



Solution Architecture Design: Nextcloud

Tommi Salo

Haaga-Helia University of Applied Sciences

Business Information Technology

Documentation

2025

Table of Contents

| | | |
|-------|---|----|
| 1 | Introduction | 1 |
| 1.1 | Chapter Structure | 1 |
| 2 | Solution Overview | 2 |
| 2.1 | Business and Technical Problem | 2 |
| 2.2 | Key Capabilities | 2 |
| 3 | Technical System Overview | 3 |
| 3.1 | Presentation Tier | 3 |
| 3.2 | Application Layer | 3 |
| 3.3 | Data Tier | 4 |
| 3.3.1 | Amazon RDS | 4 |
| 3.3.2 | Amazon S3 | 4 |
| 3.3.3 | Amazon ElastiCache | 4 |
| 3.4 | Usage Case | 4 |
| 3.5 | User identities | 5 |
| 3.6 | Domain, DNS and TLS | 5 |
| 3.7 | Network Setup Table | 5 |
| 4 | Solution Architecture | 6 |
| 4.1 | Cloud Technologies Overview Table | 6 |
| 4.2 | Solution diagram | 7 |
| 4.3 | Configuration Annotations Table | 8 |
| 5 | Estimated Costs | 9 |
| 5.1 | AWS Cost Estimation Table | 9 |
| 5.2 | Software Licensing Costs | 10 |
| 5.3 | Cost Comparison | 10 |
| 6 | Architecture Review | 11 |
| 6.1 | Domain 1: Security | 11 |
| 6.2 | Domain 2: Resilience | 11 |
| 6.3 | Domain 3: Performance | 12 |
| 6.4 | Domain 4: Cost | 12 |
| 7 | Sources | 13 |

1 Introduction

This document contains a solution architecture design for deploying Nextcloud on AWS. The solution is designed to provide a secure and cost-effective platform for private cloud file storage, document sharing and synchronization.

The design follows AWS best practices and the AWS Well-Architected Framework principles, leveraging the utility of AWS services alongside the advantages of open-source software.

This document is segmented into seven chapters, each underlining one section of the complete solution architecture.

1.1 Chapter Structure

- Chapter 2 Solution Overview: Describes the purpose and scope of the Nextcloud solution design and the business & technical problems it solves.
- Chapter 3 Technical System Overview: Details the technical requirements, usage case, architecture tiers, infrastructure components, and security principles of the solution design.
- Chapter 4 Solution Architecture: Presents the AWS services, configurations, and architecture diagrams illustrating how the system design functions.
- Chapter 5 Estimated Costs: Calculates the estimated costs of components of the system design.
- Chapter 6 Architecture Review: Reviews the system design from a WAF best practice standpoint.
- Chapter 7 Sources: Lists sources used in this document.

2 Solution Overview

Nextcloud is a web application suite for private cloud file storage and synchronization, similar to proprietary options such as Google Drive or Dropbox. Unlike those proprietary services, the self-hosted and open-source nature of Nextcloud provides greater customizability and full control over data. Nextcloud is a widely trusted open-source platform, used by major public-sector organizations, educational institutions, and private companies.

While the Nextcloud suite covers a variety of uses, this solution design focuses on the Nextcloud Files service. Nextcloud is open source under the AGPL v3 license and thus its community edition is fully free to use and deploy. Enterprise-level support subscriptions are available, providing additional documentation and long-term maintenance options. This solution design will be based on the community edition as it is sufficient for a medium-scale organization (up to 100 active users). Larger deployments may need a paid solution for mission-critical use.

2.1 Business and Technical Problem

Many organizations rely on external file-sharing platforms that store data outside their control, raising privacy and data ownership concerns or even potential GDPR conflicts. On-premises storage on the other hand often lacks scalability, cost-effectiveness, and the capability for full remote access.

These challenges can be mitigated by deploying Nextcloud on AWS instead. It gives the host full ownership of the data involved and provides the many advantages of a modern managed cloud solution. The ability to store data only in servers located within the EU provides full GDPR compliance, as opposed to proprietary options.

