Migrating Microsoft Applications to AWS like an Expert

Danny Jenkins, Solutions Architect

August 2018

aws

What Will You Takeaway From This Session?

- This is a 300 level session
- Holistic approach to migrating Microsoft Workloads
- Move fast…dive deep where necessary
- QR codes are frustrating – Links on the website http://unicornshop.lol

aws

Who Are Unicorn Shop?

“To enable anyone with the dream of being a unicorn to look like one”

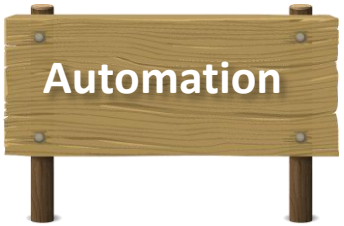
Unicornshop.lol

- Online ecommerce offering
- Brick and mortar stores
- CMS, back office applications
- .NET and SQL custom applications
- Email hosted in O365

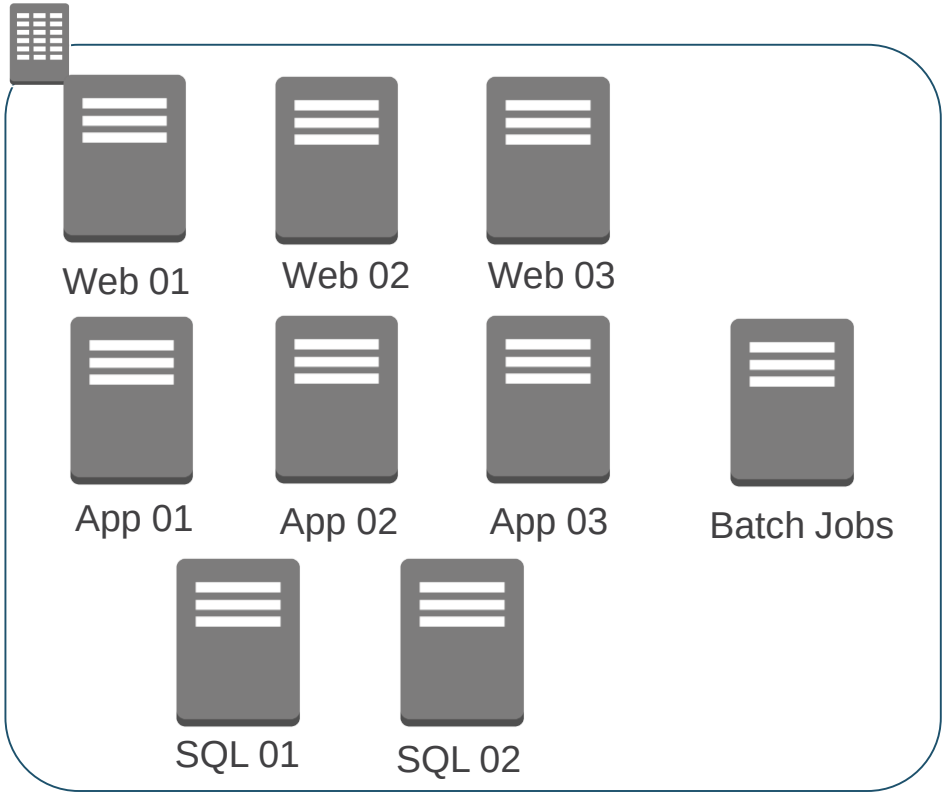
Issues:

- Wasted resources
- Capex vs Opex model
- Developers restrained and can’t help the business speed up

Migration Approach

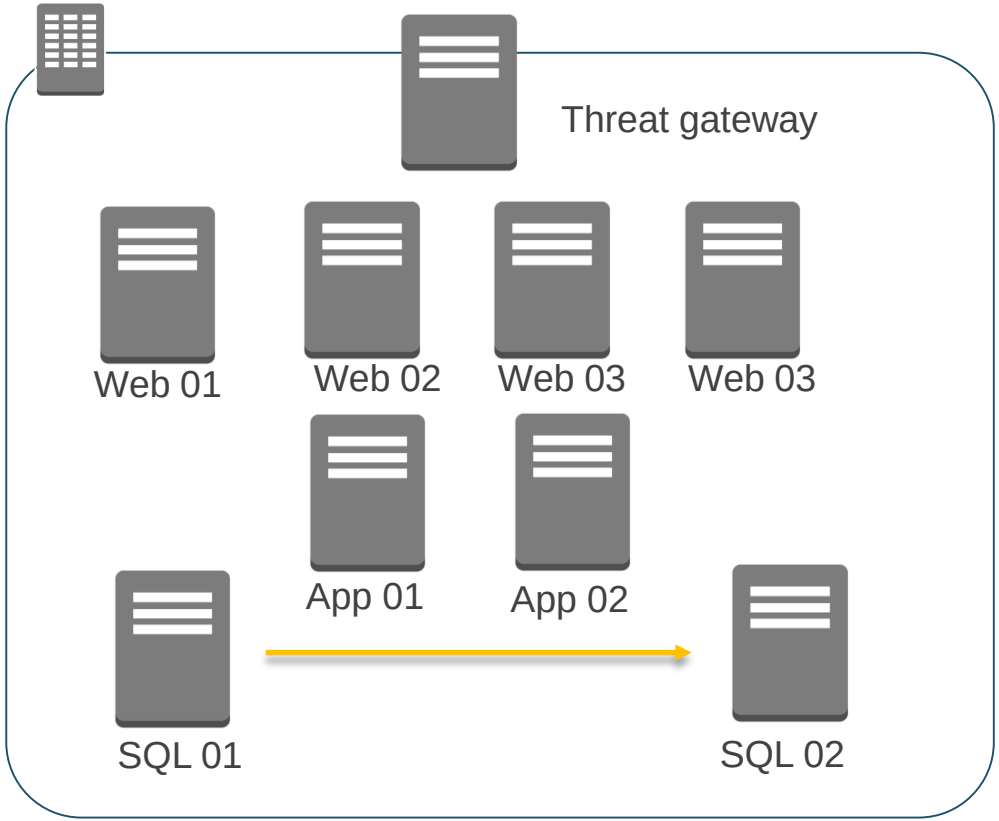


Our Web Store (PCI Compliant)



- PCI compliant workload
- Need to restrict user access to some components
- Limited to specific services
- Need to monitor access patterns

