Table of Contents

Introduction and Background

This document outlines Docupal Demo, LLC's proposal to update and upgrade Acme, Inc's (ACME-1) current Elasticsearch environment. ACME-1 currently utilizes Elasticsearch version 7.9 in an on-premise, Kubernetes-managed deployment.

Current Environment

ACME-1's existing Elasticsearch 7.9 deployment serves as a critical component of their infrastructure. However, several factors necessitate a move to a more current version.

Rationale for Upgrade

The primary driver for this upgrade is that Elasticsearch 7.9 has reached its end-of-life. This means it no longer receives official support, including critical security patches and bug fixes. Continuing to operate on an unsupported version introduces significant risks.

Beyond the end-of-life concerns, upgrading Elasticsearch will enable ACME-1 to leverage a range of new features and performance enhancements available in later versions. The current deployment experiences performance bottlenecks that can be addressed through the optimizations present in newer releases. An upgrade will also enhance overall system security and improve maintainability.

Objectives and Scope

The primary objective of this Elasticsearch update/upgrade is to enhance ACME-1's search capabilities and overall system performance. We aim to achieve a 20% improvement in query speed, fortify security measures, and streamline operational workflows. This initiative targets an upgrade to Elasticsearch version 7.17.

Upgrade Scope

This project encompasses all of ACME-1's Elasticsearch clusters, including those used for production, staging, and development environments. The scope specifically excludes the archive data cluster. Our team will focus on migrating existing data, configurations, and applications to the new Elasticsearch version. The upgrade process includes thorough testing and validation to ensure system stability and data integrity. We will provide comprehensive documentation and training to ACME-1's team to facilitate a smooth transition and ongoing management of the upgraded environment.

Current Architecture and Environment Analysis

ACME-1's current Elasticsearch environment consists of a cluster designed for both stability and performance. The cluster comprises three master nodes responsible for cluster management and fifteen data nodes that handle data storage and processing.

Cluster Configuration

The data is organized into indices, each configured with five primary shards to maximize search concurrency, alongside one replica to ensure data redundancy and high availability. This configuration allows for fault tolerance, as the replica shard can take over if a primary shard fails.

Integrations and Plugins

ACME-1 leverages several key integrations to enhance its Elasticsearch capabilities. Logstash serves as the primary data ingestion pipeline, collecting data from various sources and preparing it for indexing. Kibana provides a user-friendly interface for data visualization and exploration. Beats are deployed across different systems for lightweight data shipping. The cluster also utilizes the ingest-geoip plugin to enrich data with geographical information and analysis-icu for advanced text analysis.

Data Flow and Indexing

The data flow follows a standard pattern. Logstash receives data from diverse sources, transforms it as needed, and then forwards it to the Elasticsearch cluster. Custom indexing templates are in place to ensure that data is indexed consistently and efficiently, optimizing search performance.

Performance and Usage Metrics

Available metrics provide insights into the cluster's operational health and resource utilization. These metrics include CPU utilization, memory usage, query latency, and indexing rate. Monitoring these metrics is crucial for identifying potential bottlenecks and ensuring optimal performance.

Upgrade Impact and Benefits

The Elasticsearch update will deliver significant improvements to ACME-1's search infrastructure. This will affect performance, security, and available features. End-users will experience tangible benefits from these enhancements.

Performance Enhancements

We anticipate a 20% reduction in query latency after the upgrade. This means faster search results for ACME-1 users. Indexing speed is also expected to increase by 15%. This improvement will enable quicker processing of new and updated data.

New Features and Capabilities

The upgrade introduces an improved query language. This allows for more complex and precise searches. Enhanced security features, including an upgrade to TLS 1.3, will provide stronger data protection. New APIs will also be available. These will enable more flexible integration with other systems.

Security Improvements

Upgrading to TLS 1.3 will encrypt data in transit more effectively. This protects against eavesdropping and data breaches. Enhanced role-based access control provides more granular control over user permissions. This minimizes the risk of unauthorized access to sensitive data. ACME-1's overall security posture will improve significantly.

End-User Benefits

End-users will experience faster search results due to reduced query latency. The improved query language will also enable more relevant search results. Enhanced data visualization capabilities will provide users with better insights. These improvements will lead to increased productivity and better decision-making.

Compatibility and Dependencies

This section details the compatibility considerations for upgrading ACME-1's Elasticsearch cluster to version 7.17. We have assessed potential impacts on existing plugins, integrations, and dependencies.

