Security Change through Feedback @ Riot
MORE THAN 100 MILLION
MONTHLY ACTIVE PLAYERS

MORE THAN 27 MILLION
DAILY ACTIVE PLAYERS

7.5 MILLION
PEAK CONCURRENT PLAYERS
Who Are We?

Our Mission

We aspire to be the most player-focused game company in the world.
<table>
<thead>
<tr>
<th>Item Name</th>
<th>Technology</th>
<th>Account</th>
<th>Account Type</th>
<th>Region</th>
<th>Issue</th>
<th>Notes</th>
<th>Score</th>
<th>Justification</th>
</tr>
</thead>
<tbody>
<tr>
<td>rconsole-stage-SecondaryReplicaNode11NodeSecurityGroup-</td>
<td>securitygroup</td>
<td></td>
<td>AWS</td>
<td>us-west-2</td>
<td>Security Group ingress rule contains 0.0.0.0/0 on tcp 22</td>
<td>10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>L754615T3478 (sg-9c1... in vpc-42)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>esports-iphide (sg-b8... in vpc-0c)</td>
<td>securitygroup</td>
<td></td>
<td>AWS</td>
<td>us-west-2</td>
<td>Security Group ingress rule contains 0.0.0.0/0 on tcp 22</td>
<td>10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(sg-6b... in vpc-3b)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>awseb-e-ptqmmsbn2x-stack-AWSEBSecurityGroup-VW4W2G5899X9</td>
<td>securitygroup</td>
<td></td>
<td>AWS</td>
<td>us-west-2</td>
<td>Security Group ingress rule contains 0.0.0.0/0 on tcp 22</td>
<td>10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(sg-9e... in vpc-6a)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>canvasflow-mdb (sg-5b... in vpc-6a)</td>
<td>securitygroup</td>
<td></td>
<td>AWS</td>
<td>us-west-2</td>
<td>Security Group ingress rule contains 0.0.0.0/0 on tcp 27017</td>
<td>10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(sg-9a... in vpc-6a)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>merch_health_service (sg-98... in vpc-95)</td>
<td>securitygroup</td>
<td></td>
<td>AWS</td>
<td>ap-northeast-1</td>
<td>Security Group ingress rule contains 0.0.0.0/0 on tcp 22</td>
<td>10</td>
<td></td>
<td></td>
</tr>
<tr>
<td># esports-iphide (sg-b8... in vpc-0c)</td>
<td>securitygroup</td>
<td></td>
<td>AWS</td>
<td>us-west-2</td>
<td>Security Group ingress rule contains 0.0.0.0/0 on tcp 22</td>
<td>10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(sg-6b... in vpc-3b)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Hello Team,

Details:
Would like to report you about disclosure API key that I have found at one of your public Git repositories.

3 days ago m hillick published **aws_access_key** and **aws_access_key**

Impact:
As you probably know, its sensitive information that should be removed. Secret access keys are - as the name implies - secrets, like your password. For your own security, AWS doesn’t reveal your password to you if you forgot it (you’d have to set a new password). Similarly, AWS does not allow retrieval of a secret access key after its initial creation. This applies to both root secret access keys and AWS Identity and Access Management (IAM) user secret access keys.
Shared Accounts

- Tragedy of the commons
- Service/resource limits
- No isolation
If security introduces blocking to the org, it will be ignored, not embraced
Problem Statement

While AWS is a great place to rapidly iterate and test new features, the vast number of accounts, instances and usage has no easy way of attributing a running instance back to an owner or feature.
Why :: Incident Response is hard when you don’t know who owns what

Why :: If you don’t need it, why is it running?

