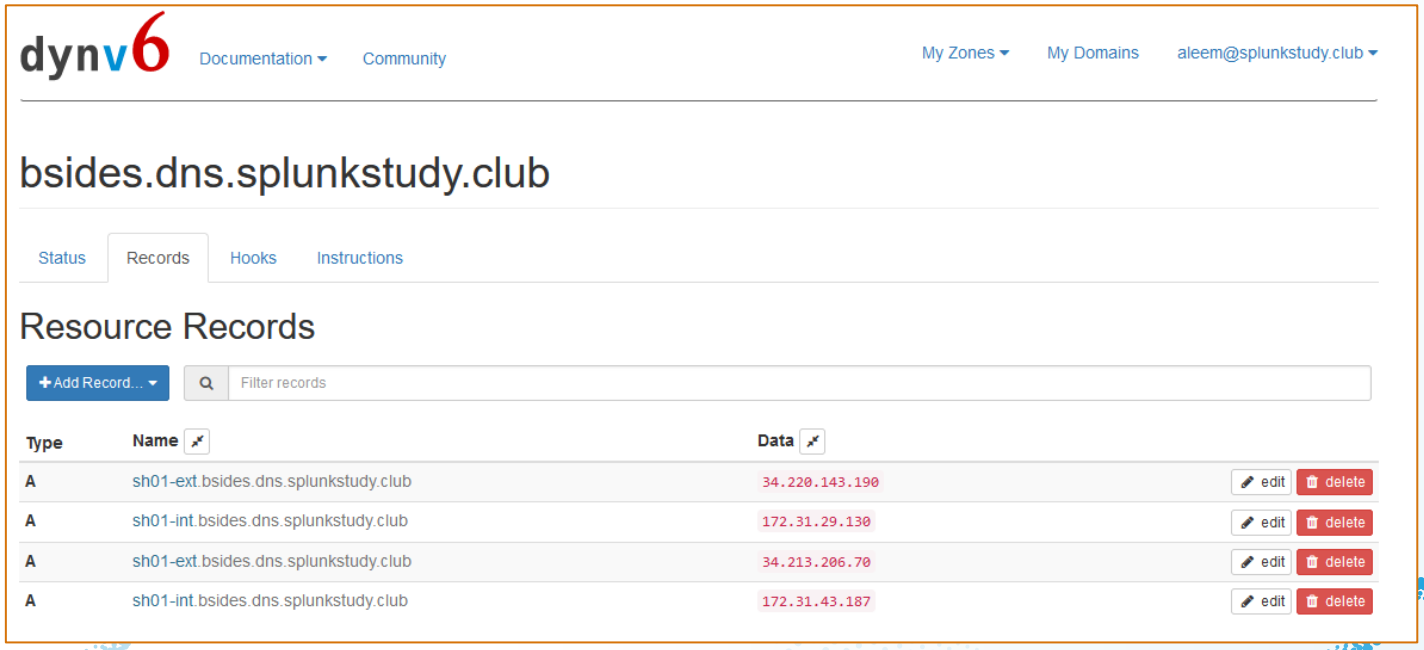


BSIDES splunk>

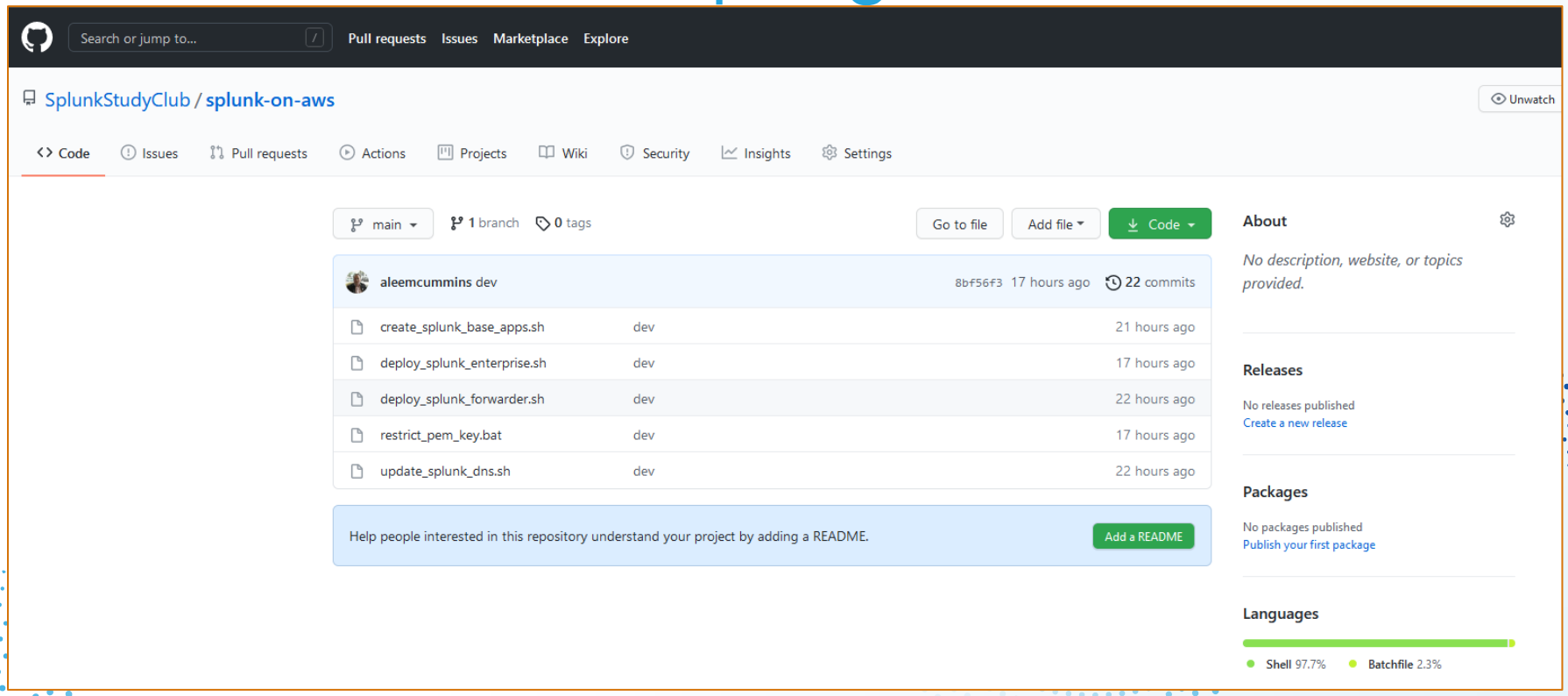
DNS Update Commands

```
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


dynv6
Documentation
Community
My Zones
My Domains
aleem@splunkstudy.club
bsides.dns.splunkstudy.club
Status
Records
Hooks
Instructions
Resource Records
+ Add Record...
Filter records
Type
Name
Data
A
sh01-ext.bsides.dns.splunkstudy.club
34.220.143.190
edit
delete
A
sh01-int.bsides.dns.splunkstudy.club
172.31.29.130
edit
delete
A
sh01-ext.bsides.dns.splunkstudy.club
34.213.206.70
edit
delete
A
sh01-int.bsides.dns.splunkstudy.club
172.31.43.187
edit
delete

DNS Scripting - GitHub



GitHub https://github.com/SplunkStudyClub

BSIDES splunk>

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!!

BSIDES splunk>

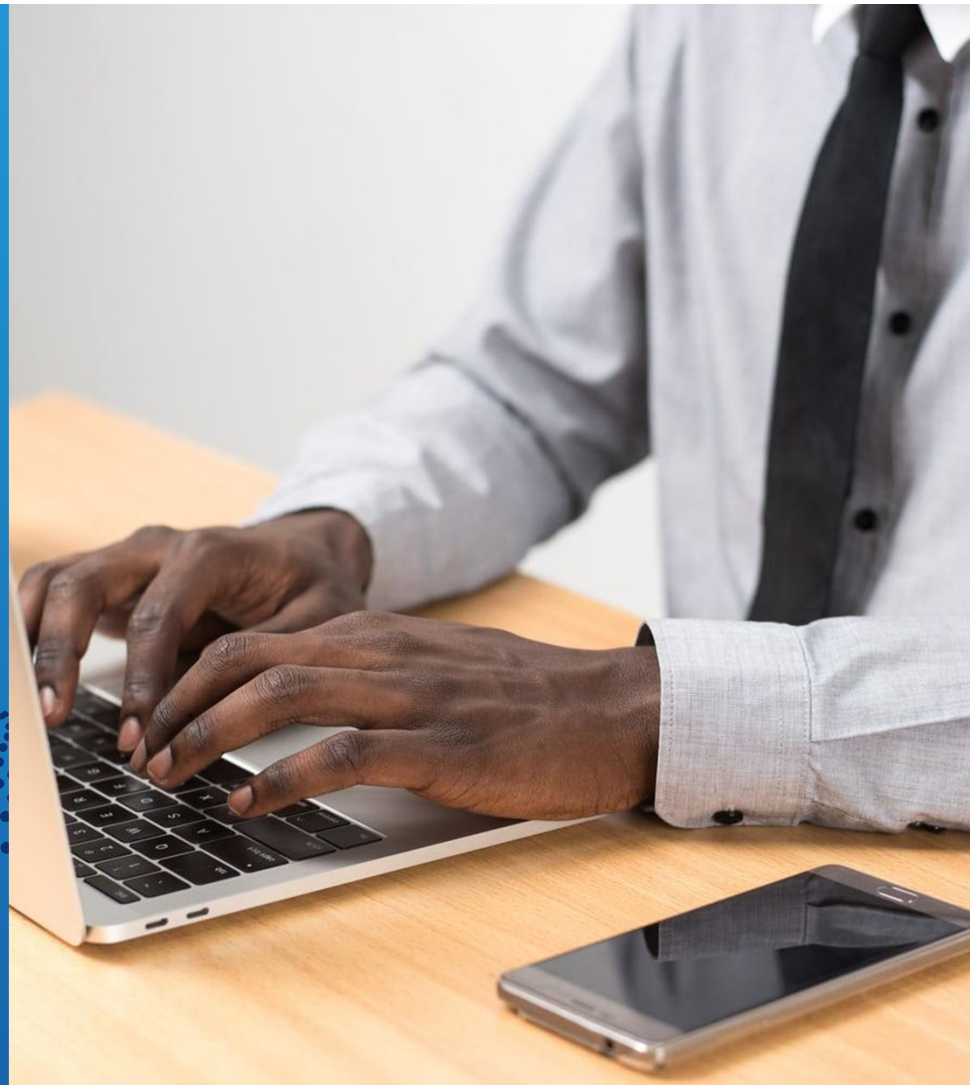
DNS Update Logs

```
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
```

BSIDES splunk>

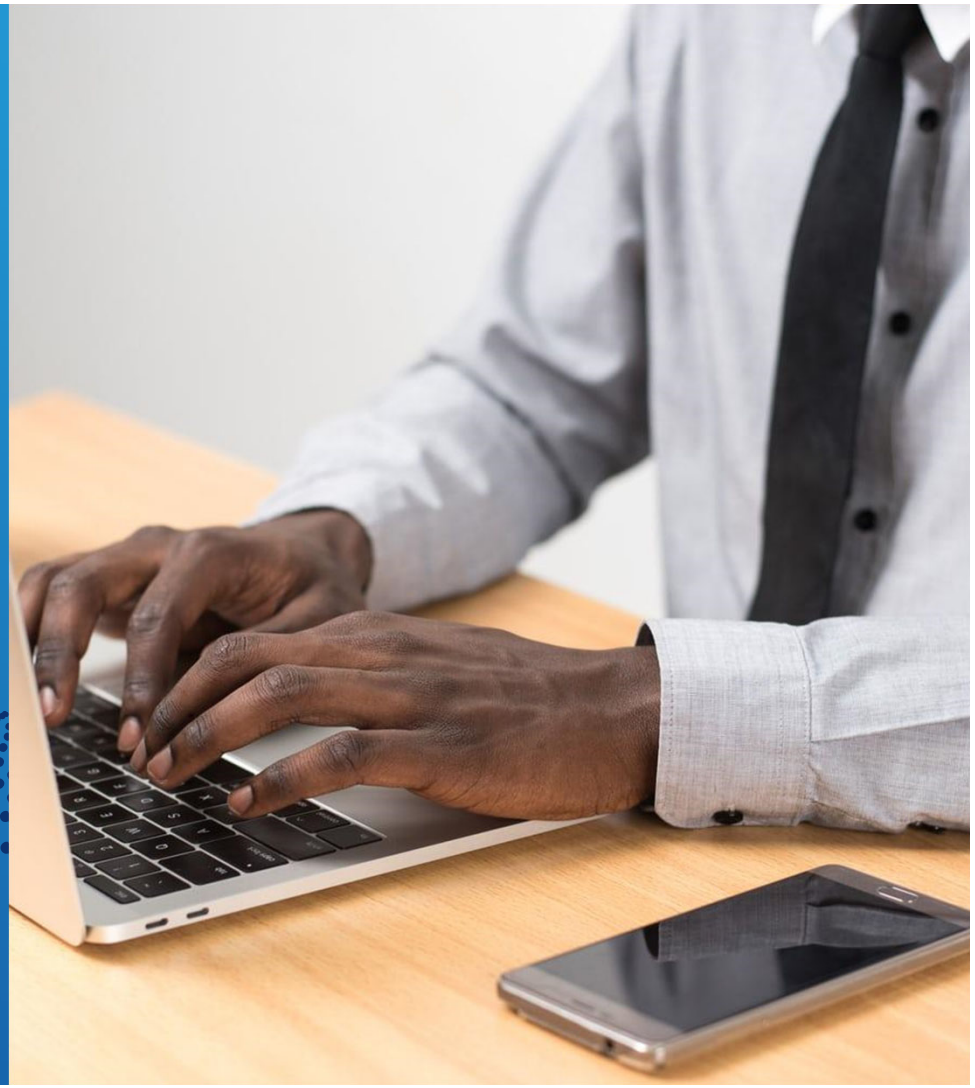
Accessing an Instance Deploying Splunk

Demo



Onboarding DNS Logs

Demo

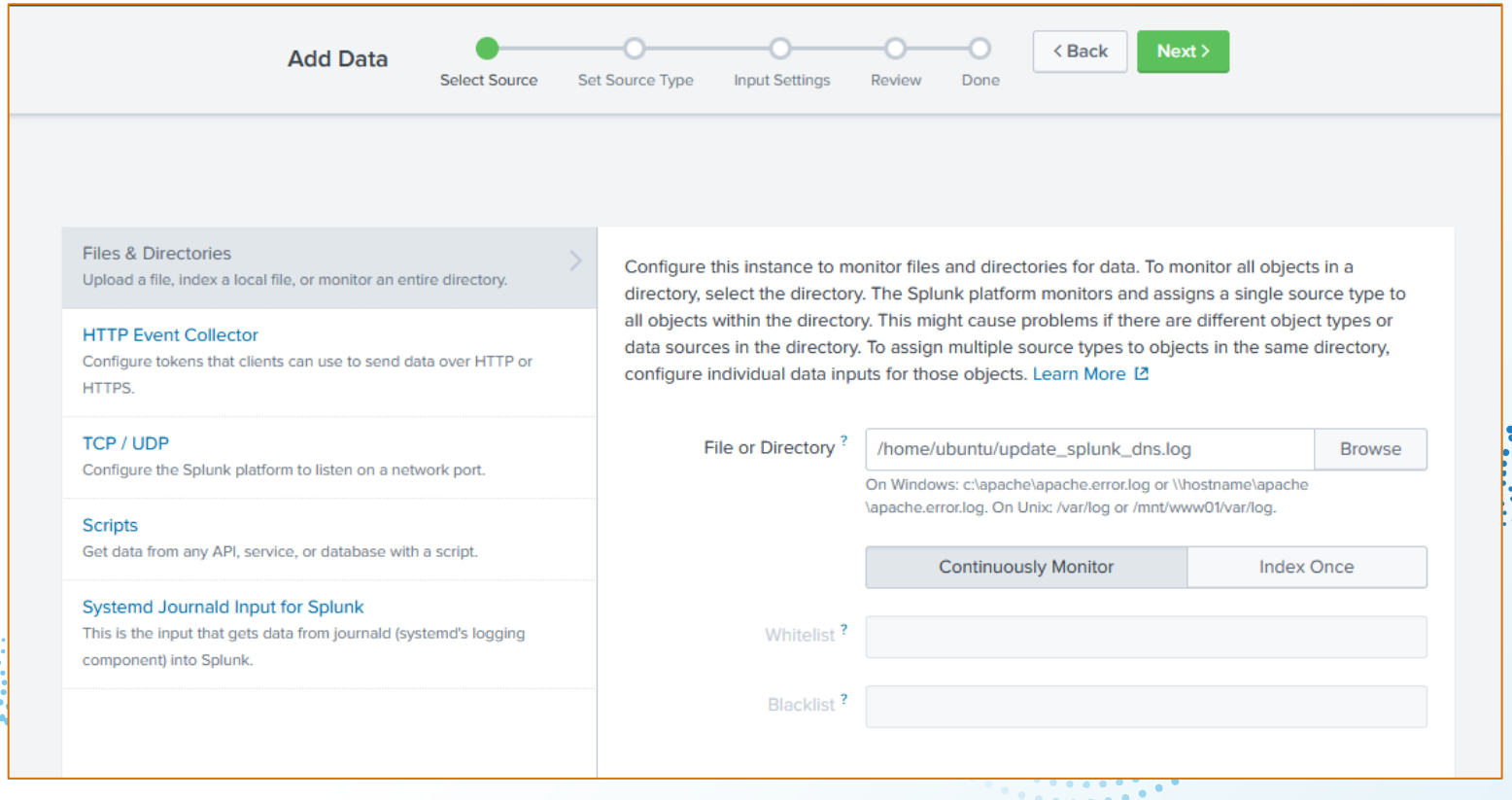


Onboarding DNS Update Logs

```
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
```

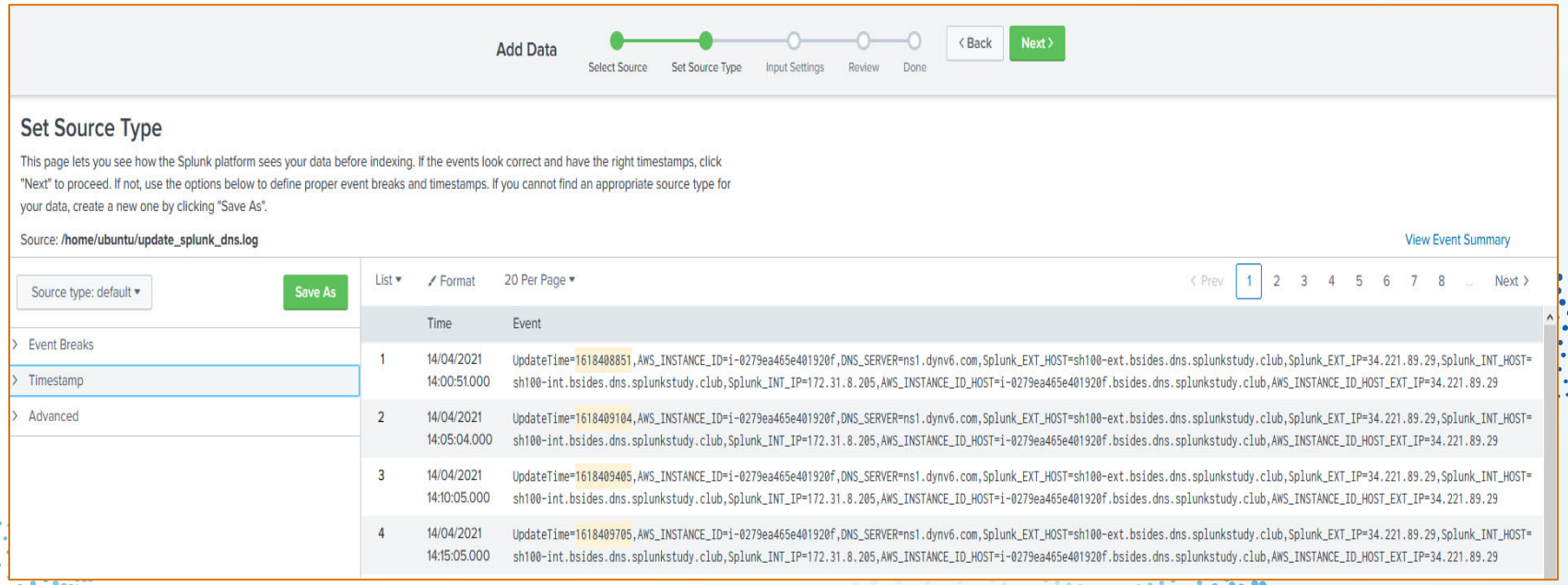
BSIDES splunk>

Onboarding DNS Update Logs



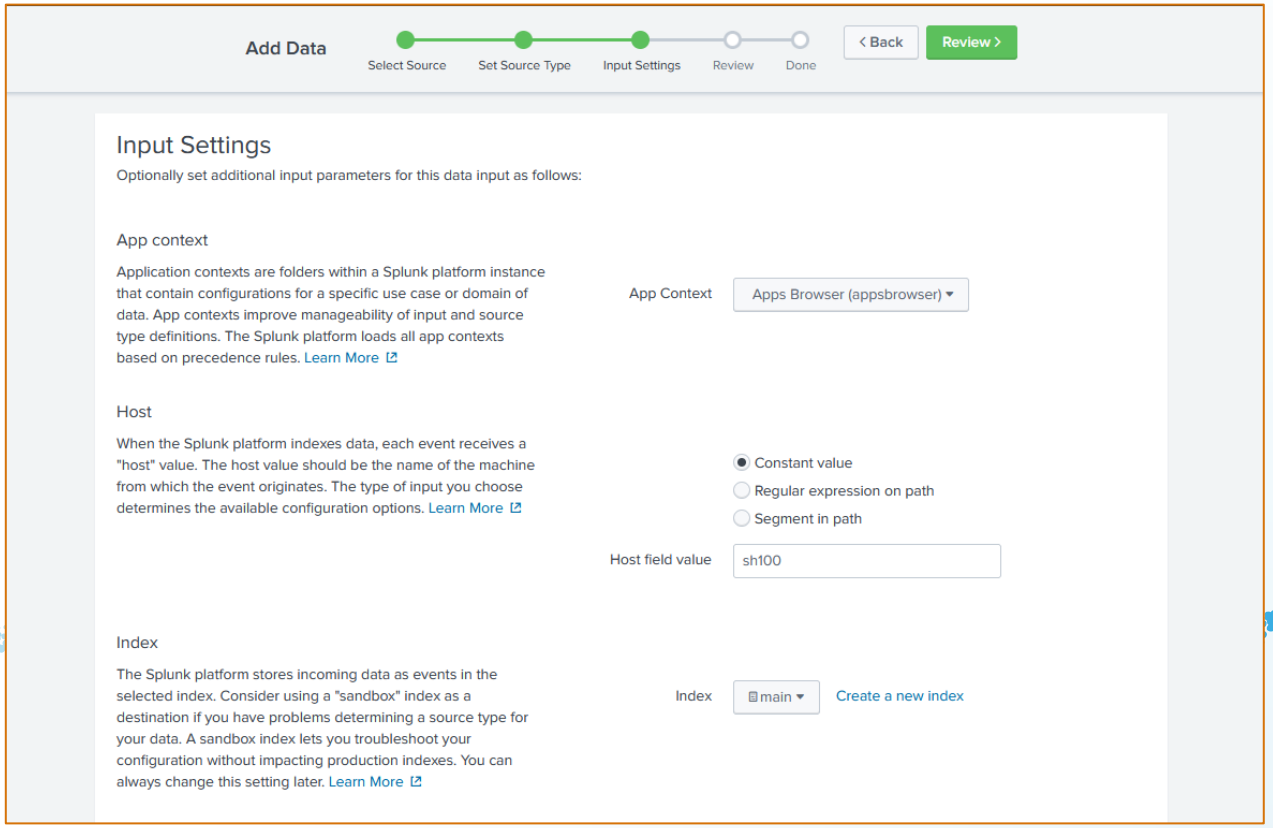
BSIDES splunk>

Onboarding DNS Update Logs



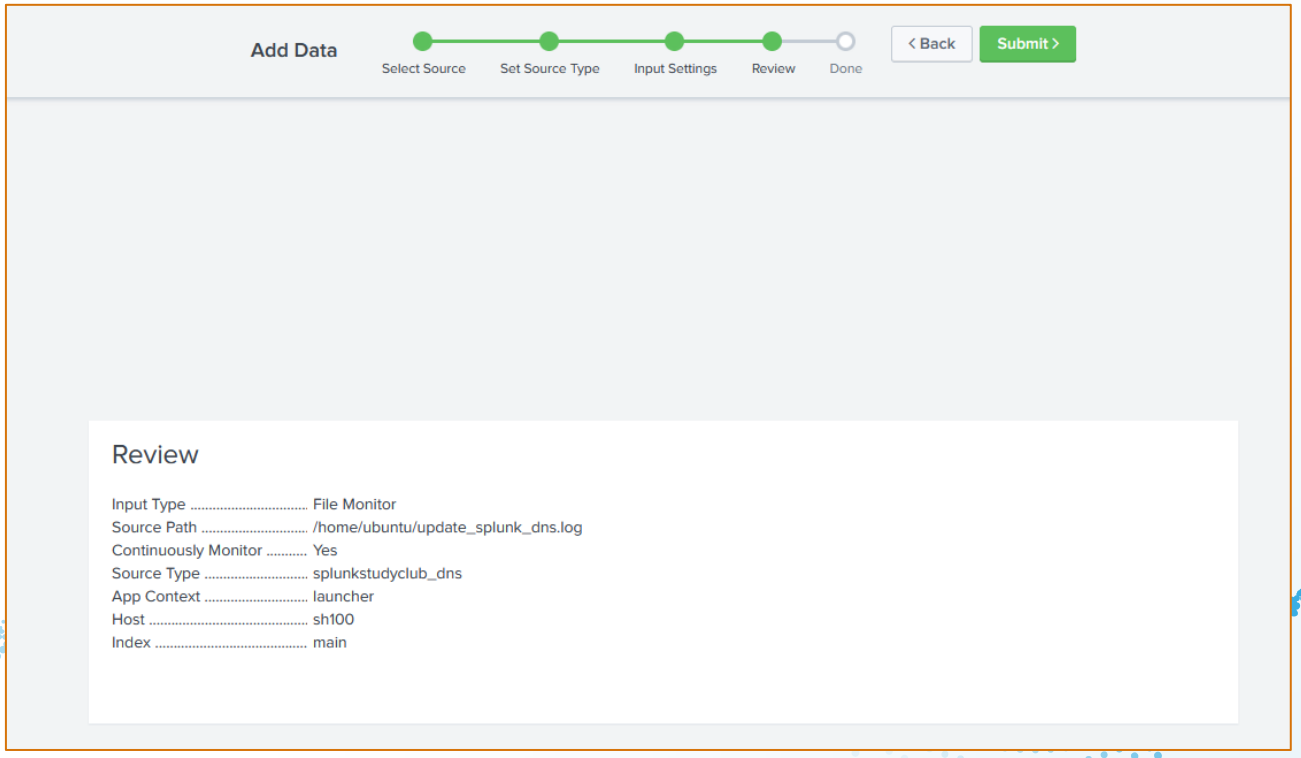
BSIDES splunk>

Onboarding DNS Update Logs



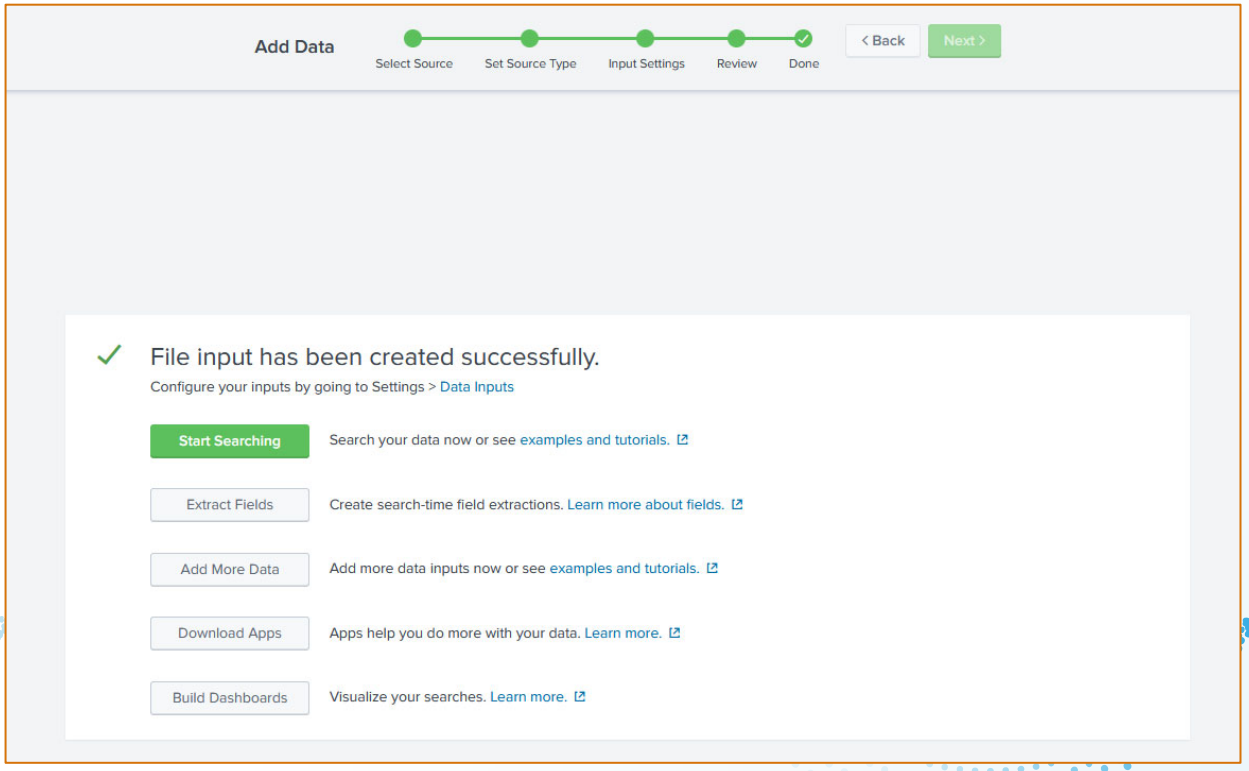
BSIDES splunk>

Onboarding DNS Update Logs



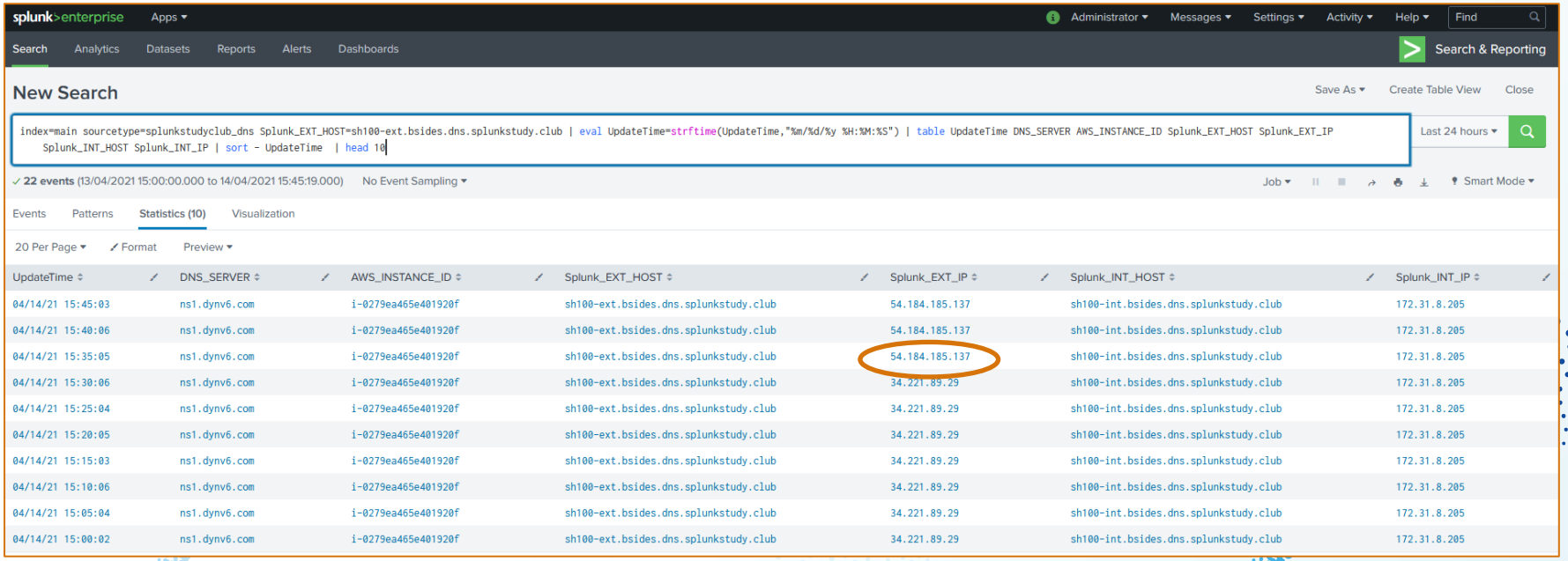
BSIDES splunk>

Onboarding DNS Update Logs



BSIDES splunk>

Working with DNS Update Logs

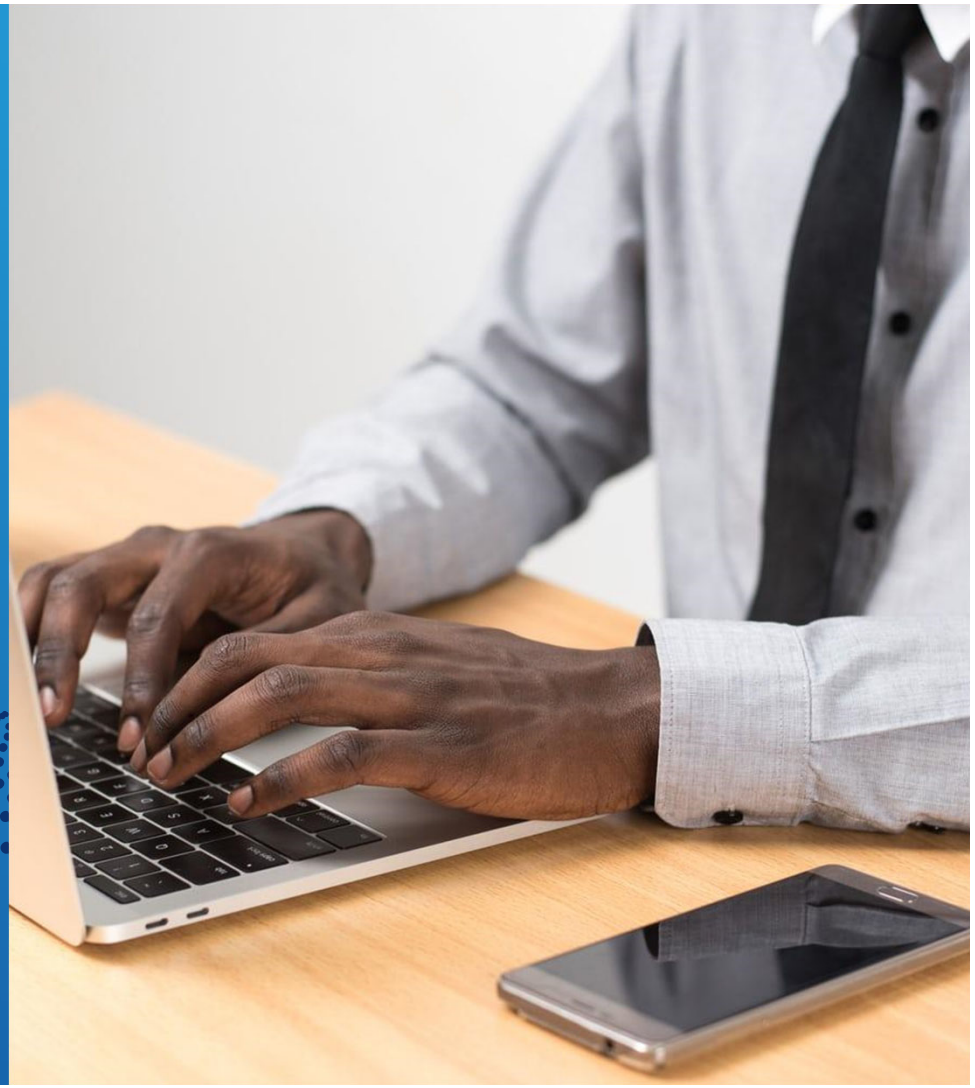



```
index=main sourcetype=splunkstudyclub_dns | eval UpdateTime=strftime(UpdateTime,"%m/%d/%y %H:%M:%S") | table UpdateTime DNS_SERVER AWS_INSTANCE_ID Splunk_EXT_HOST Splunk_EXT_IP Splunk_INT_HOST Splunk_INT_IP | sort - UpdateTime  | head 10
```

```
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

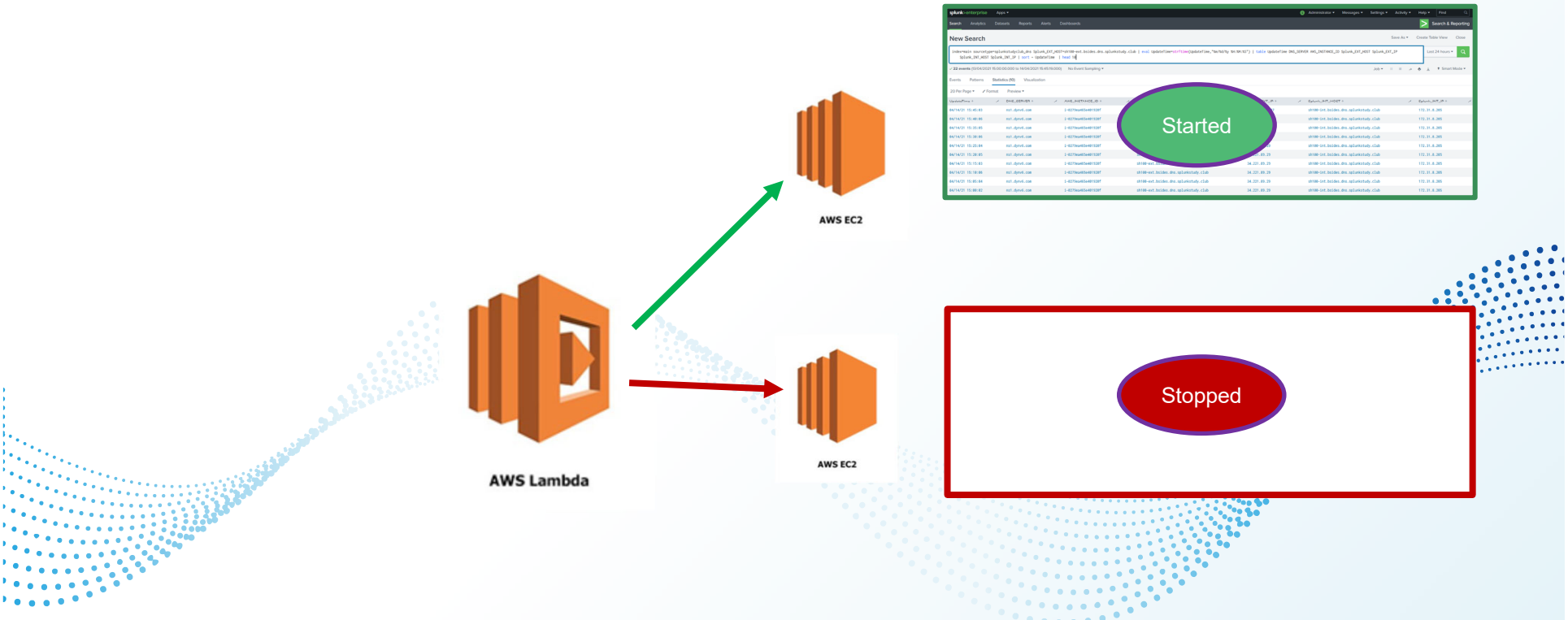


AWS Lambda

SPLUNK TRUST

jkat54

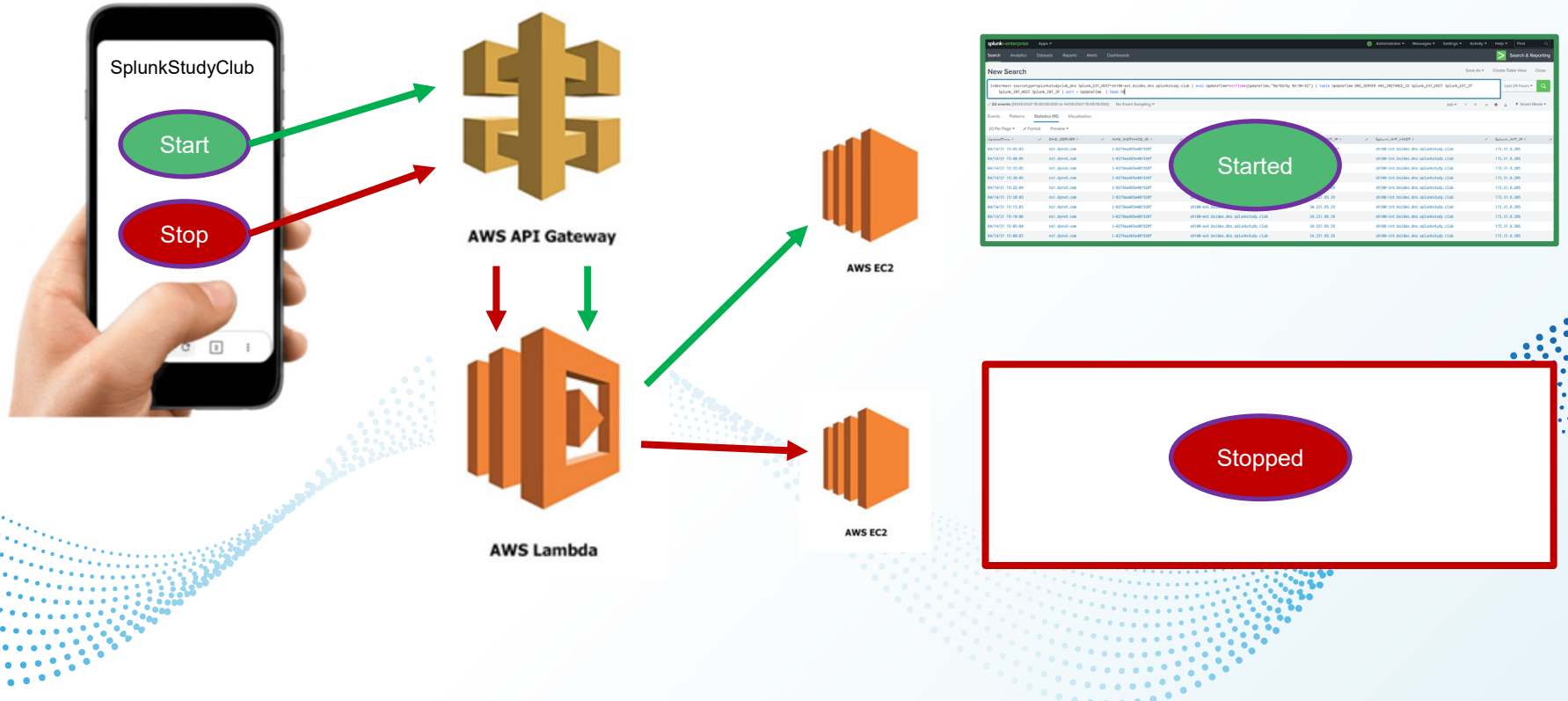
Lambda Functions - Concept



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

BSIDES splunk>

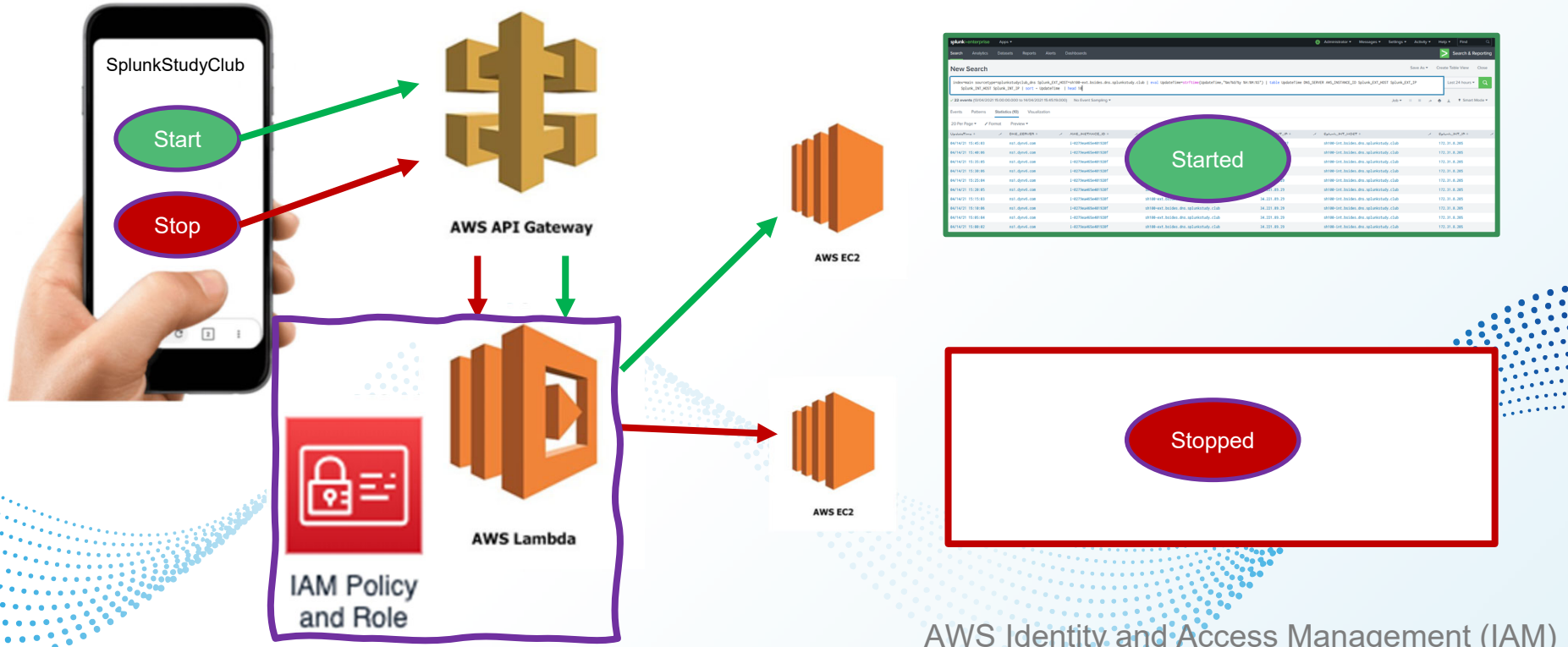
Lambda Functions - Serverless



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

BSIDES splunk>

Lambda Function - Permissions

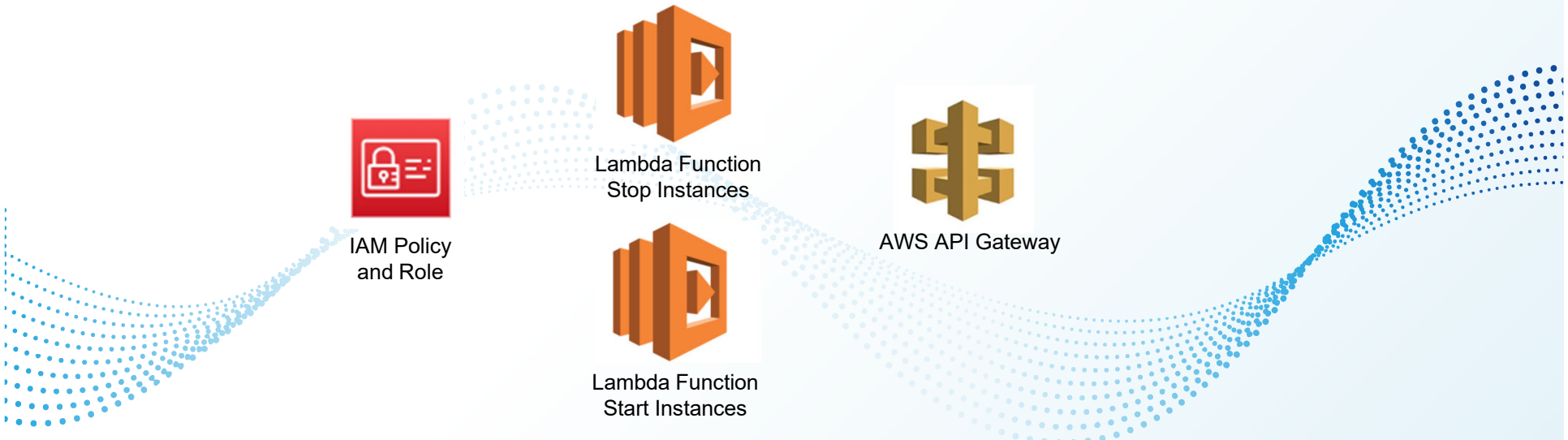


AWS Identity and Access Management (IAM)

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

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/

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

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Resource": "arn:aws:logs:*:*:*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:Start*",
        "ec2:Stop*"
      ],
      "Resource": "*"
    }
  ]
}
```

Security: 0 Errors: 0 Warnings: 0 Suggestions: 0

BSIDES splunk>

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

BSIDES 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.

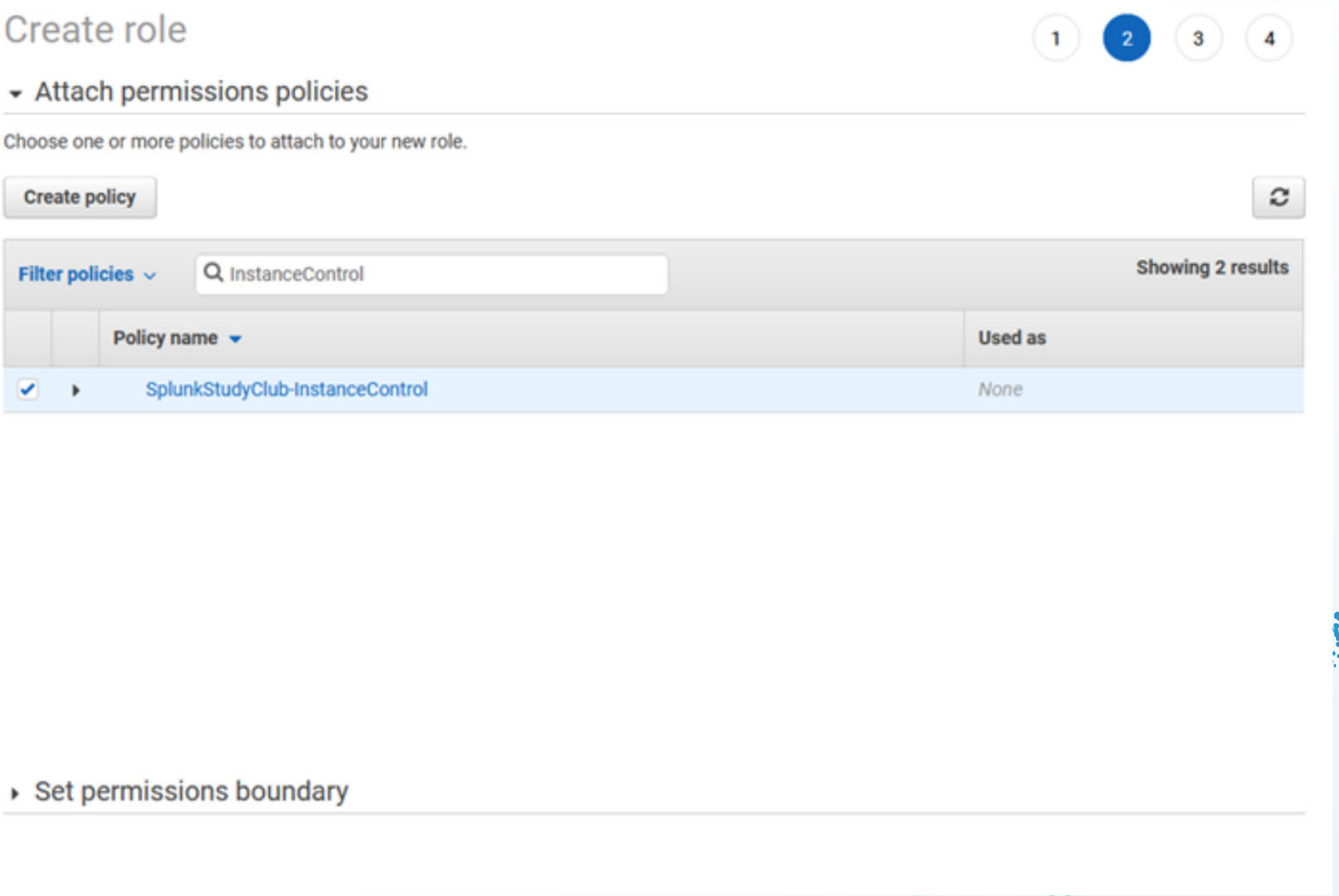
Lambda
Allows Lambda functions to call AWS services on your behalf.

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



BSIDES splunk>

IAM Policy and Role

Create role

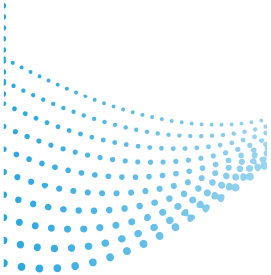
1 2 3 4

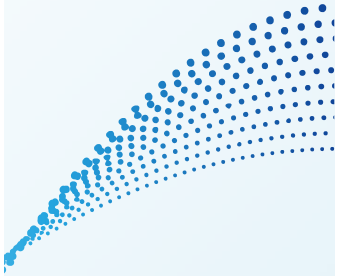
Add tags (optional)

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
Add new key		

You can add 50 more tags.





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>

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

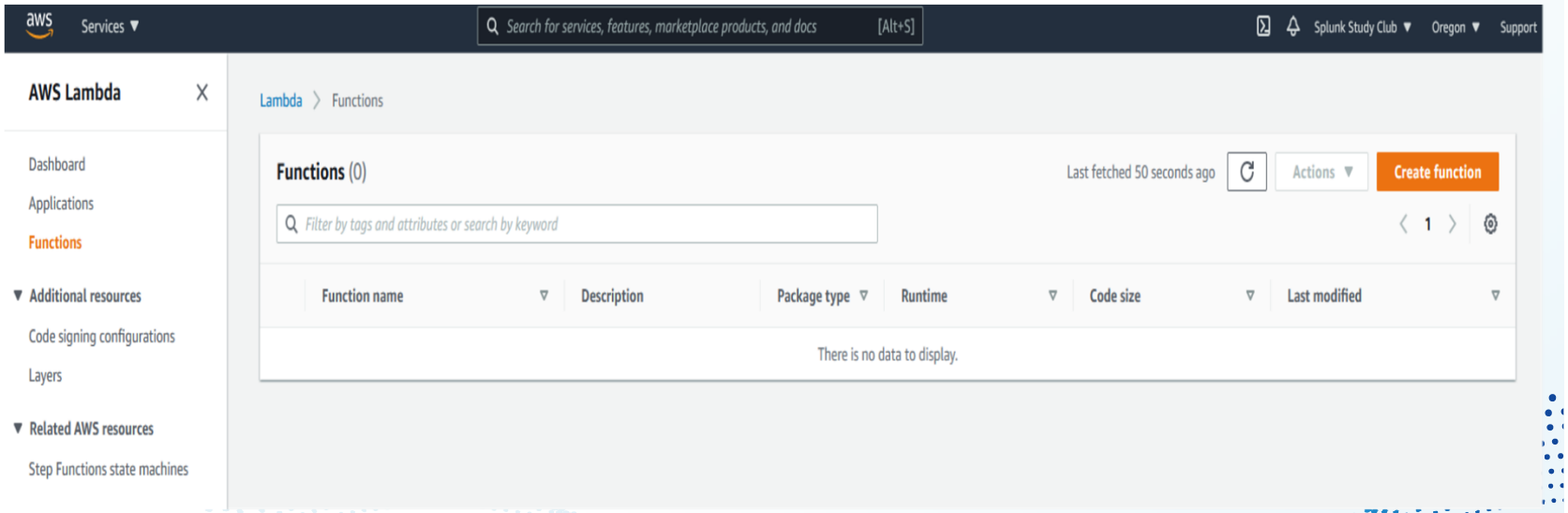
Policies SplunkStudyClub-InstanceControl

Permissions boundary Permissions boundary is not set

No tags were added.

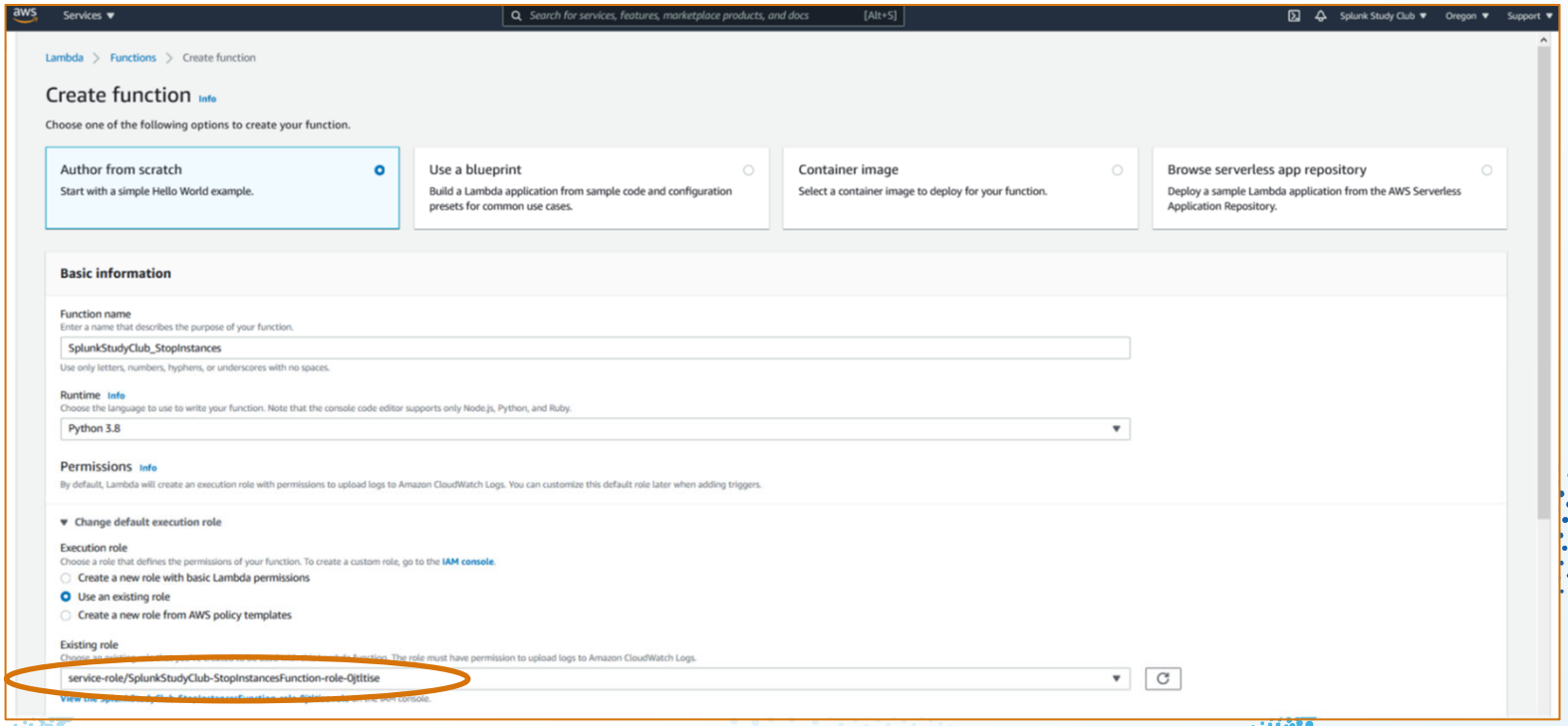
BSIDES splunk>

Lambda Function



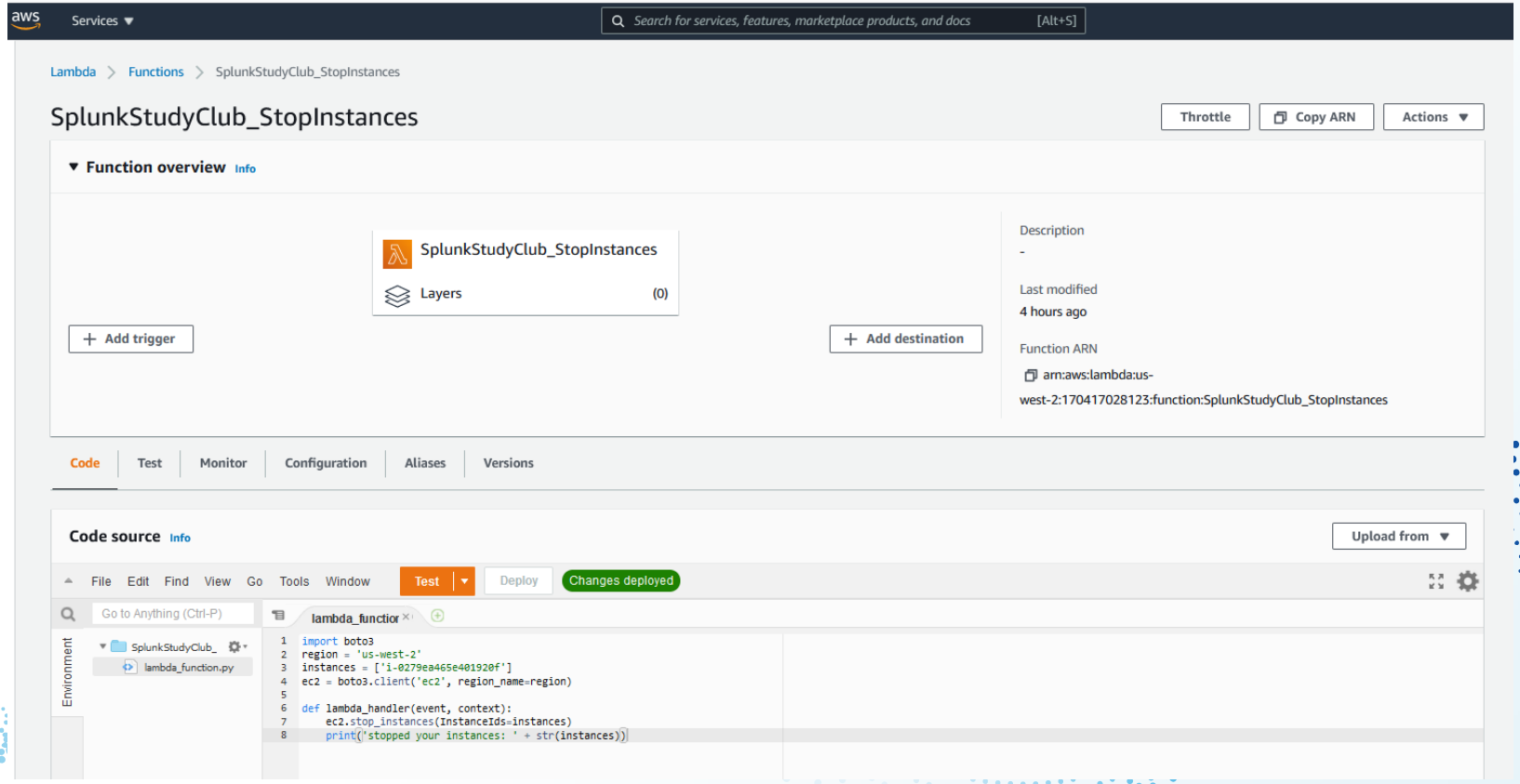
BSIDES splunk>

Lambda Function



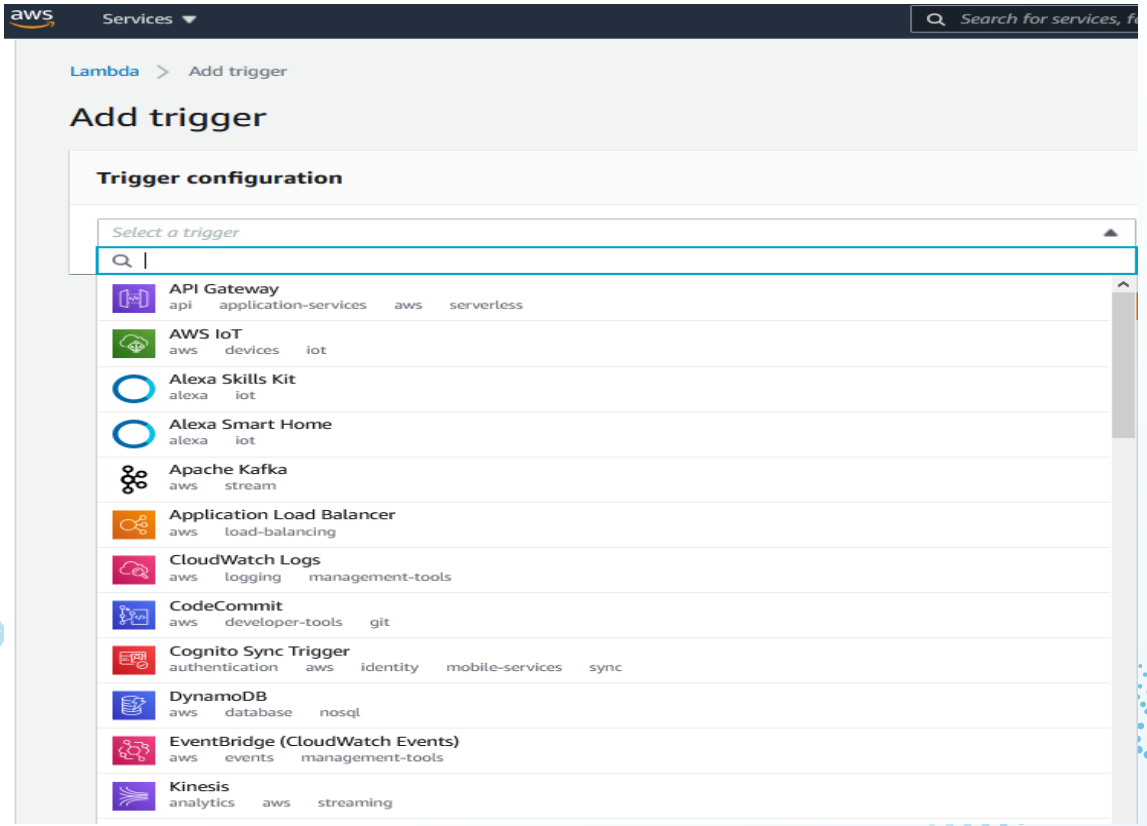
BSIDES splunk>

Lambda Function



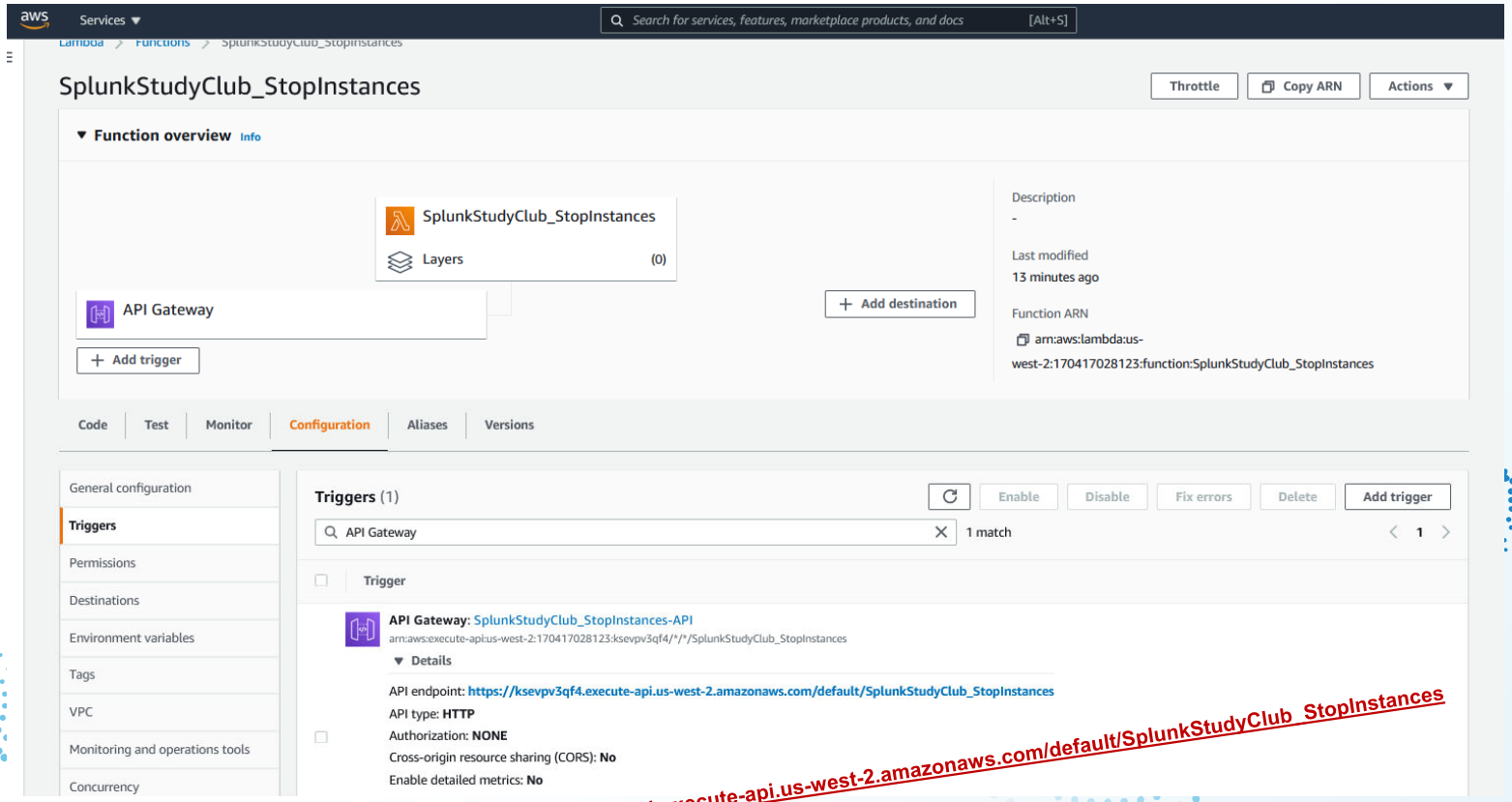
https://aws.amazon.com/premiumsupport/knowledge-center/start-stop-lambda-cloudwatch/

Lambda Function - Triggers



BSIDES splunk>

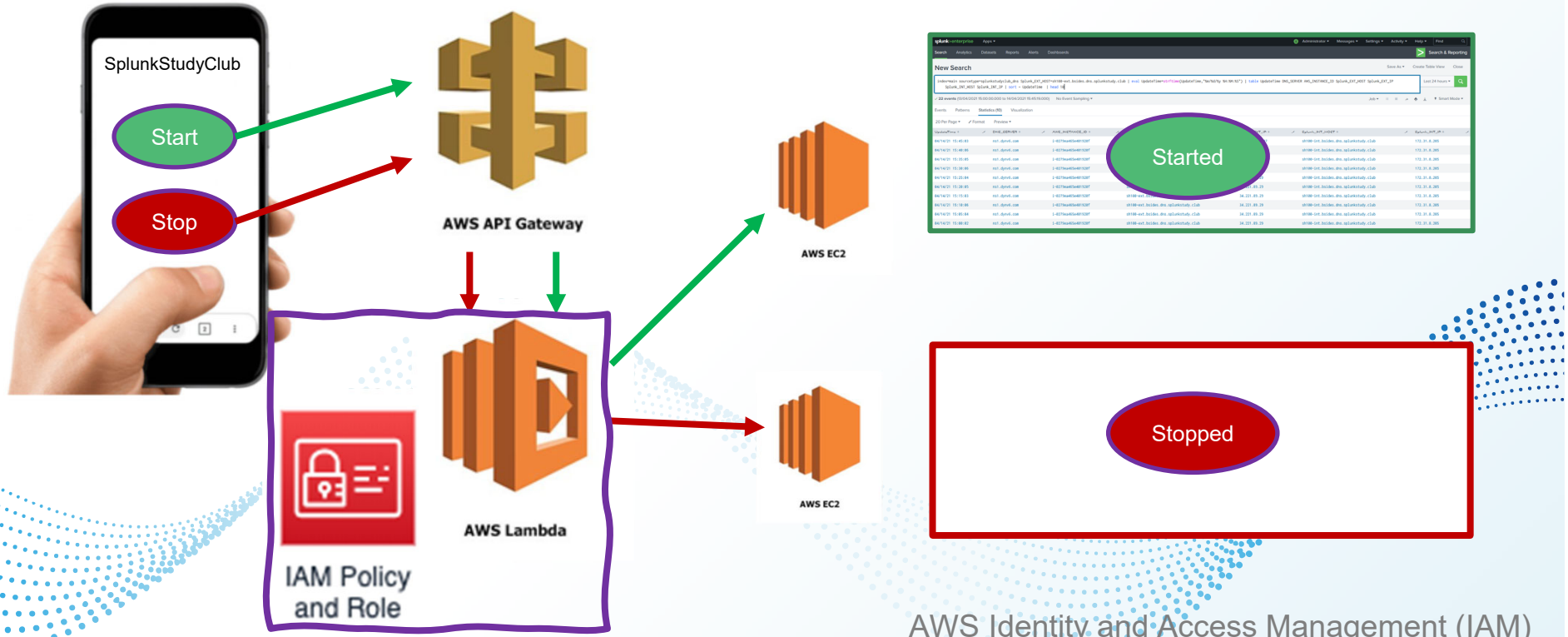
Lambda Function – API Gateway



