



The logo for AWS re:Invent features the AWS monogram in white on the left, followed by the word "re:Invent" in a large, white, sans-serif font.

CTD15

How Rovio Uses Amazon CloudFront for Secure API Acceleration

Mika Linnanoja
Senior Cloud Engineer
Rovio Entertainment Corporation

AWS
re:Invent

© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Agenda

- Me & Rovio
- What we had
- Why do this?
- Solution
- Challenges and findings
- Results
- Q & A

Me & Rovio

- 12 years in ICT
- Background in QA, releasing, **Continuous Integration**
- Keep Rovio Games cloud services platform up and running **24x7x365**



Rovio

- Games first entertainment company
- **Angry Birds**
- Founded 2003 in Finland 
- ~400 employees in FI, SWE, UK, US & CN



What we had

- Fully cloud native REST API based server infrastructure on AWS EC2 accessed by all Rovio games from all around the globe
- ~1000 instances altogether
- Single public endpoint URL with 3rd party Load Balancer & Proxy, other instances in private subnets
- DNS pointing directly to Elastic IPs of LB cluster instances, external health monitoring

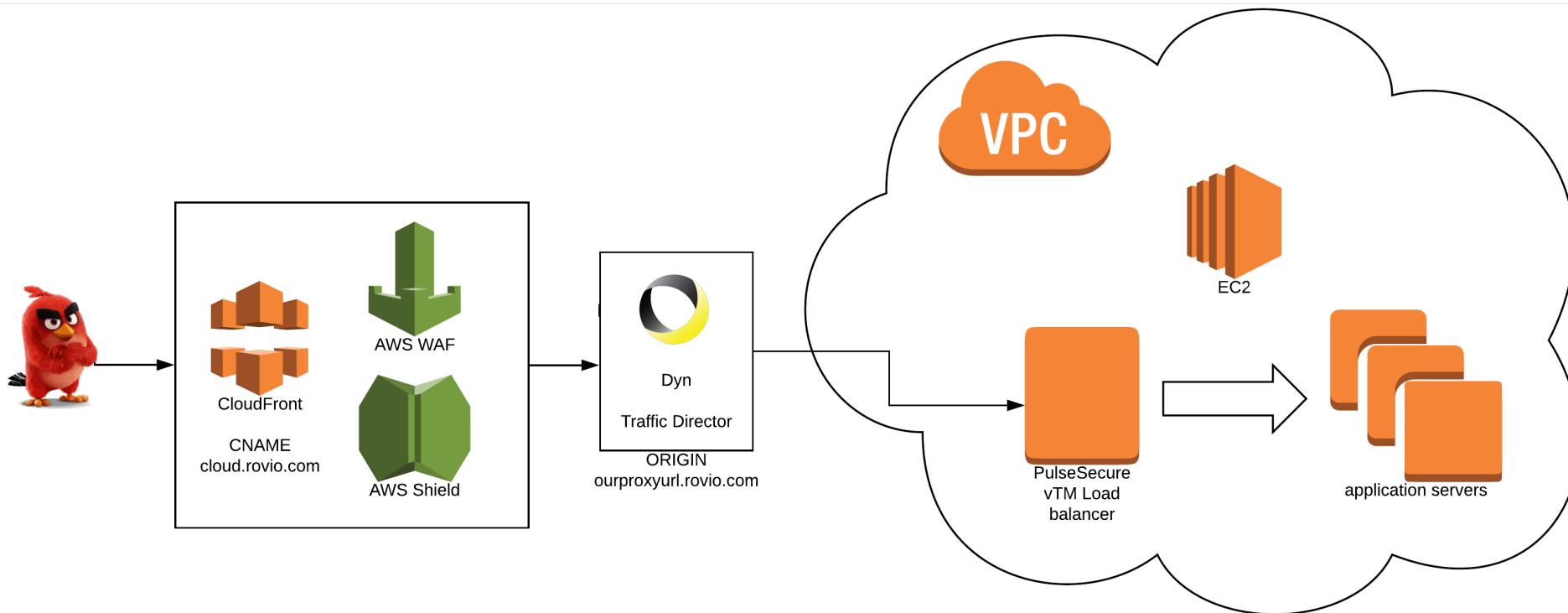
Why do this?

