

RSA® Conference 2019

San Francisco | March 4–8 | Moscone Center



BETTER.

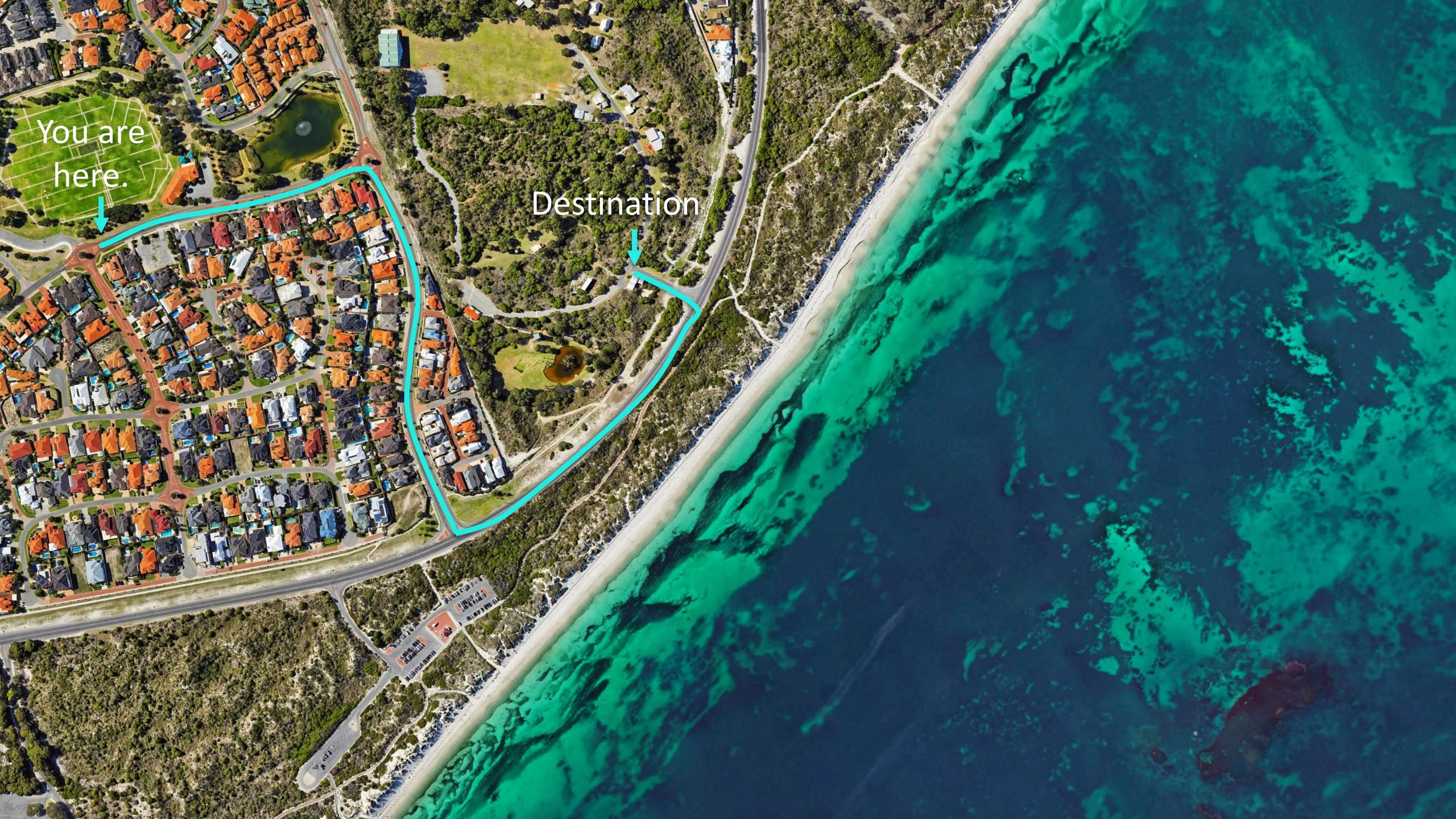
SESSION ID: IDY-T09

Delivering Automated, Modern Enterprise App Auth in Old Orgs, Quickly

Jon Lehtinen

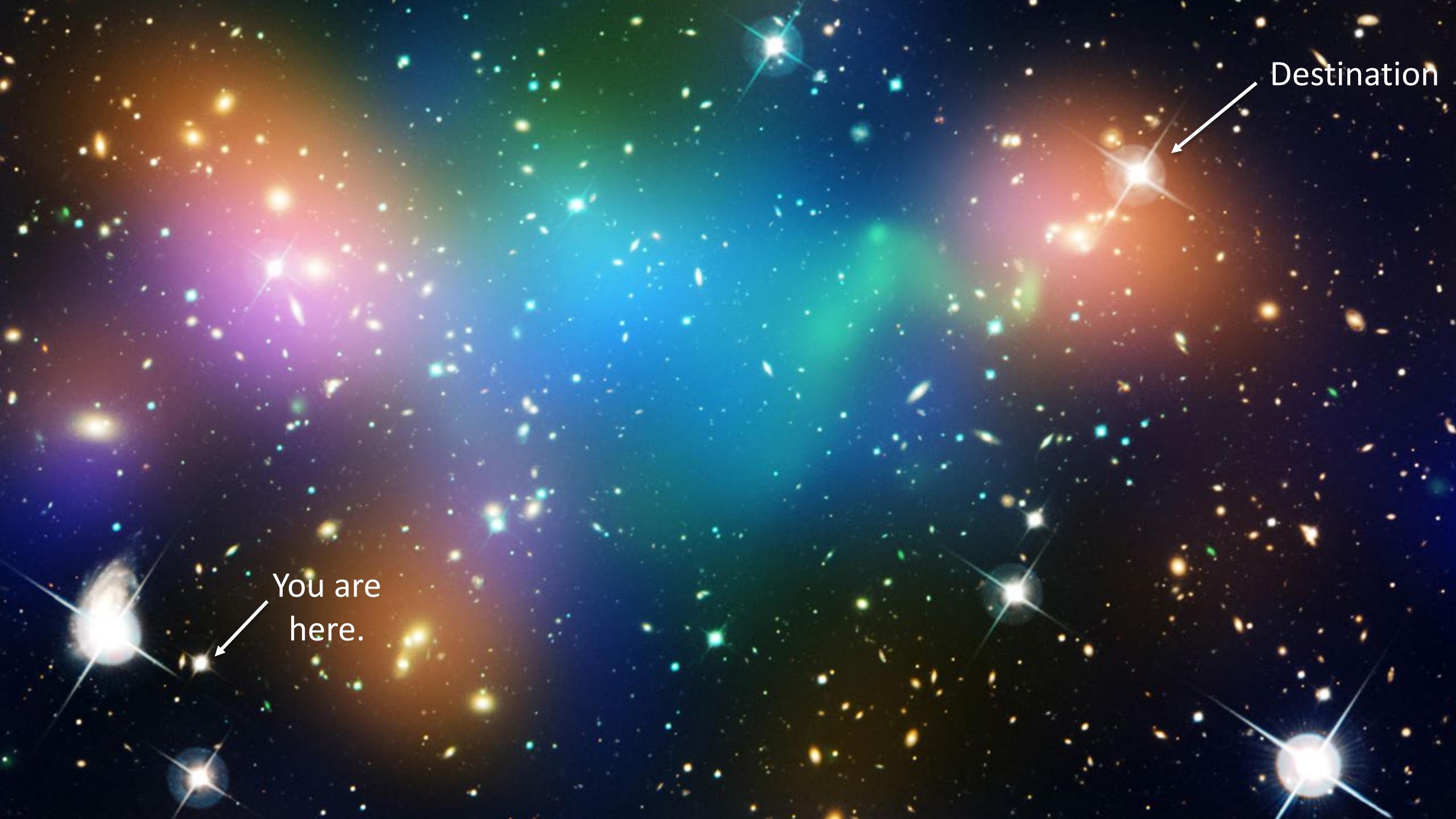
Lead Identity Engineer
Thomson Reuters
@jonlehtinen

#RSAC



You are
here.

Destination



You are
here.

Destination

RSA® Conference 2019

You can automate your enterprise
app auth.



Sweet & Maxwell
UK Legal Publisher founded

Reuters Media
Stock Info Service

West Publishing
US Legal biz founded

Hello Newspapers
Thomson buys first paper in Canada

Trust Principles
Safeguarding press integrity

Lord Thomson of Fleet
Times of London acquired

Video Terminals
Reuters FX Dealing innovation

1799

1850's

1870

1930's

1940's

1960's

1980's

Thomson Reuters Timeline: 1799 - 2019

The first 220 years

Automated News
News output now "read" by machines

2006

2003

2002

2000

1990's

1980's

Farewell Newspapers
Last Globe & Mail issues sold

TOC on NYSE
\$1B raised in share offering

Exit Travel
UK Travel biz divested

Thomson Acquires West
\$3B Cash deal

Thomson Corp & The Foundation
Reuters Foundation established

Thomson Reuters Formed
TRI on Toronto & NYSE



THOMSON
REUTERS

2008-9

Product Innovation

Jim Smith as CEO

IPS & Toronto

Sold IPS & opened Tech Center

Gender Parity

40% Sr. Female Leaders by 2020

Refinitiv

Strategic Partnership

Early
2010's

2016

Q2017

2018

2019

Westlaw Next, OneSource (global tax workstation), Eikon (Market access), Elektron (Trading infrastructure), Accelus & World-Check (Risk Mgt), Practical Law, Aumentum (gov't management), Legal workflow products & Reuters TV



What does it mean to “automate enterprise app auth?”

