What Happens If A Bear Bombs Your Azure Region?

How Will Azure Survive A Disaster?

Introducing Aidan Finn

- Cloud Mechanix
- 18 year MVP – currently Microsoft Azure
- Based in Kildare, Ireland (+5 hours from EST)
- Working as consultant/sys admin since 1996
- Windows Server, Hyper-V, System Center, desktop managment, and Azure

- http://aidanfinn.com
- http://cloudmechanix.com
- @joe_elway

Cloud Mechanix – Azure Consulting

- Training
- Cloud strategy
- Reviews
- Security
- Migration
- System design & build
- Cloud Adoption by Mentorship
- Small/medium/large business
- Microsoft partners

http://cloudmechanix.com

Online Course

Designing Secure Azure Networks

January 26/27

Discount Code For NIC

NicThePacket

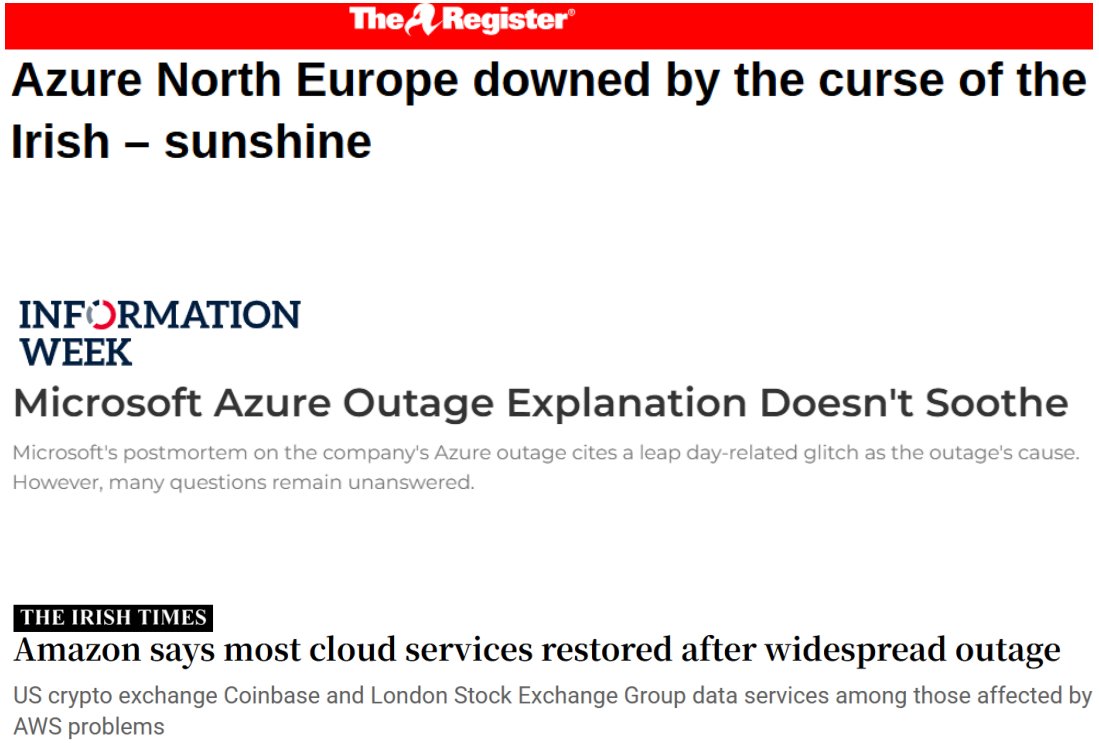
25% off

Less Slides, More Demo


MADE WITH PIKA

My Interest In This Topic

Cloud Outages



- We have seen many outages
  - Error
  - Hardware
  - Software
  - Cybercrime
  - Other external factors
- Scope
  - Cluster
  - Data centre
  - Region
  - Global
- Massive damage to business

Sabotage

- I was working for a Nordic consulting company
- I have Finnish & Norwegian government customers
- Russian “dark fleet” operations in The Baltic Sea
- I discussed this topic with military
- I read too many Tom Clancy novels when I was young

Electricity cable link to Estonia was damaged on Christmas Day in suspected Russian act of sabotage

The Cook Islands-registered oil tanker Eagle S in Porvoo, Finland, after being seized by police. Photograph: Jussi Nukari/Rex/Shutterstock

Bad Stuff Happens To On-Premises Too!

Reuters

British Airways resuming services after latest IT meltdown

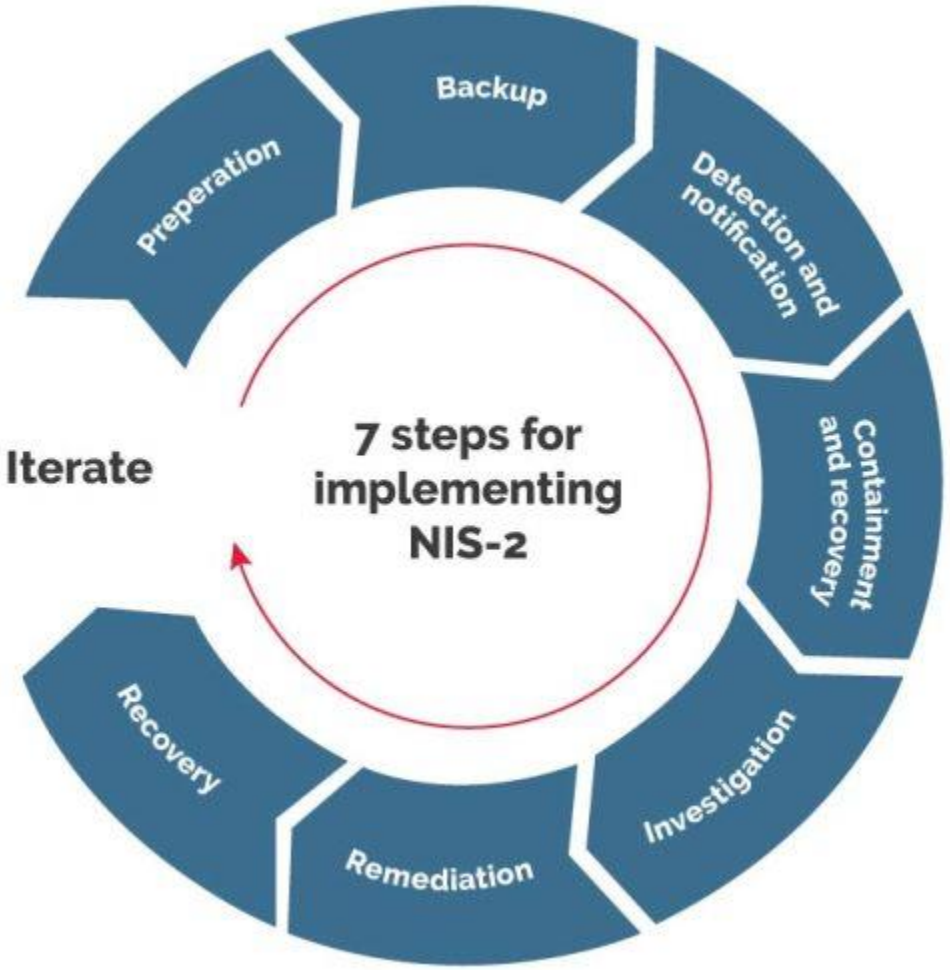
By **Andrew MacAskill** and **Paul Sandle**

August 7, 2019 5:01 PM GMT+1 · Updated August 7, 2019

- Examples:
  - Hardware
  - Software
  - Bad updates
  - Malware
  - Facilities
  - External factors
- Up to us to fix them
  - How long?
  - Skills?

