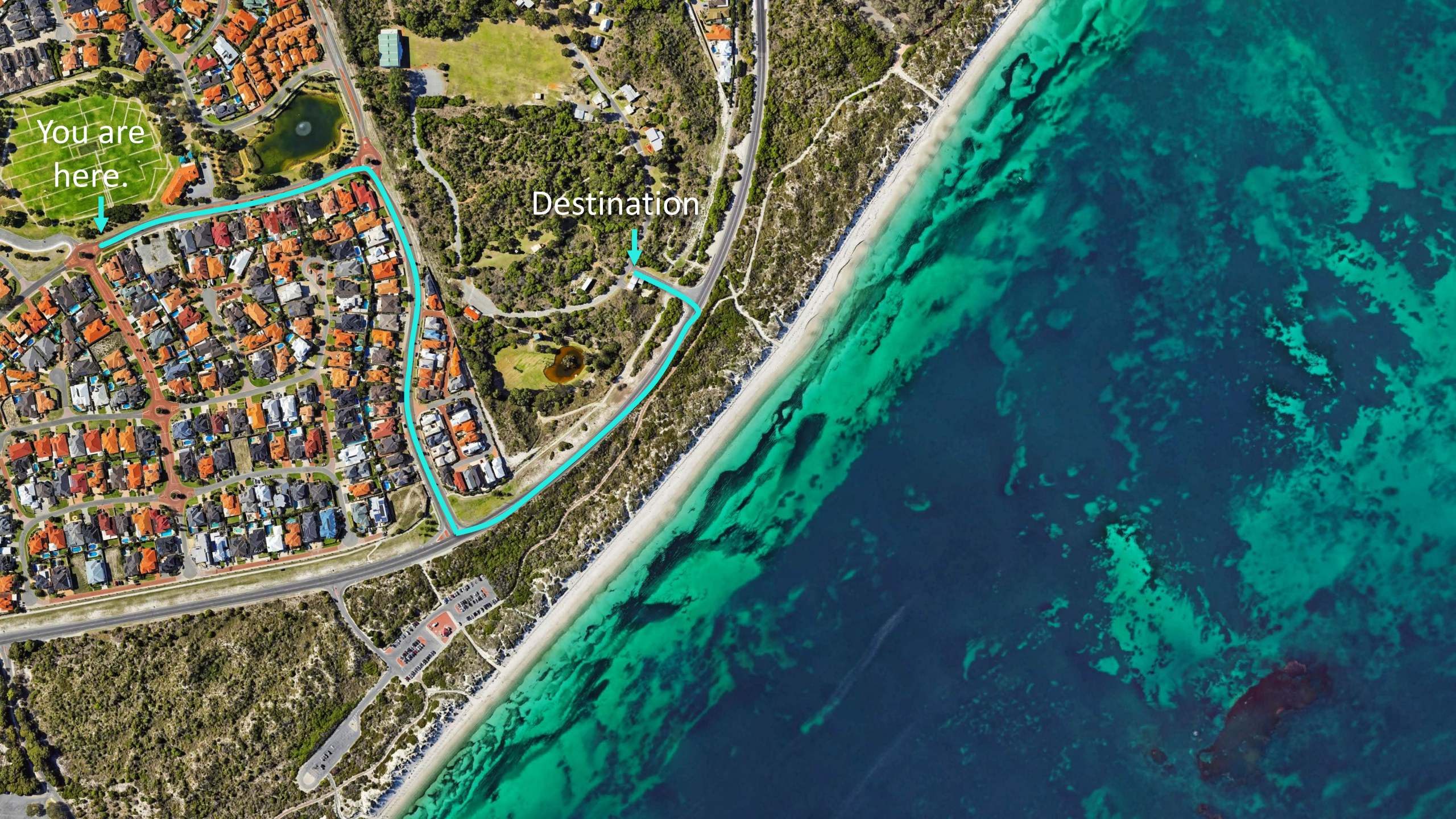
RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: IDY-T09

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

Jon Lehtinen

Lead Identity Engineer
Thomson Reuters
@jonlehtinen


You are here.
Destination

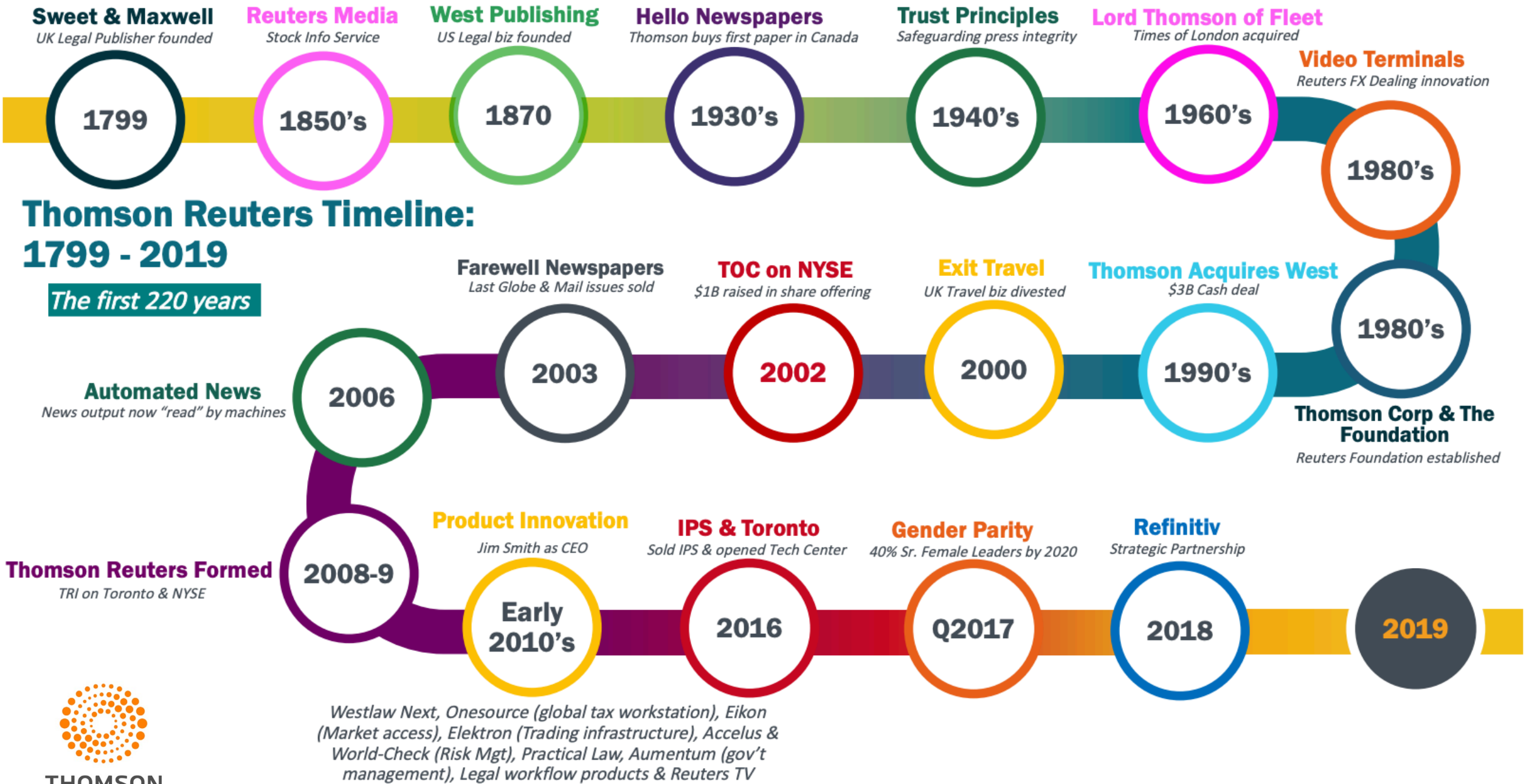

Destination
You are here.

RSAConference2019

You can automate your enterprise app auth.