- What if somebody decides to attack our platform?
- No way to **mitigate** any kind of **distributed denial of service** attack
- **Cannot scale** LB cluster endlessly. License limit in max bandwidth & database considerations
- Worst case: Complete **loss of business**, no in-app purchases nor ads in any game
- We have been ***extremely* lucky**

Solution: AWS edge services

- Talk with our AWS Solutions Architect => How about you try **CloudFront** CDN + AWS **Shield** Advanced + **WAF**?
- Benefits not just DDoS mitigation (Which we sold this to our management team):
 - Strong **DDoS protection** on 1st connection point outside our VPC
 - **Reduced latencies** in API usage i.e. acceleration
 - Possible cost savings due to **caching** of some responses and reduced data transfers
 - Future proofing our stack: **HTTP/2** + **IPv6** out of the box

Solution: What



Solution: How

- New CloudFront **distribution**. Tech known due to earlier use as static media CDN
- Control **DNS** for origin server (A records)
- Figure out optimal CloudFront settings for **dynamic API calls**
- Enable **AWS Shield & WAF Web ACL** to protect and **filter** unwanted **accesses**
- Remove extra traffic filtering and access control from existing load balancer
- A **way to roll back** quickly in case of unforeseen consequences

Challenges and findings

- In production use since February 2018 – going strong!
- No game to server e2e **latency** and connection quality **measurements** in place (yet)
- Think of **gradual rollout** - per game, region or client application
- Adding in effect another **proxy in front of our existing proxy** brought light to a HTTP 100 Continue bug => hotfix for load balancer
- **Pricing** model with high request rates and volumes
- Latency improvements are real for us based on our testing scenario

Latency measurements

```
$ ./pingtestanalyzer.py
HTTP GET mean latencies from [ EU Ireland (eu-west-1) ]
- smoke.rovio.com (Via CloudFront)
274.1 ms [50249 tests]
- <ORIGINURL>.rovio.com (Direct)
508.1 ms [49159 tests]

HTTP GET mean latencies from [ US North Virginia (us-east-1) ]
- smoke.rovio.com (Via CloudFront)
147.6 ms [50870 tests]
- <ORIGINURL>.rovio.com (Direct)
101.9 ms [51106 tests]

HTTP GET mean latencies from [ US Oregon (us-west-2) ]
- smoke.rovio.com (Via CloudFront)
323.1 ms [49950 tests]
- <ORIGINURL>.rovio.com (Direct)
514.2 ms [49099 tests]

HTTP GET mean latencies from [ ASIA Singapore (ap-southeast-1) ]
- smoke.rovio.com (Via CloudFront)
558.9 ms [48877 tests]
- <ORIGINURL>.rovio.com (Direct)
1316.6 ms [45607 tests]

HTTP GET mean latencies from [ SOUTH AMERICA Sao Paulo (sa-east-1) ]
- smoke.rovio.com (Via CloudFront)
511.4 ms [49084 tests]
- <ORIGINURL>.rovio.com (Direct)
764.2 ms [47931 tests]
```

- EU Ireland (eu-west-1):
46% decrease
 - US East (us-east-1, same datacenter):
45% increase
 - US West us-west-2:
37% decrease
 - Asia Singapore ap-southeast-1:
58% decrease
 - South America sa-east-1:
33% decrease
- => Globally helps significantly

Q & A – Ask me anything

Extra Materials for Q & A

Mandate to improve our platform

- Technology choices and **implementation** of the low level infra fully **in team hands**
- Possible extra costs involved => **Buy-in** from mgmt and technology organization: **DDoS protection!**
- "Do whatever you want to as long as **uptime** stays at 99.99 %"

