

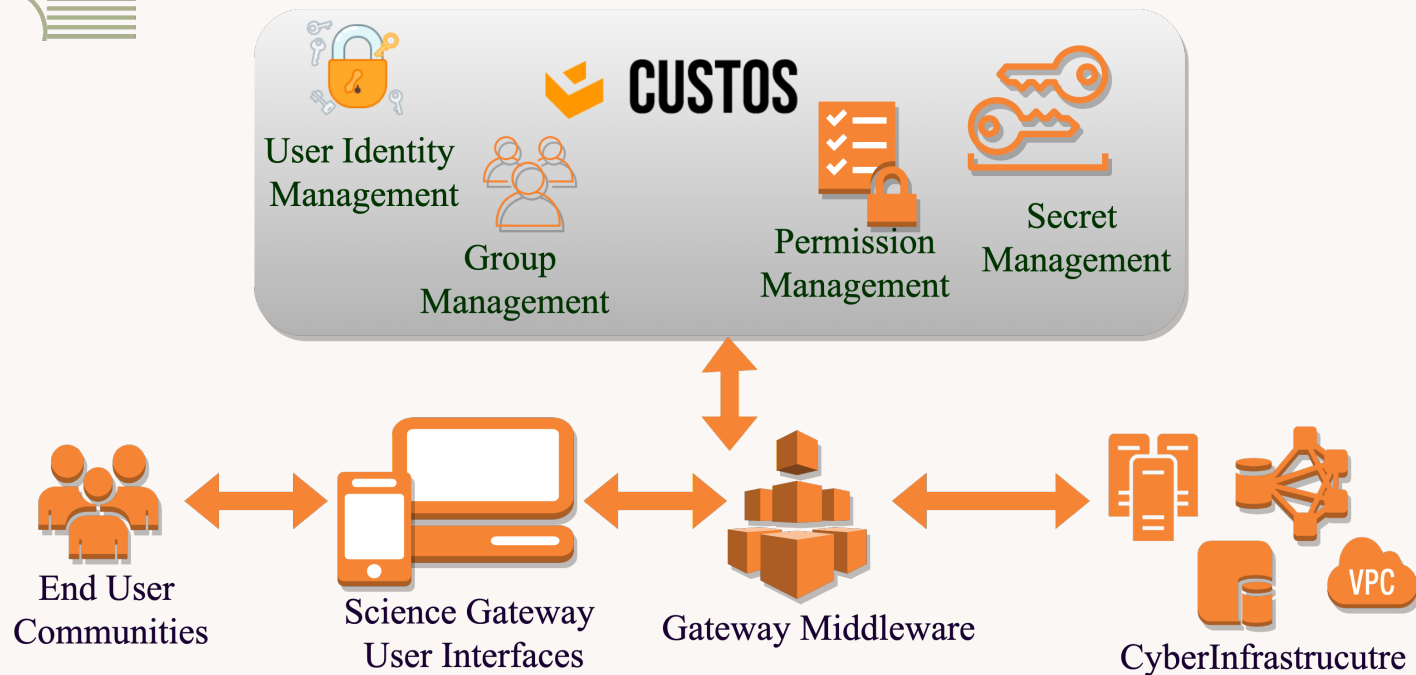


Science Gateway Integration Examples with the Custos Security Service

Isuru Ranawaka, Samitha Liyanage, Dannon Baker, Alexandru
Mahmoud, Juleen Graham, Terry Fleurry, Dimuthu
Wannipurage, Yu Ma, Enis Afgan, Jim Basney, Suresh Marru,
Marlon Pierce

