	DP Security Team Network Defense	**SOP #**	SPP-1509
		Revision #	4
		Implementation Date (MM/DD/YYYY)	02/25/2020
Page #	1 of 16	**Last Reviewed/Update Date**	06/09/2020
SOP Owner	Donald R. Phillips	**Approval**	

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. Procedure 4

5.1 Introduction 4

5.2 BigFix Procedure 5

5.3 Manual Procedure 7

5.4 Script Explanation (Still in Development) 9

5.5 Change Log (tracking) 13

5.6 Upcoming Features (Still in Development) 15

5.7 What the Script Does/Affects 16

6. References 25

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 –

System Admins/Engineers who work with customers to harden their servers according to PCI requisite guidance.

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).
3. (If running through BES task) The BigFix client: must run as admin/system in order to elicit all of the changes.
4. (If running manually) The user running the script: Must be able to run as admin in order to elicit all of the changes.

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. Procedure

5.1 Introduction

This document outlines and explains the WS2019_CIS_SetPolicy_0.x_%.ps1 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 script itself does have comments throughout (including links for references to certain functions for understanding).

This script does meet all of the same functionality as the "Lockdown.bat" script did, however in an updated manner for ease of documentation, understanding, and functionality.

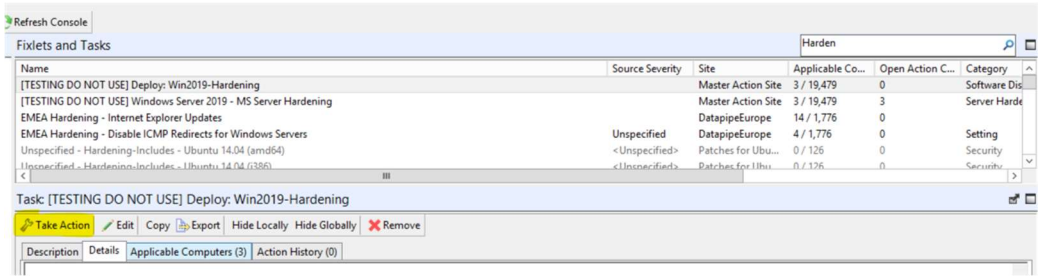
*****Important Note:**

- As of this issue of the Standard Operating Procedure and script, it is still in it's development phase. Although the script has been tested on a virtual machine for both manual and BigFix distributions/implementations, there may be some problems which occur. As those problems are found, please either update the following:
  - TASK0269771
  - Direct Ticket Link: TASK0269771

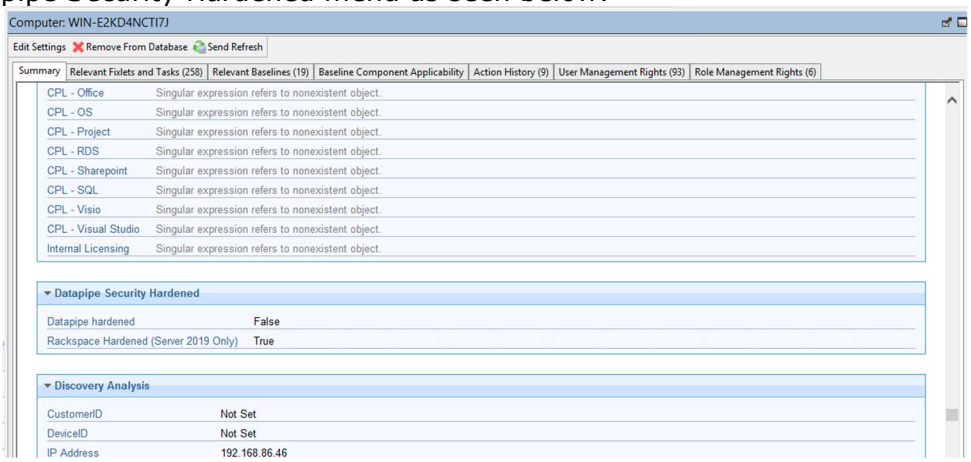
  Or alternatively, please send an email to Donald.Phillips@Rackspace.com in order for the issues to be noted and corrected in follow up versions.

