Ambiente de acesso seguro a nuvem privada: uma proposta voltada à rede da UNIPAMPA

Douglas Pires Borges
dborges@inf.ufsm.br

Maurício Sulzbach
sulzbach@uri.edu.br

Andrea Schwertner Charão
andrea@inf.ufsm.br

Benhur de Oliveira Stein
benhur@inf.ufsm.br

Roseclea Duarte Medina
rose@inf.ufsm.br

***Resumo*—A computação em nuvem apresenta-se como um novo paradigma para a oferta de serviços na Web e tem como principal ideia, a transferência da grande maioria do processamento e armazenamento das aplicações dos usuários, para um ambiente remoto de serviços. Apesar de essa abordagem trazer novas oportunidades de negócios, traz consigo também dúvidas relativas à questão da segurança e do gerenciamento das informações. Isso tem feito com que muitas instituições tenham receio em migrar seus serviços para um ambiente em nuvem. Diante disso, esse trabalho tem por objetivo apresentar uma proposta para a migração dos serviços locais, para uma infraestrutura de nuvem privada para a Universidade Federal do PAMPA – UNIPAMPA. Além disso, essa proposta também irá prover um sistema de autenticação através de *Single Sign On* (SSO), visando o acesso aos diferentes serviços da nuvem através de um único usuário.**

I. Introdução

O avanço da tecnologia tem realizado muitas mudanças, apresentando uma nova realidade às pessoas e às empresas, criando novas oportunidades de negócios, formas de comunicação e entretenimento. A cada curto período, novas tecnologias e dispositivos surgem, com a necessidade de aumentar o desempenho, a segurança, a confiabilidade e principalmente, trazer benefícios e satisfação ao usuário. Nesse sentido, a computação em nuvem ou *cloud computing* é um conceito que está emergindo rapidamente, e vem auxiliando muito esse processo de transformação. Diversas aplicações e serviços que eram anteriormente providos por uma estrutura interna em instituições, estão sendo portadas para a nuvem. Essa mudança traz consigo uma série de benefícios como o aumento do poder computacional, redução da infraestrutura e de custos, alocação de recursos conforme a necessidade, escalabilidade e alta capacidade de tolerância a falhas. Porém, migrar serviços para a nuvem também gera preocupações aos usuários com a questão de segurança e de gerenciamento das informações, uma vez que não se sabe onde e como os dados são armazenados e quem realmente tem acesso à informação.

Além disso, a *cloud,* por prover e unificar diferentes recursos e como forma de facilitar o gerenciamento e auditoria (revisão de regras de autenticação, autorização e verificação das atividades do usuário), necessita que os usuários sejam únicos para os diversos serviços, conceito este conhecido por *Single Sign On* (SSO). Nesse ponto, as Identidades Federadas, ou do inglês, *Federated Identity,* criam um suporte importante para que os usuários possam ter *Single Sign On* ao acessar diferentes aplicações na nuvem. Sendo assim, esse trabalho apresenta uma proposta para migração de serviços que estão hospedados internamente na Universidade Federal do PAMPA - UNIPAMPA, para uma nuvem privada, bem como, um modelo de autenticação e acesso seguro a um ambiente de computação em nuvem, através da utilização de Identidades Federadas. Nesse trabalho, optou-se por um ambiente de nuvem privada, devido ao fato da mesma permitir um nível de segurança maior sobre as informações e possibilitar o gerenciamento dos recursos pelo setor de tecnologia da informação da Universidade.

II. Trabalhos Correlatos

Chen, Sun e Hu [1] descrevem o processo de autenticação dos serviços e aplicações em uma rede universitária, fazendo o uso de *Single Sing On* (SSO).

Já Bhosale [2] aborda um estudo de caso de uma aplicação bancária, que visa fornecer diversos serviços aos seus clientes através da Internet. Nesse artigo, discute-se uma solução de SSO que forneça uma interface de autenticação única para todos os usuários nos diferentes serviços oferecidos.

III. Problemas de Segurança em Ambientes de Nuvem

Cloud computing ou computação em nuvem é um modelo de computação distribuída que deriva características da computação em *grids*, no que diz respeito à provisão de informações sobre demanda, para múltiplos usuários concorrentes.

Devido aos evidentes benefícios da computação em nuvem, muitas empresas e instituições estão migrando seus serviços e aplicações para a nuvem. Porém, a segurança e a disponibilidade dos serviços na nuvem ainda é um fator que gera algumas incertezas sobre migrar ou não para nuvem.

