

## Capítulo 9: Configurando a Segurança e os Usuários

Traduzido por José Henrique dos Reis

### Configurando a Segurança e os Usuários

O Plone tem um modelo de segurança poderoso e que permite ajustes finos. Ele fornece uma variedade de opções de segurança em todos os níveis, de forma que se cada objeto pode ter um nível de segurança específico para um usuário, papel, grupo, etc.

Para situar esse capítulo no contexto, gostaria de compartilhar com você esta interessante citação:

Segurança é difícil.

Jim Fulton, arquiteto-chefe do Zope.

A segurança do Plone é tão poderosa e detalhada que pode tornar-se bastante difícil para depurar e gerenciar. Mas talvez nenhuma outra coisa seja tão importante em um site Plone quanto implementar a segurança de forma correta. Uma falha de segurança em seu site é provavelmente o erro mais sério que você pode cometer e, por isso, abordarei a segurança do Plone de forma abrangente.

Nesse capítulo abordarei primeiro toda a terminologia e as principais interfaces com as quais seus usuários irão interagir. Então mostrarei como adicionar e editar usuários e grupos utilizando a interface do Plone. Veremos, então, as principais ferramentas e APIs (Application Programming Interfaces) que gerenciam usuários e seus níveis de segurança. Então, abordarei a utilização de ferramentas Python para elaborar scripts que alterem dados dos usuários e suas propriedades. Finalmente, abordarei a segurança do servidor e a como ampliar a autenticação de usuários, com um exemplo detalhado de como incorporar usuários de um servidor LDAP ( Lightweight Directory Access Protocol).

### Gerenciando Usuários

Uma das atividades mais comuns que você realizará como administrador de um site Plone é lidar com os membros do seu site. A administração envolve, geralmente, a recuperação de senhas e a alteração de configurações de membros. Você pode realizar algumas tarefas simples através da Web, mas, com certeza, o melhor amigo de qualquer administrador é uma linguagem de script, como o Python, para fazer alterações em massa. Se você tem uma grande quantidade de usuários, a seção 'Gerenciando Usuários com Scripts', mais à frente, será de seu particular interesse.

### Usuários, Papéis e Grupos

Alguns dos principais conceitos no Plone são: usuários, papéis e grupos. Antes de mostrar como editá-los, abordarei com mais detalhes exatamente o que eles são.

## Usuários

Cada pessoa que visita um site Plone é denominada \*usuário\*. O usuário pode ou não ser autenticado pelo Plone e usuários que não estão autenticados são denominados \*usuários anônimos\*. Usuários que estão autenticados o fazem através de uma conta de usuário existente. Se eles não possuem uma conta, geralmente podem criar sua própria conta.

Usuários anônimos são os usuários de nível mais *baixo*, já que para eles existe uma quantidade maior de restrições. Quando os usuários são autenticados, passam a ter os papéis atribuídos às suas contas. Um usuário é identificado por um identificador conciso, por exemplo, *andym*. Por definição, nenhum usuário é criado para você no Plone, exceto aquele adicionado ao Zope pelo programa de instalação, para permitir sua administração. O nome desse usuário é aquele que você configurou durante a instalação, geralmente *admin*.

## Papéis

Um site Plone tem uma série de papéis; um *papel* é uma classificação lógica de usuários. Ao invés de configurar individualmente as permissões dos usuários, as permissões são atribuídas a cada papel, individualmente. Cada usuário pode ter nenhum ou vários papéis. Por exemplo, um usuário pode ser membro e gerente. Cada papel é identificado por um nome elementar: *Membro*, por exemplo.

Um site Plone tem cinco papéis pré-definidos, divididos em dois grupos: papéis atribuíveis e papéis não-atribuíveis. Papéis atribuíveis são aqueles que você pode dar aos usuários, de forma que, quando eles se autenticarem, terão esse papel. Papéis não-atribuíveis são aqueles que você não pode conceder a um usuário especificamente, mas que existem em um site Plone. Por exemplo, você não pode atribuir o papel anônimo a um usuário.

Os papéis não-atribuíveis são os seguintes:

**Anônimo** (Anonymous): esse é um usuário que não se autenticou no site. Pode ser um usuário que não tem uma conta ou que simplesmente ainda não se autenticou.

**Autenticado** (Authenticated): refere-se a qualquer usuário que esteja autenticado no site, qualquer que seja seu papel. Por definição, um usuário é anônimo ou autenticado; os dois são mutuamente exclusivos. Em razão de fornecer pouca informação sobre o usuário, esse papel não é recomendado para muitas aplicações.

Os papéis atribuíveis são os seguintes:

**Dono** (Owner): esse é um papel especial atribuído aos usuários quando eles criam um objeto. Ele se aplica ao usuário somente para aquele objeto; a informação é armazenada no objeto. Normalmente você não atribui esse papel a um usuário. O Plone faz isso para você.

**Membros** (Members): esse é o papel-padrão atribuído a quem se cadastra no seu site. Qualquer pessoa que se cadastra usando o botão *cadastrar-se* na interface do Plone tem esse papel.

**Revisor (Reviewer):** esse é um usuário com mais permissões que um membro, mas menos que um gerente. Revisores são usuários que podem editar ou revisar conteúdo adicionado por um membro; eles não podem alterar a configuração do site ou uma conta de usuário.

**Gerente (Manager):** gerentes podem fazer quase tudo em um site Plone, então você deve conceder esse papel apenas para desenvolvedores e administradores confiáveis. Um gerente pode apagar ou editar conteúdo, remover usuários, alterar a configuração do site e até mesmo apagar seu site Plone.

## Grupos

O conceito de grupos é diferente do de papéis. Papéis supõem que um usuário tem permissões diferentes de outro com um papel diferente, mas um *grupo* é uma classificação lógica de usuários. Por exemplo, o departamento comercial pode ser um grupo e o departamento de engenharia pode ser outro grupo. Cada usuário pode pertencer a nenhum ou vários grupos. Grupos são opcionais; não é necessário que você os utilize, mas a equipe do Plone entendeu que eles são úteis o bastante e por isso os incorporou.

Desenvolvedores de sites podem usar os grupos da maneira que acharem mais conveniente, como para agrupar um departamento ou uma certa classe de usuários. Para a maioria dos usuários que estão usando o Plone pela primeira vez, recomendo deixar os grupos inalterados; por definição, nenhum grupo é criado para você.

**NOTA** Você implementa grupos usando o Group User Folder (GRUF). Os grupos não são componentes do Zope, mas uma ferramenta extra para o Plone. O GRUF foi desenvolvido e patrocinado pela Ingeniweb.

## A Aba Compartilhamento

Quando abordei a publicação de documentos no Capítulo 3, eu não tratei da aba Compartilhamento porque é uma opção avançada e nem sempre você vai utilizá-la. A aba Compartilhamento é uma ação em *portal\_actions* e caso você não queira que ela seja visualizada, acesse essa ferramenta na Interface de Gerenciamento do Zope (ZMI) e desmarque a opção *visible*. Entretanto, a aba Compartilhamento é muito útil porque permite que, para um objeto Plone, você dê papéis locais diferentes para usuários ou grupos.

Se você adicionou algum conteúdo ao Plone e deseja que outra pessoa possa editá-lo, então é necessário que você dê a ela mais permissões para esse objeto. A isto denominamos *papel local*; permite que você dê a determinados usuários direitos adicionais sobre um item. Se eu crio um documento no Plone, me torno o dono desse documento e ganho certos direitos. Se eu quero que meu colega Rafael colabore na elaboração desse documento antes de sua publicação, então preciso dar mais permissões a Rafael para que ele possa editar esse documento. Para fazer isso, vou até a aba Compartilhamento e dou a Rafael mais permissões.

**NOTA** Você pode atribuir papéis locais a pastas ou documentos. Se você der a um usuário um papel local sobre a pasta, então ele terá esse papel local para

todos os objetos contidos naquela pasta.

A aba Compartilhamento é exibida apenas nos locais em que você tem permissão para alterar o compartilhamento- sua pasta é um desses locais. Clique em *minha pasta* e então clique em *compartilhamento*. A figura 9-1 mostra o formulário da aba Compartilhamento. Ele tem três componentes principais; você pode atribuir um papel local a um usuário nesse objeto, você pode atribuir um papel local a um grupo nesse objeto e você pode ver quem já tem determinados papéis.

The screenshot shows a web interface for managing folder sharing. At the top, there are tabs for 'contents', 'view', 'sharing', and 'properties', with 'sharing' currently active. To the right of the tabs are buttons for 'add new item' and 'state: visible'. The main heading is 'Assign local roles to folder Chapters'. Below this, there is explanatory text about local roles and a search form. The search form includes a 'Search by' dropdown menu set to 'User Name', a 'Search Term' input field, and a 'perform search' button. Below the search form is a section for 'View groups' with a 'view groups' button. The final section is 'Currently assigned local roles in folder Chapters', which shows two user profile pictures and a 'delete selected role(s)' button.

Figura 9-1. Acessando a aba Compartilhamento.

Para encontrar um usuário e atribuir-lhe um papel, informe um nome para pesquisa (*Gavin*, por exemplo) e será exibida uma lista de usuários que atendem ao seu critério de busca; você pode então clicar no usuário e selecionar um papel. Por exemplo, na Figura 9-2, estou dando a Gavin o papel de dono para essa pasta.



Figura 9-2. Atribuindo um papel a um usuário

No exemplo anterior, eu queria atribuir permissões a um determinado usuário, mas isso pode ser trabalhoso quando se trata de uma grande quantidade de usuários...a menos que você os tenha incluído em grupos. Se eu quisesse permitir que toda a equipe de marketing editasse meu documento, poderia fazê-lo. Para ver os grupos disponíveis, clique em *Ver grupos* para abrir uma lista de grupos desse site e, então, você poderá atribuir um papel local ao grupo. Na figura 9-3 eu dou ao grupo Desenvolvimento o papel de dono nessa pasta.

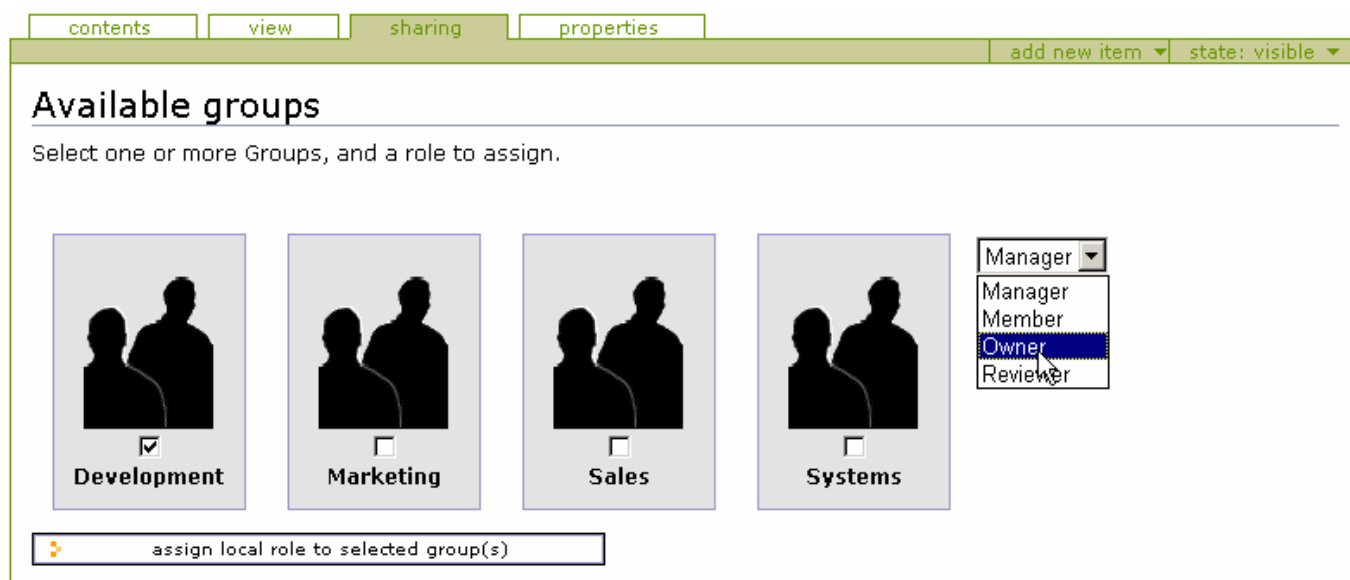


Figura 9-3. Atribuindo um papel a um grupo

Finalmente, na Figura 9-4, você verá quais usuários e grupos têm papéis para esta página e poderá excluí-los, se quiser. Uma vez que você atribui papéis locais a alguém em um objeto você permite que ele acesse a aba Compartilhamento. Dessa forma, não há nada que o impeça de excluir os papéis daquele conteúdo em seu lugar.