2.2 Key Capabilities

- Cloud file storage, synchronization, and sharing
- Document version control and recovery
- Secure web and mobile access
- Integration with AWS managed services
- Privacy and data ownership
- Scalable and cost-effective infrastructure

3 Technical System Overview

This chapter provides a technical overview of the solution design, starting with the architecture and its components. System requirements are provided to define the minimum technical capabilities that the deployment must have to function effectively. Nextcloud follows a three-tier architecture consisting of a presentation tier, application tier, and data tier. Each tier in the solution design is supported by AWS-managed services to take full advantage of its features.

3.1 Presentation Tier

The presentation tier provides secure user access to the Nextcloud application and acts as the controlled entry point into the system.

- Users can access Nextcloud through a web browser or Nextcloud desktop & mobile clients.
- Browser compatibility: Firefox, Chrome/Chromium, Microsoft Edge, Safari
- All external traffic occurs over HTTPS (TCP 443) for secure access.
- Route 53 provides DNS resolution for the Nextcloud Domain
- Application Load Balancer (ALB) terminates TLS using an AWS Certificate Manager (ACM) certificate and forwards HTTP traffic to the application tier.
- The ALB forwards requests for the application tier using HTTP (port 80).
- WebDAV communications (syncing, uploads, downloads) also occur over HTTPS.

3.2 Application Layer

The application layer consists of an Amazon EC2 instance:

- Operating System: Ubuntu Server 22.04 LTS
- Web Server: Apache HTTP Server 2.4
- Application Runtime: PHP-FPM 8.3, with required Nextcloud extensions
- CPU: 64-bit x86, recommended t3.large (2 vCPUs), up to t3.xlarge (4 vCPUs)
- Memory: Minimum 16 GB recommended for ~100 active users
- Local caching: APCu
- Local Storage: Amazon EBS 80 GB for OS & Nextcloud application files.
- Background tasks: Linux cron job runs Nextcloud maintenance tasks

Nextcloud documentation recommends horizontal scaling when approaching ~500 active users. For this design's assumed ~100 active users, a single EC2 instance is sufficient.

3.3 Data Tier

The data tier includes all persistent storage services. The system design utilizes a relational database, a caching layer and object storage.

3.3.1 Amazon RDS

Nextcloud stores all user metadata (users, groups, shares etc.) in a relational database. This service is provided by Amazon RDS (MariaDB 10.6+). Private RDS endpoint accessible only from the EC2 instance. RDS storage is encrypted using AWS KMS.

3.3.2 Amazon S3

Nextcloud's user files (documents, uploads, media etc.) are stored in Amazon S3 using Nextcloud's external storage integration. Accessible via VPC Endpoint only from the EC2 instance. S3 stores all files with SSE-KMS (server-side encryption) using AWS key management.

3.3.3 Amazon ElastiCache

Caching and file locking are handled by Amazon ElastiCache (Redis 6x) to prevent sync conflicts and to improve performance. Accessible via TLS-enabled endpoint (port 6380)

3.4 Usage Case

The following approximates the usage of resources by each user and the total requirements on the system.

- An average of 40 GB of data per user, including documents, images and small media files.
- A soft quota of 100 GB per user, leaving room for growth while keeping in the bounds of the architecture.
- Total active file data of approximately 4 TB (40 GB per 100 active users) stored in S3.

3.5 User identities

- System Administrators: Manage AWS services such as EC2 and S3 through AWS System Management.
- Nextcloud Administrators: Manage Nextcloud administrative tasks such as user accounts and sharing settings through the Nextcloud admin interface via web browser or desktop/mobile clients over HTTPS.
- End Users: Access files and sharing features via web browser or desktop/mobile clients over HTTPS.
- AWS IAM roles are used to grant least privilege access to AWS resources.

3.6 Domain, DNS and TLS

- DNS: managed using Route 53, which routes to Application Load Balancer.
- TLS certificates are issued and automatically renewed by AWS Certificate Manager.
- TLS is terminated at the ALB, which uses an ACM-managed certificate.