Ao pensar em migrar as informações de usuários para um ambiente externo à instituição, deve-se ter certeza de que estas serão armazenadas com segurança e que estejam disponíveis sempre que necessário. Os serviços que são disponibilizados na rede interna, ao serem migrados para a nuvem, devem ser ofertados de forma igual ou superior ao ambiente de rede local, visando reduzir custos com equipamentos e com pessoal técnico.

Antes de efetuar a migração do ambiente interno para a nuvem, uma questão que deve ser discutida, é a segurança da rede interna institucional. Partindo do princípio que os serviços serão acessados a partir da rede interna, se esta não for segura e eficiente, o ambiente de nuvem trará poucos benefícios.

IV. Ambiente Proposto

No modelo proposto neste trabalho, serão centralizadas as credenciais dos usuários, permitindo um gerenciamento integral do ciclo de vida das suas identidades digitais. Espera-se obter um melhor

gerenciamento das credenciais destes, eliminando problemas de utilização dos recursos computacionais, com foco na segurança e na disponibilidade. Com isso, a administração do ciclo do usuário dentro da instituição, desde a sua criação, até o seu encerramento, pode ser facilitada.

Esta proposta engloba desde a reestruturação da rede interna da instituição, até a criação de um ambiente para acesso seguro às informações que serão disponibilizadas por uma nuvem privada. A figura 1 ilustra o cenário que se deseja atingir com a reestruturação da rede interna, aplicando políticas de segurança eficientes. Também demonstra a criação de um meio de acesso seguro ao ambiente externo à instituição (nuvem privada), onde as aplicações e as informações serão hospedadas.

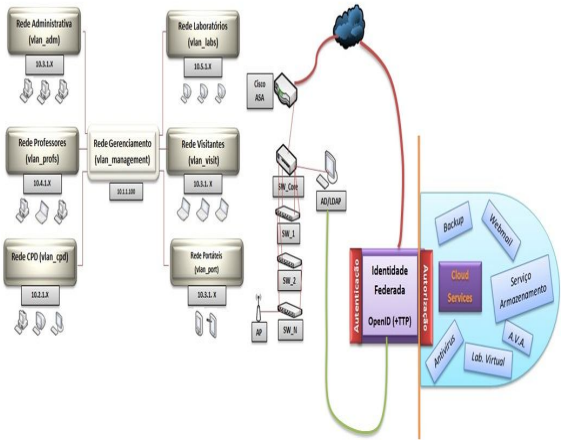

Figura 1 – Cenário de rede esperado com a implantação do modelo proposto (rede interna + ambiente de nuvem).

A seguir, será descrito o modelo de autenticação seguro para a computação em nuvem proposto neste trabalho.

V. APLICANDO A SEGURANÇA NO AMBIENTE DA NUVEM

Conforme citado anteriormente, a preocupação com a segurança do ambiente em nuvem é um fator que ainda impede uma grande parcela das instituições de migrar seus dados e aplicações para a nuvem, seja ela privada ou terceirizada.

As informações institucionais exigem um alto nível de sigilo e segurança. Ambientes de nuvem dividem-se em duas categorias principais: nuvem pública e nuvem privada. Em uma nuvem pública, a instituição que pretende utilizar o serviço de *cloud computing*, contrata uma empresa, sendo que, essa empresa fornece toda a infraestrutura de nuvem, incluindo a segurança do ambiente. Já em uma nuvem privada, os recursos computacionais são gerenciados pela instituição, sendo esta a responsável pela manutenção e segurança das informações.

Neste trabalho, serão combinadas tecnologias eficientes para prover o correto gerenciamento de um ambiente de nuvem. Devido ao cenário em questão, aconselha-se a utilização de um ambiente de nuvem privada. Pretende-se criar um ambiente de nuvem gerenciável, com um eficiente nível de autenticação e autorização de usuários. Para isso, pretende-se utilizar os recursos de *Single Sign On* (SSO), para prover um ambiente de acesso múltiplo, utilizando identidades federadas na nuvem. Serão utilizados os recursos de gerenciamento de identidade e acesso (IAM) e sistemas de gerenciamento de identidade (IMS). Para completar o modelo proposto, serão utilizados ainda, os recursos de *Mutual Protection for Cloud Computing* (MPCC) e *Trusted Third Party* (TTP) respectivamente. Dessa forma, espera-se projetar uma proposta de ambiente de acesso seguro para *cloud computing* utilizando identidades federadas.

