



SOFTWARE ENGINEERED IN TÜRKİYE

UNIFIED STORAGE SERVER — ENTERPRISE CLASS

Storage Server

**What is written is never erased.
What is recorded is evidence.**

Object (S3), file (SMB/NFS) and block (iSCSI, NVMe-oF, FC) in one appliance for energy, rail, public/defense, industry, finance and telecom. WORM retention, RFC 3161 time-stamped audit chain, dual-node HA and synchronous replication, virtualization and backup target, central log archive — the full feature set of the enterprise storage leaders, with software entirely in house at Simgenet.

1PB+

PER NODE ·
CLUSTER 10 PB+

RPO 0

METRO SYNC

WORM

RFC 3161
STAMPED

100 GbE

NVME/TCP · RDMA



Simgenet Storage Server · 1U/2U chassis, mixed SATA/SAS/NVMe, 1G–100G Ethernet

Simgenet Storage Server

Product Brochure · SMG-UB-STORAGE-EN · Rev. 3

Simgenet Mühendislik

Enerji San. ve Tic. Ltd. Şti.



01

CORPORATE

The Company That Keeps Data and Proves It

Simgenet Mühendislik is a Turkish engineering company delivering industrial networking and critical-infrastructure communication systems. The Storage Server software is **entirely original**, developed in house at Simgenet; it is not an adaptation of an off-the-shelf package.

2000

FOUNDED

500+

PROJECTS DELIVERED

30+

COUNTRIES SERVED

100+

PRODUCTS

■ Why our own storage server

The PBX, time-server, access-control and switching networks we deploy produce records every day: call recordings, event logs, configuration backups, camera archives. These records must be kept **for the legal period, immutable and provable**. The enterprise storage leaders sell this with extra licenses and extra products; the Storage Server delivers it inside the box.

■ Why our own software

- **Technological sovereignty** — no feature walls, entirely under the Simgenet license; in-house software for public and banking tenders
- **Features to specification** — the protocol, retention policy and report the project asks for are added
- **Ecosystem** — PBX recordings, NAC/GNSS/SMGOS logs and SVP reports in the same archive
- **Long life** — support across a 15–20-year infrastructure life cycle

Our departments are separate. The software of Simgenet-branded products is developed in our own **manufacturing and R&D department**; transmission systems and field deployment are run by separate specialist teams. Storage installation, data migration and legal-retention configuration are delivered under a single responsibility.

Our Mission

To deliver innovative, reliable and sustainable technology solutions for industrial networking and critical-infrastructure communication, safeguarding our customers' business continuity.

Our Vision

To become Türkiye's most trusted and innovative network-infrastructure technology partner and a globally recognized brand.

02

PLATFORM

What Is the Simgenet Storage Server?

An enterprise unified storage server that serves **object (S3), file (SMB/NFS/WebDAV/SFTP) and block (iSCSI, NVMe-oF, Fibre Channel)** from the same appliance; managed from one web panel; a legal-retention (5651/KVKK) and ransomware-resistant (WORM) backup/archive target. It delivers the full feature set of the enterprise storage leaders inside an original, single-source ecosystem.

■ Three protocols, one pool

S3, SMB 3, NFS v3/v4, iSCSI, NVMe-oF and FC from the same pool; the virtualization datastore, the file server and the object archive need no separate appliances.

■ Records that cannot be deleted

With WORM / object lock nobody — administrator included — can delete until retention expires; every night an RFC 3161 timestamp and hash chain prove integrity, verified with one click.

■ Service that never stops

Dual-controller and two-box HA, metro synchronous writes (RPO=0), metro cluster, scale-out cluster and non-disruptive updates — data access continues through maintenance and failure.

Key Capabilities

- S3 (versioning, bucket policy, expiring share links) · SMB 3 (Multichannel, "Previous Versions") · NFS v3/v4 · iSCSI · NVMe-oF (TCP/RDMA) · FC · WebDAV · SFTP · rsync
- RAID 0/1/5/6/triple parity/10/50/60, hot spare, automatic repair, monthly integrity scrub
- Snapshots (instant + scheduled + retention policy), writable clones, recycle bin
- Encryption: AES-256-GCM at rest (per tenant), TLS 1.3 in transit, full-disk encryption + TPM 2.0, KMIP external keys, SED
- Inline dedup + compression; automatic tiering NVMe → HDD → cloud S3; per-tenant quota and bandwidth limit
- WORM / object lock (compliance mode); RFC 3161 stamp; hash-chained audit log
- Dual-controller + two-box HA, metro sync (RPO=0) + asynchronous encrypted replication, S3 site replication, scale-out
- Virtualization: VMware VAAI + VASA/vVols, Hyper-V SMB3, built-in Proxmox block provider (iSCSI), Kubernetes CSI, OpenStack Cinder
- Syslog server module: TLS 6514, configurable minimum retention, daily stamp, forwarding to SIEM; SNMP trap receiver
- Web (TR/EN), REST/OpenAPI, Terraform/Ansible, AAA, SNMPv3 + MIB, X.733 alarms (with explanations), signed updates, ransomware detection

