**Information Systems & Technology**

Vulnerability fix Build guide

Application Server Hardening

|  |  |  |  |
| --- | --- | --- | --- |
| **Status** | Draft | **Revision** | 0.1 |
| **Doc No.** | #2 | | |
| **Date** | 04 Aug 2022 | | |
| **Originator** |  | | |
| **Project Location** |  | | |
| **Business Unit / Product Group** |  | **Momentum ID** | XXXXX |
| **RTTMS Demand #** | DMNDXXXXXXX | **Project #** | S2093 |
| **WBS** |  | **CAPS #** |  |

**Key search words**

*Add below key words, separated with a semi-colon, to be used to locate this guidance.*

|  |
| --- |
| Vulnerability fix deployment plan; |

**Revision history**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Date | Revision | Owner | Reviewed | Approved | Comments |
| 04/08/2022 | 1 | Hitender Yadav |  |  | Draft |
| 18/08/2022 | 2 | Achroo Batta (AB) |  |  | Addition of relevant section for I4.3 and A3.1 |

**Document responsibilities**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Role | Business Partner\* | Risk | Cyber | Project Manager | Hub PMO | G&I Finance | Area of Excellence | Service Transition to Support | Enterprise Architecture | Project Sponsor | Operations |
| RAPID | I | I | I | P | R | I | I | I | I | D | I |

\* Service Owner acts as Business Partner for IS&T-funded projects.

**Endorsements**

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Position | Signed | Date |
|  | Business Partner \* | Embedded email /  Link to approval /  DocuSign |  |
|  | Project Manager |  |  |
|  | Position, Hub PMO |  |  |

\* Service Owner acts as Business Partner for IS&T-funded projects.

**Approvals**

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Position | Signed | Date |
|  | Project Sponsor | Embedded email /  Link to approval /  DocuSign |  |
|  | Operations |  |  |
|  | Steering Committee members |  |  |

Contents page

[1. Project Overview 7](#_Toc112276435)

[**1.1.** **Summary of problem to be addressed and proposed solution** 7](#_Toc112276436)

[2. Introduction 8](#_Toc112276437)

[**2.1.** **What this document is** 8](#_Toc112276438)

[**2.2.** **What this document is not** 8](#_Toc112276439)

[**2.3.** **Audience** 8](#_Toc112276440)

[**2.4.** **Document notes** 9](#_Toc112276441)

[3. Vulnerable Server discovery and analysis 10](#_Toc112276442)

[**3.1.** **A3.1 - Clear Text** 10](#_Toc112276443)

[3.1.1. Description and cyber risk 10](#_Toc112276444)

[3.1.2. Process Flow – Discovery, Analysis, and fix deployment 10](#_Toc112276445)

[3.1.3. Vulnerable Server Discovery 11](#_Toc112276446)

[3.1.4. Server Analysis 11](#_Toc112276447)

[**3.2.** **I4.1 - RDP Timeout** 12](#_Toc112276448)

[3.2.1. Description and cyber risk 12](#_Toc112276449)

[3.2.2. Process Flow – Discovery, Analysis, and fix deployment 12](#_Toc112276450)

[3.2.3. Vulnerable Server Discovery 13](#_Toc112276451)

[3.2.4. Server Analysis 13](#_Toc112276452)

[**3.3.** **I4.3 - NTLM** 14](#_Toc112276453)

[3.3.1. Description and cyber risk 14](#_Toc112276454)

[3.3.2. Process Flow – Discovery, Analysis, and fix deployment 14](#_Toc112276455)

[3.3.3. Vulnerable Server Discovery 15](#_Toc112276456)

[3.3.4. Server Analysis 15](#_Toc112276457)

[**3.4.** **I4.5 - PowerShell v2** 17](#_Toc112276458)

[3.4.1. Description and cyber risk 17](#_Toc112276459)

[3.4.2. Process Flow – Discovery, Analysis, and fix deployment 17](#_Toc112276460)

[3.4.3. Vulnerable Server Discovery and analysis 18](#_Toc112276461)

[3.4.4. Server Analysis 18](#_Toc112276462)

[4. Vulnerability fix deployment 20](#_Toc112276463)

[**4.1.** **Overview of vulnerability fix deployment** 20](#_Toc112276464)

[4.2. Deployment method for A3.1 Clear text 20](#_Toc112276465)

[**4.2.1.** **Deployment method for I4.1 RDP timeout** 20](#_Toc112276466)

[**4.2.2.** **Deployment method for I4.3 NTLM V1 to NTLM V2** 21](#_Toc112276467)

[**4.2.3.** **Deployment method for I4.5 PowerShell version update** 22](#_Toc112276468)

[**4.3.** **Vulnerability fix deployment validation** 25](#_Toc112276469)

[**4.3.1.** **Deployment test for A3.1 Clear text** 25](#_Toc112276470)

[4.3.2. Deployment test for I4.1 RDP timeout 25](#_Toc112276471)

[**4.3.3.** **Deployment test for I4.3 NTLM V1 to NTLM V2** 25](#_Toc112276472)

[**4.3.4.** **Deployment test for I4.5 PowerShell version update** 26](#_Toc112276473)

[5. High-level project plan 27](#_Toc112276474)

[6. Appendix 28](#_Toc112276475)

1. **Project Overview**
   1. **Summary of problem to be addressed and proposed solution**

An independent cyber security review identified significant risks and control deficiencies which significantly weaken the security and resilience of Rio Tinto. This project focuses on the review of Rio Tinto’s servers in light of the assessment conducted by Rio Tinto’s Third- Party Vendor.

The goal of the project is to:

* Establish a detailed understanding of Rio Tinto’s current exposure to the vulnerabilities in the current environment and as stipulated in the Business Requirements Document Cyber Program – Server Hardening provided by Rio Tinto
* Assess Rio Tinto’s server virtual machines to define a current state baseline of existing vulnerabilities
* Track progression on remediation of those vulnerabilities across the Production environments
* Existing tools should be evaluated to analyse environment coverage and threat detection capabilities
* Identify processes to rectify/remediate each of the identified controls and facilitate the remediation.

1. **Introduction**

This document provides a high-level process flow overview of vulnerability fix and deployment methods. This is in preparation for Rio Tinto’s application server hardening project. This document covers details from each phase of project discovery and analysis, vulnerability fix build and provide detailed process flows for each phase. The document covers technical details about vulnerability fix deployment of four (4) in-scope vulnerabilities

* A3.1 - Clear Text
* I4.1 - RDP Timeout
* I4.3 - NTLM
* I4.5 - PowerShell in the environment
  1. **What this document is**

This document is a vulnerability fix deployment document covering several areas of guidance as they apply to each vulnerability and application servers differently on application servers. This document also covers recommended practices as well as the requirements discussed during the workshop that are unique to each vulnerability fix deployment.

* 1. **What this document is not**

This document is not a design (low level or high-level) document for vulnerability fix build and deployment infrastructure. It does not discuss how to use or resolve issues discovered within Rio Tinto’s applications.

* 1. **Audience**

This document assumes a 300-level knowledge of Vulnerabilities, associated vulnerable components and deployment methods e.g group policy, ansible, PowerShell script etc...

**Level 300**: Advanced material. In-depth understanding of features in a real-world environment, and strong coding skills. Provides a detailed technical overview of a subset of product/technology features, covering architecture, performance, migration, deployment, and development.

