

Veeam backup and recovery

Canonical: <https://agentic.blueapache.com/technical-excellence/veeam/veeam-solutions-with-blueapache/>

Description:

We bring Veeam technology together with our cloud, infrastructure and identity expertise to help you design and implement backup and recovery.

Details:

We use Veeam technology within our backup and recovery capability, including emPOWER Backup for Microsoft Entra ID. We bring cloud, infrastructure and identity expertise to the design, helping you connect the backup platform with the systems your business needs to recover.

Our work starts with recovery requirements. We help you identify the workloads, data and identities that matter, understand their dependencies and decide how the selected solution should be implemented and operated. You can engage us for a defined technology project or discuss protection within a managed or co-managed environment.

Build the design around business recovery

A useful backup design answers more than how much data is stored. We work through what your team would need to restore after accidental deletion, a failed change or a security incident, and the order in which services need to return.

For a business application, that may mean looking at infrastructure, application data, access and connectivity together. For an identity requirement, it means understanding which objects and configurations are needed to restore access. We use those dependencies to shape the proposed coverage and recovery process.

The Veeam product and configuration are selected for the workload. We discuss the relevant protection capability, storage requirements, access controls and operating model rather than assuming that a single product licence covers every part of your environment.

Protect identity with emPOWER Backup for Microsoft Entra ID

Our emPOWER Backup for Microsoft Entra ID offering uses Veeam technology to support protection and recovery of your identity environment. Identity is a distinct part of resilience: access to applications can be disrupted even when the application's files and infrastructure remain available.

We help you assess the identity-recovery requirement alongside your Microsoft environment and wider backup arrangements. The design discussion addresses the objects and configurations to protect, administrator responsibilities, the recovery workflow and how restored identity information will be validated.

This sits alongside our broader cloud and security capability. We connect the identity discussion with the people who own your Microsoft services, business applications and incident response so the recovery plan reflects how your environment actually operates.

Plan implementation and validation

We work with your team to define the implementation scope around practical decisions:

- The workloads, tenants and identity components included in protection.
- Recovery priorities and the data-loss tolerance for each business requirement.
- Backup storage, retention and access arrangements.
- Who monitors backup jobs and investigates exceptions.
- How recovery requests are authorised and tested.
- The handover and support responsibilities after deployment.

We discuss recovery point objectives, which describe the acceptable loss of recent data, separately from recovery time objectives, which describe how quickly a service needs to return. The achievable design depends on the workload, configuration and recovery process. We agree the requirements and validation approach for your environment.

Choose the right engagement

With TECHNOLOGY, we can support selection and implementation while your team operates the platform. With CONTROL, we can discuss sharing defined operational responsibilities with your internal team. With OUTCOME, we can discuss backup and recovery within the agreed managed-service scope.

The practical difference is who owns the ongoing work. We make monitoring, remediation, restore approval and recovery testing part of that conversation, so responsibility is clear after the project finishes.

Questions about Veeam and recovery

Can we engage you for implementation without a full managed service?

Yes. Our technology services support defined implementation requirements. We can work with your infrastructure or cloud team and agree the handover needed for them to retain operation.

Does an identity backup replace application or document backup?

No. Identity protection addresses a different recovery requirement. We review your identity, application and data dependencies together so the selected protection covers the business scenario you need to recover from.

How do we know the design will support our recovery process?

We agree representative recovery tests and the people needed to validate them. That gives your team a practical basis for reviewing recovery readiness, alongside backup-job monitoring.

Talk with our team about backup and recovery

Related expertise

- Keepit SaaS backup and recovery
- Microsoft cloud, workplace and security