3.7 Network Setup Table

| Source | Destination | Protocol | Port | Purpose |
|--------|-----------------------|----------|------|----------------------------------|
| User | ALB | HTTPS | 443 | Web access |
| ALB | EC2 | HTTP | 80 | Load balancing |
| EC2 | RDS (MariaDB) | TCP | 3306 | Database access |
| EC2 | ElastiCache (Redis) | TCP | 6380 | Caching and file locking |
| EC2 | S3 (Via VPC Endpoint) | HTTPS | 443 | External storage upload/download |

Note: All internal traffic between EC2, RDS and Redis takes place inside the private VPC, preventing exposure to the public internet.

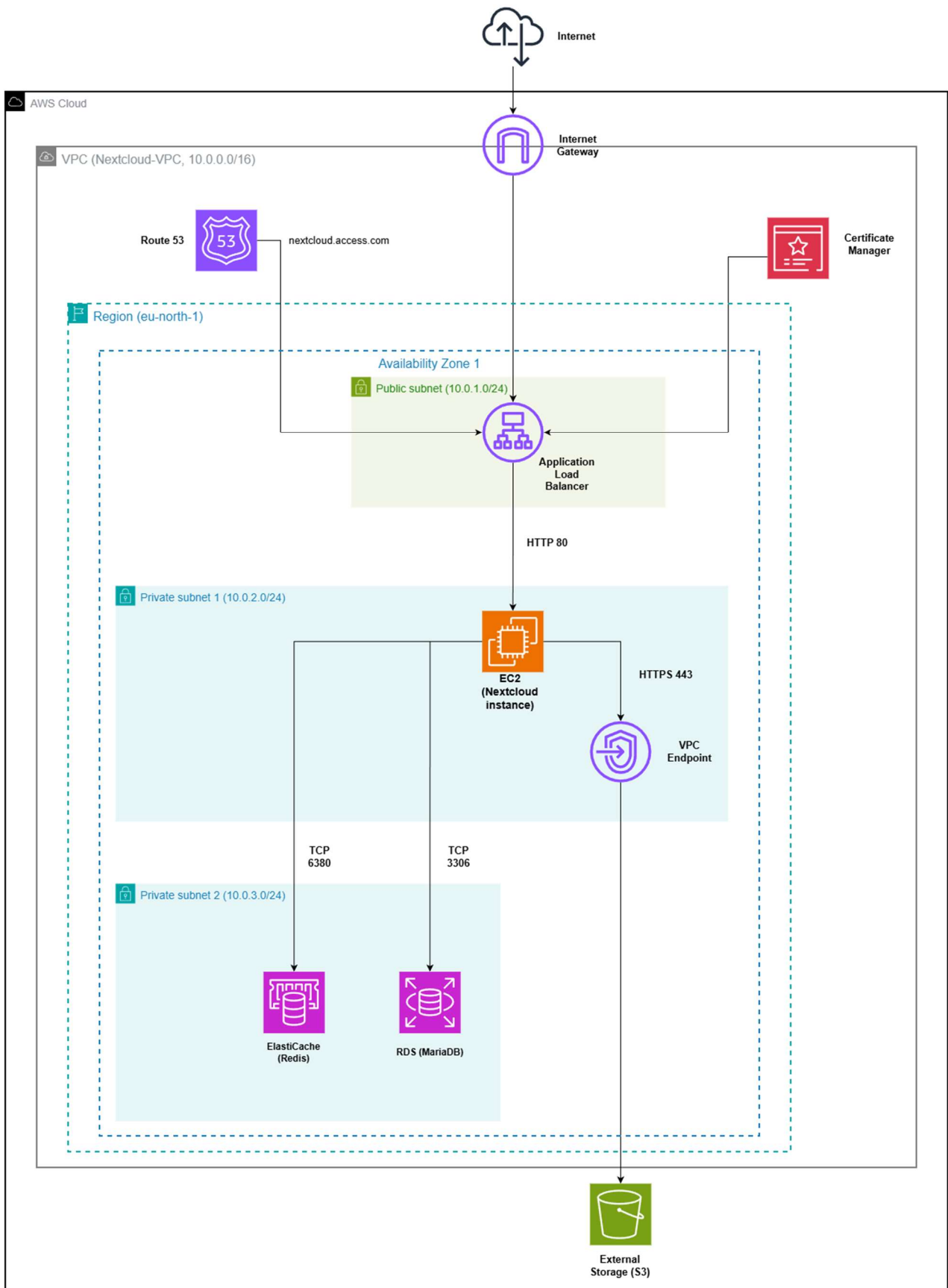
4 Solution Architecture

This chapter contains an overview of the cloud technologies used in the solution design and a diagram of the entire system architecture. Additional context on each cloud technology is provided to ensure full understanding of their functions within the solution design. Example configurations are also provided for ease of set-up.