- Operations/Infrastructure
 - Compute/Storage/Network
 - Product maintenance, upgrades & patching
 - Outages
 - Dashboarding & Service Health
 - L1 Helpdesk/L2 Operations

What does it mean to “automate enterprise app auth?”

- Service Delivery/App Integration
 - How apps engage w/ the system
 - RACI/Ownership of IAM services, app services
 - Request management
 - Feature requests/enhancements

RSA® Conference 2019

Infrastructure/Operations

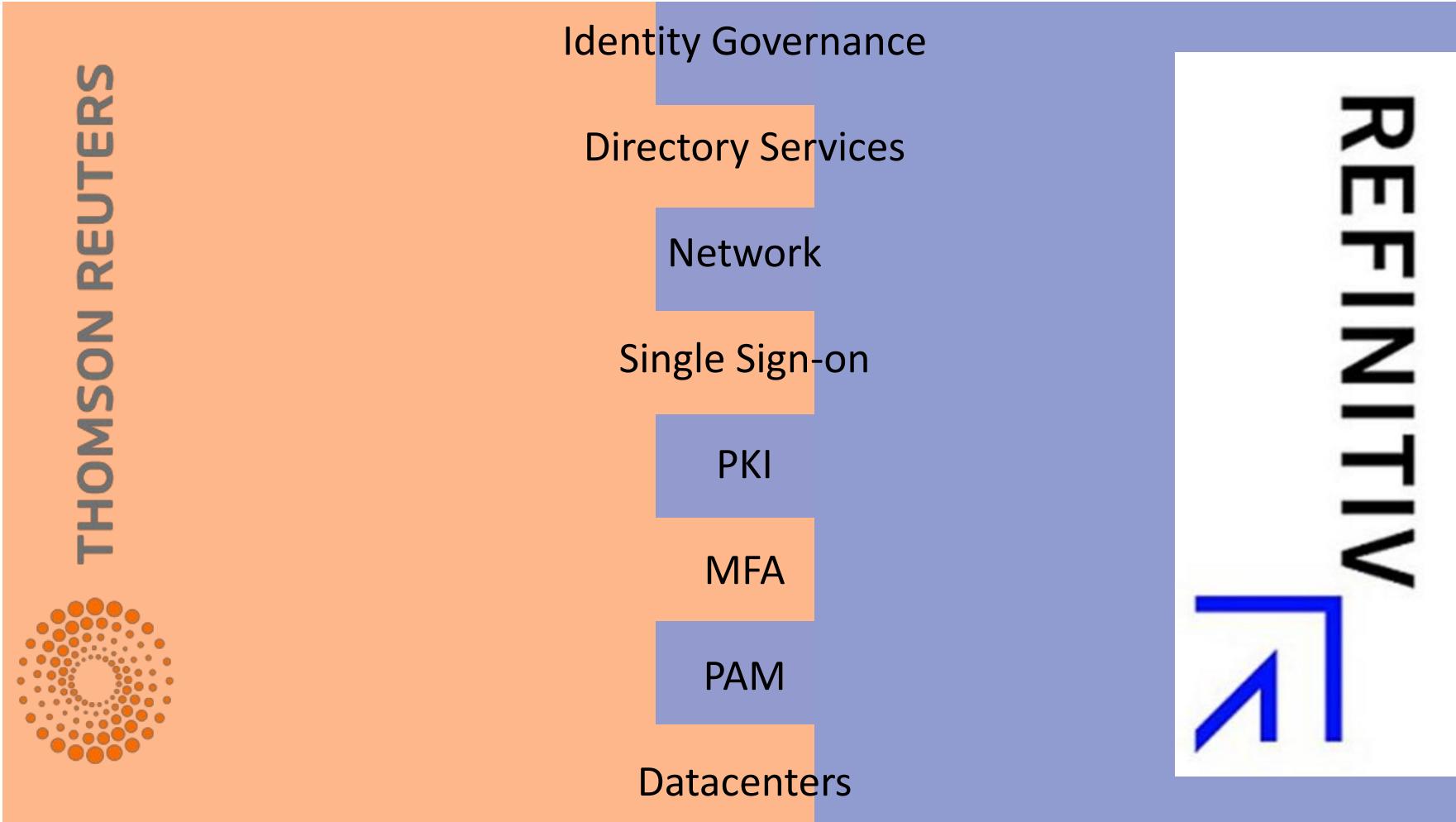


Thomson Reuters Sells Stake in Unit to Blackstone-Led Group



Thomson Reuters sold a 55 percent stake in its financial and risk business to Blackstone Group.
Carlo Allegri/Reuters

Separation





Who are our internal customers?

- ~35,000 workers
- ~4,000 apps
- Large user populations on most continents
- Access from anywhere
- Datacenter exit
- Cloud strategy

One username, one logon experience

- Multiple usernames
 - t212360886
 - \domain\t212360886
 - jon.lehtinen
 - 212360886
 - jon.lehtinen@tr.com
- Multiple logon experiences

The SAFE login screen displays two parallel logon forms: "SAFE LOG IN" on the left and "Standard" on the right. Both forms require "SAFE User ID" and "SAFE Password". The "SAFE LOG IN" form includes links for "Forgot Password?", "Remember me on this computer", and "LOG IN". The "Standard" form includes links for "What is SAFE?", "What is my SAFE User ID?", "What if I don't know my Employee or Contractor Number?", "How can I speed up my log in process?", and "Create SAFE Account".

The Thomson Reuters sign-in screen shows a "Sign in" form with fields for "someone@example.com" and "Password", and a "Next" button. A note below states: "This is a Thomson Reuters (TR) proprietary system. Unauthorized use of TR systems is prohibited & may be subject to criminal prosecution. When permitted by law, we reserve the right to monitor use of & review communications sent through these systems."

The AD LDS sign-in screen shows a "Sign in" form with fields for "AD LDS Username" and "Password", and a "Remember me" checkbox. It also features a "Sign in" button.

The Thomson Reuters sign-in screen shows a "Sign in" form with fields for "someone@example.com" and "Password", and a "Sign in" button. A note below states: "This is a Thomson Reuters proprietary system. No use is allowed unless you are a Thomson Reuters employee or have valid authorization. Your use of Thomson Reuters systems and networks is not private and is permitted only if in accordance with applicable Thomson Reuters policies, including the Code of Business Conduct and Ethics. Unauthorized use of Thomson Reuters systems or networks may be subject to disciplinary action, monetary damages, government

One username, one logon experience



THOMSON REUTERS

Enterprise Single Sign-On

USERNAME
212360886

PASSWORD

Remember my username

THIS IS NOT A SHARED DEVICE

Sign On

[Manage Password](#) | [Forgot Password](#)

- OpenID Connect
- OAuth 2
- SAML

Multifactor as an extension of SSO



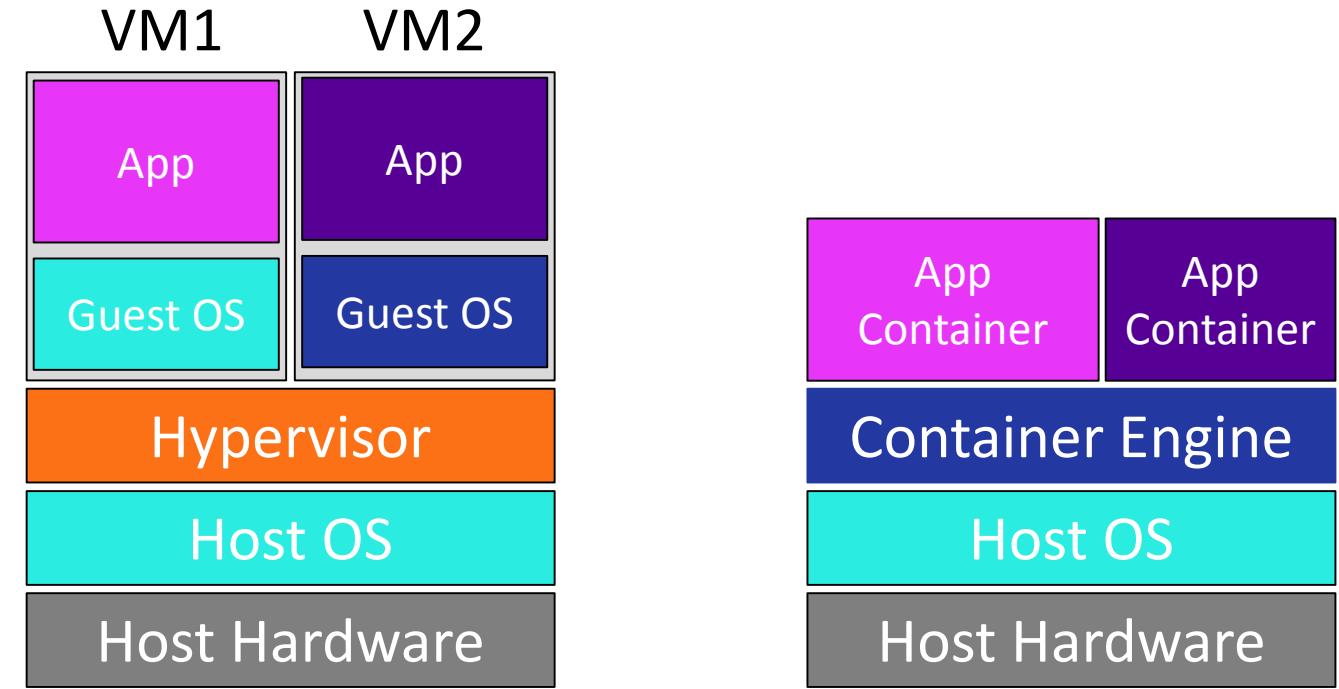
BYO... IDaaS?

