



Resilience at AWS

Michael Lin
Senior Solutions Architect
Amazon Web Services

Agenda

- Resilience and Shared Responsibility Model
- Resilience of the AWS cloud
- Resilience in the cloud
- Case studies
- Day 2 Considerations







**“Everything fails, all
the time.”**

Werner Vogels
CTO, Amazon.com

The Business Impact of Resilience

Why Resilience?

- System downtime costs Fortune 1000 companies anywhere from **\$1.25B to \$2.5B annually**
- Customers depend on a service to be available when they need it, and when it's not, it can **negatively impact an organization's brand**

Why Now?

- Expectations from consumers have shifted towards an '**always on, always available**' mindset
- Remote teams and complex, distributed systems coupled with frequent releases mean an organization and its systems need to be **more resilient than ever**



Resilience

Ability of a workload to recover from infrastructure or service disruptions

The mental model

High Availability

Resistance to common failures through design and operational mechanisms at a **primary site**



Core services, design goals to meet availability goals

Disaster Recovery

Returning to normal operation within specific targets at a **recovery site** for failures that cannot be handled by HA



Backup & Recovery, Data Bunkering, Managed recovery objectives

Continuous Improvement

CI/CD, **observability**, moving beyond pre-deployment testing towards **chaos engineering** patterns

High availability (HA)

About application availability

Smaller scale, more frequent events:

- Component failures
- Network issues
- Load spikes

Measures mean over time:

- “The 9’s” (99.99% available)

May							
		1	2	3	4	5	
		✓	✓	✓	✓	✓	
6	7	8	9	10	11	12	
✓	✓	✓	✓	✓	✓	✓	
13	14	15	16	17	18	19	
✓	✓	✓	✓	✓	✓	✓	
20	21	22	23	25	26	27	
✓	✓	✓	✓	✓	✓	✓	
28	29	30	31				
✓	✓	✓	✓				

Disaster recovery (DR)

Natural Disaster



Technical

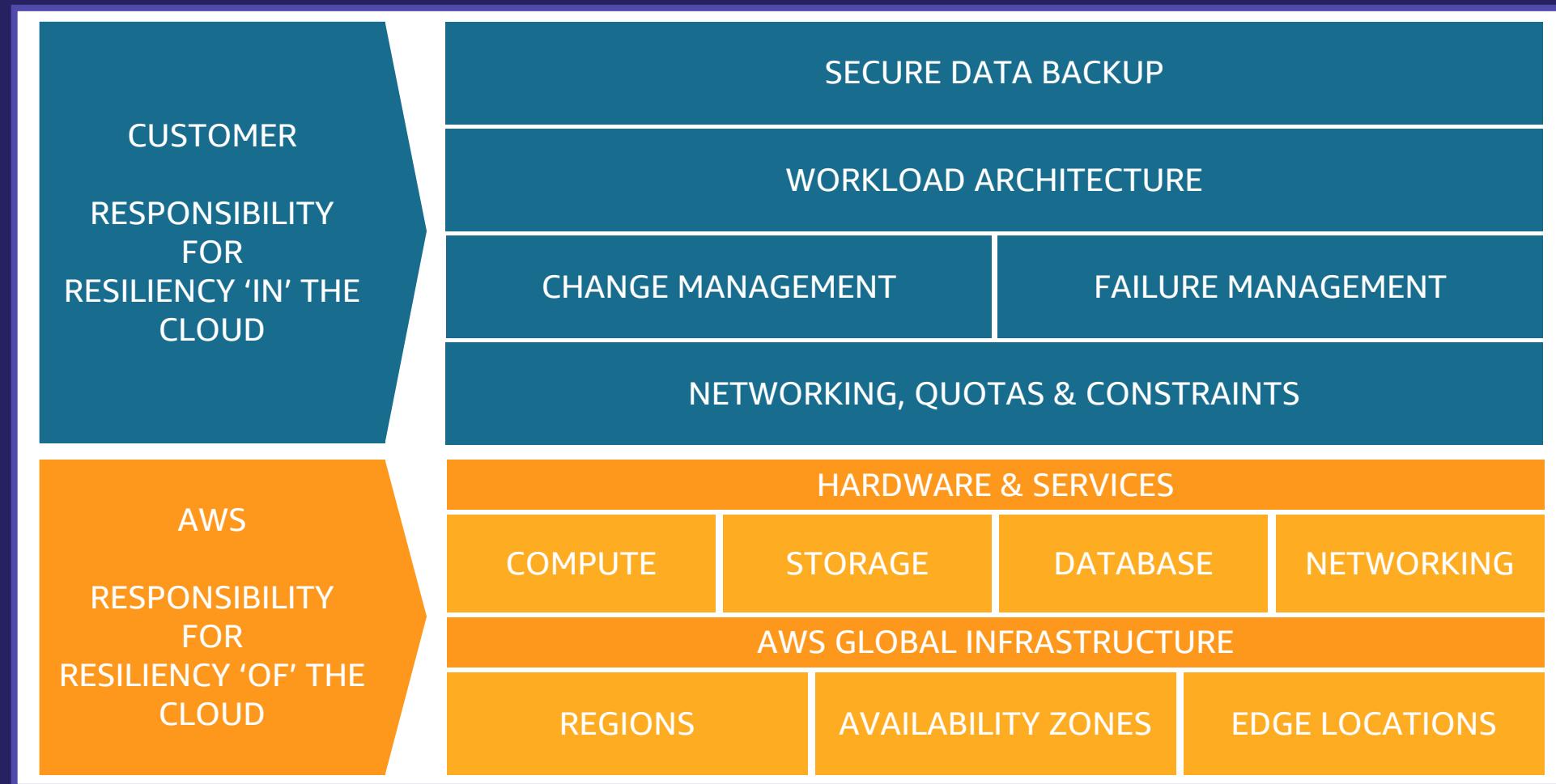


Human Actions



- About business continuity
- Larger scale, less frequent, events:
 - Natural disasters
 - Technical failures
 - Human actions
- Measures a one-time event:
 - Recovery Time
 - Recovery Point

Shared responsibility model for resilience



Resiliency of the cloud



AWS Regions and Availability Zones (AZs)

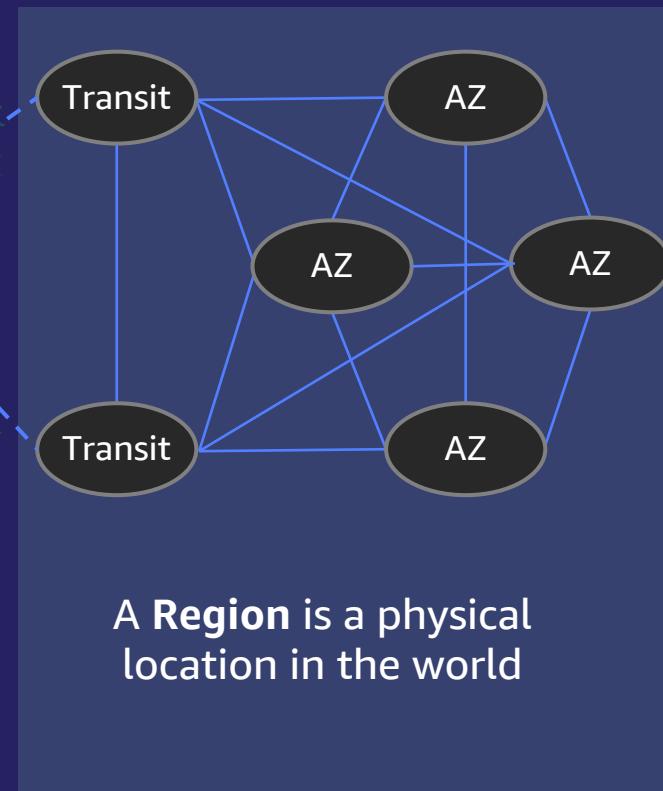
AWS Regions are physical locations around the world where we cluster data centers