* 1. **Document notes**

Throughout the document Avanade will summarize the outputs of each section. These outputs can be categorized under the following headings:

|  |  |
| --- | --- |
| Icon  Description automatically generated | ***Note***  *This header is to make the reader aware of something specific in the document and will give some additional context to the section.* |

|  |  |
| --- | --- |
| Icon  Description automatically generated | ***Important Note***  *This header is to ensure the reader is fully aware of the point being highlighted. The information provided should be fully considered when understanding the context of the section.* |

|  |  |
| --- | --- |
| Icon  Description automatically generated | ***Recommendation***  *A recommendation being made by Avanade, but not necessarily a design decision.* |

|  |  |
| --- | --- |
| Icon  Description automatically generated | ***Assumption***  *Based on the workshops and knowledge of infrastructure, assumptions on configurations and requirements are listed.* |

|  |  |
| --- | --- |
| Icon  Description automatically generated | ***Design Decision***  *A design decision based on requirements and Avanade/Microsoft recommended best practices.* |

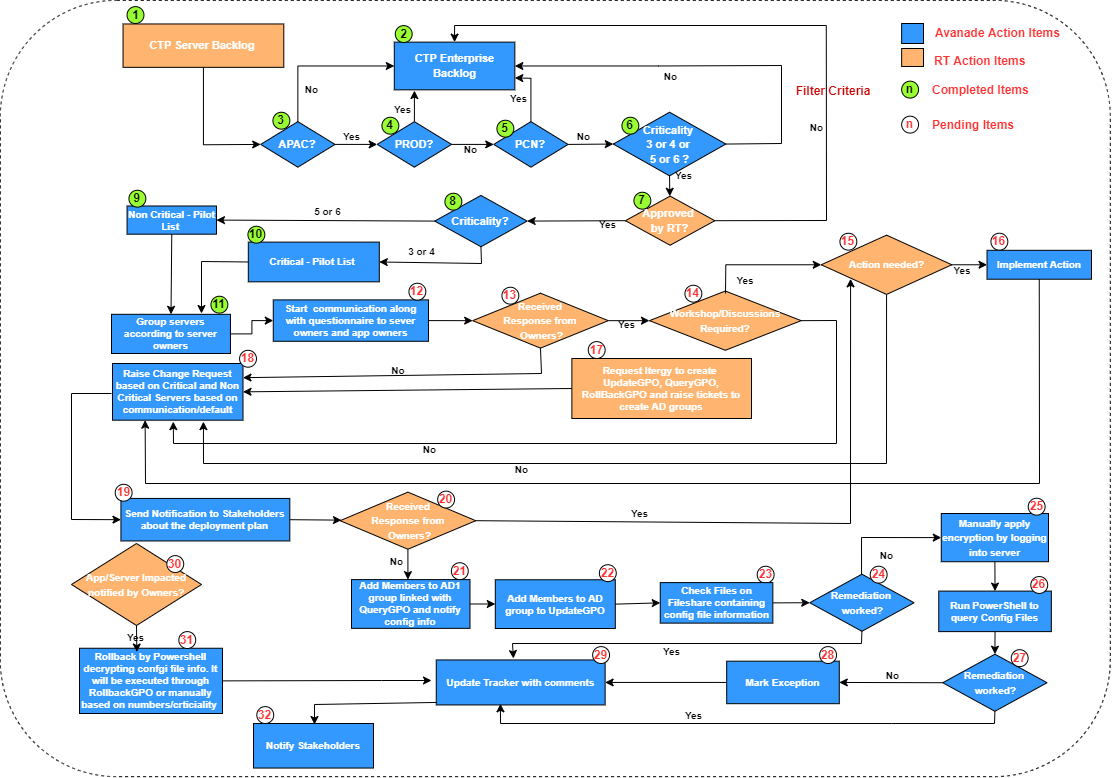
1. **Vulnerable Server discovery and analysis**
   1. **A3.1 - Clear Text**

### Description and cyber risk

A key finding of cyber security review was the presence of cleartext credentials in application configuration and code files. These credentials can allow an intruder to easily move laterally into databases and other systems.

### Process Flow – Discovery, Analysis, and fix deployment

**\*\*No 2008 servers in Pilot**



|  |  |
| --- | --- |
| **Details of process flow** | |
| 1 | Received list of 1504 servers from RT (Backlog from Rahul’ project) |
| 2 | List of servers will be considered in enterprise rollout plan |
| 3 | Only APAC servers will be considered for Pilot. Rest will be sent back to Enterprise Rollout back log. |
| 4 | Only Non-Prod servers will be considered for Pilot. Rest will be sent back to Enterprise Rollout back log. |
| 5 | Only Non PCN servers will be considered for Pilot. Rest will be sent back to Enterprise Rollout back log. |
| 6 | Criticality 3, 4, 5 or 6 will be considered for Pilot. Rest will be sent back to Enterprise Rollout back log. |
| 7 | Pilot list Approved by RT (Craig Young) |
| 8 | Based on Criticality list is segregated in Non-Critical and Critical |
| 9 | 50 Non-Critical Pilot List shortlisted |
| 10 | 20 Critical Pilot List shortlisted |
| 11 | Group servers based on server owners (use Pivot Table through Excel) |
| 12 | Send email communication to owners along with questionnaire |
| 13 | Check if you receive response from owners |
| 14 | If answer to 13 is yes, Workshop/Discussion required with owners |
| 15 | Is there any Action Item comes out from Workshop/Discussion? |
| 16 | Implement on Action Item, if there is any outcome from 15 |
| 17 | Raise RTTMS request to create three sets of ADs for QueryGPO, DeployGPO and RollBackGPO and raise request for Itergy team to create these GPOs |
| 18 | Raise change requests based on default groups mentioned in deployment schedule or as suggested by Owners |
| 19 | Send Notification to stakeholders about deployment plan and dates |
| 20 | Check if you received any response from Owners and implement actions if suggestions came |
| 21 | Add members to AD1 linked with QueryGPO, this can be done prior to deployment date, as it will just before change snapshot of config files on fileshare of terminal server AUSYDTS17 |
| 22 | Add members to AD2 linked with DeployGPO, it will do encryption and also write “after change snapshot” of config files on fileshare of terminal server AUSYDTS17 |
| 23 | Check files present in fileshare |
| 24 | Did remediate work? |
| 25 | Manually login to server and apply encryption |
| 26 | Run powershell to query config files |
| 27 | Did remediate work? |
| 28 | If not, mark it as an exception |
| 29 | Update tracker comments appropriately |
| 30 | Did App/Server Owners notified you about impact during hyper care/in case they are validating? |
| 31 | Rollback the change through Rollback GPO or manually based on count. We have remote access of pilot server. Validated. Decryption is through PowerShell commands validated earlier by Rahul. |
| 32 | Notify stakeholders appropriately |

### Vulnerable Server Discovery

|  |  |
| --- | --- |
| **Discovery overview** | |
| Server Backlog | 1818 |
| Servers Already completed in previous Pilot | 101 |
| Decommissioned Servers | 213 |
| No CTP vulnerability present or server unreachable | 38 |
| Pilot Servers – Non-critical | 50 |
| Pilot Servers – Critical | 20 |

### Server Analysis

After analysing the data and discussing in technical workshop with Rio SMEs, below criteria was agreed to perform analysis for pilot server selection:

1. Server criticality level : Non-critical (3, 4, 5 and 6)
2. Server environment : Non Production only
3. Server Region : APAC
4. PCN Servers : Any PCN server with any criticality level is not in scope for Pilot

Below table list the count of pilot servers identified as per agreed criteria.

|  |  |
| --- | --- |
| **Server-Criticality** | **Pilot Servers** |
| **Level 3** | **16** |
| Windows Server 2012 R2 Standard | 3 |
| Windows Server 2016 Datacenter | 1 |
| Windows Server 2016 Standard | 1 |
| Windows Server 2019 Datacenter | 11 |
| **Level 4** | **4** |
| Windows Server 2012 R2 Standard | 2 |
| Windows Server 2019 Datacenter | 1 |
| Windows Server 2019 Standard | 1 |
| **Level 5** | **12** |
| Windows Server 2012 R2 Standard | 6 |
| Windows Server 2019 Datacenter | 1 |
| Windows Server 2019 Standard | 5 |
| **Level 6** | **38** |
| Windows Server 2012 R2 Standard | 6 |
| Windows Server 2016 Standard | 5 |
| Windows Server 2019 Datacenter | 10 |
| Windows Server 2019 Standard | 17 |
| **Grand Total** | **70** |

* 1. **I4.1 - RDP Timeout**

### Description and cyber risk

Currently there is no time limit for idle or disconnected RDP sessions for most the most servers. This can increase risk of RDP Session Hijacking.