QA for CloudFront distribution

- Rigorous testing using all available test automata in our CI & CD system, thousands of testcases
- cURL/httpie became our best friends – service testing endpoint that returns received HTTP headers is nice
- Custom game build that connects to new endpoint from our service platform SDK
- Dummy user testing using subcontractor

Testing tools: stats

```
$ httpstat --http1.1 https://smoke.rovio.com/adsdepot/1/tests/headers
Connected to 54.192.97.35:443 from 192.168.250.2:50759

HTTP/1.1 200 OK
Content-Type: application/json; charset=utf-8
Content-Length: 435
Connection: keep-alive
Date: Tue, 09 Oct 2018 11:15:18 GMT
Request-Id: 6357629814916248092
X-Cache: Miss from cloudfront
Via: 1.1 f9a0ddc3860252ab6c4d02ab024b4891.cloudfront.net (CloudFront)
X-Amz-Cf-Id: Iof8jAqRQGMmECs4C9SS8M19c9UUC0jIC7pfsiW3ZpS3SYhH2kGgSQ==

Body stored in: /var/folders/6l/22zs2p7d6j31y812024wr2b00000gp/T/tmpRtm083

      DNS  Lookup    TCP Connection    Server Processing    Content Transfer
[      5ms     |      21ms     |      128ms     |      1ms      ]
                  |                  |                  |
namelookup: 5ms          |                  |                  |
                           connect: 26ms   |                  |
                                         starttransfer: 218ms |
                                         total: 219ms
```

httpstat

Testing tools: headers

```
$ http https://smoke.rovio.com/adsdepot/1/tests/headers
HTTP/1.1 200 OK
Connection: keep-alive
Content-Length: 470
Content-Type: application/json; charset=utf-8
Date: Tue, 09 Oct 2018 11:16:43 GMT
Request-Id: 1575855414616325623
Via: 1.1 b475a5f7d95ff68ca0dc588e3c9a3231.cloudfront.net (CloudFront)
X-Amz-Cf-Id: VQoA8i_G3wuD_T0s8TlgAvkGz-aR01BRXPB_Dgw_9PuSShXx2IRAMg==
X-Cache: Miss from cloudfront

{
  "bodyForm": null,
  "headers": {
    "Accept": "*/*",
    "Accept-Encoding": "gzip, deflate",
    "Connection": "keep-alive",
    "Host": "smoke.rovio.com",
    "User-Agent": "HTTPPie/0.9.9",
    "X-Cluster-Client-Ip": "205.251.218.157",
    "X-Forwarded-For": "[REDACTED], 205.251.218.157",
    "X-GeoIP-City-Name": "Helsinki",
    "X-GeoIP-City-Name-Base64": "SGVsc2luq2k=",
    "X-GeoIP-Country-Code": "FI",
    "X-GeoIP-Country-Name": "Finland",
    "X-GeoIP-State-Code": "13",
    "X-Is-Hsts": "true",
    "X-Real-IP": "[REDACTED]"
  },
  "parameters": []
}
```

httpie client

API Acceleration details

- In theory: CloudFront keeps connections alive towards Origin server if connections from each PoP more frequent than **HTTP Keep-Alive**
=> in a high volume global users scenario **savings** in e.g. TLS negotiation
- Extra tidbit: Due to Keep-Alive **memory** and **CPU utilization** at EC2 load balancer solution **dropped** very significantly
=> smaller instances OK
- Works for our case: lots of **small payload HTTP requests (JSON)**, no binary data e.g. image uploads/downloads via APIs

Technical Setup: CF

The screenshot shows the AWS CloudFront Distributions page for a specific distribution. The navigation bar includes links for AWS Services, Resource Groups, EC2, IAM, RDS, VPC, S3, and a user 'smoke'. The left sidebar has sections for Distributions, What's New, Reports & Analytics, Security, and various monitoring and usage metrics. The main content area displays the distribution details for 'E2FJMRSIVO0MCB'.

