Uso de Autenticação Federada como Solução para Disponibilização de Serviços

Rui de Quadros Ribeiro[1], Francisco Leonardo Bento Mota[2]

[1]Centro de Processamento de Dados (CPD)
Universidade Federal do Rio Grande do Sul (UFRGS)
Rua Ramiro Barcelos, 2574 – Portão K – Porto Alegre – RS

[2]Diretoria de Serviços e Soluções (DSS)
Rede Nacional de Ensino e Pesquisa (RNP)
SAS, Quadra 5, Lote 6, Bloco H, 7° Andar – Brasília - DF

rui.ribeiro@cpd.ufrgs.br, francisco.mota@rnp.br

Abstract. *The use of federated authentication allows the sharing and availability of services without requiring the installation of local instances on each client. For the Brazilian scientific community, 46 were delivered, with concentration of their facilities in RNP. This same infrastructure is available for the federalization of internal services of the client institutions. In this context, UFRGS realized the creation of an internal federation, with the objective of using the same authentication and authorization infrastructure to provide federated services based on SAML among its units. This same model can be adopted by other institutions..*

Resumo. *O uso de autenticação federada permite o compartilhamento e disponibilização de serviços sem que seja necessária a instalação de instâncias locais em cada cliente. Para a comunidade científica brasileira, foram entregues 46, com concentração de suas instalações na RNP. Esta mesma infraestrutura está disponível para a federalização de serviços internos das instituições clientes. Neste contexto, a UFRGS realizou a criação de uma federação interna, com o objetivo de usar a mesma infraestrutura de autenticação e autorização para fornecer serviços federados baseados em SAML entre as suas unidades. Este mesmo modelo pode ser adotado pelas demais instituições.*

1. Introdução

O relacionamento do Centro de Processamento de Dados (CPD) da Universidade Federal do Rio Grande do Sul (UFRGS) com a Rede Nacional de Ensino e Pesquisa (RNP), no escopo de Gestão de Identidade, precede a criação da "Federação CAFe". Entre 2002 e 2010 o CPD da UFRGS participou de diversos Grupos de Trabalho que exploraram as tecnologias que posteriormente viabilizaram a criação da "Federação CAFe".

Um dos principais benefícios para a UFRGS derivados dessa experiência foi a

elaboração de um diretório unificado. Tal diretório é baseado em OpenLDAP e atua como base para autenticação dos usuários da instituição nos mais diversos serviços existentes. Muito embora a UFRGS utilize ferramenta própria para coletar os dados das diversas bases, consolidá-los e posteriormente popular o diretório LDAP, a RNP disponibiliza ferramenta e suporte para que outras instituições possam atingir resultado análogo.

Outro benefício desta parceria foi a aquisição de conhecimento necessário para a constituição de uma federação interna. Nesse artigo serão abordados os principais pontos da arquitetura do serviço "Federação UFRGS" bem como os diferenciais da sua implementação.

2. Motivação

A estrutura de gestão da Universidade é distribuída entre as diversas unidades acadêmicas e administrativas existentes. Apesar dos esforços investidos ao longo dos anos, esse mesmo modelo é, em parte, refletido no escopo da TIC. Diversas unidades possuem equipe de TIC local para prestar suporte aos seus usuários e, em alguns casos, desenvolver sistemas. Uma das razões apontadas pelas unidades ao desenvolverem sistemas locais é a falta de serviço correspondente provido pelo CPD.

Nos casos onde existe desenvolvimento local de sistemas, um dos fatores de preocupação diz respeito ao armazenamento e manutenção dos dados cadastrais dos usuários. A simples duplicação dos cadastros já caracteriza um problema. Complementarmente, acredita-se que, por comodidade, os usuários tendem a utilizar nos sistemas locais as mesmas credenciais utilizadas nos demais sistemas ofertados pelo CPD da UFRGS. Tal situação constitui vulnerabilidade de segurança especialmente caso as aplicações locais não tenham sido adequadamente elaboradas.

Diante do cenário exposto, uma hipótese para prover acesso dos sistemas desenvolvidos localmente pelas unidades à base de usuários da Universidade é através de uma federação interna.