Planning For Disaster

NISv2


Preperation
Backup
Detection and notification
Containment and recovery
Investigation
Remediation
Recovery
Iterate
7 steps for implementing NIS-2

Planning for disaster recovery is *our responsibility*

We must understand Azure availability
to assess the disaster risks

Azure Geography 101

We must understand Azure before we assess risks

Microsoft Global Network

- ~65 Public Azure regions
- 185+ Edge Data Centres
  - Peering/entry points (Front Door)
  - Multiple per metro *
- Fault tolerant inter-region cabling
  - Fault tolerance
  - Active/active
  - Anycast/self-healing
- Enterprise Resilience and Crisis Management (ERCM) team mandates annual disaster recovery validation

Azure Regions

- A collection of data centres in a single location
  - Europe North
  - Europe West
  - Norway East
  - Norway West
- Hero regions:
  - North/West Europe
- Local regions:
  - Norway East/West

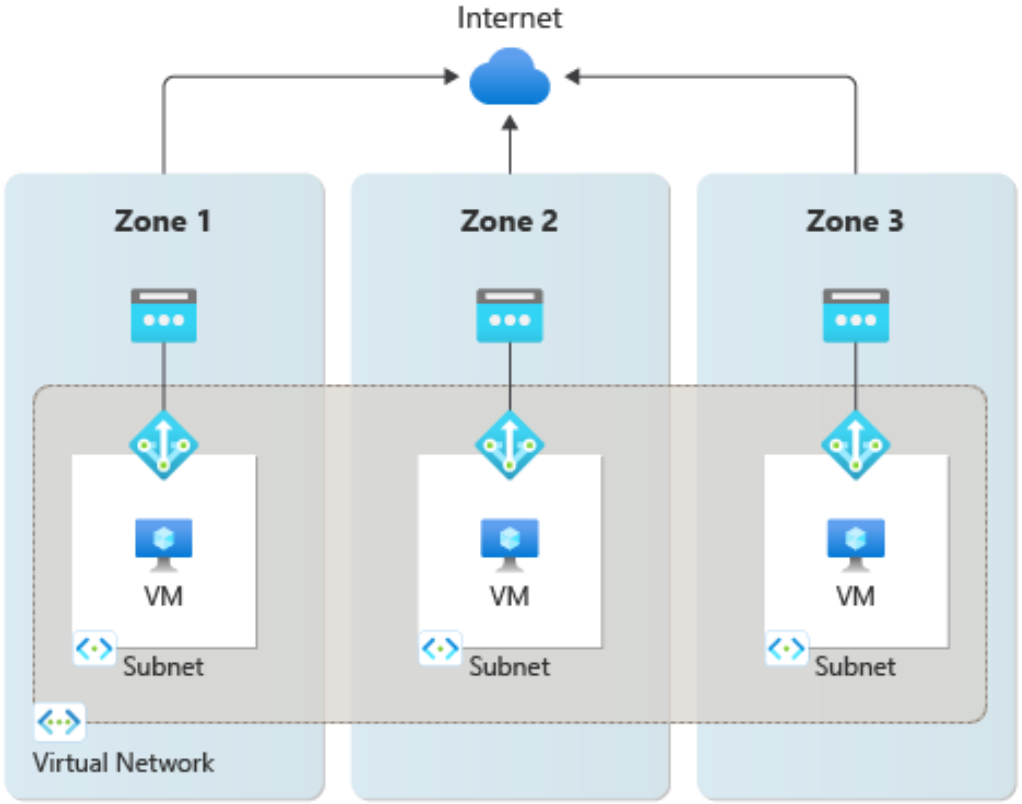
Paired Regions

- Azure regions are *mostly* deployed as paired regions
  - North Europe <> West Europe
  - Norway East <> Norway West
- Goal: Ensure a minimum distance of **300 miles (483 kilometers**) between datacenters in enabled regions
  - Not always possible
- Goal: 1 disaster should not destroy both pairs

Someone will ask me about restricted regions.
I will get to that later.

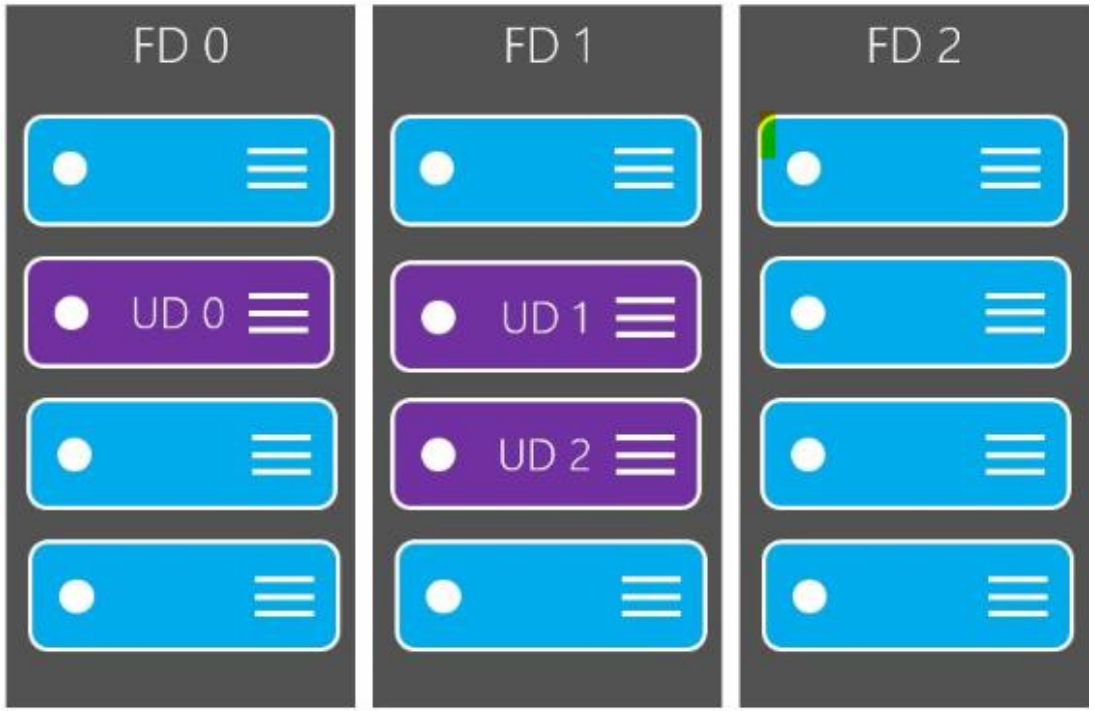
Availability Zones

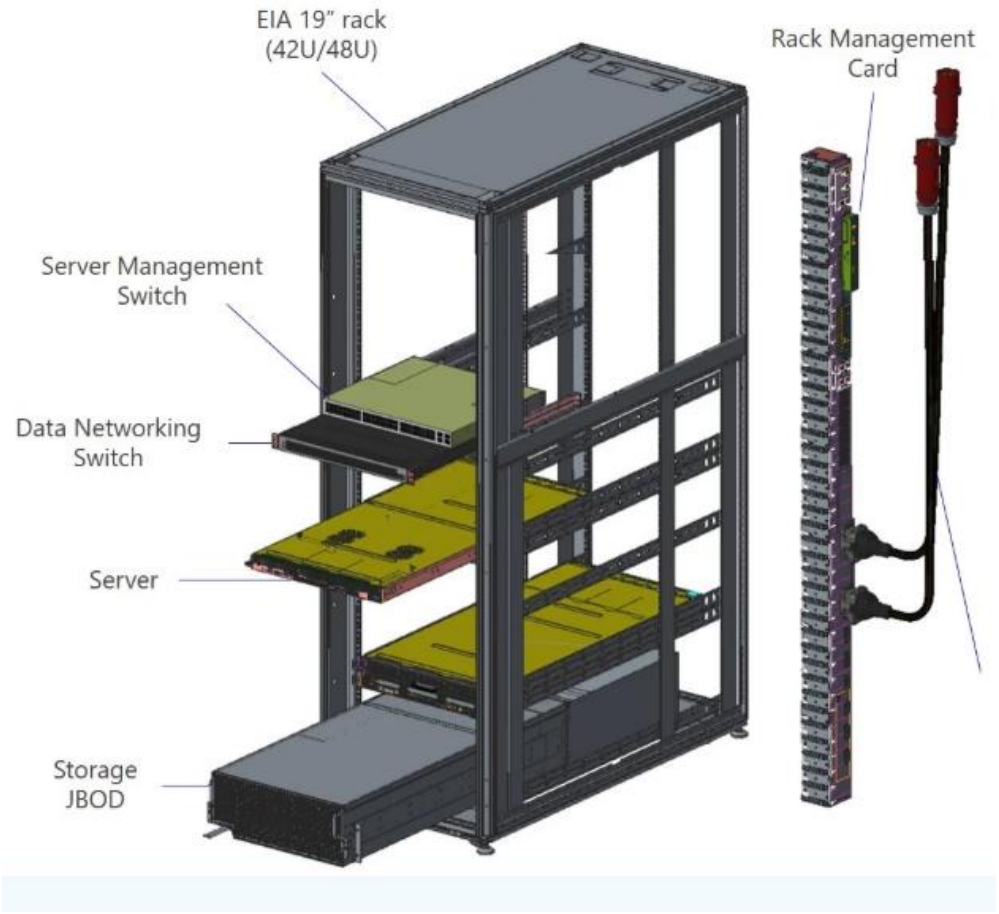
- Most Azure regions feature Availability Zones
- Data centres are split into 3 “logical zones”
  - The 3 you see can be different in every subscription
- Independent
  - Power
  - Cooling
  - External network connections
- Updates are staged across Availability Zones



https://learn.microsoft.com/en-us/rest/api/resources/subscriptions/list-locations

