

AWS Monitoring & Logging

Different log categories

AWS Infrastructure logs

- AWS CloudTrail
- Amazon VPC Flow Logs

AWS service logs

- Amazon S3
- AWS Elastic Load Balancing
- Amazon CloudFront
- AWS Lambda
- AWS Elastic Beanstalk
- ...

Host based logs

- Messages
- Security
- NGINX/Apache/IIS
- Windows Event Logs
- Windows Performance Counters
- ...

Different log categories

AWS Infrastructure logs

- AWS CloudTrail
- Amazon VPC Flow Logs

AWS service logs

- Amazon S3
- AWS Elastic Load Balancing
- Amazon CloudFront
- AWS Lambda
- AWS Elastic Beanstalk
- ...

Host based logs

- Messages
- Security
- NGINX/Apache/IIS
- Windows Event Logs
- Windows Performance Counters
- ...

Security related events

AWS CloudTrail

Records AWS API calls for your account

What can you answer using a CloudTrail event?

- **Who** made the API call?
- **When** was the API call made?
- **What** was the API call?
- **Which** resources were acted up on in the API call?
- **Where** was the API call made from and made to?

Supported services:

<http://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-supported-services.html>



What does an event look like?

```
{  
  "eventVersion": "1.01",  
  "userIdentity": {  
    "type": "IAMUser", // who?  
    "principalId": "AIDAJDPLRKLG7UEXAMPLE",  
    "arn": "arn:aws:iam::123456789012:user/Alice", //who?  
    "accountId": "123456789012",  
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",  
    "userName": "Alice",  
    "sessionContext": {  
      "attributes": {  
        "mfaAuthenticated": "false",  
        "creationDate": "2014-03-18T14:29:23Z"  
      }  
    }  
  },  
  "eventTime": "2014-03-18T14:30:07Z", //when?  
  "eventSource": "cloudtrail.amazonaws.com",  
  "eventName": "StartLogging", //what?  
  "awsRegion": "us-west-2", //where to?  
  "sourceIPAddress": "72.21.198.64", // where from?  
  "userAgent": "AWSConsole, aws-sdk-java/1.4.5 Linux/x.xx.fleetxen Java_HotSpot(TM)_64-Bit_Server_VM/xx",  
  "requestParameters": {  
    "name": "Default" // which resource?  
  },  
  // more event details  
}
```

AWS CloudTrail Best Practices

AWS CloudTrail Best Practices

1. Enable in all regions

Benefits

- Also tracks unused regions
- Can be done in single configuration step

AWS CloudTrail Best Practices

1. Enable in all regions
2. Enable log file validation

Benefits

- Ensure log file integrity
- Validated log files are invaluable in security and forensic investigations
- Built using industry standard algorithms: SHA-256 for hashing and SHA-256 with RSA for digital signing
- AWS CloudTrail will start delivering digest files on an hourly basis
- Digest files contain hash values of log files delivered and are signed by AWS CloudTrail

AWS CloudTrail Best Practices

1. Enable in all regions
2. Enable log file validation
3. Encrypted logs

Benefits

- By default, AWS CloudTrail encrypts log files using Amazon S3 server side encryption (SSE-S3)
- You can choose to encrypt using AWS Key Management Service (SSE-KMS)
- Amazon S3 will decrypt on your behalf if your credentials have decrypt permissions

AWS CloudTrail Best Practices

1. Enable in all regions
2. Enable log file validation
3. Encrypted logs
4. Integrate with Amazon CloudWatch Logs

Benefits

- Simple search
- Configure alerting on events

AWS CloudTrail Best Practices

1. Enable in all regions
2. Enable log file validation
3. Encrypted logs
4. Integrate with Amazon CloudWatch Logs
5. Centralize logs from all accounts

Benefits

- Configure all accounts to send logs to a central security account
- Reduce risk for log tampering
- Can be combined with Amazon S3 CRR

AWS Technology Partner solutions integrated with CloudTrail



Amazon VPC Flow Logs

Log network traffic for Amazon VPC, subnet or single interfaces

Amazon VPC Flow Logs

- Stores log in AWS CloudWatch Logs
- Can be enabled on
 - Amazon VPC, a subnet, or a network interface
 - Amazon VPC & Subnet enables logging for all interfaces in the VPC/subnet
 - Each network interface has a unique log stream
- Flow logs do not capture real-time log streams for your network interfaces
- Filter desired result based on need
 - All, Reject, Accept
 - Troubleshooting or security related with alerting needs?
 - Think before enabling All on VPC, will you use it?

