

User Management: How do I authenticate against Active Directory Using SAMBA/WINBIND?

How do I authenticate against Active Directory (AD) ?

There are a lot of ways to do this.

[How Do I Integrate Bright With Active Directory using the native AD provider of SSSD?](http://kb.brightcomputing.com/faq/index.php?action=artikel&cat=13&id=224) (<http://kb.brightcomputing.com/faq/index.php?action=artikel&cat=13&id=224>) discusses a way using SSSD/AD_provider authentication with multiple RHEL servers integrated to an AD domain or forest, and is recommended for most purposes.

A different way, with a single RHEL server integrated to an AD domain or forest, uses the following steps to allow a Bright Cluster to authenticate against a Windows AD Server while maintaining the user information in Bright's LDAP. These instructions were tested on Windows Server 2008 and 2012.

1. Configure `smb.conf`

Edit `/etc/samba/smb.conf` and fill in the Windows AD Server information (workgroup, password server, and realm) under the `[global]` section. In this example, `bright` is used as workgroup, `bcm.bright.local` is used as password server, and `BRIGHT.LOCAL` is used as an Active Directory realm. The rest of the parameters should be kept the same.

```
[global]
  workgroup = bright
  password server = bcm.bright.local
  realm = BRIGHT.LOCAL
  encrypt passwords = yes
  winbind enum groups = yes
  winbind enum users = yes
  winbind use default domain = yes
  security = ADS
  debuglevel = 2
  wins support = no
  idmap uid = 10000-20000
  idmap gid = 10000-20000
  template shell = /bin/false
  winbind offline logon = false
```

Tip:

Type "net config workstation" on the command line of the Windows AD Server to get the

User Management: How do I authenticate against Active Directory Using SAMBA/WINBIND?

workgroup, password server and AD realm.

```
Logon Domain = workgroup
```

```
FQDN = password server
```

```
FQDN - Computer Name = realm
```

2. Configure krb5.conf

Edit `/etc/krb5.conf` and change the following sections to match the Windows AD Server Settings. Here,

- port 88 is the default port that is used for authentication in the forest level trusts (the underlying technology by which secured Active Directory communications occur)
- port 749 is the default port that is used for kadmin utilities.

```
[logging]
default = FILE:/var/log/krb5libs.log
kdc = FILE:/var/log/krb5kdc.log
admin_server = FILE:/var/log/kadmind.log
```

```
[libdefaults]
default_realm = BRIGHT.LOCAL
dns_lookup_realm = true
dns_lookup_kdc = true
ticket_lifetime = 24h
forwardable = true
```

```
[realms]
BRIGHT.LOCAL = {
    kdc = bcm.bright.local:88
    admin_server = bcm.bright.local:749
}
```

```
[domain_realm]
.bright.local = BRIGHT.LOCAL
bright.local = BRIGHT.LOCAL
```

3. Configure Authentication Method

User Management: How do I authenticate against Active Directory Using SAMBA/WINBIND?

/etc/pam.d/system-auth-ac:

```
##%PAM-1.0
# This file is auto-generated.
# User changes will be destroyed the next time authconfig is run.
auth      required      pam_env.so
auth      sufficient    pam_unix.so nullok try_first_pass
auth      requisite     pam_succeed_if.so uid >= 500 quiet
auth      sufficient    pam_winbind.so use_first_pass
auth      required      pam_deny.so

account   required      pam_unix.so broken_shadow
account   sufficient    pam_succeed_if.so uid < 500 quiet
account   [default=bad success=ok user_unknown=ignore] pam_winbind.so
account   required      pam_permit.so

password  requisite     pam_cracklib.so try_first_pass retry=3
password  sufficient    pam_unix.so nullok try_first_pass use_authtok
password  sufficient    pam_winbind.so use_authtok
password  required      pam_deny.so

session   optional     pam_keyinit.so revoke
session   required    pam_limits.so
session   [success=1 default=ignore] pam_succeed_if.so service in crond quiet use_uid
session   required    pam_unix.so
```

/etc/pam.d/password-auth-ac:

```
##%PAM-1.0
# This file is auto-generated.
# User changes will be destroyed the next time authconfig is run.
auth      required      pam_env.so
auth      sufficient    pam_unix.so nullok try_first_pass
auth      requisite     pam_succeed_if.so uid >= 500 quiet
auth      sufficient    pam_winbind.so use_first_pass
auth      required      pam_deny.so

account   required      pam_unix.so broken_shadow
account   sufficient    pam_succeed_if.so uid < 500 quiet
account   [default=bad success=ok user_unknown=ignore] pam_winbind.so
account   required      pam_permit.so

password  requisite     pam_cracklib.so try_first_pass retry=3
password  sufficient    pam_unix.so nullok try_first_pass use_authtok
password  sufficient    pam_winbind.so use_authtok
password  required      pam_deny.so
```

