**CST8248 – emerging Technology**

**Project quality and Testing**

* **Quality Assurance Strategy**
* **Purpose**

The Team 23 will be responsible for the management, control, and oversight of the Hybrid cloud build Project. This Quality Assurance Strategy will be used to control and monitor the quality aspects of the project activities.

* **Policy**

ThisPolicy is establishes to ensure the service consistency under this project. The following objectives have been established for this plan:

* Maximize the effectiveness of contingency operations by following phases:
* Notification phase - detect and assess any notification that might cause service downtime.
* Recovery phase - restore temporary IT operations and recover service to the original system
* Reconstitution phase - restore IT services to its normal operations.
* Identify the activities, resources, and procedures needed to carry out processing requirements during prolonged interruptions to normal operations.
* Assign responsibilities to designated personnel and provide guidance.
* Ensure coordination withteam members who will participate in the project.
* **Procedure**

The Team 23 will build the environment and carry out regular day to day operation for service uptime and for fixing any kind of service disruption. Any patterns of error in the Hybrid Cloud must be corrected. The Team 23 will provide a copy of the report(s) to the management every week.

Participating Team will provide the following levels of service and timeliness for Hybrid Clod build project

* **Monitoring**

Our team will use SolarWinds server Monitoring Software that will allow us to monitor complete understandings of availability and performance monitoring, alerting, and reporting for multi-vendor servers.

* **Backup and data recovery**

We will back up the environment every day. Remote backup is out of scope of this project. We will perform on site backup. First backup should be full system backup and then we will perform incremental back up every day. We will use Veeam, as a backup software. It is one solution for simple, reliable and flexible protection of ALL of our cloud, virtual and physical workloads.

* **Security**

To prevent computer viruses from spreading to servers and to prevent unauthorized users from accessing your computer will firewall be implemented. We will use disk cleanup utility that scans server’s hard drive for files that no longer needed such as temporary files, cached webpages, and rejected items that end up in system’s Recycle Bin.

* **Point of contact for any service disruption**

Nicholas Forgues : [forg0120@algonquinlive.com](mailto:forg0120@algonquinlive.com)

Israt karim : [kari0088@algonquinlive.com](mailto:kari0088@algonquinlive.com)

* **Physical Plan for server room**

It is very important to choose a datacenter room before racked all server inside it.

So following aspect we took into consideration to choose the server room inside the college building.

* **HVAC**
* **Computer room air Condition**
* Room properly airconditioned for maintain stable temperature, humidity control, and air filter.
* Back up for air cooling system.
* There is no heat generating equipment inside the room.
* **Humidity and Temperature**
* Server room has fire, smoke, water, temperature and humidity monitors.
* Away from building water supply pipe or sewerage pipe.
* **Ventilation.**
* Space’s ceilings .
* constant circulation of air and suitable airflow planning for proper cooling.
* **Electric system**
* For short time power disruption UPS and for longer time power outage on side generator should be consider as a back-up power supply.
* Server’s two redundant power supply should be come from two different power supply source.
* Electrical systems ground properly.
* **Access Control and safety**
* Heavy duty doors with electronic locks.
* CCTV monitoring of the server room and adjacent areas.
* Biometric or security card access controls.
* Limited access for visitors and non-essential stuff.
* **Hardware Requirements**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| VMs | Platform | Core | Disk space (GB) | Memory (GB) | Network 1 | Net 2 | **Net 3** |
| AC /DNS | Win-server-2016 | 2 | 60 | 6 | Blue | Red |  |
| AC / DNS | Win-server-2016 | 2 | 60 | 6 | Blue | Red |  |
| http server | Centos 7 | 1 | 60 | 2 | Blue | Red |  |
| iSCSI | Win-server-2016 | 1 |  | 4 |  | Red |  |
| FS SMB | Win-server-2016 | 1 | 60 | 4 | Blue | Red |  |
| Veeam | Win-server-2016 | 2 | 60 | 4 | Blue | Red |  |
| Spiceworks | Win-server-2016 | 2 | 60 | 4 | Blue | Red |  |
| WAC | Win-server-2016 | 2 | 60 | 4 | Blue | Red |  |
| vSphere | vSphere 6.0 | 2 |  | 4 | Blue | Red |  |
| Client server | Centos 7 | 1 | 40 | 2 | Blue |  |  |
| Client server | Win-server-2016 | 2 | 40 | 4 | Blue |  |  |
| Azure |  |  |  |  |  |  |  |
| Value Added | | | | | | | |
| Configure azure security Center Notification through Work Flow automation and Logic App. | | | | | | | |

