HyperSphere DNA™ for AWS

AWS Deployment Guide

Customer-Deployed Reference Architecture for
AWS Marketplace and Foundational Technical Review

Version 1.1

HyperSphere Technologies, Inc.

support@hyperspheretech.com | security@hyperspheretech.com

www.hyperspheretech.com/terms

1. Introduction

This document is the official AWS Deployment Guide for HyperSphere DNA™ (Data Neutralization Appliance) for AWS. It satisfies the AWS Customer-Deployed Foundational Technical Review (FTR) and is the single source of truth for customers deploying HyperSphere from AWS Marketplace into their own AWS account.

FTR requirements addressed: INT-001 through INT-005.

1.1 Product Overview and Use Cases

HyperSphere DNA is an S3-compatible encryption proxy that transparently encrypts every object at rest with AES-256-GCM and manages the full key lifecycle. No data-encryption key is ever persisted. Keys are derived on demand within a hierarchy rooted in a system key that only exists in memory after a k-of-n VSSS unseal at boot.

Primary use cases:

- Regulated industries (financial services, healthcare, public sector) needing cryptographic separation of key material from ciphertext.
- Developers replacing bespoke envelope-encryption code with a drop-in S3-compatible API.
- Security teams consolidating on a single key-governance model across multiple buckets and accounts.
- Organizations seeking a no-persistent-data-keys architecture that limits blast radius if any node or bucket is compromised.

1.2 Typical Deployment Resource List

AWS Resource	Purpose	Typical count
Amazon VPC	Network isolation	1 per region
Private subnet(s)	Host the HyperSphere node(s)	1-2
Public subnet (optional)	NAT / egress for OS patching	1
EC2 instance (node)	Runs the HyperSphere AMI (Ubuntu 24.04, IMDSv2-only)	1
EC2 instance (portal)	Optional management portal AMI	0-1
S3 bucket(s)	Customer-owned storage targets for encrypted frames + sealed metadata	1+ (customer-owned)
Security groups	Restrict ingress to S3 API / admin ports	1-2
IAM role (instance profile)	Scoped node permissions	1
IAM role (deployment)	Assumed by operator to launch/provision	1
AWS Secrets Manager (optional)	Only if gated cloud auto-unseal is enabled	0-1
CloudWatch Log Group (optional)	Only if customer runs the CloudWatch agent	0-1
EBS volume	Node root + local state (50 GB gp3, encrypted)	1 per node

Note

No ALB, no ASG beyond size-1 for auto-recovery, no NAT Gateway required by default.

1.3 Deployment Options

Option	Summary	When to use
A. Single node (shipping)	One node in one AZ. Encrypted data survives node loss on the customer's S3 target. Recovery = rebuild-from-AMI + re-unseal.	All current production and non-production deployments.
B. Warm standby (roadmap)	Active/passive (WAL-tail, fencing, lease-gated promotion). Implemented in engine; not yet operator-configurable.	Planned for a future release. Do not rely on it for availability.
C. Independent regional	Separate single-node stacks per region with S3 Cross-Region Replication.	Global applications needing regional independence.

1.4 Expected Deployment Time

- Option A (single node): ~30 minutes with prerequisites met.
- Option C (per-region): ~30 minutes per region plus S3 replication configuration.
- Option B: not applicable in this release.

1.5 Supported AWS Regions

All AWS commercial regions where EC2, S3, VPC, and IAM are generally available. CloudWatch, Secrets Manager, and KMS are used only if the customer opts into the corresponding optional integration. AWS GovCloud (US), AWS China, and Secret/Top Secret regions are out of scope at launch.

1.6 Usage Instructions (AWS Marketplace)

The following step-by-step instructions are submitted to the AWS Marketplace Usage Instructions field and reproduced here as the canonical quick-start reference.

Documentation URL

Full deployment guide, CloudFormation templates, and API reference:
https://hyperspheretech.com/docs

Overview

HyperSphere DNA deploys as a single EC2 instance (Ubuntu 24.04 AMI) inside your VPC. It acts as an S3-compatible encryption proxy: your application writes to HyperSphere using standard S3 API calls, and every object is encrypted with AES-256-GCM before being stored in your own Amazon S3 bucket. No plaintext ever leaves the node. No encryption key is ever persisted.

Step 1 — Subscribe and Launch

Subscribe to the tier that matches your workload (Developer: t3.medium / Team: m7i.large / Business: m7i.xlarge / Capacity: m7i.2xlarge / Enterprise: Private Offer). Launch the AMI into a private subnet. Attach the provided least-privilege IAM instance profile and a 50 GB encrypted gp3 EBS volume. IMDSv2 is required and enforced by the AMI.

Step 2 — First-Boot Configuration

SSH into the instance and run:

```
sudo /opt/securestorage/setup.sh
```

This script activates your license, configures your Amazon S3 storage target, sets up your OIDC identity provider (Okta, Azure AD, Google Workspace, or Keycloak), generates the VSSS key shares, configures Nginx with TLS, and starts the ss-worker service. Alternatively, deploy using the provided CloudFormation template or Ansible playbooks (see hyperspheretech.com/docs).

Critical

The setup script displays per-custodian VSSS key-share files once. Record them securely and distribute to independent custodians. Loss of fewer than k shares (minimum k = 4) makes encrypted data permanently unrecoverable.

Step 3 — Unseal

HyperSphere boots in a sealed state. After every reboot, present the required number of VSSS shares (minimum 4) to reconstruct the root encryption key in memory:

```
ssctl unseal --share-file <custodian-share.toml>
```

Repeat for each custodian until the threshold is met. The node then transitions to ready state and begins accepting S3 API traffic.