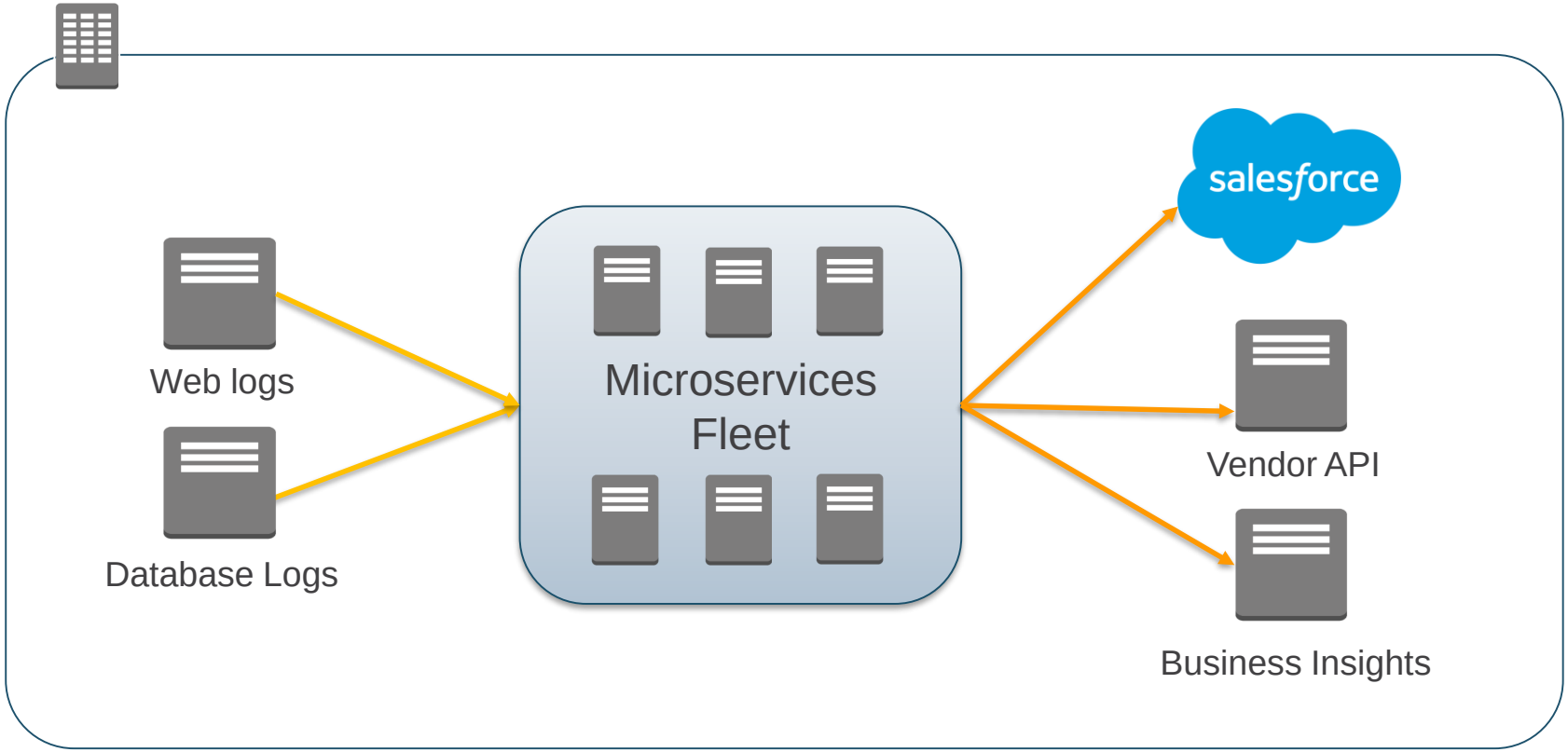
Our CMS Deployment



- Legacy threat management SPOF
- Unable to keep up to date with threat definition templates

Application Review

Microservices Deployment



Application Review

So Let’s Go!! ....Almost…

Strategy	Plan	Build & Migrate		Run
Existing IT estate evaluation	Planning & Discovery	Application design	Migration & Validation	Operation
		Application 1	Application 1	
		Application 2	Application 2	

