SPP-1509: Rackspace Win Server 2019 PCI Hardening

Document Type: Standard Operating Procedure

Table of Contents

SPP-1509: Rackspace Win Server 2019 PCI Hardening 1

Document Type: Standard Operating Procedure 1

1. Purpose – 2

2. Scope – 2

3. Prerequisites – 2

4. Responsibilities – 3

5. Script Settings 4

5.1 Introduction 4

5.2 What the Script Does/Affects 5

6. References 14

1. Purpose –

Explaining the Windows Server 2019 Rackspace PCI Hardening Script (an updated version of the legacy Lockdown.bat file ran for the legacy Datapipe customers).

2. Scope –

Customers and Clients of Rackspace who may need to understand what changes the script is making.

3. Prerequisites –

1. Operating system must be: Windows Server 2019.
2. PowerShell must be: Installed (this is the default from Microsoft, however should be confirmed).

4. Responsibilities –

1. Must be aware of whether the customer is requesting this for a domain joined machine or not.
    a. Also must be aware of whether this is being run on a Domain Controller or not.
2. (After script is run) Must ensure to check the Windows "Event Viewer" > Applications and Services Logs" > "Rackspace Hardening" log.
    a. This is where all tracking of the script running is logged to. This will report both successful and failure attempts. Failures may be caused due to services not present or various other items, regardless of the reasoning, should be reviewed.
    b. The "Rackspace Hardening" log is now also copied into the Zip file created after the script is run for historical and evidence purposes.
3. (After script is run) Confirm that the hardening Registry Key is present so that the successful application is reported to BigFix for tracking.
    a. 32-Bit Applications: HKEY_LOCAL_MACHINE\Software\Rackspace\Hardening
    b. 64-Bit Applications: HKEY_LOCAL_MACHINE\Software\WOW6432Node\Rackspace\Hardening

4. (After script is run) Confirm that the following folder is present and has backed up information present:
    a. C:\Windows\Datapipe
5. (For Domain Controllers) The script does import two policies for hardening purposes however it does NOT overwrite the Default Domain Policy or the Default Domain Controllers Policy. In order to enact these, the **customer** must decide whether to implement the policies.
    a. See the CIS_Server_2019_GPO.xlsx Excel spreadsheet which outlines which policies were or were not implemented in the policies, the reasonings, and the settings.
    b. They may also choose to copy the GPO and redact some of the settings. This choice **MUST** be made by the customer, as they are according to PCI settings however could potentially impact services/applications.
    c. When rolling back hardening, the Group Policies which were added are removed.

5. Script Settings

5.1 Introduction

This document explains the Windows Server 2019 Datapipe Hardening PowerShell script. This script was created as an update to the legacy "Datapipe_Windows_OS_Hardening"/"Lockdown.bat" script.

The reasons for this update are as follows:

1. The "Lockdown.bat" script is an older script form which is presently outpaced and outdated due to PowerShell becoming the main scripting tool of Windows.
2. The "Datapipe_Windows_OS_Hardening"/"Lockdown.bat" script was not documented at all, and pulled on legacy tools which are either no longer relevant, no longer recognized, or simply have been removed/no longer function in the script any further.
3. The last update of the Lockdown.bat was for Windows Server 2012 R2. This is a much older script which required modifications to address new challenges and issues with new PCI Requirements and System requirements to sufficiently meet our necessary testing & auditing needs.

The below outlines the settings which are being configured and can provide understanding to customers/clients who need to know what is being updated.

5.2 What the Script Does/Affects

- Function LocalPol-Backup:
  - This function simply makes a copy of the local policy that is already in place for safe keeping. Since we later import a local policy which is hardened, this may be needed for roll back if problems occur.
  - The backup copy is placed in the same ZIP file that the Log and other things are backed up to in C:\Windows

- Function Backup-Reg:
  - This function backs up all of the registry keys that are effected by the next function which hardens the registry.
  - The backup copy is placed in the same Zip file that the Log and Local Policy is backed up to in C:\Windows.

- Function Reg-Harden:
- All of the functions of the Registry keys which are added via the Reg-Harden function are aimed at meeting the PCI guidelines for SSL/TLS protocol and Cipher suites. Outside of those which have an extra line noted in Red below.
  - [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters]
    - "keepalivetime"=dword:000493e0
    - "tcpmaxdataretransmissions"=dword:00000003
    - PCI DSS Finding: 18.4.5 - An attacker who is able to connect to network applications could establish numerous connections to cause a DoS condition.