Step 4 — Create a Vault and Connect Your Application

Use the bundled web console (https://<node-ip>/) or the ssctl CLI to create a vault, attach your Amazon S3 bucket as a storage target, and mint S3 access keys. Point your application's S3 endpoint at https://<node-ip>/ — no other code changes are required. All encryption and decryption are transparent.

Health Check

```
curl -ks https://<node-ip>/health        # returns {status:ok,sealed:false} when ready
curl -ks https://<node-ip>/health/ready  # returns 200 OK when accepting S3 traffic
```

If sealed:true is returned, complete Step 3. Monitor the node using the bundled Prometheus and Grafana dashboards at https://<node-ip>/grafana/

2. Prerequisites and Requirements

FTR requirements addressed: PRQ-001, PRQ-002, PRQ-003.

2.1 Technical Prerequisites

HyperSphere ships as a hardened Ubuntu 24.04 AMI. Customers do not supply an OS, database, or web server.

Layer	Component	Notes
Operating system	Ubuntu 24.04 LTS (hardened)	CIS-aligned baseline; systemd-sandboxed worker
Storage/crypto engine	ss-worker, ssctl, ss-cli	Core S3 proxy + admin CLI + data-plane CLI
Reverse proxy / TLS	Nginx	TLS 1.3 termination in front of the worker (HSTS)
Observability	Prometheus + Grafana	Bundled behind nginx basic-auth; worker exposes /metrics
Management console	React SPA (node console)	Ships with node AMI; separate portal AMI for multi-node

Note The AMI does NOT bundle PostgreSQL, an identity provider, or a production object store. A local MinIO sidecar (127.0.0.1:9100) is present for bootstrap only and is replaced by the customer's S3 targets at first boot.

2.2 Required Skills

- Working familiarity with AWS (VPC, EC2, IAM, S3).
- Ability to deploy the provided CloudFormation template or Ansible playbooks, or to run the first-boot setup.sh script.
- Familiarity with AWS CLI v2. Basic Linux administration.

No cryptographic expertise is required; key lifecycle, derivation, and VSSS unseal are handled by the software.

2.3 Environment Configuration

1. A non-root AWS principal with the deployment IAM role attached.
2. A workstation with AWS CLI v2 (and Ansible if using the Ansible path).
3. Network reachability from the workstation to the AWS control plane.
4. Outbound connectivity from the HyperSphere subnet(s) to S3, the OIDC provider, and the license/telemetry endpoint.
5. A DNS name for the node (for TLS via ACM or Let's Encrypt).

2.4 Shared Responsibility Model

Responsibility	AWS	Hyperspheretech	Customer
Physical infra, hypervisor, network	Owns	n/a	n/a
AMI contents (OS, binaries, hardening)	n/a	Builds, signs, scans, republishes	Selects AMI; does not modify it
OS patching	n/a	Monthly patched AMIs; emergency within 24h of CVSS >= 9.0	Rolls nodes to new AMI in a change window
IAM roles / least privilege	Provides IAM	Ships least-privilege policy templates	Reviews, approves, provisions
VPC / network boundary	Provides VPC	Documents required ports (§4.9)	Owns the network boundary and egress
OIDC identity provider	n/a	Documents required OIDC config	Operates the IdP
VSSS share custody	n/a	Provides dealing ceremony (ssctl)	Distributes and safeguards shares
Customer data	Durable S3 substrate	Client-side AEAD + sealed metadata frame	Classification, retention, residency, deletion
Monitoring / audit	CloudWatch / CloudTrail	Prometheus + Grafana + HMAC-chained audit log	Reviews dashboards; optionally forwards to CloudWatch/SIEM

3. Architecture

FTR requirements addressed: ARCH-001, ARCH-004, ARCH-005, ARCH-006.