4.1 Cloud Technologies Overview Table

| Item | Description |
|----------------------------|---|
| Amazon EC2 | Provides computing infrastructure for Nextcloud application |
| Amazon EBS | Stores EC2 OS & Nextcloud application files. |
| Amazon RDS (MariaDB) | Stores structured metadata. |
| Amazon S3 | Stores all user files via external object storage integration |
| Amazon ElastiCache (Redis) | Provides file locking and caching. |
| Amazon VPC | Private cloud networking environment with isolated subnets. |
| VPC Gateway Endpoint | Provides access to S3 from the VPC |
| Application Load Balancer | Balances traffic and terminates TLS |
| AWS Certificate Manager | Manages TLS certificates |
| Amazon Route 53 | Hosts DNS and routes traffic to the ALB. |
| IAM Roles | Provide least-privilege access to AWS resources. |
| AWS Systems Manager | Provides secure administration of the EC2 instance. |

4.2 Solution diagram



4.3 Configuration Annotations Table

| Category | Item | Configuration |
|-----------------|----------------------|-------------------------------|
| DNS | DNS service | Route 53 |
| | Domain name | nextcloud.access.com |
| | Record type | A-record |
| VPC | VPC name | Nextcloud-VPC |
| | VPC CIDR | 10.0.0.0/16 |
| | AWS region | eu-north-1 |
| Subnets | Public subnet | 10.0.1.0/24 |
| | Private subnet 1 | 10.0.2.0/24 |
| | Private subnet 2 | 10.0.3.0/24 |
| Security Groups | ALB security group | Allow HTTPS 443 from Internet |
| | EC2 security group | Allow HTTP 80 from ALB |
| | RDS security group | Allow TCP 3306 from EC2 |
| | Redis security group | Allow TCP 6380 from EC2 |
| Route Tables | Public route table | 0.0.0.0/0 → Internet Gateway |
| | Private route table | No Internet Gateway route |
| | S3 access | Gateway VPC Endpoint |

Note: AWS region must be set within EU for GDPR compliance. All subnets are deployed within a single Availability Zone.

5 Estimated Costs

This chapter aims to estimate the total cost of the solution design based on its composite parts. For the purposes of this solution design, the cost estimation is based on a single production environment. The costs are estimated based on figures established in chapter 3. This is only an estimation and may vary depending on the deployment.

5.1 AWS Cost Estimation Table

| Item | Details | Cost (monthly) |
|---------------------|---|----------------|
| EC2 | 3-year Compute Savings Plan | 36.50 USD |
| EBS | gp3, 80 GB | 6.69 USD |
| RDS (MariaDB) | db.t3.medium, OnDemand, 100 GB, Single-AZ | 61.64 USD |
| ElastiCache (Redis) | cache.t4g.small, OnDemand, 1 node. | 28.47 USD |
| S3 | S3, standard, 4 TB | 94.21 USD |
| ALB | ~1 GB/hour processed data | 23.03 USD |

When these costs are added together, the final monthly cost of the deployment is ~250 USD / month.

5.2 Software Licensing Costs

A significant advantage of this solution design is the elimination of software licensing costs. The use of open-source software components such as Nextcloud, MariaDB, Linux, and Redis removes the need for commercial licenses. As a result, costs are primarily driven by cloud infrastructure consumption rather than proprietary software fees.

5.3 Cost Comparison

As mentioned in Chapter 2, there are proprietary alternatives to the type of Nextcloud deployment described in this document. To provide context, a brief cost comparison is presented below.

Google Workspace offers similar file storage and collaboration capabilities through its Business Standard plan at approximately 13.60 € per user per month, resulting in a monthly cost of 1,360 € for 100 active users.

Dropbox Business provides similar functionality via its Business Standard plan at approximately 12 € per user per month, resulting in a monthly cost of 1,200 € for 100 active users.