Availability Sets: Update & Fault Domains





Some Extra Notes

- Proximity Placement Groups (PPGs)
  - Minimum latency required between compute nodes
  - Sacrifice availability by placing nodes as close together as possible
- PaaS
  - Runs in VMs (somewhere in the platform)
  - Some do not use availability zones until you configure it
    - “Zonal deployment” or “regional deployment”
    - Probably using Availability Sets
  - Opting into Availability Zones
    - Check the docs first if there is a pricing impact

Resource Groups

- The resource group ID is part of the resource ID
  - /subscriptions/abcdefgh-1234-abcd-b683-4d935b701111/resourceGroups/p-db1hub-net
  - /subscriptions/abcdefgh-1234-abcd-b683-4d935b70111/resourceGroups/p-db1hub-net/providers/Microsoft.Network/virtualNetworks/p-db1hub-vnet
- Scenario:
  - Resource Group location = North Europe
  - North Europe goes down
  - Failover resource must be configured
  - Failover resource ID contains the Resource Group => *No CRUD operations*

Azure Resources & Availability

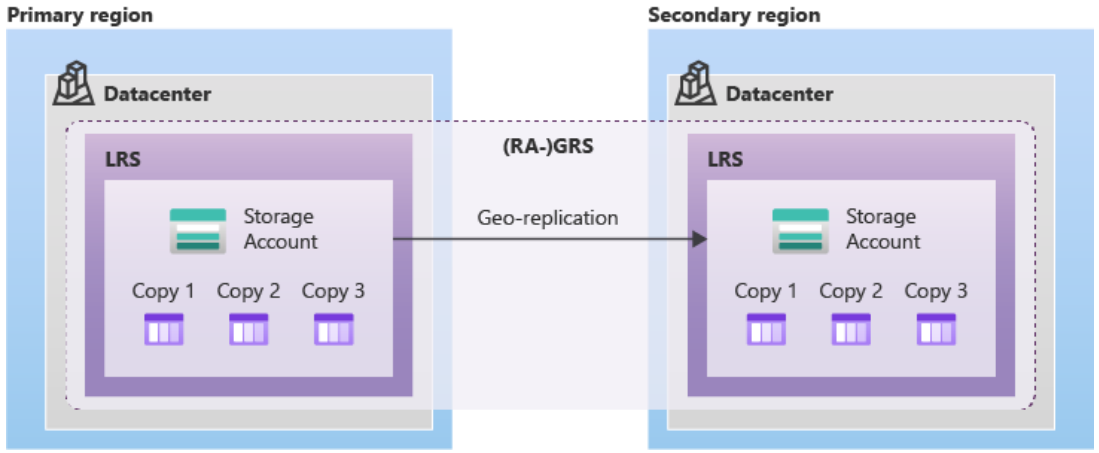
Understanding the most common resource types

Managed Disks

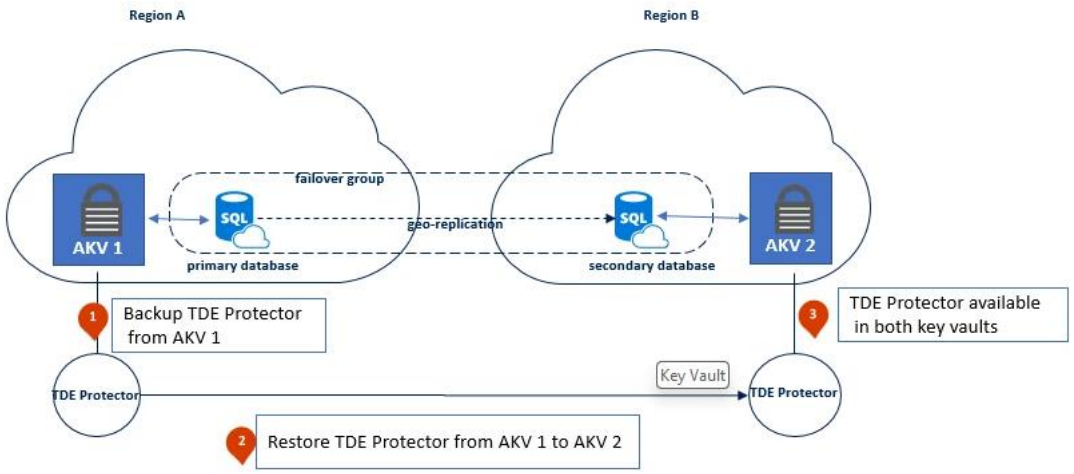
- Can be:
  - Locally redundant: 3 copies in one storage cluster/data centre
  - Zone redundant: 3 copies across 3 Availability Zones
- Zone Redundant failover:
  1. VM goes down with a single data centre
  2. Force-detach the disk(s)
  3. Attack the disk(s) to a new VM
  4. Start the new VM

Storage Accounts

- Locally Redundant Storage:
  - 3 copies of every block in “availability set” in one storage cluster/data centre
- Zone Redundant Storage:
  - 3 copies in different Availability Zones
- Replication only to (available) paired region
  - Geo-Redundant Storage (GRS)
  - Read-Access Geo-Redundant Storage (RA-GRS)
  - Geo-Zone-Redundant Storage (GZRS)
  - Read-Access Geo-Zone-Redundant storage (RA-GZRS)



Key Vault



- Automatically uses Availability Zones
- Failover managed by Microsoft
- Replicated only to (available) paired region
- Automatic replication to (available) paired region, except:
  - Brazil South
  - Brazil Southeast
  - West US 3

Azure SQL

Feature	SQL Database	Managed Instance	SQL Server on VM
HA Built-in	✅ Yes	✅ Yes (Business Critical)	❌ Manual setup required
Zone Redundancy	✅ Premium tier	✅ Business Critical	✅ With AG or FCI
Cross-region DR	✅ Auto-Failover Groups	✅ Auto-Failover Groups	✅ With AG or log shipping
Full SQL Server features	❌ Limited	✅ Near full	✅ Full

Cosmos DB

- Not zone-redundant by default
  - Can be enabled
- Multi-region
  - Select any supported region
  - Comes with substantial complexity: consistency management

Networking

Connecting Services

Connecting to Azure Services

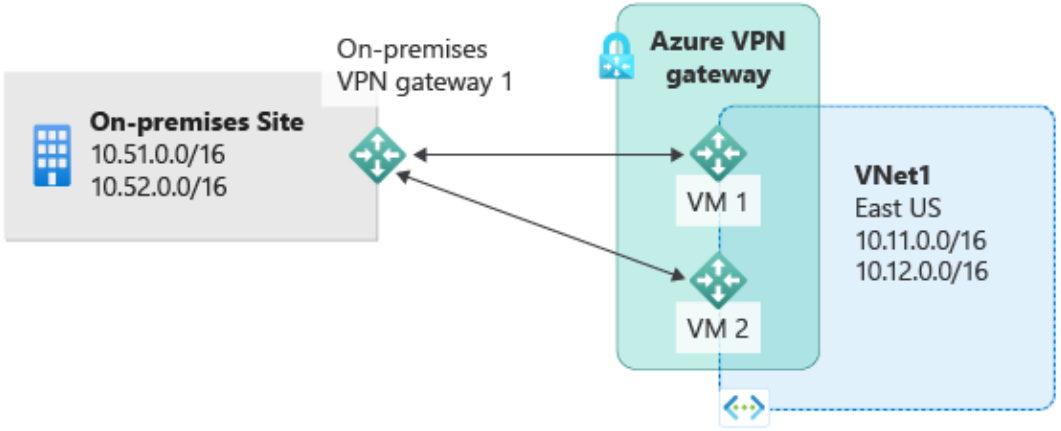
- We access most Microsoft cloud services via Front Door
- Anycast redirects us to the nearest available Edge Data Centre
- Our connections transit across the Microsoft Global Network

