BUILDING A PRODUCTION-GRADE OCI LANDING ZONE FOR A REAL DISASTER RECOVERY PROJECT

Oronzo Antonelli, Senior Consultant - Cloud Architect

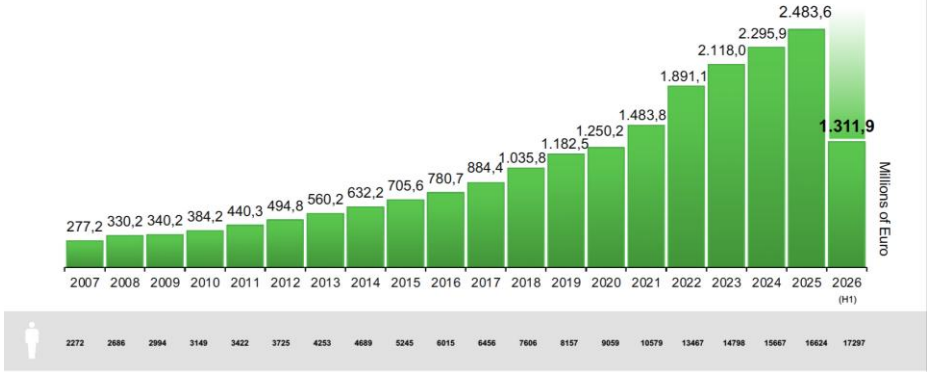
REPLY TECHNOLOGY

REPLY CORPORATE INTRODUCTION

REPLY

To excel in helping our customers exploit relevant innovation brought about by economic changes and driven by internet technologies.

REVENUE & PEOPLE



WHERE WE ARE

REPLY SERVICES

PEOPLE
DIGITAL HUMANS · COPILOTS · WORKPLACES

MACHINES
ROBOTICS · AUTONOMOUS THINGS · IOT & CONNECTED PRODUCTS

DIGITAL EXPERIENCE
PRODUCT DESIGN BRAND EXPERIENCE · DIGITAL MARKETING · IMMERSIVE EXPERIENCES

ENTERPRISE PLATFORMS
ADVANCED ANALYTICS · INDUSTRY SPECIFIC PLATFORMS · APPLICATION SUITES & CX PLATFORMS

ARTIFICIAL INTELLIGENCE

TECHNOLOGY FOUNDATIONS
COMPUTING · DATA · CYBERSECURITY · NETWORK

BUSINESS FOUNDATIONS
BUSINESS ENGINEERING · OPERATIONAL EXCELLENCE · RESILIENCE AND RISK

TECHNOLOGY REPLY

«Digital Innovation, Delivered»

TECHNOLOGY, IN NUMBERS

FOUNDING YEAR
1996

EMPLOYEES
800+

CERTIFIED
650+

OFFICES
8

ITALIAN PRESENCE
Turin | Milan | Roma | Genova | Verona | Padua | Treviso | Bari

LEARNING
Through specialization courses provided by the main software vendors and participation in Beta Programs, we pursue a process of constant technological and methodological innovation.

SKILLS SET
Agentic AI Solution Architects
AI Experts
Analytics Expert
Appian Expert
Cloud Architects
Data Architects
Data Engineers
Data Scientists
DB Administrators
DevOps Engineers
Full Stack Developers
Project Managers
Scrum Masters
System Administrators

PARTNERSHIPS

Thanks to the strength of the alliance, we successfully implement **Oracle Cloud-based solutions** with excellent results and reduced development time. We can also boast a **Qlik** and **Appian** competence centre.

COMPETENCES

In addition to our partners' technologies, we have **in-depth expertise on different tools and services** we integrate into our solutions.

Java · python · Scala · Apache Airflow · OpenCV · DELL BigQuery · Data Factory · amazon REDSHIFT · snowflake · Qlik · React · Swift · Flutter · APACHE Camel · IONIC · kubernetes · mongoDB · Kotlin · TensorFlow · CLOUDERA · Spark · MySQL · EASYVISTA · vmware · solace · dbt · DEDAGROUP STEALTH · hadoop · kafka · Azure · OpenAI · ANTHROP\C · Amazon Bedrock · ollama · HITACHI · Hugging Face · Vertex AI · OCI Generative AI

OFFER LINES

The **Technology Reply** offer is structured around **seven different pillars** that enable us to design, engineer, develop and maintain technologically complex **end-to-end solutions**.

1. MICROSERVICES & DEVOPS
2. DATA ANALYTICS
3. CLOUD OPERATION
4. GOVERNANCE
5. OBSERVABILITY
6. ARTIFICIAL INTELLIGENCE
7. LOW CODE

YOUR PRIMARY DATACENTER STOPS NOW. DO YOU KNOW WHAT IT TAKES TO COME BACK?

In most organizations the honest answer is "I do not know".

Failover is the last **5 per cent** of the work. The rest is what sits underneath, and it is called a landing zone.

HOW THIS TALK IS BUILT

ONE QUESTION, AND THE ORDER IN WHICH WE ANSWER IT

1. **Foundations.** The primary site, what has to be protected, and what a landing zone is
2. **Recovery strategy.** Which services come back, and by which mechanism
3. **The landing zone.** Identity, network, operations and code, layer by layer
4. **Workloads on top.** VMware, the backup, the directory and the database, on top of it
5. **Wrap-up.** The big picture, all of it in one drawing, and what to take home

The order is the argument. The first three steps are the ground. The fourth is what lands on it. The drawing comes last, because only by then does every box mean something.

