13.5 Cluster und Hochverfügbarkeit

Einordnung

Diese Seite gehört zum Kapitel:

Server, Virtualisierung und Hochverfügbarkeit

Auf den vorherigen Seiten ging es um Server-Grundlagen, Virtualisierung, Hypervisor-Verwaltung, Storage, Snapshots und Backups.

Jetzt geht es um:

Cluster und Hochverfügbarkeit

Diese Themen sind wichtig, weil Dienste möglichst zuverlässig erreichbar bleiben sollen, auch wenn einzelne Systeme oder Komponenten ausfallen.

Grundidee

Ein einzelner Server kann ausfallen.

Mögliche Ursachen:

Ursache	Beispiel
Hardwaredefekt	Netzteil, Mainboard, RAM oder Festplatte defekt
Softwarefehler	Betriebssystem oder Dienst stürzt ab
Wartung	Updates oder Hardwaretausch
Netzwerkproblem	Switch, Kabel oder Netzwerkkarte defekt
Stromausfall	Server verliert Strom
Storageproblem	Datenspeicher nicht erreichbar

Wenn ein wichtiger Dienst nur auf einem einzelnen Server läuft, ist dieser Server ein Risiko.

Ein Cluster soll dieses Risiko verringern.

Was ist ein Cluster?

Ein Cluster ist ein Zusammenschluss mehrerer Server, die gemeinsam arbeiten.

Die einzelnen Server im Cluster nennt man **Nodes** oder **Knoten**.

Beispiel:

Cluster	Nodes
Virtualisierungscluster	HV01, HV02, HV03
Datenbankcluster	DB01, DB02
Webserver-Cluster	WEB01, WEB02, WEB03

Ziel ist meist:

Ziel	Bedeutung
Hochverfügbarkeit	Dienste sollen bei Ausfall weiterlaufen oder schnell wieder starten
Lastverteilung	Arbeit wird auf mehrere Systeme verteilt
Skalierbarkeit	Weitere Systeme können ergänzt werden
Wartbarkeit	Einzelne Systeme können gewartet werden

Merksatz

Ein Cluster ist ein Verbund mehrerer Server, die gemeinsam Dienste bereitstellen oder absichern.

Was bedeutet Hochverfügbarkeit?

Hochverfügbarkeit bedeutet, dass ein Dienst möglichst dauerhaft erreichbar bleibt.

Ein System ist hochverfügbar, wenn Ausfälle einzelner Komponenten nicht sofort zum Ausfall des gesamten Dienstes führen.

Beispiel:

Ein Unternehmen betreibt wichtige virtuelle Maschinen auf drei Hypervisor-Hosts.

Wenn ein Host ausfällt, können die VMs auf einem anderen Host neu gestartet werden.

Hochverfügbarkeit bedeutet nicht immer unterbrechungsfrei

Wichtig:

Hochverfügbarkeit bedeutet nicht automatisch, dass es gar keine Unterbrechung gibt.

Oft gibt es eine kurze Unterbrechung.

Beispiel:

Situation	Ergebnis
Host fällt aus	VM wird auf anderem Host neu gestartet
Dienst startet neu	Benutzer merken kurze Unterbrechung
Cluster erkennt Fehler	Automatisches Failover erfolgt

Merksatz:

Hochverfügbarkeit reduziert Ausfallzeiten, verhindert sie aber nicht immer vollständig.

Verfügbarkeit

Verfügbarkeit beschreibt, wie zuverlässig ein Dienst erreichbar ist.

Beispiel:

Verfügbarkeit	Bedeutung
99 %	Dienst darf ca. 3,65 Tage pro Jahr ausfallen
99,9 %	Dienst darf ca. 8,76 Stunden pro Jahr ausfallen
99,99 %	Dienst darf ca. 52,6 Minuten pro Jahr ausfallen
99,999 %	Dienst darf ca. 5,26 Minuten pro Jahr ausfallen

Je höher die gewünschte Verfügbarkeit, desto aufwendiger und teurer wird die technische Umsetzung.

Warum Hochverfügbarkeit wichtig ist

Viele IT-Dienste sind für Unternehmen kritisch.

Beispiele:

Dienst	Auswirkung bei Ausfall
Domain Controller	Anmeldung kann gestört sein
DNS	Systeme können Namen nicht auflösen
DHCP	Neue Clients bekommen keine IP-Konfiguration
Fileserver	Benutzer kommen nicht an Dateien
Datenbankserver	Anwendungen funktionieren nicht
Webserver	Webseite oder Portal nicht erreichbar

Dienst	Auswirkung bei Ausfall
Mailserver	E-Mail-Kommunikation gestört
ERP-System	Geschäftsprozesse betroffen

Single Point of Failure

Ein Single Point of Failure ist eine einzelne Komponente, deren Ausfall einen Dienst oder ein ganzes System lahmlegen kann.

Beispiele:

Single Point of Failure	Risiko
Einziger Server	Dienst fällt komplett aus
Einziger Switch	Netzwerk nicht erreichbar
Einziges Netzteil	Server geht aus
Einziger Storage	VM-Daten nicht erreichbar
Einzige Internetleitung	Externer Zugriff fällt aus
Einziger Domain Controller	Anmeldung und DNS gefährdet

Cluster und Redundanz sollen Single Points of Failure reduzieren.

Redundanz

Redundanz bedeutet, dass wichtige Komponenten mehrfach vorhanden sind.

Beispiele:

Komponente	Redundanz
Server	Mehrere Cluster-Nodes
Netzteil	Zwei Netzteile
Netzwerk	Mehrere Netzwerkkarten
Switch	Zwei Switches
Storage	RAID, Replikation oder verteiltes Storage
Internet	Zweite Leitung
Dienste	Mehrere Server mit gleicher Rolle

Merksatz:

Redundanz bedeutet, dass eine kritische Komponente nicht nur einmal vorhanden ist.