Plugin Compatibility

Currently, ACME-1 utilizes the ingest-geoip plugin. While we anticipate minimal impact, thorough testing of this plugin will be conducted in the test environment to ensure continued proper functionality after the upgrade. All other plugins will be reviewed and tested as well.

API and Integration Compatibility

A key focus will be ensuring forward and backward compatibility of APIs and integrations. Before commencing the upgrade, Docupal Demo, LLC will verify that all existing integrations are compatible with Elasticsearch version 7.17. This proactive approach aims to minimize disruptions and ensure a seamless transition.

Breaking Changes and Mapping Definitions

Elasticsearch version 7.17 includes potential breaking changes, particularly concerning mapping definitions. Docupal Demo, LLC will analyze ACME-1's current mapping configurations and make necessary adjustments to align with the new version's requirements. This may involve updating existing mappings or creating new ones to maintain data integrity and search performance. The team will work to identify and mitigate potential issues related to these changes.

Dependency Version Constraints and Migration

Careful attention will be given to dependency version constraints. Docupal Demo, LLC will document all dependencies and their respective versions to ensure compatibility with Elasticsearch 7.17. Any necessary migration paths for dependencies will be clearly outlined and executed in a controlled manner.

Risk Assessment and Mitigation Strategies

This section identifies potential risks associated with upgrading the Elasticsearch cluster and outlines mitigation strategies. We aim to minimize disruption and ensure a smooth transition to the new version.

Potential Risks

The primary risks associated with the Elasticsearch upgrade are:

- **Data Loss:** Data corruption or loss during the upgrade process.
- **Downtime:** Interruption of service during the upgrade.
- **Application Incompatibility:** Issues arising from incompatibility between the upgraded Elasticsearch version and existing applications.

Mitigation Strategies

To mitigate these risks, we will implement the following strategies:

- **Full Cluster Backup:** Before initiating the upgrade, a complete backup of the entire Elasticsearch cluster will be performed. This backup will serve as a safety net, allowing us to restore the cluster to its previous state in case of unforeseen issues.
- **Rolling Upgrade Strategy:** We will employ a rolling upgrade approach. This involves upgrading nodes one at a time, minimizing downtime and maintaining cluster availability throughout the process. Each node will be upgraded and tested before moving on to the next, ensuring stability.
- **Compatibility Testing:** Prior to the production upgrade, we will conduct thorough compatibility testing in a staging environment. This testing will identify and address any potential issues between the upgraded Elasticsearch

version and existing applications.

Contingency Plans

In the event of critical issues during or after the upgrade, we have the following contingency plans in place:

- **Rollback to Version 7.9:** If the upgraded cluster exhibits significant problems, we can quickly roll back to the previous Elasticsearch version (7.9) using the pre-upgrade backup.
- **Restore from Backup:** In the event of data loss or corruption, we can restore the cluster from the most recent backup. We will regularly verify our backups to ensure their integrity.

Testing and Validation Plan

This plan outlines the testing strategy for validating the Elasticsearch update/upgrade. We will use a multi-faceted approach to ensure a stable and performant environment for ACME-1.

Testing Types

We will conduct the following types of tests:

- **Functional Testing:** Verifies that all features are working as expected after the upgrade.
- **Performance Testing:** Measures the system's responsiveness and stability under load.
- **Integration Testing:** Confirms that Elasticsearch integrates correctly with other systems.
- **Regression Testing:** Ensures that existing functionality remains intact after the upgrade.

Testing Environments

Testing will occur across three environments:

1. **Development:** Initial testing and issue identification.
2. **Staging:** A production-like environment for comprehensive testing.

3. **Production:** Limited testing post-upgrade to confirm stability.

Success Measurement

Success will be measured by comparing performance metrics before and after the upgrade. Key metrics include search latency, indexing speed, and resource utilization. We will establish baseline metrics prior to the upgrade against which post-upgrade performance will be judged. Acceptable variance thresholds will be defined for each metric. Successful completion of all test types, without critical errors, in each environment will be required for final validation.

Implementation and Rollback Plan

This section outlines the plan for implementing the Elasticsearch update/upgrade, including key phases, timelines, and rollback procedures.

Upgrade Implementation Phases

The upgrade process will consist of five key phases: planning, preparation, testing, execution, and validation. Each phase is designed to ensure a smooth and controlled transition to the new Elasticsearch version.