VPC Flow Logs

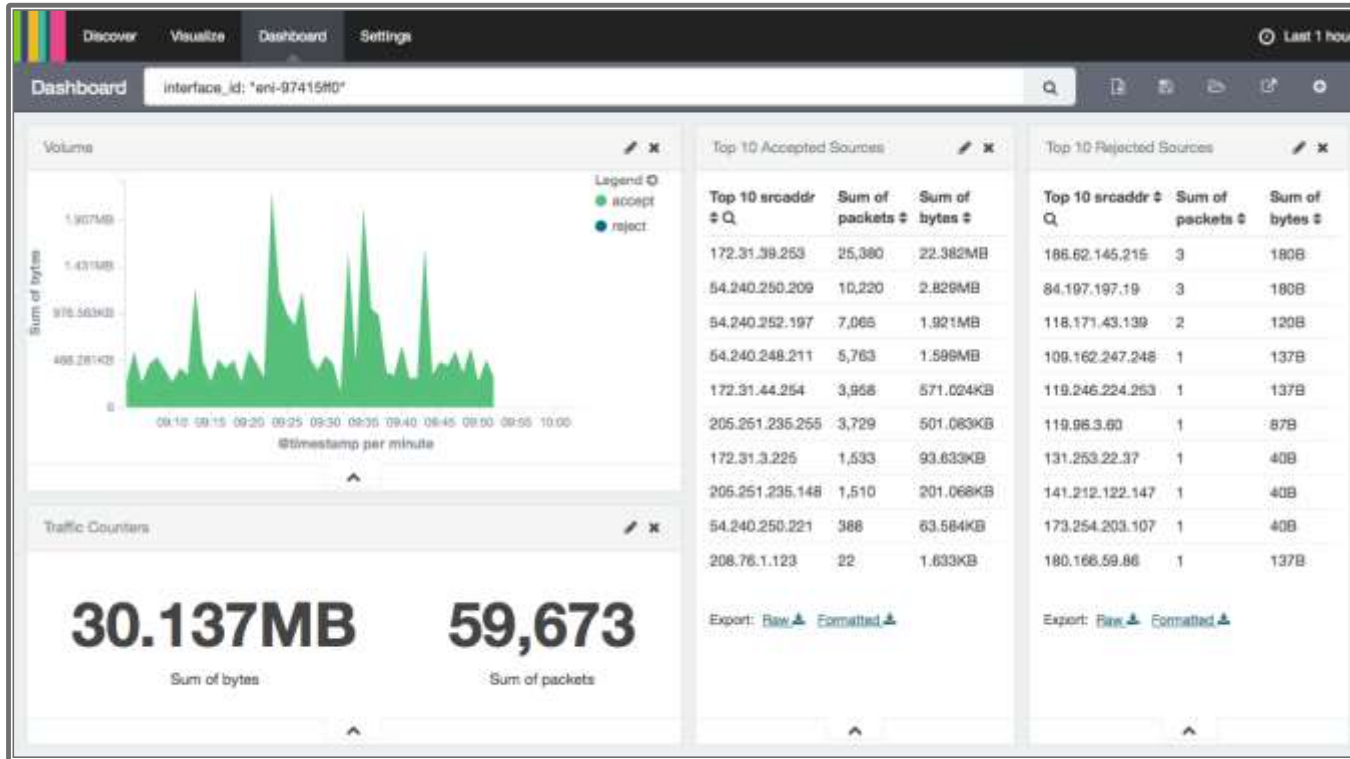
- Agentless
- Enable per ENI, per subnet, or per VPC
- Logged to AWS CloudWatch Logs
- Create CloudWatch metrics from log data
- Alarm on those metrics

Diagram illustrating VPC Flow Logs data structure with annotations:

- Interface**: Points to the ENI ID (eni-b30b9cd5).
- Source IP**: Points to the source IP address (119.147.115.32).
- Source port**: Points to the source port (6000).
- Protocol**: Points to the protocol number (22).
- Packets**: Points to the packet count (6).
- Accept or reject**: Points to the REJECT OK status.
- Destination IP**: Points to the destination IP address (10.1.1.179).
- Destination port**: Points to the destination port (6000).
- Bytes**: Points to the byte count (140).
- Start/end time**: Points to the start and end timestamps (1442975475 and 1442975535).
- AWS account**: Points to the account ID (241747).