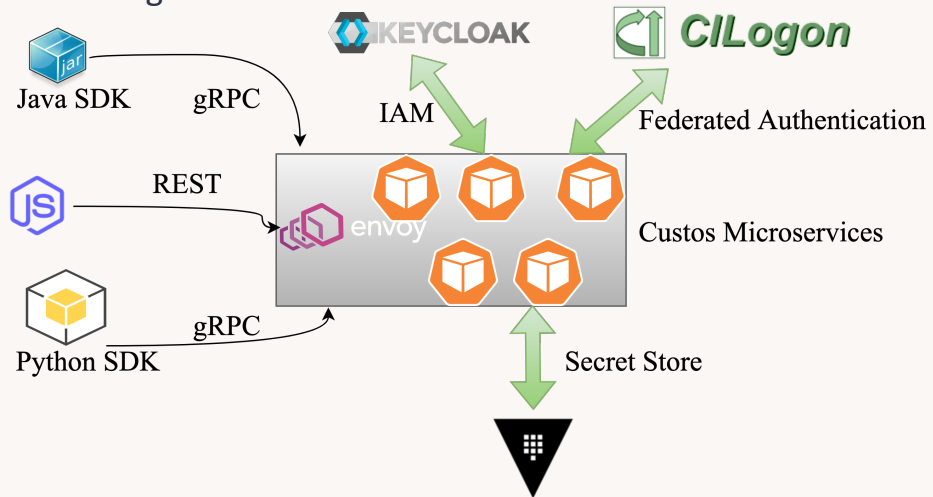
NSF award #1840003

Science Gateways: Science-centric views to Cyberinfrastructure



What is Custos?

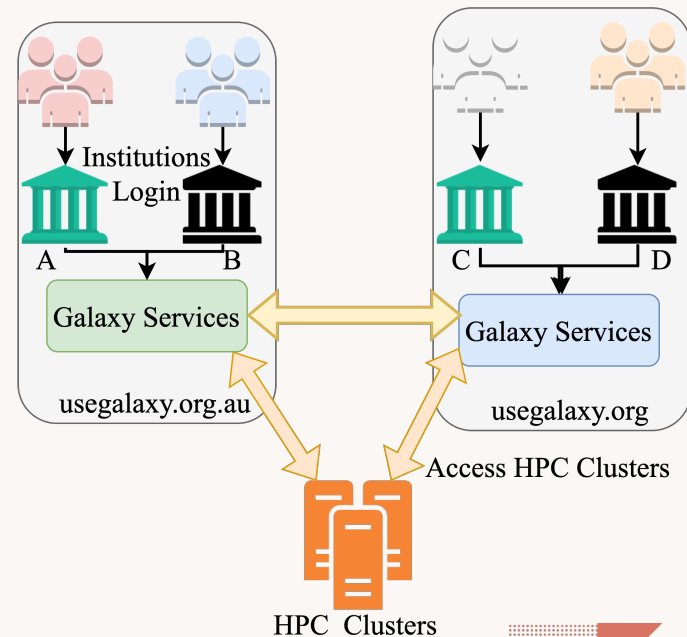
- Open source security middleware for Science Gateways
 - Supports federated authentication via CILogon.
 - IAM solutions




- Deployed as a service on secured Indiana University network on behalf on Clients




Leveraging Custos: Galaxy

- Researchers from different institutions need to access Galaxy services through their institutional IDP
- Since there are vast number of institutions supporting all IDPs from Galaxy is not manageable.
- Custos provides CILogon based federation for Galaxy.
- Next step: Galaxy can use Custos to manage user-provided secrets, like API keys
- Big picture: Multiple Galaxy deployments can federate user accounts and permissions with Custos.



Galaxy using Custos

 Galaxy Test

[Workflow](#) [Visualize](#) [Shared Data](#) [Help](#) [Login or Register](#)   

Welcome to Galaxy, please log in

Public Name or Email Address

Password

[Forgot password? Click here to reset your password.](#)

Login

Use existing institutional login

Select your institution

☐ Remember institution selection

Sign in with Custos*

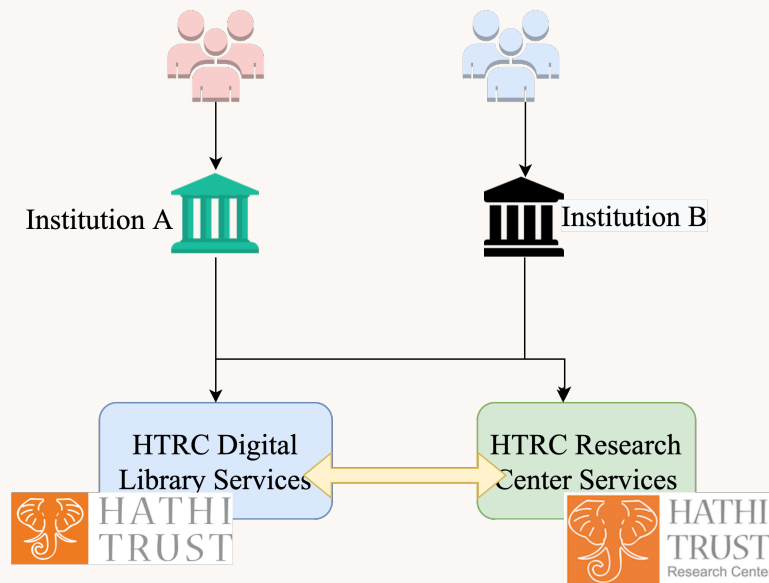
* Galaxy uses CILogon via Custos to enable you to log in from this organization. By clicking 'Sign In', you agree to the CILogon privacy policy and you agree to share your username, email address, and affiliation with CILogon, Custos, and Galaxy.