### Process Flow – Discovery, Analysis, and fix deployment

Diagram

Description automatically generated

|  |  |
| --- | --- |
| **Details of Process Flow** | |
| 1 | Received list of servers from RT |
| 2 | List of servers will be considered in enterprise rollout plan |
| 3 | Only APAC servers will be considered for Pilot. Rest will be sent back to Enterprise Rollout back log. |
| 4 | Only Non-Prod servers will be considered for Pilot. Rest will be sent back to Enterprise Rollout back log. |
| 5 | Only Non PCN servers will be considered for Pilot. Rest will be sent back to Enterprise Rollout back log. |
| 6 | Criticality 3, 4, 5 or 6 will be considered for Pilot. Rest will be sent back to Enterprise Rollout back log. |
| 7 | Pilot list Approved by RT (Craig Young) |
| 8 | 50 Pilot Listed confirmed |
| 9 | Group servers based on server owners (use Pivot Table through Excel) |
| 10 | Send email communication to owners along with questionnaire |
| 11 | Raise Change Requests |
| 12 | Check for response from owners |
| 13 | Workshop/Discussion required with owners |
| 14 | Is there any Action Item comes out from Workshop/Discussion? |
| 15 | Implement on Action Item, if there is any outcome from Workshop/Discussion |
| 16 | Send reminder email to owners |
| 17 | Check if you receive response from owners |
| 18 | Send email communication to Owners along with change request and deployment date |
| 19 | Check if you receive response from owners |
| 20 | Check RDP Session time out and result set of policy by running PS script or logging to the server |
| 21 | Request Itergy to link GPO through security filtering with servers |
| 22 | Check RDP Session time out and result set of policy by running PS script or logging to the server |
| 23 | Did remediation work? |
| 24 | If remediation did not work, reboot the servers |
| 25 | Check RDP Session time out and result set of policy by running PS script or logging to the server |
| 26 | Did remediation work? |
| 27 | Mark server as exception if remediation did not work |
| 28 | Update trackers with appropriate comments |
| 29 | App/Server Got Impacted. Did you receive any communication on the same? |
| 30 | Rollback by unlinking GPO |
| 31 | Notify stakeholders appropriately |

### Vulnerable Server Discovery

|  |  |
| --- | --- |
| **Discovery overview** | |
| Server Backlog | 5798(To be updated) |
| Pilot Servers – Non-critical | 50 |

### Server Analysis

After analysing the data and discussing in technical workshop with Rio SMEs, below criteria was agreed to perform analysis for pilot server selection:

1. Server criticality level : Non-critical (3, 4, 5 and 6)
2. Server environment : Non Production only
3. Server Region : APAC
4. PCN Servers : Any PCN server with any criticality level is not in scope for Pilot

Below table list the count of pilot servers identified as per agreed criteria.

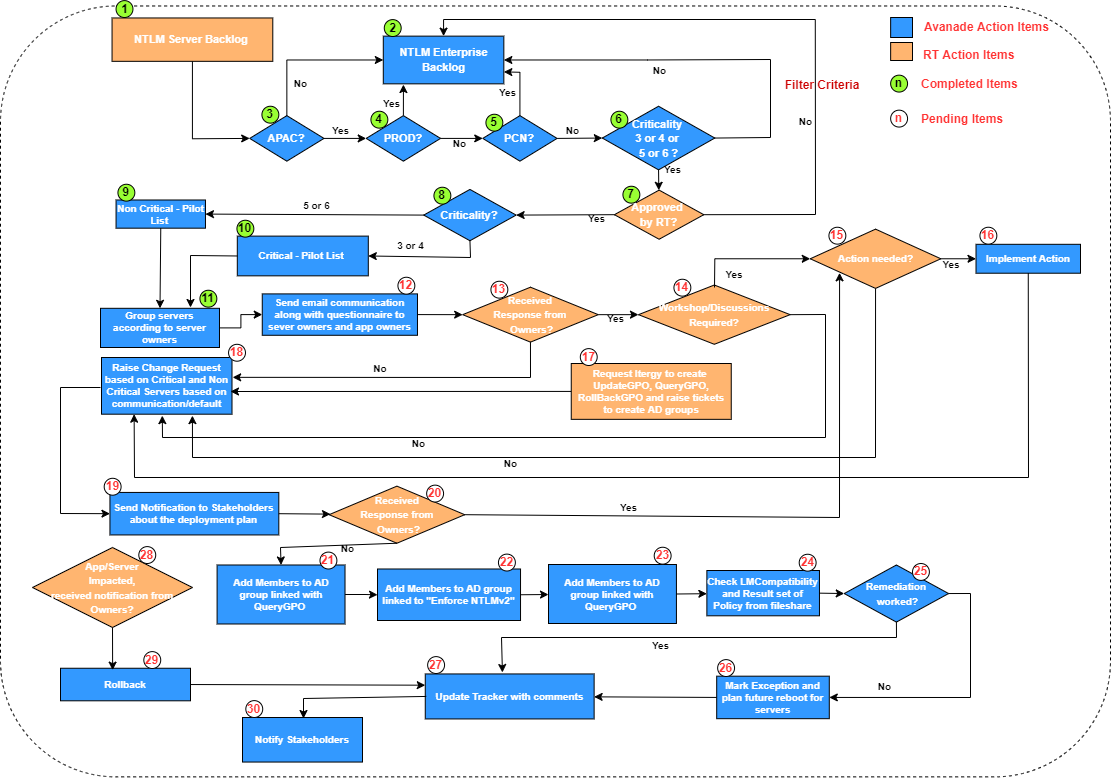
|  |  |
| --- | --- |
| **Criticality** | **Pilot Server** |
| **Level 3** | **4** |
| Windows Server 2008 R2 Enterprise | 1 |
| Windows Server 2008 R2 Standard | 1 |
| Windows Server 2012 R2 Standard | 2 |
| **Level 4** | **8** |
| Windows Server 2008 R2 Enterprise | 2 |
| Windows Server 2012 R2 Standard | 6 |
| **Level 5** | **6** |
| Windows Server 2008 R2 Standard | 2 |
| Windows Server 2012 R2 Standard | 2 |
| Windows Server 2016 Standard | 2 |
| **Level 6** | **32** |
| Windows Server 2003 | 1 |
| Windows Server 2008 R2 Standard | 1 |
| Windows Server 2012 R2 Datacenter | 2 |
| Windows Server 2012 R2 Standard | 14 |
| Windows Server 2016 Datacenter | 1 |
| Windows Server 2016 Standard | 12 |
| Windows Server 2019 Datacenter | 1 |
| **Grand Total** | **50** |

* 1. **I4.3 - NTLM**

### Description and cyber risk

New Technology LAN Manager (NTLM) v1 lacks crucial security protocols like including a timestamp in response and generating a variable-length challenge, which has been built into NTLMv2

