Proof of Concept (PoC)

Distributed Cloud Storage Using Repurposed Hardware on enterprise-grade RHEL-compatible Linux (Rocky Linux or AlmaLinux)

Copyright Notice (SMEs and Educational Institutions)

---

1. Executive Summary

This Proof of Concept (PoC) presents a cost-effective, resilient, and scalable **shared cloud storage service for Small and Medium-sized Enterprises (SMEs)**. The platform is built using **retired or written-off desktops and laptops sourced from corporate organizations** undergoing regular IT refresh cycles. These corporate IT assets are securely repurposed to form a multi-tenant private cloud infrastructure.

Leveraging **enterprise-grade RHEL-compatible Linux (Rocky Linux or AlmaLinux)**, an enterprise-grade, RHEL-compatible operating system, and **GlusterFS** as the distributed storage layer, the system aggregates multiple storage nodes into a single logical storage platform with built-in replication, redundancy, and self-healing capabilities.

The PoC addresses key SME challenges: rising commercial cloud subscription costs, limited IT budgets, data sovereignty requirements, business continuity risks, and sustainability obligations. Multiple independent SMEs consume this cloud service concurrently while maintaining strict logical data separation and ownership.

2. Objectives

The objectives of this PoC are to:

- Deliver a **shared cloud storage service** accessible to multiple SMEs
- Reduce SME dependence on recurring commercial cloud subscriptions
- Repurpose retired corporate IT assets to maximize hardware lifecycle value
- Ensure continuous data availability through replication and redundancy
- Support SME data sovereignty, compliance, and local control
- Enable incremental scaling aligned with SME onboarding and growth
- Demonstrate measurable environmental and ESG benefits

---

3. Scope

Included

- Use of retired or written-off desktops and laptops from corporate organizations
- Deployment of a shared, multi-tenant cloud storage platform
- Enterprise Linux-based distributed storage architecture
- Replication, redundancy, and fault-tolerance validation
- Evaluation of feasibility for broad SME adoption

Excluded

- Hyperscale cloud feature parity
- Industry-specific regulatory certification audits
- Fully managed 24/7 commercial service operation

---

4. Architecture Overview

The system uses a **peer-based distributed storage architecture** designed to support **secure hybrid access over both local networks and the public internet**. Each node contributes local disk storage to a shared storage pool, while access to data is provided through controlled and encrypted channels.

Key Characteristics

- Multi-tenant design with logical isolation per organization (SMEs, NGOs, schools)
- No single point of failure
- Horizontal scalability
- Automatic self-healing

- POSIX-compliant filesystem interface
- **Hybrid access model: secure web access and VPN-based access**

---

5. Hardware Configuration

Component	Specification
Nodes	3 minimum (scales horizontally)
Hardware	Retired corporate desktops and laptops
CPU	x86_64 compatible
Memory	4 GB minimum (8 GB recommended)
Storage	HDD or SSD, mixed sizes supported
Network	Gigabit Ethernet

Laptops provide additional resilience due to integrated battery backup, improving tolerance to short power interruptions.

---

6. Software Stack

Layer	Technology
Operating System	Enterprise-grade RHEL-compatible Linux (Rocky Linux or AlmaLinux)
Filesystem	XFS
Distributed Storage	GlusterFS (Replicated Volume)
Web Access	HTTPS-based portal (e.g., Nextcloud)
Secure Remote Access	VPN (e.g., WireGuard / OpenVPN)

—|———| | Operating System | enterprise-grade RHEL-compatible Linux (Rocky Linux or AlmaLinux) (latest stable release) | | Filesystem | XFS | | Distributed Storage | GlusterFS (Replicated Volume) | | Web Access | HTTPS-based portal (e.g., Nextcloud) | | Secure Remote Access | VPN (e.g., WireGuard / OpenVPN) |

—|———| | Operating System | enterprise-grade RHEL-compatible Linux (Rocky Linux or AlmaLinux) 9 (Minimal) | | Filesystem | XFS | | Distributed Storage | GlusterFS (Replicated Volume) | | Access Methods | SMB / NFS / Web-based cloud (e.g., Nextcloud) |

---

7. Implementation Methodology

7.1 Operating System Deployment

- Enterprise-grade RHEL-compatible Linux (Rocky Linux or AlmaLinux) installed on all nodes
- Minimal installation profile
- Static IP addressing configured
- Systems updated to latest security patches
- enterprise-grade RHEL-compatible Linux (Rocky Linux or AlmaLinux) (latest stable release) installed on all nodes
- Static IP addressing configured
- Systems updated to latest security patches

7.2 Network and Access Configuration (Hybrid Model)

- Firewall deployed at network perimeter
- HTTPS access enabled for web-based cloud services
- VPN configured for secure remote access to storage services
- Network segmentation used to separate management, storage, and public access traffic