3. Federação UFRGS

A "Federação UFRGS" é baseada na especificação *Security Assertion Markup Language* (SAML) e, por conseguinte, possui arquitetura similar à "Federação CAFe". Nela existem os seguintes componentes:

- Provedor de Identidade (IDP): possui acesso ao servidor de diretório e é responsável por autenticar os usuários e, posteriormente, enviar os atributos dos usuários autenticados ao Provedor de Serviço que requisitou a autenticação.
- Provedor de Serviço (SP): possui um serviço *web* relevante que demanda autenticação para conceder acesso aos usuários. Com base nos atributos recebidos do IDP, o SP pode aplicar diferentes regras de autorização.

Embora seja tecnicamente possível a existência de múltiplos IDPs em uma federação, a "Federação UFRGS" possui um único IDP. Isso é decorrente do fato do CPD deter exclusividade sobre o acesso ao diretório LDAP que possui uma base consolidada de todos usuários da instituição. Como desdobramento dessa premissa, não existe a necessidade de um *Discovery Service* cuja finalidade seria direcionar o usuário

ao IDP de sua instituição de origem.

O IDP utilizado na "Federação UFRGS" é o mesmo que provê autenticação junto às demais federações que a Universidade possui parceria – ArcGIS, CAFe, eduGAIN, e REGESD (Figura 1). Isso faz com que o usuário se habitue a uma única interface de autenticação. Seu funcionamento é baseado no *middleware* Shibboleth IDP e sua configuração é fundamentada nos roteiros disponibilizados pela RNP em sua Wiki (Rede Nacional de Ensino e Pesquisa, 2016). A principal diferença de configuração do IDP em relação às demais federações é quanto ao conjunto de atributos entregues aos SPs. No âmbito da "Federação UFRGS" é entregue um atributo composto chamado *ufrgsVinculo* e que possui diversas informações pertinentes ao vínculo de servidor e/ou aluno, por exemplo: local de lotação, local de exercício, cargo, curso, e etc.

A maioria dos SPs da "Federação UFRGS" utiliza o SimpleSAMLphp que é uma aplicação PHP que pode ser utilizada tanto para atuar como IDP quanto como SP. Com o intuito de facilitar o uso e ampliar sua adoção, foi criada uma instalação compartilhada no serviço de Hospedagem de Site PHP. Isso permite que os usuários possam usufruir da comodidade da autenticação federada sem precisar compreender detalhes da configuração.

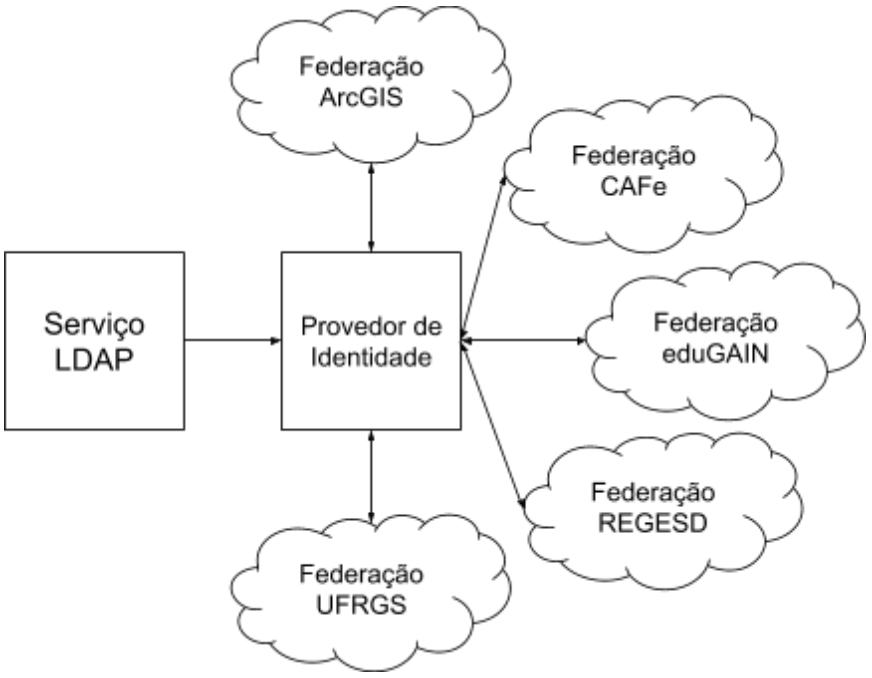

Figura 1. Relacionamento do IDP UFRGS com as diversas federações

4. Resultados - Estatísticas de Acesso

A análise das estatísticas de acesso no período compreendido entre 01/01/2018 e 22/04/2018 apontou um total de 51.682 autenticações no IDP. Desse total de acessos, 33.600 (65%) correspondem a SPs da "Federação UFRGS" e 14.913 (28,9%) a SPs da "Federação CAFe". Os SPs que concentram maior número de acessos são Portal de Bolsas (28.207) e o Portal de Periódicos da CAPES (14.207). As Figuras 3 e 4 apresentam graficamente esses dados.

