

TLA+ COMMUNITY EVENT 2023

TLA+ at AWS: Past, Present, and Future

Cezara Drăgoi
Principal Applied Scientist
AWS

Scarlet Schwiderski-Grosche
Principal Tech Program Manager
AWS



Agenda

Introduction

- Automated Reasoning at AWS
- Open Source at AWS

TLA+ at AWS

- Past, Present, and Future

Conclusions



Motivation for joining the TLA+ Foundation

- Formal methods



Motivation for joining the TLA+ Foundation

- Formal methods
- Open Source



TLA+ track record at AWS

- One of the main industry users
- Over more than 10 years
- Dozens of projects



DOI:10.1145/2699417

Engineers use TLA+ to prevent serious but subtle bugs from reaching production.

BY CHRIS NEWCOMBE, TIM RATH, FAN ZHANG, BOGDAN MUNTEANU, MARC BROOKER, AND MICHAEL DEARDEUFF

How Amazon Web Services Uses Formal Methods

S3 is just one of many AWS services that store and process data our customers have entrusted to us. To safeguard that data, the core of each service relies on fault-tolerant distributed algorithms for replication, consistency, concurrency control, auto-scaling, load balancing, and other coordination tasks. There are many such algorithms in the literature, but combining them into a cohesive system is a challenge, as the algorithms must usually be modified to interact properly in a real-world system. In addition, we have found it necessary to invent algorithms of our own. We work hard to avoid unnecessary complexity, but the essential complexity of the task remains high.

Complexity increases the probability of human error in design, code, and operations. Errors in the core of the system could cause loss or corruption of data, or violate other interface contracts on which our customers de-

Communications of the ACM | April 2015 | Vol. 58 | No. 4



amazonjobs

Search for jobs by title or keyword



Location



Your job application

Leadership Principles

We use our Leadership Principles every day, whether we're discussing ideas for new projects or deciding on the best way to solve a problem. It's just one of the things that makes Amazon peculiar.

Customer Obsession

Leaders start with the customer and work backwards. They work vigorously to earn and keep customer trust. Although leaders pay attention to competitors, they obsess over customers.

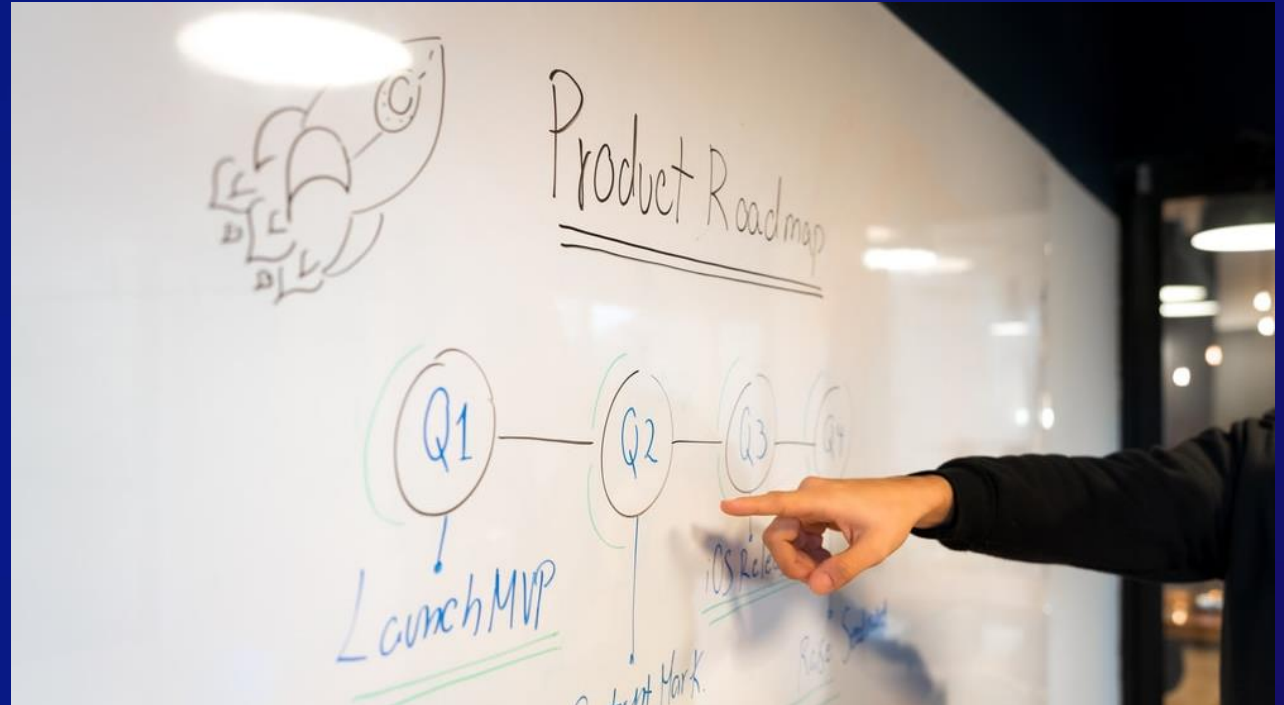


Customer Obsession

Leaders start with the customer and work backwards. They work vigorously to earn and keep customer trust. Although leaders pay attention to competitors, they obsess over customers.

