Account Lockout

31 March 2023 02:43 PM

1. **NT account is getting locked very frequently, can we add account to No lockout exception (FGPP)**
   No, you must not add account to FGPP group
   Follow the lockout troubleshooting process

2. **NT account lockout shows local system (laptop\desktop system) as lockout source.**
   Make sure user has follow these steps

3. **Lockout tool does not show any sources or tool is down.**
   You can provide the sources from Splunk tool https://splunkcs.dell.com/en-US/app/dell_all_IAM-Ops/ad_account_lockouts__lockout_trend_analysis_copy

4. **User lockout shows only DC and not any sources.**
   You can use Splunk tool to find the failed activity. *Index=cim EventCode =4771 user=<username>*
   Or can use index=cim sourcetype=netlogon SERVICEFILWLDAO ("0xC0000234" OR "0xC000006A")

5. **Lockout sources are showing Exchange server.**
   User might have stored credentials for outlook on laptop. Kindly ask to clear Credential Manager from control panel
   Kindly ask user to un-enroll his mobile device from Dell network and then re-configure.
   ** You can refer these steps for checking exchange logs.

6. **Lockout shows VDS as source**
   User has already changed password, but still the sources are showing as VDS.
   Search in SPLUNK
   index=radiantlogic source=D:\\radiantone\\vds\\r1syncsvcs\\log\\*pwdsynctopo\\*capture.log <NTID>

   If the above search is empty it means that the ICS agent running on the domain controllers, did not send the password update to the ICS cluster. Using the same issue, submit a task (similar to this TASK7693232), assign it to SECURITY-DIRECTORY-L3 and ask them to check the ICS agent. If necessary, ask them to restart it.

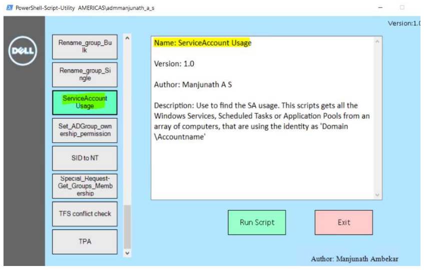
   Once the above task is completed, ask the user to change the password again. If the problem persists, assign the issue to us for investigation. I will share further details about the troubleshooting process to get help from you to resolve this problems much faster.

7. **Can user access our Splunk Dashboard or can I share to user?**
   No, access is restricted only to our team usage.

8. **I have a request to add service account manually to no lockout exception. Which group to add?**
   You must use the below groups to add the accounts to no lockout exception group manually.
   Generally, user can use the Service Account form to request add the account to exception max upto 10 days.

FGPP_AMER_TEMP_NLG_AUTO	AMER.DELL.COM
FGPP_EMEA_ TEMP_NLG_AUTO	EMEA.DELL.COM
FGPP_JAPN_ TEMP_NLG_AUTO	JAPN.DELL.COM
FGPP_APAC_ TEMP_NLG_AUTO	APAC.DELL.COM
FGPP_CORP_TEMP_NLG_AUTO	CORP.EMC.COM
FGPP_Production_TEMP_NLG_AUTO	production.online.dell.com

9. **Is there a way to find the usage of Service Account?**
   Yes, only from the list of servers provided, you can use the script loaded onto GUI tool


PowerShell-Script-Utility AMERICAS\admmanjunath_a_s
Version:1.0
Rename_group_Bulk
Rename_group_Single
ServiceAccount Usage
Set_ADGroup_ownership_permission
SID to NT
Special_Request-Get_Groups_Membership
TFS conflict check
TPA
Run Script
Exit
Author: Manjunath Ambekar