Services from AWS ecosystem

AWS Application discovery service

AWS DMS

AWS SMS

Amazon Cloudwatch

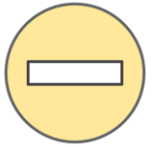
AWS Config

Approaching The Migration With The 6 R's

Retain

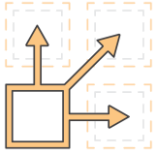
Replatform

Retire



Refactor

Rehost

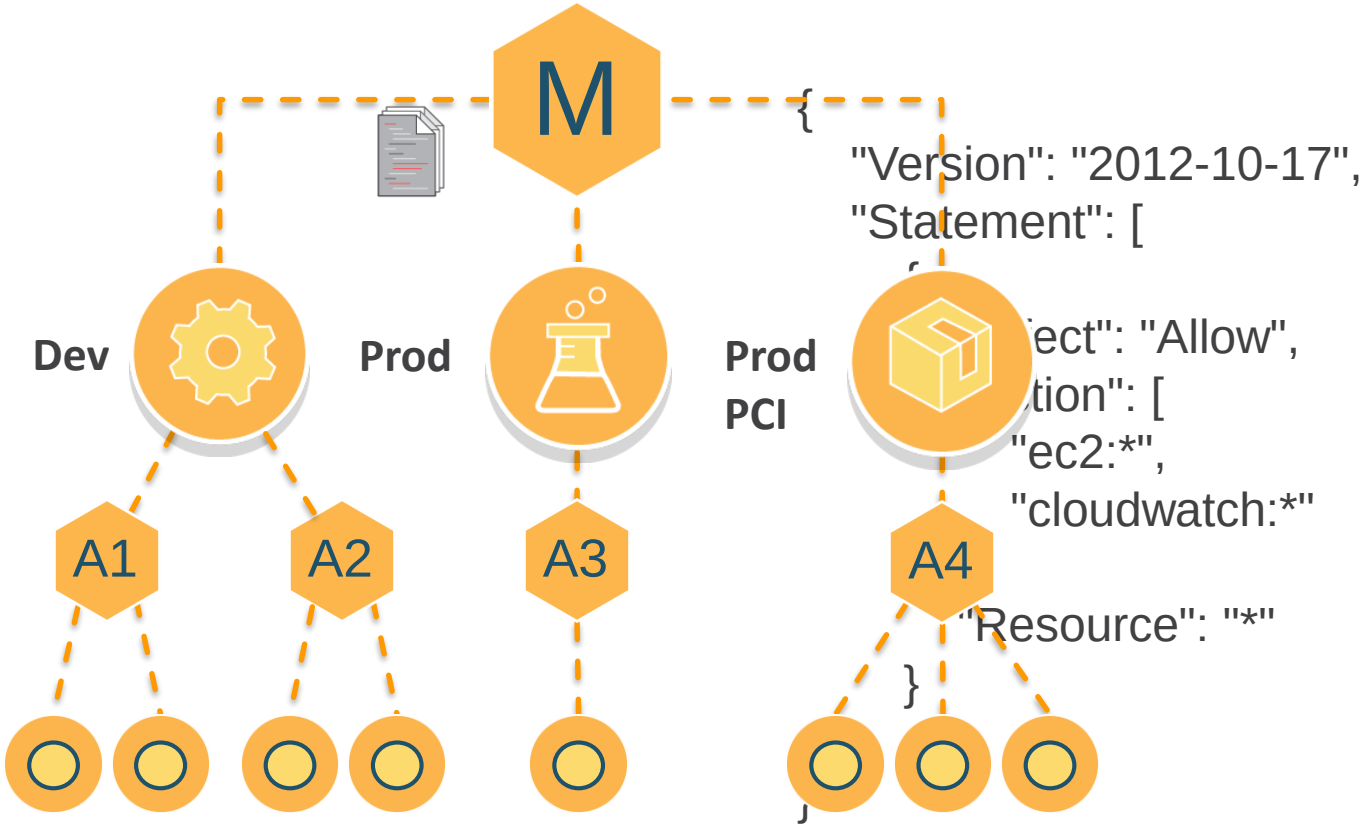


Repurchase

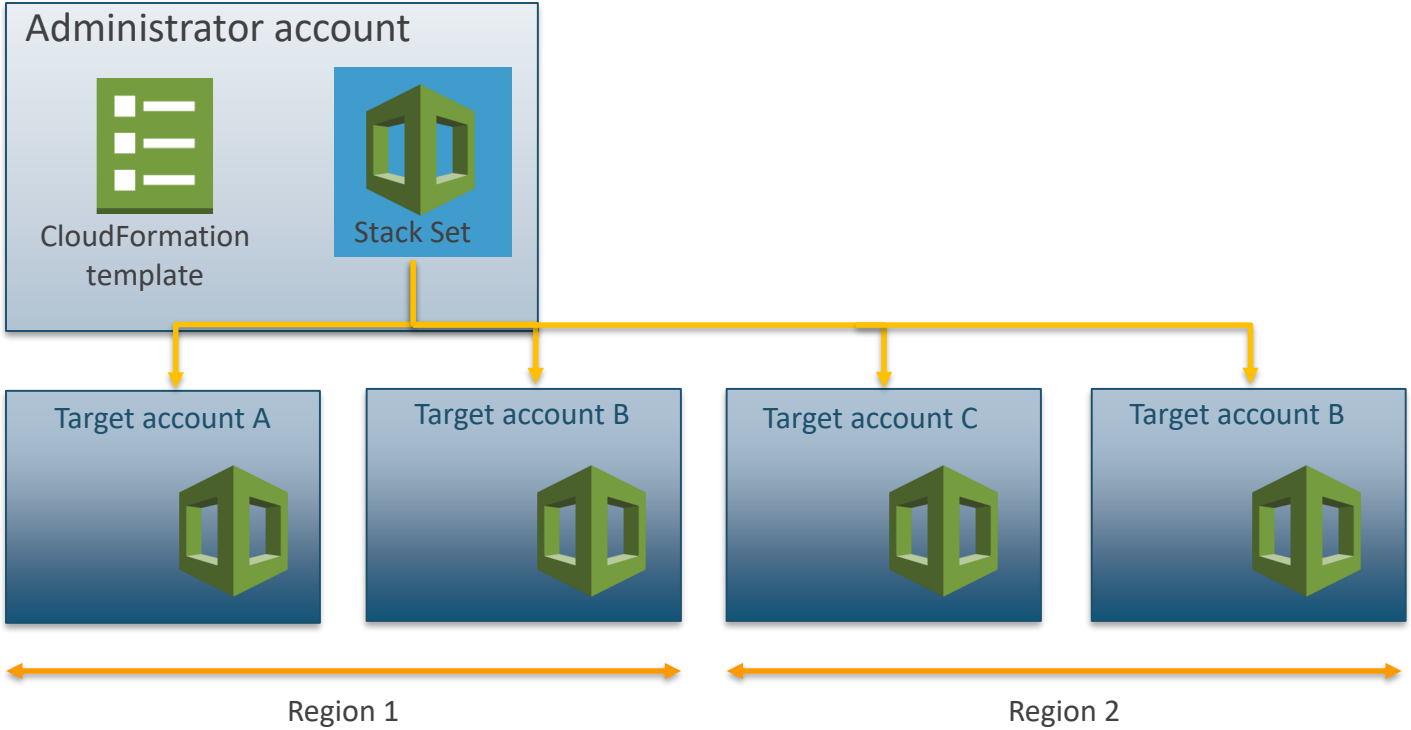
Building Our Landing Zone

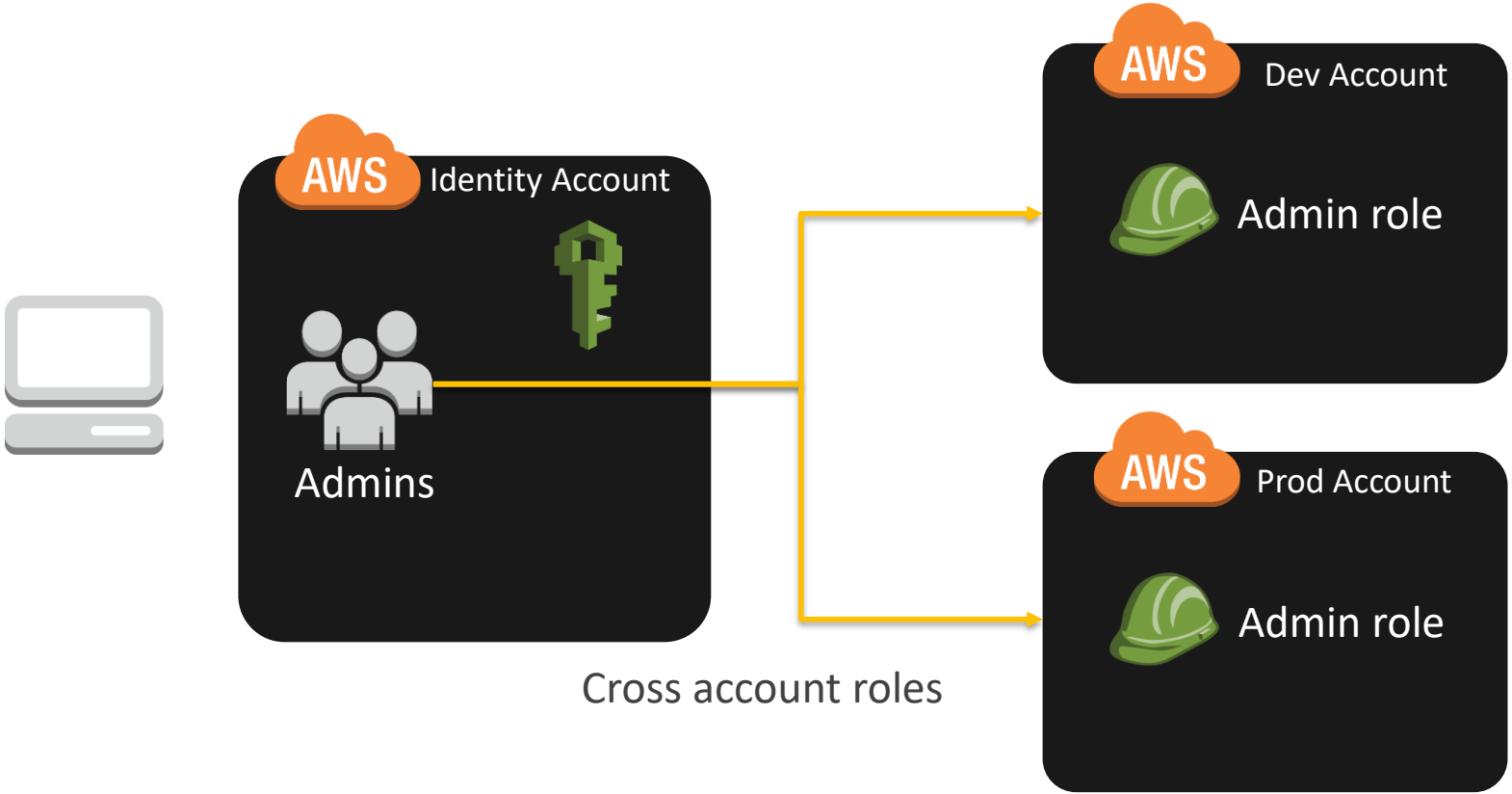
- Multiple accounts in Organisations + SCPs
- How to create a **monolithic** identity approach
  (don't judge me quite yet…)
- Amazon GuardDuty event execution
- AWS Config enforcing encryption demo
- Connectivity to support our Hybrid state during migration

Let’s Deploy Our Organisation’s Structure



Identity As A Monolith?





Landing Zone

Stack Set

Demo

Amazon GuardDuty – Event Execution

Recon:EC2/PortProbeUnprotectedPort

EC2 instance has an unprotected port which is being probed by a known malicious host.

Severity	Region	Count
Low	ap-southe...	49
Account ID	**Resource ID**	**Threat list name**
[redacted]	i-0bb7606...	ProofPoint

UnauthorizedAccess:EC2/SSHBruteForce

[redacted] is performing SSH brute force attacks against i-0ad41[redacted]. Brute force attacks are used to gain unauthorized access to your instance by guessing the SSH password.

Severity	Region	Count
Low	ap-southeast-2	2
Account ID	**Resource ID**	
[redacted]	i-0ad41[redacted]	

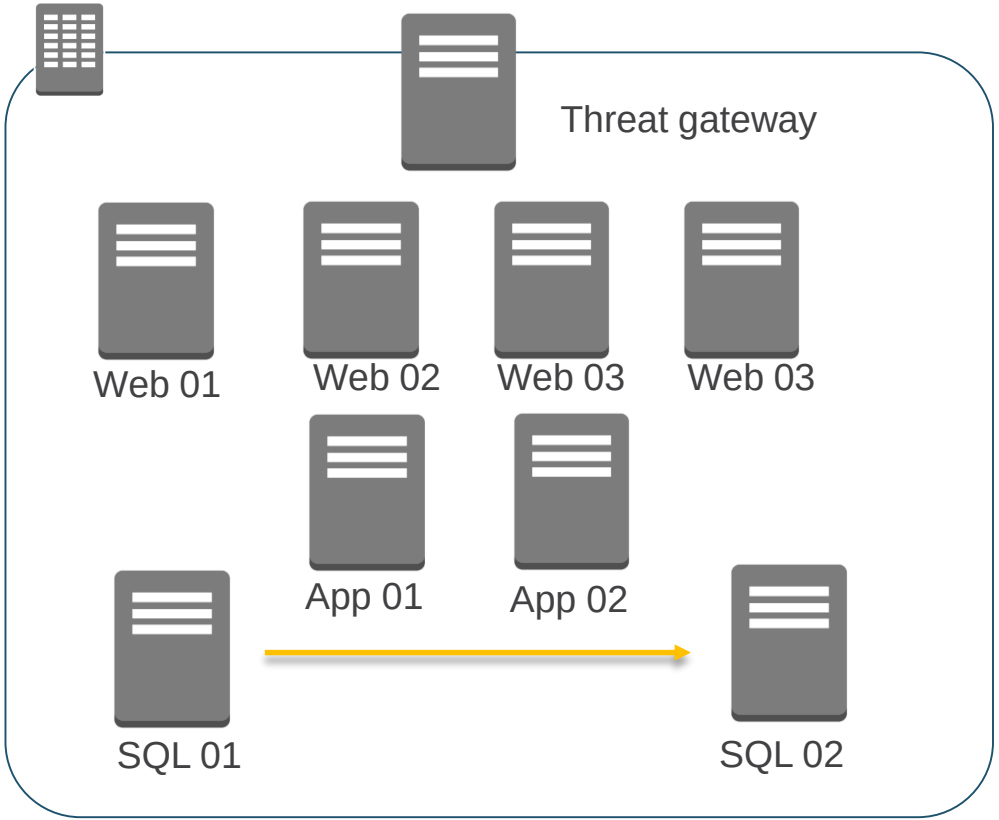
Last seen
2018-01-27 02:55:56 (a month ago)