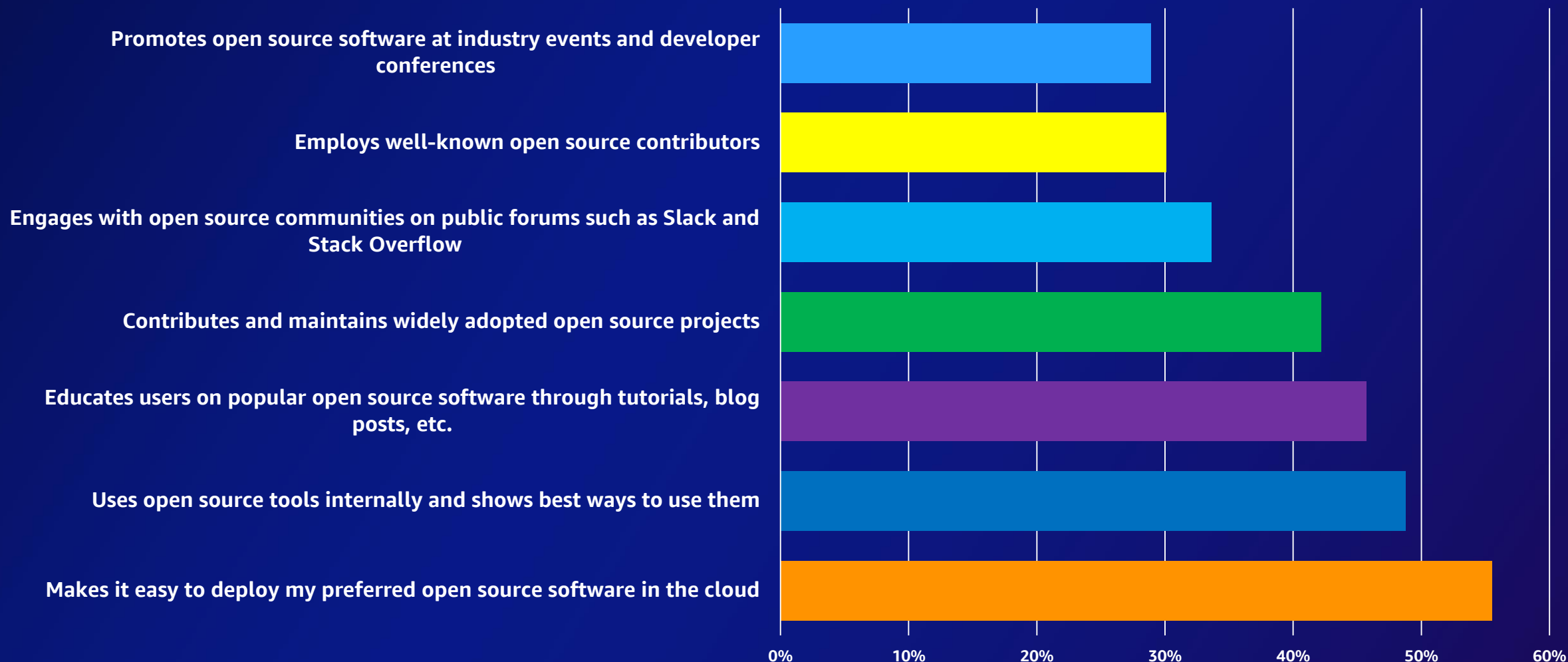


90% of the AWS roadmap is driven by direct customer feedback, and this is also true of open source.



[@slidebean](#)