- Consumable through self-service
- On-prem shrinks, cloud footprint grows
- Global orgs should actually have global services
- Late-night ops incidents make me grouchy

Build, buy, or cloudify?



Native Cloud Services



Virtual Machines

Containers

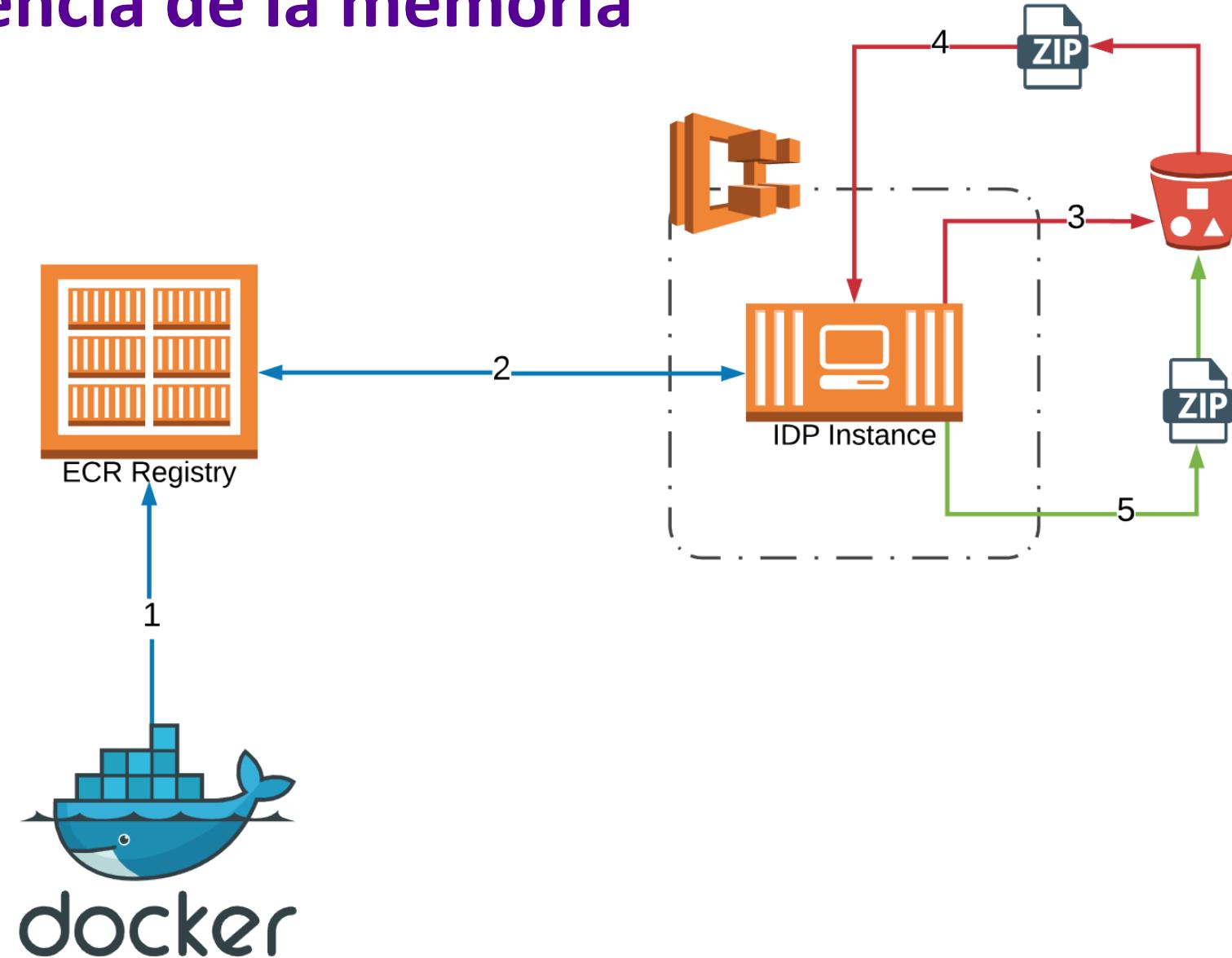
Containerizing an on-prem SSO product

- Not a lot of vendor guidance or prior art (March 2018)
- Docker networking/AWS security group considerations
- No secrets in the dockerfile/configs
- No root users

