UNIVERSIDADE FEDERAL FLUMINENSE
CIÊNCIA DA COMPUTAÇÃO
DEPARTAMENTO DE CIÊNCIA DA COMPUTAÇÃO

UENES LUCIO VILAÇA FERREIRA

Implantação de Infraestrutura da Federação CAFe na UFF

NITERÓI
2013

UENES LUCIO VILAÇA FERREIRA

Implantação de Infraestrutura de Federação

Monografia apresentada ao Departamento de Ciência da Computação da Universidade Federal Fluminense como parte dos requisitos para obtenção do grau de Bacharel em Ciência da Computação

Orientador:

Prof. PhD.EUGENE FRANCIS VINOD REBELLO

Niterói

2013

UENES LUCIO VILAÇA FERREIRA

Implantação de Infraestrutura de Federação

Monografia apresentada ao Departamento de Ciência da Computação da Universidade Federal Fluminense como parte dos requisitos para obtenção do grau de Bacharel em Ciência da Computação

---

Prof. Eugene Francis Vinod Rebello

Profª. Débora C. Muchaluat Saade

Profª. Aline de Paula Nascimento

Niterói

2013

Agradecimentos

Quero primeiramente agradecer a Deus, pelos parentes e amigos pelo apoio e força durante este curso. Agradecer ao meu orientador, Vinod Rebello pela paciência e confiança depositada em mim e no trabalho, pelas críticas tão preciosas que foram fundamentais. E finalmente agradecer a todas as pessoas da STI da UFF que contribuíram para tornar este projeto possível.

Resumo

As aplicações online vêm ganhando cada vez mais espaço nos últimos anos. Como por exemplo, Facebook, Twiter, serviços da Google como Gmail, buscas personalizadas, Google Docs, dentre outros. Como consequência, nossas informações tanto quanto nosso comportamento estão espalhadas pela grande rede. Por isto cada vez mais privacidade torna-se essencial neste cenário. São bibliotecas, histórico de pesquisa com interesses, fotos pessoais e profissionais, dentre outros serviços.

À medida que o tempo passa temos percebido na segurança das informações que os atacantes sempre estão um passo a frente da defesa. Sites do governo têm sido invadidos, manifestações em sites de políticos, caixa de entrada dos e-mails violadas e vírus a frente do antivírus. A informação tornou-se tão valiosa que mesmo que grandes empresas e sites governamentais invistam em segurança, o estímulo dos crackers pela invasão torna-se suficiente para alcançá-la. Quem dirá em sistemas e estruturas que subestimem a segurança da informação. Tendo esta perspectiva precisamos prezar pela segurança e dá-la um papel de maior destaque.

Este trabalho tem por propósito implantar uma infraestrutura de federação de identidade na UFF de acordo com as exigências da Comunidade Acadêmica Federada (CAFe). Isto proporcionará uma relação de ganho para todos os envolvidos, empresas provedoras de serviço, usuários e UFF. Com a implantação certamente a UFF terá um potencial maior para oferecer em segurança da informação, contribuição da privacidade dos usuário, oferecimento de maior conforto para seus usuários e maior integração com serviços externos a instituição.

Sumário

1. INTRODUÇÃO

"Tudo tem começo e meio. O fim só existe para quem não percebe o recomeço"
Luiz Gasparetto

1.1 Contexto: Gestão de Identidades, privacidade

Vivemos rodeados de muitos serviços, várias bibliotecas, laboratórios, serviços bancários. Mas não é qualquer um que pode entrar , por exemplo, em um laboratório e usá-lo. Este serviço pode ser destinado a somente um conjunto de usuários. Como descobrir quem é o usuário e se este pode utilizar o serviço? Esta necessidade é sanada com a gestão da identidade. Mas para isso faremos uma definição inicial de identidade. Pfitzmann e Hansen [15] definem identidade como: "A identidade de uma pessoa pode compreender em muitas identidades parciais no qual cada uma representa a pessoa em um específico contexto ou função. A identidade parcial é um subconjunto de valores de atributos de uma identidade completa, onde a identidade completa é a união de todos os atributos da identidades desta pessoa". O conjunto de atributos que definem a identidade no Laboratório de Computadores da Computação na UFF certamente não é o mesmo conjunto de atributos que definem a identidade para o uso de serviços bancários. Pela criticidade e natureza do serviço, o banco exige um conjunto de informações maior do que o uso de máquinas no laboratório de computadores.

Para utilização de serviços bancários como transferência, o cliente do banco precisa utilizar de procedimentos exigidos pelo próprio banco para mostrar que é quem diz ser. Ou seja, para eu fazer uma transferência financeira da minha conta para outra conta, preciso apresentar meu cartão bancário e apresentar minha senha. Supostamente, somente o usuário autorizado para tal operação conterá o cartão do banco e saberá a senha desta conta. Isto chama-se autenticação. No Capítulo 2 terá mais detalhadamente sobre este tema. Mas, como visto, a senha tem grande importância e acumula muita responsabilidade em sua confidencialidade. A função do login e senha para a maioria das aplicações online é de autenticar o usuário.

Na média os usuários tem cerca de 6.5 senhas, cada usuário tem cerca de 25 contas que exigem senha para acesso [17]. Isto resulta em escolha de senhas fracas pelo usuário para poder lembrar de cada uma delas. Com máquinas cada vez mais eficientes, senhas fracas

podem ser quebradas pelo método *brute force* facilmente. *Brute force* consiste em um algoritmo gerador de candidatos para senha, busca exaustiva de tentativa e erro para quebra da senha. Torna-se, então, mais seguro para o usuário conter somente uma senha forte do que várias senhas fracas. Algumas características na política de senha pode forçar ao usuário a criação de senhas consideradas fortes, duas delas são:

- Tamanho mínimo – Dependendo do tamanho mínimo escolhido o ataque de *Brute Force* torna-se muito custoso ou inviável. Cada novo *caractere* faz o custo de quebra aumentar exponencialmente;
- Complexidade da senha – Assim como o tamanho mínimo, a exigência de alguns símbolos de determinados grupos (Maiúsculo, minúsculo, algarismos e caracteres alfa-numéricos) tornam a senha mais protegida. Não permitir o uso de dados do próprio usuário também tende a contribuir na força da senha;

1.2 Motivação

O usuário terá uma única identificação com login e senha para muitos serviços como CAPES, DreamSpark, GISELA Science Gateway, dentre outros. Essa será uma comodidade para o usuário, pois reduz a quantidade de cadastros que precisaria ser feito para cada um desses serviços separadamente. Além da quantidade de formas de autenticação nos serviços, como os periódicos da CAPES que somente permitia acesso dos usuários que estivessem dentro do *range* de IPs da instituição de ensino que tem assinaturas. A decisão pela forma de autenticação, quando fica nas mãos dos provedores de serviço, se diversifica muito. Dificultando o usuário com cartões com código de barras, padrões de senha distintos e login diferente. Outro ganho em comodidade é no uso do navegador, aonde poderá se autenticar uma única vez e utilizar diversos serviços sem a necessidade de várias autenticações. Este benefício chama-se SSO, Single Sign-On.

Os ganhos não abrangem somente os serviços acadêmicos. Muitos serviços externos a universidade podem se beneficiar. Serviços que precisem de informações atualizadas e seguras sobre o vínculo de uma pessoa na instituição de ensino. Como por exemplo, no cinema ou *E-Academy License Management System da Microsoft*. Então o usuário para obter o serviço bastará se autenticar com a identificação na instituição de origem.

A privacidade dos dados do usuário também é outro grande benefício. Quando o usuário precisa provar seu vínculo com a instituição de ensino apresenta documentos como

histórico acadêmico, por exemplo. Esse tipo de documento informa muito mais do que o provedor de serviço precisa. Uma das soluções obtidas nesse trabalho é informar somente o que é necessário.

Existem serviços que, independentemente de onde o usuário estiver, ele poderá utilizá-lo. Estando em uma universidade em outro estado ainda poderia se beneficiar dos serviços desta universidade ao se autenticar com a mesma identificação da instituição de origem. O usuário poderá utilizar a rede sem fio da instituição ou obter livros nas bibliotecas podendo até devolver o livro na instituição de origem. Usuários poderão fazer uso dos computadores do laboratório ou se beneficiar dos restaurantes universitários de qualquer instituição de ensino e pesquisa do país. O que definirá a autorização para uso destes serviços será o próprio provedor do serviço.

Para os provedores de serviço tem um grande benefício na economia de tempo e investimento. Todo gerenciamento de identificação estará centralizado na instituição de origem. A garantia dos dados atualizados e confiáveis é de responsabilidade da instituição de origem do usuário. O provedor de serviço confiará na gestão de identidade das instituições participantes desta rede de confiança. E de fato, a integridade e confiabilidade destas informações sobre o usuário são de grande valia para a instituição de ensino. Esta instituição gera, por exemplo, carteirinhas e documentos oficiais como diplomas para os seus alunos, o que exige grande responsabilidade.

Esse grande leque de possibilidades vem através da infra-estrutura de federação que já está consolidado em diversos países. Com o SWITCH na Suíça, FEIDE na Noruega, WAYF na Dinamarca, dentre outros. Essa estrutura oferece um provedor de identidade da instituição de origem para todos os provedores de serviço que desejarem se beneficiar da terceirização da autenticação e cadastro de usuários, além do aumento da confiabilidade da informação.

1.3 Objetivo

Este projeto tem por objetivo implantar uma solução com padrão de nível internacional em gestão de identidade, autorização e autenticação na Universidade Federal Fluminense. Documentá-lo nesta monografia detalhando os conceitos aprendidos e aplicados para implantação da solução e as decisões em termos de infraestrutura tomadas para a conclusão do objetivo. Para isso será necessário seguir as exigências da RNP (Rede Nacional de Ensino e Pesquisa) que é a gerenciadora da Comunidade Acadêmica Federada, rede de confiança no âmbito nacional, com padrões e políticas no gerenciamento das identidades e autenticação dos

usuários. O projeto passará por testes de homologação para então estar disponível para uso com as configurações de produção.

1.4 Contribuição

Este trabalho deixará um grande legado para a UFF, os usuários vinculados à instituição poderão utilizar os serviços de outras instituições independente da localidade do serviço. Em todo território nacional, tendo o provedor de serviço vinculado a esta rede de confiança, os usuários poderão se autenticar sem o ônus de um novo cadastro. Com os dados de autenticação da instituição de origem poderá provar a identidade para o provedor sem divulgar informações não necessárias para a transação em questão.

Os ganhos de serviços compartilhados por uma estrutura de federação que atravessa instituições está sendo potencializado com a estrutura que amplia para serviços de vários países. Essa tendência de integração favorecerá bastante pela gama de serviços integrados com a identificação da instituição de origem. Quando um usuário da UFF estiver em congressos ou *workshops* em um desses países poderá fazer uso de um serviço vinculado nesta rede de confiança com os dados da autenticação da instituição de origem.

Os usuários da instituição que se vinculam com a federação desfrutam de SSO (Single Sign On), extinguindo a necessidade de nova autenticação para cada serviço acessado. Caso tenha sido autenticado, o usuário pode utilizar os outros serviços ligados à federação pois tecnicamente estarão com a comprovação da autenticação por causa de uma única autenticação do IdP (*Identity Provider*). Este é um dos principais ganhos oferecidos pelo trabalho pois, mais uma vez o crescimento da adesão de outros serviços tornará cada vez mais cômodo para o usuário a ideia de uma única autenticação.

Colaborará oferecendo desafios para a gerência da estrutura que cada vez mais aumentará a criticidade do serviço e precisará oferecer alta disponibilidade. Este trabalho incentivará na instituição a perspectiva de segurança e qualidade na infraestrutura. Um projeto deste porte, em longo prazo, exige uma política de segurança madura e investimento na infraestrutura. Como a unicidade da autenticação aumentará a importância das credencias e da estrutura, uma simples credencial de login e senha que oferecia acesso a poucos serviços, oferecerá uma gama bem maior de serviços.

Neste grande desafio de implantar a infraestrutura de federação, que contribuirá bastante com o avanço da universidade nos padrões nacionais da federação, existe a tendência

de grande acúmulo de conhecimento e crescimento profissional sobre temas críticos deste projeto para os envolvidos. Com as exigências do projeto de, inclusive grande responsabilidade, sem dúvida oferece uma grande possibilidade de crescimento. Pelo grau de criticidade do provedor, suportar pressão e colaborar em decisões importantes e de grande impacto serão fundamentais para o crescimento pessoal. Implantação de ferramentas que põem em prática muitos conceitos estudados no curso. Além da satisfação de estar contribuindo com uma universidade mais transparente, segura, integrada, evoluída no âmbito tecnológico e na gestão das identificações.

Com este trabalho a Universidade Federal Fluminense terá adequação aos padrões nacionais de autenticação estabelecidos pela RNP na CAFe. Uma das pressões feitas para que as instituições de ensino e pesquisa do Brasil abrace esta rede de confiança foi feita pela informação de que um serviço importante será oferecido somente pela federação. Neste caso foi a autenticação no portal de periódicos da CAPES. Este serviço é visto por alguns usuários como muito importante pois contribui para pesquisas de professores, fonte para escrita de trabalhos servindo como bibliografia.

A STI, Superintendência de Tecnologia e Informação da UFF, ofereceu todo apoio necessário para implantação do projeto. Portanto, toda infraestrutura necessária, como servidores e apoio técnico, foi providenciada para conclusão do projeto e implantação deste em produção. A STI mantém vários serviços, hoje, fundamentais para a gestão de muitos processos na UFF. Mantém o Sistema Acadêmico de Graduação (chamado IdUFF), que envolve inclusive lançamento de notas pelos professores, Inscrição Online dos Alunos, gestão de diplomas, extração de histórico e declarações assinadas digitalmente para o aluno, dentre outras funções para gestão. Contém também Sistema da Pós Graduação (Sispos), Sistema de Monitoria, além de outros.

A monografia está estruturada introduzindo no capítulo 2 os conceitos que envolvem a federação de identidade, assim como autenticação e exemplos de federações. Estarão descritos os benefícios das partes envolvidas na federação e algumas tecnologias utilizadas no projeto. No capítulo 3 a abordagem é sobre o processo de implantação da infraestrutura de federação na UFF, os problemas enfrentados e soluções, e as decisões diferenciadas na implementação. No capítulo 4 alguns exemplos de uso da federação na prática, com passo a passo de acesso para dois serviços federados que mais interessam os usuários atualmente, os periódicos da Capes e o DreamSpark da Microsoft. Uma forma de mostrar de forma objetiva o uso do trabalho e os ganhos diretos. E então, finalizando com o capítulo 5 com as conclusões tiradas

sobre o projeto, perspectivas de pequeno, médio e longo prazo e análise das decisões tomadas ao longo do projeto.

2. FEDERAÇÕES DE IDENTIDADE

"Não tenho medo dos computadores. Temo a falta deles."
Isaac Asimov

Neste capítulo o objetivo é apresentar os conceitos sobre federação de identidade e definições prévias necessárias para o melhor entendimento do projeto e entendimento dos termos utilizados ao longo da monografia. Será feita uma breve introdução com alguns termos básicos sobre o tema e logo na próxima seção será apresentado sobre identificação e autorização. Além dos conceitos básicos prévios e sobre a federação, serão apresentados também alguns exemplos de federação de identidade. Federação CAFe deste trabalho, InCommon e eduroam são as federações exemplo deste capítulo.

2.1 Introdução

Antes de entrar na descrição sobre identidade federada precisamos definir alguns conceitos. Alguns termos podem ser diferentes pela forma em que são chamados dependendo do autor que estivermos nos baseando. O termo usuário em computação tem sido tradicionalmente relacionado a um ser humano que interage com o sistema, ou seja, os que estão dentro do conjunto de pessoas que utilizam o sistema independente dos fins. Costuma ser visto como o elemento central de foco para os esforços de formar uma boa experiência com o sistema. Outro termo fundamental para seguirmos, abrange inclusive o usuário, o termo entidade. Este termo transmite uma associação entre um sistema de computador e uma entidade que pode ser um ser humano ou um sistema, um agente programado [2].

As informações do usuário são geralmente encapsuladas em uma conta, algumas vezes referenciada como um *profile*. A conta do usuário contém informações para a autenticação e pode conter um conjunto de atributos que descrevem o usuário. Cada conta de usuário é associada com um identificador que deve ser único para cada usuário. Naturalmente o sistema tem que ter como distinguir os usuários.

Um *subject* é o termo usado para identificar um processo em execução. Cada *subject* assume a identidade e o privilégio de uma única entidade. Uma entidade pode lançar vários processos dentro de um única sessão de login e assim será associada com múltiplos *subjects*, cada um acoplado com a identidade na sessão do login.

2.2 Identificação e Autorização

O processo de estabelecer a identidade do usuário é conhecido como Identificação. O objetivo é ter somente o usuário autorizado acesso a um sistema, rede ou serviço particular. A autenticação visa descobrir se quem tenta o acesso é realmente quem diz ser. Seria como mostrar um documento de identidade para uma autoridade, as credenciais da pessoa. Então, partindo deste ponto, validando a identidade do usuário, os demais dados do usuário, o *profile*, possibilitam ao sistema que provê o serviço decidir quais recursos este usuário poderá utilizar. Verificar se o usuário está ativo no estado do seu vínculo, por exemplo, com a instituição de ensino, ou verificar quais vínculos este usuário tem com a instituição de origem. Com a UFF o usuário pode ter o perfil de docente, estudante ou técnico, e até a composição de alguns destes perfis.

Cada usuário é associado a uma credencial de autenticação que é conhecida ou pertence somente ao usuário e que pode ser verificada pelo sistema. Esta credencial torna-se então a busca pela garantia de que somente o próprio usuário que é de direito pode informar. A premissa que uma entidade mantém secreta sua credencial é fundamental para a segurança, exceto quando precisa compartilhar esta credencial com o campo do sistema computacional designado para checar a autenticidade da identidade associada com a entidade. Ou seja, somente o próprio usuário tem a credencial, o sistema tem como checá-la e esta credencial é informada no momento em que se precisa provar a identidade. Existem três métodos para autenticação:

- Apresentação de algo que o usuário conhece: A senha, um número de identificação pessoal e uma palavra passe são esquemas comumente usados nesta categoria. O custo e a simplicidade do uso da autenticação via senha torna-a a forma de autenticação mais utilizada. Mas este método tem seus problemas e desvantagens. Senhas fortes são difíceis de serem lembradas e acabam contribuindo com comportamentos ruins dos usuários, como anotá-las em papéis ou em arquivos para lembrança. Senhas fáceis de se lembrar têm muitas vezes informações pessoais do usuário combinadas como data de nascimento, palavras muito recorrentes como Deus, nome do time de futebol, etc;
- Apresentação de algo que o usuário tem: Este esquema de autenticação guarda a informação da credencial em um dispositivo que geralmente é portável e pequeno como um cartão. Este dispositivo normalmente chamado de *token*. Por

ser mais custoso costuma ser utilizado como uma forma de incrementar a segurança de serviços críticos como bancos que relacionam transações financeiras.

- Apresentação de algo que o usuário é: Este esquema confia em algum traço biométrico que distingue usuários. Impressão digital, geometria da mão, desenho dos olhos, voz e reconhecimento de face assim como a assinatura com a mão.

2.3 Gerenciamento de Identidade

Nesses dias temos visto o crescimento dos serviços oferecidos para os mais diversos grupos de indivíduos através da Web. Recursos disponíveis por um conjunto crescente de tipos de negócios. As indústrias de entretenimento, música, cinema, estão todas incrementando a competitividade de seus negócios com o uso de tecnologia de cloud computing e virtualização. Neste cenário, cada vez mais o gerenciamento da identidade é fundamental para customização e melhora da experiência do usuário, proteção da privacidade e implementação de um controle regulatório. Identidade digital pode ser definida como a representação digital do conhecimento das informações sobre um indivíduo ou organização. Estas informações costumam ser usadas para vários propósitos, desde a prova da identidade da entidade como para oferecer permissão do uso de um conjunto de serviços. Identidade digital pode incluir informações sobre um indivíduo, como nome ou dados sobre documentos. Da perspectiva de prova da identidade pode conter informações biométricas, como iris, senhas ou impressões digitais dos dedos.

