SUMMIT

Proxmox VE Disaster Recovery, powered by Veeam

A SECOND PLACE TO RUN YOUR KVM WORKLOADS.

Challenge

Proxmox cluster high availability restarts a virtual machine on another node when a host fails. It does nothing when the building loses power, when the shared storage array fails, or when ransomware reaches the cluster and the backups stored inside it. Backups answer a different question — can we get the data back — and the answer is measured in hours, into infrastructure the business must already have somewhere else.

Organizations that moved to Proxmox VE from VMware often had replication-based disaster recovery on vSphere and arrived on Proxmox without it. Proxmox's own storage replication works between nodes of one cluster on ZFS; Proxmox Backup Server syncs backup copies, not running replicas. Neither gives the business a tested, second place to run.

Summit's Proxmox VE Disaster Recovery as a Service replicates Proxmox VE virtual machines to a Summit-hosted Proxmox VE recovery cluster using the native Proxmox VE replication in Veeam Backup & Replication 13.1, and provides Summit-run failover, failback, and scheduled DR testing against a customer-approved runbook.

How We Do It

NATIVE PROXMOX VE REPLICATION

Veeam helper appliances on the customer's Proxmox VE hosts and on the Summit recovery cluster move changed blocks over a private interconnect, using QEMU dirty-bitmap change tracking. Replicas are kept in native Proxmox VE format as powered-off virtual machines, each with a configurable number of restore points stored as Proxmox VE snapshots.

FAILOVER IN SECONDS, FROM THE POINT YOU CHOOSE

Because restore points are native snapshots, a replica powers on as a fully functional VM within seconds of Summit initiating failover — from the latest point, or from one that pre-dates a corruption or ransomware event. Multiple VMs are failed over in a single operation, in the order the runbook defines.

FULLY MANAGED OPERATIONS

Summit provisions the recovery tenant, configures and monitors replication, maintains the DR runbook with the customer, executes failover and failback on declaration, and runs scheduled DR tests with a delivered report. Your team declares; ours recovers.

Deployment Models

Both models deliver the same underlying service. The difference is where the production Proxmox VE environment lives and therefore how the replication interconnect is provided.

PROXMOX VE AT SUMMIT

The customer's production Proxmox VE hosts run in a Summit data center and replicate to a Summit recovery cluster in a second Summit location over Summit's backbone. Shortest path to a tested cross-site posture.

PROXMOX VE AT THE CUSTOMER SITE

Production stays on-premises or in third-party colocation. Summit deploys workers into that environment and replicates across a private interconnect or site-to-site VPN to the Summit recovery cluster.

Key capabilities

PROXMOX VE TO PROXMOX VE REPLICATION

Replication of Proxmox VE 8.2 through 9.2 QEMU/KVM virtual machines to a Summit-hosted Proxmox VE recovery cluster in Veeam Backup & Replication 13.1. Host-to-host, cross-data-center, and cross-storage-type replication are supported.

30 MINUTE-SCALE RECOVERY POINTS

Replication runs on a periodic schedule set in hours or minutes, with an optional replication window to protect production hours. The achievable recovery point is set per customer from change rate and interconnect bandwidth.

SNAPSHOT-BASED RESTORE POINTS

Each replication session adds a replica restore point as a native Proxmox VE snapshot. Failover can select any retained point, which is how recovery to a pre-ransomware state works.

SUMMIT-RUN FAILOVER AND FAILBACK

Failover, undo failover, permanent failover, failback to the original VM or to a VM restored in a different location, and commit or undo failback, executed by Summit from the Veeam console per the customer-approved runbook.

NETWORK REMAPPING

Source networks are mapped to recovery-cluster networks and VLANs so failed-over replicas attach to the right customer networks. Addressing is handled by the DR network design agreed at onboarding.

SCHEDULED DR TESTING

Test failovers run in an isolated recovery network, applications are validated by the customer, undo failover returns everything to its pre-test state, and a test report is delivered as audit and cyber-insurance evidence.

PER-CUSTOMER ISOLATION

Each customer receives a dedicated tenant on the recovery cluster — dedicated storage, mapped networks, reserved compute, and a dedicated Summit worker — so replicas are never visible to other tenants.