[Don't have an account? Register here.](#)

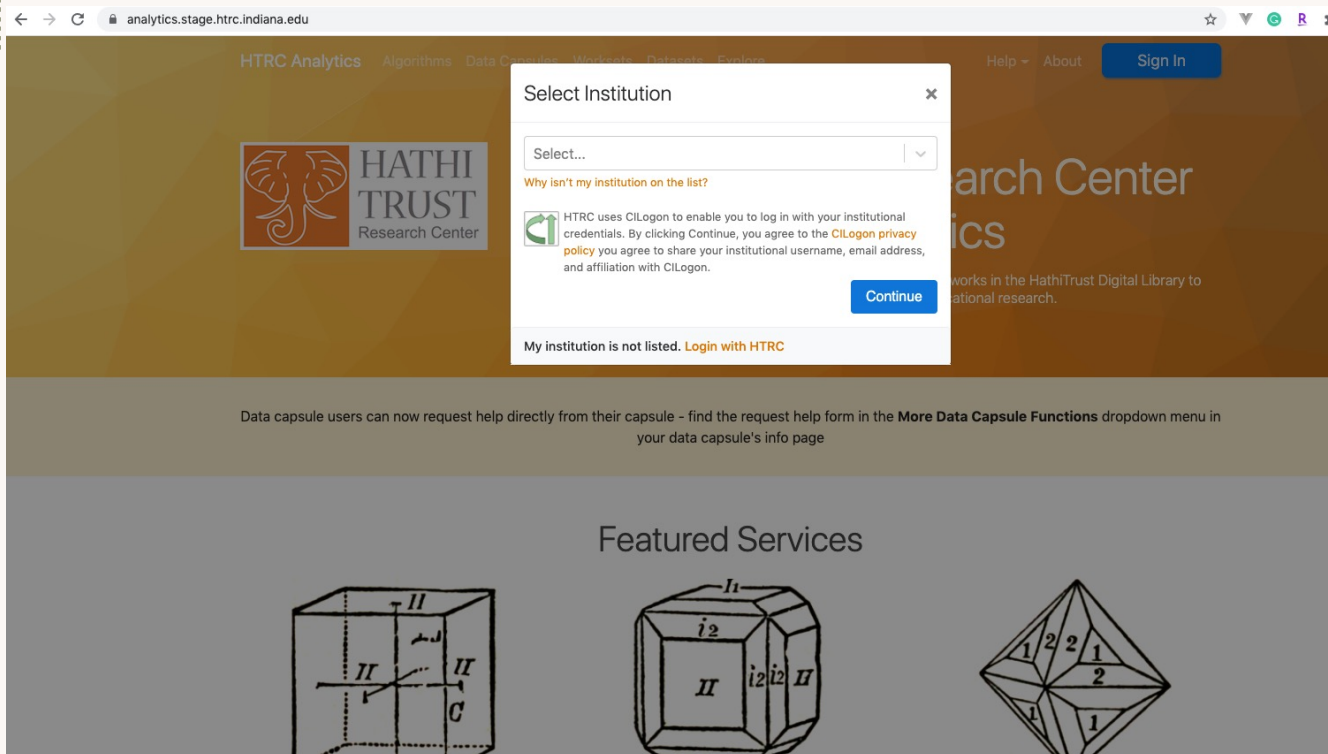
Leveraging Custos: HathiTrust Research Center



- Hathi Trust is the world largest nonprofit digital library in the world.
- Hathi Trust Digital Library and Hathi Trust Research Center are two separate entities
- Users from different Institutions need to access HTRC services and Digital Library Services through HTRC analytics gateway
- Custos provides federated authentication for HTRC analytics gateway and allows seamless access to services provided from both entities.