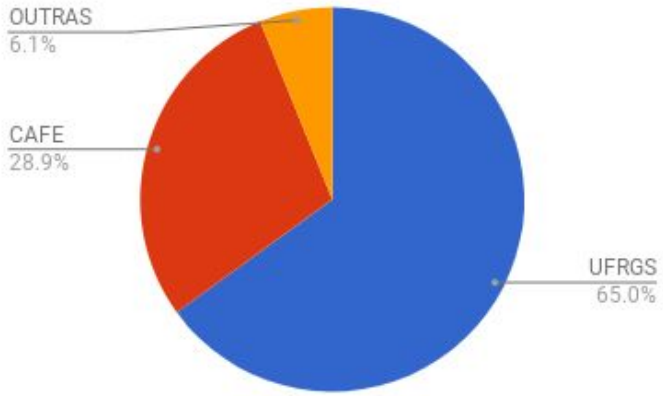

Figura 3. Distribuição de acessos entre as federações

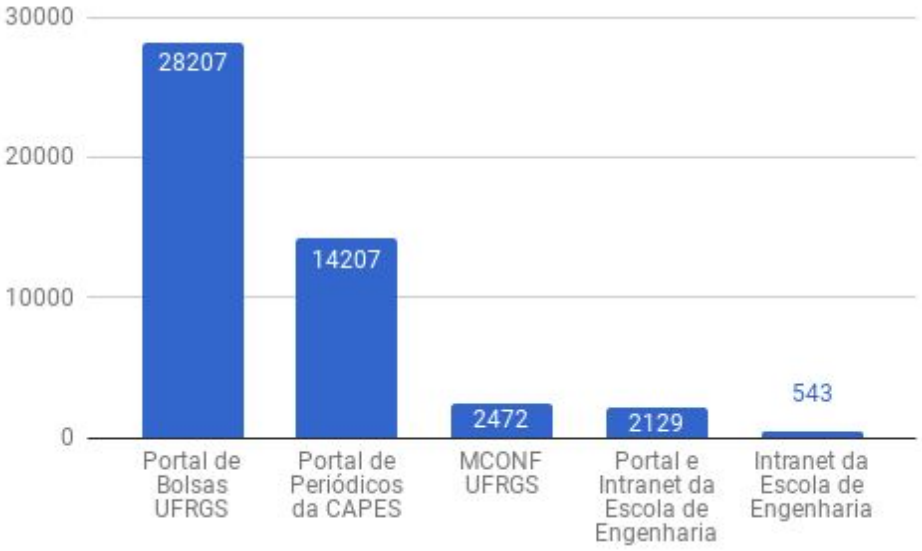

Figura 4 - Cinco serviços mais acessados através do IDP da UFRGS

5. A Federação CAFe

A federação CAFe assumiu no ano de 2017 o sétimo lugar no ranking de federações estudantis ligadas à eduGAIN quando considerado o número de provedores de identidade (IdP). O uso uso da autenticação federada permitiu que 46 serviços estejam disponíveis para a comunidade científica brasileira, evitando que estes precisassem ser instanciados em cada instituição. Porém, quando considerado o número de serviços disponibilizados, a federação brasileira assume o 24º lugar no ranking (Metadata Explorer Tool, 2018).

Quando considerado o perfil de uso destes serviços, é possível perceber um grande destaque para o uso do Portal de Periódicos da CAPES, tendo os demais serviços uma quantidade mínima de acessos. A Figura 5 mostra o comparativo dos acessos

realizados pela UFRGS em comparação com a UFPE, UFU e UnB, mostrando os dois serviços de acesso disponibilizado para a federação mais utilizados entre elas.