Open Source Leadership



OpenJDK



mxnet



ROS



PyTorch



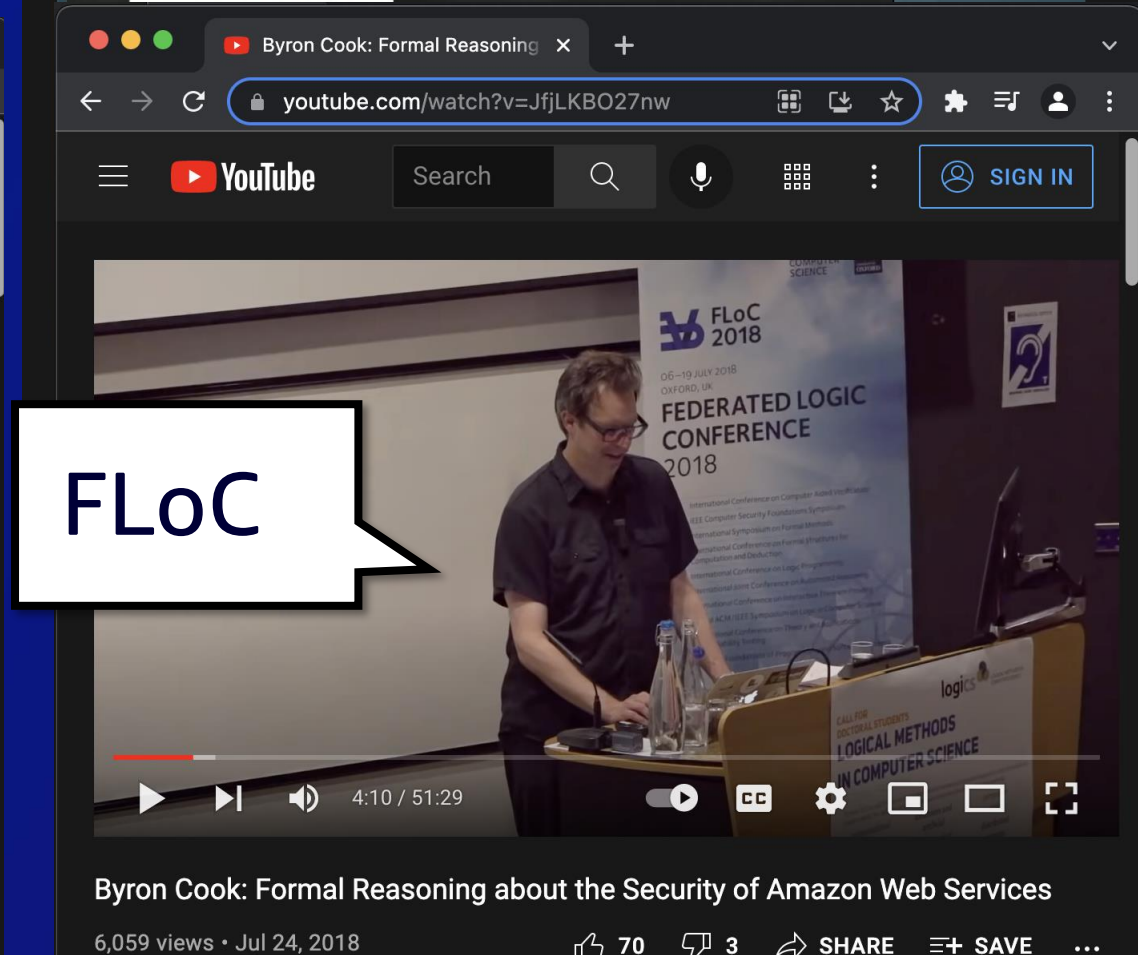