33 AWS Regions worldwide

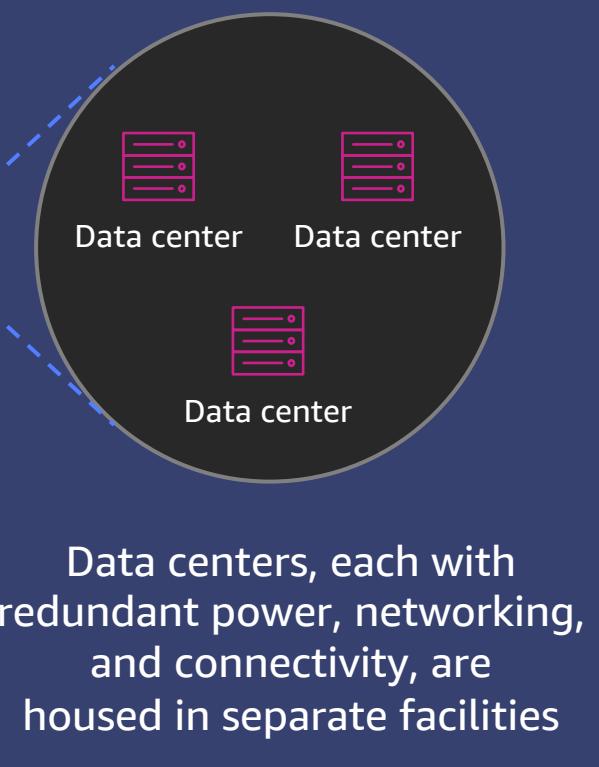


- AWS Regions
- Announced Regions

Each AWS Region has multiple AZs



Each AZ is one or more discrete data centers

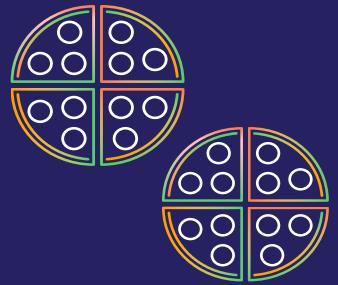


AWS 宣布在台灣推出基礎設施區域

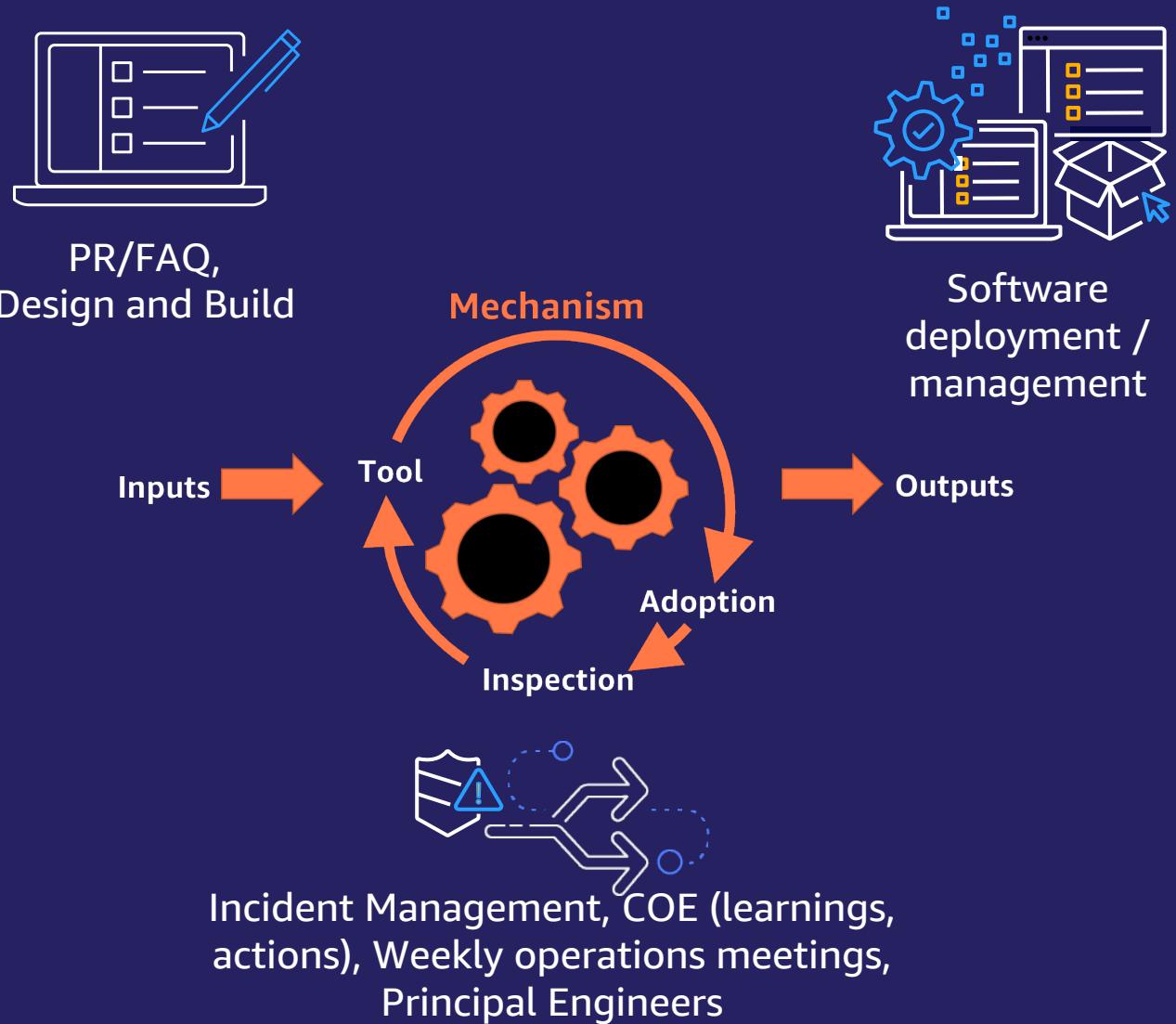
- AWS 亞太（台北）區域將助力客戶在台灣執行工作負載並安全地儲存資料，同時以更低的延遲為終端用戶提供服務。
- 新區域體現了 AWS 致力於滿足台灣和整個亞太地區對雲端服務強大需求的長期承諾。
- AWS 計畫在台灣投資數十億美元以支援新區域。