Amazon GuardDuty

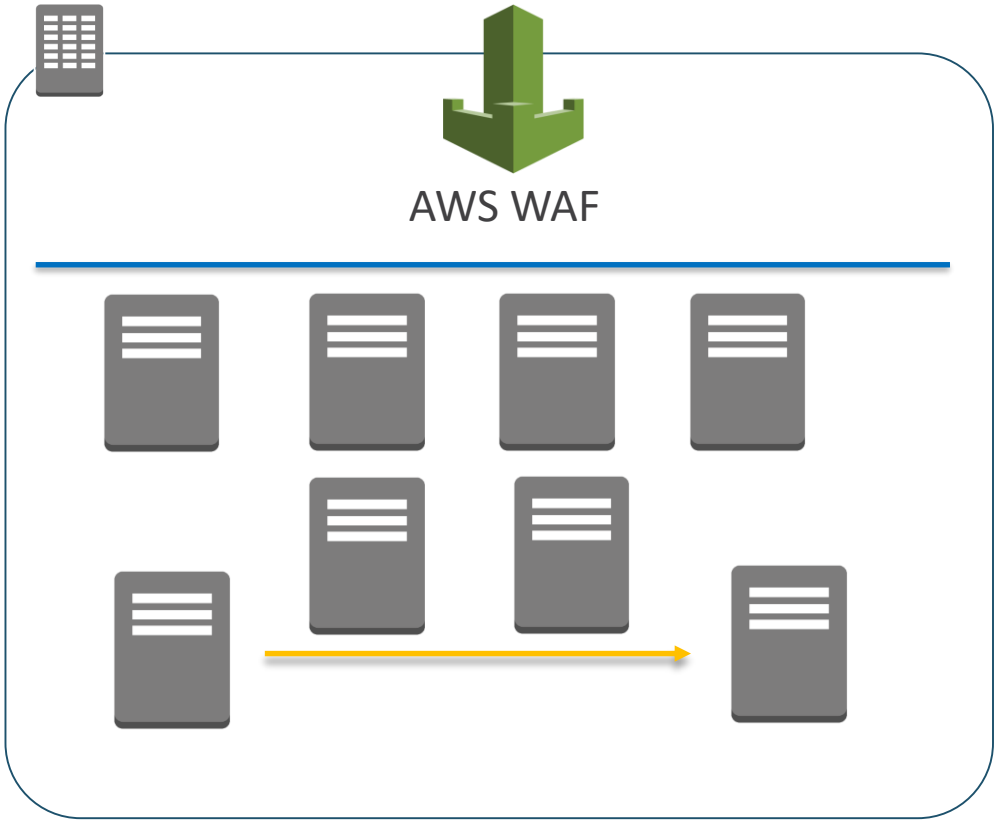
```
aws events put-rule --name Test --event-pattern "{\"source\":[\"aws.guardduty\"]}“

aws events put-rule --name Test --event-pattern "{\"source\":[\"aws.guardduty\"],\"detail-type\":[\"GuardDuty Finding\"],\"detail\":{\"severity\":[5.0,8.0]}}“

aws events put-targets --rule Test --targets Id=1,Arn=arn:aws:lambda:us-east-1:111122223333:function:<your_function>
```

