

GT- CILogon

UFSM & IFC

Dezembro de 2025

Roteiro

- Sobre o GT
- Contexto
- Desafios de Identidade e Acesso
- CILogon
 - Arquitetura
- CManage
 - Funcionalidades
- Fluxo de Integração
- Vantagens e Benefícios
- Desenvolvimento das Atividades
- Conclusões e Perspectivas Futuras

Sobre o GT-CILogon

- Composição
 - Walter Priesnitz Filho** (Ph.D. Segurança) - UFSM
 - João Marco Cardoso Silva** (Ph.D. Informática) - UMinho
 - Renato Preigschadt** (Ph.D. Informática) - UFSM
 - Heitor Scalco Neto** (MSc. Computação) - IFC
 - José C. Lacerda Lopes Neto** (Esp. DevOps) - ???
 - Gustavo Peretti** (Graduando) - IFC
 - Gabriel Denarde** (Graduando) - UFSM

Contexto: e-Ciência e Colaboração Global

- **e-Ciência:** pesquisa baseada em infraestrutura digital multi-institucional.
- **Desafios:** acesso compartilhado e seguro a HPC (*High Performance Computing*), repositórios e plataformas entre países e federações.
- **Obstáculo Histórico:** IdAM (*Identity and Access Management*) fragmentado forçava projetos a criar soluções próprias, desviando foco da ciência.
- **Necessidade:** interoperabilidade e confiança entre federações acadêmicas.
- **Solução:** Eliminar a fadiga de "mais um usuário e senha".

Desafios de Identidade e Acesso

- Múltiplas credenciais e senhas reduzem a adesão.
- Diferenças de protocolos (SAML, OIDC, OAuth) e atributos.
- Dificuldade para gerenciar permissões por projeto e por papel.
- Compatibilidade entre CAFE, InCommon e logins sociais.



CILogon: Gateway de Protocolos e Federações

- Ponto central de autenticação e tradução de protocolos.
- Integra CAFE (Brasil), InCommon (EUA) e logins sociais (Google, ORCID, GitHub).
- Converte SAML 2.0 em OIDC/OAuth 2.0 para aplicações modernas.
- Benefícios: login federado, sem múltiplas contas e com alcance internacional.

Arquitetura e Funcionalidades do CILogon

- Tradução SAML → OIDC e agregação de atributos.
- Vinculação de identidades: CAFe/InCommon/ORCID a um perfil único.
- Interoperabilidade com aplicações legadas e modernas via JWT.

COmanage: Registro e Autorização Colaborativa

- Controla participação e privilégios em projetos (CO Person, CO Groups).
- Gestão delegada para coordenadores de projetos (VOs).
- Governança clara de quem pode acessar quais recursos.
- Funcionalidades:
 - a. Ciclo de vida da identidade: registro, aprovação e desprovisionamento.
 - b. Provisionamento via LDAP, SCIM e APIs; evita duplicidades (COmanage Match).
 - c. Trilhas de auditoria e conformidade (REFEDS/AARC).

Fluxo Integrado (CILogon + CManage)

1. Autenticação no IdP (CAFe/InCommon).
2. CILogon recebe a *assertion* e busca dados no CManage.
3. CManage retorna afiliações e grupos (*isMemberOf*).
4. CILogon emite o token OIDC (JWT) com *claims*.