Thomson Reuters Timeline: 1799 - 2019

The first 220 years



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

THOMSON REUTERS


99 1784-0

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

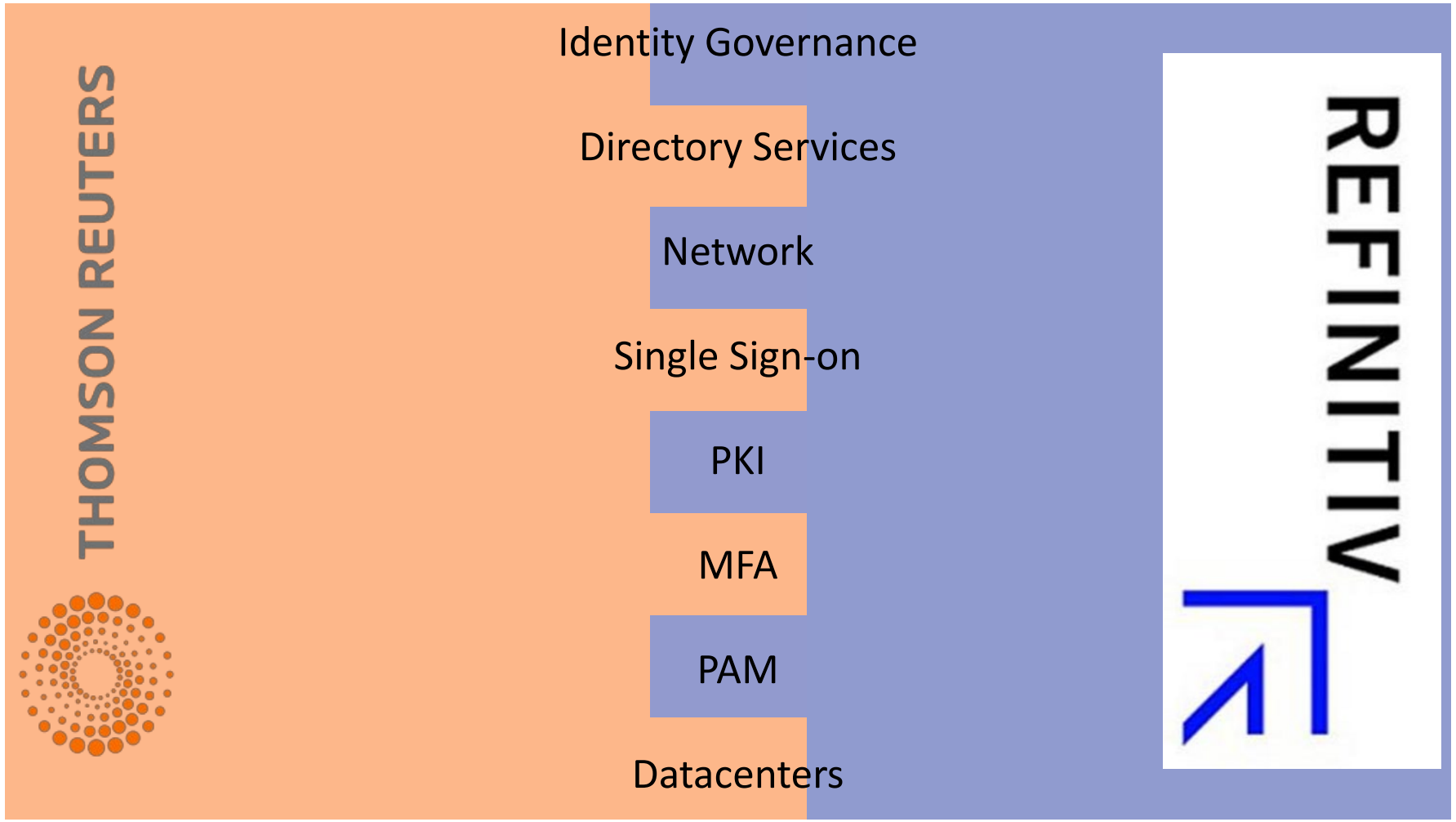
RSAConference2019

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

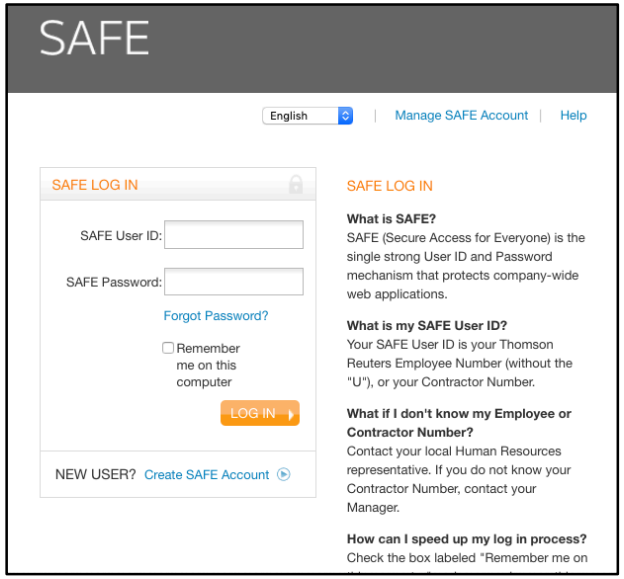

THOMSON REUTERS
Identity Governance
Directory Services
Network
Single Sign-on
PKI
MFA
PAM
Datacenters
REFINITIV

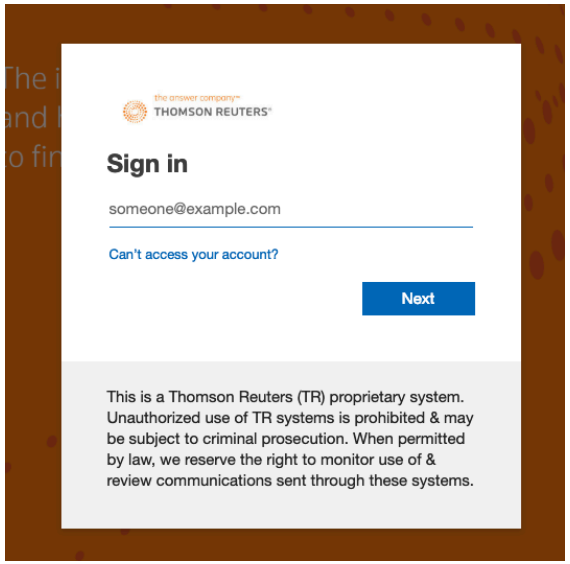
Who are our internal customers?

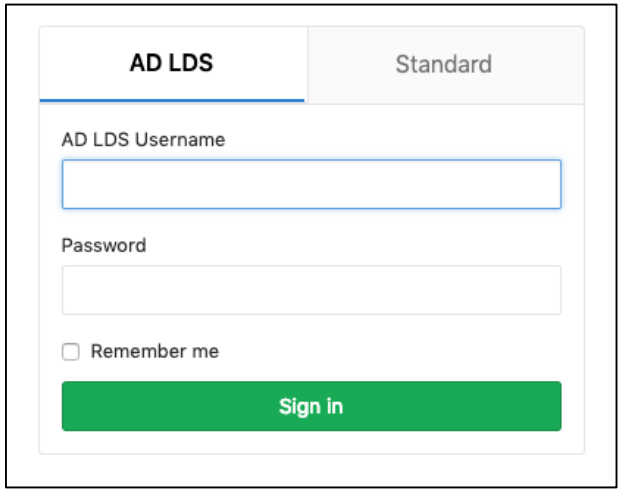
- ~35,000 workers
- ~4,000 apps
- Large user populations on most continents
- Access from anywhere
- Datacenter exit
- Cloud strategy