Landing Zone

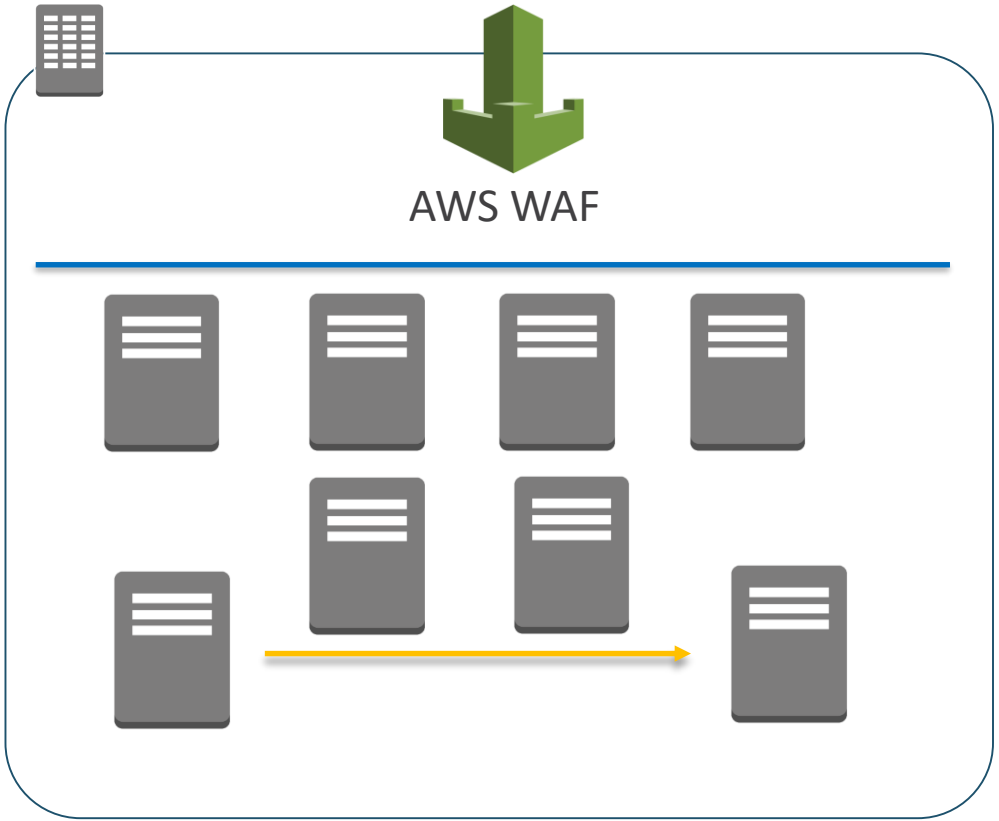
Our CMS Threat Management Layer



AWS WAF – Managed web application firewall



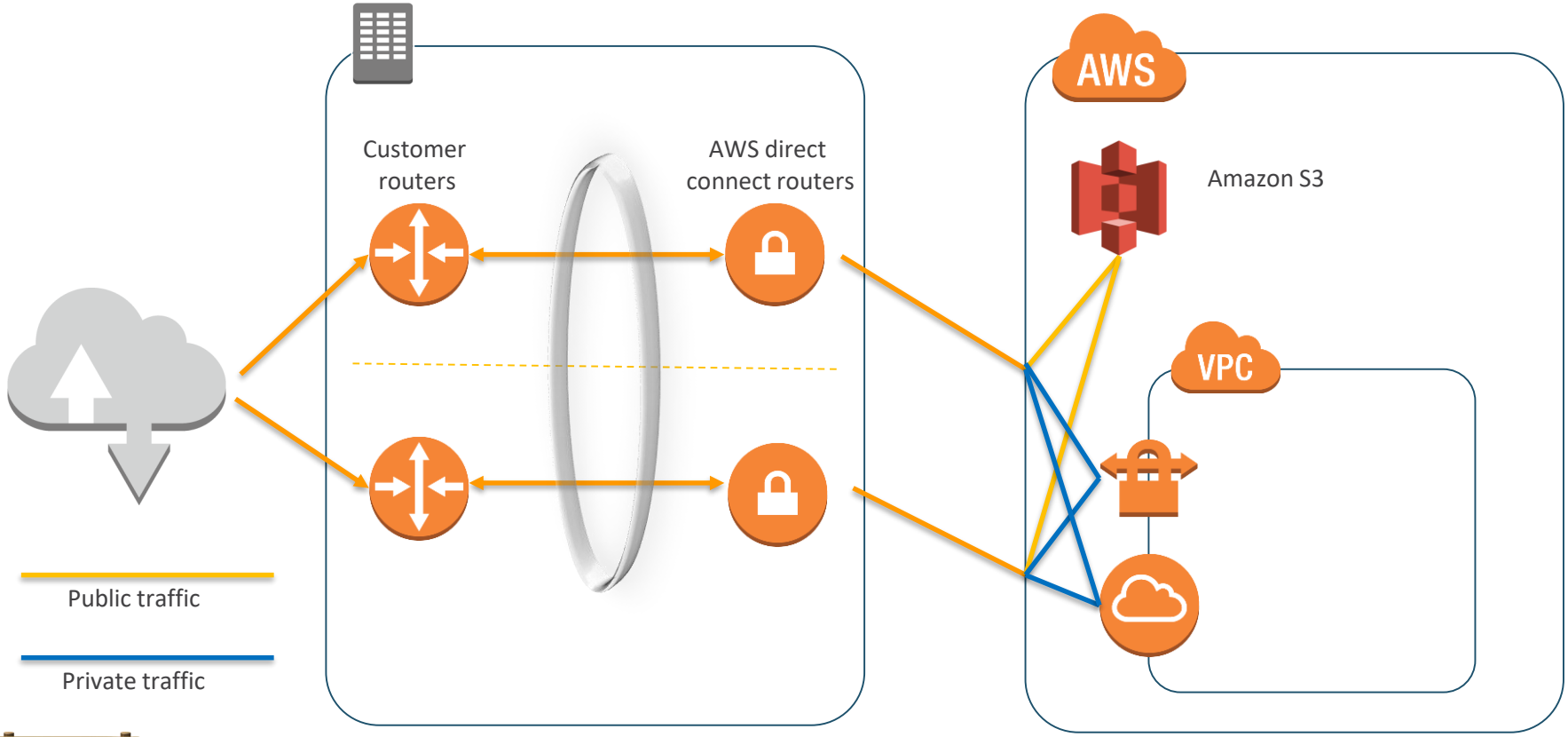
AWS WAF – Working with managed rulesets



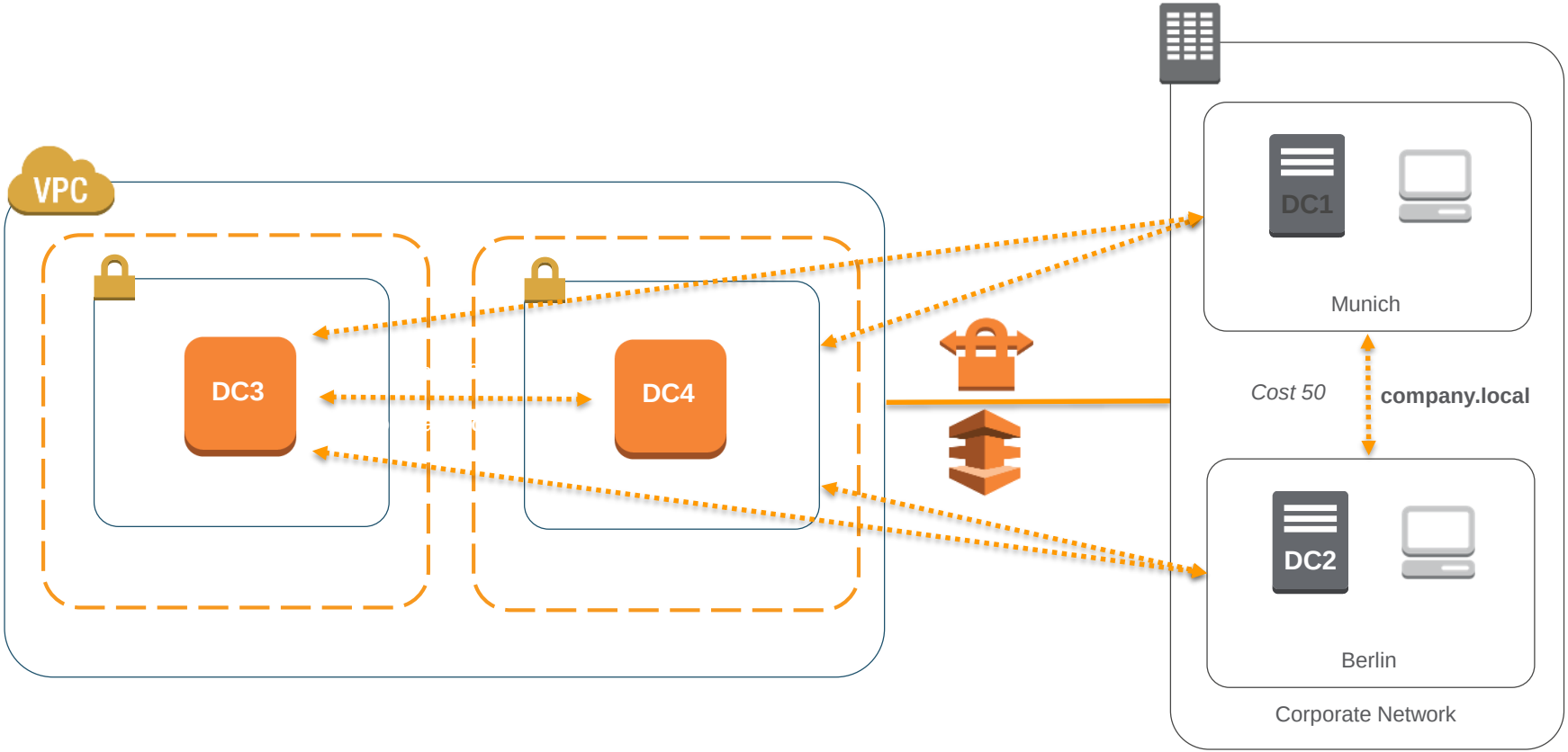
- PCI
- OWASP Top 10
- Bot protection
- SQLi/XSS
- IP reputation
- CMS protection