7.3 Storage Preparation

- Dedicated disks allocated per node
- Disks formatted with XFS
- Mounted as GlusterFS brick directories

7.4 Distributed Storage Deployment

- GlusterFS server installed on all nodes
- Nodes peered into a trusted storage pool
- Replicated volumes created with a replica factor of three

---

8. Replication and Redundancy Model

- Each file is stored simultaneously on multiple nodes
- Synchronous replication ensures consistency
- Automatic self-healing restores replicas after recovery
- Service remains available during individual node or disk failure

---

9. Validation and Testing

9.1 Functional Testing

- Successful creation and mounting of distributed volumes
- Read/write operations across multiple tenants

9.2 Failure Testing

Test Case	Expected Result	Outcome
Single node shutdown	Data remains accessible	Pass
Node reintegration	Automatic data healing	Pass
Write operations during failure	No data corruption	Pass

---

10. Results

The PoC successfully demonstrated:

- Reliable shared storage using retired corporate hardware
- Continuous access to SME data during simulated failures
- Automatic recovery without specialist intervention
- Stable operation on enterprise-grade Linux

SME Cost Perspective

For SMEs participating in the shared service, projected cost reductions of **60–80% per SME** over a 3–5 year period were identified when compared to individual commercial cloud subscriptions, excluding electricity and basic operational costs.

---

11. Risks and Limitations

- Performance constrained by network throughput
- Requires basic Linux administration capability by operators
- Not a substitute for off-site backup without additional configuration
- Production deployment requires further security hardening

---

12. Future Enhancements

With additional funding, the following enhancements are proposed:

- Migration to **Ceph** for unified file, block, and object storage
- Integration with **Nextcloud** for SME-facing cloud services

- Encryption at rest and in transit by default
- Monitoring, reporting, and SLA metrics
- Off-site replication for disaster recovery
- Multi-site and regional deployment models

---

13. Conclusion

This Proof of Concept demonstrates that a shared, resilient, and environmentally responsible cloud storage service for SMEs can be built using **retired corporate IT assets** and open-source enterprise software. The model reduces costs, strengthens data sovereignty, and maximizes the value of existing hardware while delivering measurable sustainability benefits.

With targeted funding, this architecture can be scaled into a repeatable shared SME cloud platform, supporting digital transformation, business continuity, and local economic resilience.

---

14. Sector-Specific Use-Case Scenarios – Education (Private & Public Schools)

This Proof of Concept explicitly supports **both private and public schools** as first-class tenants within the shared cloud platform. The architecture, access model, and governance are designed to meet the operational, financial, and regulatory needs of educational institutions.

14.1 Private School Use Case

Private schools typically require flexible, cost-effective digital infrastructure that supports teaching, administration, and parent engagement while maintaining data privacy and operational independence.

Key Requirements: - Secure remote access for teachers and staff - File storage for lesson materials, assessments, and internal documents - Backup target for school management systems - Predictable monthly costs

PoC Support: - Web-based access (HTTPS) for staff and students - VPN access for administrative systems and backups - Tenant isolation ensuring full separation from other schools - Subscription-based pricing aligned with private school budgets

---

14.2 Public School Use Case

Public schools require robust, low-cost infrastructure that aligns with government policies, child-safety expectations, and data protection requirements.

Key Requirements: - Strong security and access controls - Support for large numbers of users - Compliance with public-sector data handling principles - Minimal on-site infrastructure

PoC Support: - Centralized cloud storage accessed via secure web portal - Role-based access control for students, teachers, and administrators - No direct exposure of storage services to the public internet - Deployment suitable for district, regional, or state-level pilots

---

14.3 Shared Education Cloud Model

Multiple schools (public and private) may coexist on the same physical infrastructure while remaining **logically isolated tenants**.

Benefits include: - Reduced per-school cost through shared infrastructure - Centralized security management - Simplified onboarding for new schools - Scalable model for education departments and NGOs

---

15. SME Deployment Models (Shared Infrastructure)

15.1 Small Shared Cloud (5–10 SMEs)

- 5–7 storage nodes
- Quota-based tenant allocation
- Suitable for business hubs and incubators

15.2 Medium Shared Cloud (10–30 SMEs)

- 8–15 storage nodes
- Dynamic quota allocation
- Suitable for regional service providers

---

16. SME Risk Register (Multi-Tenant Environment)

Risk	Impact	Mitigation
Hardware failure	Low	Replication across nodes
Disk failure	Low	Self-healing replicas

Risk	Impact	Mitigation
Tenant data leakage	High	Logical isolation, permissions, encryption
Resource contention	Medium	Quotas and monitoring
Power interruption	Medium	UPS, laptops, controlled shutdown

---

17. SME Return on Investment (ROI) Timeline

Year 1

- Initial deployment using retired corporate hardware
- Onboarding of first SME tenants

Years 2–3

- Additional SMEs onboarded with minimal marginal cost
- Cost per SME decreases as utilization increases

Years 4–5

- Incremental hardware refresh
- Long-term predictable operating costs

Estimated outcome: - **60–80% cost reduction per SME** - Improved resilience and data control

---

18. Technical Appendix

This Technical Appendix provides detailed information on system architecture, redundancy mechanisms, scalability paths, **hybrid public internet access**, and environmental impact metrics to support technical and funding review.