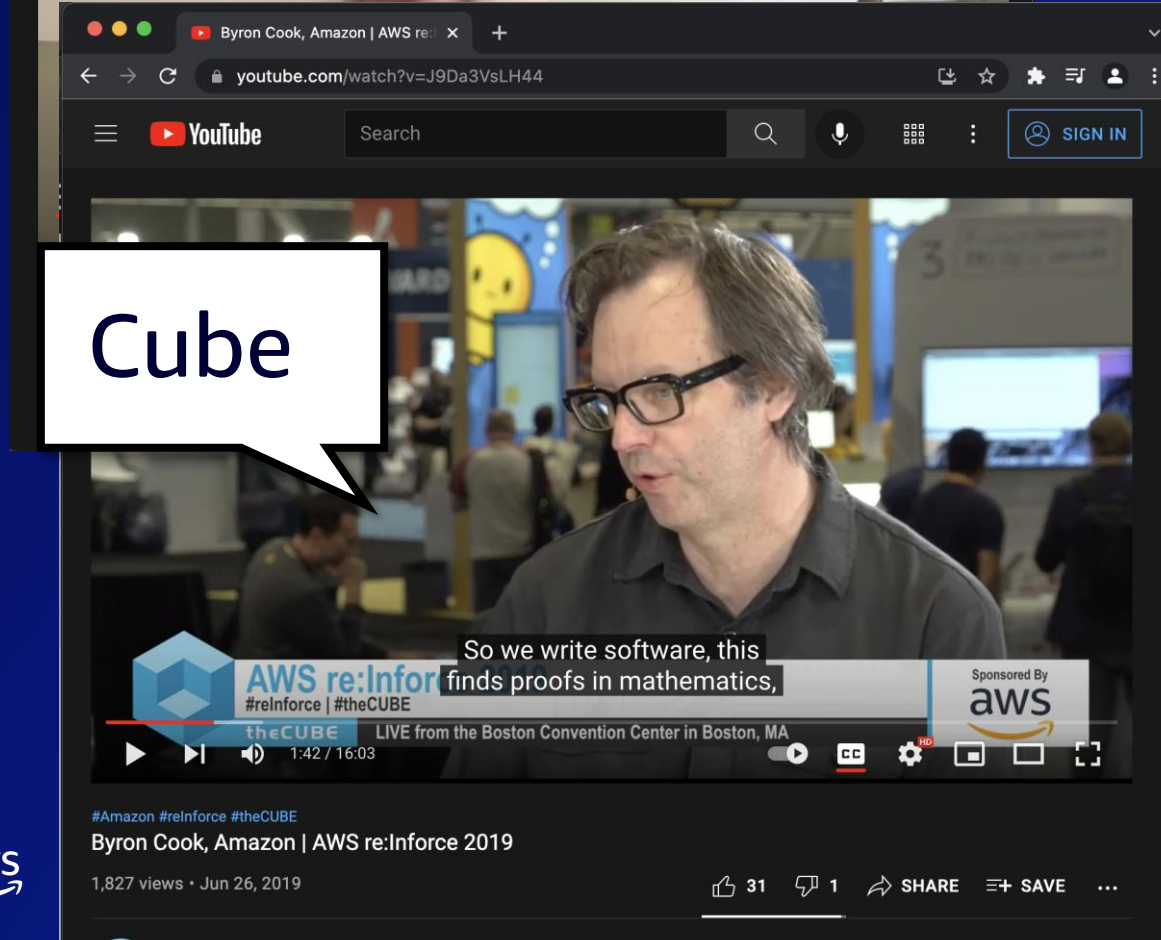
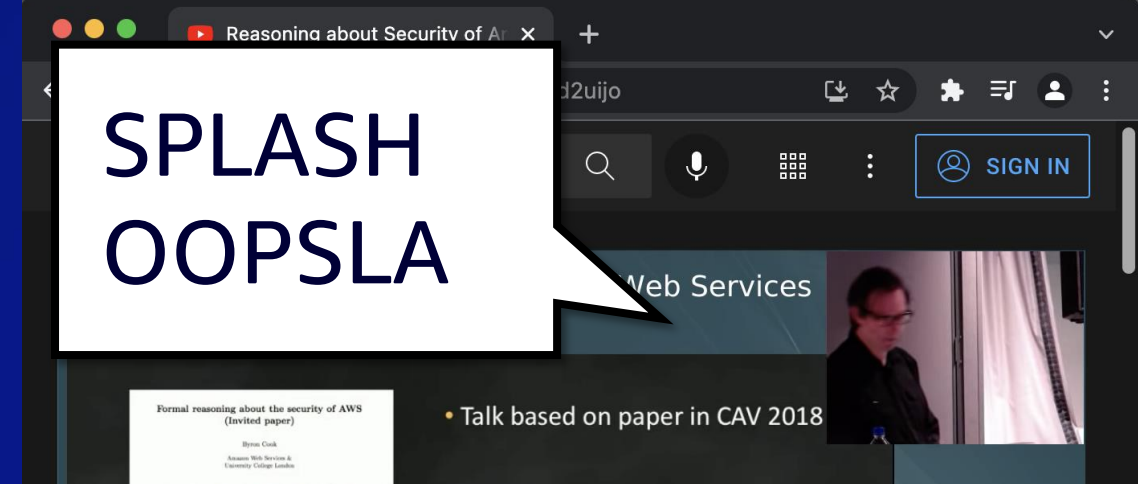
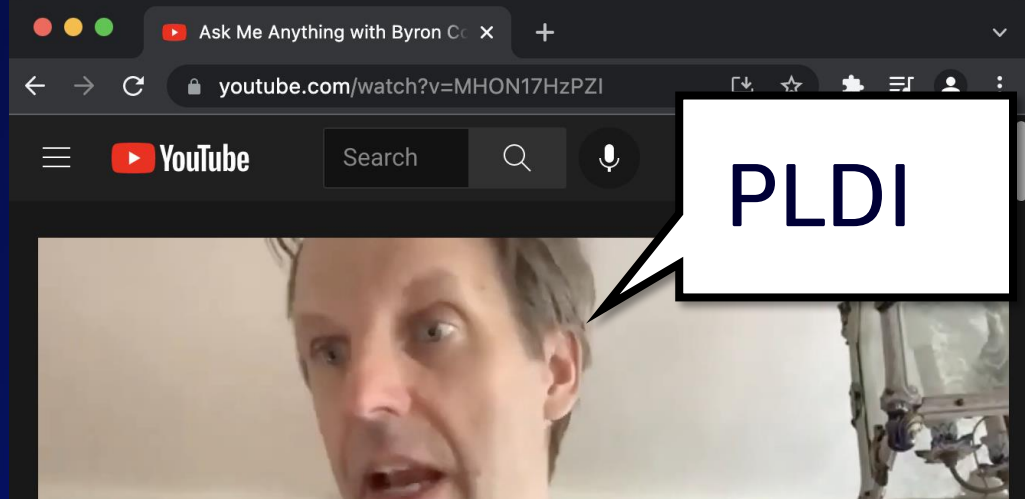
NGINX



