**Note: - This Generalized guidelines for New VM Build and adding security groups, enabling backup and much more as per client requirement.**  
  
**Reference: - Arvinas: New Azure VM for indica-HALO - ARVAZRITP0004: 115885  
  
Name: ARVAZRITP0004**

**Subscription: Arvinas -Prod**

**NV v4 series VM with 16 processor cores**

**Memory: 32 GB RAM**

**GPU: NVidia GPU**

**128GB OS Disk with Windows 11 Pro version 22H2- Standard SSD Azure Encrypted**

**512GB Application Disk - Standard SSD Azure Encrypted**

**TAGS:**

**Business Unit: RIT**

**Business owner: Andrew Sargent**

**Business Function: Indica-HALO**

**IT owner: Debra Nickischer**

**Create Security Groups:  
Create ACL-ARVAZRITP0004-Access**

**Create ACL-ARVAZRITP0004-Admin**

**Domain**

**Add to domain and place in OU**

**Add system to Disable Remote Print Service Group**

**Add system to Disable Point and Print Service Group**

**Add system to Disable Print Spooler (print not required)**

**ACL-ARVAZRITP0004-Admin add to Administrators – Local**

**ACL-ARVAZRITP0004-access add to Remote Desktop Users – Local**

**Set Time Zone: Eastern Standard Time**

**Install Log Analytics**

**Install Crowdstrike**

**Install Sysmon**

**Install Artic Wolf Agent**

**Install CyberArk Agent**

**Add to Azure patching cycle (RIT)**

**Add to Azure Standard backup**

**Install N-Able**

**Install Automox**

**Exempt from Qualys Vulnerability Assessment Tool**

**Enable Azure Defender**

**Enable Azure Insights**

**Create ACLC-Azure-ARVAZRITP0004-POWER (Azure security group).**

**Add permissions for members of this group to power off/restart the VP**

**Add permissions for members of this group to view Azure Insights**

**Owner of this security group: Andrew Sargent, Darin Lori**

**Members: Debra Nickisher**

🡺 While building the VM You need to have these details mandatory like naming convention, VM Size, Vnet & subnet, disk (standard sssd or premium), tags, etc..  
  
🡺 Regarding VM Size check the preferable size which matches to client’s requirement. (Sometimes size is not available or the operation fails due to non-allowed SKU). Then we need to modify policy to allow the respective SKU (**Akula** has access to make these changes).  
  
🡺 Don’t enable public IP address to the resource unless client specifies.  
🡺 Don’t enable the option Automatic patch orchestration (only Manual patching) as already client specifies.  
🡺Don’t enable Auto-shutdown, please make it off.  
  
🡺 Make tags are entered correctly.  
🡺Remaining entries are mostly we keep it as default or otherwise if client specifies we will add to build the VM.

**Add to domain and place in OU**

🡺 for this login to VM == right click on THIS PC == properties == click on domain or work group **A screenshot of a computer

Description automatically generated  
  
  
A screenshot of a computer

Description automatically generated**Then under computer name click on change === Then click on domain & add domain name **A screenshot of a computer

Description automatically generated**Then it will ask username & password whose account has role of domain admin. Then it will ask to restart & reboot it. After few minutes check are you able to login with above used AD credentials.  
 **Create Security Groups:  
Create ACL-ARVAZRITP0004-Access**

**Create ACL-ARVAZRITP0004-Admin**

For this login to Secondary DC == **ARVNHAPPP0040** and go to Active directory Users & Computers == got to the Domain groups == security groups == right click on security groups & enter the details click ok. Now the group has been created.   
  
In this way create both access & admin groups.  
  
  
A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Next add members (client will specify to whom we need to add) to those groups by double clicking on those group. Apply & click ok.  
  
A screenshot of a computer

Description automatically generated

==> Once done cross-verify those groups.  
  
A screenshot of a computer

Description automatically generated

**ACL-ARVAZRITP0004-Admin add to Administrators – Local**

**ACL-ARVAZRITP0004-access add to Remote Desktop Users – Local**

🡺For this Login to the new server then on search bar run & enter **lusrmgr.msc**. Then add the admin group to Administrators.  
  
🡺 on the same page click on Remote desktop users and add access security group.  
  
A screenshot of a computer

Description automatically generated  
  
**Install Crowdstrike**

**Install Sysmon**

**Install Artic Wolf Agent**

**Install CyberArk Agent**

**Install Automox**

For these agents first we will install Automox agent (Access key & installation file contact IC).  
Once Automox is installed we will ask client to push remaining agents from Automox portal.  
  
**Install N-Able**

**Install Automox**

**Exempt from Qualys Vulnerability Assessment Tool**

**Enable Azure Defender**

🡺For this we have an SOP Arvinas on-boarding process. [Arvinas On-Board process jahnavi.docx](https://snp-my.sharepoint.com/:w:/p/jahnavi_k/ESPFcU5cYANMuhwS1A6DPHYBqOt9ht4xvUJE6-AhW5_98A?e=LUXBhX)  
  
For enabling Azure Insights (VM INSIGHTS) go to the resource == on left pane search monitor and insights == enable DCR.   
  
A screenshot of a computer

Description automatically generated  
  
  
  
**Create ACLC-Azure-ARVAZRITP0004-POWER (Azure security group).**

**Add permissions for members of this group to power off/restart the VP**

**Add permissions for members of this group to view Azure Insights**

For this we have already SOP’s please go through it. [Virtual Machine Power Users.docx](https://snp-my.sharepoint.com/:w:/p/sathish_a/Ed0SPmkaMJZMipruvqlVaT8BiJlbj2FS6IoBOj5Lr7Rx5w?e=SdKBPT)

[Role assignments on Security groups.docx](https://snp-my.sharepoint.com/:w:/p/jayaram_b/EQhG2RVFNEZNmE0mCJdAyMYBTiFvTDFrrQfi85y6qcEqlg?e=bpYzmH)

**Add system to Disable Remote Print Service Group**

**Add system to Disable Point and Print Service Group**

**Add system to Disable Print Spooler (print not required)**

For this we are doing it at Individual VM level. Login to VM == go to control pannel == network adapter settings == uncheck files & printer option and save it. Secondly stop & disable print spooler service from windows services.  
  
Alternatively if we want to do at AD level, please follow the below links. (Right now we don’t do at GPO level and we are not using this process now).  
  
<https://support.globalsign.com/Certificate%20Automation%20Manager/how-create-and-link-gpo-active-directory>   
  
<https://www.cswrld.com/2023/12/how-to-disable-print-spooler-on-domain-controllers/#:~:text=Let's%20create%20a%20new%20Group,policy%20setting%20and%20select%20Disabled>.