General Tab (Selected)

Distribution ID	E2FJMRSIVO0MCB
ARN	arn:aws:cloudfront:::distribution/E2FJMRSIVO0MCB
Log Prefix	-
Delivery Method	Web
Cookie Logging	Off
Distribution Status	Deployed
Comment	proxy-dev, CDN for smoke stingray
Price Class	Use All Edge Locations (Best Performance)
AWS WAF Web ACL	smoke-test-rules-for-cloudfront
State	Enabled

Alternate Domain Names (CNAMEs)

- st.rovio.com
- .rovio.com
- dev.rovio.com
- g-dev.rovio.com
- dev.rovio.com
- dev.rovio.com
- v.rovio.com
- uiui-dev.rovio.com
- uiui-dev.rovio.com
- ev.rovio.com
- av.rovio.com

SSL Certificate

- *.rovio.com (b72c4ed5-6c6e-4666-9ce7-672c36e7aff8)

Domain Name

- .cloudfront.net

Custom SSL Client Support

All Clients (\$600/month prorated charge applies. [Learn about pricing](#))

Security Policy

- TLSv1

Supported HTTP Versions

- HTTP/2, HTTP/1.1, HTTP/1.0

IPv6

- Disabled

Default Root Object

-

Last Modified

- 2018-04-12 10:32 UTC+3

Log Bucket

-

Technical Setup: CF

Relevant main details for cloudfront distribution

- Custom **SSL cert** for HTTPS access (imported)
- **SNI** in use due to legacy game clients
- **Alternate Domain Names (CNAMEs)** for all subdomained admin websites
- All TLS protocols
- HTTP/2 enabled
- IPv6 disabled due to geo mapping issues

Technical Setup: CF

The screenshot shows the 'Edit Origin' configuration page for CloudFront. The top navigation bar includes links for AWS, Services (with a dropdown), Resource Groups (with a dropdown), EC2, IAM, RDS, VPC, S3, and a star icon. The main section is titled 'Edit Origin' and contains a 'Origin Settings' tab. The configuration fields include:

- Origin Domain Name: /.rovio.com
- Origin Path: (empty)
- Origin ID: Custom-1 (with a dropdown menu showing /.rovio.com)
- Origin SSL Protocols:
 - TLSv1.2
 - TLSv1.1
 - TLSv1
 - SSLv3
- Origin Protocol Policy:
 - HTTP Only
 - HTTPS Only
 - Match Viewer
- Origin Response Timeout: 60
- Origin Keep-alive Timeout: 60
- HTTP Port: 80
- HTTPS Port: 443
- Origin Custom Headers: A table with two columns, 'Header Name' and 'Value'. The first row has empty input fields. A '+' button is located at the bottom right of the table.

Technical Setup: CF

Origin details

- TLS v1.0, 1.1, 1.2 - waiting for 1.3
- Protocol selection as match viewer – both HTTP and HTTPS cases
- Maximum response timeout 60 s
- Maximum keep-alive 60 s – **IMPORTANT**
- Default ports
- No extra header adding

Technical Setup: CF

The screenshot shows the 'Edit Behavior' page for a CloudFront distribution. The top navigation bar includes 'Services' (dropdown), 'Resource Groups' (dropdown), 'EC2', 'IAM', and 'RDS'. The main section is titled 'Default Cache Behavior Settings'.