OpenSSL
Cryptography and SSL/TLS Toolkit

containerd







#AWS

AWS re:Invent 2020 - Developer Keynote with Dr. Werner Vogels

417,708 views • Dec 18, 2020

401 23 SHARE SAVE ...

Examples of customer-facing features



Services ▼

☒ New VPC Experience
Tell us what you think

VPC Dashboard **New**

Filter by VPC:

🔍 Select a VPC

▶ VIRTUAL PRIVATE
CLOUD

▶ SECURITY

▼ REACHABILITY

Reachability Analyzer

VPC Reachability
Analyzer

Examples of customer-facing features



Services ▾

 New VPC Experience
Tell us what you think

VPC Dashboard **New**

Filter by VPC:

 Select a VPC

▶ VIRTUAL PRIVATE
CLOUD

▶ SECURITY


▼ REACHABILITY

Reachability Analyzer

Rules > Add rule

Add rule

Add rules to define the desired configuration settings of your AWS resource. To add a custom rule, you must create an AWS Lambda function for the rule.

 Add custom rule

ec2

approved-amis-by-id

Checks whether running instances are using specified AMIs. Specify a list of approved AMI IDs. Running instances with AMIs that are not on this list are noncompliant.

EC2

approved-amis-by-tag

Checks whether running instances are using specified AMIs. Specify the tags that identify the AMIs. Running instances with AMIs that don't have at least one of the specified tags

EC2

desired-instance-tenancy

Checks instances for specified tenancy. Specify AMI IDs to check instances that are launched from those AMIs or specify Host IDs

desired-instance-type

Checks whether your EC2 instances are of the specified instance types.

cloudwatch-alarm-resource-check **New**

Checks whether the specified resource type has a CloudWatch alarm for the specified metric. For resource type, you can specify EBS volumes, EC2 instances, RDS clusters,

CloudWatch

ebs-optimized-instance

Checks whether EBS optimization is enabled for your EC2 instances that can be EBS-optimized.

EC2

ec2-managedinstance-applications-bl...

Checks that none of the specified applications are installed on the instance. Optionally, specify the version. Newer versions will not be blacklisted. Optionally,

Systems Manager


Managed
Config Rules

VPC Reachability
Analyzer

Examples of customer-facing features



Services ▾

 New VPC Experience
Tell us what you think

VPC Dashboard **New**

Filter by VPC:

 Select a VPC

► VIRTUAL PRIVATE
CLOUD

► SECURITY


▼ REACHABILITY

Reachability Analyzer

Rules > Add rule

Add rule

Add rules to define the desired configuration settings of your AWS resource. For a custom rule, you must create an AWS Lambda function for the rule.



ec2

approved-amis-by-id

Checks whether running instances are using specified AMIs. Specify a list of approved AMI IDs. Running instances with AMIs that are not on this list are noncompliant.

EC2

approved-amis-by-tag

Checks whether running instances are using specified AMIs. Specify the tags that identify the AMIs. Running instances with AMIs that don't have at least one of the specified tags

EC2

cloudwatch-alarm-resource-check **New**

Checks whether the specified resource type has a CloudWatch alarm for the specified metric. For resource type, you can specify EBS volumes, EC2 instances, RDS clusters,

CloudWatch

desired-instance-tenancy

Checks instances for specified tenancy. Specify AMI IDs to check instances that are launched from those AMIs or specify Host IDs

desired-instance-type

Checks whether your EC2 instances are of the specified instance types.

ebs-optimized-instance

Checks whether EBS optimization is enabled for your EC2 instances that can be EBS-optimized.

EC2

ec2-managedinstance-applications-bl...

Checks that none of the specified applications are installed on the instance. Optionally, specify the version. Newer versions will not be blacklisted. Optionally,

Systems Manager

Managed Config Rules

VPC Reachability Analyzer

Block public access (account settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, or both. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block *all* public access. These settings apply account-wide for all current and future buckets. AWS recommends that you turn on Block *all* public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

☒ Block *all* public access

Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

☐ Block public access to buckets and objects granted through *new* access control lists (ACLs)

S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3

☐ Block public access to buckets and objects granted through *any* access control lists (ACLs)

☐ Block public access to buckets and objects granted through *new* public bucket policies

S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access bucket policies. This setting doesn't change any existing policies

☐ Block public access to buckets and objects granted through *any* public bucket policies

S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access bucket policies. This setting doesn't change any existing policies

S3 Block Public Access

Examples of customer-facing features



Services ▾



New VPC Experience

Tell us what you think

VPC Dashboard **New**

Filter by VPC:

Select a VPC

▶ VIRTUAL PRIVATE CLOUD

▶ SECURITY

▼ REACHABILITY

Reachability Analyzer

Rules > Add rule

Add rule

Add rules to define the desired configuration settings of your AWS resource. For a custom rule, you must create an AWS Lambda function for the rule.

Add custom rule

ec2

approved-amis-by-id

Checks whether running instances are using specified AMIs. Specify a list of approved AMI IDs. Running instances with AMIs that are not on this list are noncompliant.

EC2

approved-amis-by-tag

Checks whether running instances are using specified AMIs. Specify the tags that identify the AMIs. Running instances with AMIs that don't have at least one of the specified tags

EC2

cloudwatch-alarm-resource-check **New**

Checks whether the specified resource type has a CloudWatch alarm for the specified metric. For resource type, you can specify EBS volumes, EC2 instances, RDS clusters,

CloudWatch

desired-instance-tenancy

Checks instances for specified tenancy. Specify AMI IDs to check instances that are launched from those AMIs or specify Host IDs

desired-instance-type

Checks whether your EC2 instances are of the specified instance types.

ebs-optimized-instance

Checks whether EBS optimization is enabled for your EC2 instances that can be EBS-optimized.

EC2

ec2-managedinstance-applications-bl...