- As of this issue of the Standard Operating Procedure and script, due to the development stage still being active, there are functions and tools within the script which do not function, or have been commented out. While our goal is to make these functions work, there was a limited time to script deployment, and we wanted to address the core functionality first.

5.2 BigFix Procedure

1. If you are trying to automate deployment of this script, first log in to one of the Datapipe BigFix consoles using your Datapipe credentials after logging into one of the SANTA environments.
    a. BESConsole01.datapipe.net
    b. BESConsole02.datapipe.net
2. Once you have successfully RDP'd to one of the above servers, launch the "IBM BigFix Console", and log in with either your Datapipe or Intensive credentials.
3. Once the console has fully loaded (please allow 10-20 minutes for this to occur, select "Fixlets and Tasks" in the top of the "All Content" menu.
4. Once this has loaded, in the top right Search box, type in the correct form of the script which you are attempting to run **This will be updated once further functions within the script are completed**:
    a. Member Servers/Non-Domain Joined Servers/Non-Domain Controllers/Domain Controllers which do **NOT** want to include our PCI GPOs:
    "Windows Server 2019 – MS Server Hardening"
    b. Domain Controllers:
    "Windows Server 2019 – DC Server Hardening"
    c. Member Server, Non-Domain Joined Servers, or Domain Controllers having **ALL** the policies rolled back:
    "Windows Server 2019 – Full Rollback"
    d. Member Server, Non-Domain Joined Servers, or Domain Controllers having **ONLY** the File ACLs, Registry, Windows Services rolled back:
    "Windows Server 2019 – FS Only Rollback"
5. Once you have selected the function you wish to take, summarily click "Take Action" on the task.
    a. 

    b. When selecting the action, do **not** select a reboot after, as the reboot could potentially interrupt the script running which can take a fair amount of time.
    c. The machine however **WILL** require a reboot after the script has completed in order to apply some of the settings for local policy, registry, etc.

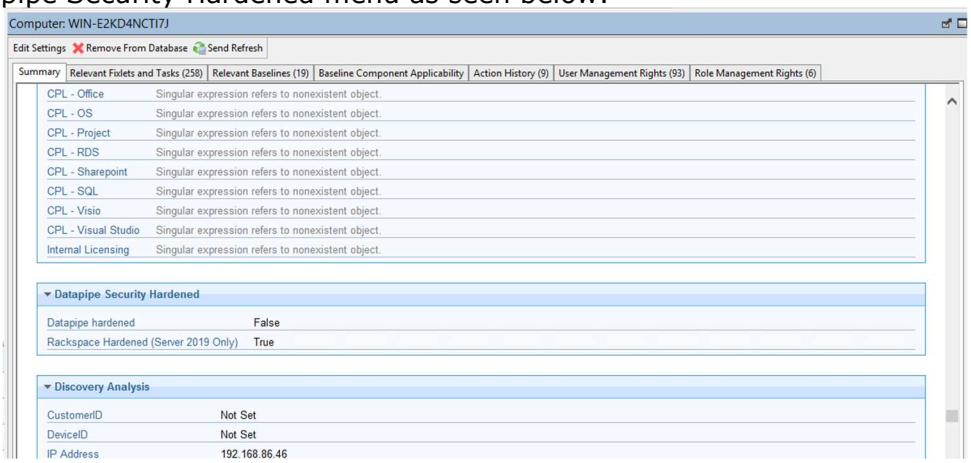
6. Once the script has completed, you should be able to view the logged actions and successes/failures within check the Windows "Event Viewer" > Applications and Services Logs" > "Rackspace Hardening" log.
    a. The "Rackspace Hardening" log is also backed up in the Zip folder which is created at the end of the script for historical/evidence purposes.
7. If there are any issues with running the script, or if services/functions which should have run successfully report an error, please log them in DPOne under the following ticket:
    a. TASK0269771
    b. Direct Ticket Link: TASK0269771
8. Once the script has run, within 24 hours (analysis updates once per day) the hardening should reflect within the BigFix > Computers > %ComputerName% > Datapipe Security Hardened menu as seen below:
    a. 

