|  |  |  |
| --- | --- | --- |
| 1. **Pre-Replication Tasks – Source Server** | | |
| * 1. Exclude Anti-Virus software functions on Mobility Services agent client folders. | Make sure Anti-Virus software excludes the location:  C:\ProgramData\ASR\agent | DevOps |  |
| * 1. Make sure RDP service is enabled and Firewall allows RDP from local networks | Enable RDP on the source server:   1. Click **Start**, click **Control Panel**, and then click **System**. 2. Click the **Remote** tab, click to select the **Allow users to connect remotely to your computer** check box, and then click **OK**.   (OR)  Execute the below in an administrator command prompt:  reg add "HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG\_DWORD /d 0 /f  Allow RDP in Firewall:  *CMD Option:*  netsh firewall set service type = remotedesktop mode = enable  netsh advfirewall firewall set rule group="remote desktop" new enable=Yes  netsh advfirewall firewall add rule name="Open Remote Desktop" protocol=TCP dir=in localport=3389 action=allow  *PowerShell Option:*  Enable-NetFirewallRule -Name "RemoteDesktop-UserMode-In-TCP"  Enable-NetFirewallRule -Name "RemoteDesktop-UserMode-In-UDP" | DevOps |  |
| * 1. Check SAN policy | On the source server:   1. Enter **diskpart**. 2. Enter **SAN**. If the drive letter of the guest operating system isn't maintained, **Offline All** or **Offline Shared** is returned. 3. At the **DISKPART** prompt, enter **SAN Policy=OnlineAll**. This setting ensures that disks are brought online, and it ensures that you can read and write to both disks. | DevOps |  |
| * 1. Add local admin account | Add a local user account to the source server with the predefined username and password.  Add the user account to both “Administrators” and “Remote Desktop Users” group.  User Name: cpnntlcl | DevOps |  |
| * 1. No pending Windows updates | Make sure there are no pending windows updates. Install all pending windows updates if any. | DevOps |  |
| * 1. Install Mobility Service Agent | Push Installation:  Refer 2.1.6  If push installation fails for any reason, try manual installation method.  Manual Installation:  <https://docs.microsoft.com/en-us/azure/site-recovery/vmware-physical-mobility-service-overview#install-the-mobility-service-using-ui>   1. Copy installer from Configuration Server and run the application.   **Location:** \\**<ConfigServerName>**\i$\Program Files (x86)\Microsoft Azure Site Recovery\home\svsystems\pushinstallsvc\repository\Microsoft-ASR\_UA\_9.32.0.0\_Windows\_GA\_10Jan2020\_Release.exe   1. Select Install Mobility service and click Next.      1. Select default location and click Next.        1. Enter the IP address of Configuration Server and the Phassphrase and then click Register.     Manual Installation Command Line:   1. Copy installer from Configuration Server to temp folder.   **Location:** \\**<ConfigServerName>**\i$\Program Files (x86)\Microsoft Azure Site Recovery\home\svsystems\pushinstallsvc\repository\Microsoft-ASR\_UA\_9.32.0.0\_Windows\_GA\_10Jan2020\_Release.exe   1. Extract the installer.   cd C:\Temp  ren Microsoft-ASR\_UA\_version\_Windows\_GA\_date\_release.exe MobilityServiceInstaller.exe  MobilityServiceInstaller.exe /q /x:C:\Temp\Extracted  cd C:\Temp\Extracted   1. Install agent.   UnifiedAgent.exe /Role "MS" /InstallLocation "C:\Program Files (x86)\Microsoft Azure Site Recovery" /Platform "VmWare" /Silent   1. Register agent.   cd C:\Program Files (x86)\Microsoft Azure Site Recovery\agent  UnifiedAgentConfigurator.exe /CSEndPoint <CSIP> /PassphraseFilePath <PassphraseFilePath> | DevOps |  |
| 1. **Replication Tasks** | | |
| * 1. Create replication | 1. Go to “Replicated Items” in the target RS Vault.      1. Click on “Replicate”.      1. In the Enable Replication blade for ‘Source’, provide the below information. Provide the appropriate Source Location and Process Server details and click OK.   **For On-Premesis Source VMs:**  **Source Location:** US**SJ**CAZMG001PRD  **Process Server:** US**SJ**CAZMG001PRD (OR) US**SJ**CAZMG002PRD  **For Azure Source VMs:**  **Source Location:** US**AZ**AZMG001PRD  **Process Server:** US**AZ**AZMG001PRD     1. For Target, provide the details as below. Provide appropriate values for “Subscription”, “Post-failover resource group”, “Post-failover Azure network” and “Subnet” and click OK. Refer to the wave plan spreadsheet to get the target environment details.   **For Dev/UAT Targets:**  **Subscription:** Retail Dev  **Post-failover Resource Group:** <Refer to target sizing in wave plan spreadsheet>  **Post-failover Azure network:** PZ\_VNET\_RETSOL\_DEV\_VNET\_01  **Subnet:** <Refer to target sizing in wave plan spreadsheet>  **For Prod Targets:**  **Subscription:** Retail Prod  **Post-failover Resource Group:** <Refer to target sizing in wave plan spreadsheet>  **Post-failover Azure network:** TBD  **Subnet:** <Refer to target sizing wave plan spreadsheet>     1. For Virtual Machines, select the Server(s) from the list. Select all dependent servers if they need to failover as part of the same application.      1. In Properties, select the managed disk type for the VMs, cache storage account and user to push install the mobility agent (defaults to admin). Refer to the Source/Target Size Mapping document for correct target disk types.      1. In Replication Settings, select the replication policy to use and check Yes for Multi-VM consistency to create a Replication Group if replicating more than one server as part of an application and they need to replicate and failover together.      1. Click OK and the replication will start. | DevOps |  |
