Eduroam para Visitantes: Acesso Seguro, Federado e Temporário à Rede Sem Fio*

Luciano F. da Rocha[1], Anderson Almeida[1] André Forigato[1], Jonathan Welley[1], Calebe Sousa[1], Edelberto Franco[2]

[1] Rede Nacional de Ensino e Pesquisa - RNP

[2]Universidade Federal de Juiz de Fora - UFJF/DCC

Abstract. *The relevance of Internet access for academic institutions is already consolidated. The RNP offers secure federated wireless access service to its partners, called eduroam. Today, the eduroam federation in Brazil has more than 120 institutions as partners and approximately 2400 access points, being the largest community in Latin America. However, this do not cover all institutions. Based on this scenario, this work shows an evolution of the eduroam service through a new functionality that allows its use by people who are not yet connected to any institution that is part of the eduroam federation. This work presents the concept, motivation, technology, benefits, possibilities and the experience lived by RNP's consultants to create the eduroam for visitors.*

Resumo. *O entendimento da importância do acesso à Internet para o meio acadêmico já é uma realidade consolidada. A Rede Nacional de Ensino e Pesquisa oferece o serviço de acesso sem fio seguro e federado eduroam a seus parceiros. A federação eduroam no Brasil tem hoje mais de 120 instituições participantes e aproximadamente 2400 pontos de acesso, sendo a maior comunidade na América Latina. No entanto, os números apresentados correspondem a apenas uma parte das instituições que podem fazer uso do serviço. Diante deste cenário, este trabalho apresenta uma evolução do serviço eduroam através de uma nova funcionalidade que permite a sua utilização por pessoas que ainda não estejam ligadas a nenhuma instituição integrante da federação eduroam. Este trabalho apresenta o conceito, a motivação, a tecnologia envolvida e os benefícios e possibilidades de utilização desta solução chamada de eduroam para visitantes.*

1. Introdução

O protocolo RADIUS (*Remote Authentication Dial-In User Service*) [Rubens et al. 2000] oferece a comunicação entre cliente e servidor para AAA (Autenticação, Autorização e *Accounting*). Quando utilizado em conjunto com o IEEE 802.1X [Smith et al. 2003], o RADIUS é capaz de realizar autenticação segura a dispositivos conectados à rede sem fio. O caso de maior sucesso desta solução é o projeto eduroam - *Education Roaming*[1] [Wierenga et al. 2015] -. O eduroam fornece acesso seguro e transparente para usuários

*Contato: luciano.rocha@rnp.br, edelberto@ice.ufjf.br – Agradecemos às NRENs: RNP, SWITCH, SURFnet, Inictel e REUNA pelo apoio ao desenvolvimento deste trabalho. Em especial aos pesquisadores Javier (Inictel), Florian (SURFnet) e Wladimir (SURFnet).

[1]http://www.eduroam.org.br

de instituições parceiras com base no conceito de federação, permitindo que o usuário se autentique à rede em qualquer instituição parceira utilizando suas credenciais únicas a partir do seu provedor de identidade de origem, facilitando o intercâmbio entre estudantes e pesquisadores. Desde 2011 a Rede Nacional de Ensino e Pesquisa, a RNP, opera este serviço. No Brasil, com mais de 120 instituições participantes e aproximadamente 2400 pontos de acesso hoje, a RNP é responsável pela maior comunidade eduroam na América Latina.

Apesar do grande número de instituições participantes do eduroam no Brasil, algumas características impedem que o serviço seja adotado por diversas outras instituições. Um exemplo claro é a infraestrutura restrita de algumas dessas instituições, o que pode impedir, por exemplo, que diversas redes sem fio com diferentes SSID (*Service Set Identifier*) sejam ofertadas[2]. O custo relacionado à aquisição de infraestrutura, treinamento, e manutenção de equipamentos na maioria das vezes torna o processo complexo ou até mesmo inviável para muitas instituições. Uma forma de auxiliar na solução deste problema seria a utilização de apenas um único SSID por toda a instituição, e.g. eduroam - uma vez que suporta AAA para usuários internos e externos. Porém, apesar de viável em um primeiro momento, a proposta contempla somente integrantes da federação eduroam, excluindo àqueles que não fazem parte dela, e impedindo o acesso, por exemplo, de visitantes que não tenham conta eduroam associada[3]. Uma forma de solucionar este problema é criar contas temporárias para estes usuários visitantes. Da mesma forma, contas temporárias para visitantes podem ser utilizadas para oferecer acesso sem fio seguro a grandes eventos, a pesquisadores visitantes de instituições que não fazem parte da federação eduroam, ou ainda, pessoas vinculadas à empresas privadas. É importante destacar que o **eduroam para visitantes** se apoia e oferece o mesmo serviço seguro e federado à rede sem fio, garantindo maior confiabilidade que redes sem fio abertas ou de senha compartilhada em geral oferecidas nesse contexto.