    b. This analysis is based off of the existence of a Registry key:
        i. 32-Bit Applications: HKEY_LOCAL_MACHINE\Software\Rackspace\Hardening
        ii. 64-Bit Applications: HKEY_LOCAL_MACHINE\Software\WOW6432Node\Rackspace\Hardening
9. (After script is run) Confirm that one the following Zip files is present and has backed up information present:
    a. For Hardening: C:\Windows\Datapipe_Hardened_%DateTime%.zip
    b. For Rollback: C:\Windows\Datapipe_RolledBack_%DateTime%.zip

5.3 Manual Procedure

1. If you have downloaded the script from BigFix or are planning to download it, the links are as follows:
   **Be aware, the zip file contains extensive files for Domain Controller policies and other tools, the script MUST be run from the same folder that is extracted from the Zip file, otherwise connections will not be made successfully.
   a. BigFix -BigFix Zip File
   b. Share Drive - RAX Global Sharepoint - Shared Link
      i. For this, make sure to select the most recent version. The updates should be listed with a MajorRelease.MinorRelease number "PCI-Hardening_0.8.zip" is the most recent release as of writing this.
2. Once you have downloaded the zip file, copy the Zip over to the computer that you are going to be running it on. Once you extract the folder, ensure that all files and the script reside in the same location.
3. The folder that is extracted will contain a number of different files and folders as well as (at the time of this writing) 3 scripts. Please select the correct script for the function you are trying to complete.
   a. Member Servers/Non-Domain Joined Servers/Non-Domain Controllers/Domain Controllers which do **NOT** want to include our PCI GPOs:
      "WS2019_CIS_SetPolicy_0.6_MS-Hardening.ps1"
   b. Member Server, Non-Domain Joined Servers, or Domain Controllers having **ALL** the policies rolled back:
      "WS2019_CIS_SetPolicy_0.6_RB-Full.ps1"
   c. Member Server, Non-Domain Joined Servers, or Domain Controllers having **ONLY** the File ACLs, Registry, Windows Services rolled back:
      "WS2019_CIS_SetPolicy_0.6_FSOnly.ps1"
   d. Domain Controllers which want to include our PCI GPOs:
      "WS2019_CIS_SetPolicy_0.8_DC-Hardening.ps1"
4. Each of the scripts performs a number of functions which can be reviewed in:
   a. Section 5.4.
5. Launch PowerShell and run Get-ExecutionPolicy.
   a. If the response from the computer is anything other than "Unrestricted", you cannot simply click to run the script.
   b. You will need to run the following from PowerShell:
   %FolderPathToScript%\%ScriptSelected%.ps1 -executionpolicy Unrestricted -WindowStyle Hidden -NonInteractive

6. Once the script has completed, you should be able to view the logged actions and successes/failures within check the Windows "Event Viewer" > Applications and Services Logs" > "Rackspace Hardening" log.
   a. This is also backed up in the Zip file created upon script finishing.

7. If there are any issues with running the script, or if services/functions which should have run successfully report an error, please log them in DPOne under the following ticket:
    a. TASK0269771
    b. Direct Ticket Link: TASK0269771
8. Once the script has run, within 24 hours (analysis updates once per day) the hardening should reflect within the BigFix > Computers > %ComputerName% > Datapipe Security Hardened menu as seen below:
    a. 

    b. This analysis is based off of the existence of a Registry key:
        i. 32-Bit Applications: HKEY_LOCAL_MACHINE\Software\Rackspace\Hardening
        ii. 64-Bit Applications: HKEY_LOCAL_MACHINE\Software\WOW6432Node\Rackspace\Hardening
9. (After script is run) Confirm that one the following Zip files is present and has backed up information present:
    a. For Hardening: C:\Windows\Datapipe_Hardened_%DateTime%.zip
    b. For Rollback: C:\Windows\Datapipe_RolledBack_%DateTime%.zip

5.4 Script Explanation (Still in Development)

- Note – If you are curious as to which settings are enacted in the Default Domain Policy or Default Domain Controllers Policy (group policies) that can be found at the following: CIS_Server_2019_GPO.xlsx
- I highly suggest reading through the script as it is commented throughout, and referencing the "References" section either in this document or in the script itself. They contain the same links.
- The below explanations are for the "Function %%" included in the script.