## Currently assigned local roles in folder Chapters

These users currently have local roles assigned in this folder:

Assigned Roles Chapters

			
<b>admin</b> Role(s): Owner	<input type="checkbox"/> <b>andym</b> Role(s): Owner	<input type="checkbox"/> <b>gavin</b> Role(s): Owner	<input checked="" type="checkbox"/> <b>Development</b> Role(s): Owner

 delete selected role(s)

Figura 9-4. Vendo e removendo papéis

### Gerenciando através da Web

Por meio da interface do Plone você pode, facilmente, modificar o usuário que foi incluído em determinados grupos, alterar as informações dos usuários, adicionar grupos, e assim por diante. Você pode fazer quase tudo isso por meio do painel de controle do Plone; clique em \*configurações do plone\* e selecione Administração de Usuários e Grupos. Você verá duas abas: usuários e grupos.

Clique na aba Usuários para ter acesso à lista de usuários do sistema. O formulário é auto-explicativo: você pode excluir um usuário, limpar a senha (envia um e-mail avisando o usuário) ou alterar um e-mail, tudo isso nesse formulário, conforme pode ser visto na Figura 9-5.

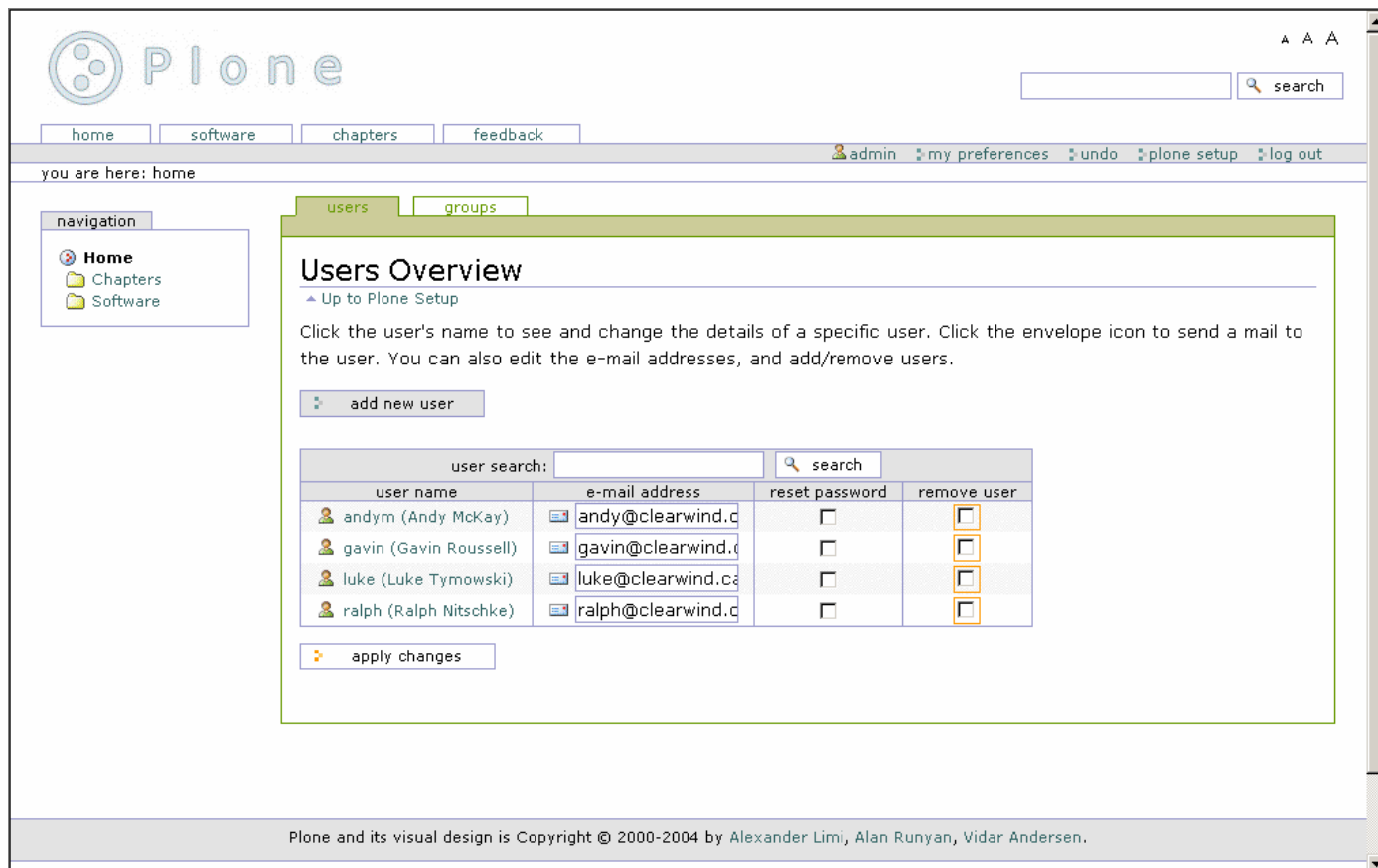


Figure 9-5. Editando usuários

Clicando em um usuário você acessa o formulário de propriedades daquele usuário, faz alterações e, então, clica em Salvar. Para adicionar um novo usuário, clique em \*adicionar novo usuário\*. Será exibido o formulário de registro de usuário que permite que você edite os dados daquele usuário. Como a quantidade de usuários em um site pode se tornar razoavelmente grande, os dados serão tratados em lote, à maneira familiar do Plone. Você pode digitar um texto e realizar uma pesquisa no cadastro de usuários para encontrar todos nomes e endereços de e-mail compatíveis.

Você pode adicionar, modificar e excluir grupos, clicando na aba Grupos. Para adicionar um grupo, clique no botão Adicionar Novo Grupo. Será exibido um formulário; o único campo de preenchimento obrigatório é Título, o qual deve conter um nome curto e significativo para o grupo; geralmente um grupo é diretamente relacionado a negócios ou atividades do site.

Agora que você adicionou um grupo e têm alguns usuários, você pode relacioná-los. Novamente, você pode fazê-lo utilizando o painel de controle do Plone. Você pode clicar em um usuário e incluí-lo em alguns grupos ou colocar usuários naquele grupo.

### Quando usar grupos?

A utilização de grupos é opcional e você pode optar por nunca usá-los. Uma boa forma de utilização de grupos, entretanto, é a criação de \*áreas de trabalho\*. Em um site Plone simples, usuários podem adicionar e modificar conteúdo em suas próprias pastas; cada item nessa pasta é de propriedade da pessoa que o criou. Mas isto não funciona bem quando a quantidade de usuários aumenta muito.

Afinal, o desejável é que poucas pessoas possam editar um documento e compartilhá-lo.

É aí que os grupos e as áreas de trabalho ajudam. Do mesmo jeito que existe uma pasta para os membros que contém todas as pastas de usuários para os membros, há também uma pasta chamada *GroupWorkspaces*. Ela é criada automaticamente quando um grupo é adicionado e, nessa pasta há outra pasta para cada grupo. Assim, se você adicionar um grupo chamado *Marketing*, poderá encontrar uma pasta em *GroupWorkspaces/Marketing*. Qualquer usuário do grupo *Marketing* terá permissão para adicionar, modificar e excluir conteúdo na área de trabalho *Marketing*; em outras palavras, agora você tem uma pasta para esse grupo. Isso equivale a adicionar um grupo e depois atribuir a ele um papel local para aquela pasta.

Esse é apenas um exemplo do quanto um grupo pode ser útil; outro é a utilização de grupos nos workflows. No capítulo anterior eu abordei o workflow e como você pode enviar um e-mail para determinada pessoa quando algo acontece. Se um membro do grupo de *Marketing* adicionar um item, por exemplo, você pode enviar um e-mail para todos os usuários desse grupo, ao invés de enviar para todos os usuários. A seção 'Calculando os Outros Usuários em um Grupo' mostra como fazer isso.

No site do Plone, por exemplo, os usuários estão em grupos de desenvolvimento que são responsáveis por partes do Plone, assim como a equipe de divulgação e a equipe de documentação.

### **Administrando Grupos**

Por meio do painel de controle do Plone, você pode administrar grupos de duas formas. Você pode escolher um usuário e clicar em seus grupos ou escolher um grupo e clicar nos usuários que fazem parte dele. Para incluir um usuário em um grupo, entretanto, vá para a página de pesquisa de usuários, clique em um usuário e clique na aba Grupos, que mostrará os grupos para aquele usuário. Por exemplo, a Figura 9-6 mostra os grupos para o usuário *andym*.

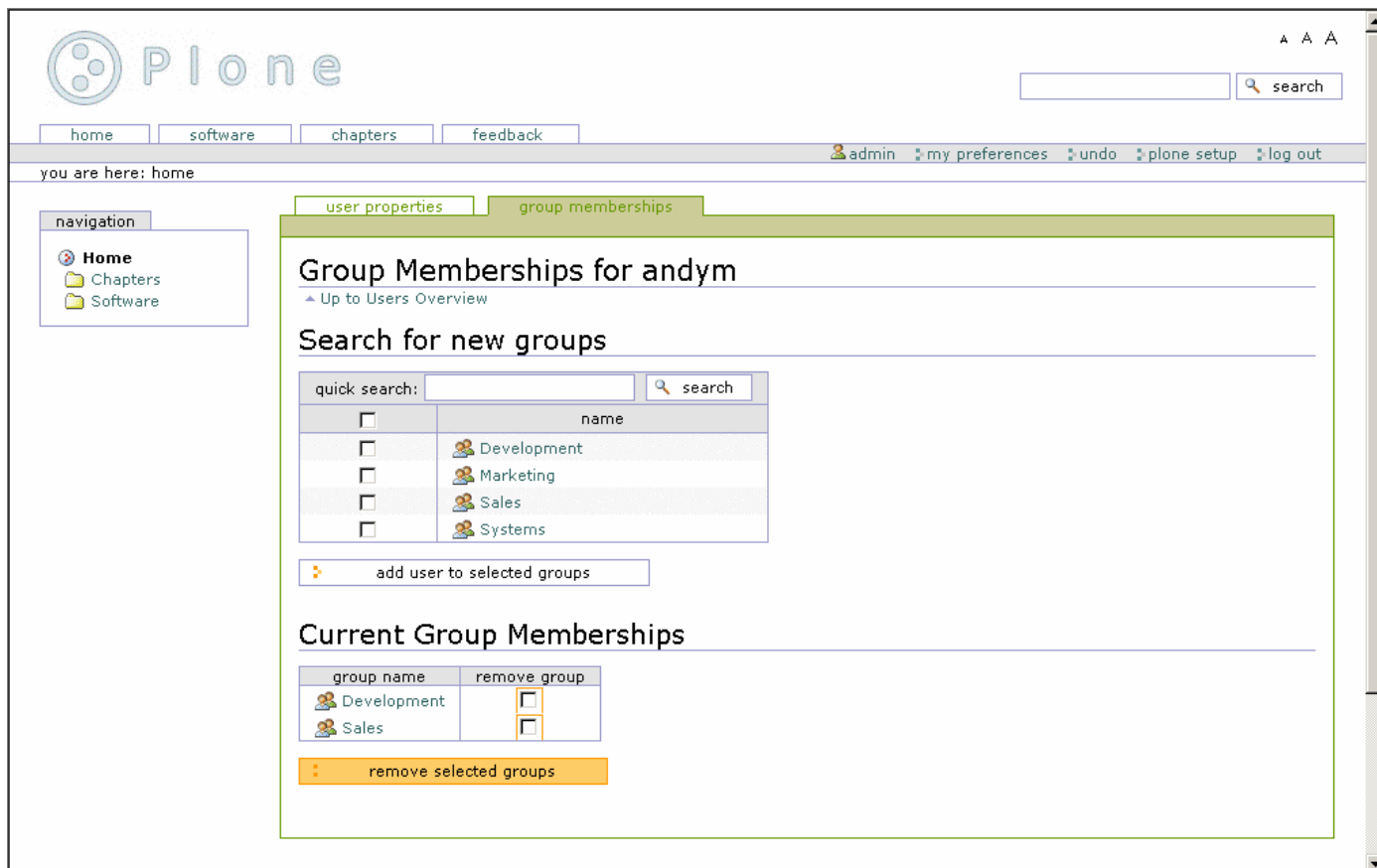


Figure 9-6. Grupos para o usuário

Para incluir o usuário em um novo grupo, clique na caixa de seleção do grupo desejado e então clique em \*adicionar usuário nos grupos selecionados\*.

Da mesma forma, você pode excluir um usuário de um grupo clicando na caixa próxima ao grupo e acionando o botão *excluir os grupos selecionados*. Você verá uma interface similar para administração de grupos se você clicar em \*configurações do plone\*, selecionar Administração de Grupos e Usuários, e clicar em *grupos*. Clique em um grupo, depois em *membros do grupo* para obter uma lista de membros daquele grupo e você poderá incluir e excluir membros nessa tela.

### Atribuindo Papéis aos Grupos

Você viu que usuários podem desempenhar papéis e também que grupos podem ter papéis. Isso pode parecer um pouco estranho, mas imagine, por exemplo, um grupo de supervisores que necessita fazer qualquer coisa em conteúdos adicionados pelos membros de sua equipe. Para fazer isso em um site, eles necessitariam ter o papel de revisor. Para criar um grupo de supervisores, clique em \*configurações do plone\*, selecione Administração de Usuários e Grupos, clique em *grupos* e então clique em *adicionar novo grupo*. Dê a esse grupo o nome **Supervisor** e preencha o formulário. No próximo formulário, você terá a lista de grupos e os papéis associados a eles. Para atribuir o papel de revisor a esse grupo, clique nas caixas de seleção que correspondem ao papel de revisor para esse grupo, conforme mostrado na Figura 9-7.

users groups

## Groups Overview

▲ Up to Plone Setup

Groups are logical collections of users, such as departments and business units. Groups are not directly related to permissions on a global level, you normally use Roles for that - and let certain Groups have a particular role.

add new group

group search:		roles				remove group
group name	member	reviewer	manager	owner		
Development	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Marketing	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Sales	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Supervisor	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Systems	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

apply changes

Figure 9-7. Atribuindo o papel de revisor ao grupo Supervisor

Dessa forma fica fácil dar o papel de revisor aos usuários e agora você pode administrar os revisores por meio da interface do Plone. Além disso, é simples calcular a quantidade de revisores, por meio de programação, porque você pode examinar o grupo e obter uma lista de seus membros.

A idéia de grupos terem papéis é uma pequena mudança de paradigma no desenvolvimento em Zope, já que costumemente papéis eram atribuídos a usuários. Você ainda pode fazer isso no Plone, mas atribuir papéis a grupos é fácil no Plone.

**NOTA** Por definição, quando se verifica a permissão de um usuário para um objeto se leva em conta alguns fatores. Em primeiro lugar, são verificados os papéis atribuídos ao usuário. Depois, são verificados os papéis que um usuário recebe por participar de um ou mais grupos. Isso dá o conjunto total de papéis que um usuário possui.

## Ferramentas para Registro de Usuários

Para que usuários tornem-se membros de seu site, é necessário que antes eles se registrem. Os usuários podem se registrar facilmente clicando no link *cadastrar-se*, localizado no canto superior direito do site Plone. Eu abordei esse assunto detalhadamente no início do Capítulo 3, onde mostrei como usuários podem se registrar em um site. O processo de registro de usuários é simples e direto, mas há algumas opções disponíveis. Esse processo é controlado por três ferramentas principais: *portal\_registration*, *portal\_memberdata* e *portal\_membership*. As próximas seções apresentam essas três ferramentas.

## Portal Registration

A ferramenta *portal\_registration* é um provedor de ações e provê uma ação fundamental no Plone: cadastro. Ao clicar nesse link, será apresentado o formulário de registro. Por definição, qualquer usuário (inclusive anônimo)

que ainda não se autenticou pode clicar nesse link para se cadastrar.

Quando os usuários se registram, utilizando o formulário de cadastro, terão duas opções: ter seu e-mail validado ou não. A única forma de realmente validar um e-mail é enviar um e-mail para o endereço e verificar se uma resposta apropriada é devolvida. Por definição, a validação de e-mail está desativada, assim, quando um usuário se registra, fornece seu nome, e-mail e senha para o Plone. Ele pode se autenticar e usar o site da forma usual. Esse é o formulário que você viu no Capítulo 3. Se a validação de e-mail for ativada, entretanto, os usuários podem fornecer apenas o nome completo, o nome do usuário e o e-mail, conforme pode ser visto na Figura 9-8.

Figura 9-8. Registrando um usuário com a validação de e-mail ativada

Depois de clicar no link contido na mensagem recebida, será apresentada a tela de acesso e o processo de registro continua normalmente.

Para ativar a validação usando a interface do Plone, clique em \*configurações do plone\* e selecione Configurações do Portal. No tópico Política de Senhas, selecione *Gerar e enviar por e-mail a senha inicial dos membros* e clique em Salvar para gravar as alterações.

Se você quiser ver ou modificar o e-mail que é enviado aos usuários, você pode editar a page template que o gera. Você pode encontrar o template clicando em *plone\_skins*, depois em *plone\_templates* e, então, em *registered\_notify\_template*.

\*\*\*Início de coluna lateral\*\*\*

Se você quiser acrescentar quaisquer outras ações para os usuários, antes que eles se registrem, esse é o local ideal para colocá-las. Por exemplo, se você

quiser adicionar uma página que apresenta a política de privacidade, esse é um bom lugar. Para fazer isso, primeiro adicione a página que contenha toda informação que faça parte da política. Seria aconselhável dar um nome apropriado a essa página, como *privacidade.html*, e colocá-la na raiz do seu site Plone.

Na ZMI, vá para *portal\_registration* e adicione uma nova ação com a seguinte informação:

```
Name: Privacidade
Id: privacidade
Action: string: ${portal_url}/privacidade.html
Condition: not: member
Permission: Add portal member
Category: user
Visible: selected
```

Agora você terá o link privacidade apontando para sua página de privacidade, se você não estiver autenticado. Ao atribuir *user* para Category, você assegura que ele aparecerá na sua barra pessoal

**\*Fim de coluna lateral\***

### Portal Member Data

A ferramenta *portal\_memberdata* armazena os dados de cada usuário. Um usuário Plone tem várias opções como: configurações da aparência, data do último acesso, editor de conteúdo, dentre outras. Quando um usuário se cadastra no site, um registro-padrão é criado em *portal\_memberdata*. Você configura as propriedades que serão armazenadas nesse registro com essa ferramenta. Clique em *portal\_memberdata* e selecione Properties para ver o conjunto padrão de propriedades, que são as seguintes:

- email**: endereço de e-mail do usuário.
- portal\_skin**: desatualizado; ignore essa propriedade.
- listed**: exibe o usuário no diretório de *Membros* (lógico). Por definição, está ativado.
- login\_time**: data em que o usuário se autenticou nesta sessão.
- last\_login\_time**: data da última vez que o usuário se autenticou.
- fullname**: nome completo do usuário.
- error\_log\_update**: utilizado pelo formulário de registro de erros; ignore essa propriedade.
- **formtooltips**: Nas versões anteriores do Plone, havia opções para exibir um formulário de ajuda. Não é mais necessário, ignore-o.
- visible\_ids**: Exibe os IDs (ou nomes) dos objetos. Ao ativar essa opção, o

primeiro campo no formulário de edição para cada tipo de conteúdo passa a ser Nome e, com essa alteração, os usuários podem renomear objetos. Por definição, está ativada.

-**wysiwyg\_editor**: esse é o editor utilizado nos formulários.

Você pode adicionar ou remover itens dessa lista por meio da interface do Zope. Entretanto, adicionar ou remover elementos dessa forma não altera automaticamente o formulário que os usuários efetivamente utilizam. No Capítulo 3 você viu que, ao clicar em *\*minhas preferências\**, os usuários podem acessar e alterar muitas dessas propriedades. Se você quiser alterar essas preferências, então terá que adequar o formulário. Os valores contidos nesses campos são os valores-padrão para um usuário recém-registrado; por exemplo, por definição todos os membros são listados na aba Membros, a menos que os usuários indiquem explicitamente o contrário.

Se, por exemplo, você quiser padronizar que todos os membros não serão listados em uma pesquisa, então será necessário alterar a configuração desse formulário. No formulário *portal\_memberdata*, encontre a propriedade *Listed* e desmarque-a. Clique em Save Changes e, a partir daí, todos os novos usuários não serão selecionados.

A ferramenta *portal\_groupdata* contém os dados correspondentes para grupos. As propriedades padrão para os grupos são as seguintes:

- **title**: um título para o grupo
- **description**: uma descrição para o grupo
- **email**: um endereço de e-mail
- **listed**: se o grupo deve ser listado para os usuários

Essas ferramentas armazenam os dados de usuários e grupos em si mesmas e não na pasta *acl\_users* principal. Se você quiser mover informações de usuários entre servidores Plone, então você terá que mover essas ferramentas também; apenas mover a pasta *acl\_users* não basta. Você pode fazer isso importando e exportando essas ferramentas; entretanto, antes de importar no novo site Plone, é necessário apagar a ferramenta existente, senão ocorrerá um erro.

## Portal Membership

A ferramenta *portal\_membership* trabalha com mais algumas propriedades; especificamente ela relaciona os dados dos membros com os membros. Acessar *portal\_membership* a partir da ZMI permite um grande leque de opções, sendo as seguintes as mais importantes:

- **Set members folder**: essa é a pasta onde são colocadas as pastas dos membros. Essa pasta deve existir. Por definição, seu valor é *Member*.

- **Control creation of member areas**: por definição, é criada uma área para cada usuário quando ele se registra. Entretanto, essa criação é opcional. Clique em *Turn folder creation off* para desativá-la. O padrão é estar ativado.

Na aba Actions você encontrará várias ações relativas aos usuários quando eles estão autenticados, como *my favorites*, *my preferences*, dentre outras. Todas elas têm a categoria *user* de forma que as ações aparecerão no canto superior direito.

A ferramenta *portal\_groups* apresenta opções similares a *portal\_membership*, mas para grupos. Da mesma forma, quando um grupo é criado, um espaço de trabalho é criado para o grupo, onde todos os membros daquele grupo podem adicionar e editar conteúdo.

## APIs úteis

A ferramenta *portal\_membership* contém o conjunto mais utilizado de funções de API. Frequentemente você desejar obter informações-chave como: que usuário está autenticado no momento, se o usuário é anônimo, dentre outras. A ferramenta *portal\_membership* coloca esses métodos a seu dispor, sendo os seguintes os mais importantes:

- `isAnonymousUser()`: retorna *verdadeiro* se o usuário é anônimo.
- `getAuthenticatedMember()`: retorna o usuário atualmente autenticado, acrescido com as propriedades de *portal\_metadata*. Se nenhum usuário estiver autenticado, retorna um usuário especial *nobody* com mapeamentos nulos para as propriedades de *portal\_metadata*.
- `listMemberIds()`: retorna os IDs de todos os usuários.
- `listMembers()`: retorna todos os objectos usuário.
- `getMemberById(id)`: retorna o objeto usuário para um determinado ID.
- `getHomeFolder(id=None)`: retorna a pasta pessoal para um determinado ID. O ID é opcional e, caso se não informado, retorna a pasta pessoal do usuário atual.
- `getHomeUrl(id=None)`: retorna uma URL para a pasta pessoal do membro. O ID é opcional e, se não fornecido, retorna a URL da pasta pessoal do usuário atual.

O usuário retornado por essas funções é 'empacotado' nos dados da ferramenta *portal\_memberdata*, de forma que as propriedades são atributos do objeto usuário. Esse, por exemplo, é um pequeno objeto Script (Python) que obtém o endereço de email do usuário *andy*:

```
::
```

```
##parameters=
u = context.portal_membership.getMemberById("andy")
return u.email
```

## Autenticação por Cookie

Por definição, o Plone utiliza autenticação por cookie para seus usuários; dessa forma os usuários devem ter a opção de cookies ativada em seus browsers para se autenticar. Essa autenticação é realizada em um site Plone pelo objeto *cookie\_authentication*, que contém as funcionalidades necessárias para que os usuários se autenticem. Se você deseja utilizar a autenticação Hypertext Transfer Protocol (HTTP), então você pode simplesmente remover esse objeto; entretanto, eu não recomendo que o faça, porque a autenticação HTTP não é boa para muitos sites.

Esse objeto contém os seguintes itens que você pode editar usando a ZMI:

- **Authentication cookie name:** esse é o nome do cookie que será utilizado para armazenar a autenticação do usuário. Isso é feito por meio do armazenamento de um token para o usuário, que preserva a autenticação do usuário. O padrão é *\_\_ac*.

- **User name form variable:** esse é o nome da variável do formulário de autenticação que contém o nome do usuário. O padrão é *\_\_ac\_name*.

- **User password form variable:** esse é o nome da variável do formulário de autenticação que contém a senha do usuário. O padrão é *\_\_ac\_password*.

- **User name persistence form variable:** esse é o nome da variável do formulário de autenticação que contém o token de persistência. O padrão é *\_\_ac\_persistent*.

- **Login page ID:** se um usuário necessita se autenticar, essa é página que será apresentada. O padrão é *require\_login*.

- **Logout page ID:** se um usuário desejar deixar de ser autenticado, será apresentada uma página com uma mensagem. A página é esse ID. O padrão é *logged\_out*.

- **Failed authorization page ID:** quando a autenticação falha, essa é a página que será mostrada. Por padrão, fica em branco, já que o Plone faz algo diferente.

- **Use cookie paths to limit scope:** faz com que o cookie contenha autenticação para a pasta atual e todas as pastas abaixo dela. Deixe em branco (padrão) de forma que o usuário se autentique para todo o site, independente de onde tenha clicado *acessar*.

Para alterar o cookie que está sendo usado, ao invés de usar o padrão, basta alterar os dados desse formulário e clicar em Save Changes. Entretanto, gostaria de alertar que se você alterar o nome do cookie, todos os cookies existentes nos computadores dos usuários serão ignorados e eles terão que se autenticar novamente. Se você quiser uma página de acesso diferente, então você pode customizar a page template *require\_login* ou alterar o valor dessa variável.

## A Pasta de Usuários

Você pode ter acesso à pasta de usuários de um site Plone clicando na pasta `acl_users` na ZMI. Isso abrirá a interface do Group User Folder (GRUF), que oferecerá uma variedade de opções.

A interface do GRUF é bastante similar à opção de administração de usuários existente no painel de controle do Plone. Você pode adicionar e editar usuários e grupos por meio de uma interface concisa. Ao clicar em Users e Groups será permitido a você editar esses itens. Se você clicar na aba Contents, poderá escolher entre Groups ou Users; clique em Users e, em seguida, clique em `acl_users`. Finalmente você terá acesso à pasta de usuários real para um usuário. Ela se assemelha à pasta de usuários padrão. Você verá uma lista de usuários e, para editar um usuário, apenas clique no nome do usuário, como na Figura 9-9.



Figura 9-9. Editando os dados do usuário

A partir daqui você pode alterar a senha do usuário ou seus papéis. Note que, nesse ponto, o grupo Supervisor é representado como um papel para assegurar que não haverá colisão de nomes. O nome foi alterado para `group_Supervisor`. Se você quiser que esse usuário seja membro desse grupo, é possível fazê-lo aqui. Não há muito que fazer aqui que não possa ser feito em níveis mais elevados, então não desça até esse nível a não ser que tenha que fazer algo como alterar uma senha ou configurar um domínio.

## Atribuindo Permissões

Até agora abordamos usuários, papéis e grupos, mas há mais; o nível mais baixo de opções de segurança é a permissão. Como o nome sugere, dar ao usuário uma \*permissão\* significa dar a ele a capacidade para fazer algo, como ver um

objeto, adicionar um documento, obter a lista de conteúdo de uma pasta, e por aí vai. Cada permissão é identificada de forma única por um nome significativo como *View*, *Add portal content* ou *List folder contents*.

Permissões não são concedidas a um usuário individual, mas para um papel. Cada papel recebe permissões particulares, e então o usuário recebe esses papéis particulares. Você encontra todas as opções de segurança do Zope na aba Security da ZMI. Isso engloba: o site Plone, a pasta raiz do Zope, todos os objetos e conteúdo de um site Plone e as configurações de aparência. Quando você clica na aba Security, são exibidas todas as permissões e papéis, mapeados em forma de tabela, conforme a Figura 9-10.

Plone Site at [/Plone](#) [Help!](#)

The listing below shows the current security settings for this item. Permissions are rows and roles are columns. Checkboxes are used to indicate where roles are assigned permissions. You can also assign [local roles](#) to users, which give users extra roles in the context of this object and its subobjects.

When a role is assigned to a permission, users with the given role will be able to perform tasks associated with the permission on this item. When the *Acquire permission settings* checkbox is selected then the containing objects's permission settings are used. Note: the acquired permission settings may be augmented by selecting Roles for a permission in addition to selecting to acquire permissions.

Permission	Roles					
	Anonymous	Authenticated	Manager	Member	Owner	Reviewer
<b>Acquire permission settings?</b>						
<input checked="" type="checkbox"/> Access Transient Objects	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Access arbitrary user session data	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Access contents information	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Access future portal content	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Access inactive portal content	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Access session data	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Add Accelerated HTTP Cache Managers	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Add Archetypes Tools	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Add BTreeFolder2s	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Add Browser Id Manager	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<b>Acquire?</b>	Anonymous	Authenticated	Manager	Member	Owner	Reviewer
<input checked="" type="checkbox"/> Add CMF Action Icons Tools	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> Add CMF Caching Policy Managers	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Figura 9-10. Configurações de segurança

É possível ver na Figura 9-10 que esse objeto tem uma série de opções de segurança, exibidas como uma grade de caixas de seleção. À esquerda ficam as permissões em ordem alfabética e no topo ficam os papéis, também em ordem alfabética. Essa página é um tanto grande e complicada e por isso há outras formas de visualização. Clique na permissão para ver todos os papéis que detém essa permissão; a Figura 9-11, por exemplo, mostra a configuração da permissão *Access future portal content*.

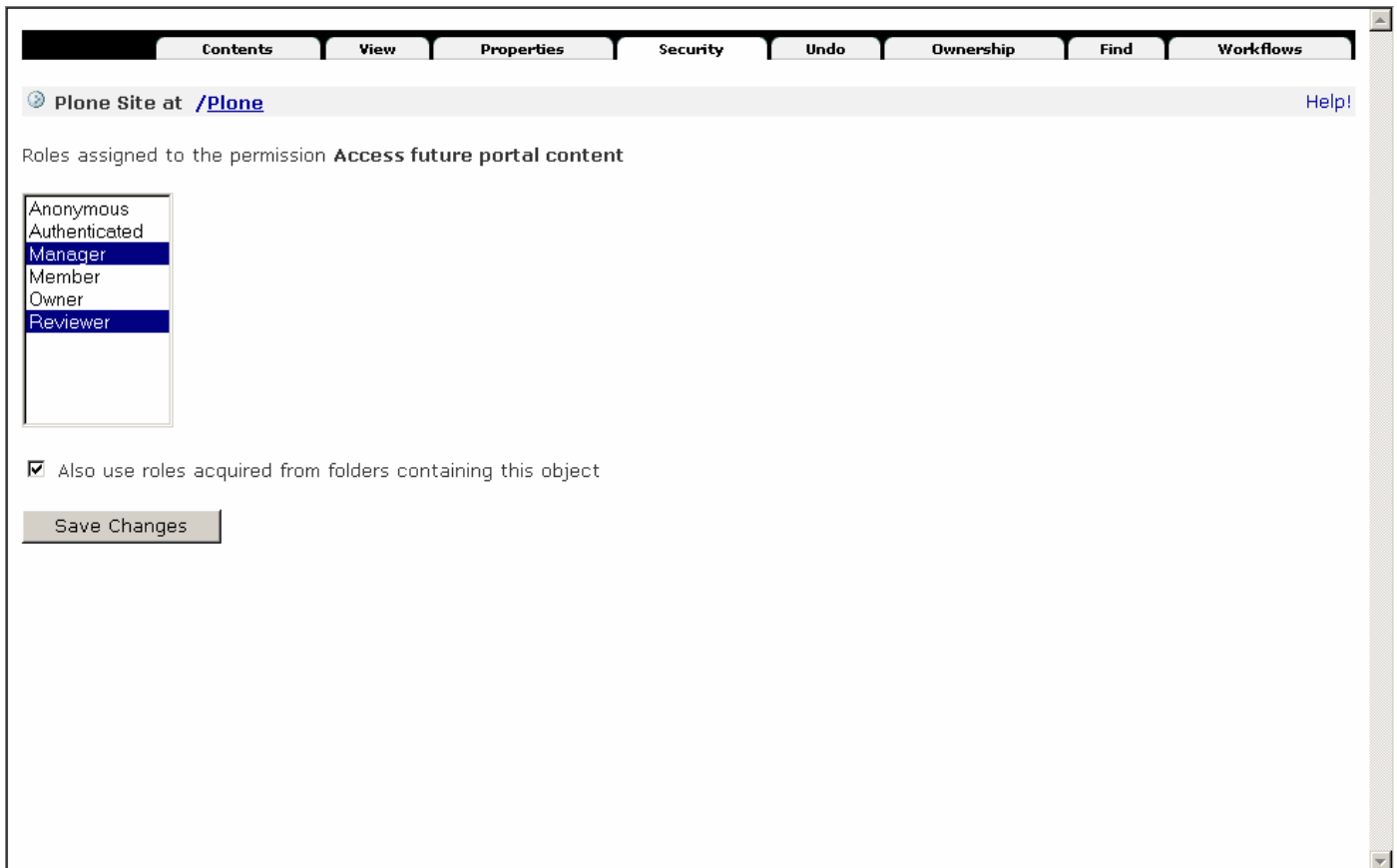


Figura 9-11. Configuração de uma permissão

E você pode clicar no papel para obter todas as opções configuradas para aquele papel, muito mais simples do que uma longa lista, conforme Figura 9-12.

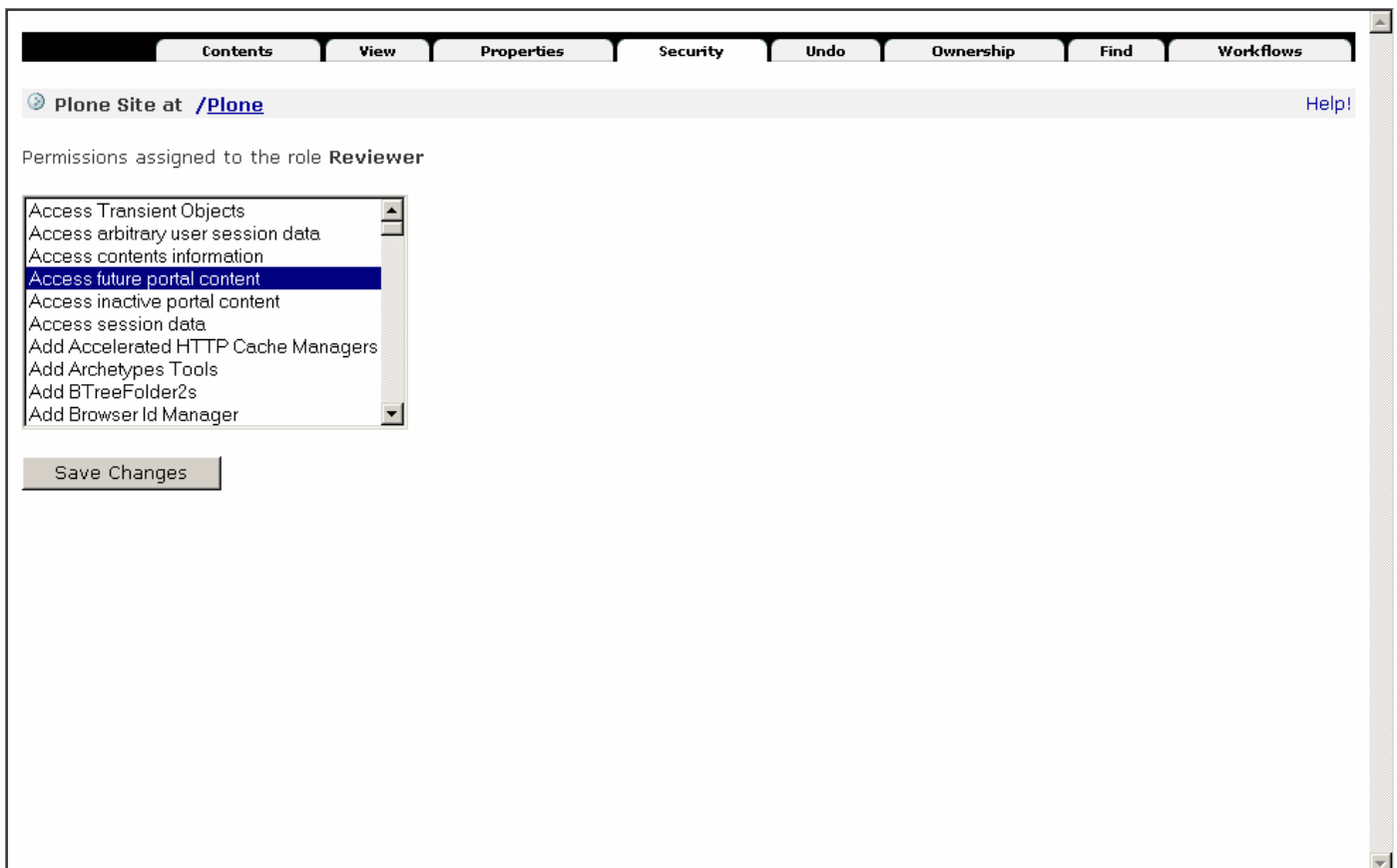


Figura 9-12. Opções para o papel reviewer

Tudo se resume a clicar nas caixas de seleção para as permissões que você deseja configurar ou selecionar as opções na lista de seleção e clicar em Save. Quando a opção *Acquire Permission* está ativada, as opções de segurança para essa permissão serão adquiridas; quando estiver desativada, as permissões não serão adquiridas. \*Aquisição\* (Acquisition) é a habilidade de um objeto pesquisar a hierarquia de objetos para encontrar permissões e então combiná-las para obter a permissão geral.

**NOTA** A página de permissões ativará para você as opções de segurança para o usuário manager; deixar o usuário manager sem permissões pode ser um desastre, por isso é bom que esta opção esteja ativada.

Agora dê uma olhada na permissão *Access contents information*. Na ZMI, vá para a raiz do site Plone e clique na aba *Security*. Na configuração padrão para essa permissão não há papéis disponíveis, isto é, a configuração pra cada usuário está em branco. Entretanto, a opção *Acquire Settings* está ativada, indicando que você deve olhar o objetos superiores na hierarquia para determinar as permissões para esse objeto. Vá para a pasta raiz do Zope e clique na aba *Security*. Será mostrada a lista de permissões para a pasta raiz, e com certeza haverá algumas configurações para a permissão *Access contents information* nessa pasta; isto é, os papéis *anonymous* e *manager* têm essa permissão.

Já que as permissões são adquiridas, todas as subpastas também adquirirão essas permissões configuradas. Isso significa que o site Plone e todos os objetos no site Plone terão essas permissões. Dessa forma, se você deseja atribuir uma permissão de segurança para o site como um todo, basta configurar a permissão na raiz do Plone e a maioria dos objetos a adquirirão.

**NOTA** A exceção são os objetos de workflow, os quais desativam a aquisição. Isso é abordado na seção '*Segurança e Workflow*' mais à frente nesse capítulo.

Você pode configurar as permissões para qualquer objeto no Zope por meio da ZMI. Isso pode ser feito na raiz do Zope, no site Plone, em uma pasta como a pasta *Members* ou em um objeto qualquer. Cada objeto tem seu próprio conjunto de permissões, mas nem todos os objetos têm as mesmas opções de permissões. Por exemplo, a permissão *Add...* existe em todas as pastas. Mas, uma vez que essas permissões não fazem sentido em objetos que não são pastas (por definição um objeto deve ser uma pasta para ter itens adicionados a ele), elas não estão presentes nesses objetos.

Qualquer produto ou programa Python em seu site Zope pode definir sua própria permissão de segurança, assim pode ser difícil definir com exatidão o que uma permissão deixa você fazer. A tabela 9-1 descreve algumas das principais permissões e o que elas significam.

Tabela 9-1. Permissões Plone mais comuns

**\*\*Permissão      Descrição\*\***

*Access contents information*      Permite o acesso a um objeto, sem necessariamente exibir o objeto. Por exemplo, um usuário pode querer ver o

título do objeto em uma lista de resultados, mesmo que não possa exibir o conteúdo do arquivo.

**\*Add...\*** Há diversas permissões para adicionar, cada uma relacionada ao tipo de objeto que o usuário gostaria de adicionar. Para um site Plone normal, todas as permissões são agrupadas em *Add portal content*.

*Add portal member* Permite o cadastramento de usuários no site Plone e a criação de uma conta de usuário.

*Copy or Move* Dá o direito de copiar ou mover um objeto. Mesmo que os usuários tenham esse direito, necessitam ainda de ter permissão para colar o objeto no destino.

*Delete objects* Dá o direito de apagar um objeto. No Zope padrão, essa permissão é ativada na pasta; no Plone a verificação é feita em cada objeto.

*List folder contents* Lista o conteúdo de uma pasta; não verifica se você tem o direito de ver o objeto listado.

*List portal members* Dá o direito de ver a lista de membros do site e fazer pesquisas nessa lista.

*Modify portal content* Essa é a permissão “toda-poderosa” para fazer qualquer modificação em um objeto, como: alterar o conteúdo, suas palavras-chave, ou outras propriedades. Essa permissão se aplica a quase todos os objetos.

*Set own password* Dá o direito de alterar sua senha em um site Plone.

*Set own properties* Dá o direito de alterar suas propriedades em um site Plone.

*View* Permite a um usuário ver o objeto em questão. *View* não significa ver apenas o código HTML mas também via File Transfer Protocol (FTP), WebDAV, e outras formas de acesso.

## Adicionando um Papel

Ao atribuir papéis a usuários é necessário definir um conjunto compatível de permissões para cada papel de forma que o agrupamento de permissões faça sentido. Isso nem sempre é possível. De vez em quando um determinado usuário necessita de algo diferente de outros usuários similares.

Entretanto, do ponto de vista do desenvolvedor, quanto em menor quantidade e mais simples você mantiver os papéis, mais fácil será. Não é tão complicado, mas aquela vontade inicial de criar um papel para cada opção de segurança é, sem dúvida, má idéia. Você se verá rapidamente imerso em confusão. Eu aconselho que você deixe a quantidade de papéis a menor possível e os faça genéricos para todo o site.

Para adicionar um papel, vá para a pasta raiz do Plone, clique na aba Security e role a tela até o fim da página (é longe). No fim da página há um formulário simples para adicionar mais papéis ou remover um papel. Adicione o nome do

novo papel e clique em Add Role.

### **Executando Tarefas Comuns**

Você pode configurar fácil e rapidamente algumas opções de segurança para executar tarefas rotineiras. Antes que você faça alterações na configuração de segurança, aconselho-o a fazer uma cópia de segurança do site Plone. Mostro como se faz isso no Capítulo 14.

### **Impedindo que Usuários se Registrem em seu Site**

Para impedir que usuários se registrem em seu site, você deve configurar a permissão Add portal member na raiz do Zope para usuários anônimos. Você pode desativar essa opção para usuários anônimos nesse local ou então ir para seu Plone site e desativar a opção Acquire Permission.

### **Impedindo que Usuários Pesquisem seu Site**

Para impedir que os usuários façam pesquisas em seu site, você deve configurar a permissão *Search ZCatalog* para usuários anônimos na raiz do seu site Plone. Dessa forma, altere lá a permissão, desativando a opção para Anonymous ou outro usuário qualquer.

### **Impedindo que Usuários Anônimos Acessem seu Site**

Ah, bem, impedir que usuários anônimos acessem seu site exige alguns truques, porque é complicado remover acessos anônimos ao site completamente; os usuários ainda precisam acessar seu site para poder se autenticar! O que você realmente deseja, nesse caso, é poder restringir o acesso ao seu conteúdo. Você pode fazer isso restringindo as permissões no seu workflow.

### **Segurança e Workflow**

Como vimos no Capítulo 7, o workflow gerencia a segurança de cada objeto no workflow. Isso é feito por meio de alteração das permissões existentes em um objeto. Eu acabei de mostrar como ver as configurações de segurança para cada objeto, assim você pode agora ver como as configurações de segurança do objeto em um estado podem ser diferentes das configurações do objeto em outro estado. Se você clicar em *portal\_workflow*, selecionar a aba Contents, clicar em *plone\_workflow*, e então selecionar a aba States verá todos os estados disponíveis. Clique em um estado, selecione Permissions e você verá as permissões para aquele estado, conforme a Figura 9-13.

Workflow State at [/Plone/portal\\_workflow/plone\\_workflow/states/published](/Plone/portal_workflow/plone_workflow/states/published)

When objects are in this state they will take on the role to permission mappings defined below. Only the [permissions managed by this workflow](#) are shown.

Acquire permission settings?	Permission	Roles					
		Anonymous	Authenticated	Manager	Member	Owner	Reviewer
<input checked="" type="checkbox"/>	Access contents information	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Change portal events	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Modify portal content	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	View	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Figura 9-13. Permissões para o estado published

Como você pode ver, quando um objeto passa para o estado published, usuários anônimos terão as permissões *Access contents information* e *View*. Isso significa que qualquer um pode ver o conteúdo. Observe que os membros e proprietários não podem editar seu próprio conteúdo, porque eles não têm essa permissão. As permissões aplicadas pelo workflow constam da aba Permissions, onde você pode configurar todas as permissões que serão gerenciadas pelo workflow.

Depois que você alterar as configurações de segurança, é necessário ir à ferramenta *plone\_workflow* e clicar em *Update security settings*, senão a segurança dos objetos e do workflow serão diferentes.

**NOTA** Uma vez que as permissões mudam quando um objeto sofre uma transição, quaisquer outras alterações de permissões que você tenha feito no objeto usando a ZMI são removidas se (e somente se) essas permissões são gerenciadas pelo workflow. Por isso, você deve sempre resistir à vontade de fazer ajustes na segurança de tipos de conteúdos pela ZMI; opte por alterar o objeto no site Plone e o workflow.

## Proteções

Todas as transições têm em si uma proteção que permite ao administrador selecionar as permissões necessárias antes que usuário possa executar a transição. Ao verificar se um usuário pode efetuar a transição, serão executados os seguintes passos, nessa ordem: verificação de permissões, verificação de papéis e verificação da expressão. Se todas essas verificações forem bem sucedidas, então ocorrerá a transição.

As configurações para a proteção são as seguintes:

- **Permission:** lista de todas as permissões aceitas, separadas por ponto-e-vírgula (;)-por exemplo, *Review portal content; Modify portal content*.

- **Roles:** lista dos papéis aceitos para essa transição, separados por ponto-e-vírgula (por exemplo, *Manager; Reviewer*).

- **Expression:** essa é uma expressão Template Attribute Language Expression Syntax (TALES) de workflow que permite inserir uma condição personalizada. Por exemplo, a seguinte transição somente ocorrerá se isso estiver em uma pasta chamada *Members*; não é propriamente uma permissão, mas é um truque interessante:

```
python: if 'Members' in state_object.getPhysicalPath()
```

**NOTA** *getPhysicalPath* é um método de todos os objetos Zope que retorna a localização dentro da hierarquia de objetos do Zope, ignorando qualquer hospedagem virtual que possa existir.

## Papéis Proxy

No capítulo anterior eu apresentei alguns métodos para notificar os usuários e mover o conteúdo no site quando o conteúdo tem seu estado de workflow alterado. Quando isso acontece, o script é executado assim que o usuário realiza uma transação de workflow. Nesse caso, seu script pode fazer algo que seu usuário pode ou não ter permissão para fazer. Por exemplo, você pode não permitir a um usuário adicionar coisas a uma pasta chamada *public*, exceto para os casos de workflow. Isso é um problema; pois você precisa assegurar que o script seja executado com um papel superior.

Um *papel proxy* é algo com que seus usuários não irão interagir e muito menos saber que existe, mas é um método para você resolver esse problema. Por exemplo, digamos que você queira que um usuário possa selecionar um usuário dentre aqueles existentes no site. Você não quer permitir que o usuário possa ver todos os usuários mas apenas os usuários nesse contexto particular. Para executar o script, o usuário necessitará ter a permissão *List portal members* para obter uma lista dos membros, mas você não deseja dá-la a usuários anônimos.

O script que executa esse comando necessitará de um papel proxy superior, provavelmente *Member*. Para fazer isso, vá para o script na ZMI, clique na aba Proxy, e clique em Member. Se esse script está no sistema de arquivos, essa informação pode ser adicionada ao arquivo metadata. Por exemplo, o arquivo *.metadata* deverá ter a seguinte linha: *proxy = Member*. Agora esse script será executado como um membro, resolvendo seu problema de segurança!

## Scripts para Usuários

Então você tem punhado de usuários em seu site Plone... agora você precisa de alguns scripts para auxiliar na administração desses usuários. Ao ultrapassar a casa de algumas centenas de usuários, pode ficar bastante difícil fazer alterações por meio da Web, assim as seções seguintes dão alguns exemplos de scripts que realizam algumas tarefas importantes.

## Registrando Usuários em Massa

Se você tem um grande número de usuários para registrar, então você precisará de um script para importá-los. Esses usuários podem ser de qualquer sistema que você esteja migrando para o Plone. Entretanto, se você já tem usuários em uma fonte externa, como LDAP, banco de dados relacional ou outra fonte, você pode integrar-se diretamente com essa fonte.

