Fermilab Federated Identity Project Status Update

Mine Altunay

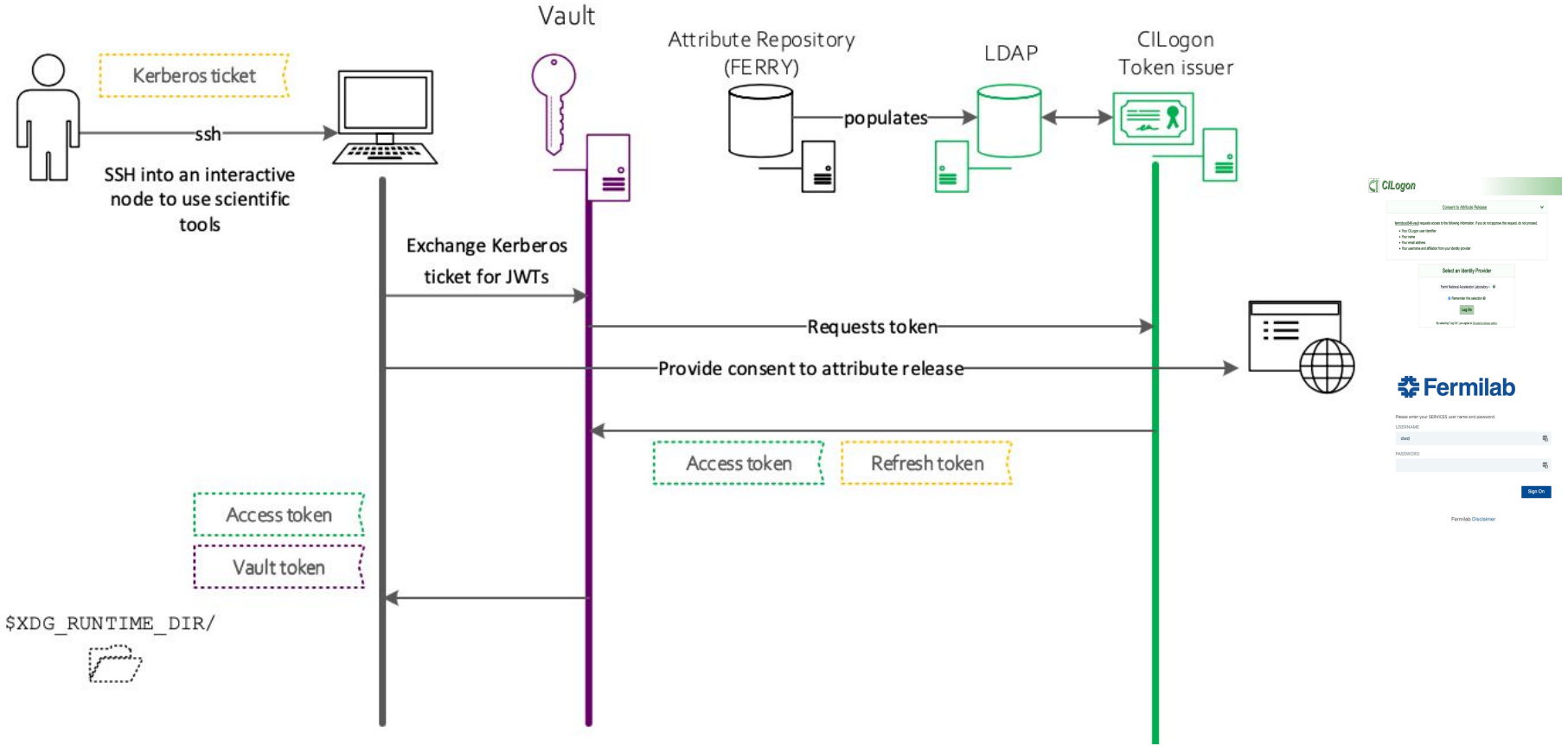
WLCG Grid Deployment Board

June 9, 2021

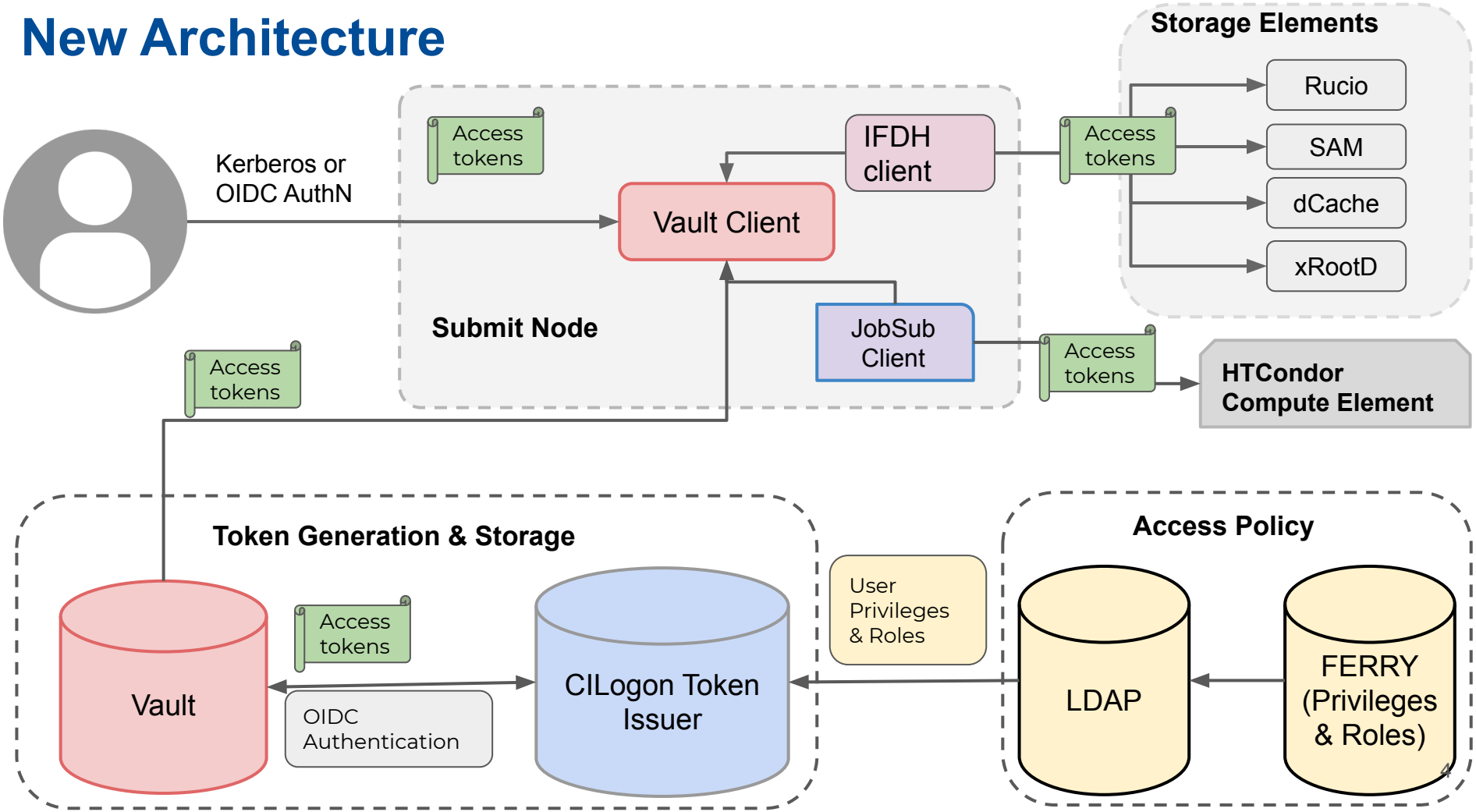
Federated Identity Project at Fermilab

- The goal of our project is to provide our scientific collaborators with federated access to our lab's scientific infrastructure and resources.
  - Our collaborators will access the lab's resources by using their identity credentials issued by our partner institutions.
- There are two phases of the project.
  - We are in Phase 1, where we design and build the architecture and will only allow access to users with Fermilab accounts.
  - In Phase 2, we will develop policy and procedures to design how to extend the federated access to users at our partner institutions.