Checks that none of the specified applications are installed on the instance. Optionally, specify the version. Newer versions will not be blacklisted. Optionally,

Systems Manager

Managed Config Rules

VPC Reachability Analyzer

Block public access (account settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, or both. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block *all* public access. These settings apply account-wide for all current and future buckets. AWS recommends that you turn on Block *all* public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

☒ Block *all* public access

Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

☐ Block public access to buckets and objects granted through *new* access control lists (ACLs)

S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3

S3 Block Public Access

Block public access to buckets and objects granted through *new* access control lists (ACLs)

Block public access to buckets and objects granted through *new* public bucket policies

S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access bucket policies for existing buckets and objects. This setting doesn't change any existing policies that allow public access to S3

Block public access to buckets and objects granted through *any* public bucket policies

S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access bucket policies for existing buckets and objects. This setting doesn't change any existing policies that allow public access to S3



Services ▾

Resource Groups ▾



IAM > Access Analyzer > Create analyzer

Create analyzer [Info](#)

The analyzer scans the resources within the zone of trust.

Region

US East (N. Virginia)

You should enable Access Analyzer in each Region where you use AWS resources.

Name

AccessAnalyzerIsGreat

Maximum 255 characters

Zone of trust [Info](#)

Policies for all supported resources within your zone of trust are analyzed to identify access allowed from outside the zone of trust.

Current account (796744228948)

IAM Access Analyzer

Replacing features

 New VPC Experience
Tell us what you think

VPC Dashboard **New**

Filter by VPC:

 Select a VPC

▶ VIRTUAL PRIVATE CLOUD

▶ SECURITY


▼ REACHABILITY

Reachability Analyzer

Rules > Add rule

Add rule

Add rules to define the desired configuration settings of your AWS resource. For a custom rule, you must create an AWS Lambda function for the rule.

 Add custom rule

ec2

approved-amis-by-id

Checks whether running instances are using specified AMIs. Specify a list of approved AMI IDs. Running instances with AMIs that are not on this list are noncompliant.

EC2

approved-amis-by-tag

Checks whether the specified resource type is using specified AMIs. Specify the tags that identify the AMIs. Running instances with AMIs that don't have at least one of the specified tags

EC2

cloudwatch-alarm-resource-check **New**

Checks whether the specified resource type has a CloudWatch alarm for the specified metric. For resource type, you can specify EBS volumes, EC2 instances, RDS clusters,

CloudWatch

desired-instance-tenancy

Checks instances for specified tenancy. Specify AMI IDs to check instances that are launched from those AMIs or specify Host IDs

desired-instance-type

Checks whether your EC2 instances are of the specified instance types.

ebs-optimized-instance

Checks whether EBS optimization is enabled for your EC2 instances that can be EBS-optimized.

EC2

ec2-managedinstance-applications-bl...

Checks that none of the specified applications are installed on the instance. Optionally, specify the version. Newer versions will not be blacklisted. Optionally,

Systems Manager

Managed Config Rules

VPC Reachability Analyzer

Block public access (account settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, or both. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply account-wide for all current and future buckets. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

☒ Block all public access

Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

☐ Block public access to buckets and objects granted through new access control lists (ACLs)

S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change existing permissions that allow public access to S3

S3 Block Public Access

☐ Block public access to buckets and objects granted through new public bucket policies

S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access bucket policies. This setting doesn't change any existing policies

☐ Block public access to buckets and objects granted through any public bucket policies

S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access bucket policies. This setting doesn't change any existing policies

☐ Block public access to buckets and objects granted through any access control lists (ACLs)

S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change existing permissions that allow public access to S3

ForkliftMonitoring **Edit**

Rerun analysis

Create input

Publish

State

State name

Normal

▼ OnEnter (3) [Add event](#)

1 Create awake timer

2 Publish to asset property

3 Alert if too heavy

▼ OnInput (1) [Add event](#)

1 Reset_timer

▼ OnExit [Add event](#)

AWS IoT Events

IAM Access Analyzer

aws Services ▼ Resource Groups ▼

[IAM](#) > [Access Analyzer](#) > Create analyzer

Create analyzer [Info](#)

The analyzer scans the resources within the zone of trust.

Region

US East (N. Virginia)

You should enable Access Analyzer in each Region where you use AWS resources.

Name

AccessAnalyzerIsGreat

Maximum 255 characters

Zone of trust [Info](#)

Policies for all supported resources within your zone of trust are analyzed to identify access allowed from outside the zone of trust.