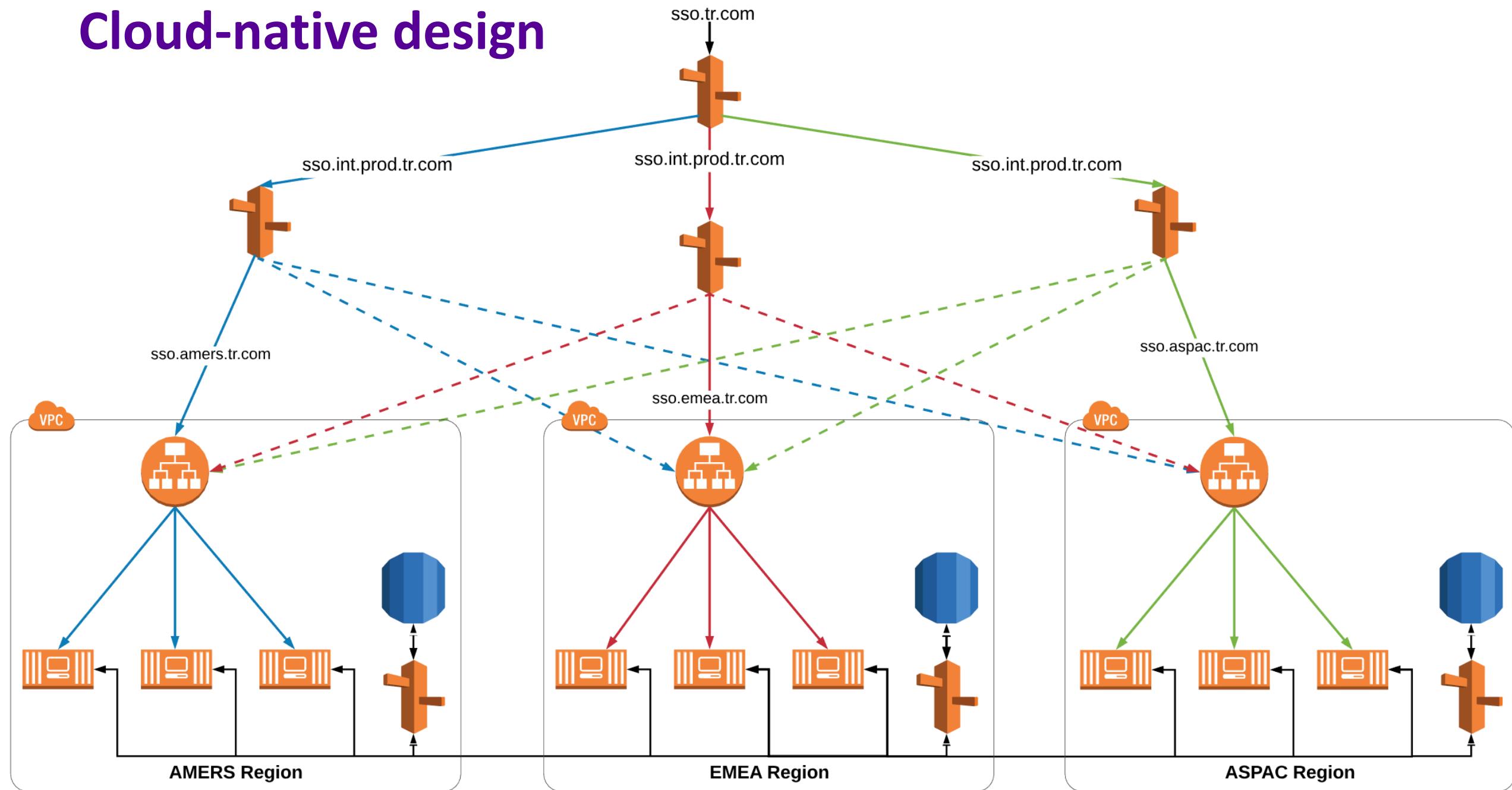
Ship of Theseus



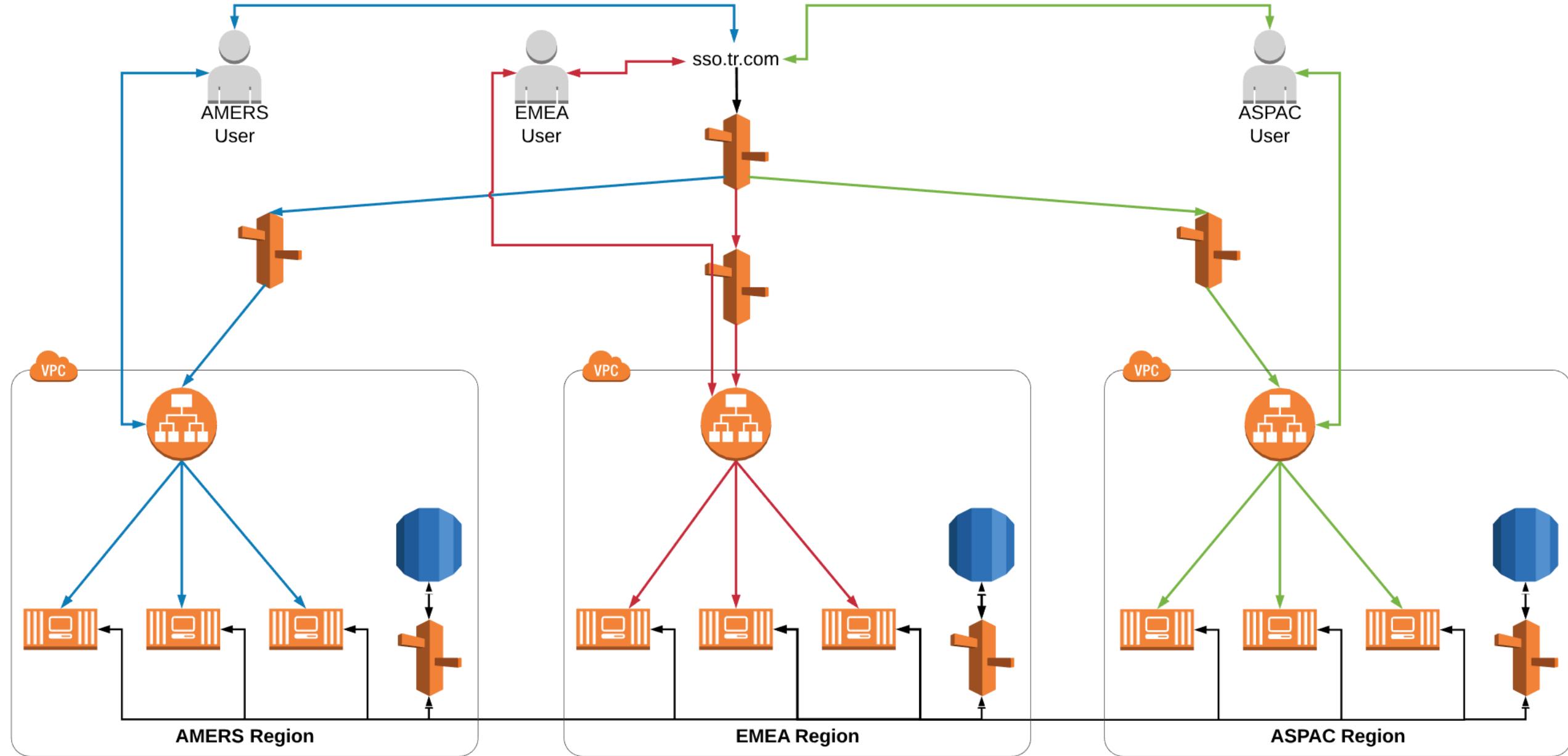
La persistencia de la memoria



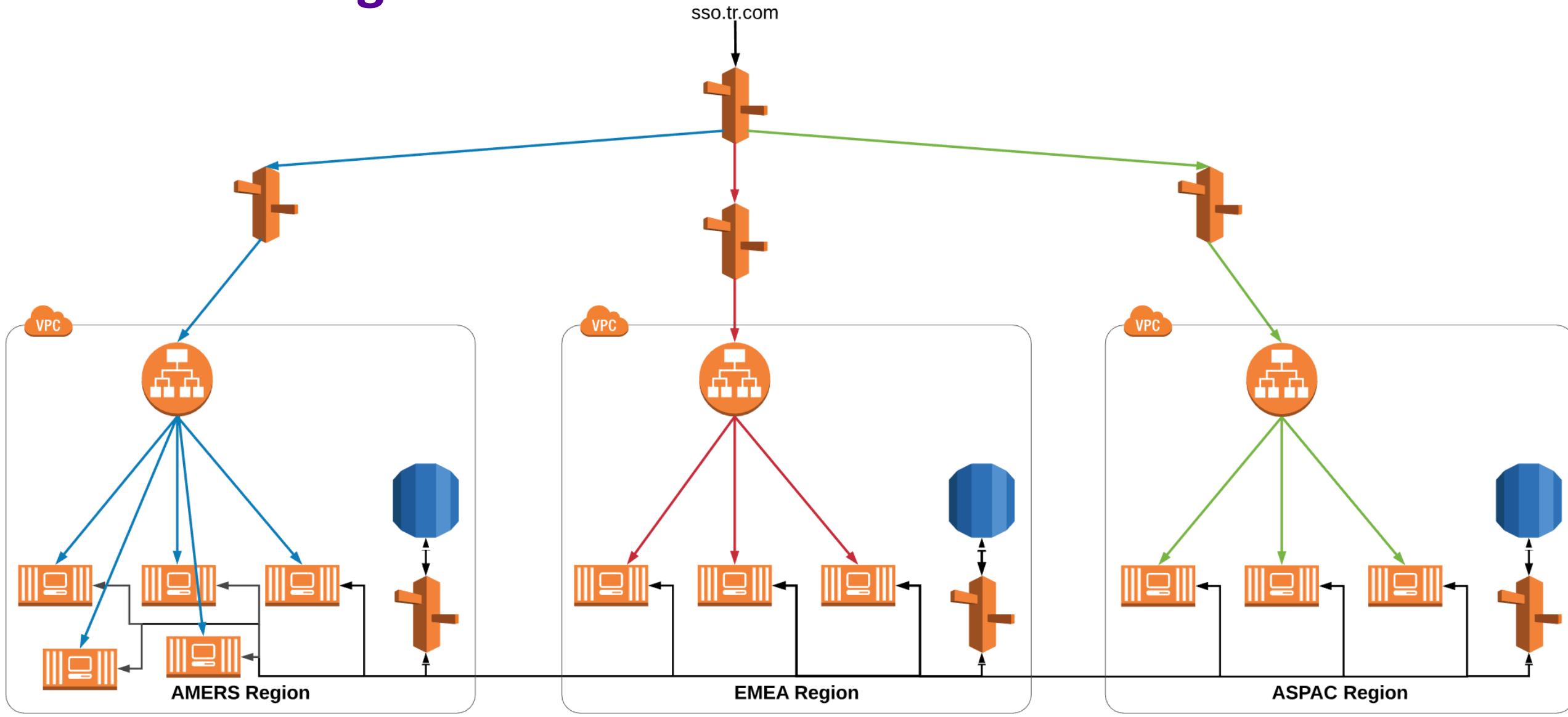
Cloud-native design



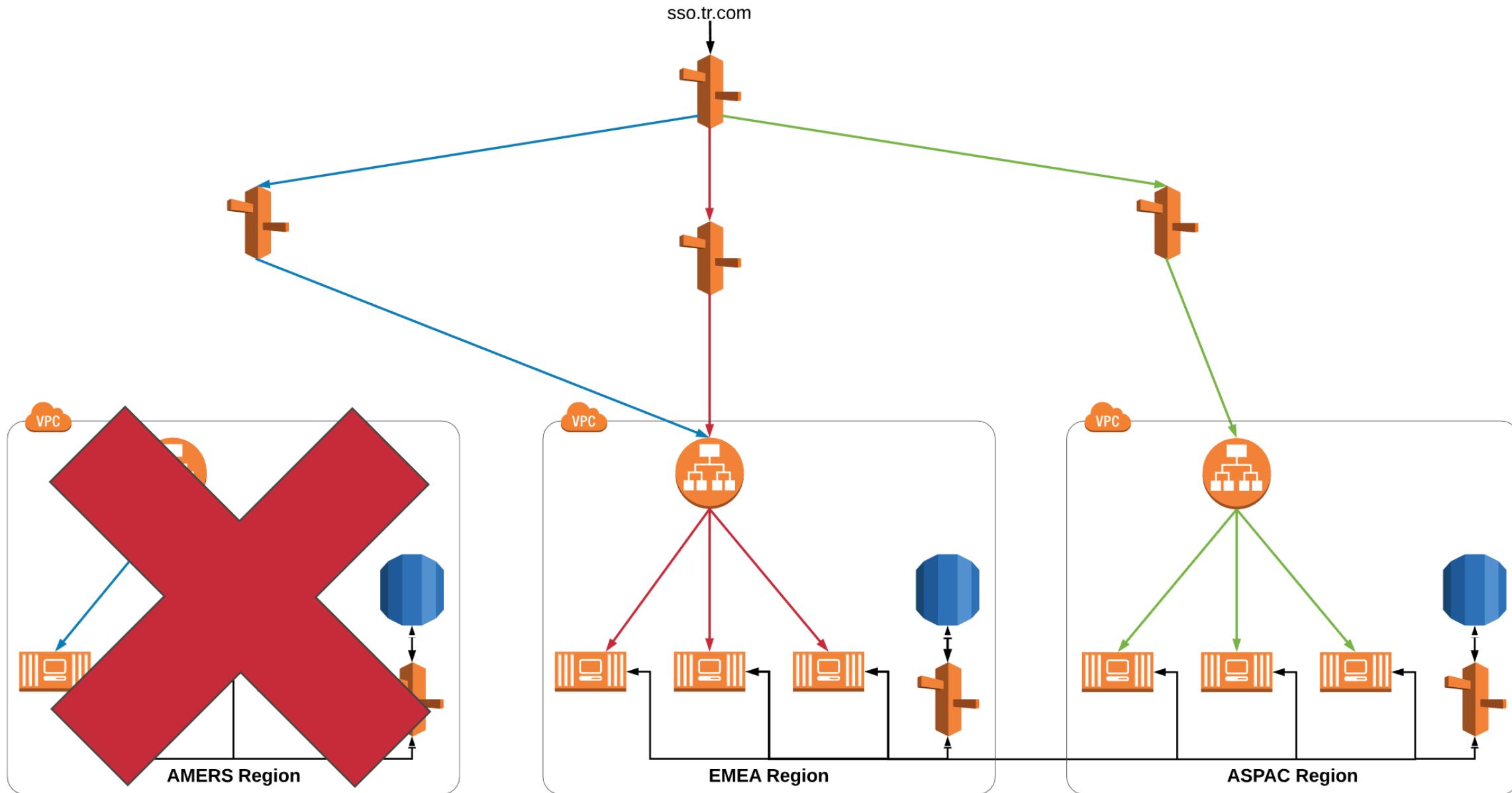
Location-aware routing & regional sub-clusters



Auto Scaling



High-availability & disaster recovery



Operational support

- Dashboard shows the service is up
- Check the test apps
- Can you get a token using curl?
- Attach proof or L2 will reject incident



RSA®Conference2019

Impact of Infrastructure/Operations Automation

One script to rule them all

```

1 RBILoadBalancerIngressRule:
2   Type: RBI::SCP::SecurityGroupIngress
3   Description: Inbound rule for the RBI SLB, traffic limited to Bastion CoolDudeSecurityGroup
4   DependsOn: RBILoadBalancerSecurityGroup
5   Properties:
6     FromPort: 443
7     ToPort: 443
8     GroupId: !Ref RBILoadBalancerSecurityGroup
9     IpProtocol: TCP
10    SourceSecurityGroupId: !Ref CoolDudeSecurityGroup
11
12 - RBILoadBalancerEgressRule:
13 -   Type: RBI::SCP::SecurityGroupEgress
14 -   Description: Outbound rule for RBI SLB, traffic goes to CORHostSecurityGroup on 4587
15 -   DependsOn: RBILoadBalancerSecurityGroup
16 -   Properties:
17 -     FromPort: 4587
18 -     ToPort: 4587
19 -     GroupId: !Ref RBILoadBalancerSecurityGroup
20 -     IpProtocol: TCP
21 -     DestinationSecurityGroupId: !Ref CORHostSecurityGroup
22
23 EngineLoadBalancerSecurityGroup:
24   Type: RBI::SCP::SecurityGroup
25   Description: Security group for the Engine SLB
26   Properties:
27     DDCId: !Ref DDC
28     GroupDescription: Access to the load balancer that sits in front of COR
29     Tags:
30       - Key: Name
31       | Value: !Sub ${EnvironmentName}-EngineSLB-${RBIRegionAbbreviation}-${EnvironmentType}
32       - Key: tr:application-asset-insight-id
33       | Value: !Ref AssetInsightID
34       - Key: tr:environment-type
35       | Value: !Ref EnvironmentType
36       - Key: tr:resource-owner
37       | Value: !Ref ResourceOwner
38       - Key: tr:financial-identifier
39       | Value: !Ref FinancialID
40
41 - EngineLoadBalancerIngressRule:
42 -   Type: RBI::SCP::SecurityGroupIngress
43 -   Description: Ingress rule for the Engine SLB, takes traffic from Bastion WebWorld Security Group
44 -   DependsOn: EngineLoadBalancerSecurityGroup
45 -   Properties:
46 -     FromPort: 443
47 -     ToPort: 443
48 -     GroupId: !Ref EngineLoadBalancerSecurityGroup
49 -     IpProtocol: TCP
50 -     SourceSecurityGroupId: !Ref WebWorldSecurityGroup