  - [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Security]
    - "WarningLevel"=dword:0000005a
    - PCI DSS Finding: 18.4.12 - If the Security log reaches 90 percent of its capacity and the computer has not been configured to overwrite events as needed, more recent events will not be written to the log. If the log reaches its capacity and the computer has been configured to shut down when it can no longer record events to the Security log, the computer will shut down and will no longer be available to provide network services.

  - [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters]
    - "DisableIPSourceRouting"=dword:00000002
    - PCI DSS Finding: 18.4.2 - An attacker could use source routed packets to obscure their identity and location. Source routing

allows a computer that sends a packet to specify the route that the packet takes.

- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager]
  - "SafeDllSearchMode"=dword:00000001
  - PCI DSS Finding: 18.4.8 - If a user unknowingly executes hostile code that was packaged with additional files that include modified versions of system DLLs, the hostile code could load its own versions of those DLLs and potentially increase the type and degree of damage the code can render.

- [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon]
  - "AutoAdminLogon"="0"
  - PCI DSS Finding: 18.4.1 - If you configure a computer for automatic logon, anyone who can physically gain access to the computer can also gain access to everything that is on the computer, including any network or networks that the computer is connected to. Also, if you enable automatic logon, the password is stored in the registry in plaintext. The specific registry key that stores this setting is remotely readable by the Authenticated Users group. As a result, this entry is appropriate only if the computer is physically secured and if you ensure that untrusted users cannot remotely see the registry.

- [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon]
  - "ScreenSaverGracePeriod"="0"
  - PCI DSS Finding: 18.4.9 - The default grace period that is allowed for user movement before the screen saver lock takes effect is five seconds. If you leave the default grace period configuration, your computer is vulnerable to a potential attack from someone who could approach the console and attempt to log on to the computer before the lock takes effect. An entry to the registry can be made to adjust the length of the grace period.

- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL]
  - "EventLogging"=dword:00000001

- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers]

- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\AES 128/128]
  - "Enabled"=dword:ffffffff
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\AES 256/256]
  - "Enabled"=dword:ffffffff
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\DES 56/56]
  - "Enabled"=dword:00000000
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\NULL]
  - "Enabled"=dword:00000000
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC2 128/128]
  - "Enabled"=dword:00000000
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC2 40/128]
  - "Enabled"=dword:00000000
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC2 56/128]
  - "Enabled"=dword:00000000
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 128/128]
  - "Enabled"=dword:00000000
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 40/128]
  - "Enabled"=dword:00000000
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 56/128]
  - "Enabled"=dword:00000000
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 64/128]
  - "Enabled"=dword:00000000

- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\Triple DES 168/168]
  - "Enabled"=dword:ffffffff
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\CipherSuites]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Hashes]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Hashes\MD5]
  - "Enabled"=dword:00000000
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Hashes\SHA]
  - "Enabled"=dword:ffffffff
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Hashes\SHA256]
  - "Enabled"=dword:ffffffff
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Hashes\SHA384]
  - "Enabled"=dword:ffffffff
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Hashes\SHA512]
  - "Enabled"=dword:ffffffff
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\KeyExchangeAlgorithms]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\KeyExchangeAlgorithms\Diffie-Hellman]
  - "Enabled"=dword:ffffffff
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\KeyExchangeAlgorithms\ECDH]
  - "Enabled"=dword:ffffffff
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\KeyExchangeAlgorithms\PKCS]

        - "Enabled"=dword:ffffffff

    - [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols]

    - [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\Multi-Protocol Unified Hello]

    - [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\Multi-Protocol Unified Hello\Server]
        - "Enabled"=dword:00000000

    - [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\PCT 1.0]

    - [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\PCT 1.0\Server]
        - "Enabled"=dword:00000000

    - [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0]

    - [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0\Client]
        - "DisabledByDefault"=dword:00000001

    - [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0\Server]
        - "Enabled"=dword:00000000

    - [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0]

    - [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Server]
        - "Enabled"=dword:00000000

    - [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0]

    - [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Server]
        - "Enabled"=dword:ffffffff
        - "DisabledByDefault"=dword:00000000

- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Client]
  - "Enabled"=dword:00000001
  - "DisabledByDefault"=dword:00000000
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Server]
  - "Enabled"=dword:ffffffff
  - "DisabledByDefault"=dword:00000000
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2]
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client]
  - "Enabled"=dword:00000001
  - "DisabledByDefault"=dword:00000000
- [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server]
  - "Enabled"=dword:ffffffff
  - "DisabledByDefault"=dword:00000000
- [HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Cryptography\Configuration\SSL\00010002]
  - "Functions"="TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P384,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P521,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P256,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P521,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256_P256,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256_P384,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256_P521,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384_P384,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384_P521,TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P256,TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P384,TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P521,TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384_P384,TLS_ECDHE_EC