RECOVERY FROM BACKUPS FOR EVERYTHING ELSE

Bundled with Proxmox VE Backup as a Service, VMs outside the replication scope recover from Summit backups: entire VM restore into Proxmox VE, Instant Recovery to VMware vSphere, Hyper-V, or Nutanix AHV, or restore to Microsoft Azure, AWS, or Google Cloud. Instant Recovery back into Proxmox VE carries experimental support status from Veeam.

ONE ESTATE WITH BACKUP

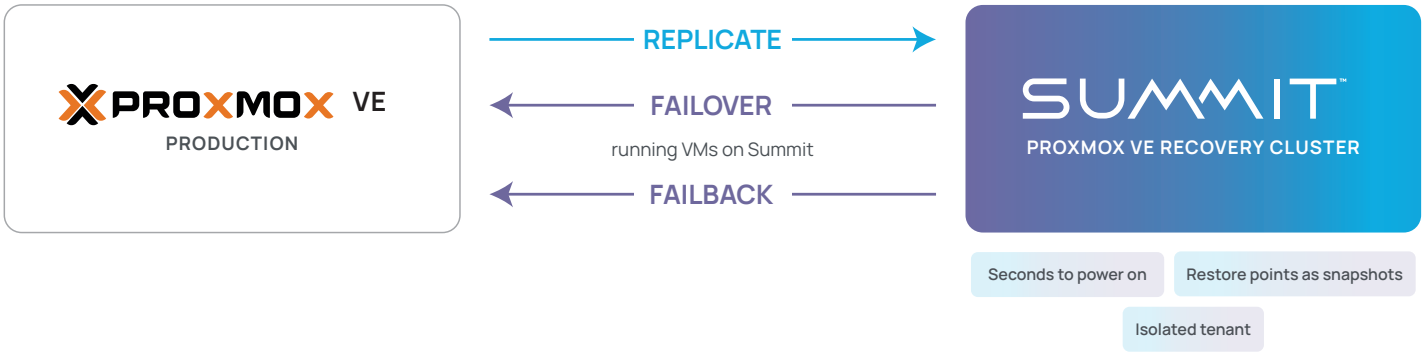
Shares the Veeam backup server, Proxmox VE workers, and Veeam Universal License pool with Proxmox VE Backup as a Service. A VM that is both backed up and replicated consumes one license instance; recovery-cluster hosts need no license.

MONITORING AND REPORTING

Continuous monitoring of replication jobs, workers, and recovery-point age against the contracted target, with alerting on recovery-point breaches; scheduled reports on replication success, current recovery point per VM, and replica storage; a report after every DR test.

Your Business Data

DISASTER RECOVERY AND BUSINESS CONTINUITY SOLUTIONS



WHAT GETS REPLICATED:

- Virtual machine disks and configuration
- Windows and Linux guests
- SQL Server, Oracle, and PostgreSQL workloads
- Line-of-business and domain services
- Multiple restore points per VM

Benefits

A TESTED SECOND PLACE TO RUN, WITHOUT A SECOND DATA CENTER

RECOVER THE BUSINESS, NOT ONLY THE DATA	Replicas power on in seconds on the Summit recovery cluster. Recovery points are minutes to hours old, not last night's backup, and any retained point can be chosen.
PROTECTION PROXMOX HA CANNOT GIVE YOU	Site loss, storage failure, and ransomware inside the cluster all leave Proxmox HA with nothing to fail over to. Replicas live in a separate Summit location, isolated per customer.
DR YOU CAN PROVE	A maintained runbook, scheduled test failovers, and a delivered report after each test satisfy auditors, regulators, and cyber-insurance carriers — without disrupting production.
REMOVE THE OPERATIONAL BURDEN	No second site to lease, no recovery cluster to run, no Veeam or Proxmox DR expertise to hire. Summit operates the replication, the recovery cluster, the testing, and the failover.

Service Details

PROTECTED WORKLOADS:

Proxmox VE 8.2 through 9.2 virtual machines (QEMU/KVM) on x86-64 hosts installed from the official Proxmox ISO, standalone or clustered, replicated to a Summit-hosted Proxmox VE recovery cluster.