* **Network Plan:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Service** | **Blue IP** | **Red IP** | **Green IP** |
| DC1- AD/DNS | 172.20.65.1 | 172.30.65.1 |  |
| DC2- AD/DNS | 172.20.65.2 | 172.30.65.2 |  |
| vSphere | N/A | 172.30.65.10 | ?.10 |
| iSCSI | N/A | 172.30.65.15 | ?.15 |
| WAC | 172.20.65.20 | 172.30.65.20 |  |
| Spiceworks IMS | 172.20.65.25 | 172.30.65.25 | ?.25 |
| Veeam | 172.20.65.30 | 172.30.65.30 |  |
| File Server | 172.20.65.35 | 172.30.65.35 | ?.35 |
| HTTP | 172.20.65.40 | 172.30.65.40 |  |
| Web Server | Public IP | Front-end subnet |  |
| PostgreSQL | Back-end | Back-end subnet |  |
| Linux Client | 172.20.65.101 | N/A | N/A |
| Windows Client | 172.20.65.102 | N/A | N/A |

* **Network Topology**



* **Test Plan:**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Source | Destination | connectivity (icmp) | Service | Test command | **Result** | Comment | Test Date |
| Win Client | Win File Server |  | SMB | Net Use |  | Check Firewall, service status, permissions, server/share name, DNS |  |
| AD | client |  | AD | dsquery, dsmod |  |  |  |
| iSCSI Initiator | iSCSI Target |  | iSCSI | mkdir |  |  |  |
| all hosts | all hosts <team23.domain> |  | DNS | nslookup |  |  |  |
| Virtual disk | Backup server |  | Enterprise Backup | C:\<veeam.exe> /backup <ID#> |  | Ensure Backups |  |
| IMS | any host |  | IMS | Tools > IP Scanner |  | Ensure device inventory is present |  |
| WAC | windows client |  | WAC | Enable-PSRemoting |  | Management of Windows 10 client |  |
| WAC | outside of WAC subnet |  | WAC | Set-NetFireWallRule < |  | Secure admin access |  |
| WAC | any host |  | WAC | Tools > <Tool> |  | Manage server connections through GUI |  |
| Azure | Azure |  | Azure | az monitor log-analytics workspace table show |  |  |  |
| Web Server | PostgreSQL Server |  | PostgreSQL | ssh |  | Verify access for admin to backend |  |
| Web Server | PostgreSQL |  | PostgreSQL | gmake check |  | Regression testing |  |
| Web Server | PostgreSQL |  | PostgreSQL | ./psql -h <hostname> <Database name> |  | Check access to database |  |
|  |  |  |  | [az HYPERLINK "https://docs.microsoft.com/en-us/cli/azure/postgres/server/private-endpoint-connection?view=azure-cli-latest" HYPERLINK "https://docs.microsoft.com/en-us/cli/azure/postgres/server/private-endpoint-connection?view=azure-cli-latest"postgres HYPERLINK "https://docs.microsoft.com/en-us/cli/azure/postgres/server/private-endpoint-connection?view=azure-cli-latest" server private-endpoint-connection show](https://docs.microsoft.com/en-us/cli/azure/postgres/server/private-endpoint-connection?view=azure-cli-latest) |  |  |  |
| Client VM | Web server |  | Webserver | [http://domain.name](http://domain.name/) |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |