How AWS handles security

Aurelijus Banelis

VilniusPHP 0x52
2019-09-05

Aurelijus Banelis

Backend/DevOps

aurelijus.banelis.lt
aurelijus@banelis.lt

```
PGP    0x320205E7539B6203
130D C446 1F1A 2E50 D6E3
3DA8 3202 05E7 539B 6203
```

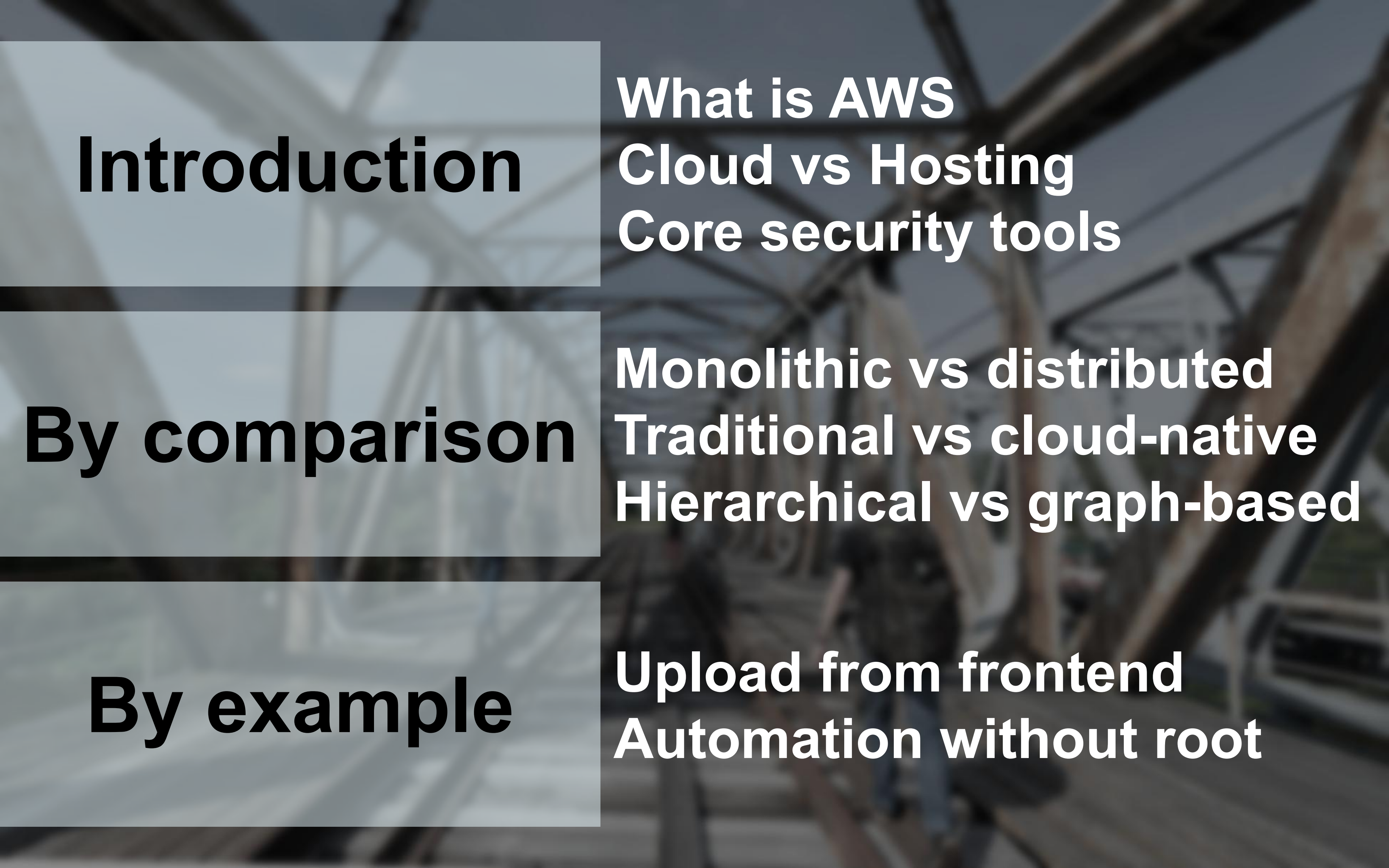
.NFQ

AKADEMIJA .NFQ

Auginte

home24

Security patterns in AWS



Introduction

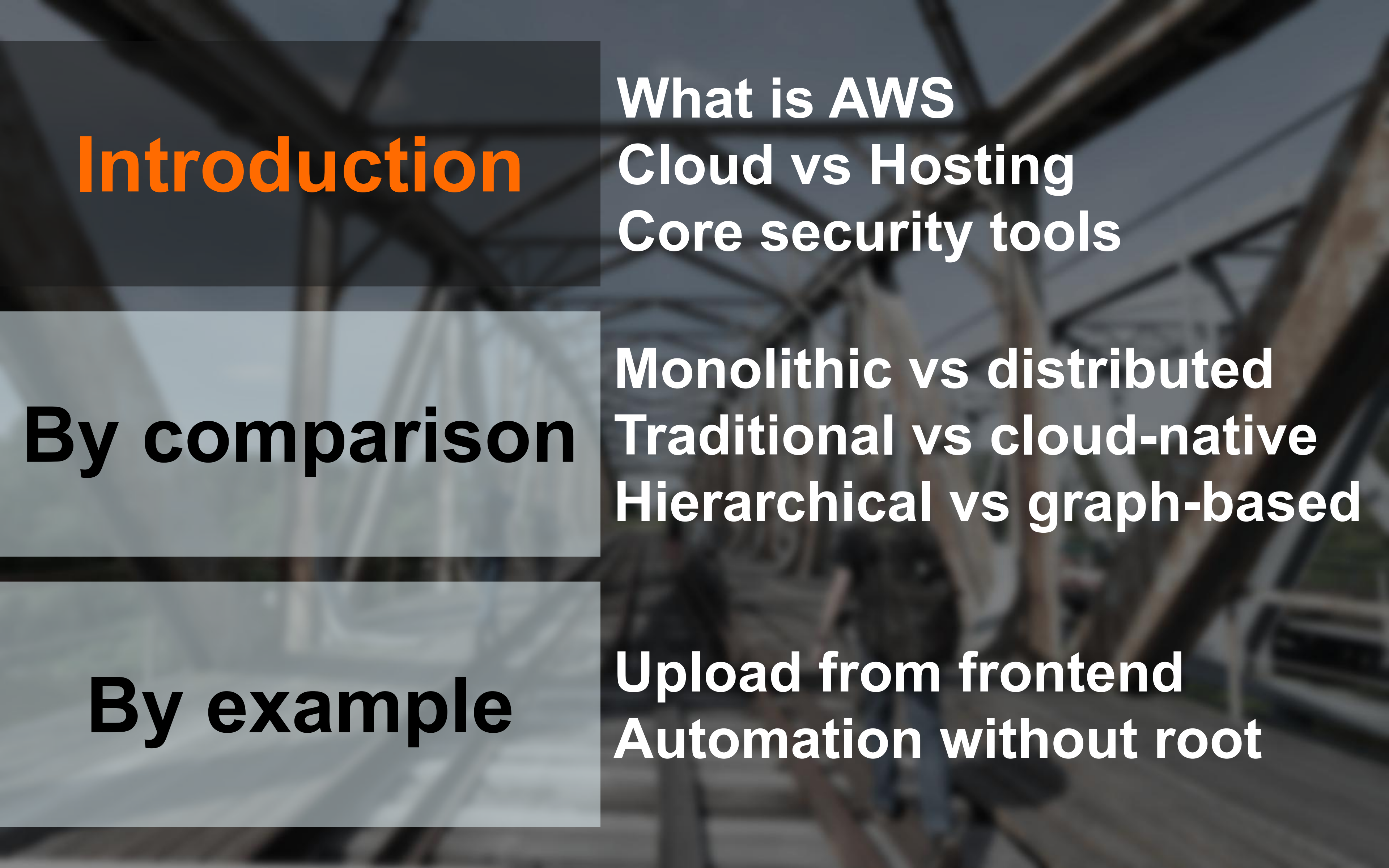
What is AWS
Cloud vs Hosting
Core security tools

By comparison

Monolithic vs distributed
Traditional vs cloud-native
Hierarchical vs graph-based

By example

Upload from frontend
Automation without root



Introduction

What is AWS
Cloud vs Hosting
Core security tools

By comparison

Monolithic vs distributed
Traditional vs cloud-native
Hierarchical vs graph-based

By example

Upload from frontend
Automation without root

AWS

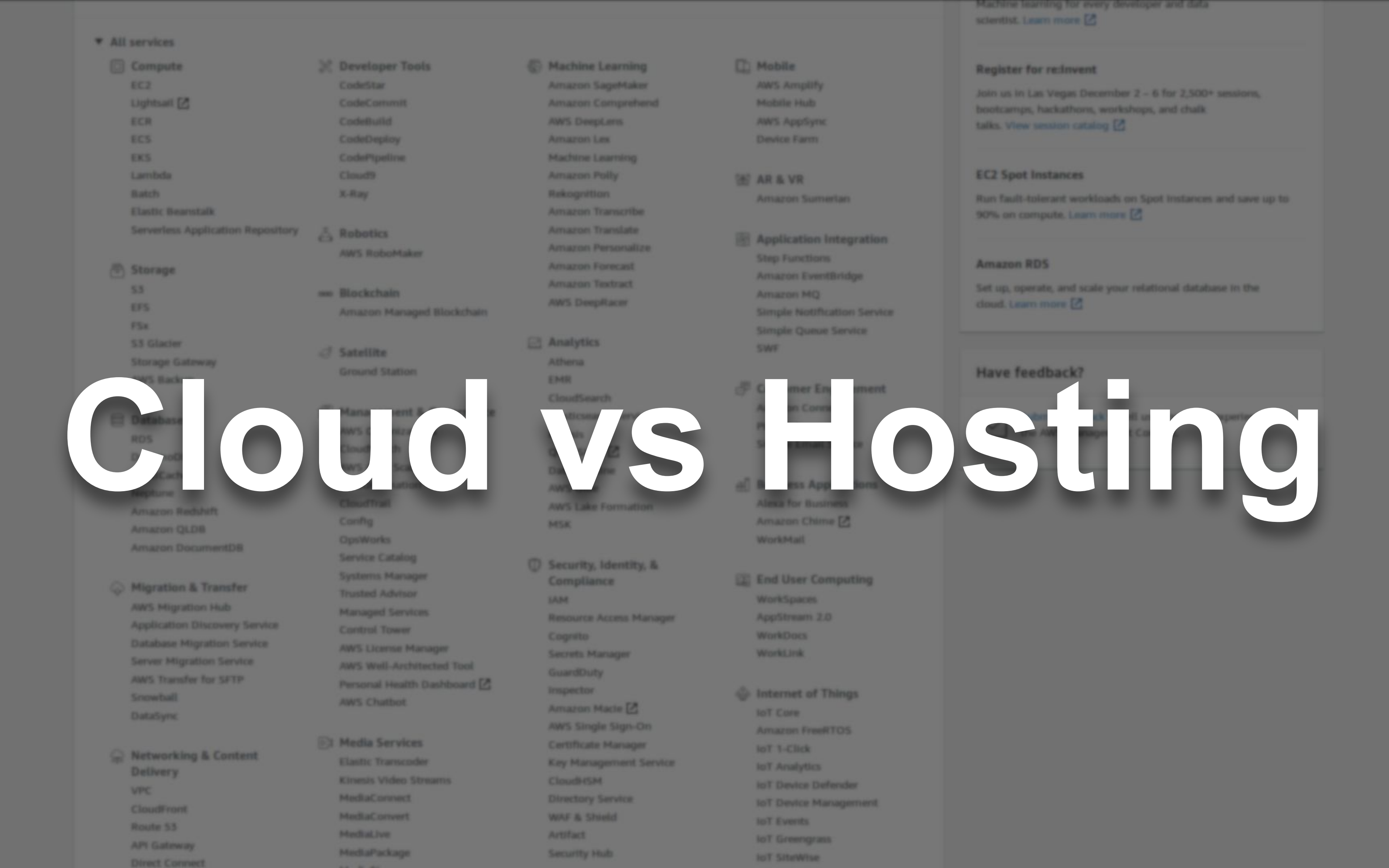
Monthly costs by service
Daily
Bar
Group by: API Operation
Service
Linked Account
Region
Instance Type
Usage Type
Tag
Availability Zone
Platform
Purchase Option
Tenancy
More
Costs ($)
CreateVolume-Gp2
RunInstances
Storage
StandardStorage
PublicIP-Out
Others
To see usage data, filter by "Usage Type" or "Usage Type Group" filters with matching units (e.g., hours).
Download CSV
Operation
Operation Total
Total cost ($)
CreateVolume-Gp2 ($)
RunInstances ($)

Infrastructure as a service

AWS

Pay on demand

Cloud vs Hosting



All services

Compute
EC2
Lightsail
ECR
ECS
EKS
Lambda
Batch
Elastic Beanstalk
Serverless Application Repository

Storage
S3
EFS
FSx
S3 Glacier
Storage Gateway
AWS Backup

Database
RDS
DynamoDB
ElastiCache
Neptune
Amazon Redshift
Amazon QLDB
Amazon DocumentDB

Migration & Transfer
AWS Migration Hub
Application Discovery Service
Database Migration Service
Server Migration Service
AWS Transfer for SFTP
Snowball
DataSync

Networking & Content Delivery
VPC
CloudFront
Route 53
API Gateway
Direct Connect

Developer Tools
CodeStar
CodeCommit
CodeBuild
CodeDeploy
CodePipeline
Cloud9
X-Ray

Robotics
AWS RoboMaker

Blockchain
Amazon Managed Blockchain

Satellite
Ground Station

Management & Governance
AWS Organizations
CloudWatch
AWS Auto Scaling
CloudFormation
CloudTrail
Config
OpsWorks
Service Catalog
Systems Manager
Trusted Advisor
Managed Services
Control Tower
AWS License Manager
AWS Well-Architected Tool
Personal Health Dashboard
AWS Chatbot

Media Services
Elastic Transcoder
Kinesis Video Streams
MediaConnect
MediaConvert
MediaLive
MediaPackage

Machine Learning
Amazon SageMaker
Amazon Comprehend
AWS DeepLens
Amazon Lex
Machine Learning
Amazon Polly
Rekognition
Amazon Transcribe
Amazon Translate
Amazon Personalize
Amazon Forecast
Amazon Textract
AWS DeepRacer

Analytics
Athena
EMR
CloudSearch
Elasticsearch Service
Kinesis
QuickSight
Data Pipeline
AWS Glue
AWS Lake Formation
MSK

Security, Identity, & Compliance
IAM
Resource Access Manager
Cognito
Secrets Manager
GuardDuty
Inspector
Amazon Macie
AWS Single Sign-On
Certificate Manager
Key Management Service
CloudHSM
Directory Service
WAF & Shield
Artifact
Security Hub

Mobile
AWS Amplify
Mobile Hub
AWS AppSync
Device Farm

AR & VR
Amazon Sumerian

Application Integration
Step Functions
Amazon EventBridge
Amazon MQ
Simple Notification Service
Simple Queue Service
SWF

Customer Engagement
Amazon Connect
Pinpoint
Simple Email Service

Business Applications
Alexa for Business
Amazon Chime
WorkMail

End User Computing
WorkSpaces
AppStream 2.0
WorkDocs
WorkLink

Internet of Things
IoT Core
Amazon FreeRTOS
IoT 1-Click
IoT Analytics
IoT Device Defender
IoT Device Management
IoT Events
IoT Greengrass
IoT SiteWise

Machine learning for every developer and data scientist. Learn more

Register for re:Invent
Join us in Las Vegas December 2 – 6 for 2,500+ sessions, bootcamps, hackathons, workshops, and chalk talks. View session catalog

EC2 Spot Instances
Run fault-tolerant workloads on Spot Instances and save up to 90% on compute. Learn more

Amazon RDS
Set up, operate, and scale your relational database in the cloud. Learn more

Have feedback?

