# Network Storage Integration

This playbook outlines the steps for integrating and managing network-attached storage (NAS) and storage area networks (SAN) within an existing network infrastructure. It covers initial deployment, configuration, and ongoing management tasks.

### Step 1: Assessment

Perform an assessment of the current network infrastructure to ensure compatibility and identify potential integration points for NAS or SAN solutions.

### Step 2: Planning

Develop a detailed plan that includes the network storage requirements, chosen NAS or SAN systems, data migration strategies, and backup solutions.

### Step 3: Procurement

Procure the necessary hardware and software for NAS or SAN deployment based on the planning and assessment.

### Step 4: Installation

Install the network storage hardware in the server environment and ensure it is powered and connected to the network.

### Step 5: Configuration

Configure the NAS or SAN devices to fit the network's needs, including setting up RAID levels, network access, and user permissions.

### Step 6: Integration

Integrate the NAS or SAN with the existing network, ensuring that it is properly mapped and accessible to the appropriate users and systems.

### Step 7: Data Migration

Transfer existing data to the new storage solution, ensuring data integrity and minimal downtime during the migration process.

### Step 8: Testing

Conduct thorough testing of the network storage to confirm that it is functioning correctly and efficiently, and that all systems can access it as intended.

### Step 9: Monitoring

Establish monitoring systems to continuously check the health and performance of the NAS or SAN, and set up alerts for potential issues.

### Step 10: Maintenance

Implement a maintenance schedule for regular hardware and software updates, backups, and periodic reviews of user access and data usage policies.

## General Notes

### Documentation

Keep detailed documentation of the network storage infrastructure, including network diagrams, device configurations, and change logs.

### Security

Ensure that security best practices are applied, including using encryption for sensitive data and implementing strong authentication mechanisms.

### Compliance

Verify that the deployment and management processes adhere to relevant industry standards and legal requirements to maintain compliance.