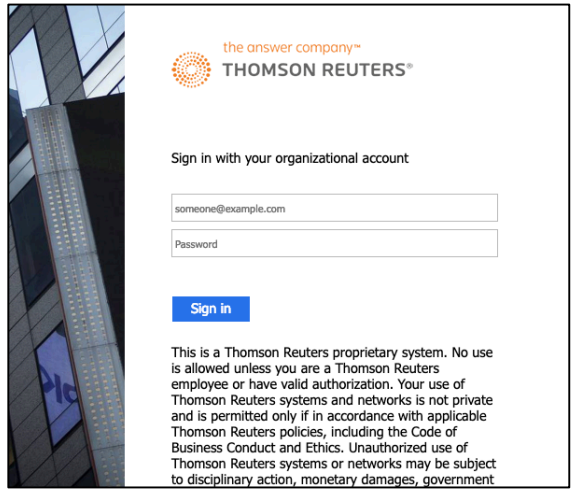
One username, one logon experience

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

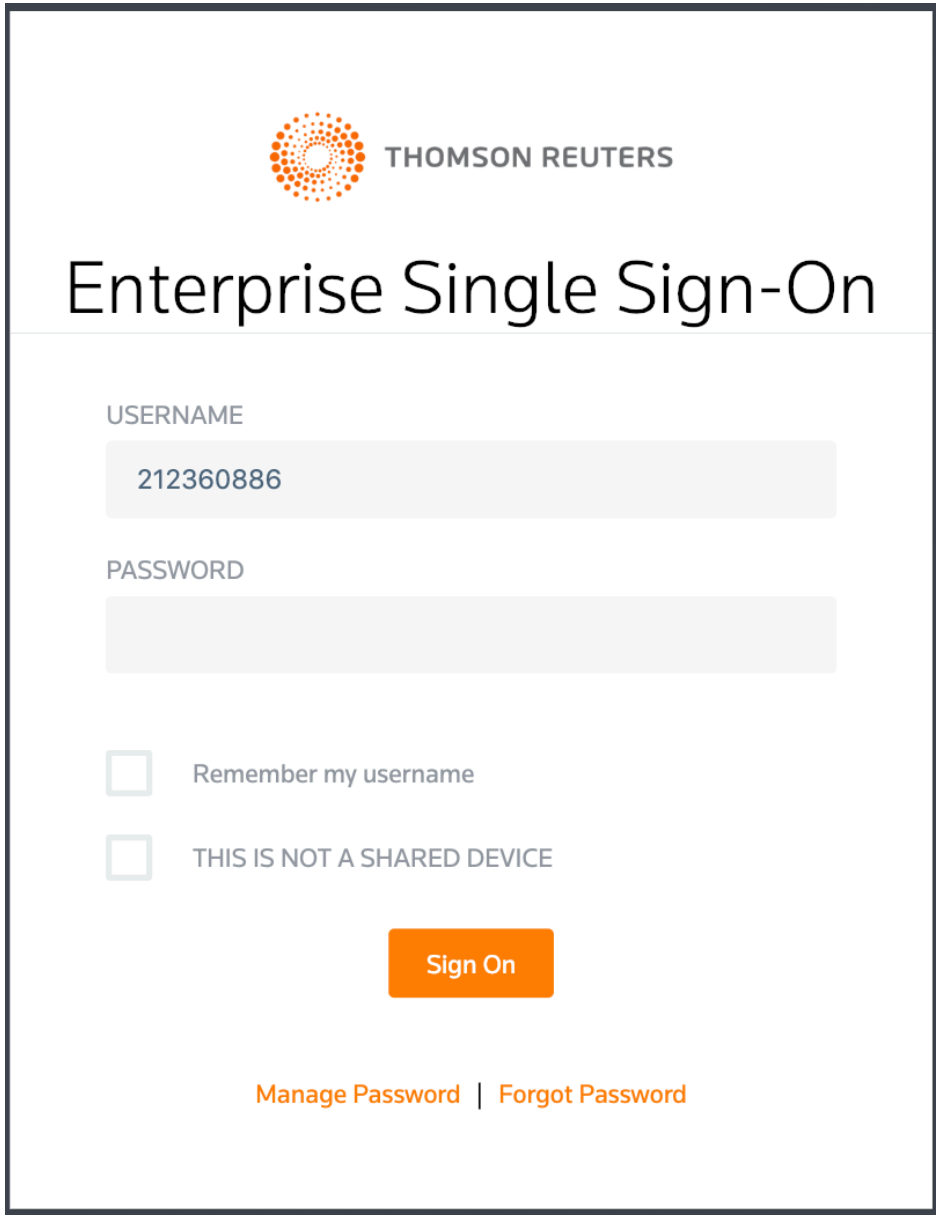








One username, one logon experience



- OpenID Connect
- OAuth 2
- SAML

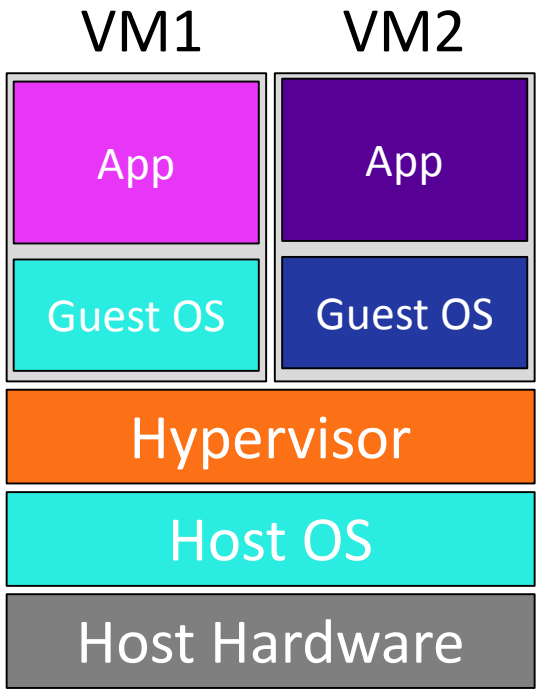
Multifactor as an extension of SSO

BYO… IDaaS?

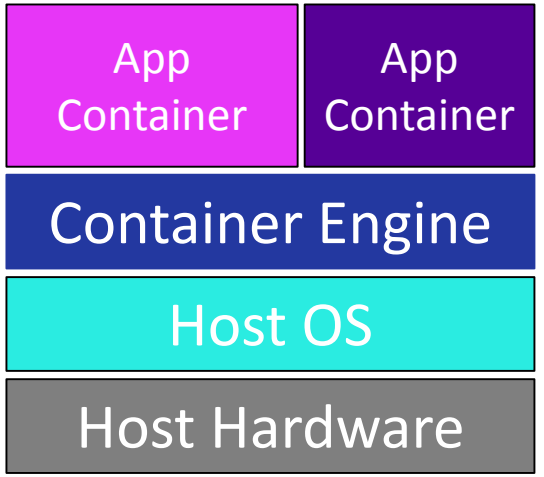
- Consumable through self-service
- On-prem shrinks, cloud footprint grows
- Global orgs should actually have global services
- Late-night ops incidents make me grouchy

Build, buy, or cloudify?