### Process Flow – Discovery, Analysis, and fix deployment



|  |  |
| --- | --- |
| **Details of Process Flow** | |
| 1 | Received list of 5798 servers from RT |
| 2 | List of servers will be considered in enterprise rollout plan |
| 3 | Only APAC servers will be considered for Pilot. Rest will be sent back to Enterprise Rollout back log. |
| 4 | Only Non-Prod servers will be considered for Pilot. Rest will be sent back to Enterprise Rollout back log. |
| 5 | Only Non PCN servers will be considered for Pilot. Rest will be sent back to Enterprise Rollout back log. |
| 6 | Criticality 3, 4, 5 or 6 will be considered for Pilot. Rest will be sent back to Enterprise Rollout back log. |
| 7 | Pilot list Approved by RT (Craig Young) |
| 8 | Based on Criticality list is segregated in Non-Critical and Critical |
| 9 | 50 Non-Critical Pilot List shortlisted |
| 10 | 20 Critical Pilot List shortlisted |
| 11 | Group servers based on server owners (use Pivot Table through Excel) |
| 12 | Send email communication to owners along with questionnaire |
| 13 | Check if you receive response from owners |
| 14 | If answer to 13 is yes, Workshop/Discussion required with owners |
| 15 | Is there any Action Item comes out from Workshop/Discussion? |
| 16 | Implement on Action Item, if there is any outcome from 15 |
| 17 | Request Itergy to create GPOs (Rollback and Query). Enforce NTLMv2 is already present. Raise Ticket to create AD groups for these GPOs |
| 18 | Raise Change Requests based on Non-critical/Critical/feedbacks of owners |
| 19 | Send email communication to Owners along with change request and deployment date |
| 20 | Received Response from Owners? |
| 21 | Add members to AD for queryGPO. It will write files on fileshare with results |
| 22 | Add members to AD for "Enforce NTLM v2”. It will enable NTLM v2 |
| 23 | Add members to AD for queryGPO2 (after deployment). It will write files on fileshare with results |
| 24 | Check LM Compatibility and result set of policy from files on fileshare |
| 25 | Did remediation work? |
| 26 | If remediation did not work, mark it as an exception and update comments to plan future reboot after discussing with server owners |
| 27 | Update trackers with appropriate comments |
| 28 | Did App/Server Owner any interruption? |
| 29 | Rollback using Rollback GPO |
| 33 | Notify stakeholders appropriately |

### Vulnerable Server Discovery

|  |  |
| --- | --- |
| **Discovery overview** | |
| Server Backlog | 5798 |
| Pilot Servers – Non-critical | 50 |
| Pilot Servers – Critical | 20 |

### Server Analysis

After analysing the data and discussing in technical workshop with Rio SMEs, below criteria was agreed to perform analysis for pilot server selection:

1. Server criticality level : Non-critical (3, 4, 5 and 6)
2. Server environment : Non Production only
3. Server Region : APAC
4. PCN Servers : Any PCN server with any criticality level is not in scope for Pilot

Below table list the count of pilot servers identified as per agreed criteria.

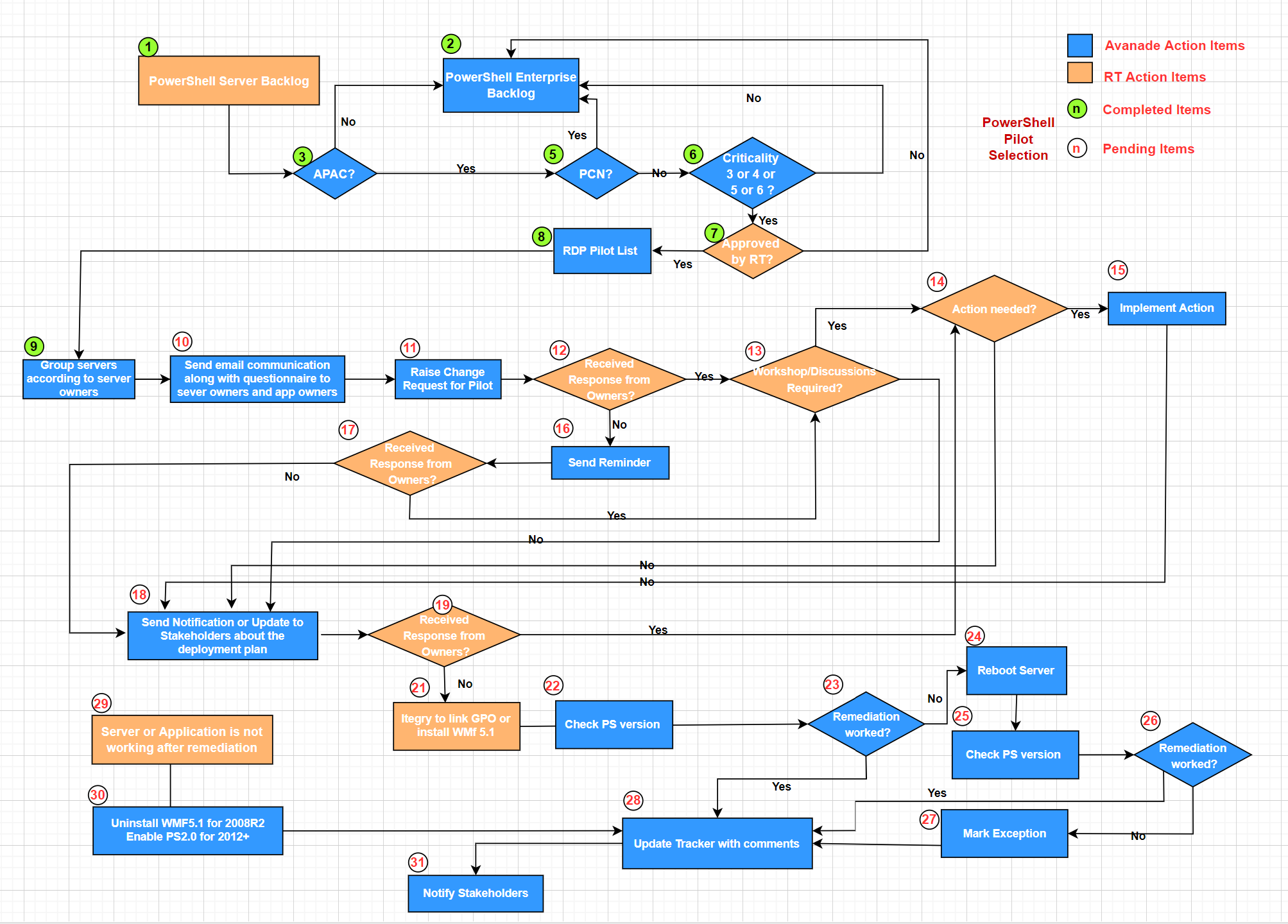
|  |  |
| --- | --- |
| **Server-Criticality** | **Pilot-Servers** |
| **Level 3** | **6** |
| Windows Server 2012 R2 Datacenter | 3 |
| Windows Server 2016 Standard | 1 |
| Windows Server 2019 Standard | 2 |
| **Level 4** | **14** |
| Windows Server 2012 R2 Datacenter | 1 |
| Windows Server 2012 R2 Standard | 3 |
| Windows Server 2016 Standard | 4 |
| Windows Server 2019 Standard | 6 |
| **Level 5** | **11** |
| Windows Server 2008 R2 Standard | 2 |
| Windows Server 2012 R2 Standard | 3 |
| Windows Server 2016 Standard | 2 |
| Windows Server 2019 Datacenter | 2 |
| Windows Server 2019 Standard | 2 |
| **Level 6** | **39** |
| Windows Server 2008 R2 Enterprise | 4 |
| Windows Server 2008 R2 Standard | 1 |
| Windows Server 2012 R2 Datacenter | 4 |
| Windows Server 2012 R2 Standard | 2 |
| Windows Server 2016 Datacenter | 1 |
| Windows Server 2016 Standard | 9 |
| Windows Server 2019 Datacenter | 1 |
| Windows Server 2019 Standard | 17 |
| **Grand Total** | **70** |

* 1. **I4.5 - PowerShell v2**

### Description and cyber risk

PowerShell v2 lacks security protections that have been built into later versions. It has been deprecated 5 years ago and needs to be updated to improve security posture.