Normatizações relativas à gestão de identidade estão em andamento em muitas organizações. A busca da melhor ferramenta para gerenciar a infraestrutura ou a própria decisão estrutural para utilização e gestão da identidade. Algumas destas normatizações incluem a definição de identidade. Por exemplo, a recomendação ITU-T Y.2720 [16] define identidade como "Informação sobre uma entidade que é suficiente para identificar que a entidade está em um contexto particular.". Podemos pensar na identidade dividindo em três diferentes tipos de dados:

- Identificadores: Uma série de dígitos, caracteres e símbolos ou qualquer outra forma de dado que identifique uma entidade. Fundamental para distinguir um usuário do outro, ainda que seja um conjunto de caracteres que não faça sentido para os usuários, este tipo de informação é fundamental para a gestão da identidade;

- Credenciais: Um conjunto de dados que fornecem evidências para alegações sobre identidades. Uma credencial pode ser gerada baseada em um ou mais credenciais. Por vezes a senha, certificados digitais, impressão digital e SAML assertions;
- Atributos: O conjunto de dados que descrevem características da entidade. Como, por exemplo, nome completo, data de nascimento e endereço.

Uma das maiores preocupações da gestão da identidade nos dias de hoje é a privacidade que tem sido apreciada como "um fundamental direito humano". Privacidade engloba um conjunto grande de conceitos, como o direito de ser deixado sozinho, proteção da personalidade, da intimidade.

2.4 Federações Acadêmicas

Dentre os elementos de segurança da informação em computação o conceito inicial que costuma preceder os demais é a identidade. Uma identidade é a representação para o computador de uma entidade que pode ser física ou pode ser um agente programado. Uma entidade pode representar um usuário, um grupo de usuários, uma organização como um todo, um host de sistema ou algum dispositivo na rede. O gerenciamento da Identidade tem emergido entre questões que envolvem a proliferação da identidade entre as várias plataformas dentro dos limites das empresas e atravessando várias empresas e organizações.

A autorização é motivada pela necessidade de conceder acesso a informação, recursos e serviços para entidades autorizadas somente. Uma entidade é um termo genérico que referencia um agente ativo capaz de iniciar ou executar algum tipo de ação, ou que tem acesso a alguma informação.

Os recursos da web, que são confidenciais, são protegidos por alguma forma de autenticação tecnológica. Para acessar esses recursos seja via uma rede pública ou rede privada na intranet, os usuários têm sua identidade virtual verificada pelo sistema do próprio serviço[12]. Cada serviço tem sua própria gestão da identidade dos seus usuários gerando custo na criação desta funcionalidade de autenticação e custo no ciclo de vida das identidades [1].

A federação é composta por dois tipos de servidores, o provedor de serviço e o provedor de identidade. Estes provedores são descritos de forma mais detalhada nos próximos tópicos. Mas para que a comunicação e integração entre os servidores seja viabilizada, todos devem seguir o mesmo padrão. padrão de comunicação, formato dos dados compartilhados,

padrão na forma da autenticação, etc.

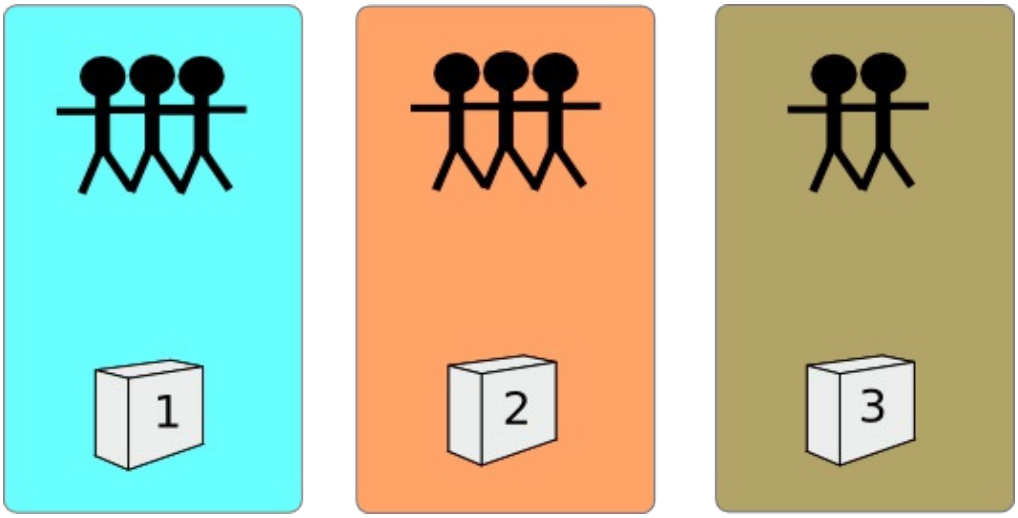


Figura 2.4.1 Autenticação dos provedores de Serviço sem uso de Federação

A figura 2.4.1 representa a estrutura de autenticação de provedores de serviço sem federação. Ou seja, cada serviço, 1, 2, 3, contém seus usuários cadastrados e gerenciados a sua própria maneira, sem padrões definidos. Tendo inclusive usuários na base do serviço 1, 2 e 3 simultaneamente.

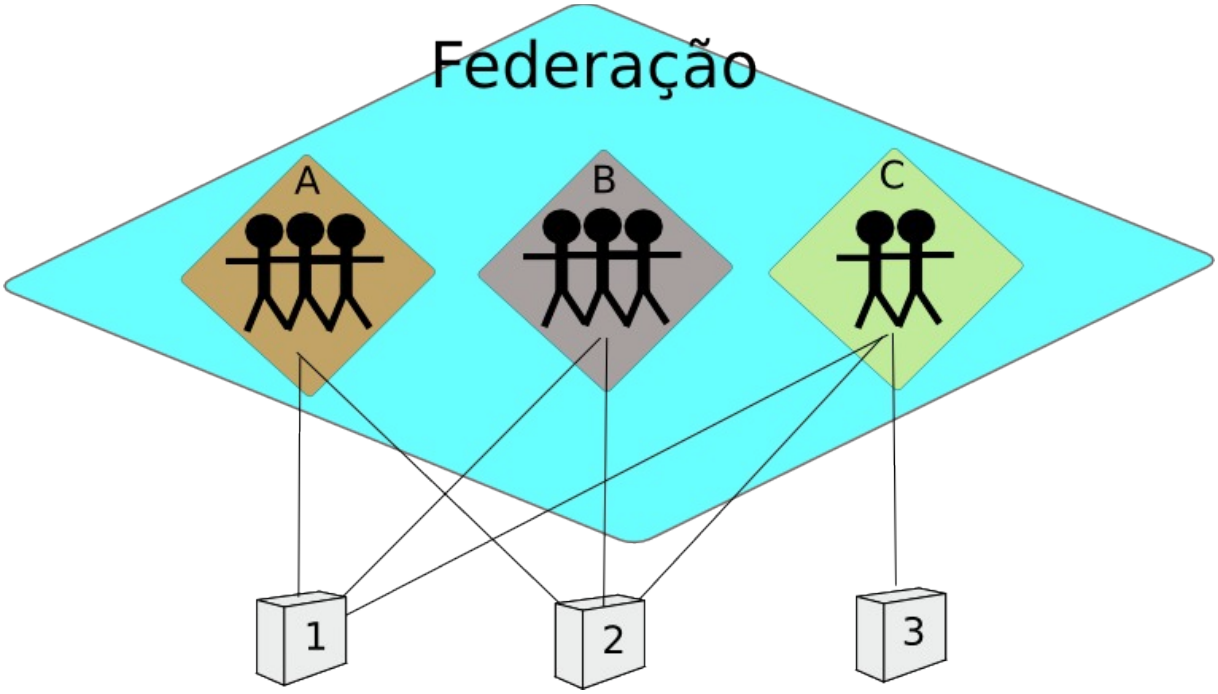


Figura 2.4.2 Acesso de Provedores de Serviço com uso de Federação

Nesta figura 2.4.2, há padronização do acesso dos serviços. Ou seja, para o serviço 1, não faz diferença se estes usuários se autentiquem no provedor de identidade A, B ou C. Importa que se autentique na federação, nesta grande rede de confiança.

A federação se manifesta no nível de identidade pelo mecanismo usado para permitir que um participante de uma organização acesse um provedor de serviço de outra organização. Transmite um senso genérico de flexibilidade e atividades flexíveis de um conjunto de entidades que cooperam. O resultado é que cada um dos provedores de serviço em uma federação terão atingido uma quantidade de identidades, de usuários, sem ter de gerir nenhuma destas identidades.

2.5 Provedor de Serviço

Provedores de serviço são os responsáveis por oferecer serviços ou recursos para os usuários. Por exemplo, são potenciais provedores de serviço os serviços de empresas ou instituições que têm como público os usuários vinculados a instituições de ensino ou precisem oferecer um valor diferenciado para algum tipo de usuário dessas instituições para federações acadêmicas. Como a Microsoft que oferece produtos gratuitos para os alunos do Instituto de Computação. A confiabilidade dessa informação que interessa a esse tipo de empresa é extremamente importante, visto que lida diretamente com o lucro da própria empresa.

Existem hoje muitos serviços oferecidos pela própria UFF que podem se tornar provedor de serviço e aproveitar dos ganhos que um provedor de serviço tem ao se vincular à Comunidade Acadêmica Federada. Alguns exemplos deste tipo de provedores na UFF são Sistema de Monitoria, IdUFF, Sistema de Pós-Graduação, Conexão UFF, PIBIC. Centralizando a autenticação e oferecendo SSO (Single Sign On). Além desses provedores de serviços web poderíamos acrescentar também outros tipos de serviço que terão plenas condições de se beneficiarem. Como por exemplo Bibliotecas, Restaurantes Universitários e Laboratórios de Computadores.

Quando o Provedor de Serviço se vincula a Federação passa a não ter mais dados diretos dos usuários, não precisa gerenciar as identificações. Passando a utilizar da gerência de identificação da instituição de origem. Ainda assim pode a partir de identificadores para cada usuário implementar estudos sobre o comportamento para oferecer um serviço inteligente e personalizado. Esse tipo de informação o Provedor de Serviço pode trabalhar. Não precisará saber que Uenes Lucio Vilaça Ferreira se interessa em produtos e serviços sobre esporte. Basta saber que o usuário 93847 tem esse interesse. Em uma estrutura como essa, um roubo das informações do provedor de serviço oferece um risco reduzido. Nas bases do provedor de serviço não há as informações dos usuários, quando o usuário se autentica no provedor, este recebe os dados necessários para oferecer o serviço ao usuário. Ao desconectar o provedor de

serviço não terá mais os dados pessoais do usuário. Se considerarmos o seguinte cenário, seis provedores de serviço onde cada um gerencie as identificações dos mesmos usuários. A vulnerabilidade dos dados de usuários aumenta consideravelmente quando tem um ou mais de um gerenciador de identidades muito vulnerável em termos de segurança da informação.

Não precisar investir recursos no cadastro e na manutenção torna essa escolha interessante financeiramente para os provedores de serviço. O custo de tempo da mão de obra para se construir e dar manutenção pode ser canalizada para outras melhorias ou mesmo economizada.

Ter informações sobre os usuários atualizadas é fundamental para oferecer o serviço a quem de fato deve receber. A desatualização pode tanto prejudicar o usuário quanto prejudicar quem presta o serviço. Caso um aluno se forme no primeiro período de 2011 e tente aproveitar que a validade da Carteira do Estudante é válida até o fim de 2011 poderá ganhar descontos no cinema ou criar uma conta bancária universitária. Neste exemplo apresentamos um ganho do usuário baseando em uma informação desatualizada. Por outro lado o aluno pode ter feito desvinculação com permanência de vínculo (por exemplo reingresso na faculdade). Podendo não ter forma rápida de provar para uma determinada empresa que ainda tem vínculo ativo com a instituição de ensino. No caso do vínculo do provedor de serviço com a federação, receberá informações com uma atualização satisfatória.

Outro problema frequente para o provedor de serviço que será minimizado é a fraude. Hoje em dia não tem sido muito utilizada a verificação eficiente dos documentos apresentados por um usuário para garantir um serviço ou uma vantagem desejada. Como por exemplo a carteira de estudante de qualquer instituição de ensino. Como não existem padrões definidos abre a facilidade da criação de carteiras falsas. A falta da padronização força ao orgão, que deseja autenticar o documento, a ter diversas formas de validação para garantia de validade dos documentos. Inviabilizando, assim, o processo de validação abrindo brechas para falsificações.

2.6 Provedor de Identidade

A dificuldade proveniente de muitos provedores de serviços que gerenciam os dados dos usuários é sanada com uma base centralizada. Aonde as identificações dos usuários são gerenciadas e servem de base autenticadora para os serviços. Provedor de Identidade é o provedor que se responsabiliza pela gestão dos dados dos usuários da instituição de ensino, autenticação e fornecimento de informações necessárias para os provedores de serviço. [10]

Ocorre um acordo entre o provedor de serviço e o provedor de identidade, essas informações são passadas para o provedor de serviço quando ocorre a autenticação. Essas informações são as necessárias para a avaliação sobre a autorização do usuário.

O provedor de identidade, no modelo mais comum, assume a responsabilidade de acordar sobre os atributos dos usuários que serão oferecidos para cada provedor de serviço vinculado a federação. Os atributos que serão passados para o provedor de serviço tratar da autorização de seus recursos serão fornecidas a cada autenticação realizada e, naturalmente, somente se a autenticação for bem sucedida.

2.7 Exemplos

Dentre os exemplos apresentados, este trabalho será mais detalhado na CAFe por a federação em questão, usada neste trabalho. Passará um *overview* sobre a comparação da CAFe com outras federações.

2.7.1 CAFe

A Comunidade Acadêmica Federada (CAFe) tem como objetivo alcançar as instituições de ensino e pesquisa do Brasil. Gerenciada pela Rede Nacional de Ensino e Pesquisa, esta federação visa favorecer a padronização na autenticação e autorização onde seus usuários poderão usufruir de maior conforto e segurança, mantendo suas informações somente na instituição de origem [8].

As instituições, detentoras dos dados dos usuários, assumem o papel de provedoras de identidade, centralizando a autenticação dos usuários que estão vinculados com a mesma. Tendo a responsabilidade de gerir os dados dos usuários, mantê-los devidamente atualizados e confiáveis para o uso da federação. O papel do provedor de serviço é mais abrangente, as instituições ou organizações que têm interesse neste conjunto de usuários de instituições de ensino são potenciais provedores de serviço.

O usuário por sua vez só precisa usar uma credencial, e somente precisará se autenticar uma única vez para acessar diversos serviços, além de ter a confiança de que seus dados permanecem em um único local, sua instituição de origem, e sua autenticação será feita nesta. Tornando desnecessários os vários cadastros e o fornecimento de dados pessoais causados pela aderência a vários serviços.

Figura 2.7.1: Acesso a serviços federados [9]

Por intermédio do *browser* o usuário tenta acessar um serviço federado, como na figura 2.7.1. Este por sua vez redirecionará o usuário para instituição de origem para que possa autenticá-lo. Com a autenticação do usuário bem sucedida, o provedor de identidade envia assertivas de autenticação e os atributos do usuário para o provedor de serviço requisitado inicialmente. A partir deste ponto o provedor de serviço poderá oferecer para o usuário o serviço condizente com seu *profile*.

Após a autenticação, o provedor de serviço poderá receber informações do usuário. Estas informações são chamadas de atributos, que poderão ser sobre o vínculo do usuário com a instituição de origem, os tipos de vínculo ou a data sobre o início destes. Estes atributos poderão ser usados para que o provedor de serviço trabalhe na autorização dos usuários.

A federação tem o papel também de definir os padrões de comunicação entre as partes envolvidas. No caso da CAFe o padrão para comunicação entre os provedores de serviço e provedores de identidade é o protocolo SAML[18]. Além de utilizar a aplicação Shibboleth[19] que engloba um conjunto de protocolos mundialmente reconhecidos pela eficiência em segurança ou no que se propõe. Este sistema foi desenvolvido nos EUA no projeto Internet2, este faz parte da sugestão da CAFe para provedores de serviço e de identidade. Naturalmente as instituições que não abraçarem o software sugerido reduzem o suporte da RNP para implantação do provedor e este escolhido deve ser compatível em termos de comunicação com o Shibboleth [19].

No modelo da CAFe com uso do Shibboleth, a responsabilidade da decisão sobre a liberação dos atributos para cada provedor de serviço fica a critério do provedor de identidade. Este pode decidir por oferecer determinados atributos para cada provedor de identidade, até em um contato sobre reunião das necessidades do provedor de serviço na autorização do usuário.

Em outro movimento para padronização, a CAFe definiu *schemas* padrão para as instituições manterem em suas respectivas bases LDAP [3] com as informações dos seus usuários. São estes os *schemas:*

- BrEduPerson: Contém informações sobre os usuários para a realidade do país [20] como e-mail, CPF, Passaporte, etc;
- EduPerson: Tem o propósito de facilitar na comunicação entre as maiores instituições de ensino. Consiste em um conjunto de dados ou atributos sobre os indivíduos das instituições. Informações como afiliação do usuário com a instituição, *distinguished name* (DN) da entrada do diretório que representa a instituição, dentre outros atributos.

O schema BrEduPerson utilizado pela CAFe encontra-se no anexo A.

Um conceito importante utilizado pela CAFe para aumento da confiabilidade entre as partes envolvidas é parecido com a *Trusted Third Party* (TTD). Este contém os metadados das instituições participantes com os endereços de cada uma. Conhecido como Where Are You From (WAYF), centraliza as informações para que o usuário possa ser direcionado para o provedor de identidade correto e retornar para o provedor de serviço inicial que motivou a autenticação do usuário. Pois com a inclusão de mais de um provedor de identidade não tem como o provedor de serviço saber qual instituição de origem do usuário que requisita o serviço. Mas com o WAYF pode-se pedir para que o usuário indique, resolvendo o problema. Como na figura 2.7.2 que difere da figura 2.7.1 na inclusão desta solução, inclusão do servidor da RNP que contém os metadados. A diferença no processo está após a requisição do serviço pelo usuário que precisará, dentre as opções, indicar qual instituição de origem pertence.

A estrutura oferecida também dá suporte para o SSO (Single Sign-on) através da utilização do protocolo padrão SAML. O que permite uma única autenticação para o uso de diversos serviços sem a necessidade de nova autenticação. Gerando um maior conforto para o usuário.

Figura 2.7.2: Componentes da Federação CAFe [9]

2.7.1.1 Atualização do LDAP

As instituições envolvidas na CAFe podem seguir as recomendações e construir uma base de dados LDAP. A RNP disponibiliza um *schema* chamado BrEduPerson que contém os dados necessários e sugeridos que são esperados pela federação.

Quando as organizações, no caso instituições de ensino e pesquisa, iniciam o processo de adesão a CAFe, estes tendem a encontrar-se mais provavelmente em uma das seguintes circunstâncias sobre suas bases de dados de vinculados:

- Várias bases distintas com atributos de alunos, professores e funcionários;
- Única base de dados consolidada de usuários vinculados à instituição.

Pela primeira situação nas instituições ser muito frequente, a RNP criou dois programas para exportação e importação de diretórios a partir das bases institucionais que consegue juntar todas estas bases em uma só. Assim, as instituições que contêm várias bases de dados que, com a interseção destas bases, o todo compõe a base completa dos vinculados com a

instituição, podem instalar e configurar essas ferramentas para atualização periódica dos dados no LDAP. Este software também pode ser utilizado para atualização do LDAP a partir de uma única base institucional.

Esta solução se divide em duas partes e dois softwares distintos: EID e EID2LDAP. O primeiro tem a função de agrupar as informações das bases da instituição em uma base intermediária local em MySQL. A ferramenta EID consegue ler de várias tipo de bases como Oracle, Mysql e até planilha. Além disso, coopera na conciliação de registros duplicados, visto que cada usuário deverá ter somente uma identificação. Nesta base intermediária os dados já estarão organizados bem próximos da estrutura e diferenciação de vínculos que o LDAP precisará. Através da criação de *selects* que executarão na base da instituição e 'popularão' a base intermediária da aplicação EID.

Em um segundo momento ocorre a importação no LDAP pela aplicação EID2LDAP que recebe os dados necessários para concluir a intenção. A comunicação entre estas duas aplicações ocorre via WebService residente dentro do EID.

Programas estes que possibilitam a adição e importação para o LDAP de novos atributos. Através das configurações destes dois programas podemos pegar atributos que também acreditemos que fazem sentido serem migrados para o LDAP. Ou seja, de acordo com as necessidades da instituição, pode vir a ser necessário que um novo atributo se propague, assim como os outros dados, para o LDAP.

2.7.1.2 Instituição de Origem do Usuário

Outro componente essencial na organização da estrutura da CAFe, já mencionado anteriormente, é o chamado *Where Are You From*. Quando o usuário deseja se autenticar em um serviço, como existem muitas instituições e o usuário pode pertence a qualquer uma, cabe ao WAYF obter a resposta sobre a instituição de origem do usuário. Assim poderá encaminhar o usuário para a tela correta de autenticação no IdP (*Identity Provider*) da instituição de origem.

