Universidade Federal do Rio Grande do Norte
Instituto Metrópole Digital

SmartMetropolis – Plataforma e Aplicações para Cidades Inteligentes

WP4 – Infraestrutura

Relatório de Controle de Acesso

Natal-RN, Brasil
Julho 2017

Equipe Técnica

Docentes

Prof. Dr. Carlos Eduardo da Silva (Coordenador) - IMD/UFRN

Discentes
Irene Ginani Costa Pinheiro

Pesquisadores vinculados
Welkson Renny de Medeiros - PPGSW

Sumário

1 Introdução

O projeto SmartMetropolis, conduzido pelo Instituto Metrópole Digital (IMD) da Universidade Federal do Rio Grande do Norte (UFRN), tem como objetivo o desenvolvimento de soluções de tecnologia da informação e comunicação para Cidades Inteligentes e Humanas.

O projeto é organizado em seis Pacotes de Trabalho (Work Packages - WP) temáticos, liderados cada por um coordenador. Cada WP possui um conjunto de objetivos a serem alcançados ao longo dos cinco anos de execução do projeto.

Este relatório está inserido no contexto do WP 4 - Infraestrutura Computacional, que no contexto do segundo ano de execução do projeto Smart Metropolis, tem os seguintes objetivos principais:

- Operação de Infraestrutura: Este objetivo engloba a operação e manutenção da instância Fiware do projeto, incluindo ferramentas para monitoramento da infraestrutura, e para gerenciamento de aplicações.
- Segurança da Informação e Controle de Acesso: Este objetivo engloba o estudo aprofundado dos mecanismos de segurança da plataforma Fiware com o fim de oferecer uma solução de controle de acesso que possa ser utilizada pelas aplicações que irão executar sobre a infraestrutura Fiware.

Neste contexto, este relatório corresponde ao entregável definido pela **Meta 1.9: Estudo sobre os conceitos, ferramentas e bibliotecas relacionados a controle de acesso (autenticação e autorização)**. Nesse novo trimestre houveram dificuldades que acabaram atrasando os avanços que estavam sendo realizados, a principal ocorreu com a mudança de bolsista, fazendo assim com que tivéssemos toda a parte de adequação ao projeto para que assim pudéssemos dar a devida continuidade. Dessa forma, como resultado desse estudo iremos apresentar nesse relatório os estudos realizados para a parte de autenticação, realização de materiais e revisões realizadas. Para a autorização foi possível editar a aplicação feita anteriormente e dar prosseguimento na política que está sendo feita para o contexto do SGEOL.

2 Estudos Realizados

2.1 Objetivos

Com a saída da bolsista que era responsável por cuidar dos estudos e desenvolver as aplicações na área de controle de acesso, para assumir uma bolsa sobre responsabilidade da RNP, foi necessário ambientar a nova bolsista com os conceitos básicos, as tarefas desenvolvidas e as tarefas futuras que seriam desenvolvidas no WP-Infraestrutura, para que assim pudesse dar prosseguimento nas tarefas pendentes o mais rápido possível.

2.2 Material Estudado

Inicialmente, foram passados artigos para que com a leitura pudessem ser entendidos os conceitos de autenticação e autorização teoricamente e praticamente, através da plataforma FIWARE, seus GE's(Generic Enablers) e demais ferramentas que, na prática, tornam a utilização desses conceitos possível. Assim, se atendo aos conceitos, primeiramente, foi estudado o artigo do Sandhu[5] para que fosse entendido, de forma intuitiva e clara, como funciona a autenticação e a autorização, entendendo também como se dão suas subcategorias, como políticas baseadas em papéis ou em atributos, por exemplo no caso da autorização.

Posteriormente, trabalhamos os conceitos, para saber mais do funcionamento detalhado, do que foi visto no conteúdo inicial. Dessa forma, para a parte de autenticação demos um enfoque na área de autenticação federada, mais precisamente no seu gerenciamento, utilizando as referências encontradas em [1] e [6]. Assim, demos prosseguimento aos estudos e na parte de autorização escolhemos duas políticas para serem estudadas com mais afinco: a política baseada em papéis e a política baseada em atributos.

Dessa forma, utilizamos as especificações dispostas no site do NIST, para o RBAC e ABAC, que são as políticas citadas acima. Além de usar também o material disposto em [4] e [3], para poder assim ter um aprofundamento nos conceitos e começar a trabalhar de fato nas aplicações e demais atividades efetuadas pelo Work Package.

2.3 Material Produzido

Para que o conhecimento adquirido fosse avaliado de alguma forma, foi elaborado uma apresentação exibindo todos esses conceitos levantados na leitura dos artigos citados, e depois essa apresentação pode ser feita para os demais entregantes do WP, para que assim todos pudessem dar um retorno do que poderia ser melhorado. Ainda foi pedido que fosse feito a revisão de um minicurso elaborado no ano passado, para que assim o material tivesse uma melhoria e uma revisão mais detalhada.

2.4 Decisões Tomadas

Ao terminar os estudos, sobre os conceitos mais essenciais, decidimos dar prioridade ao trabalho que estava sendo desenvolvido anteriormente com a Prefeitura do Natal para a criação de uma política de controle de acesso para o aplicativo do SGEOL e posteriormente estudar as tecnologias necessárias para a aplicação do que foi visto. Dessa forma estudamos casos de uso e de aplicação da política baseada em papéis (RBAC), um desses casos pode ser visto em [2]. Logo após, analisamos os dados passados pela SEMURB e começamos a avaliar qual seria a melhor estratégia para definir a política desejada. Assim foi decidido que, neste momento, utilizaríamos a política baseada em papéis.

Então com os dados fornecidos, se fez necessário aprender as tecnologias que fazem o controle de acesso funcionar e para isso começamos a mexer na aplicação exemplo já desenvolvida anteriormente.

3 Autorização

Ao receber os dados da Prefeitura do Natal, observamos, juntamente com alguns integrantes da equipe da WP-Middleware que foram destacadas as operações de criar, editar, visualizar e remover, que são utilizadas, respectivamente, para criar os atributos, modificá-los, visualizá-los e remove-los, já que a política irá trabalhar em cima dos atributos de um objeto. Assim os papéis terão as permissões de exercer essas operações sobre determinados recursos disponíveis na prefeitura. Dessa forma identificamos oito papéis que possuem algum tipo de permissão sobre os atributos do objeto manipulado na plataforma SGEOL, que no nosso caso de estudo seria um lote. Assim, teríamos para organização dos papéis, uma divisão em 3 grupos. Inicialmente teríamos o grupo relacionado ao geoprocessamento que seriam os papéis de:

- Técnico de Geoprocessamento;
- Chefe do Setor de geoprocessamento

Posteriormente o grupo relacionado a funções mais administrativas com os papéis de:

- Secretário;
- Diretores de Departamento;
- Chefe do Setor;
- Analistas

E por fim os papéis que dizem respeito aos usuários do sistema de uma forma mais geral, que seriam:

- Usuário Interno;
- Usuário Externo

Então, criamos tabelas que relacionam as permissões aos papéis, que estão representadas como a possibilidade ou não de efetuar uma das operações sobre determinado atributo. Para o primeiro grupo temos:

Tabela 1: Grupo 1: Geoprocessamento

Atributo	**Papel**	**Criar**	**Editar**	**Vizualizar**	**Remover**
Operação	Técnico em Geoprocessamento	S	S	S	S
Operação	Chefe do Setor de Geoprocessamento	S	S	S	S
Nº Doc	Técnico em Geoprocessamento	S	S	S	S
Nº Doc	Chefe do Setor de Geoprocessamento	S	S	S	S
Status	Técnico em Geoprocessamento	S	S	S	S
Status	Chefe do Setor de Geoprocessamento	S	S	S	S
Data	Técnico em Geoprocessamento	S	S	S	S
Data	Chefe do Setor de Geoprocessamento	S	S	S	S
ID Parcela	Técnico em Geoprocessamento	S	S	S	S
ID Parcela	Chefe do Setor de Geoprocessamento	S	S	S	S
Nº Unidades	Técnico em Geoprocessamento	S	S	S	S
Nº Unidades	Chefe do Setor de Geoprocessamento	S	S	S	S
Nº Pav	Técnico em Geoprocessamento	S	S	S	S
Nº Pav	Chefe do Setor de Geoprocessamento	S	S	S	S
Tipo Imóvel	Técnico em Geoprocessamento	S	S	S	S
Tipo Imóvel	Chefe do Setor de Geoprocessamento	S	S	S	S
Estrutura	Técnico em Geoprocessamento	S	S	S	S
Estrutura	Chefe do Setor de Geoprocessamento	S	S	S	S
Qualidade	Técnico em Geoprocessamento	S	S	S	S
Qualidade	Chefe do Setor de Geoprocessamento	S	S	S	S
Patrimônio	Técnico em Geoprocessamento	S	S	S	S
Patrimônio	Chefe do Setor de Geoprocessamento	S	S	S	S
Uso	Técnico em Geoprocessamento	S	S	S	S
Uso	Chefe do Setor de Geoprocessamento	S	S	S	S
Nº da Porta	Técnico em Geoprocessamento	S	S	S	S
Nº da Porta	Chefe do Setor de Geoprocessamento	S	S	S	S

Em relação ao grupo com funções administrativas temos (tabela 2 e 3):

Por fim, teremos o último grupo representando(na tabela 4) os usuários mais genéricos da aplicação e para eles temos as suas respectivas permissões.

Tabela 2: Grupo 2: Funções Administrativas

Atributo	**Papel**	**Criar**	**Editar**	**Vizualizar**	**Remover**
Operação	Secretário	N	N	S	N
Operação	Diretores de Departamento	N	N	S	N
Operação	Chefe do Setor	N	N	S	N
Operação	Analistas	N	N	S	N
Nº Doc	Secretário	N	N	S	N
Nº Doc	Diretores de Departamento	N	N	S	N
Nº Doc	Chefe do Setor	N	N	S	N
Nº Doc	Analistas	N	N	S	N
Status	Secretário	N	N	S	N
Status	Diretores de Departamento	N	N	S	N
Status	Chefe do Setor	N	N	S	N
Status	Analistas	N	N	S	N
Data	Secretário	N	N	S	N
Data	Diretores de Departamento	N	N	S	N
Data	Chefe do Setor	N	N	S	N
Data	Analistas	N	N	S	N
ID Parcela	Secretário	N	N	S	N
ID Parcela	Diretores de Departamento	N	N	S	N
ID Parcela	Chefe do Setor	N	N	S	N
ID Parcela	Analistas	N	N	S	N
Nº Unidades	Secretário	N	N	S	N
Nº Unidades	Diretores de Departamento	N	N	S	N
Nº Unidades	Chefe do Setor	N	N	S	N
Nº Unidades	Analistas	N	N	S	N
Nº Pav	Secretário	N	N	S	N
Nº Pav	Diretores de Departamento	N	N	S	N
Nº Pav	Chefe do Setor	N	N	S	N
Nº Pav	Analistas	N	N	S	N
Tipo Imóvel	Secretário	N	N	S	N
Tipo Imóvel	Diretores de Departamento	N	N	S	N
Tipo Imóvel	Chefe do Setor	N	N	S	N
Tipo Imóvel	Analistas	N	N	S	N
Estrutura	Secretário	N	N	S	N
Estrutura	Diretores de Departamento	N	N	S	N
Estrutura	Chefe do Setor	N	N	S	N
Estrutura	Analistas	N	N	S	N
Qualidade	Secretário	N	N	S	N
Qualidade	Diretores de Departamento	N	N	S	N
Qualidade	Chefe do Setor	N	N	S	N
Qualidade	Analistas	N	N	S	N
Patrimônio	Secretário	N	N	S	N
Patrimônio	Diretores de Departamento	N	N	S	N
Patrimônio	Chefe do Setor	N	N	S	N
Patrimônio	Analistas	N	N	S	N

Tabela 3: Continuação das permissões do Grupo 2

Atributo	Papel	Criar	Editar	Vizualizar	Remover
Uso	Secretário	N	N	S	N
Uso	Diretores de Departamento	N	N	S	N
Uso	Chefe do Setor	N	N	S	N
Uso	Analistas	N	N	S	N
Nº da Porta	Secretário	N	N	S	N
Nº da Porta	Diretores de Departamento	N	N	S	N
Nº da Porta	Chefe do Setor	N	N	S	N
Nº da Porta	Analistas	N	N	S	N

Assim observamos que os papéis do mesmo grupo possuem permissões semelhantes, o que auxilia na criação e manutenção da política.