Current account (796744228948)

AWS product categories



Analytics



Application Integration



Blockchain



Business Applications



Cloud Financial Management



Compute



Containers



Customer Engagement



Database



Developer Tools



End User Computing



Front-End Web & Mobile



Game Tech



Internet of Things



Machine Learning



Management & Governance



Media Services



Migration & Transfer



Networking & Content
Delivery



Quantum Technologies



Robotics



Satellite



Security, Identity &
Compliance



Serverless

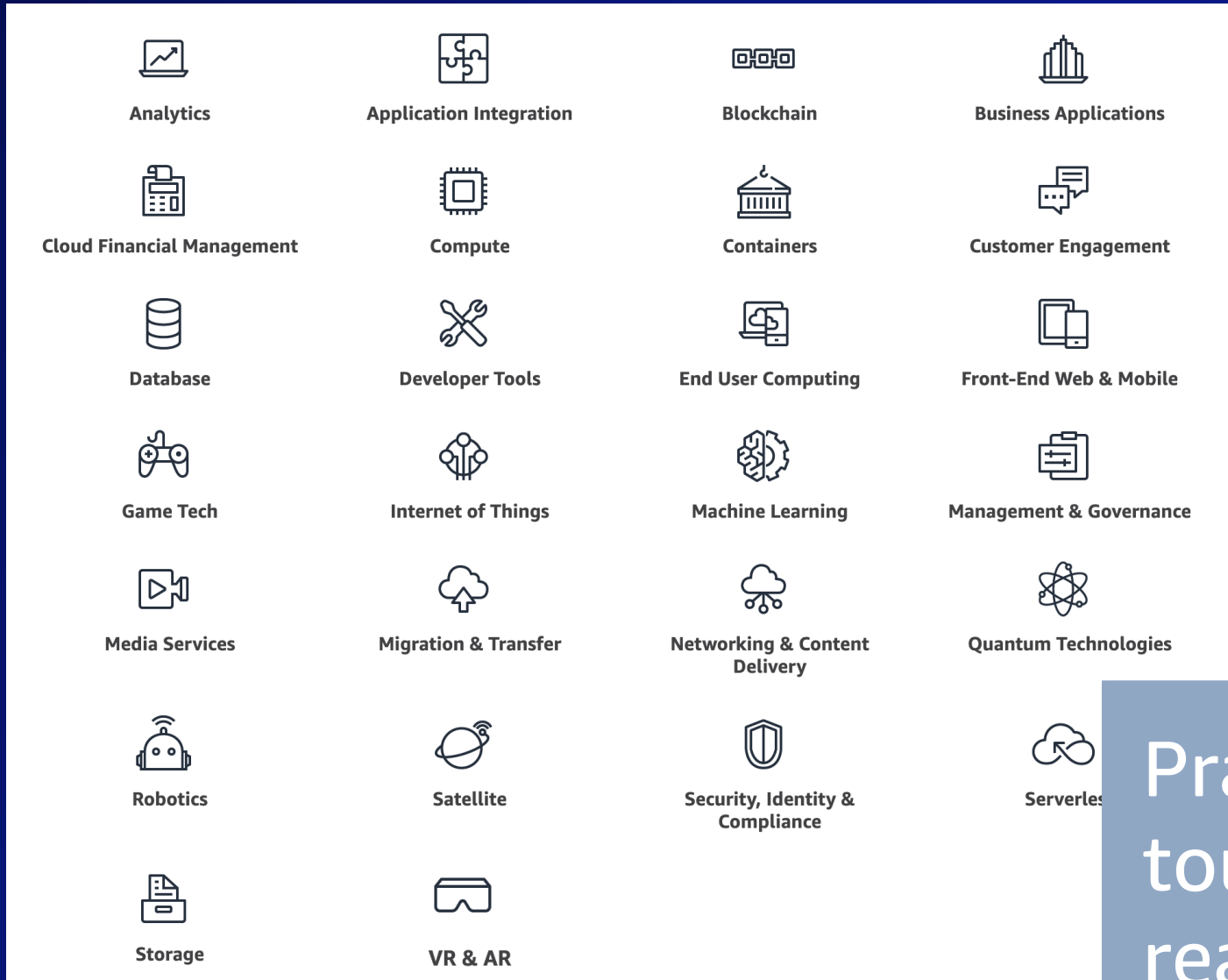


Storage



VR & AR

AWS product categories



Practically every area touched by automated reasoning in some way

Scientists at *Principal* level or above



[View Badge Photo](#)

Rajeev
Joshi



Gustavo
Petri



Dominic
Mulligan



Emina
Torlak



Tancred
Lepoint



[View Badge Photo](#)

Jim
Grundy



Muhammad
Naveed



Cezara
Drăgoi



Leo
de Moura



Aws
Albarghouthi



[View Badge Photo](#)

Jared
Davis



John
Harrison



Willem
Visser



Zvonimir
Rakamaric



Cesar
Munoz



Byron
Cook



[View Badge Photo](#)

Jaco
Geldenhuys



Mike
Whalen



Andrew
Gacek



Murat
Demirbas



Ben
Liblit



Mark
Tuttle



Nathan
Chong



[View Custom Photo](#)

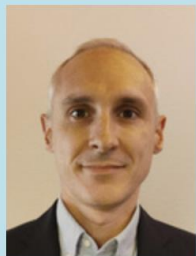
Ernie
Cohen



Mike
Hicks



Sean
McLaughlin



Remi
Delmas



Rustan
Leino



Serdar
Tasiran



Bruno
Dutertre



Temesghen
Kahsai



Daniel
Kroening



Dimitra
Giannakopoulou



Lee
Pike



John
Backes



Rod
Chapman

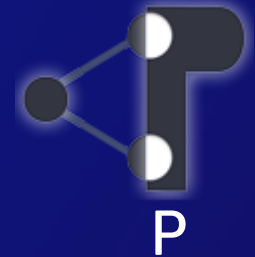


AWS Zelkova

AMZN Dust



AWS Shuttle



AWS Tiros



CEDAR



TLA+

FOUNDATION

Over to Cezara



"Use of formal methods at AWS" paper –2014

- "Since 2011, engineers at Amazon Web Services (AWS) have been using formal specification and model checking to help solve difficult design problems in critical systems."
- "We have found that testing the code is inadequate as a method to find subtle errors in design"