Cluster-Node

Ein Cluster-Node ist ein einzelner Server innerhalb eines Clusters.

Beispiel:

Node	Aufgabe
HV01	Virtualisierungshost 1
HV02	Virtualisierungshost 2
HV03	Virtualisierungshost 3

Alle Nodes zusammen bilden den Cluster.

Cluster-Ressource

Eine Cluster-Ressource ist ein Dienst, eine VM, eine IP-Adresse oder ein Speicherbereich, der vom Cluster verwaltet wird.

Beispiele:

Cluster-Ressource	Erklärung
Virtuelle Maschine	Kann auf verschiedenen Hosts laufen
IP-Adresse	Wird einem aktiven Dienst zugeordnet
Dateifreigabe	Wird vom aktiven Node bereitgestellt
Datenbankdienst	Kann auf anderem Node starten
Storage	Gemeinsamer Speicherbereich
Anwendung	Wird vom Cluster überwacht

Failover

Failover bedeutet, dass ein Dienst bei Ausfall eines Systems auf ein anderes System wechselt.

Beispiel:

Schritt	Ereignis
1	VM läuft auf HV01
2	HV01 fällt aus

Schritt	Ereignis
3	Cluster erkennt den Ausfall
4	VM wird auf HV02 neu gestartet
5	Dienst ist wieder erreichbar

Merksatz:

Failover bedeutet Übernahme bei Ausfall.

Failback

Failback bedeutet, dass ein Dienst nach der Reparatur wieder auf das ursprüngliche System zurückverschoben wird.

Beispiel:

Schritt	Ereignis
1	VM läuft ursprünglich auf HV01
2	HV01 fällt aus
3	VM wird auf HV02 gestartet
4	HV01 wird repariert
5	VM wird zurück auf HV01 verschoben

Failback kann automatisch oder manuell erfolgen.

Automatisches Failover

Beim automatischen Failover erkennt der Cluster einen Fehler selbst und startet die betroffene Ressource auf einem anderen Node.

Vorteile:

Vorteil	Erklärung
Schnelle Reaktion	Kein manuelles Eingreifen nötig
Weniger Ausfallzeit	Dienst schneller wieder verfügbar
Bessere Verfügbarkeit	Besonders bei kritischen Diensten

Nachteil:

Automatisches Failover muss gut geplant werden, damit es nicht durch Fehlalarme oder Netzwerkprobleme zu unerwünschten Umschaltungen kommt.

Manuelles Failover

Beim manuellen Failover stößt ein Administrator die Umschaltung bewusst an.

Typische Gründe:

Grund	Beispiel
Wartung	Node soll aktualisiert werden
Test	Failover-Funktion prüfen
Lastverteilung	Ressource auf anderen Node verschieben
Fehleranalyse	Dienst bewusst verlagern

Manuelles Failover ist kontrollierter, aber nicht so schnell wie automatisches Failover.

Heartbeat

Heartbeat ist ein regelmäßiges Signal zwischen Cluster-Nodes.

Damit prüfen die Nodes gegenseitig, ob sie noch erreichbar sind.

Beispiel:

Node	Signal
HV01	sendet Heartbeat
HV02	sendet Heartbeat
HV03	sendet Heartbeat

Wenn ein Node keine Heartbeat-Signale mehr sendet, kann der Cluster einen Ausfall vermuten.

Heartbeat ist nicht gleich echter Serverausfall

Ein fehlender Heartbeat kann verschiedene Ursachen haben.

Ursache	Bedeutung
Server ist wirklich ausgefallen	Node ist nicht mehr aktiv
Netzwerkproblem	Node lebt, ist aber nicht erreichbar
Switchproblem	Verbindung zwischen Nodes gestört

Ursache	Bedeutung
Firewallproblem	Heartbeat wird blockiert
Überlastung	Node reagiert zu langsam

Deshalb braucht ein Cluster zusätzliche Entscheidungsmechanismen wie Quorum.

Quorum

Quorum ist ein Entscheidungsmechanismus in einem Cluster.

Es legt fest, welcher Teil eines Clusters weiterarbeiten darf.

Ziel:

Der Cluster soll auch bei Kommunikationsproblemen eine eindeutige Entscheidung treffen können.

Merksatz:

Quorum verhindert, dass mehrere Cluster-Teile gleichzeitig unabhängig voneinander aktiv werden.

Warum Quorum wichtig ist

Beispiel:

Ein Cluster besteht aus zwei Nodes.

Die Netzwerkverbindung zwischen beiden Nodes bricht ab.

Problem:

Beide Nodes könnten denken:

Der andere Node ist ausgefallen, also übernehme ich.

Wenn beide gleichzeitig aktiv werden und auf dieselben Daten schreiben, kann es zu Datenkorruption kommen.

Quorum soll genau das verhindern.

Split-Brain

Split-Brain ist ein gefährlicher Zustand in einem Cluster.

Dabei verlieren Cluster-Teile die Verbindung zueinander und arbeiten gleichzeitig weiter, obwohl sie nicht mehr sauber koordiniert sind.

Problem:

Beide Seiten können glauben, sie seien der aktive Cluster.

Mögliche Folgen:

Folge	Erklärung
Datenkorruption	Mehrere Systeme schreiben auf dieselben Daten
Inkonsistente Dienste	Unterschiedliche Zustände
Datenverlust	Änderungen können verloren gehen
Komplexe Wiederherstellung	Manuelle Reparatur nötig

Merksatz:

Split-Brain ist ein gefährlicher Cluster-Zustand, bei dem getrennte Cluster-Teile gleichzeitig aktiv werden.