Path Pattern: Default (*)

Origin: Custom... rovio.com

Viewer Protocol Policy: HTTP and HTTPS
 Redirect HTTP to HTTPS
 HTTPS Only

Allowed HTTP Methods: GET, HEAD
 GET, HEAD, OPTIONS
 GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE

Field-level Encryption Config: [dropdown]

Cached HTTP Methods: GET, HEAD (Cached by default)
 OPTIONS

Cache Based on Selected Request Headers: All [Learn More](#)

Object Caching: Use Origin Cache Headers
 Customize
When you choose 'All' for 'Cache based on selected request headers', CloudFront doesn't cache your objects. In that configuration, Minimum TTL must be 0 seconds. [Learn More](#)

Min TTL: 0

Max TTL: 31536000

Default TTL: 86400

Forward Cookies: All

Query String Forwarding and Caching: Forward all, cache based on all

Smooth Streaming: Yes
 No

Restrict Viewer Access (Use Signed URLs or Signed Cookies): Yes
 No

Compress Objects Automatically: Yes
 No

Lambda Function Associations:

CloudFront Event	Lambda Function ARN
Select Event Type	[dropdown]

[Learn More](#)

Technical Setup: CF

Behaviors setup

- Protocols separately
- All HTTP methods – **IMPORTANT**
- “Cache based on selected request headers”: All - **IMPORTANT**
- Above for disabling caching for API traffic
- Forward all cookies so admin website logins work
- Compression (gzip) enabled for all traffic

Cache Stats (prod)

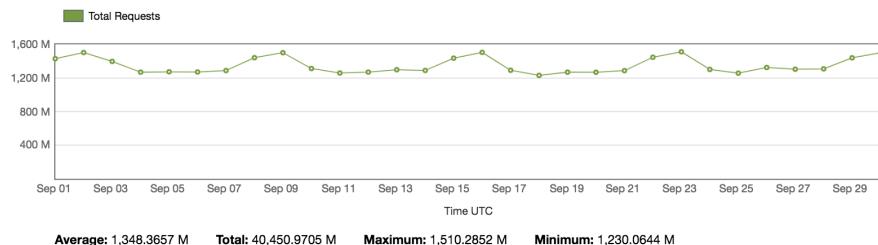
CloudFront Cache Statistics Reports

Start Date Granularity Web Distribution

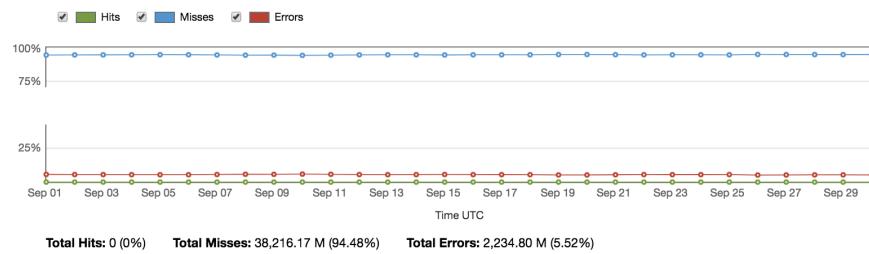
End Date Viewer Location

The following charts show selected values from CloudFront access logs. In the access logs for a distribution, each row corresponds with one viewer request. If you chose your web distributions that had activity during the specified period and that have not been deleted. Data for deleted distributions and RTMP distributions is not available. Viewers making the request while [Usage Reports](#) are based on CloudFront Billing Region.

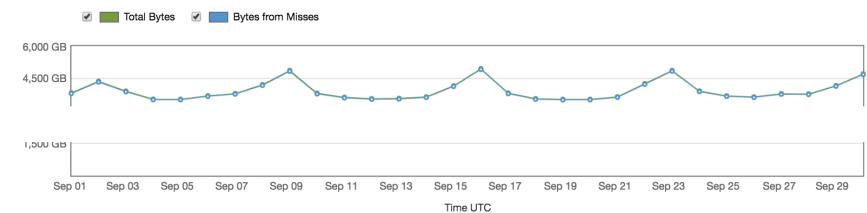
Total Requests (Millions | Thousands | Not Scaled) [Show Details](#)



