



ENGINEERING STANDARDS LIBRARY / DATABASE AND STORAGE

Storage, Search, and Backup Architecture Standard

Storage tiering, indexing and search, backup integrity, recovery validation, retention, and evidence-driven data protection.

PERMANENT DOCUMENT ID

MYTHOS-DBS-0002

PUBLICATION

Candidate Standard
Version 1.0.0-candidate

ASSURANCE PROFILE

Standard / Advanced
High Assurance

PERMANENT PUBLICATION IDENTITY

Storage, Search, and Backup Architecture Standard

DOCUMENT ID
MYTHOS-DBS-0002

VERSION
1.0.0-candidate

STATUS
Candidate Standard

PUBLISHER
Mythos Systems

PUBLICATION DATE
2026-07-24

SCHEDULED REVIEW
2027-01-24

12	6	4	1
ATOMIC CRITERIA	ASSURANCE VIEWS	IMPLEMENTATION PROFILES	PERMANENT IDENTITY

Publication doctrine. This publication establishes durable guidance or requirements for its defined scope. Interpretation must preserve the permanent document identity, recorded evidence, controlled exceptions, and formal revision history.

MYTHOS-DBS-0002 inside the database and storage standard constellation



Connected assurance	Architecture, implementation, operations, evidence, and lifecycle are evaluated as one controlled system.
Specialization rule	Companion standards may add precision, but they cannot silently weaken this publication's requirements.

EXECUTIVE POSITION

Storage, Search, and Backup Architecture Standard

The architecture of data storage, search, and backup has failed.

Evidence-bearing delivery path



Assurance maturity spectrum



CONTENTS

Publication navigation

MYTHOS-DBS-0002 inside the database and storage standard constellation	3
Storage, Search, and Backup Architecture Standard	4
Assurance model and evaluation surface	7
Criteria and evidence map	8
Requirements, evaluation methodology, and implementation guidance	9
Executive Mandate	9
Scope and Applicability	9
In Scope	9
Out of Scope	10
Audience	10
Definitions and Taxonomy	10
Storage & Search Dimensions	10
The Storage & Backup Doctrine	10
Evaluation Methodology	11
Scoring Model	11
Weighting	11
Evaluation Categories	11
Backup Immutability and Ransomware Resilience (Weight: 20%)	11
WORM Enforcement	11
Restore Testing and DR Validation (Weight: 20%)	12
Recovery Assurance	12
Search Architecture and CDC Decoupling (Weight: 15%)	12
Query Performance	12
Storage Tiering and Lifecycle Management (Weight: 15%)	13
Economic Optimization	13
Data Sanitization (Crypto-Shredding) (Weight: 15%)	13
Secure Deletion	13
High Availability and Quorum Protection (Weight: 15%)	13
Split-Brain Prevention	13

The Mythos Storage & Backup Suite (MSBS) 14

 Suite Composition 14

 MSBS-Ransomware 14

 MSBS-Search 14

 Execution Protocol 14

Implementation evidence and review gates 15

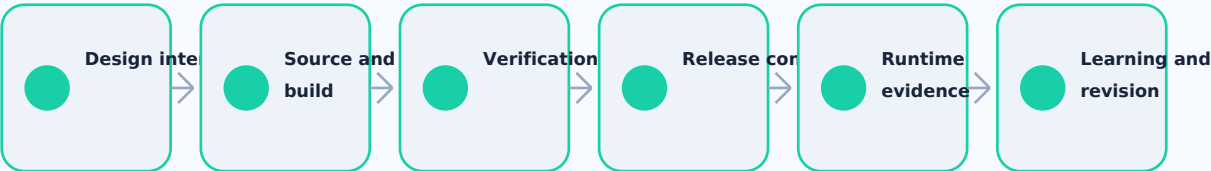
 Current authority register 15

Assurance model and evaluation surface

The standard is assessed as an evidence-bearing system. Capability scores do not replace mandatory gates, implementation proof, or operational validation.