A. *Proposta de Acesso: Autenticação, Autorização e Validação dos Usuários*

Uma das principais questões projetadas neste trabalho será a forma de acesso aos recursos providos pela nuvem. A figura 2 ilustra o processo de inclusão de um novo usuário na instituição e todas as ações que esse processo envolve.

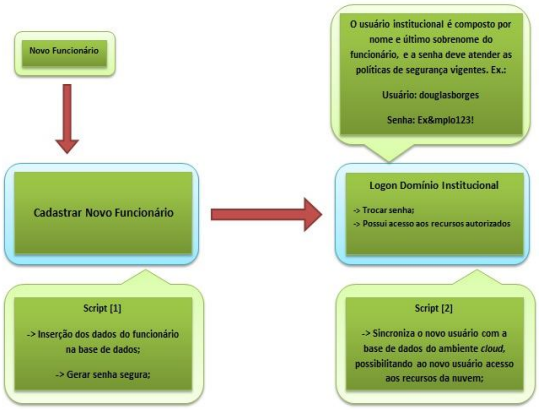

Figura 2 – Processo de inclusão de novo usuário no ambiente institucional e de nuvem.

O processo de criação de usuário local e do ambiente de *cloud* é realizado de forma automatizada, através da comunicação do servidor de autenticação local e do servidor de autenticação da nuvem.

O processo de autenticação no domínio institucional, ou seja, na rede interna, será realizado através da utilização de algum serviço de gerenciamento de usuários e domínio que melhor atenda as necessidades da instituição. Após o primeiro *logon* no domínio local, o usuário será automaticamente replicado na base de dados do ambiente da nuvem, possibilitando o acesso aos serviços e aplicações. Nessa etapa entra o conceito de *Single Sign On* (SSO), que possibilita acesso a diversos serviços e aplicações, utilizando um único conjunto de usuário e senha [3].

Ao projetar-se a utilização da tecnologia SSO, pensou-se nos riscos de segurança, ao fornecer apenas um usuário e senha para várias aplicações. Porém, após uma análise, constatou-se que o nível de aceitação do usuário em relação a várias senhas diferentes, é muito baixo. Sendo assim, devido à necessidade de memorização de várias senhas diferentes, o mesmo pode acabar por realizar anotações, até mesmo em sua mesa, contribuindo para uma possível falha de segurança. Ao implantar um processo de senha unificada, torna-se possível a criação de

uma senha forte, consistente e aceitável seguindo os padrões atuais.

O processo de *login* será concretizado através de um meio de conexão seguro, utilizando esquemas de verificação, validação e liberação de acesso aos sistemas. O esquema de *login* foi projetado utilizando-se os conceitos de Identidades Federadas. Segundo WANGHAM et al. [4], através de uma federação é possível otimizar a troca de informações relacionadas a identidades através das relações de confiança construídas nas federações. Dessa forma, é possível estabelecer acordos entre os provedores de identidades, garantindo que identidades emitidas em um domínio sejam reconhecidas por provedores de serviços de outros domínios, possibilitando assim, uma autenticação única entre os diferentes domínios.

O padrão de gerenciamento de identidades federadas proposto neste trabalho é o *OpenID*. O *OpenID* é um padrão aberto e descentralizado para autenticação de usuários e controle de acesso, permitindo fazer *logon* em muitos serviços com a mesma identidade. É um protocolo simples para acesso único, com suporte a gestão de identidades digitais na web [5].

Além disso, esse modelo é composto pelas tecnologias de gerenciamento de identidades, conhecidas como IAM (*Identity and Access Management*) e IMS (*Identity Management System*). Um *Identity and Access Management* pode ser definido com um método que proporciona um nível adequado de proteção dos recursos e dados de uma organização através de regras e políticas que são impostas aos usuários, tais como senhas, concessão de privilégios e provisionamento de contas de usuário [6]. Já um *Identity Management System*, de forma resumida, refere-se a um sistema de informação ou a um conjunto de tecnologias que podem ser usados para gerenciamento de identidades em empresas ou em aplicações em rede [7].