Witness

Ein Witness ist eine zusätzliche Entscheidungsinstanz für das Quorum.

Er hilft dem Cluster, eine Mehrheit zu bilden.

Beispiele:

Witness-Art	Erklärung
File Share Witness	Netzwerkfreigabe als Zeuge
Disk Witness	Gemeinsamer Datenträger als Zeuge
Cloud Witness	Cloud-Dienst als Zeuge

Besonders bei Clustern mit gerader Node-Anzahl ist ein Witness wichtig.

Beispiel mit zwei Nodes und Witness

Komponente	Stimme
Node 1	1 Stimme
Node 2	1 Stimme
Witness	1 Stimme

Wenn Node 1 die Verbindung zu Node 2 verliert, entscheidet die Mehrheit.

Der Teil, der noch die Mehrheit besitzt, darf weiterarbeiten.

Aktiv/Passiv-Cluster

Bei einem Aktiv/Passiv-Cluster ist ein Node aktiv und ein anderer Node wartet als Reserve.

Beispiel:

Node	Zustand
Node 1	Aktiv
Node 2	Passiv / Standby

Wenn Node 1 ausfällt, übernimmt Node 2.

Vorteile:

Vorteil	Erklärung
Einfaches Konzept	Leicht verständlich
Klare Zuständigkeit	Ein aktives System
Gute Absicherung	Reserve steht bereit

Nachteile:

Nachteil	Erklärung
Ressourcen ungenutzt	Passiver Node macht im Normalbetrieb wenig
Teurer	Hardware wird als Reserve vorgehalten

Aktiv/Aktiv-Cluster

Bei einem Aktiv/Aktiv-Cluster arbeiten mehrere Nodes gleichzeitig.

Beispiel:

Node	Zustand
Node 1	Aktiv
Node 2	Aktiv
Node 3	Aktiv

Vorteile:

Vorteil	Erklärung
Bessere Ressourcennutzung	Alle Nodes arbeiten
Skalierbarkeit	Last kann verteilt werden
Flexibilität	Dienste können verteilt laufen

Nachteile:

Nachteil	Erklärung
Komplexer	Planung und Konfiguration aufwendiger
Abhängigkeiten	Anwendungen müssen dafür geeignet sein
Failover-Reserve nötig	Trotz Aktiv/Aktiv muss Kapazität für Ausfälle bleiben

---

Aktiv/Passiv vs. Aktiv/Aktiv

Merkmal	Aktiv/Passiv	Aktiv/Aktiv
Normalbetrieb	Ein Node aktiv, einer wartet	Mehrere Nodes aktiv
Ressourcennutzung	Weniger effizient	Effizienter
Komplexität	Einfacher	Komplexer
Beispiel	Datenbankdienst mit Standby	Mehrere Webserver
Failover	Passiver Node übernimmt	Andere aktive Nodes übernehmen zusätzlich

---

High Availability

High Availability bedeutet Hochverfügbarkeit.

Ziel:

Ein Dienst soll möglichst wenig ausfallen.

Typische Maßnahmen:

Maßnahme	Wirkung
Mehrere Server	Ausfall eines Servers abfangen
Redundantes Netzwerk	Netzwerkfehler reduzieren
Redundanter Storage	Speicherverfügbarkeit erhöhen
Monitoring	Fehler erkennen
Failover	Dienst auf anderem System starten

Maßnahme	Wirkung
Backups	Wiederherstellung ermöglichen
USV	Stromausfälle abfangen

Fault Tolerance

Fault Tolerance bedeutet Fehlertoleranz.

Dabei soll ein Dienst möglichst ohne Unterbrechung weiterlaufen, auch wenn eine Komponente ausfällt.

Unterschied:

Begriff	Bedeutung
High Availability	Dienst wird nach Ausfall schnell wiederhergestellt
Fault Tolerance	Dienst läuft möglichst ohne merkbare Unterbrechung weiter

Fault Tolerance ist technisch aufwendiger als normale Hochverfügbarkeit.

Hochverfügbarkeit vs. Backup

Hochverfügbarkeit und Backup sind nicht dasselbe.

Hochverfügbarkeit	Backup
Soll Ausfallzeit reduzieren	Soll Daten wiederherstellen
Hilft bei Hardware- oder Dienstausfall	Hilft bei Datenverlust
Arbeitet oft automatisch	Restore muss geplant werden
Schützt nicht vor falschen Daten	Kann ältere Zustände wiederherstellen
Kein Ersatz für Backup	Kein Ersatz für HA

Beispiel:

Wenn eine Datei gelöscht wird, repliziert oder übernimmt ein HA-System diesen Zustand eventuell ebenfalls.

Ein Backup kann eine ältere Version wiederherstellen.

Cluster vs. Backup

Ein Cluster schützt nicht automatisch vor Datenverlust.

Beispiel:

Ereignis	Hilft Cluster?	Hilft Backup?
Host fällt aus	Ja	Nicht primär
Dienst stürzt ab	Teilweise	Nicht primär
Datei gelöscht	Nein	Ja
Ransomware verschlüsselt Daten	Nein	Ja, wenn Backup geschützt ist
Storage komplett defekt	Nur bei redundantem Storage	Ja, wenn Backup getrennt liegt
Fehlkonfiguration	Teilweise nein	Ja, wenn alter Stand vorhanden

Merksatz:

Ein Cluster erhöht Verfügbarkeit, ein Backup schützt vor Datenverlust. Beides wird benötigt.

Virtualisierungscluster

Ein Virtualisierungscluster besteht aus mehreren Hypervisor-Hosts.

