**Standard Server Build template**

**Generic template**

|  |  |
| --- | --- |
| vCPU | 4 |
| Physical Memory | 16G |
| Disk | **256G** |
| Disk Type [ SSD | HDD] | Std SSD LRS |
| Estimated Cost |  |

**Database template – Select this automatically based on “SQL / Or not)**

|  |  |
| --- | --- |
| vCPU | 4 |
| Physical Memory | 16G |
| Disk | **Default 3 drives (128+128+128)** |
| Disk Type [ SSD | HDD] | Prm SSD |
| Estimated Cost |  |

* **VM naming conventions need to be followed.**
  + **DSV[W|L][OpCO][M|G|]**

**\*\* Exception process to be followed – if anything else is required around this server.**

**OS options**

**Server OS options**

1. Windows Server
   1. Latest and Latest -1
      1. **Windows Server 2022**
      2. **Windows Server 2019**
2. Linux
   1. Latest and Latest -1
      1. **RHEL 9**
         * RHEL 9.2 (5.14.0-284.11.1.el9\_2)
         * RHEL 9.1 (5.14.0-162.6.1.el9\_1)
         * RHEL 9.0 (5.14.0-70.13.1.el9\_0)
      2. **RHEL 8**
         * RHEL 8 (4.18.0-80)
         * RHEL 8.1-8.8
3. OVA option
   1. If any OVA is based on above OS versions – lets proceed to host it.
   2. If any OVA is not based on above OS Versions – Get Security exceptions to host it in AZURE.
      1. Separate tasks should be created for it assign it to Cybersec team.

**Standard SKUs**

* + - * **Turnaround -?**

**Non-Standard SKUs**

* + - * **Turnaround - ?**

**Extra Compute – Exception process**

**Server Type - Production | No-Prod**

* 1. Application Category – Mission C | MS | Engineering | Manu| Services
  2. Application subcategory
  3. Application Name –
  4. Application Owner - <Select from list>

**Domain Joining – Name [ Dover ] [ MI ]**

* + - * Web Servers are non-domain joined which are public facing ?

**Software Requirement**

* + - * Should we consider it now ?
      * Revisit – may be we can handle this separately.

**Network Requirement**

* + - * **~~Need Internet Access ?~~**
      * Host in DMZ [Yes][No] – Rephrase it?
      * Which Region ?
      * Enable port 8089 and 9997 for Splunk
      * 80 and 443 for public facing
        1. Inbound connection
      * Enable specific ports for external Infra applications – Crowdsrike, Solarwinds/Lansweeper ( Check with Venu).
      * RDP shouldn’t be enabled on public facing hosts / DMZ.
      * Splunk should be deployed on all Production Servers.
      * Vnet / Subnet
        1. How to find out these details automatically ?
        2. For Automation.

**Backup Requirement ( Discuss with Patrick)**

* + - * Need backup – [yes] [No] – For noProduction systems ?
        1. Cost associated.
      * If Production – Commvault onboarding
        1. RTO – Populate Automatically
        2. RPO - Populate Automatically
        3. Backup Schedule

**Monitoring**

* + - * Enable host monitoring ? Not Alerting for all
      * If Production – Enable alerting
        1. Based on criticality – Priority should be defined

Mission Critical

Mission Support

Engineering / Manufacturing

* + - * WMI Credentials
        1. Service Account through GPO – once added to Dover Global Domain
        2. Need to see how to do it for

Non – Dover Domain

Or DMZ servers

* + - * SW onboarding

**Patching**

* + - * **Windows**
        1. SCCM agent installation and configuration – Through GPO
      * **Linux ( Always non-domain joined ??)**
        1. **Linux patch repository.**
      * Select Patching schedule \*\*

**Security Requirement**

* + - * Install and configure following Security foundation tools on each VMs
        1. Crowdstrike – Already happening through Policy
        2. Tenable – Only for Onprem Servers
        3. Splunk – Production Servers
      * If Production and in DMZ/Public facing
        1. Put this behind WAF
        2. Send a SCTASK to cyber team to configure it. – Automate it

**User access control –**

* + - * **Do user has “a” account ? [Yes | No ]**
      * **If No**
        1. **Provide link to get the a account created.**
      * **If Yes**
        1. Select the “a-account” which all need access to the server?
      * **Tickets to global AD**
        1. **Create AD security Group if not already exist.**
        2. **Add the “a-Account” added to given security group.**

1-2 days??