DEPLOYMENT MODELS:

Production Proxmox VE hosted at Summit, or at the customer site with Summit-deployed workers. Same underlying service in both.

NOT IN SCOPE:

LXC containers, VM templates, linked clones, VMs sharing a BIOS UUID, iSCSI-attached and passthrough disks, VMs on BTRFS or custom storage, and Proxmox VE permissions, users, API tokens, and HA group membership. Cross-hypervisor replication is not available: replicas run only on Proxmox VE; recovery to VMware, Hyper-V, Nutanix AHV, or public cloud is from backups. These are limitations of Veeam Backup & Replication and are read to the customer at scoping.

Service Details

RECOVERY TIME:
Replica power-on within seconds of failover initiation. End-to-end recovery time for the protected VM set includes declaration, runbook execution for recovery order, and network and DNS steps.

FAILOVER OPERATIONS:
Failover (per restore point, multiple VMs per operation), undo failover, permanent failover, failback to the original VM or to a VM restored in a different location, commit or undo failback. Automated failover plans, planned failover, re-IP rules, replica seeding, and replication from backup are not available for Proxmox VE; recovery ordering and address changes are handled by the Summit runbook and network design.

CONNECTIVITY:
Routed connectivity (IPv4, no NAT) between the customer's Proxmox VE hosts and workers, Summit's Veeam backup server, and the recovery cluster, over a private interconnect or site-to-site VPN. Sized for change rate, recovery point, and the initial full replication.

REPORTING:
Continuous replication and recovery-point monitoring by Summit operations; scheduled replication and capacity reports; a report after each DR test; semi-annual review of scope, reserved capacity, restore points, and intervals.

LICENSING:
Per protected virtual machine through Veeam Universal License instances, shared with Proxmox VE Backup as a Service for VMs in both; recovery-cluster hosts are unlicensed. Plus reserved recovery compute and storage, and DR test or declared-failover runtime beyond the tier's allowance.

COMPLIANCE:
SOC 2 Type II across Summit data centers and processes. DR test reports available as business-continuity audit evidence. HIPAA BAA available on request.

REPLICATION INTERVAL AND RECOVERY POINT:
Periodic, set in hours or minutes per customer from change rate and interconnect bandwidth, with an optional replication window. Veeam publishes no minimum interval; the recovery point is contracted per tier once service tiers are defined.

RESTORE POINTS:
Configurable number of replica restore points per VM, retained as Proxmox VE snapshots on the recovery cluster.

DR TESTING:
Scheduled test failovers in an isolated recovery network with customer application validation, undo failover, and a delivered test report. Cadence per service tier (pending definition), plus a validated test at go-live.

ENCRYPTION:
Encrypted in transit across the interconnect; replica storage on Summit infrastructure.

ONBOARDING:
Approximately three to four business weeks from order to a validated DR test, including interconnect and recovery-network provisioning, recovery tenant provisioning, worker deployment, replication configuration, initial replication, test failover, and runbook sign-off. The customer provides a root-equivalent account on each Proxmox VE node (password-based SSH, by requirement), file-level snapshot-capable storage for workers, network paths, the QEMU Guest Agent in guests, a designated disaster-declaration authority, and runbook approval.

SUPPORT MODEL:
24x7x365 incident response through the Summit NOC; declared disasters are handled as critical incidents around the clock through the emergency contact path in the runbook. Change requests, scope adjustments, and non-urgent configuration changes are handled during business hours.

Related Summit Services

PROXMOX VE BACKUP AS A SERVICE	SUMMIT NETWORK SERVICES	MANAGED BACKUP AND DRAAS
Application-aware, image-level backup of Proxmox VE virtual machines to immutable Summit repositories, on the same Veeam platform and license pool. The recommended companion: replicas do not replace long-term, immutable retention.	Private interconnect, site-to-site VPN, and recovery-site network design — VLANs, routing, firewall policy, and the addressing or DNS approach used at failover.	Extend a single data protection and recovery strategy across Proxmox VE, VMware, Hyper-V, physical, and SaaS workloads.