3.1 Single-Node Deployment Topology

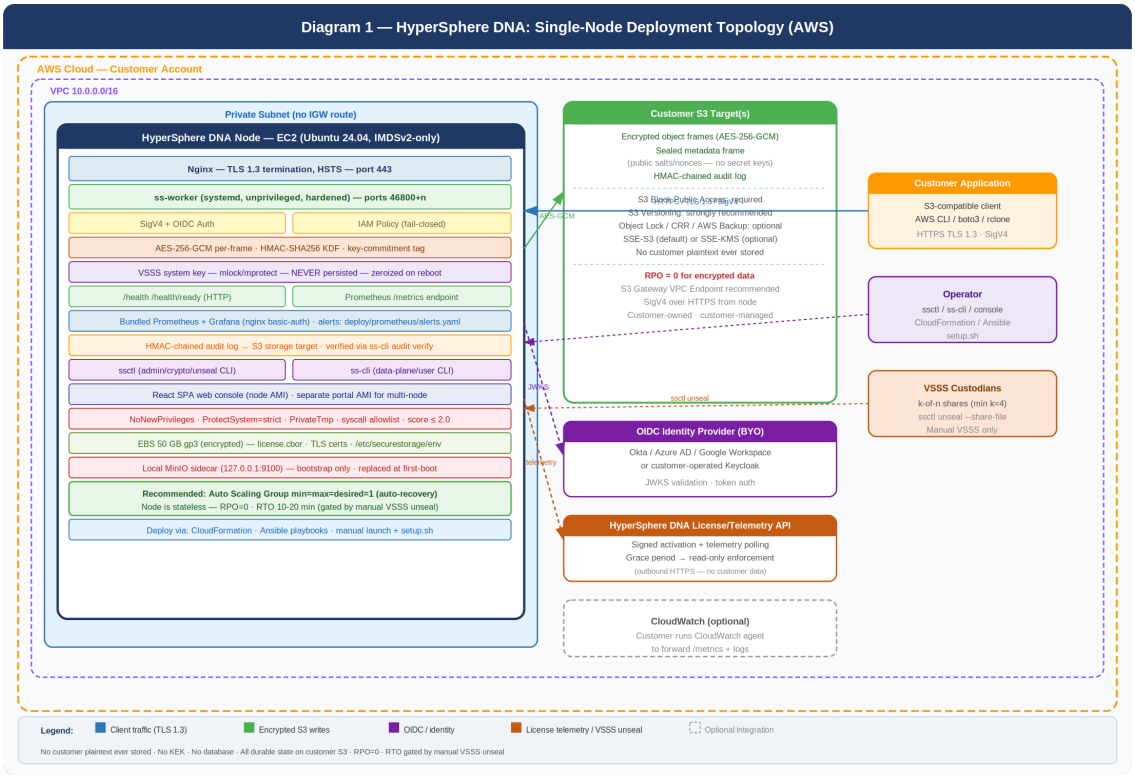

Figure 1: Single-Node Deployment Topology on AWS

3.2 Cryptographic Key Hierarchy

No data-encryption key is persisted. At boot, the operator supplies k of n VSSS shares; the system key is reconstructed in mlock/mprotect-protected memory. All lower keys are HMAC-SHA256 derived on demand and zeroized after use. There is no KEK and no wrapped key material.

```
system_key  (VSSS k-of-n reconstructed at boot; mlock/mprotect; NEVER persisted)
  HMAC-SHA256(system_key, 'vault_key' || vault_id || vault_salt) -> vault_key
  HMAC-SHA256(vault_key, 'SS/fmk/v2', version_nonce)             -> FileMasterKey
  HMAC-SHA256(FMK, 'frame_key'|'frame_nonce', frame_index)       -> frame_key/nonce
```