The ecosystem's archive. Simgenet PBX call recordings to S3, NAC / GNSS / SMGOS / SMG-SW event logs directly over TLS syslog, SMGOS configuration and software backups as a target — in one box, stamped and WORM-protected.



03

ARCHITECTURE

Roles, High Availability and Scale

One appliance takes on five roles; from a single controller to dual-node HA, and on to metro cluster and scale-out cluster, it **grows with the same software**. Data access is not interrupted during maintenance or failure.

■ NAS / file server

SMB 3 (AD/LDAP users, encrypted SMB, Multichannel/Direct), NFS, WebDAV, SFTP; folder and tenant quotas; snapshots in Windows "Previous Versions".

■ Virtualization datastore

NFS datastore mode with one click; iSCSI multi-LUN, thin provisioning; VMware VAAI (4/4) and VASA/vVols; Hyper-V SMB3; built-in block provider for Proxmox (iSCSI; automatic LUN the moment a virtual disk is created); Kubernetes CSI, OpenStack Cinder.

■ Backup target

S3 + object lock and SMB/NFS targets for backup software; immutable backups against ransomware; expiring, download-limited share links.

■ Central log and record archive

Syslog server module (UDP/TCP 514, TLS 6514; RFC 3164/5424), SNMP trap receiver, PBX call recordings, NAC/GNSS/SMGOS/SW events; per-source search, live view, CSV; quota-managed pool, configurable minimum retention, daily stamp, forwarding to SIEM.

■ Forensic / compliance archive

WORM compliance mode (SEC 17a-4(f) / FINRA 4511 / CFTC 1.31 class), RFC 3161 qualified timestamp (TÜBİTAK or in-house TSA), hash-chained audit log, signed audit bundle; 5651 and KVKK retention.

Redundancy and Scale

Dual-controller HA

Shared JBOD, SCSI-3 PR fencing; two-box HA: virtual IP, witness node

Replication

Metro synchronous (RPO=0, DRBD 9) and asynchronous encrypted; S3 site replication active-active

Metro cluster

Stretched across two sites; uninterrupted through a site disaster

Scale-out

Add nodes, automatic rebalancing; 10 PB+ cluster

Non-disruptive updates. A/B boot environments and HA together: the update goes to the passive node first, failover, then the other — service is not interrupted; one-step return to the previous environment when needed.



04

DATA SERVICES

Protocols, Protection and Efficiency

■ Object — S3

- TLS, versioning, bucket policy, access keys
- Expiring and download-limited share links
- Object lock (WORM), lifecycle policy, tiering to cloud
- S3 site replication (active-active)

■ File — SMB / NFS / WebDAV / SFTP

- SMB 3: AD/LDAP users, encrypted SMB, Multichannel/Direct, "Previous Versions" (snapshots)
- NFS v3/v4; hypervisor datastore mode with one click; Kerberos
- WebDAV, SFTP, rsync target
- Folder and tenant quotas; recycle bin and versioning

■ Block — iSCSI / NVMe-oF / FC

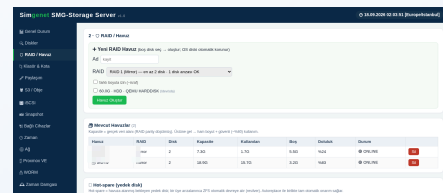
- iSCSI: CHAP, multi-LUN, thin provisioning; VAAI ATS · XCOPY · WRITE_SAME · UNMAP
- NVMe/TCP target (allowed-client list) · NVMe-oF RDMA
- Fibre Channel
- Built-in Proxmox block provider (iSCSI): automatic LUN the moment a virtual disk is created

■ Protection and efficiency

- RAID 0/1/5/6/triple parity/10/50/60; hot spare; automatic repair; monthly integrity scrub; 2–3 disk failure tolerance
- Snapshots: instant + scheduled + retention policy; unlimited; writable clones (zero copy)
- Inline dedup + compression; automatic tiering NVMe → HDD → cloud
- Per-tenant quota and bandwidth limit; ransomware detection → alarm + protective snapshot

■ Encryption and key management

- AES-256-GCM at rest, separate key per tenant; TLS 1.3, Kerberos, IPsec, SMB3 encrypted path in transit — no clear-text path
- Full-disk encryption + TPM 2.0; device vault (recovery key kept centrally)
- KMIP external key management; self-encrypting drives (SED)



RAID / pool management

Pool creation, hot-spare assignment, disk topology and automatic repair on one screen.