Darauf laufen virtuelle Maschinen.

Beispiel:

Node	Aufgabe
HV01	Host für VMs
HV02	Host für VMs
HV03	Host für VMs

Wenn ein Host ausfällt, können VMs auf einem anderen Host neu gestartet werden.

Beispiel Virtualisierungscluster

VM	Läuft aktuell auf
DC01	HV01
FILE01	HV01
WEB01	HV02
DB01	HV03

VM	Läuft aktuell auf
MON01	HV02

Wenn HV01 ausfällt:

VM	Neuer Host
DC01	HV02
FILE01	HV03

Voraussetzung:

Die anderen Hosts müssen genug freie Ressourcen haben.

Ressourcenreserve im Cluster

Ein Cluster braucht Reserven.

Wenn ein Node ausfällt, müssen die verbleibenden Nodes dessen VMs übernehmen können.

Beispiel:

Cluster	Problem
3 Hosts, alle zu 100 % ausgelastet	Kein Host-Ausfall abfangbar
3 Hosts mit Reserve	Ausfall eines Hosts kann abgefangen werden

Merksatz:

Ein Cluster ohne freie Ressourcen kann kein sinnvolles Failover leisten.

N+1-Prinzip

N+1 bedeutet:

Es gibt eine zusätzliche Reservekomponente.

Beispiel:

Für die normale Last werden zwei Hosts benötigt.

Ein dritter Host ist als Reserve vorhanden.

Benötigt	Vorhanden

2 Hosts	3 Hosts

Wenn ein Host ausfällt, können die verbleibenden Hosts die Last übernehmen.

N+2-Prinzip

N+2 bedeutet:

Es gibt zwei zusätzliche Reservekomponenten.

Beispiel:

Für die normale Last werden drei Hosts benötigt.

Es sind fünf Hosts vorhanden.

Benötigt	Vorhanden
3 Hosts	5 Hosts

Dadurch kann der Cluster den Ausfall von zwei Hosts besser verkraften.

Shared Storage im Cluster

Shared Storage ist gemeinsamer Speicher, auf den mehrere Cluster-Nodes zugreifen können.

Beispiel:

Host	Zugriff auf Storage
HV01	Ja
HV02	Ja
HV03	Ja

Vorteil:

Wenn eine VM auf einem anderen Host gestartet werden soll, kann dieser Host direkt auf die VM-Daten zugreifen.

Beispiele für Shared Storage

Storage-Art	Erklärung
SAN	Storage Area Network
NAS	Network Attached Storage

Storage-Art	Erklärung
iSCSI	Blockspeicher über IP
Fibre Channel	Dediziertes Storage-Netz
NFS	Netzwerkdateisystem
SMB 3.0	Dateifreigabe für bestimmte Hyper-V-Szenarien

Risiko bei Shared Storage

Shared Storage kann selbst ein Single Point of Failure sein.

Beispiel:

Wenn alle Hosts auf denselben Storage zugreifen und dieser Storage ausfällt, sind alle VMs betroffen.

Deshalb muss auch der Storage redundant geplant werden.

Maßnahmen:

Maßnahme	Wirkung
RAID	Schutz vor Festplattenausfall
Redundante Controller	Schutz vor Controllerdefekt
Mehrere Netzwege	Schutz vor Netzwerkfehler
Zwei Switches	Schutz vor Switchausfall
Replikation	Kopie auf anderem Storage
Backup	Wiederherstellung bei Datenverlust

Shared-Nothing-Cluster

Bei einem Shared-Nothing-Cluster hat jeder Node eigenen lokalen Speicher.

Die Daten werden zwischen den Nodes repliziert oder verteilt.

Beispiele:

Technologie	Prinzip
Ceph	Verteilter Storage
VMware vSAN	Verteilter Speicher über Hosts
Storage Spaces Direct	Microsoft verteilter Storage

Technologie	Prinzip
GlusterFS	Verteiltes Dateisystem

Vorteil:

Kein einzelner zentraler Storage muss zwingend vorhanden sein.

Nachteil:

Die Einrichtung ist komplexer und benötigt ein gutes Netzwerk.

Cluster-Netzwerke

Ein Cluster verwendet oft mehrere getrennte Netzwerke.

Beispiele:

Netzwerk	Aufgabe
Management-Netz	Verwaltung der Hosts
VM-Netz	Netzwerkverkehr der virtuellen Maschinen
Storage-Netz	Zugriff auf SAN, NAS, iSCSI oder NFS
Migration-Netz	Live Migration von VMs
Cluster-Heartbeat	Überwachung der Nodes
Backup-Netz	Datenverkehr für Sicherungen

Diese Trennung kann physisch oder über VLANs erfolgen.

Warum Netztrennung wichtig ist

Grund	Erklärung
Sicherheit	Management und Storage nicht im normalen Clientnetz
Performance	Storage- und Backupverkehr stören nicht den Benutzerverkehr
Übersicht	Klare Trennung der Aufgaben
Fehlerbegrenzung	Probleme in einem Netz betreffen nicht alles
Hochverfügbarkeit	Redundante Wege möglich

Live Migration im Cluster

Live Migration bedeutet, dass eine laufende VM von einem Host auf einen anderen Host verschoben wird.

Beispiel:

Vorher	Nachher
VM läuft auf HV01	VM läuft auf HV02

Die VM soll dabei weiterlaufen.