51
52 EngineLoadBalancerEgressRule:
53   Type: RBI::SCP::SecurityGroupEgress
54   Description: Outbound rule for Engine SLB, traffic goes to CORHostSecurityGroup on 3333
55   DependsOn: EngineLoadBalancerIngressRule
56   Properties:
57     FromPort: 3333

```

```

1 RBILoadBalancerIngressRule:
2   Type: RBI::SCP::SecurityGroupIngress
3   Description: Inbound rule for the RBI SLB, traffic limited to Bastion CoolDudeSecurityGroup
4   DependsOn: RBILoadBalancerSecurityGroup
5   Properties:
6     FromPort: 443
7     ToPort: 443
8     GroupId: !Ref RBILoadBalancerSecurityGroup
9     IpProtocol: TCP
10    SourceSecurityGroupId: !Ref CoolDudeSecurityGroup
11
12 + # RBILoadBalancerEgressRule:
13 + #   Type: RBI::SCP::SecurityGroupEgress
14 + #   Description: Outbound rule for RBI SLB, traffic goes to CORHostSecurityGroup on 4587
15 + #   DependsOn: RBILoadBalancerSecurityGroup
16 + #   Properties:
17 + #     FromPort: 4587
18 + #     ToPort: 4587
19 + #     GroupId: !Ref RBILoadBalancerSecurityGroup
20 + #     IpProtocol: TCP
21 + #     DestinationSecurityGroupId: !Ref CORHostSecurityGroup
22
23 EngineLoadBalancerSecurityGroup:
24   Type: RBI::SCP::SecurityGroup
25   Description: Security group for the Engine SLB
26   Properties:
27     DDCId: !Ref DDC
28     GroupDescription: Access to the load balancer that sits in front of COR
29     Tags:
30       - Key: Name
31       | Value: !Sub ${EnvironmentName}-EngineSLB-${RBIRegionAbbreviation}-${EnvironmentType}
32       - Key: tr:application-asset-insight-id
33       | Value: !Ref AssetInsightID
34       - Key: tr:environment-type
35       | Value: !Ref EnvironmentType
36       - Key: tr:resource-owner
37       | Value: !Ref ResourceOwner
38       - Key: tr:financial-identifier
39       | Value: !Ref FinancialID
40
41 + # EngineLoadBalancerIngressRule:
42 + #   Type: RBI::SCP::SecurityGroupIngress
43 + #   Description: Ingress rule for the Engine SLB, takes traffic from Bastion WebWorld Security Group
44 + #   DependsOn: EngineLoadBalancerSecurityGroup
45 + #   Properties:
46 + #     FromPort: 443
47 + #     ToPort: 443
48 + #     GroupId: !Ref EngineLoadBalancerSecurityGroup
49 + #     IpProtocol: TCP
50 + #     SourceSecurityGroupId: !Ref WebWorldSecurityGroup
51
52 EngineLoadBalancerEgressRule:
53   Type: RBI::SCP::SecurityGroupEgress
54   Description: Outbound rule for Engine SLB, traffic goes to CORHostSecurityGroup on 3333
55   DependsOn: EngineLoadBalancerIngressRule
56   Properties:
57     FromPort: 3333

