**lusrmgr.msc**

**gpedit.msc**

**gpupdate /force**

**secpol.msc**

**rsop.msc**

**Check for the Events (1074 - Planned Reboot / 6008 - Unexpected Reboot / 6006 – Event Log Stopped / 6005 – Event Log Started) in System Event based on the server uptime.**

|  |
| --- |
| Event ID 4625 |
| failed attempt at logging on to a local computer |

|  |
| --- |
| service status change to disable or start |
| event ID 7040   |  | | --- | | user login time: 4688 | | user locked time: 4800 |  |  | | --- | | IIS | | Install-WindowsFeature -name Web-Server -IncludeManagementTools |  |  | | --- | | *Get-WindowsFeature Windows-Server-Backup* | | *Install-WindowsFeature -Name Windows-Server-Backup* |   User property check  get-aduser -Identity “accountname” -Properties passwordlastset  eventlog check:  Get-WinEvent -FilterHashtable @{logname = 'System'; id = 1074} | Format-Table -wrap  Port check:  Test-NetConnection -ComputerName servername -Port 137  wbadmin start systemstatebackup -backuptarget:d:   |  | | --- | | Check system is VM or physical | | get-wmiobject win32\_computersystem | fl model | | systeminfo /s %computername% | findstr /c:"Model:" /c:"Host Name" /c:"OS Name" |   wmic bios get serialnumber |

DISM /online /Cleanup-Image /SpSuperseded  --------- Space clean up from winsxs

dism /image:c:\ /remove-package /packagename:

SHUTDOWN /r /f /t 5 /c "Weekely Scheduled Reboot" (task scheduler)

shutdown /f /r /m \\IP address : force reboot from jump server

resetsp from putty to reset IMM

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CHKDSK /r/f : On All Drives (from VM console) à First attempt   Defrag /a /u /v   |  | | --- | | To verify the NTP server | | w32tm /query /peers | | w32tm /query /status | | w32tm /resync | |
| UNC access port. |
| TCP 135 , 139, 445 UDP 135, 137, 138   |  | | --- | | Know for 32 or 64 bit | | echo %PROCESSOR\_ARCHITECTURE% | | Set pro |   Command to get windows security patches in details: C:\ wmic qfe list  wmic qfe list > UpdateList.txt : How to Get a List of All of the Installed Updates on Windows   |  | | --- | | Whenever Windows updates website scans and install any updates or patches, it gets stored on the below location. %windir%\softwaredistribution\download | | net stop wuauserv rmdir %windir%\softwaredistribution /s /q net start wuauserv exit | |

vssadmin list shadows

|  |
| --- |
| To Turn Off: NetSh Advfirewall set allprofiles state off To Turn On: NetSh Advfirewall set allprofiles state on To check the status of Windows Firewall: Netsh Advfirewall show allprofiles |
| How to Terminate a Remote Desktop Session from the Command Line Remotely   |  | | --- | | Public private | | Get-NetConnectionProfile | | Set-NetConnectionProfile -Name “Unidentified network” -NetworkCategory Private | |
| Login thru jump server |
| C:> qwinsta /server: servername |
| C:> rwinsta 6 /server: servername |