Culture of reliability at AWS



Engineering Culture:
Clear scope of ownership



Resiliency in the cloud



The most mission critical workloads run on AWS



Moved 100 business applications, including SAP, to AWS in 8 months with zero business downtime

US NAVY

Moved SAP ERP that supports 6 U.S. Navy commands, 72,000 users, \$7B worth of parts and goods to AWS 10 months ahead of schedule



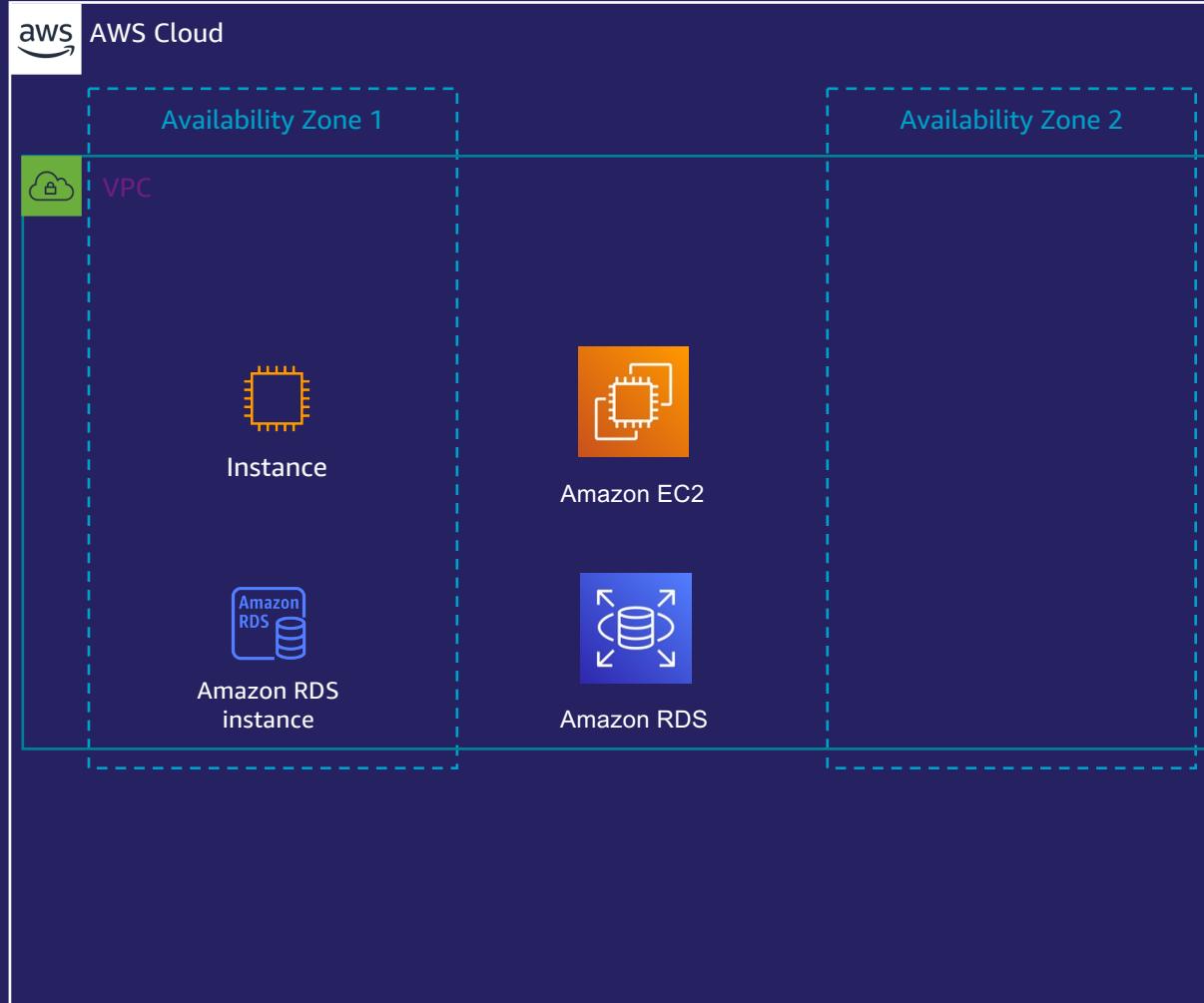
Improved business process performance by 60% while reducing costs by 40% for mission-critical SAP systems



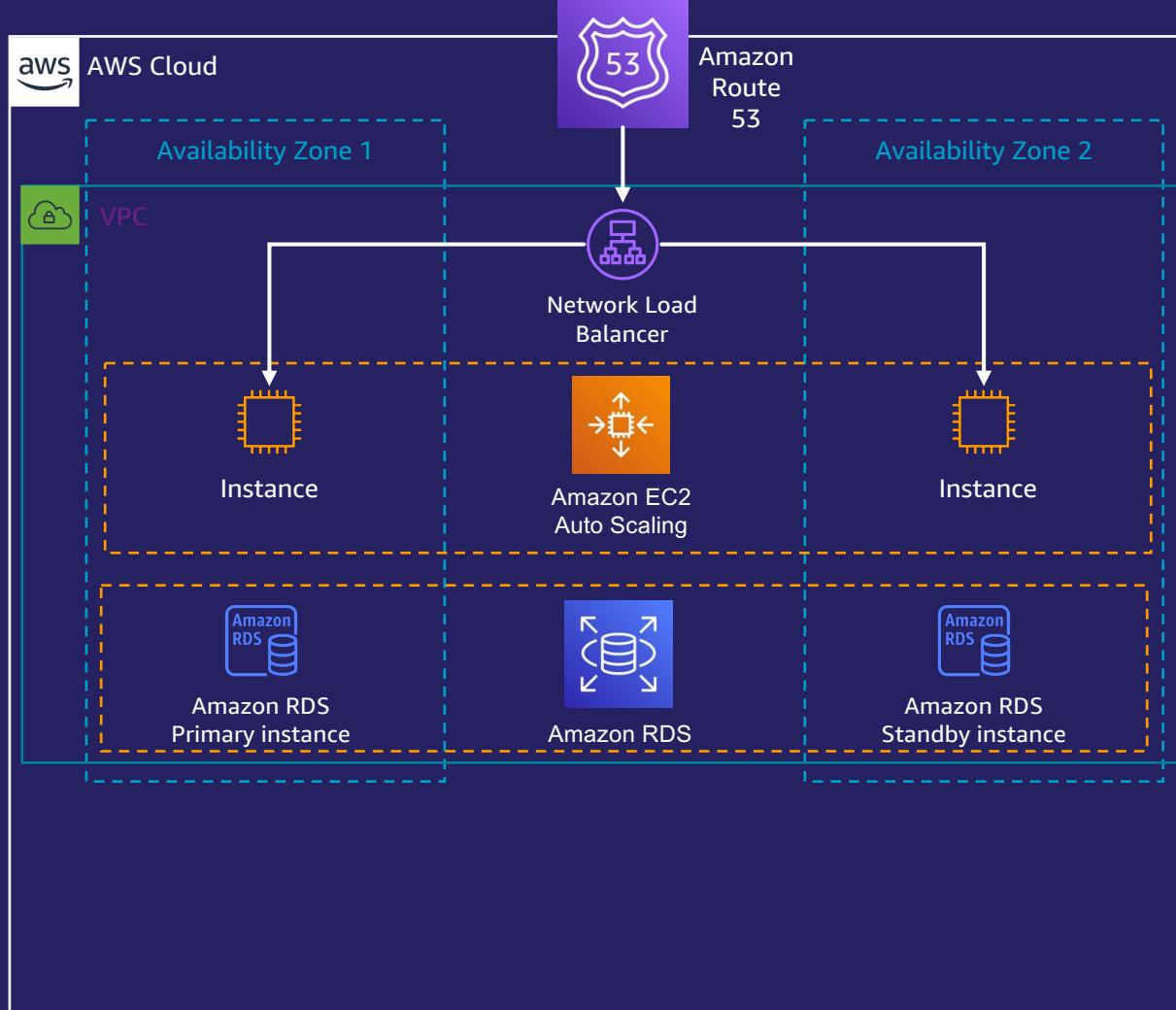
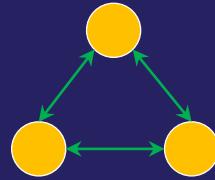
High Availability