Redirecting Internet Client To Our Services

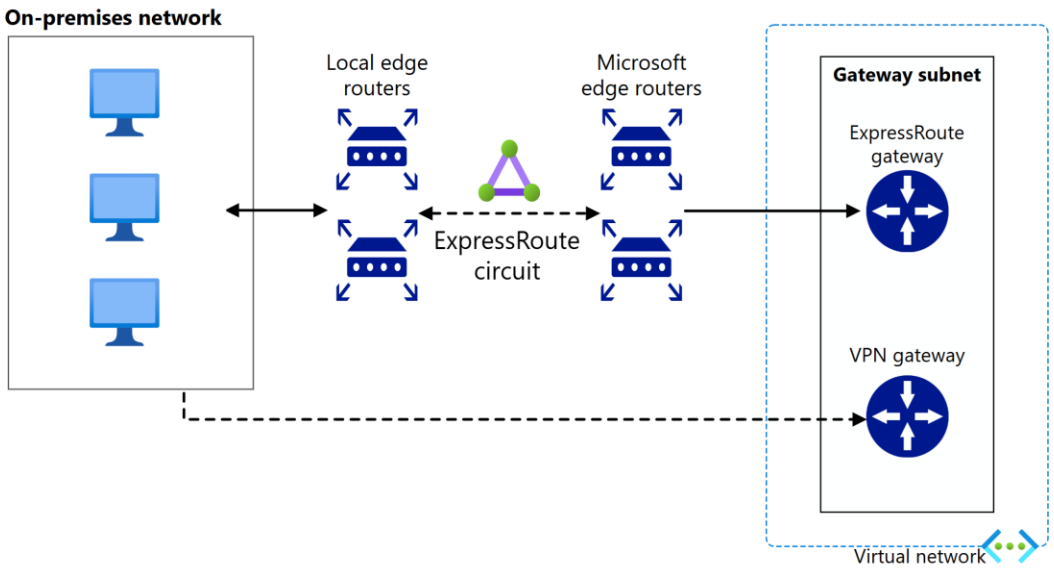
Feature / Capability	Azure Front Door	Azure Traffic Manager	Azure Load Balancer (Geo)
Type	Global application delivery network (Layer 7)	DNS-based traffic routing	IP-based global load balancing (Layer 4)
Routing Method	HTTP/HTTPS routing with path-based rules	DNS redirection based on health/performance	Any TCP/UDP traffic via public IPs
Failover Speed	Near-instant (active monitoring + probe fail)	DNS TTL dependent (can be slow)	Near-instant (probe-based)
Protocol Support	HTTP/HTTPS only	All protocols (via DNS)	TCP/UDP
Health Probes	Yes (per endpoint, per path)	Yes (per endpoint)	Yes (per region)
SSL Termination	✅ Yes	❌ No	❌ No
Custom Domain Support	✅ Yes	✅ Yes	✅ Yes
Session Affinity	✅ Yes (cookie-based)	❌ No	✅ Yes (source IP)
Geo Routing	✅ Yes (based on client location)	✅ Yes	✅ Yes
Caching & Acceleration	✅ Yes (built-in CDN)	❌ No	❌ No
WAF Integration	✅ Yes (native)	❌ No	❌ No
Use Case	Web apps, APIs, global websites	Lightweight DNS failover, legacy apps	Global TCP/UDP services, gaming, IoT
HA Scope	Multi-region, zone-aware	Multi-region (DNS-based)	Multi-region (IP-based)

Site-to-Site VPN

- VPN Gateway
  - Active/passive by default
  - Run Availability Zone support at the same cost
- Deploy Active/Active
  - Second Public IP Address
  - Support 2 connections from 1 remote site
- Ideally, second VPN:
  - From firewall cluster
  - Via second ISP/media
- See multi-resilient VPN



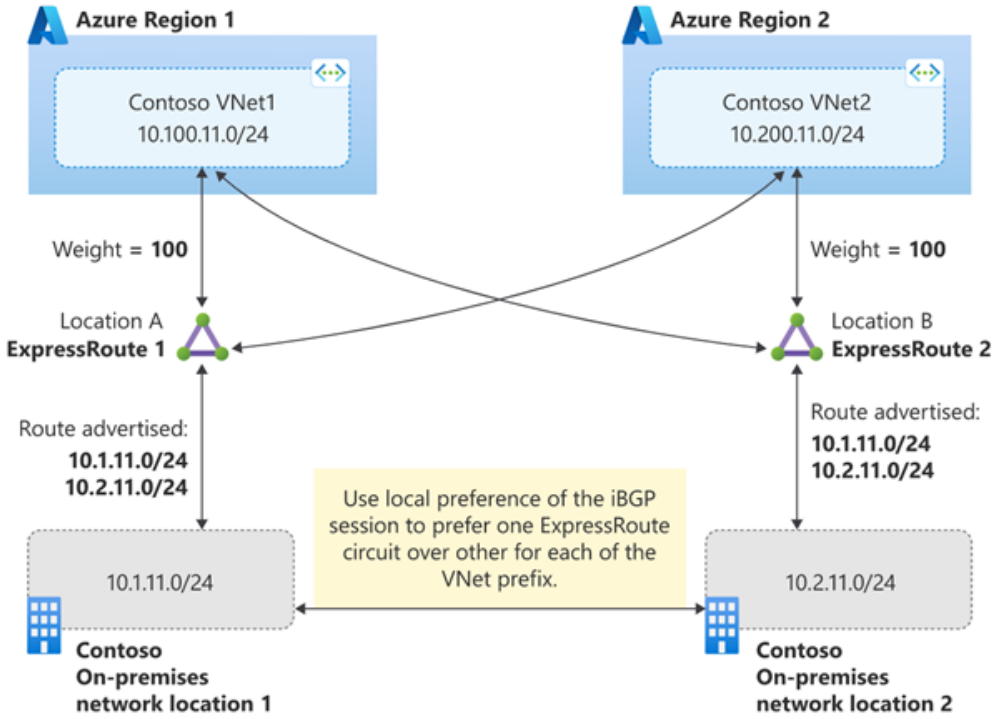
ExpressRoute & VPN



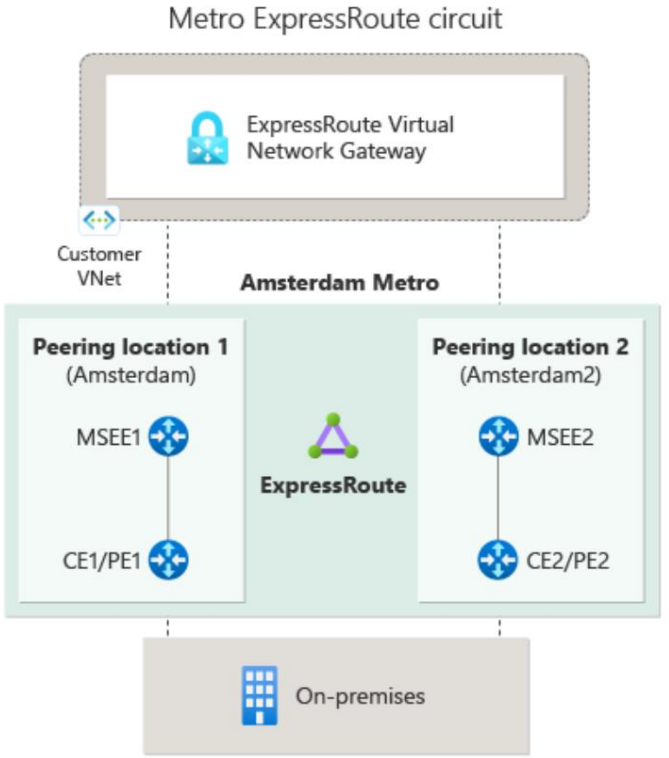
- ExpressRoute is HA
  - Dual routers at every point
  - Dual wires in the circuit
- Accidents happen!
- Run a parallel VPN
  - Azure prefers ExpressRoute
  - Will automatically failover to VPN
- Ensure that all prefixes are available via VPN
  - Local Network Gateway
  - BGP propagation

ExpressRoute Resilience

ExpressRoute Bow-Tie



ExpressRoute Metro



Technical Risk Assessment

Understanding the nature of outages

Single Fault Domain Outage

- Storage
  - Locally redundant at least
- PaaS
  - Use at least 2 instances
- Highly Available Virtual Machines
  - Choose Availability Sets at least
- Monolithic Virtual Machines
  - Use Zone Redundant Managed Disks
  - Use VM replication/failover