DSA_WITH_AES_256_GCM_SHA384_P521,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P521,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P256,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P384,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P521,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P256,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P384,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P521,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P256,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P384,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P521,TLS_DHE_DSS_WITH_AES_128_CBC_SHA256,TLS_DHE_DSS_WITH_AES_256_CBC_SHA256,TLS_DHE_DSS_WITH_AES_128_CBC_SHA,TLS_DHE_DSS_WITH_AES_256_CBC_SHA,TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_3DES_EDE_CBC_SHA"

- Import-LocalPols –
    - This function is importing a local group policy to replace any currently installed group policies. The local GPO is identical to the "RS Default Domain Policy" which would be imported to a Domain Controller if running on a DC. The policy contains hundreds of settings to make it compliant with PCI DSS Benchmarks and requirements.
    - For further clarification on this, see the included "CIS_Server_2019_GPO.xlsx" which provides clarification on all of the settings which both are and are not configured and why. It provides (as you can see in the screenshot) the CIS Principal number which it is assigned to, the content that is being modified, the setting which was curated for it, and the reasoning for this.

- Disable-Service –
- This function disables multiple services which (per PCI DSS guidelines) can be insecure and cause security vulnerabilities. Not all services will be on every device. The script will log which it doesn't find to the log file. List of service names below.
    - Alerter
    - AudioEndpointBuilder
    - CiSvc
    - ERSvc
    - Fax
    - fdPHost
    - FDResPub

  - helpsvc
  - hidserv
  - iphlpsvc
  - MSDTC
  - MSFtpsvc
  - p2pimsvc
  - p2psvc
  - PNRPAutoReg
  - PNRPsvc
  - RasAuto
  - RasMan
  - RDSessMgr
  - RpcLocator
  - ShellHWDetection
  - SimpTcp
  - SMTPSVC
  - SNMPTRAP
  - Spooler
  - TapiSrv
  - WinRM
  - WmdmPmSN
  - WZCSVC

- Set-LocalPerms –
- This function sets the permissions to the Windows Event Log per the requirements set forward by PCI DSS Principal 10 dealing with event logs.
  - The functionality of the script corrects the permissions to provide even administrators with "Read Only" access.
  - The reasoning for this is that if a bad actor were to gain access to your system(s) and escalate privilege, with only "Read Only" access it will be much more difficult to wipe/clear logs and hide advancement.

- DomainPol-Backup –
  - As this sounds like, on Domain Controllers, this will back up domain policies to ensure that there is a safe and unmodified repository of the current (when the script was run) Group Policy Objects.

- ApplyRS-GPO –
  - This function imports (but does not Link or otherwise modify in-place GPO's/OU's) the group policies which we have created for PCI DSS compliance.
  - These policies include a number of GPO's however there are some which are not set due to the potential for negative effects for SQL, IIS, and other common functionalities.

- It will be up to the Customer/OS Team to implement these policies and link them, and they should be HEAVILY reviewed before doing so. Both the Default Domain Policy and the Default Domain Controllers policy include nearly 300 settings and although they are majorly compliant with PCI DSS, these could potentially have negative impact on functionality if not reviewed AND tested.
- These are more intended to be starter PCI GPO's which people can add/remove/modify at their behest.
- The additions are not taken when run as a "member" server, which the current script is set to run as.

6. References

1. For your awareness, these same references can also be found in the script itself. They are listed in one of the top Comment sections for reference if needed when running manually.
    a. Note - All folders referenced are either deployed in the same zip/folder, or created within the script:

- **$PSScriptRoot** - $PSScriptRoot
- **Function LogMessage** - LogMessage/Log\Rollback-Info\Warn\
- **Menu1/Menu2/RBMenu** - http://serverfixes.com/powershell-radiobuttons
- **Import-LocalPols** - Import-LocalPols
- **Import-GPO** - Import-GPO
- **Restore-GPO** - Restore-GPO
- **Backup-GPO** - Backup-GPO
- **Function Reg-Harden** - Reference output from Menu2, selected function will produce variable, referenced for RegHarden **Presently removed from the script**
- **Function Set-LocalPerms** - Set-LocalPerms
- **Function Backup Reg** - Backup-Reg
- **Dynamic Parameters** - Dynamic Parameters
- **Configuring regular and Dynamic Parameters** - Combining Static and Dynamic Parameters Together
- **Compress-Output & Extract-Output** - Compress- & Extract-Output
- **Compress-Output (Output the registry key for piping)** - Registry Key Sourcing
- **Overall Script Documentation** - Script Documentation (Sharepoint)
- **Problem/Suggestion Tracking in ticket:**
    - TASK0269771
    - Ticket Link