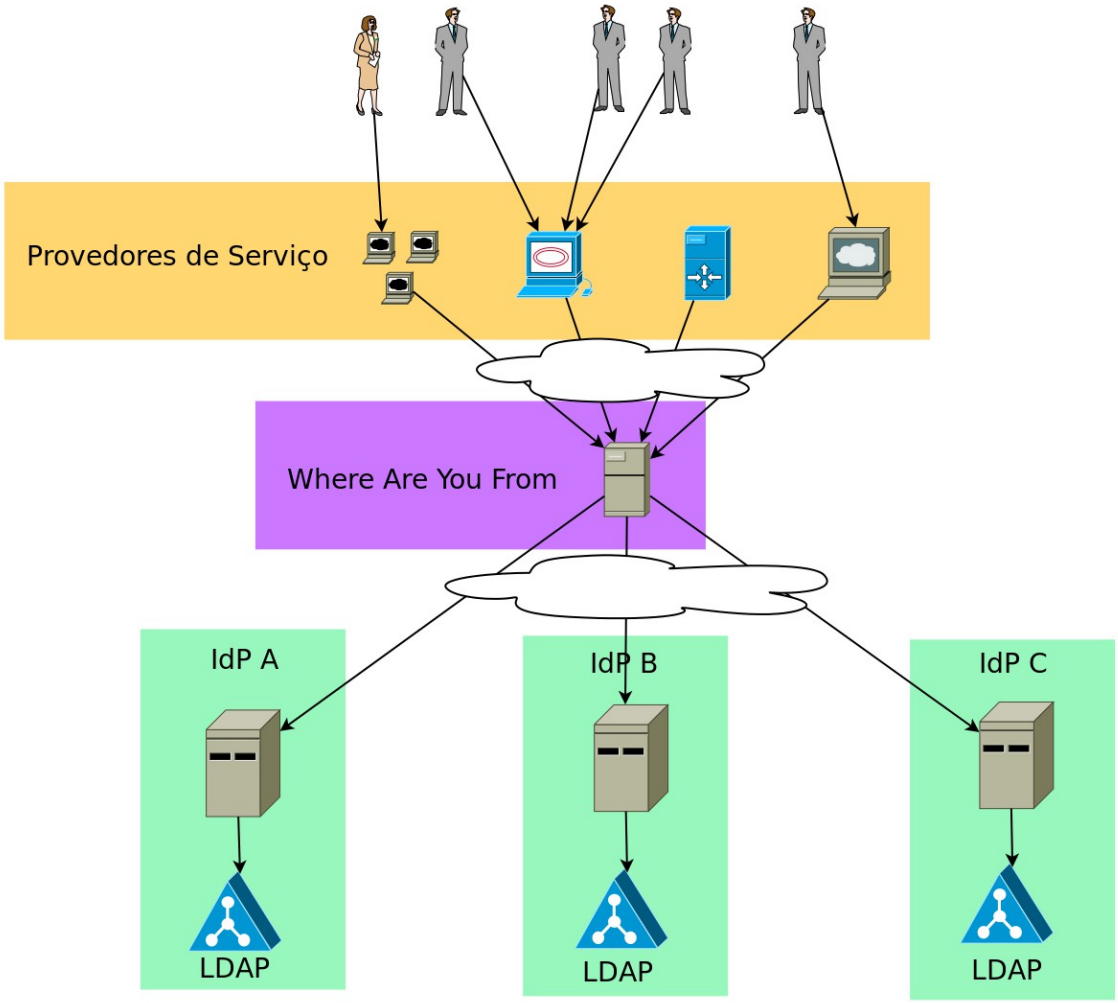


Figura 2.7.3 Estrutura montada da federação CAFe

A figura esquemática 2.7.3 representa a importância do WAYF, quando usuário busca um serviço federado. Como o serviço não sabe para qual provedor de identidade encaminhar o usuário, faz uso então do servidor que contém os meta dados da CAFe. Dentre as informações uma delas é quais instituições estão vinculadas a federação e estão prontas para autenticarem seus usuários.

2.7.2 InCommon

Assim como a CAFe, InCommon é uma federação acadêmica. Sendo que esta é destinado às instituições de ensino dos EUA. Mas tem uma estrutura bem parecida com a CAFe. Em termos de tecnologia, a federação InCommon também utiliza o Shibboleth como ferramenta e protocolo de comunicação SAML (*Security Assertion Markup Language*).

Mas um ponto que diferencia da federação CAFe é o pagamento de taxa anual. Para instituições de ensino do Brasil, juntar-se a CAFe é livre de taxas e custos. Mas no caso da InCommon existe uma taxa anual para cada instituição vinculada a federação, além da taxa de registro.

2.7.4 EduRoam

O Eduroam é um serviço de *roaming* federado que oferece acesso seguro a rede sem fio pela autenticação do usuário com suas credenciais no seu *Identity Provider* [5]. Voltado para a comunidade internacional de ensino e pesquisa, Eduroam (*Education Roaming*) permite que estudantes, pesquisadores e pessoas participantes deste vínculo de instituições de ensino possam ter conectividade com a internet através do campus que estiverem visitando. Bastando somente utilizar seu dispositivo seja smartphone, tablet ou laptop, na rede do campus contribuindo com a mobilidade [6]. A experiência que o Eduroam quer passar para o usuário é "Abra seu laptop e está online".

Este projeto teve início na Europa dentro da força tarefa TF-Mobility da TERENA (*Trans-European Research and Education Networking Association*) em 2003 com a adesão para o teste inicial em cinco instituições dos seguintes países: Finlândia, Portugal, Croácia, Reino Unido e Holanda. Posteriormente foi chamado de Eduroam.

Hierarquicamente o servidor RADIUS (Remote Authentication Dial-In User Service) é utilizado para estabelecer a autenticação através de uma requisição do usuário vinda da instituição visitada. Onde cada instituição tem um servidor RADIUS e este conectado a uma base local que contém os usuários na instituição de origem. Estes servidores das instituições são conectados a um servidor central de proporções nacionais [7].

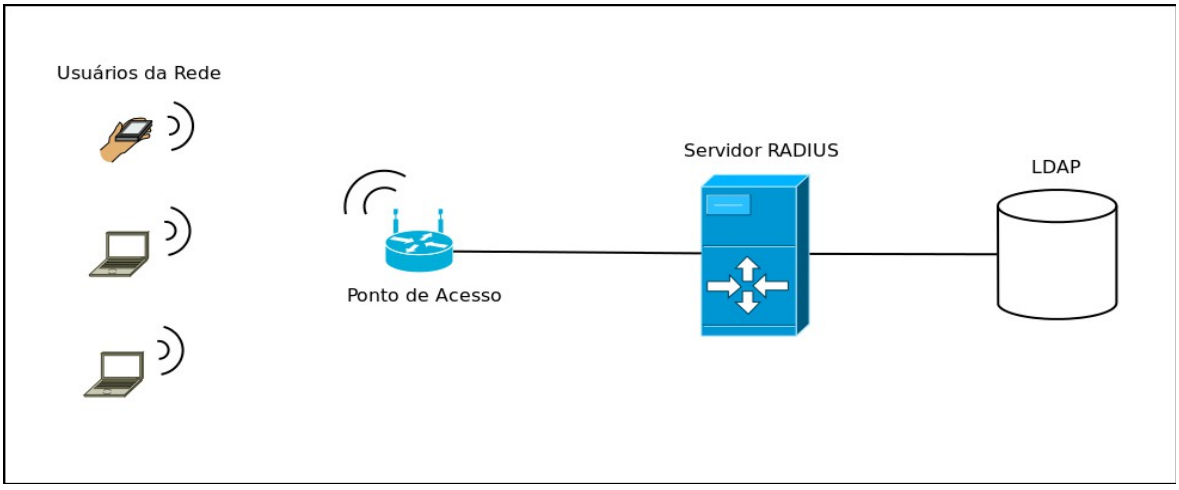


Figura 2.9.1: Acesso de dentro da instituição de origem no Eduroam

A figura 2.9.1 ilustra o uso local da rede wireless disponibilizada pela Federação EduRoam para o caso dos usuários locais da instituição. Os usuários utilizando na maioria seus dispositivos móveis para acesso a rede. A autenticação ocorre no próprio servidor RADIUS da instituição. O servidor acessa então a base local LDAP da instituição para validar a autenticação feita pelo usuário.

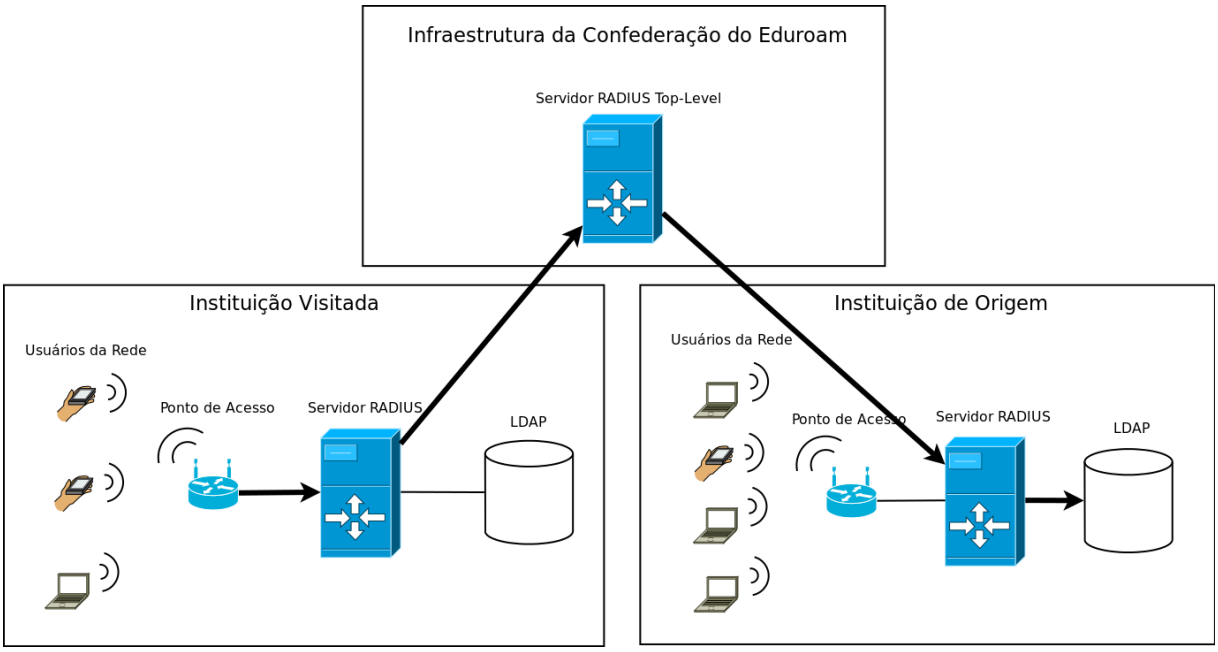


Figura 2.9.2: Acesso de fora da instituição de origem no Eduroam

Quando o usuário tenta acessar o serviço da rede wireless de fora da sua instituição de origem ocorre o processo que está na figura 2.9.2. A tentativa de acesso é direcionada ao RADIUS da instituição de origem passando por um nível mais alto da infraestrutura. Este nível é servidor RADIUS hierarquicamente acima dos servidores locais das instituições, responsável inclusive por este redirecionamento. Então o usuário poderá autenticar-se na instituição de origem.

2.8 Usuários

O publico alvo deste trabalho são os usuários vinculados com a Universidade Federal Fluminense. Todos estes poderão ser afetados com o resultado da implantação da federação na instituição, como alunos graduandos, pós-graduandos, funcionários técnicos e professores. Um dos interessados deste trabalho é a Superintendência de Tecnologia e Informação da UFF.

2.9 Benefícios

2.9.1 Provedor de Serviço

O provedor de serviço é uma das partes mais beneficiadas no ambiente de federação pela relevância dos ganhos. Um destes benefícios está no custo gasto para construção do cadastro dos usuários. Dispensa-se este custo pois este é como se estivesse terceirizado, sendo feito pelo provedor de identidade. Visto que o Provedor de Identidade já tem um banco com os dados dos usuários devidamente cadastrados e validados, oferecerá então este trabalho realizado no início do vínculo do usuário. A base de dados dos provedores de serviço para autenticação será equivalente aproximadamente a todas as bases das instituições de ensino participantes da federação. Pois estarão à disposição para uso aquelas que tiverem acordo com o provedor de identidade.

Além da autorização que deixará de ser responsabilidade do provedor de serviço. Ao descobrir a instituição de ensino do usuário, o usuário será encaminhado para se autenticar na instituição de origem. Outra mudança de foco na responsabilidade está na veracidade das informações fornecidas. Esta responsabilidade passa a ser do Provedor de identidade. Cada provedor de identidade deverá ser responsável pelos usuários a ele vinculados.

A necessidade de atualização periódica do vínculo do usuário torna-se custoso, pois sem federação esta informação não é atualizada imediatamente, menos ainda pela instituição de origem. Há poucos anos atrás a renovação de vínculo na biblioteca das Engenharias e Ciência da Computação na UFF exigia um plano de estudo dos estudantes a cada novo semestre. Esta renovação de cadastro normalmente é feita por intermédio do próprio usuário que tendencioso a manter o acesso ao serviço pode tomar atitudes incorretas. Dando margem até para falsificações de documentos na intenção do usuário manter acesso.

Quando o usuário precisa fazer alguma alteração nos seus dados cadastrais na instituição de origem precisa haver algum tipo de comprovação, como apresentação de documento. Logo, a tendência é que os provedores de serviço usufruam desta garantia feita pela instituição detentora e gestora destes dados. Em um cenário de amadurecimento das informações na base de dados dos usuários faria sentido a instituição ter vinculado o documento *scaneado* do usuário, seja por causa do cadastro inicial ou por alguma alteração cadastral. Estando apto a responder a qualquer auditoria a confiabilidade do processo.

No cenário sem federação, onde cada provedor de identidade tem sua própria base de

dados de usuários, tem-se uma duplicidade muito maior de dados. Em cada provedor de serviço conterá muitas vezes informações sobre o mesmo usuário. Isto dá margem para uma maior inconsistência, visto que nem todos poderão ter o mesmo nível de rigidez sobre a forma de cadastro e as possibilidades de alteração de informações cadastrais. Outro ponto que pode ser comum ficar inconsistente ou desatualizado é o vínculo do usuário com a instituição. Para propagar esta informação por todas as bases de serviço exigirá algum tipo de prova periódica sobre o vínculo do usuário com a instituição.

2.9.2 Provedor de Identidade

O Provedor de Identidade terá como ganho uma maior integração com serviços externos a instituição. Com isto a comodidade oferecida ao usuário tenderá a ser grande.

Além disto, tendo serviços internos a instituição, como bibliotecas, sites de gestão de alunos graduandos ou de bolsa oferecidas, poderão se tornarem provedores de serviço neste cenário de federação. Nisto abraçará todos os benefícios que os provedores de serviços têm, além de uma maior satisfação do usuário.

A padronização dos dados no que se refere ao LDAP, *schemas* em comum, na forma de acesso, permite uma maior utilização dos dados. Facilita e estimula a integração de novos serviços a federação e esta padronização é transparente. Qualquer serviço que quiser avaliar a possibilidade de se integrar a federação pode acessar os documentos que explicitam essa padronização usada.

2.9.3 Usuário

Em um cenário comum, cada serviço acessado exige uma autenticação realizada. Isto aparenta, se não incômodo, desnecessário para a visão crítica do usuário. Pois bastaria provar uma única vez que o usuário é de fato quem diz ser. Fazendo isto na federação, autenticando uma única vez, poderá acessar todos os serviços que tem de direito sem necessidade de nova autenticação. Isto chama-se Single Sign-On, da sigla SSO. Largamente utilizado por grandes organizações como o google por exemplo, bastando fazer login uma única vez para acessar Gmail, Google Calendar, Google Plus, dentre outros serviços.

Ao aderir em um novo serviço, na maioria das vezes basta se cadastrar e utilizar. Mas se considerarmos todos os serviços que temos acesso, são tantos serviços que seria muito mais confortável se somente houvesse um cadastro para vários serviços. Hoje temos uma

quantidade grande de cadastros já realizados e que realizamos com o tempo. Vários servidores contém nossos dados cadastrais, o que gera um esforço grande comparado com a estrutura da federação.

Utilizar uma única conta para muitos serviços evita que existam inúmeros logins e senhas distintos para o usuário guardar. Até por que as decisões sobre regras para logins sempre variam de serviço para serviço. Uns utilizam um e-mail, outros login, números de documentos, código gerado pelo sistema, etc. Outro problema que deriva desta multiplicidade de autenticações distintas é sobre a senha. Por causa da despadronização das regras de segurança para formação de senha segura, naturalmente o usuário cria diversas senhas distintas. Quando um usuário precisa fazer essas diversas senhas distintas acaba optando por senhas fracas [10] que sejam fáceis de lembrar ou guardando estas senhas em papéis, e-mails ou arquivos dentro da máquina pessoal. Todas estas formas de guardar a senha são falhas de segurança para devida inviolabilidade de acesso a serviços relevantes. Assim também quando assumimos uma única senha para diversos serviços, o peso da responsabilidade desta autenticação aumenta consideravelmente. Se com a mesma senha acessamos saldos do banco, professores lançam notas e compras, a tendência é que o usuário torne a senha mais segura e tenha facilidade de guardá-la. Além do mais é uma única senha.

Privacidade tem assumido um papel de destaque ultimamente. Com a vida dos usuários cada vez mais exposta ou guardada na nuvem, a violação de um servidor pode gerar problemas sérios de privacidade. Nos moldes do caso da solução sugerida, o provedor de serviço não guarda informações de dados cadastrais dos usuários. No caso da violação de um dos servidores os dados dos usuários não serão acessados pelo invasor, antes somente acessará um id único que representa um usuário na federação. O que não oferece diretamente informação nenhuma sobre o usuário. Qualquer personalização de serviço baseada no comportamento do usuário será pelo atrelamento do comportamento com o id do usuário e não com seus dados cadastrais.

2.10 Tecnologias

2.10.1 Shibboleth

A aplicação *open source* Shibboleth [19] foi criada para oferecer *Single Sign-on* atravessando as organizações. Ou seja, com somente uma identidade e informações de conta pode-se usufruir de muitos outros sistemas que estejam vinculados a federação independente

de qual organização ou instituição. Em termos de privacidade, os provedores de serviço não gerenciam as identificações podendo ainda assim, quando solicitado tratar a autorização do usuário.

Shibboleth tem se comprometido com a incorporação de padrões de identidade federada. Um destes padrões é o SAML (Security Assertion Markup Language) [18], um xml com formatação para intercâmbio de atributos na autenticação e autorização entre provedores de identidade e provedores de serviço. Ferramenta desenvolvida para ser aberta e gratuita, facilitando o gerenciamento de identidades e permissões.

De modo geral o Shibboleth trabalha similarmente como outros sistemas de SSO, com um diferencial para sua aderência com padrões. Além disso outro ponto que o distingue dos outros sistemas de SSO é o suporte fornecido para múltiplas organizações diferentes da organização do usuário, mantendo e protegendo a privacidade deste.

No caso abaixo são os passos para realização do SSO, mas não está levando em consideração o SSO dentro da federação, ou seja, estamos tratando somente de uma organização.

1. Tentativa de acesso do usuário ao recurso

O usuário inicia tentativa de acesso ao recurso protegido pelo provedor de serviço. Como este não está com a sessão ativa, ou seja, ainda não se identificou, o provedor inicia processo de SSO.

2. Provedor de Serviço questiona pela Requisição de Autenticação

O provedor de serviço, sabendo o endereço do provedor de identidade, prepara uma requisição de autenticação e envia. Geralmente o provedor de serviço e o recurso encontram-se no mesmo servidor.

3. Usuário Autenticado pelo Provedor de Identidade

Agora a avaliação é por parte do provedor de identidade. Caso o usuário já estivesse com uma sessão, com a autenticação já realizada, esta informação seria enviada para o provedor de serviço. No caso, o provedor de identidade percebe que o usuário não tem uma

sessão existente. O usuário então se autentica no provedor de identidade, com suas credenciais.

4. Provedor de Identidade cria a Resposta da Autenticação

Após a autenticação do usuário bem sucedida, o provedor de identidade prepara uma resposta de autenticação para o provedor de serviço e envia. A resposta de autenticação contém a informação de sucesso na autenticação e os atributos do usuário acordados entre o provedor de serviço e de identidade. Além disto encaminha o browser do usuário para o serviço novamente.

5. Provedor de Serviço analisa a Resposta

Quando a resposta de autenticação do usuário chega do provedor de identidade, o provedor de serviço irá validar a resposta, criar uma sessão para o usuário. Depois disto o usuário é enviado para o recurso.

6. Recurso Retorna o Conteúdo

Como no primeiro passo o usuário tenta acessar um recurso protegido mas desta vez este tem sessão e o recurso sabe quem ele é. Com esta informação o recurso pode decidir se este está permitido para a requisição do usuário e envia de volta o dado requisitado.

SSO Federado

Quando relacionado o nome do sistema Shibboleth pode vir a memória alguns títulos como federação ou Single Sign-On Federado. De fato, este sistema provê SSO e os passos são os mesmos com o Single Sign-On descrito acima, com a adição de um componente que é a federação. No SSO simples estão sendo considerados um Provedor de Identidade e Provedores de Serviço da mesma organização.

Pareceria bem razoável se, além de querermos trabalhar com um provedor de identidade para vários provedores de serviço, também trabalharmos com a ideia de um provedor de serviço para vários provedores de identidade. Quando um grupo de provedores de identidade e provedores de serviço organizam-se para trabalhar juntos no que tange a

autenticação e autorização, usualmente chamamos de federação. A inclusão desta teoria dentro do SSO implica a potencialização dos ganhos iniciais do próprio SSO. Ganhos no conforto do usuário que com somente uma autenticação poderá acessar muitos serviços, assim também o *logout* que serve para todos os outros serviços.

Atributos do Usuário

O Shibboleth também tem a funcionalidade de receber dados do usuário a partir do provedor de identidade. Esses dados de usuários são chamados de atributos ou atributos do usuário, esta informação que o provedor de identidade contém é interessante para vários provedores de serviço. Dados como: Nome, e-mail do usuário, número de telefones, informações relevantes do usuário na organização como status do vínculo, grupos que o usuário pertence, privilégios, etc.

Naturalmente com todos estes dados é preciso um cuidado especial no que tange a privacidade. Inclusive este é um tema que é visto como prioridade para a aplicação em questão. Dentro do provedor de identidade é possível o controle das políticas de compartilhamento de todos os atributos. Todas estas preocupações são centralizadas na gestão de quem implementa a solução na instituição de origem do usuário.

2.7.2 LDAP

Lightweight Directory Access Protocol é um protocolo padrão para comunicação entre clientes e servidores de diretórios. Ou seja, define o formato da mensagem e o transporte utilizado. Antes de descrever mais detalhes sobre o LDAP, passaremos por uma breve introdução sobre diretórios. O que permitirá um melhor entendimento do que se trata LDAP e sua origem.

2.7.2.1 Diretório

Diretório é um banco de dados especializado, uma coleção de componentes organizados em uma estrutura de árvore. O nome dessa estrutura é chamada *Directory Information Tree* (DIT), aonde as entradas do DIT são identificadas, sem ambigüidade, pelo *Distinguished Name* (dn). A estrutura é comparável com a estrutura de DNS na sua organização. Como os endereços .com representando o comércio, .edu instituições

relacionadas a educação. No diretório também podemos ter c=BR (*Country*) representando o Brasil e outro c=US para os Estados Unidos. Em um nível menor da árvore o=Google e com ou=Suporte e outro ou=Marketing. O atributo o representa a organização e o atributo ou representa a unidade da organização (*Organizational Unit*). A figura 2.7.1 expõe a estrutura de diretório:

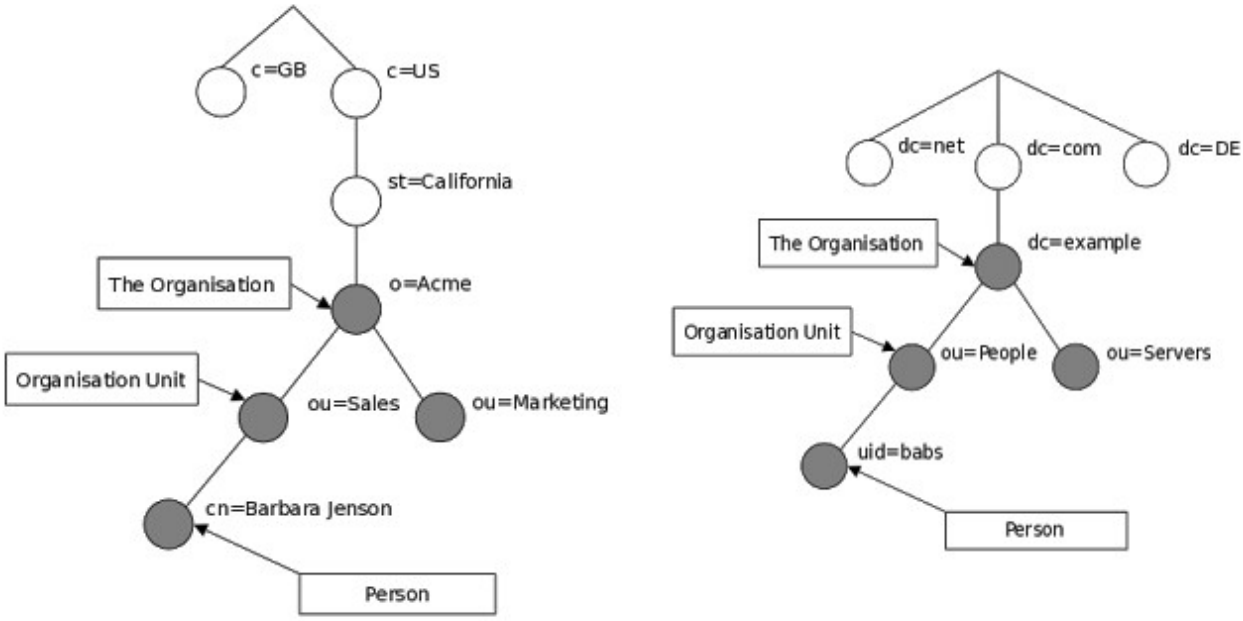


Figura 2.7.1 – Comparação entre a estrutura de diretório e DNS

Um Serviço de Diretório é uma coleção de software, hardware, processos, políticas e procedimentos administrativos para fazer a informação no diretório disponível para uso. O diretório de um Serviço de Diretório inclui inclusive os seguintes componentes:

- Informação contida no diretório;
- Servidores que suportem esta informação;
- Sistemas clientes da parte do usuário ou outra entidade que acesse esta informação;
- O hardware que estes clientes e servidores rodam;
- Sistemas de suporte como Sistemas Operacionais e driver de device;
- Infraestrutura de redes que conectará clientes e servidores;
- Política de quem poderá acessar o diretório, o que pode ser guardado, etc;

Como para alguns nichos da computação a base de dados relacional pode ser mais utilizada e se obtém um conhecimento maior, para facilitar o entendimento podemos fazer um comparativo entre este e diretórios. A primeira diferença que podemos destacar é no propósito, Banco de Dados Relacional é de propósito geral. Ou seja, oferece suporte total para todo tipo de operação, tem muita abrangência, mas pouca especialidade. A diferença sobre diretório é por uma base de dados especializada, ou seja, não é de propósito geral.

Por esse motivo deve ser refletido em que circunstância ou como o diretório pode contribuir. O perfil da informação é simples, a característica dos dados deve ser relativamente estático, que tem um baixo índice de *update* (escrita). Informações, como por exemplo, o histórico ou log do rastro de usuários em um determinado sistema é o tipo de informação completamente contrária à eficiência e suporte dos diretórios. Os logs dos sistemas são raramente acessados apesar de ser uma das habilidades mais relevantes para o uso de diretórios. Dados como, login e senha de usuário, documentos e nome são informações que usufruiriam muito bem dos benefícios oferecidos por diretórios. Pois são informações com alto índice de acessos e de consultas, exatamente o que tornam os diretórios interessantes. Pois diretórios são estruturas com especialidade no acesso a dados. Para este fim diretórios são muito mais eficientes que outras bases de dados. E esta é mais uma diferença das duas bases. A maior eficiência no alto volume de acessos do tipo *read* (leitura) em diretórios. Apesar de banco de dados relacionais serem constantes e oferecerem suporte para alto volume de acesso, é inferior quando comparado com os diretórios.

Entretanto, diretórios não dão suporte a transações. Pela seguinte definição transações: São operações que, ou devem ser feitas por completo ou não devem ser feitas, o claro tudo ou nada. Caso seja um sistema bancário, as operações de transferências causariam um grande transtorno se não fosse utilizada uma base de dados com suporte a transações.

Outra diferença fundamental é na forma de acessar os dados. Um erro visto comumente é causado pela popularidade das bases relacionais. Não se faz *select* nestas bases especializadas de diretórios. *Select* é um tipo de *query*, que por sua vez faz parte de um poderoso método de acesso chamado *Structured Query language*. Visto que diretórios são especialistas em acessos do tipo *read* e *search*, podem fazer uma busca simples e bastante otimizada como protocolo de acesso.

2.7.2.1 LDAP

A padronização do protocolo permite o benefício da interoperabilidade entre clientes e servidores. Este protocolo é considerado um protocolo "*Lightweight*", o que significa que é eficiente e fácil de implementar, enquanto se mantém altamente funcional.

A aceitação deste protocolo também tem sua relevância. As plataformas sejam desktop ou servidores (Microsoft Windows, Unix e Apple OS) das maiores organizações têm fácil integração e uso do LDAP. LDAP roda em cima do protocolo TCP/IP e tem várias APIs para várias linguagens.

A utilização do TCP/IP é um dos motivos de se chamar leve (*Lightweight*), pois o protocolo X.500 [11], anterior ao LDAP, usa o modelo de camadas Open Systems *Interconnection* (OSI). Comparado com o TCP/IP, há um maior overhead. Outro motivo é que o LDAP omite muitas operações do X.500 que são raramente usadas.

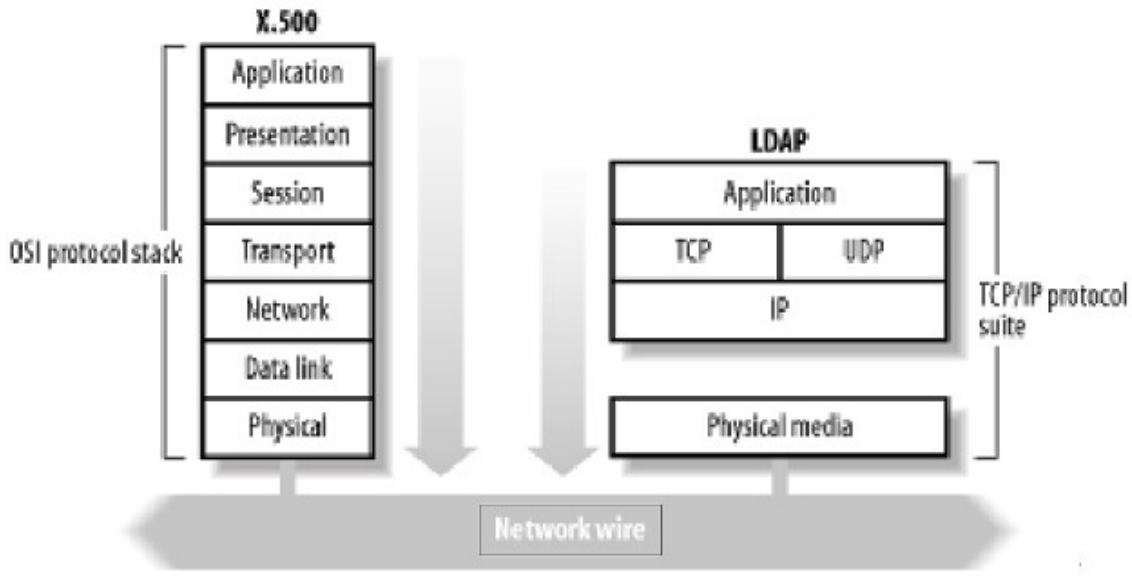


Figura 2.7.2.1 X.500 em cima do OSI versus LDAP sob TCP/IP [14]

LDAP tem a competência de receber múltiplas requisições simultaneamente. Mas, não necessariamente responde na ordem de chegada, ou seja, LDAP é assíncrono. Caso um cliente envie várias requisições, esse cliente pode receber as respostas em uma ordem diferente.

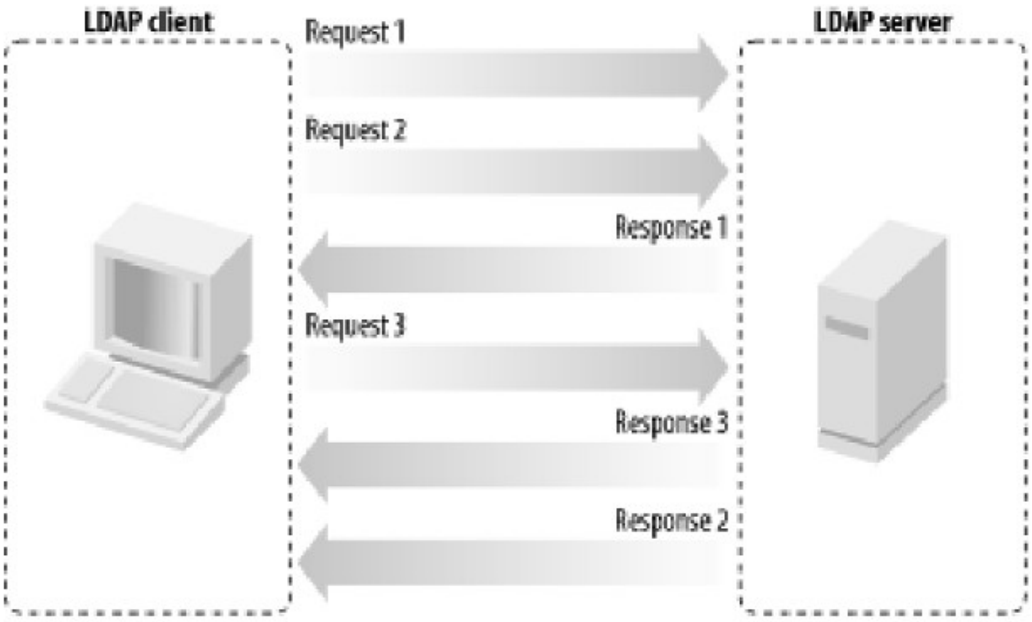


Figura 2.7.2.2 Requisições e respostas do LDAP [14]

O LDAP contém um modelo funcional com três conjuntos de operações:

Operações de Interrogação: Abrange busca e recuperação de dados do diretório. A operação de busca serve não somente para buscar entradas no diretório, mas também para retornar entradas individuais. No LDAP não tem uma operação específica para leitura, para ler uma entrada utiliza-se a busca com os critérios que retornem a entrada desejada e recuperação;

Operações de atualização: Este conjunto contém adição, deleção, renomeação e alteração de entradas;

Operações de Autenticação e Controle: Com identificação (*bind* e *unbind*) e controle de sessão (*abandon*). A operação *bind* serve para autenticar um cliente no diretório e o servidor, de acordo com as permissões do cliente, oferece os privilégios previamente especificados. A operação *unbind* desconecta o cliente fechando inclusive a conexão TCP.

LDAP pode oferecer alguns pontos interessantes como [21]:

- A possibilidade de gerenciamento centralizado de usuários, grupos, dispositivos e outros dados;
- A centralização da base de autenticação de muitas aplicações e sistemas operacionais em um mesmo diretório;
- Diminuição no custo pelo número reduzido de diretórios que deverá gerenciar;

- Evita a restrição de plataformas, visto que todas dão suporte ao LDAP;

2.7.3 Resumo

Este capítulo apresentou um *overview* sobre identidade e autenticação, pré-requisitos necessários para a introdução do tema de identidade federada. Que através da apresentação dos conceitos explicitou as soluções que agregam alguns problemas comuns no processo de adesão, autenticação e atualização dos usuários nos provedores de serviço. Além de dar exemplos de federações, incluindo a federação implantada por este trabalho de conclusão de curso. Mas para este trabalho também foi necessário o conhecimento básico de algumas tecnologis, frameworks e protocolos que são descritos também neste capítulo.

3. IMPLANTAÇÃO

"Vivemos todos sob o mesmo céu, mas nem todos temos o mesmo horizonte."
Konrad Adenauer

O objetivo deste capítulo é descrever o processo de implantação da infraestrutura de federação. Passando por uma descrição do quadro encontrado antes da implantação do trabalho, como funciona a estrutura de autenticação na UFF. Apresentação da expectativa de mudança esperada com o trabalho e o passo a passo realizado para instalação e configuração das aplicações necessárias para conclusão do projeto.

3.1 Infraestrutura Atual de Autenticação dos Serviços da Instituição

A infraestrutura de autenticação para os serviços e soluções existentes na UFF está baseada em um portal para algumas das aplicações. Essa solução tem por base a centralização da autenticação. Todos os sistemas institucionais desenvolvidos pela STI estão sendo incluídos debaixo da autenticação do portal. Quando o usuário decide-se por autenticar em um dos sistemas desenvolvidos é direcionado para o portal, caso não esteja já autenticado.

Para os serviços externos, não desenvolvidos pela Superintendência de Tecnologia e Informação da UFF, a gerência das identificações de seus usuários é diferente do modelo apresentado anteriormente. Neste caso o próprio provedor de serviço se compromete em realizar a gerência das identidades. O Bandejão, por exemplo, precisa criar seu próprio mecanismo para garantir a identidade do usuário, pois o preço é diferenciado para alunos, bolsistas, funcionários ou pessoas sem vínculo com a UFF. Como esses provedores de serviço atualmente não têm acesso às informações dos usuários por nenhuma funcionalidade, precisam manter as informações dos alunos atualizadas ou correm o risco de oferecer serviço a quem não poderia receber pela política interna de cada servidor, como mostrado na figura 3.1.1.

Algumas bibliotecas buscando facilitar a simples informação, para o Sistema Acadêmico da UFF, do status dos alunos que desejam pegar livro, pedem para ter acesso a essa informação junto aos gerenciadores do sistema. Visto que os funcionários das bibliotecas têm o vínculo de funcionários dentro da base, basta relacionar esse recurso para o vínculo do funcionário e, no início do período pode checar cada aluno se está com o status de ativo no

sistema.

No caso dos laboratórios, cada um trata de gerenciar as identificações isoladamente. O que gera um contínuo trabalho de criação e/ou manutenção da parte do gerenciamento de identificação. A tarefa de atualização do status e curso dos alunos ficam por conta da administração local. A figura 3.1.1 mostra em um desenho o modelo de autenticação de alguns serviços da UFF. Exemplificando como um dos usuários, usando o portal, pode ser identificado pelos funcionários das bibliotecas que precisam de informações sobre o vínculo dos alunos. Mostra o exemplo de outros tipos de serviço que têm bases locais e gerenciam cada um suas próprias bases, como no caso dos laboratórios de computadores e restaurante universitário.

