GUIDE
RDP Troubleshooting for AWS Users

v1.0.0

Author:

Eldon Gabriel

August 31, 2025

TABLE OF CONTENTS

REVISION HISTORY

Version	Date	Author	Description of Changes
v1.0.0	08/31/2025	Eldon G.	Initial draft.

1.0 PROJECT OVERVIEW

1.1 Objective

Troubleshoot Remote Desktop Protocol (RDP) access issues for a user account on an AWS-hosted Windows 10 virtual machine and ensure proper remote login functionality.

1.2 Scope

Focused on Windows account management, group membership verification, RDP configuration, and validation.

Disclaimer: This guide was created as part of independent lab practice to troubleshoot Remote Desktop Protocol (RDP) access issues in an AWS cloud-hosted Windows environment. It is intended for portfolio demonstration only and is not official course material.

2.0 ISSUE IDENTIFICATION

2.1 Problem

The newly created user account could not log in via Remote Desktop (RDP) to the AWS-hosted Windows 10 VM.

2.2 Initial Observations

- The new user account was visible in **Local User Management**, but it did not appear in the AWS VM's Start Menu sign-in options.

- On AWS Windows 10 VMs, the RDP session automatically configures a dedicated user account in the registry. This means the standard local login process isn't available—logon and logoff actions only work with that single dedicated account.

- To allow a user account to access the VM, a new RDP connection profile was created specifically for that user, enabling remote recognition without modifying the default dedicated account.

3.0 TROUBLESHOOTING STEPS

3.1 Local Group Membership

- Verified the user account was created and active in Local User Management.
- Confirmed membership in the **Remote Desktop Users** group.

3.1.1 Why It Matters

RDP relies on this group for access validation; without it, logins are denied regardless of account status

---

3.2 RDP Settings

- Opened `sysdm.cpl` → **Remote** tab.
- Checked **Allow remote connections to this computer**.
- Enabled **Allow connections only from computers running Remote Desktop with Network Level Authentication** (recommended).

3.2.1 Why It Matters

These settings let you secure RDP connections and make sure the system only accepts trusted users.

3.3 Adding a User to RDP (CLI Automation)

GUI Method:

- Open `sysdm.cpl` → Remote **tab** → **Select Users** → **Add** → Enter `[User Name]` → **Check Names** → **OK** → **Apply** → **OK.**

Command-Line Method (Concrete Example with Dummy User):

```cmd
net localgroup "Remote Desktop Users" Eldon /add
```

Automation Context:

This command can be incorporated into a batch script to add multiple users at once:

```cmd
@echo off

# REM Add multiple users to the Remote Desktop Users group

net localgroup "Remote Desktop Users" Eldon /add
net localgroup "Remote Desktop Users" User2 /add
net localgroup "Remote Desktop Users" User3 /add
echo All users added successfully
```

Using this approach allows for repeatable deployments or onboarding of multiple accounts on VMs without manually navigating the GUI.

3.3.1 Why It Matters

Explicitly granting RDP rights via the command line ensures users can access the system even if the VM doesn't automatically recognize them, and it supports automated provisioning in enterprise or cloud environments.

3.4 Firewall and Policy Checks

Verified inbound firewall rules:

- Opened **Windows Defender Firewall with Advanced Security → Inbound Rules**.
- Ensured **Remote Desktop (TCP-In)** was enabled on port 3389.

Checked Group Policy restrictions:

- `gpedit.msc` → **Computer Configuration → Administrative Templates → Windows Components → Remote Desktop Services → Remote Desktop Session Host**.
- Confirmed: **Allow users to connect remotely using Remote Desktop Services** was set to *Enabled*.

3.4.1 Why It Matters

Working with cloud environments can introduce additional issues. Firewalls and policy restrictions often stop RDP attempts. Your local settings might be fine, but the connection still fails.

4.0 RESOLUTION & VALIDATION

- Created a new RDP connection profile for a user account, allowing the account to be recognized remotely on the AWS VM.
- This resolved the issue of the dedicated RDP session only permitting the initially provisioned user, enabling the user account to log in without shutting down the VM.
- With the new session active, the exercise “Use the Windows registry to restrict the permissions of untrusted user accounts” could be completed successfully.
- Ran `whoami` within the remote session to confirm the correct user identity.
- Documented final group membership, RDP configuration, and firewall/policy settings to ensure repeatable access and proper permissions.

5.0 KEY TAKEAWAYS

- A local account must be properly surfaced at the VM level before it can authenticate through RDP.
- Membership in the **Remote Desktop Users** group is a required step for enabling access.
- Firewall rules and Group Policy checks are essential when troubleshooting cloud-hosted RDP issues.
- A systematic approach beginning with local permissions, then validating RDP configuration, and finally testing firewall/policy behavior is the most efficient way to resolve RDP failures.