Upgrading Registry to v3.3.0

Manual Schema Update May Be Required

⚠ *These alter table steps should now automatically be handled by UpgradeShell.*

Some columns have been resized. Due to a bug in the underlying schema management library, this resize may not automatically happen on Postgres. If necessary, manually resize the columns.

```
sql=> alter table cm_ssh_keys alter column type type varchar(32);
sql=> alter table cm_co_jobs alter column job_type type varchar(32);
sql=> alter table cm_co_localizations alter column text type varchar(512);
```

Manual Data Update May Be Required

Registry v2.0.0 introduced an internal flag to identify "automatic" groups, ie: those where Registry automatically manages the population. Groups created since this update will have the correct flag, however groups that existed prior to this update will have a NULL value in the relevant column. While in general most capabilities will work correctly, Identifier Assignment for CO Groups (a new capability introduced in Registry v3.3.0) may not correctly apply to CO Groups that were created prior to Registry v2.0.0. Ordinarily, this would be corrected as part of upgradeVersion, however due to limitations of the framework this fix must be applied manually.

It is recommended that all deployments that were first established on a release earlier than v2.0.0, whether or not they plan on using Identifier Assignment for CO Groups, run the following SQL command:

```
sql=> update cm_co_groups set auto=false where auto is null;
```

Enrollment Flow Steps "Deny" and "Send Approval Notification" Removed

Registry v3.3.0 consolidates three Enrollment Flow Steps into the *Approve* step, eliminating the *Deny* and *Send Approval Notification* steps. Custom plugins that execute after *Deny* or *Send Approval Notification* should be updated to execute after *Approve* instead.

SSH Key Authenticator Plugin

SSH Key management has moved into an Authenticator Plugin. During the upgrade to v3.3.0, any CO that has SSH Keys attached to a CO Person will have an SSH Key Authenticator automatically instantiated, and existing keys will be attached to that Authenticator. COs that do not have any SSH Keys will need to instantiate an Authenticator before SSH keys can be managed.

SSH Keys are no longer managed directly from the CO Person Canvas, but are now available via the *Authenticators* link in the sidebar.

Authenticator Plugin Documentation

The guidance for when Authenticator Plugins should trigger provisioning has been corrected.

JobShell and Job Plugins

Registry v3.3.0 introduces Job Plugins, as executed by the Registry Job Shell. All existing deployments will likely need to update their cron configuration, as described in Registry Installation - Cron.

API User Changes

As of Registry v3.3.0, API Users are assigned to specific COs. Full information is available in the documentation, however the following changes should be noted:

- New API Users must be named with their CO as a prefix.
- Self selected passwords are no longer supported, instead randomly generated API Keys are used.
- Platform API Users are now created via the COmanage CO.

Existing API Users (those created prior to upgrade) will continue to function as is, and will be automatically assigned to the COmanage CO as Platform API Users (without being renamed). However any subsequent changes to existing API Users will require conformance with the new naming and API Key requirements. It is recommended that existing API Users be manually transitioned at a convenient time.

cm_users View Removed

The cm_users database view has been removed. This view should not have been accessed by other applications.

Unix Cluster Plugin

Registry v3.3.0 introduces Cluster Plugins, and specifically the Unix Cluster Plugin. As a result, the behavior of the LDAP Provisioning Plugin as it relates to the posixAccount schema. Deployers dependent on the previous (Registry v3.2.x and earlier) experimental behavior should review the new mechanism carefully before upgrading.

Service Tokens (Application Specific Passwords)

Two experimental plugins, *CoServiceToken* and *LdapServiceTokenProvisioner*, have been removed. Service Token functionality is available via the Password Authenticator Plugin and LDAP Provisioning Plugin. No automatic conversion mechanism is provided, but Service Tokens are stored as plain text, so it should be possible to directly convert them to Passwords of type PasswordEncodingEnum::Plain. (This will require direct SQL manipulation.)

> ⚠️ Deployments that are using the voPerson schema **and** have an LDAP Provisioner configured with *Unconfigured Attribute Mode* set to *Remove* will need to update to the (currently draft) 2.0.0 version of voPerson due to the addition of the voPersonApplicationPassword attribute.
>
> Note that voPerson 2.0.0 changes OIDs for all attributes. Registry is not directly affected by the OID change as the LDAP Provisioner only uses attribute names, not OIDs, however the new voPersonApplicationPassword is only defined in the new OID space. It is recommended that all OIDs be updated when upgrading.

HTTP Server SSL Certificate Configuration

HTTP Server configurations now support the ability to enable and disable SSL certificate and hostname verification. By default, existing configurations (used only by the Crowd Provisioning Plugin) will have verification enabled as part of the upgrade process, matching the default behavior of v3.2.x.

voPerson Schema Changes

The LDAP Provisioning Plugin adds support for the attribute voPersonApplicationPassword. This attribute is defined in voPerson 2.0.0, which has not been released yet. Deployers using voPerson may need to update their LDAP servers to support the draft 2.0.0 schema, which is available here.

voPerson 2.0.0 also changes the OID space in which attributes are numbered. While this does not directly affect the Plugin (which only uses attribute names, not OIDs), LDAP servers using voPerson may need to be reconfigured to use the new OID numbers. This process varies by LDAP server, but should generally only require a reconfiguration and not a full data reload.