

Secret Management & Backups: Complete Learning Guide

1. Background

Modern distributed systems require secure handling of API keys, passwords, certificates, and tokens.

Backup strategies evolved from manual copies to automated, encrypted, and geo-redundant systems.

2. Core Concepts

Secret storage, rotation, encryption, and access control.

Backup types: full, incremental, differential.

3-2-1 backup rule.

Encryption at rest and in transit.

3. How to Learn

Learn encryption basics and TLS.

Practice Vault or cloud secret managers.

Automate database and file backups.

Test disaster recovery scenarios.

4. Skill Levels

Beginner: Secure storage and manual backups.

Intermediate: Automated rotation and scheduled backups.

Advanced: Multi-region strategies and key policies.

Architect: Enterprise governance and DR design.

5. Certifications

HashiCorp Vault Associate.

AWS Security Specialty.

Azure Security Engineer.

CISSP.



6. Tools

Vault, AWS Secrets Manager, Azure Key Vault.

KeePassXC.

Veeam, Restic, Bacula.

AWS Backup, Azure Backup.

Conclusion

Secret management and backups ensure security and business continuity.