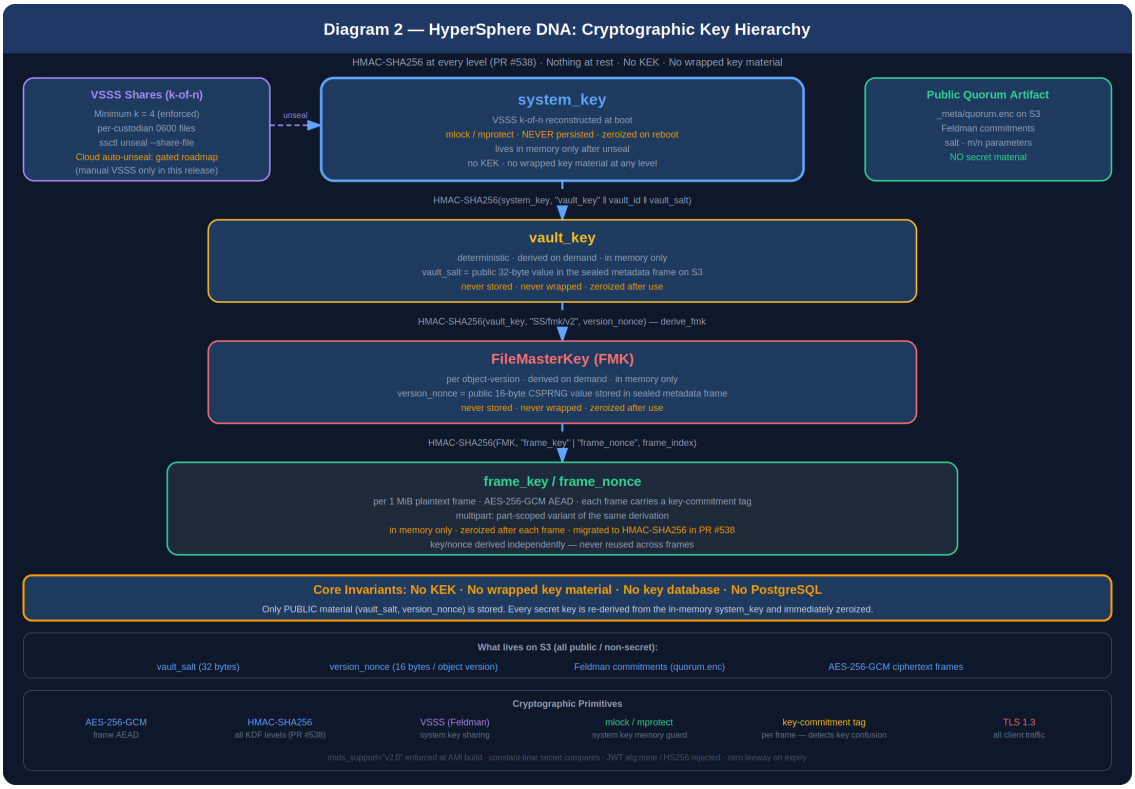

Figure 2: Cryptographic Key Hierarchy — HMAC-SHA256 derived, nothing at rest

3.3 Deployment Options and Recovery Model

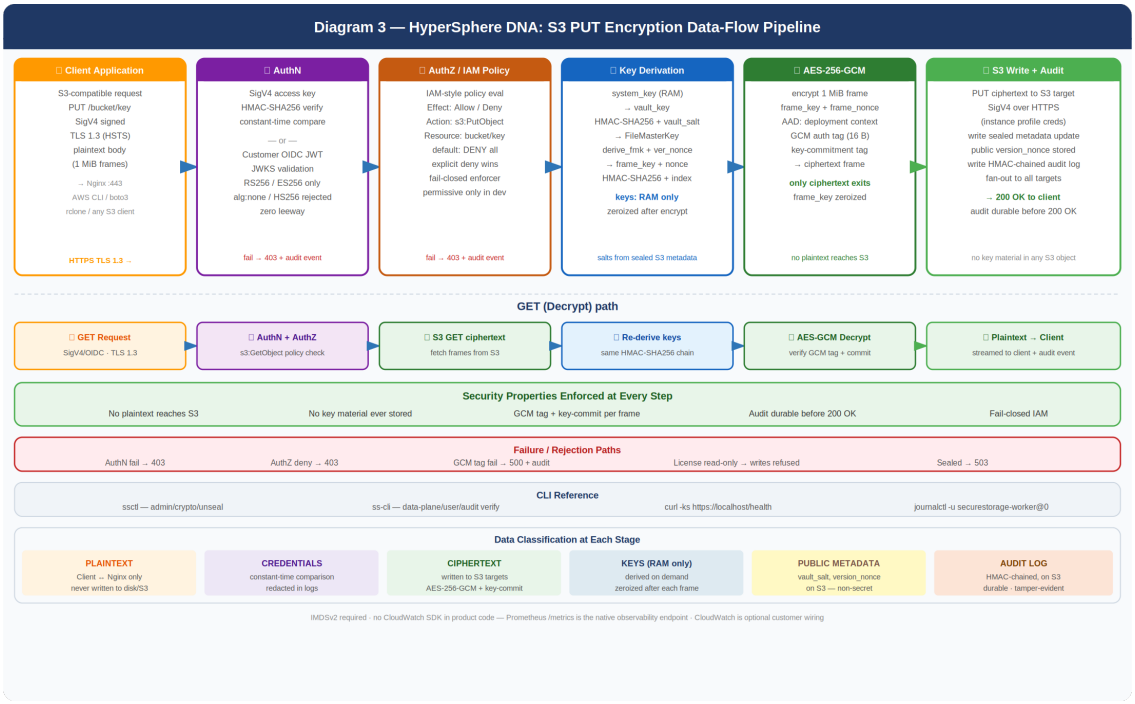

Figure 3: Deployment Options, Sizing, and Backup/Recovery Model

3.4 Data Flow Pipeline

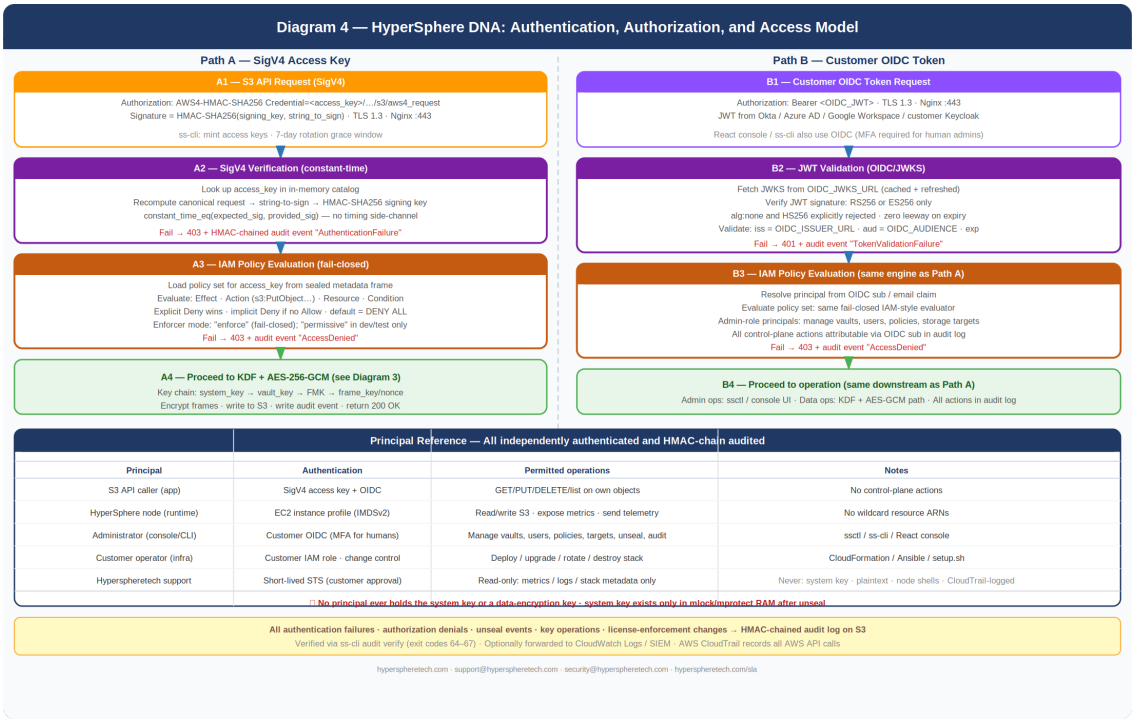

Figure 4: S3 PUT Encryption Data-Flow Pipeline

3.5 Single-Node Topology (Option A — Shipping)

The node holds no durable state (all encrypted data, sealed metadata, and the audit log live on the customer's S3 target). RPO is zero. Run the node in an ASG with min=max=desired=1 for auto-replacement.

3.6 Warm Standby (Option B — Roadmap)

Roadmap The warm-standby design is implemented in crates/engine/src/ha/ but is NOT wired into the running appliance in this release. Do not plan production availability around it.

3.7 Independent Regional Deployments (Option C)

Deploy independent HyperSphere stacks per region with S3 Cross-Region Replication. HyperSphere initiates no cross-region traffic. Each region has a distinct system key and VSSS share set.