Integrating token-based technologies



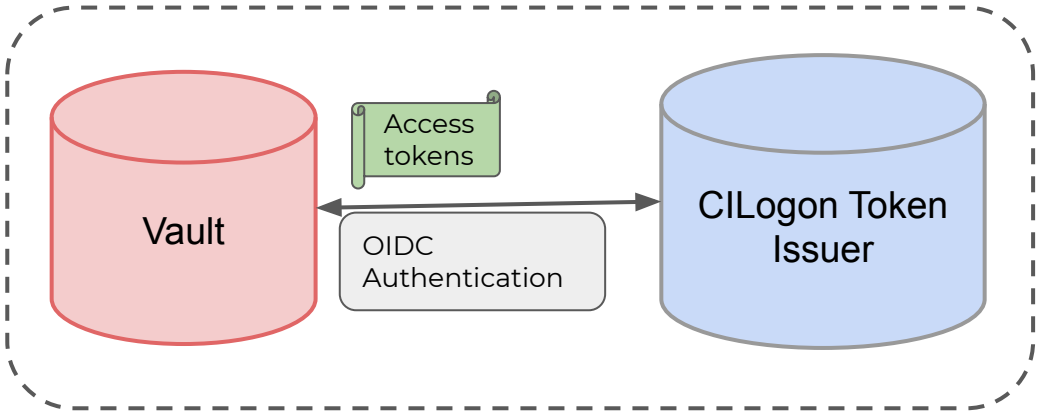
New Architecture



New Architecture

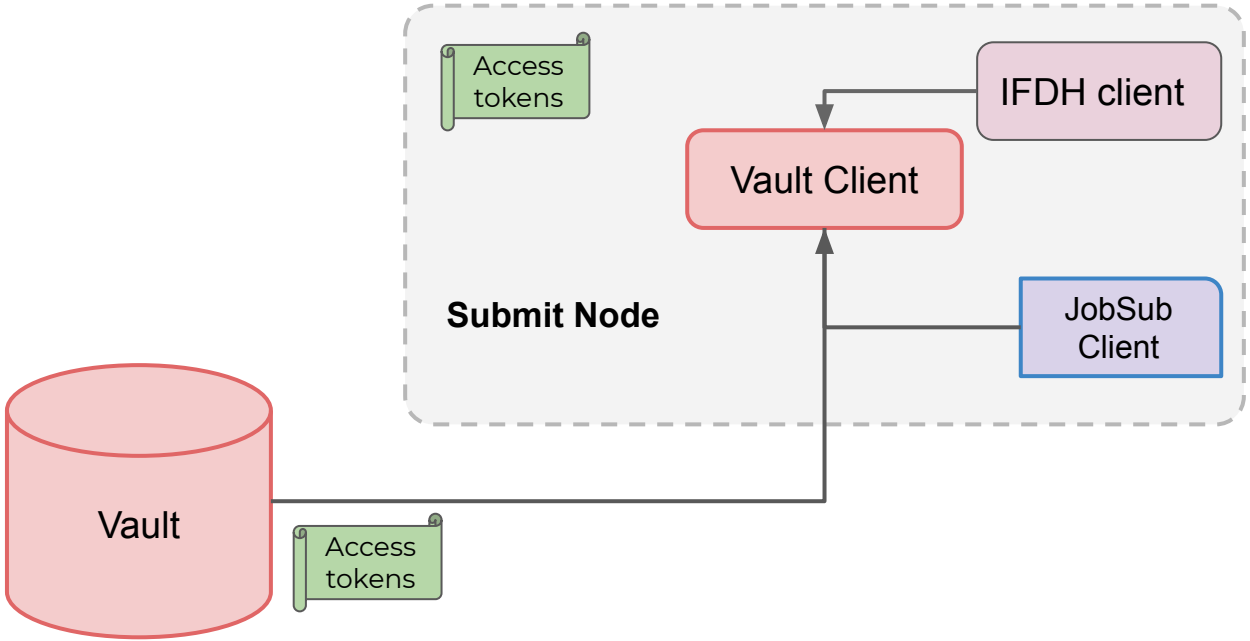
- Vault, CILogon and Ferry+LDAP are the main components of our architecture.
- CILogon is our Token Issuer.
- Vault is our token repository and also a client to CILogon Token Issuer to generate and receive tokens.
- Vault Client is at the submit node and retrieves generated tokens from the Vault repository. If there is no stored token, Vault generates a new one and sends it to the Vault Client.
- Ferry is the central database where we store each users' privileges and roles (access policy). These privileges are sent to LDAP so that CILogon Token Issuer can read them programmatically and generate tokens accordingly.