Innovate with provider

Cloud vs Hosting

Thinking model

▼ All services

Compute
EC2
Lightsail
ECR
ECS
EKS
Lambda
Batch
Elastic Beanstalk
Serverless Application Repository

Storage
S3
EFS
FSx
S3 Glacier
Storage Gateway

RDS
Amazon Redshift
Amazon QLDB
Amazon DocumentDB

Migration & Transfer
AWS Migration Hub

Networking & Content Delivery
VPC
CloudFront
Route 53
API Gateway
Direct Connect

Developer Tools
CodeStar
CodeCommit
CodeBuild

Robotics
AWS RoboMaker

Blockchain
Amazon Managed Blockchain

Satellite
Ground Station

CloudTrail
Config
OpsWorks
Service Catalog
Systems Manager
Trusted Advisor
Managed Services

Media Services
Elastic Transcoder
Kinesis Video Streams
MediaConnect
MediaConvert
MediaLive
MediaPackage

Machine Learning
Amazon SageMaker
Amazon Comprehend
AWS DeepLens
Amazon Transcribe
Amazon Translate
Amazon Personalize
Amazon Forecast
Amazon Textract
AWS DeepRacer

Analytics
Athena
EMR
CloudSearch
AWS Lake Formation
MSK

Security, Identity, & Compliance
IAM
Resource Access Manager
Certificate Manager
Key Management Service
CloudHSM
Directory Service
WAF & Shield
Artifact
Security Hub

Mobile
AWS Amplify
Mobile Hub
AWS AppSync
Device Farm

Application Integration
Step Functions
Amazon EventBridge
Amazon MQ
Simple Notification Service
Simple Queue Service
SWF

Alexa for Business
Amazon Chime
WorkMail

End User Computing
WorkSpaces
AppStream 2.0
WorkDocs
WorkLink

IoT Core
IoT 1-Click
IoT Analytics
IoT Device Defender
IoT Device Management
IoT Events
IoT Greengrass
IoT SiteWise

Machine learning for every developer and data scientist. Learn more

Register for re:Invent

Join us in Las Vegas December 2 – 6 for 2,500+ sessions, bootcamps, hackathons, workshops, and chalk talks.

Run fault-tolerant workloads on Spot Instances and save up to 90% on compute. Learn more

Amazon RDS

Set up, operate, and scale your relational database in the cloud. Learn more

Have feedback?

Security tools

Complex system

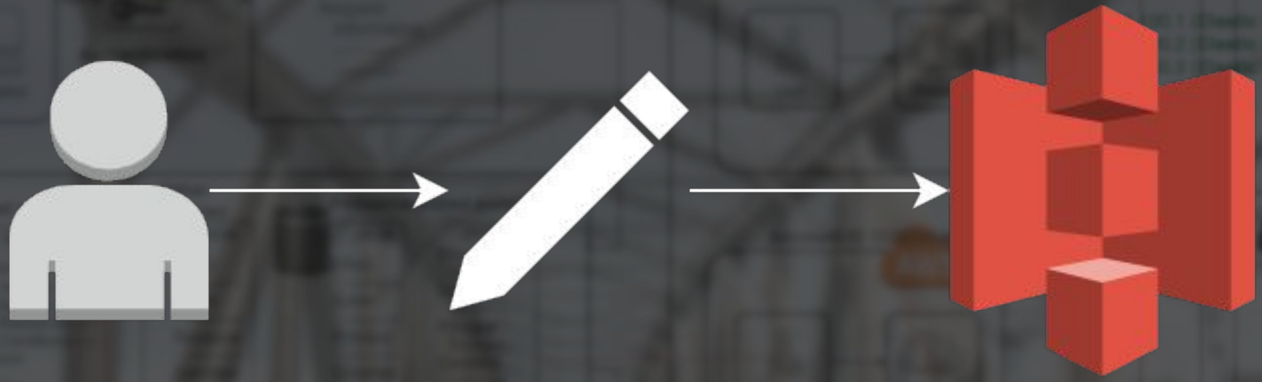
Security tools

Network, storage, auditing, reaction, application level

Complex system

Security tools

Network, storage, auditing, reaction,
application level



Principal

Who

Identified by HTTPS signing

Action

What

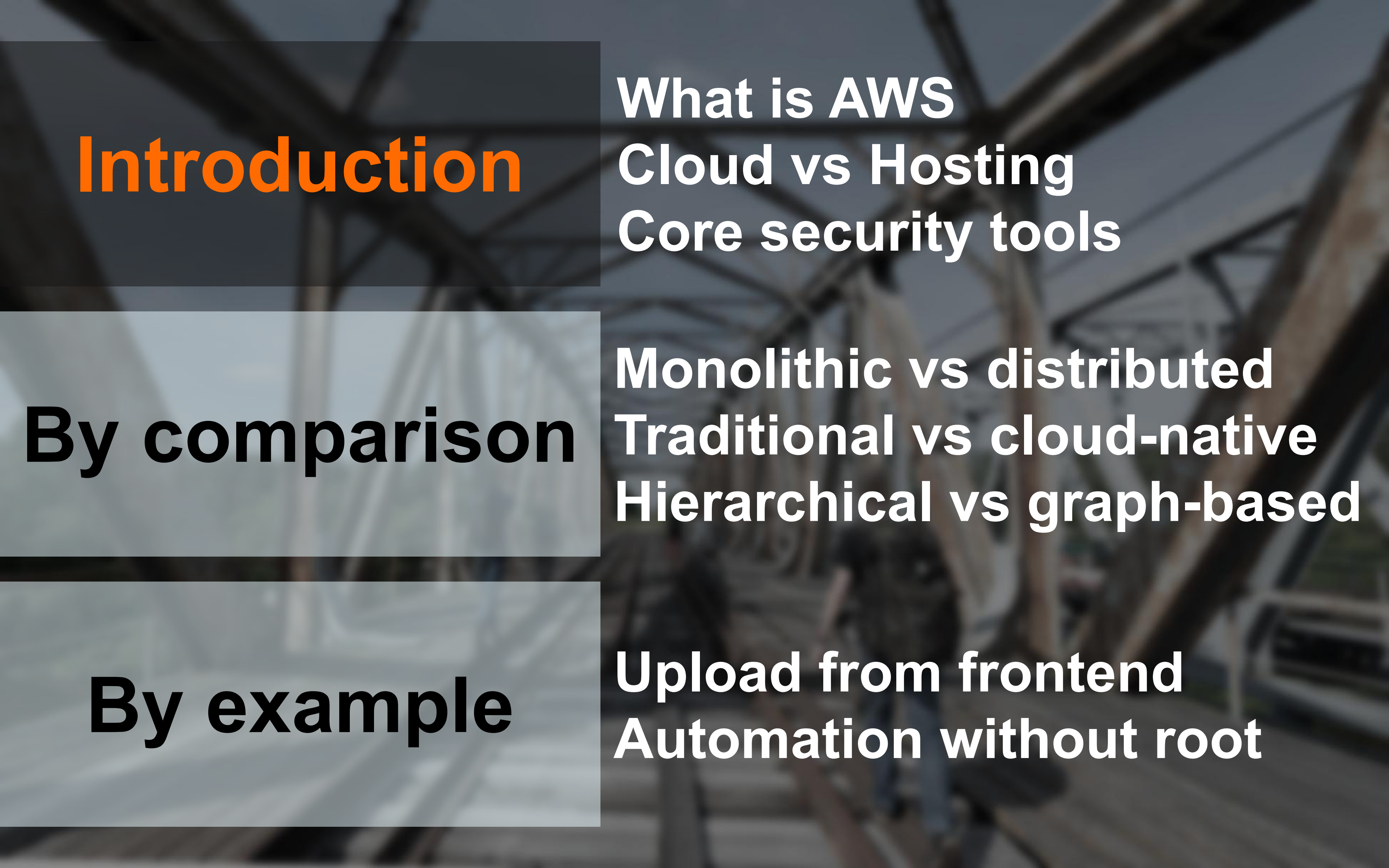
Differs by AWS service

Resource

Where

Uniquely identified by ARN (URL-like name)

Simplified IAM Policy



Introduction

What is AWS
Cloud vs Hosting
Core security tools

By comparison

Monolithic vs distributed
Traditional vs cloud-native
Hierarchical vs graph-based

By example

Upload from frontend
Automation without root

Introduction

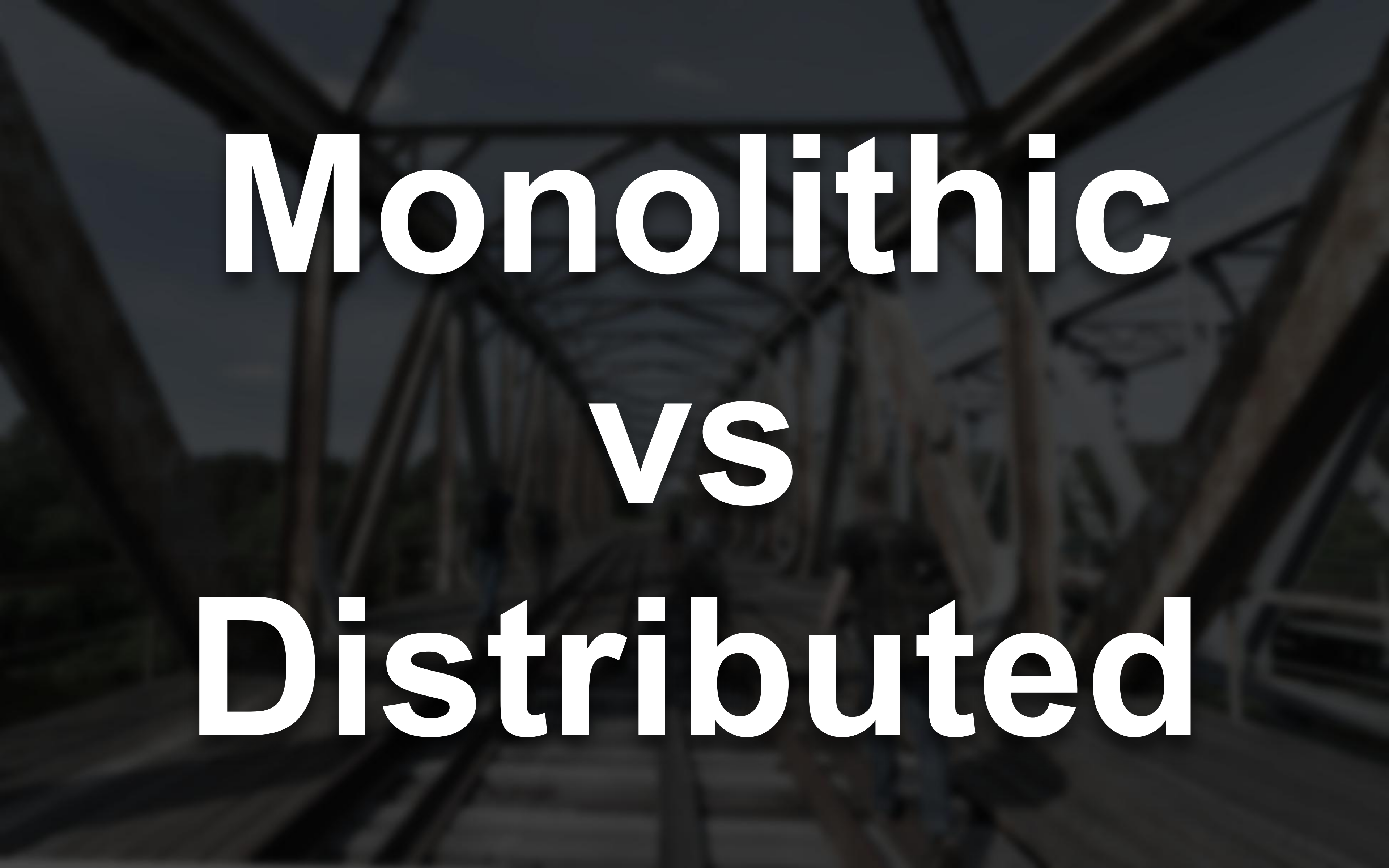
- What is AWS
- Cloud vs Hosting
- Core security tools

By comparison

- Monolithic vs distributed
- Traditional vs cloud-native
- Hierarchical vs graph-based

