## Document for Backing Up On-Prem Nexus

### Introduction

This document outlines a comprehensive backup strategy for an on-premises Nexus repository manager. It covers essential components, detailed procedures, and best practices to ensure data protection and disaster recovery.

### Understanding Nexus Components

* **Database:** Stores metadata about artifacts, users, roles, permissions, and configuration settings.
* **Blob Store:** Contains the actual artifact files (JARs, WARs, etc.).
* **Configuration Files:** Store Nexus-specific settings, repository configurations, and system parameters.

### Backup Strategy

#### Backup Components

* **Database Backup:** Create a complete backup of the database using the native backup tools or Nexus-provided mechanisms.
* **Blob Store Backup:** Back up the blob store containing artifacts using appropriate methods based on the storage type (file-based or object-based).
* **Configuration Backup:** Backup Nexus configuration files to preserve system settings.

#### Backup Schedule and Retention Policy

* Define a backup schedule based on data criticality and change frequency.
* Establish a retention policy to determine how long backups are kept.
* Consider incremental backups to optimize backup time and storage.

#### Backup Destination

* Choose a reliable and secure location for backups (e.g., local storage, network share, cloud storage).
* Implement data encryption for enhanced security.

#### Backup Verification and Testing

* Regularly test the restore process to ensure backup integrity and recoverability.
* Document the restoration procedures for reference.

### Detailed Backup Procedures

#### Database Backup

1. **Stop Nexus:** Ensure Nexus is stopped to avoid inconsistencies.
2. **Access Database:** Establish a connection to the database using appropriate credentials.
3. **Create Database Dump:** Use the database system's native backup tool to create a full dump.
   * Example: pg\_dump -h your\_host -p your\_port -U your\_user your\_database > database\_backup.sql
4. **Transfer Backup:** Move the backup file to the designated backup destination.

#### Blob Store Backup

* **File-Based Blob Store:**
  1. Stop Nexus.
  2. Compress the blob store directory using tar or zip.
  3. Transfer the compressed file to the backup destination.
* **Object-Based Blob Store:**
  1. Utilize the storage provider's built-in backup or versioning features.

#### Configuration Backup

1. Identify configuration files (e.g., nexus.properties, nexus-default.properties).
2. Copy configuration files to the backup destination.

### Backup Automation

* Consider using scripting or scheduling tools to automate the backup process.
* Implement error handling and notifications for backup failures.

### Restore Procedures

* Outline steps for restoring Nexus from backups.
* Include procedures for restoring the database, blob store, and configuration.

### Additional Considerations

* **Backup Compression:** Compress backup files to save storage space.
* **Backup Encryption:** Encrypt backups for enhanced security.
* **Backup Storage Optimization:** Implement strategies for managing backup storage.
* **Disaster Recovery Planning:** Integrate backup procedures into a comprehensive disaster recovery plan.

### Appendices

* Include detailed instructions for specific database systems and blob store types.
* Provide examples of backup scripts and automation tools.
* List relevant contact information for support.

**Note:** This outline provides a general framework. Customize the document based on your specific Nexus environment, database system, blob store type, and security requirements.

## Deep Dive: Data Migration for Nexus on OpenShift (Step 5)

This section delves into the details of migrating data during your Nexus move from on-premises to OpenShift. It covers the three key components: database, blob store, and configuration files.

### 5.1 Database Migration (if applicable)

* **Identify Database Type:** Determine the database management system used by your on-prem Nexus instance (e.g., PostgreSQL, MySQL).
* **Export Database Schema and Data:** Use appropriate tools for your database type to export the schema and data. Common tools include mysqldump for MySQL and pg\_dump for PostgreSQL.
* **Import to OpenShift Database:**
  + **Target Database:** Choose a suitable database service on OpenShift (e.g., PostgreSQL operator).
  + **Import Tool:** Utilize the corresponding import tool for the OpenShift database (e.g., psql for PostgreSQL).
  + **Security:** Ensure secure connection methods like SSH tunneling or secure credentials for the import process.
* **Database User and Permissions:**
  + **Create User:** Create a dedicated database user on the OpenShift database with appropriate permissions for Nexus operations.
  + **Grant Privileges:** Grant the user necessary privileges for accessing and modifying the migrated data within the database.

### 5.2 Blob Store Migration

* **Identify Blob Store Type:** Determine the type of storage used for Nexus artifacts (e.g., local filesystem, network-attached storage).
* **Data Transfer Method:** Choose a method to transfer blob store data to the OpenShift persistent volume:
  + **Manual Copy:** If the data volume is small, consider manually copying the data using tools like scp or rsync.
  + **Backup and Restore:** Utilize existing backup solutions for your on-prem blob store and restore the data to the OpenShift persistent volume.
  + **Streaming Tools:** For large datasets, explore streaming tools like rsync with the -avz flags for efficient transfer with compression.
* **Permissions:** Ensure the Nexus service account on OpenShift has read/write permissions on the mounted persistent volume for blob storage.

### 5.3 Configuration File Restoration

* **Locate Configuration Files:** Identify the location of your Nexus configuration files on the on-premises system (e.g., /etc/nexus-repository-manager).
* **Transfer Configuration Files:** Securely transfer the configuration files to the OpenShift environment (e.g., using scp).
* **Placement and Permissions:** Place the configuration files in the appropriate location within the Nexus container image (as defined by the operator).
  + **Operator Configuration:** Refer to the documentation for your specific Nexus operator to determine the intended location for configuration files.
* **Permissions:** Ensure the Nexus service account has read permissions on the configuration files within the container.

**Important Considerations**

* **Data Integrity:** Verify the consistency and completeness of migrated data after each step (database, blob store, configuration).
* **Security:** Prioritize secure connections and access controls during data transfer and storage on OpenShift.
* **Downtime:** Depending on data volume and chosen methods, expect some downtime during the migration process.

**Additional Tips**

* **Test Migration:** Consider performing a test migration on a non-production environment to validate the process and identify any potential issues.
* **Documentation:** Document the specific tools, commands, and configurations used during the migration for future reference.
* **Version Compatibility:** Ensure compatibility between your on-prem data formats and the OpenShift database and Nexus operator versions.

By following these detailed steps and considering the additional recommendations, you can effectively migrate your Nexus data to OpenShift, ensuring a smooth transition to your new containerized environment.