Permissoes

Segurança em Projetos

Este documento centraliza as informações sobre a segurança em projetos que seguem o padrão 3PUP.

Os níveis de segurança são balizados por necessidades de negócio e também pelas características das ferramentas utilizadas nos projetos, com ênfase central nos produtos Atlassian Jira (gerência de atividades), Atlassian Confluence (wiki corporativa), Atlassian FishEye (visualizador de repositório versionado), Atlassian CrowD (autenticador e autorizador) e diretórios corporativos nos padrões mais comuns, como Active Directory e LDAP.

Política de Liberdade

Todo o fundamento de segurança em um ambiente é balizado pela política de liberdade da organização, as quais indicam qual o nível de acesso primário (ou seja, quando nada é especificado) para o conteúdo. Assim, as organizações podem ser caracterizadas como tendo políticas restritivas ou permissivas.

Em organizações norteadas por políticas restritivas, exceto explicitamente documentado, tudo é restringido.

Em organizações norteadas por políticas permissivas, exceto explicitamente documentado, tudo é permitido.

Política de Liberdade em Projetos 3PUP

A opção por um determinado tipo de política de liberdade é influenciado por diversos fatores, cada qual possuindo um peso em virtude do tipo de negócio da organização. Organizções bancárias, por exemplo, tendem a obtar por políticas restritivas, uma vez que as informações financeiras envolvidas geralmente têm impacto estratégico no negócio. Já projetos em software livre, por exemplo, geralmente possuem políticas permissivas, pois o objetivo central é disseminar a informação.

Considerando os fatores que influenciam o 3PUP, a política de liberdade adotada é a a permissiva.

Modelos de Segurança

Idealmente, a segurança em projetos pode ser aplicada com base nos papéis desempenhados pelos envolvidos. Assim, níveis diferenciados de acesso poderiam ser alocados para gerentes, diretores, gestores, estagiários, etc. Ainda, poderiam ser elencadas as áreas de atuação dos envolvidos, dando margem a gerentes financeiros, gerentes administrativos, diretores de marketing, etc. Independente ao uso vinculado de cargos e áreas, podemos asumir esses elementos apenas como sendo *papéis* desempennados por alguma pessoa, ou mesmo um serviço (sistema externo) que interage no projeto.

Para alcançar níveis detalhados de gerenciamento de permissões, as ferramentas devem ter suporte a modelos extremamente granulares, podendo vincular perfis, áreas e permissões em níveis elementares.

Infelizmente, esse modelo de segurança nem sempre é bem desenvolvido nas soluções de mercado, e por isso, elas acabam optando por modelos mais simples, como aqueles encontrados em diretórios corportativos, como LDAP ou Active Directory.

Nesses modelos, o conceito de papel (ou *role*, no jargão de TI) é substituído pela aglutinação de elementos (usuário) em conjuntos maiores, que são os grupos. Um grupo poderia ser então algo como *gerentes* ou *gerentes_do_financeiro* ou *diretores_de_marketing*. Ao leigo, isso soaria como conceitos iguais. Entretanto isso não é verdade.

Grupos são apenas aglutinações de usuários. Papéis ou Roles (vamos adotar esse teremo de agora em diante), representam a vinculação entre um usuário ou grupo e sua função no sistema. Para ficar mais claro esse conceito, observe a figura abaixo:

TODO: Colocar figura com um sistema e suas operações a esquerda e a direta usuarios e grupos. No meio da figura, colocar os papeis, e fazer entao ligacao entre os elementos.

Nessa figura, fica clara a possibilidade de um mesmo usuário (ou grupo) possuir roles diferentes em sistemas diferentes. Assim, as roles resolvem problemas comuns que seriam encontrados em um sistema de segurança baseado somente em grupos e usuários, que seria a necessidade de um mesmo grupo (ou usuário) precisar desempenhar papéis diferentes em sistemas diferentes (em outras palavras, o problema seria a proliferação de grupos no mecanismo de controle, como o Active Directory, LDAP ou outra ferramenta).

Modelos de Segurança nas Ferramentas Adotadas pelo 3PUP

Mesmo tendo noção que o modelo de segurança baseado em roles é muito mais interessante, como dito, nem todas ferramentas o suportam. Assim, é importante analisar as ferramentas adotadas no 3PUP.