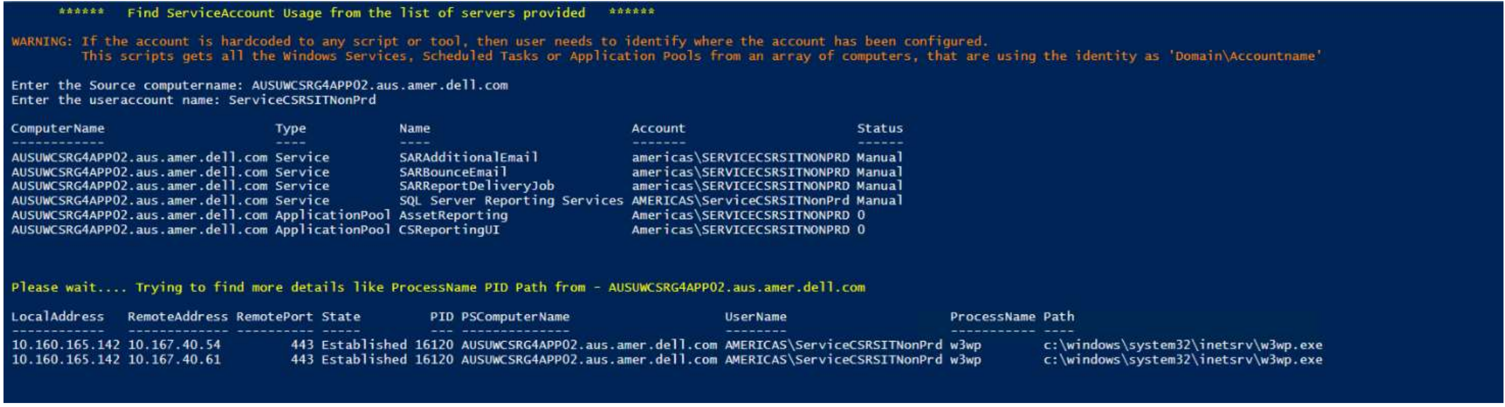
Name: ServiceAccount Usage

Version: 1.0

Author: Manjunath A S

Description: Use to find the SA usage. This scripts gets all the Windows Services, Scheduled Tasks or Application Pools from an array of computers, that are using the identity as 'Domain \Accountname'

Sample how the output looks like.



```
       ******   Find ServiceAccount Usage from the list of servers provided   ******

WARNING: If the account is hardcoded to any script or tool, then user needs to identify where the account has been configured.
         This scripts gets all the Windows Services, Scheduled Tasks or Application Pools from an array of computers, that are using the identity as 'Domain\Accountname'

Enter the Source computername: AUSUWCSRG4APP02.aus.amer.dell.com
Enter the useraccount name: ServiceCSRSITNonPrd

ComputerName                      Type            Name                          Account                        Status
------------                      ----            ----                          -------                        ------
AUSUWCSRG4APP02.aus.amer.dell.com Service         SARAdditionalEmail            americas\SERVICECSRSITNONPRD Manual
AUSUWCSRG4APP02.aus.amer.dell.com Service         SARBounceEmail                americas\SERVICECSRSITNONPRD Manual
AUSUWCSRG4APP02.aus.amer.dell.com Service         SARReportDeliveryJob          americas\SERVICECSRSITNONPRD Manual
AUSUWCSRG4APP02.aus.amer.dell.com Service         SQL Server Reporting Services AMERICAS\ServiceCSRSITNonPrd Manual
AUSUWCSRG4APP02.aus.amer.dell.com ApplicationPool AssetReporting                Americas\SERVICECSRSITNONPRD 0
AUSUWCSRG4APP02.aus.amer.dell.com ApplicationPool CSReportingUI                 Americas\SERVICECSRSITNONPRD 0



Please wait.... Trying to find more details like ProcessName PID Path from - AUSUWCSRG4APP02.aus.amer.dell.com

LocalAddress   RemoteAddress RemotePort State         PID PSComputerName                    UserName                     ProcessName Path
------------   ------------- ---------- -----         --- --------------                    --------                     ----------- ----
10.160.165.142 10.167.40.54         443 Established 16120 AUSUWCSRG4APP02.aus.amer.dell.com AMERICAS\ServiceCSRSITNonPrd w3wp        c:\windows\system32\inetsrv\w3wp.exe
10.160.165.142 10.167.40.61         443 Established 16120 AUSUWCSRG4APP02.aus.amer.dell.com AMERICAS\ServiceCSRSITNonPrd w3wp        c:\windows\system32\inetsrv\w3wp.exe
```