SysAdmin has Restricted the Types of Logon_RDP SSH

Last updated by | Kevin Gregoire | Oct 21, 2022 at 9:06 AM PDT


Tags
cw.TSG   cw.RDP-SSH

Contents

- Symptoms
    - Reference
- Root Cause Analysis
    - Tracking close code for this volume
- Customer Enablement
- Refresher / Training Template
- Mitigation

- Need additional help or have feedback?

Symptoms

1. You get below error when you try to RDP to the Azure VM through the RD gateway.

   ```
   The system administrator has restricted the types of logon (network or interactive) that you may use. For
   assistance, contact your system administrator or technical support.
   ```
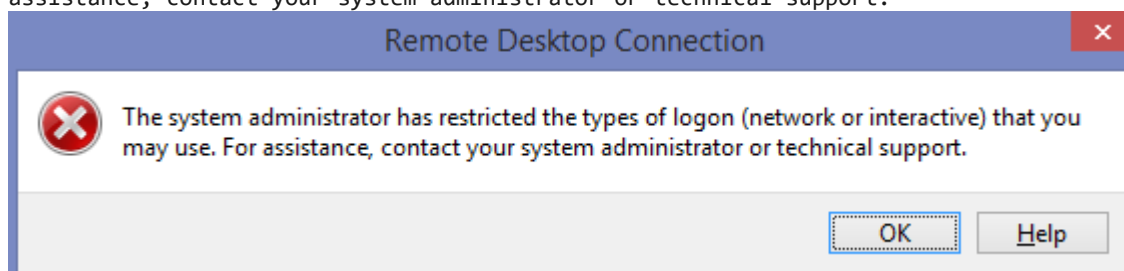

Reference

- secedit ↗
- UserRights PowerShell Module ↗

Root Cause Analysis

There's a policy that is applied on this machine that is setting the VM to deny connections in the network.

Tracking close code for this volume

Root Cause	Product	Support Topic	Cause Tracking code	Bug
1	*Azure Virtual Machine – Windows*	*Routing Azure Virtual Machine V3\Cannot Connect to my VM\Failure to connect using RDP or SSH port*	*Root Cause - Windows Azure\Virtual Machine\Guest OS - Windows\Identity\Azure Active Directory\Misconfiguration*	

To know how to flag a bug on a case please refer to [How to do Proper Case Coding](#)

Customer Enablement

https://docs.microsoft.com/en-us/windows-server/remote/remote-desktop-services/troubleshoot/cannot-authenticate-or-must-authenticate-twice#access-denied-restricted-type-of-logon ⧉

Refresher / Training Template

- For the purpose of training or following along with this TSG, you can use the following link to deploy a VM with this scenario built-in. You will need to enable JIT for the VM. This lab is not to be shared with customers.

[Deploy to Azure]

Mitigation

Note: Please do not apply the below mitigations to a **Domain Controller!** Engage **Windows Directory Services team** for issues impacting a domain controller for further assistance.

1. Ask the customer to ensure the following policies are setup to allow the built-in administrators to start up with (minimum access) and also to not deny this access over the network:

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Allow log
Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Deny acce
Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Deny log
```
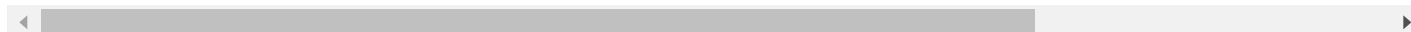
2. You can still mitigate the issue applying to the VM the **Default Standard Security Template** with the built-in tool *Secedit.exe* (located in %windir%\system32).

   1. You can use any method available to apply the security template (Run Command, Custom Script Extension, Serial Console CMD Channel, remote management like [PsExec](#) or [Remote PowerShell](#))
   2. Running the below command which will export to a TXT file the current user rights:
      ```
      secedit /export /areas USER_RIGHTS /cfg C:\temp\UserRightsBefore.txt
      ```
   3. Now run the below command which will apply the Default Standard Security Template to the VM
      ```
      secedit /configure /cfg C:\Windows\inf\defltbase.inf /db defltbase.sdb /verbose
      ```

4. After you recover the access to the VM using RDP, you can run the below command to compare the security applied to the VM:

```
secedit /export /areas USER_RIGHTS /cfg C:\temp\UserRightsAfter.txt
```

Need additional help or have feedback?

To engage the Azure RDP-SSH SMEs...	To provide feedback on this page...	To provide kudos on this page...
Please reach out to the **RDP-SSH SMEs** ↗ for faster assistance. Make sure to use the **Ava process** for faster assistance.	Use the **RDP-SSH Feedback** form to submit detailed feedback on improvements or new content ideas for RDP-SSH. ***Please note*** the link to the page is required when submitting feedback on existing pages! If it is a new content idea, please put N/A in the Wiki Page Link.	Use the **RDP-SSH Kudos** form to submit kudos on the page. Kudos will help us improve our wiki content overall! ***Please note*** the link to the page is required when submitting kudos!