Keyfactor Command Upgrade: 10.4.3 to 11.0

Summary of Required Configuration and Code Changes

This document outlines the required changes and considerations when upgrading Keyfactor Command from version 10.4.3 to 11.0. The upgrade introduces key architectural modifications, feature deprecations, and enhanced capabilities. The following summary provides a high-level checklist of tasks to ensure compatibility and system continuity.

## 1. Migration from Classic (CMS) API

* The Classic API is fully removed in version 11.0.
* Any integrations using CMSService.asmx or SOAP-based endpoints must be migrated to the Keyfactor REST API (/KeyfactorAPI).
* As a temporary fallback, the AllowDeprecatedApiCalls setting may be enabled, but this is not recommended for long-term use.

## 2. Replacement of Keyfactor Java Agent

* The Keyfactor Java Agent is deprecated in favor of the Universal Orchestrator (UO) and the Remote File Orchestrator (UFO).
* If the Java Agent is currently used to manage JKS, PEM, or similar store types, transition to the Remote File Orchestrator extension.
* Update orchestrator registration and relevant store type definitions to align with the new model.

## 3. Script and Handler Management

* PowerShell scripts for handlers and workflows are now stored in the database, not the filesystem.
* During the upgrade, existing scripts will be auto-imported into the database.
* All new scripts must be registered using the Script Management API or through the administrative user interface.
* Scripts should be reviewed for compatibility with PowerShell 7.

## 4. Updated Role and Permission Model

* A new granular permission system replaces the previous model.
* Permissions under the 'PKI Admin' umbrella are now split into: Certificate Authorities (Read/Modify) and Certificate Templates (Read/Modify).
* Existing roles will be mapped automatically, but manual review is recommended to confirm access integrity.

## 5. vSCEP Installation Change

* The vSCEP service is no longer included with the main installer.
* If required, it must be deployed separately on a dedicated server.
* Plan for this separation as part of the infrastructure upgrade.

## 6. OAuth 2.0 and Identity Provider Changes

* Keyfactor 11.0 supports OpenID Connect (OIDC) for authentication.
* Admin users must now be configured using the <AdminUsers> configuration format.
* Any script or integration utilizing the Security Role API must now use version 2 (v2) endpoints.
* SSH key management is currently not supported under OIDC.

## 7. Certificate Store Type Updates

* The following built-in store types are removed unless currently in use: IIS, F5, AWS ACM, NetScaler.
* If you rely on these types, deploy the corresponding orchestrator extensions (e.g., IIS or F5 extension).
* Recreate certificate store types where necessary and install updated orchestrator plugins.

## 8. Deprecation of Prescript and Postscript Functionality

* The pre/post script execution capabilities in orchestrators are deprecated.
* Transition to using workflow job completion handlers or event-driven scripts in Keyfactor Command.

## 9. Changes to Expiration Alerts

* Expiration alerts now store their own execution timestamps.
* Confirm that each alert runs independently and is not affected by a shared schedule.
* Remove any use of the LastRun attribute in automation scripts or alert logic.

## 10. Orchestrator Job and Heartbeat Configuration

* New orchestrator settings have been introduced: LockTimeout, HeartbeatInterval.
* These must be defined in appsettings.json for high-availability or distributed deployments.
* All orchestrator agents should be updated to ensure compatibility with Keyfactor Command 11.0.

## 11. Remote File Orchestrator (UFO)

* For management of file-based certificates (PEM, JKS, Apache, etc.), ensure use of the UFO with Universal Orchestrator version 10.4 or higher.
* The Java Agent and Windows Orchestrator are deprecated and should no longer be used.
* Containerized deployment of the Universal Orchestrator is now supported and recommended for scalable environments.

## 12. Orchestrator Version Compatibility

* Minimum Recommended: Version 10.4
* - May still function but lacks full compatibility with newer features.
* - Not recommended for future-proofing or scalability.
* Fully Supported and Recommended: Version 11.0
* - Provides access to updated extensions, container support, and enhanced orchestrator APIs.
* - Required for new capabilities such as distributed locking and container-based orchestration.
* Incompatible: Version 10.1
* - Not supported for use with Command 11.0.
* - Must be upgraded.

## Summary Recommendation

* All orchestrators currently running on version 10.1 must be upgraded.
* Orchestrators running on version 10.4 should be upgraded to version 11.0 for full feature parity and long-term support.
* Align orchestrator configurations with version 11.0 requirements to prevent operational disruptions.