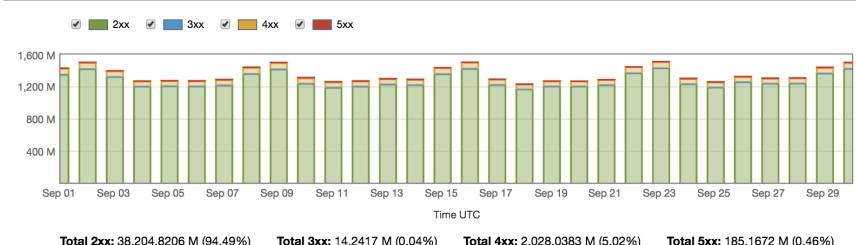
Percentage of Viewer Requests by Result Type [Show Details](#)



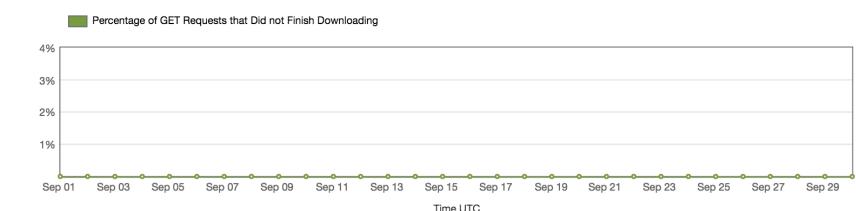
Bytes Transferred to Viewers ([Gigabytes](#) | [Megabytes](#) | [Kilobytes](#)) [Show Details](#)



HTTP Status Codes ([Millions](#) | [Thousands](#) | [Not Scaled](#)) [Show Details](#)



Percentage of GET Requests that Did not Finish Downloading [Show Details](#)



Cache Stats (prod)

- **September stats**
 - 40 billion requests in month => ~ 15000 requests / second
 - 117 000 GB transferred => ~ 400 Mbps
 - **Estimations prior to production use**
 - ~20000 requests / second
 - 200 000 GB / month
- => Not trivial to get **exact** incoming/outgoing traffic figures to your endpoint

Technical Setup: WAF



AWS Services Resource Groups EC2 IAM RDS VPC S3 Global Support

smoke

AWS WAF

Web ACLs

Create web ACL Delete

Filter Global (CloudFront)

Name smoke-test-rules-for-cloudfront

smoke-test-rules-for-cloudfront

Requests Rules Logging

If a request matches all of the conditions in a rule, take the corresponding action Edit web ACL

Order	Rule	Type	Action
1	aws-outbound	Regular	Allow requests
2	rovio-office-and-nebula	Regular	Allow requests
3	restricted-websites	Regular	Allow requests

If a request doesn't match any rules, take the default action

Default action Block all requests that don't match any rules

AWS resources using this web ACL Add association

Resource	Type
E2FJMRSIVO0MCB - rovio.com - proxy-dev, CDN for smoke	CloudFront distribution

AWS re:Invent

© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.



Technical Setup: WAF



AWS Services Resource Groups EC2 IAM RDS VPC S3 Global Support smoke

AWS WAF

Web ACLs

Rules

Marketplace

Conditions

Cross-site scripting

Geo match

IP addresses

Size constraints

SQL injection

String and regex matching

aws-outbound

Create rule Delete

Filter Global (CloudFront) Viewing 1 to 3 10

Name	Type
aws-outbound	Regular
restricted-websites	Regular
rovio-office-and-nebula	Regular

When a request originates from an IP address in aws

IP Addresses in aws

- 1... 15/32
- ... /32
- ... 0/32
- ... 1/32
- ... 3/32

AWS Services Resource Groups EC2 IAM RDS VPC S3 Global Support smoke

AWS WAF

Web ACLs

Rules

Marketplace

Conditions

Cross-site scripting

Geo match

IP addresses

Size constraints

SQL injection

String and regex matching

restricted-websites

Create rule Delete

Filter Global (CloudFront) Viewing 1 to 3 10

Name	Type
aws-outbound	Regular
restricted-websites	Regular
rovio-office-and-nebula	Regular

When a request originates from an IP address in subcontractors

No IP addresses are in this IP match condition. [Edit](#)

And

When a request matches at least one of the filters in the string match condition **restricted-websites**

Filters in restricted-websites

Header 'host' matches exactly to: "l...rovio.com".

