

Internal error - MachineKeys_RDP SSH

Last updated by | Kevin Gregoire | Nov 9, 2022 at 1:31 PM PST

Tags

[cw.TSG](#)[cw.RDP-SSH](#)

Contents

- [Symptoms](#)
- [Root Cause Analysis](#)
- [ONLINE Troubleshooting](#)
- [ONLINE Mitigation](#)
- [OFFLINE Troubleshooting](#)
- [OFFLINE Mitigation](#)
- [Customer Enablement](#)
- [Refresher / Training Template](#)
- [Need additional help or have feedback?](#)

Symptoms

1. In the Guest OS logs you could find:

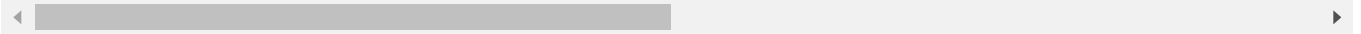
1. In **System** you could find event 1058 and/or event 1057 as the following:

Log Name: System
Source: Microsoft-Windows-TerminalServices-RemoteConnectionManager
Date: 6/12/2016 12:53:55 PM
Event ID: 1058
Task Category: None
Level: Error
Keywords: Classic
User: N/A
Computer: contoso
Description:

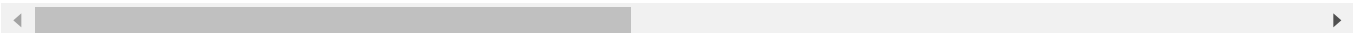
The RD Session Host Server has failed to replace the expired self signed certificate used for RD



Log Name: System
 Source: Microsoft-Windows-TerminalServices-RemoteConnectionManager
 Date: 6/12/2016 12:53:55 PM
 Event ID: 1058
 Task Category: None
 Level: Error
 Keywords: Classic
 User: N/A
 Computer: contoso
 Description:
 RD Session host server has failed to create a new self-signed certificate to be used for RD Sess:



Time: 7/18/2019 8:08:07 PM
 ID: 1057
 Level: Error
 Source: Microsoft-Windows-TerminalServices-RemoteConnectionManager
 Machine: contoso.local
 Message: The RD Session Host Server has failed to create a new self signed certificate to be used

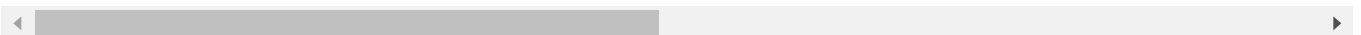


2. In **System** you could also find event 36870 with error codes *0x8009030D* or *-2146893043* which stands for *SEC_E_UNKNOWN_CREDENTIALS* as the following:

Log Name: System
 Source: Schannel
 Date: 10/31/2016 9:37:55 AM
 Event ID: 36870
 Task Category: None
 Level: Error
 Keywords:
 User: SYSTEM
 Computer: contoso.local
 Description:
 A fatal error occurred when attempting to access the TLS server credential private key. The error



Time: 7/28/2019 5:49:19 AM
 ID: 36870
 Level: Error
 Source: Schannel
 Machine: contoso.local
 Message: A fatal error occurred when attempting to access the SSL server credential private key



3. In **Windows Remote Desktop Services** you could also find event 226:

Log Name: Microsoft-Windows-RemoteDesktopServices-RdpCoreTS/Operational
 Source: Microsoft-Windows-RemoteDesktopServices-RdpCoreTS
 Date: 17/10/2016 09:36:52 p.m.
 Event ID: 226
 Task Category: RemoteFX module
 Level: Warning
 Keywords:
 User: NETWORK SERVICE
 Computer: contoso.local
 Description:
 RDP_TCP: An error was encountered when transitioning from StatePreparingX224CC in response to Ev

2. In **WinGuestAnalyzer\Health Signal** tab you can see the thumbsprint of the certificate tied to the RDP listener. You could tell if it is expired by looking at the expiration date:

```

{
  "remoteAccess": {
    "windows": {
      "rdpPort": 3389,
      "rdpEnabled": true,
      "rdpTcpListenerSecurityConfiguration": {
        "nlaUserAuthenticationRequired": true,
        "authenticationSecurityLayer": "TLS",
        "protocolNegotiationAllowed": true
      },
      "rdpTcpListenerMaxConnections": 2,
      "rdpFirewallAccess": "Allowed",
      "rdpAllowedUsers": [
        "BLSVR"
      ],
      "rdpCertificateDetails": {
        "subject": "CN=AZ-SFTP01",
        "thumbprint": "D631CBA7538EF80BA193881F90A05C30435CE5EE",
        "validFrom": "2017-03-06T21:32:23Z",
        "validTo": "2017-09-05T21:32:23Z"
      },
      "rdsLicensingStatus": null
    }
  }
}

```

Root Cause Analysis

Something is preventing the RDP Application to access the local RSAs keys under the MachineKeys folder on the VM. Usually this happens when:

1. Wrong set of Access Control Lists (ACL)s in the Machinekeys folder and/or the RSAs files.
2. Corrupted/missing RSA key.
3. RSA certificate expired.