FOUNDATIONS

1. **Foundations**
2. Recovery strategy
3. The landing zone
4. Workloads on top
5. Wrap-up

WHAT HAS TO BE PROTECTED

A LARGE DATACENTER, GROWN OVER YEARS.

Virtualization

- **VMware vSphere**, with about **370 virtual machines**, one console for nearly everything
- **Oracle Linux Virtualization Manager (OLVM)**, small, with the **mission-critical database**

What runs on top

- About **180 Windows servers** and **20 Linux servers**
- About **170 virtual desktops** for users

Those same servers run around 50 databases, Oracle and SQL Server, and each one comes back with the machine it sits on. The one that does not is the OLVM one.

These applications move as they are. What runs on-prem today has to run the same way on the recovery site, with the same versions and the same addresses.

WHAT A LANDING ZONE IS

THE RULES YOU AGREE BEFORE THE FIRST MACHINE

A landing zone is not a cloud account. It is **identity, network, security and governance**, decided and built before any workload lands.

Without a landing zone	With a landing zone
You create a machine and start	You agree the rules first
Access belongs to whoever was there	Identity is federated and traced
Logs end up everywhere	Logs land in one place
Every project builds its own network	The network is one design

The provider gives you the pieces. The landing zone is the picture you build with them.

THE DR SITE STANDS ON ITS OWN

THE RECOVERY SITE CANNOT DEPEND ON WHAT IT IS SAVING

- **Identity.** It must authenticate even if the primary identity provider is unreachable
- **Network.** It must have its own path, not one going through the site that is down
- **Governance and logs.** They must stay readable during the incident, not after
- **Data.** It has to be there before the disaster, not start moving during it

Independence is something you keep, not something you build in the emergency

- Every dependency on the primary site is **one more way the recovery fails with it**
- The site has to be **working at all times**, including the months nobody looks at it

A DR site with a single dependency on the primary site is not a DR site.

THE GOAL OF THE PROJECT

BUILD A SITE WHERE THE BUSINESS CAN START AGAIN

The project in one line. Take a datacenter that runs on-prem today, and build in the cloud the place where it can come back, close enough for the data to travel.

- A place able to **restart the datacenter**, so the people who depend on it keep working
- Applications **come across as they are**, because rewriting them is not on the table
- You move **the hypervisor**, so the machines travel exactly as they are, with the same team and the same console

And rules were given to us.

- **All traffic** is governed and inspected by the firewalls
- The **corporate identity provider** is the only source of identities for the cloud console
- The console is for **OCI users only**, never for end users

RECOVERY STRATEGY

1. Foundations
2. **Recovery strategy**
3. The landing zone
4. Workloads on top
5. Wrap-up

WHAT WE PROTECT, AND HOW

FOUR SERVICE CATEGORIES, AND TWO MECHANISMS

Rubrik drives every restore, and **Data Guard** the switchover.

Service category	From	To	Mechanism
Front-end	VMware	OCVS	Restore from backup
App services	VMware	OCVS	Restore from backup
Ordinary databases	VMware	OCVS	Restore from backup
The critical database	OLVM	DBCS Managed service	**Switchover**

Restore from backup rebuilds the machine at a chosen point in time. **Switchover** hands the role to a live copy.

The critical database needs near-zero RTO.

WHO DECIDES RPO AND RTO

NOT THE INFRASTRUCTURE TEAM, AND NOT THE TOOL EITHER

For everything restored from backup, the two numbers are **set by the customer**, machine by machine, inside the backup policies.

- Each machine gets a policy chosen on **how critical that machine is**
- The policy fixes **how often** a snapshot is taken and replicated, and how long it is kept
- Those settings **are** the recovery point, and most of the recovery time

One service is the exception. For the critical database the target is **zero data loss**.

So what does the landing zone have to guarantee?

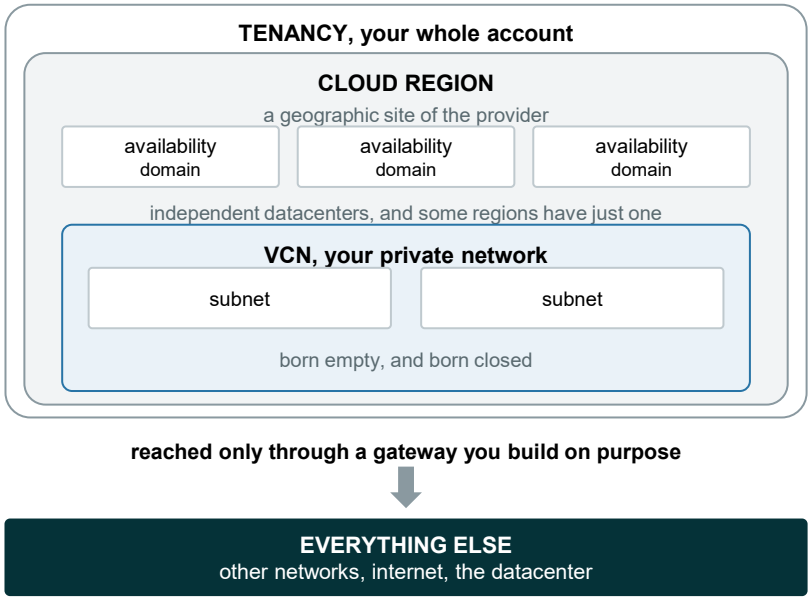
That **the restore works on the day it is asked for**, because network, identity and platform underneath are standing.