05

COMPLIANCE

Legal Retention, WORM and Log Archive

The evidential value of a record depends on proving **that it was not altered and when it was written**. The Storage Server provides this inside the box, without extra products: object lock, qualified timestamp, hash chain and signed audit bundle.

■ WORM / object lock

- Compliance mode: until retention expires nobody — **administrator included** — can delete or modify
- SEC 17a-4(f) / FINRA 4511 / CFTC 1.31 class retention; 5651 and KVKK periods
- Retention clock is GNSS-disciplined (Simgenet GNSS Server) — the period cannot be manipulated
- Deletion attempts are rejected and logged as alarm / audit events

■ Timestamp and audit chain

- **RFC 3161** qualified timestamp: TÜBİTAK or in-house TSA
- Manifest + stamp every night; audit log hash chain stamped daily
- One-click integrity verification; signed audit bundle (for court / auditor)
- JIT access and four-eyes (dual approval) control of destructive operations

■ Syslog server module

- UDP/TCP 514, TLS 6514; RFC 3164 and 5424; source devices appear automatically
- Silence alert (a source went quiet), dropped-message counter; search, live view, CSV
- Quota-managed pool archive (oldest day rotates when full); configurable minimum retention
- Forwarding to SIEM; SNMP trap receiver into the same archive



Syslog server screen

Listening ports, TLS, archive pool and retention, daily RFC 3161 stamp, source device list on one page.

Ready for Simgenet products. NAC Server, GNSS Server, SMGOS router and SMG-SW switch events directly over TLS syslog; PBX call recordings nightly to S3; backup software to S3 + object lock; SMGOS configuration and software backups as a target. An event's log is still found with its stamp three months later.

06

MANAGEMENT

Web Panel, Security and Operations

One HTTPS panel, TR/EN matrix interface, four-step installation. Destructive operations require two-stage approval; every change is in the hash-chained audit log.

Web panel (HTTPS, TR/EN)

- Tabs: Overview · Alarms · Disks · RAID/Pool · Folders & Quota · Shares · S3/Object · iSCSI / NVMe · Snapshots · Connected Devices · Time · Network · Virtualization · WORM · Timestamp · Syslog Server · HA · Users · Replication · License · Logs
- TLS enforced, security headers, rate limiting; live sessions (SMB/NFS/iSCSI/S3)
- Multi-NIC: auto-discovery, bond/LACP, VLAN, MTU 9000, management/data separation
- REST / OpenAPI; infrastructure-as-code with Terraform and Ansible

Identity and access

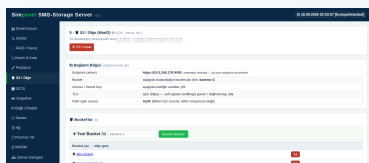
- AAA: RADIUS + TACACS+ + LDAP/AD, role mapping; local fallback administrator
- Roles: Administrator · Operator · Viewer; four-eyes approval for destructive operations; JIT access
- Brute-force lockout; device certificate via EST, OCSP revocation checking
- Multi-tenant: separate encrypted space + users + quota + IP allow-list

Monitoring and alarms

- SNMP v2c/v3 + Simgenet MIB (pool, disk, capacity, service, license) + traps
- X.733 Alarms: each alarm explained (what happened, why it matters, probable cause, what to do), automatic clearing, acknowledgement
- E-mail / webhook notification; daily e-mail report; call-home telemetry
- Ransomware detection (mass rename/delete, encrypted writes, canary files); capacity and disk warnings

Installation and operations

- Plug-and-play installation ISO (UEFI); first setup in 4 steps: IP → pool → share/bucket → user
- Full-disk encryption + TPM 2.0, boot-loader password, certificate-based SSH, firewall closed by default
- Configuration backup and restore; reset to defaults; signed updates; non-disruptive updates (A/B + HA)
- License: signed, hardware-bound, module + capacity; one-command diagnostic bundle



S3 / object

Bucket creation, access keys, TLS; object lock and lifecycle.