```

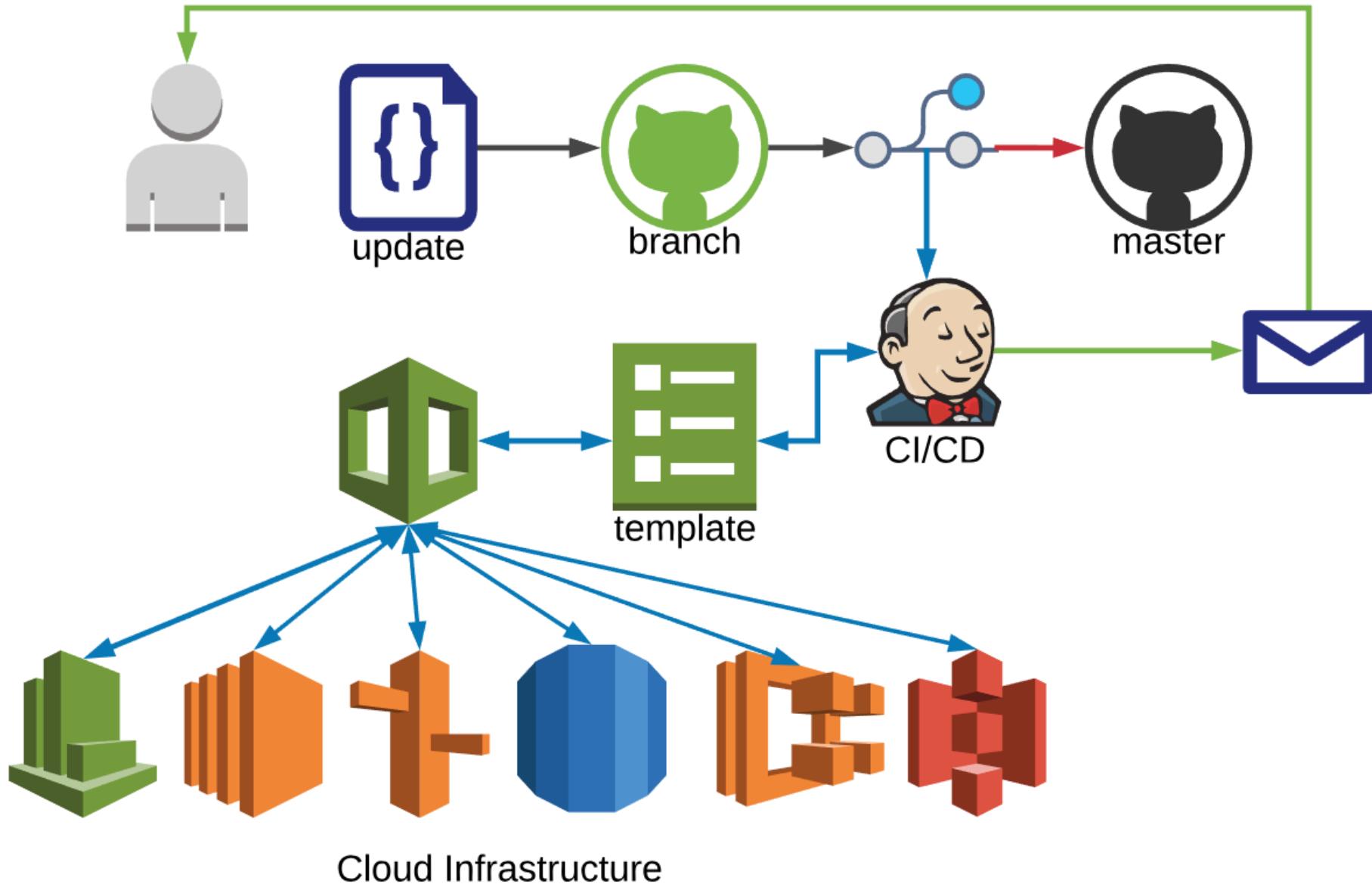


Product upgrades

```
6.1.3
1 FROM scratch
2
3 COPY docker-build-files /tmp/docker-build-files
4
5 -WORKDIR /opt/idp-6.1.3/idpserver
6
7 RUN apt-get update \
8 && apt-get install -y unzip \
9 && unzip /tmp/docker-build-files/idp-*.zip -d /opt \
10 && ls /tmp/docker-build-files/jre*.tar.gz | xargs -i tar -xf {} -C /opt \
11 && unzip /tmp/docker-build-files/knowledge2017.zip -d ./assets/fonts \
12 && cp -r /tmp/docker-build-files/idpserver/* . \
13 && cp /tmp/docker-build-files/startup.sh /usr/bin/ \
14 && groupadd -r idp-nonrootuser \
15 && useradd -r -g idp-nonrootuser idp-nonrootuser \
16 && chown -R idp-nonrootuser:idp-nonrootuser ../ \
17 && chmod +x /usr/bin/startup.sh \
18 && chown idp-nonrootuser:idp-nonrootuser /usr/bin/startup.sh \
19 && rm -r /tmp/docker-build-files
20
21 ENV JAVA_HOME /opt/jdk1.8.0_172
22 -ENV PF_HOME /opt/idpserver-6.1.3/idpserver
23
24 EXPOSE 443
25
26 USER idp-nonrootuser:idp-nonrootuser
27
28 ENTRYPOINT ["/usr/bin/startup.sh"]
```

```
6.2
1 FROM scratch
2
3 COPY docker-build-files /tmp/docker-build-files
4
5 +WORKDIR /opt/idp-6.2/idpserver
6
7 RUN apt-get update \
8 && apt-get install -y unzip \
9 && unzip /tmp/docker-build-files/idp-*.zip -d /opt \
10 && ls /tmp/docker-build-files/jre*.tar.gz | xargs -i tar -xf {} -C /opt \
11 && unzip /tmp/docker-build-files/knowledge2017.zip -d ./assets/fonts \
12 && cp -r /tmp/docker-build-files/idpserver/* . \
13 && cp /tmp/docker-build-files/startup.sh /usr/bin/ \
14 && groupadd -r idp-nonrootuser \
15 && useradd -r -g idp-nonrootuser idp-nonrootuser \
16 && chown -R idp-nonrootuser:idp-nonrootuser ../ \
17 && chmod +x /usr/bin/startup.sh \
18 && chown idp-nonrootuser:idp-nonrootuser /usr/bin/startup.sh \
19 && rm -r /tmp/docker-build-files
20
21 ENV JAVA_HOME /opt/jdk1.8.0_172
22 +ENV PF_HOME /opt/idpserver-6.2/idpserver
23
24 EXPOSE 443
25
26 USER idp-nonrootuser:idp-nonrootuser
27
28 ENTRYPOINT ["/usr/bin/startup.sh"]
```

Continuous integration, continuous deployment



Self-service through dynamic client registration

```

1 POST /as/clients.oauth2 HTTP/1.1
2 Content-Type: application/json
3 Accept: application/json
4 Authorization: Bearer eyJhbGciOiJSUzI1NiIsImtpZCI6ImsxIn0
5 Host: sso.thomsonreuters.com
6
7 {
8     "client_name": "Jon's Cool App",
9     "redirect_uris": [
10         "https://redbeardidentity.com/coolapp",
11         "https://redbeardidentity.com/coolerapp"
12     ],
13     "scope": "openid profile mfa",
14     "grant_types": [
15         "authorization_code",
16         "refresh_token"
17     ]
18 }
```

```

1 HTTP/1.1 201 Created
2 Date: Fri, 21 Oct 2018 15:30:00 GMT
3 Referrer-Policy: origin
4 Content-Type: application/json
5 Transfer-Encoding: chunked
6
7 {
8     "client_id": "dc-rqUtii4vRXj5NMztkAeJ1S",
9     "client_name": "Jon's Cool App",
10    "redirect_uris": [
11        "https://redbeardidentity.com/coolapp",
12        "https://redbeardidentity.com/coolerapp"
13    ],
14    "token_endpoint_auth_method": "client_secret_basic",
15    "grant_types": [
16        "authorization_code",
17        "refresh_token"
18    ],
19    "client_secret": "p7MD0Ul1DNI9xRDc5kc0xs",
20    "client_secret_expires_at": 0,
21    "scope": "openid profile mfa",
22    "validate_using_all_eligible_atms": false,
23    "refresh_token_rolling_policy": "server_default",
24    "persistent_grant_expiration_type": "server_default",
25    "grant_access_session_revocation_api": false
26 }
```

Total cost of ownership

- Saves \$1.2mm per year over existing TR SSO & MFA systems
- \$2.2mm less per year compared to retail enterprise IDaaS
- \$700,000 less per year compared to bulk rate enterprise IDaaS

RSA® Conference 2019

Challenges



Containers, DevOps, Cloud

- Trial and error, limited cloud/development knowledge
- Endless tinkering
 - refinements continue (now under change control) to this day
- Operational handoff is more difficult
- Kubernetes for transportability

RSA® Conference 2019

You can automate your enterprise
app auth.