aws

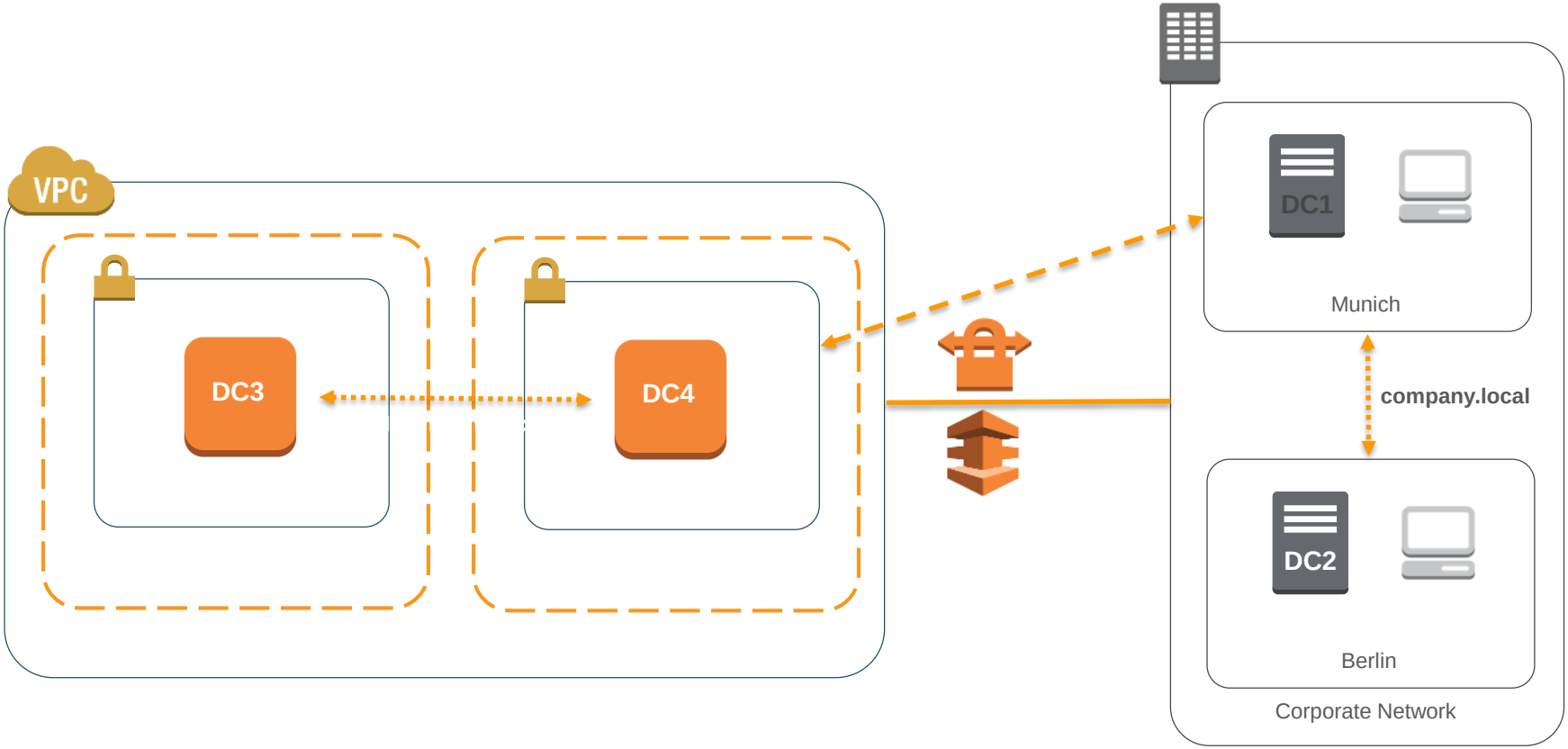
Let’s Get Our Networking Right…



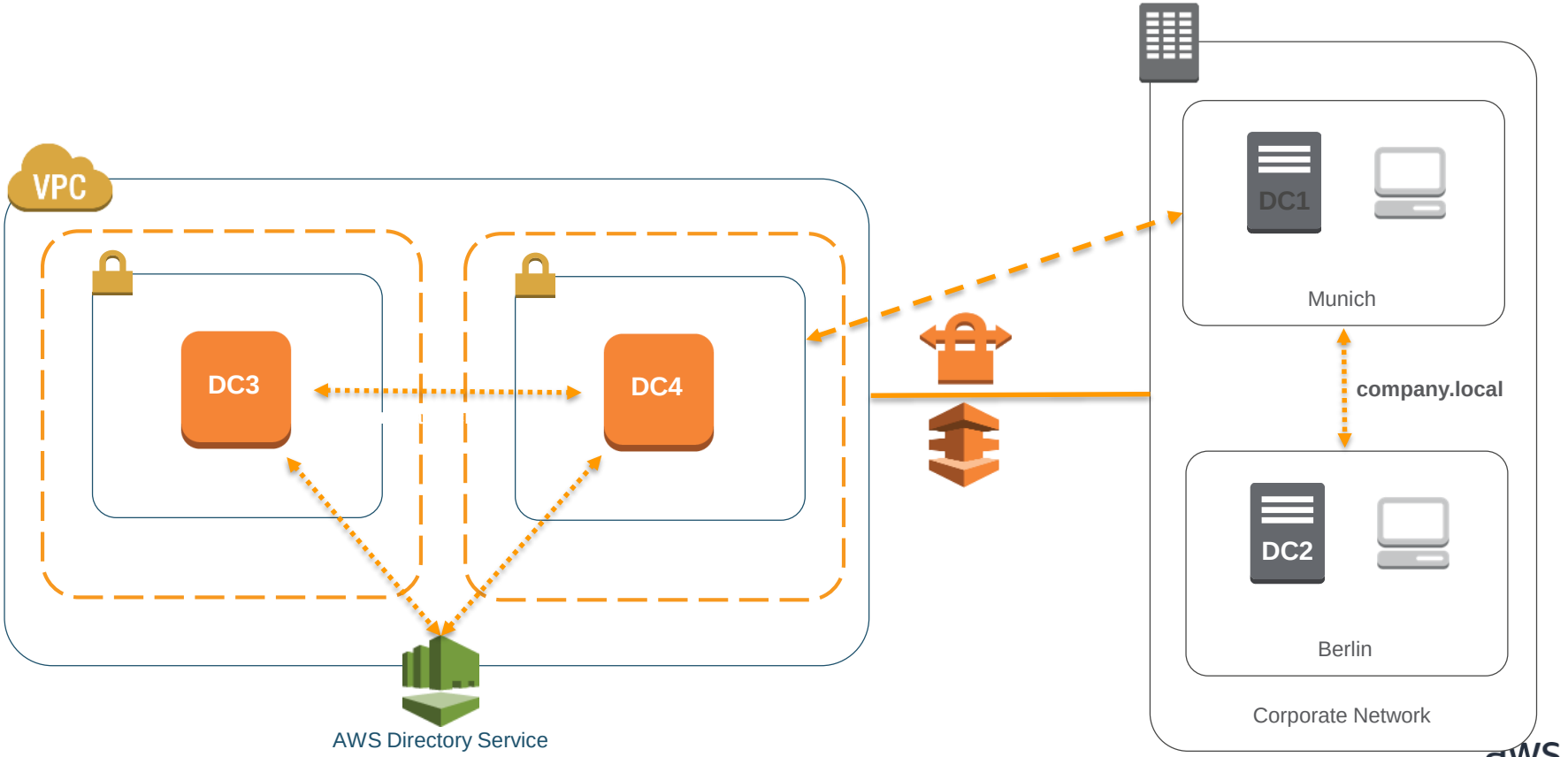
Single domain extended to multiple sites

