

VMware Migration Assessment Checklist

25 Prüfpunkte zur Bewertung eines VMware-Ausstiegs —
von Inventarisierung und Abhängigkeiten über
Souveränität und GPU-Workloads bis zur
Kostenentwicklung.

So nutzen Sie diese Checkliste

Diese Checkliste mit 25 Prüfpunkten gibt Infrastrukturverantwortlichen, Plattform-Engineers und CIO-Bereichen eine strukturierte Methode, um die Bereitschaft für einen VMware-Ausstieg zu bewerten. Es ist dasselbe Ausgangsframework, das Aenix im Rahmen des **Platform Readiness Assessment** verwendet — einer 14-tägigen Zusammenarbeit, die die Checkliste in einen maßgeschneiderten Migrationsplan überführt.

Nutzen Sie sie auf drei Arten:

1. **Selbstbewertung** — gehen Sie die Punkte mit Ihrem Plattform-Team in einem Workshop durch. Jedes nicht abgehackte Feld wird zu einem Klärungspunkt.
2. **Ausschreibungs-Scoping** — teilen Sie die Liste mit Anbietern, damit alle auf derselben Grundlage antworten.
3. **Vorstandsreife** — die Abschnittszusammenfassungen lassen sich direkt in ein entscheidungsreifes Migrations-Briefing überführen.

Jeder Prüfpunkt entspricht einer strukturellen Entscheidung in Ihrer Zielarchitektur. Eine „unbekannt“-Antwort ist wertvoller als eine Vermutung — sie zeigt den Arbeitsstrang auf, der zuerst bewertet werden muss.

Übersichtskarte

Abschnitt	Prüfpunkte
1. Inventarisierung	4
2. Abhängigkeiten	4
3. Netzwerk- und Speicher-Redesign	4
4. Mandantenfähigkeit	2
5. KI- / GPU-Workloads	3
6. Souveränität & Compliance	3
7. Betriebliche Bereitschaft	3
8. Kostenentwicklung	2

Abschnitt 1 Inventarisierung

- ☐ **Workload-Anzahl nach Kritikalitätsstufe** — Gesamtzahl der VMs, aufgeschlüsselt nach Kritikalität (geschäftskritisch / wichtig / unkritisch). Uptime-SLO je Stufe angeben.
- ☐ **Betriebssystem- und Kernel-Mix** — Verteilung der Gast-Betriebssystem- und Kernel-Versionen sowie End-of-Life-Status. Kernel, die älter als 5 Jahre sind, identifizieren.
- ☐ **Ressourcenprofil je Workload** — vCPU, RAM, angebundener Speicher, Netzwerkbandbreite (Spitze/Durchschnitt) je VM. Über- und unterdimensionierte Systeme kennzeichnen.

- ☐ **Verantwortlichkeit auf Anwendungsebene** — Benanntes Verantwortungsteam je Workload, Datum der letzten Änderung, Deployment-Kadenz (manuell / skriptbasiert / GitOps).

Tipp. Workloads ohne benannten Verantwortlichen treiben die Migrationskosten in die Höhe. Klären Sie die Verantwortlichkeit, bevor Sie den Aufwand schätzen.

Abschnitt 2 Abhängigkeiten

- ☐ **vSAN-Abhängigkeiten erfasst** — Workloads, die auf vSAN-spezifische Funktionen angewiesen sind (Snapshots auf Datastore-Ebene, Deduplizierung, RAID auf Speicherebene). Ersatzstrategie je Workload auflisten.
- ☐ **NSX-Konfigurationen exportiert** — Regeln der Distributed Firewall, Mikrosegmentierungs-Richtlinien, Edge-Gateway-Konfigurationen. Hinweis: vieles lässt sich nicht 1:1 übertragen.
- ☐ **vCloud-Director-Mandantenmodell (vCD) dokumentiert** — Organization-VDCs, Katalogstruktur, Rollenzuweisungen, vApp-Vorlagen. Auf das Ziel-Mandantenmodell abbilden (z. B. Cozystack Tenant CRD).
- ☐ **Individuelle Integrationen katalogisiert** — vRealize Automation/Operations, Drittanbieter-Backup (Veeam, Rubrik), Monitoring-Agents, Lizenzserver. Hersteller-Support für die Zielpattform auflisten.

Achtung. Die Semantik der NSX Distributed Firewall lässt sich selten 1:1 auf Kubernetes NetworkPolicy oder Cilium abbilden. Planen Sie ein **Redesign** der Netzwerksicherheitsrichtlinien ein, kein Lift-and-Shift.

Abschnitt 3 Netzwerk- und Speicher-Redesign

- ☐ **Netzwerktopologie dokumentiert** — VLANs, IP-Plan, MTU, ggf. BGP/OSPF, Ingress-/Egress-Edges. Auf das Ziel-CNI (Cilium / Calico) und Gateway-Modell abbilden.
- ☐ **Storage-Klassen auf das Ziel abgebildet** — vSAN-Tiers, Datastore-Richtlinien, IOPS-Zusagen. Auf LINSTOR / Ceph / Longhorn oder gleichwertige Storage-Klassen abbilden.
- ☐ **Snapshot- und Replikations-SLAs** — Aktuelle Snapshot-Zeitpläne, Replikationsziele, RPO/RTO-Zusagen. Lücken im Ziel-Storage-Backend identifizieren.
- ☐ **L2-Stretched- / Multi-Site-Netzwerke** — Standortübergreifendes L2, vMotion über Rechenzentren hinweg, Stretched Cluster. Das Meiste übersteht eine Migration nicht; identifizieren Sie Workloads, die dies wirklich benötigen.

