6 Datensicherung & Notfall

- Backup & Wiederherstellung
  - Backup- & Restore-Plan
  - Rollen & Verantwortlichkeiten
  - Veeam B&R 12 – Backup-Jobs (Hyper-V TerraXaler i3)
  - Veeam – Wiederherstellungsleitfaden (VM/Files/AD)
  - Immutable Repository & Offsite Kontrolle
  - Proxmox Backup Server – Richtlinien & Wiederherstellung
  - Restore-Testprotokoll – Vorlage
  - Wiederanlaufplan (Disaster Recovery Runbook)
  - Backup Monitoring & Alarmierung
  - Änderungsprotokoll & Nachweise

Backup & Wiederherstellung

Backup- & Restore-Plan

Backup- & Restore-Plan

Übersicht

Ziel: Geschäftskontinuität durch definierte RPO/RTO je System sowie geprüfte Wiederherstellungsverfahren.
Umfang: Hyper-V-VMs (TerraXaler i3, 2 Nodes) über *Veeam Backup & Replication 12*, Linux-Dienste auf *Proxmox* über *Proxmox Backup Server (PBS)*.
Immutable/Offsite: Veeam-Backup-Repository ist *immutable*. Offsite-Kopien (Copy-Jobs) gemäß Plan unten.

RPO/RTO-Matrix

System/Service	RPO	RTO	Verfahren	Testintervall	Letzter Test/Nachweis
Fileserver (VM)	4h	8h	Veeam VM-Backup (App-aware)	Quartal	{{Datum/Link}}
Active Directory (VM)	4h	8h	Veeam VM-Backup + AD-Autoritativ-Restore-Plan	Halbjahr	{{Datum/Link}}
GLPI (Proxmox, Debian)	6h	8h	PBS VM/Container-Backup + DB-Dump	Quartal	{{Datum/Link}}
BookStack (Proxmox)	6h	8h	PBS + App-Dumps	Quartal	{{Datum/Link}}
3CX (Proxmox)	6h	4h	PBS + 3CX-Config-Backup	Quartal	{{Datum/Link}}

Hinweis: RPO/RTO jährlich im Änderungsfenster Q1 prüfen und vom IT-Leiter freigeben.

Backup-Strategie

- **Hyper-V / Veeam B&R 12**
  - Primärjobs: tägliche inkrementelle Sicherung, wöchentliche synthetische Vollsicherung.
  - Retention: 30 Restore Points (GFS: Monatlich 12, jährlich 7).
  - **Immutable Repo:** Hardened Linux Repo, Immutability {{14–30}} Tage; SSH hartening; kein Root-Login.
  - Copy-Jobs: Offsite/zweites Repo {{Standort/Bucket}} (Bandbreite/Window beachten).
- **Proxmox / PBS**
  - Zeitpläne: täglich inkrementell, wöchentlich Voll.
  - Retention: `keep-last: 30`, `keep-monthly: 12`, `keep-yearly: 7`.
  - Verifikation: `prune` + `verify` wöchentlich, `gc` monatlich.

Restore-Tests (Regelwerk)

- **Ziel:** Pro Quartal je Plattform mindestens 1 repräsentativer Restore (Hyper-V VM + Proxmox VM/CT).
- **Abnahmekriterien:** Boot/Services ok, Anwendungsprüfung, Prüfer*in zeichnet Protokoll ab.
- **Nachweise:** Testprotokolle, Screenshots, Veeam/PBS-Job-Reports in {{Ablage/Link}}.

Kontakte & Eskalation

- **Rollen:** Siehe Seite „Rollen & Verantwortlichkeiten“.
- **Eskalation:** P1 (Ausfall produktiv): sofort CIO/IT-Leitung, Anbieter-Support (Veeam/PBS).

Änderungs- & Review-Zyklen

- Plan-Review: halbjährlich.
- Technische Tests: siehe „Restore-Testprotokoll – Vorlage“.
- Monitoring/Alarmierung: siehe „Backup Monitoring & Alarmierung“.

Rollen & Verantwortlichkeiten

Rollen & Verantwortlichkeiten

Rolle	Person/Gruppe	Aufgaben	Stellvertretung
Backup Owner	{{Name/Gruppe}}	Strategie, Compliance, Freigaben	{{Name}}
Backup Operator (Veeam)	{{Name}}	Job-Pflege, Restores, Tests	{{Name}}
PBS Operator	{{Name}}	Schedules/Retention, Verify, Restores	{{Name}}
Security	{{Name}}	Immutable-Kontrolle, Offsite-Checks	{{Name}}
Service Owner (Systeme)	{{Name}}	Abnahmetests, Fachprüfung	{{Name}}

Vier-Augen-Prinzip: Änderungen an Retention/Immutability nur mit Gegenzeichnung Security.