Multi-zonal high availability



Multi-zonal high availability

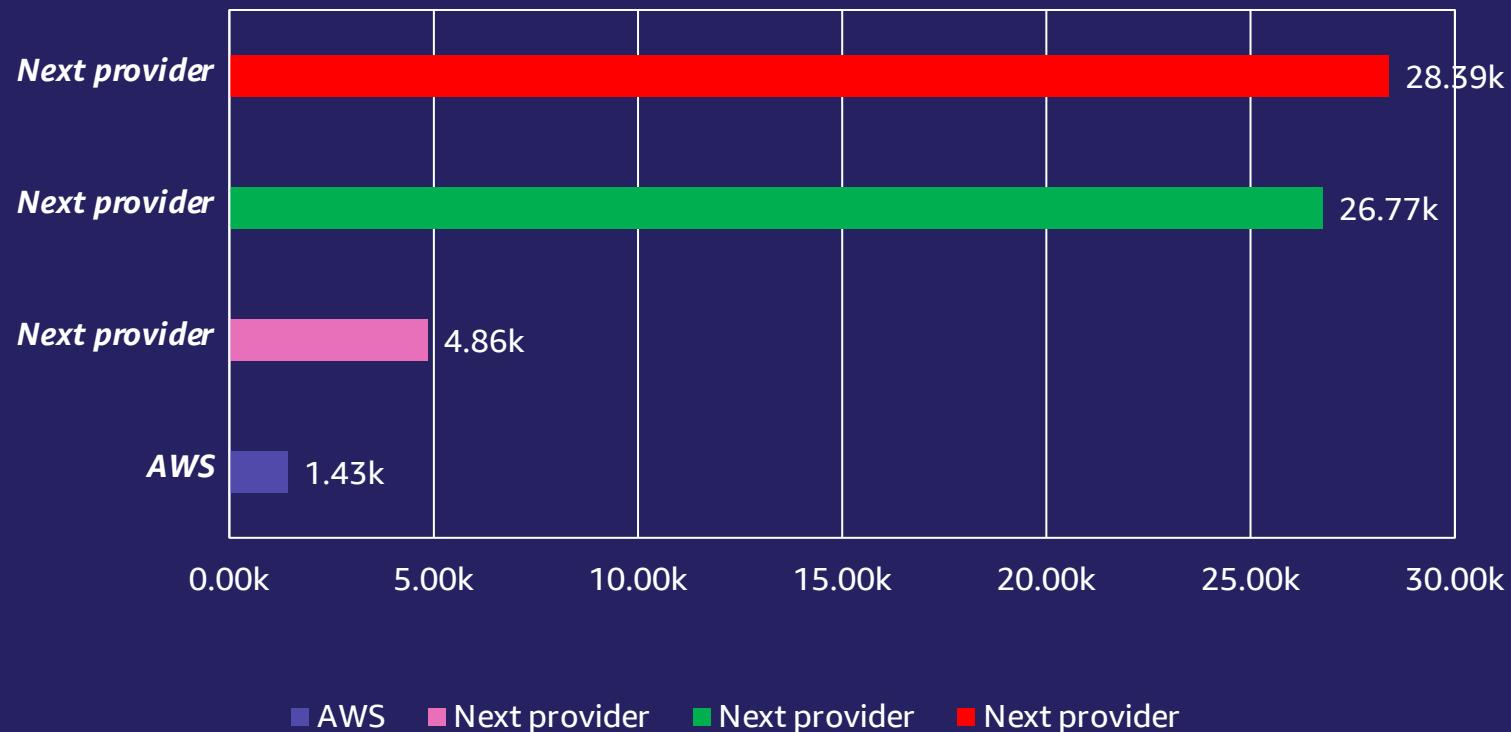


AWS Cloud Infrastructure Designed to Scale with Highest Availability

AWS Investments on Underlying Higher Resilient Infrastructure

Total Incident Hours (Public) by Provider in 2023

Incident hours published = Incident hours published * Regions Impacted * Services Impacted



* Sources: Public Status Pages for Cloud Providers. Incidents Types include = Incidents, Degradation, Disruption, and Outages of Services



© 2024, Amazon Web Services, Inc. or its affiliates.

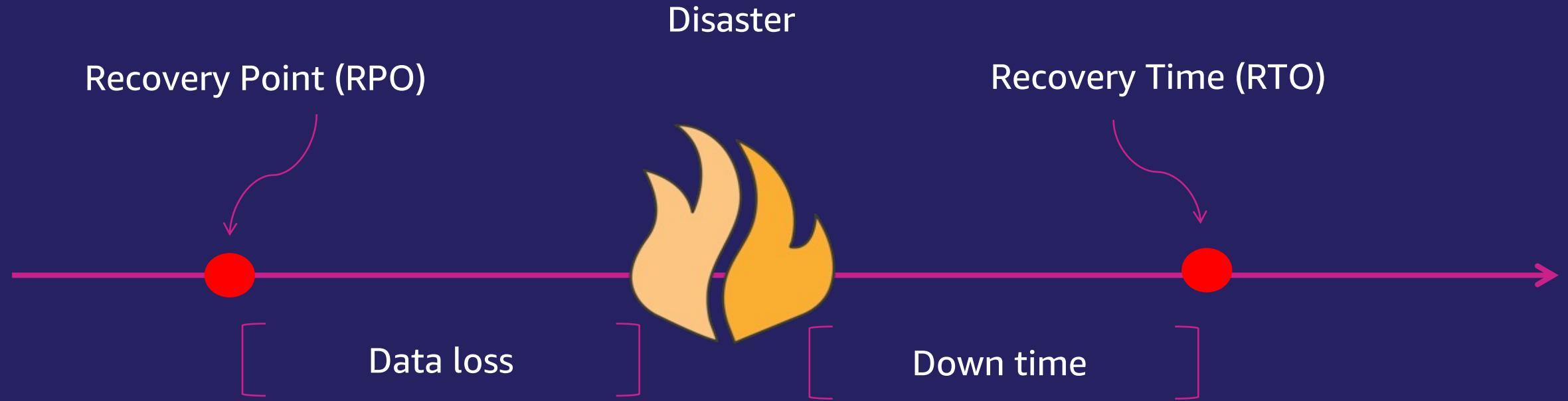
Disaster Recovery



Recovery Point and Recovery Time Objective (RPO/RTO)

How much data can you afford to recreate or lose?