https://ksevpv3qf4.execute-api.us-west-2.amazonaws.com/default/SplunkStudyClub_StopInstances

BSIDES splunk>

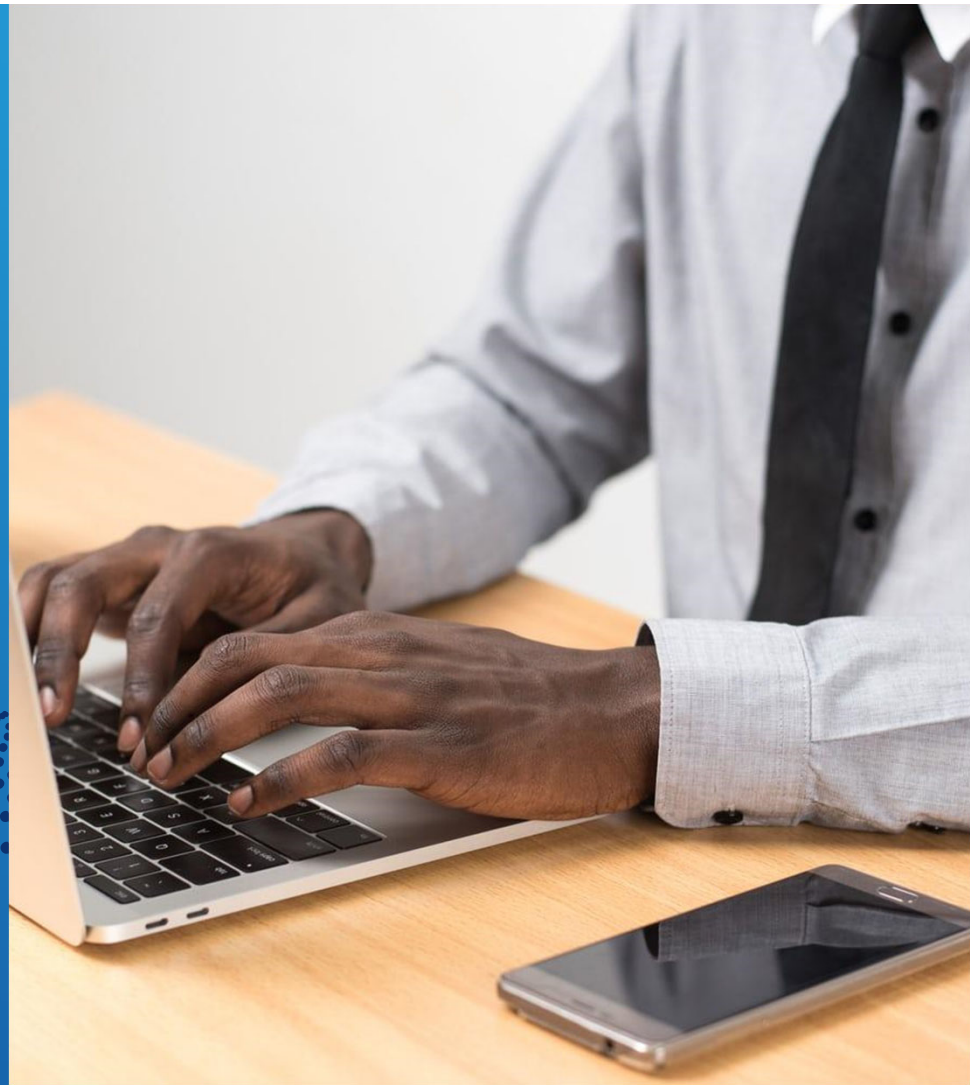
AWS Instance Management



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

Growth

Splunk Licensing

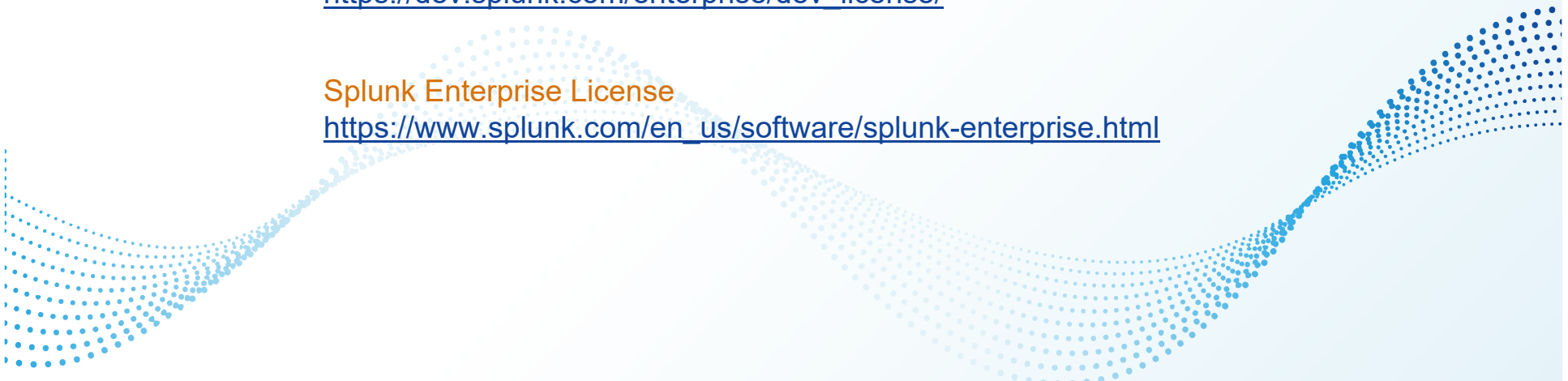


Splunk Licenses

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



BSIDES splunk>


Splunk Study Club
aws
Free Tier
Cloud Compute
BSIDES
splunk>

Thanks!

Any questions?

Aleem Cummins
Community Enablement Warrior
Independent

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

SplunkTrust
Splunk User Group London
Splunk Study Club

Suman Gajavelly
CTO / Co-founder
BitsIO Inc

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

Fort Worth Splunk User Group

Request your own DNS zone at http://ddns.splunkstudy.club

http://slack.splunkstudy.club

GitHub https://github.com/SplunkStudyClub

BSIDES splunk>