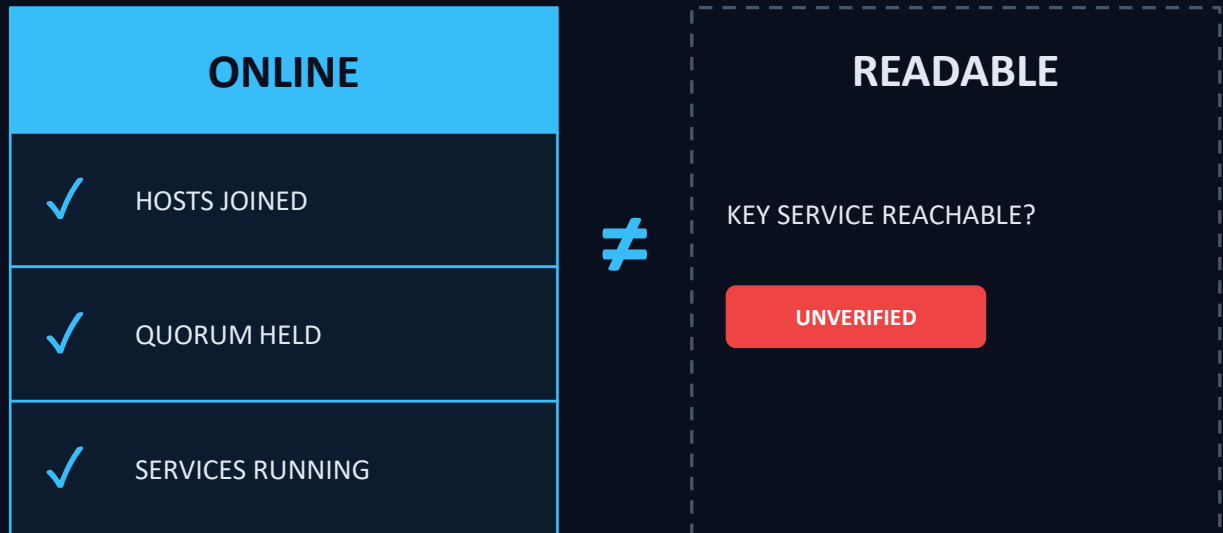


The cluster came back. The keys didn't.

A KMS circular dependency, as vSAN and Nutanix document it.

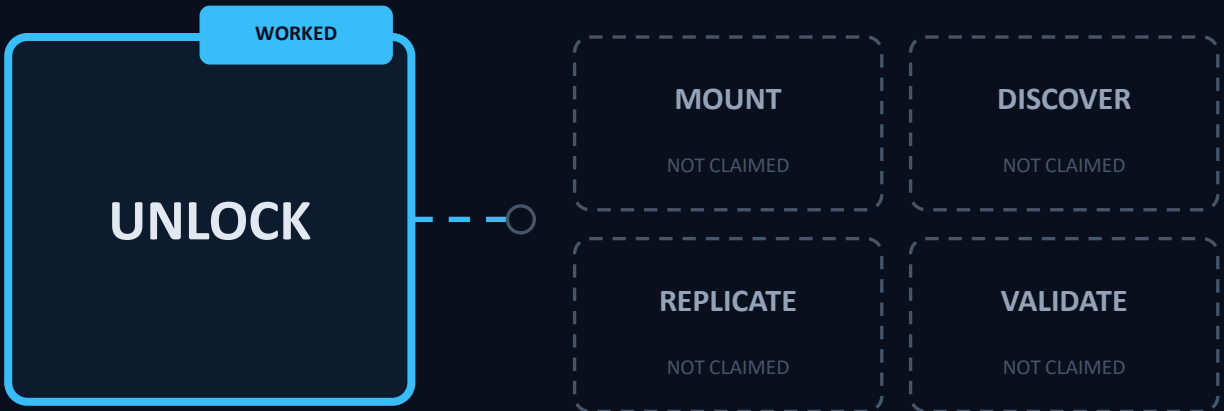


Online is not readable.



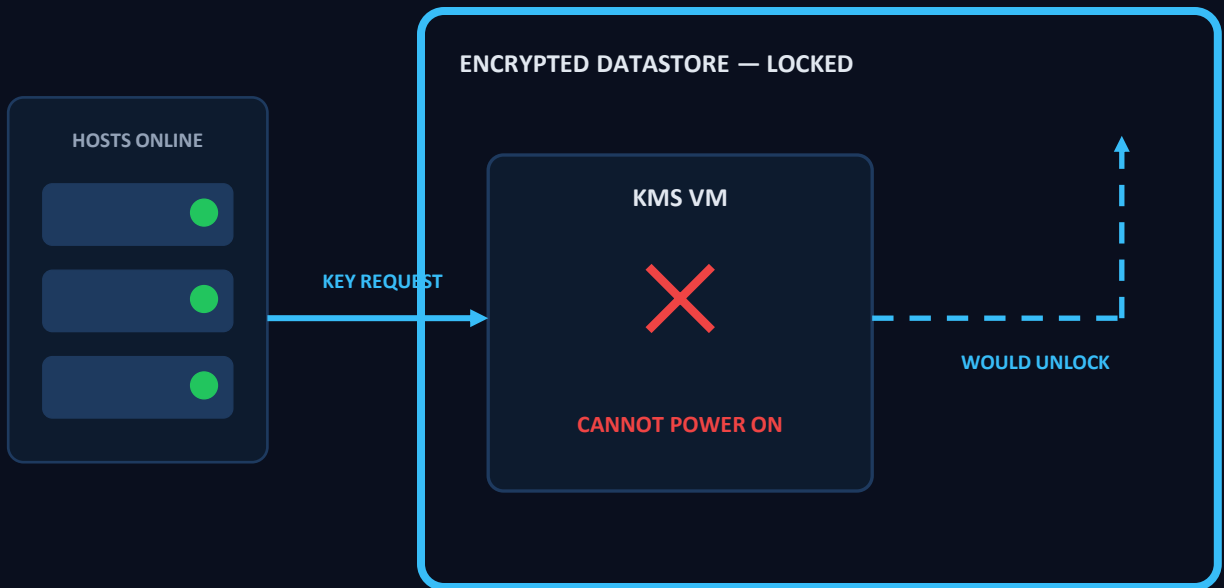
Coordination checks and key reachability are separate questions.

One function. Not five.



The post works unlock. Mount, discover, replicate, and validate are the same question, unclaimed.

vSAN documents the loop.



Hosts can't mount encrypted disk groups without the KMS. The KMS VMs can't power on from the locked datastore.

Broadcom KB 453198 · vSAN 8.x, 9.x

Nutanix documents the warning, not the sequence.

DEPENDENCY

The CVM retrieves keys from an external KMS.

DOCUMENTED

CONSEQUENCE

No correct keys, no data access (SED). A hosted KMS VM:
complete data loss.

DOCUMENTED

SEQUENCE

How a hosted-KMS startup unfolds.

NOT DOCUMENTED

Don't host the KMS VM on the encrypted cluster that uses it. No ranking follows.

Nutanix AOS Security 7.6 guide

Where does your KMS run?

DIAGNOSTIC QUESTION

If every host powered off at once, which service has to answer before the first datastore mounts, and where does it run?

Run it against your own cluster.

rack2cloud.com | Follow The Architect for more