Native Cloud Services



Virtual Machines



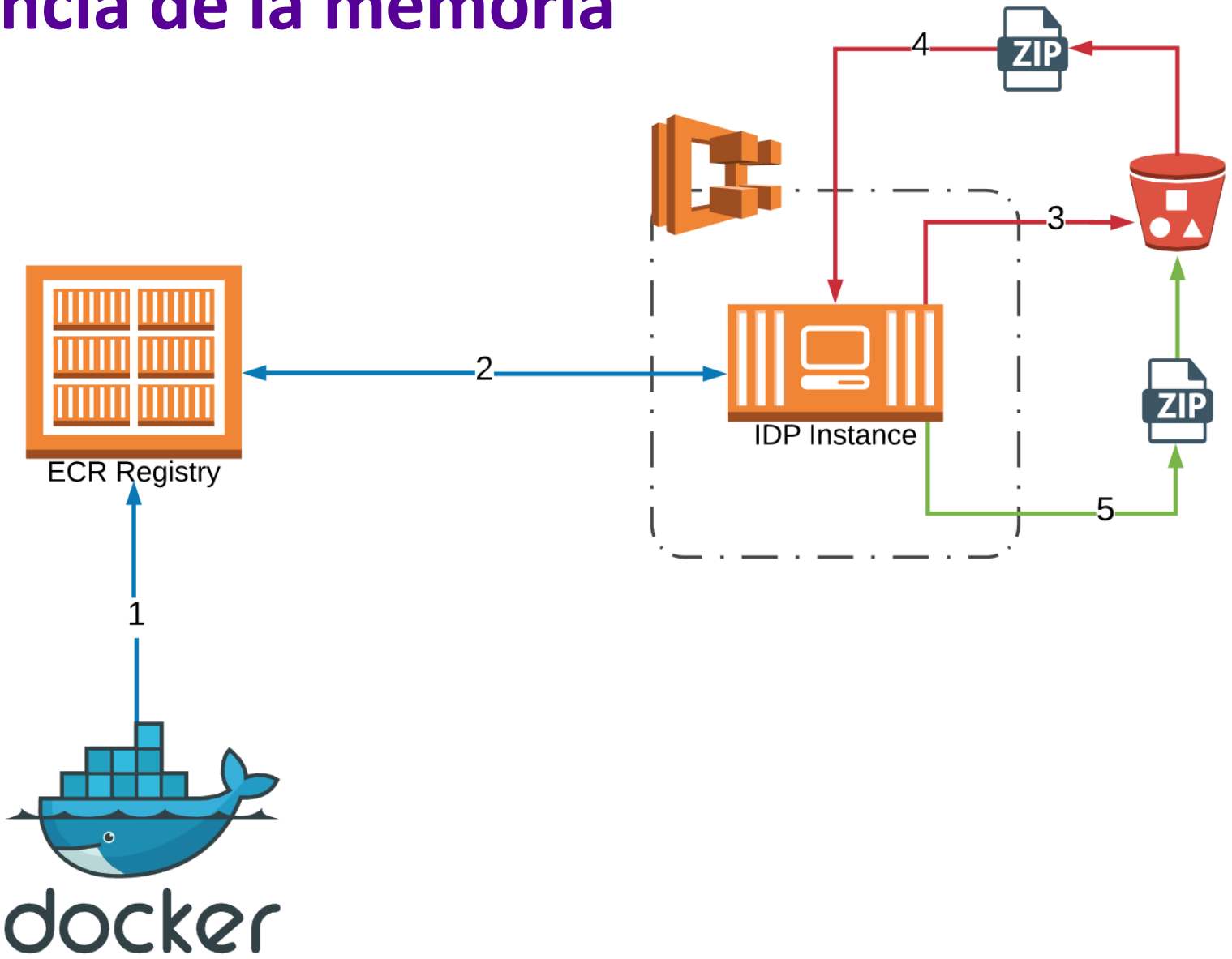
Containers

Containerizing an on-prem SSO product

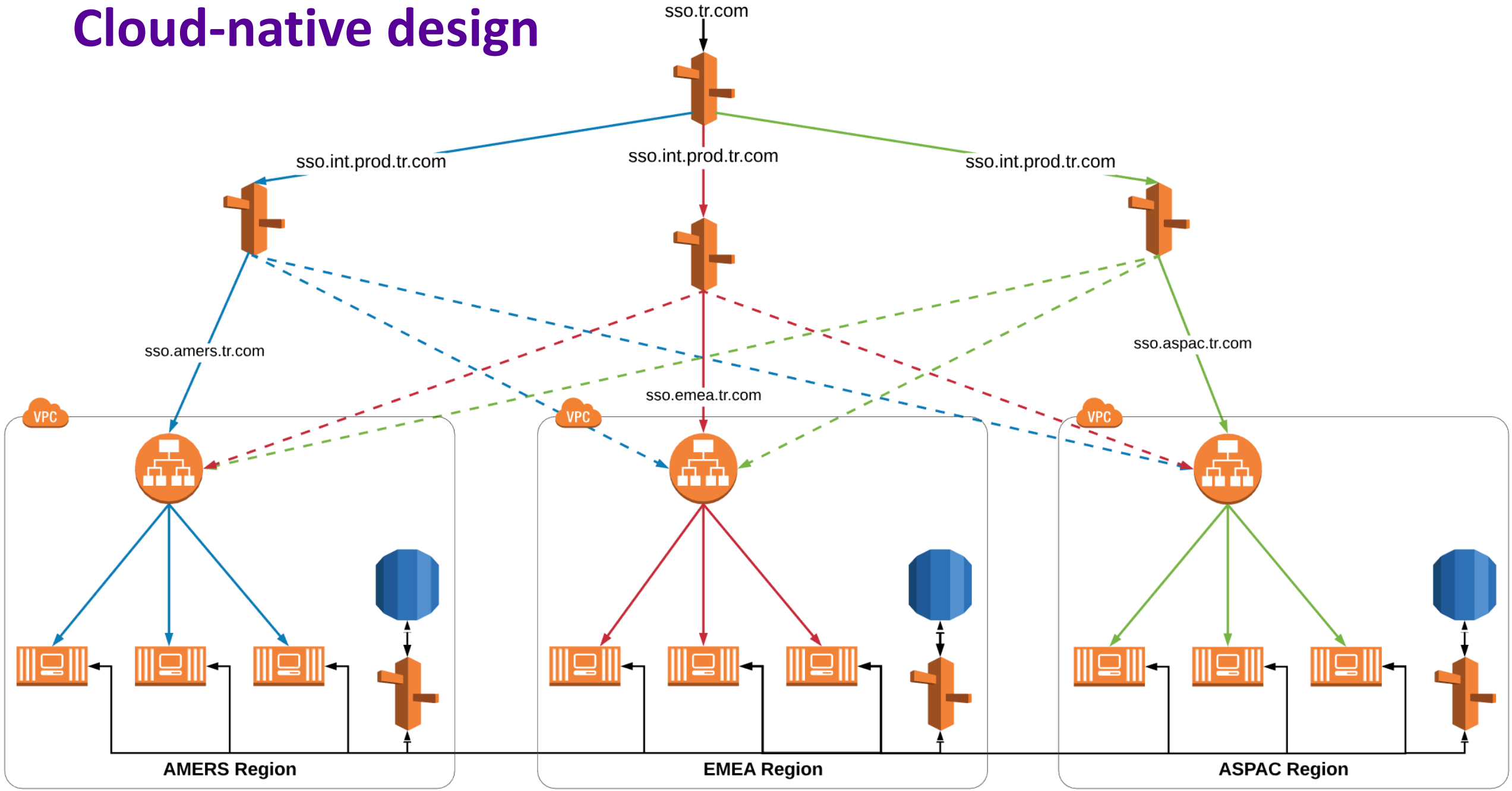
- Not a lot of vendor guidance or prior art (March 2018)
- Docker networking/AWS security group considerations
- No secrets in the dockerfile/configs
- No root users