3.8 Integration Points

Integration point	Direction	Protocol	Scope
Customer S3-compatible API	Customer to HyperSphere	HTTPS (TLS 1.3)	GET/PUT/DELETE/list on encrypted objects
Upstream S3 target	HyperSphere to S3	SigV4 over HTTPS	Read/write encrypted frames + sealed metadata
OIDC provider	HyperSphere to IdP	OIDC/HTTPS	Token validation (JWKS)

Integration point	Direction	Protocol	Scope
Prometheus scrape	Prometheus to HyperSphere	HTTP /metrics	Metrics (bundled Prometheus/Grafana)
License/telemetry endpoint	HyperSphere to Hypersphere API	HTTPS (signed)	Activation, telemetry, enforcement polling
CloudWatch (optional)	CloudWatch agent to CloudWatch	AWS API/HTTPS	Optional customer forwarding of metrics/logs
Secrets Manager (optional, gated)	HyperSphere to Secrets Manager	AWS API/HTTPS	Only if gated cloud auto-unseal is enabled

3.9 Data Residency

- Deployed entirely inside the customer's AWS account. No HyperSphere-owned data plane.
- Encrypted frames and sealed metadata reside only in the customer-provided S3 target(s).
- The only outbound telemetry is the signed license check-in — no object data or key material.

4. Security

FTR requirements addressed: DSEC-002 through DSEC-012.

4.1 Non-Root Deployment (DSEC-002)

HyperSphere is never deployed as the AWS account root user. The worker runs as the unprivileged securestorage system user under systemd with NoNewPrivileges=yes, ProtectSystem=strict, PrivateTmp, PrivateDevices, and a syscall allowlist (hardening score <= 2.0).

4.2 Least-Privilege IAM (DSEC-003)

- Instance profile: S3 object read/write scoped to declared target bucket(s); outbound HTTPS to license endpoint; CloudWatch/Secrets Manager only if opted in.
- Policy ships as deploy/iam/securestorage-target-policy.json, wired into the CloudFormation template.
- No IAM user credentials in the AMI. Runtime credentials via IMDSv2 instance profile only.

4.3 Public Resources (DSEC-004)

- No public-read/write S3 bucket policies. Target bucket must have S3 Block Public Access enabled.
- No public IPv4 required on the node for in-VPC clients.

4.4 IAM Roles (DSEC-005)

IAM construct	Purpose	Principal	Scope
HyperSphereNodeRole	Runtime role for EC2 node	ec2.amazonaws.com	S3 object verbs on target bucket(s); optional CloudWatch/Secrets Manager only if in use
HyperSphereDeploymentRole	Operator launch/provision	Customer administrator	Scoped CRUD on EC2, VPC, IAM
HyperSphereBackupRole (optional)	AWS Backup snapshots	backup.amazonaws.com	ec2:CreateSnapshot/CopySnapshot on HyperSphere volumes

4.5 Key Management (DSEC-006)

Key	Purpose	Location	Customer action
System key	Root of hierarchy; reconstructed from VSSS shares	Memory only (mlock/mprotect) after unseal	Custody the shares; supply k at unseal
Vault key	Per-vault derivation key	Memory only; HMAC-SHA256-derived	None
FileMasterKey	Per object-version key	Memory only; derived on demand	None
Frame key / nonce	Per-frame AEAD key and nonce	Memory only; zeroized after each frame	None

Key	Purpose	Location	Customer action
VSSS share	One share of k-of-n	Custodian custody (offline 0600 file)	Distribute to independent custodians; supply k at unseal

Key invariant No KEK and no per-object wrapped key. Only public salts/nonces are stored on S3.

4.6 Secret Rotation (DSEC-007)

- Manual VSSS (ssctl unseal --share-file) is the only non-gated unseal path. Cloud auto-unseal is compile-time gated.
- ssctl crypto credential-rewrap re-seals stored storage-target credentials. System-key rotation-with-re-encryption is a roadmap item.

4.7 Data Storage Locations (DSEC-008)

Data class	Storage location	Encryption at rest
Encrypted object frames	Customer-owned S3 target	AES-256-GCM (HyperSphere) + S3 SSE
Sealed metadata frame (public salts/nonces; no secret keys)	Customer-owned S3 target	HyperSphere AEAD + S3 SSE
Audit logs (HMAC-chained)	Customer S3 target; optionally CloudWatch/SIEM	HyperSphere AEAD + S3 SSE
Node config (license.cbor, TLS certs, env)	Node EBS volume	EBS encryption (customer-managed KMS)

4.8 Encryption Configuration (DSEC-009)

- AES-256-GCM per 1 MiB object frame. Each frame carries a key-commitment tag.
- S3 SSE on the target bucket (SSE-S3 default; SSE-KMS with customer-managed key supported).
- EBS encryption on node volumes with customer-managed KMS key by default.
- TLS 1.3 for all client-to-node traffic (HSTS). Replace the self-signed default with ACM or Let's Encrypt for production.

Warning Do not run production on the self-signed TLS default.

4.9 Network Configuration (DSEC-010)

Construct	Purpose	Default
VPC	Isolation boundary	10.0.0.0/16 (customer-configurable)
Private subnet(s)	Host the node(s)	No default route to IGW
Security group (node)	Restrict ingress	Ingress 443 from app CIDR; SSH 22 from admin CIDR only; egress to S3/OIDC/license

Construct	Purpose	Default
VPC endpoints	Keep S3 traffic on AWS network	Gateway endpoint for S3 recommended

4.10 IMDSv2 Enforcement (DSEC-011)

AMI built with imds_support='v2.0'. Set HttpTokens=required, HttpEndpoint=enabled, HttpPutResponseHopLimit=1 on launch. Audit drift with AWS Config.

4.11 Credential Provider Chain (DSEC-012)

Standard AWS credential provider chain only: (1) env vars; (2) shared credentials; (3) container credentials; (4) EC2 IMDSv2. No credentials hard-coded. Never use long-lived IAM user keys for S3 targets.