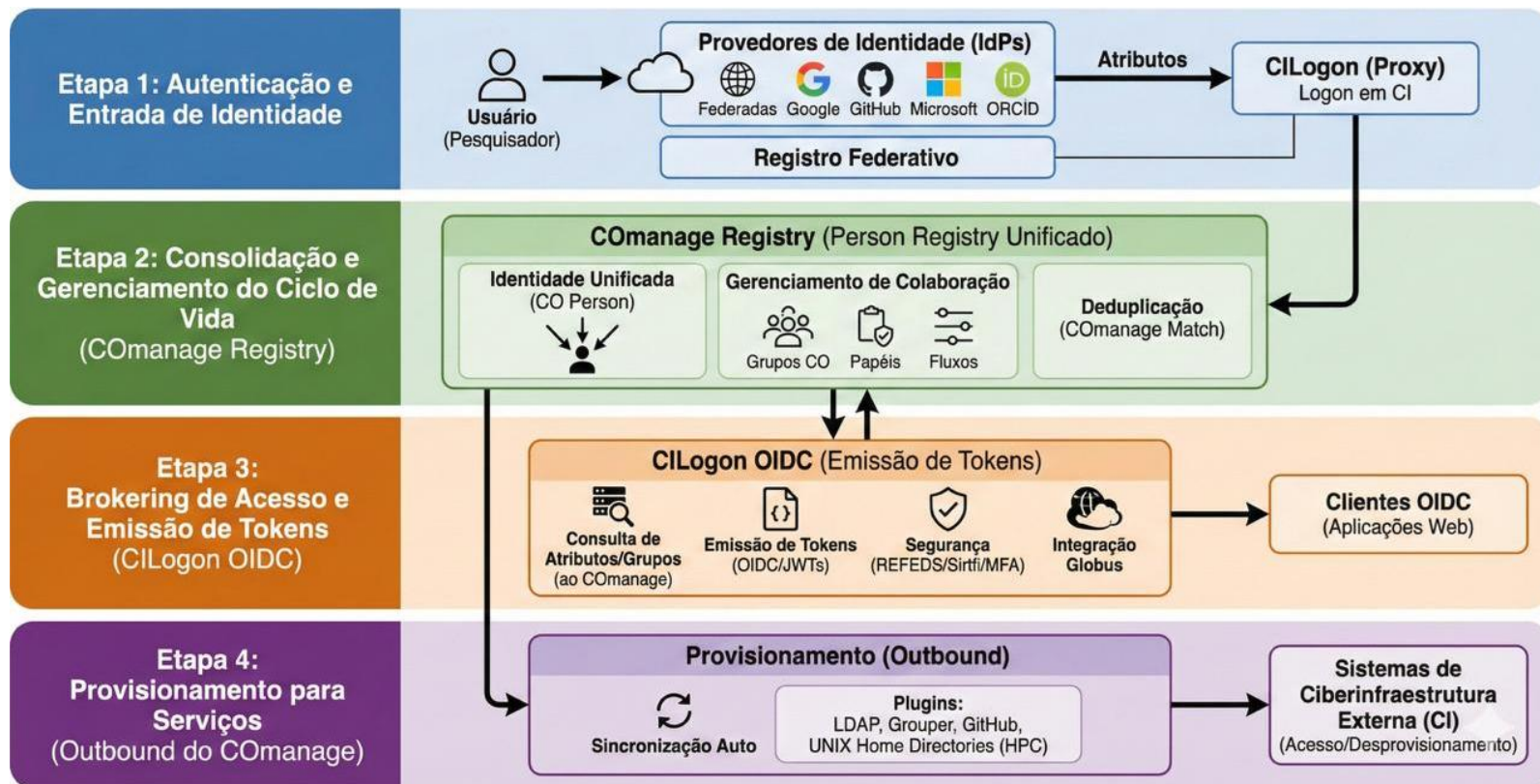
Vantagens Técnicas e Operacionais

- Protocolo único (OIDC) para todas as aplicações.
- Fonte única de verdade/confiança para grupos e afiliações (COmanage).
- Reduz carga sobre TI e aumenta segurança.
- Resiliente a mudanças e alinhado a REFEDS/AARC.

Benefícios para Gestores e Pesquisadores

- **Pesquisadores:** login único, rápido e seguro.
- **Gestores:** visibilidade e controle de permissões.
- **TI:** simplificação e automação de provisionamento.
- **Impacto:** aceleração da ciência colaborativa.

Arquitetura de Comunicação CILogon & Comanage



Desenvolvimento das Atividades

Agosto

- Implantação de ambientes de testes/desenvolvimento, hospedados na UFSM, com replicação na RNP
 - **Tecnologias:** Docker, Docker Swarm, Traefik, pilha cilogon-java (Keycloak, banco de dados)
 - **Foco:** Escalabilidade, segurança (criptografia, controle de acesso), interoperabilidade
- Progresso
 - **Concluído:** Planejamento e configuração inicial (hardware/software, DNS, otimizações no Dockerfile, regras de firewall com SNAT, ajustes no Traefik e Docker Swarm)
 - **Resultados:** Ambientes configurados, estabilidade e segurança validadas, documentação

Setembro

- Provisionamento da infraestrutura em ambiente disponibilizado pela RNP.
- Progresso
 - **Concluído:** Scripts para configuração e provisionamento dos serviços via IaC executados no ambiente da RNP.
 - **Resultados:** Cluster docker swarm configurado entre os 4 servidores no ambiente da RNP. Criação de regras de firewall e usuários e grupos com permissões necessárias para execução dos serviços.
- Deploy dos containers com os serviços.

Desenvolvimento das Atividades

Outubro

- Foco CILogon-service e Shibboleth
- Provisionamento da infraestrutura em ambiente disponibilizado pela RNP.
- Progresso
 - **Concluído:** Scripts para configuração e provisionamento dos serviços via IaC executados no ambiente da RNP.
 - **Resultados:** Cluster docker swarm configurado entre os 4 servidores no ambiente da RNP. Criação de regras de firewall e usuários e grupos com permissões necessárias para execução dos serviços.
- Em Andamento: Deploy dos containers com os serviços.

Novembro

- Foco no CILogon-service e Shibboleth
- CILogon-service
 - Funcionamento com o Shibboleth
 - Continuam os estudos
 - Implantação de um IdP de testes
 - Auxílio do Fiter com um container
 - Funcionando com o Shibboleth - CAFE Expresso
- Infraestrutura RNP
 - Provisionamento da infraestrutura em ambiente disponibilizado pela RNP.
 - Progresso
 - Estrutura igual a que temos na UFSM

Trabalho em andamento



Conclusões e Perspectivas Futuras

- CILogon e CManage = pilares da identidade federada.
- Adoção alinhada à CAFé, InCommon e eduGAIN.
- Próximos passos: expandir integrações e automatizar provisionamento.

Dúvidas???

GT- CILogon

UFSM & IFC

Dezembro de 2025