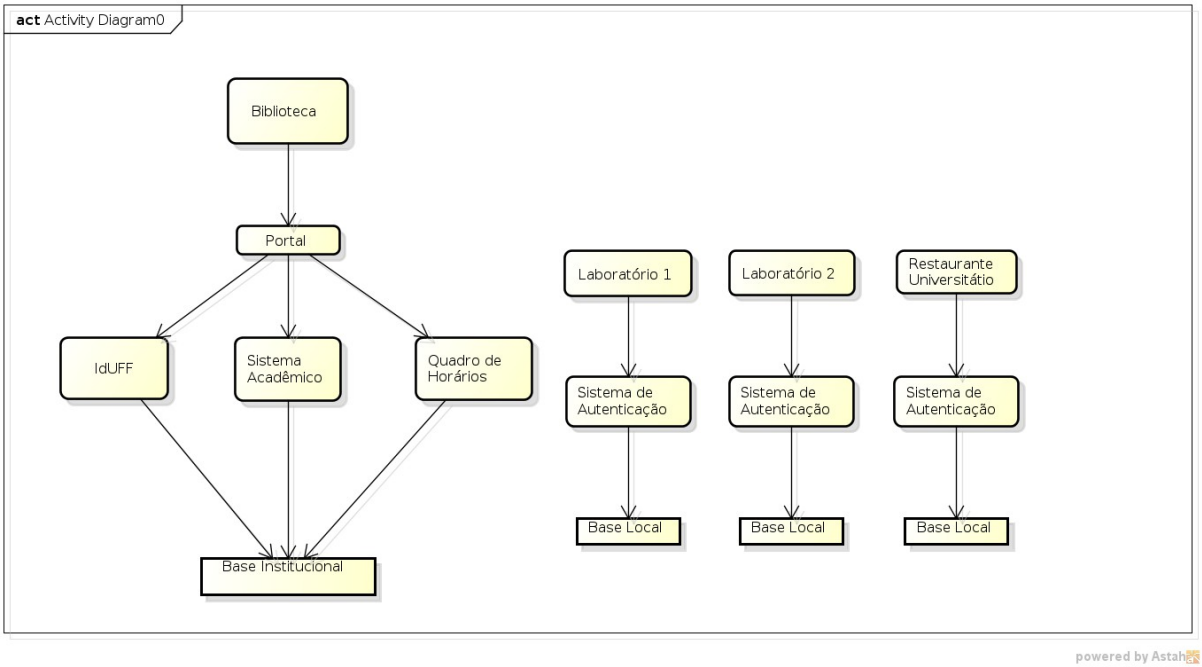


Figura 3.1.1 – Modelo interno de autenticação

3.2 Expectativas de mudança

Uma das expectativas das mudanças de curto prazo é o usufruto dos serviços que já fazem parte da federação e podem ser utilizados pelos usuários que têm vínculo com a Universidade Federal Fluminense. Como a CAPES, que já se encontra como provedor de serviço e os usuários que têm direito aos serviços da CAPES poderão usufruir do serviço. Além dos outros serviços das instituições federadas que podem ser oferecidos para usuários vinculados à UFF.

A implantação desta estrutura influenciou na criação de um LDAP contendo as contas

e informações da identificação dos usuários com a informação dos seus respectivos vínculos. A partir desta base, outra visão de curto prazo, está relacionada com paradigma da Infraestrutura utilizada para autenticação centralizada e com preocupações em segurança. Com essa ferramenta podemos implantar, internamente, para os funcionários habilitados, autenticação nas estações de trabalho da Superintendência de Tecnologia e Informação. Esta solução a partir do Samba para máquinas com sistema operacional Windows, abre as restrições que contas locais causam, onde para cada máquina somente pode autenticar quem tem uma conta local criada. Modificação que possibilita um melhor uso dos recursos e estimula que contas de usuários locais deixem de ser compartilhadas. Quando um funcionário mudar de localização ou tiver a máquina comumente usada poderá usar qualquer máquina que estiver ociosa, evitando a ociosidade do funcionário na espera da criação de conta local. No cenário de conta local, no mesmo problema anteriormente citado, acaba forçando para evitar a ociosidade, que usuários compartilhem contas. O que oculta e desprotege em termos de responsabilidade o dono da conta local para um possível erro ou ato suspeito realizado pelo funcionário visitante. Em termos de segurança, não existirão contas genéricas criadas para algum visitante, por exemplo. Facilita o gerenciamento de funcionários e estagiários que saem da organização e precisam ter sua conta excluída. A centralização em uma ferramenta e gerenciá-la em grupo, onde retirar a conta do grupo será suficiente para impossibilitar o acesso às máquinas e aos outros serviços baseados nesta visão.

O aproveitamento da estrutura gerada por causa da CAFe se estenderá facilmente para sites que o domínio da instituição comporta para os professores, por exemplo. Sistemas de gestão de conteúdo como Joomla e Drupal que são largamente utilizados, poderão aproveitar da base LDAP. Pois esta base se manterá atualizada e estruturada com grupos e a lista de controle de acesso que sejam convenientes para esta integração. Esta centralização facilitará o gerenciamento dos usuários, quando por exemplo perder o vínculo com a instituição e for necessário fechar os acessos para o mesmo em alguns serviços.

O conjunto de serviços que se juntarão a esta grande rede de confiança dentro da própria instituição deve crescer. Bibliotecas poderão ancorar nesta solução investindo mais recursos no gerenciamento da biblioteca e deixando de se preocupar com gerência de identificação. Laboratórios poderão buscar soluções dentro da estrutura que o núcleo de tecnologia da instituição pode oferecer.

Hoje vários sistemas criados pela própria instituição que criou como solução para a gestão da identidade, um portal. Este portal centraliza a identificação dos usuários para um

conjunto de sistemas implementando inclusive o SSO. Vislumbramos a possibilidade de unificar a gestão no IdP criado para tomar conta da gestão destes sistemas também. Dentre eles temos o Sistema Acadêmico (IdUFF), Sistema de Monitoria, Quadro de Horários, Inscrição, SisPos, etc. São sistemas legados que terão esta unificação com o IdP. Mas para isto o ideal é a evolução de alguns aspectos que hoje temos, principalmente a atualização do LDAP.

3.3 O processo de adesão da UFF na CAFe

O processo de adesão da UFF na CAFe foi baseado, na maior parte, na documentação da RNP em sua Wiki [13]. Com algumas alterações para adequação aos interesses da própria instituição. Estas alterações estarão descritas, assim como a explicação do que a motivou.

3.3.1 Instalação e Configuração Básica do Ubuntu 10.04 LTS

Introdução

A Federação CAFe recomenda e suporta a utilização da distribuição Ubuntu para instalar os servidores da Federação CAFe por disponibilizar os pacotes do Java 6 nativamente, software que é necessário para executar o EID, EID2LDAP e o Shibboleth-IDP. Além disso, o Ubuntu 10.04 LTS (Lucid) terá suporte para atualizações de segurança até Abril de 2015 [13].

Recursos da Máquina

Os recursos da máquina virtual que contém o EID e EID2LDAP são os seguintes:

- Memória RAM: 4096 MB
- Espaço em Disco: 15 GB

Instalar Diretório com o Esquema EduPerson

Extrair Dados Para o Metadiretório

3.3.2 Instalação EID

Introdução

Na parte inicial da exportação e importação de dados, das bases existentes da

instituição para o diretório, a ferramenta *Export/Import Directory* (EID) colabora com uma parte importante da exportação dos dados. Tem a funcionalidade de extrair os dados de várias bases e agrupá-las centralizadas. Muito importante quando a instituição tiver muitas bases que contribuirão para alimentar o diretório. No caso da UFF essa funcionalidade não é aproveitada pelo fato de termos uma única base com os dados necessários, o que minora muitos as possibilidades de problemas proveniente com mais de uma base legada.

Quando o uso desta funcionalidade, convergência de múltiplas bases, se faz necessário, o risco de ter mais de uma identificação ou conta para um mesmo usuário aumenta. Pois supondo o seguinte cenário: Em uma base A estejam armazenadas as informações sobre professores, na base B alunos de graduação e na base C alunos da pós-graduação. Naturalmente cada base guarda a identificação de seus usuários.

O risco encontrado em popular a base com identificadores duplicados é alta quando a instituição tem várias bases de dados com as informações dos usuários. Pois cada usuários deverá ter vinculado para si uma única identificação, sendo que um mesmo usuário pode já ter sido aluno de graduação, pós-graduando e atualmente um docente ativo. Este tipo de mapeamento sem uma eficiente ferramenta de apoio gera muitas dificuldades.

Para unificar as bases precisaríamos escolher um atributo único de um usuário que una todas as identificações. Considerando a possibilidade de uma das bases ter esse atributo inconsistente será gerada uma duplicidade de registro para um mesmo usuário. Pois caso o atributo do usuário X, usado para unificação, for diferente entre as bases, por qualquer que seja o motivo, as duas identificações se passarão como distintas, logo como usuários distintos. Para esse tipo de problema a ferramenta EID disponibiliza uma funcionalidade de unificação de registros duplicados. Buscando na base extraída registros que, provavelmente, estão duplicados e oferecendo a possibilidade de unificação.

O EID trabalha com o conceito de Metadiretório, uma base relacional intermediária entre as fontes efetivas dos dados e o diretório LDAP. Uma importante funcionalidade do EID é a capacidade de importar informações de outros sistemas, permitindo assim integrar e consolidar bases legadas, servindo como ponto intermediário para construção de um ou mais diretórios.

Qualquer sistema que armazene seus dados em bancos de dados relacionais e/ou arquivos de texto CSV podem ser importados pela ferramenta. O EID disponibiliza um Web Service para exportação e consulta de dados, o que facilita o acesso por aplicações que

utilizem tecnologias diversas. O Web Service serve de base também para outras ferramentas de exportação, como o EID2LDAP.

A seguir serão apresentados os requisitos bem como roteiro para a referida instalação. É importante ressaltar que ao longo da instalação existem variáveis (entre chaves{}) que devem ser substituídas manualmente pelos seus respectivos valores.

Para conhecimento de parte do modelo do banco de dados Oracle que foi é a base origem que será mapeado para o LDAP, segue figura 3.1.2

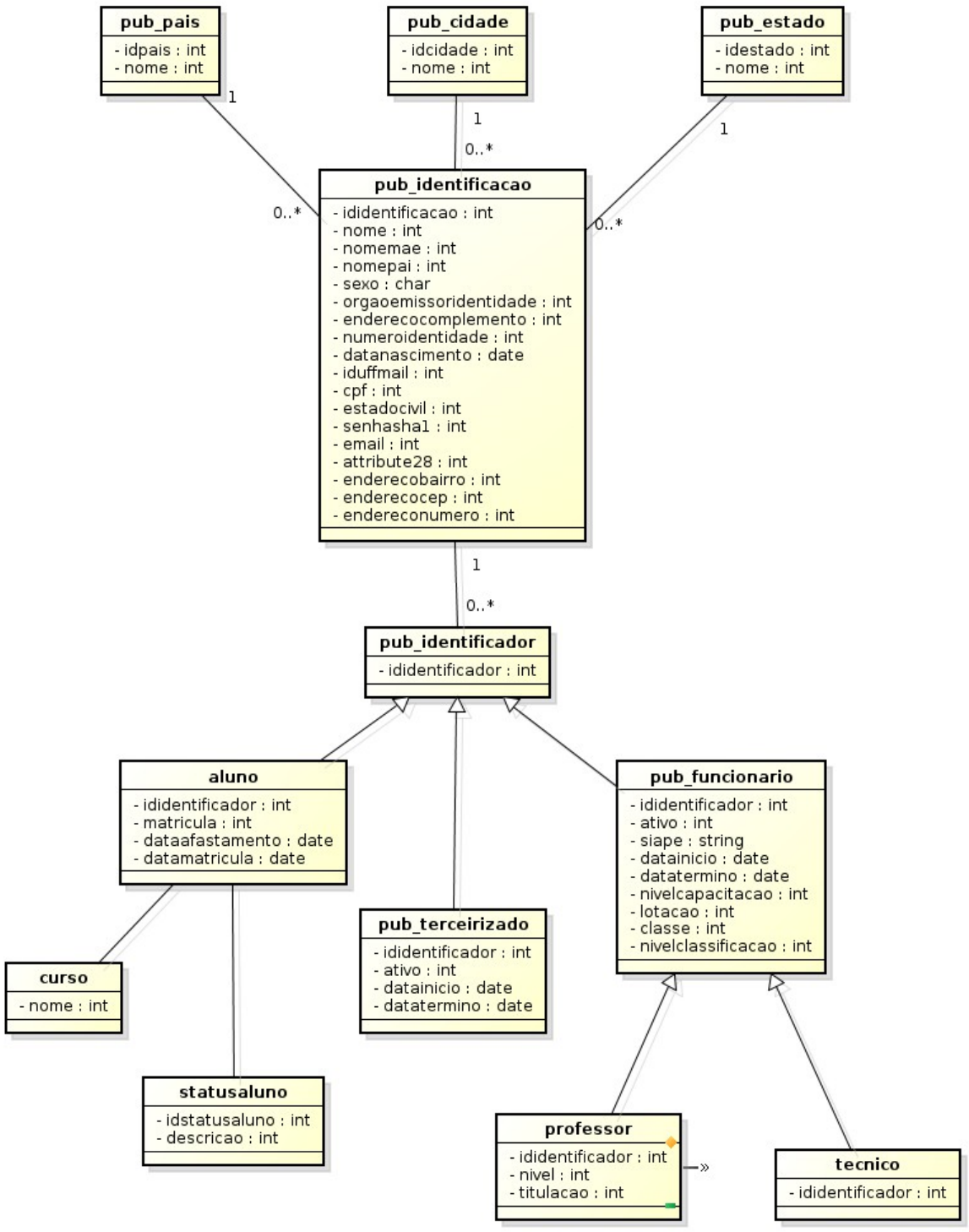


Figura 3.1.2 Modelo de parte da base relacional da UFF no Oracle

Instalação

Introdução

Esta aplicação foi criada com a intenção de receber em uma base MySQL intermediária a junção das bases da instituição necessárias para popular o LDAP com os perfis de Aluno, Técnico e Professor. Como existem instituições com este tipo de demanda que

geraria um custo alto implementar solução conciliadora, a RNP investiu na ferramenta que inclusive verifica a base e implementa a conciliação, além de indicar as possíveis identificações duplicadas de um mesmo usuário. Esta conciliação e sugestão de conciliação é feita pelo algoritmo Jaro Winkler, que por sua vez necessitará ser instalado dentro do EID.

Base de dados

A solução do guia de instalação sugere instalação e configuração do MySQL local, na própria máquina. Mas esses dados são dos usuários da instituição, vindos diretamente de uma base institucional. Logo, a adequação às normas e políticas internas é essencial. Na STI temos um provedor de serviços MySQL, diferenciando do passo a passo sugerido pela wiki da RNP, entregamos o serviço das bases MySQL necessárias aos DBAs da instituição.

O arquivo necessário para executar um dump na base eid e pcollecta foram fornecidos pelo guia de instalação, que pode variar de acordo com a versão da aplicação.
Ex.:

Versão 1.3.5

```
wget https://svn.rnp.br/repos/CAFe/ubuntu/hardy/instalacao-eid/eid-$VERSAO_EID.dump
-O /tmp/eid-$VERSAO_EID.dump --no-check-certificate
wget https://svn.rnp.br/repos/CAFe/ubuntu/hardy/instalacao-eid/pcollecta-
$VERSAO_EID.dump -O /tmp/pcollecta-$VERSAO_EID.dump --no-check-certificate
```

```
mysql -hmysqlapps.sti.uff.br -ueid -p eid < /tmp/eid-$VERSAO_EID.dump
mysql -hmysqlapps.sti.uff.br -ueid -p pcollecta < /tmp/pcollecta-$VERSAO_EID.dump
```

Dados do Servidor MySQL Utilizado

DNS: mysqlapps.sti.uff.br
Porta (Default): 3306

Configuração

Tomcat6

Alteração das configurações das opções do java no arquivo ***/etc/default/tomcat6***, relacionado também ao algoritmo Jaro Winkler:

```
JAVA_OPTS="-XX:MaxPermSize=512M -Xmx512M -Duser.timezone=America/Sao_Paulo
-Duser.language=pt -Duser.country=BR -Djava.library.path=$JARO_WINKLER_DIR
-Dfile.encoding=UTF-8"
```

Edição do arquivo */etc/tomcat6/tomcat-users.xml* como sugerido pelo passo a passo. Este arquivo é para configuração de usuários do tomcat.

```
<tomcat-users>
<role rolename="manager"/>
<user username="eid" password="{SENHA_EID}" roles="manager"/>
</tomcat-users>
```

No site *http://sourceforge.net/projects/eid/files/eid* encontram-se várias versões do EID. Naturalmente o recomendado é adquirir a última versão disponível.

Crie a pasta da aplicação na pasta opt na raiz e descompacte o arquivo da aplicação baixado anteriormente na pasta criada:

```
mkdir /opt/eid-$VERSAO_EID/
unzip /root/softwares/{ARQUIVO_BAIXADO.WAR} -d /opt/eid-$VERSAO_EID/
```

No arquivo /etc/tomcat6/Catalina/localhost/eid.xml estarão alguns dados de configuração do eid e deploy no tomcat6.

```
<Context docBase="/opt/eid-$VERSAO_EID/"
          privileged="true"
          antiResourceLocking="false"
          antiJARLocking="false"
          unpackWAR="false"
          swallowOutput="true"
          workDir="work/Catalina/localhost/eid">

  <Realm className="org.apache.catalina.realm.MemoryRealm" />

  <Resource
    name="jdbc/pCollecta"
    type="javax.sql.DataSource"
```

```
        validationQuery="SELECT 1"
        testOnBorrow="true"
    driverClassName="com.mysql.jdbc.Driver"
    maxIdle="10"
    maxWait="5000"
    username="root"
    password="$SENHA_MYSQL"
    url="jdbc:mysql://localhost:3306/pcollecta"
    maxActive="50"
    factory="org.apache.tomcat.dbcp.dbcp.BasicDataSourceFactory"/>

  <Resource
    name="jdbc/eid"
    type="javax.sql.DataSource"
    validationQuery="SELECT 1"
        testOnBorrow="true"
    driverClassName="com.mysql.jdbc.Driver"
    maxIdle="10"
    maxWait="5000"
    username="root"
    password="$SENHA_MYSQL"
    url="jdbc:mysql://localhost:3306/eid"
    maxActive="50"
    factory="org.apache.tomcat.dbcp.dbcp.BasicDataSourceFactory"/>

  <WatchedResource>WEB-INF/web.xml</WatchedResource>

</Context>
```

Comentário

Localização da instalação do EID.

```
<Context docBase="/opt/eid-$VERSAO_EID/"
```

Usuário e senha configurados no servidor MySQL.

```
username="root"
password="$SENHA_MYSQL"
```

O localhost, 3306 e pcollecta é o endereço do servidor MySQL, porta (3306 é a padrão do MySQL) e base de dados, respectivamente.

```
url="jdbc:mysql://localhost:3306/pcollecta"
```

Algoritmo Jaro Winkler

Configuração e instalação do algoritmo de conciliação Jaro Winkler entro do EID. Posteriormente configuramos um algoritmo muito mais simples que não executa a conciliação, apenas insere as pessoas considerando que não existem pessoas duplicadas. Este algoritmo é um pouco mais rápido que o algoritmo que faz a conciliação mais pesada. Por fazer carga de uma única base de dados não precisamos da conciliação feita pelo EID, logo esta abordagem é interessante para nosso caso. Esta modificação está detalhada na parte de edições do EID.

Criação da variável de ambiente Jaro Winkler:

```
 mkdir -p $JARO_WINKLER_DIR
```

Como a máquina configurada é 64 bits (x86-64) é necessário fazer uma mudança no Makefile do algoritmo para compilar corretamente. Foi nosso caso, a máquina configurada que ficará com as aplicações de carga é x86-64. A pasta contendo o Makefile e os arquivos para compilação está em /opt/eid-$VERSAO_EID/WEB-INF/classes/br/ufmg/lcc/eid/model/conciliator. Abaixo está a modificação que deve ser feita:

```
...

List: List.c List.h
         gcc -fPIC -c -o ${JARO_WINKLER_DIR}/List.o List.c

...

compile: JaroWinklerConciliationAlgorithm.c List
       gcc -o ${JARO_WINKLER_DIR}/libJaroWinklerLib.so -shared -fPIC -Wl,-
soname,JaroWinklerLib -I/${JAVA_HOME}/include/ -I/${JAVA_HOME}/include/linux
JaroWinklerConciliationAlgorithm.c ${JARO_WINKLER_DIR}/List.o -lc

...
```

Para compilar o algoritmo dentro do EID, basta executar os seguintes comandos:

```
cd /opt/eid-$VERSAO_EID/WEB-INF/classes/br/ufmg/lcc/eid/model/conciliator
make compile
```

Edições

Conciliador

A funcionalidade de conciliação é importante para o objetivo do EID, unificando mais de uma base institucional. Para a tabela de identificação, que contém dados do usuário, a relação de usuários e registro de identificações existentes deve ser um para um. Cada usuário deverá conter somente uma identificação. Para solução do problema da existência de dois ou mais registros de identificação para um usuário a aplicação trabalha com um algoritmo de comparação. Através do algoritmo Jaro Winkler a aplicação compara dados do usuário, como Nome, Data de Nascimento, Nome do pai e da mãe, para encontrar registros duplicados ou informar possíveis usuários com duas identificações.

Naturalmente esta funcionalidade tem custo. Cada novo usuário inserido inicia a execução do conciliador na comparação deste usuário com os usuários já existentes. Enquanto o usuário não passa pelo processo de conciliação, não está apto para ser transportado para o LDAP. O tempo total de carga da base institucional para o LDAP aumenta consideravelmente.