| * 1. Monitor Replication | 1. Go to “Replicated Items” in the RS Vault and check if the replicating machines are healthy. Diagnose accordingly if there are any problems. | DevOps |  |
| * 1. Perform Test Failover | 1. Add exceptions to policies attached to the target Resource Group. Especially the policies that enforces tagging. 2. Go to “Replicated Items” in the RS Vault and select the server from the list. 3. Click “Test Failover”. 4. Select the latest app-consistent recovery point.      1. Test failover will start once you click OK. 2. Verify the test VM worked. 3. Cleanup Test Failover by clicking on the “Cleanup test failover” option in the replicated server info blade. | DevOps |  |
| * 1. Perform Failover (Cut-over) | 1. Add exceptions to policies attached to the target Resource Group. Especially the policies that enforces tagging. 2. Stop services and applications on the source server if required. In addition, give it enough time for ASR to get a good replication restoration point. For e.g. Connections from clients to a DB server should stop in order not to lose transactions in memory and transit. 3. Make sure the target machine sizing is correct. Go to Replicated Items and the VM and select ‘Compute and Network’ and ‘Disks’ to check the target sizing and modify accordingly.   Make sure ‘**Already have an eligible Server License?**’ is set to **Yes** to enable Hybrid Benefits for OS licensing. Refer to the Source/Target Size Mapping document for correct sizing of the target VM.     1. Go to the Replicated Items and select the server you want to failover.      1. In the following blade, select the recovery point. It is not required to shut down the source machine for migration scenarios but if the application demands do check the option.      1. Verify the failover happened properly and the VM has started running. | DevOps |  |
| 1. **Post Replication Tasks - Azure** | | |
| * 1. Verify login | Verify you can RDP and login to the server. If the domain account does not work, try the local administrator account added before replication. | DevOps |  |
| * 1. Join VM to Domain Controller | Check if the VM has joined the Domain Controller. | DevOps |  |
| * 1. ~~Remove local admin user~~ | ~~Remove the local admin user added before replication.~~ | DevOps |  |
| * 1. Remove agent | Uninstall Site Recovery provider/agent from the VM. | DevOps |  |
| * 1. Remove Cisco AMP | Uninstall Cisco AMP | DevOps |  |
| * 1. Remove VMware agents | Uninstall VMware agents from the VM. | DevOps |  |
| * 1. Resize OS Disk | Resize the target VMs OS disk to 128 GB. | DevOps |  |
| * 1. Make IP Address static | Change IP Address setting on NIC of the VM to static. |  |  |
| * 1. Check the temp drive D: is created | Check temp drive D: is created in the target machine. | DevOps |  |
| * 1. Change Page File drive | Change the Page File drive to the temp drive (usually D: drive). | DevOps |  |
| * 1. Add tags to VM resource | Add tags according to Calpine policies to VM resources created in Azure. |  |  |
| * 1. Reboot Server for AD Migration Tool changes | Reboot the server so ADMT could perform Domain migration changes. Wait for the changes to complete before proceeding to next step. | DevOps |  |
| * 1. Add \_svc\_admt account to local admins | Add \_svc\_admt account to local administrators group on the servers migrating via GPO policies. | Tanner Gates |  |
| * 1. Inform Application Teams | Once ADMT changes are complete on the server, inform the application teams to perform testing. | DevOps |  |
| * 1. Perform application related changes | Bring online app services and start testing. Document and perform all changes that are required to make the applications work like connection string updates and configuration updates etc. | Application Teams |  |
| * 1. Complete migration | When the VM is tested working, in Replicated Items, right click the VM and select “Complete Migration”. | DevOps |  |
| * 1. Enable Backup (Post Migration) | Enable backup of VM and Disks and SQL Server. | DevOps |  |
| * 1. Enable Monitoring (Post Migration) | Enable monitoring on the servers. Make sure the monitoring agents are installed on the server within a day or two after the failover to Azure. Make sure the agent is reporting pings to Log Analytics. | DevOps |  |
| * 1. Inform Security to add Patch Management | Inform Security to add Patching Cycle Management. | DevOps |  |
| 1. **Post Replication Tasks – On-Premises** | | |
| * 1. Move app traffic | Move app traffic over to the app running on the migrated Azure VM instance. | Application Team/Tanner |  |
| * 1. Remove VM from inventory | Remove the on-premises VMs from your local VM inventory. | Tanner |  |
| * 1. Remove VM backups | Remove the on-premises VMs from local backups. | Tanner |  |
| * 1. Update documentation | Update any internal documentation to show the new location and IP address of the Azure VMs. | Tanner |  |
| 1. **Back-Out Tasks – On-Premises** | | |
| * 1. Bring online app services | Bring online app services on source servers. | Application Team/Tanner |  |
| * 1. Resume monitoring on source servers | Ensure source servers are being monitored. | Tanner |  |
| * 1. Fail-back acceptance | Calpine Solutions acceptance of fail back to source server, and Calpine Solutions has operational responsibility for the source. | Application team/Tanner |  |