wmic useraccount where sid="S-1-5-21-329068152" get name

wmic useraccount where name='test\_user' get sid

|  |
| --- |
| to check PID of service |
| *sc queryex servicename* |

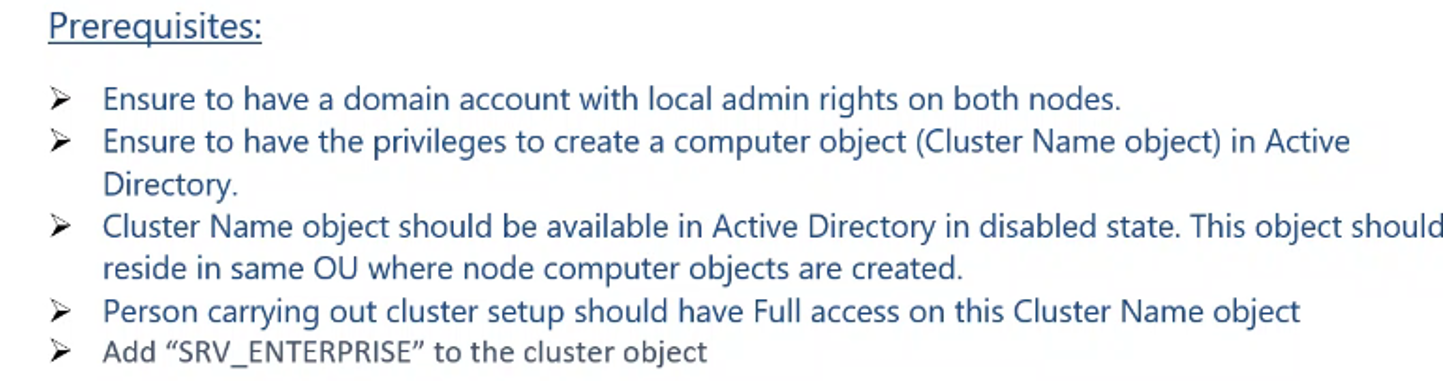
taskkill /PID service name /f

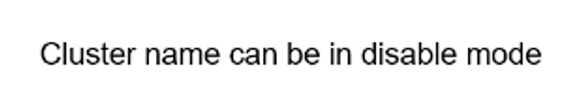
|  |
| --- |
| sc queryex servicename find the PID  taskkill /f /pid [PID] |
| taskkill /F /IM .exe |

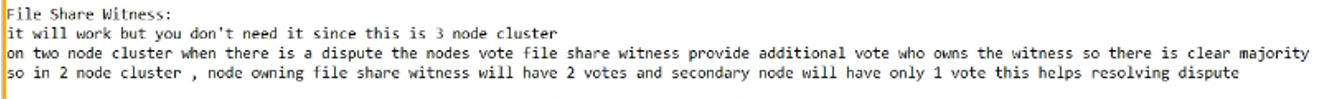
WinDbg.exe

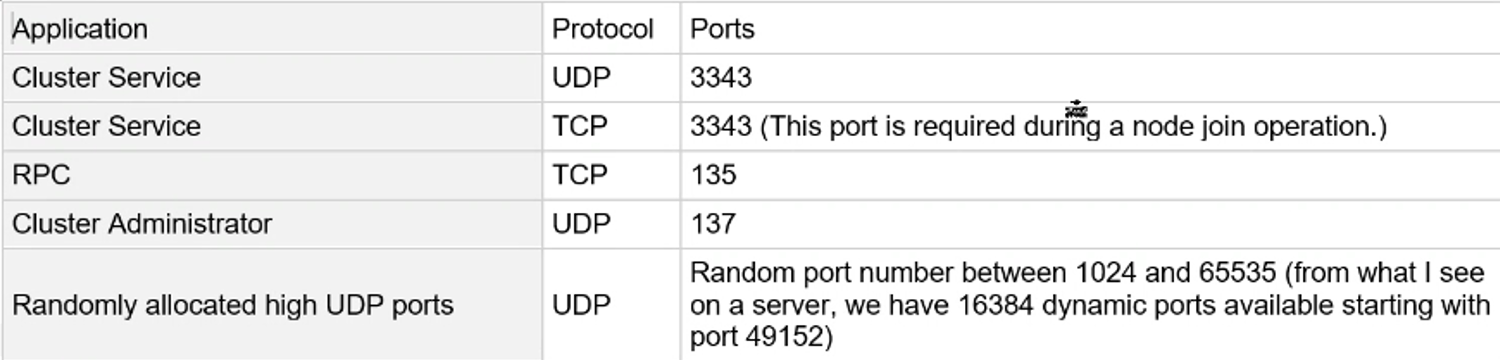
|  |
| --- |
| netstat -ano |findstr "port number" |
| netstat -an |find /i "listening" |

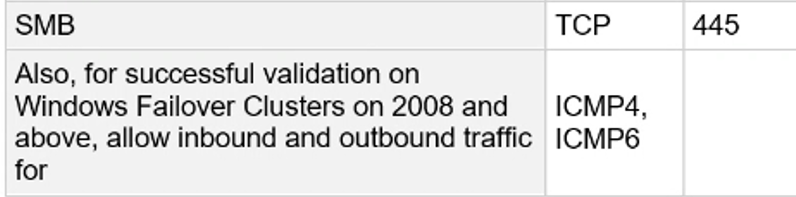
Prerequisites:  
Ø Ensure you have a domain account with local admin rights on both nodes.   
Ø Ensure you have the privileges to create a computer object (Cluster Name object) in Active Directory.   
Ø Cluster Name object should be available in Active Directory in disabled state. This object should reside in same OU where node computer objects are created.  
Ø Person carrying out cluster setup should have Full access on this Cluster Name object









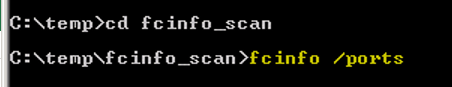


Mulipath checking command:













**Remediation steps for Cluster issue:**

If any node is showing down in cluster, need to check some basic troubleshooitng

1. Check both node status
2. Check Heartbeat communication status and also check Heartbeat NIC should be in Private network.
3. Check cluster serivce status.