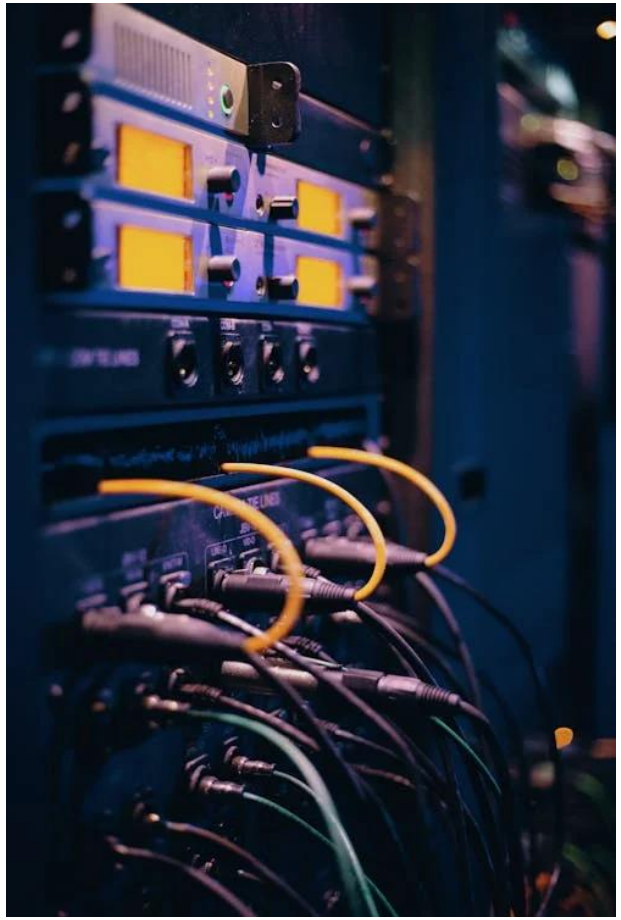
Single Data Centre/Availability Zone Outage

- Storage
  - Zone-redundant at least
- PaaS
  - Availability Zones at least
- Highly Available Virtual Machines
  - Choose Availability Zones at least
- Monolithic Virtual Machines
  - Zone Redundant Managed Disks
  - VM replication/failover

Regional Outage

- Storage
  - Geo-redundant at least
  - Multi-region replication
- PaaS
  - Multiple deployments
- Highly Available Virtual Machines
  - Multiple deployments
  - VM replication/failover
- Monolithic Virtual Machines
  - VM replication/failover

Site-To-Site Outage



- Single office
  - Active-active/multi-resilient VPN
  - ExpressRoute Metro/bow-tie
- Multiple offices
  - Multiple connections from offices > route via WAN
  - Active-active/multi-resilient VPN
  - ExpressRoute bow-tie/ExpressRoute Metro
- Mult-Cloud
  - Office > Other Cloud > Azure

Photo by Josh Sorenson

Complete Azure Outage

- It happens
  - I actually had an AWS joke here ☺
- Go multi-cloud?
  - Easy to say
  - Not easy to do
- Challenges:
  - Double the cost: Cloud is already expensive
  - Double the complexity: Different platforms and resources to manage & integrate
  - Double the skills: Already hard to find Azure skills

Extended Local Power Outage

- Does your site have generators?
  - Probably
- Does your ISP have local generators?
  - Probably not
  - Routers will go down
- Can your on-premises services survive a cloud outage?
- Critical services: Consider Hybrid Cloud

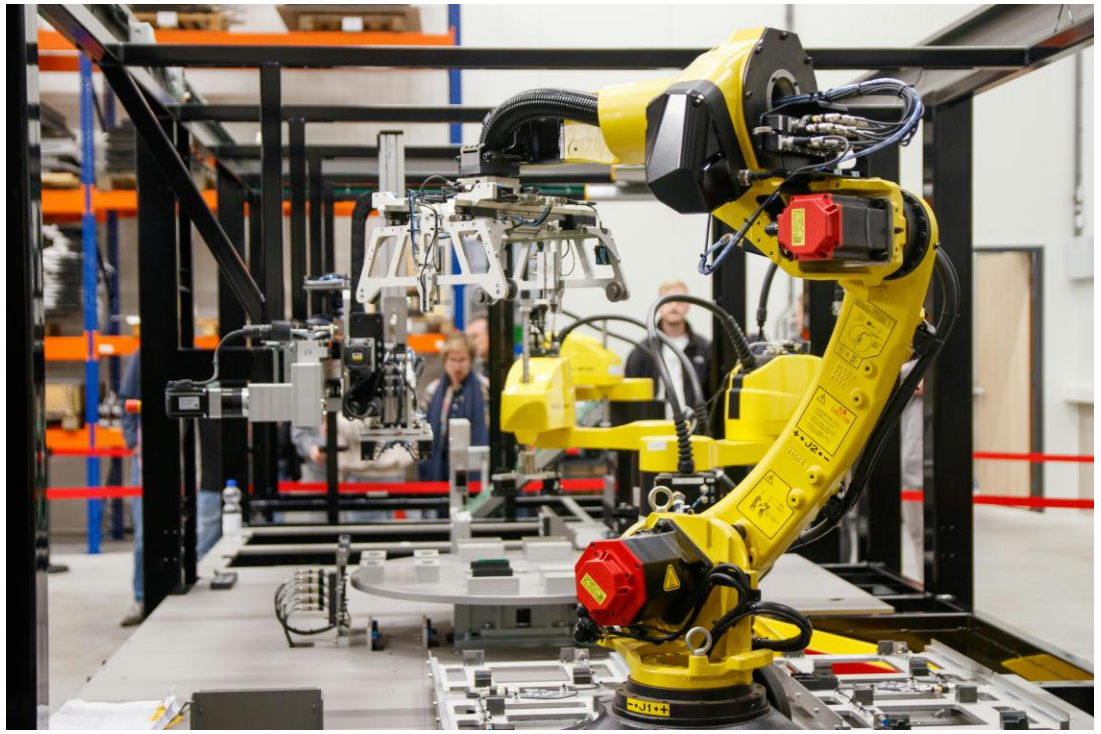


Photo by Freek Wolsink

Gotchas

Just when you thought you had it all under control

Non-Paired Regions

- Some regions have no pair at all!
- We can replicate to elsewhere:
  - Azure VMs
  - Databases
- But what about?
  - Storage accounts
  - Key Vault
  - Backup/Recovery Services Vaults

https://learn.microsoft.com/en-us/azure/reliability/regions-list

Unavailable Regions

- Most local paired regions are restricted
  - Small size
  - Few resource types/sizes
  - **Selected customers only**
- Norway West *exists*
- Most of you cannot use it
  - GRS does not work
- Storage accounts, Key Vault, Backup/Recovery Services Vaults?!?!?!

Asymmetrically Paired Regions

- Most pairs are symmetrical:
  - North Europe <> West Europe
- Some regions are asymmetrical (one way):
  - Brazil South > South Central US
  - US Gov Arizona > US Gov Texas > US Gov Virginia
  - West India > South India > Central India
  - West US 3 > East US <> West US

Tensions With The USA

The tangerine divide

Rising Tensions

BBC Greenland again tells Trump it is not for sale

US suspends all military aid to Ukraine in wake of Trump-Zelenskyy row

The Guardian

Clementine Cloud Curtain?

POLITICO

Trump can pull the plug on the internet, and Europe can't do anything about it

The Register

Under Trump 2.0, Europe's dependence on US clouds back under the spotlight

Technologist Bert Hubert tells *The Reg* Microsoft Outlook is a huge source of geopolitical risk

techovedas
SEMICONDUCTOR INSIGHTS UNLOCKED

Why Europe's Saying 'No Thanks' to US Cloud Providers Under Trump ?

War

Most of us never thought that this was a possibility

Russia Invades Ukraine

- May 1997
  - Treaty on Friendship, Cooperation, and Partnership
- February 2014
  - Russian troops without insignia seized control of Crimea.
- March 2014
  - Russia formally annexed Crimea after a disputed referendum.
- April 2014
  - Russian-backed separatists began fighting in Donbas (eastern Ukraine).
- Sept 2014
  - Minsk 1 peace agreement
- February 2025
  - Minsk 2 peach agreement
- 24 February 2022
  - Russia launched a full-scale invasion across multiple fronts, including Kyiv, Kharkiv, and the south.