Ship of Theseus

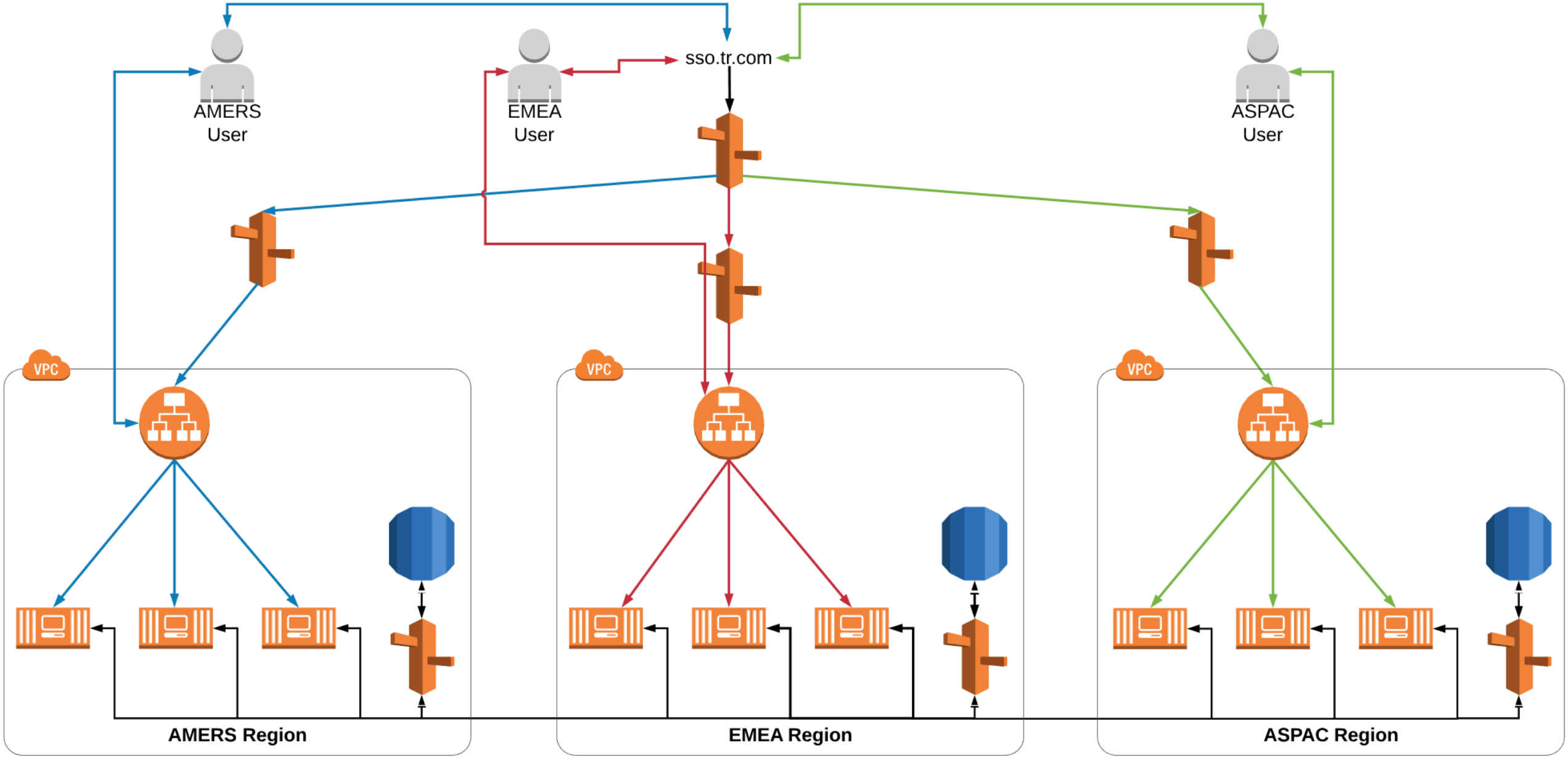
La persistencia de la memoria



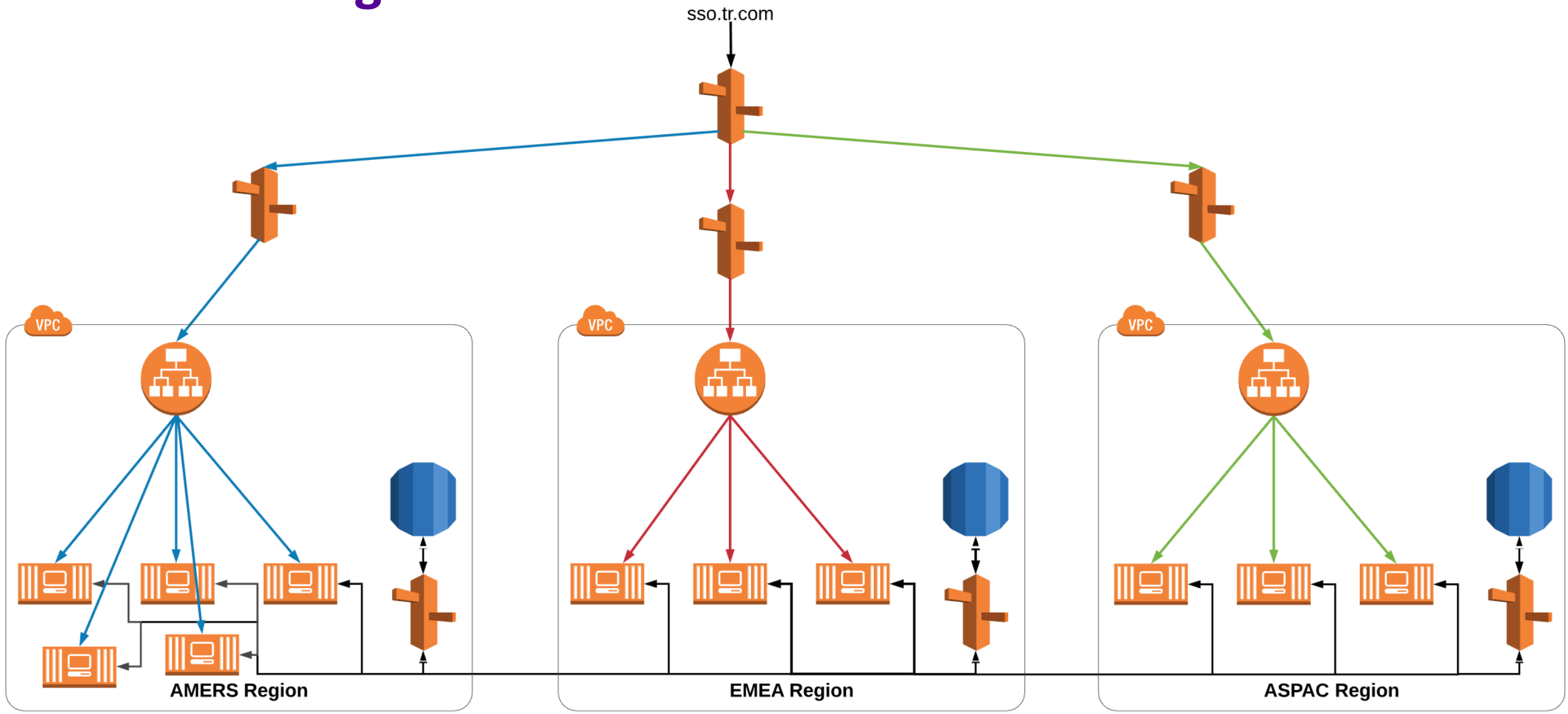
Cloud-native design



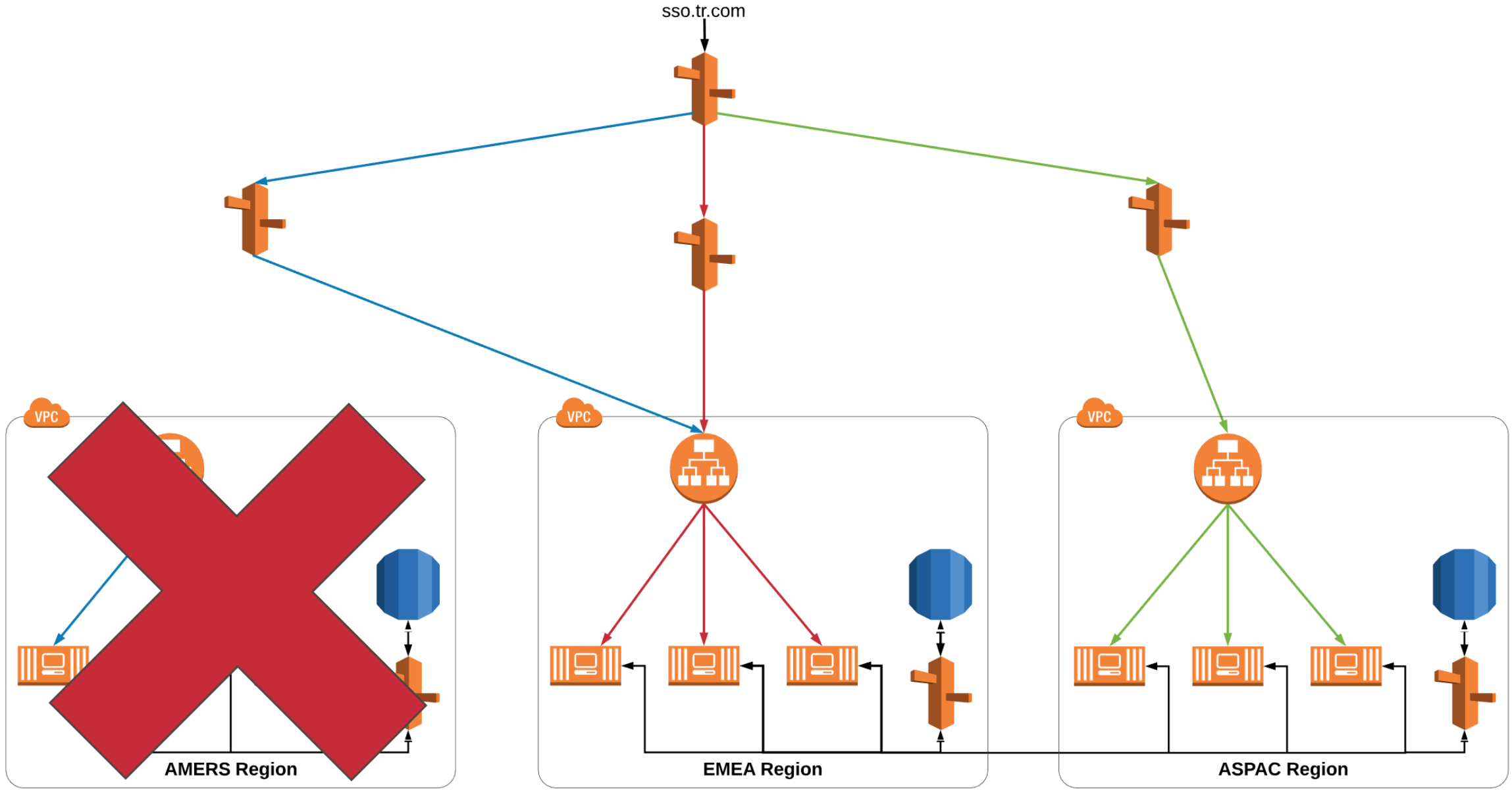
Location-aware routing & regional sub-clusters