- **Atlassian Jira**: O Jira permite um modelo híbrido e muito granular de permisões. Ele suporte o conceito de roles e também de grupos. Ainda, permite agrupar roles em níveis mais altos ainda, formando o conceito de esquemas de segurança. Assim usuários e grupos podem ser atrelados a roles diversas; cada role pode estar associada a várias operações dentro do sistema e ao final, as roles são aglutinadas em esquemas de segurança, os quais são vinculados a um projeto. Como mecanismo de extensão, o Jira ainda permite criar a chamada "segurança horizontal", que significa que uma tarefa de projeto pode ser visualizada por uma role específica, a qual pode ou não fazer parte do esquema de segurança e ser composta de grupos, usuários ou mesmo outras roles.
- **Atlassian Confluence**: O Confluence é menos flexível que o Jira, e permite somente o controle de acesso através de grupos ou usuários. A vantagem é que o Confluence pode reusar os grupos e usuários do Jira de forma simples e transparente.
- **Atlassian FishEye**: O FishEye permite o controle de segurança por grupos e usuários, e não permite compartilhar essas informações com o Jira nem com o Confluence.

- **Atlassian Crowd**: É um centralizador de segurança para todos os sistemas da Atlassian ou mesmo produtos externos. Ele reusa grupos e usuários de serviços como LDAP e Active Directory e permite que o Jira, Confluence e o FishEye valam-se desses usuários e grupos para definir suas permissões. Assim, toda a gerência de usuários e grupos fica no Crowd.
- **JForum**: É um sistema para fóruns de discussao construido em java. Possui modo hibrido para controle de usuarios, grupos. Por padrao, seus usuarios e grupos sao definidos na propria ferramenta. Mas tambem suporta a integracao de usuarios e grupos definidos na ferramenta Atlassian Crowd (o que eh interessante pra os casos onde o JForum eh instalado dentro da Wiki Confluence, por exemplo). Ja as permissoes, estas sempre sao definidas dentro da propria ferramenta JForum.
- **Subversion**: O subversion, ou simplesmente SVN é a ferramenta de versionamento de conteúdo padrão no modelo 3PUP. Ele é balizado por grupos e usuários, e pode compartilhar essas informações de diretórios corporativos como LDAP e Active Directory.

Usuários e Grupos Padrões

Independente do suporte da ferramenta, grupos e usuários são o denominador comum de qualquer modelo de segurança.

Após análise cuidadosa de todos os aspectos dos projetos, o seguinte modelo padrão de grupos e usuários é utilizado:

NOTA 1: A utilização de prefixos e sufixos é utilizada para facilitar o gerenciamento de usuários e grupos em bloco.

NOTA 2: Embora não mostrado, todos usuários devem, obrigatoriamente, pertencerem aos grupos padrões *jira-users* e *confluence-users*. Estes não são mostrados na tabela para evitar a poluição visual.

NOTA 3: Valores iniciados por $ (cifrão) denotam nomes de variáveis que devem ser substituídos pelo valor final adequado. Caso nomes de variáveis sejam compostos, use a sintaxe camelCase, iniciando sempre com a letra minúscula.