User Management: How do I authenticate against Active Directory Using SAMBA/WINBIND?

```
session optional pam_keyinit.so revoke
session required pam_limits.so
session [success=1 default=ignore] pam_succeed_if.so service in crond quiet use_uid
```

```
session required pam_unix.so
```

/etc/pam.d/php

```
auth sufficient pam_winbind.so
```

```
account sufficient pam_winbind.so
```

Tip:

If you're using Red Hat based distributions, you may use "authconfig-tui" tool to autogenerate system-auth-ac and password-auth-ac, but then you'll have to check that the smb.conf still has the correct configurations.

3. Test The Connectivity to Windows Active Directory Server

Add an entry for the AD server "bcm.bright.local" into /etc/hosts.

/etc/hosts:

```
10.2.184.194 bcm.bright.local bright bright.local
```

Run the following command, which fetches the domain Security Identifier (SID) and stores it in the local secrets.tdb:

```
# net rpc getsid -S bcm.bright.local
Storing SID S-1-5-21-547601799-235048094-3373437802 for Domain BRIGHT
in secrets.tdb
```

User Management: How do I authenticate against Active Directory Using SAMBA/WINBIND?

Make sure that the winbind service can start successfully

```
# /etc/init.d/winbind restart
```

```
# /etc/init.d/winbind status
```

```
winbindd (pid 17966) is running..
```

4. Join the Windows AD Domain

```
# net ads join -U Administrator -S bcm.bright.local
Enter Administrator's password:
Using short domain name -- BRIGHT
Joined 'AD-TEST' to dns domain 'bright.local'
```

5. Verify Authentication

a. Add user in Bright:

```
# cmsn
% user
% add user adel
%set password
% commit
```

b. Add user in Windows AD Server with different password.

c. At this stage:

* a log in attempt with the password that is stored in Bright's LDAP should be denied, and

* a log in with the password that is stored in Windows AD Server should be allowed.

User Management: How do I authenticate against Active Directory Using SAMBA/WINBIND?

6. Configuring Userportal Authentication Method

Edit /etc/pam.d/php to include the following lines:

```
auth sufficient pam_winbind.so
```

```
account sufficient pam_winbind.so
```

Restart the httpd service:

```
# /etc/init.d/httpd restart
```

Troubleshooting

Issue

```
# net rpc getsid -S bcm.bright.local  
Unable to find a suitable server for domain BRIGHT.LOCAL
```

Resolution

smb.conf and krb5.conf need to be reconfigured

Issue

```
# net join -U Administrator -S bcm.bright.local  
Enter Administrator's password:  
Failed to join domain: failed to find DC for domain BRIGHT.LOCAL  
ADS join did not work, falling back to RPC...  
Unable to find a suitable server for domain BRIGHT.LOCAL  
Unable to find a suitable server for domain BRIGHT.LOCAL
```

Resolution

samba.conf and krb5.conf need to be reconfigured

Issue

```
# net ads join -U Administrator -S bcm.bright.local  
Enter Administrator's password:  
Using short domain name -- BRIGHT  
Joined 'AD-TEST' to dns domain 'bright.local'  
kerberos_kinit_password AD-TEST$@BRIGHT.LOCAL failed: Clock skew too great
```

Resolution

User Management: How do I authenticate against Active Directory Using SAMBA/WINBIND?

Timezone between the AD server and Bright Cluster differs. Fix that.

Issue

```
# net join -U Administrator -S bcm.bright.local
Enter Administrator's password:
Using short domain name -- BRIGHT
Joined 'AD-TEST' to dns domain 'bright.local'
DNS Update for ad-test.cm.cluster failed: ERROR_DNS_GSS_ERROR
DNS update failed!
```

Resolution

A DNS error is normal if the server is not a domain DNS server. This is because the DNS record of the server cannot be updated. This error will not block joining the AD domain. It's related to the Windows DNS Server in which the AD is registered. To test that the join was successful:

```
# net ads testjoin
Join is OK
```

Issue

```
# net ads join -U Administrator -S bcm.bright.local
```

```
Enter Administrator's password:
kinit succeeded but ads_sasl_spnego_krb5_bind failed: Server not found in Kerberos database
Failed to join domain: failed to connect to AD: Server not found in Kerberos database
```

Resolution

```
re-issue "net rpc getsid -S bright.bcm.local"
```

Unique solution ID: #1006

Author: Martijn de Vries

Last update: 2014-11-04 09:47