HTRC using Custos

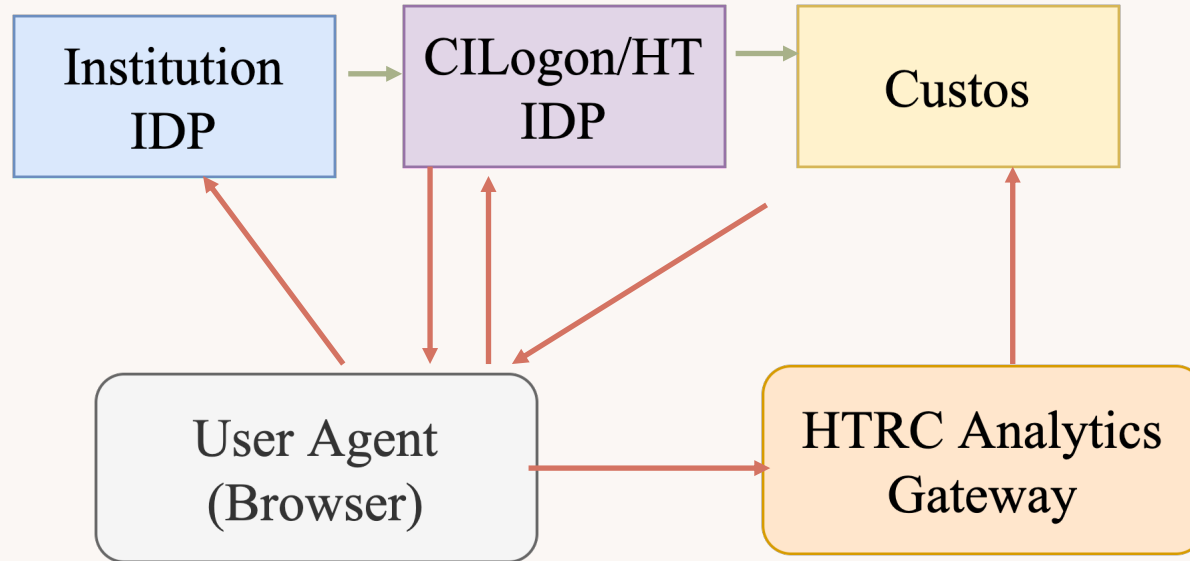


The screenshot shows the HTRC Analytics website interface. A modal dialog titled "Select Institution" is open in the center. The dialog contains a dropdown menu with "Select..." as the placeholder. Below the dropdown, there is a link "Why isn't my institution on the list?". A green circular icon with a white 'C' is next to the text: "HTRC uses CILogon to enable you to log in with your institutional credentials. By clicking Continue, you agree to the [CILogon privacy policy](#) you agree to share your institutional username, email address, and affiliation with CILogon." A blue "Continue" button is at the bottom right of the dialog. At the bottom of the dialog, it says "My institution is not listed. [Login with HTRC](#)".

The background website shows the HathiTrust Research Center logo and navigation links: HTRC Analytics, Algorithms, Data Capsules, Workflows, Datasets, Explore, Help, About, and a Sign In button. Below the modal, a message states: "Data capsule users can now request help directly from their capsule - find the request help form in the **More Data Capsule Functions** dropdown menu in your data capsule's info page".

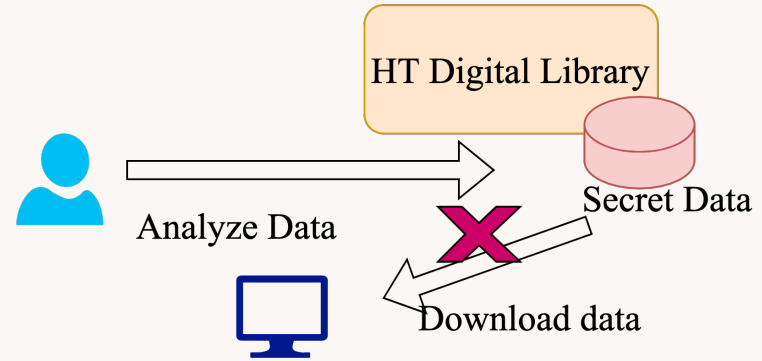
Below the message, the "Featured Services" section displays three 3D geometric diagrams: a cube with axes labeled II , II , and C ; a cube with axes labeled I_1 , i_2 , and II ; and a diamond-shaped polyhedron with axes labeled 1 , 2 , and 1 .

