

OCTOBER 2011

Workaround: Centrify DirectControl for Mac OSX 10.7 (Lion) Using .local Domain

Problem

After installing the Centrify DirectControl agent on Mac OS 10.7, the following issues are observed.

1. If the home directory is located on a SMB share, it will take a long time to login.
2. If an Active Directory user logs in and tries to mount a SMB share folder in the Finder, it will take a long time to mount.
3. Centrify may be in disconnected mode. (To confirm this, open the Terminal utility and run the command: `adinfo -V.`)

Cause

For the Mac OS 10.7 (Lion) release, Apple changed the way a .local domain is handled by reserving it for Bonjour. When a user tries to login to a .local domain with only one level (that is, xxx.local), OS 10.7 first tries to resolve the name using multicast. It will try several times (with a default timeout of 5 seconds for each try), and if login fails it will then use standard DNS, causing the login delay and the delay in mounting SMB shares. Under these conditions, it may not be possible to ping domain.local, and therefore the adclient process will stay in disconnected mode for up to 60 seconds

This issue affects all Mac OS 10.7 users in a .local domain and is not specific to DirectControl-managed systems. Other hostnames are resolved first using multicast and then unicast.

Workaround

The following steps require root or sudo privileges. Important: Save a backup of the original files in another location, to provide a means of recovering from any mistakes made in editing.

Step 1

The following step forces Mac 10.6/10.7 to do both a multiicast and unicast query to xxx.local.

On the DNS server (Active Directory or Unix), create a primary zone "local". You do not need to modify it. Just SOA (Start of Authority) needs to exist in this zone.

After configuration, restart mDNSResponder on the Mac by running `# sudo killall mDNSResponder`. Then you should be able to ping domain.local.

Step 2

Mac 10.7 always does both an IPv4 and IPv6 query. We can configure IPv6 to be disabled and that will improve performance.

Unfortunately, you cannot disable IPv6 from System Preferences, and so you need to manually edit the `/Library/Preferences/SystemConfiguration/preferences.plist` on the Mac.

Find the network adapter (Ethernet or Airport) under NetworkServices key, and then edit the IPv6 setting, changing the config method to `__INACTIVE__`:

```
<plist version="1.0">
<dict>
<key>CurrentSet</key>
<string>/Sets/XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX</string>
...
<key>NetworkServices</key>
<dict>
<key>XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX</key>
<dict>
...
<key>IPv6</key>
<dict>
<key>ConfigMethod</key>
<string>__INACTIVE__</string>
</dict>
...

```

Step 3

There's no way to change the DNS lookup order, but you can reduce the multicast DNS timeout by editing `mdns_timeout`, located here:

`/System/Library/SystemConfiguration/IPMonitor.bundle/Contents/Info.plist`

The default setting is 5. Set `mdns_timeout` to 0 as shown below.

```
<key>mdns_timeout</key>  
<integer>0</integer>
```

Step 4

If you set `mdns_timeout` to 0, then you won't be able to ping any ".local" host/domain, but other apps such as Finder and Apple's Active Directory plugin work well (it can resolve a .local hostname). You can login as a network home user very quickly.

If you try to mount a SMB share in the Finder, you can ignore the prompt that says there's a problem connecting to the server. If you wait for several seconds and retry, it will eventually connect. This prompt can be removed by adding the machine that hosts the DNS server and Windows share into `/etc/hosts` file on the Mac:

```
192.168.x.x server.domain.local  
192.168.x.x anotherserver.domain.local
```

where 192.168.x.x is the IP address of the DNS server in your organization.

Note: Because you cannot ping `domain.local`, `adclient` will stay in disconnected mode for up to 60 seconds after start (which means you need to wait for more than 1 minute after reboot). Adding `domain.local` into `/etc/hosts` solves the disconnect issue.

Step 5

Reboot the Mac after performing steps 1) through 4).

Step 6

Login to the Mac, and you should not see any delay during login. Also, you should not see any delay when mounting a SMB folder in Finder.

Resolution

Awaiting a fix from Apple. Centrify has opened Bug 9887516 with Apple and has provided the above steps as a workaround after testing in our lab. For more information on Bonjour and how it works:

<http://www.apple.com/support/bonjour/>

Note: Sample files with the changes for step 2 and step 3 are available for your convenience, but we recommend you change the files directly on the Mac in question.