Domain Controller Could Not Be Contacted

Error Description

When I try to join a new Windows workstation or server to an Active Directory (AD) domain, I sometimes encounter the following error: “An Active Directory Domain Controller (AD DC) for the domain ‘domainname’ could not be contacted.”

This error can occur due to any of several reasons, from a simple incorrect DNS server IP address to a much more complex issue. In this blog, I will walk you through the steps you need to troubleshoot this problem, from the simplest to the most complex.

When the Error Arises

The error can be displayed when you attempt to join a workstation or server to a domain. Here are the steps that lead up to the error:

1. Right-click on the `Start` button and select `System`:
   ad1.webp
2. On the next screen, click `Change settings`:
   ad2.webp
3. In the System Properties window, click the `Change` button. Then enter the name of the new computer and specify which domain you want to join it to, being sure to enter the FQDN (fully qualified domain name) of the domain. Click `OK`. This is when the error might be displayed:
   ad3.webp

Initial Troubleshooting Steps

First, ensure that you typed the domain name correctly.

If that’s not the problem, click `Details` to get information about the error.

The following sections detail the steps to take to get to the root of the problem. In most cases, the issue is related to one of the following: incorrect DNS settings or a wrong IP address on your system, DNS misconfiguration on the domain controller (DC) side, or ports that are blocked on the firewall.

If you do not know the root of the problem, I suggest proceeding through these troubleshooting options in order. However, if you have additional information, feel free to proceed directly to the step that you think is likely to solve the problem.

Verify that the IP Settings are Correct

Make sure that the network interface of your computer has the right IP address. The IP address can be explicitly defined in the network adapter settings or can be obtained from a DHCP server. To get the computer's current network settings, use this command:

```
ipconfig /all
```

ad4.webp

Make sure the DNS Client Service is Running

Next, check whether the DNS client service is up and running using this command:

```
Get-Service dnscache
```

ad5.webp

Check the Host File for Domain Entries

Make sure there are no entries for your domain or domain controller names in the hosts file located at `C:\Windows\System32\Drivers\etc\hosts` on the PC. Open the file with Notepad or any other text editor. If there are any entries for your domain or DC names, delete them.

To view the contents of the hosts file on the PC, use this command:

```
get-content C:\Windows\System32\Drivers\etc\hosts
```

ad6.webp

Restart the DNS Cache Service

Open an elevated command prompt and clear the DNS cache using this command:

```
ipconfig /flushdns
```

Then stop and restart the dnscache service using this command:

```
net stop dnscache && net start dnscache
```

ad7.webp

Alternatively, you can use the Service.msc console. Right-click on `DNS Client` to open its properties dialog:
ad8.webp

Click use the `Stop` and `Start` buttons to stop and restart the service:

ad9.webp

Check whether the DC is Reachable from the Client

To determine whether the domain controller is reachable from the client, first run the following commands from a command prompt:

```
ping your_domain_name.com
```

ad10.webp

Then run this command:

```
tracert your_domain_name.com
```

ad11.webp

You should also check the availability of the DC from another workstation on the same network. If your client cannot access the DC but other clients can, there could be a problem with your client's cable or hardware, or with a device in the middle. To narrow down the problem, try a different network jack or go wireless.

Check the DC's Accessibility using PowerShell

Alternatively, you can use the following PowerShell cmdlets to check the connectivity to the DC.

To display the IP address:

```
Get-NetIPConfiguration –All
```

ad12.webp

To ping the DC:

```
Test-NetConnection domainname
```

ad13.webp

To trace the routes to the DC:

```
Test-NetConnection –TraceRoute domainname
```

ad14.webp

Add the DNS server to the TCP/IP settings of your Network Adapter

If the domain controller can be reached, try adding the IP address of your DNS server to your network adapter's Advanced TCP/IP settings.

1. Open `Control Panel`, click `Network and Sharing Center`, and then click `Change adapter settings`:
   ad15.webp

ad16.webp

2. Right-click on the network adapter and select `Properties`.
   ad17.webp
3. Right-click on `Internet Protocol Version 4 (TCP/IPv4)` and choose `Properties`.
4. Click the `Advanced` button and go to the DNS tab.
5. On the `DNS` tab, click the `Add` button, provide the IP address of your DNS server and click `OK`. (Note that the DNS server might be a DC, especially if it's a small organization.)
   ad18.webp
6. If multiple IP addresses are listed, use the arrow buttons to move your preferred one to the top of the list. Then click `OK`.
   ad19.webp
7. Click `OK` again to save your changes.
8. Restart the workstation or server so the changes will take effect, and try again to join the workstation or server to the Active Directory domain.

Check whether you're using the Right DNS servers

Before you go too deep down the rabbit hole, double-check that you are using the correct DNS servers. Specifically, the DNS servers that DCs are aware of are used to register records that help AD-connected devices locate resources like DCs; DNS servers that are not AD-integrated do not have these records.