By example

- Upload from frontend
- Automation without root



Monolithic vs Distributed

Monolithic

Security Firewall

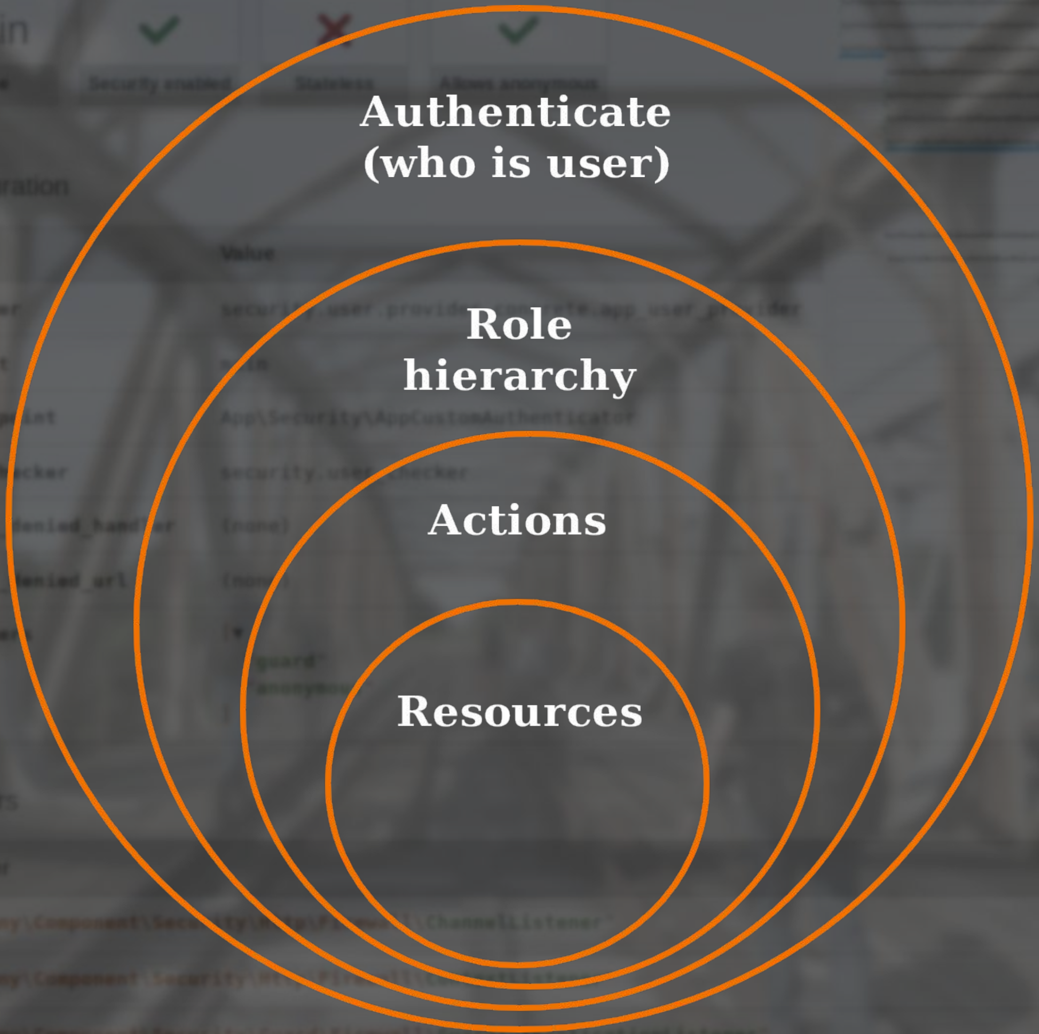
main	✓	✗	✓
Name	Security enabled	Stateless	Allows anonymous

Configuration

Key	Value
provider	security.user.provider.concrete.app_user_provider
context	main
entry_point	App\Security\AppCustomAuthenticator
user_checker	security_user_checker
access_denied_handler	(none)
access_denied_url	(none)
listeners	[▼ "guard" "anonymous"]

Listeners

Listener	Duration	Response
"Symfony\Component\Security\Http\Firewall\ChannelListener"	0.02 ms	(none)
"Symfony\Component\Security\Http\Firewall\ContextListener"	3.45 ms	(none)
"Symfony\Component\Security\Guard\Firewall\GuardAuthenticationListener"	0.04 ms	(none)
"Symfony\Component\Security\Http\Firewall\AnonymousAuthenticationListener"	0.00 ms	(none)



Authenticate (who is user)

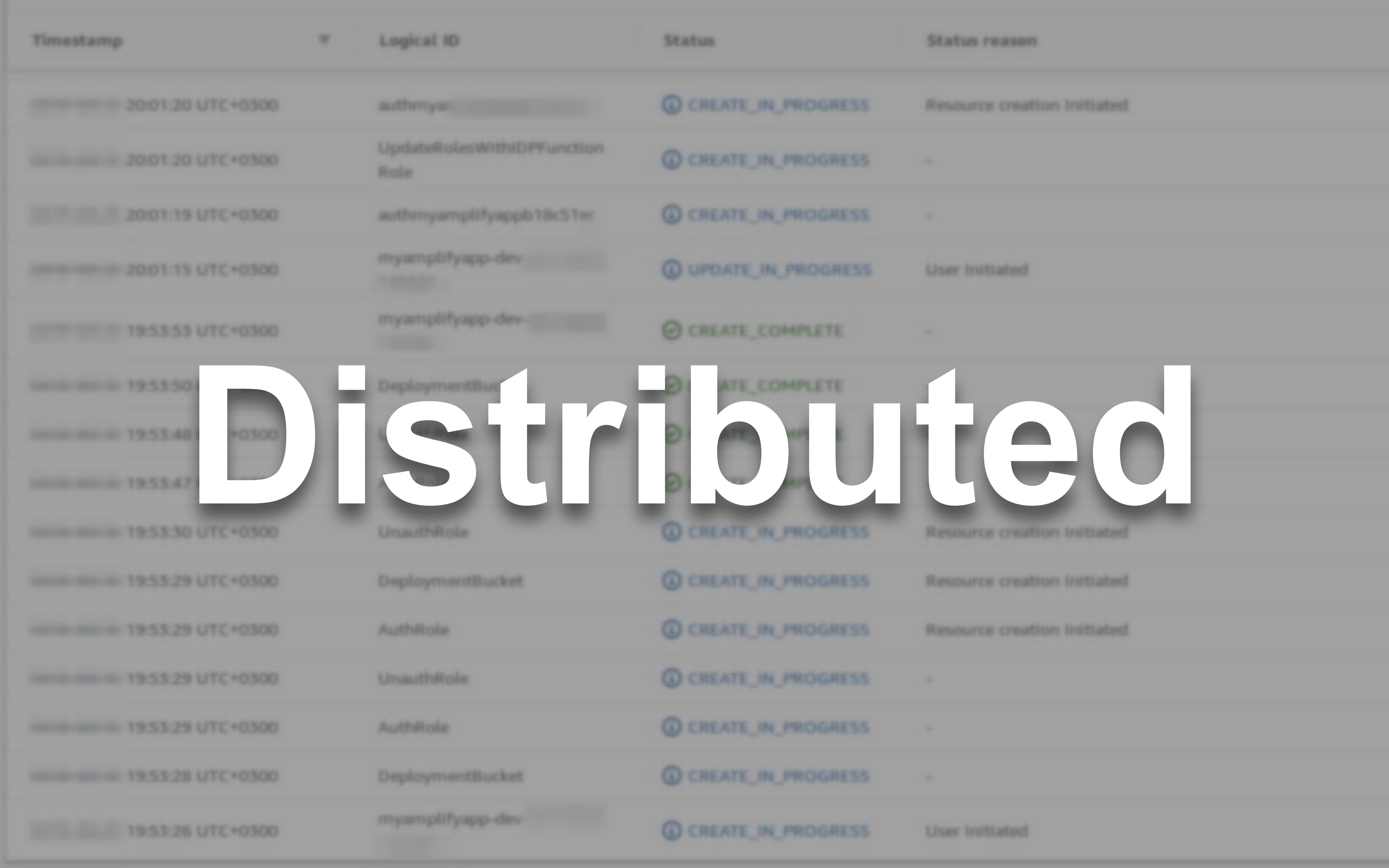
Role hierarchy

Actions

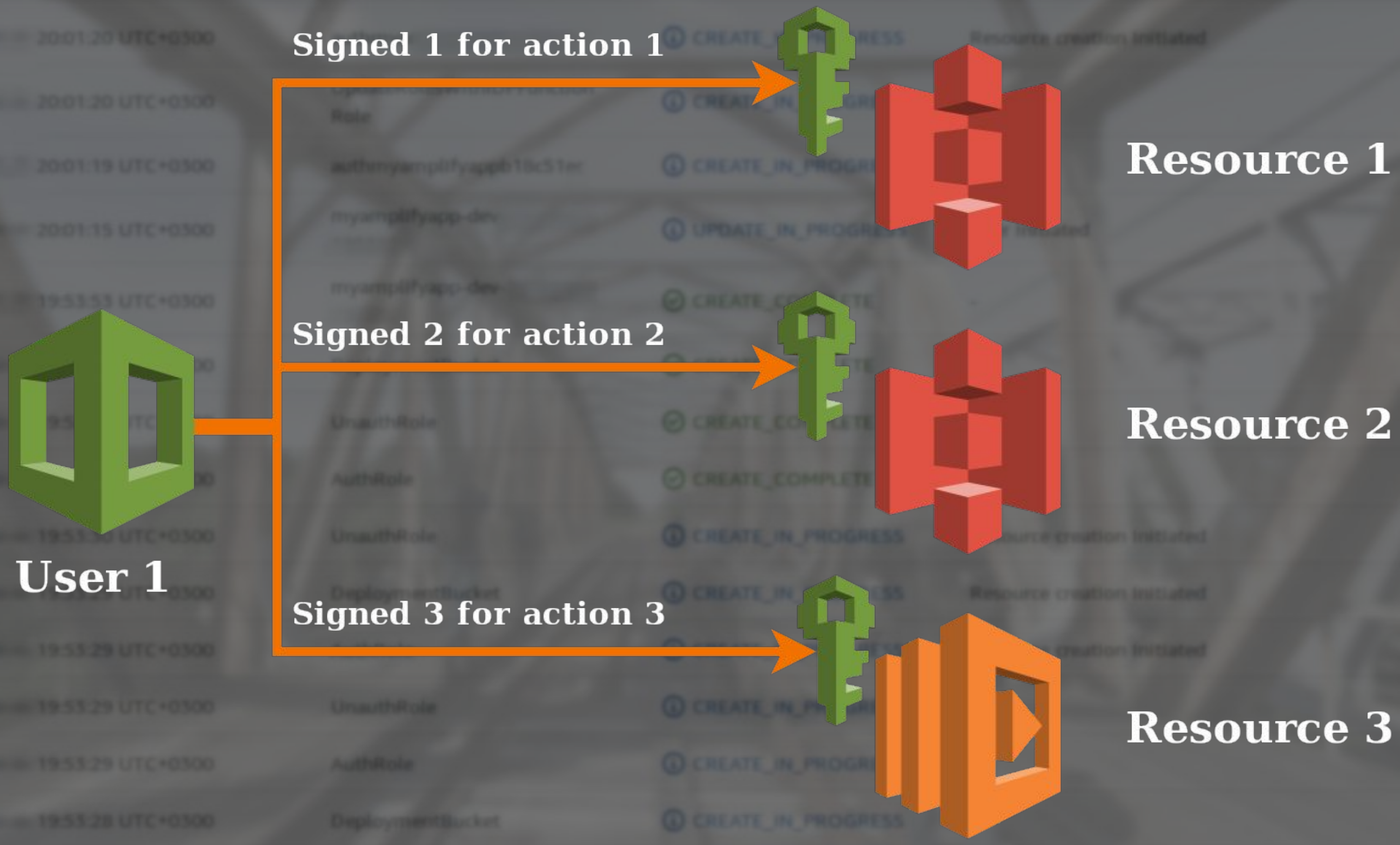
Resources

Onion-like architecture

Distributed



Timestamp	Logical ID	Status	Status reason
[redacted] 20:01:20 UTC+0300	authmya[redacted]	CREATE_IN_PROGRESS	Resource creation Initiated
[redacted] 20:01:20 UTC+0300	UpdateRolesWithIDPFunctionRole	CREATE_IN_PROGRESS	-
[redacted] 20:01:19 UTC+0300	authmyamplifyappb18c51ec	CREATE_IN_PROGRESS	-
[redacted] 20:01:15 UTC+0300	myamplifyapp-dev[redacted]	UPDATE_IN_PROGRESS	User Initiated
[redacted] 19:53:53 UTC+0300	myamplifyapp-dev-[redacted]	CREATE_COMPLETE	-
[redacted] 19:53:50	DeploymentBuc	ATE_COMPLETE	
[redacted] 19:53:48 +0300	U		
[redacted] 19:53:47	A		
[redacted] 19:53:30 UTC+0300	UnauthRole	CREATE_IN_PROGRESS	Resource creation Initiated
[redacted] 19:53:29 UTC+0300	DeploymentBucket	CREATE_IN_PROGRESS	Resource creation Initiated
[redacted] 19:53:29 UTC+0300	AuthRole	CREATE_IN_PROGRESS	Resource creation Initiated
[redacted] 19:53:29 UTC+0300	UnauthRole	CREATE_IN_PROGRESS	-
[redacted] 19:53:29 UTC+0300	AuthRole	CREATE_IN_PROGRESS	-
[redacted] 19:53:28 UTC+0300	DeploymentBucket	CREATE_IN_PROGRESS	-
[redacted] 19:53:26 UTC+0300	myamplifyapp-dev[redacted]	CREATE_IN_PROGRESS	User Initiated