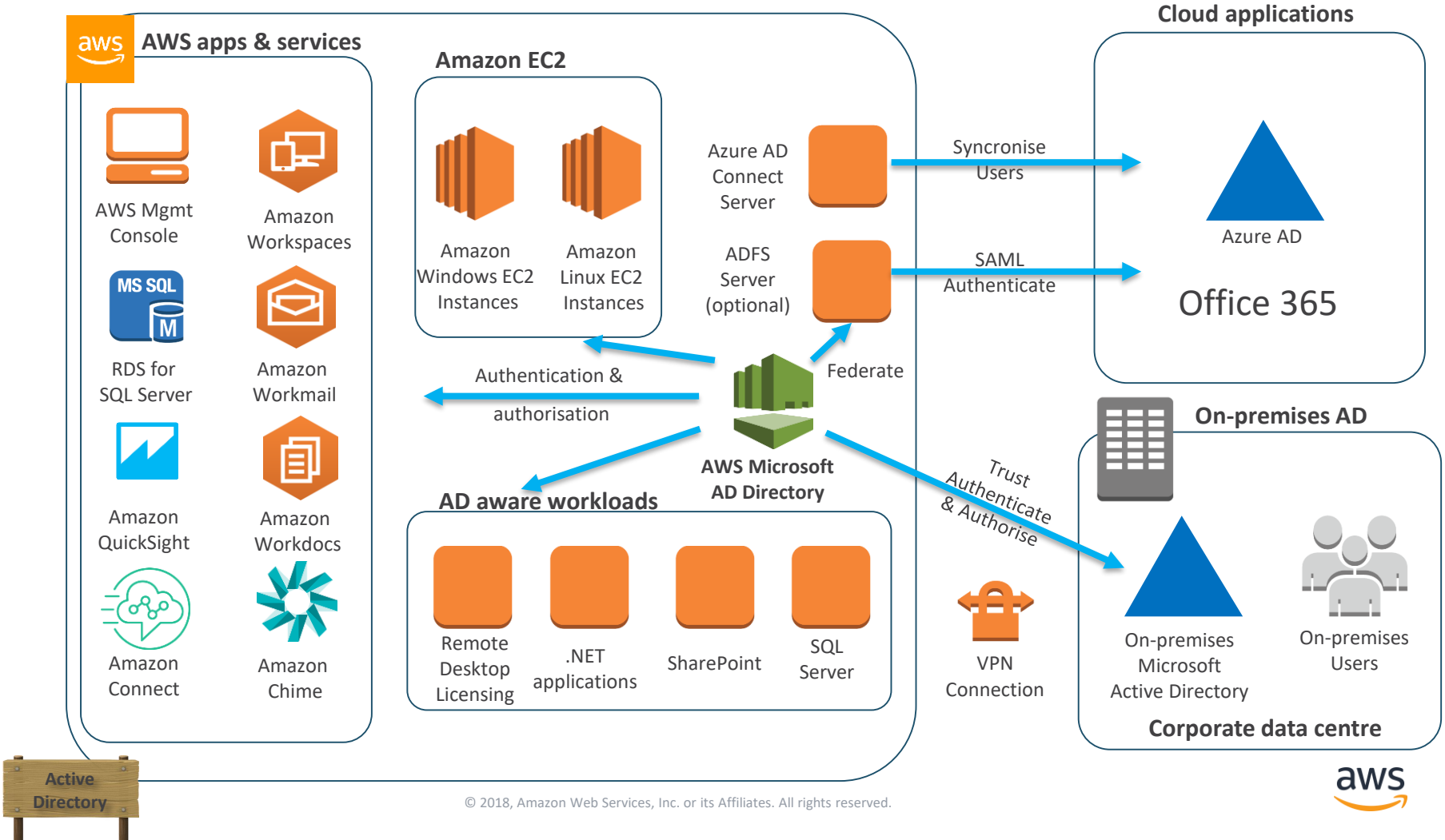


One subdomain per site

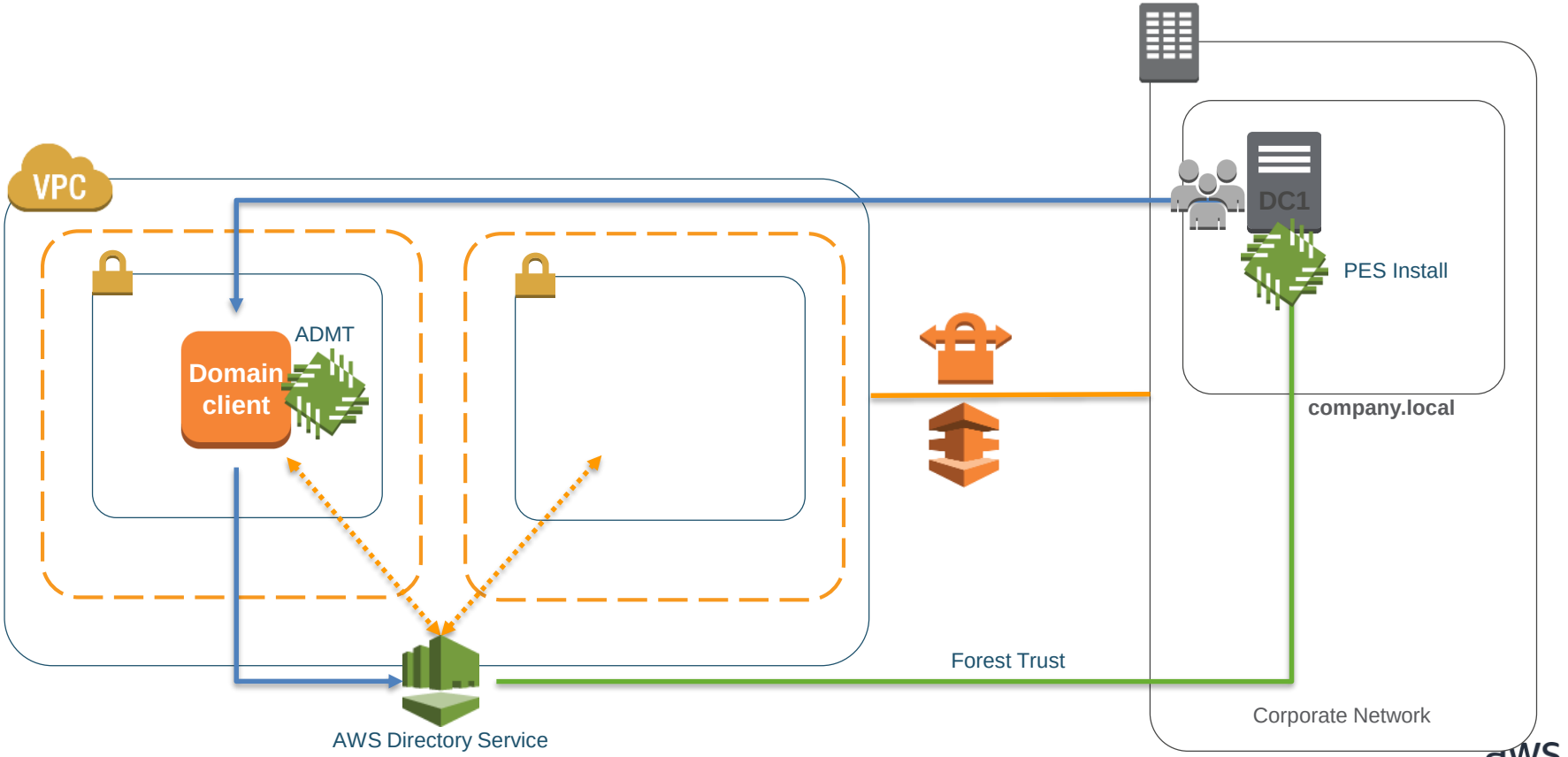


One forest per site and trust





ADMT Migration details



What Next? Migrating Databases – Which approach?

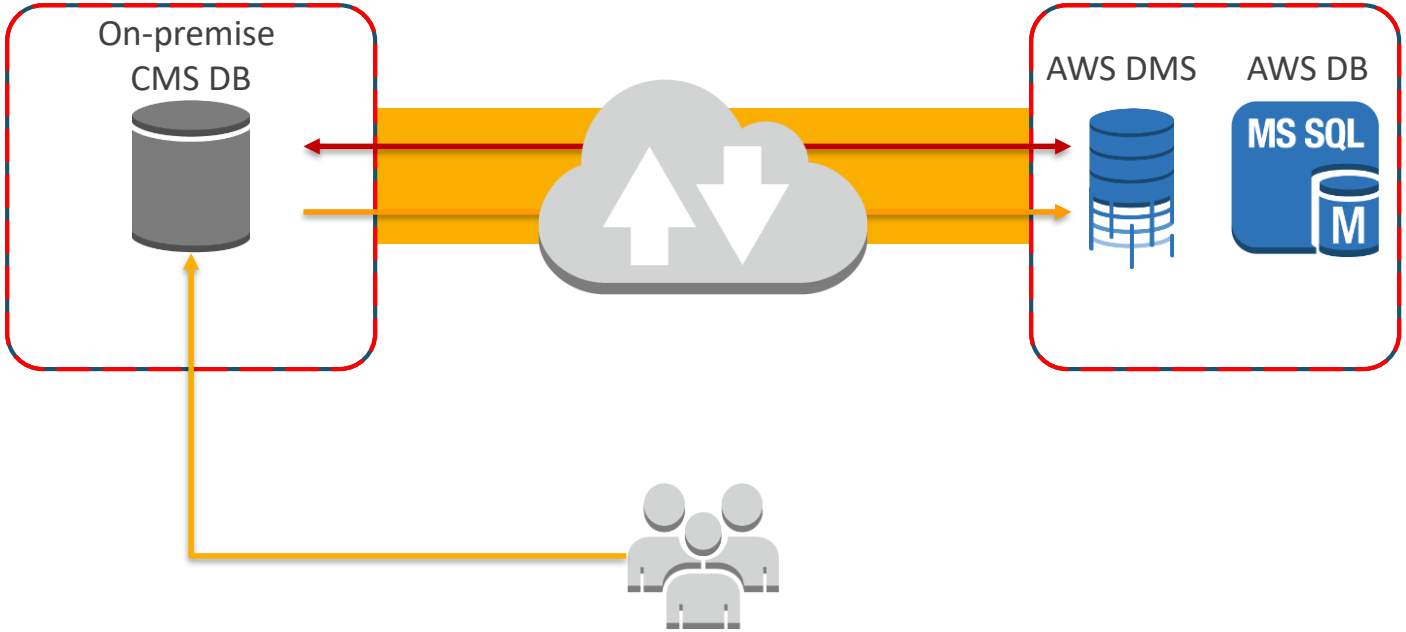
Migration method	Amazon RDS Target	Amazon EC2 Target	Downtime	DB Objects	Cross-Engine
Backup/Restore	Yes	Yes	Yes (hrs)	Data, Schemas, Stored Procedures, Triggers, Indexes	No
Import/Export Bulk Copy	Yes	Yes	Yes (mins-hrs)	Data, Schemas, Stored Procedures, Triggers, Indexes	No
SQL Log Shipping	No	Yes	Minimal (secs-min)	Pre-create the DB, sync	No
Hybrid Architecture	No	Yes	Minimal (secs-min)	Pre-create the DB, sync	No
AWS DMS	Yes	Yes	Minimal (secs-min)	With SCT (Data, Schemas, Stored Procedures, Triggers, Indexes)	Yes (SCT)