Capability family	Evaluation nodes
Backup Immutability and Ransomware Resilience (Weight: 20%)	1
Restore Testing and DR Validation (Weight: 20%)	1
Search Architecture and CDC Decoupling (Weight: 15%)	1
Storage Tiering and Lifecycle Management (Weight: 15%)	1
Data Sanitization (Crypto-Shredding) (Weight: 15%)	1
High Availability and Quorum Protection (Weight: 15%)	1
Suite Composition	2
Additional Evaluation Dimension	4

Lifecycle control loop



EVALUATION INDEX

Criteria and evidence map

#	Capability family	Criterion
1	Backup Immutability and Ransomware Resilience (Weight: 20%)	WORM Enforcement
2	Restore Testing and DR Validation (Weight: 20%)	Recovery Assurance
3	Search Architecture and CDC Decoupling (Weight: 15%)	Query Performance
4	Storage Tiering and Lifecycle Management (Weight: 15%)	Economic Optimization
5	Data Sanitization (Crypto-Shredding) (Weight: 15%)	Secure Deletion
6	High Availability and Quorum Protection (Weight: 15%)	Split-Brain Prevention
7	Suite Composition	MSBS-Ransomware
8	Suite Composition	MSBS-Search
9	Additional Evaluation Dimension	Storage & Search Dimensions
10	Additional Evaluation Dimension	The Storage & Backup Doctrine
11	Additional Evaluation Dimension	Scoring Model
12	Additional Evaluation Dimension	Suite Composition

NORMATIVE PUBLICATION

Requirements, evaluation methodology, and implementation guidance

The following body preserves the substantive source standard while normalizing publication status, identity, navigation, and visual presentation.

Executive Mandate

The architecture of data storage, search, and backup has failed.

Organizations treat backups as a nightly chore, writing snapshots to the same mutable cloud storage bucket as their production data. When ransomware hits, the backups are encrypted alongside the primary data. They attempt to implement full-text search by running complex LIKE queries against their relational database, crippling the CPU and destroying transactional performance. They store cold archival data on expensive hot block storage, wasting millions in capital.

This standard exists because:

- 1 A Mutable Backup is a Ransomware Target: A backup that can be overwritten or deleted by the same credentials that manage the production system provides zero resilience against ransomware. Backups **MUST** be written to Write-Once-Read-Many (WORM) immutable storage with Object Lock, completely air-gapped from production credentials.
- 2 A SQL LIKE Query is Not a Search Engine: Relational databases are optimized for set-based ACID transactions, not inverted index traversals. Forcing full-text search through SQL causes lock contention and catastrophic latency. Systems **MUST** decouple search into dedicated engines (OpenSearch/Elasticsearch) via Change Data Capture (CDC).
- 3 Untested Backups are Placebos: An untested backup is a hope, not a guarantee. Organizations discover their backups are corrupted only when a disaster occurs. Systems **MUST** automate daily restoration tests in isolated environments, mathematically verifying data integrity.
- 4 Storage Tiers Must Match Data Temperature: Storing 5-year-old compliance logs on NVMe SSDs is economic malpractice. Systems **MUST** implement automated data lifecycle policies, tiering cold data to cheap object storage (e.g., AWS Glacier) and utilizing crypto-shredding for secure deletion.

This document establishes the Mythos Storage & Backup Standard (MSBS), a comprehensive, evidence-based methodology for evaluating storage and search architectures against ransomware resilience, query performance, and data durability.

Scope and Applicability

In Scope

This standard covers the evaluation of:

- 1 Object storage architectures (S3, MinIO, Azure Blob) and WORM (Object Lock)
- 1 Block and file storage tiering (NVMe, HDD, archival tape/glacier)

- 1 Search engines and inverted indexes (OpenSearch, Elasticsearch, Solr)
- 1 Change Data Capture (CDC) for decoupled search indexing
- 1 Backup strategies (3-2-1-1-0 rule, immutable vaults, Velero/Veeam)
- 1 Disaster Recovery (DR) testing and automated restore validation
- 1 Data sanitization (Crypto-shredding, secure erasure)

Out of Scope

- 1 Relational and time-series database internal scaling (covered in MYTHOS-DBS-0001)
- 1 General data sovereignty and egress controls (covered in MYTHOS-DAT-0003)
- 1 General infrastructure-as-code for storage provisioning (covered in MYTHOS-PLT-0002)

Audience

- 1 Storage architects and backup engineers
- 1 Platform engineers managing stateful Kubernetes and object storage
- 1 Security engineers designing ransomware resilience
- 1 Data architects building search pipelines
- 1 Standards bodies seeking a reference storage and backup methodology