Check cluster events for further analysis

**Failover cluster manager** or type in Run : **cluadmin.msc**

Power-shell commands:

Check also through command cluster node and resources.

|  |  |  |
| --- | --- | --- |
| get-clusterresource | ft cluster,name,ownernode,resourcetype,iscoreresource   |  | | --- | | Get-ClusterResource | | Get-ClusterNode |   move-clustergroup "cluster Group" |
|  |
|  |
| ====================================================  Heartbeat NIC should be assign as Private.  If it is Public then make it private  as checked from the below command and change to private.  *Get-NetConnectionProfile* |
| *Set-NetConnectionProfile -Name “Unidentified network” -NetworkCategory Private*  quarantine state when the node connectivity has an issue Start-ClusterNode -ClearQuarantine   * both nodes and cluster object should be in same OU   dsregcmd /status to check the Azure AD joined status  dsregcmd.exe /leave  Administrators group users and groups were showing the SID and it was not resolving with the name  Check DNS side and then try to below  HKLM\Software\Policies\Microsoft\Windows NT\RPC\EnableAuthEPResolution registry key from 1 to 0  (the default value)       Repair the EFI Bootloader on a GPT Disk of UEFI Computer First of all, find a FAT32 hidden partition and assign a drive letter to it (the size of this partition is 100-300MB,  it is used to store the Windows bootloader which is called by the EFI bootloader).  Diskpart List vol    detected that it is Volume 1 with the label BOOTSTRAP  Select this EFI partition and assign a drive letter to it:  select volume 2 assign letter M: exit  Re-create the BCD bootloader configuration file:  cd /d m:\efi\microsoft\boot\ ren BCD BCD.bak bcdboot E:\Windows /l en-us /s M: /f ALL  Create bootloader configuration files on the E:\ drive:  bcdboot E:\Windows /S E:  The “Boot files successfully created Re-create a Master Boot Record (MBR):bootrec.exe /FixMbr bootrec.exe /FixBoot bootrec.exe /RebuildBc ref: https://www.lifewire.com/how-to-rebuild-the-bcd-in-windows-2624508 |

SCCM Agent Uninstallation

cd c:\Windows\ccmsetup

ccmsetup.exe /uninstall

SCCM Agent Cleanup

1. Check if the SMS Agent Host service is gone
2. Checks if CCMSetup service is gone
3. Check if below directories are deleted (if not, delete them)
   1. %windir%\ccm
   2. %windir%\ccmsetup
   3. %windir%\ccmcache
4. Check if these files are deleted (if not, delete them)
   1. %windir%\smscfg.ini
   2. %windir%\sms\*.mif

Advanced cleanup

These steps are usually not needed. Perform only if automatic uninstall fails or you can check if auto uninstall cleaned up properly.

1. Delete from registry
   1. HKLM\software\Microsoft\ccm
   2. HKLM\software\Microsoft\CCMSETUP
   3. HKLM\software\Microsoft\SMS
2. Delete from WMI
   1. root\cimv2\sms
   2. root\ccm
3. Delete from TaskScheduler any tasks under Microsoft / Configuration Manager

Secondary login issue fix during server access through PAM

registry Settings:  
HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services  
Property : fPromptForPassword  
Value: 0 = Disable  
  
  
HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp  
Property: fInheritAutoLogon  
Valud: 1 = Enable  
  
Group Policy:  
  
Administrative Templates --> Windows Components --> Remove Destip Services --> Remote Desktop Session Host --> Security  
  
Always prompt for pasword upon connection - Disabled

net user APP01 admin@123 /ADD /FULLNAME:"APP1" /comment:"RITM"  
net user APP02 admin@123 /ADD /FULLNAME:"APP2" /comment:"RITM]"  
net localgroup administrators APP1 APP2 /add

|  |
| --- |
| WSUS |
| wuauclt /detectnow |
| wuauclt /reportnow |

netsh winsock reset catalog  
netsh int ipv4 reset reset.log  
netsh int ipv6 reset teset.log

back up on any volume:

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\wbengine\SystemStateBackup\  
Name:AllowSSBToAnyVolume  
Data type:DWORD  
Value data:1  
Note When this value is set to 1, system state backups to any volume are enabled.