Para atingir o nível de segurança esperado, propõe-se ainda, juntamente aos servidores de credenciais locais e da nuvem, um método de segurança e criptografia de informações, conhecido como TTP (*Trusted Third Party*). O modelo TTP pode ser caracterizado como uma terceira parte envolvida em uma interação entre outras duas partes garantindo uma relação de confiança entre ambas [8]. Dessa forma, quando um usuário efetua *logon* no domínio local, e está prestes a fazer *logon* no ambiente de nuvem, o TTP atua como um intermediário entre o serviço de domínio local e o serviço de *logon* na nuvem (*OpenID*). Desse modo, os dados são criptografados e as informações continuam seguras. Segundo Leandro [3], *Mutual Protection for Cloud Computing*, é baseado na *Philosophy of Reverse Access Control*, onde os clientes controlam e tentam aplicar meios da nuvem fornecer controle de autenticação e autorização dentro de um ambiente dinâmico e a nuvem garante que o cliente não viole a sua estrutura de segurança.

Durante o processo de *logon*, o usuário, sem perceber, passará por uma série de testes, onde serão verificadas a sua autenticidade e integridade. De forma simples, pode-se resumir o processo acima descrito, analisando a figura 3.

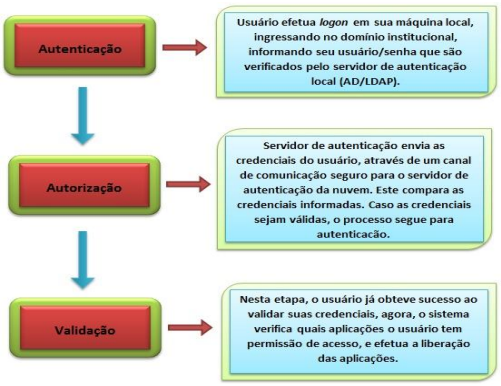

Figura 3 – Modelo de *logon* baseado em três níveis sequenciais: Autenticação, Autorização e Validação.

A cada alteração realizada nas informações dos utilizadores, o serviço de gerenciamento de usuários local enviará uma solicitação de alteração ao servidor de gerenciamento de usuários da nuvem, para que ambos possam iniciar um processo de atualização de suas informações. A cada tentativa de *login*, o processo de verificação de credenciais dos usuários, entre o ambiente local e da nuvem, é iniciado. A figura 4 demonstra esse processo.

Figura 4 – Modelo de sincronização entre serviço de *logon* local e serviço de *logon* da nuvem.

O processo de *logon* suportará ainda diferentes subdomínios, dentro de um único domínio institucional. A figura 5 ilustra o cenário onde diferentes domínios, com suas redes, poderão ser autenticados e autorizados.

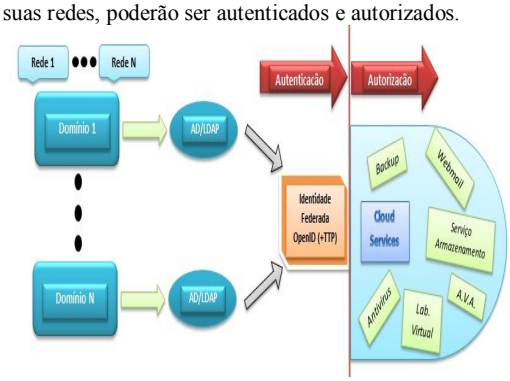

Figura 5 – Vários domínios passando pelo processo de autenticação e autorização do modelo proposto.

VI. Contribuições do Ambiente Proposto

Embora o modelo proposto nesse trabalho não tenha sido implantado, tem-se grande expectativa de bons resultados após sua efetivação. Os benefícios irão englobar desde o setor de tecnologia da informação, até os usuários finais da Instituição. De forma inicial, alguns objetivos tornam-se mais visíveis, sendo descritos a seguir.

A. Para a Equipe de Tecnologia da Informação

Em algumas universidades, que possuem estrutura multi campus, opta-se pela centralização dos sistemas e serviços, que são oferecidos aos usuários e comunidade em geral. Juntamente com a adoção de uma estrutura centralizada, fatores como o gerenciamento e a disponibilidade das informações são minuciosamente pensados.

Com a adoção de um ambiente de computação em nuvem, os serviços podem ser gerenciados de forma simples e centralizada (visando o aspecto de controle dos serviços) e de forma descentralizada (tendo em vista, que o ambiente institucional local torna-se irrelevante, pois o responsável por determinado serviço, poderá prestar qualquer tipo de suporte, independente de sua localização). Dessa forma, fica claro, que o ambiente de nuvem proposto nesse pode colaborar em vários sentidos para a equipe de tecnologia da informação da UNIPAMPA, bem como, aos demais setores prestadores de serviço à comunidade em geral.