Veeam B&R 12 – Backup-Jobs (Hyper-V TerraXaler i3)

Veeam B&R 12 – Backup-Jobs (Hyper-V TerraXaler i3)

Ziel

Definierte Jobs für alle produktiven VMs auf dem TerraXaler i3 Hyper-V-Cluster (2 Nodes).

Standardprofil

- **Mode:** Forward Incremental, wöchentliche synthetische Full.
- **App-Aware:** aktiv (AD, Fileserver, SQL/Apps).
- **Storage:** {{Repo-Name (Immutable)}}, Blockgröße Auto, Compression Optimal.
- **Transport:** Hot-Add / NBD je nach Pfad.
- **Retry/Window:** 3 Retries, Backup window {{22:00–06:00}}.

Schritt-für-Schritt (Neuer Job)

1. **Veeam Console → Home → Backup Jobs → Virtual machine → Microsoft Hyper-V.**
2. **Name & Description:** `PRD_HV_Daily_{{Bereich}}`.
3. **Objects:** Cluster/VMs auswählen; **Exclusions:** Test/Dev ausnehmen.
4. **Storage:** Zielrepo *ImmutableRepo01*; Retention `30` Restore Points; **GFS**: Monatlich `12`, jährlich `7`.
5. **Guest Processing:** App-Aware **ON**, Credentials {{…}}, Truncate Logs falls DB.

6. **Schedule:** täglich 22:00; **Retry** 3× alle 10 Min; **If failed, retry** aktiv.
7. **Save → Run Now (erstmaliger Full)** innerhalb des Wartungsfensters.

Copy-Job (Offsite)

- **Homescreen → Backup Copy → Immediate copy.**
- **Source:** o.g. Primärjobs
- **Target:** {{OffsiteRepo/Bucket}}, Encryption ON, WAN-Accel optional.
- **Immutability Offsite:** {{n}} Tage (wenn unterstützt).

Pflege

- Monatlich Job-Review (fehlende VMs? Wachstum?).
- Quartalsweise SureBackup/Instant-VM-Test (wenn verfügbar).

Veeam – Wiederherstellungsleitfaden (VM/Files/AD)

Veeam – Wiederherstellungsleitfaden

A) Vollständige VM (Instant VM + Final Restore)

1. **Home → Backups → Disk → Rechtsklick VM → Instant Recovery to Hyper-V.**
2. Ziel-Host/Cluster wählen, Netzwerk trennen (Test) oder produktiv zuordnen (Notfall).
3. Starten, **Smoke-Tests**: Ping, Dienste, Anwendungs-Login.
4. **Migrate to production** (Storage vMotion-ähnlich) sobald Performance ok.
5. **Dokumentation:** Testprotokoll ausfüllen, Screenshots beifügen.

B) Datei-/Objekt-Restore (Windows/Linux)

1. **Home → Backups → Disk → Rechtsklick → Restore guest files.**
2. Browser öffnen, Zielpfad wählen, Wiederherstellung durchführen.
3. **Nachkontrolle:** NTFS/ACLs, Virenscan auf wiederhergestellten Daten.

C) Active Directory (nicht-authoritativ / autoritativ)

- Nicht-authoritativ: System State Restore, anschließend Replikationsabgleich.
- Autoritativ (z. B. OU gelöscht): AD-Restore im Directory Services Restore Mode (DSRM), `ntdsutil` mark authoritative; **nur nach Freigabe Security**.
- Siehe **Checkliste AD-Restore**:
  - DSRM-Kennwort geprüft?
  - FSMO-Rollen/Partner erreichbar?
  - Zeitquelle/NTP intakt?

Wiederanlauf-Kriterien

- Service Owner bestätigt Funktionsfähigkeit.
- Monitoring keine kritischen Alarme > 30 Min.

Immutable Repository & Offsite Kontrolle

Immutable Repository & Offsite Kontrolle

Tägliche/Wöchentliche Checks

- **Veeam Alarme**: Job-Fehler, Repository-Free-Space > {{20%}}.
- **Immutability Window**: `{{14–30}} Tage` → Änderungen nur via Vier-Augen-Prinzip.
- **SSH/Härtung**: Passwortloser Root-Login AUS; Updates monatlich; Audit-Logs sichern.
- **Offsite Copy**: Letzte erfolgreiche Kopie < {{24h}}.

