# Migration Challenges

* [AAP 2.4 to 2.6](https://docs.google.com/document/d/1TiNImee2mNfRCKu3RJ9LrKFS59SM2YAhc5VpcuAOF90/edit?tab=t.0#heading=h.7zyo512i8thg)

### Authentication & Identity

* **Platform Gateway introduction** (introduced in 2.5)
  + Centralized point for managing and accessing components of the platform.
* **All SSO (SAML, LDAP, OIDC, RADIUS) must be reconfigured** against the gateway instead of directly into the Controller/Hub.
* **Custom authentication scripts** (e.g., Django middleware or Python extensions in /etc/tower/conf.d/) may break because the gateway now intermediates login flows.
* **API tokens are now gateway-issued**, not service-issued. If scripts or integrations depend on old token flows, they’ll fail.
* **Account linking:** After the upgrade, users must link Controller/Hub accounts to a single gateway identity. If automation relies on “service accounts” tied to the Controller, this may disrupt playbook runs and API calls.
* **LDAP User migration** ([link](https://docs.redhat.com/en/documentation/red_hat_ansible_automation_platform/2.5/html-single/installing_on_openshift_container_platform/index#con-migrate-LDAP-users_aap-post-upgrade))
  + LDAP configurations not migrated automatically
  + Legacy settings are carried over, acts as reference and facilitate the migration
  + A new configuration targeting the gateway LDAP authenticator is needed
  + Mapping between organizations/teams and LDAP groups must be redone at the gateway. ([link](https://docs.redhat.com/en/documentation/red_hat_ansible_automation_platform/2.5/html-single/access_management_and_authentication/index#gw-mapping))

### API & Integration Compatibility

* **Controller and Hub APIs still respond** but are flagged as deprecated; long term, consumers must move to the gateway API. ([link](https://docs.google.com/document/d/1UlEoeuGJbcTIzCdO7DasQX6zOJqAgeivE19ifpabHVQ/edit?tab=t.0#heading=h.q86q5bm3enbc))
* Integrations with ServiceNow, ticketing, CMDB, or custom API scripts may break if they rely on authentication headers or endpoints that change.
* **OAuth apps**: Controller OAuth apps do not migrate. Integrations that depend on them will break unless recreated at the gateway.

### 

### Network & Automation Mesh

* Gateway adds a new hop. If firewall/proxy rules were tightly scoped for Controller/Hub only, automation will fail until updated.
  + *Our guess is the network is opened between the OCP cluster -> execution node, if Citi intends to re-use the existing execution nodes for the network deployment, then the existing rules should suffice.*
* Remote execution nodes
  + *RHEL 8 seems to be still supported (see* [*link*](https://docs.redhat.com/en/documentation/red_hat_ansible_automation_platform/2.5/html-single/installing_on_openshift_container_platform/index#operator-add-execution-nodes_operator-upgrade)*). This will be validated by Red Hat Services prior to the upgrade.*
* **TLS requirements:** Cipher suite defaults may have shifted. If you use TLS inspection or pinned certs, connections may fail.

### Load Balancers & Proxies

* **Known break:** Controller behind LB may show “Error connecting to Controller API” until CSRF\_TRUSTED\_ORIGIN includes the gateway URL.
* **Proxy edge cases:** If you terminate TLS at the proxy and re-encrypt internally, the gateway may reject mismatched headers or untrusted certs.

### 

### Minimizing downtime

* Assuming 2 cluster-scoped operators, Is a **few hours** of downtime per namespace upgrade **acceptable**?
  + YES, **Recommendation:** *In Place Two Operators*
    - We need to test will real data to estimate the maintenance window
    - **Worst case scenario:** upgrade time + post upgrade tasks + rollback + buffer
  + NO, **Recommendation:** *Side by Side One Cluster*
    - **Complexity:** Due to replication
    - **Easier to rollback:** Remove replicated namespaces & second operator
    - Existing deployments will remain unmodified and running until ready

### Lab for testing

* Ayyappa 2.5 upgrade test was performed in a temporary cluster, which was **only available for a few days**.
* There are two lab environments available at Citi to test with. Lab 04d and lab 06d. Proper communication with the OCP engineering/operations teams should be ensured to best utilize the two environments for migration testing.
* How can we handle 2.5 and 2.6 in LAB?

### Coordination & Communications

* Teams involved and responsibilities
  + DB, OCP, AAP, Networking
* Customers communications
* How should we track? Confluence ? Spreadsheets?

### COB Cluster

* Architecture
  + DB shared with Prod
  + Only one up at the same time
* How is it handled when not in use?
  + AAP deployments scaled down?
  + Up but no traffic?
* How should we handle this cluster ?

### 

### Platform Install Automation (Bitbucket)

* We may need to adjust the Ansible role and job template survey.
* Any additional platform-related operations, whether manual or automated, that we should be aware of?
  + Especially operations whose results will not be reflected in the database or CR.

### Anything else?