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

RSAConference2019

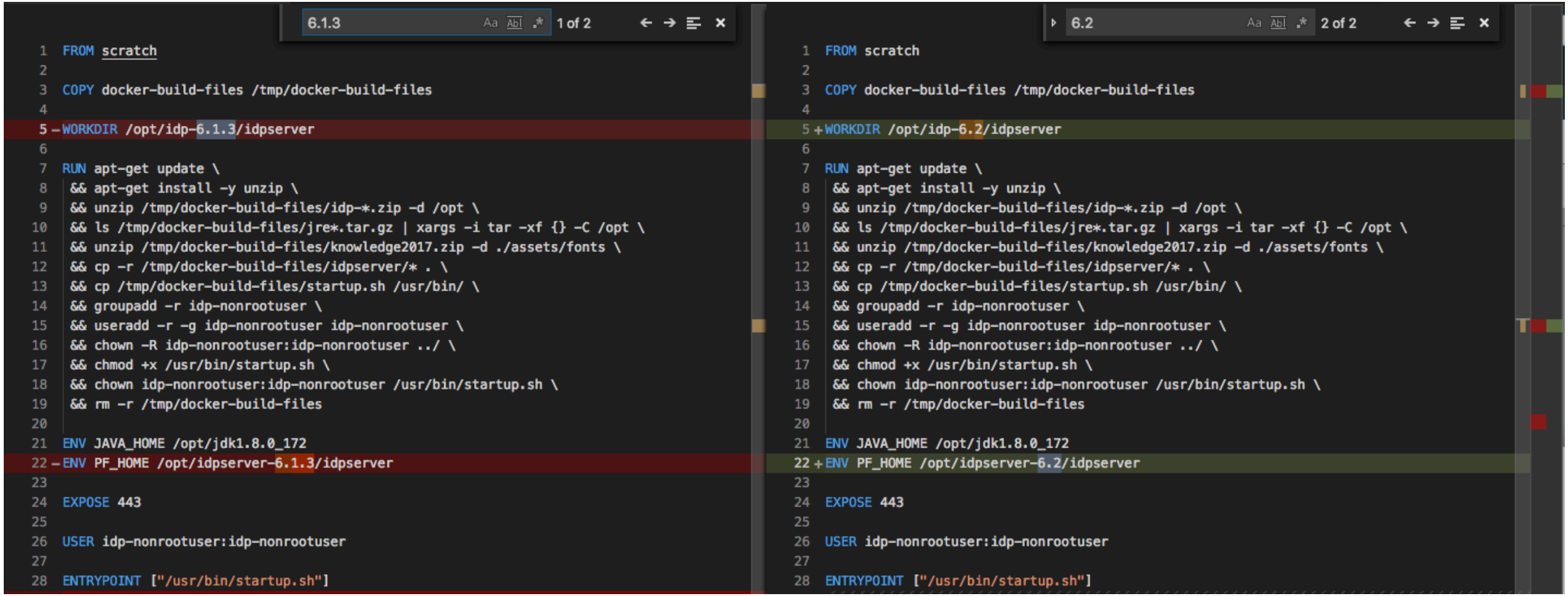
Impact of Infrastructure/Operations Automation

One script to rule them all

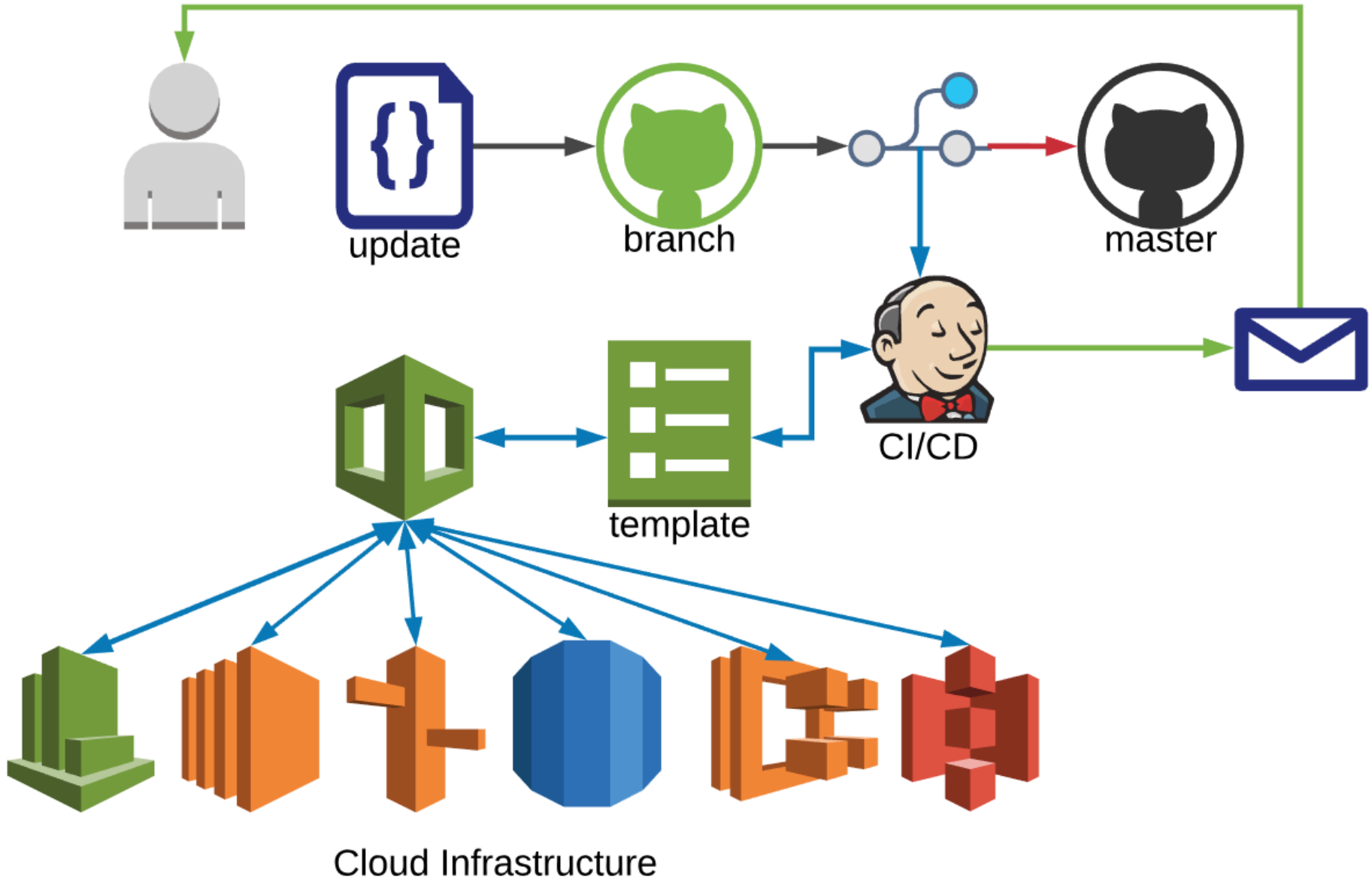
```
RBILoadBalancerIngressRule:
        Type: RBI::SCP::SecurityGroupIngress
        Description: Inbound rule for the RBI SLB, traffic limited to Bastion CoolDudeSecurityGroup
        DependsOn: RBILoadBalancerSecurityGroup
        Properties:
            FromPort: 443
            ToPort: 443
            GroupId: !Ref RBILoadBalancerSecurityGroup
            IpProtocol: TCP
            SourceSecurityGroupId: !Ref CoolDudeSecurityGroup

    RBILoadBalancerEgressRule:
        Type: RBI::SCP::SecurityGroupEgress
        Description: Outbound rule for RBI SLB, traffic goes to CORHostSecurityGroup on 4587
        DependsOn: RBILoadBalancerSecurityGroup
        Properties:
            FromPort: 4587
            ToPort: 4587
            GroupId: !Ref RBILoadBalancerSecurityGroup
            IpProtocol: TCP
            DestinationSecurityGroupId: !Ref CORHostSecurityGroup

    EngineLoadBalancerSecurityGroup:
        Type: RBI::SCP::SecurityGroup
        Description: Security group for the Engine SLB
        Properties:
            DDCId: !Ref DDC
            GroupDescription: Access to the load balancer that sits in front of COR
            Tags:
                - Key: Name
                  Value: !Sub ${EnvironmentName}-EngineSLB-${RBIRegionAbbreviation}-${EnvironmentType}
                - Key: tr:application-asset-insight-id
                  Value: !Ref AssetInsightID
                - Key: tr:environment-type
                  Value: !Ref EnvironmentType
                - Key: tr:resource-owner
                  Value: !Ref ResourceOwner
                - Key: tr:financial-identifier
                  Value: !Ref FinancialID

    EngineLoadBalancerIngressRule:
        Type: RBI::SCP::SecurityGroupIngress
        Description: Ingress rule for the Engine SLB, takes traffic from Bastion WebWorld Security Group
        DependsOn: EngineLoadBalancerSecurityGroup
        Properties:
            FromPort: 443
            ToPort: 443
            GroupId: !Ref EngineLoadBalancerSecurityGroup
            IpProtocol: TCP
            SourceSecurityGroupId: !Ref WebWorldSecurityGroup

    EngineLoadBalancerEgressRule:
        Type: RBI::SCP::SecurityGroupEgress
        Description: Outbound rule for Engine SLB, traffic goes to CORHostSecurityGroup on 3333
        DependsOn: EngineLoadBalancerIngressRule
        Properties:
            FromPort: 3333
```

```
RBILoadBalancerIngressRule:
        Type: RBI::SCP::SecurityGroupIngress
        Description: Inbound rule for the RBI SLB, traffic limited to Bastion CoolDudeSecurityGroup
        DependsOn: RBILoadBalancerSecurityGroup
        Properties:
            FromPort: 443
            ToPort: 443
            GroupId: !Ref RBILoadBalancerSecurityGroup
            IpProtocol: TCP
            SourceSecurityGroupId: !Ref CoolDudeSecurityGroup

    # RBILoadBalancerEgressRule:
    #     Type: RBI::SCP::SecurityGroupEgress
    #     Description: Outbound rule for RBI SLB, traffic goes to CORHostSecurityGroup on 4587
    #     DependsOn: RBILoadBalancerSecurityGroup
    #     Properties:
    #         FromPort: 4587
    #         ToPort: 4587
    #         GroupId: !Ref RBILoadBalancerSecurityGroup
    #         IpProtocol: TCP
    #         DestinationSecurityGroupId: !Ref CORHostSecurityGroup

    EngineLoadBalancerSecurityGroup:
        Type: RBI::SCP::SecurityGroup
        Description: Security group for the Engine SLB
        Properties:
            DDCId: !Ref DDC
            GroupDescription: Access to the load balancer that sits in front of COR
            Tags:
                - Key: Name
                  Value: !Sub ${EnvironmentName}-EngineSLB-${RBIRegionAbbreviation}-${EnvironmentType}
                - Key: tr:application-asset-insight-id
                  Value: !Ref AssetInsightID
                - Key: tr:environment-type
                  Value: !Ref EnvironmentType
                - Key: tr:resource-owner
                  Value: !Ref ResourceOwner
                - Key: tr:financial-identifier
                  Value: !Ref FinancialID

    # EngineLoadBalancerIngressRule:
    #     Type: RBI::SCP::SecurityGroupIngress
    #     Description: Ingress rule for the Engine SLB, takes traffic from Bastion WebWorld Security Group
    #     DependsOn: EngineLoadBalancerSecurityGroup
    #     Properties:
    #         FromPort: 443
    #         ToPort: 443
    #         GroupId: !Ref EngineLoadBalancerSecurityGroup
    #         IpProtocol: TCP
    #         SourceSecurityGroupId: !Ref WebWorldSecurityGroup

    EngineLoadBalancerEgressRule:
        Type: RBI::SCP::SecurityGroupEgress
        Description: Outbound rule for Engine SLB, traffic goes to CORHostSecurityGroup on 3333
        DependsOn: EngineLoadBalancerIngressRule
        Properties:
            FromPort: 3333
```