Signed 1 for action 1

Signed 2 for action 2

Signed 3 for action 3

User 1

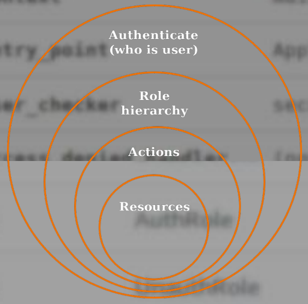
Resource 1

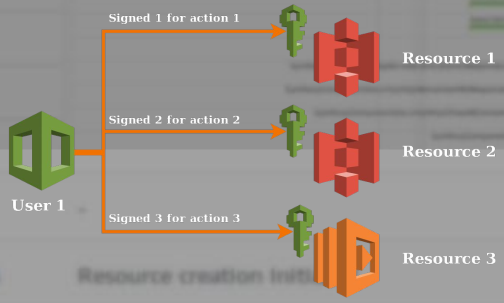
Resource 2

Resource 3

Sidecar-like architecture

Monolithic vs Distributed





Traditional vs Cloud-native

Traditional

https://gdpr-info.eu/issues/encryption/

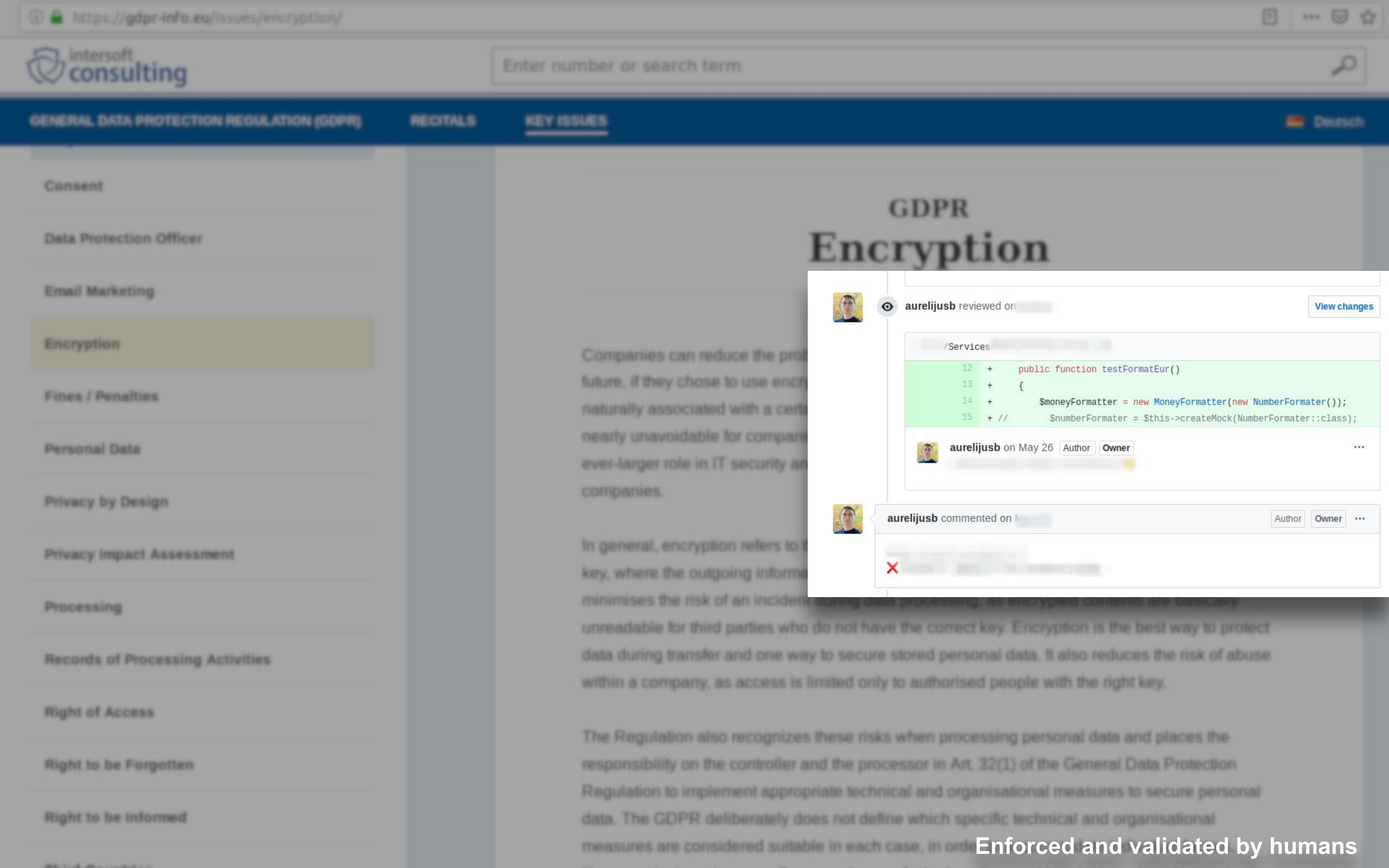
GDPR

Encryption

Companies can reduce the probability of a data breach and thus reduce the risk of fines in the [illegible]ure, [illegible]ey c[illegible]e to [illegible] encryption of personal data. The processing of pers[illegible] data is [illegible]ura[illegible] ass[illegible] w[illegible] certa[illegible] of ris[illegible] [illegible]ly now[illegible] [illegible]here [illegible]er-attacks are [illegible]arly [illegible]voi[illegible]e for [illegible]pa[illegible] abov[illegible] give[illegible]ze. [illegible]efore, risk m[illegible]age[illegible] plays an [illegible]er-la[illegible]r ro[illegible] IT se[illegible]ty [illegible] data e[illegible]ptio[illegible]s suit[illegible] am[illegible] [illegible] [illegible]r these [illegible]mpa[illegible]s.

In general, encryption refers to the procedure that converts clear text into a hashed code using a key, where the outgoing information only becomes readable again by using the correct key. This minimises the risk of an incident during data processing, as encrypted contents are basically unreadable for third parties who do not have the correct key. Encryption is the best way to protect data during transfer and one way to secure stored personal data. It also reduces the risk of abuse within a company, as access is limited only to authorised people with the right key.

The Regulation also recognizes these risks when processing personal data and places the responsibility on the controller and the processor in Art. 32(1) of the General Data Protection Regulation to implement appropriate technical and organisational measures to secure personal data. The GDPR deliberately does not define which specific technical and organisational measures are considered suitable in each case, in order to accommodate individual factors.



GDPR

Encryption

Companies can reduce the pro
future, if they chose to use encry
naturally associated with a certa
nearly unavoidable for compani
ever-larger role in IT security a
companies.

In general, encryption refers to t
key, where the outgoing informa
minimises the risk of an incident during data processing, as encrypted contents are basically unreadable for third parties who do not have the correct key. Encryption is the best way to protect data during transfer and one way to secure stored personal data. It also reduces the risk of abuse within a company, as access is limited only to authorised people with the right key.

The Regulation also recognizes these risks when processing personal data and places the responsibility on the controller and the processor in Art. 32(1) of the General Data Protection Regulation to implement appropriate technical and organisational measures to secure personal data. The GDPR deliberately does not define which specific technical and organisational measures are considered suitable in each case, in orde

aurelijusb reviewed on

/Services

```
+     public function testFormatEur()
+     {
+         $moneyFormatter = new MoneyFormatter(new NumberFormater());
+ //        $numberFormater = $this->createMock(NumberFormater::class);
```

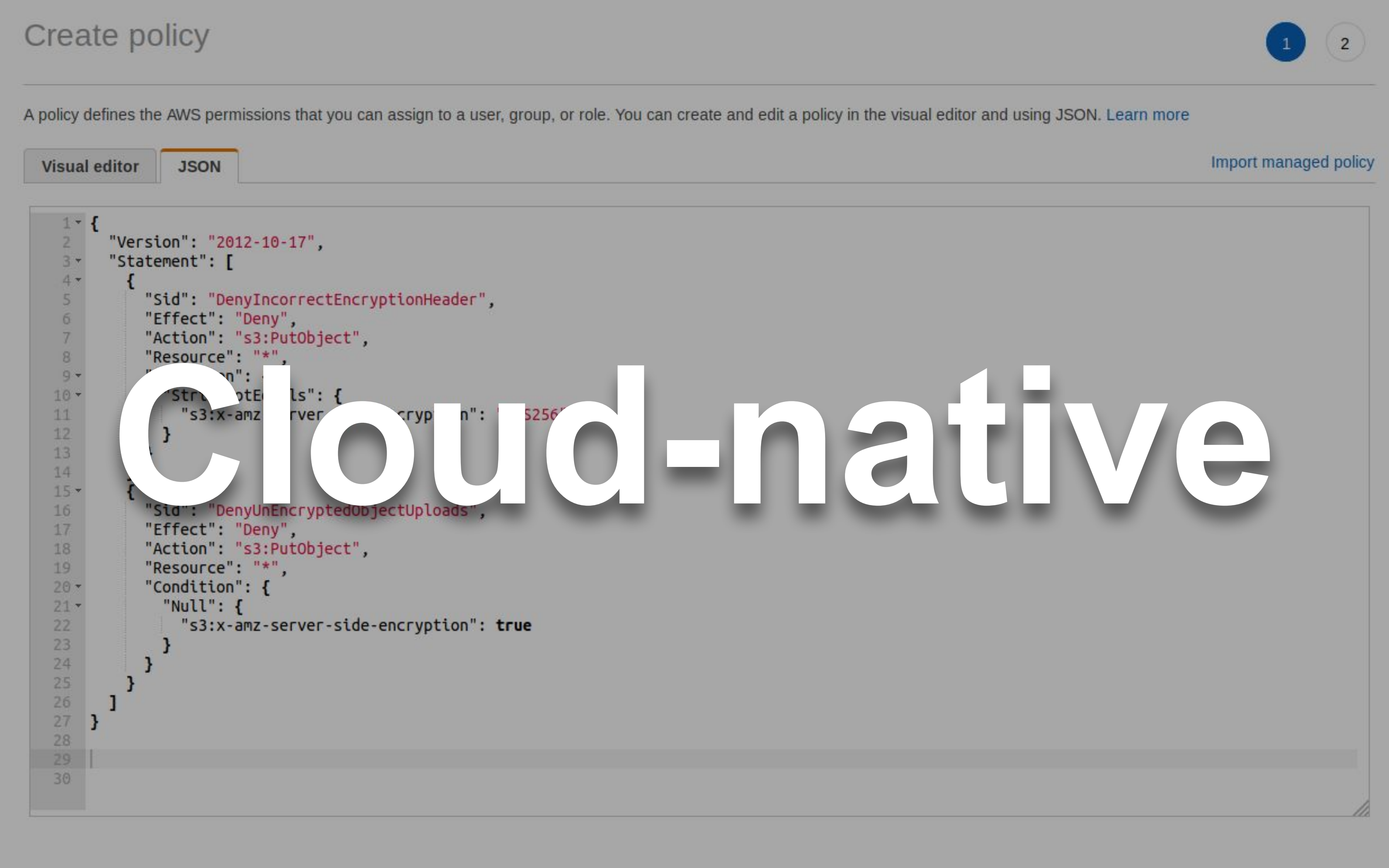
aurelijusb on May 26 Author Owner

aurelijusb commented on Author Owner

❌

Enforced and validated by humans

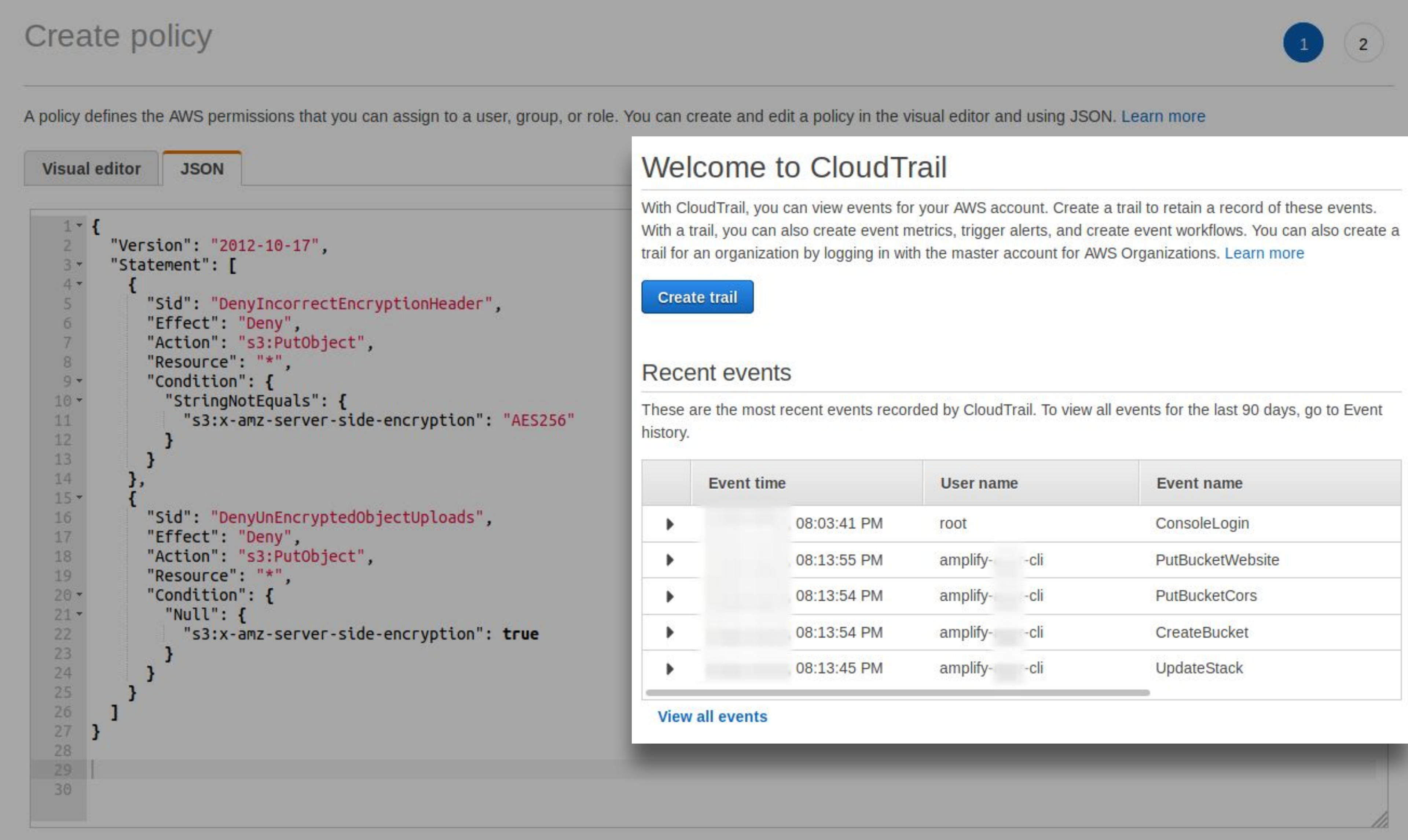
Cloud-native



Create policy

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

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyIncorrectEncryptionHeader",
      "Effect": "Deny",
      "Action": "s3:PutObject",
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "s3:x-amz-server-side-encryption": "AES256"
        }
      }
    },
    {
      "Sid": "DenyUnEncryptedObjectUploads",
      "Effect": "Deny",
      "Action": "s3:PutObject",
      "Resource": "*",
      "Condition": {
        "Null": {
          "s3:x-amz-server-side-encryption": true
        }
      }
    }
  ]
}
```



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

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyIncorrectEncryptionHeader",
      "Effect": "Deny",
      "Action": "s3:PutObject",
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "s3:x-amz-server-side-encryption": "AES256"
        }
      }
    },
    {
      "Sid": "DenyUnEncryptedObjectUploads",
      "Effect": "Deny",
      "Action": "s3:PutObject",
      "Resource": "*",
      "Condition": {
        "Null": {
          "s3:x-amz-server-side-encryption": true
        }
      }
    }
  ]
}
```