Event Data
2 41747 eni-b30b9cd5 119.147.115.32 10.1.1.179 6000 22 6 1 40 1442975475 1442975535 REJECT OK
2 41747 eni-b30b9cd5 169.54.233.117 10.1.1.179 21188 80 6 1 40 1442975535 1442975595 REJECT OK
2 41747 eni-b30b9cd5 212.7.209.6 10.1.1.179 3389 3389 6 1 40 1442975596 1442975655 REJECT OK
2 41747 eni-b30b9cd5 189.134.227.225 10.1.1.179 39664 23 6 2 120 1442975655 1442975716 REJECT OK
2 41747 eni-b30b9cd5 77.85.113.238 10.1.1.179 0 0 1 1 100 1442975656 1442975716 REJECT OK
2 41747 eni-b30b9cd5 10.1.1.179 198.60.73.8 512 123 17 1 76 1442975776 1442975836 ACCEPT OK

VPC Flow Logs



- Amazon Elasticsearch Service
- Amazon CloudWatch Logs subscriptions

Amazon CloudWatch

Monitor Logs from Amazon EC2 Instances in Real-time

Ubiquitous logging and monitoring

Amazon CloudWatch Logs lets you **grab everything** and **monitor activity**

- Managed service to collect and keep your logs
- CloudWatch Logs Agent for Linux and Windows instances
- Integration with **Metrics** and **Alarms**
- Export data to S3 for analytics
- Stream to Amazon ElasticSearch Service or AWS Lambda

CloudWatch Metrics

- Supports custom metrics.
- Memory is a custom parameter
- 5 minute interval by default, 1 minute available with detailed.
- Can be used as a forensics tool because it keeps instance information for 2 weeks.
- Information stored in time series format.
- Provides dashboarding capabilities and an API for extraction.
- Use as a foundational component of auto-scaling.



Managing, Monitoring & Processing Logs

CloudWatch Logs

- Near real-time, aggregate, monitor, store, and search

Amazon Elasticsearch Service Integration (or ELK stack)