- **Planning (2 weeks):** This initial phase involves detailed assessment of the current environment, compatibility checks, resource allocation, and defining specific upgrade objectives. We will finalize the upgrade strategy and create a detailed project plan.
- **Preparation (2 weeks):** This phase focuses on preparing the environment for the upgrade. This includes backing up existing data, preparing the new Elasticsearch cluster or nodes, and configuring necessary settings.
- **Testing (4 weeks):** A comprehensive testing phase will be conducted in a non-production environment. This will include functional testing, performance testing, and user acceptance testing to identify and resolve any potential issues before the production upgrade.
- **Execution (1 week):** The execution phase involves performing the actual upgrade on the production environment. This will be carefully monitored to ensure a smooth transition.
- **Validation (1 week):** After the upgrade, a thorough validation process will be conducted to ensure that all systems are functioning correctly and that the upgrade has been successful.

Rollback Plan

In the event of a critical failure during or after the upgrade, a rollback plan is in place to restore the system to its previous state. Two rollback procedures are defined:

1. **Restore from Backup:** Prior to the upgrade, a full backup of the Elasticsearch data and configuration will be created. In case of a catastrophic failure, the system can be restored from this backup. This rollback strategy will cause downtime dependent on the data size.
2. **Rollback to Previous Version:** Where feasible, the upgrade will be designed to allow a rollback to the previous Elasticsearch version. This involves reverting the changes made during the upgrade process. This rollback strategy will be employed if possible to minimize downtime.

The rollback plan will be tested during the testing phase to ensure its effectiveness. The decision to initiate a rollback will be made based on the severity of the issues encountered and the estimated time to resolution. A detailed communication plan will be executed to keep all stakeholders informed throughout the rollback process.

Cost and Resource Analysis

This section outlines the estimated costs and resource allocation required for the Elasticsearch update/upgrade project for ACME-1. The costs include hardware (if necessary), software subscriptions, and labor. We have also considered the licensing implications of new features in the upgraded Elasticsearch version.

Resource Allocation

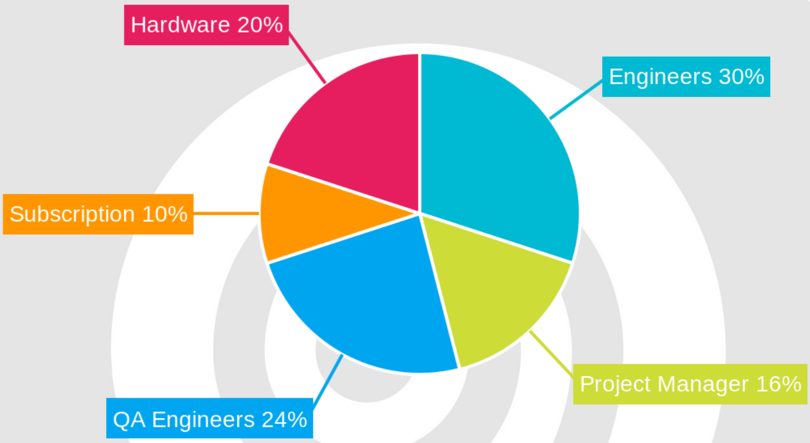
The following human resources will be allocated to this project:

- 2 Elasticsearch Engineers
- 1 Project Manager
- 2 QA Engineers

Cost Estimation

The following table breaks down the estimated costs associated with the Elasticsearch upgrade. Note that hardware costs are contingent on whether the existing infrastructure can support the upgraded Elasticsearch version.

Item	Estimated Cost (USD)
Elasticsearch Engineers	15,000
Project Manager	8,000
QA Engineers	12,000
Software Subscription Adjustments (if applicable)	5,000
Hardware (if required)	10,000
Total Estimated Cost	**50,000**



Licensing

We will review the licensing implications of any new features introduced in the upgraded Elasticsearch version with Elastic to ensure compliance and optimize cost-effectiveness.

Timeline and Milestones

Project Timeline and Milestones

This Elasticsearch update/upgrade project is anticipated to take 10 weeks. We will avoid any upgrade activities during ACME-1's peak business hours.