Users Accessing On Premise

Database Migration

aws

Migrating Database Writes Across



Database Migration

Endpoint Update and On Premise Decommission

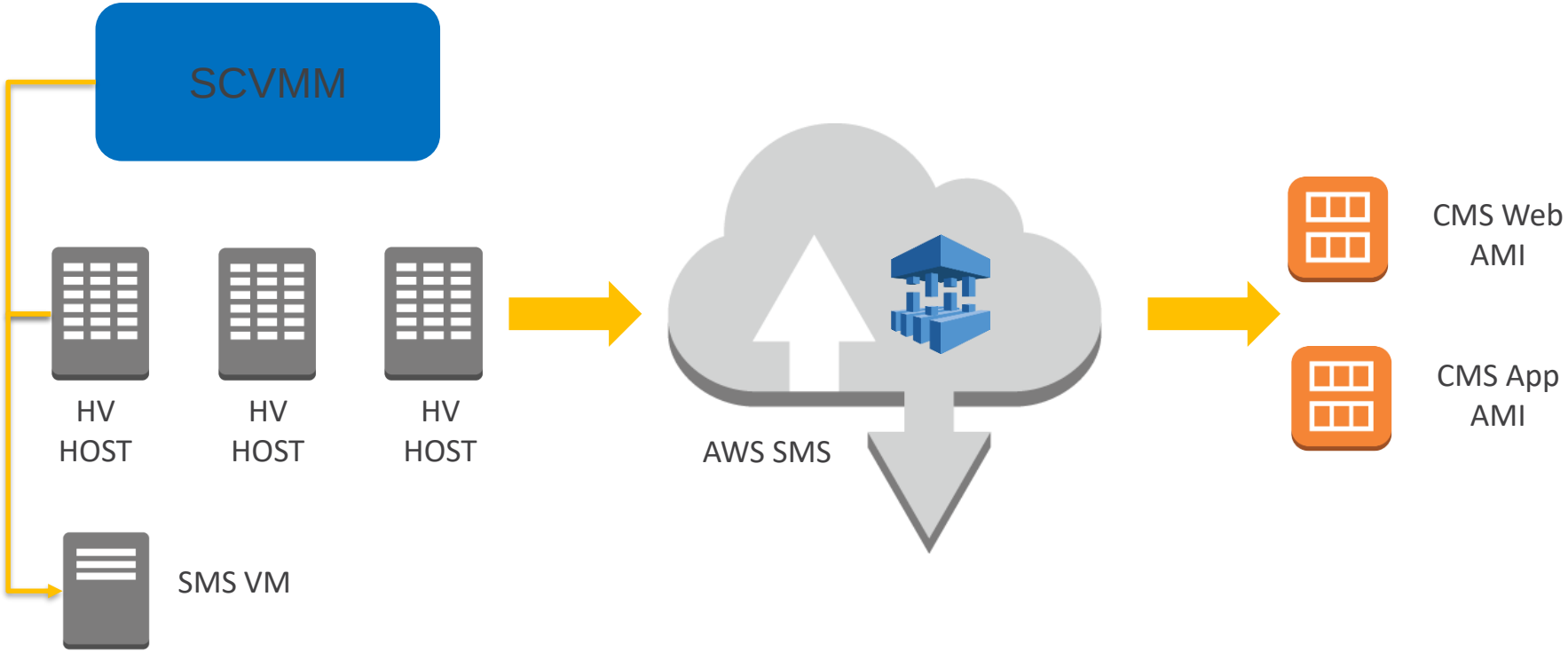
Database Migration

What To Migrate After SQL Server?

Fan out / deploy multiple systems in parallel:

- Exchange
- SharePoint
- Skype for Business
- System Centre Configuration Manager
- System Centre Operations Manager
- Etc…

AWS Server Migration Service



Windows? Containers? Actually Yes…

State in containers, you can but what is the goal?

For unicornshop, short lived stateless apps

How to migrate apps to containers? Containers are portable..

Do you have a CICD process already?

ECS With 2 Autoscaling Groups

Example spot pricing

C4	1a	1b	1c	On-Demand
8XL	$0.50	$0.27	$0.29	$1.76
4XL	$0.21	$0.30	$0.16	$0.88
2XL	$0.08	$0.07	$0.08	$0.44
XL	$0.04	$0.05	$0.04	$.22
L	$0.01	$0.01	$0.04	$0.11

Instance diversity

- m4.xlarge
- m3.xlarge
- c4.xlarge
- c3.xlarge
- r4.xlarge
- r3.xlarge

Application Migration

aws

Scheduled Tasks? .Net Core 2.0 Lambda

Upload Users

S3 Bucket

Data dropped in S3
Schedule / event triggered

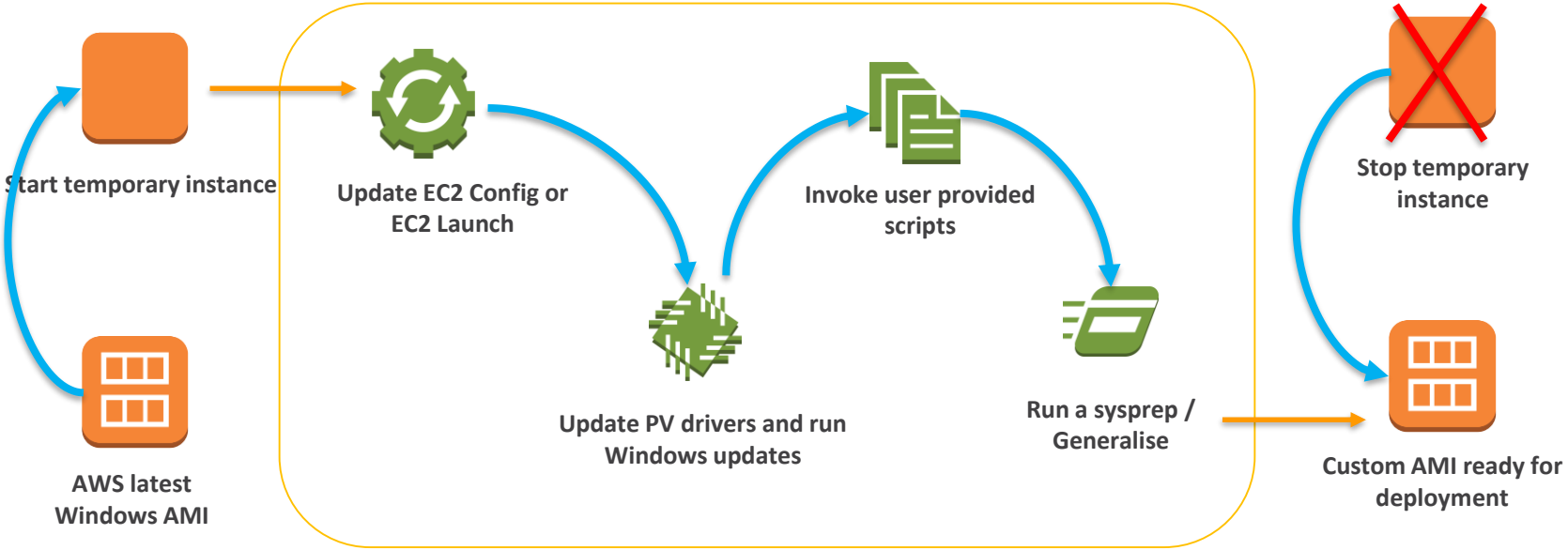
Lambda function

Pull data from CSV file
Perform ETL
Insert data into SQL table

DB in private subnet

VPC private subnet

Automation Is Key, How Do I Automate Updates?



Searching for a solution to host its MSFT SharePoint sites, the company chose AWS because of cost, and to improve operational efficiency.

By running on AWS, Dole can launch a new SharePoint website in minutes, host business intelligence and mobile applications globally, and **estimates savings of more than $350,000 in operating expenses.**

"We can grow anytime we want, we don't have to go and acquire new hardware"

Joanna Dyer – Director, IT Solutions

Wrapping It Up

- Understand the dependency chain in your Microsoft applications
- Build your migration plan around the dependency chain
- Know how Microsoft licensing on AWS works and plan accordingly

Thank you!