AWS re:Invent

© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.

aws

Technical Setup: WAF



The screenshot shows the AWS WAF Rules page. On the left sidebar, under the 'Rules' section, the 'rovio-office-and-nebula' rule is selected. The main panel displays the rule configuration:

Rules

Create rule **Delete**

Filter Global (CloudFront) Viewing 1 to 3 of 10

Name	Type
aws-outbound	Regular
restricted-websites	Regular
rovio-office-and-nebula	Regular

rovio-office-and-nebula

Edit rule

When a request originates from an IP address in **rovio-office**

IP Addresses in rovio-office

- 24
- /24
- /32

Technical Setup: WAF

WAF Setup

- Single Web ACL with a few rules linked to CF distribution
- Dev
 - block all requests by default
 - allow traffic in from few known IPs (AWS + office)
- Stage and Prod
 - allow all requests by default
 - block restricted endpoints unless from known IPs
- Very simple IP and host header based checks

Technical Setup: Shield Advanced



AWS Services Resource Groups EC2 IAM RDS VPC S3 Global Support

smoke

AWS WAF Web ACLs Rules Marketplace Conditions Cross-site scripting Geo match IP addresses Size constraints SQL injection String and regex matching

AWS Shield **Summary** Protected resources Incidents Global threat environment

Summary of protected resources

0 Load Balancers (max 100)	0 Elastic IP addresses (max 100)	1 CloudFront distributions (max 100)	0 Route 53 hosted zones (max 100)
----------------------------	----------------------------------	--------------------------------------	-----------------------------------

Incidents in the last 24 hours

No incidents in the last 24 hours.

Past 18-24 hrs Past 12-18 hrs Past 12-6 hrs Past 6 hrs

Authorize DRT support

This account is subscribed to the Enterprise Support Plan.

Authorize the DRT to create WAF rules in your account: **Authorized with arn:aws:iam:::role/DRT-Support role**

Authorize the DRT to access your flow logs stored in S3 buckets: **No associated buckets**

[Learn more](#) [Edit](#)

Additional contacts

You can add other contacts to be notified by email about escalations to the DRT and proactive customer support. To add additional email addresses, choose **Edit**.

[Edit](#)

Technical Setup: Shield Advanced



Screenshot of the AWS WAF console showing a CloudFront distribution protected by AWS Shield Advanced.

The left sidebar shows the following navigation:

- AWS WAF
- Web ACLs
- Rules
- Marketplace
- Conditions
- Cross-site scripting
- Geo match
- IP addresses
- Size constraints
- SQL injection
- String and regex matching

The main content area displays the "Protected resources" section with the following buttons:

- Add protected resources
- Manage existing protections

Below these buttons is a search bar labeled "Filter by resource name" and a "Delete selected protection" button.

A table lists the protected resources:

AWS resource	Resource type	Status	CloudWatch alarm enabled	Network attack visibility	Network attack mitigation	Web attack visibility	Web attack mitigation	Associated web ACL
E2FJMR5IVO0MCB	CloudFront distribution	OK	-	✓	✓	✓	✓	smoke-test-rules-for-clo...

Technical Setup: Shield Advanced



Shield Advanced

- Enable **once** per organization umbrella
- **Subscription fee** once, data traffic per usage
- Toggle on for all supported resources – CF, ALB/ELB, EIP
- DDoS Response Team (**DRT**) Cloudformation stack

Thank you!

Mika Linnanoja

mika.linnanoja@rovio.com

AWS
re:Invent

© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.





Please complete the session
survey in the mobile app.