Disbale SMB V1 and reboot. DisableWindowsOptionalFeature -Online -FeatureName smb1protocol, ref the KB-

<https://support.microsoft.com/en-us/help/2696547/detect-enable-disable-smbv1-smbv2-smbv3-in-windows-and-windows-server>

To check SMB V1 Status:-  
Get-WindowsFeature FS-SMB1  
Get-WindowsOptionalFeature –Online –FeatureName SMB1Protocol   
  
  
To disable SMB V1 on Servers: -  
Set-SmbServerConfiguration -EnableSMB1Protocol $false  
Disable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol

## Key Management Service

|  |
| --- |
| KMS TCP listening port should be configured to 1688 |
| To confirm the activation method set on the device, run the following command: |
| slmgr -dlv |
| Look for the **Product Key Channel** setting. **Volume:GVLK** means the device uses to **KMS activation**, **Volume:MAK** means the device uses to **MAK** activation. |
| KMS machine IP |
| Request activation from the KMS |
| slmgr.vbs /ato or manually |
| slmgr.vbs /skms servername:1688 |
| The KMS infrastructure is very simple: just install Volume Activation Services role on Windows Server,  add your KMS Host Key (from Microsoft Volume Licensing Service Center) and activate your corporate  KMS server on Microsoft (this operation is performed only once). After that your enterprise KMS clients  can send activation requests to the KMS server and activate on it. |

slmgr /ipk “key”