Product upgrades



Continuous integration, continuous deployment



Self-service through dynamic client registration

```
POST /as/clients.oauth2 HTTP/1.1
Content-Type: application/json
Accept: application/json
Authorization: Bearer eyJhbGciOiJSUzI1NiIsImtpZCI6ImsxIn0
Host: sso.thomsonreuters.com

{
  "client_name":"Jon's Cool App",
  "redirect_uris":[
    "https://redbeardidentity.com/coolapp",
    "https://redbeardidentity.com/coolerapp"
  ],
  "scope":"openid profile mfa",
  "grant_types":[
    "authorization_code",
    "refresh_token"
  ]
}
```

```
HTTP/1.1 201 Created
Date: Fri, 21 Oct 2018 15:30:00 GMT
Referrer-Policy: origin
Content-Type: application/json
Transfer-Encoding: chunked

{
  "client_id": "dc-rqUtii4vRXj5NMztkAeJ1S",
  "client_name": "Jon's Cool App",
  "redirect_uris": [
    "https://redbeardidentity.com/coolapp",
    "https://redbeardidentity.com/coolerapp"
  ],
  "token_endpoint_auth_method": "client_secret_basic",
  "grant_types": [
    "authorization_code",
    "refresh_token"
  ],
  "client_secret": "p7MD0Ul1DNI9xRDc5kcOxs",
  "client_secret_expires_at": 0,
  "scope": "openid profile mfa",
  "validate_using_all_eligible_atms": false,
  "refresh_token_rolling_policy": "server_default",
  "persistent_grant_expiration_type": "server_default",
  "grant_access_session_revocation_api": false
}
```

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

RSAConference2019

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

RSAConference2019

You can automate your enterprise app auth.

RSAConference2019

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

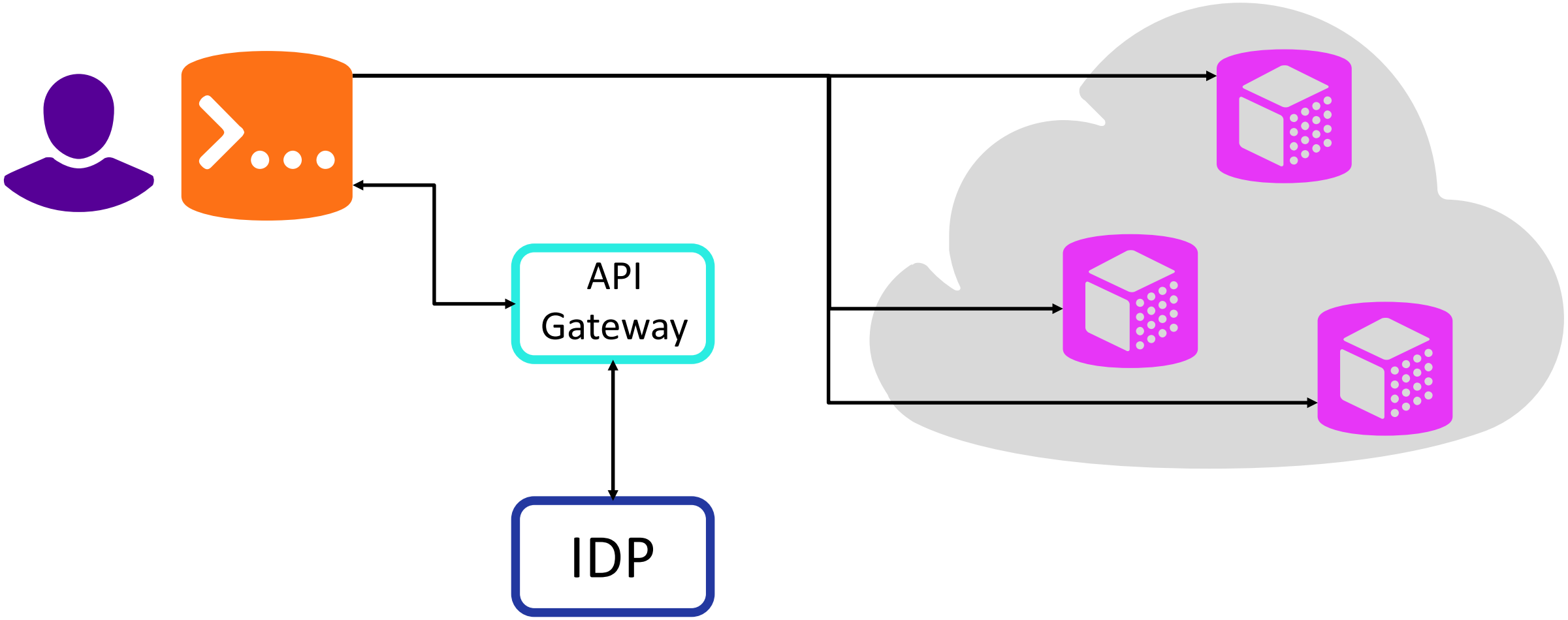
Who are our customers?