Por enquanto, imagine um arquivo de usuários, com campos separados por vírgula, com os seguintes dados: nome de usuário, nome completo, e-mail e grupos. Nesse exemplo, você percorrerá essa lista, adicionará cada usuário com essas informações e alterará suas propriedades de forma que eles tenham as configurações corretas. O arquivo `.csv` deverá se parecer com o seguinte:

```
"Nome de Usuário", "Nome Completo", "Email", "Grupos"
"Andy", "Andy Mckay", "andy@enfoldsystems.com", "Systems,Sales,Development"
...
```

Um arquivo `.csv` contém dados separados por vírgula e pode ser criado ou editado na maioria dos programas de planilha como Microsoft Excel ou OpenOffice.org. Você poderá então exportar o arquivo como um arquivo com dados separados por vírgulas e importá-lo no Plone. Como isso envolve a utilização de métodos que são restritos, será necessário utilizar um `external method`:

```
# Um external method para importar usuários
import csv

# caminho completo para o arquivo csv
fileName = "/var/zope.zeo/Extensions/test.csv"

def importUsers(self):
    reader = csv.reader(open(fileName, "r"))
    pr = self.portal_registration
    pg = self.portal_groups
    out = []

    # se o seu arquivo csv contém uma linha de cabeçalho que
    # explica o conteúdo de cada coluna
    ignoreLine = 1
```

Esse é apenas o código de configuração; ou seja, define todas as variáveis que serão usadas no script. No início, o módulo `csv` é importado; esse módulo vem com o Python 2.3 e possibilita o processamento rápido de arquivos `.csv`. O arquivo `.csv` está na variável `fileName`, que contém o caminho completo para o arquivo; se você utilizar um caminho relativo, o Plone pode acabar procurando no lugar errado. Como você já viu antes, `self` é passado para o método, e a partir dele você pode obter as duas ferramentas necessárias: `portal_registration` que fornece o acesso à API de registro e `portal_groups` que dá acesso à API de grupos:

```

for row in reader:
    if ignoreLine:
        ignoreLine = 0
        continue

    # verifica se temos exatamente 4 itens
    assert len(row) == 4
    id, name, email, groups = row
    groups = groups.split(,)

    # cria uma senha
    password = pr.generatePassword()

```

Depois, lemos cada linha e obtemos o ID, nome, e-mail e grupos. Então, geramos uma senha aleatória chamando *generatePassword*. Uma senha aleatória de seis caracteres composta de caracteres em caixa alta, caixa baixa e números é gerada. Se você desejar derivar o ID ou a senha das informações existentes, como o nome de usuário ou o e-mail, então essa é a oportunidade de fazê-lo. Nesse caso, eu incluí cada grupo no mesmo campo, separados por vírgula (por exemplo, "Vendas,Marketing"). Portanto, é necessário separá-los em uma lista de nomes individuais, dessa forma:

```

try:
    # adiciona um membro
    pr.addMember(id = id,
                 password = password,
                 roles = ["Member",],
                 properties = {
                     'fullname': name,
                     'username': id,
                     'email': email,
                 }
    )

    # grupos são separados por vírgulas
    for groupId in :
        group = pg.getGroupById(groupId)
        group.addMember(id)

    out.append("Usuário adicionado %s" % id)

except ValueError, msg:
    # informa a razão de não inclusão de determinado usuário
    out.append("Não incluído %s, motivo: %s" % (id, msg))

# retorna alguma coisa
return "\n".join(out)

```

Já que você tem toda as informações do usuário que necessita, pode realizar o registro efetivo. Para fazer isso, chame a função *addMember*, pertencente a *portal\_registration*, que registra o usuário. Um dicionário com pares chave/valor, como e-mail e nome, é passado para a função. Então, para cada grupo, é chamado *getGroupById* para obter o grupo e chamar *addMember* para o grupo. Como o nome sugere, isso registrará o usuário no grupo. A última linha

trata de imprimir alguma coisa para a pessoa que está realizando a importação.

Para executar isso em seu site, você terá que colocá-lo no diretório *Extensions* do seu servidor Plone e chamá-lo de *import\_users\_with\_groups.py*. Em seguida, será necessário que você adicione manualmente os grupos que existirão no seu site; esse script não cria os grupos para você. Então, prepare o arquivo *.csv*; se você tiver seus usuários armazenados em algum outro sistema, terá que encontrar uma maneira de exportá-los para esse formato. Altere o nome do arquivo no script para apontar para seu arquivo. Em seguida, adicione um *external method* em seu Plone site, com os seguintes valores:

- **ID:** *import\_users\_with\_groups*
- **Module name:** *import\_users\_with\_groups*
- **Function name:** *importUsers*

Após adicionar o *external method*, clique na aba *Test* para executar o método, e você obterá o resultado!

### Alterando Propriedades de Usuários

Se você instalar um novo produto ou fizer uma nova configuração, poderá ser necessário alterar por atacado os metadados dos usuários. Por exemplo, se você instalar um novo editor WYSIWYG e quiser ele seja o padrão para todos os usuários, então duas coisas devem acontecer:

- Altere a configuração padrão para cada novo usuário. Para fazer isso, clique em *portal\_metadata* e selecione a aba *Properties*. Informe o padrão e todos os usuários novos obterão esse valor.

- Altere as configurações para cada usuário existente, o que só poderá ser feito com o seguinte *external method*:

```
def fixUsers(self):
    pm = self.portal_membership
    members = pm.listMemberIds()

    out = []
    for member in members:
        # obtém um membro existente
        m = pm.getMemberById(member)
        # obtém a propriedade editor desse membro
        p = m.getProperty(wysiwyg_editor, None)

        out.append("%s %s" % (p, member))
        if p is not None and p != 'Epoz':
            m.setMemberProperties({'wysiwyg_editor': Epoz,})
            out.append("Propriedade alterada para %s" % member)
    return "\n".join(out)
```

Coloque esse programa em um módulo Python no diretório *Extensions* de sua instância Plone. Chame o módulo de *fixUserScript.py*. Então, na ZMI, adicione um

external method com os seguintes parâmetros:

- ID: *fixUsers*
- Module name: *fixUserScript*
- Function name: *fixUsers*

Clique na aba Test para rodar o script. Ele percorrerá todos os membros do seu site e definirá o valor de editor WYSIWYG para "Epoz". O script faz isso obtendo, primeiro, a lista de todos os membros; há um método em *portal\_membership* chamado *listMemberIds* que faz isso para você. Para cada membro, ele examina a propriedade usada pelo Plone para determinar o editor (nesse caso, a propriedade *wysiwyg\_editor*). Se essa propriedade não for "Epoz", então é chamada *setMemberProperties* para alterá-la.

Essa é uma maneira conveniente de percorrer a lista de todos os membros. Então, usando os métodos *getProperty* e *setMemberProperties*, você pode examinar ou alterar qualquer propriedade que um usuário possa ter.

### Calculando os Outros Usuários em um Grupo

Discuti anteriormente sobre a possibilidade de enviar um e-mail para todas as pessoas de um grupo de trabalho de um objeto. Você pode adicionar isso ao workflow, mas precisará de um script para essa tarefa. Esse exemplo utiliza algumas funções para chegar aos usuários. A seguir apresento o script *getGroupUsers* que, a partir de um objeto, retorna uma lista de usuários:

```
##parameters=object=None
# object é o objeto a partir do qual procuraremos todos os membros do mesmo
grupo
users = []
# obtém o criador
userName = object.Creator()
user = context.portal_membership.getMemberById(userName)
pg = context.portal_groups

# percorre os grupos a que o usuário pertence
for group in user.getGroups():
    group = pg.getGroupById(group)

    # percorre a lista de usuários em cada um desses grupos
    for user in group.getGroupUsers():
        if user not in users and user != userName:
            users.append(user)

return users
```

Nesse script, é passado um objeto, então é necessário encontrar o criador dele, chamando o método *Creator*. Uma vez obtido o usuário, você pode chamar *getGroups*, e um método do objeto usuário lista todos os nomes de todos os grupos em que em um usuário está. Depois disso, você obtém cada um desses grupos e, dessa lista, você obtém os nomes de usuários para um grupo. Então,

finalmente, você tem cada nome de usuário. Para cada um desses usuários, você precisa de usuários que não são duplicados ou que não são o usuário que fez a alteração no objeto. A lista de usuários conterá todos os outros usuários que estão nos mesmos grupos que a pessoa que é dona do objeto.

Você pode inserir esse código no script de notificação de e-mail para workflow do Capítulo 7 para torná-lo mais versátil. Por exemplo, para o script de notificação por e-mail do workflow, você deve se lembrar que fez o seguinte:

```
for user in mship.listMembers():
    if "Reviewer" in mship.getMemberById(user.id).getRoles():
```

Isso percorre todos os usuários e verifica se eles têm o papel associado. O script anterior foi chamado *getGroupUsers* e colocado na pasta *portal\_skins/custom*. Isso significa que você pode acessá-lo através do namespace do contexto por meio de aquisição; em resumo, *context.getGroupUsers(object)* retornará os usuários:

```
users = context.getGroupUsers(object)
for id in users:
    user = mship.getMemberById(id)
```

Agora você enviará um e-mail para todos no grupo, ao invés de todos os revisores!

### Informações de usuários em Page Templates

No Capítulo 6, você criou uma page template que permitia ao usuário enviar respostas ao administrador do site, por meio de um formulário. Naquele formulário, um campo permitia ao usuário digitar um endereço de e-mail, que então era validado. Entretanto, se o usuário estiver autenticado e você souber o endereço de e-mail, seria uma boa idéia preencher o campo automaticamente para o usuário.

O código atual para o campo é o seguinte:

```
<input type="text" name="email_address"
      tal:attributes="tabindex tabindex/next;
                    value request/email_address|nothing" />
```

Se um valor para o e-mail já existe na requisição de uma tentativa anterior de preencher o formulário, então você pode mostrá-lo. Caso contrário, então você pode verificar se um endereço de e-mail existe para o usuário atual. As seguintes alterações do formulário garantirão que o endereço de e-mail seja preenchido:

```
<input type="text" name="email_address"
      tal:define="user context/portal_membership/getAuthenticatedMember;
                email user/email|nothing"
      tal:attributes="tabindex tabindex/next;
                    value request/email_address|email|nothing" />
```

## Depurando e Entendendo a Segurança

Eu descobri que a segurança não é apenas um dos componentes mais difíceis de se entender no Plone, mas é também um dos mais difíceis de depurar e testar. Em função de o modelo ser granular e complicado, pode ser extremamente difícil de encontrar o porquê e onde um erro ocorre. Algumas vezes a mensagem de erro ou a informação dada é difícil de decifrar ou até mesmo é difícil de encontrar alguma informação a respeito.

Testar a segurança também é difícil porque em sites com vários papéis definidos, é necessário fazer um teste de regressão completo com cada tipo de usuário em cada tipo de situação. Em função do custo envolvido, entretanto, as pessoas geralmente não fazem esses testes de regressão completos. Além do mais, um erro de segurança é a pior coisa que pode ocorrer em um site se ele deixar vaziar informações confidenciais. O Plone deixará você fazer aquilo que queira; deixará até que você dê um tiro no próprio pé; então seja cuidadoso!

### VerboseSecurity

VerboseSecurity é um produto adicional que já vem incluso nos instaladores. Você também pode baixar o VerboseSecurity de <http://hathaway.freezope.org/Software/VerboseSecurity>. Como o nome sugere, ele fornece uma mensagem de erro detalhada quando você não pode fazer algo no Plone em razão de não ser autorizado. Entretanto, se você foi negligente na configuração da segurança, esse produto não vai ajudá-lo.

VerboseSecurity roda em um servidor Plone sem causar problemas de desempenho, então você pode rodá-lo nos seus servidores de produção e desenvolvimento. Pode haver uma pequena sobrecarga quando alguém tentar executar algo não permitido e um erro for apontado e o novo módulo de segurança entrar em cena.

Entretanto, uma vez que a mensagem de erro é detalhada, não é aconselhável ser exposta aos usuários. Ela revela muito mais do seu sistema do que um usuário deveria saber! Ela nunca revelará senhas- apenas informações a respeito dos usuários, papéis e permissões. É claro que seu servidor de produção sempre rodará perfeitamente, então não há motivo para instalar o produto nele.

A implementação original das rotinas de verificação de permissão foi feita em Python. Assim que as API ficaram estáveis e os desenvolvedores se deram conta da sobrecarga que a segurança causava, elas foram reescritas em C. Por padrão, a implementação C, mais rápida, está rodando, mas isso significa que o VerboseSecurity não pode modificar o módulo de permissão para ser mais prolixo. Eu raramente tive que usar esse nível de detalhe, geralmente encontrei informação suficiente nesse nível. Entretanto, se você precisa de mais informações, terá que rodar o Plone com a seguinte variável de ambiente:

```
ZOPE_SECURITY_POLICY=PYTHON
```

Para fazer o VerboseSecurity funcionar, você tem apenas que se certificar que ele está em seu diretório *Products* (para mais detalhes, veja o Capítulo 10) e, então, reiniciar o Plone. Encontre o objeto *cookie\_authentication*, que contém a lista de opções para autenticação no seu site e, no formulário, altere a opção *Auto-Login page ID* de *require\_login* para vazio, como exibido na Figura 9-14.

