Connect with Keiran O'Reilly, Peter Zuzula and Stephan Turgeon. to get assistance for server/app owner Include Craig and Rousko when scheduling meetings

Scott Goody – Application Coordinator

Abdul Karim – Application coordinator

**Account name - CORP\SA-ClearText-Remediation (service account details)**

User ID: SA-CTRemediation

Password:PRic6a9r

**Clear Text Password**

1. Get a list of servers from Rio
2. Run powershell or ask ansible team to do it and provide them with details **(review powershell and understand how it works)**
3. Add rows in sharepoint site with required fields

<https://riotinto.sharepoint.com/sites/S0261-RemoveClearTextPasswords/Shared%20Documents/Forms/AllItems.aspx?newTargetListUrl=%2Fsites%2FS0261%2DRemoveClearTextPasswords%2FShared%20Documents&viewpath=%2Fsites%2FS0261%2DRemoveClearTextPasswords%2FShared%20Documents%2FForms%2FAllItems%2Easpx&id=%2Fsites%2FS0261%2DRemoveClearTextPasswords%2FShared%20Documents%2FGeneral%2Fzzz%20Old%20Project%20Docs%20before%20Reset%2FDiscovery%2FScripts&viewid=5be2c2ac%2Da502%2D4288%2Db838%2D424681aed946>

1. Follow up if remediation does not happen
2. Change requests need not be raised, if you are not working on fix
3. IS&T remediation is Avanade responsibility

**NTLM approach steps**

server - server owner ---X

app1 owner - Y1

app2 owner - Y2

....

appn owner - Yn

Y1--Yn (it can be a same person, for one particular server)

X (permission) ---NTLM

Y1, Y2 ---- Yn (notification) (T1, T2..... Tn provide kro--- testers)

v1tov2 --- z date t time

Green signal

----------------------------------

Red signal -- sabne hath khade kr diye

Yellow Signal -kuch ne hath khade kr diye

Rollback plan -- ntlm v2tov1

Step 1 - Find the OU location of the computer object. Using DSA.MSC-> Advances Feature -> Find Computer object and check object tab

Step 2- Add the computer object into group named "NTLMv2-Servers"

Open DSA.MSC -> Find the group named "NTLMv2-Servers"- > Add computer object

Step 3 - Link the GPO named "EnforceNTLMv2" to the OU location using GPMC.msc

Step 4: Wait for AD replication to finish automatically Or manually enforce using "repadmin /syncall /AePdq"  - RT -

Step 5 : Wait for Group Policy to hit the phase one machines automatically or run "gupdate /force" for manual pull latest group policy changes. Can verify this with event ID 1704 under application logs

Questions

1. Do you use to send emails to App owners with change request, that you are planning to carry out NTLMv2 enabling on the servers?
2. Once you applied NTLMv2 on servers, did RioTinto carry some kind of testing that change did not effect any functionality. if yes, how the communication proceeds on that part. any template on emails

Answers

[Monday 7:01 pm] Mitul Naroia

1. I used to send email to App Owner first to seek approval and once they approve I used to mention about requirement of tester with planned date and time. Used to mention them over call that change management process will be followed. Once they approve usage then used to send email with Change detail
2. For testing, application server owner (as shared in point 1) tester details were shared and they used to test and confirm the functionality of the application which was hosted on server on which NTLMv2 was upgraded. I can share sample emails

Steps for change requests

Update our GPO named "Enforce NTLMv2" with below configuration - PT - Mitul and Arun

Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Network security: LAN Manager authentication level-> Send NTLMv2 response only/refuse LM and NTLM

2. Add our group to the GPO "Enforce NTLMv2" under security filtering of the GPO "Enforce NTLMv2"  - PT - Mitul and Arun

3. Add computer account to the group named NTLMv2-servers - RT - Tyson

4. Link the GPO  to following location - RT - AD Team

OU=Servers,OU=Infrastructure,OU=Accenture Cloud,OU=IST,DC=corp,DC=riotinto,DC=org

OU=au-Perth,OU=Servers,OU=APAC,DC=corp,DC=riotinto,DC=org

5. Wait for AD replication to finish automatically Or manually enforce using "repadmin /syncall /AePdq"  - RT - AD Team

6. Wait for Group Policy to hit the phase one machines automatically or run "gupdate /force" for manual pull latest group policy changes. Can verify this with event ID 1704 under application logs - RT - Application testers  / PT - Arun

7. Need to run Nexpose tool again to check status  NTLMv2 protocol on list of phase one servers - RT - Tyson

**Sharepoint Learning/Questions**

If you are having an issue with SharePoint/CMDB Data, then you will need to raise a SR?

Need sample SR (Rahul will provide sharepoint DL) for cmdb, server team can help [Wednesday 7:09 pm] Rahul Shrivastava (Accenture) (Guest)

**RTTMS Assignment Group - IST Infra APAC Servers**

Need deployment plan for clear text  (we don’t have any specific)

Who or how we can find out CMDB Name Application Name corresponding to server name? [possibly through powershell] (we need to fill in sharepoint)

Pls run powershell script and showcase the result. (Need to contact Ansible Team

Create a service account (Rahul will do it in next session)

Admin acct for each server, login to server, powershell and run it

Put 5 in (Feddrick hamelson (overall infra read) ) on request

Few fields in IIS Server list are not clear like UAT passed, MS Framework V

How to get admin access to power apps and how we can give access to App owners so that they can fill data

If you do not have access to the MS PowerApps, raise a RTTMS Service Request to eb added to the Azure AD Group ‘AzureADALL’.  **{SAMPLE RTTMS}**

**App owner/coordinator get access automatically**

**Rahul will make me owner to manage powerApps**

You will receive a Weekly Summary Email with a link to the MS PowerApps to manage the data.{Which email is being talked here}

What is connection string, how we can find it