Desta forma é possível, também, divulgar e fortalecer a importância do serviço junto às instituições-alvo do eduroam no Brasil. Para ilustrar um caso motivador e prático neste contexto de expansão do eduroam, tem-se: a utilização por um professor de uma instituição não participante do serviço; uma vez que este usuário tem acesso à rede sem fio segura do eduroam e utiliza todos os benefícios intrínsecos do serviço, pode se tornar um porta voz em sua instituição de origem pela adesão ao serviço.

Para implantação do serviço foram realizadas buscas por serviços similares e estudadas as principais soluções que têm relação com objetivo desta meta. Encontradas soluções similares, foi realizado contato e avaliação da possibilidade de aproveitamento de uma mesma solução utilizada por outro país parceiro. Ao final foi verificada a necessidade de desenvolvimento de uma solução própria.

Para apresentar o novo serviço e a experiência vivenciada para a sua implantação, o trabalho está organizado em: a Seção 2 relata a cronologia para criação da solução; a Seção 2 apresenta o funcionamento sob o olhar prático; e, por fim, a Seção 4 conclui o texto.

[2]Exemplo de diferentes redes e SSID: eduroam, wifi-universidade, visitante etc.

[3]O visitante é aquele que não tem conta em uma das instituições pertencentes à federação eduroam. Seja por ele não ser membro de alguma instituição, ou seja membro mas a instituição não aderiu ao serviço.

2. Relato da Experiência

Primeiramente se levantou a documentação do principal serviço mundial que oferece uma função muito similar, e inspirou este trablho, o eVA (*eduroam Visitor Access*)[4] desenvolvido pela SURFnet, e apresentado no TNC de 2014[5] como um serviço. Porém, ao entrarmos em contato com os responsáveis foi retornado que ainda não funciona com adoção aberta à comunidade e sim como um piloto. Para realizar pilotos a SURFnet depende de verba de pesquisa vinculada a ela para integração com quaisquer federações eduroam e estas já estavam alocadas no momento.

Da mesma forma foi avaliada outra solução, a eduroamPass[6], desenvolvida pela NREN Chilena, REUNA. Porém, a indicação foi, seguindo a mesma linha da SURFnet, de que não haveria, no momento, corpo técnico disponível para auxílio à utilização do serviço e o mesmo não estaria disponível de forma aberta.

A solução encontrada foi, portanto, desenvolver sua própria solução baseada no conceito do eduroam visitante. O serviço VHO – *Virtual Home Organisation*[7] - da SWITCH tem papel essencial no processo, e foi adotado para atender à premissa de cadastro de contas temporárias por responsáveis com permissão. O VHO é um serviço já existente no âmbito da RNP e, basicamente, permite a criação de um provedor de identidade (IdP) para contas temporárias em uma federação (*e.g.* eduroam, CAFe etc). Com base neste serviço e a criação de um sincronizador de contas foi possível exportar as contas e atributos criados no VHO/MySQL para uma base LDAP CAFe/eduroam. Uma vez esta base referente ao IdP em funcionamento a RNP ficou responsável pela sua manutenção e inclusão na federação eduroam.

3. Funcionamento

Nesta seção é apresentada a infraestrutura por trás do serviço, ela é composta de uma interligação à federação Chimarrão CAFe, a fim de permitir que o administrador se autentique na interface VHO; Já para o serviço eduroam visitante em si há: 1 servidor VHO, responsável pela criação e armazenamento das contas dos visitantes; Uma base de dados MySQL, integrada ao VHO que armazena, de fato, os atributos e contas; 1 serviço de sincronização entre o MySQL do VHO e o LDAP, realizada pela aplicação LSC (*LDAP Synchronization Connector*)[8]; 1 base LDAP no formato CAFe; 1 servidor SP eduroam para validação com FreeRadius 3.0.17. Este último representa um SP eduroam de uma instituição.