ONLINE Troubleshooting

Before you start any mitigation please make sure you follow the [premitigation steps](#), if they are applicable.

ONLINE Mitigation

1. Setup the correct permissions on the **RDP Certificate** and its folder. You could do this in multiple ways:
 1. If you have a working Azure Agent, you can use [Custom Script Extension](#) to push the [Restore RSA MachineKeys Folder Access.ps1](#) script

Note: The script will:

1. Take ownership of the MachineKeys folder
 2. Reset the Permissions of this folder and all the files within
 3. Create two logs file, one before the script (c:\temp\BeforeScript_permissions.txt) and another after the script (c:\temp\AfterScript_permissions.txt)
2. Once the access over the RSA files and its holding folder were ensured to be accurate, if the problem is still not resolved, you could force the OS to renew the RDP certificate. Please refer to [How to renew the RDP Self sign certificate remotely](#).

OFFLINE Troubleshooting

Before you start any mitigation please make sure you follow the [premitigation steps](#), if they are applicable.

OFFLINE Mitigation

▼ Click here to expand or collapse this section

Applies to Citrix VMs

1. Refer to *Mitigation 2* on [Fail RDP connection on a Citrix VM](#)

Customer Enablement

- [An internal error occurs when you try to connect to an Azure VM through Remote Desktop](#) ☑
- [Remote desktop connection is sometimes stuck on the Securing remote connection screen](#) ☑

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.



1. If this doesn't work out, please reach out to the [Unable to RDP-SSH SME channel on teams](#) ☑ for advise providing the case number, issue description and your question
2. If the RDP SMEs are not available to answer you, you could engage the RDS team for assistance on this.
 1. Ensure you collect the Windows Performance SDP package from the VM and upload that into the DTM workspace.
 1. This would be easily done by running the following script on Serial Console on a powershell instance:

```
#Create a download location and setup the console to prioritize TLS1.2 connections
remove-module psreadline
[Net.ServicePointManager]::SecurityProtocol = "tls12, tls11, tls"
md c:\temp

#Download the Windows SDP file
$source = "https://aka.ms/getTSSv2"
$destination = "c:\temp\TSSv2.zip"
$wc = New-Object System.Net.WebClient
$wc.DownloadFile($source,$destination)

#Expand and run the SDP package for Setup, Network and Performance
Expand-Archive -LiteralPath $destination -DestinationPath C:\temp

#recommended to run the new packages:
C:\temp\TSSv2.ps1 -SDP Setup
C:\temp\TSSv2.ps1 -SDP NET
C:\temp\TSSv2.ps1 -SDP Perf

#Note: you still can run old SDP packages, in case is required:
C:\temp\psSDP\Get-psSDP.ps1 Setup
C:\temp\psSDP\Get-psSDP.ps1 Net
C:\temp\psSDP\Get-psSDP.ps1 Perf
```

2. Collect the following files to the DTM workspace of this case:

1. C:\MS_DATA\SDP_Setup\tss_DATETIME_COMPUTERNAME_psSDP_SETUP.zip
2. C:\MS_DATA\SDP_NET\tss_DATETIME_COMPUTERNAME_psSDP_NET.zip
3. C:\MS_DATA\SDP_Perf\tss_DATETIME_COMPUTERNAME_psSDP_PERF.zip


2. Cut a problem with the following details:

- Product: **Azure\Virtual Machine running Windows**
- Support topic: **Routing Issue with Remote Desktop Service (RDS) on Azure\Issue with connectivity using RDS**

If you are uncertain that we may need this snapshot by the end of this case for RCA purposes, then just leave it.

1. If the issue is already fix and no further RCA analysis is needed, then proceed to remove the OS Disk backup we created at the beginning of the case
 1. If the **disk is managed** using the portal so the snapshot section and select the snapshot you created previously as a backup.
 2. If the **disk is unmanaged** then
 1. If this is an CRP Machine - ARM, then no further action is required
 2. If this is an Classic - RDFS machine, then
 1. Check the storage account where the OS disk of this machine is hosted using [Microsoft Azure Storage Explorer](#) ☑ right click over the disk and select *Managed Snapshots*
 2. Proceed to delete the snapshot of the broken machine

Need additional help or have feedback?

<i>To engage the Azure RDP-SSH SMEs...</i>	<i>To provide feedback on this page...</i>	<i>To provide kudos on this page...</i>
<p>Please reach out to the RDP-SSH SMEs  for faster assistance.</p> <p>Make sure to use the Ava process for faster assistance.</p>	<p>Use the RDP-SSH Feedback form to submit detailed feedback on improvements or new content ideas for RDP-SSH.</p> <p>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.</p>	<p>Use the RDP-SSH Kudos form to submit kudos on the page. Kudos will help us improve our wiki content overall!</p> <p>Please note the link to the page is required when submitting kudos!</p>