What :: Tagging is incredibly easy to use to identify ownership
Configuration as code

Able to ship quickly

Contains the IAM policies used with our AWS accounts to grant people the required access

- 113 commits
- 8 branches
- 0 releases
- 8 contributors

- roles: reformatted using 4 space indent
- tests: Modifying Root Dir
- .gitignore: Writing semi-explicit policy that confirm with length limit
- README.md: Modifying readme and better logging for length_check
- Riot_Admin.json
- Riot_InfoSec_Audit.json: Allow inquisitor to update trust policy documents for roles
- Riot_NetEng.json: Adding AWS Glue
- Riot_PowerUser.json: Adding AWS Glue
- Riot_ReadOnly.json: Adding AWS Glue
- Riot_SecurityMonkey.json: Adding samlprovider permissions
- Riot_StandardUser.json: Adding AWS Glue
- Riot_SuperAdmin.json: Adding SuperAdmin role
- Riot_SysEng.json: Adding AWS Glue

Deployment Quick-Reference

Default AWS access policies and roles are automatically created and updated for accounts configured for auditing via our AwsAudits deployment.
Change by Tools

**AWS:** KMS, IAM, ACM, STS, CloudTrail, CloudWatch, VPC Flowlogs, GuardDuty

**EXTERNAL:** Security Monkey, Terraform, Packer, Elasticsearch/Kibana

**RIOT-DEVELOPED:** AWSKey (Temporal Keys), Cloud Inquisitor
RFCs=Tech Design
Not an approval process, it’s about receiving advice!

Received comments & iterate through the draft

Becomes a standard through adoption @ scopes
RFCs that we’ve written:

- **AWS Standards and Best Practices**
- **Securing AWS environments and their Applications**
- **Securing AWS data at rest**
- **Minimising local AWS accounts**
- **AWS Ownership Attribution**
Note: RFC 0026-v2 - AWS Ownership and Cost Attribution has been proposed as a successor for this RFC.

Problem Statement

While AWS is a great place to rapidly iterate and test new features the vast number of accounts, instances and usage has no easy way of attributing a running instance back to an owner or feature. Especially for accounting and projecting of costs this is causing a lot of extra work and uncertainty, as well as not providing teams visibility into the commitments they make in the name of the company, something crucially needed in order to achieve total ownership.

Version History / Status

<table>
<thead>
<tr>
<th>Date</th>
<th>Version</th>
<th>Updated By</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>2013-03-06</td>
<td>1.1</td>
<td>Ramil Lim</td>
<td>Original rfc, orphaned.</td>
</tr>
<tr>
<td>2014-10-08</td>
<td>1.2</td>
<td>Felix Nenz</td>
<td>Taking over this orphaned RFC to extend it to cover ownership entirely.</td>
</tr>
<tr>
<td>2015-02-12</td>
<td>1.3</td>
<td>Felix Nenz</td>
<td>Integrating feedback. Changing per project codes to per initiative, adding of ContactEmail tag.</td>
</tr>
<tr>
<td>2015-03-12</td>
<td>1.4</td>
<td>Felix Nenz</td>
<td>Added how to adopt section.</td>
</tr>
<tr>
<td>2015-03-17</td>
<td>1.5</td>
<td>Felix Nenz</td>
<td>Updated the proposal with some final edits, moving into a new document to reset discussion. ContactEmail is now owner.</td>
</tr>
<tr>
<td>2016-01-27</td>
<td>1.6</td>
<td>Marty Chong</td>
<td>Updated the COA to reflect current accounting codes.</td>
</tr>
<tr>
<td>2016-02-03</td>
<td>1.7</td>
<td>Marty Chong</td>
<td>Modified the code section to reflect current tagging standards...removed roll-up sheet as wasn't being used.</td>
</tr>
<tr>
<td>2016-03-31</td>
<td>1.8</td>
<td>Marty Chong</td>
<td>Updated the tagging standards.</td>
</tr>
<tr>
<td>2016-09-22</td>
<td>1.9</td>
<td>Asbjorn Kjaer</td>
<td>Removed the Chart of Accounts section, as its no longer applicable.</td>
</tr>
<tr>
<td>2016-11-12</td>
<td>1.10</td>
<td>Asbjorn Kjaer</td>
<td>Added link to RFC 0026a - Enforcement Implementation of Tag Detection in AWS(v1).</td>
</tr>
<tr>
<td>2017-02-07</td>
<td>1.11</td>
<td>Mark Hillick</td>
<td>Added snippet from RFC 0026a - Enforcement Implementation of Tag Detection in AWS(v1) for more context in Enforcement section.</td>
</tr>
</tbody>
</table>

Stakeholders

Click here to expand...