THE LANDING ZONE

1. Foundations
2. Recovery strategy
3. **The landing zone**
4. Workloads on top
5. Wrap-up

THE WORDS YOU NEED FIRST

THE CLOUD WORDS THIS TALK USES



Tenancy. Your account with the provider, and it holds **more than one region**.

Region. A geographic site of the provider. What you build there stays there.

Availability domain. An independent datacenter inside a region. Our recovery region has **only one**.

VCN. Your private network, cut into subnets. **Born empty** until you create something in it, **born closed** until you draw a path.

Nothing here connects by default. Every path is one somebody drew.

TWO REGIONS, TWO JOBS

TWO REGIONS DOING TWO DIFFERENT JOBS

Home region. This is where identities, groups and policies are managed, and where their original definitions live. It is fixed by the account that holds everything, not a choice.

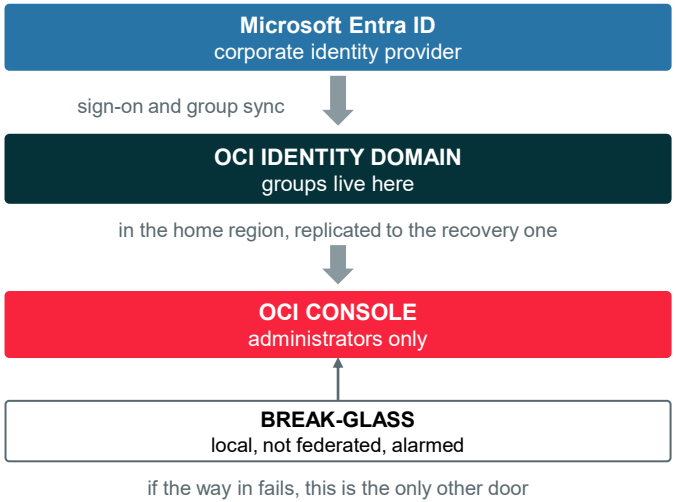
Disaster recovery region. This is where the real recovery site lives, that is the virtualization platform, the replicated data and the machines that will have to start again.

Why they are not the same, and it was a choice

- **It does not have to be this way.** A single region can hold both, and often does
- Here the home region follows **where identity and user management already live**, and the recovery region follows **where the workloads have to restart**
- The recovery region is chosen **close to the datacenter you protect**, for latency and bandwidth
- Keeping them apart **leaves room to grow**, which is why it was worth it here

IAM: HOW ADMINISTRATORS GET IN

THE CLOUD CONSOLE IS FOR OCI USERS, NEVER FOR END USERS



Federation delivers the requirement, one source of identities. Two steps.

- **Single sign-on**, so closing one account closes every door
- **Group sync**, because sign-on alone does not keep groups up to date

Groups live in an identity domain, replicated to the recovery region.

If federation is down, break-glass accounts are the only other way in.

One emergency key, and every use of it rings an alarm.

IAM: COMPARTMENTS AND ROLES

NOW THAT YOU ARE IN, WHAT ARE YOU ALLOWED TO TOUCH

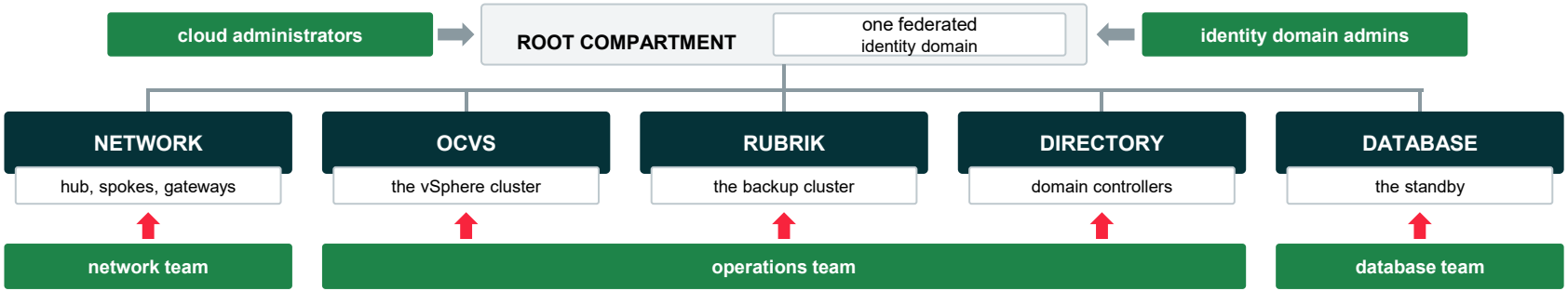
A **compartment** is a box you put resources in, and permissions follow the box. A policy says who can do what **inside which compartment**.

Compartment	Who operates in it
Everything, at tenancy level	Cloud administrators
Network, hub, spokes, the link out	Network team
OCVS, **Rubrik** and **Directory**, one box each	Operations team
Database	Database team

A policy is written on a compartment, so the boxes follow who administers what.

IAM: HOW THE TENANCY IS SPLIT

SPLIT IT INTO THE RIGHT BOXES, AND PERMISSIONS GET SIMPLE



one group can hold more than one box, when the same people run them

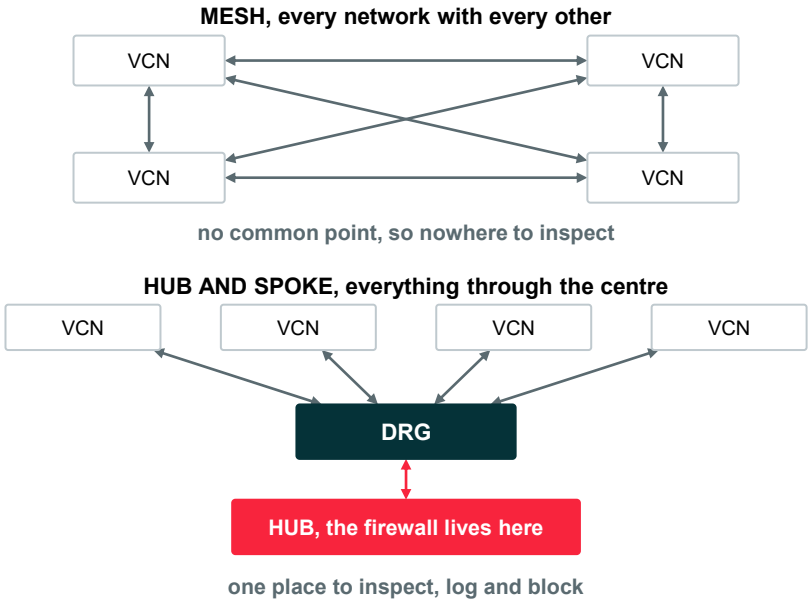
Splitting is what keeps permissions manageable. Each box is granted on its own.

- **One box per thing that is operated**, so OCVS, the backup and the directory stay apart
- **One group can hold several boxes**, when the same people run them
- **The root is not empty.** The identity domain lives there, with admins of its own

Draw the boxes around who operates what, and the policies get easy to write.

NETWORK: WHY HUB AND SPOKE

HOW TO DESIGN A NETWORK THAT CAN GROW



5 networks make 10 links. 10 networks make 45. A mesh has no common point to inspect.

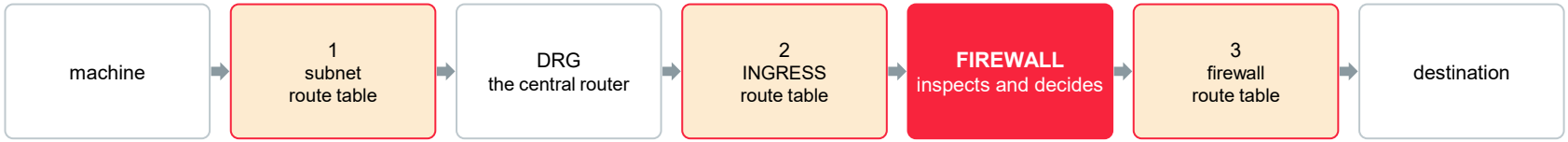
- The **DRG** is the router everything attaches to
- The **hub** is one network among them, but the **firewall** lives there
- **No spoke has an exit of its own**

This shape delivers the requirement, all traffic inspected by the firewalls.

So how do we make traffic reach that firewall?

NETWORK: THE JOURNEY OF A PACKET

A ROUTE TABLE SAYS WHERE TRAFFIC GOES, AND THE DRG IS THE ROUTER.



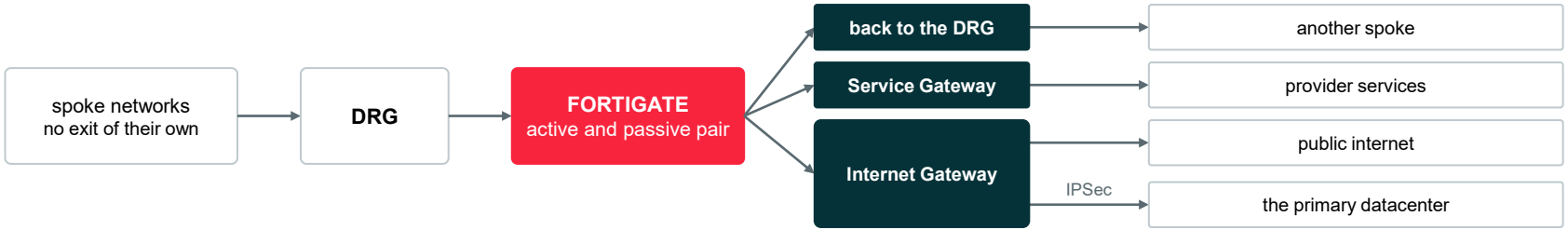
Three tables, one purpose. Making the firewall unavoidable.

1. **On the spoke subnet.** Everything goes to the **DRG**
2. **On the DRG hub attachment.** Everything from the spokes is sent to the **firewall address**
3. **On the firewall inside leg.** The firewall decides if the traffic is allowed, and sends it on

Traffic must cross the firewall both ways, or the firewall drops half a conversation.

NETWORK: FOUR ROADS, ONE FIREWALL

A SPOKE HAS FOUR ROADS, AND EVERY ONE OF THEM CROSSES THE FIREWALL.