RSA®Conference2019

Service Delivery/App Integration

The baseline

- Staff, contractors, different verticals
- Support per SOW
- Difficult for customers
- Difficult for IAM staff
- Proprietary WAM with request-based integration process
- Some SAML
- POC OIDC, OAuth

SSO Organization



Engineering - Design



Integrations - Build



Operations - Run

What do we need for automation?

Protocol:	WAM	SAML	OIDC
API:	YES	YES	YES
Lightweight:	NO	YES-ish	YES
Strategic:	NO	YES	YES

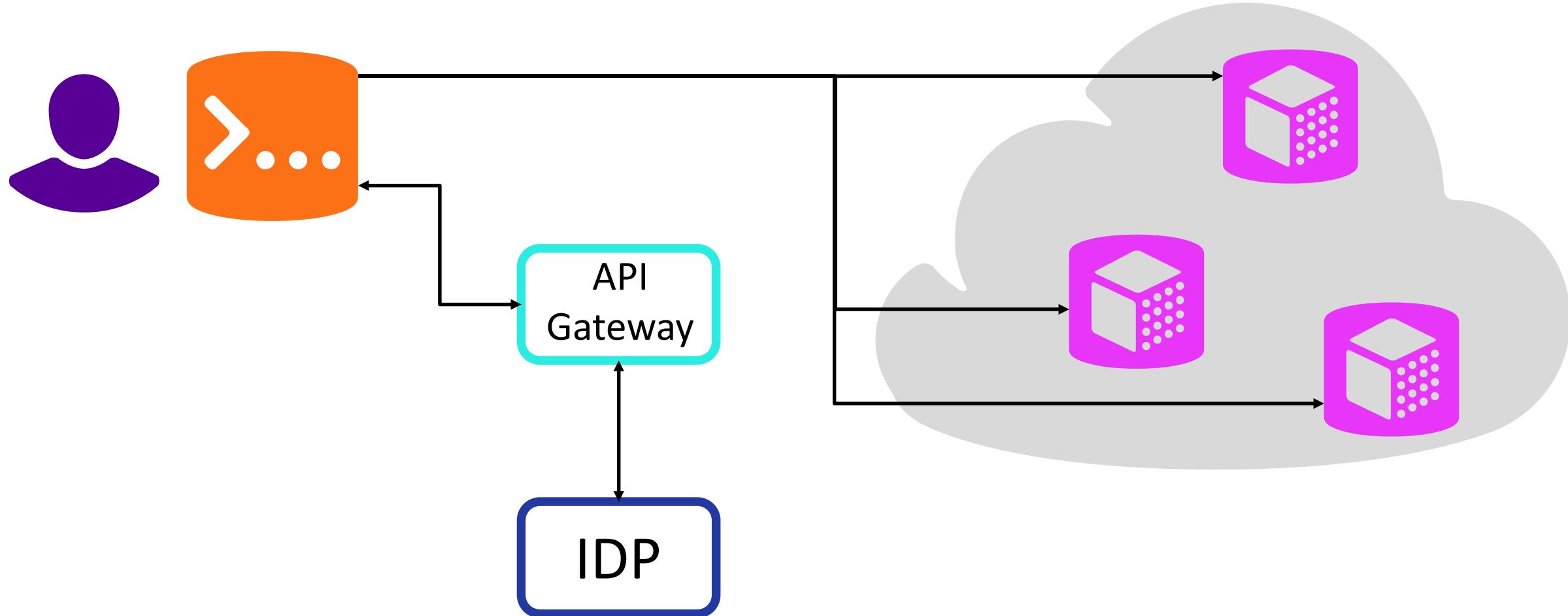
Who are our customers?

- Technically-savvy power users
 - Cloud architects
 - Mobile devs
 - Small group, but loud and resentful
- Checklisters
 - Project managers
 - App/web admins
 - Forced to engage for project/audit reasons