Slmgr.vbs /ipk kms key   
  
Slmgr.vbs /ato   
  
SLMGR /skms servername:1688

|  |
| --- |
| netsh interface ipv4 show inter |
| netsh interface ipv4 set interface 8 dadtransmits=0 store=persistent (check which IDX = 8)     |  | | --- | | Black screen | | CTRL+SHIFT+ESC | | In the task manager, goto File --> Run new task and type “explorer.exe”, it will load and show the normal desktop |  |  | | --- | | eventviewer issue ---- | | C:\ProgramData\Microsoft\Event Viewer\Views | | delete the file view0 | | local group check | | net localgroup administrators   |  | | --- | | **Group Policy to set session time limits for all users:** | |  | | 1. Cmd prompt, gpedit.msc | | Computer Configuration, Admin Templates, Windows Components, Remote Desktop Services,  Remote Desktop Session Host, Session Time Limits | | Enable appropriate group policies and modify as needed | | We recommend setting this one because it will prevent disconnected sessions from consuming server  resources — “Set time limit for disconnect sessions” | | After modifying group policies, you can force an update without rebooting by  typing “gpupdate /force” at cmd prompt   |  | | --- | | systeminfo |find "Available Physical Memory"  systeminfo | find "Virtual Memory" | | wmic ComputerSystem get TotalPhysicalMemory | | wmic OS get FreePhysicalMemory | | |   IIS reset   |  | | --- | | iis reset | | iisreset /noforce   |  | | --- | | <https://support.oneidentity.com/one-identity-safeguard-for-privileged-passwords/kb/262161/psm-rdp-error-the-connection-has-been-terminated-because-an-unexpected-server-authentication-certificate-was-received-from-the-remote-computer-> | | The connection has been terminated because an unexpected server authentication  certificate was received from the remote computer   |  | | --- | | port getting exhaustion in windows rdp issue | | <https://docs.microsoft.com/en-us/windows/client-management/troubleshoot-tcpip-port-exhaust>  [3:06 PM] Murugaiyan, Srinivasan M (Ext)     SLA Priority Incident Response Time Incident Resolution Time P1 15 Minutes 1 Hour P2 15 Minutes 3 Hours P3 30 Minutes 8 Hours P4 2 Hours 48 Hours   |  | | --- | | Boot time: | | Wmic os get lastbootuptime | | Systeminfo | find "System Boot Time" | |  | | Get-WinEvent -FilterHashtable @{logname = 'System'; id = 1074, 6005, 6006, 6008} -MaxEvents 6 |  Format-Table -wrap | |  | | vssadmin list shadows vssadmin delete shadows /all   |  | | --- | | HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\RCM\GracePeriod | | just rename the grace period | | Right Click and go to Permission – Advanced – Owner. Change the ownership to Administrator Account | | RDs licensing issue facing |   Software update folder rename:   |  | | --- | | net stop wuauserv and press the ENTER key.  Type ren c:\windows\SoftwareDistribution softwaredistribution.old and press the ENTER key.  Type: net start wuauserv and press the ENTER key.  Crash Dump creation | |  | | HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\CrashControl   Set CrashDumpEnabled to 1 and then reboot.  gwmi Win32\_PerfFormattedData\_PerfOS\_System -co "computername" | fl \*  wmic /node:"computername" path Win32\_PerfFormattedData\_PerfOS\_System get systemuptime      **Splunk** is a software platform widely **used** for monitoring,  TCP **port** 8089 by default                Issue : “ \_\_\_\_\_“group got removed from the “Remote desktop users” group.  Analysis : Permission at RDS Farm level and Server level (Remote desktop users group)  is not at same level. If session collection get refreshed at any time, it will remove all the groups  which are not a member of RDS Farm from            Remote desktop users group. Certificate renewal doesn’t remove any group.  Root cause : Misconfiguration of RDS farm. Not configured as per NVS standard.  Solution :  Make the permission level same at Farm and Server level (Remote desktop users group).  Recommendation : Correct the permission and make it same at farm  and Remote desktop users group to avoid reoccurrence of the issue.  Also, not to add any individual ID and domain users to farm or Remote desktop group.  Permission need to provide at farm level only. It will get added automatically to Remote desktop user  group on all servers        Collection name : dev.contoso.com  Servers: srv1.contoso.com 192.168.01 and srv2.contoso.com 192.168.0.2  DNS register for this  Nslookup dev.contoso.com  Registered IP 192.168.0.1  192.168.0.2  Vulnerabilities:  Idle Session Time” and “Disconnected Session Time” local group policy on the server has been configured  to 2 day. As per OS Standard Idle Session Time and Disconnected Session Time should be 15 mins  and 5 mins respectively. If it is your Application requirement, please raise an exception with ISRM Team  to avoid these policies being detected as failure in IT360 Scan or QG Scan report | | | | | |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

|  |
| --- |
| **Finding Type** |
| 4135 - Status of the 'Set Time Limit for Disconnected Sessions' Group Policy setting (Terminal Services) |
| 4137 - Status of the 'Set time limit for active but idle Terminal Services sessions (and Idle session limit)' Group Policy setting |
|  |

remediation plan for the reported vulnerabilities and SSC Failures in the server

**Windows Service Weak Permissions detected:**

**Administrator Account's Password Does Not Expire**

**SMB Version 1 Enabled**

**Sysinternals PsExec Elevation of Privilege Vulnerability**

**EOL/Obsolete Software:**

Below are SSC Failures, with attach Compliance report.

|  |
| --- |
| 2582 - Status of the 'User Account Control: Detect application installations and prompt for elevation' setting |
| 2606 - Status of the 'User Account Control: Switch to the secure desktop when prompted for elevation' setting |
| 2586 - Status of the 'User Account Control: Admin Approval Mode for the Built-in Administrator account' setting How To use Nltest Dsgetsite to Retrieve Current AD Site Name nltest /dsgetsite |
| machine is a member of the **Default-First-Site-Name**Active Directory site in the below example.  nltest /DSGETDC:  nltest /sc\_query:domainname  set L  echo %logonserver%  nltest /dclist:  **Nltest uses** the secure channel for logons between client computers and a domain controller, or for directory service replication between domain controllers  set l  will respond with the variables for both localappdata and for logonserver. However, logonserver is the only variable you are interested in, and the one which will tell you the name of the domain controller you authenticated against.  ---------------------------------------------------------  **Set Logonserver** the name of the domain controller that authenticated the user will be returned  Using **echo %username%**will allow you create a script to identify the authenticating domain controller |
| If you just desire to identify which domain controller the user retrieved group policies from you can type **gpresult /r**. The returned results will provide you the name of the domain controller that provided the logged on user with GPOs  Group Policy was applied from: Domain name  LOGONSERVER=\\servername |