Status summary · alarms

```
System healthy – no active warnings
Pool records  RAID-6  ONLINE  48/120 TB (40%)
Disks          12 · SMART OK · spare ready
HA             primary active · peer in sync
Snapshot       last 02:00 · Syslog 37 sources · stamp ✓
MAJOR 02:14 disk fault → spare engaged, rebuild 38%
CRITICAL WORM 'forensic-2026' delete attempt REJECTED
```



07

CAPACITY AND USE

Scale, Scenarios and the Difference

Up to 1 PB

Single node; 10 PB+ with clustering

RPO = 0

Metro synchronous writes: two data nodes + witness

Up to 100 GbE

10/25/100 GbE, NVMe cache, NVMe/TCP and RDMA

2–3 disks

RAID-6 / triple-parity failure tolerance; unlimited snapshots

■ Energy, rail, public / defense

WORM and stamped retention of substation and station recorders, NAC/GNSS/switch event logs and camera archives for the legal period; replication between two centers; a single-source ecosystem.

■ Finance and regulated organizations

Compliance-mode object lock (SEC 17a-4(f) / FINRA 4511 / CFTC 1.31 class), qualified timestamp, signed bundle for the auditor; 5651/KVKK retention; four-eyes approval.

■ Industry, telecom and enterprise IT

Virtualization datastore (VAAI/vVols, Hyper-V, Proxmox, Kubernetes, OpenStack), ransomware-resistant backup target, shared space and file server; departmental separation with per-tenant quota and bandwidth limits.

■ The Simgenet difference

- The legal-retention chain (WORM + RFC 3161 + hash chain + signed bundle) inside the box, no extra product
- GNSS-disciplined retention clock; TPM 2.0 full-disk encryption + device vault
- Built-in block provider for Proxmox (iSCSI); VAAI 4/4; PBS S3 target
- No feature walls, transparent pricing; TR/EN matrix interface; single-source ecosystem

Evidence-based delivery. At the end of installation, HA failover, replication, WORM behavior and the syslog stamp chain are measured with Simgenet SVP; the customer receives a lockable acceptance report.

08

SPECIFICATIONS

Simgenet Storage Server

FEATURE	SIMGENET STORAGE SERVER
Product class	Enterprise unified storage server (object + file + block); legal-retention and ransomware-resistant archive target; software entirely in house at Simgenet
Roles	NAS / file server · virtualization datastore · backup target · central log and record archive · forensic / compliance archive
Object	S3 (TLS, versioning, bucket policy, access keys, expiring/download-limited share links) · object lock (WORM) · lifecycle and cloud tier · S3 site replication (active-active)
File	SMB 3 (AD/LDAP, encrypted SMB, Multichannel/Direct, "Previous Versions") · NFS v3/v4 (Kerberos, datastore mode) · WebDAV · SFTP · rsync · folder/tenant quotas · recycle bin · versioning
Block	iSCSI (CHAP, multi-LUN, thin provisioning, VAAI ATS/XCOPY/WRITE_SAME/UNMAP) · NVMe/TCP (allowed-client list) · NVMe-oF RDMA · Fibre Channel · built-in Proxmox block provider (iSCSI)
Data protection	RAID 0/1/5/6/triple parity/10/50/60 · dRAID · RAIDZ expansion · L2ARC / SLOG / special vdev · hot spare · automatic repair · monthly integrity scrub · snapshots (instant, scheduled, retention policy; unlimited) · writable clones
Efficiency	Inline dedup + compression · automatic tiering NVMe → HDD → cloud S3 · per-tenant quota and bandwidth limit · ransomware detection (alarm + protective snapshot)
Encryption	AES-256-GCM at rest (key per tenant) · TLS 1.3 / Kerberos / IPsec / SMB3 encrypted in transit · full-disk encryption + TPM 2.0 · device vault (recovery key held centrally) · KMIP · SED
Compliance	WORM compliance mode (administrator cannot delete; SEC 17a-4(f) / FINRA 4511 / CFTC 1.31 class) · RFC 3161 qualified timestamp (TÜBİTAK / in-house TSA) · hash-chained audit log, daily stamp · signed audit bundle · GNSS-disciplined retention clock · 5651 / KVKK
Log archive	Syslog server module: UDP/TCP 514, TLS 6514, RFC 3164/5424, source auto-discovery, silence alert, dropped-message counter, search/live/CSV, quota-managed pool, configurable minimum retention, daily manifest + stamp, forwarding to SIEM · SNMP trap receiver
Redundancy	Dual-controller HA (shared JBOD, SCSI-3 PR fencing) · two-box HA (virtual IP, witness node) · metro synchronous writes (RPO=0, DRBD 9) · asynchronous encrypted replication (certificate pinning) · metro / stretched cluster · scale-out cluster (add nodes, automatic rebalancing) · non-disruptive updates (A/B + HA)

Continued on the next page: virtualization, management, monitoring, security, capacity, hardware and reference standards.