Welcome to CloudTrail

With CloudTrail, you can view events for your AWS account. Create a trail to retain a record of these events. With a trail, you can also create event metrics, trigger alerts, and create event workflows. You can also create a trail for an organization by logging in with the master account for AWS Organizations. Learn more

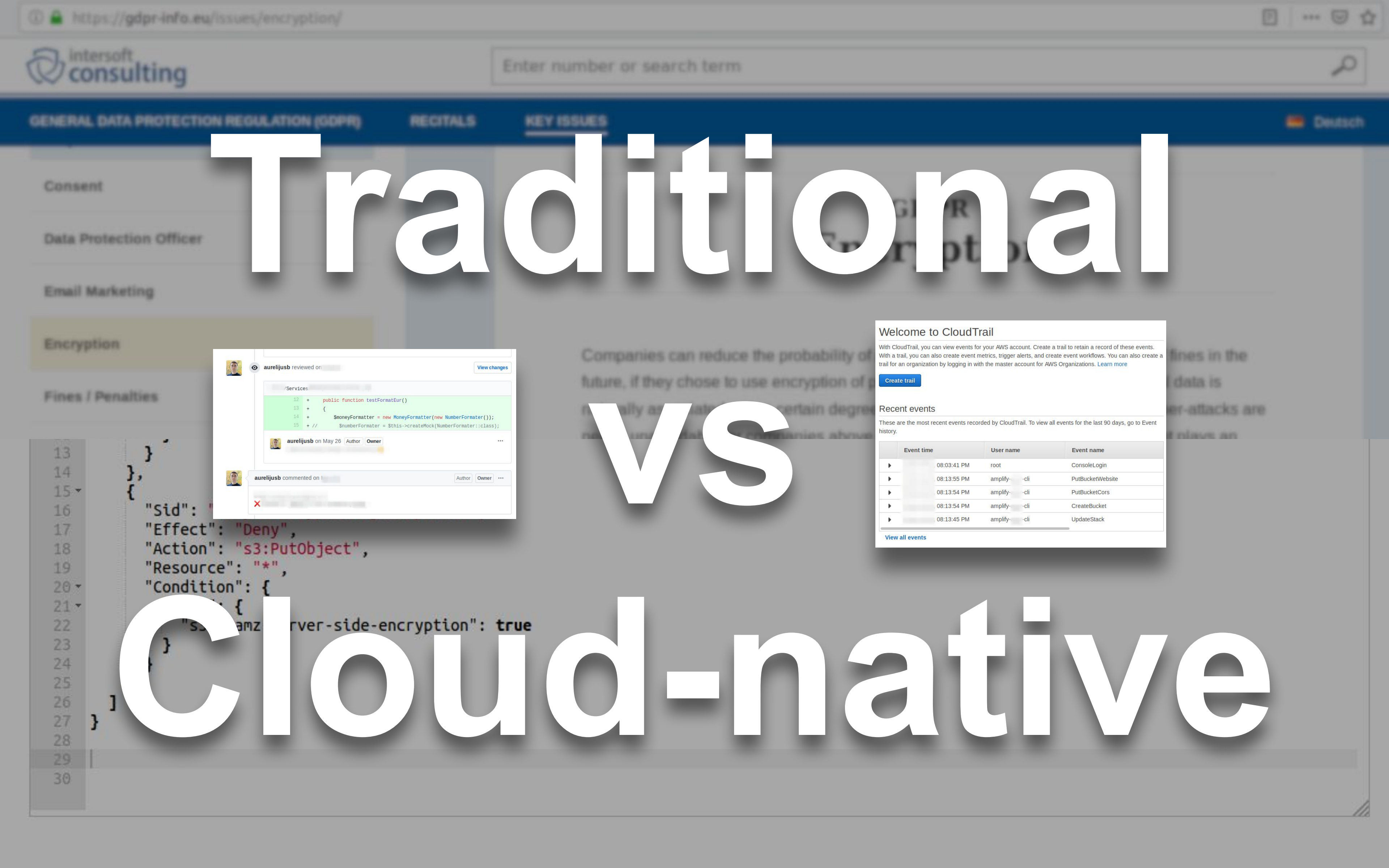
Recent events

These are the most recent events recorded by CloudTrail. To view all events for the last 90 days, go to Event history.

	Event time	User name	Event name
▶	[redacted] 08:03:41 PM	root	ConsoleLogin
▶	[redacted] 08:13:55 PM	amplify-[redacted]-cli	PutBucketWebsite
▶	[redacted] 08:13:54 PM	amplify-[redacted]-cli	PutBucketCors
▶	[redacted] 08:13:54 PM	amplify-[redacted]-cli	CreateBucket
▶	[redacted] 08:13:45 PM	amplify-[redacted]-cli	UpdateStack

Enforced and validated by computers

Traditional vs Cloud-native



Companies can reduce the probability of … fines in the future, if they chose to use encryption of p… data is … certain degree … -attacks are …

```
        }
    },
    {
        "Sid": "
        "Effect": "Deny",
        "Action": "s3:PutObject",
        "Resource": "*",
        "Condition": {
                : {
            "s3 amz rver-side-encryption": true
            }
        }
    ]
}
```

aurelijusb reviewed on [redacted] View changes

/Services[redacted]

```
12 +     public function testFormatEur()
13 +     {
14 +         $moneyFormatter = new MoneyFormatter(new NumberFormater());
15 + //         $numberFormater = $this->createMock(NumberFormater::class);
```

aurelijusb on May 26 Author Owner ···

[redacted]

aurelijusb commented on [redacted] Author Owner ···

[redacted]

Welcome to CloudTrail

With CloudTrail, you can view events for your AWS account. Create a trail to retain a record of these events. With a trail, you can also create event metrics, trigger alerts, and create event workflows. You can also create a trail for an organization by logging in with the master account for AWS Organizations. Learn more

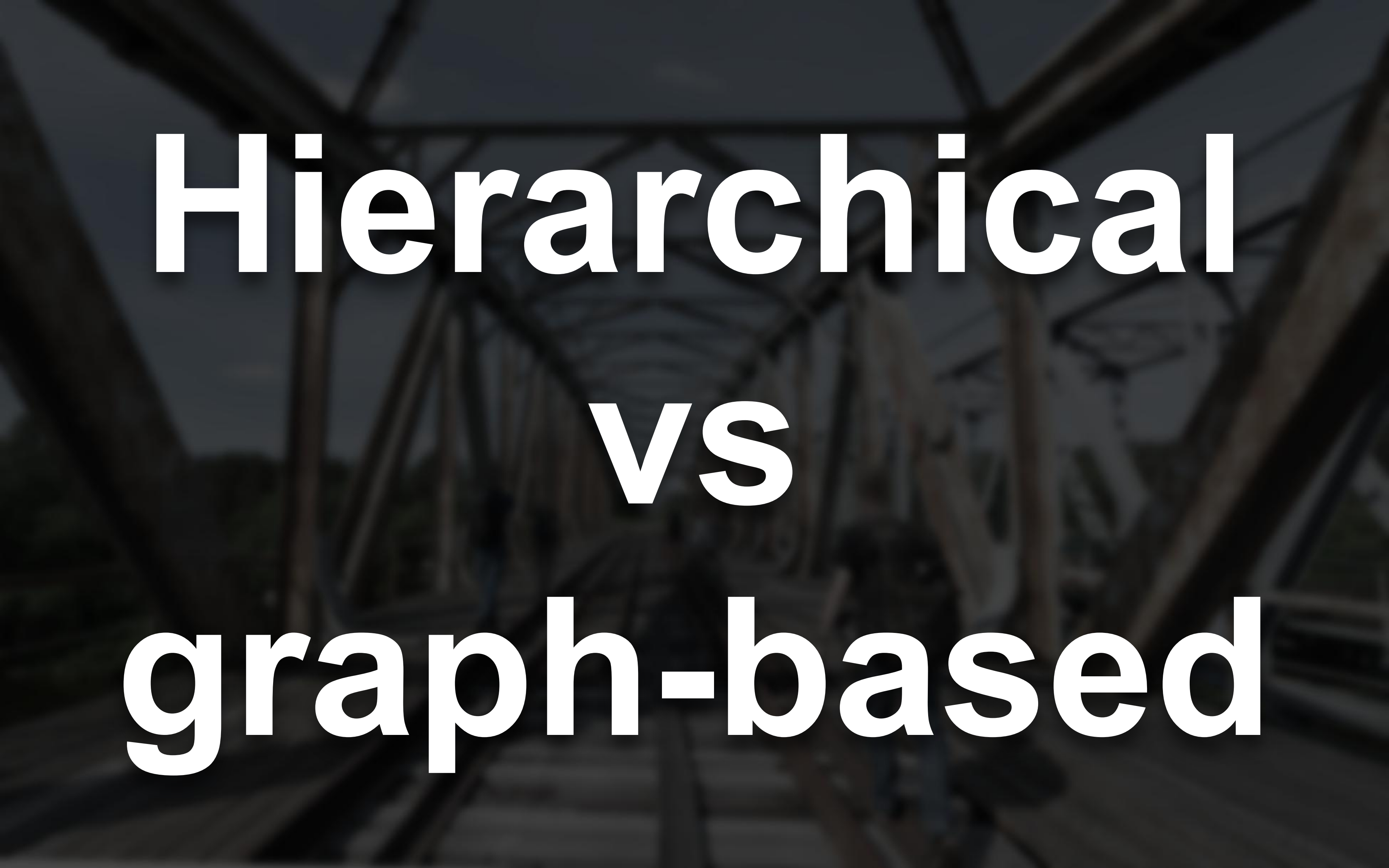
Create trail

Recent events

These are the most recent events recorded by CloudTrail. To view all events for the last 90 days, go to Event history.

	Event time	User name	Event name
▶	[redacted] 08:03:41 PM	root	ConsoleLogin
▶	[redacted] 08:13:55 PM	amplify-[redacted]-cli	PutBucketWebsite
▶	[redacted] 08:13:54 PM	amplify-[redacted]-cli	PutBucketCors
▶	[redacted] 08:13:54 PM	amplify-[redacted]-cli	CreateBucket
▶	[redacted] 08:13:45 PM	amplify-[redacted]-cli	UpdateStack