It should be noted that these proprietary solutions include additional services and require significantly less maintenance. The estimated cost of approximately 250 USD per month for the Nextcloud deployment represents a base-level configuration, and additional services or higher availability requirements could increase overall costs. Nevertheless, the proposed solution offers strong advantages in terms of data sovereignty, cost efficiency, and deployment flexibility.

6 Architecture Review

This chapter reviews the proposed design solution against the AWS Well-Architected Framework (WAF) to evaluate its adherence to AWS best practices. Each part will be reviewed from the perspective of security, resilience, performance and cost optimization.

The goal is to highlight the current capabilities of the solution design while also identifying potential improvements and the scalability of the architecture.

6.1 Domain 1: Security

This solution design follows AWS security best practices by employing network isolation and encryption. All public access to the system is routed through the ALB, while the EC2 instance, database and cache are deployed in private subnets. Security groups are used to restrict traffic between architectural layers, ensuring that only explicitly permitted communication is allowed.

Data in transit is protected using HTTPS with TLS certificates managed by AWS Certificate Manager. Data at rest is encrypted using AWS Key Management Service (KMS) for Amazon RDS and Amazon S3. Access to AWS services is handled through IAM roles, applying the principle of least privilege and avoiding the use of static credentials.

Security could be further enhanced by introducing managed monitoring and threat detection services such as AWS GuardDuty and more sophisticated IAM policies.

6.2 Domain 2: Resilience

The solution design leverages AWS managed services such as RDS, S3 and ElastiCache, which provide built-in features such as automated backups and limited fault tolerance. S3 provides high durability for file storage, minimizing the risk of data loss. The separation of application and data layers also limits the blast radius of potential failures.

The current design is limited to a single Availability Zone, which reduces infrastructure costs but may negatively impact availability in the event of an Availability Zone failure. This could be solved by deploying the application across multiple Availability Zones.

6.3 Domain 3: Performance

The performance capability of the solution design is addressed by selecting appropriately sized compute- and database resources for the expected workload of ~100 active users. ElastiCache is used to handle file locking and caching, reducing database load. S3 is used as the primary storage for user files, enabling scalable storage without placing significant load on the application or database tiers.

Performance could be further optimized, if necessary, by introducing horizontal scaling of EC2 instances. Monitoring and performance analysis using Amazon CloudWatch metrics could help identify and address performance bottlenecks.

6.4 Domain 4: Cost

Cost optimization is in part achieved by using open-source software components, eliminating software licensing fees. AWS managed services are leveraged to provide infrastructure at a predictable and reasonable cost. 3-year Compute Savings Plan is applied to the EC2 instance, providing a long-term production deployment at a reduced cost, while keeping necessary adaptability. All storage and resource sizing are aligned with actual workload requirements.

Further cost optimization could be achieved through leveraging metrics to determine the exact workload requirements for the deployment. If long-term usage becomes predictable, Reserved Instances for database services could provide additional cost savings.

7 Sources

Amazon Web Services. (2024). AWS Well-Architected Framework. Available at:

<https://docs.aws.amazon.com/wellarchitected/latest/framework/>

Amazon Web Services. (2024). Amazon EC2 Documentation. Available at:

<https://docs.aws.amazon.com/ec2/>

Amazon Web Services. (2024). Amazon RDS User Guide. Available at:

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/>

Amazon Web Services. (2024). Amazon S3 User Guide. Available at:

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/Welcome.html>

Amazon Web Services. (2024). AWS Pricing Calculator. Available at:

<https://calculator.aws/>

Amazon Web Services Academy. AWS Academy Cloud Architecting – Course Materials. Amazon Web Services.

Nextcloud GmbH. (2025). Nextcloud Administration Manual. Available at:

https://docs.nextcloud.com/server/latest/admin_manual/

Nextcloud GmbH. (2025). System Requirements. Available at:

https://docs.nextcloud.com/server/latest/admin_manual/installation/system_requirements.html

Google LLC. (2025). Google Workspace Pricing. Available at:

<https://workspace.google.com/pricing.html>

Dropbox, Inc. (2025). Dropbox Business Pricing. Available at:

<https://www.dropbox.com/business>