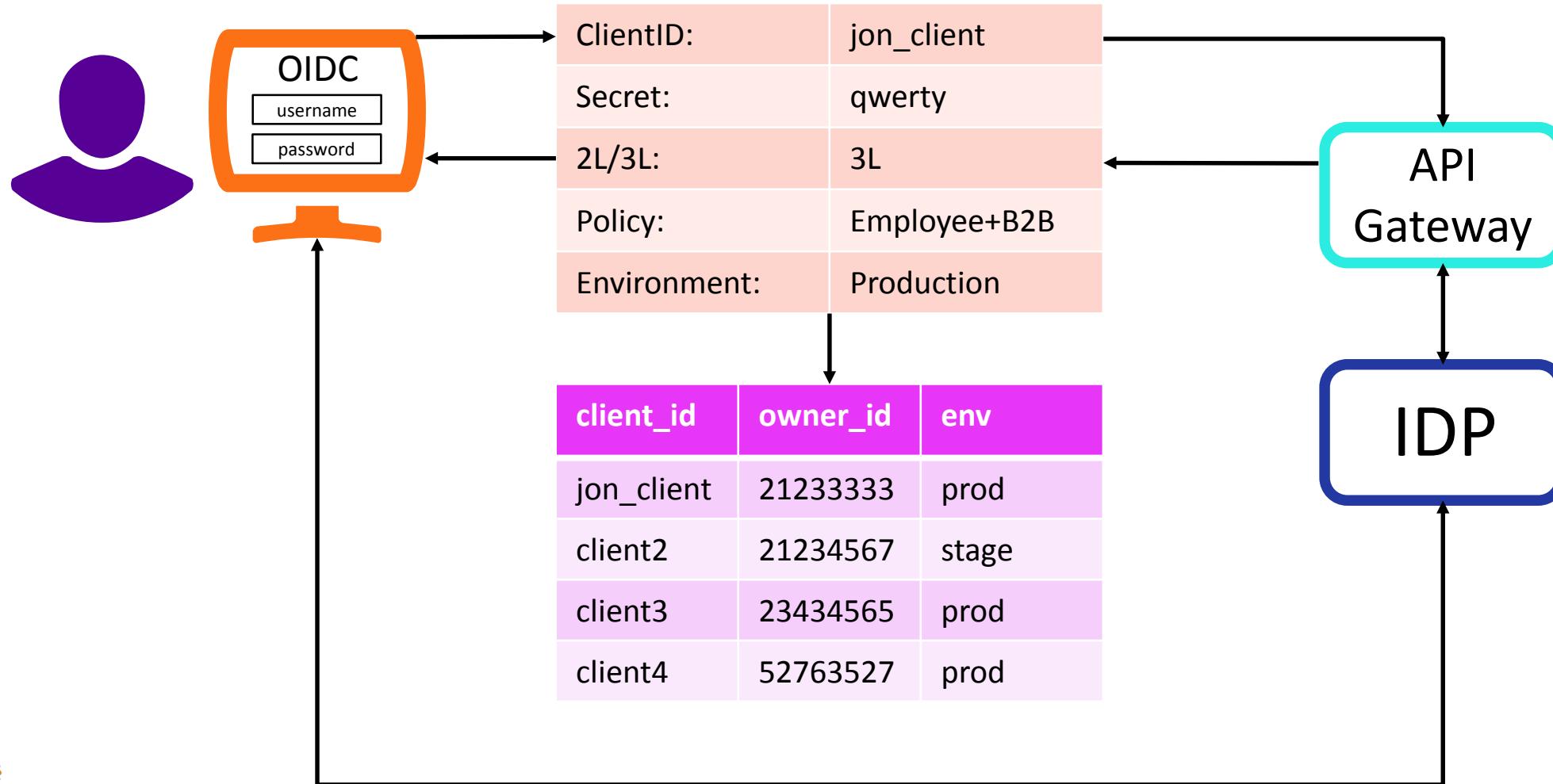
RSA®Conference2019

Self-Service is the new automation

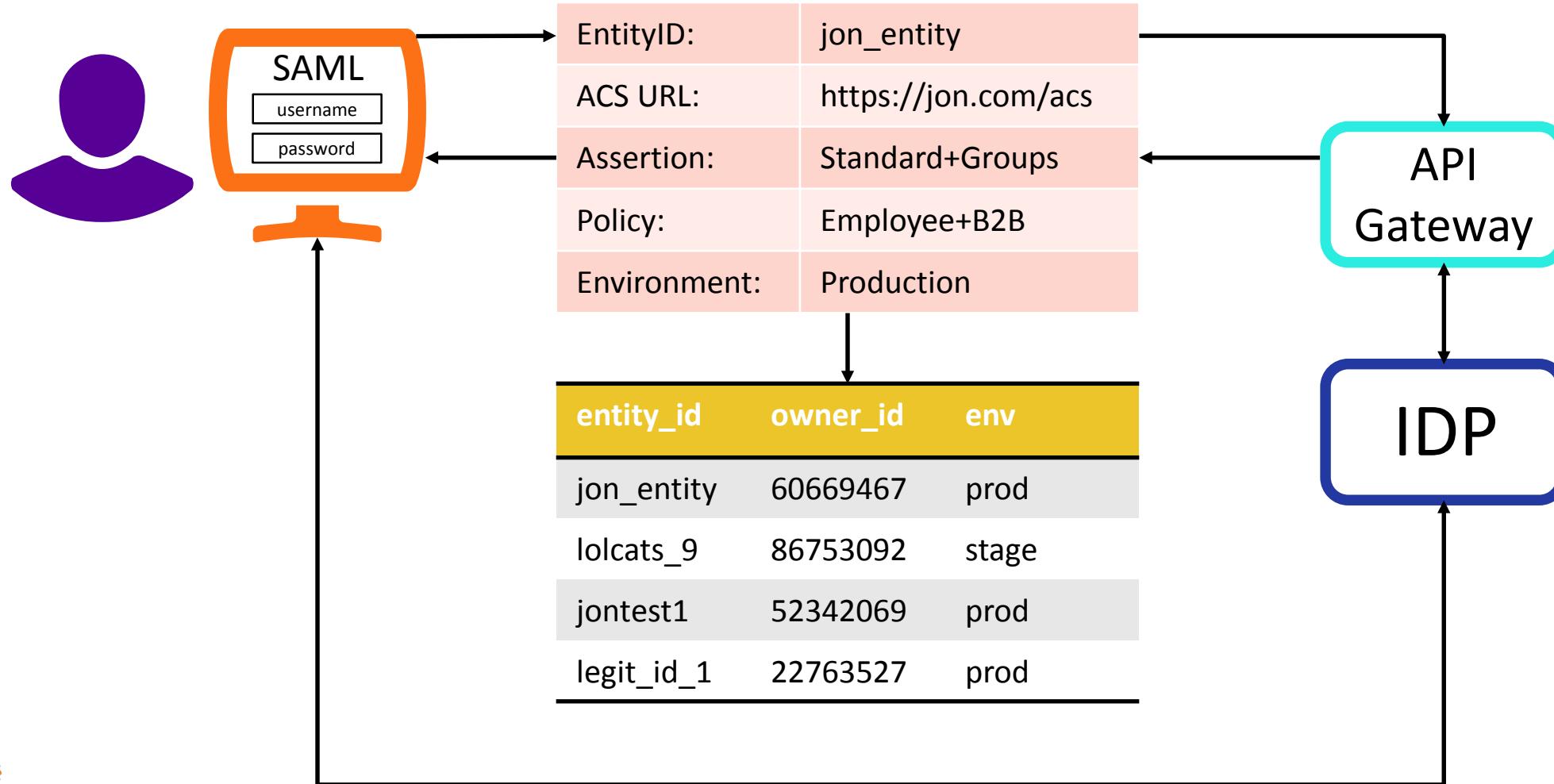
Q4 2015 Self-Service API



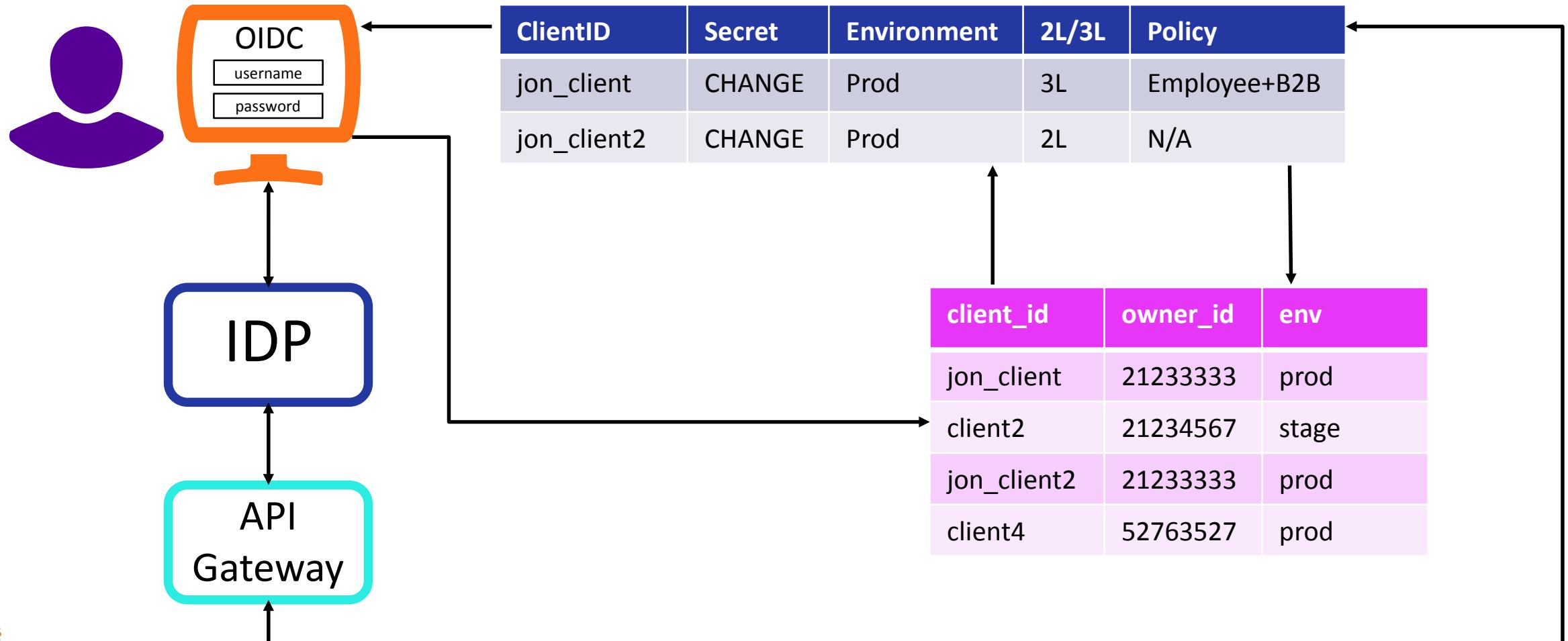
Web Portal (Create)



Web Portal (Create)



Web Portal (Read, Update, Delete)



How do apps use auth services?

- App-level integration
- Web-tier integration
- Solutions *don't* have to come from centralized team
- Standards allows solution flexibility





EXIT

From the Customer's Perspective

Engagement Type	Process	Speed	Solutions	Customization	Support
Integrations Team	Familiar	10 day SLA	OIDC, SAML, WAM	Limitless	Live Collaboration
Self-Service	Unfamiliar	Instant	OIDC, SAML	Preconfigured	Documentation

Chargeback model

- Charge per integration
 - OIDC was cheap
 - SAML was reasonable
 - WAM was expensive



Service Level Agreements



From the Customer's Perspective

Engagement Type	Process	Speed	Solutions	Customization	Support
Integrations Team	Familiar	10 day SLA	OIDC, SAML, WAM	Limitless	Live Collaboration
Self-Service	Unfamiliar	Instant	OIDC, SAML	Preconfigured	Documentation

From the Customer's Perspective

Engagement Type	Process	Speed	Solutions	Customization	Support	Cost
Integrations Team	Familiar	42 day FIFO	OIDC, SAML, WAM	Limitless	Live Collaboration	\$-OIDC \$\$-SAML \$\$\$\$-WAM
Self-Service	Semi-familiar	Instant	OIDC, SAML	Preconfigured	Documentation	Free

RSA®Conference2019

Impact of Service Delivery Automation

Adoption of authentication services

June 2015



800 clients

37 OIDC

June 2017



10,048 clients

8,515 OIDC

SAML

900 Service Providers

SAML

5,005 Service Providers



7200 applications



~_(ツ)_/~ applications

Business impact

- **\$3.2 million** 2016-2017 year/year labor
- **\$1.3 million** WAM retirement savings
- **\$4.5 million total savings by end of 2017**
- Standards
- API economy

Timeline - 3.5 years

- Q4 2013 Establish Integrations Team
- Q2 2014 Expanded service library
- Q4 2015 POC Self-Service
- Q4 2016 Legacy solutions dropped from support
- Q2 2017 Self-Service for OIDC/SAML only

RSA® Conference 2019

You can automate your enterprise
app auth.



What does it mean to “automate enterprise app auth?”

- Operations/Infrastructure
 - Leverage modern cloud/DevOps practices
 - Embrace your sloth, design for “touchless”
 - Manage support expectations

What does it mean to “automate enterprise app auth?”

- Service Delivery/App Integration
 - Self-service
 - Sample solutions
 - Product management
 - Iterative improvements

You can automate your enterprise app auth.

- Next week you should:
 - Identify what Ops/Service Delivery practices & services are candidates for automation/self-service
- Within the next three months you should:
 - Launch a regular customer touchpoint to understand what their needs are, and how you can drive them to use self-service using those needs as the incentive
- Within the next six months you should:
 - Launch an MVP self-service capability for your enterprise app auth service, and/or design new services to use ephemeral infra

Questions?

@jonlehtinen

jon.lehtinen@thomsonreuters.com

jlehtinen@idpro.org

jon.lehtinen@gmail.com