Current Status: Token Generation and Storage



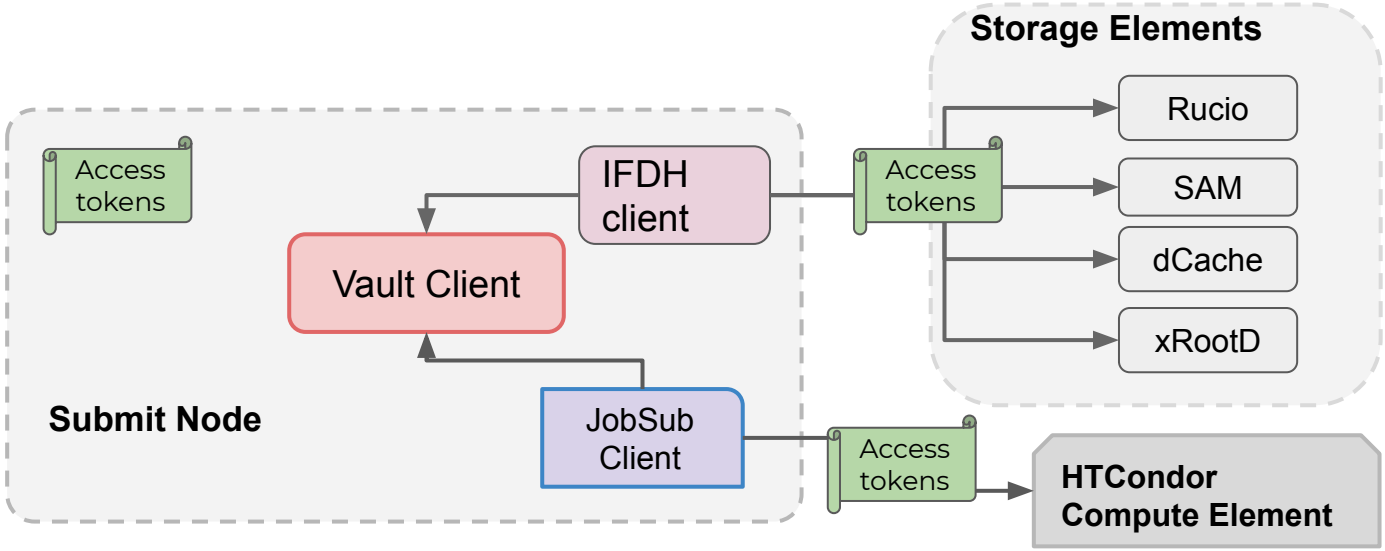
- CILogon Token Issuer is installed and successfully generates tokens.
- Vault is installed, and it successfully requests, receives and stores tokens.
- The OIDC authentication handshake between Vault and CILogon is successful and crucial for the success of our project.

Current Status: Token Renewal and Retrieval



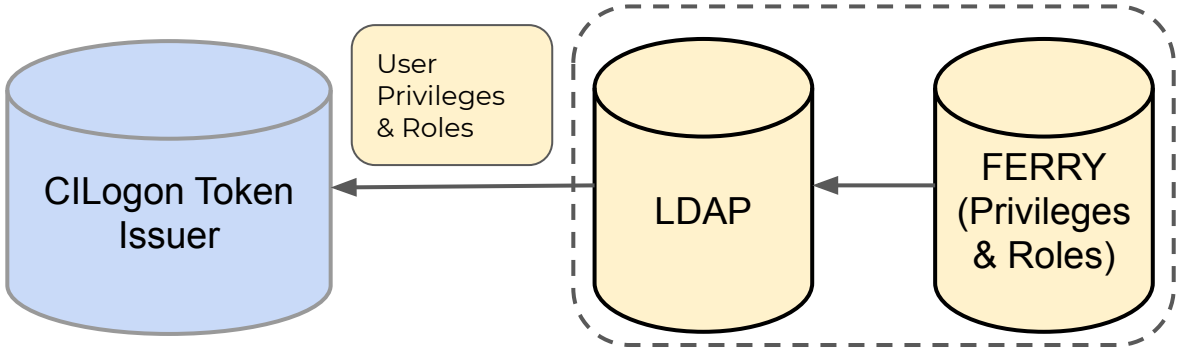
- We implemented the Vault Client and tested it with the Vault server.
- We can successfully store access tokens on the submit node.
- When tokens expire, Vault can renew access tokens and stores them.

Current Status: Compute and Storage Access with Tokens



- We generated a test token with storage capabilities. We successfully gained access to dCache by using this token.
- We generated a test token with the job compute capabilities. We can successfully submit and run a test job.
- We repeated our tests with individual tokens and the robot tokens used for automated processes successfully.
- Due to a recently discovered bug in HTCondor, we will repeat our tests after the bug is fixed by HTCondor.

Current Status: Access Policy



- An LDAP server is installed and tested.
- Initially the privileges are entered into LDAP manually for test purposes.
- We are in the process of building a programmatic connection between LDAP and Ferry. Most of the methods that are needed to populate the LDAP with attributes from Ferry have been implemented.
- The programmatic connection between LDAP and CILogon Token Issuer is tested successfully. We can generate tokens according to the test capabilities entered into the LDAP.

Remaining Work and Future

- Basic building blocks of our architecture is installed and tested.
- We are in very good synch with CERN and WLCG.
- Our top priority in Phase 1 is to complete and test our architecture with tokens.
  - Repeat our test with compute jobs.
  - Complete the programmatic connection between Ferry and LDAP.
  - Test our architecture with token based and certificate based access. We need both of them to work simultaneously during the transition phase.