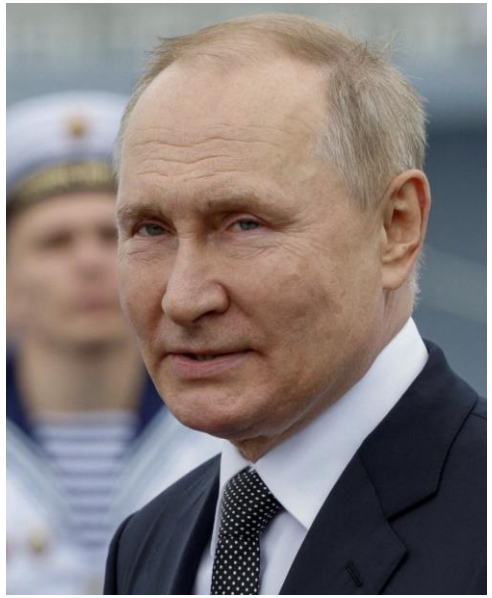
Land For Peace / Escalate to De-Escalate

Alexander I

Year	Event / Treaty	Outcome
1807	*Treaty of Tilsit* (with Napoleon)	Russia became a nominal ally of France. Alexander accepted terms that spared Russian territory and gained influence.
1809	War with Sweden	Russia annexed the **Grand Duchy of Finland**, expanding westward.
1812	Russo-Turkish War ends	Russia acquired **Bessarabia** from the Ottoman Empire.

Joseph Stalin

Year	Event / Treaty	Outcome
1939	*Molotov–Ribbentrop Pact* (with Nazi Germany)	Secret protocol divided Eastern Europe; USSR annexed eastern Poland, Baltic states, and parts of Romania and Finland JSTOR .
1940	*Annexation of Baltic States*	Estonia, Latvia, and Lithuania forcibly incorporated into the USSR.
1944–45	*Postwar Occupations*	Red Army occupied Eastern Europe; installed pro-Soviet regimes in Poland, Hungary, Romania, Bulgaria, and East Germany Revision World .
1947	*Paris Peace Treaties*	Formalized Soviet territorial gains in Eastern Europe and the Balkans.



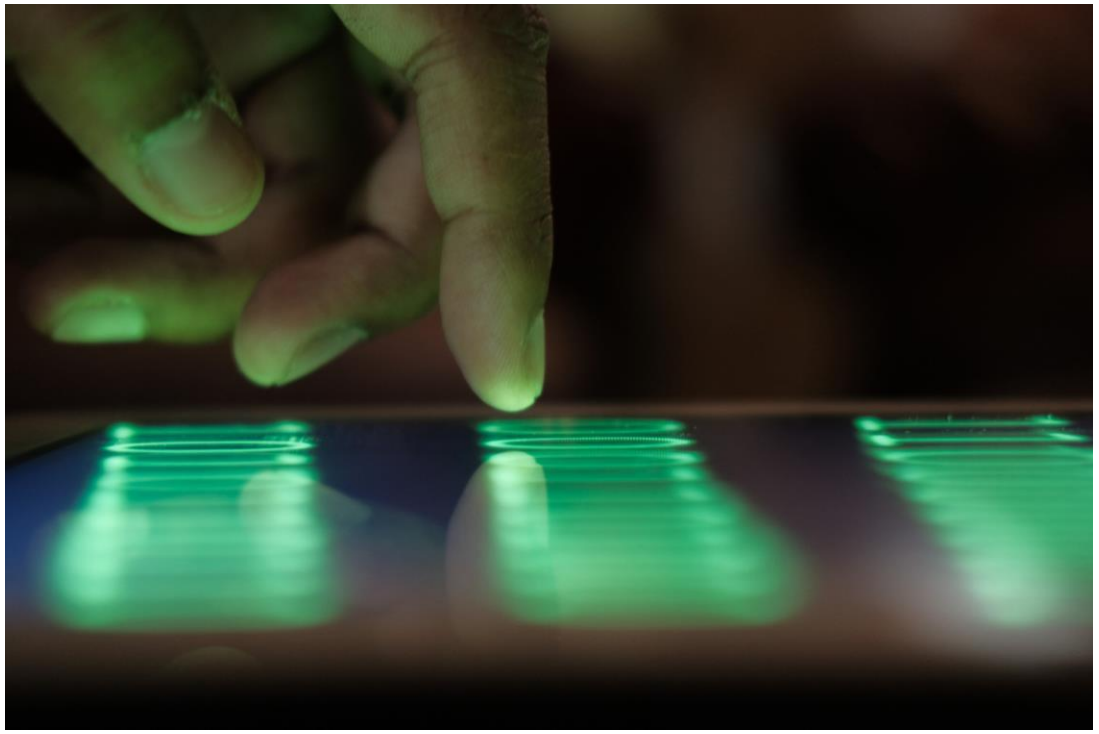
Vladimir Putin

Year	Event / Tactic	Outcome
2008	*Invasion of Georgia*	Russia occupied Abkhazia and South Ossetia; recognized them as independent states.
2014	*Annexation of Crimea*	Russia seized Crimea after covert military action and a disputed referendum.
2014–2021	*Donbas destabilization*	Supported separatists in eastern Ukraine; created frozen conflict zones.
2022	*Full-scale invasion of Ukraine*	Captured large parts of Donetsk, Luhansk, Zaporizhzhia, and Kherson; declared annexation.

After Ukraine?

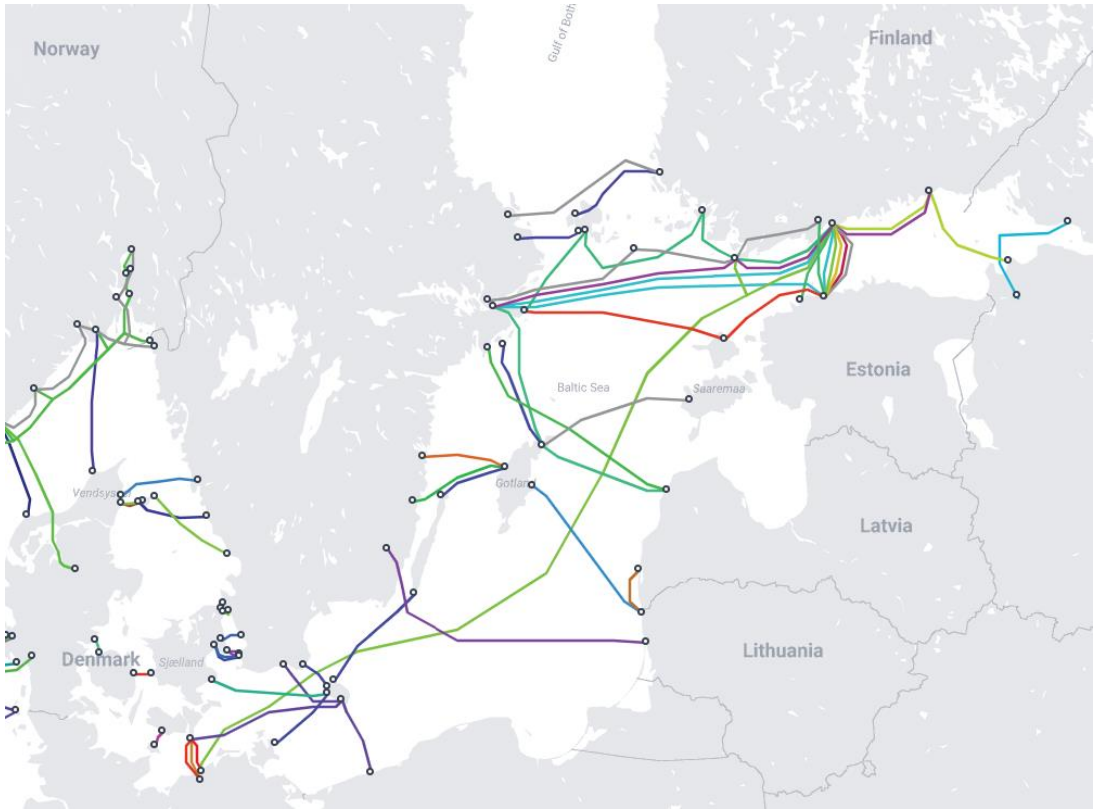
- Widely thought the Balkans are next:
  - Estonia
  - Latvia
  - Lithuania
- Those countries expect it
- Large Russian-speaking populations
- Isolates the Kaliningrad enclave