Definitions and Taxonomy

Storage & Search Dimensions

Dimension	Definition
WORM (Write-Once-Read-Many)	A storage paradigm (e.g., S3 Object Lock in Compliance Mode) where data, once written, cannot be overwritten or deleted by any user, including root admins, until the retention period expires.
Change Data Capture (CDC)	A pattern that continuously monitors a database's transaction log (WAL) and streams row-level changes to downstream systems (like a search engine) without burdening the primary database.
3-2-1-1-0 Backup Rule	3 copies of data, on 2 different media, 1 offsite, 1 offline/immutable, 0 errors verified via testing.
Crypto-Shredding	The process of rendering data permanently unreadable by securely destroying the encryption keys used to encrypt it, rather than attempting to overwrite the physical storage.
Inverted Index	A database index data structure storing a mapping from content (words) to its locations in a document, enabling sub-second full-text search.

The Storage & Backup Doctrine

A SQL LIKE query is not a search engine. A mutable snapshot is a ransomware target. An untested backup is a placebo. If the storage tier doesn't match the data temperature, the architecture is economically unsustainable.

Evaluation Methodology

Scoring Model

Each capability is scored from 0 to 5.

Score	Meaning
0	Fails basic task; SQL searches, mutable backups, untested restores, single-tier storage
1	Basic search engine exists, but backups are still mutable
2	Functional backups, but lacks WORM immutability or automated restore testing
3	Solid production performance; Decoupled search (CDC), 3-2-1-1-0 backups, WORM Object Lock, lifecycle tiering
4	Strong performance; Crypto-shredding, cross-region immutable vaults, zero-downtime search re-indexing
5	Best-in-class; sets the standard for mathematically verified, ransomware-proof data architectures

Weighting

Category	Weight	Rationale
Backup Immutability & Ransomware Resilience	20%	Mutable backups guarantee total loss during a ransomware attack
Restore Testing & DR Validation	20%	An untested backup is a liability, not a recovery mechanism
Search Architecture & CDC Decoupling	15%	SQL-based search destroys transactional database performance
Storage Tiering & Lifecycle Management	15%	Keeping cold data on hot storage destroys cloud budgets
Data Sanitization (Crypto-Shredding)	15%	Physical deletion in distributed object storage is impossible
High Availability & Quorum Protection	15%	Split-brain in search clusters causes massive data loss

Total: 100%

A system **MUST** score at least 3.0 in Backup Immutability and Restore Testing to be considered for production use.

Evaluation Categories

Backup Immutability and Ransomware Resilience (Weight: 20%)

WORM Enforcement

Are backups protected against modification or deletion by compromised admin credentials?

Score	Criteria
0	Backups stored on the same SAN/NAS as production; root admin can delete them
1	Backups pushed to a different cloud region, but using the same IAM credentials
2	Dedicated backup account with separate credentials, but data is still mutable
3	WORM (Write-Once-Read-Many) Object Lock enforced; even root admins cannot delete backups until retention expires
4	Air-gapped immutable vaults; backups cannot be accessed via the production network plane
5	Perfect resilience: formally verified immutable boundaries, zero ability to tamper with historical data, cryptographic proof of backup integrity

Restore Testing and DR Validation (Weight: 20%)

Recovery Assurance

Is the organization mathematically certain that backups can be restored?

Score	Criteria
0	Backups run nightly, but restores are never tested
1	Manual restore tests conducted annually (guarantees gaps in coverage)
2	Automated restore tests run monthly
3	Automated daily restore tests in an isolated environment; hash verification (checksums) validates data integrity
4	Full DR failover tests executed quarterly, verifying RTO/RPO bounds
5	Perfect assurance: formally verified restore pipelines, zero silent corruption, mathematical proof of zero data loss

Search Architecture and CDC Decoupling (Weight: 15%)

Query Performance

How is full-text and semantic search implemented across enterprise data?

Score	Criteria
0	Full-text search executed via SQL LIKE queries against the primary database
1	Periodic batch jobs dump data from SQL to Elasticsearch (high latency, stale data)
2	Application-level dual-writes to both SQL and search engine (risk of data inconsistency)
3	Change Data Capture (CDC) via Debezium streams WAL changes to OpenSearch; zero application burden
4	Search cluster utilizes vector indexing (k-NN) for hybrid (text + semantic) search
5	Perfect architecture: formally verified index synchronization, zero query latency impact on transactions, mathematical proof of search consistency

Storage Tiering and Lifecycle Management (Weight: 15%)

Economic Optimization

Is data automatically moved to the cheapest viable storage tier?