Analysis

As part of the AWS working group in collaboration with Amazon we investigated the attribution challenge. We believe that using tags within AWS is the best approach to make this better. We are extending the existing usage of tags for instances and other resources so that we can attribute cost back to an initiative. Using the Accounting tag, we provide visibility for finance into the actual spend, allowing them to allocate cost back to products.
Solution

Shrink the change => No decision paralysis

Feedback & moved to the adoption stage

Standard across Riot
Tagging Details

**Required Tags ::** Name, Owner & Accounting

**Schedule**

- At 0, 21 and 27 days => Notify Gatekeeper and owner (if possible)
- At 4 weeks => Shutdown Instance
- At 12 weeks => Terminate Instance
Cloud Inquisitor moves from ideation to implementation

Let’s go write some code
Cloud Inquisitor moved from notification into shutdown *murdering* mode.

**Clubs outage Oct 2016 -- November Update!**

*Riot martlet (NA) submitted 12 months ago in Miscellaneous*

**UPDATE 11/1**

We know some of you are seeing continued issues with club membership and tags. Currently, we are tracking down 2 main issues:

- Some owners not being able to see the club they own
- Clubs appear as not having any owner

Once we get some further info, we'll make sure to update everyone!
FYI. we're getting a list of teams which could have been affected by this and going to have those teams proactively brought online to check their stuff.

@jbrewer with the tool disabled, would you like someone from InfoSec to hang around?

I think we're good from that point.

Okay, I've sent a note to infosec as a fyi.

We have visibility into AWS land, so it's just a matter of pulling team names and cross referencing with service registry.

I suspect it's not 100% accurate with regard to AWS.

Agree.
Joe Santos: 23:05
@mhillick, can you provide time the bot ran so I have a more accurate time when things started to get affected?

Mark Hillick: 23:11
@jsantos 1 sec

Mark Hillick: 23:12
@mhillick looks like my autoscaling group had the right tags: https://us-west-2.console.aws.amazon.com/ec2/autoscaling/home?region=us-west-2#AutoScalingGroups:id=+globalriot.uswest2infra1;view=tags;filter=infra1
but the instances were killed anyway?

Mark Hillick: 23:12
I just added them @ploy
ROD DICKERSON 22:47
I feel pretty strongly that stopping a service for this reason is never correct (not just because it's Friday). I think it would be good to make sure that viewpoint has a champion at the high level.

MARK HILLICK 22:48
@rdickerson makes sense and I can understand that, this is the first time we've been given that feedback despite our previous comms. This makes me think that our previous comms were not clear enough or understood.

McDONALD RICHARDS 22:48
I think you underestimate our orphaned instances
Feels bad & yes, we received a lot of feedback

But we still work at Riot

Open & transparent Root Cause Analysis (RCA)
“By doing a RCA, the team has truly showed themselves to be part of Engineering. We all make mistakes - this is how we learn and improve. /fistbump ”

Cam Dunn (Tech Director), Dec. 2016
Our communications & planning sucked

Confusion around RFC Adoption & lack of clarity on aspects of the RFC

Our notification code had bugs
Improved UX, error-handling & new functionality

Manual checking of instances for important products

Over-Indexing on communication & lots of checks on alignment
2nd Adoption, Yay!

bcc Engineering

“Thanks for everyone's input and consideration for RFC0026, aka MurderBot, over the last several weeks. This is now adopted at Riot scope.”

Mike Seavers (Director of Engineering), Feb. 2017
Cinq Features

Removes incorrectly tagged & un-owned AWS objects

Checks that security features are turned on throughout our AWS Infra

DNS hijacking & IAM policy management
IAM Role called 'cinq_role' configured with policy that trusts AWS Instance Profile from cinq AWS Account
Cinq Tech

Back-End :: Modular framework (Py 3.5+), Flask, SQL Alchemy & MySQL

Front-End :: AngularJS on Nginx

Deployment :: Packer & Docker (dev only)
### Auditor: CloudTrail (auditor_cloudtrail)