How quickly must you recover?
What is the cost of downtime?



Disaster Recovery Benefits of the Cloud

Traditional disaster recovery

- Massive upfront & ongoing hardware cost
- Management and infrastructure overhead
- Data growth increases costs
- Separation of test and production environment
- Vulnerable to cyber threats/hacking

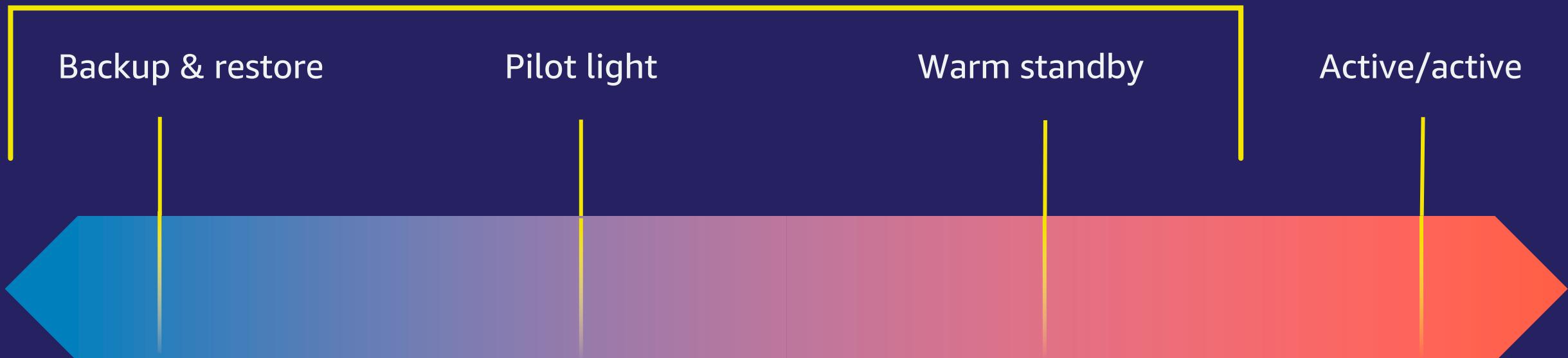
Disaster recovery in the cloud

- Pay as you go for the rightsized compute/storage
- Lower IT overhead
- (MUCH!) More automation
- Easy and repeatable testing
- Systems up in minutes (not hours/days!)