Para o caso da UFF seria interessante que tivéssemos a opção de desabilitar a funcionalidade. Pois a UFF tem somente uma base. Portanto não tem ganhos mas assume o custo vinculado a funcionalidade. Para tanto, buscamos orientação para desabilitar a funcionalidade obtivemos a seguinte solução para minimizar os custos:

Abrir o arquivo /opt/eid-VERSAO/WEB-INF/classes/ModelConfig.xml;
Substituir a linha

```
<bean id="br.ufmg.lcc.eid.model.conciliator.ConciliatorBO"
class="br.ufmg.lcc.eid.model.conciliator.JaroWinklerNativeConciliatorBO"/>
```

por

```
<bean id="br.ufmg.lcc.eid.model.conciliator.ConciliatorBO"
class="br.ufmg.lcc.eid.model.conciliator.NullConciliatorBO"/>
```

Reestart no tomcat6 com o comando:

```
service tomcat6 restart
```

Com isso trocamos o algoritmo de conciliação por um que não faz a conciliação, apenas insere as pessoas considerando que não existem pessoas duplicadas, ele é um pouco mais rápido que o algoritmo que faz a conciliação mais pesada.

Servidor MySQL

A STI tem um servidor de MySQL que na arquitetura centraliza as bases MySQL em um único servidor para gerência e domínio dos DBAs.
Para mudança da base MySQL local para o servidor da instituição foram feitas as seguintes modificações:

- Abrir o arquivo /etc/tomcat6/Catalina/localhost/eid.xml;
- Alterar as configurações do arquivo para
  DNS: appsmysql.sti.uff.br
  Usuário: eid
- Entrar no eid.sti.uff.br:8080/eid e modificar as configurações da base do metadiretório em Configuração>Repositório de dados.

Permissão e Negação de Acesso via Tomcat6

Estas duas aplicações de carga são gerenciadas via Browser na porta 8080. A forma de acesso é via login e senha, mas a aplicação EID contém um webservice que não exige autenticação para consultar a base. Com o conhecimento destes métodos disponibilizados pelo webservice pode-se consultar qualquer dado da base MySQL do EID. Conhecimento esse que pode ser obtido pelo manual do EID disponibilizado na web.

Logo o acesso de algum atacante com más intenções pode resultar em extração de informações muito importantes, inclusive a senha dos usuários em encriptação sha1. Oferecendo os dados necessários para um brute-force attack.

Remote Address Filter

O Remote Address Filter suporta os seguintes atributos de configuração [4]:

- **className**: Nome da classe para uso - org.apache.catalina.valves.RemoteAddrValve ;
- *allow*: Com uma lista de expressões regulares podemos relacionar os IP's que poderão ter acesso à aplicação;
- *deny*: Com uma lista de expressões regulares podemos relacionar os IP's que terão acesso negado à aplicação;

Exemplo:

```
<Valve className="org.apache.catalina.valves.RemoteAddrValve"
allow="200.20.1.50,127.0.0.1,200.20.1.205"/>
```

Problemas e Soluções

Conciliação

Problema

Um dos problemas recorrentes está na conciliação dos usuários no EID. Pois enquanto o usuário não passar pelo algoritmo de conciliação a aplicação não o considera apto para o EID2LDAP exportá-lo para a base LDAP. Dentre as buscas pela solução, a sugestão é realizar as seguintes consultas:

- Verificar se antes de executar a carga do EID2LDAP o conciliador já terminou de verificar os usuários. Para tanto o select abaixo executado na base eid deve resultar em zero:

```
select count(*) from TBL_EID_OBJECT WHERE pending=true
```

Se o EID não está sendo executado e o resultado do select acima não diminui, então temos algum problema no conciliador. Verifique o log de erros do catalina que pode fornecer informações sobre o problema.

Este problema é provavelmente no conciliador, que pode ter causas diversas.

Problema

Log de erro do Catalina.out crescendo muito jogando o seguinte erro:

```
740  ERROR [Eid Person Conciliator thread]
br.ufmg.lcc.eid.controller.EidServletContextListener     - Error processing
conciliation
```

```
br.ufmg.lcc.eid.commons.EidException: Error retrieving object:
org.hibernate.InstantiationException, Cannot instantiate abstract class or
interface: br.ufmg.lcc.eid.dto.EidClass

    at
br.ufmg.lcc.eid.commons.EidException.eidErrorHandling(EidException.java:46)

    at br.ufmg.lcc.eid.model.EidFacade.runConciliator(EidFacade.java:71)

    at
br.ufmg.lcc.eid.controller.EidServletContextListener$EidPersonConciliatorThre
ad.run(EidServletContextListener.java:113)

    at java.lang.Thread.run(Thread.java:679)

1134 ERROR [Eid Person Conciliator thread]
br.ufmg.lcc.arangi.model.Facade     - Error retrieving object:
org.hibernate.InstantiationException, Cannot instantiate abstract class or
interface: br.ufmg.lcc.eid.dto.EidClass
```

A solução encontrada foi a identificação que esse erro ocorre quando são removidos registros diretamente no banco ou quando ocorre alguma falha que provoca inconsistências no banco. Os passos para corrigi-lo são os seguintes:

1 - Abra uma conexão com o banco de dados "eid" utilizando algum cliente;

2 - Execute o seguinte SQL:

```
delete from TBL_EID_CLASS where id not in
(
select id from TBL_SVC_ALUNO
union
select id from TBL_SVC_CONTA
union
select id from TBL_SVC_CONTAUSUARIOUFF
union
select id from TBL_SVC_EMAIL
union
select id from TBL_SVC_ENDERECO
union
select id from TBL_SVC_PROFESSOR
union
select id from TBL_SVC_TECNICO
union
select id from TBL_SVC_TELEFONE
```

```
union
select id from TBL_SVC_GRUPO
union
select id from TBL_SVC_IDENTIFICACAO
);
delete from TBL_EID_OBJECT where guid not in (
select eidObject_guid from TBL_EID_CLASS);
```

Usuário com Duas Identificações

Problema

Pode acontecer de um usuário ter duas ou mais identificações na base institucional, por erro humano no cadastro no Sistema Acadêmico. O que pode ajudar a definir que o usuário tem duas identificações são os seguintes indícios:

- Mesmo nome (Mais forte);
- Pais com mesmo nome;
- Mesma data de nascimento;

O sistema do IdUFF tem uma funcionalidade aberta para central de atendimento e administradores que unifica duas identificações. Criada para corrigir exatamente esses casos.

Carga

Problema

Ao executar a carga, no log de erro da própria carga, aparece o erro:

```
12/07/2012 10:35:32 Erro na transformação do registro: Mapeamento para chave
estrangeira não encontrada na tabela de mapeamentos do sistema. FK antiga: 177639,
IU da Origem177639. Linha: 7901, coluna: eid_object_guid.
```

Quando uma das classes busca algum usuário que não se encontra em identificação e conta, ocorre este erro. Execute novamente a carga a partir de identificação e conta.

3.3.3 Instalação do EID2LDAP

Baixar Programa

O endereço para visualizar as versões disponíveis

```
http://sourceforge.net/projects/eid2ldap/files/
```

Criamos o diretório que ficará a aplicação

```
mkdir /opt/eid2ldap-{VERSÃO_EID2LDAP}/
```

Descompactação do arquivo baixado

```
unzip /root/softwares/{ARQUIVO_BAIXADO.WAR} -d /opt/eid2ldap-{VERSÃO_EID2LDAP}/
```

Configuração da Aplicação

Crie o arquivo /etc/tomcat6/Catalina/localhost/eid2ldap.xml que sera responsável pela configuração e deploy do EID. Lembrando de substituir a versão do EID2LDAP instalado, e as configurações da base de dados.

```
<?xml version="1.0" encoding="UTF-8"?>

<Context docBase="/opt/eid2ldap-{VERSÃO_EID2LDAP}/"
          privileged="true"
          antiResourceLocking="false"
          antiJARLocking="false"
          unpackWAR="false"
          swallowOutput="true"
          workDir="work/Catalina/localhost/eid2ldap">

  <Resource
    name="jdbc/eid2ldap"
    type="javax.sql.DataSource"
    driverClassName="com.mysql.jdbc.Driver"
    maxIdle="10"
    maxWait="5000"
    username="root"
    password="{SENHA_EID2LDAP}"
    url="jdbc:mysql://localhost:3306/eid2ldap"
    maxActive="50"
    factory="org.apache.tomcat.dbcp.dbcp.BasicDataSourceFactory"/>

  <WatchedResource>META-INF/context.xml</WatchedResource>

</Context>
```

Finalização

Atribua as respectivas permissões a pasta do EID2LDAP, reinicie o Tomcat.

```
chown -R tomcat6:tomcat6 /opt/eid2ldap-{VERSÃO_EID2LDAP}/
/etc/init.d/tomcat6 restart
```

3.3.4 Mapeamento de Selects do EID para Carga

Aluno

```
select
        al.ididentificador,
        idcao.ididentificacao,
        al.matricula,
        cur.nome as nomecurso,
        al.datadesvinculacao as dataafastamento,
        al.datamatricula as datavinculacao,
        stal.descricao as estadovinculo
        from aluno al
join pub_identificador idor on idor.ididentificador = al.ididentificador
join pub_identificacao idcao on idcao.ididentificacao =
idor.identificacao_ididentificacao
join curso cur on cur.idcurso = al.idcurso
join statusaluno stal on stal.idstatusaluno = al.idstatusaluno
left outer join pub_pais p on p.idpais = idcao.nacionalidade_idpais
left outer join pub_estado es on es.idestado = idcao.naturalidade_idestado
where idcao.cpf is not null
```

Conta

```
select
        idcao.IDUFFMAIL,
        idcao.ididentificacao,
        'sha' as algoritmosenha,
        idcao.IDUFF as login,
        trim(idcao.senhasha1) as senha_origem,
        'uff.br' as dominio
from pub_identificacao idcao
left outer join pub_pais p on p.idpais = idcao.nacionalidade_idpais
left outer join pub_estado es on es.idestado = idcao.naturalidade_idestado
where idcao.cpf is not null
```

Email

```
select
        idcao.ididentificacao,
        idcao.iduffmail || '@id.uff.br' as email,
        'uff.br' as servidor,
        'Principal' as tipo
from pub_identificacao idcao
left outer join pub_pais p on p.idpais = idcao.nacionalidade_idpais
left outer join pub_estado es on es.idestado = idcao.naturalidade_idestado
where idcao.cpf is not null
```

Endereço

```
select
        idcao.ididentificacao,
        idcao.enderecobairro as bairro,
        idcao.enderecocep as cep,
        cid.nome as cidade,
        idcao.enderecocomplemento as complemento,
        'Rio de Janeiro' as estado,
        idcao.endereconumero as numero,
        'Brasil' as pais,
        'Residencial' as tipo
from pub_identificacao idcao
left outer join pub_cidade cid on cid.idcidade = idcao.enderecocidade_idcidade
left outer join pub_pais p on p.idpais = idcao.nacionalidade_idpais
left outer join pub_estado es on es.idestado = idcao.naturalidade_idestado
where idcao.cpf is not null
```

Identificação

```
select
        idcao.ididentificacao,
        idcao.cpf,
        idcao.datanascimento,
        idcao.estadocivil,
        idcao.nome as nomeCompleto,
        idcao.nomemae,
        idcao.nomepai,
        idcao.sexo,
        idcao.identidadeorgao as orgaoemissoridentidade,
        es.nome as estadoNascimento,
        idcao.identidade as numeroidentidade,
        p.nome as paisnascimento,
```

```
        p.nome as nacionalidade,
        idcao.identidadeorgao as ufidentidade
from pub_identificacao idcao
left outer join pub_pais p on p.idpais = idcao.nacionalidade_idpais
left outer join pub_estado es on es.idestado = idcao.naturalidade_idestado
where idcao.cpf is not null
```

Professor

```
select
        idcao.ididentificacao,
        pr.classe as classe,
        pr.DATAALOCACAO as dataadmissao,
        pr.DATATERMINO as dataafastamento,
        pr.ATIVO as estadovinculo,
        pr.IDORGAO as lotacao,
        pr.nivel as nivel,
        fu.siape as siape,
        pr.DATAALOCACAO as dataingresso
from pub_funcionario fu
join professor pr on pr.idfuncionario = fu.ididentificador
join pub_identificador idor on idor.ididentificador = pr.ididentificador
join pub_identificacao idcao on idcao.ididentificacao =
idor.identificacao_ididentificacao
left outer join pub_pais p on p.idpais = idcao.nacionalidade_idpais
left outer join pub_estado es on es.idestado = idcao.naturalidade_idestado
where idcao.cpf is not null and pr.DATAALOCACAO is not null and pr.ATIVO = 1
```

Técnico

```
select
        idcao.ididentificacao,
        fu.siape,
        fu.DATAINICIO as dataAdmissao,
        fu.DATATERMINO as dataAfastamento,
        fu.ATIVO as estadoVinculo,
        fu.FUNCAOPRINCIPAL as funcaoPrincipal,
        fu.NIVELCAPACITACAO as nivelCapacitacao,
        fu.NIVELCLASSIFICACAO as padrao,
        fu.lotacao as lotacao,
        fu.classe as classe
from pub_funcionario fu
join pub_identificador idor on idor.ididentificador = fu.ididentificador
join pub_identificacao idcao on idcao.ididentificacao =
idor.identificacao_ididentificacao
left outer join pub_pais p on p.idpais = idcao.nacionalidade_idpais
```

```
left outer join pub_estado es on es.idestado = idcao.naturalidade_idestado
where idcao.cpf is not null
```

3.3.5 Instalação do Shibboleth

Instalação com Personalização voltada para o ambiente da UFF, mas esta foi baseada no roteiro oferecido pela RNP [13]. Não há quase nenhuma novidade na instalação e configuração do Shibboleth comparando com o roteiro.

Primeiro passo foi a instalação do Apache:

```
apt-get update

apt-get install apache2 libapache2-mod-jk
```

As configurações de firewall foram feitas de forma independente, mas considerando as necessidades da CAFe. Não teve responsabilidade deste trabalho pois teria que estar de acordo com os padrões e necessidades da própria instituição, criado então pelo próprio setor responsável pela segurança da informação na UFF.

Para configuração do Java editamos o arquivo */etc/java-6-openjdk/security/java.security* e adicionar as linhas 10 e 11 listadas abaixo:

```
security.provider.8=sun.security.smartcardio.SunPCSC

security.provider.9=sun.security.pkcs11.SunPKCS11 ${java.home}/lib/security/nss.cfg

…

security.provider.10=edu.internet2.middleware.shibboleth.DelegateToApplicationProvid
er

security.provider.11=org.bouncycastle.jce.provider.BouncyCastleProvider
```

Editar arquivo */etc/tomcat6/server.xml* para definir o redirecionamento para a porta 8443.

```
<Connector port="8009" protocol="AJP/1.3" redirectPort="8443" />
```

E foi adicionada as linhas a seguir:

```
<Connector port="8443”

           maxHttpHeaderSize="8192”

           maxSpareThreads="75”

           scheme="https”
```

```
            secure="true”
            clientAuth="want”
            SSLEnabled="true”
            sslProtocol="TLS”
            keystoreType="PKCS12”
            keystoreFile="/opt/shibboleth-idp/credentials/idp.p12”
            keystorePass="changeit”
            truststoreAlgorithm="DelegateToApplication” />
```

Criar o arquivo */etc/tomcat6/Catalina/localhost/idp.xml* contendo o caminho para auto-deploy do Shibboleth-IDP.

```
<Context docBase="/opt/shibboleth-idp/war/idp.war"
         privileged="true"
         antiResourceLocking="false"
         antiJARLocking="false"
         unpackWAR="false"
         swallowOutput="true" />
```

Criar o arquivo */etc/apache2/sites-available/idp-SSO* com o seguinte conteúdo:

```
<VirtualHost 200.20.0.28:443>
        ServerName cafe.sti.uff.br
        ServerSignature Off
        SSLEngine               on
        SSLCertificateKeyFile   /etc/ssl/private/chave-apache.key
        SSLCertificateFile      /etc/ssl/certs/certificado-apache.crt
        DocumentRoot /var/www/vazio/

        <Directory /var/www/vazio/>
                Options -Indexes -FollowSymLinks -MultiViews
                AllowOverride None
                Order deny,allow
                Deny from all
```

```
        </Directory>

    JkMount /idp/ ajp13_worker

        CustomLog /var/log/apache2/access-idp-443.log combined

        LogLevel warn

        ErrorLog /var/log/apache2/error-idp-443.log

</VirtualHost>
```

Criar o *arquivo /etc/apache2/conf.d/idp.conf* com o seguinte conteúdo:

```
JkWorkersFile   /etc/libapache2-mod-jk/workers.properties

JkShmFile       /var/run/apache2/jk-runtime-status

JkLogFile       /var/log/apache2/mod_jk.log

JkLogLevel      info
```

Comandos para finalizar a configuração do Apache:

```
mkdir /var/www/vazio/

a2dissite default

a2ensite idp-SSO

a2enmod ssl

a2enmod jk
```

Adicionar certificados de servidor à cadeia de certificados confiáveis do java, executando os seguintes comandos:

```
cd /etc/ssl/certs/

wget https://svn.rnp.br/repos/CAFe/softwares/certs/ds.chimarrao.cafe.rnp.br.crt
--no-check-certificate

wget https://svn.rnp.br/repos/CAFe/softwares/certs/ds.cafe.rnp.br.crt --no-check-
certificate

wget https://svn.rnp.br/repos/CAFe/softwares/certs/ACRaizdaICPEDU.crt --no-check-
certificate
```

```
wget https://svn.rnp.br/repos/CAFe/softwares/certs/ACUFSC.crt --no-check-certificate

wget https://svn.rnp.br/repos/CAFe/softwares/certs/AC_SSL_UFSC.crt --no-check-
certificate

keytool -importcert -keystore /etc/ssl/certs/java/cacerts \

        -alias ds.chimarrao.cafe.rnp.br -file
/etc/ssl/certs/ds.chimarrao.cafe.rnp.br.crt \

        -storetype JKS -storepass changeit -noprompt

keytool -importcert -keystore /etc/ssl/certs/java/cacerts \

        -alias ds.cafe.rnp.br -file /etc/ssl/certs/ds.cafe.rnp.br.crt \

    -storetype JKS -storepass changeit -noprompt

keytool -importcert -keystore /etc/ssl/certs/java/cacerts \

        -alias ACRaizdaICPEDU -file ACRaizdaICPEDU.crt \

        -storetype JKS -storepass changeit -noprompt

keytool -importcert -keystore /etc/ssl/certs/java/cacerts \

        -alias ACUFSC -file ACUFSC.crt \

        -storetype JKS -storepass changeit -noprompt

keytool -importcert -keystore /etc/ssl/certs/java/cacerts \

        -alias AC_SSL_UFSC -file AC_SSL_UFSC.crt \

        -storetype JKS -storepass changeit -noprompt
```

Instalar o Shibboleth-IDP e bibliotecas Java

A versão instalada do Shibboleth foi a 2.1.5. Executando os seguintes comandos para instalação:

```
cd /root/

wget https://svn.rnp.br/repos/CAFe/softwares/shibboleth-identityprovider-2.1.5-
bin.zip --no-check-certificate

wget https://svn.rnp.br/repos/CAFe/softwares/bcprov-jdk16-144.jar --no-check-
certificate

cp bcprov-jdk16-144.jar /usr/lib/jvm/java-6-openjdk/jre/lib/

unzip shibboleth-identityprovider-2.1.5-bin.zip

cd shibboleth-identityprovider-2.1.5/

cp -r endorsed /usr/share/tomcat6/

cp lib/shibboleth-jce-1.1.0.jar /usr/lib/jvm/java-6-openjdk/jre/lib/ext/
```

```
cat > src/installer/resources/install.properties -<<EOF

idp.home=/opt/shibboleth-idp

idp.home.input=/opt/shibboleth-idp

idp.hostname=`hostname -f`

idp.hostname.input=`hostname -f`

idp.keystore.pass=changeit

EOF

./install.sh

chown tomcat6:tomcat6 /opt/shibboleth-idp/logs/

chown tomcat6:tomcat6 /opt/shibboleth-idp/metadata/
```

Configuração do Shibboleth-IDP

Editar o arquivo */opt/shibboleth-idp/conf/handler.xml*, comentar a seção referente a *RemoteUser* e habilitar a seção do *UsernamePassword*. Arquivo anexado.