User Identity Federation



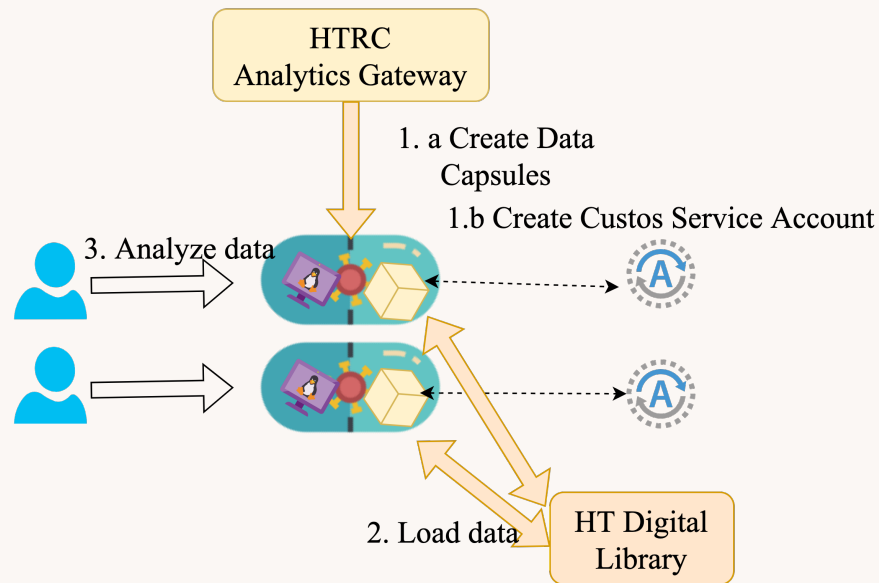
Beyond Identity Federation

- HTRC users need to analyze sensitive HT data
- HTRC does not allow to expose data to public.
- HTRC came up with Data Capsules which provides secured environment to load and analyze data



HTRC Data Capsule System

- Data capsules need to authenticate with HT data APIs to load data.
- Each data capsules needs to be audited and all operations carried out over data are logged.
- Custos provides service accounts-based authentication for Data capsules