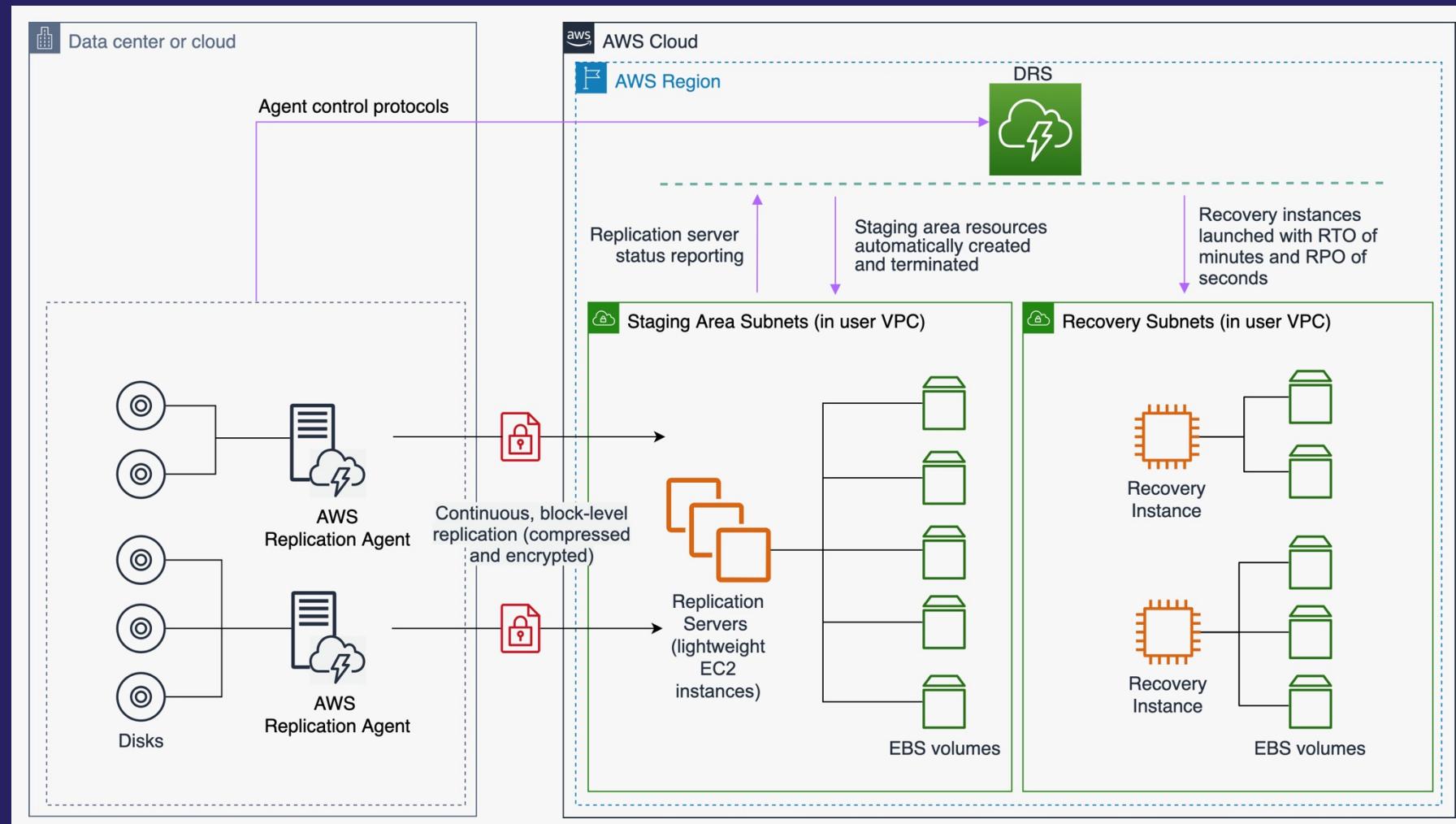


Strategies for disaster recovery

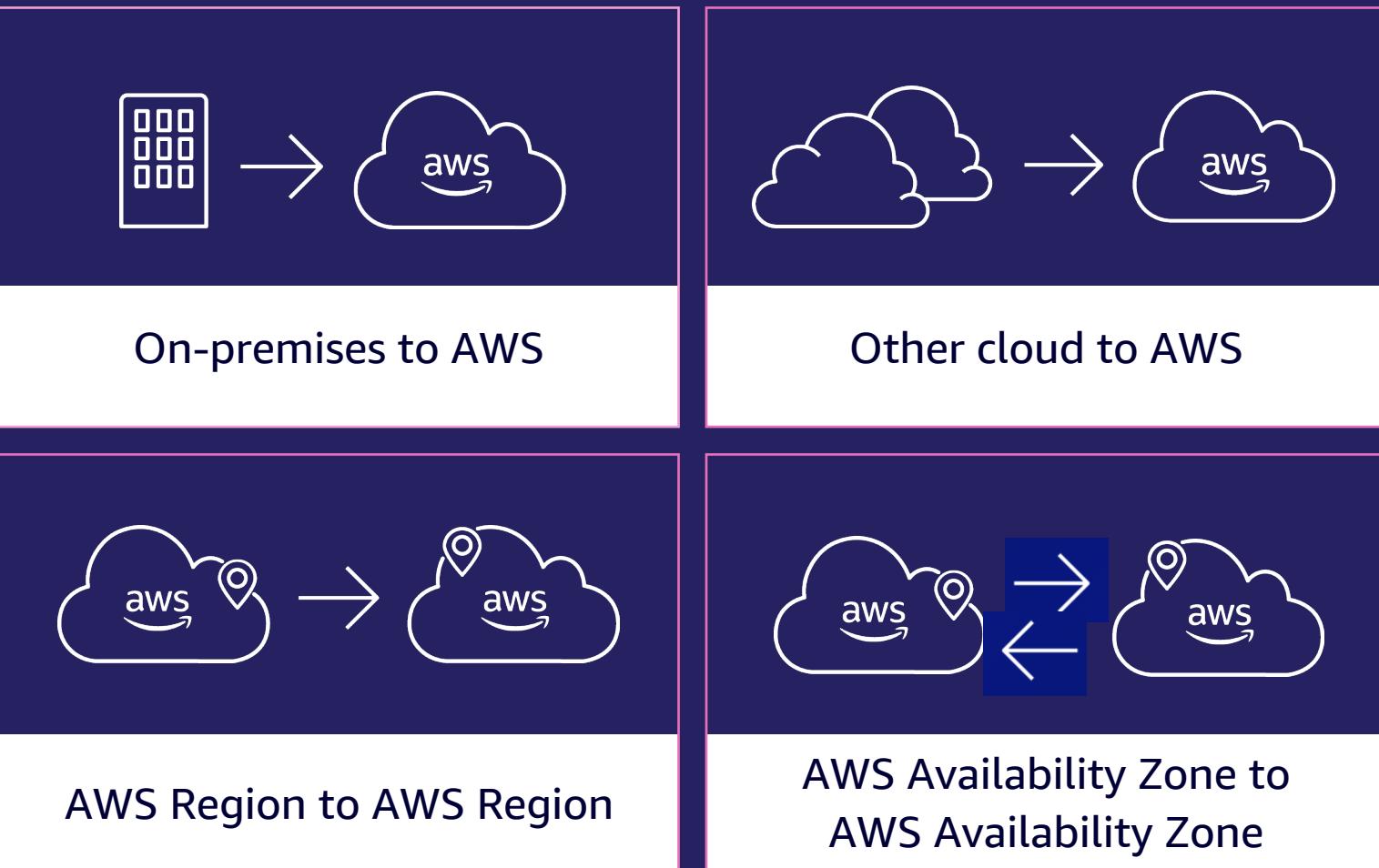
Active/passive strategies



AWS Elastic Disaster Recovery



Elastic Disaster Recovery deployment patterns



AWS DRS wide platform support*

Any application	ORACLE E-BUSINESS SUITE 	ORACLE PEOPLESOFT Microsoft IIS	 SAP CRM	SAP Hybris 	 SAP ERP				
		Microsoft SharePoint		Microsoft Active Directory	Microsoft Exchange	Microsoft Dynamics CRM			
Any database	Microsoft SQL Server	ORACLE DATABASE	 SAP HANA	 MySQL™	 cassandra	 MongoDB®			
x86 operating systems	 Red Hat	 CentOS	 ORACLE LINUX	 ubuntu	 debian	 SUSE	Windows Workstations	Windows Server 2003	Windows 10
	Windows Server 2008	Windows Server 2012	Windows Server 2016			Windows Server 2019	Windows Server 2022		
Source infrastructure			 VMware AWS			Cloud provider			
		Physical data centers	Microsoft Hyper-V						

*See documentation for a complete list and supported versions



AWS Elastic Disaster Recovery key benefits



Faster recovery

Recovery time objectives (RTOs) of minutes



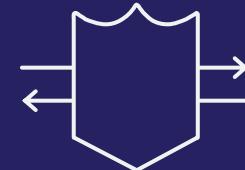
Easy testing

Conduct non-disruptive drills to verify readiness



Lower costs

No need to pay for idle recovery site resources



Data protection

Recovery point objectives (RPOs) of seconds



Ransomware recovery

Launch unlocked and unencrypted versions of your applications

Case Studies



南部某公家單位三天完成系統災備到 AWS

案例情境

颱風路徑臨時下修，氣象局發布海葵颱風豪大雨及滯留警報，客戶緊急要求 DR 上雲。

任務挑戰

1. 人力資源問題：因應颱風防災資訊，更新網站資料庫
2. 地端機房檢查繁鎖：滯留警報檢查機房供電，防水事務繁忙
3. 系統及資料頻繁負載：風災資訊更新頻繁網站資料庫，民眾大量存取造成惡性循環

解決方案

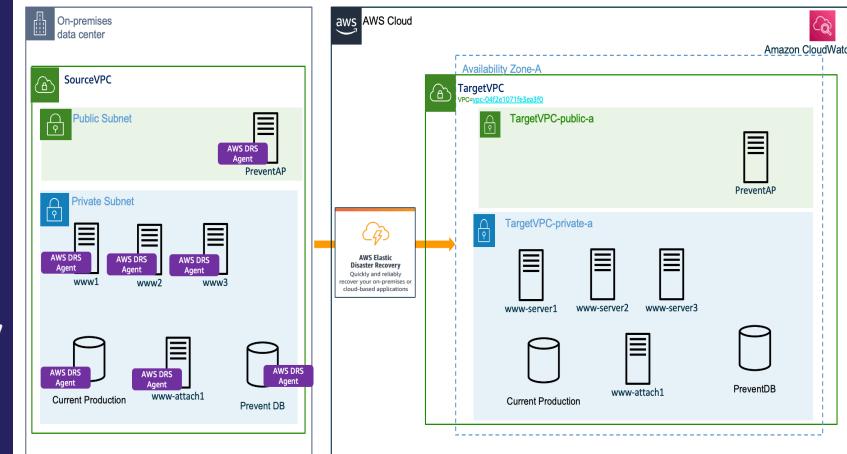
1. 引進 AWS Elastic DR service 直接在4台 web server, 1台 Windows file server, 2台 DB server 安裝 Agent
2. 透過ISP之穩定專線，直接依 block-level change 抄寫至海外 Region 規避天災
3. 持續且接近即時之雲地的硬碟block-level 同步
4. 中途經歷人力資源吃緊之偶發事件(網路事件及安裝) 因全自動化同步

取得成果

1. 第一天完成防災 AP+DB 上雲備份，第二天完成官網上雲備份，及陸續完成官網 DB, File server 上雲DR 備份，未來若頻寬加大可以全部一起上雲
2. 持續且接近即時之雲地同步，支援天災人或人為即時切換



AWS Elastic Disaster Recovery for Government Typhoon Event



© 2023, Amazon Web Services, Inc. or its Affiliates. All rights reserved. Amazon Confidential and Trademark.