### Process Flow – Discovery, Analysis, and fix deployment



|  |  |
| --- | --- |
| **Details of Process Flow** | |
| **1** | Received list of servers from RT |
| **2** | List of servers will be considered in enterprise rollout plan |
| **3** | Only APAC servers will be considered for Pilot. Rest will be sent back to Enterprise Rollout back log. |
| **5** | Only Non PCN servers will be considered for Pilot. Rest will be sent back to Enterprise Rollout back log. |
| **6** | Criticality 3, 4, 5 or 6 will be considered for Pilot. Rest will be sent back to Enterprise Rollout back log. |
| **7** | Pilot list Approved by RT (Craig Young) |
| **8** | 50 Pilot Listed confirmed |
| **9** | Group servers based on server owners (use Pivot Table through Excel) |
| **10** | Send email communication to owners along with questionnaire |
| **11** | Raise Change Requests |
| **12** | Check for response from owners |
| **13** | Workshop/Discussion required with owners |
| **14** | Is there any Action Item comes out from Workshop/Discussion? |
| **15** | Implement on Action Item, if there is any outcome from Workshop/Discussion |
| **16** | Send reminder email to owners |
| **17** | Check if you receive response from owners |
| **18** | Send email communication to Owners along with change request and deployment date |
| **19** | Check if you receive response from owners |
| **21** | Request Itergy to link GPO through security filtering with servers |
| **22** | Check PS version by running PS script or logging to the server |
| **23** | Did remediation work? |
| **24** | If remediation did not work, reboot the servers |
| **25** | Check PS version by running PS script or logging to the server |
| **26** | Did remediation work? |
| **27** | Mark server as exception if remediation did not work |
| **28** | Update trackers with appropriate comments |
| **29** | App/Server Got Impacted. Did you receive any communication on the same? |
| **30** | Rollback by unlinking GPO or uninstalling WMF5.1 |
| **31** | Notify stakeholders appropriately |

### Vulnerable Server Discovery

PowerShell v2 needs to be removed and updated to Version 5.1 if possible. PowerShell version 2 (PSv2) comes pre-installed on Windows Server 2008. It is also installed on other versions of Windows Server OS in Rio Tinto fleet.

|  |  |
| --- | --- |
| **Discovery overview** | |
| Server Backlog | 189+XX |
| Pilot Servers – Non-critical | 50 |

### Server Analysis

After analysing the data and discussing in technical workshop with Rio SMEs, below criteria was agreed to perform analysis for pilot server selection:

1. Server criticality level : Non-critical (3, 4, 5 and 6)
2. Server environment : Non Production, Production low criticallity
3. Server Region : APAC
4. PCN Servers : Any PCN server with any criticality level is not in scope for Pilot

Below table list the count of pilot servers identified as per agreed criteria.

|  |  |
| --- | --- |
| **Server-Criticality** | **Pilot-Servers** |
| Level 3 | 3 |
| Windows Server 2008 R2 Standard | 2 |
| Windows Server 2016 Datacenter | 1 |
| Level 4 | 8 |
| Windows Server 2008 R2 Enterprise | 1 |
| Windows Server 2008 R2 Standard | 2 |
| Windows Server 2012 R2 Datacenter | 1 |
| Windows Server 2016 Datacenter | 1 |
| Windows Server 2019 Standard | 3 |
| Level 5 | 10 |
| Windows Server 2008 R2 Enterprise | 1 |
| Windows Server 2008 R2 Standard | 3 |
| Windows Server 2012 R2 Standard | 3 |
| Windows Server 2016 Datacenter | 2 |
| Windows Server 2019 Standard | 1 |
| Level 6 | 29 |
| Windows Server 2008 R2 Enterprise | 1 |
| Windows Server 2008 R2 Standard | 23 |
| Windows Server 2012 R2 Standard | 2 |
| Windows Server 2019 Standard | 3 |
| Grand Total | 50 |

As part of analysis of PowerShell version2 and the supportability of PowerShell on different operating system versions, below table list the server count and vulnerability fix deployment decisions:

|  |  |  |
| --- | --- | --- |
| **Operating System** | **Count** | **Deployment Decisions** |
| Windows Server 2003 | 14 | Windows 2003 Server cannot be updated to PowerShell version higher than 2.0. Out of Scope for PS version upgrade. |
| Windows Server 2008 | 15 | Windows 2003 Server cannot be updated to PowerShell version higher than 2.0. Out of Scope for PS version upgrade. |
| Windows Server 2008 R2 | 273 | In Scope for PowerShell V 5.1 upgrade. |
| Windows Server 2012 | Not provided yet | Windows 2012 Server that have PS 2.0 version installed as well as higher version of PS. PowerShell version 2 will be disabled and removed. |
| Windows Server 2016 | Not provided yet | Windows 2016 Server that have PS 2.0 version installed as well as higher version of PS. PowerShell version 2 will be disabled and removed. |
| Windows Server 2019 | Not provided yet | Windows 2019 Server that have PS 2.0 version installed as well as higher version of PS. PowerShell version 2 will be disabled and removed. |

1. **Vulnerability fix deployment**
   1. **Overview of vulnerability fix deployment**

During technical workshops various options were explored to deploy the vulnerability fixes. It was discussed and agreed that successful deployment method of vulnerability fix deployment on Pilot servers will pave the way for enterprise deployment. This section covers the deployment approach and rollback plan for each vulnerability.

## Deployment method for A3.1 Clear text

To apply vulnerability, fix for Clear text password, various options were discussed and in order to execute the fix deployment in controlled manner with velocity to target bulk servers it was agreed to make use of group policy to execute PowerShell script.

In essence, running below set of PowerShell commands by GPO through Security Filtering, will encrypt the content in web config files. Server reboot/IIS reset may require based on requirement.

**Deployment Instructions**

1. Open the CMD window on the server
2. Go to Server Drive Letter that ClearText File is located
3. Enter below command  
   **reg query “HKLM\SOFTWARE\Microsoft\Net Framework Setup\NDP” /s**
4. Check most recent .Net Framework Version
5. Traverse to that specific directory found in step 4
6. Enter below command

**ASPNET\_REGIIS -pef “connectionStrings” “application folder path”**

**Rollback Instructions**

Manually login to the faulty server or use Rollback GPO to decrypt config file info using below command

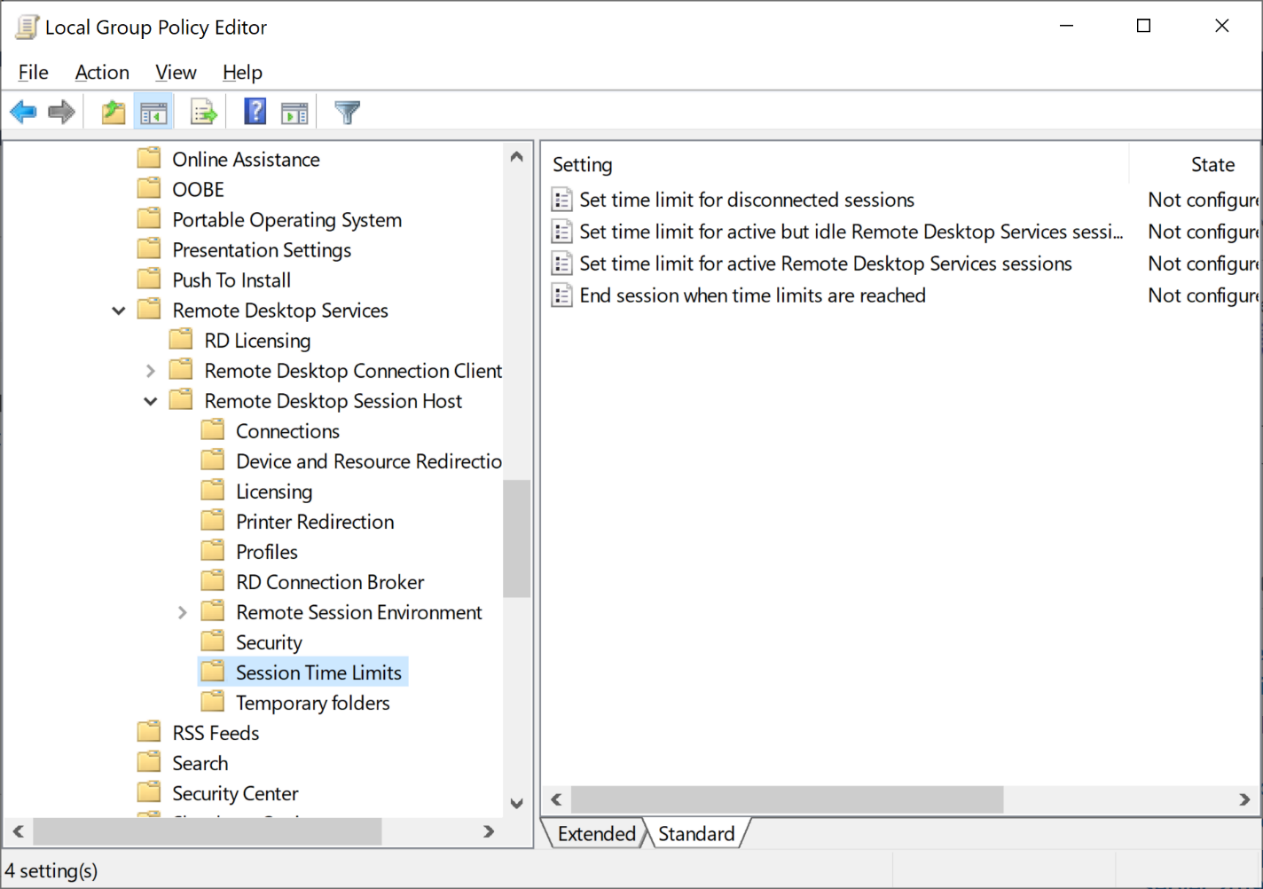
**ASPNET\_REGIIS -pef “connectionStrings” “application folder path”**

* + 1. **Deployment method for I4.1 RDP timeout**

Based on technical discussion, it was agreed to use Group Policy for limiting the RDP idle timeout and disconnected session timeout. The idle time out and disconnection timeout value are both 24 hours.

Group Policy configuration.

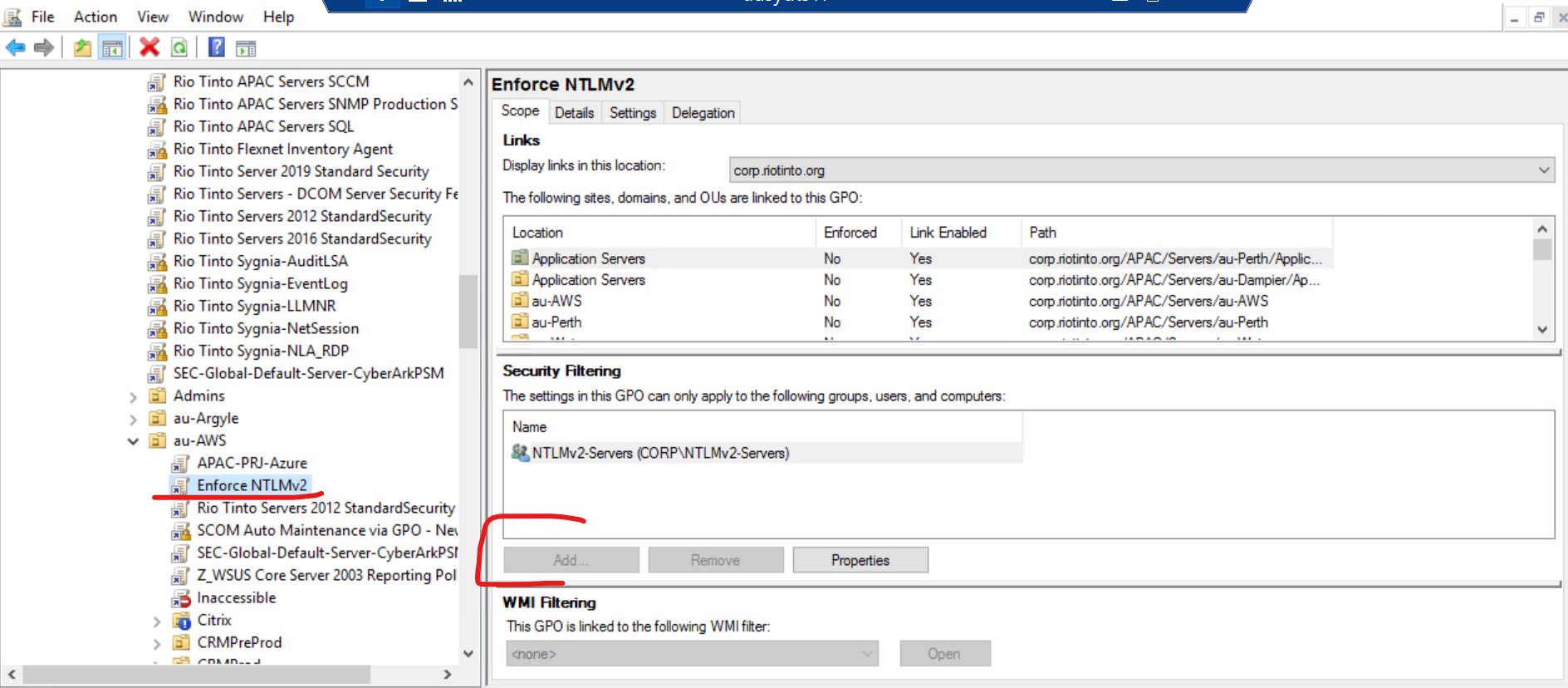
* Raise a ticket with Itergy to create a new Group Policy “Vulnerabilty\_fix\_RDP\_timeout” and security group “RDP\_timeout\_pilot” for 50 Pliot servers
* Itergy to link GPO “Vulnerabilty\_fix\_RDP\_timeout” to respective OUs.
* Under computer configuration navigate to Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Session Time Limits.
* In the right panel, double-click the Set time limit for active but idle Remote Desktop Services sessions policy: in the modal window that will appear, activate it by switching the radio button from Not configured to Enabled, then set 24 hours in the drop-down list right below.
* Double-click the Set time limit for disconnected sessions policy: in the modal window that will appear, activate it by switching the radio button from Not configured to Enabled, then set 24 hours in the drop-down list right below. Click Apply button.
* Screenshot below for the group policy settings.



Rollback instructions:

* Remove the server from “RDP\_timeout\_pilot” security group.
  + 1. **Deployment method for I4.3 NTLM V1 to NTLM V2**

As part of the previous project to configure NTLM V2 on few servers, a Group Policy was created, and security filtered to a security group. As part of this project, it was agreed to leverage the existing GPO for deployment and project team will coordinate with Itergy to link GPO and add new confirmed pilot servers to the security group which is part of security filtering.



Enforce NTLMv2 GPO policy is present, we can add members in Security Filtering with the help of Itergy Team. Add servers to NTLMv2 Servers appeared in security filtering.

**Rollback Instructions**

Delete the members from NTLMv2 servers group and verify older GPO is applied by querying LMcompatibility and result set of policies.