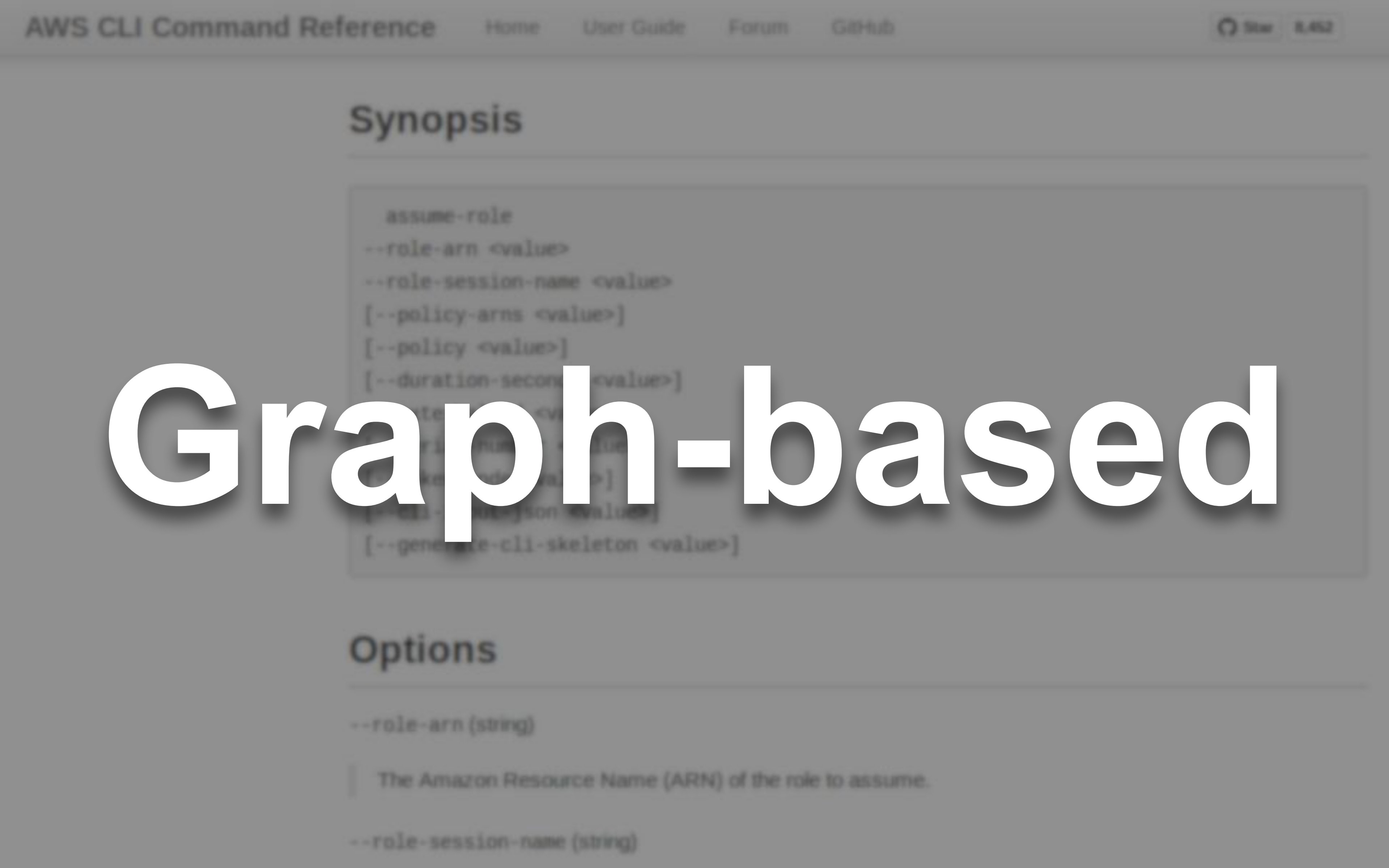
View all events



Hierarchical vs graph-based

Hierarchical

Graph-based



AWS CLI Command Reference Home User Guide Forum GitHub Star 8,452

Synopsis

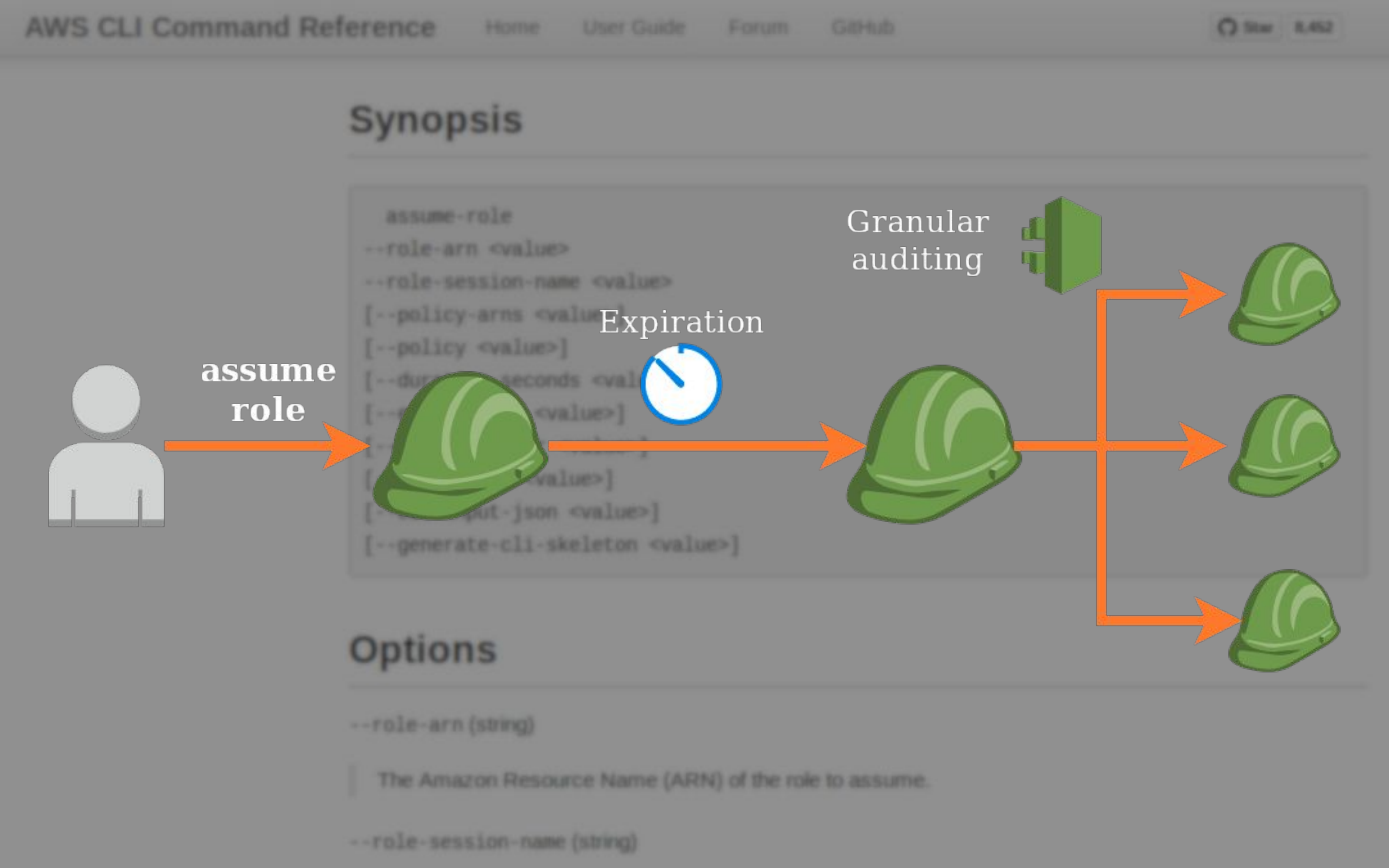
```
  assume-role
--role-arn <value>
--role-session-name <value>
[--policy-arns <value>]
[--policy <value>]
[--duration-seconds <value>]
[--external-id <value>]
[--serial-number <value>]
[--token-code <value>]
[--cli-input-json <value>]
[--generate-cli-skeleton <value>]
```

Options

--role-arn (string)

> The Amazon Resource Name (ARN) of the role to assume.

--role-session-name (string)



AWS CLI Command Reference Home User Guide Forum GitHub Star 8,452

Synopsis

```
  assume-role
--role-arn <value>
--role-session-name <value>
[--policy-arns <value>]
[--policy <value>]
[--duration-seconds <value>]
[-- <value>]
[-- value>]
[ value>]
[--cli-input-json <value>]
[--generate-cli-skeleton <value>]
```

Options

--role-arn (string)

> The Amazon Resource Name (ARN) of the role to assume.

--role-session-name (string)

Hierarchical vs graph-based

```
  assume-role
--role-arn <value>
--role-session-name <value>
[--policy-arns <value>]
[--policy <value>]
[--duration-seconds <value>]
[--external-id <value>]
[--serial-number <value>]
[--token-code <value>]
[--cli-input-json <value>]
[--generate-cli-skeleton <value>]
```

Introduction

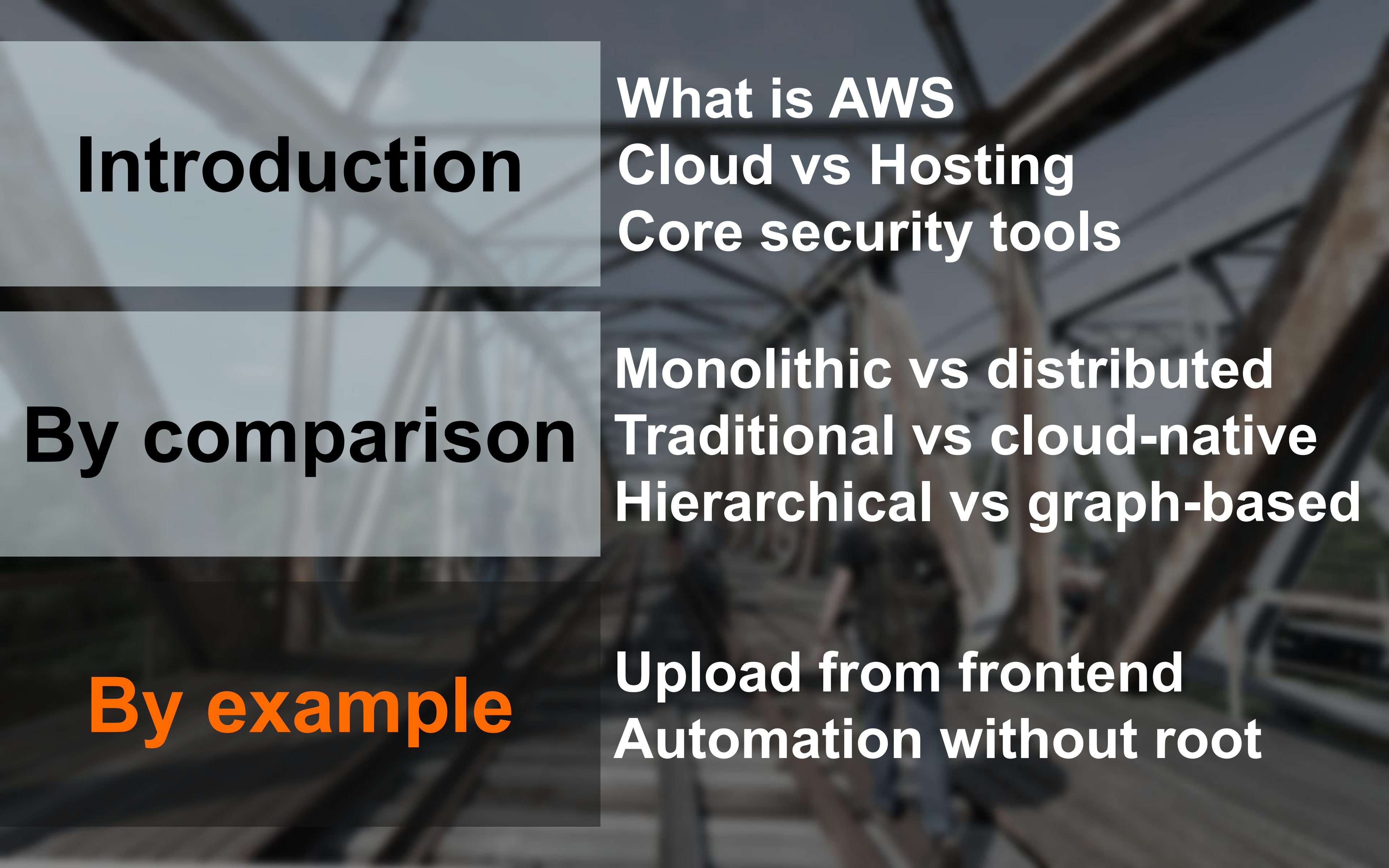
What is AWS
Cloud vs Hosting
Core security tools

By comparison

Monolithic vs distributed
Traditional vs cloud-native
Hierarchical vs graph-based

By example

Upload from frontend
Automation without root



Introduction

- What is AWS
- Cloud vs Hosting
- Core security tools

By comparison

- Monolithic vs distributed
- Traditional vs cloud-native
- Hierarchical vs graph-based

By example

- Upload from frontend
- Automation without root

Upload from frontend

```
use Aws\S3\S3Client;
use Aws\Exception\AwsException;
```

Sample Code

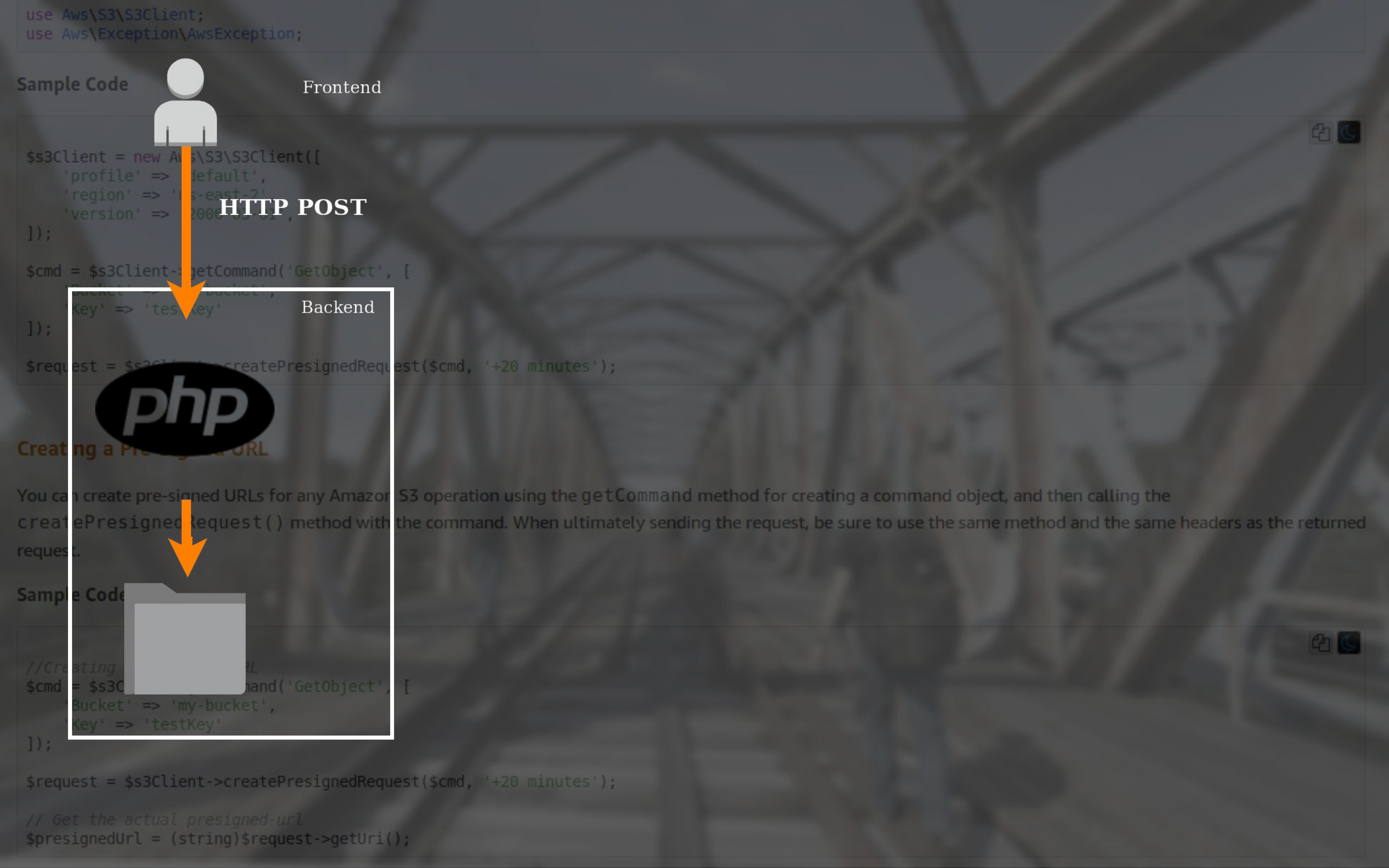
```
$s3Client = new Aws\S3\S3Client([
    'profile' => 'default',
    'region' => 'us-east-2',
    'version' => '2006-03-01',
]);

$cmd = $s3Client->getCommand('GetObject', [
    'Bucket' => 'my-bucket',
    'Key' => 'testKey'
]);

$request = $s3Client->createPresignedRequest($cmd, '+20 minutes');
```

Creating a Pre-Signed URL

You can create pre-signed URLs for any Amazon S3 operation using the `getCommand` method for creating a command object, and then calling the `createPresignedRequest()` method with the command. When ultimately sending the request, be sure to use the same method and the same headers as the returned request.