Nutzen:

Situation	Vorteil
Wartung	Host kann aktualisiert werden
Lastverteilung	VMs können besser verteilt werden
Hardwaretausch	VM vorher verschieben
Clusterbetrieb	Flexible Verwaltung

Failover vs. Live Migration

Begriff	Situation	Unterbrechung
Failover	Fehler oder Ausfall	Häufig kurze Unterbrechung
Live Migration	Geplante Verschiebung	Möglichst keine Unterbrechung

Beispiel:

Situation	Richtiger Begriff
Host fällt plötzlich aus	Failover
Admin verschiebt VM vor Wartung	Live Migration

Wartungsmodus

Ein Cluster-Node kann in den Wartungsmodus versetzt werden.

Typischer Ablauf:

Schritt	Erklärung
Wartungsmodus aktivieren	Host soll keine produktiven VMs mehr betreiben
VMs migrieren	VMs auf andere Hosts verschieben

Schritt	Erklärung
Updates installieren	Host aktualisieren
Neustart durchführen	Falls nötig
Funktion prüfen	Host kontrollieren
Wartungsmodus beenden	Host wieder nutzen

Wartungsmodus hilft, geplante Arbeiten ohne unnötige Ausfälle durchzuführen.

Cluster-Monitoring

Ein Cluster muss überwacht werden.

Wichtige Werte:

Bereich	Messwert
Nodes	Online, offline, Fehler
VMs	Läuft, gestoppt, migriert
Ressourcen	CPU, RAM, Storage
Netzwerk	Heartbeat, Paketverlust, Latenz
Storage	Freier Speicher, IOPS, Latenz
Failover-Ereignisse	Wann wurde umgeschaltet?
Quorum	Ist Quorum vorhanden?
Backups	Erfolgreich oder fehlgeschlagen?

Cluster-Logs

Cluster-Logs helfen bei Fehlersuche.

Typische Fragen:

Frage	Warum wichtig?
Warum wurde ein Failover ausgelöst?	Ursache finden
Welcher Node war betroffen?	Fehler eingrenzen
Gab es Heartbeat-Probleme?	Netzwerk prüfen
War Storage erreichbar?	Storagefehler erkennen
Gab es Ressourcenmangel?	Kapazität prüfen
Wurde Quorum verloren?	Split-Brain-Risiko prüfen

Cluster und Updates

Updates in einem Cluster müssen geplant werden.

Typischer Ablauf:

Schritt	Erklärung
Backup prüfen	Sicherung vorhanden?
Clusterzustand prüfen	Alle Nodes gesund?
Node in Wartungsmodus setzen	Keine produktiven VMs dort
VMs verschieben	Live Migration nutzen
Updates installieren	Host aktualisieren
Neustart durchführen	Falls erforderlich
Funktion prüfen	Node wieder gesund?
Nächsten Node aktualisieren	Schrittweise vorgehen

Merksatz:

Cluster-Updates sollten nacheinander und kontrolliert erfolgen, nicht auf allen Nodes gleichzeitig.

Cluster und Backup

Auch in einem Cluster braucht man Backups.

Warum?

Risiko	Cluster reicht nicht
Datei wird gelöscht	Löschung bleibt im Cluster gültig
Datenbank wird beschädigt	Beschädigung kann repliziert werden
Ransomware	Daten können überall verschlüsselt werden
Fehlkonfiguration	Falscher Zustand bleibt aktiv
Storagefehler	Cluster hilft nur bei passender Storage-Redundanz

Deshalb:

Cluster und Backup gehören zusammen.

Clusterfähige Anwendungen

Nicht jede Anwendung ist automatisch clusterfähig.

Eine Anwendung ist clusterfähig, wenn sie in einer Umgebung mit mehreren Systemen zuverlässig betrieben werden kann.

Beispiele:

Anwendung / Dienst	Clusterfähigkeit
Webserver	Meist gut skalierbar
Datenbank	Benötigt spezielle Cluster- oder Replikationsfunktion
Dateiserver	Benötigt gemeinsamen oder replizierten Speicher
Alte Einzelplatzsoftware	Oft nicht geeignet
Domain Controller	Mehrere DCs möglich, aber kein klassischer Failover-Cluster

---

Stateful und Stateless

Für Cluster ist wichtig, ob eine Anwendung zustandsbehaftet oder zustandslos arbeitet.

Begriff	Bedeutung
Stateless	Server speichert keinen wichtigen Sitzungszustand lokal
Stateful	Server speichert Sitzungszustand oder lokale Daten

Stateless-Anwendungen sind einfacher zu skalieren.

Stateful-Anwendungen brauchen besondere Konzepte wie gemeinsamen Speicher, Replikation oder Session-Persistenz.

Beispiel Stateless

Ein Webserver liefert statische Webseiten aus.

Mehrere Webserver können dieselben Dateien bereitstellen.

Ein Load Balancer verteilt Anfragen.

Wenn ein Webserver ausfällt, übernimmt ein anderer.

Das ist vergleichsweise einfach.

Beispiel Stateful

Eine Datenbank speichert laufend Transaktionen.

Mehrere Datenbankserver müssen genau wissen, welche Daten aktuell gültig sind.

Das ist deutlich komplexer.

Hier braucht man Replikation, Failover-Konzepte oder spezielle Datenbankcluster.

Clusterarten

Es gibt verschiedene Arten von Clustern.

Clusterart	Ziel
Failover-Cluster	Dienst bei Ausfall auf anderem Node starten
Load-Balancing-Cluster	Anfragen auf mehrere Systeme verteilen
Storage-Cluster	Speicher verteilt oder hochverfügbar bereitstellen
Datenbank-Cluster	Datenbank hochverfügbar oder skalierbar betreiben
Virtualisierungscluster	VMs auf mehreren Hosts betreiben
Container-Cluster	Container auf mehreren Nodes betreiben

Failover-Cluster

Ein Failover-Cluster ist darauf ausgelegt, Dienste bei Ausfall auf einem anderen Node weiterzuführen oder neu zu starten.