4 Implementação

Para que a política fosse de fato utilizada foi necessário inicialmente realizar sua implementação. Inicialmente estudamos as tecnologias que envolviam sua implementação, e utilizando a aplicação exemplo desenvolvida para o minicurso que está sendo criado sobre controle de acesso foi possível ter uma visão geral do que era necessário para que de fato pudéssemos implementar a política na aplicação da SGEOL. Assim utilizando a plataforma FIWARE montamos um ambiente com as GE's para autenticação e autorização, dessa forma utilizamos o Keyrock, PEP e PDP, utilizando protocolos REST além do OAuth na parte de autenticação assim como o KeyRock.

Dessa forma para que possamos implementar a política na aplicação utilizaremos os conhecimentos prévios, além do AuthZForce, tudo isso atrelado a linguagem Python que também é utilizada durante o projeto.

5 Considerações Finais

Assim, observamos que estamos fazendo avanços em relação ao controle de acesso e fornecendo o suporte de infraestrutura necessário para os demais WP's, porém com as dificuldades encontradas, como a troca de bolsistas, acabamos não avançando tanto quanto o desejado em alguns aspectos. No entanto com a ambientação dos que se integram ao grupo podemos dar continuidade ao trabalho.

Assim para os próximos meses é necessário que a nova bolsista se integre ainda mais diante as tecnologias e conceitos utilizados no controle de acesso, além da necessidade da continuidade do trabalho na aplicação do SGEOL junto com WP-Middleware, para que assim, possa ser entregue ao nosso usuário final, o qual auxiliamos em melhorias através da tecnologia, que é a Prefeitura do Natal.

Tabela 4: Grupo 3: Usuários

Atributo	**Papel**	**Criar**	**Editar**	**Vizualizar**	**Remover**
Operação	Usuário Interno	N	N	S	N
Operação	Usuário Externo (WEB)	N	N	N	N
Nº Doc	Usuário Interno	N	N	S	N
Nº Doc	Usuário Externo (WEB)	N	N	N	N
Status	Usuário Interno	N	N	S	N
Status	Usuário Externo (WEB)	N	N	N	N
Data	Usuário Interno	N	N	S	N
Data	Usuário Externo (WEB)	N	N	N	N
ID Parcela	Usuário Interno	N	N	S	N
ID Parcela	Usuário Externo (WEB)	N	N	N	N
Nº Unidades	Usuário Interno	N	N	S	N
Nº Unidades	Usuário Externo (WEB)	N	N	N	N
Nº Pav	Usuário Interno	N	N	S	N
Nº Pav	Usuário Externo (WEB)	N	N	N	N
Tipo Imóvel	Usuário Interno	N	N	S	N
Tipo Imóvel	Usuário Externo (WEB)	N	N	N	N
Estrutura	Usuário Interno	N	N	S	N
Estrutura	Usuário Externo (WEB)	N	N	N	N
Qualidade	Usuário Interno	N	N	S	N
Qualidade	Usuário Externo (WEB)	N	N	N	N
Patrimônio	Usuário Interno	N	N	S	N
Patrimônio	Usuário Externo (WEB)	N	N	N	N
Uso	Usuário Interno	N	N	S	N
Uso	Usuário Externo (WEB)	N	N	S	N
Nº da Porta	Usuário Interno	N	N	S	N
Nº da Porta	Usuário Externo (WEB)	N	N	S	N

Referências

[1] David W. Chadwick. *Federated Identity Management*, pages 96–120. Springer Berlin Heidelberg, Berlin, Heidelberg, 2009.

[2] HL7 Security Technical Committee. Hl7 role-based access control (rbac) role engineering process) definition and considerations. 1.3, 2007.

[3] Vincent C. Hu, David Ferraiolo, Rick Kuhn, Adam Schnitzer, Kenneth Sandlin, Robert Miller, and Karen Scarfone. Guide to attribute based access control (ABAC) definition and considerations. *NIST Special Publication*, 2014.

[4] Vincent C. Hu, David Ferraiolo, Rick Kuhn, Adam Schnitzer, Kenneth Sandlin, Robert Miller, and Karen Scarfone. Guide to role based access control (RBAC) definition and considerations. *NIST Special Publication*, 2014.

[5] Ravi Sandhu and VB Year. The ascaa principles for next-generation role-based access control. *Engineer*, 1:E1, 2008.

[6] Michelle S. Wangham, Emerson Ribeiro de Mello, Davi da Silva Böger, Marlon Guerios, and Joni da Silva Fraga. *Gerenciamento de Identidades Federadas*. Livro de Minicursos do SBSEG, Porto

Alegre, 2010.