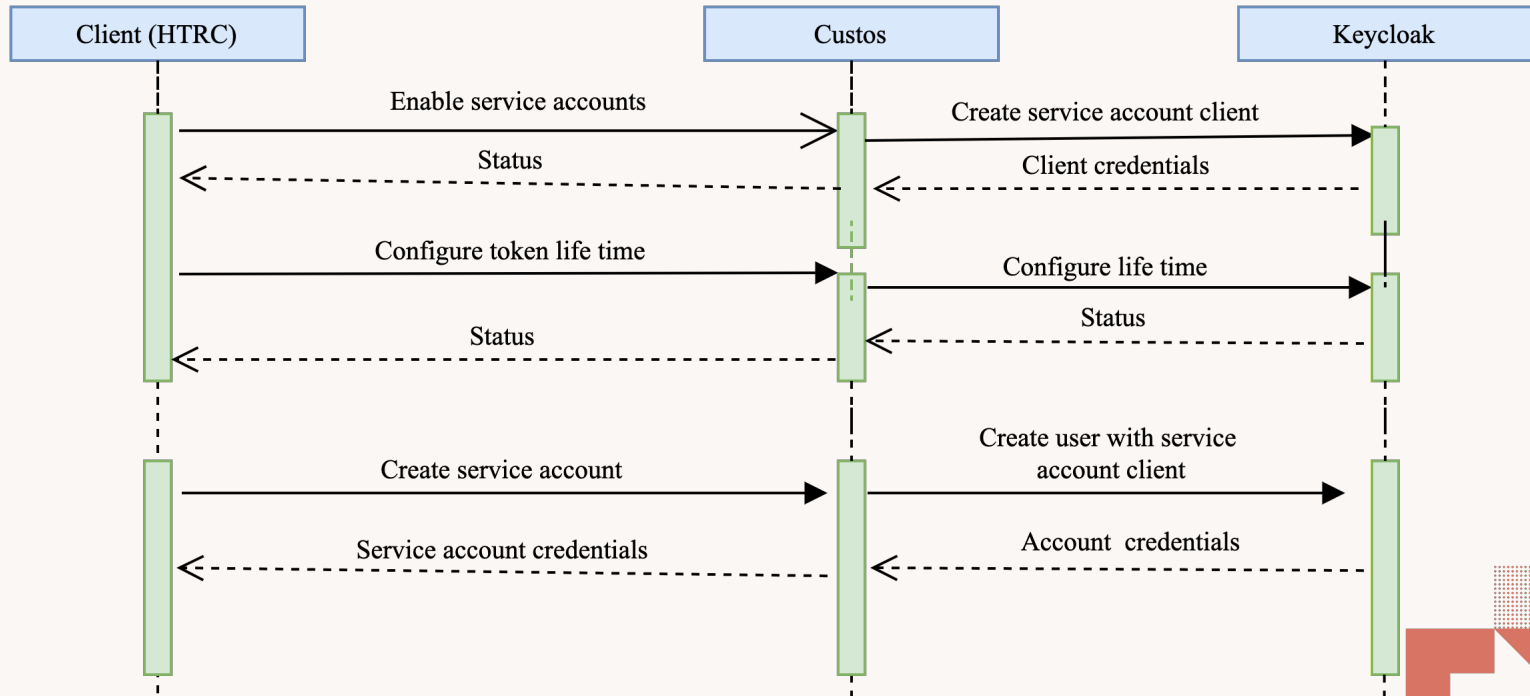


Ubuntu VM with preconfigured tools



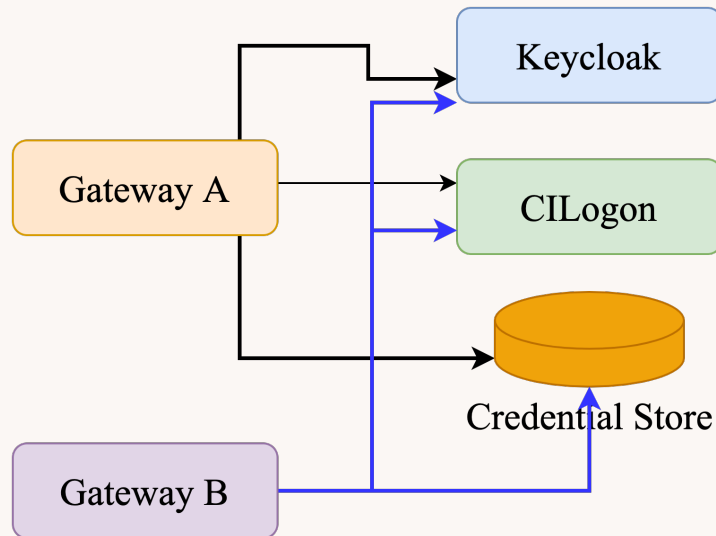
Custos Service Accounts

- Service Account Creation Process

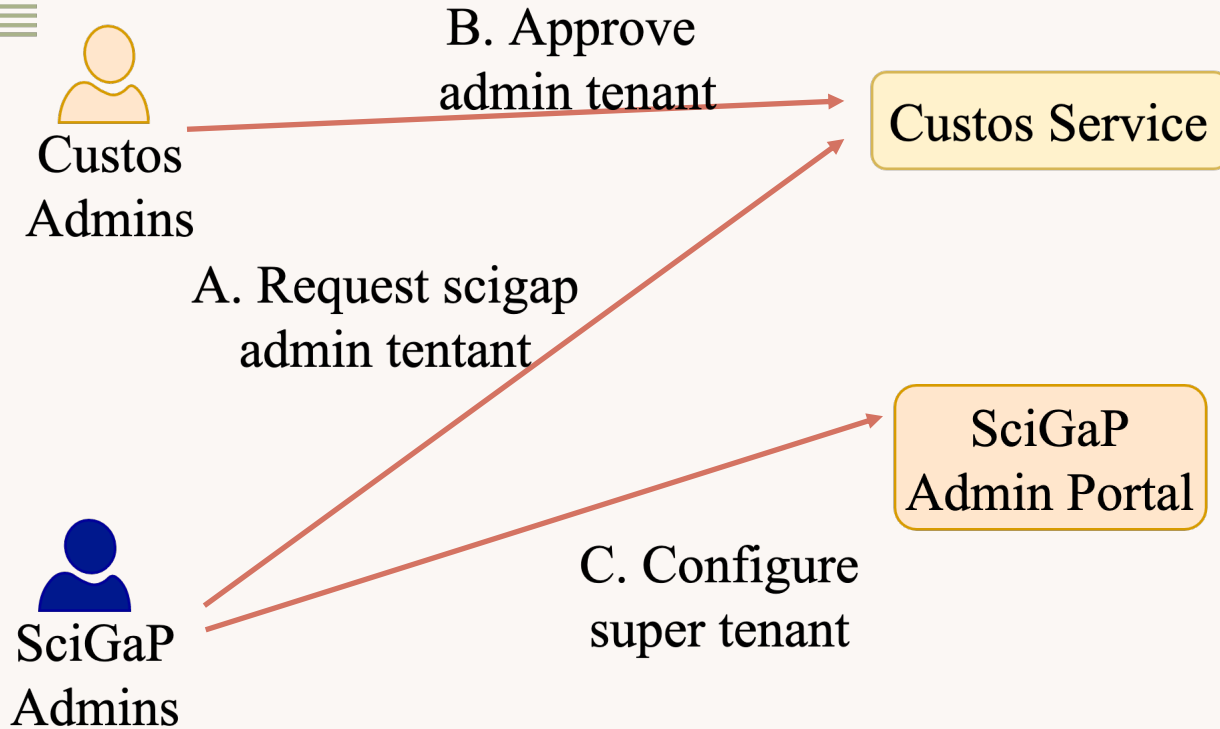


Apache Airavata Platform Integration

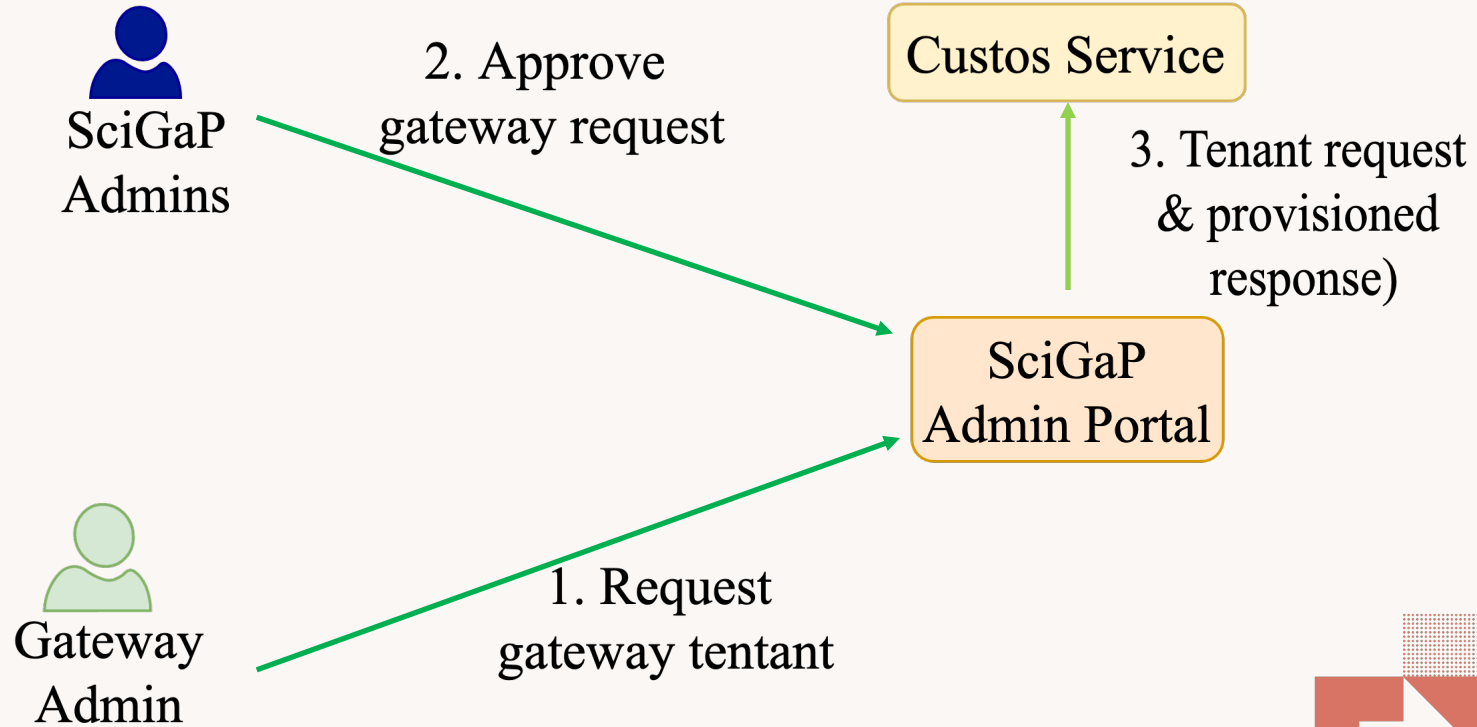
- SciGaP
 - Science Gateways Platform as a Service
 - Supports over 40 science gateways.
- Challenges
 - Manual creation of Keycloak Realm
 - Manually configure CILogon Client
 - Store credentials in local credential store
 - Repeat this procedure for all Gateways and
 - It's a time consuming process
- Solution: Replace Keycloak, CILogon and Credential Store with Custos Service