- **To another spoke**, back through the DRG
- **To provider services**, out of the **Service Gateway**, never touching internet
- **To internet**, out of the Internet Gateway
- **To the datacenter**, out of that same gateway, inside an **IPSec tunnel**

One road does not go out at all. Inside a VCN traffic never meets the firewall unless you ask.

OBSERVABILITY: EYES ON THE SITE

A SITE THAT SLEEPS STILL HAS TO BE READY THE DAY IT IS NEEDED

What an alarm is for. To tell you that a piece of the site is down, or that everything is still working as it should. Nobody watches a dashboard for six months, so the site has to call you.

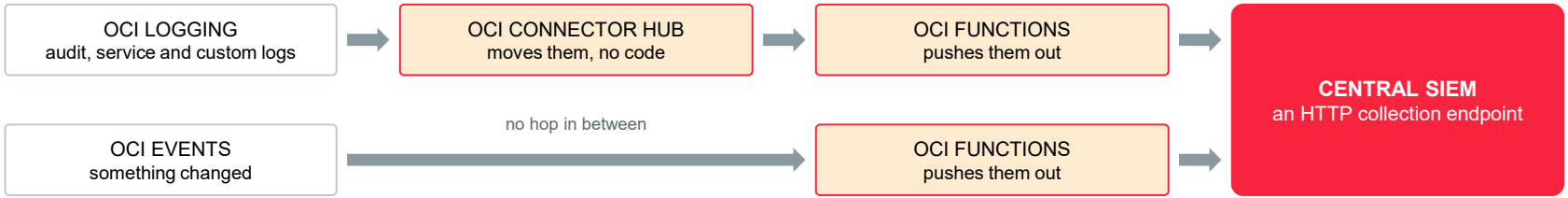
- **Is the link to the datacenter up**, is the replication still arriving
- **Are the domain controllers answering**, because without them nothing restarts
- **Is there room left**, because a restore needs space it does not have to ask for

Every alarm has an owner, the network team, the database team, the same split the compartments already draw, so an alarm nobody owns is an alarm nobody answers.

Metrics and logs are shipped to Datadog, the platform the organization already runs across its clouds, so the recovery site is watched where everything else is watched, and **security events go to the central SIEM**.

OBSERVABILITY: FEEDING THE SIEM

HOW LOGS AND EVENTS TRAVEL, WITH SERVERLESS ARCHITECTURE



Two chains, side by side. The only thing they share is the endpoint.

Two chains, side by side. The SIEM takes no connector of its own, it exposes an **HTTP endpoint**.

- **Logs.** OCI Logging collects them, **OCI Connector Hub** moves them, and a **function** pushes
- **Events.** They call the **function** straight away, with no hop in between
- Both chains end the same way, on **the endpoint the SIEM publishes**

The recovery site reports where security already looks.

IAC: WHY INFRASTRUCTURE AS CODE

WHY IT IS WRITTEN DOWN INSTEAD OF CLICKED

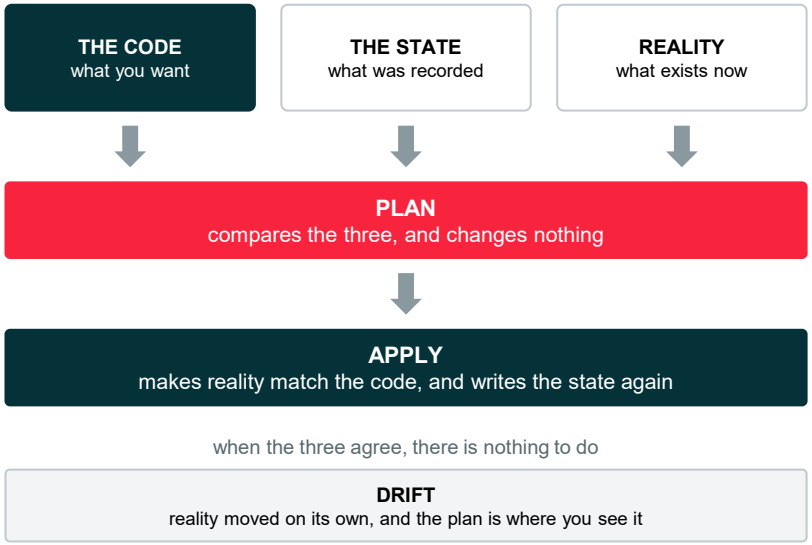
The site is described in code. **This is what that buys.**

What you get	What it means here
Blast radius, the reach of a mistake	A network mistake cannot touch identity
Dependencies	Written down, not living in somebody's head
History	You see how the site got here, and go back
Review	Read and agreed before it happens, not after

Not speed on the bad day. Control on all the ordinary ones.

IAC: CODE, STATE AND REALITY

WHAT A PLAN COMPARES, AND WHAT AN APPLY CHANGES



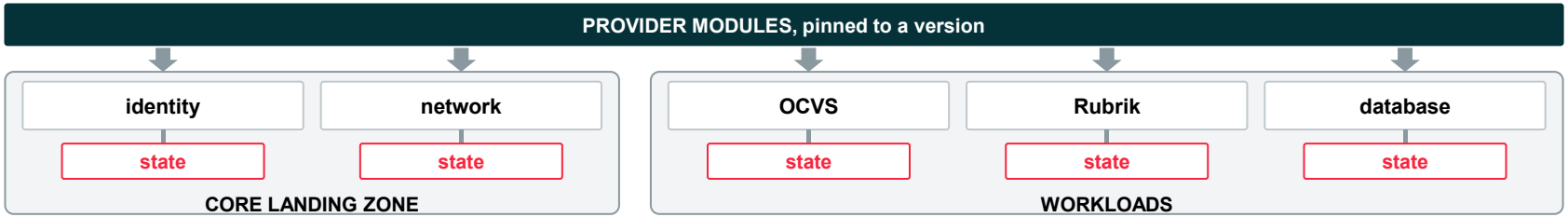
The code says what you want. **The state** is what was recorded last time. **Reality** is what exists right now.