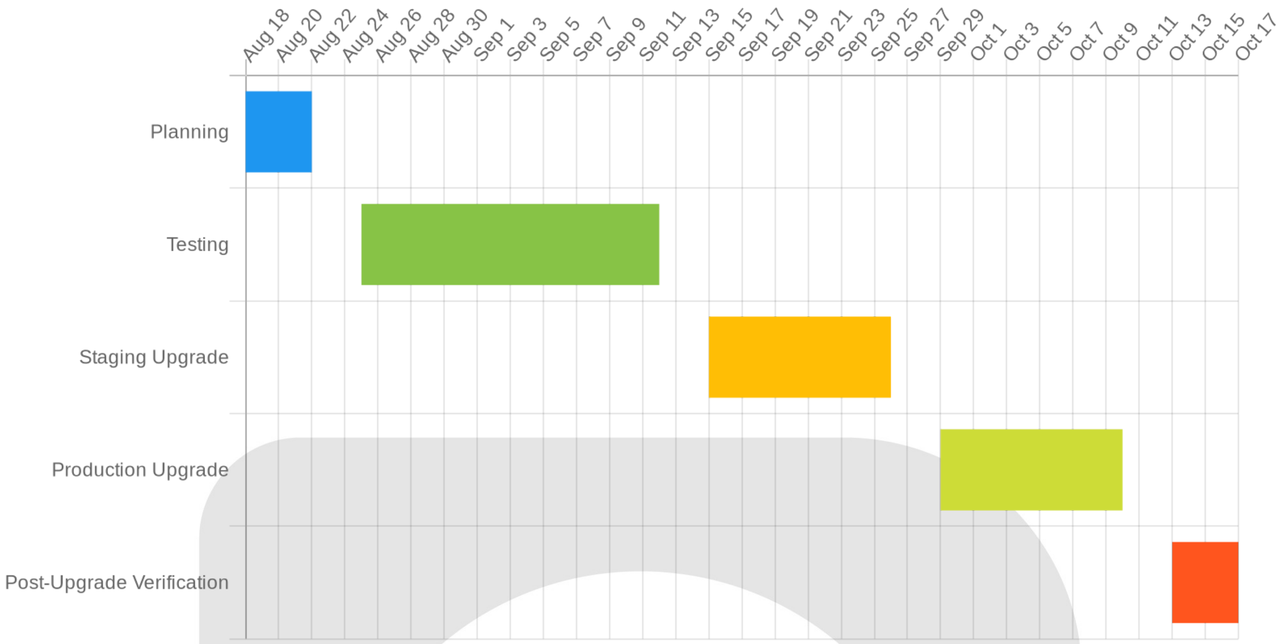
Key Milestones

The project includes these critical milestones:

- Completion of testing.
- Successful upgrade of the staging environment.
- Production upgrade.

Detailed Schedule

Task	Start Date	End Date
Planning	2025-08-18	2025-08-22
Testing	2025-08-25	2025-09-12
Staging Upgrade	2025-09-15	2025-09-26
Production Upgrade	2025-09-29	2025-10-10
Post-Upgrade Verification	2025-10-13	2025-10-17



Conclusion and Recommendations

The proposed Elasticsearch upgrade to the latest version offers significant advantages for ACME-1. Staying on a supported version is crucial for receiving security patches and bug fixes. This upgrade will enhance system performance and provide access to the newest features.

Key Takeaways

The primary benefits of this upgrade include:

- **Enhanced Security:** Ensures ACME-1 benefits from the latest security measures.
- **Improved Performance:** Optimizes Elasticsearch for faster data processing and retrieval.
- **Continued Support:** Guarantees access to ongoing updates and support from Elastic.

Recommendation

We strongly recommend proceeding with the Elasticsearch upgrade. We await final approval from the ACME-1 security team to commence the upgrade process. This upgrade is a strategic investment that will safeguard ACME-1's data and improve operational efficiency.

Appendices and References

This section provides supplementary information related to the Elasticsearch update/upgrade proposal for ACME-1. It includes supporting documents and technical references used in preparing this proposal by Docupal Demo, LLC.

Supporting Documents

- Upgrade Guide: Details the step-by-step process for the Elasticsearch upgrade.
- Test Plan: Outlines the testing procedures to validate the upgraded Elasticsearch environment.
- Rollback Procedure: Describes the steps to revert to the previous Elasticsearch version if needed.

Technical References

- Elasticsearch Version Change Logs: Official Elasticsearch documentation detailing changes between versions.