„Wir nutzen vSAN für alles“ bedeutet meist 4–6 unterschiedliche Speicherprofile. Erfassen Sie sie alle — die Dimensionierung der Zielpattform hängt von genauen IOPS-/Durchsatzwerten je Klasse ab.

Abschnitt 4 Mandantenfähigkeit

- ☐ **vCD-Organisationsmodell übertragen** — Jede vCD-Org entspricht einer Ziel-Mandantengrenze (Tenant CRD, Namespace-Bundle, Projekt). Kontingente, Netzwerkisolation und IAM je Org abbilden.
- ☐ **Self-Service-Umfang definiert** — Self-Service über Portal, API oder YAML für Mandanten. Festlegen, was Mandanten dürfen und was nicht (Provisionierung, Skalierung, Netzwerkrichtlinien, Auswahl der Storage-Klasse).

Abschnitt 5 KI- / GPU-Workloads

- ☐ **GPU-Inventar** — vGPU vs. Passthrough, GPU-Modell (A100 / H100 / L40S / Blackwell), Workload-Zuordnung je Karte. Herstellergebundene Funktionen notieren (z. B. MIG-Profile).
- ☐ **Abbildung vGPU auf KubeVirt-vGPU** — Bestätigen, dass das Ziel die benötigte GPU-Klasse und das Slicing-Modell unterstützt. Treiberversionen validieren.
- ☐ **Architektonische Eignung der KI-Workloads** — Inferenz vs. Fine-Tuning vs. Training; Anforderungen an die Mandantenisolation; Souveränitätsvorgaben für Modellgewichte und Trainingsdaten.

Achtung. Die vGPU-Lizenzbedingungen von VMware unterscheiden sich wesentlich von der direkten NVIDIA-Lizenzierung unter Kubernetes. Klären Sie dies mit einem NVIDIA-Partner, bevor Sie einen Migrationszeitplan festlegen.

Abschnitt 6 Souveränität & Compliance

- ☐ **Regulatorischer Geltungsbereich bestimmt** — DORA / NIS2 / DSGVO / branchenspezifische / nationale Vorgaben, die für die betroffenen Workloads gelten. Je Workload abbilden, nicht je Umgebung.
- ☐ **Verwahrung der Verschlüsselungsschlüssel** — Aktuelles Schlüsselmanagement (herstellerverwaltet / kunden-verwaltet / HSM-gestützt). Ziel-Modell der Schlüsselverwahrung und Anforderung an die Transparenz des Anbieters definieren.
- ☐ **Vollständigkeit des Audit-Trails** — Aufbewahrung, Unveränderlichkeit und Exportierbarkeit der Werhat-wann-was-Protokolle. Auf die Audit-Pipeline der Zielplattform abbilden (z. B. VictoriaLogs + unveränderliches Backend).

Abschnitt 7 Betriebliche Bereitschaft

- ☐ **Runbook-Inventar** — Dokumentierte Runbooks je Workload-Klasse (Provisionierung, Backup, Wiederherstellung, Failover, Patch). Lücken durch nicht dokumentiertes Erfahrungswissen identifizieren.
- ☐ **Bereitschaftsdienst-Abdeckung** — Aktuelle Rotation, Eskalationsstufen, MTTA-/MTTR-Ziele. Prüfen, ob die Zielplattform zur Kapazität des Bereitschaftsteams passt.

- ☐ **Plan für den Wissenstransfer** — Erforderlicher Kompetenzaufbau für den Zielstack (Kubernetes, KubeVirt, Cozystack-Betrieb). Stunden je Engineer sowie Schulungsformat.

Tipp. Die meisten VMware-nativen Betriebsteams benötigen 60–120 Stunden strukturierte Kubernetes-Schulung, bevor sie ein Kubernetes-basiertes Ziel eigenständig betreiben können. Planen Sie dies in den Migrationszeitplan ein, nicht danach.

Abschnitt 8 Kostenentwicklung

- ☐ **TCO-Eingangsdaten erhoben** — Aktuelle VMware-Lizenzierung (VCF-Abonnementstufe, Host-Anzahl, Support-Stufe, Ablaufdatum). Hardware-Erneuerungszyklus. Betriebskosten (FTE, Support, Rechenzentrumsanteil).
- ☐ **Ablauf von Verpflichtungen abgebildet** — Ende der VMware-Vertragslaufzeit, Ende der Hardware-Garantie. Diese bestimmen das Migrationsfenster. Frühere Ablaufdaten wirken als treibender Faktor.

Kombinieren Sie diese Checkliste mit dem **Cloud Repatriation TCO Worksheet**, um die Zielökonomie quantitativ zu modellieren.

Nächste Schritte

Option 1 — Eigenständige Bearbeitung anhand dieser Checkliste. Gehen Sie die Liste mit Plattform-, Betriebs- und Compliance-Teams durch. Wandeln Sie nicht abgehackte Felder in ein Backlog um. Die meisten Organisationen finden 8–12 nicht abgehackte Felder, die Klärungsarbeit erfordern.

Option 2 — Platform Readiness Assessment mit Aenix (14 Tage). Aenix arbeitet die Checkliste gemeinsam mit Ihnen durch, modelliert die Zielarchitektur und erstellt einen phasenweisen Migrationsplan. Festpreis-Engagement.

Option 3 — Vollständiges Migrationsprojekt. Mehrmonatiger Aufbau mit Architektur, Umsetzung, Migrationswellen und operativer Übergabe. Der Umfang wird durch Phase 2 des Assessments festgelegt.

Vereinbaren Sie ein Erstgespräch. aenix.io/services/platform-readiness-assessment/

Aenix ist das Team hinter Cozystack (CNCF Project) und bietet die Aenix Platform — unser kommerzielles, produktisiertes Angebot auf Basis von Cozystack. aenix.io