- **Plan** compares the three and shows you the difference, and it changes nothing
- **Apply** makes reality match the code, and writes the state again
- Nobody opens a recovery site for months, so **drift is what you are watching for**

Every layer of this site is described in code, and that is how it stays the way you designed it.

IAC: ONE STACK PER LAYER

HOW THE CODE IS CUT, AND WHY NOT IN ONE BLOCK



the modules are not ours, the stacks and the states are

- **One layer, one stack, one state**, and never a shared one
- Each stack **runs on its own**, because the layers change at different speeds
- The building blocks are the **provider's own modules**, pinned to a version and already built to its security benchmark
- **In one single block** the reach of a mistake is the whole site

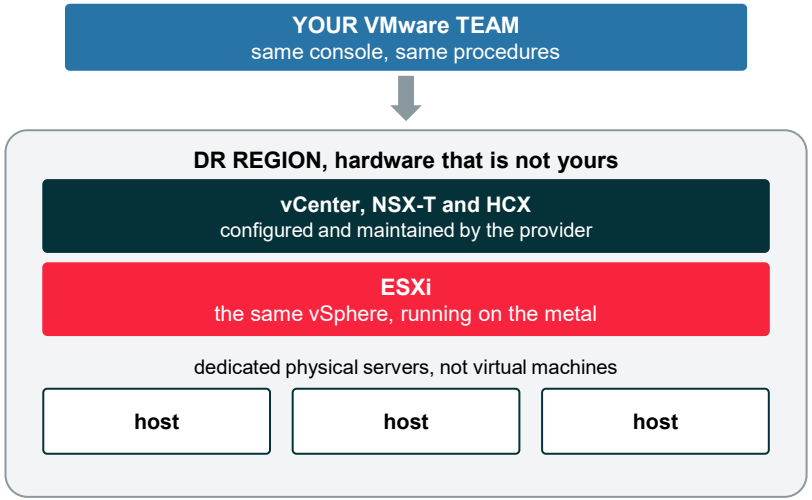
You do not read a site in one file. You read it one layer at a time.

WORKLOADS ON TOP

1. Foundations
2. Recovery strategy
3. The landing zone
4. **Workloads on top**
5. Wrap-up

OCVS, VMWARE ON METAL

THE FIRST WORKLOAD, AND IT SITS IN A SPOKE OF ITS OWN



OCVS runs VMware on **dedicated physical servers**, not on virtual machines.

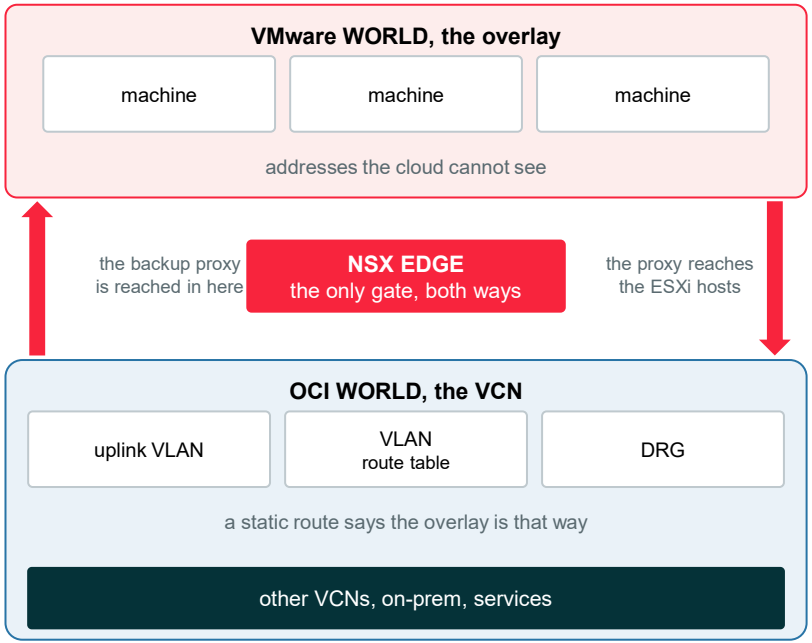
- The provider gives you **vCenter, NSX-T and HCX** already configured, and maintains them
- You stay the **VMware administrator**, with your tools and your procedures

One cluster, three active hosts, sized to restart what matters.

From here on every workload lands in a spoke. This is the first.

OCVS, WHERE THE TWO WORLDS MEET

WHO HAS TO CROSS THAT GATE, AND IN WHICH DIRECTION



The restore crosses that gate in both directions. The cluster reaches **in** to the backup proxy, which lives inside the overlay, and the proxy reaches **out** to the **ESXi hosts**.