Typische Beispiele:

Einsatz	Beispiel
Virtualisierung	VM startet auf anderem Host
Dateiserver	Dateidienst wechselt auf anderen Node
Datenbank	Datenbankinstanz übernimmt auf anderem Node
Anwendung	Dienst startet auf Ersatzsystem

Load-Balancing-Cluster

Ein Load-Balancing-Cluster verteilt Anfragen auf mehrere aktive Systeme.

Beispiel:

System	Aufgabe

Load Balancer	Verteilt Anfragen
WEB01	Webserver
WEB02	Webserver
WEB03	Webserver

Ziel:

Ziel	Erklärung
Mehr Leistung	Mehrere Server teilen sich Arbeit
Bessere Verfügbarkeit	Ausfall eines Servers kann abgefangen werden
Skalierbarkeit	Weitere Server können ergänzt werden

Load Balancing wird auf einer eigenen Seite genauer behandelt.

Failover-Cluster vs. Load Balancing

Merkmal	Failover-Cluster	Load Balancing
Hauptziel	Ausfallsicherheit	Lastverteilung
Normalbetrieb	Oft eine aktive Ressource	Mehrere Systeme aktiv
Ausfall	Ressource wechselt oder startet neu	Anfragen gehen an andere Server
Beispiel	VM startet auf anderem Host	Webanfragen auf WEB01/WEB02
Typische Dienste	VMs, Datenbanken, Dateiserver	Webserver, APIs, Anwendungen

---

Cluster in Windows-Umgebungen

In Windows-Umgebungen gibt es den Failover Cluster.

Typische Begriffe:

Begriff	Bedeutung
Failover Cluster	Microsoft-Clusterfunktion
Cluster Node	Server im Cluster
Cluster Resource	Verwaltete Ressource
CSV	Cluster Shared Volume
Quorum	Entscheidungsmechanismus
Witness	Zusätzlicher Zeuge
Live Migration	VM wird laufend verschoben

Cluster in VMware-Umgebungen

In VMware-Umgebungen sind typische Begriffe:

Begriff	Bedeutung
ESXi	Hypervisor
vCenter	Zentrale Verwaltung
vMotion	Live Migration
HA	Hochverfügbarkeit
DRS	Automatische Lastverteilung
Datastore	Speicherbereich
Cluster	Gruppe von ESXi-Hosts

Cluster in Proxmox-Umgebungen

In Proxmox-Umgebungen gibt es ebenfalls Clusterfunktionen.

Typische Begriffe:

Begriff	Bedeutung
Node	Einzelner Proxmox-Host
Cluster	Zusammenschluss mehrerer Nodes
HA Manager	Verwaltung hochverfügbarer Ressourcen
Ceph	Verteilter Storage
Quorum	Mehrheitsentscheidung
Migration	VM oder Container verschieben
VMID	Eindeutige ID einer VM oder eines Containers

Cluster in Container-Umgebungen

Container können ebenfalls in Clustern betrieben werden.

Beispiele:

Plattform	Bedeutung
Kubernetes	Container-Orchestrierung
Docker Swarm	Einfacherer Container-Cluster

Plattform	Bedeutung
Nomad	Workload-Orchestrierung

Typische Funktionen:

Funktion	Erklärung
Scheduling	Container auf Nodes verteilen
Self-Healing	Fehlerhafte Container neu starten
Scaling	Mehr Instanzen starten
Service Discovery	Dienste auffindbar machen
Rolling Updates	Schrittweise Updates durchführen

Kapazitätsplanung im Cluster

Ein Cluster muss so geplant werden, dass ein Ausfall abgefangen werden kann.

Wichtige Fragen:

Frage	Bedeutung
Wie viele Nodes gibt es?	Grundstruktur
Wie viele Nodes dürfen ausfallen?	Verfügbarkeitsziel
Reicht CPU nach Ausfall?	VMs müssen weiterlaufen
Reicht RAM nach Ausfall?	RAM ist oft kritisch
Reicht Storage?	VM-Daten und Snapshots
Reicht Netzwerkbandbreite?	Migration, Storage, Backup
Gibt es Quorum?	Cluster muss entscheiden können

Beispiel Kapazitätsplanung

Ein Cluster hat drei Hosts.

Jeder Host hat:

Ressource	Wert
CPU	32 Kerne
RAM	256 GB
Storagezugriff	Shared Storage

Wenn ein Host ausfällt, müssen zwei Hosts die Last von drei Hosts tragen können.

Deshalb sollte der Cluster nicht dauerhaft zu stark ausgelastet sein.

Typische Fehler bei Clustern

Fehler	Auswirkung
Kein Quorum-Konzept	Split-Brain-Gefahr
Kein Witness bei zwei Nodes	Unsichere Mehrheitsentscheidung
Cluster voll ausgelastet	Failover nicht möglich
Shared Storage nicht redundant	Storage bleibt Single Point of Failure
Keine Netzwerkredundanz	Heartbeat oder Storage fällt aus
Kein Backup	Cluster schützt nicht vor Datenverlust
Keine Dokumentation	Fehlersuche wird schwierig
Keine Failover-Tests	Funktion im Ernstfall unsicher
Updates auf allen Nodes gleichzeitig	Gesamtausfall möglich
Monitoring fehlt	Probleme werden zu spät erkannt

Gute Praxis bei Clustern

Empfehlung	Grund
Quorum sauber planen	Split-Brain verhindern
Witness verwenden	Besonders bei gerader Node-Anzahl
Ressourcenreserve einplanen	Failover ermöglichen
Storage redundant auslegen	Storage-Ausfall vermeiden
Netzwerk redundant auslegen	Heartbeat, Storage und Migration absichern
Cluster regelmäßig testen	Failover-Funktion prüfen
Backups unabhängig halten	Schutz vor Datenverlust
Dokumentation pflegen	Betrieb nachvollziehbar machen
Monitoring einrichten	Fehler früh erkennen
Updates schrittweise durchführen	Ausfallrisiko senken

Prüfungsnahes Beispiel 1

Aufgabe:

Ein Unternehmen betreibt eine wichtige VM auf einem einzelnen Hypervisor-Host. Wenn dieser Host ausfällt, ist die VM nicht verfügbar.