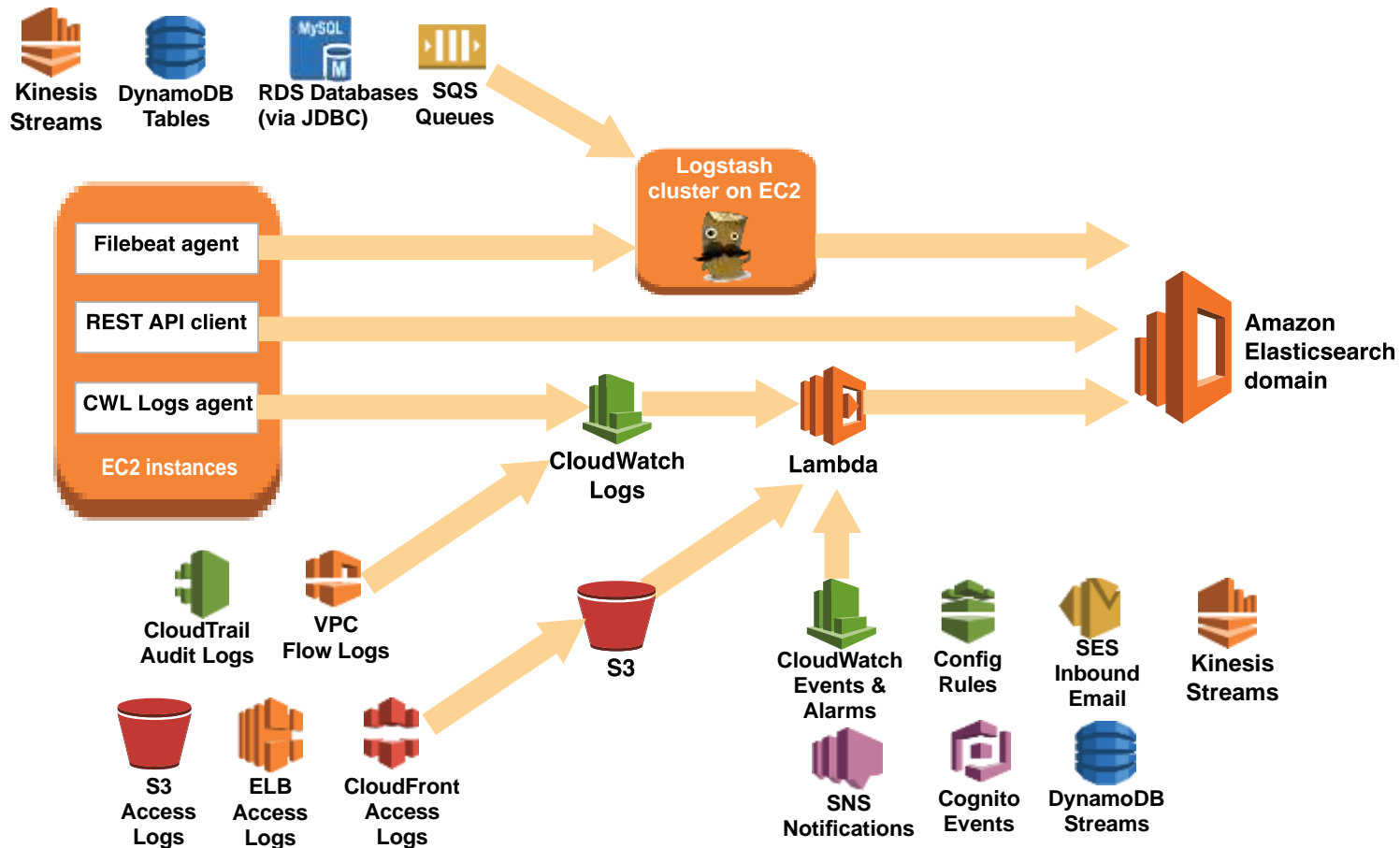
- Analytics and Kibana interface

AWS Lambda & Amazon Kinesis Integration

- Custom processing with your code

Export to S3

- SDK & CLI batch export of logs for analytics



Automating your compliance checks

Multiple levels of automation

Self managed

- AWS CloudTrail -> Amazon CloudWatch Logs -> Amazon CloudWatch Alerts
- AWS CloudTrail -> Amazon SNS -> AWS Lambda