Usuários

Tipo	Nome padrão	Grupos padrões	Roles padrões diretas (Jira)	Permissões padrões	Exemplos	Descrição
Usuário comum	$nome.$sobrenome	empresa-$empresa	TODO	TODO	joao.netto carlos.silva jpaulo.silva	A utilização do formato nome.sobrenome é adotada para suportar o cenário de crescimento da base de usuários. Ainda, na eventualidade de repetições começarem a surtir, prefixos podem ser usados, preferencialmente a primeira inicial do nome seguido do segundo nome e depois, pelo sobrenome (terceiro exemplo, o onde o nome da pessoa provavelmente é João Paulo da Silva). NOTA: Idealmente, todos usuários devem pertencer a uma empresa. Porém, nem sempre isso é possível, pois como em projetos de software livre, muitos integrantes são elementos dispersos, sem vínculo com nenhuma instituição.
Usuário de nível cliente padrão da entidade	user.$empresa	empresa-$empresa	TODO	Ver todos projetos da sua empresa Criar comentários em todos projetos da sua empresa	user.trt4 user.herc	Este usuário deve ser criado toda vez que um grupo de empresa é criado. Esse usuário é utilizado pela empresa cliente do projeto para acompanhar as demandas de **todos** os seus projetos. NOTA 1: Para empresas que não desejar dar permissões para este usuário acompanhar todos os projetos (pois são emnpresas clientes que adotam modelo restritivo), então é importante que essas empresas não divulguem as senhas de acesso de usuário para pessoas que não devem ter esse acesso.
Usuários padrao de sistema	$nome.admin	TODO	TODO	Pode executar qualquer operacao dentro do sistema para o qual ele eh definido	jira.admin confluence.admin jforum.admin	**TODO (para marcelo.mrack de marcelo.mrack): Estou verificando esse padrao, e ainda nao esta 100% definido, mas as ferramentas da Atlassian seguem este padrao, e acho que pode ser estendido para todo o ambiente, ou seja, no formato $nomeDoSistema.admin.**
Usuário administrador de plataforma de sistema e serviços	user.sysadmin	system	TODO	Instalar, reconfigurar, atualizar, remover sistema e seus componentes e gerenciar permissões e efetuar backup e restore	user.sysadmin	É o mais alto nível de permissões nos sistemas, podendo executar quaisquer operações no serviços e sistema acessado, incluindo sua remoção. Este usuário não deve ser utilizado em processos normais do dia-a-dia, mas sim somente em momentos críticos, como instalações, configurações de ambiente, atualização de serviços e outras atividades que necessitem acesso realmente deliberativo. Geralmente, este usuario tem privilegios (ou mesmo uma conta) associada no Sistema Operacional e outros recursos externos so servico que ele gerencia, como contas de email, FTP, SSH, etc.
Usuário administrador de sistema	user.admin	system	TODO	Reconfigurar partes do sistema, gerenciar permissões e efetuar backup e restore, quando viável com este usuário	user.admin	É o segundo mais alto nível de permissões nos sistemas, podendo executar a maioria das operações administrativas. Geralmente, este usuário é utilizado por mecanismos de integração B2B (ou seja, entre sistemas) e por usuários (pessoas) que precisam realizar operações em modo administrativo. Também utilizasse esse usuário para processos de backup e restore. Geralmente, este usuario *nao tem* privilegios (ou mesmo uma conta) associada no Sistema Operacional ou outros recursos externos.

Grupos

Tipo	Nome padrão	Roles padrões diretas no Jira	Exemplos	Descrição
Grupo padrao de uma entidade /empresa	empresa-$empresa	Cliente	empresa-herc empresa-lm2 empresa-trt4	É o grupo padrão onde todo colaborador da referida empresa deve estar contido. É usado para agrupar todos colaboradores da empresa e possibilita dar/negar direitos de forma única.
Grupo de diretores de um entidade /empresa	empresa-$nome-diretoria	Empresa - Diretoria	empresa-lm2-diretoria empresa-3layer-diretoria	É o grupo de pessoas que representam a gestão da empresa. Geralmente têm o mesmo nível de permissão que os usuários do grupo empresa-$empresa, exceto que podem ver ver todos projetos que sua empresa administra, em qualquer nível de detalhamento. Em outras palavras, geralmente eles não podem realizar qualquer operação sobre os projetos/documentos/áreas, mas podem efetivamente ver tudo que está acontecendo. Caso os diretores também precisem alterar informações nos projetos, então eles precisam fazer parte de grupos superiores, como os desenvolvedores, coordenadores e gerentes de projeto.
Grupo de usuários de uma área de uma entidade/empresa	empresa-$nome-$area	N/A	empresa-lm2-desenv empresa-lm2-administrativo empresa-lm2-rh	São grupos opcionais, usados para aglutinar usuários de determinadas áreas da empresa. Segue a mesma lógica do grupo de diretores, exceto que suas pemissões de visualização restringem-se às áreas da empresa a que pertencem.

			empresa-lm2-marketing	
Grupo de usuários envolvidos em um projeto	$empresa-$projeto-users	Cliente Empresa	lm2-jboss-users	Usuários nesse grupo têm direito a "ver" o projeto, mas geralmente não ter privilégios para realizar quaisquer operações sobre ele, exceto comentários sobre atividades/págins/documentos, por exemplo.
Grupo de usuários envolvidos em um projeto com direitos avançados	$empresa-$projeto-developers	Empresa - Desenvolvedores	lm2-jboss-developers	
Grupo de usuários coordenadores e gerentes de um projeto	$empresa-$projeto-administrators	Empresa - Gerentes Empresa - Coordenadores	lm2-jboss-administrators	
Grupo de sistema ou serviço	$sistema-users	N/A	confluence-users jira-users fisheye-users system	Usuários nesses grupos têm direito a "logar" nas referidas aplicações, e terão privilégio conforme os outros grupos ou roles que pertencerem. NOTA: Observe que a diferença de nomenclatura: grupos de projeto usam 3 partes para o nome do grupo; e grupos de sistema apenas 2 partes.
Grupo de sistema sistema ou serviço	$sistema-administrators	N/A	confluence-adminstrators jira-administrators fisheye-administrators subversion-administrators system	Usuários nesses grupos têm direito para adminstrar as referidas aplicações, porém, privilégios de uso dentro da aplicação vão depender dos grupos e roles a que eles pertencerem. Em outras palavras, mesmo que alguém seja parte do grupo "jira-administrators", ele somente poderá remover uma issue se ele fazer parte do grupo de adminstradores do projeto a qual a issue pertence.