Frage:

Welche Lösung verbessert die Verfügbarkeit?

Mögliche Antwort:

Eine Lösung wäre ein Virtualisierungscluster aus mehreren Hosts. Die VM kann dann bei Ausfall eines Hosts auf einem anderen Host neu gestartet werden. Zusätzlich werden gemeinsamer oder replizierter Storage, Netzwerkredundanz, Monitoring und Backups benötigt.

Prüfungsnahes Beispiel 2

Aufgabe:

Ein Cluster mit zwei Nodes verliert die Netzwerkverbindung zwischen den Nodes. Beide Nodes greifen auf denselben Speicher zu.

Frage:

Welches Risiko entsteht?

Mögliche Antwort:

Es besteht die Gefahr eines Split-Brain-Zustands. Beide Nodes könnten glauben, dass der jeweils andere ausgefallen ist und gleichzeitig aktiv werden. Wenn beide auf dieselben Daten schreiben, kann es zu Datenkorruption kommen. Ein korrektes Quorum mit Witness soll das verhindern.

Prüfungsnahes Beispiel 3

Aufgabe:

Ein Unternehmen hat einen Drei-Node-Cluster. Alle Hosts sind dauerhaft zu 95 Prozent ausgelastet.

Frage:

Warum ist das problematisch?

Mögliche Antwort:

Bei Ausfall eines Nodes müssten die verbleibenden Hosts dessen Last übernehmen. Wenn sie bereits fast vollständig ausgelastet sind, reicht die Kapazität dafür nicht aus. Ein Cluster benötigt Ressourcenreserven, zum Beispiel nach dem N+1-Prinzip.

Prüfungsnahes Beispiel 4

Aufgabe:

Ein Administrator meint: „Wir brauchen keine Backups, weil unsere Server im Cluster laufen.“

Frage:

Warum ist diese Aussage falsch?

Mögliche Antwort:

Ein Cluster erhöht die Verfügbarkeit, schützt aber nicht zuverlässig vor Datenverlust. Versehentlich gelöschte Dateien, Ransomware, Datenkorruption oder Fehlkonfigurationen können im Cluster ebenfalls wirksam werden. Backups sind weiterhin notwendig.

Typische Prüfungsfrage: Was ist ein Cluster?

Mögliche Antwort:

Ein Cluster ist ein Zusammenschluss mehrerer Server, die gemeinsam Dienste bereitstellen oder absichern. Ziel ist meistens Hochverfügbarkeit, Lastverteilung, Skalierbarkeit oder bessere Wartbarkeit.

Typische Prüfungsfrage: Was ist ein Cluster-Node?

Mögliche Antwort:

Ein Cluster-Node ist ein einzelner Server innerhalb eines Clusters. Mehrere Nodes bilden zusammen den Cluster.

Typische Prüfungsfrage: Was ist Failover?

Mögliche Antwort:

Failover bedeutet, dass ein Dienst oder eine Ressource bei Ausfall eines Systems auf ein anderes System wechselt oder dort neu gestartet wird. Dadurch wird die Ausfallzeit reduziert.

Typische Prüfungsfrage: Was ist Failback?

Mögliche Antwort:

Failback bedeutet, dass ein Dienst nach der Reparatur oder Wiederverfügbarkeit des ursprünglichen Systems wieder dorthin zurückverschoben wird.

Typische Prüfungsfrage: Was ist Quorum?

Mögliche Antwort:

Quorum ist ein Entscheidungsmechanismus in einem Cluster. Es legt fest, welcher Teil des Clusters weiterarbeiten darf. Dadurch wird verhindert, dass mehrere Cluster-Teile gleichzeitig aktiv werden und Daten beschädigen.

Typische Prüfungsfrage: Was ist Split-Brain?

Mögliche Antwort:

Split-Brain ist ein gefährlicher Zustand, bei dem getrennte Cluster-Teile gleichzeitig glauben, aktiv sein zu dürfen. Wenn beide Seiten auf dieselben Daten schreiben, kann es zu Datenkorruption kommen. Quorum und Witness helfen, Split-Brain zu verhindern.

Typische Prüfungsfrage: Was ist ein Witness?

Mögliche Antwort:

Ein Witness ist eine zusätzliche Entscheidungsinstanz in einem Cluster. Er hilft beim Quorum, eine Mehrheit zu bilden. Beispiele sind File Share Witness, Disk Witness oder Cloud Witness.

Typische Prüfungsfrage: Unterschied Aktiv/Passiv und Aktiv/Aktiv

Aktiv/Passiv	Aktiv/Aktiv
Ein Node ist aktiv, ein anderer wartet	Mehrere Nodes arbeiten gleichzeitig
Einfacher Aufbau	Bessere Ressourcennutzung
Passiver Node als Reserve	Alle Nodes können produktiv genutzt werden
Beispiel: Dienst mit Standby-Node	Beispiel: mehrere Webserver

---

Typische Prüfungsfrage: Unterschied Hochverfügbarkeit und Fehlertoleranz

Hochverfügbarkeit	Fehlertoleranz
Dienst wird nach Ausfall schnell wiederhergestellt	Dienst läuft möglichst ohne Unterbrechung weiter
Kurze Unterbrechung möglich	Möglichst keine merkbare Unterbrechung
Häufiger in normalen IT-Umgebungen	Technisch aufwendiger

Typische Prüfungsfrage: Warum braucht ein Cluster trotzdem Backups?