1. Starting from the top of the script, the intro, version of the script, various information for the scripts uses (including a Change Log for each version).
2. The references section, as stated above, the references are for various functions within the script which are explained better from the links for understanding their usage and what they are doing.
3. Run-PCIHard –
    a. This is the first function in the script, and at this point is largely commented out due to having some trouble with collocating regular Parameters as well as Dynamic Parameters.
    b. The reason this was commented out was to stop troubleshooting the issues for quicker release of the script. At some point, this will take either command line arguments, and for usage to automate the script from BigFix.
    c. Essentially this function identifies which arguments are passed to the script in order to run the appropriate functions through the rest of the script.
4. Make-Log –
    a. As this sounds like, it is creating a new event log on the computer that it is running on.
    b. Then creating the sources needed to log to the new event log correctly.
5. Log-Info/Warn & Rollback-Info/Warn –
    a. This is creating various functions to both write out to the console and to simultaneously log to the event log with minimal command input and for cleaner scripting.
6. Test-OS –
    a. Exactly as it sounds like, this tests and confirms that the Operating System is Windows Server 2019 before continuing on in the script. Because this script was sculpted around the Server 2019 PCI guidelines, accidentally running it on a non-2019 machine could cause issues.
7. Test-DC –
    a. Exactly as it sounds, this tests the computer to see if the Domain Controller role(s) are installed to determine whether it is a DC or not.

While this will not prevent the Member Server script from running on a Domain Controller (if the customer does not want to import our curated PCI Group Policies), it will prevent the Domain Controller script from running on Member Servers which would cause a number of errors.

8. Menu1/Menu2 –
    a. These are vbscript out-menus which will be functional and usable in a later version of the script. These are essentially just pretty/nice interfaces with buttons that people could use to run the script once all of the functionality issues have been remediated.
    b. Clicking on the buttons would essentially pass in specific arguments to the parameters. Once the parameters are set for the options the user wants to take, the script would run the same as doing so automated through BigFix or using one of the preconfigured scripts.
9. Create-GPSource –
    a. This function creates a backup directory for all of the settings that are exported/backed up during the running of the script.
10. LocalPol-Backup -
    a. This function has 3 componenents:
        i. Export the local group policy settings from: C:\Windows\System32\GroupPolicy
        ii. Export the local Security Policy
        iii. Export the local Audit Policy
    b. All of these are backed up at C:\Windows\Datapipe
11. Backup-Reg –
    a. This backs up a number of keys (listed in the script) which are modified during the running of the script for more hardened settings.
    b. They are backed up to the same Windows\Datapipe folder in multiple .Reg files and then create a merged file with all of the settings compiled for rollback later if needed.
12. Reg-Harden –
    a. Since we just backed up the registry keys, this function pulls a .Reg master key file (located in the script folder at the "Tools" directory.
13. Import-LocalPols -
    a. Since local policies have been backed up, we now import PCI compliant local policies which are more restrictive from the "LocalPolicy" folder within the unpacked Zip file.
14. Disable-Service –
    a. Exactly as this sounds, the function pulls a list of services from the folder which was unpacked (the list is "Services.txt") which can potentially make your server more susceptible.
    b. The script provides read-out in the PowerShell window if you are running it manually, otherwise it will log the attempts to stop & disable services within the event log. It will try 3 times before failing.