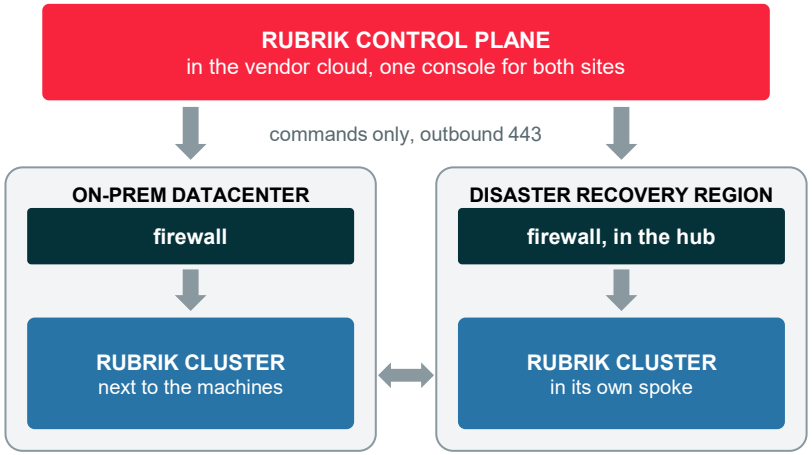
The two things you do by hand

- **Addressing.** The cloud cannot see the VMware segments, so the plan is kept by hand
- **Routing.** A static route says those segments sit behind the **Edge**

HCX stretches a datacenter segment into the cloud, so a machine **keeps its address**.

RUBRIK, THE BACKUP PLATFORM

THE SECOND WORKLOAD, IN A SPOKE OF ITS OWN, TALKING TO THE FIRST



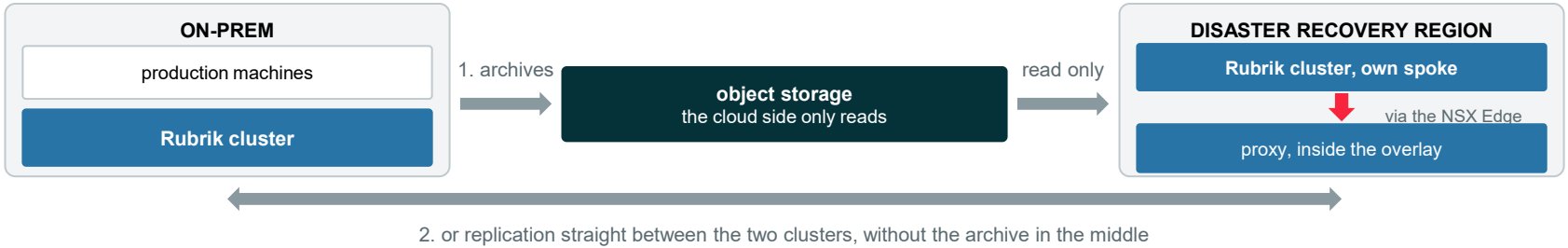
nothing comes in. The clusters call out

- **Rubrik** is the backup platform, and its **control plane is a SaaS**, one console driving both clusters
- **One outbound path per cluster**, north-south, through the firewall
- **Nothing comes in**, and only the orders go through the vendor, never the data
- It reaches **the VMware spoke** to write machines back, and that path crosses the firewall too

A control plane you do not host is one more dependency on the day of the disaster.

RUBRIK, FROM BACKUP TO RESTART

TWO ROADS FOR THE DATA, AND THE SAME RESTORE

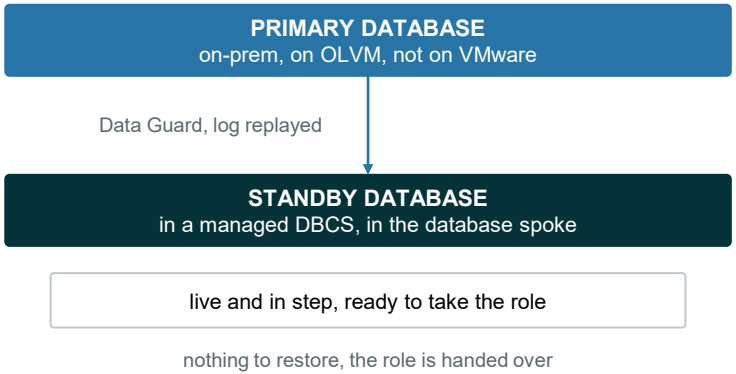


- **Through the archive.** The cloud cluster reads the same object storage **read only** and restores from there. Cheap, and **nothing on this side can change what is already written**
- **Replicating between clusters.** Snapshots pass straight from one to the other, and cost more

The restore is the same in both cases. A proxy living inside the overlay writes the machine back into the **vSphere cluster**. The cluster reaches that proxy by crossing the firewall and the **NSX Edge**, which is why that gate has to open inwards.

DATA GUARD, THE CRITICAL DATABASE

ONE DATABASE DOES NOT GET RESTORED. IT IS ALREADY RUNNING.

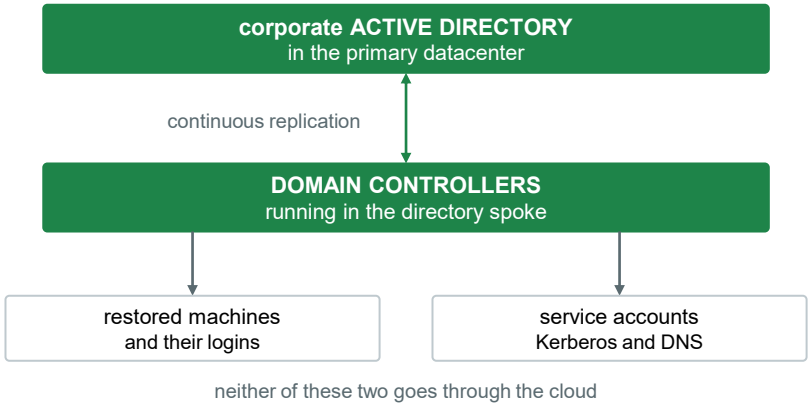


All machines are restored from backup, **except one**, and it comes from **OLVM**.