Editar /*opt/shibboleth-idp/conf/relying-party.xml* para substituir o bloco correspondente à tag *MetadataProvider id="URLMD"* pelo bloco abaixo:

```
<MetadataProvider id="URLMD" xsi:type="FileBackedHTTPMetadataProvider"
xmlns="urn:mace:shibboleth:2.0:metadata"


metadataURL="https://ds.chimarrao.cafe.rnp.br/metadata/chimarrao-metadata.xml"

                          backingFile="/opt/shibboleth-idp/metadata/chimarrao-
metadata.xml">

            <MetadataFilter xsi:type="ChainingFilter"
xmlns="urn:mace:shibboleth:2.0:metadata">

<!--

                <MetadataFilter xsi:type="RequiredValidUntil"
xmlns="urn:mace:shibboleth:2.0:metadata"

                                maxValidityInterval="604800" />

                <MetadataFilter xsi:type="SignatureValidation"
xmlns="urn:mace:shibboleth:2.0:metadata"

                                trustEngineRef="shibboleth.MetadataTrustEngine"

                                requireSignedMetadata="true" />

-->
```

```
                    <MetadataFilter xsi:type="EntityRoleWhiteList"
xmlns="urn:mace:shibboleth:2.0:metadata">
                    <RetainedRole>samlmd:SPSSODescriptor</RetainedRole>
                </MetadataFilter>
            </MetadataFilter>
        </MetadataProvider>
```

Configuração de resolução/liberação de atributos

Arquivos anexados com máscara na senha.

- */opt/shibboleth-idp/conf/attribute-resolver.xml*
- */opt/shibboleth-idp/conf/attribute-filter.xml*

Configuração da autenticação LDAP

- */opt/shibboleth-idp/conf/login.config*

Chaves e Certificados SSL

Feita edição do arquivo *openssl.cnf.*

```
[ req ]
default_bits = 2048 # Size of keys
string_mask = nombstr # permitted characters
distinguished_name = req_distinguished_name

[ req_distinguished_name ]
# Variable name   Prompt string
#----------------------   ----------------------------------
0.organizationName = UFF - Universidade Federal Fluminense
organizationalUnitName = STI - Superintendência de Tecnologia e Informação
emailAddress = atendimento@id.uff.br
emailAddress_max = 40
localityName = Centro
stateOrProvinceName = RJ
```

```
countryName = BR

countryName_min = 2

countryName_max = 2

commonName = cafe.sti.uff.br

commonName_max = 64


# Default values for the above, for consistency and less typing.

# Variable name   Value

#------------------------------   ------------------------------

#0.organizationName_default =

organizationalUnitName_default = STI

#localityName_default = Niterói

#stateOrProvinceName_default = Rio de Janeiro

countryName_default = BR

commonName_default = cafe.sti.uff.br
```

Apache

```
openssl genrsa 2048 -config openssl.cnf > /etc/ssl/private/chave-apache.key

openssl req -new -x509 -nodes -days 1095 -sha1 -key /etc/ssl/private/chave-
apache.key -set_serial 00 \

        -config /tmp/openssl.cnf > /etc/ssl/certs/certificado-apache.crt

chown root:ssl-cert /etc/ssl/private/chave-apache.key /etc/ssl/certs/certificado-
apache.crt

chmod 640 /etc/ssl/private/chave-apache.key
```

Shibboleth IDP

No quarto comando, informe os seguintes dados:

- Confirme o código do País (BR)
- Unidade da federação (Rio de Janeiro)
- Cidade (Rio de Janeiro)
- Instituição (UFF - Universidade Federal Fluminense)

- Departamento da instituição (STI - Superintendência de Tecnologia e Informação)
- Confirme que o Hostname está correto (cafe.sti.uff.br)

No quinto comando, informe a senha "changeit". A senha está cadastrada no arquivo */etc/tomcat6/server.xml* e o tomcat6 precisará dela para abrir o keystore que está sendo gerado.

```
cd /opt/shibboleth-idp/credentials/

rm -f idp

openssl genrsa 2048 -config /tmp/openssl.cnf > idp.key

openssl req -new -x509 -nodes -days 1095 -sha1 -key idp.key -set_serial 00
-config /tmp/openssl.cnf > idp.crt

openssl pkcs12 -export -in idp.crt -inkey idp.key -out idp.p12 -name idp -caname
selfsigned
```

Copie o conteúdo entre as linhas BEGIN CERTIFICATE e END CERTIFICATE:

```
cat /opt/shibboleth-idp/credentials/idp.crt
```

Edite o arquivo de metadados */opt/shibboleth-idp/metadata/idp-metadata.xml* e exclua o certificado incorreto. Há 2 ocorrências desse certificado no arquivo, as duas dentro das seguintes tags xml:

```
        <KeyDescriptor>

            <ds:KeyInfo>

                <ds:X509Data>

                    <ds:X509Certificate>

INSIRA_AQUI_O_CONTEUDO_DO_ARQUIVO_DO_CERTIFICADO

INSIRA_AQUI_O_CONTEUDO_DO_ARQUIVO_DO_CERTIFICADO

INSIRA_AQUI_O_CONTEUDO_DO_ARQUIVO_DO_CERTIFICADO

                    </ds:X509Certificate>

                </ds:X509Data>

            </ds:KeyInfo>

        </KeyDescriptor>
```

Ainda no arquivo de metadados (*/opt/shibboleth-idp/metadata/idp-metadata.xml*), inclua a identificação da Instituição e contato técnico entre as tags *</AttributeAuthorityDescriptor>* e *</EntityDescriptor>* conforme o exemplo abaixo. Lembre-se de fazer as devidas adaptações.

```
</AttributeAuthorityDescriptor>


    <Organization>
      <OrganizationName xml:lang="en">UFF - Universidade Federal
Fluminense</OrganizationName>
      <OrganizationDisplayName xml:lang="en">UFF - Universidade Federal
Fluminense</OrganizationDisplayName>
      <OrganizationURL xml:lang="en">http://www.uff.br/</OrganizationURL>
    </Organization>


    <ContactPerson contactType="technical">
       <SurName>Uenes Vilaça</SurName>
       <EmailAddress>uenesvilaca@id.uff.br</EmailAddress>
    </ContactPerson>


</EntityDescriptor>
```

Finalização Iniciando os Serviços

```
/etc/init.d/apache2 restart

/etc/init.d/tomcat6 restart
```

3.4 Resumo

A descrição da parte prática do trabalho foi feita neste capítulo, também os problemas mais relevantes enfrentados e as soluções praticadas. Os comandos utilizados para instalação e configuração do ambiente de infraestrutura estão todos descritos. Assim também os detalhes de configuração dos equipamentos e recursos disponíveis para implantação da estrutura da federação.

4. UTILIDADE

"Sempre necessitamos ambicionar alguma coisa que, alcançada, não nos faz desambiciosos."

Carlos Drummond de Andrade

Para expor alguns dos resultados deste trabalho serão expostos os serviços que estão disponíveis para uso dos usuários da UFF. Com descrição do serviço e sua importância para comunidade. Mostrando a relevância prática já usufruída por este trabalho na instituição. Com *screenshot* de acesso para serviços chave pela importância dada pelos usuários.

4.1 Periódicos da CAPES

O Portal de Periódicos da Capes é uma das maiores bibliotecas virtuais do mundo. Criado em novembro do ano de 2000 agrupando materiais científicos. Estudantes de graduação, pós-graduação e professores podem fazer pesquisas dentro do portal para buscar antigos, revistas para contribuir com seus trabalhos e agregar conhecimento.

4.1.1 Acesso via CAFe

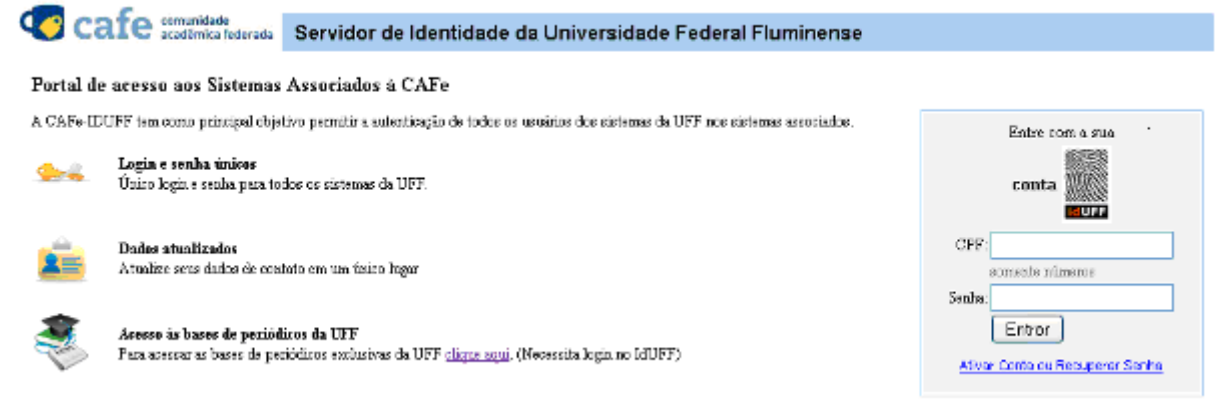
O primeiro requisito para poder acessar os recursos oferecidos pelo vínculo com a

federação é ativar o acesso com o IdUFF ou saber suas credenciais com a instituição. Tendo este requisito satisfeito, basta acessar o Portal de Periódicos da Capes e selecionar meu espaço:

Após este passo, poderá optar pela autenticação via CAFe ao invés da forma antiga de se autenticar.

O próximo passo está relacionado com o *Where Are You From*, ou seja, o serviço deseja saber qual a instituição de origem do usuário para poder encaminhá-lo para o IdP.

Nesta próxima tela o usuário estará na página do Identity Provider da instituição de origem, no caso da UFF. Então, este deverá apresentar suas credenciais do IdUFF para autenticação.



Então, conferindo o login e senha da instituição, o usuário será devolvido para o Portal de Periódicos da Capes autenticado. No primeiro acesso do usuário será pedido o acesso antigo para poder vincular as contas.

4.2 DreamSpark

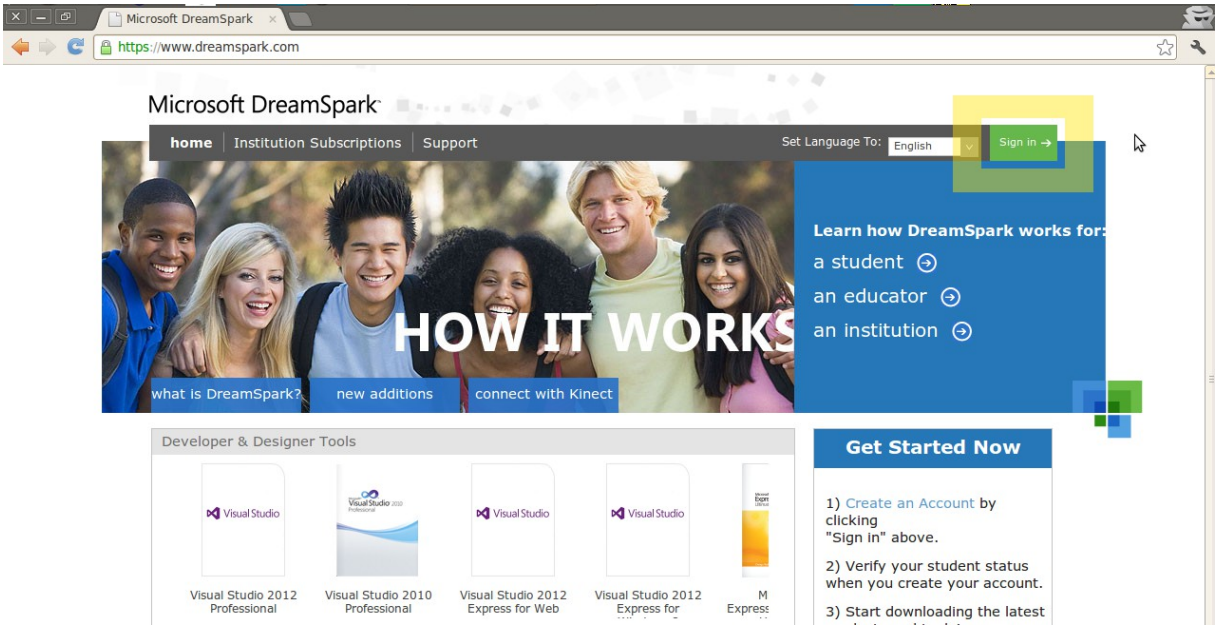
A gigante empresa Microsoft oferece para a comunidade acadêmica vinculada com a

mesma ferramentas profissionais de desenvolvimento e design sem custo. Estimulando estrategicamente o uso de sua tecnologia dentro da comunidade para fortificar sua marca e a dependência de sua plataforma. Este benefício, que antes era realizado autenticando na própria página do DreamSpark, hoje pode ser feito via federação CAFe.

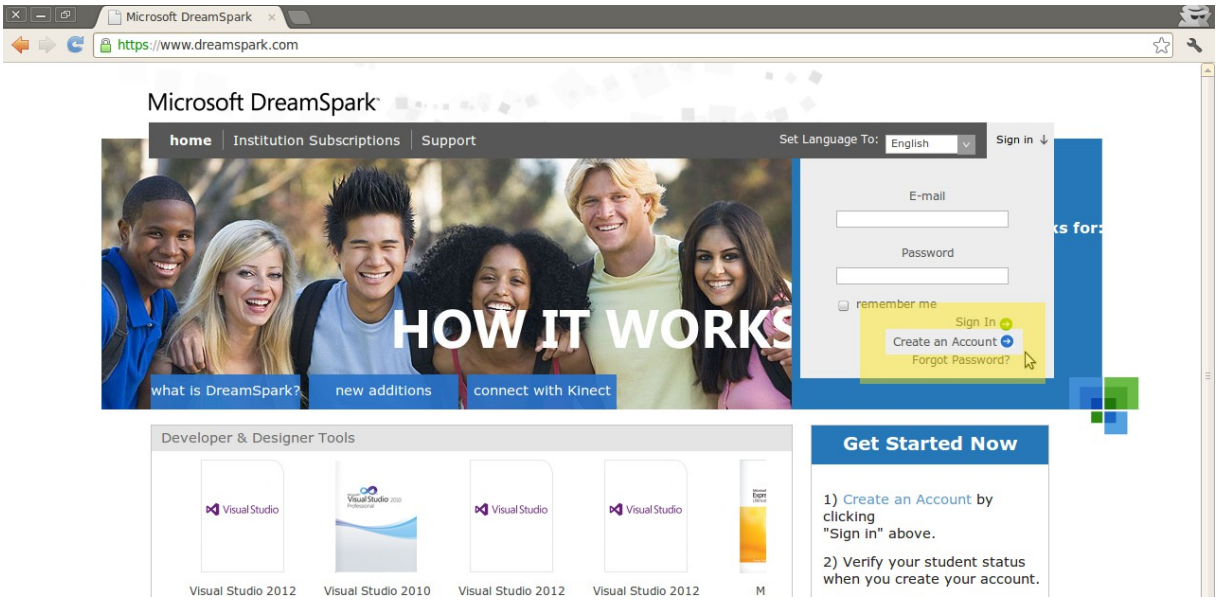
A DreamSpark não abraçou completamente o uso da federação, exigindo que o usuário se autentique com a instituição de origem anualmente para revalidação do vínculo com a instituição. No primeiro momento em que faz o primeiro acesso, contabilizando um ano então, será exigido uma nova autenticação pela federação para verificar o vínculo com a instituição. Visto que somente tem direito a realizar o download dos aplicativos gratuitamente os estudantes que estiverem com víncilo ativo com a instituição. Antes o usuário tinha um status não atualizado dando benefícios quase que vitalícios pois não realizava a atualização dos dados do usuário.

4.2.1 Verificação do Vínculo via CAFe

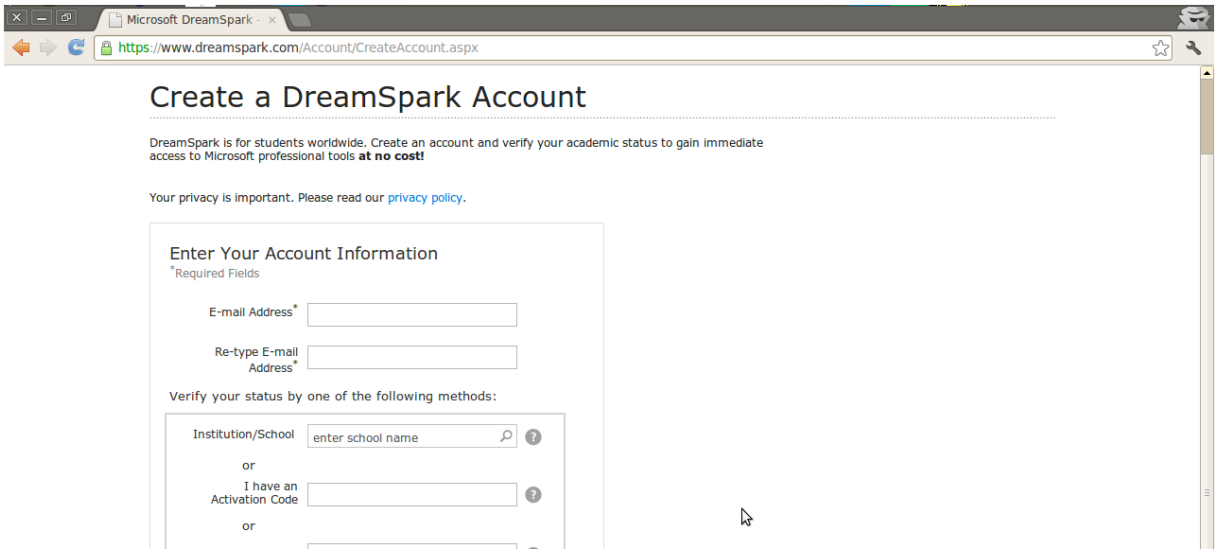
Acesso ao site https://www.dreamspark.com/. Selecione em *Sign In*.



Selecione em *Create an Account* (Crie uma conta). Os usuários com o cadastro expirado no antigo site do Dreamspark poderão fazer este mesmo passo.



Preencha os campos, em *Institution/School* digite UFF e selecione a primeira opção da Universidade Federal Fluminense.

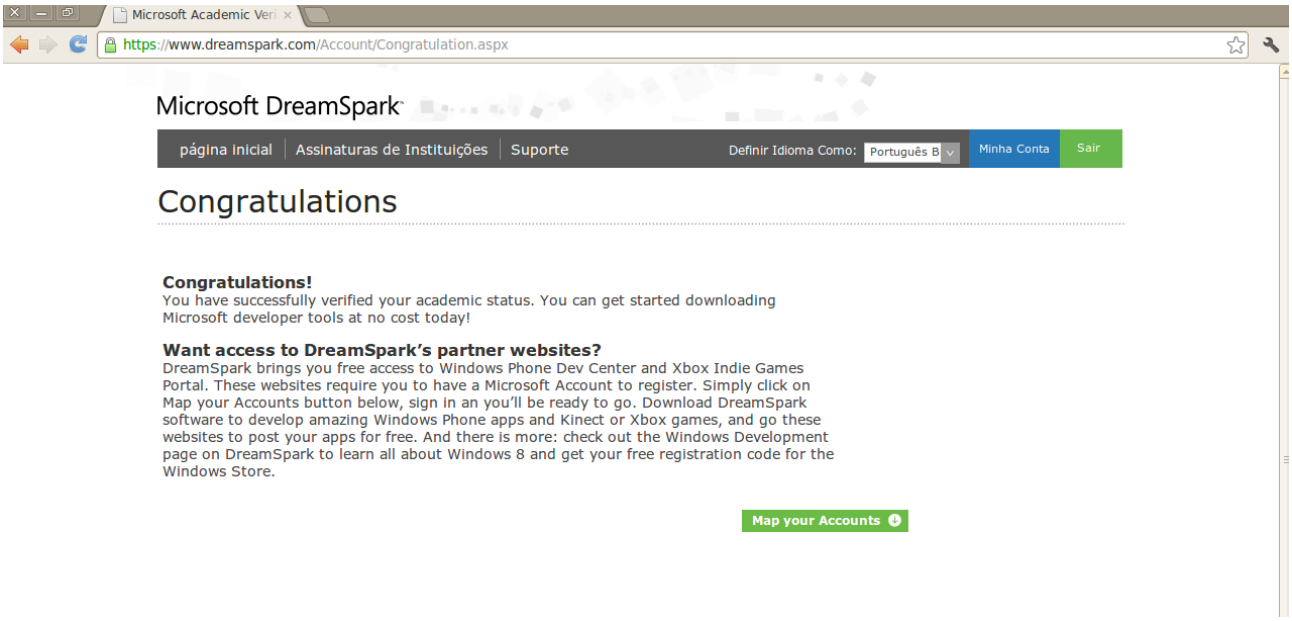


Neste momento o usuário será direcionado para a CAFe. Podendo pedir para aceitar o Certificado auto assinado da UFF.