15. Set-LocalPerms –
    a. This function sets more restrictive permissions on the Event Logs than default. Making sure that the permissions are set to only allow members of the Administrator group the permissions to read and not modify.
    b. The reason for this is to lower the attack vector of potential bad actors, if one were to gain access to the system and escalate to Administrator privileges, they could potentially remove/delete event log entries or the logs themselves, harming our ability to successfully audit an intrusion.
16. DomainPol-Backup –
    a. This is only used for Domain Controller implementations (not active yet)
    b. Runs a backup of all domain policies that exist within a domain. They can be rolled back or otherwise restored using the "Restore-GPO" command within the GroupPolicy module.
    c. The function does **NOT** delete/remove any policies, just creates a backup in case of any unforeseen activities.
17. ApplyRS-GPO –
    a. Again, only used for Domain Controller implementations (not active yet).
    b. Imports two policies:
        i. RS Default Domain Policy
        ii. RS Default Domain Controllers Policy
    c. The two policies do NOT replace the existing Default Domain Policy or Default Domain Controllers Policy, as they are significantly restrictive and implementation should be left to the customer to decide whether to implement them or not.
    d. If the customer decides to implement them, they can use the policy to overwrite their existing policy or to otherwise link that policy instead of the Default Domain Policy(ies)/in tandem with their Default Domain Policy(ies).
18. Hardening-Complete –
    a. This essentially just writes to the event log and PowerShell screen to let the person know that the script has completed.
    b. This does prompt the user (if running manually) if they would like to reboot the computer now. The user running the script is not REQUIRED to reboot the computer immediately, however certain hardening steps will not be present until reboot is completed.

>>>This is the end of the main Hardening section, below this is the Rollback functions explanation.<<<

19. RBPolicy-Menu1 –
    a. Reference Step 8. Menu1/Menu2
    b. This is the same style of menu, however only utilized if the user is running manually and selects to perform a rollback function rather than a hardening function.
20. Rollback-SecPol –
    a. This section pulls the previously backed up Local Group Policy, Local Security Policy, and Local Audit Policy.
    b. If there are no backups, then this function cannot be completed. Check the Rackspace Hardening Event Log if you do not find any folders/files under C:\Windows\Datapipe\GPOBak for rollback.
21. Rollback-GPO –
    a. If there were Domain GPO's that were backed up previously, this function provides a restoration of those Group Policies to their default location and settings from when they were backed up.
22. Rollback-Reg –
    a. If there were Registry keys which were backed up in initial hardening, this will replace them in the Registry, removing the previous settings.
23. Rollback-Services –
    a. This will utilize the same list from Step 14. Disable Services to attempt to re-enable any services which were disabled previously.
24. RB-Complete –
    a. This essentially just writes to the event log and PowerShell screen to let the person know that the script has completed.
    b. This does prompt the user (if running manually) if they would like to reboot the computer now. The user running the script is not REQUIRED to reboot the computer immediately, however certain rollback steps (Group policy, audit policy, etc.) steps will not be present until reboot is completed.
25. Compress-Output –
    a. This function zips all of the output and places it into the following: C:\Windows\Datapipe%date%.zip
    b. The reasoning for this is that if the files are left in place and another hardening event is pushed, the group policy and registry hardening tend to hang forever.
    c. We also don't want to hold more information than necessary on customer systems.
    d. After establishing variables, the script checks for whether the function taken is hardening or rollback and adds the appropriate title to the name of the Zip.
    e. The function then copies the "Rackspace Hardening" log as a 'moment-in-time' snapshot to the zip file folder in order to ensure accuracy.
    f. The function then zips the folder and it's files, and removes the existing folder.

g. This function is used at the end of both hardening AND rollback in order to minimize files laying around. They are named appropriately per the step in 26.d above.