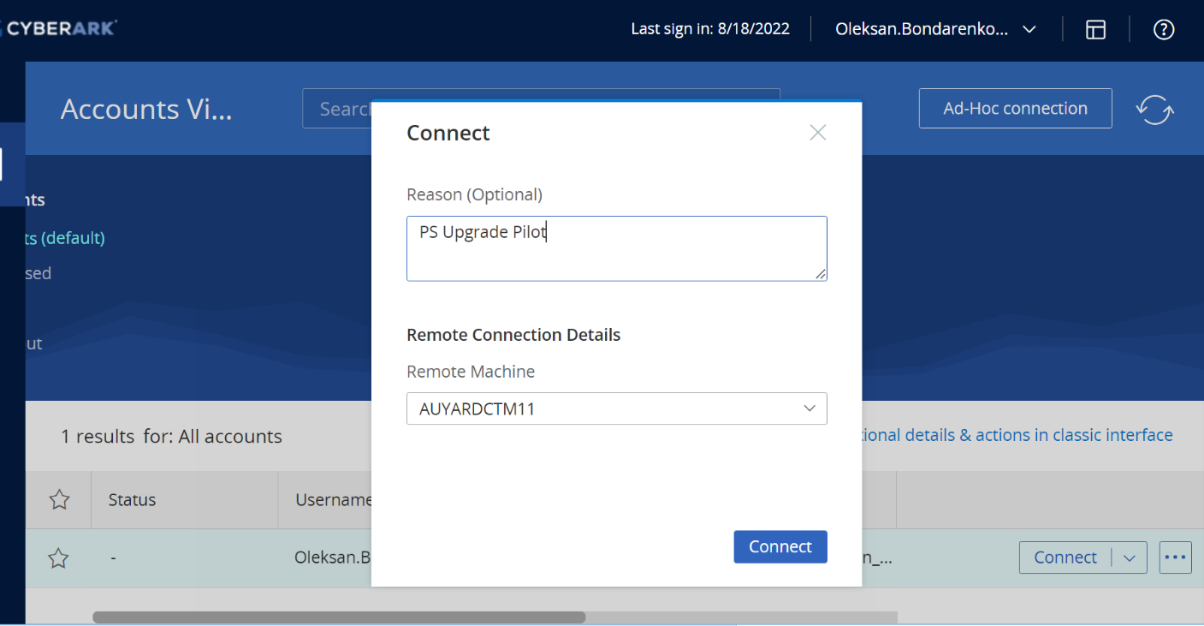
* + 1. **Deployment method for I4.5 PowerShell version update**

Based on technical discussion, we have identified 2 deployments methods that are going to be used for PowerShell vulnerability fix.

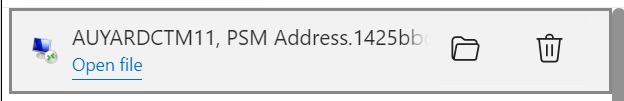
The first method is running PowerShell Script on Windows 2008 R2 Servers to install PowerShell v5.1.

**Deployment instructions**

1. Request Rio Tinto server team to make a back up of the server prior the change.
2. Restart the server if it has not been restarted for more than 30 days or any restart pending
3. Remote to the server and run the PowerShell scrip to update PS to version 5.1.
4. Connect to server via CyberArk



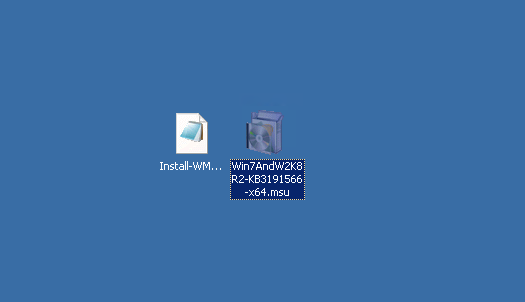
1. Click on Open file



1. Using RDP clipboard copy 2 files to desktop of the target server

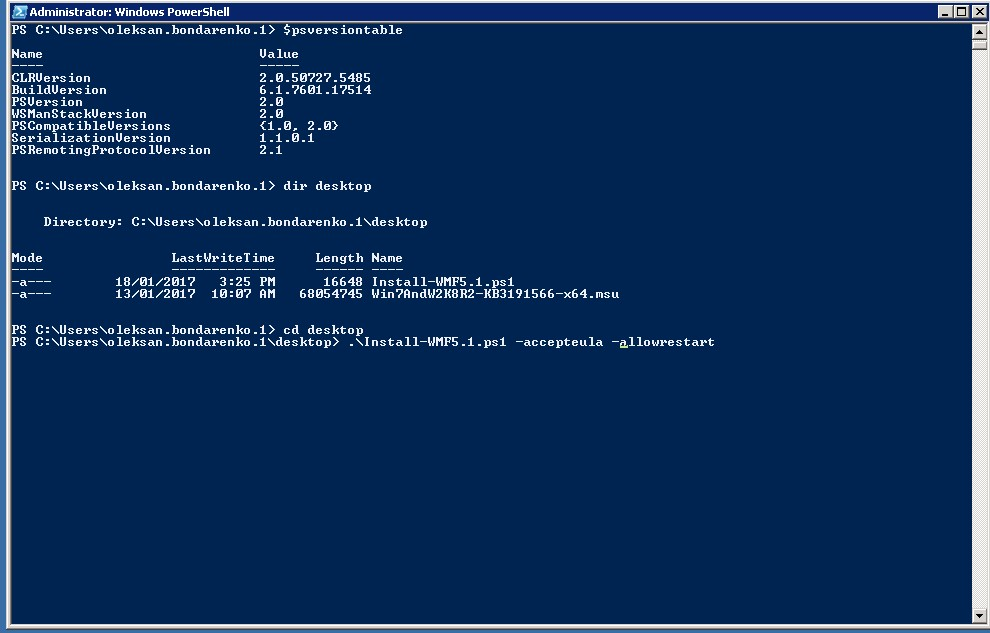
Install-WMF5.1.ps1

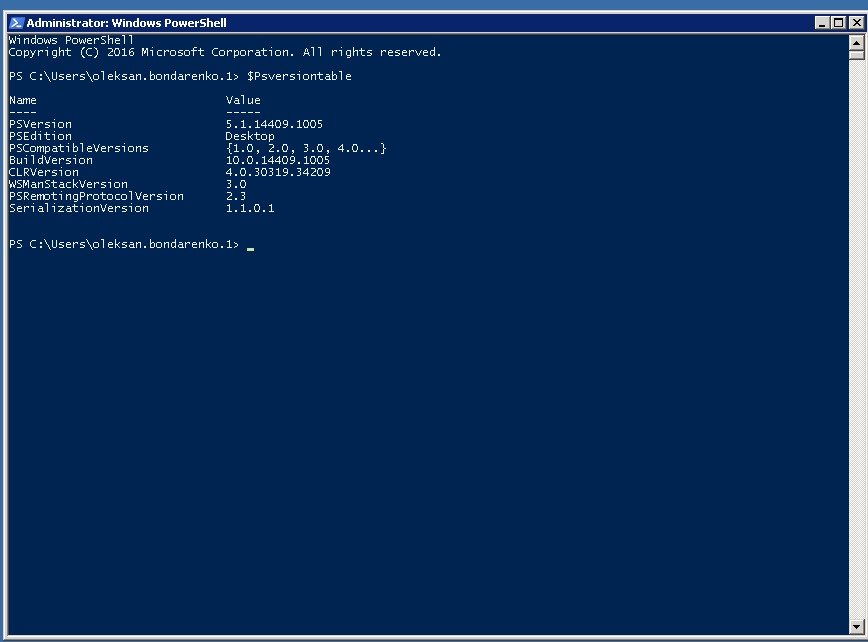
Win7AndW2K8R2-KB3191566-x64.msi



1. Execute Install-WMF5.1.ps1 script by running

.\Install-WMF5.1.ps1 -accepteula -allowrestart

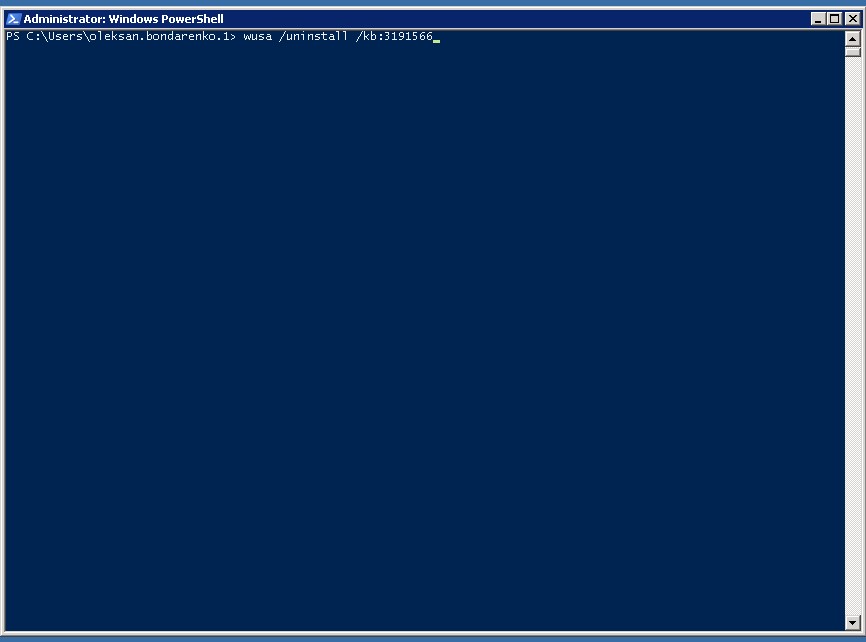


1. The Server will restart automatically after installation is completed. Estimated time 2 minutes.
2. After server restarted repeat step 2 and log in to Server again.
3. Check the PowerShell Version by running $PSVersionTable. Expected result is PSVersion 5.1