Compliance validation

- AWS Config Rules

Host based Compliance validation

- AWS Inspector

Active Change Remediation

- Amazon CloudWatch Events

AWS Config

Resource and Configuration Tracking

What **Resources** exist?

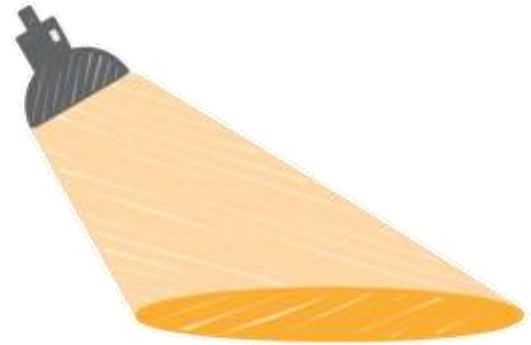
Get inventory of AWS resources

Discover new and deleted resources

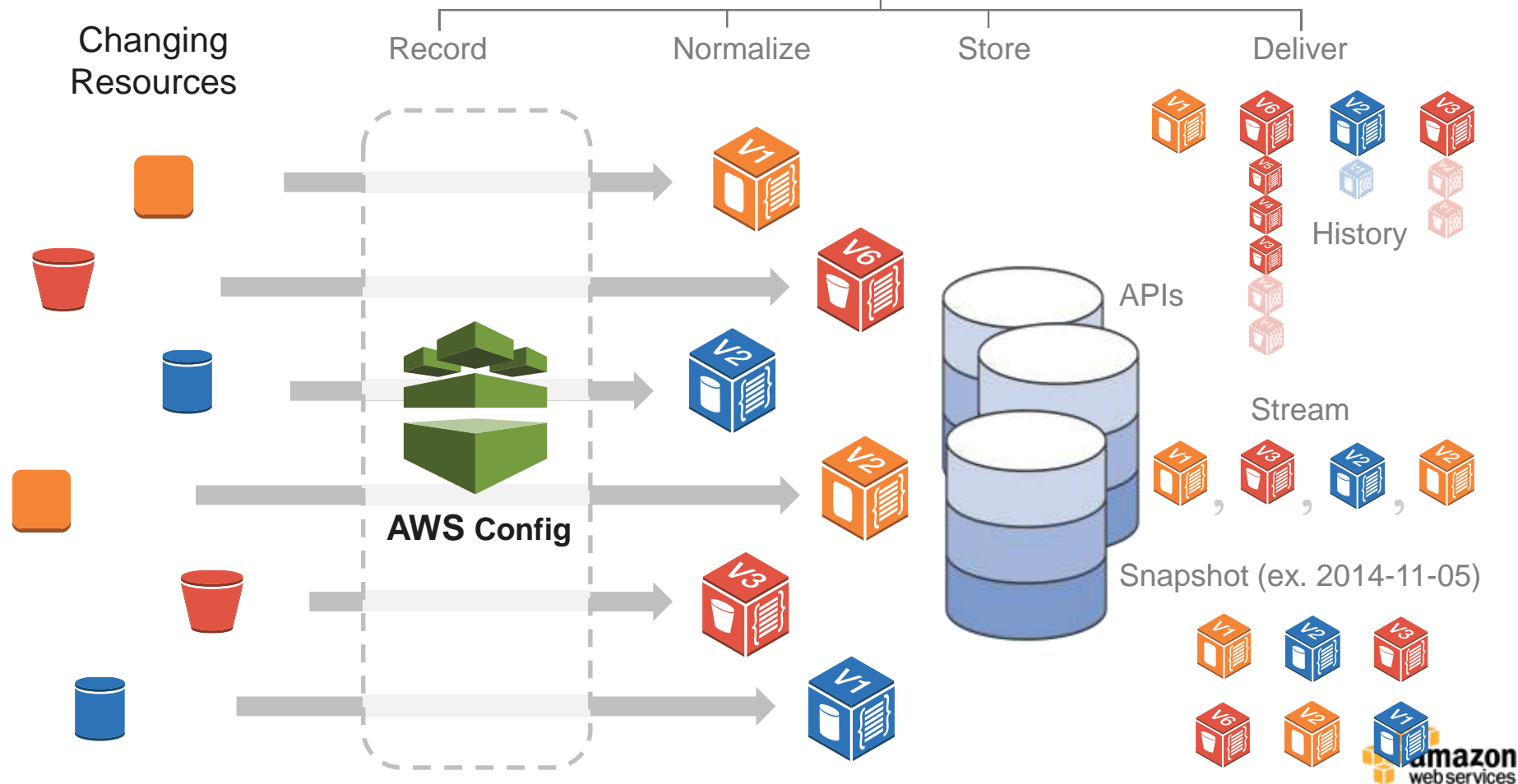
*Record configuration changes
continuously*

Get notified when configurations change

*Know resource relationships
dependencies*



AWS Config



EC2 VPC vpc-3547f950

at September 01, 2015 1:50:07 PM Pacific Daylight Time (UTC-07:00)

Manage Resource



Configuration Details

[View Details](#)

Amazon Resource Name: `arn:aws:ec2:us-east-1:232378813418:vpc/vpc-3547f950`

Resource type: `AWS::EC2::VPC`

Resource ID: `vpc-3547f950`

Availability zone: `Multiple Availability Zones`

Created at: `null`

Tags (0)

Demo:Demo

AWS:ServiceAccount

Name

VPC ID: `vpc-3547f950`

State: `available`

VPC CIDR: `172.16.0.0/16`

DHCP Options Set: `dhcp622a3e00`

Default VPC: `false`

Instance tenancy: `default`

Relationships

Changes (2)

Configuration Changes (0)

Relationship Changes (2)

Field	From	To
AWS::EC2::Instance		"i-L418F1961"
AWS::EC2::NetworkInterface		"eni-ea7810d0"

Evidence for compliance

Many compliance audits require access to the state of your systems at arbitrary times (i.e., PCI, HIPAA).

A complete inventory of all resources and their configuration attributes is available for any point in time.

AWS Config Rules

Automate Response to Changes

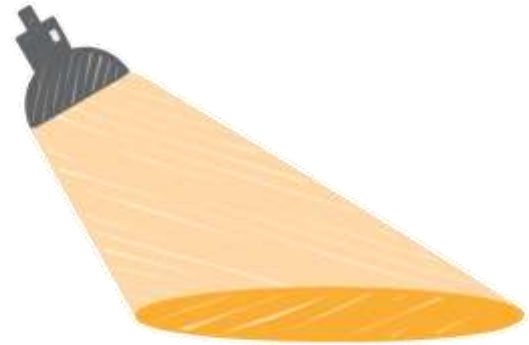
Automated **Response** to Change

Set up rules to check configuration changes recorded

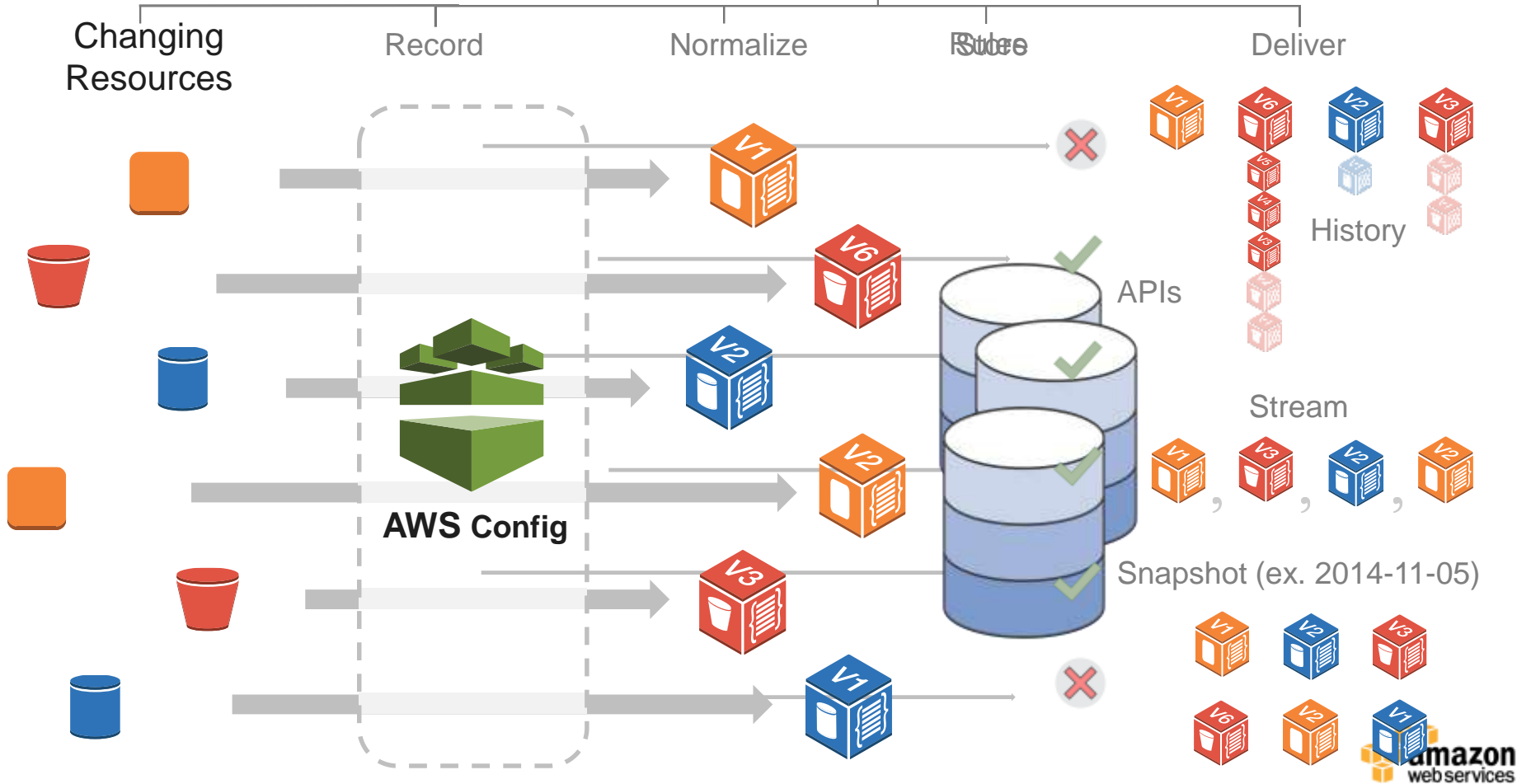
Use pre-built rules provided by AWS

*Author custom rules using AWS Lambda
Invoked automatically for continuous
assessment*

*Use dashboard for visualizing
compliance and identifying changes*



AWS Config & Config Rules



AWS managed rules

1. All EC2 instances must be inside a VPC.
2. All attached EBS volumes must be encrypted, with KMS ID.
3. CloudTrail must be enabled, optionally with S3 bucket, SNS topic and CloudWatch Logs.
4. All security groups in attached state should not have unrestricted access to port 22.
5. All EIPs allocated for use in the VPC are attached to instances.
6. All resources being monitored must be tagged with specified tag keys:values.
7. All security groups in attached state should not have unrestricted access to these specific ports.

AWS Config Rules Repository

AWS Community repository of custom Config rules

<https://github.com/awslabs/aws-config-rules>

Contains Node and Python samples for Custom Rules for AWS Config

AWS CloudWatch Events

The central nervous system for your AWS environment

Tools - Amazon CloudWatch Events

Trigger on event

- Amazon EC2 instance state change notification
- **AWS API call** (*very specific*)
- AWS console sign-in
- **Auto Scaling**

Or Schedule

- **Cron is in the cloud!**
- No more Unreliable Town Clock
- Min 1 min

Single event can have multiple targets

AWS Inspector

Automated security assessment service

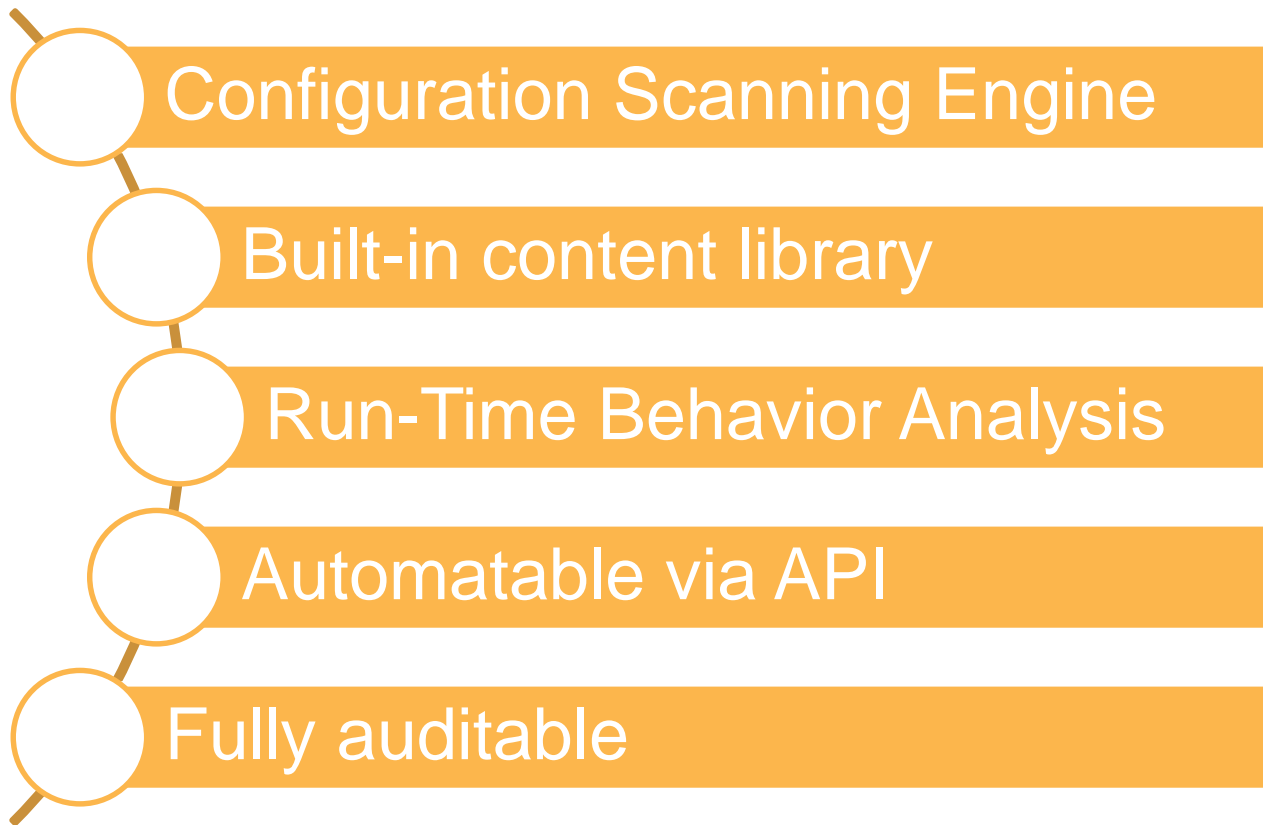
Why Amazon Inspector?

Applications testing key to moving fast but staying safe

Security assessment highly manual, resulting in delays or missed security checks

Valuable security subject matter experts spending too much time on routine security assessment

Amazon Inspector features



Amazon Inspector rulesets



Amazon Inspector benefits



Increased agility



Embedded expertise








Improved security posture



Streamlined compliance

AWS Security tools: What to use?

Service	Type	Use cases
 AWS CloudTrail	Continuous logging	Records AWS API calls for your account and delivers log files to you
 AWS Config Rules	Continuous evaluations	Codified internal best practices, misconfigurations, security vulnerabilities, or actions on changes
 AWS Inspector	On-demand evaluations	Security insights into your application deployments running inside your EC2 instance
 AWS Trusted Advisor	Periodic evaluations	Cost, performance, reliability, and security checks that apply broadly
 CloudWatch Events	Actions in response to APIs and state change	AWS APIs use triggers custom Lambda actions



Services and tools to aid security in the cloud





AWS Security and Compliance

Security of the cloud





Don't forget built-in reporting

AWS Trusted Advisor checks your account





Recommended Actions

- **Security Groups - Specific Ports Unrestricted**Updated: 9/29/14 7:19 AM





Checks security groups for rules that allow unrestricted access (0.0.0.0/0) to specific ports.

2 of 71 security group rules allow unrestricted access to a specific port.
- **IAM Use**Updated: 9/17/14 12:39 PM

Checks for your use of AWS Identity and Access Management (IAM).

At least one IAM user, group, or role has been created for this account.
- **MFA on Root Account**Updated: 9/17/14 12:39 PM

Checks the root account and warns if multi-factor authentication (MFA) is not enabled.

MFA is enabled on the root account.
- **Service Limits**Updated: 9/17/14 12:39 PM

Checks for usage that is more than 80% of the service limit.

0 of 42 items have usage that is more than 80% of the service limit.

