

Failure-State Envelope

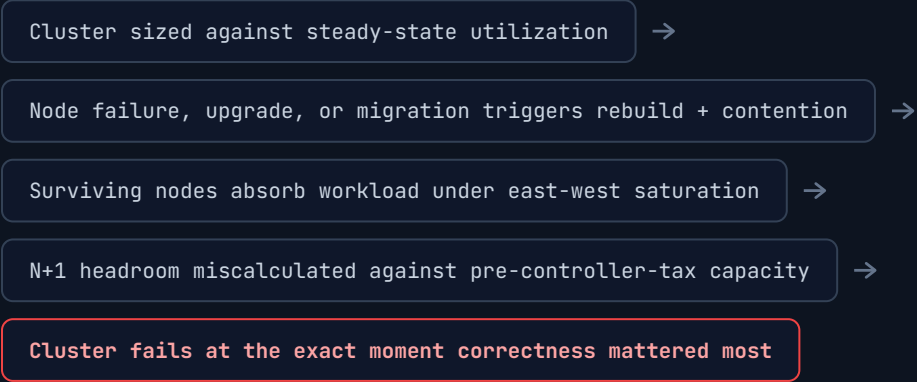
DEFINITION

The operational resource boundary an HCI cluster must be sized against — unifying controller tax, rebuild amplification, N+1 headroom, upgrade window buffer, migration burst capacity, and replication traffic into a single model — so the cluster remains deterministic during degraded conditions, not only at steady state.

FRAMEWORK FLOW

01 The Condition The cluster is sized against steady-state utilization — controller tax and replication traffic accounted for only at baseline, guest headroom calculated against nominal capacity.	02 The Boundary A node failure, rolling upgrade, or large-scale migration introduces rebuild amplification, controller contention, and reserve-capacity consumption simultaneously — the point where steady-state sizing and the Failure-State Envelope diverge.	03 Failure State Surviving nodes absorb the workload while rebuild traffic floods the east-west fabric alongside normal production writes; N+1 headroom calculated against total node capacity rather than post-controller-tax effective capacity proves insufficient.	04 Consequence A cluster that passed pre-production validation compounds into cascading instability during the exact window — failure, upgrade, or migration — when correctness mattered most; discovered mid-incident, not during sizing.
--	---	---	---

Failure State: Steady-State Sizing Collides With Failure-State Reality



THE DIAGNOSTIC SIGNAL

ENVELOPE OWNERSHIP Ask whether controller tax, N+1 headroom, or upgrade buffer is individually accounted for in the sizing model. The answer is usually yes — each input is modeled correctly on its own.	COMPOSITE OWNERSHIP Ask who owns the combined resource condition when rebuild amplification, controller contention, and reserve consumption occur simultaneously. The honest answer is nobody — the six inputs are modeled independently, never as one concurrent boundary.
TRIGGER CONDITION A node failure, rolling upgrade, or high-throughput migration is the activation condition — sizing that never has to survive one of these events never enters the envelope at all.	REMEDIATION SHAPE Model the envelope as a single unified sizing boundary before procurement — N+1 headroom calculated against post-controller-tax effective capacity, not total node capacity — architectural, not a bigger cluster.

THE SIX-INPUT SIZING MODEL

CONTROLLER TAX The CPU, memory, and network baseline consumed by the storage controller before any guest workload allocates resources.	REBUILD AMPLIFICATION The additional east-west traffic generated when a node fails and data protection rebuilds to the surviving nodes.
N+1 HEADROOM The spare capacity required to absorb a node loss without triggering cascading contention across the surviving fleet.	UPGRADE WINDOW BUFFER The additional controller contention created during rolling node evacuations — a scheduled event that shares the same resource math as an unscheduled failure.
MIGRATION BURST CAPACITY The replication saturation created when large workloads move onto the cluster, competing with baseline replication and guest I/O simultaneously.	REPLICATION TRAFFIC The baseline east-west load from the cluster's replication factor under normal production writes — the floor the other five inputs are added on top of.

ARCHITECTURAL RELATIONSHIPS

No relationships mapped Failure-State Envelope has no registered relationship_metadata at this time. Two candidate comparisons appear in adjacent source content (Governance Portability Gap, Fragmented Control Plane) but both attach to Platform Gravity — an unregistered concept in the same source's Cluster 05 — not to Failure-State Envelope itself. No relationship is asserted here on that basis.
ANCHOR /modern-virtualization-learning-path/hci-architecture/ FRAMEWORK HOME Platform-agnostic — the six-input envelope applies across HCI convergence models (Nutanix AHV, vSAN, Proxmox/Ceph) regardless of vendor-specific implementation.

"Every individual sizing input can be modeled correctly in isolation. Nobody can explain why the cluster fails under load — not because any input was neglected, but because the six inputs were never modeled as one boundary."