09

SPECIFICATIONS

Integration, Management and Hardware

FEATURE	SIMGENET STORAGE SERVER
Virtualization / cloud	VMware VAAI (4/4) + VASA/vVols · Hyper-V SMB3 · Proxmox (NFS/iSCSI datastore, built-in provider, PBS S3 target) · Kubernetes CSI · OpenStack Cinder · backup software (S3 + object lock, SMB/NFS)
Management	HTTPS web (TR/EN; 20 tabs; TLS enforced, rate limiting) · REST / OpenAPI · Terraform / Ansible · multi-NIC (bond/LACP, VLAN, MTU 9000, management/data separation) · multiple GNSS / NTP sources, automatic or manual selection (Simgenet GNSS Server) · configuration backup and restore · reset to defaults · signed software updates · license (signed, hardware-bound, module + capacity) · one-command diagnostic bundle
Identity and access	RADIUS + TACACS+ + LDAP/AD, role mapping · roles: Administrator / Operator / Viewer · hash-chained audit log with results · EST device certificate + OCSP · local fallback administrator · two-stage approval (four eyes) · JIT access · brute-force lockout · multi-tenant isolation (encrypted space, quota, IP allow-list)
Monitoring	SNMP v2c/v3 + Simgenet MIB + traps · X.733 Alarms tab (explanations, automatic clearing, acknowledgement) + Events · thresholds (capacity, temperature, SMART, pool) · e-mail / webhook · daily report · call-home telemetry · ransomware detection · capacity and disk warnings · Connected Devices live sessions
Capacity	Up to 1 PB per node · 10 PB+ cluster · 10/25/100 GbE, NVMe cache, NVMe/TCP and RDMA · RAID-6 / triple-parity 2–3 disk tolerance · unlimited snapshots · per-tenant quota and bandwidth limit
Hardware	Long-life server systems designed for 24/7 continuous operation · 1U / 2U chassis · mixed SATA / SAS / NVMe · hardware-agnostic (any NIC / HBA / RAID card) · 1G–100G Ethernet · FC (option) · protected operating-system disk · TPM 2.0
Installation	Plug-and-play ISO (UEFI, full-disk encryption + TPM, boot-loader password, certificate-based SSH, firewall closed by default) · first setup in 4 steps (IP → pool → share/bucket → user) · device vault (recovery key held centrally)
Simgenet ecosystem	PBX call recordings to S3 · NAC / GNSS / SMGOS / SMG-SW events over TLS syslog · SMGOS configuration and software backup target · retention clock from GNSS · acceptance measured with SVP
Language	TR / EN

Reference Standards

S3 API · SMB 3 · NFS v3 / v4 (RFC 1813 / 7530) · iSCSI (RFC 7143) · NVMe-oF · Fibre Channel · WebDAV (RFC 4918) · SFTP · RFC 3161 (timestamp) · RFC 3164 / 5424 / 5425 (syslog, TLS) · RFC 3411–3418 (SNMPv3) · KMIP · TPM 2.0 · EST (RFC 7030) · OCSP · SEC 17a-4(f) · FINRA 4511 · CFTC 1.31 · Turkish Law No. 5651 · KVKK · X.733



Why Simgenet Storage Server

Never erased, always evidence

WORM object lock, RFC 3161 qualified stamp, hash-chained audit log and signed audit bundle — inside the box.

Object + file + block, one pool

S3, SMB 3, NFS, iSCSI, NVMe-oF, FC; the virtualization datastore, file server and archive need no separate appliances.

Service that never stops

Dual-controller HA, metro sync (RPO=0), metro cluster, scale-out and non-disruptive updates; from 1 PB to 10 PB+ with the same software.

Original, ecosystem, proven

Software entirely in house at Simgenet; PBX, NAC, GNSS and switch records in the same archive; acceptance delivered with an SVP report.

GET IN TOUCH

Address

Kartal / İstanbul, Türkiye

Phone

+90 555 600 4506

E-mail · Web

info@simgenet.net · simgenet.net

Simgenet Mühendislik Enerji San. ve Tic. Ltd. Şti.

Product Brochure · SMG-UB-STORAGE-EN · Rev. 3 · © 2026

Software Engineered in Türkiye