Security



2 1 0

IAM Credential Reports

Dashboard

Details

Groups

Users

Roles

Identity Providers

Password Policy

Credential Report

Credential Report

Click the button to download a report that lists all your account's users and the status of their various credentials. After a report is created, it is stored for up to four hours. For more information see the [documentation](#).

Download Report

user	arn	user_created	password	password_last_used	password_expiration	password_reset_required	mfa_active
<root_account>	arn:aws:iam::111111111111:root	2014-06-01T00:00:00Z	not_supported	2014-11-05T23:02:18+00:00	not_supported	not_supported	TRUE
amacdermott	arn:aws:iam::111111111111:user:amacdermott	2014-08-14T00:00:00Z	TRUE	no_information	2014-09-21T00:00:00Z	2014-11-11T00:00:00Z	FALSE
cwhalley	arn:aws:iam::111111111111:user:cwhalley	2014-08-14T00:00:00Z	TRUE	no_information	2014-08-14T00:00:00Z	2014-10-01T00:00:00Z	FALSE
gilec	arn:aws:iam::111111111111:user:gilec	2014-06-11T00:00:00Z	TRUE	no_information	2014-09-21T00:00:00Z	2014-11-11T00:00:00Z	FALSE
lford	arn:aws:iam::111111111111:user:lford	2014-08-14T00:00:00Z	TRUE	no_information	2014-09-21T00:00:00Z	2014-11-11T00:00:00Z	FALSE
llegal	arn:aws:iam::111111111111:user:llegal	2014-08-14T00:00:00Z	TRUE	no_information	2014-09-21T00:00:00Z	2014-11-11T00:00:00Z	FALSE
mbretan	arn:aws:iam::111111111111:user:mbretan	2014-10-14T00:00:00Z	TRUE	2014-10-22T17:27:25+00:00	2014-10-14T00:00:00Z	2014-12-01T00:00:00Z	FALSE
mhaddox	arn:aws:iam::111111111111:user:mhaddox	2014-08-14T00:00:00Z	TRUE	no_information	2014-09-21T00:00:00Z	2014-11-11T00:00:00Z	FALSE
pmalhotra	arn:aws:iam::111111111111:user:pmalhotra	2014-08-14T00:00:00Z	TRUE	no_information	2014-09-21T00:00:00Z	2014-11-11T00:00:00Z	FALSE
rdevinen	arn:aws:iam::111111111111:user:rdevinen	2014-09-11T00:00:00Z	TRUE	no_information	2014-09-21T00:00:00Z	2014-11-11T00:00:00Z	FALSE
rlavadia	arn:aws:iam::111111111111:user:rlavadia	2014-08-14T00:00:00Z	TRUE	no_information	2014-09-21T00:00:00Z	2014-10-30T00:00:00Z	FALSE
sandaget	arn:aws:iam::111111111111:user:sandaget	2014-06-11T00:00:00Z	TRUE	no_information	2014-10-01T00:00:00Z	2014-11-21T00:00:00Z	TRUE
sduffer	arn:aws:iam::111111111111:user:sduffer	2014-08-14T00:00:00Z	TRUE	no_information	2014-09-21T00:00:00Z	2014-11-11T00:00:00Z	FALSE
stwaddle	arn:aws:iam::111111111111:user:stwaddle	2014-08-14T00:00:00Z	TRUE	no_information	2014-09-21T00:00:00Z	2014-11-11T00:00:00Z	FALSE
ttstrobell	arn:aws:iam::111111111111:user:ttstrobell	2014-08-14T00:00:00Z	TRUE	no_information	2014-09-21T00:00:00Z	2014-11-11T00:00:00Z	FALSE
woolfc	arn:aws:iam::111111111111:user:woolfc	2014-06-11T00:00:00Z	TRUE	2014-11-05T23:20:03+00:00	2014-11-01T00:00:00Z	2014-12-21T00:00:00Z	FALSE
zfatemi	arn:aws:iam::111111111111:user:zfatemi	2014-08-14T00:00:00Z	TRUE	no_information	2014-09-21T00:00:00Z	2014-11-11T00:00:00Z	FALSE

Rounding up

- Leverage built-in tools for monitoring and compliance
- Storage is cheap, not knowing can be very expensive – Log if possible
- Alerting is good, automating your security response is better
- Use managed services and built-in reporting to offload and automate
- See the Big Picture, what info do you want and what tool can give it to you

AWS Services

- CloudWatch – Events, Logs, Metrics
- VPC Flow Logs
- CloudTrail
- Config & Config Rules
- Inspector
- Trusted Advisor
- IAM – credential report & policy simulator
- Indirect tools – Elasticsearch, S3, Kinesis.

Move
Fast

AND

Stay
Secure