Mögliche Antwort:

Ein Cluster schützt vor Ausfällen einzelner Systeme, aber nicht vor versehentlichem Löschen, Ransomware, Datenkorruption oder Fehlkonfiguration. Backups werden benötigt, um ältere oder saubere Datenstände wiederherzustellen.

Typische Prüfungsfrage: Was ist der Unterschied zwischen Failover und Live Migration?

Failover	Live Migration
Reaktion auf Fehler oder Ausfall	Geplante Verschiebung
Häufig kurze Unterbrechung	Möglichst ohne Unterbrechung
Beispiel: Host fällt aus	Beispiel: Wartung eines Hosts

Typische Prüfungsfrage: Warum braucht ein Cluster Ressourcenreserven?

Mögliche Antwort:

Wenn ein Node ausfällt, müssen die verbleibenden Nodes dessen Dienste oder VMs übernehmen können. Sind alle Nodes bereits voll ausgelastet, ist kein zuverlässiges Failover möglich. Deshalb braucht ein Cluster freie CPU-, RAM-, Storage- und Netzwerkressourcen.

Wichtige Begriffe

Begriff	Kurz erklärt
Cluster	Verbund mehrerer Server
Node	Einzelner Server im Cluster
Cluster-Ressource	Vom Cluster verwalteter Dienst oder Objekt
Hochverfügbarkeit	Dienst soll möglichst wenig ausfallen
Failover	Übernahme bei Ausfall
Failback	Rückkehr auf ursprüngliches System
Heartbeat	Regelmäßiges Signal zwischen Nodes
Quorum	Entscheidungsmechanismus im Cluster
Witness	Zusätzlicher Zeuge für Quorum
Split-Brain	Getrennte Cluster-Teile werden gleichzeitig aktiv
Aktiv/Passiv	Ein aktiver Node, ein Standby-Node
Aktiv/Aktiv	Mehrere Nodes arbeiten gleichzeitig
High Availability	Hochverfügbarkeit

Begriff	Kurz erklärt
Fault Tolerance	Fehlertoleranz
Shared Storage	Gemeinsamer Speicher
Shared-Nothing	Kein zentral gemeinsamer Speicher
N+1	Eine Reservekomponente
N+2	Zwei Reservekomponenten
Wartungsmodus	Node für Wartung vorbereiten
Live Migration	Laufende VM verschieben
Single Point of Failure	Einzelne kritische Ausfallstelle
Redundanz	Kritische Komponenten mehrfach vorhanden

Wichtige Merksätze

Ein Cluster ist ein Verbund mehrerer Server, die gemeinsam Dienste bereitstellen oder absichern.

Hochverfügbarkeit reduziert Ausfallzeiten, verhindert aber nicht automatisch jede Unterbrechung.

Failover bedeutet Übernahme bei Ausfall.

Failback bedeutet Rückkehr auf das ursprüngliche System.

Heartbeat dient zur Überwachung der Cluster-Nodes.

Quorum verhindert gefährliche Split-Brain-Situationen.

Ein Witness hilft dem Cluster bei der Mehrheitsentscheidung.

Ein Cluster braucht Ressourcenreserven, sonst kann er keinen Ausfall abfangen.

Shared Storage muss ebenfalls redundant geplant werden.

Ein Cluster ersetzt kein Backup.

Snapshots ersetzen kein Backup.

RAID ersetzt kein Backup.

Live Migration ist für geplante Verschiebungen, Failover für Fehlerfälle.

Kurzzusammenfassung

Cluster und Hochverfügbarkeit dienen dazu, wichtige IT-Dienste zuverlässiger bereitzustellen.

Ein Cluster besteht aus mehreren Nodes.
Diese Nodes können Dienste, virtuelle Maschinen oder andere Ressourcen gemeinsam verwalten.

Wichtige Ziele sind:

Ziel	Bedeutung
Hochverfügbarkeit	Weniger Ausfallzeit
Failover	Übernahme bei Ausfall
Wartbarkeit	Systeme können nacheinander gewartet werden
Skalierbarkeit	Weitere Nodes können ergänzt werden
Redundanz	Einzelne Ausfälle besser abfangen

Besonders wichtig sind:

Thema	Kerngedanke
Quorum	Eindeutige Entscheidung im Cluster
Witness	Hilft bei Mehrheitsentscheidung
Split-Brain	Gefährlicher Zustand bei Kommunikationsverlust
Ressourcenreserve	Notwendig für echtes Failover
Shared Storage	Praktisch, aber selbst kritisch
Backup	Weiterhin zwingend notwendig
Monitoring	Fehler früh erkennen
Dokumentation	Betrieb nachvollziehbar machen

Für die IHK ist besonders wichtig:

Prüfungsrelevanter Punkt	Bedeutung
Cluster erklären können	Mehrere Server arbeiten zusammen
Failover erklären können	Dienst übernimmt auf anderem System
Quorum verstehen	Verhindert falsche Mehrfachaktivität
Split-Brain kennen	Gefahr für Datenkonsistenz
Aktiv/Aktiv und Aktiv/Passiv unterscheiden	Unterschiedliche Clusterkonzepte
Cluster vs. Backup unterscheiden	Verfügbarkeit ist nicht Datensicherung
Ressourcenreserven beachten	Cluster muss Ausfall abfangen können

Der nächste logische Schritt ist:

Failover, Quorum und Split-Brain