<table>
<thead>
<tr>
<th>Key</th>
<th>Type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>bucket_account</td>
<td>string</td>
<td></td>
</tr>
<tr>
<td>bucket_name</td>
<td>string</td>
<td></td>
</tr>
<tr>
<td>bucket_region</td>
<td>string</td>
<td>us-west-2</td>
</tr>
<tr>
<td>enabled</td>
<td>bool</td>
<td>Disabled</td>
</tr>
<tr>
<td>global_events_region</td>
<td>string</td>
<td>us-west-2</td>
</tr>
<tr>
<td>interval</td>
<td>int</td>
<td>60</td>
</tr>
<tr>
<td>sns_topic_name</td>
<td>string</td>
<td>cloudtrail-log-notification</td>
</tr>
<tr>
<td>sqs_queue_account</td>
<td>string</td>
<td></td>
</tr>
<tr>
<td>sqs_queue_name</td>
<td>string</td>
<td></td>
</tr>
<tr>
<td>sqs_queue_region</td>
<td>string</td>
<td>us-west-2</td>
</tr>
</tbody>
</table>

### Auditor: Domain Hijacking (auditor_domain_hijack)

<table>
<thead>
<tr>
<th>Key</th>
<th>Type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>email_recipients</td>
<td>array</td>
<td></td>
</tr>
<tr>
<td>enabled</td>
<td>bool</td>
<td>Disabled</td>
</tr>
<tr>
<td>interval</td>
<td>int</td>
<td>20</td>
</tr>
</tbody>
</table>
The following instances are not compliant with the RFC-0026 tagging standards. This information is also available on demand by going to the AWS Audit Tool.

Instances that are not tagged appropriately within a month of being detected as non-compliant will be shutdown automatically until tags have been added. To prevent this from happening have the owners of the instances to tag their assets correctly.

**Issues**

<table>
<thead>
<tr>
<th>Instance</th>
<th>Account</th>
<th>Region</th>
<th>Missing tags</th>
<th>Notes</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packer Builder (-07412...)</td>
<td></td>
<td>us-west-2</td>
<td>owner, accounting</td>
<td>No Notes</td>
<td>Stopped, delete in 12 weeks</td>
</tr>
</tbody>
</table>

You received this message because you are subscribed to the Google Groups "[redacted]" group. To unsubscribe from this group and stop receiving emails from it, send an email to [redacted]. To post to this group, send email to [redacted]. To view this discussion on the web visit [redacted].
<table>
<thead>
<tr>
<th>Instance</th>
<th>Account</th>
<th>Region</th>
<th>Missing Tags</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>eu-west-1</td>
<td>Owner, Name, Accounting</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td></td>
<td>us-west-2</td>
<td>Owner, Name, Accounting</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td></td>
<td>us-west-2</td>
<td>Owner, Name, Accounting</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td></td>
<td>eu-west-1</td>
<td>Owner, Name, Accounting</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td></td>
<td>us-west-2</td>
<td>Owner, Name, Accounting</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td></td>
<td>us-west-2</td>
<td>Owner, Name, Accounting</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td></td>
<td>us-west-2</td>
<td>Owner, Name, Accounting</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td></td>
<td>us-west-2</td>
<td>Owner, Name, Accounting</td>
<td>None</td>
</tr>
</tbody>
</table>
Problem :: Left in the corner  
Solution :: Build relationships, get alignment & iterate

Problem :: Silver bullet?  
Solution :: Best ⚒ for the job, i.e. solve the specific problem

Problem :: Boil The Ocean  
Solution :: Shrink the change – biggest impact, lowest effort possible
OSS

Repo :: https://github.com/RiotGames/cloud-inquisitor

Collaboration :: Slack, GitHub Issues

Contributions Welcome :: Roadmap, Ideas & Pull Requests
Futures

All Taggable AWS Objects (revised RFCs) - Implementation

EBS Snapshots, S3, AMIs & AWS Organizations compatibility

GDPR Auditor
Minimize the use of local, long-lived AWS IAM Keys

Provides temporary AWS API tokens (via STS) & activity monitoring

Reduce impact of an API Key Compromise
 AWSKey Unique User Count

47
Unique Users

AWSKey Keys Generated

436
Keys Generated

AWSKey Total

1,977
Total Logs

AWSKey Unique Users per Week

@timestamp per week

AWSKey Key Created

AWSKey Started

AWSKey Bad Requests

AWSKey Bad Requests
Thank You