明基佳世達集團

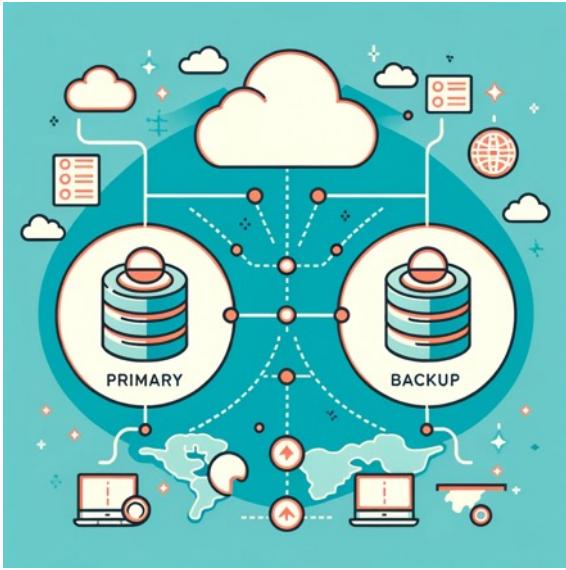
成立於1984年，為一橫跨資訊產業、醫療事業、智慧解決方案及網路通訊事業之全球科技集團。

入選為湯森路透Thomson Reuters「全球科技百強」領導者、富比士「全球最佳雇主」、「亞洲最佳企業雇主」及「台灣十大永續典範企業」。

Qisda

許智翔
明基佳世達 經理

為何明基佳世達選擇雲端



地緣政治 – 跨境備援

傳統異地雙資料中心備援方案受地緣政治因素影響，已大幅降低企業目前的數位韌性。而雲端的全球既成機房，可讓企業在短時間內將核心系統部署至全球多個區域



成本控制

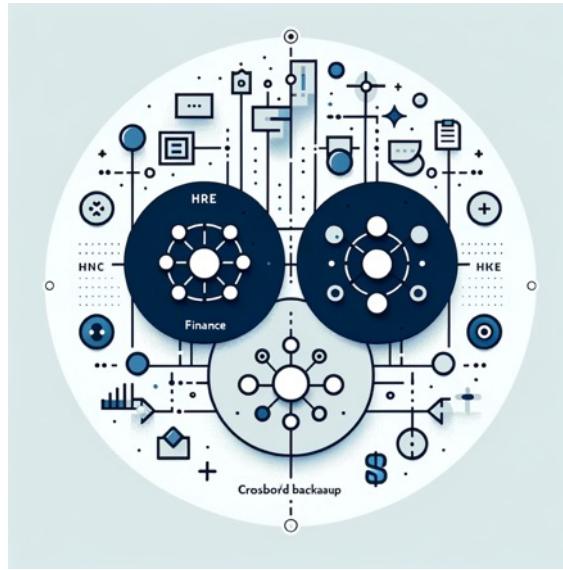
在跨境備援情境下，採用自建機房/設備的方式將在無法肯定解決方案可行性的情況下，耗費過高的初期建置成本。雲端的隨付即用政策可很好的讓企業控制驗證階段的成本



時程急迫性

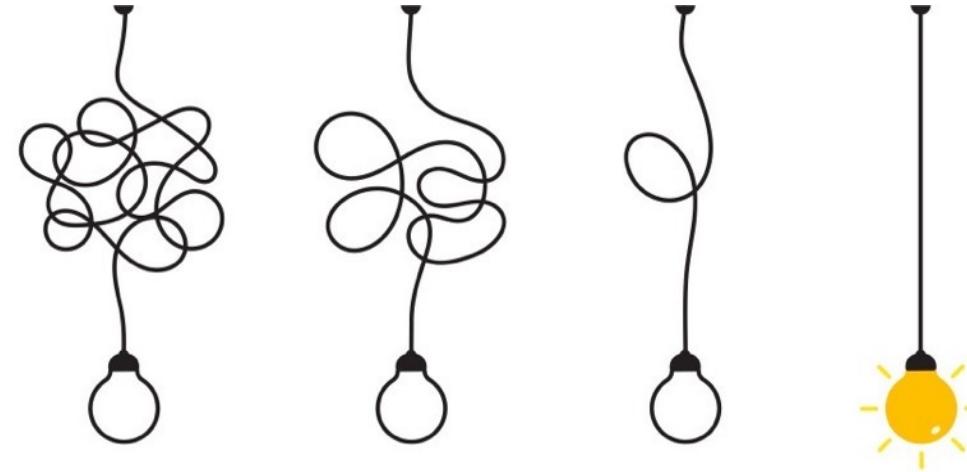
僅數月時間就要完成測試環境POC與生產環境導入與演練，並確認所有專案目標達成。而雲端只需要簡單的操作便可快速建立相關環境進行可行性驗證。

明基佳世達的災難備援見解與相關經驗



何謂企業核心系統？

不僅僅是單一系統，而是由多個系統集合而成，這些系統之間相互協同作業。



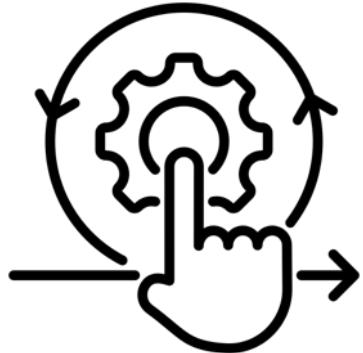
核心系統自帶解決方案的問題

不同的核心系統都有自己的災難備援最佳實踐方案，但導入往往需要高技術門檻。且需要依賴多個外部顧問的技術支援，使得整個核心系統的集成復原計畫變得更加複雜。

明基佳世達要的解決方案

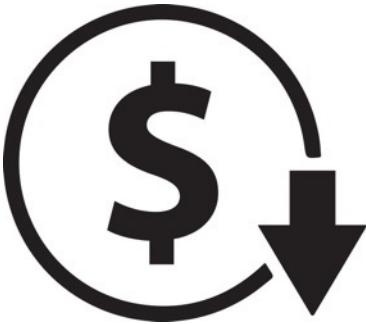
最簡單、最直接的方式來執行復原作業。複雜的SOP或是依賴多個顧問團隊的協助都會帶來額外的風險。

為何明基佳世達選擇AWS DRS



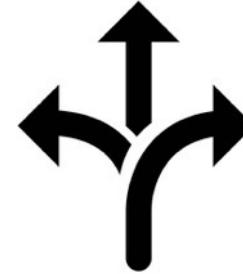
簡易性

不同的系統主機都能使用同一種方式進行備援。同時其工法可滿足明基佳世達之業務持續運作目標。



成本

平時在複寫階段主要的成本是儲存資源費用，而非啟用的伺服器費用。相較傳統高可用雙主動架構節省大量成本。



彈性

不論是單一主機或單一系統發生災難，都可以個別在雲端進行復原並與地端協同作業。即便整個資料中心遭受災難，也能夠將核心系統集成在雲端復原，且復原後不影響海外據點的持續營運。