- A **standby database** is already running on the other side, in a managed **DBCS**
- **Oracle Data Guard** is how it stays in step, shipping the transaction log and replaying it
- The standby is **live**, so nothing is restored. The role is handed over

THE FOREST REACHES THE CLOUD

NOBODY LOGS IN WITHOUT IT



Federation covers the console. **These two levels use Active Directory instead.**

- **The users.** A restored machine authenticates **here**, and a domain login has **no local fallback**
- **The applications.** Service accounts, Kerberos and the **DNS** they resolve with
- **Two of them**, in the **existing forest**, replicating so nothing goes stale

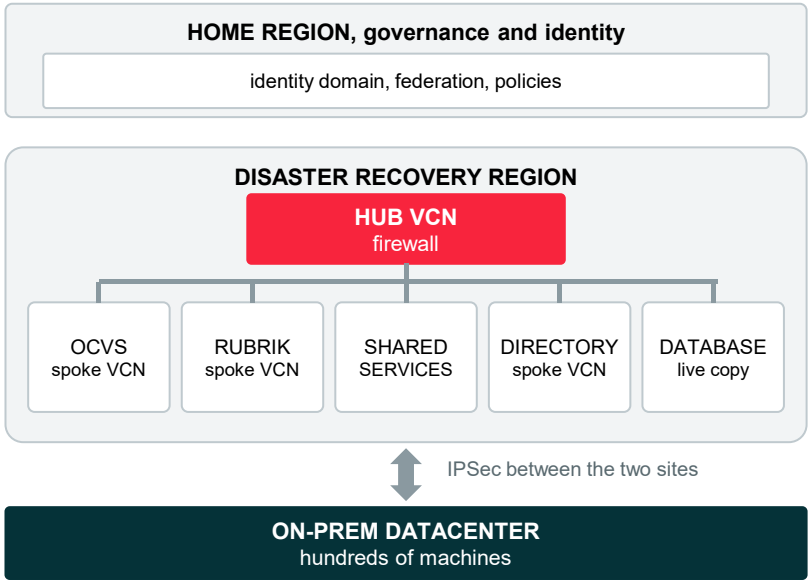
A recovery site that cannot authenticate is a room full of servers you cannot log into.

WRAP-UP

1. Foundations
2. Recovery strategy
3. The landing zone
4. Workloads on top
5. **Wrap-up**

THE BIG PICTURE

EVERYTHING IN THIS TALK, IN ONE DRAWING

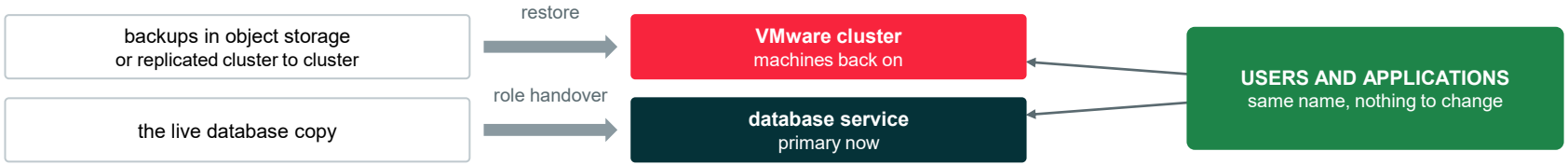


- **Hub**, the firewall, and all traffic crosses it
- **OCVS spoke**, the machines coming back
- **Rubrik spoke**, the cluster that writes them back
- **Directory and database spokes**, the logins and the live copy
- **Home region**, identity and policies

The platform is one spoke among the others, not the landing zone.

THE DAY IT IS NEEDED

WHAT HAPPENS, AND WHAT THE PEOPLE WHO USE IT SEE



two mechanisms, and the people reach what comes back

- **The machines.** Rubrik writes them back into the VMware cluster, and vCenter powers them on
- **The database.** Nothing is restored. The live copy takes the primary role
- **Before either**, the domain controllers have to be up, or nobody can use them
- **And their people.** A machine comes back with **the same address** and the same name, and database clients ask for a **service name** that lives only where the primary is

This is the answer to the question we opened with.

WHAT TO TAKE HOME

FIVE THINGS WORTH REMEMBERING

1. **Disaster recovery is built from the foundations.** Failover is the last 5 per cent
2. **Federation covers the console, and nothing else.** Everything that has to restart authenticates against a directory, and that directory lives in the datacenter you just lost
3. **The order matters.** Who can do what, who gets in, where the traffic goes, workloads last
4. **Hub and spoke is the recommended answer** in a context where all traffic has to be governed and inspected by the firewalls
5. **What the inspection does not cover is a decision.** Inside one network nothing is inspected unless you ask for it, so where you put a system is a security question

Oronzo Antonelli, Senior Consultant - Cloud Architect, o.antonelli@reply.it