Sample Code

```
//Creating a presigned URL
$cmd = $s3Client->getCommand('GetObject', [
    'Bucket' => 'my-bucket',
    'Key' => 'testKey'
]);

$request = $s3Client->createPresignedRequest($cmd, '+20 minutes');

// Get the actual presigned-url
$presignedUrl = (string)$request->getUri();
```



```
use Aws\S3\S3Client;
use Aws\Exception\AwsException;
```

Sample Code

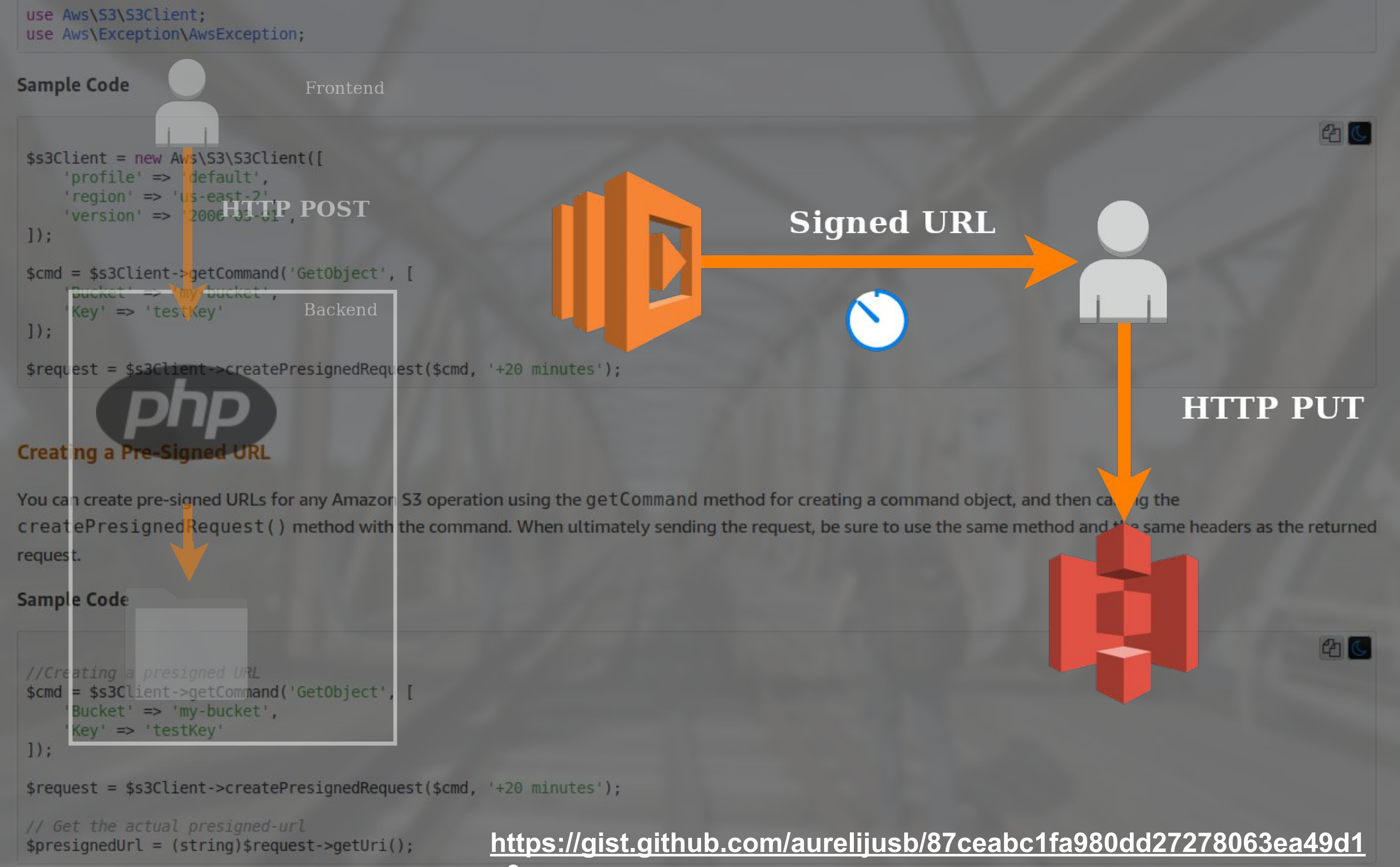
```
$s3Client = new Aws\S3\S3Client([
    'profile' => 'default',
    'region' => 'us-east-2',
    'version' => '2006-03-01',
]);

$cmd = $s3Client->getCommand('GetObject', [
    'Bucket' => 'my-bucket',
    'Key' => 'testKey'
]);

$request = $s3Client->createPresignedRequest($cmd, '+20 minutes');
```

Creating a Pre-signed URL

You can create pre-signed URLs for any Amazon S3 operation using the `getCommand` method for creating a command object, and then calling the `createPresignedRequest()` method with the command. When ultimately sending the request, be sure to use the same method and the same headers as the returned request.

Sample Code

```
//Creating a presigned URL
$cmd = $s3Client->getCommand('GetObject', [
    'Bucket' => 'my-bucket',
    'Key' => 'testKey'
]);

$request = $s3Client->createPresignedRequest($cmd, '+20 minutes');

// Get the actual presigned-url
$presignedUrl = (string)$request->getUri();
```



```
use Aws\S3\S3Client;
use Aws\Exception\AwsException;
```

Sample Code

```
$s3Client = new Aws\S3\S3Client([
    'profile' => 'default',
    'region' => 'us-east-2',
    'version' => '2006-03-01',
]);

$cmd = $s3Client->getCommand('GetObject', [
    'Bucket' => 'my-bucket',
    'Key' => 'testKey'
]);

$request = $s3Client->createPresignedRequest($cmd, '+20 minutes');
```

Creating a Pre-Signed URL

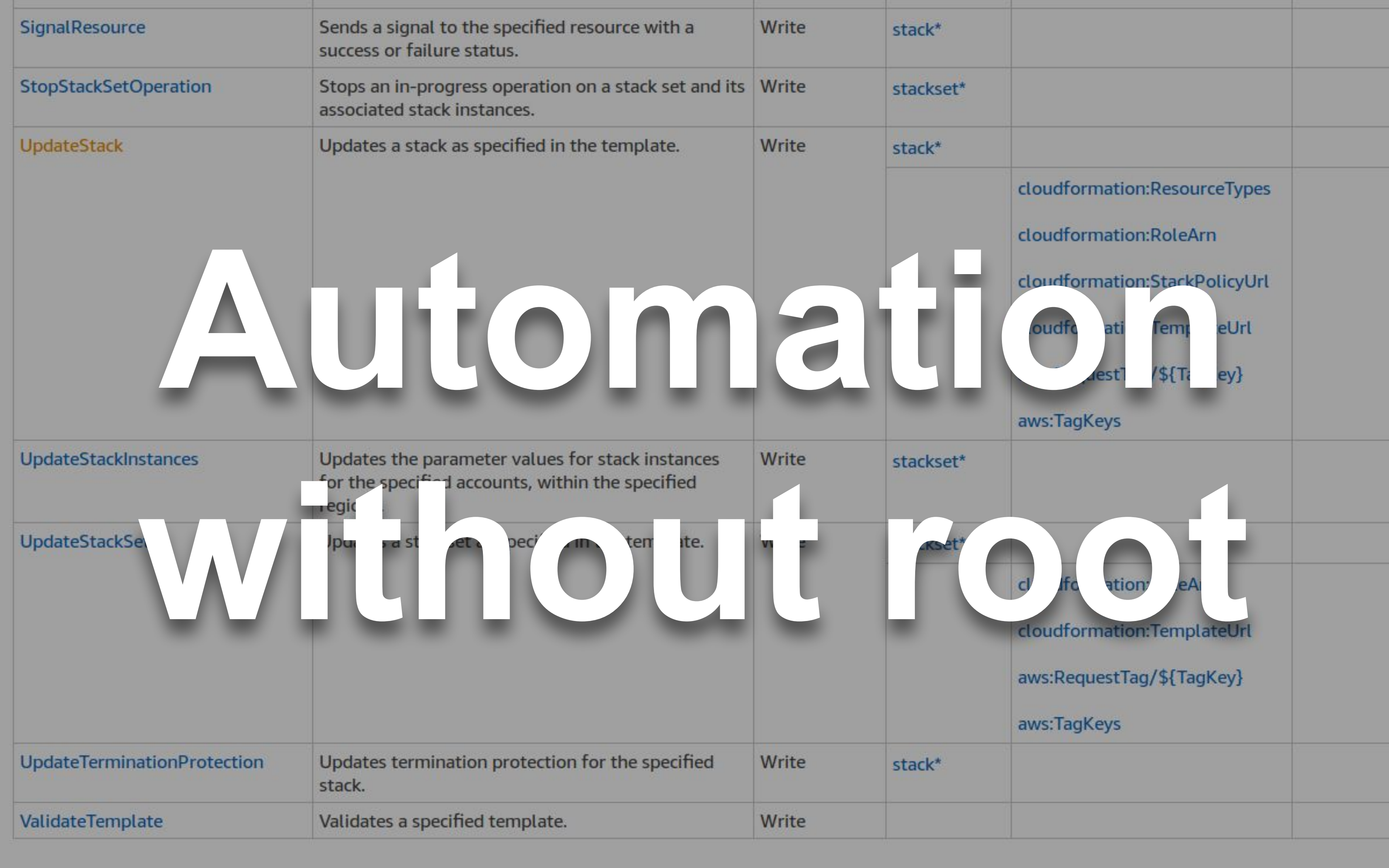
You can create pre-signed URLs for any Amazon S3 operation using the `getCommand` method for creating a command object, and then calling the `createPresignedRequest()` method with the command. When ultimately sending the request, be sure to use the same method and the same headers as the returned request.

Sample Code

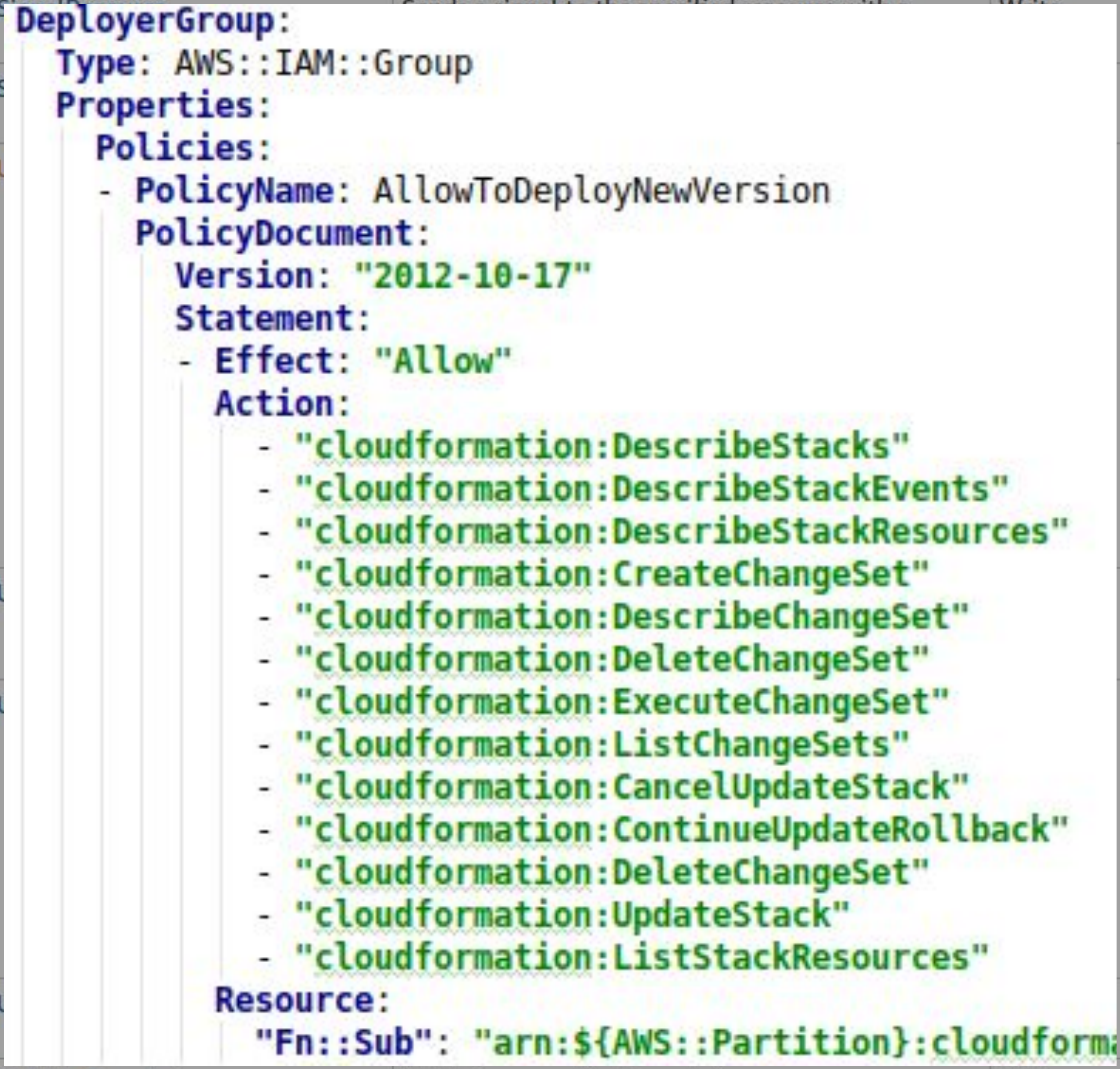
```
//Creating a presigned URL
$cmd = $s3Client->getCommand('GetObject', [
    'Bucket' => 'my-bucket',
    'Key' => 'testKey'
]);

$request = $s3Client->createPresignedRequest($cmd, '+20 minutes');

// Get the actual presigned-url
$presignedUrl = (string)$request->getUri();
```

https://gist.github.com/aurelijusb/87ceabc1fa980dd27278063ea49d1e6c

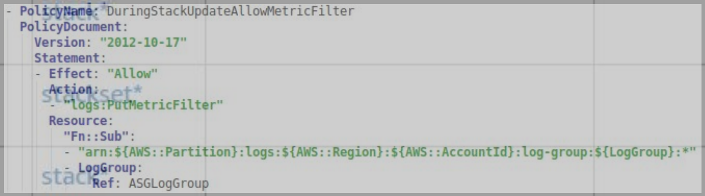
Automation without root



SignalResource	Sends a signal to the specified resource with a success or failure status.	Write	stack*		
StopStackSetOperation	Stops an in-progress operation on a stack set and its associated stack instances.	Write	stackset*		
UpdateStack	Updates a stack as specified in the template.	Write	stack*		
				cloudformation:ResourceTypes cloudformation:RoleArn cloudformation:StackPolicyUrl cloudformation:TemplateUrl aws:RequestTag/${TagKey} aws:TagKeys	
UpdateStackInstances	Updates the parameter values for stack instances for the specified accounts, within the specified regions.	Write	stackset*		
UpdateStackSet	Updates a stack set as specified in the template.	Write	stackset*		
				cloudformation:RoleArn cloudformation:TemplateUrl aws:RequestTag/${TagKey} aws:TagKeys	
UpdateTerminationProtection	Updates termination protection for the specified stack.	Write	stack*		
ValidateTemplate	Validates a specified template.	Write			



```
DeployerGroup:
  Type: AWS::IAM::Group
  Properties:
    Policies:
    - PolicyName: AllowToDeployNewVersion
      PolicyDocument:
        Version: "2012-10-17"
        Statement:
        - Effect: "Allow"
          Action:
            - "cloudformation:DescribeStacks"
            - "cloudformation:DescribeStackEvents"
            - "cloudformation:DescribeStackResources"
            - "cloudformation:CreateChangeSet"
            - "cloudformation:DescribeChangeSet"
            - "cloudformation:DeleteChangeSet"
            - "cloudformation:ExecuteChangeSet"
            - "cloudformation:ListChangeSets"
            - "cloudformation:CancelUpdateStack"
            - "cloudformation:ContinueUpdateRollback"
            - "cloudformation:DeleteChangeSet"
            - "cloudformation:UpdateStack"
            - "cloudformation:ListStackResources"
          Resource:
            "Fn::Sub": "arn:${AWS::Partition}:cloudforma
```