Os passos referentes à Figura 1 são: **(1)** Administrador solicita autenticação no SP VHO; **(2)** SP VHO redireciona ao SP Chimarrão/CAFe; Os passos de uma autenticação CAFe acontecem normalmente: **(3)** SP Chimarrão/CAFe redireciona para o WAYF, **(4)** Administrador é requisitado a selecionar sua instituição para autenticação, **(5)** Administrador seleciona sua instituição para autenticação, **(6)** WAYF redireciona usuário Administrador para a instituição (IdP (4) Chimarrão/CAFe) para autenticação, **(7)** Usuário

[4] https://www.surf.nl/en/services-and-products/eduroam/eduroam-visitor-access/index.html

[5] https://tnc2014.terena.org/core/presentation/56

[6] http://eduroam.reuna.cl/solicitud-eduroampass

[7] https://www.switch.ch/it/aai/join/vho/

[8] http://lsc-project.org/

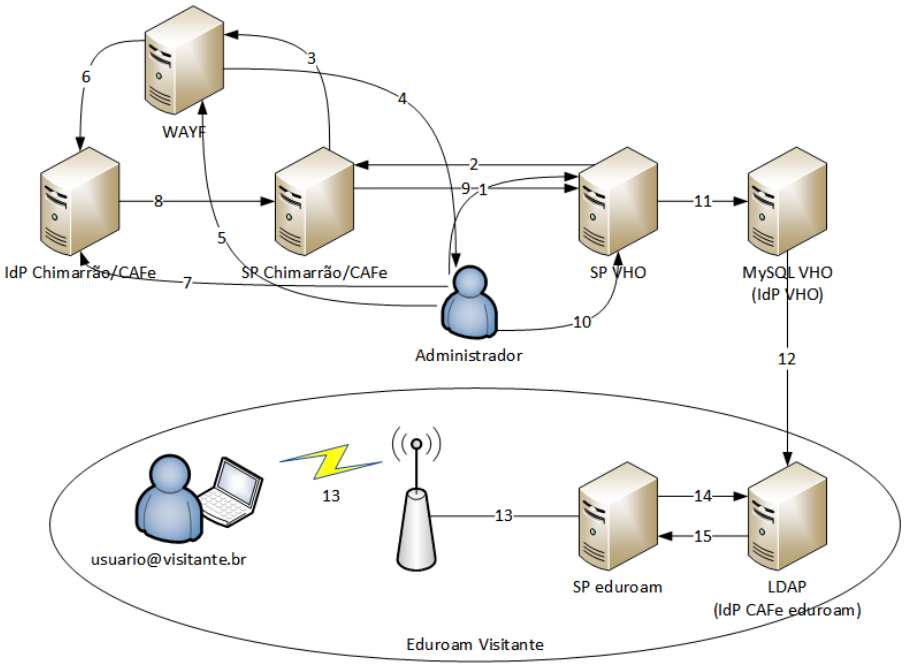

Figura 1. Autenticação e cadastro do Administrador, e autenticação e autorização do Visitante eduroam.

Administrador se autenticação no IdP Chimarrão/CAFe da instituição, **(8)** IdP Chimarrão/CAFe redireciona atributos do usuário Administrador ao SP Chimarrão/CAFe e **(9)** SP Chimarrão/CAFe encaminha atributos e autenticação do Administrador ao SP VHO. **(10)** Administrador cria conta de visitante - O Administrador deve selecionar a expiração para a conta (*e.g.* 7 dias). **(11)** Conta de visitante é armazenada no MySQL VHO (IdP VHO). **(12)** Sincronização entre MySQL e LDAP é realizada (IdP CAFe eduroam). **(13)** Usuário Visitante se autentica na rede eduroam utilizando o *realm* **@visitante.br**. **(14)** SP eduroam consulta credenciais e **(15)** SP recebe e valida credenciais do usuário Visitante no eduroam.

4. Conclusões

Como breve conclusão, este trabalho apresentou a experiência no desenvolvimento de uma nova solução de serviço apoiada no eduroam, o eduroam para visitantes. Uma solução nacional que visa se estender à comunidade eduroam mundial e, mais que isso, auxiliar instituições a utilizarem ainda mais, ou mesmo ingressarem, no serviço de AAA federado para acesso sem fio seguro.

Referências

Rubens, A., Rigney, C., Willens, S., and Simpson, W. A. (2000). Remote Authentication Dial In User Service (RADIUS). RFC 2865.

Smith, A., Zorn, G., Roese, J., Ph.D., D. B. D. A., and Congdon, P. (2003). IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines. RFC 3580.

Wierenga, K., Winter, S., and Wolniewicz, T. (2015). The eduroam Architecture for Network Roaming. RFC 7593.