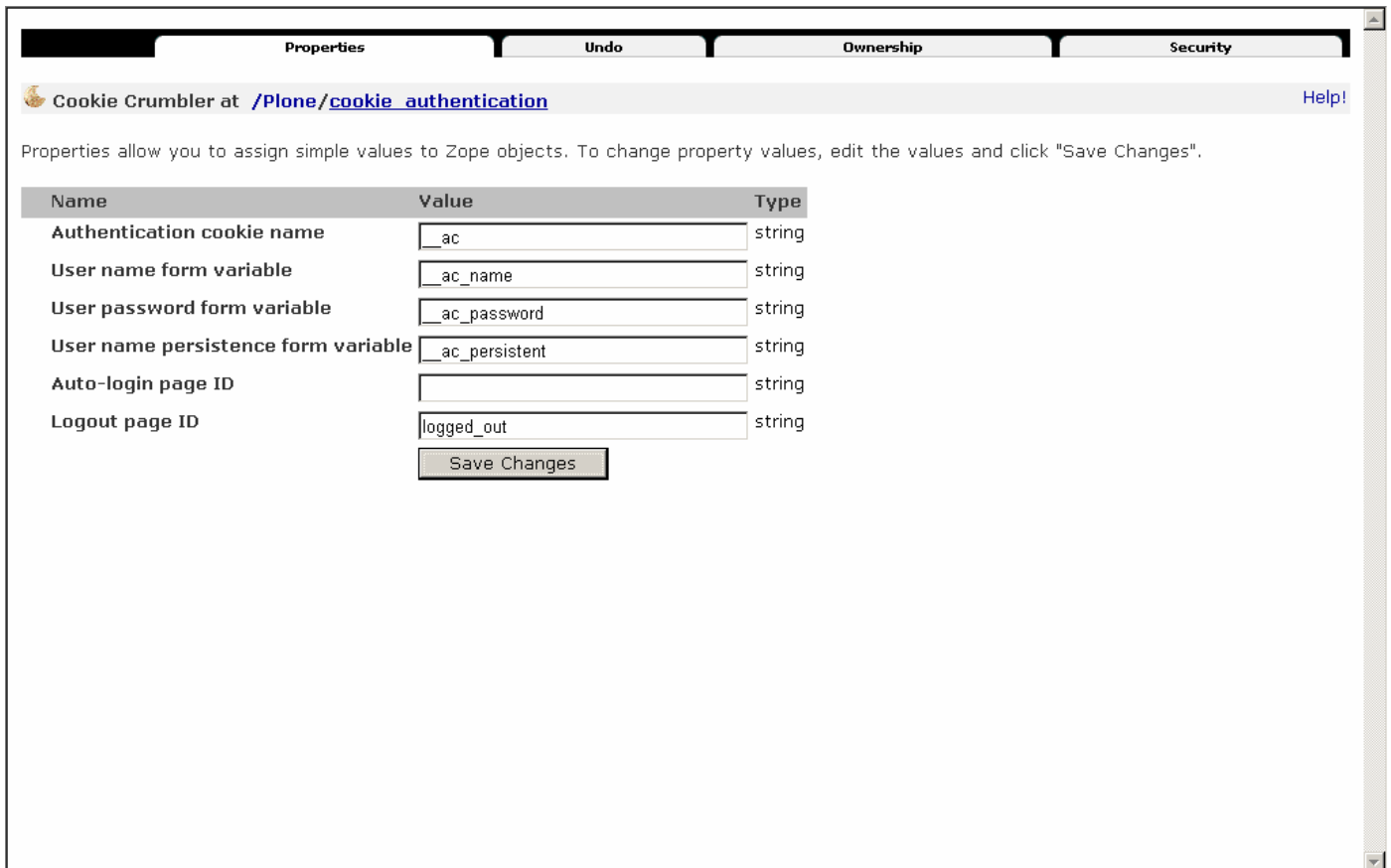
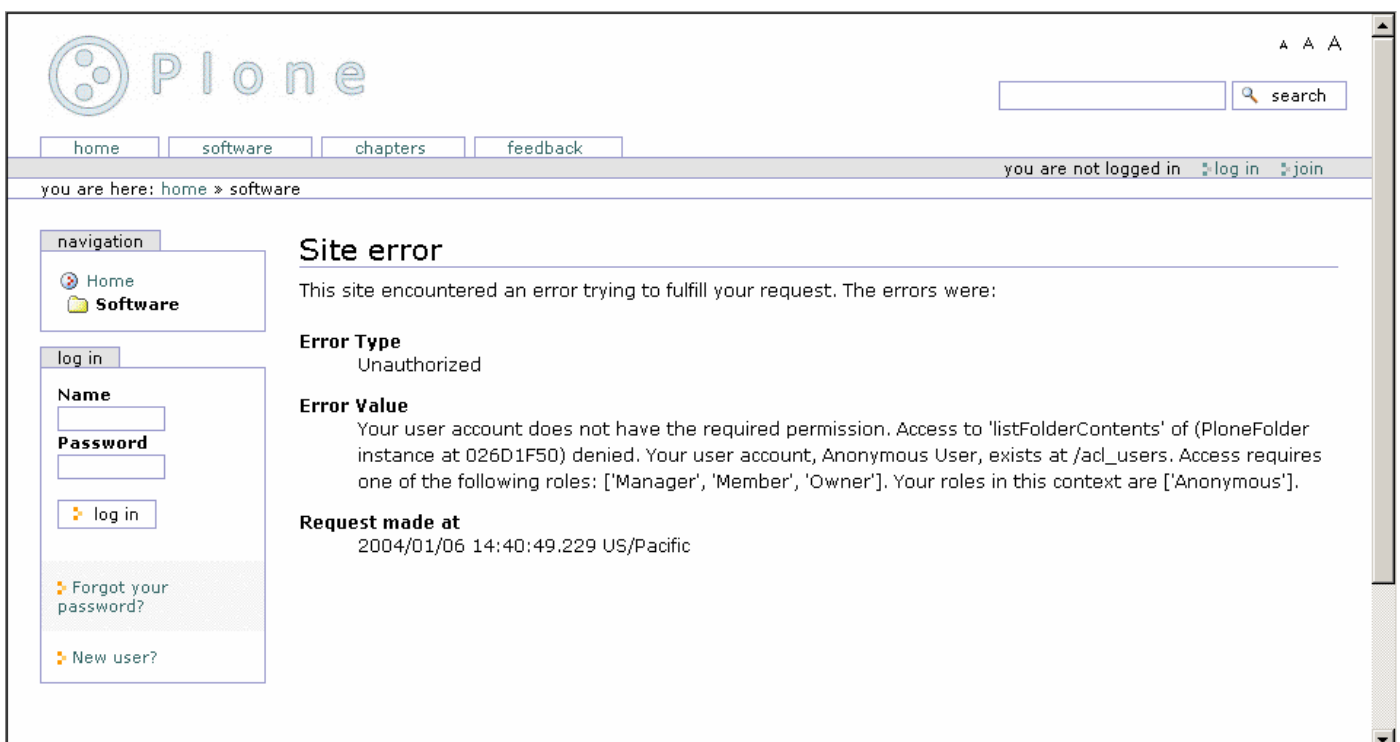


Figura 9-14. Alterando as configurações de autenticação de seu site  
 Agora você pode tentar recriar as circunstâncias para o erro que você deseja depurar. \*Lembre-se de se autenticar como o usuário que ocasionou o erro\*. Aqui é que é vantajoso ter dois navegadores diferentes para acessar o site Plone: um para administrar e outro para testar. Quando o erro ocorrer, uma janela de diálogo para autenticação HTTP será exibida na tela. Nesse momento, clique em Cancelar, e você obterá uma mensagem de erro detalhada, como a exibida na Figure 9-15.



## Figura 9-15. Uma mensagem de erro detalhada satisfatória

A mensagem é um tanto longa e auto-explicativa. Nesse momento, eu geralmente mudo para o outro navegador e examino as configurações de permissões para os objetos envolvidos para ver qual a possível causa.

### Problemas Comuns

Alguns problemas são fáceis de aparecer quando você lida com o Plone. O primeiro não é especificamente relacionado com o Plone mas vale a pena repetir: Verifique se o usuário que ocasiona o erro é realmente quem você pensa que é. Muitas vezes ouvi dizerem, 'Funciona em um navegador mas não em outro.' Isso geralmente acontece porque quando você troca de navegador, você também troca de usuário.

Continuando com o óbvio, tenha certeza de que o usuário tem o papel que você imagina que ele deva ter. Isso significa ir ao *acl\_users*, ver que papel o usuário tem e verificar se é o que você espera. Depois, pense em quaisquer grupos que o usuário pode estar. Mais uma vez, olhar em *acl\_users* poderá ser útil, porque os usuários podem obter papéis extras de um grupo. Finalmente, lembre-se de que o papel de um usuário pode também ser alterado por papéis locais em pastas ou objetos; isso torna difícil limitar o escopo porque não há um jeito fácil de saber qual pasta ou objeto tem papéis locais.

Quando estiver seguro de quem é o usuário e o papel que ele tem no objeto, você poderá ver quais são as reais permissões para o objeto. Como você já viu, dois objetos similares (dois documentos, por exemplo) podem ter permissões diferentes e papéis diferentes. O usuário que criou o documento terá o papel de dono para aquele documento e outro usuário terá apenas o papel de membro. Considere também que o workflow altera as permissões em um documento quando ele muda de estado.

### Fechando o Plone

Não há, na verdade, uma maneira simples de fazer isto já que não existe realmente um conceito de um site 'fechado'. No entanto, o princípio básico é que os usuários estão aptos a fazer o mínimo que necessitam e nada além disso- você deve verificar as configurações padrão e remover as opções de segurança que eles não precisam.

Para os paranóicos de verdade, você também pode remover partes da Interface de Usuário, modificando as folhas de estilo (CSS), para evitar que os usuários fiquem vagueando pelo site. Lembre-se, é claro, que remover a aba de uma ação ou negar acesso a um page template não é o suficiente se o usuário ainda pode, digamos, editar um documento. Conhecendo o Plone, eles podem chegar à página por meio de um script ou outro mecanismo malicioso. Com o Plone você vai descobrir que, freqüentemente, se você tentar com afinco, conseguirá obter a página de edição de um documento que você está visualizando capturando seu uniform resource locator (URL). No entanto, você não poderá realmente editar a página; você poderá apenas chamar o formulário de edição.

Se seu servidor está desprotegido, sem restrição de acesso, assegure-se de que você está rodando outro servidor Web defrente o ZServer do Zope. Conforme

exposto no capítulo 10, o ZServer que vem no pacote é uma implementação simples, desprovida de todos os controles e segurança que um servidor Web robusto precisa. Se possível, considere o uso de proxies para outros serviços Zope como FTP e WebDAV, caso você deixe que usuários não-confiáveis usem esses serviços (esse, normalmente, não é o caso).

## Integrando o Plone com Outros Serviços

As seções seguintes abordarão a segurança externa de uma instância Plone (todas as configurações de segurança que você precisa para rodar o Plone em um servidor, por exemplo). Depois veremos como usar o Plone com LDAP de forma que o Plone possa usar usuários de um servidor externo.

## Segurança em Seu Servidor

Eu abordei a segurança de usuários dentro do sistema Plone, mas há outra questão importante: a segurança e configuração de do sistema operacional de seu servidor Plone. Como em qualquer aplicação Web, tornar seu servidor seguro antes de expô-lo ao mundo é crítico. O processo de instalação do Zope 2.7 é muito bom e proporciona a maior parte do que você precisa, mas há alguns detalhes a considerar, que apresentarei agora.

## Usuário que Roda o Zope

Você deve se assegurar que o usuário que roda o Zope tenha a quantidade mínima de permissões para realizar a tarefa. O usuário que roda o Zope necessitará ler e escrever em todos os diretórios do Zope do sistema de arquivos. O usuário necessitará escrever os diretórios que contém os logs e banco de dados da sua instância Zope; esses são os diretórios *var* e *Log* da sua instância Zope.

A melhor maneira de fazer isso no Linux é criar uma conta de usuário dedicada denominada, digamos, *plone*, que se incumbirá disso; você pode limitar, então, o acesso desse usuário no caso improvável do Plone ser invadido.

No Linux, se você quiser ter o Plone funcionando em uma porta baixa (abaixo de 1024) como a 21 ou a 80, então normalmente você terá que rodar o Plone como root. Ele se conectará a essas portas como root e então mudará para outro usuário efetivo. Para fazer isso, é necessário especificar um valor para *effective-user* no arquivo de configuração, *zope.conf*. Ele fará a conexão e então mudará para esse usuário; um exemplo disso é *effective-user zope*. O melhor é não fazer isso e, alternativamente, rodar o Zope numa porta alta como a 8080; você pode então proteger essa porta no firewall e usar o Apache ou outro servidor Web para rodar na porta 80 e se comunicar com a porta 8080. O Capítulo 10 cobre esse assunto mais extensamente.

O equivalente em Windows é o usuário que roda o serviço que, por padrão, é a conta *LocalSystem*. Mais uma vez, você pode alterar o usuário que roda o Plone. Se você está pensando em rodar o Plone em um computador Windows que não tenha serviços (o que não recomendo ou apóio), então o Plone rodará localmente como o usuário que iniciou o servidor manualmente.

Alguns produtos podem exigir a instalação de software extra que forneça opções como: manipulação de imagem, conversão de documentos, dentre outros. Se você instalou alguma dessas ferramentas, tenha em mente que elas podem exigir um

pouco de trabalho para interagir com êxito com seu site Plone. Por exemplo, eu instalei *pdftohtml* no Windows para conversão de Portable Document Format (PDF), mas para que o comando pudesse ser lido, tive que rodar o serviço como um usuário com mais privilégios para que o Zope pudesse interagir com esse software. Nesse caso, como o servidor estava protegido por um firewall, não houve problema.

### Obtendo Acesso de Emergência

Se você tem um site Plone mas não pode acessar a ZMI porque você não sabe ou esqueceu a senha, então você pode obter uma conta de acesso de emergência. Para isso, é necessário ter acesso ao sistema de arquivos da instância do seu site Plone. Se você não tem, primeiro terá que achar uma maneira de obtê-lo.

Vá à raiz da sua instância e chame o script *zpasswd.py*. Você encontrará esse script no diretório do Zope (em *ZOPE\_HOME*). No meu computador o script *zpasswd.py* encontra-se em */opt/Zope-2.7/bin/zpasswd.py*. Para criar uma senha, faça o seguinte:

```
$ cd /var/zope
$ python /opt/Zope-2.7/bin/zpasswd.py access
```

Username: emergency

Password:

Verify password:

Please choose a format from:

SHA - SHA-1 hashed password

CRYPT - UNIX-style crypt password

CLEARTEXT - no protection.