B. Para a Rede Interna Institucional

Uma das etapas que antecedem a possível implantação do ambiente de nuvem privado aqui proposto envolve uma reestruturação da rede interna da Instituição.

A rede interna deverá passar por uma série de testes e padronizações, onde serão aplicadas normas e métodos, para colaborar com o correto gerenciamento da rede interna da instituição, bem como a adoção de padrões de estruturação de redes de computadores. Dessa forma, problemas de má administração e gerenciamento, tendem a ser solucionados, colaborando para a implantação do projeto de migração dos serviços para um ambiente de nuvem.

C. Para os Usuários Finais

Uma vez implantado, o modelo proposto proporcionará a comunidade acadêmica a possibilidade de acesso às informações nos mais variados lugares, fazendo com que os usuários não tenham necessidade de estar na instituição para utilizar os serviços oferecidos.

Neste sentido, funcionários, professores e alunos terão uma estrutura de serviço disponível sempre que necessário, possibilitando assim o acesso às informações da instituição, impactando na correta utilização dos serviços oferecidos e colaborando para a integração acadêmica, entre alunos, professores, funcionários e universidade.

VII. Conclusão

Esse trabalho apresentou uma proposta de ambiente de acesso seguro para *cloud computing* utilizando conceitos de identidades federadas, *Trusted Third Party* (TTP) e *OpenID*. Através dessa proposta, acredita-se que caso os serviços sejam migrados para a nuvem privada, o método de autenticação e validação de usuários será eficiente, atingindo o nível de segurança esperado. Utilizando identidades federadas é possível unificar *logins* de acesso para diversos provedores de nuvem (SSO), possibilitando um melhor gerenciamento dos usuários e acesso único a diferentes serviços e aplicações.

Durante o desenvolvimento desta proposta, foram levantadas uma série de premissas e questões fundamentais de segurança envolvendo o ambiente de nuvem e o ambiente da rede local. Através destas informações, tornou-se possível a criação de um modelo de ambiente de nuvem, com um nível de segurança que se enquadra nos padrões atualmente exigidos.

Como sugestão de trabalho futuro, objetiva-se testar o ambiente computacional proposto neste. Espera-se, que com os testes a serem realizados, seja possível verificar a confiabilidade e integridade do modelo apresentado. Juntamente com os testes, espera-se aprimorar o modelo inicial, proporcionando um nível de segurança maior, aumentando a confiabilidade dos ambientes local e de nuvem.

Referências

[1] J. Hu, Q. Sun, H. Chen. Application of Single Sign-on (Sso) in Digital Campus. Broadband Network and Multimedia Technology (IC-BNMT). 3rd IEEE International Conference on, 2010.

[2] S.K. Bhosale. Architecture of A Single Sign on (Sso) for Internet Banking. Wireless, Mobile and Multimedia Networks. IET International Conference on, 2008.

[3] M. A. P. Leandro, T. J. Nascimento, D. R. S. Santos, C. M. Westphall, C. B. Westphall. Multi-Tenancy Authorization System with Federated Identity for Cloud-Based Environments Using Shibboleth. ICN 2012 : The Eleventh International Conference on Networks.

[4] M. S. Wangham, E. R. de Mello, D. da S. Böger, M. Guerios, J. da S. Fraga Gerenciamento de Identidades Federadas. Disponível em: <http://dainf.ct.utfpr.edu.br/~maziero/lib/exe/fetch.php/ceseg:2010-sbseg-mc1.pdf>. Acesso em: 14/07/2012.

[5] Openid. O que é OpenID?. Disponível em: <http://www.openid.org.pt/2010/04/o-que-e-o-openid/>. Acesso em: 14/06/2012.

[6] S. A. Almulla, C. Y. Yeun. Cloud Computing Security Management. IEEE, 2010.

[7] Researcher's. Federated Identity Management in Cloud Computing. Disponível em: <http://clean-clouds.com/2012/04/25/federated-identity-management-in-cloud-computing-2/>. Acesso em: 12/06/2012.

[8] P. T. Endo, G. E. Gonçalves, J. Kelner, D. Sadok. A Survey on Open-source Cloud Computing Solutions. VIII Workshop em Clouds, Grids e Aplicações, 2010.