Monatscheck (Vorlage)

Datum	Prüfer	Immutability-Tage	Repo-Free-Space	Offsite-Status	Bemerkung
{{YYYY-MM-DD}}	{{Name}}	{{n}}	{{%}}	{{OK/NOK}}	{{…}}

Nachweisablage: {{Pfad/Link}}.

Proxmox Backup Server – Richtlinien & Wiederherstellung

Proxmox Backup Server – Richtlinien & Wiederherstellung

Schedules & Retention (Standard)

- **Zeitpläne:** täglich 23:00 inkrementell, Sonntag Vollbackup.
- **Retention:** `keep-last: 30`, `keep-monthly: 12`, `keep-yearly: 7`.
- **Verify:** Wöchentlich `verify` Jobs; `prune` wöchentlich; `gc` monatlich.

Restore (VM/CT)

1. **Proxmox GUI → Knoten/VM → Backup** → Snapshot auswählen → *Restore*.
2. **Target Storage/Node** wählen (ggf. anderer Node für Tests).
3. Starten, **Apptests** (GLPI/BookStack/3CX):
   - GLPI: Web-Login, DB-Abfragen.
   - BookStack: Seitenaufruf, Upload-Test.
   - 3CX: eingehender/ausgehender Testcall.
4. **Dokumentation:** Restore-Testprotokoll ausfüllen.

Datenbank-Sicherungen (Empfehlung)

- GLPI/MySQL: täglicher Dump via `mysqldump` + PBS.
- BookStack (MariaDB/Postgres + Uploads): Dumps + Files.
- 3CX: integrierte Config-Backups zusätzlich zum PBS.

Restore-Testprotokoll – Vorlage

Restore-Testprotokoll

Datum	System	Backup-Quelle (Job/Repo)	Umfang (Full/Teilstück)	Methode (Instant/Full/PBS)	Prüfumfang (Smoke/App)	Ergebnis (OK/NOK)	Prüfer	Maßnahmen/Follow-ups

Prüfschritte (ankreuzen)

- ☐ Restore gestartet, Log gesichert
- ☐ Boot/Service OK
- ☐ Applikation OK (Fachtest)
- ☐ Sicherheit geprüft (z. B. AV-Scan)
- ☐ Abschaltung/Entfernung der Test-VM
- ☐ Protokoll abgelegt unter {{Pfad}}

Wiederanlaufplan (Disaster Recovery Runbook)

Wiederanlaufplan (DR Runbook)

Auslöser & Entscheidung

- P1-Incident, Produktionsstillstand > 30 Min → DR-Leitung übernimmt.
- Kriterien: Ausmaß, erwartete Dauer, Datenintegrität.

Reihenfolge Wiederanlauf (Beispiel)

1. **Core-Infra:** AD/DNS/NTP
2. **Storage/Fileserver**
3. **Kommunikation:** 3CX
4. **Fachanwendungen:** GLPI, BookStack
5. **Sonstiges**

Entscheidungslog

Zeitpunkt	Entscheidung	Begründung	Verantwortlich

Kommunikationsmatrix

Stakeholder	Kanal	Frequenz	Nachrichtenvorlage
Management	{{Telefon/Teams}}	60 Min	{{...}}
Belegschaft	{{E-Mail/Intranet}}	120 Min	{{...}}
Kunden	{{E-Mail}}	Ad-hoc	{{...}}

Backup Monitoring & Alarmierung

Backup Monitoring & Alarmierung

Veeam

- **Benachrichtigungen:** SMTP/Teams-Webhook für Job-Status (Success/Warning/Failed).
- **Reports:** Daily Summary 07:00; Weekly Trend Montag 08:00.
- **Schwellenwerte:** Repo-Füllstand > 80 % → P2; > 90 % → P1.

PBS

- **E-Mails:** Job-Result, Verify/Prune/GC-Ergebnis.
- **Checks:** Letztes erfolgreiches Backup je VM/CT < 24 h.

Ticketing

- **GLPI Vorlage:** „Backup-Fehler“ → Pflichtfelder: System, Job, Zeit, Log-Link, erste Einschätzung.

Änderungsprotokoll & Nachweise

Änderungsprotokoll & Nachweise

Datum	Änderung	System	Betroffene Jobs/Retention	Beantragt von	Genehmigt von	Nachweis/Link
{{YYYY-MM-DD}}	{{z. B. Retention von 14→30 Tagen}}	{{Repo/VM}}	{{Job-Name}}	{{Name}}	{{Name}}	{{Ticket/Link}}