4.12 Access Model and Principals

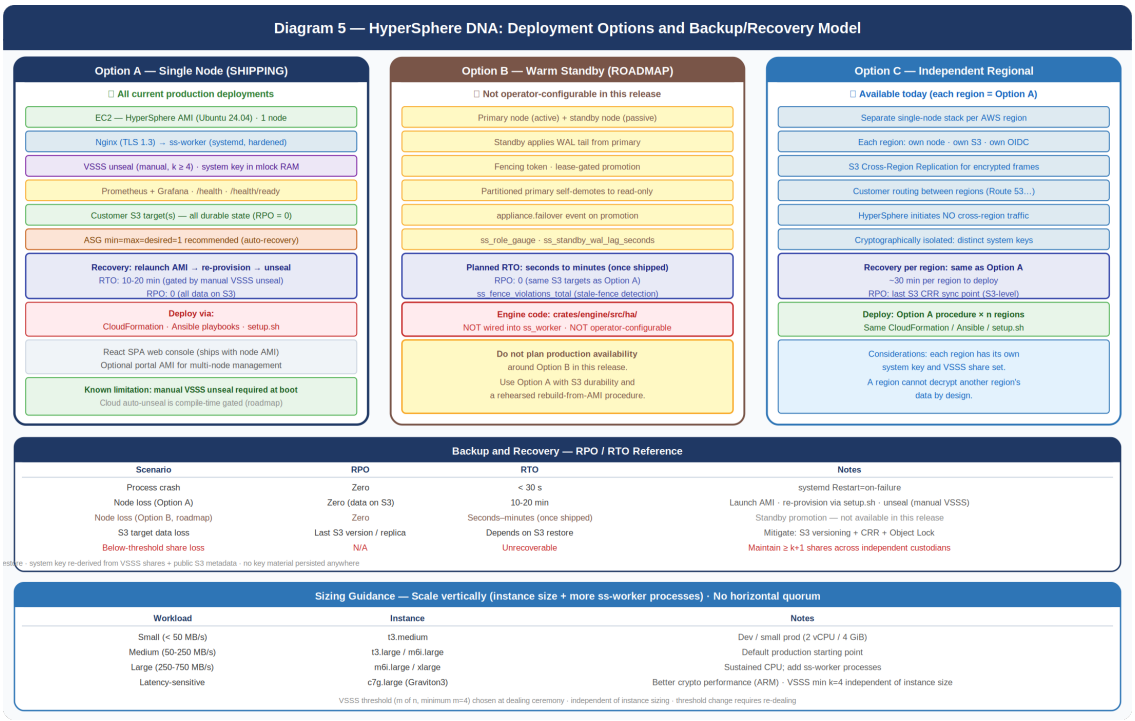

Figure 5: Authentication, Authorization, and Access Model

4.13 Logging and Audit

Category	What is recorded	Destination	Optional forwarding
Tamper-evident audit log	Auth failures, unseal events, AuthZ denials, license-enforcement changes (HMAC-chained)	Customer S3 target; verified via ss-cli audit verify (exit codes 64-67)	CloudWatch Logs / SIEM
Application/access events	S3 operations, caller, salted key hash, frame count, latency, outcome	Structured worker logs (journald)	CloudWatch Logs / SIEM

Category	What is recorded	Destination	Optional forwarding
Operational metrics	Request rate, error rate, S3 latency, seal state	Prometheus /metrics; bundled Grafana	Amazon Managed Prometheus / CloudWatch
AWS API-call activity	Every AWS API call the node makes	AWS CloudTrail (automatic)	CloudTrail Lake

5. Costs and Licensing

FTR requirements addressed: CST-001, CST-002.

5.1 Billable AWS Services

AWS service	Mandatory?	Cost driver
Amazon EC2 (node)	Mandatory	Instance-hours — tier determines instance type (see §5.2)
Amazon EBS (node volume)	Mandatory	50 GB gp3 per node
Amazon S3 (encrypted frames + metadata)	Mandatory	GB-month + request counts
VPC endpoints	Recommended	Interface-endpoint hours + data processed
Amazon CloudWatch (optional)	Optional	Only if customer runs the CloudWatch agent
NAT Gateway	Optional	Omit if using VPC endpoints only
AWS Secrets Manager	Optional	Only if gated cloud auto-unseal is used
AWS KMS	Optional	Customer-managed keys for EBS and S3 SSE-KMS
AWS Backup	Optional	Backup storage + restore

For a single-node Business tier deployment (m7i.xlarge, ~1 TB/month), typical AWS infrastructure cost is USD 200-350/month depending on region and data transfer.

5.2 HyperSphere Licensing

HyperSphere DNA is licensed per node per hour through AWS Marketplace, billed by tier. The tier determines the instance type and maximum data band.

Tier	Developer	Team	Business	Capacity	Enterprise / Gov
Instance	t3.medium	m7i.large	m7i.xlarge	m7i.2xlarge	Custom
Data band	10 GB	100 GB	1 TB	10 TB	Unlimited / custom
License $/node/hr	$0.35	$1.25	$2.95	~$5.50 (TBC)	Private Offer
Min / rec nodes	1 / 1	2 / 2	2 / 3	2 / 3	Custom

Tier notes:

- Developer (t3.medium, 10 GB): development and evaluation only — not recommended for production.
- Team (m7i.large, 100 GB): small production workloads; minimum 2 nodes recommended.
- Business (m7i.xlarge, 1 TB): standard production; minimum 2, recommended 3 nodes.
- Capacity (m7i.2xlarge, 10 TB): high-throughput; ~$5.50/node/hr pricing TBC at GA.

- Enterprise / Gov: custom instance, unlimited/custom data band, Private Offer — contact sales@hyperspheretech.com.