According, make sure you are using one of the following:

- A DNS server with Active Directory integration
- A DNS server that replicates records from another DNS server that is aware of Active Directory
- A DNS server configured to query either an AD-integrated DNS server or a DNS server with duplicated records via forwarding

To check that your DNS server is one of these, use the PowerShell cmdlet shown below in a PowerShell session on a domain-joined PC. (If you don't have another domain client to use, you will need to contact your network staff.)

```
Get-DnsClientServerAddress
```

ad20.webp
The DNS servers used by the computer running the cmdlet are listed in the ServerAddesses column.

Option 1: Update the Computer’s DNS Client Settings

If you need to update the computer’s DNS client settings, you can use the following cmdlet:

```
Set-DnsClientServerAddress
```

Alternatively, you can use the IPv4 Properties dialog box for the computer’s network card: Go to Control Panel –> Network –> Internet –> Network Connections. Then right-click on the network card, select `Properties` and then `Internet Protocol Version 4 (TCP/IPv4)`, and then `Properties`. Review the settings:
ad21.webp
If the network supports Dynamic Host Configuration Protocol (DHCP), ensure that both the `Obtain an IP address automatically` and `Obtain DNS server address automatically` boxes are checked.

If your network does not use DHCP, change the values for `Preferred DNS server` and `Alternative DNS server` to the ones you found previously (when you ran the `Set-DnsClientServerAddress` cmdlet).

Option 2: Connect to the Domain through Windows Settings

Another option is to connect to the domain through Windows Settings:

1. Press the `Windows` and `I` keys on your keyboard to open the Window Settings window.
2. Click `Accounts`.
   ad22.webp
3. In the left menu, click `Access work or school`. Then click `Connect`.
   ad23.webp
4. At the bottom of the Microsoft account window, click `Join this device to a local Active Directory domain`.
   ad24.webp
5. Provide a valid, contactable domain name and click `Next`.
   ad25.webp
6. Next, provide a domain account to use for joining this workstation to a domain. This account must have the permissions to join a workstation to a domain. Click `OK`.
   ad26.webp
7. If you do not get an error, your workstation is now joined with the domain. On the next screen, provide a user account for this PC and then click `Next`.
   ad27.webp
8. Click `Restart` so your changes will take effect.

Check whether a Firewall is blocking port 53 on the DC

Check whether the DNS service on the DC is being blocked by a firewall. To see whether port 53 is available on the DC, use this cmdlet:

```
test-netconnection 172.168.5.160 -port 53
```

Check the value of “TcpTestSucceeded”. A value of “True” as shown below indicates that the DNS service on the DC is operational.
ad28.webp

Check whether your Computer can resolve the Domain Name of the DC

Next, check whether the workstation can accurately resolve the domain name to the DC’s IP address. Use the fully qualified domain name of the domain to which you are trying to join your workstation with the Resolve-DNSName cmdlet, as shown here:

```
Resolve-DNSName fabrikam.local
```

ad29.webp
This command should return one or more DNS server records.

Check whether the Workstation can Contact the DNS server that hosts the DNS zone

Next, check whether:

- The computer can communicate with the DNS server that hosts the DNS zone or resolves DNS names for the domain.
- The DNS server for the client is configured correctly and that it is connected to it.
- You can find a domain and connect to the DC from your computer.

To get the domain and DC information, along with the IP address, use the following cmdlet:

```
nltest /dsgetdc:fabrikam.local
```

ad30.webp

If the command completes successfully, it will return information like the following:

```
DC: \\FRGC1.fabrikam.local
Address: \\10.20.6.41
Dom Guid: c64586c9-2c18-4fc4-9fe1-18f2a262d90d
Dom Name: fabrikam.local
Forest Name: fabrikam.local
Dc Site Name: Default-First-Site-Name
Our Site Name: Default-First-Site-Name
Flags: PDC GC DS LDAP KDC TIMESERV WRITABLE DNS_DC DNS_DOMAIN DNS_FOREST CLOSE_SITE
FULL_SECRET WS DS_8 DS_9 DS_10
The command completed successfully
```

Restart the Netlogon Service on the Domain Controller

Restart the Netlogon service on the DC using this command:

```
net stop netlogon && net start netlogon
```

ad31.webp

Alternatively, simply reboot the DC.

When the server restarts, it will try to register the necessary SRV records on the DNS server.

Re-register the DC’s DNS records

Re-register the DC’s DNS records by running this command:

```
ipconfig /registerdns
```

ad32.webp
Wait for the records to arrive in DNS and for them to propagate across the domain.

Original Article

Revision #1
Created 2023-11-10 05:08:08 UTC by Ryan
Updated 2025-02-12 01:12:25 UTC by Ryan