Insira o login (CPF) e senha do IdUFF.

Caso o país de origem esteja incorreto, altere para *Brazil*. Dentre as opções para verificar a conta selecione 'Obter verificação através da minha escola' e digite UFF. Então o sistema autenticará na CAFe.

Conseguindo a autenticação o site da Dreamspark informará o êxito na verificação. Neste momento o usuário já estará autenticado no Dreamspark.



4.3 Resumo

Este capítulo explicita o uso da federação para autenticar alguns dos principais serviços hoje disponíveis para os usuários. Demonstra já o usufruto dos ganhos obtidos para a autenticação de serviços. Para a maior parte dos usuários, os alunos, o DreamSpark é um grande atrativo. Pois poder adquirir vários sistemas gratuitamente da Microsoft, esta gigante empresa extremamente relevante na área de softwares nos dias de hoje. O outro serviço

também é muito requisitado e utilizado, os periódicos da Capes. Este serviço agrupa vários trabalhos, revistas e artigos que são muito importantes para pesquisa e referência na criação de produções acadêmicas.

5. CONCLUSÃO

"A privação é uma parte integral e universal da nossa experiência no amor."
C. S. Lewis

Este trabalho possibilitou a UFF ser a primeira instituição de ensino do Rio de Janeiro a aderir a federação CAFe. O que é mais um marco que nos destaca a frente de outras instituições que são referência também em termos de tecnologia. Estamos sendo referência para outras universidades passando experiência com o processo e avaliando as decisões tomadas. Isto colaborará para que outras instituições tenham cada vez menos impacto com o processo de adesão e permita ter cada vez mais conforto na transição. Talvez até estas organizações poderão trilhar por caminhos diferentes visto que conhecem alguns dos resultados destas nossas decisões.

Podemos vislumbrar a estrutura organizacional da instituição, com organogramas estruturais, importados para dentro do LDAP fazendo uso da estrutura de grupos. Deste modo teremos uma imediata resposta a alterações de carga de usuários e até permissões revogadas quando ocorre o desvínculo do funcionário ou administrador. Hoje a perda dos privilégios de um funcionário dentro do sistema requer um processo manual e humano. O que torna lento e propenso a falhas por causa do próprio fator humano. Tornando a estrutura criada com o LDAP com mais responsabilidades por conter mais informações estruturais, fará com que os sistemas que vincularem a autorização a recursos tenham um ganho muito grande. Pois o desvínculo acarretará nas perdas imediatas dos privilégios que o cargo proporcionava. Esta demanda gera oportunidades de trabalhos futuros. Portanto, existe o ganho de uma estrutura mais eficiente mapeando a estrutura hierárquica da UFF para dentro da estrutura do LDAP.

Podemos esperar em longo prazo uma convergência de serviços internos da UFF aderindo a solução da CAFe como forma única de autenticação. Isto tornará mais forte a solução pois demandará cada vez mais investimento em estabilidade e segurança. Contribuirá com todos os benefícios já descritos no trabalho para a organização, serviços e vinculados. A UFF contém muitos serviços internos e um portal próprio. Muitos sistemas já aderem e trabalham com SSO baseado na autenticação com o portal. Mas aderindo a solução e padronização do IdP da federação diminuirá pela metade os pontos de prováveis falhas, pontos para manutenção.

Em um curto prazo temos a tendência de integrar mais a cada dia a base LDAP consolidada como ponto de encontro para outras autenticações, como sistemas operacionais no ambiente de trabalho da STI, já temos laboratório em que a máquina autentica via pam/LDAP no sistema Linux, o projeto eduroam também faz uso desta base.

Existe um conjunto de sistemas que implementam um protocolo de rede para autenticação segura chamado Kerberos. As funções do Kerberos abrangem as funções do Shibboleth e oferece outras funcionalidades. Portanto, pode tornar-se mais interessante para a instituição a migração do uso do Shibboleth para o Kerberos, pela integração de várias outras soluções que são um grande atrativo. Isto é, o Kerberos é uma ferramenta mais estrutural pois além de fazer o papel da autenticação, compatível com o Shibboleth, cria uma interface para que outras aplicações se autentiquem por ele. Esta nova camada blindará o LDAP de ser acessado diretamente. Por ter alta aceitação, muitas aplicações podem ser configuradas para apontar para o Kerberos. No ambiente intra-organizacional pode ser bastante interessante autenticar webmail, SSH, Samba, dentre outras aplicações, via Kerberos. Em nível de aplicação, gera um *token* para o ganho de SSO e comunica-se com o LDAP de forma segura. Além de ajudar no gerenciamento de usuários, grupos, *hosts* e outros aspectos de segurança da rede. Estruturalmente é interessante inclusive para autorização. A desvantagem desta substituição é a perda do suporte da RNP. Neste caso, o apoio da RNP para solução de problemas de autenticação limita-se visto que o Kerberos não é a solução sugerida para a infraestrutura. Contudo existem outras possibilidades de solução, como manter o Shibboleth e passar a autenticá-lo no Kerberos, ou utilizar o RADIOS do eduroam para este fim de autenticação de aplicações e nova camada de segurança para o LDAP.

Existem outras possibilidades de evolução de trabalhos nesta área, como a liberação de atributos dos usuários. Neste modelo, a negociação sobre quais atributos serão cedidos para o provedor de serviço é de responsabilidade do provedor de identidade. Mas faria sentido que fosse em nível de usuário, ou pelo menos o usuário soubesse quais atributos são cedidos para cada provedor de serviço para aceitar usar ou não. Este assunto lida com a privacidade do usuário, tema em grande destaque nos dias atuais.

A implantação tem pontos para amadurecer e novas perspectivas e desafios. Como as aplicações de apoio para cargas que atualizam o LDAP poderiam ser muito otimizadas se houvesse o abandono da carga periódica da base institucional para o LDAP, integrando-o nas persistências que alterem e insiram novos dados. Ou seja, a atualização de uma dado ou criação de um novo usuário fosse refletido na base institucional original e também no LDAP.

O que reduziria o *gap* de tempo necessário para propagar uma alteração para o LDAP, reduzindo as chamadas para a central de atendimento e aumentando a satisfação do usuário. Esta solução é uma sugestão de trabalho futuro para aperfeiçoar este processo. Pode ser feito pela execução de triggers dentro do banco de dados para o LDAP, evitando assim pontos de falhas nas aplicações e mapeamentos ineficientes sobre os pontos de atualização dos atributos.

Bibliografia

[1] E. Bertino, e K. Takahashi. Identity Management – Concepts, technologies, and Systems. Artech House, 1ª Edição, 2011.

[2] Messaoud Benantar. Control System – Security, Identity Management and Trust Models. Springer , 1ª Edição, 2006.

[3] T. A. Howes, M. C. Smith, G. S. Good, Understand and Deploying LDAP Directory Services, First Edition, 1998.

[4] http://tomcat.apache.org/tomcat-6.0-doc/config/valve.html, The Apache Software Foundation, Version 6.0.36, Oct 16 2012.

[5] Eduroam Compliance Statement v1.0, eduroam Documentation, https://www.eduroam.org/index.php?p=docs, 2011.

[6] http://www.midiacom.uff.br/eduroam-br/, Projeto Eduroam-Br, 2013.

[7] M. Milinović, Srce / CARNet, Stefan Winter, RESTENA and members of the SA3 T2 group, Eduroam Police Service Definition, Version 2.8, 2012.

[8] http://portal.rnp.br/web/servicos/cafe, Rede Nacional de Ensiono e Pesquisa, 2013.

[9] Termo de Referência da Federação CAFe, versão 1.0, Rede Nacional de Ensino e Pesquisa, 2012.

[10] D. Florencio e C. Herley . A Large-Scale Study of Web Password Habits - Microsoft Research , One Microsoft Way , 2007

[11] http://docs.oracle.com/javase/jndi/tutorial/ldap/models/x500.html, Oracle, 03/2013.

[12] S. Shim, G. Bhalla, V. Pendyala, "Federated identity management," *IEEE Computer* , vol.38, no.12, pp.120-122, Dez. 2005.

[13] A. G. Robertson, R. Q. Ribeiro, http://wiki.rnp.br/display/cafewebsite/Roteiro+de+Atividades+para+Entrada+de+um+IDP, 21/03/2011.

[14] G. Carter, LDAP System Administrator, O'Really, 2003.

[15] Pfitzmann, A., and M. Hansen, "A Terminology for Talking About Privacy by Data Minimization: Anonymity, Unlinkability, Undetectability,

Unobservability, Pseudonymity, and Identity Management," 2009.

[16] NGN Identity Management Framework, ITU-T Recommendation, Y.2720.

[17] D. Florêncio e C. Henley, A Large-Scale Study of Web Password Ha bits, Microsoft Research, One Microsoft Way, 2007.

[18] J. Kemp, S. Cantor, P. Mishra, R. Philpott, E. Maler, Authentication Context for the OASIS Security Assertion markup Language (SAML) V2.0, OASIS Standard, 2005.

[19] http://shibboleth.net/about/index.html, 19/03/2013.

[20] Esquema brEduPerson, versão 1.0, Outubro de 2009.

Anexo A

```
#--------------------------------------------------------------------
#
# Definicao do esquema brEduPerson
# Versao: 20080917-0.0.6
# Data: Setembro, 2008
# Baseado no documento: "Proposta de Esquema brEduPerson - Federacao Cafe - agosto
de 2008"
# (brEduPerson-20080714.0.0.4-3.pdf)
#
# A ultima versao deste documento esta disponivel no site
# http://www.rnp-eaa.ufc.br/?/brEduPerson-20080917-0.0.6.schema.txt
#
#--------------------------------------------------------------------
#
# Changelog
#
# 20080917 - 0.0.6
#          - Alteracao do atributo brEduAffiliation
# 20080911 - 0.0.5
#          - Inclusao do atributo brEduVoIPphone
#          - Alteracao da classe brEduVoIP para incluir o atributo brEduVoIPphone
# 20080714 - 0.0.4
#          - Exclusao do atributo brEduPersonUniqueId
#          - Exclusao do atributo brRelatedIdentification
#          - Criacao do atributo brEduAffiliation
#          - Exclusao da classe brEduPersonAffiliation
#          - Exclusao da classe brEduRelatedInfo
#          - Alteracao da classe brEduPerson
# 20080401 - Versao inicial
#
#--------------------------------------------------------------------

#--------------------------------------------------------------------
# Atributos
#--------------------------------------------------------------------

# brPersonCPF
# Descrip: Documento que identifica contribuinte pessoa fisica perante a Secret. da
Receita Federal do Brasil.
# Format: Free string.
# Example: brcpf: 757065432-33
attributetype ( 1.3.6.1.4.1.15996.100.1.1.1.1
```

```
    NAME ( 'brPersonCPF' 'brcpf')
    DESC 'Cadastro Pessoa Fisica'
    EQUALITY caseIgnoreMatch
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
    SINGLE-VALUE )

# brPersonPassport
# Descrip: Documento emitido por um governo nacional.
# O valor desse atributo é complementado pela informação no atributo ``país de
cidadania''.
# Format: Free string.
# Example: brpassport: 1234456ZF
attributetype ( 1.3.6.1.4.1.15996.100.1.1.1.2
    NAME ( 'brPersonPassport' 'brpassport')
    DESC 'Numero do passaporte'
    EQUALITY caseIgnoreMatch
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
    SINGLE-VALUE )

# brEduAffiliationType
# Descrip: Tipo de vinculo que a pessoa possui com a instituicao.
# Format: Free string.
# Common values: faculty, student, staff, position, scholarshipawardee, other
# Example: brafftype: student
attributetype ( 1.3.6.1.4.1.15996.100.1.1.2.1
    NAME ( 'brEduAffiliationType' 'brafftype')
    DESC 'Tipo de vinculo com a instituicao'
    EQUALITY caseIgnoreMatch
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
    SINGLE-VALUE )

# brEntranceDate
# Descrip: Data de inicio do vinculo da pessoa com a instituicao
# Format: Numeric value YYYYMMDD, using 4 digits for year, 2 digits
#          for month and 2 digits for day as described in RFC 3339.
# Example: brentr: 19660412
attributetype ( 1.3.6.1.4.1.15996.100.1.1.2.2
    NAME ( 'brEntranceDate' 'brentr')
    DESC 'Data de inicio do vinculo com a instituicao'
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.36
    SINGLE-VALUE )

# brExitDate
# Descrip: Data de fim do vinculo da pessoa com a instituicao.
# Format: Numeric value YYYYMMDD, using 4 digits for year, 2 digits
```

```
#          for month and 2 digits for day as described in RFC 3339.
# Example: brexit: 20000512
attributetype ( 1.3.6.1.4.1.15996.100.1.1.2.3
    NAME ( 'brExitDate' 'brexit')
    DESC 'Data de fim do vinculo com a instituicao'
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.36
    SINGLE-VALUE )

# brEduAffiliation
# Descrip: Identificador unico de um vinculo com a instituicao.
# Format: Integer.
# Example: braff: 3
attributetype ( 1.3.6.1.4.1.15996.100.1.1.2.4
    NAME ( 'brEduAffiliation' 'braff')
    DESC 'Identificador unico de um vinculo com a instituicao'
    EQUALITY IntegerMatch
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.27
    SINGLE-VALUE )

# brCaptureDate
# Descrip: Representa a data de captura do dado biometrico da pessoa.
# Format: Numeric value YYYYMMDD, using 4 digits for year, 2 digits
#          for month and 2 digits for day as described in RFC 3339.
# Example: brcapt: 20060509
attributetype ( 1.3.6.1.4.1.15996.100.1.1.3.1
    NAME ( 'brCaptureDate' 'brcapt')
    DESC 'Data de captura do dado biometrico da pessoa'
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.36
    SINGLE-VALUE )

# brBiometricSource
# Descrip: Representa uma fonte biometrica da pessoa.
# Format: Free string.
# Common values: left-thumb, left-index, left-middle, left-ring, left-little,
# right-thumb, right-index, right-middle, right-ring, right-little.
# Example: brbiosrc: left-middle
attributetype ( 1.3.6.1.4.1.15996.100.1.1.3.2
    NAME ( 'brBiometricSource' 'brbiosrc')
    DESC 'Fonte biometrica da pessoa'
    EQUALITY caseIgnoreMatch
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
    SINGLE-VALUE )

# brBiometricData
# Descrip: Representa o dado capturado de uma fonte biometrica da pessoa.
```

```
# Format: Binary.
# Example: brbiodata: ?
attributetype ( 1.3.6.1.4.1.15996.100.1.1.3.3
    NAME ( 'brBiometricData' 'brbiodata')
    DESC 'Dado capturado de uma fonte biometrica da pessoa'
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.5 )

# brEduVoIPalias
# Descrip: Numero do telefone IP.
# Format: Numeric string.
# Example: brvoipalias: 5780
attributetype ( 1.3.6.1.4.1.15996.100.1.1.4.1
    NAME ( 'brEduVoIPalias' 'brvoipalias')
    DESC 'Numero do telefone IP'
    EQUALITY numericStringMatch
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.36
    SINGLE-VALUE )

# brEduVoIPtype
# Descrip: Categoria do usuario para tratamento diferenciado.
# Format: Free string.
# Common values: pstn, celular, ?
# Example: brvoiptype: pstn
attributetype ( 1.3.6.1.4.1.15996.100.1.1.4.2
    NAME ( 'brEduVoIPtype' 'brvoiptype')
    DESC 'Tipo do telefone IP'
    EQUALITY caseIgnoreMatch
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
    SINGLE-VALUE )

# brEduVoIPadmin
# Descrip: DN do responsavel pela criacao do telefone do usuario.
# Format: Distinguished Name.
# Example: brvoipadmin:
attributetype ( 1.3.6.1.4.1.15996.100.1.1.4.3
    NAME ( 'brEduVoIPadmin' 'brvoipadmin')
    DESC 'Administrador responsavel por telefone VoIP'
    EQUALITY distinguishedNameMatch
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.12 )

# brEduVoIPcallForward
# Descrip: Telefone comum para redirecao de chamada caso o usuario nao esteja
online.
# Format: International form of telephone numbers.
# Example: brvoipfwr: +55 21 3456 3456
```

```
attributetype ( 1.3.6.1.4.1.15996.100.1.1.4.4
    NAME ( 'brEduVoIPcallforward' 'brvoipfwr')
    DESC 'Numero do telefone comum para redirecao de chamada'
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.50 )

# brEduVoIPaddress
# Descrip: Registra um endereço IP autorizado para telefone VoIP.
# Format:
# Example: brvoipaddr: 200.1.345.234
attributetype ( 1.3.6.1.4.1.15996.100.1.1.4.5
    NAME ( 'brEduVoIPaddress' 'brvoipaddr')
    DESC 'Endereco IP do telefone'
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.26{128} )

# brEduVoIPexpiryDate
# Descrip: Ao atribuir um telefone IP, o administrador pode determinar uma data de
expiracao para a atribuicao.
# A existencia desse campo com data anterior a data atual identifica uma conta
obsoleta.
# Caso o campo nao exista ou contenha data posterior a atual, supoe-se que a conta
esteja ativa.
# Format: Numeric value YYYYMMDD, using 4 digits for year, 2 digits
#          for month and 2 digits for day as described in RFC 3339.
# Example: brvoipexpiry: 20060509
attributetype ( 1.3.6.1.4.1.15996.100.1.1.4.6
    NAME ( 'brEduVoIPexpiryDate' 'brvoipexpiry')
    DESC 'Data de expiracao do telefone IP'
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.36
    SINGLE-VALUE )

# brEduVoIPbalance
# Descrip: Creditos restantes em um telefone IP (em segundos).
# Format: Integer.
# Example: brvoipbalance: 250000
attributetype ( 1.3.6.1.4.1.15996.100.1.1.4.7
    NAME ( 'brEduVoIPbalance' 'brvoipbalance')
    DESC 'Creditos restantes em um telefone IP (em segundos)'
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.27
    SINGLE-VALUE )

# brEduVoIPcredit
# Descrip: Total de creditos aos quais o usuario tera direito (em segundos).
# Format: Integer.
# Example: brvoipcredit: 360000
attributetype ( 1.3.6.1.4.1.15996.100.1.1.4.8
```

```
    NAME ( 'brEduVoIPcredit' 'brvoipcredit')
    DESC 'Total de creditos do usuario (em segundos)'
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.27
    SINGLE-VALUE )

# brEduVoIPphone
# Descrip: Identificador unico de um telefone do usuario.
# Format: Integer.
# Example: brvoipphone: 4
attributetype ( 1.3.6.1.4.1.15996.100.1.1.4.9
    NAME ( 'brEduVoIPPhone' 'brvoipphone')
    DESC 'Identificador unico de telefone'
    EQUALITY IntegerMatch
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.27
    SINGLE-VALUE )

#-----------------------------------------------------------------------
# ObjectClasses
#-----------------------------------------------------------------------

# brPerson
objectclass ( 1.3.6.1.4.1.15996.100.1.2.1
    NAME 'brPerson'
    DESC 'Atributos sobre pessoas nascidas ou residentes no Brasil, nao se
restringe somente ao ambito educacional'
    SUP 'top'
    AUXILIARY
    MAY ( brcpf $ brpassport ) )

# brEduPerson
objectclass ( 1.3.6.1.4.1.15996.100.1.2.2
    NAME 'brEduPerson'
    DESC 'Atributos referentes a uma pessoa com insercao em instituicao brasileira
de ensino ou pesquisa'
    SUP 'top'
    STRUCTURAL
    MUST ( braff $ brafftype)
    MAY ( brentr $ brexit ) )

# brBiometricData
objectclass ( 1.3.6.1.4.1.15996.100.1.2.3
    NAME 'brBiometricData'
    DESC 'Atributos sobre dados biometricos das pessoas'
    SUP 'top'
    STRUCTURAL
```

```
    MUST ( brbiosrc $  brbiodata )
    MAY (  brcapt ) )

# brEduVoIP
objectclass ( 1.3.6.1.4.1.15996.100.1.2.4
    NAME 'brEduVoIP'
    DESC 'Atributos com dados relativos a um telefone IP'
    SUP 'top'
    STRUCTURAL
    MUST ( brvoipphone $ brvoipalias $  brvoiptype $  brvoipadmin )
    MAY (  brvoipfwr $  brvoipaddr $  brvoipexpiry $  brvoipbalance $  brvoipcredit
) )
```