Enabling RDP in Directory Services Restore Mode (DSRM)

This procedure allows you to remote into a Domain Controller while it is booted into **Directory Services Restore Mode (DSRM)** using RDP. This is not officially supported by Microsoft and should be used only for recovery and troubleshooting.

⚠ Important

- Use this only on isolated or lab systems, or during controlled recovery windows.
- RDP in DSRM temporarily changes Safe Mode behavior and weakens security.
- Always remove these changes once recovery activities are complete.

---

1. Prerequisites

- Server is a Domain Controller running Windows Server (2016+ recommended).
- You can log on locally (console or hypervisor console) as a local Administrator / DSRM Administrator.
- You know the **DSRM password** for the server.

DSRM Logon Format

When using RDP in DSRM, you must log on as: `.\Administrator` (local account) using the **DSRM password**, not the domain password.

---

2. Boot the Domain Controller into DSRM

1. On the DC, run:

```
bcdedit /set safeboot dsrepair
```

2. Reboot the server.
3. The DC will start in **Directory Services Restore Mode** (Safe Mode). Log on using the **DSRM Administrator** credentials.

Tip

After you are done with recovery work, remember to remove SafeBoot:

```
bcdedit /deletevalue safeboot
```

---

3. Enable the RDP Service in Safe Mode

By default, the Remote Desktop Services (TermService) service does not start in Safe Mode / DSRM. We add a SafeBoot registry entry to allow it.

1. Open an elevated **Command Prompt** or **PowerShell** window.
2. Run the following command to allow TermService in Safe Mode with Networking:

```
REG ADD
"HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\TermService"
/VE /T REG_SZ /D "Service" /F
```

3. Start the Remote Desktop service:

```
net start TermService
```

Note

If you see an error that dependencies are not running, complete the networking steps below and then re-run `net start TermService`.

---

4. Enable Networking in DSRM

DSRM typically starts with minimal or no networking. To allow RDP, we must enable some core network services.

1. Add the MSIServer entry under SafeBoot (helps some services start correctly):

```
REG ADD
"HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\MSIServer"
/VE /T REG_SZ /D "Service" /F
```

2. Start key networking services (run what is applicable; some may already be running or may not exist on all builds):

```
net start msiserver
net start nlasvc
net start dhcp
net start dnscache
```

3. Start Remote Desktop Services again (if needed):

```
net start TermService
```

Verification

Confirm that RDP is listening on TCP 3389:

```
netstat -ano | findstr 3389
```

If you see a `LISTENING` entry on port 3389, the RDP listener is active.

---

5. Allow RDP Through the Firewall

Group Policy is not processed normally in DSRM, so we explicitly open the RDP firewall rule set.

1. Enable the built-in Remote Desktop firewall group:

   ```
   netsh advfirewall firewall set rule group="remote desktop" new
   enable=Yes
   ```

2. (Optional) For lab or emergency use, you may temporarily disable the firewall entirely:

   ```
   netsh advfirewall set allprofiles state off
   ```

Security Warning

Do not leave the firewall disabled longer than necessary. Re-enable it or restore normal security once recovery is complete.

---

6. Connect via RDP in DSRM

1. From an admin workstation, open **Remote Desktop Connection** (mstsc).
2. Connect to the server using its IP address or hostname.
3. When prompted for credentials, use:
   1. **Username:** `.\Administrator`

2. **Password:** the **DSRM password** (set when the DC was promoted).

You should now have a full RDP session into the server while it is in **Directory Services Restore Mode**, allowing you to run tools like **NTDSUTIL**, copy recovery files, and perform other repair tasks more comfortably.

---

7. Cleanup After Recovery

Once you have finished your AD repair or recovery work and are ready to return the DC to normal operation, perform the following cleanup.

7.1 Remove Safe Mode / DSRM Boot

1. From an elevated command prompt:

```
bcdedit /deletevalue safeboot
```

2. Reboot the server into normal mode.

7.2 Remove the SafeBoot TermService Override

1. Open an elevated command prompt.
2. Delete the TermService SafeBoot entry:

```
REG DELETE
"HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\TermService"
/F
```

7.3 Restore Normal Firewall Settings

- If you disabled the firewall, re-enable it:

```
netsh advfirewall set allprofiles state on
```

- Validate that only the expected firewall rules are enabled for RDP and other services.

Summary

By adding TermService and MSIServer to the SafeBoot configuration, starting a minimal set of networking services, and enabling the RDP firewall rules, you can securely RDP into a Domain Controller while it is in DSRM. Remember to remove these changes once recovery is complete to return the server to its standard, hardened state.

Revision #1
Created 2025-11-30 13:07:04 UTC by joliveira
Updated 2025-11-30 13:07:18 UTC by joliveira