Cyber Attacks



- Cyber attacks will be the start
- Targets:
  - Government
  - Health
  - Military
  - Telecoms
  - Utilities
  - Transport
  - Manufacturing
  - Finance
- Disrupt logistics/government
- Cause confusion/panic/distractions

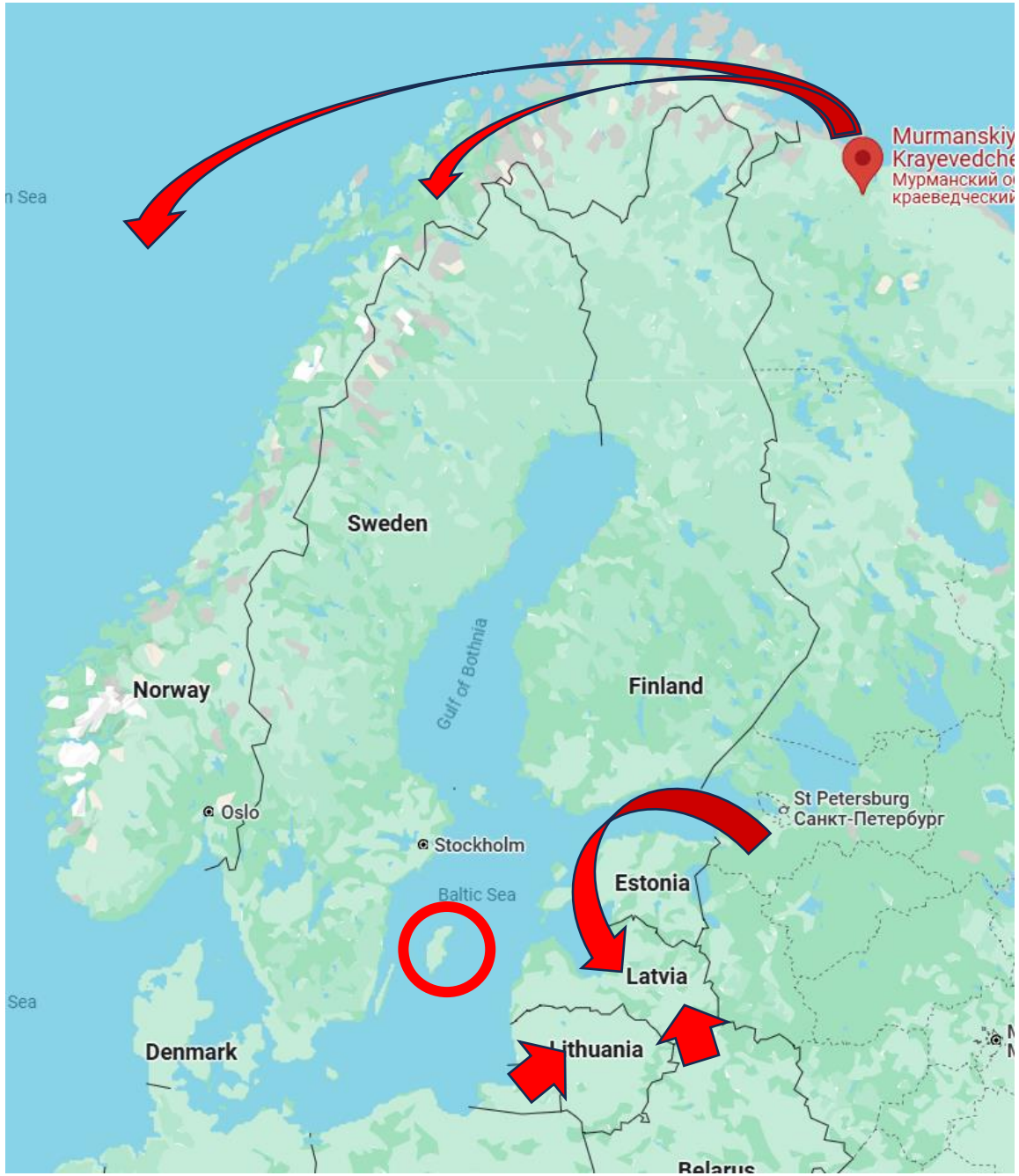
Have We Seen “Research”?



- Oct 2023 – Newnew Polar Bear damaged telecom cables between Finland and Estonia while dragging anchor.
- Nov 2023 – Swedish telecom cables disrupted in territorial waters; linked to foreign vessel activity.
- Dec 2023 – Finnish telecom cable damaged off Porkkalanniemi; anchor dragging suspected.
- Jan 2024 – Estonian cable outage traced to seabed disturbance; no official attribution.
- Mar 2024 – Lithuanian cable briefly disrupted; cause undetermined.
- May 2024 – German–Swedish cable interference reported; no damage confirmed.
- Nov 2024 – C-Lion1 and BCS East-West Interlink cut within hours; sabotage suspected.
- Dec 2024 – Estlink 2 and two telecom cables severed by oil tanker Eagle S near Finland.
- Jan 2025 – Latvian–Swedish fibre cable cut near Gotland; suspicious vessel spotted nearby.

Attack On Baltics

- Mass naval movement from Murmansk
- Naval/EMP attack on Gotland/Sweden
- Navy from St. Petersburg
- Army from Belarus
- Army from Kaliningrad enclave



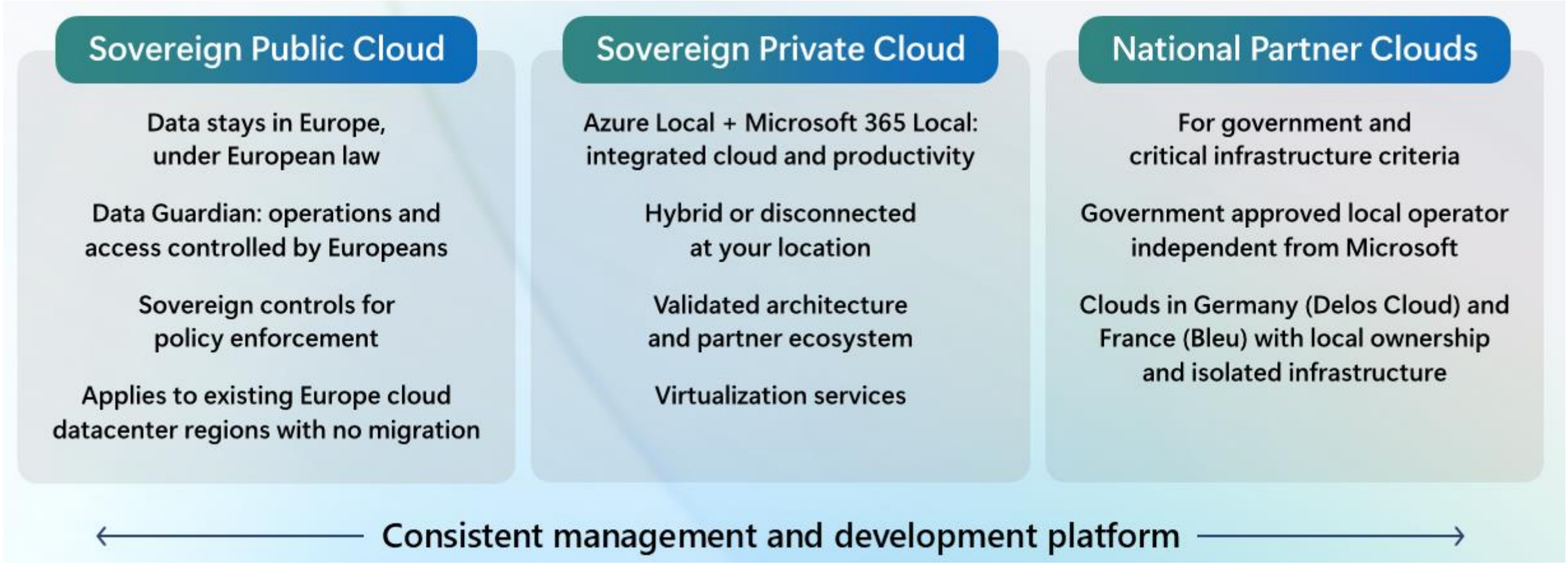
Attack (Microsoft) Cloud

- Norway East > Norway West
- Sweden Central > Sweden South
- “Finland South” > ?
- What happens when the primary regions go offline?