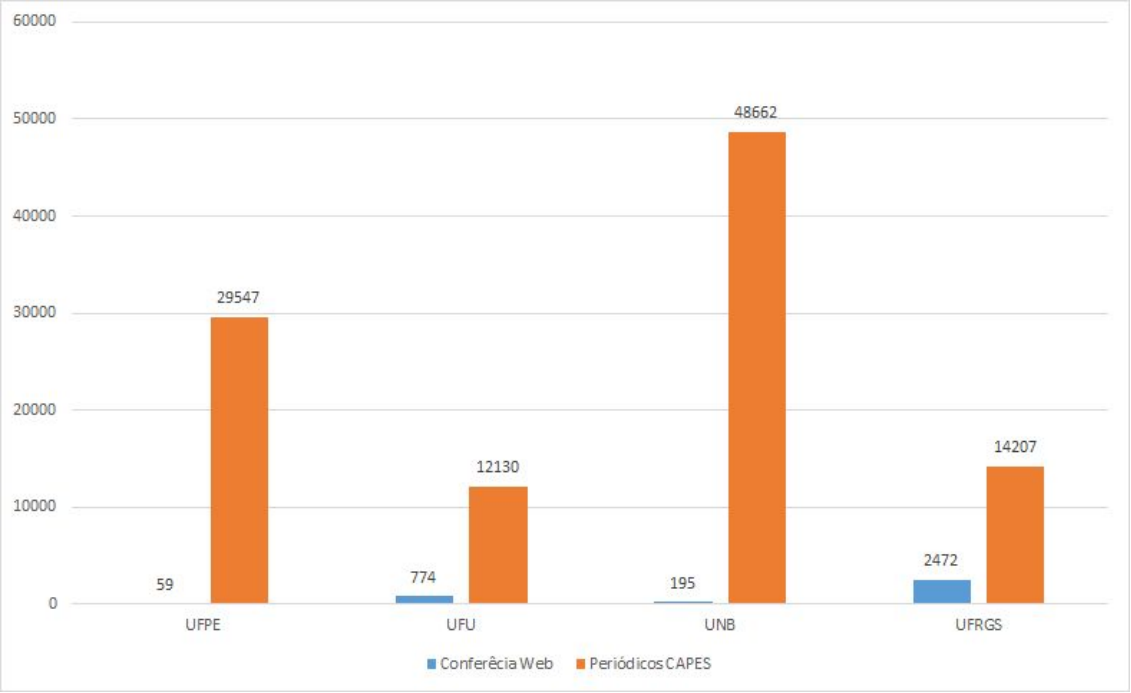

Figura 4 - Comparação dos serviços mais utilizados pelos clientes

É possível perceber que o perfil de acesso se mantém o mesmo em ambas as instituições, tendo o Portal de Periódicos da CAPES como o serviço com o maior número de acessos e o serviço de Webconferência em segundo lugar, mas mostrando um número inexpressivo em relação ao primeiro lugar. Os demais serviços nem foram considerados nesta demonstração por apresentarem um número ainda menor de acessos federados em relação ao segundo colocado.

6. Conclusão

A utilização do modelo de acesso federado permite o compartilhamento de recursos em larga escala, diminuindo os problemas operacionais e pontos de falha que podem vir a existir na instalação de serviços individualizados mesmo quando estes são de interesse mútuo de uma comunidade. Embora o estabelecimento de padrões para Gestão de Identidade e a adoção de tecnologias necessárias necessitem de uma curva de aprendizado que não pode ser considerada trivial, os benefícios alcançados podem se estender em escala nacional em um curto espaço de tempo.

Além disso, o perfil apresentado permite perceber que ainda há espaço para que o próprio meio acadêmico se mobilize no desenvolvimento e compartilhamento de serviços, seja este entre seus campi ou com outras instituições, uma vez que a realidade técnica e administrativa é semelhante entre estas instituições, quando observado que o número de serviços disponíveis ainda não é relevante e em maior parte disponibilizado por uma única instituição.

Adicionalmente, os serviços disponibilizados pela RNP ainda não são amplamente utilizados, havendo espaço para divulgação e aproveitamento das funcionalidades destes.

Referências

GÉANT. (2018) “Metadata Explorer Tool”. Acesso em 23 de abril de 2018, disponível em: https://met.refeds.org/.

Rede Nacional de Ensino e Pesquisa. (2016) “Procedimentos Operacionais da Federação CAFe”. Acesso em 20 de Abril de 2018, disponível em: https://wiki.rnp.br/pages/viewpage.action?pageId=69968456.

SimpleSAMLphp. (2018) “SimpleSAMLphp”. Acesso em 20 de Abril de 2018, disponível em: https://simplesamlphp.org/.