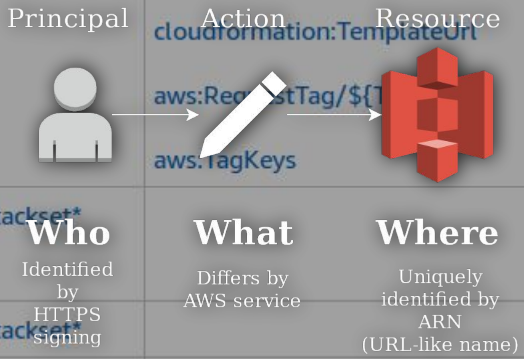
```
- PolicyName: DuringStackUpdateAllowMetricFilter
  PolicyDocument:
    Version: "2012-10-17"
    Statement:
    - Effect: "Allow"
      Action:
      - "logs:PutMetricFilter"
      Resource:
        "Fn::Sub":
        - "arn:${AWS::Partition}:logs:${AWS::Region}:${AWS::AccountId}:log-group:${LogGroup}:*"
        - LogGroup:
            Ref: ASGLogGroup
```

cloudformation:ResourceTypes

cloudformation:RoleArn

cloudformation:StackPolicyUrl

cloudformation:TemplateUrl


Principal
Action
Resource
Who
Identified by HTTPS signing
What
Differs by AWS service
Where
Uniquely identified by ARN (URL-like name)

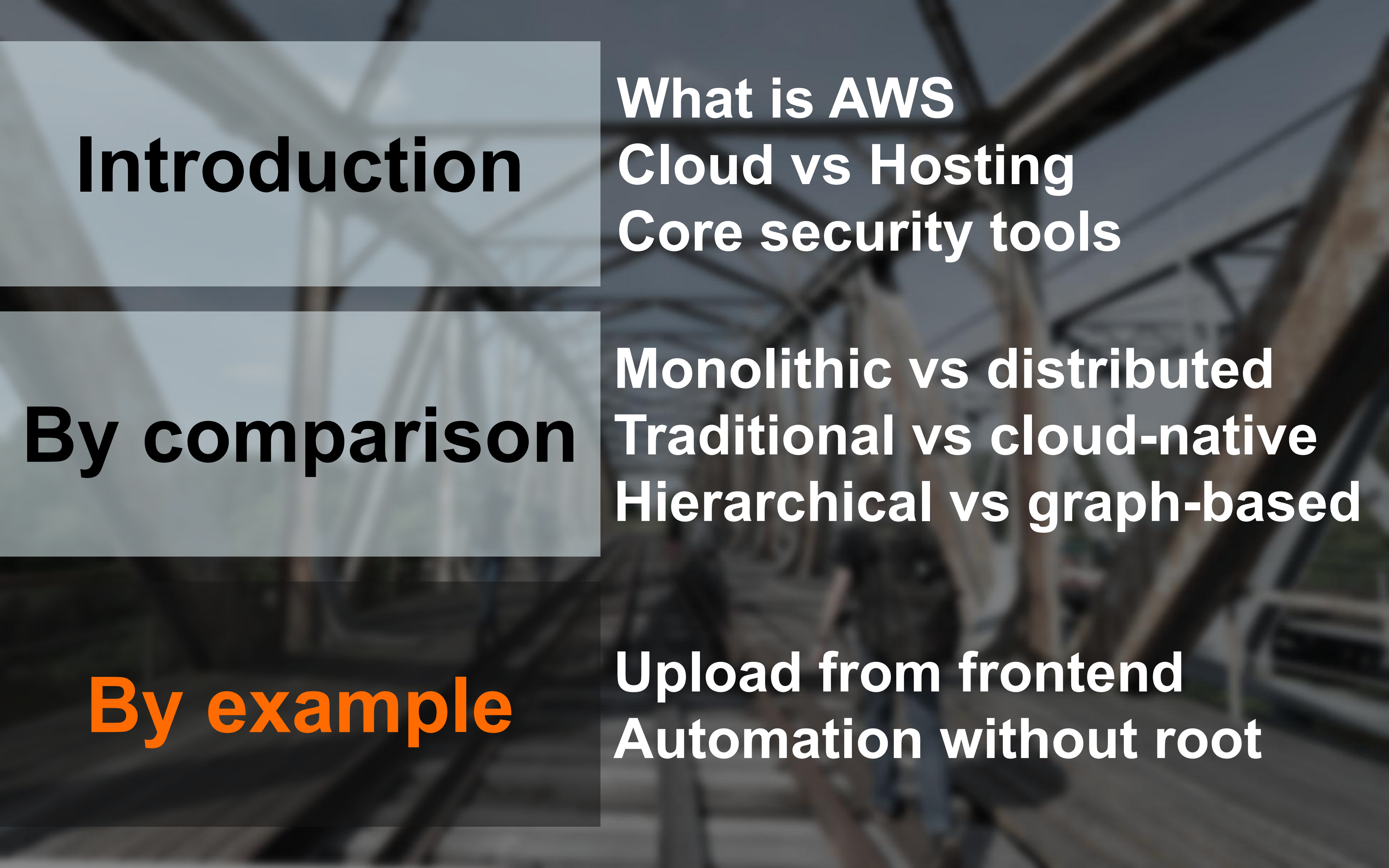
cloudformation:RoleArn

cloudformation:TemplateUrl

aws:RequestTag/${TagKey}

aws:TagKeys

ValidateTemplate	Validates a specified template.	Write		



Introduction

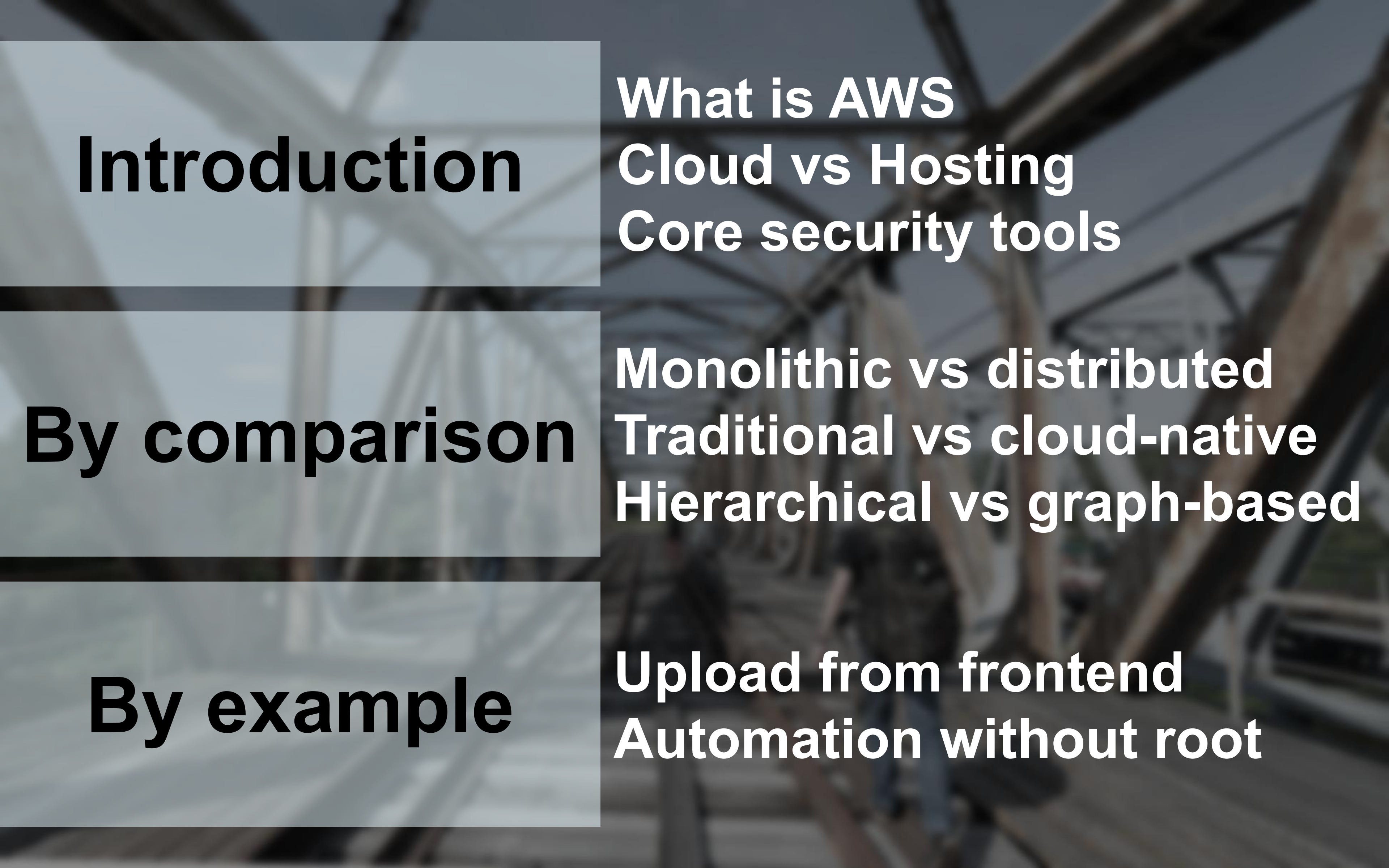
- What is AWS
- Cloud vs Hosting
- Core security tools

By comparison

- Monolithic vs distributed
- Traditional vs cloud-native
- Hierarchical vs graph-based

By example

- Upload from frontend
- Automation without root



Introduction

What is AWS
Cloud vs Hosting
Core security tools

By comparison

Monolithic vs distributed
Traditional vs cloud-native
Hierarchical vs graph-based

By example

Upload from frontend
Automation without root

Conclusion

Problems

harder

Perspective

wider

References and further reading

- AWS Best practices: https://aws.amazon.com/architecture/well-architected/
- Summaries as illustrations: https://www.awsgeek.com/
- Community managed resources: https://github.com/open-guides/og-aws#security-and-iam
- Thinking about the Cloud: from application perspective: http://shop.oreilly.com/product/0636920072768.do
- Thinking about the Cloud: from infrastructure tools perspective: http://shop.oreilly.com/product/0636920075837.do

How AWS handles security

Thank you

Discussion?

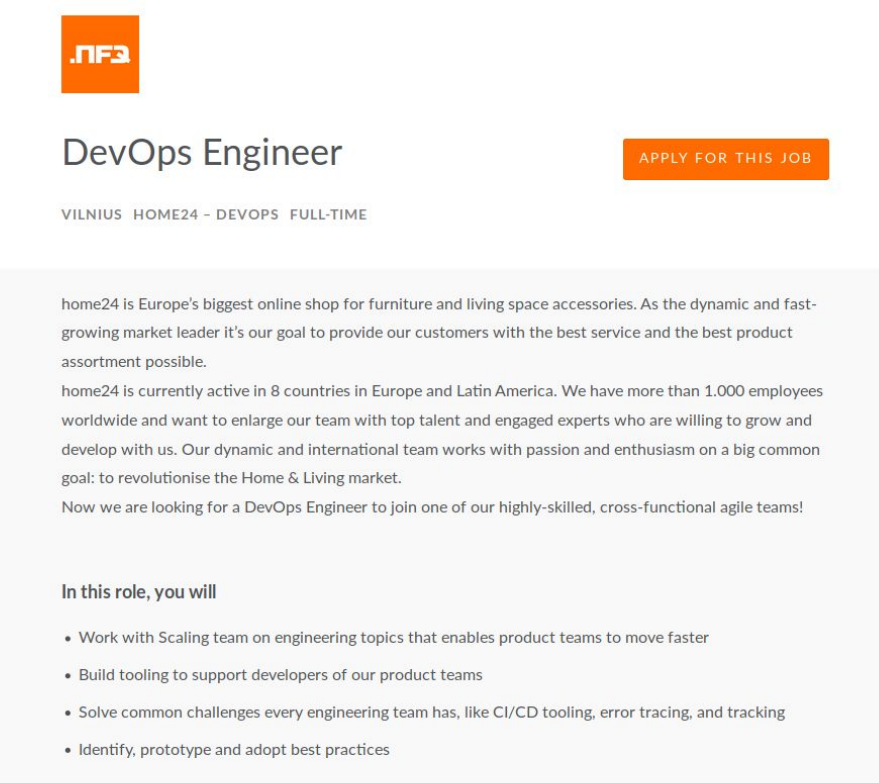
Aurelijus Banelis

VilniusPHP 0x52
2019-09-05

Like what we do here @ NFQ?

By the way I am searching for a new team member…

...and I split bonus with them (current colleagues can prove that)



DevOps Engineer

VILNIUS HOME24 - DEVOPS FULL-TIME

home24 is Europe's biggest online shop for furniture and living space accessories. As the dynamic and fast-growing market leader it's our goal to provide our customers with the best service and the best product assortment possible.

home24 is currently active in 8 countries in Europe and Latin America. We have more than 1.000 employees worldwide and want to enlarge our team with top talent and engaged experts who are willing to grow and develop with us. Our dynamic and international team works with passion and enthusiasm on a big common goal: to revolutionise the Home & Living market.

Now we are looking for a DevOps Engineer to join one of our highly-skilled, cross-functional agile teams!

In this role, you will

- Work with Scaling team on engineering topics that enables product teams to move faster
- Build tooling to support developers of our product teams
- Solve common challenges every engineering team has, like CI/CD tooling, error tracing, and tracking
- Identify, prototype and adopt best practices