Safeguarding Ukraine's Data



<https://www.youtube.com/watch?v=PPunA7tPMyk&t=910s>

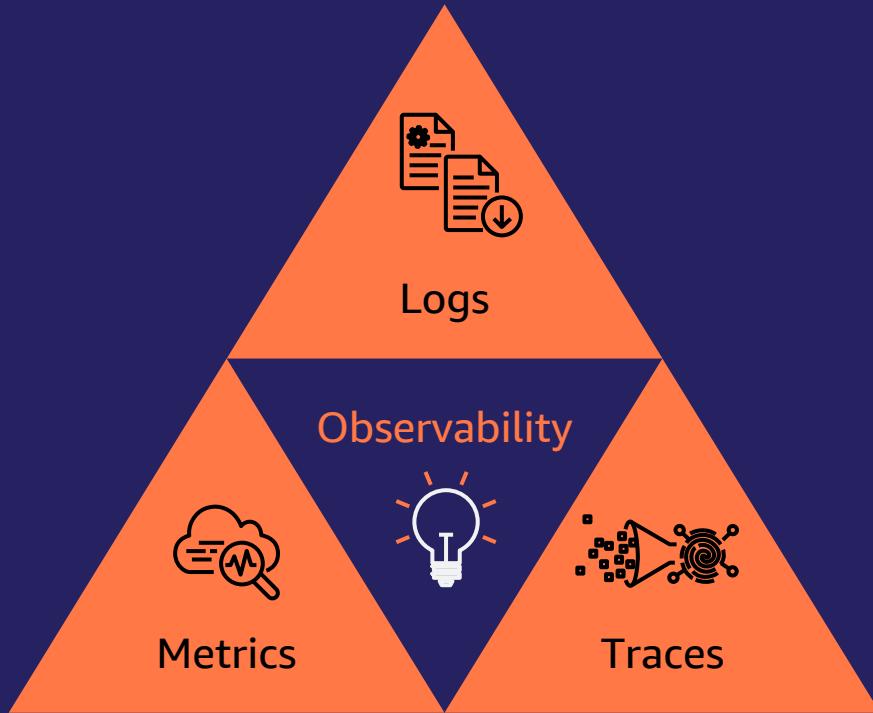
- There are 61 government data migrations to AWS, with more to come
 - 27 Ukrainian ministries
 - 18 Ukrainian universities
 - The largest remote learning K-12 school
 - 10 PB of data
- Ukraine's largest private bank also moved all its operations to the cloud
 - 270 applications
 - 4 PB of client data

Integrated Observability



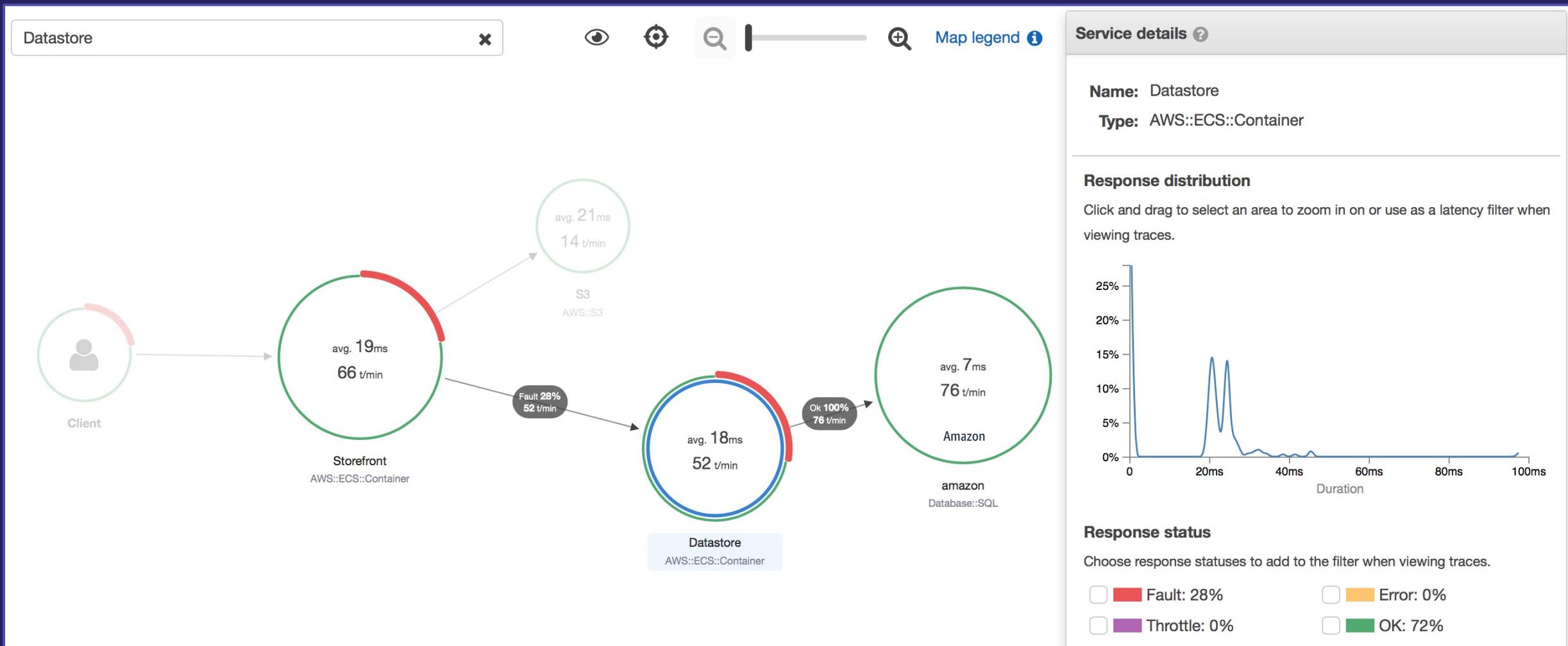
Monitor the health of your applications

THREE PILLARS OF OBSERVABILITY TOOLING



- Metrics:
 - Numeric data
 - Measured at various time intervals
 - Such as SLIs
- Logs:
 - Timestamped records of discrete events
- Traces:
 - User's journey across multiple applications & systems

Identify performance bottlenecks



Continuous Resilience - finding the unknowns



Chaos experiment

Inject events that simulate

- Hardware failures, such as servers dying
- Software failures, such as malformed responses
- Nonfailure events, such as spikes in traffic or scaling events

Any event capable of disrupting steady state



“



Pearson

We have integrated AWS Fault Injection [Service] into our CI/CD pipelines in GitLab, enabling us to conduct chaos experiments seamlessly and automatically.

AWS FIS is a powerful tool ... to identify and rectify any underlying weaknesses – before they affect our customers.

Shridhar Navanageri

VP, Architecture and Platform Engineering
Pearson



“We needed to build systems that embrace failure as a natural occurrence.”

Werner Vogels

Amazon CTO





Thank you!

Michael Lin

linmicht@amazon.com