



Complemento
liberdade e tecnologia

Integrações com LDAP

Treinamento OTRS Help Desk



Sumário

Licenciamento deste Manual/Documento.....	3
Introdução.....	4
# Autenticação de Atendentes.....	5
# Mapeamento de Propriedades dos Atendentes.....	6
# Relacionando grupos do AD com papéis do OTRS.....	7
# Autenticação de Cliente no Active Directory.....	8
# Usuários do AD como Clientes do OTRS.....	9



Licenciamento deste Manual/Documento

Atribuição – Compartilhamento pela mesma Licença (by-sa)



Esta licença permite que outros remixem, adaptem, e criem obras derivadas ainda que para fins comerciais, contanto que o crédito seja atribuído ao autor e que essas obras sejam licenciadas sob os mesmos termos. Esta licença é geralmente comparada a licenças de software livre. Todas as obras derivadas devem ser licenciadas sob os mesmos termos desta. Dessa forma, as obras derivadas também poderão ser usadas para fins comerciais.

O trabalho Manual de Configuração de Chamados do OTRS Help Desk de www.complemento.net.br foi licenciado com uma Licença Creative Commons - Atribuição-Compartilha Igual 3.0 Não Adaptada.

Com base no trabalho disponível em www.complemento.net.br. Podem estar disponíveis autorizações adicionais ao âmbito desta licença em www.complemento.net.br/contato.

[Saiba mais sobre a licença \(by-sa\).](#)

<http://creativecommons.org/licenses/by-sa/3.0/br/>



Introdução

A integração que permite os usuários do AD se autenticarem no OTRS ou mesmo que permite o OTRS entregar informações de clientes no AD são parametrizadas no arquivo **Config.pm**

Neste documento, disponibilizamos trechos de código que devem ser colados neste arquivo, de acordo com a necessidade de integração e, adaptados à realidade de sua empresa.

Uma forma interessante de verificar se o servidor linux está acessando o servidor de diretórios AD, é utilizando o comando abaixo:

```
ldapsearch -h 192.168.1.10 -b "DC=DOMINIO,DC=LOCAL" -D  
"CN=otrs,CN=Users,DC=DOMINIO,DC=LOCAL" -w senha "(objectClass=group)"
```

Este comando faz a listagem do seu diretório de usuários. É necessário instalar o ldapsearch em seu servidor. No CentOS pode ser instalado com o comando:

```
yum install openldap-clients
```

Autenticação de Atendentes

```
#####  
# Autenticação de Atendentes #  
#- Aqui definimos a integração que permite ao OTRS reconhecer usuários #  
# do Active Directory de sua organização. #  
#- Importante: os usuário devem possuir o campo "email" preenchido #  
# no AD para poderem se autenticar #  
#####  
$Self->{AuthModule1} = 'Kernel::System::Auth::LDAP';  
# Abaixo, colocamos o IP ou hostname do servidor  
$Self->{'AuthModule::LDAP::Host1'} = '192.168.30.50';  
# A seguir, o DistinguishedName (DN) onde buscaremos os usuários  
$Self->{'AuthModule::LDAP::BaseDN1'} = 'DC=complemento,DC=net,DC=br';  
# A seguir, a propriedade do AD onde encontraremos o nome de usuário  
$Self->{'AuthModule::LDAP::UID1'} = 'sAMAccountName';  
# Aqui definimos em qual grupo o usuário deve estar para poder se logar no OTRS,  
# Este parametro é opcional e pode ser comentado com #  
$Self->{'AuthModule::LDAP::GroupDN1'} = 'CN=Atendentes,OU=OTRS Groups,DC=complemento,DC=net,DC=br';  
# O parametro abaixo não deve ser modificado  
$Self->{'AuthModule::LDAP::AccessAttr1'} = 'member';  
# Aqui definimos o usuário e senha de uma conta que tenha permissão de buscar informações na árvore de nosso AD.  
# É aconselhavel criar um usuário exclusivo para o OTRS  
$Self->{'AuthModule::LDAP::SearchUserDN1'} = 'CN=otrs,CN=Users,DC=complemento,DC=net,DC=br';  
$Self->{'AuthModule::LDAP::SearchUserPw1'} = 'Brasil123!';  
# Note que há o número "1" no fim das definições realizadas entre "{ }"  
# O OTRS permite que você se conecte com até 9 módulos diferentes de autenticação, ou 9 Ads diferentes por exemplo.
```

Mapeamento de Propriedades dos Atendentes

```
# Aqui podemos mapear os dados dos atendentes, tais como nome e sobrenome, e-mail etc.
# Os valores abaixo servem para uma instalação padrão. Adapte para seu sistema.
$Self->{AuthSyncModule} = 'Kernel::System::Auth::Sync::LDAP';
$Self->{'AuthSyncModule::LDAP::UserAttr'} = 'DN';
$Self->{'AuthModule::LDAP::UserAttr'} = 'DN';
$Self->{'AuthSyncModule::LDAP::Host'} = '192.168.30.50';
$Self->{'AuthSyncModule::LDAP::BaseDN'} = 'DC=complemento,DC=net,DC=br';
$Self->{'AuthSyncModule::LDAP::UID'} = 'sAMAccountName';
$Self->{'AuthSyncModule::LDAP::SearchUserDN'} = 'CN=otrs,CN=Users,DC=complemento,DC=net,DC=br';
$Self->{'AuthSyncModule::LDAP::SearchUserPw'} = 'Brasil123!';
$Self->{'AuthSyncModule::LDAP::UserSyncMap'} = {
    # DB -> LDAP
    UserFirstname => 'givenName',
    UserLastname  => 'sn',
    UserEmail     => 'mail',
    UserCargo     => 'description',
    UserPhoneNumber => 'telephoneNumber',
};
$Self->{'AuthSyncModule::LDAP::AccessAttr'} = 'member';
# Você pode escolher grupos padrões para seus usuários. Basta descomentar as 3 linhas abaixo e definir os grupos
# $Self->{'AuthSyncModule::LDAP::UserSyncInitialGroups'} = [
#     'users',
# ];
```

Relacionando grupos do AD com papéis do OTRS

```
#####  
#- Gestão de papéis do sistema #  
#- Aqui você deve fazer as associações entre os grupos #  
# do Active Directory e dos papéis no OTRS. #  
#- Você deve adicionar linhas aqui sempre que criar um novo papel #  
# no OTRS ou grupo no Active Directory #  
#####  
  
$Self->{'AuthSyncModule::LDAP::UserSyncRolesDefinition'} = {  
    # Grupo no Active Directory  
    'CN=Administradores OTRS,OU=OTRS Groups,DC=complemento,DC=net,DC=br' => {  
        # Papel no OTRS  
        'Administrador' => 1,  
    },  
    'CN=Service Desk,OU=OTRS Groups,DC=complemento,DC=net,DC=br' => {  
        # Papel no OTRS  
        'Atendente de Primeiro Nível' => 1,  
    },  
    'CN=Desenvolvedores,OU=OTRS Groups,DC=complemento,DC=net,DC=br' => {  
        'Desenvolvedor' => 1,  
# Você pode definir mais que um papel para o mesmo grupo do AD  
# 'Papel 2' => 1,  
    },  
};
```

Autenticação de Cliente no Active Directory

```
$Self->{'Customer::AuthModule2'} = 'Kernel::System::CustomerAuth::LDAP';
$Self->{'Customer::AuthModule::LDAP::Host2'} = '192.168.30.50';
$Self->{'Customer::AuthModule::LDAP::BaseDN2'} = 'DC=complemento,DC=net,DC=br';
$Self->{'Customer::AuthModule::LDAP::UID2'} = 'sAMAccountName';
$Self->{'Customer::AuthModule::LDAP::AccessAttr2'} = 'member';
$Self->{'Customer::AuthModule::LDAP::SearchUserDN2'} = 'CN=otrs,CN=Users,DC=complemento,DC=net,DC=br';
$Self->{'Customer::AuthModule::LDAP::SearchUserPw2'} = 'Brasil123!';
# A linha abaixo serve para não trazer usuarios desativados: (!(userAccountControl:1.2.840.113556.1.4.803:=2))
# Fonte: http://www.petri.co.il/ldap\_search\_samples\_for\_windows\_2003\_and\_exchange.htm
$Self->{'Customer::AuthModule::LDAP::AlwaysFilter2'} =
    '(&(objectclass=user)(!(objectclass=computer))(!(userAccountControl:1.2.840.113556.1.4.803:=2)))';

# $Self->{'Customer::AuthModule::LDAP::Die2'} = 0;
# A linha abaixo serve para permitir que apenas usuários de um determinado grupo acessem o sistema como clientes
# $Self->{'Customer::AuthModule::LDAP::GroupDN'} = 'CN=Clientes OTRS,OU=OTRS Groups,DC=complemento,DC=net,DC=br';
```


Usuários do AD como Clientes do OTRS

```
#####  
# Exibe os colaboradores do AD como clientes internos #  
# Lembre-se que os usuários no AD devem ter o campo mail #  
# preenchido corretamente #  
#####  
$Self->{CustomerUser1} = {  
    Name => 'Active Directory Complemento',  
    Module => 'Kernel::System::CustomerUser::LDAP',  
    Params => {  
        Host => '192.168.30.50',  
        BaseDN => 'DC=complemento,DC=net,DC=br',  
        SSCOPE => 'sub',  
        UserDN => 'CN=otrs,CN=Users,DC=complemento,DC=net,DC=br',  
        UserPw => 'Brasil123!',  
        # A linha abaixo serve para não trazer usuarios desativados: (!(userAccountControl:1.2.840.113556.1.4.803:=2))  
        # Fonte: http://www.petri.co.il/ldap\_search\_samples\_for\_windows\_2003\_and\_exchange.htm  
        AlwaysFilter => '(&(objectclass=user)(!(objectclass=computer))(!(userAccountControl:1.2.840.113556.1.4.803:=2)))',  
        SourceCharset => 'utf-8',  
        DestCharset => 'utf-8',  
        Params => {  
            port => 389,  
            timeout => 120,  
            async => 0,  
            version => 3,  
        },  
    },  
    CustomerKey => 'sAMAccountName',  
    CustomerID => 'mail',  
    CustomerUserListFields => ['cn','mail'],  
    CustomerUserSearchFields => ['sAMAccountName', 'cn', 'mail','givenname', 'sn'],  
    CustomerUserSearchPrefix => '*',  
    CustomerUserSearchSuffix => '*',  
    CustomerUserSearchListLimit => 500,  
    CustomerUserPostMasterSearchFields => ['mail'],  
    CustomerUserNameFields => ['givenname', 'sn'],  
    CustomerUserEmailUniqCheck => 0,  
    CustomerUserExcludePrimaryCustomerID => 0,  
    AdminSetPreferences => 0,  
    ReadOnly => 1,  
    CacheTTL => 180,  
    Map => [  
        # note: Login, Email and CustomerID are mandatory!
```

```
# var, frontend, storage, shown (1=always,2=lite), required, storage-type, http-link, readonly
[ 'UserTitle',      'Title',      'title',          1, 0, 'var', '', 0 ],
[ 'UserFirstname', 'Firstname',  'givenname',     1, 1, 'var', '', 0 ],
[ 'UserLastname',  'Lastname',   'sn',            1, 1, 'var', '', 0 ],
[ 'UserLogin',     'Username',   'sAMAccountName', 1, 1, 'var', '', 0 ],
[ 'UserEmail',     'Email',      'mail',          1, 1, 'var', '', 0 ],
[ 'UserCustomerID', 'CustomerID', 'sAMAccountName', 0, 1, 'var', '', 0 ],
[ 'UserPhone',     'Phone',      'telephonenumber', 1, 0, 'var', '', 0 ],
[ 'UserAddress',   'Address',    'postaladdress',  1, 0, 'var', '', 0 ],
[ 'UserComment',   'Comment',    'dn',            1, 0, 'var', '', 0 ],
[ 'DN',            'DN',         'dn',            1, 0, 'var', '', 0 ],
```

```
],
```

```
};
```