Score	Criteria
0	All data (logs, backups, active records) stored on expensive NVMe/SSD block storage
1	Manual migration of old data to cheaper storage
2	Basic S3 lifecycle policies moving objects to Standard-IA after 30 days
3	Automated tiering: hot data on NVMe, warm on HDD, cold data to Glacier/Archive within hours
4	AI-driven lifecycle policies predicting data access patterns and pre-tiering
5	Perfect optimization: formally verified data temperature bounds, zero wasted capital, mathematical proof of optimal tier placement

Data Sanitization (Crypto-Shredding) (Weight: 15%)

Secure Deletion

How is data permanently destroyed in a distributed object storage system?

Score	Criteria
0	Relies on DELETE API calls (data actually persists on degraded drives for months)
1	Multi-pass overwrite tools used on block storage
2	Basic object deletion with versioning suspended
3	Crypto-shredding: all objects encrypted with unique Data Encryption Keys (DEKs); deletion = destroying the KEK (Key Encryption Key)
4	Automated key destruction policies triggered by data retention expiry
5	Perfect sanitization: formally verified zero-recoverability, cryptographic attestation of key destruction, zero plaintext remnants

High Availability and Quorum Protection (Weight: 15%)

Split-Brain Prevention

How do search and storage clusters survive network partitions?

Score	Criteria
0	Single-node search/storage clusters (guaranteed data loss on crash)
1	Multi-node clusters, but no quorum enforcement (split-brain corrupts indices)
2	Basic replica shards, but failover is manual
3	Consensus-based quorum (Raft/Paxos) ensuring a single write master; automated failover
4	Cross-zone replication ensuring RPO=0 for search indices
5	Perfect resilience: formally verified consensus bounds, zero split-brain risk, self-healing index rebalancing

The Mythos Storage & Backup Suite (MSBS)

Traditional benchmarks measure backup write speed (MB/s). The MSBS evaluates ransomware resilience, restore integrity, and search decoupling.

Suite Composition

MSBS-Ransomware

- 1 Root Admin Attack: 100+ tests using compromised root credentials to attempt deletion of recent backups, verifying WORM Object Lock prevents the deletion.
- 1 Silent Corruption Test: 50+ tests injecting bit-rot into backup archives, verifying the restore pipeline detects checksum mismatches and quarantines the corrupt blocks.

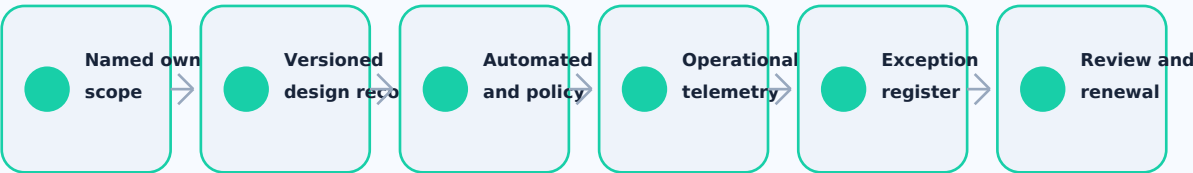
MSBS-Search

- 1 Dual-Write Elimination Test: 100+ tests verifying the application does not write directly to the search engine, and that CDC latency from SQL to OpenSearch is < 2 seconds.
- 1 Failover Test: 50+ tests destroying the primary search node during peak query load, verifying the cluster rebalances shards without dropping user requests.

Execution Protocol

Implementation evidence and review gates

Required assurance chain



A passing score is not sufficient without current evidence. High-assurance adoption requires traceable design decisions, reproducible builds, independently reviewable tests, controlled secrets, runtime observability, failure exercises, and a dated exception register.

Assurance maturity spectrum



Current authority register

Authority	Version / snapshot	Applicability	Review by
OpenTelemetry Project: OpenTelemetry Documentation and Specification	Rolling specification snapshot; profiles public alpha and declarative configuration stable in 2026	High	2026-10-22
PostgreSQL Global Development Group: PostgreSQL Documentation	Rolling official documentation snapshot	High	2026-10-22

Research limitation. Official documentation establishes published interfaces and declared behavior. It does not prove the performance, security, interoperability, cost, or operational suitability of a specific implementation. Those claims require controlled testing and retained evidence.