A. Hybrid Access Architecture (Public Internet + Private Network)

The platform supports a **hybrid access model** enabling SMEs, NGOs, and educational institutions to access services securely over the public internet while maintaining strict security controls.

1. Web-Based Public Access

- HTTPS-only access

- User authentication and role-based access control
- Suitable for schools, NGOs, and remote users

2. VPN-Based Secure Access

- Encrypted VPN tunnels (WireGuard / OpenVPN)
- Required for SMB/NFS access and system backups
- Suitable for SMEs and administrative users

3. Security Controls

- Firewall rules restricting direct exposure of storage services
- No public exposure of SMB/NFS ports
- Logging and monitoring of remote access

B. Updated Logical Access Flow

```
Internet Users (SMEs / NGOs / Schools)
        |
        | HTTPS / VPN
        v
Firewall & Access Gateway
        |
        | Authenticated & Encrypted Traffic
        v
Multi-Tenant Access Layer
        |
        v
Distributed Storage Cluster (enterprise-grade RHEL-compatible Linux (Rocky Li
nux or AlmaLinux) + GlusterFS)
```

C. Compliance and Data Protection Considerations

- Encryption in transit enforced for all internet access
- Tenant isolation maintained across access methods
- Suitable for educational and NGO data sensitivity levels

---

30. School Compliance & Child-Safety Appendix (Global / Universal)

This appendix defines how the Proof of Concept complies with **child-safety, education data protection, and public-sector expectations** for both private and public. The platform is designed to be adaptable to national and state-level education department requirements.

30.1 Core Child-Safety Principles (All Regions)

The platform is designed around the following universal principles:

- Students access data only through controlled web interfaces (HTTPS)
- No direct filesystem, SMB, or NFS access for students
- Role separation enforced (Student / Teacher / Administrator)
- Least-privilege access by default
- All access is logged and auditable

These principles align with widely adopted education IT and child-safety standards.

30.2 Applicability to Public and Private Education Systems (Global)

This Proof of Concept is designed to align with common requirements shared across public and private education systems internationally.

Common Considerations: - Child safety and student wellbeing obligations - Secure handling of student and staff data - Data residency and sovereignty requirements as defined by local regulations

PoC Alignment: - HTTPS-only access for students and teachers - VPN-restricted access for administrators - Centralized audit logging - Deployment suitable for school, district, regional, or national education programs

---

31. School-Specific Pricing Model (Universal)

The pricing model is designed to support **public schools, private schools, and NGO-supported educational institutions** across different regions, while remaining adaptable to local funding structures.

31.1 Public Schools

- Pricing model: Per-school or per-district subscription
- Indicative cost: **Low-cost, grant- or government-funded model**
- Suitable for shared infrastructure across multiple schools

31.2 Private Schools

- Pricing model: Monthly or annual subscription
- Indicative cost: **Tiered based on storage, users, and support level**
- Predictable budgeting aligned with school fee structures

31.3 NGO-Supported Schools

- Pricing model: Subsidized or donor-funded
- Indicative cost: **Minimal per-school cost to enable digital inclusion**

---

32. Education-Specific Access Diagram (Logical)

```
Students & Teachers
(Browser / HTTPS)
        |
        v
Education Web Portal (DMZ)
        |
        | Role-Based Access Control
        v
School Tenant Space
        |
        v
Distributed Storage Cluster
(enterprise-grade RHEL-compatible Linux (Rocky Linux or AlmaLinux) + GlusterF
S)

Administrators
(VPN Only)
        |
        v
Secure Admin Network
```

This model ensures: - Students never access raw storage services - Administrative access is tightly controlled - Public internet exposure is limited to web services only

---

33. Education Department–Tailored Wording (Recommended Use)

The following wording is suitable for inclusion in education grant or department submissions:

> *The proposed platform provides secure, browser-based access to educational resources for students and teachers, while ensuring strong role separation, access logging, and child-safety controls. Administrative access is restricted to encrypted VPN connections. The shared infrastructure model enables multiple schools to benefit from reliable digital services while maintaining full data isolation and compliance with public-sector education requirements.*

Document Status: Proof of Concept Complete – Education, SME, NGO Ready (Global / Universal)