Custos supports automatic gateway provisioning

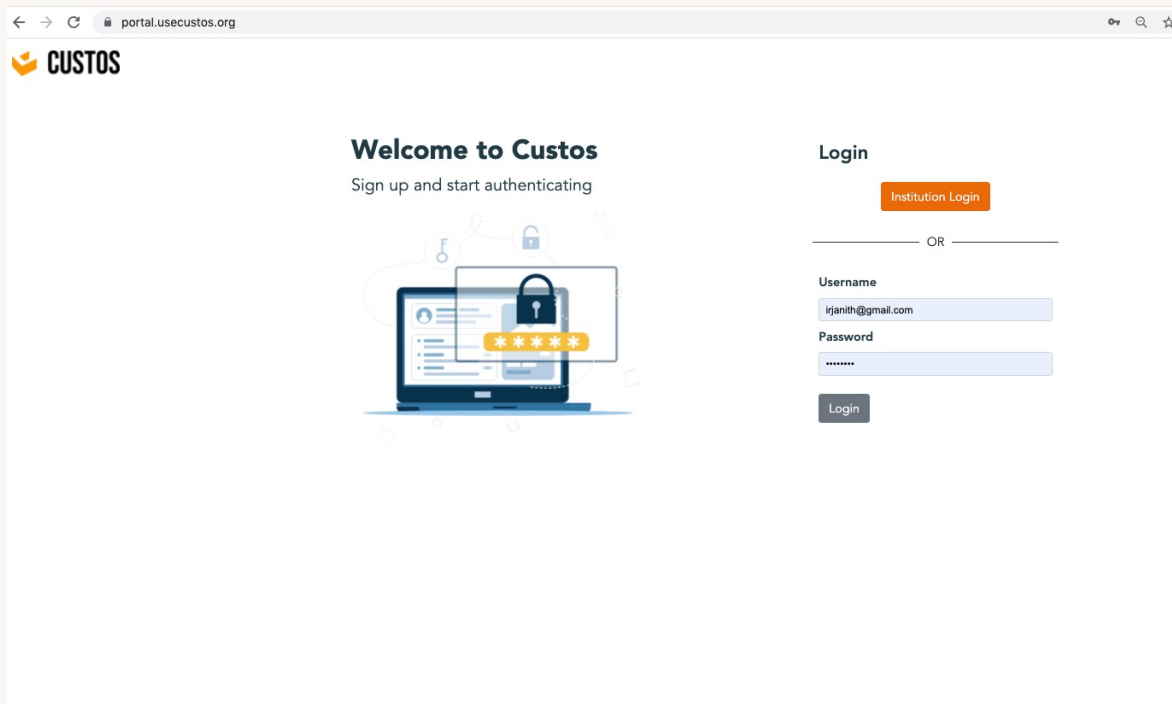


Cont...



Custos Administrative Portal

- User interface for Custos operations



The screenshot shows the Custos Administrative Portal user interface in a web browser. The browser's address bar displays "portal.usecustos.org". The page features the Custos logo in the top left corner. The main content area is divided into two sections. On the left, a "Welcome to Custos" message is followed by the instruction "Sign up and start authenticating" and an illustration of a laptop with a lock icon and a password field. On the right, a "Login" section contains an "Institution Login" button, an "OR" separator, and fields for "Username" (containing "irjanith@gmail.com") and "Password" (masked with asterisks). A "Login" button is positioned at the bottom of the login section.

Tenant Dashboard

Isuru Ranawaka
isjarana@iu.edu

EMC Production Tenant

[Custos production tenant](#) / [EMC Production Tenant](#) / Tenant Profile

Save Changes

Profile

Tenant Profile

Roles

Permission Types

Entity Types

Users

Groups

Entities

Child Tenants

Tenant Name

EMC Production Tenant ✓

The Client Name is displayed to end-users on the Identity Provider selection page.

Client ID



Secret



Redirect URI

https://scigap09.sciencegateways.iu.edu/callback ✓

Remove

https://localhost:8080/callback ✓

Remove

https://gateway.iubemcenter.indiana.edu/callback ✓

Remove

[Add another URI](#)

Scope

☒ openid ☒ email ☒ profile ☒ org.cilogon.userinfo[Information on scopes](#)

Domain

scigap09.sciencegateways.iu.edu ✓

Client URI

https://scigap09.sciencegateways.iu.edu/ ✓

Logo URI

Conclusion

- Integration statistics
 - Federated authentication
 - Galaxy, HTRC, SciGaP
 - Secret management
 - Galaxy, SciGaP
 - Service Accounts
 - Galaxy, HTRC, Airavata MFT



- Subscribe Custos mailing list: custos-subscribe@airavata.apache.org
- Repository: <https://github.com/apache/airavata-custos.git>



Thank You