License mechanics:

- Appliance activates at first boot against the Hypersphere license API (writes signed license.cbor).
- Periodic signed telemetry polling; enforcement state updated on each cycle.
- On expiry: grace period, then read-only enforcement (writes refused, reads served).
- Exceeding the tier's data band triggers enforcement — upgrade to the next tier to resolve.

6. Sizing Guidance

FTR requirement addressed: SIZ-001.

Each tier maps to a specific instance type and data band. Within a tier, throughput scales by adding ss-worker processes (ports 46800+n). HyperSphere does not scale horizontally by adding quorum members.

Tier	Instance	Data band	$/node/hr	Min / rec nodes	Use case
Developer	t3.medium	10 GB	$0.35	1 / 1	Development and evaluation
Team	m7i.large	100 GB	$1.25	2 / 2	Small production workloads
Business	m7i.xlarge	1 TB	$2.95	2 / 3	Standard production
Capacity	m7i.2xlarge	10 TB	~$5.50 (TBC)	2 / 3	High-throughput production
Enterprise / Gov	Custom	Unlimited / custom	Private Offer	Custom	Large-scale / regulated / custom SLA

Note VSSS threshold (minimum m = 4) is chosen at the dealing ceremony and is independent of tier and instance sizing.

Upgrade path Subscribe to the new tier on Marketplace, relaunch on the tier-appropriate instance, re-provision against the same S3 target(s), and unseal. Data is preserved (RPO = 0).

7. Deployment Assets

FTR requirements addressed: DAS-001, DAS-004.

7.1 Step-by-Step Deployment

Step 1 — Subscribe on AWS Marketplace

Sign in as a non-root IAM principal. Subscribe to HyperSphere DNA at your chosen tier, accept the EULA, select the AMI and target region.

Step 2 — Deploy the node

Path A: CloudFormation (recommended):

```
aws cloudformation deploy \
  --stack-name securestorage-prod \
  --template-file deploy/cloudformation/securestorage-node.yaml \
  --capabilities CAPABILITY_IAM \
  --parameter-overrides AmiId=<ami-id> VpcId=<vpc-id> \
      PrivateSubnetId=<subnet-id> StorageBucketName=<bucket> \
      AppClientCidr=<cidr> AdminCidr=<cidr>
```

Path B: Ansible — run deploy/ansible/ playbooks against an EC2 instance launched from the HyperSphere AMI.

Path C: Manual — launch AMI, attach security group (443 from app CIDR, SSH 22 from admin CIDR), attach instance profile, allocate 50 GB gp3 EBS (encrypted).

Step 3 — First-boot configuration (setup.sh)

6. Activate appliance against the license API (writes license.cbor).
7. Write /etc/securestorage/env with S3 target and OIDC configuration (OIDC_ISSUER_URL, OIDC_JWKS_URL, OIDC_AUDIENCE).
8. Run the ssctl dealing ceremony to produce VSSS shares.

Critical Record the VSSS shares securely — they are shown once. Lose fewer than k shares and you lose access to your data.

9. Configure Nginx + TLS (pass --tls letsencrypt for production; or terminate TLS at an ALB with ACM).
10. Enable and start the ss-worker systemd service.

Step 4 — Unseal

```
ssctl unseal --share-file <custodian-share.toml>
```

Repeat until the k-of-n threshold is met (minimum k = 4). The S3 API then becomes available.

Step 5 — Create vaults and access keys

Use the React SPA console or ssctl to create a vault, attach S3 target(s), and mint S3 access keys.

Step 6 — Configure your S3 client

Point AWS CLI, boto3, rclone, or any S3-compatible client at the HyperSphere endpoint (Nginx on 443). All data is transparently encrypted on write and decrypted on read.

7.2 Testing and Troubleshooting

11. Health check: curl -ks https://localhost/health
12. Round-trip encrypt/decrypt test.
13. Audit chain: ss-cli audit verify
14. Worker logs: journalctl -u securestorage-worker@0
15. Confirm Prometheus /metrics and Grafana dashboards are populated.

Symptom	Likely cause	Resolution
{status:ok, sealed:true}	Not unsealed after reboot	Run ssctl unseal --share-file with k custodian shares
S3 client 403 Forbidden	Invalid access key/secret	Verify with ss-cli storage-target list-access-keys --vault <n>
SignatureDoesNotMatch	Clock skew > 15 min	Sync NTP on both sides
Connection refused on 443	Nginx not running / TLS misconfig	systemctl status nginx; check error.log
Writes refused, reads work	License grace expired or data band exceeded	Renew or upgrade tier; confirm telemetry egress
Threshold not met on unseal	Fewer than k valid shares supplied	Provide additional shares (minimum k = 4)
High latency	Instance undersized for tier	Upgrade to next tier; add ss-worker processes

8. Health Checks and Monitoring

FTR requirement addressed: HLCH-001.

16. Grafana (nginx basic-auth): confirm request/error rate, S3 latency, seal state dashboards.
17. Prometheus: confirm scraping /metrics; no alert rules in deploy/prometheus/alerts.yaml firing.
18. Health endpoints: GET /health returns 200 (running); GET /health/ready returns 503 until unsealed.
19. journalctl -u securestorage-worker@0 for errors; ss-cli audit verify for audit chain integrity.

CloudWatch CloudWatch is an optional customer integration. The appliance exposes Prometheus /metrics natively. Run the CloudWatch agent to forward metrics and logs. AWS CloudTrail automatically records all AWS API calls made by the node.

9. Backup and Recovery

FTR requirement addressed: BAR-001.