- 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

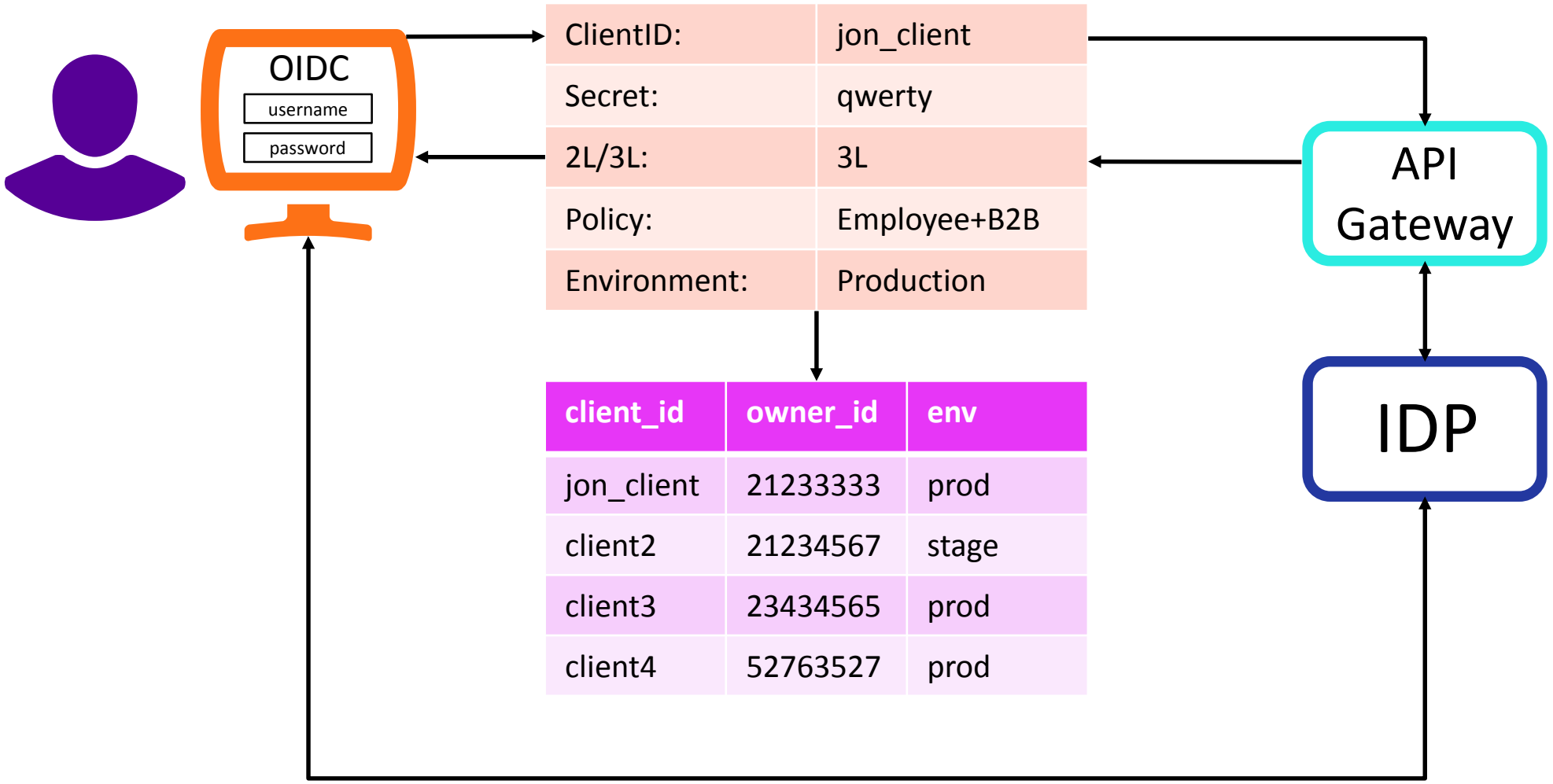
RSAConference2019

Self-Service is the new automation

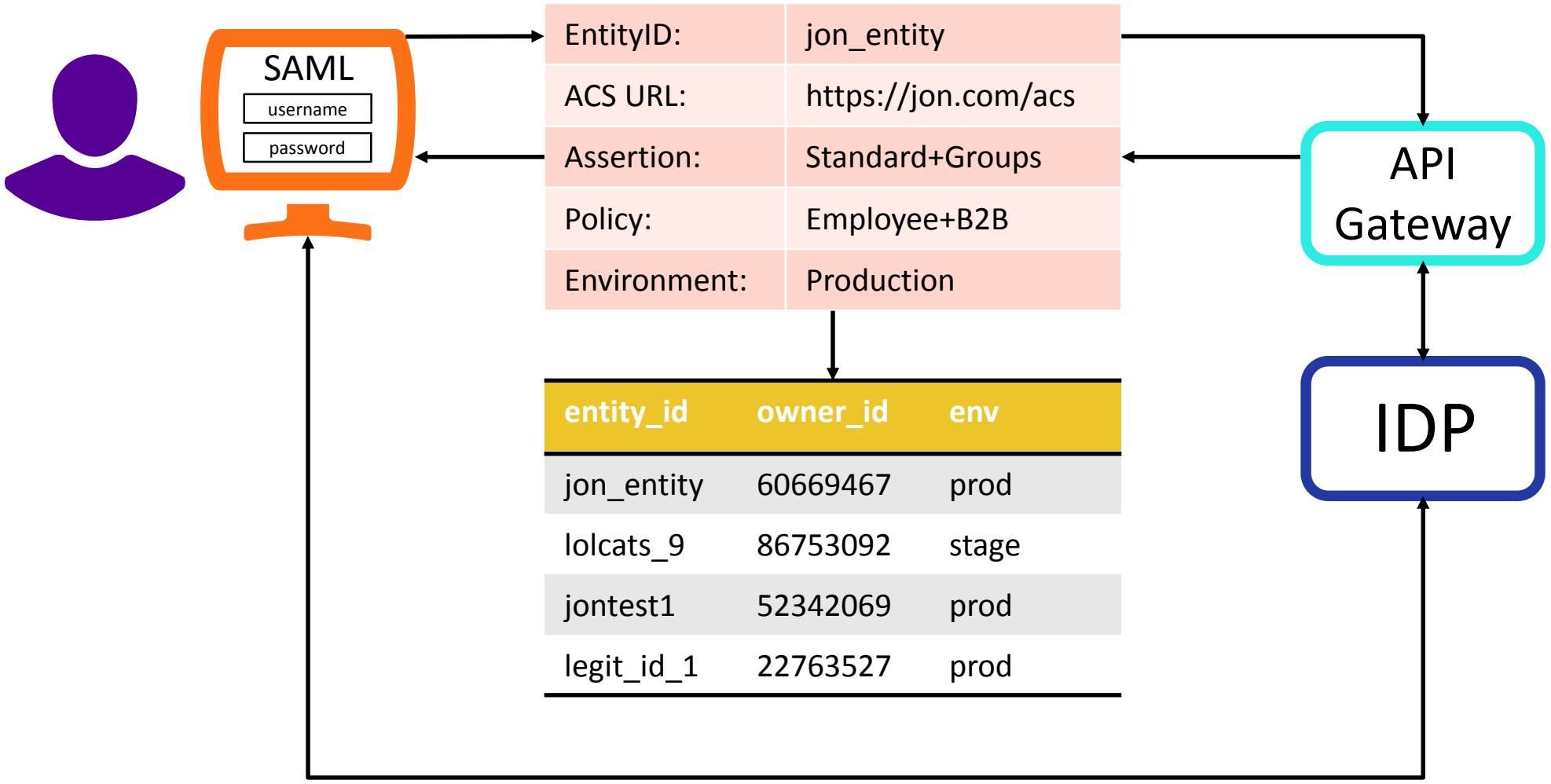
Q4 2015 Self-Service API



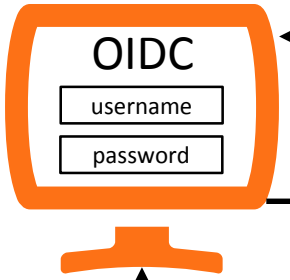
Web Portal (Create)



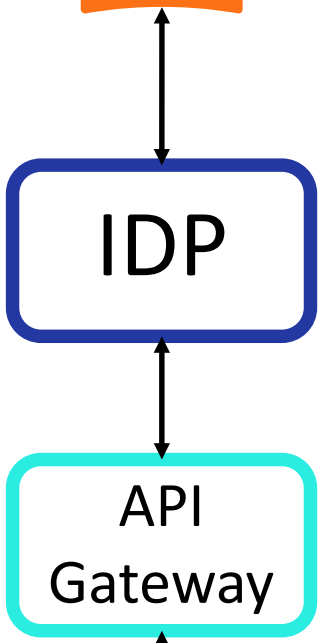
Web Portal (Create)



Web Portal (Read, Update, Delete)



ClientID	Secret	Environment	2L/3L	Policy
jon_client	CHANGE	Prod	3L	Employee+B2B
jon_client2	CHANGE	Prod	2L	N/A



client_id	owner_id	env
jon_client	21233333	prod
client2	21234567	stage
jon_client2	21233333	prod
client4	52763527	prod

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

RSAConference2019

Impact of Service Delivery Automation

Adoption of authentication services

June 2015

800 clients

37 OIDC

SAML

900 Service Providers

7200 applications

June 2017

10,048 clients

8,515 OIDC

SAML

5,005 Service Providers

¯_(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

RSAConference2019

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