**Rollback instructions**

1. Connect to the server via CyberArk following steps 4 and 5 from Deployment instructions.
2. Run PowerShell command

Wusa /uninstall /kb:3191566



1. Reboot the server

The second method is to disable PowerShell v 2.0 on Windows 2012, 2016 and 2019. Those servers have already installed PowerShell V3.0 and up.

Group Policy configuration.

Avanade recommends 2 stage approach for removing PowerShell v2.0 from Windows Servers 2012, 2016, 2019.

In the first stage the script will disable the PowerShell v2.0 but not remove it from the system. It can be easily re enabled by running enable script without a need of reboot if roll back is required.

In the second stage if no issues are reported the second script will be applied that will remove PowerShell v2.0 from Server completely.

* Raise a ticket with Itergy to create a new Group Policy “Powershellv2\_disable” and security group “Powershellv2\_disable \_pilot” for 50 Pliot servers. Avanade to share the Powershell script with Itergy.
* Itergy to link GPO “Powershellv2\_disable” to respective OUs.
* PS Script to run “Disable-WindowsOptionalFeature -Online -FeatureName MicrosoftWindowsPowerShellV2“
* {To be discussed with Itergy where to store the PS script}
* Raise a ticket with Itergy to create a new Group Policy “Powershellv2\_remove” and security group “Powershellv2\_remove \_pilot” for 50 Pliot servers. Avanade to share the Powershell script with Itergy.
* Itergy to link GPO “Powershellv2\_remove” to respective OUs.
* PS Script to run “Disable-WindowsOptionalFeature -Online -FeatureName MicrosoftWindowsPowerShellV2 -Remove“
* {To be discussed with Itergy where to store the PS script}

Rollback instructions

* Raise a ticket with Itergy to create a new Group Policy “Powershellv2\_enable” and security group “Powershellv2\_enable \_pilot” for 50 Pliot servers. Avanade to share the Powershell script with Itergy.
* Itergy to link GPO “Powershellv2\_enable” to respective OUs.
* PS Script to run “Enable-WindowsOptionalFeature -Online -FeatureName MicrosoftWindowsPowerShellV2“
* {To be discussed with Itergy where to store the PS script}
  1. **Vulnerability fix deployment validation**
     1. **Deployment test for A3.1 Clear text**

Running PowerShell commands against the servers will help to determine that all config file, no longer contains clear text information.

|  |  |  |
| --- | --- | --- |
| **ServerName** | **Before Deployment** | **After Deployment** |
| Server1 | config file1 with IsFlagged/HasFlaggedBackup as True | config file1 with IsFlagged/HasFlaggedBackup as False |
|  | config file2 with IsFlagged/HasFlaggedBackup as True | config file2 with IsFlagged/HasFlaggedBackup as False |
|  | config file3 with IsFlagged/HasFlaggedBackup as True | config file3 with IsFlagged/HasFlaggedBackup as False |
| Server2 | config file1 with IsFlagged/HasFlaggedBackup as True | config file1 with IsFlagged/HasFlaggedBackup as False |
|  | config file2 with IsFlagged/HasFlaggedBackup as True | config file2 with IsFlagged/HasFlaggedBackup as False |
| . | config file3 with IsFlagged/HasFlaggedBackup as True | config file3 with IsFlagged/HasFlaggedBackup as False |
| . | config file 4 with IsFlagged/HasFlaggedBackup as True | config file 4 with IsFlagged/HasFlaggedBackup as False |
| Server3 | config file 1 with IsFlagged/HasFlaggedBackup as True | config file 1 with IsFlagged/HasFlaggedBackup as False |
| Server 4 | config file 1 with IsFlagged/HasFlaggedBackup as True | config file 1 with IsFlagged/HasFlaggedBackup as False |
|  | config file 2 with IsFlagged/HasFlaggedBackup as True | config file 2 with IsFlagged/HasFlaggedBackup as False |
| . | config file 3 with IsFlagged/HasFlaggedBackup as True | config file 3 with IsFlagged/HasFlaggedBackup as False |

### Deployment test for I4.1 RDP timeout

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Server Name** | **Before Deployment** | | | **After Deployment** | | |
| **REGEDIT** | **GPEDIT** | **GPO** | **REGEDIT** | **GPEDIT** | **GPO** |
| Server1 |  |  |  |  |  |  |
| Server2 |  |  |  |  |  |  |
| Server3 |  |  |  |  |  |  |
| . |  |  |  |  |  |  |
| . |  |  |  |  |  |  |
| N |  |  |  |  |  |  |

* + 1. **Deployment test for I4.3 NTLM V1 to NTLM V2**

Querying LM Compatibility level and result set of policies will confirm if NTLM authentication changed from v1 to v2. The following table will help to determine testing of fix.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Server Name** | **Before Deployment** | | **After Deployment** | |
| **REGEDIT** | **GPO** | **REGEDIT** | **GPO** |
| Server1 |  |  |  |  |
| Server2 |  |  |  |  |
| Server3 |  |  |  |  |
| . |  |  |  |  |
| . |  |  |  |  |
| N |  |  |  |  |

* + 1. **Deployment test for I4.5 PowerShell version update**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Server Name** | **Before Deployment** | | | **After Deployment** | | |
| PSVersionTable | **PS versions** | **GPO** | PSVersionTable | **PS version** | **GPO** |
| AUBNEW2K8D001 | 2.0 | 2.0 | NA | 5.1 | 5.1 | NA |
| AUBNEWTest(not tested) | 5.1 | 2.0, 5.1 | Not applied | 5.1 | 5.1 | Applied |
| Server3 |  |  |  |  |  |  |
| . |  |  |  |  |  |  |
| . |  |  |  |  |  |  |
| N |  |  |  |  |  |  |

1. **Appendix**

|  |  |  |
| --- | --- | --- |
| **Item** | **Description** | **Comments/Inputs** |
| I4.5-Powershell v5.1 Install | This script installs PowerShell v5.1 |  |
| I4.5-Powershell v2 disable | This script disables PowerShell v2. Applicable to Server 2012, 2016, 2019 | Disable-WindowsOptionalFeature -Online -FeatureName MicrosoftWindowsPowerShellV2 |
| I4.5-Powershell v2 enable | This script enables PowerShell v2. Applicable to Server 2012, 2016, 2019. Rollback script. | Enable-WindowsOptionalFeature -Online -FeatureName MicrosoftWindowsPowerShellV2 |
| I4.5-Powershell v2 remove | This script removes PowerShell v2. Applicable to Server 2012, 2016, 2019 | Enable-WindowsOptionalFeature -Online -FeatureName MicrosoftWindowsPowerShellV2 -Remove |
| A3.1 - IISDiscovery | This script helps to identify config files with vulnerabilities, when executed inside the server. |  |
| A3.1 - Encryption/Decryption Instructions | This file contains encryption/decryption instructions which will be used to remediate CTP vulnerability. |  |
|  |  |  |