What Is Microsoft Doing?

Rapid response to fear

Microsoft Sovereign Clouds



Microsoft Sovereign Cloud Public

- An evolution of “regular” Azure
  - Access to all the features
  - Hyperscale
- Will be offered
  - All existing European datacenter regions, for all European customers
  - Enterprise services such as Microsoft Azure, Microsoft 365, Microsoft Security and Power Platform
- Features:
  - EU Data Boundary: Data in EU/EFTA stays in EU/EFTA
  - Data Guardian: Only MS staff in Europe can access European systems
  - 5 European digital commitments
  - Azure Confidential Computing
  - External key management: Store customer encryption keys *in* a European HSM
  - Regulated Environment Management: Manage the sovereignty features

Azure Local

- The latest private cloud brand
  - System Center Virtual Machine Manager Self-Service Portal 2.0 Service Pack 2.0
  - Windows Azure Pack
  - Azure Stack
  - Azure Stack Hub / Azure Stack Edge / Azure Stack HCI
- You place it where you want
- Limited services
- Not as flexible as Hyper-V!
- Azure Local Disconnected is very restricted
- Decision:
  - Azure Local: If you need private ***cloud***
  - Hyper-V/Nutanix/KVM/Proxmox: If you need on-premises compute

National Partner Clouds

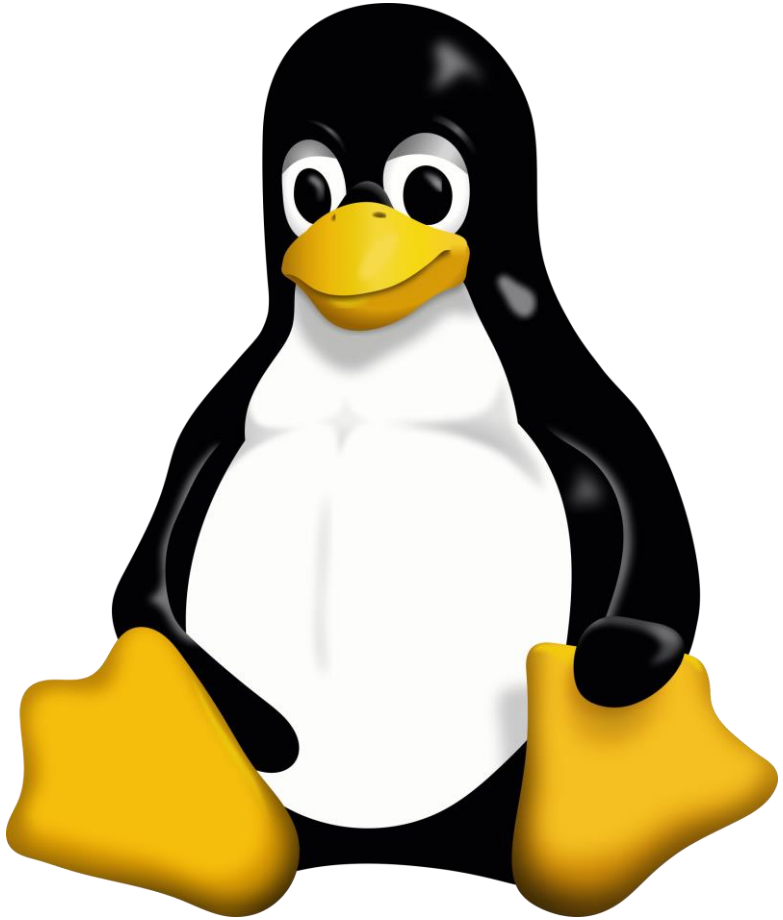
- Remember “Black Forest”?
  - German operated Azure 2016-2021
  - Retired because it wasn’t legally required & too expensive
- That model is back!
  - Germany:
    - “Delos Cloud”
    - Microsoft, SAP, and Arvato Systems
  - France:
    - “Bleu”
    - Microsoft, Capgemini, and Orange
- The source code is being put into escrow in Europe

European Clouds

- Cloud:
  - Self-service
  - Broad network access
  - Resource pooling
  - Rapid elasticity
  - Measured service
- Beware the use of “Cloud” by marketing
  - May be just VMs and S3 compatible storage
- Migration/failover may be more limited challenging than you imagine

Bake It Yourself Cloud

- Be prepared for permanent “noob” status
- Many Azure features:
  - Originated as open source
  - Have open source alternatives
- Do you want to bake your own?
  - SQL clusters
  - Kubernetes
  - Logic Apps



Some On-Premises Alternatives

Azure Service	On-Premises Alternative	Notes
Azure Kubernetes Service (AKS)	Rancher, OpenShift, K3s, Kubeadm	Full Kubernetes orchestration with enterprise support.
Azure Functions	OpenFaaS, Knative, Kubeless	Serverless frameworks for event-driven workloads.
Azure Blob Storage	MinIO, Ceph, NetApp ONTAP, Dell ECS	Object storage with S3-compatible APIs.
Azure Active Directory	Windows AD, FreeIPA, Keycloak	Identity and access management for local domains.
Azure Key Vault	HashiCorp Vault, Thales HSM, CyberArk	Secrets and key management with HSM integration.
Azure Monitor / Log Analytics	Elastic Stack (ELK), Grafana + Loki, Splunk	Observability and log aggregation platforms.
Azure DevOps / GitHub	GitLab, Jenkins, TeamCity	CI/CD and repo management on-premises.
Azure Policy / Defender for Cloud	OpenSCAP, Wazuh, Falco, Tenable.sc	Compliance and security posture management.
Azure Event Grid / Service Bus	Apache Kafka, RabbitMQ, NATS	Messaging and event-driven architecture.
Azure Container Registry	Harbor, Docker Registry, Quay	Local container image storage and management.

Geo-Political Risk Assessment

Understanding the nature of outages

Undersea Cable Attacks

- For organisations with International operations
- Build failover paths in site-Azure connections
  - Consult with ISP about their connectivity
- Build multiple connections from your sites
- Multi-cloud?
  - Alternative routes: Oracle<>Azure, GCP<>Azure, AWS<>Azure
- Route via WAN to active connections
  - “Self-healing” SD-WAN

Measure The Risks

- Will the USA really cripple their top 5 largest companies?
  - NVIDA: $4.66 trillion
  - Microsoft: $3.96 trillion
  - Apple: $3.94 trillion
  - Alphabet: $3.22 trillion
  - Amazon: $2.42 trillion
- Will Russia bring Europe into a war?
  - European economic ties would be 100% severed
  - Military has struggled with Ukraine
  - Male population is depleted

Should We Still Use Public Cloud?

- The Cloud still makes sense
- Advantages:
  - Instant availability
  - Hyperscale
  - Access to “cloud-only” services
  - Developer operator friendly
- Businesses:
  - If you abandon The Cloud
  - What happens to you if your competitors do not?

The Clementine Curtain Dropping

- Use Sovereign Public Cloud
  - Consider compute/data mobility (VM/container)
  - Replicate to on-premises using Veeam/etc
  - Going to be somewhat restrictive/complicated
- Sovereign Private Cloud
  - Still going to be a reliance on Azure (billing & management)
  - Use Hyper-V/Nutanix/Proxmox instead?
- Use National Partner Clouds
  - If you are happy with data in Germany/France
  - Always going to be less capable than Azure
  - Always going to be more expensive than Azure

Russian Invasion

- Replicate to alternative Azure regions
  - “Sorry, the hotel is full”
- Replicate to remote/secure virtualisation farms
  - Guaranteed capacity
  - Use VMs/containers for mobility
  - Leverage Veeam, etc, for replication/backup

Conclusions

Wrapping Up

Closing Thoughts

- “The world is on fire”
  - Great click-bait
  - Giving certain consultants lots of money
- Should you build for resilience?
  - Yes
- How?
  - Assess the risks – MEASURE them
  - Compare cost/complexity/feature loss of building availability VS measured risk
  - Build the availability that is required
  - Design cloud pattern applications

Thank You!

Join in Room 2 at 14:00

- Aidan Finn
- http://aidanfinn.com
- http://cloudmechanix.com
- @joe_elway

Online Course

Designing Secure Azure Networks

January 26/27

Discount Code For NIC

NicThePacket

25% off