Configurações Adicionais em Ferramentas

Esta seção mostra as peculiaridades para configuração da segurança em cada uma das ferramentas adotadas pela metodologia 3PUP.

Atlassian Jira

Segurança Horizontal

Como digo, a *segurança horizontal* visa restringir um elemento que corresponde a uma linha de informação, quando considerarmos dados provenientes de uma tabela, por exemplo. Seria como dizer que, dado uma tabela onde todos tem acesso a ela, uma linha específica pode ou não ser mostrada a um usuário, grupo ou role específico conforme a necessidade.

Como exemplo, imagine um projeto genérico de adminsitração de ambiente, onde devem ser gerenciadas prospecções de negócio em diversos clientes. Deseja-se que cada cliente possa acompanhar as tarefas de prospecção que estão sendo desenvolvidas em sua empresa. Assim, fica claro que todas as empresas clientes devem ter acesso a este projeto genérico de administração. Entretanto, é conveniente (talvez por fins estratégicos de concorrência) que ao logarem no sistema, os clientes somente possam ver as *suas prospecções*, e não as dos outros clientes. Para resolver esta situação, usa-se a chamada segurança horizontal.

A segurança horizontal permite dar acesso ao projeto para todos os usuários ao mesmo tempo que permite restringir o acesso a uma tarefa em específico para um usuário, grupo ou role particular.

No Jira, isso é implementado através do conceito de Security Levels. Um Security Level nada mais é do que um conjunto de usuários, grupos ou roles. Diversos conjuntos desses podem ser agrupados, formando um Security Level Scheme, o qual então é ligado a um projeto em particular. Para saber mais sobre Security Levels, acesse TODO.

No 3PUP, define-se os seguintes Security Levels:

Security Level Scheme: Parceria LM2 (TODO - Revisar e finalizar)

Security Level	Usuários / Grupos / Roles / Custom Field	Descrição
Todos	Project Role (3PUP - Cliente) Project Role (3PUP - Empresa)	É o default e mais aberto nível de permissão horizontal, onde qualquer integrante do projeto pode ver a tarefa.
Cliente	Project Role (3PUP - Empresa) User Custom Field Value (custom field: Visivel para) Group Custom	É o default. Quando utilizado, somente os integrantes da role Empresa podem interagir com as tarefas (conforme seus níveis de permissão no projeto - neste caso, níveis de permissão verticais). Porém, opcionalmente, os campos customizados (Visivel para os grupos e Visivel para os usuarios) podem ser usados em conjunto. Nesse caso, além dos integrantes da role Empresa, os usuários grupos indicados nesses campos poderão ver e interagir com as tarefas, conforme seu nível de permissão no projeto. São justamente esses campos os utilizados para resolver a situação de prospecção de negócios descrita acima, onde especifica-se nesses campos quem são os clientes que podem ter acesso a tarefa.

	Field Value (custom field: Visivel para os grupos)	
$empresa	Group (empresa-$empresa)	Esse nível de permissão horizontal é usado para tarefas que somente devam ser visíveis para integrantes da empresa.
$empresa e $empresaParceira	Group (empresa-$empresa) Group (empresa-$empresaParceira)	

Grupos e Permissões

O controle de acesso em projetos baseados na metodologia 3PUP é definido por *roles* padrões, que são ligadas aos perfis definidos nos projetos.

Na figura abaixo, um exemplo de configuração de permissões no Confluence, que não suporta roles e sim faz a configuração por grupos:

DICA: Para mais informações sobre os níveis de permissões, acesse http://www.atlassian.com/software/jira/docs/latest/project_role_management.html.