26. Extract-Output –
    a. In the case of Rolling back functions, you will need to extract the previously created archive.
    b. Lots of variables for what seems like nothing but they're necessary to auto-magically find the most recent backup.
    c. First the function establishes variables for usage later.
    d. Then the function tests to make sure that backup(s) exist.
    e. If the backup(s) exist, it finds the newest one, and extracts it to the original C:\Windows\Datapipe location.
    f. After extraction, the files will be available for the rest of the rollback to run successfully.
27. Run-%%% -
    a. This section is simply a conglomeration function which runs the specific tasks which pertain to each Hardening or Rollback procedure.

5.5 Change Log (tracking)

- The below change log is also available within the script and is labeled, including the upcoming features.
- 0.1 –
  - Script Created
- 0.6 –
  - Multiple untracked changes including commenting out the exits, menus, and parameters for the time being.
  - Initial release, dropped only with MS hardening, and both rollbacks as separate change tasks.
  - Created the documentation at: Sharepoint Link
  - Tracking in ticket: TASK0269771 Ticket Link
- 0.7 –
  - Updated the script to include the Domain Policies correctly backed up.
  - Updated the above documentation link with repos for each release version.
- 0.8 –

- Removed the comments around the "[Environment]::Exit(1)" after determining the issue with the core script tasks exiting unnecessarily.
  - The problem was that it was referencing variables from another function that weren't imported from the other function.
- Created the DC policy successfully and tested deployment.
- Added the following functions: "Function Compress-Output" & "Function Extract-Output" as well as a reference for information.
- Added a variable to the Zip file so that it would be identified correctly for later historical evidence.
- Tested both the Compress and Extract output functions which ran successfully.
- Found a problem with the Registry key import for hardening. In my stupidity, the only key it would apply would be "Hardened" but it wouldn't correct to "Rolled back" if the policy was rolled back.
  - Added the registry key correction to the "Rollback-Reg" function.
- Added Log-Info and Log-Warn to the Rollback steps as well to ensure that all Functions would run & log correctly.
- Added a check in the Registry rollback to search for which key existed (32 or 64-Bit) and modify only the correct key.

- 0.90-
  - Modified the group policy setting for Renaming the Local Administrator account.
    - After Lonny Motto (Windows) tested this on a device, he found that the local policy wasn't applying correctly and was renaming the "dpadmin" account back to "Administrator"
    - Modified the policy and reapplied to the VM I had been testing on.
    - Relieved a policy that disallowed local and RDP log in for local accounts and specifically dpadmin.
  - Disable-Service and Start-SmartCard functions -
    - Modified the "Count" that updated each time it tried to start/stop a service from "le" to "lt" due to a coding mistake.
    - Added the argument "-WarningAction SilentlyContinue" because the script was producing a large number of warning messages (originally believed that -ErrorAction would silence them fully)
  - Added a bypass for the Reboot step from "Hardening Complete" and "RBComplete" functions
    - Previously the Read-Input was requesting input before finalizing the script.
    - Because of the requested input it wouldn't finish the script until input was received. For automated runs, this will/would obviously be a problem.

- Corrected the verbiage and cleaned up the function "Disable-Services" for more clean input and output.
- Removed the "Start-SmartCard" function as it was not working as intended and would routinely stop itself.
- Reconfigured the "Set-LocalPerms" function so that the ACLs wouldn't error as much and would only return relevant information.
- Updated the "Compress-Output" function as it wasn't correctly finding the Hardening key and adding it to the zip file created.

5.6 Upcoming Features (Still in Development)

- Colocating all 4 possible actions to a single script. (instead of separate scripts for different actions for Member Servers Vs. Domain Controllers and Hardening Vs. Rollback.
  - This will also change the BigFix task name to a singular task when it is functional and (much like the legacy Datapipe Hardening task, will prompt you for the action you are trying to take).
- Interactive interface including menus which you can select when running the script manually to select the actions you want to take, and providing readout within the PowerShell window as it goes along while simultaneously logging to the Windows Event Log.
- Updating the script to include/creating a new script for, or updating previous versionings of the Legacy Datapipe Hardening script:
  - Windows Server 2016
  - Windows Server 2012 R2
- Potentially creating VB Menus for the Reboot prompt at the end of running the functions.

5.7 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.

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