Encoding: SHA

Domain restrictions:

Será criado um arquivo *access* na sua instância Zope. Reinicie o Zope e se autentique na ZMI usando o nome de usuário e senha informados no script. Esse usuário tem um significado especial para o Plone e é chamado *emergency user*. Quando estiver autenticado como usuário de emergência você não poderá criar objetos, mas pode criar um novo usuário e se autenticar como esse usuário. Por razões de segurança você deve, então, eliminar o arquivo *access*.

### Obtendo Acesso de Emergência no Windows

A instalação do Plone no Windows oferece uma aplicação com interface gráfica para facilitar a obtenção do acesso de emergência. Selecione Iniciar - Programas - Plone - Plone e clique na opção Emergency User. Isso permitirá a criação de um novo usuário, a alteração da senha do usuário de emergência ou a eliminação do usuário de emergência, conforme exibido na Figura 9-16.

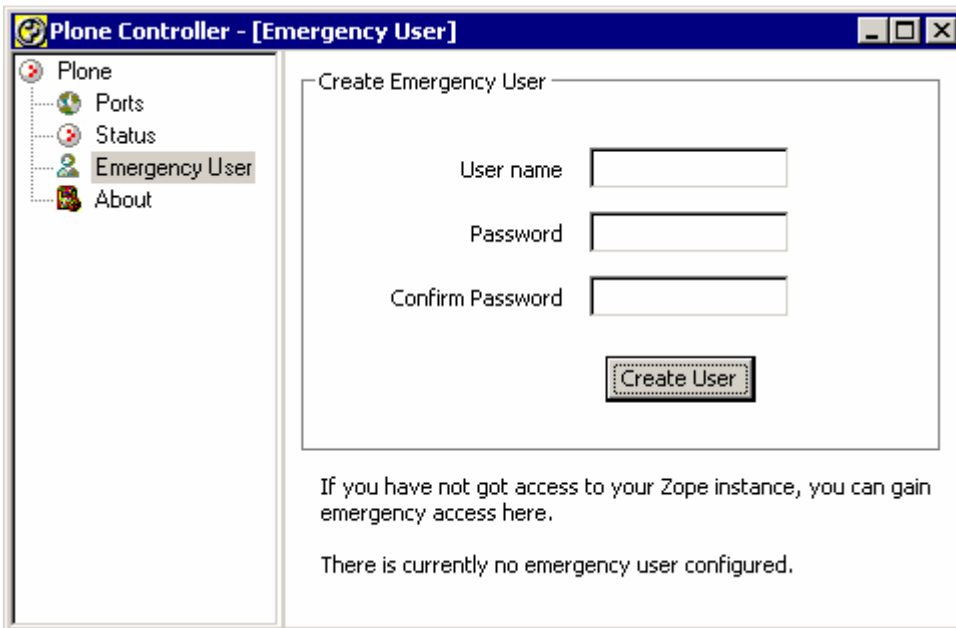


Figura 9-16. Criando um novo usuário de emergência

Para criar um novo usuário, clique em **Create User**. Na caixa de diálogo que se abrirá, informe o nome do usuário e a senha. Isso criará um arquivo no sistema de arquivos que conterà o nome do usuário e a senha. Igualmente, clique em **Change Password** para alterar a senha do usuário. Depois de adicionar ou alterar a senha, é necessário reiniciar o Zope. Para reiniciar o Plone, clique na aba **Control**, clique em **Stop** e depois clique em **Start**. Em seguida, clique em **Manage Root** e forneça o nome de usuário e senha que você acabou de criar. Você se autenticará como o usuário de emergência, o que significa que você não pode criar objetos, mas pode agora criar um novo usuário e se autenticar como esse usuário.

### Usando Sistemas de Autenticação Externos

Como vimos no Capítulo 8, o Plone armazena todos seus usuários no banco de dados orientado a objetos do Zope, em uma lista de usuários à parte. Como sempre, nada é perfeito e, em algumas situações, você pode querer utilizar outro serviço para autenticar seus usuários. A alternativa mais comum é o LDAP ou o Active Directory da Microsoft, que se comunica usando LDAP.

Entretanto, você pode até querer integrar com outra aplicação que armazena os usuários em um banco de dados relacional. Enquanto escrevia esse livro, o site ActiveState ASPN utilizava o Zope para todo o conteúdo, mas os usuários podiam se autenticar usando o sistema Passport da Microsoft. Na verdade, a instalação de esquemas extras para autenticação de usuários é bem direta graças ao excelente trabalho de vários desenvolvedores. Durante o processo de configuração, descobri que o mais difícil é criar o software e estabelecer a integração entre os sistemas.

**CUIDADO** Na próxima seção você “flertará” com a pasta `acl_users` do site Plone. Nunca apague ou altere a pasta `acl_users` na raiz da sua instância Zope. Se fizer isso e houver um problema com a pasta, por qualquer razão (o servidor caiu, por exemplo), todo seu site será bloqueado e você não poderá mais obter acesso, mesmo como administrador. Tenha certeza de alterar somente a pasta de usuário no site Plone!

## Usando LDAP

Primeiro você tem que configurar um servidor LDAP, ou algo que se comunica via LDAP, como o Active Directory (apesar de, aparentemente, o Active Directory apresentar algumas peculiaridades). Nesse exemplo, instalei o openLDAP nos meus servidores Red Hat e Windows. Para Windows, você encontrará uma versão pré-compilada em <http://www.zope.org/Members/volkerw/LdapWin32>. Eu a testei com o Python 2.3.

Faça o download, descompacte o arquivo e, então, aloje seu conteúdo em `c:\Arquivos de Programas\Plone\Python\Lib\site-packages`. Depois instale o `LDAPUserFolder`.

No Linux, você pode obter downloads do openLDAP em <http://www.openldap.org/>. A versão testada inclui os RPMs 2.0.27-2.8.0 e 2.0.27-2.8.0. Depois de instalá-lo, seguindo as instruções, fui para <http://python-ldap.sourceforge.net/>, obtive e compilei as bibliotecas Python LDAP apropriadas. No meu caso, a versão testada foi `2.0.0pre05-1.i386.rpm`. Assegure-se de usar o mesmo interpretador Python que você está usando para rodar o Plone.

Depois de dar todas essas voltas, é necessário ter certeza que o módulo `_ldap.so` pode ser importado pelo Python. A maneira mais fácil de testar isso é rodar o seguinte:

```
$ python -c "import _ldap"
```

Se voce não receber mensagens de erro, então foi importado corretamente. Se obtiver erros, você deverá repassar as etapas anteriores. Pegue então o `LDAPUserFolder` em <http://www.dataflake.org/software/Ldapuserfolder>. A versão testada era 2.1 beta 2. Baixe o arquivo, descompacte-o, e coloque-o em `Products`. Por exemplo:

```
$ tar -zxf LDAPUserFolder-2_1beta2.tgz
$ mv LDAPUserFolder /var/zope/Products
```

Reinicie o Plone, vá para o painel de controle e assegure-se que ele apareça corretamente na página de Produtos do painel do controle. Darei mais detalhes sobre isso no Capítulo 10.

Depois disso, você deve ser capaz de clicar em `acl_users`, clicar em Sources e, então, acessar a opção `Users source #1`. Selecione `LDAPUserFolder` e marque `I'm sure`, conforme a Figura 9-17. Isso criará uma nova pasta de usuários e substituirá a existente, então certifique-se que você não perderá nada crítico. De fato, esse é um bom momento para fazer uma cópia de segurança. Finalmente, clique em OK.

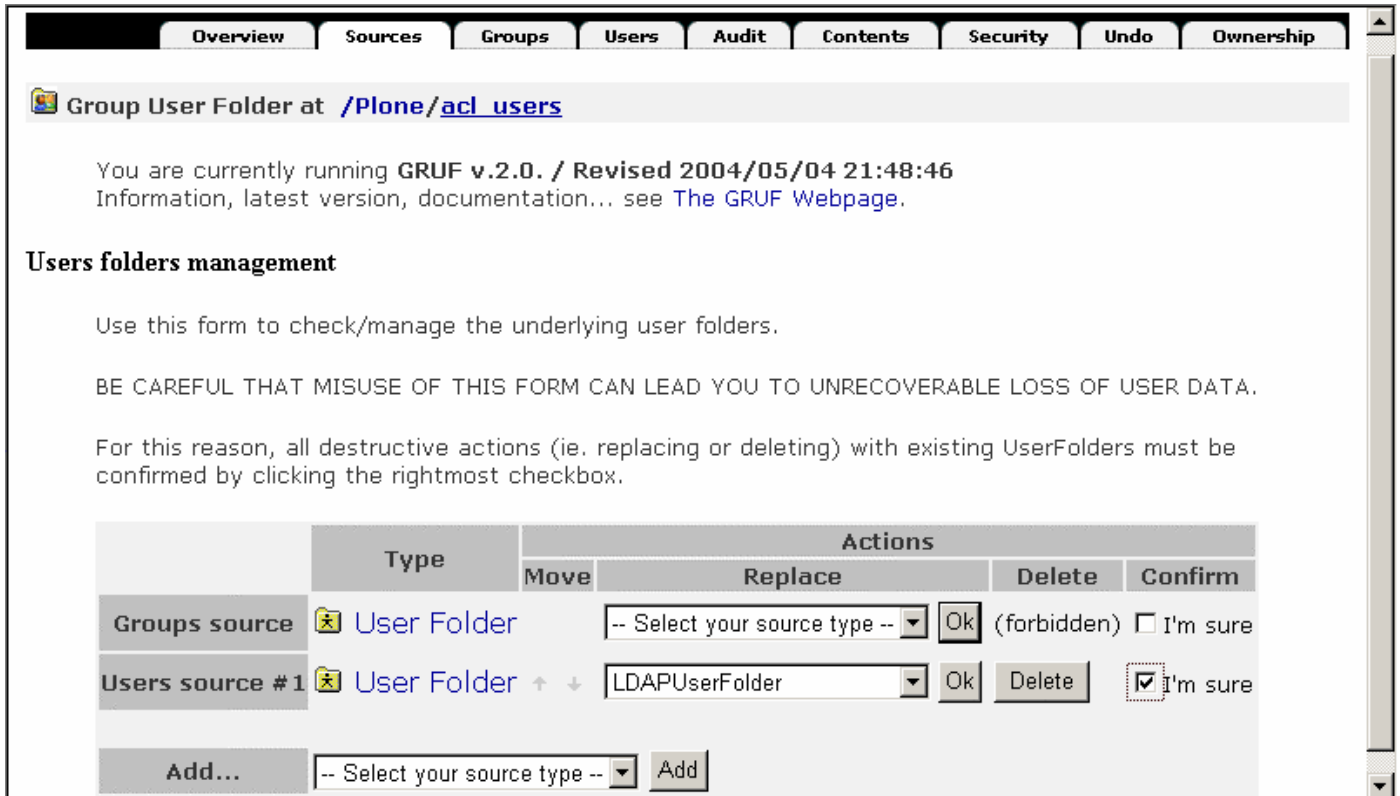


Figure 9-17. Adicionando o *LDAPUserFolder*

Nas configurações do *LDAPUserFolder*, faça as alterações que se adequem à sua configuração LDAP. A essa altura você deve ser capaz de clicar na aba *Users* e pesquisar usuários que já existem no seu diretório LDAP.

### Bancos de Dados Relacionais e Outros

Uma excelente pasta de usuário alternativa é a *exUserFolder*, que significa *extensible user folder* (pasta de usuário expansível). Ela é fácil de instalar; baixe-a de [http://prdownloads.sourceforge.net/exuserfolder/exUserFolder-0\\_20\\_0.tgz](http://prdownloads.sourceforge.net/exuserfolder/exUserFolder-0_20_0.tgz), descompacte-a e copie-a na sua pasta *Products*. Mais uma vez, após reiniciar o Plone, você deve ser capaz de clicar em *acl\_users*, selecionar *Users* e acessar a opção *Users source #1*. Selecione então *exUserFolder*, e marque *I'm sure*.

Na realidade, *exUserFolder* autenticará os usuários usando os seguintes serviços:

- Radius
- SMB
- LDAP
- Relational databases

Para fazer isso você precisará instalar o adaptador de banco de dados específico para o banco de dados relacional; felizmente existem adaptadores para os bancos mais utilizados. Para mais informações, você pode encontrar excelentes informações nos diretórios do *exUserFolder*, que contém arquivos

*ReadMe* para quase todos os assuntos. O Livro do Zope aborda a configuração do acesso a um banco de dados relacional em [http://zope.org/Documentation/Books/ZopeBook/2\\_6Edition/RelationalDatabases.stx](http://zope.org/Documentation/Books/ZopeBook/2_6Edition/RelationalDatabases.stx)

.