TLA+ modeling at Amazon

Code repo search shows more than 100 TLA+ models S3

- DynamoDB
- EBS
- Lambda
- Several internal services

Grassroots TLA+ use

Engineer has a hard distributed/concurrency problem

- hears about TLA+
- learns it on their own in less than a week
- writes a model, designs/mends the protocol
- moves on. . .

Takeaways

TLA+ did fill an important need

Use has been sporadic and on ad hoc basis

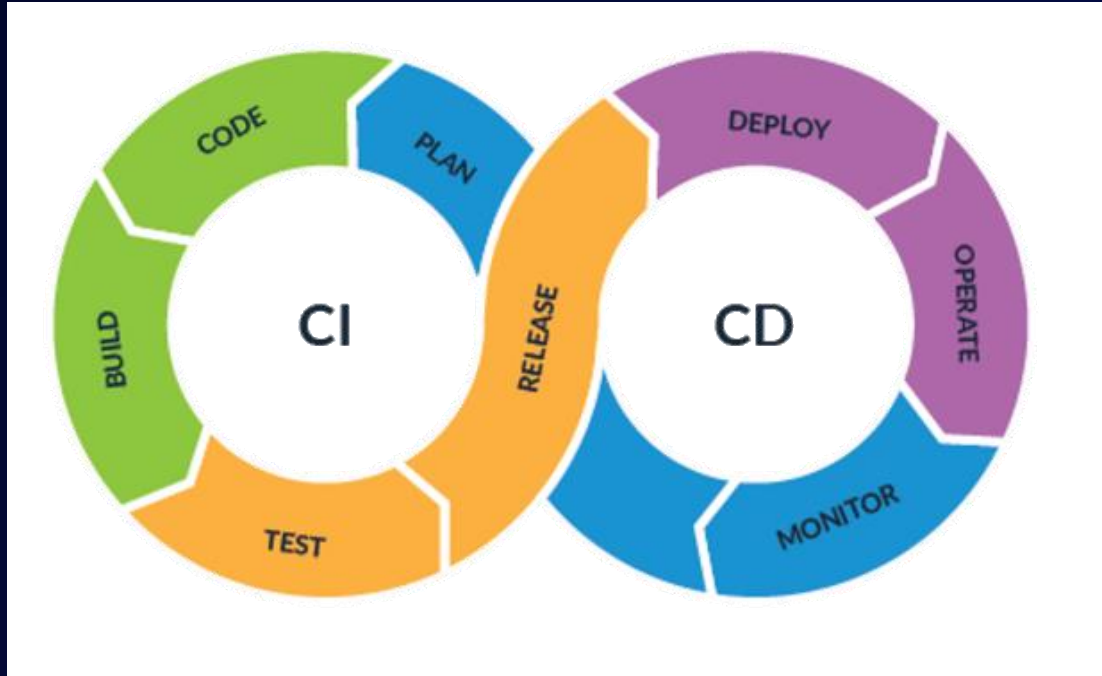
Motivated by an itch to scratch, quick ramp up was possible
(survival bias?)

Present day software

- very large code bases
- composition of system of systems
- large teams
- continuous integration / continuous deployment (CI/CD)

We have found that testing the code is VERY DIFFICULT
for software

CI/CD



- exploring protocols
- debugging concurrency
- code conformance
- adding features
- preventing code regression

TLA strengths and weaknesses

- TLA+ is declarative,
- succinct,
- high-level,
- is great for rapidly exploring distributed/concurrent protocol design space

But it is weak at

- Avoiding code drift
- Model-based testing
- Conformance checking
- Integration testing

Automated Reasoning at Amazon

- SMT solvers
- Code conformance checking support (Shuttle, P)
- High level modeling support (TLA+)
- Proofs and code generation from proved models (Dafny)

Dealing with scale

- random coverage rather than full coverage
- reference implementation testing
- compositional testing with abstract/mocks
- differential testing

- TLA+ is still going strong because it is very strong at what it does: Debugging Designs!
- TLA+ is still grassroots and ad hoc

Future of TLA+: Reuse, Reduce, Recycle

- Without taking from the strengths of TLA+, can we bridge the gap between TLA+ modeling and large scale software deployments via CI/CD
- Reuse: How do we make TLA+ models more reusable?
- Reuse: How do we make TLA+ models more reusable to serve composable system of systems software?
- Recycle: Can we keep TLA+ sticky and check/prevent code drift from model?

Reducing friction

This was great!

- VSCode integration
- Adding statistical support peripherally
- Hillel's work on popularizing TLA+

Can we do more?

Thank you!

