User Management: How do I integrate Bright with multiple AD servers using SSSD capabilities?

In the Knowledge Base article [How do I integrate Bright with AD Using SSSD Capabilities?](http//kb.brightcomputing.com/faq/index.php?action=artikel&id=159) (http//kb.brightcomputing.com/faq/index.php?action=artikel&id=159), the integration of a single AD server with Bright is discussed.

For multiple AD servers, as indicated by the following, the configuration for the client configuration file `krb5.conf` and server configuration file `sssd.conf` should point to all the AD servers and no default realm should be included:

/etc/krb5.conf

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

[libdefaults]
#default_realm = BCM.LOCAL
dns_lookup_realm = false
dns_lookup_kdc = false
ticket_lifetime = 24h
renew_lifetime = 7d
forwardable = true

[realms]
BCM.LOCAL = {
kdc = win2008.bcm.local
admin_server = win2008.bcm.local
}
BCM.LOCAL2 = {
kdc = win.bcm.local2
admin_server = win.bcm.local2
}

[domain_realm]
.bcm.local = BCM.LOCAL
bcm.local = BCM.LOCAL

.bcm.local2 = BCM.LOCAL2
bcm.local2 = BCM.LOCAL2
```

/etc/sssd/sssd.conf

```
[sssd]
```

```
domains = BCM.LOCAL, BCM.LOCAL2
services = nss, pam
config_file_version = 2
#sbus_timeout = 30

[nss]
filter_groups = root
filter_users = root

[pam]
offline_credentials_expiration = 0

[domain/BCM.LOCAL]
# changing or commenting this value will not allow sssd service to
start
id_provider = ldap

# to find the AD server
ldap_uri = ldap://win2008.bcm.local

# allow access to what is defined here
ldap_access_filter = memberOf=cn=brightusers,cn=Users,dc=bcm,dc=local

# User that can read from AD, any normal user should work as long as
it
# can get a ticket. Update as necessary
ldap_default_bind_dn = cn=Administrator,cn=Users,dc=bcm,dc=local

# Leave this as password
ldap_default_authtok_type = password

# The ldap users actual password, update as necessary
ldap_default_authtok = Ch@ngeMe

# to get user information (UID/GID) from the active directory
ldap_user_object_class = user
ldap_user_home_directory = unixHomeDirectory
ldap_group_object_class = group
ldap_force_upper_case_realm = True

# allow getent to query the AD
enumerate = true

# kerberos config
auth_provider = krb5
krb5_server = win2008.bcm.local
krb5_realm = BCM.LOCAL
```

User Management: How do I integrate Bright with multiple AD servers using SSSD capabilities?

```
[domain/BCM.LOCAL2]
# changing or commenting this value will not allow sssd service to
start
id_provider = ldap

# to find the AD server
ldap_uri = ldap://win.bcm.local2

# allow access to what is defined here
ldap_access_filter =
memberOf=cn=brightusers2,cn=Users,dc=bcm,dc=local2

# User that can read from AD, any normal user should work as long as
it
# can get a ticket. Update as necessary
ldap_default_bind_dn = cn=Administrator,cn=Users,dc=bcm,dc=local2

# Leave this as password
ldap_default_authtok_type = password

# The ldap users actual password, update as necessary
ldap_default_authtok = Ch@ngeMe2

# to get user information (UID/GID) from the active directory
ldap_user_object_class = user
ldap_user_home_directory = unixHomeDirectory
ldap_group_object_class = group
ldap_force_upper_case_realm = True

# allow getent to query the AD
enumerate = true

# kerberos config
auth_provider = krb5
krb5_server = win.bcm.local2
krb5_realm = BCM.LOCAL2
```

sssd should be restarted after this configuration change. For example:

```
service sssd restart
```

Unique solution ID: #1223
Author: Frank Furter
Last update: 2014-08-15 14:27