Data store	Backup mechanism	Recovery
Encrypted object frames	S3 versioning, replication, Object Lock, AWS Backup	S3 version restore / replica
Sealed metadata frame (public salts/nonces; no secret keys)	Same S3 protections as object frames	Hydrated at boot from S3 target
VSSS shares	Custodian custody (offline 0600 files)	Custodians supply k shares to ssctl unseal
Node config (license.cbor, TLS certs, env)	EBS snapshot, or re-provision via setup.sh	Restore snapshot or re-run first boot
Audit logs	S3 target; optionally CloudWatch/SIEM	Restored with S3 target; verified via ss-cli audit verify

Scenario	RPO	RTO	Notes
Process crash	Zero	< 30 s	systemd Restart=on-failure
Node loss (Option A)	Zero for encrypted data	10-20 min	Launch new AMI, re-provision, unseal
Node loss (Option B, roadmap)	Zero	Seconds to minutes (once shipped)	Not available in this release
S3 target data loss	Last S3 version/replica	Depends on S3 recovery	Mitigate with versioning / CRR / Object Lock
Below-threshold share loss	N/A	Unrecoverable	Maintain >= k+1 shares across independent custodians

10. Routine Maintenance

FTR requirements addressed: RM-001, RM-002, RM-003, RM-004.

10.1 Credential and Key Rotation (RM-001)

Credential / key	Cadence	How
S3 access keys	Per policy	ss-cli or console; 7-day rotation grace window
VSSS shares (re-dealing)	Per policy or custodian change	ssctl dealing ceremony
ssctl crypto credential-rewrap	Per policy	Re-seals stored storage-target credentials
Node TLS certificate	Annually or as required	ACM renewal or Let's Encrypt
Instance-profile credentials	Automatic (hourly)	EC2 IMDSv2 refresh; no operator action required

10.2 Software Patches and Upgrades (RM-002)

Patched AMIs published monthly; emergency AMIs within 24h of CVSS >= 9.0 fix. Upgrade: subscribe to release notifications, launch from new AMI, provision against same S3/OIDC config, unseal, verify, cut traffic over.

10.3 License and Tier Management (RM-003)

- Keep the Marketplace subscription active at the correct tier.
- Monitor data band usage; upgrade before the limit is reached. Exceeding triggers enforcement.
- Ensure outbound HTTPS to the license/telemetry endpoint; sustained failure triggers read-only enforcement after the grace period.
- Tier upgrade: subscribe to new tier, relaunch on tier-appropriate instance, re-provision, unseal. Data preserved (RPO = 0).

10.4 AWS Service Limits (RM-004)

Review before deployment: EC2 vCPUs for the instance family, VPCs per region, security groups per VPC. If optional integrations are used: CloudWatch log groups (+1), Secrets Manager secrets (+1), KMS keys (+1).

11. Emergency Maintenance

FTR requirements addressed: EMER-001, EMER-002.

11.1 Fault Handling (EMER-001)

Fault	Symptoms	Runbook
Worker unhealthy	/health failing	Inspect journalctl; systemd auto-restarts; confirm S3 target reachable
Node unreachable	/health failing; node down	Rebuild from AMI, re-provision against same S3 target(s), re-unseal (§11.2)
Sealed after reboot	sealed:true; /health/ready 503	ssctl unseal --share-file with k custodian shares
License enforcement	Writes refused	Reactivate/upgrade license; restore telemetry egress
Data band exceeded	Writes refused	Upgrade to next tier on Marketplace; relaunch on tier instance
Catalog boot-check failure	Worker refuses to serve	Confirm S3 target/metadata intact; SS_CATALOG_SKIP_BOOT_CHECK=1 for supervised DR only

11.2 Software Recovery (EMER-002)

20. Re-subscribe on Marketplace if lapsed.
21. Launch fresh node from AMI; run setup.sh with same S3 target(s) and OIDC configuration.
22. Unseal with k VSSS shares (ssctl unseal --share-file).
23. Verify: curl -ks https://localhost/health, worker journal, sample encrypt/decrypt round trip.

Full recovery typically takes 15-30 minutes.

12. Support

FTR requirements addressed: SUP-001, SUP-002, SUP-003.

12.1 How to Receive Support

Open a case via support.hyperspheretech.com, email support@hyperspheretech.com, or AWS re:Post (tag hyperspheretech). Security issues: security@hyperspheretech.com.

12.2 Support Tiers

Tier	For	Channels	Coverage
Standard (included)	All Marketplace customers	Portal, email, re:Post, docs	Business hours, Mon-Fri
Premium	Production deployments	Portal, email, chat, phone	24x7 for Sev-1/2; business hours for Sev-3/4
Enterprise	Committed customers with a named TAM	Portal, email, chat, phone, named TAM	24x7 for Sev-1 through Sev-3

12.3 Service Level Agreements

Tier	Sev-1	Sev-2	Sev-3	Sev-4
Standard	4 business hours	8 business hours	Next business day	3 business days
Premium	2 hours	4 hours	8 business hours	2 business days
Enterprise	1 hour	2 hours	4 business hours	1 business day

Full SLA: hyperspheretech.com/sla

Appendix A — FTR Requirement Traceability Matrix

Requirement ID	Section
INT-001 .. INT-005	§1.1 – §1.6
PRQ-001 .. PRQ-003	§2.1 – §2.3
ARCH-001, ARCH-004, ARCH-005, ARCH-006	§3.1 – §3.9
DSEC-002 .. DSEC-012	§4.1 – §4.13
CST-001, CST-002	§5.1, §5.2
SIZ-001	§6
DAS-001, DAS-004	§7.1, §7.2
HLCH-001	§8
BAR-001	§9
RM-001 .. RM-004	§10.1 – §10.4
EMER-001, EMER-002	§11.1, §11.2
SUP-001 .. SUP-003	§12.1 – §12.3

— End of Deployment Guide —