**PUSL2010**

**PART B - Implementation Brief**

**LAHIRU**

Patches are released by VMware regularly to handle the application’s core functionality or for the seamless connectivity of third-party products in this platform like Cisco Distributed Virtual Switch. These patches are stored in patch repository and new releases are rolled out from this repository where VMware will update these patches frequently. This is done to ensure the stability of the core application and supporting applications.

Among the patch repository and the host machine, there is a link known as the URL based patching. This will allow the host to be notified through the Update Manager regarding a new patch availability when VMware releases a new patch. By default, the vCenter Serve application will use the VMware repository URL that is assigned, and this will be used to interact if the necessary settings are not modified. A custom URL can also be configured to be used this. Using either type, default URL or the customer URL is sufficient enough for the specified operation. But within the perspective of cybersecurity, the custom URL is more secure as it would be difficult for any unauthorized parties trying to access the link in between. During the configuration of a custom addition configuration is required but this will be highly beneficial for clients that store and transfer sensitive data across the network.

As to the link from the firewall to the banks' network, a custom patch URL is also an added advantage for the circumstances of the bank-based customer updates. This is because this link can be visible to the outside world, meaning that third-party or unauthorized parties could try to access the data packets flowing through the link. But if a custom URL is configured it would be difficult for the unauthorized parties to gain access into the network link.

The custom URL will ensure the security of the link than the traditional default URL which is assigned automatically.

Within regular time gaps, Update Manager will interact with the VMware and retrieve the latest up to date notifications which can be related to patch recalls (patch with a bug is requesting to revert from the host), new fixes, and alerts.

As Update Manager retrieves the notifications from VMware there are some notifications that trigger an alarm that executes a certain action. There are three types of notifications, *(Types of Update Manager Notifications, 2020)*

* Information Notifications – By clicking this notification the notifications details windows will open. And these notifications do not trigger an alarm.
* Alert Notifications – These notify the patch recalls for a patch that contains a bug. By clicking this notification, the Patch Recall Details window will open. It also triggers an alarm, as it also appears in the vSphere Web Client Alarms panel.
* Warning Notifications – These notify the fix for the patch recalls repairing the broken patches. By clicking this notification, the Patch Recall Details window will open. This also triggers an alarm, it appears in the vSphere Web Client Alarms panel.

When a bug is found in a patch, VMware will mark the patch by updating the patch metadata. This will result in the Update Manager to specify this patch as recalled. The Update Manager will discard all the recalled patches from the patch repository to ensure that no host will retrieve the unstable patch. If a user tries to install a patch that contains a bug and if it is marked as recalled, the Update Manager will notify the host and will prevent from downloading and installing to the host machine. But if the host is already running the patch within the application the Update Manager will check the currently running patch metadata and will notify the host. This will result in the user to downgrade the application to a previous patch version or pause the patch from running until a fix is released by VMware. *(Configuring and Viewing Notifications, 2020)*

Once VMware releases a fix for the patch bug, Update Manager downloads and verifies the user to install the fix the patch to resolve the issue that causes the dug. But if the user had somehow managed to install a patch that contains a bug and if this patch is marked as recalled, the user is notified that the patch version is recalled and the installation of the fix is available.

If the host machines are running offline, the Update Manager will retrieve the updated metadata (metadata.zip) file and notify the status of the patch when a new importation of data files has occurred. Once the fix for the broken patch is released and the fix is imported, the Update Manager discards the recalled patch from the patch repository and the user will be notified about installing the fix to the broken patch.

**RANUL**

This brief will cover all assumptions we took for the implementation along with screenshots as evidence, We considered setting up a proper start up routine for each virtual machine using vApp feature available on VMware vSphere Client, so the programs within each machine won’t be affected due to delayed or broken machines. Each machine was given considerable delay time so it will be completely turned on when the machines in second group starts to turn on, we also set the machines to shutdown safely with a guest shutdown rather than an direct power off from the system.

DRS was enabled so when host are required to be sent to maintenance for upgrades virtual machines will be migrated to another host will allows them to come online or stay online if required without effecting the maintenance process.

External resources such as VMware docs and other literature material was referred to understand best implementation methods such as the NTP server is required to start after the DNS server has started and Database server to start before DHCP as it stores information in the database.

Other considerations such as using a Thin Provisioning for disks allows save storage rather than allocating them before this also allows to expand the storage for a Thick Provisioning if required.

Due to the fact the system runs on Windows machines turning on secure boot from host will protect the VM further as it’s an supported feature, upgrading the ESXi to latest version allowed to enable vMotion which protect highly sensitive data that’s gets transferred during the process. Initially we enabled security level to normal from disabled so the VMs could accessed be from console in an event the vCenter fails, this is better that strict mode but this blocks SSH requests completely, later on we enabled SSH request from only an trusted IP range and set of users such as managers and admins to access using SSH using a client like PuTTY, we think security is major factor to consider so we also configured the host based firewall aside of the provided firewalls and enabled and storage based encryption policy so even in an event the virtual disk file gets stolen it cannot be read due to the encryption.

Other factors we setup was templates of the virtual machines within the workgroup, this allowed us to created multiple copies of the same virtual machine settings and image although not an exact clone of it which was also possible in our tests, after setting up a sample domain we was able to setup roles for users much easily and allow secure access to the system as single sign on feature can be used with active directory enabled.

Finally we prepared the infrastructure using the best possible methods we learned during the coursework and by referring external literature material, we believe the implemented infrastructure is secure, robust and liable, reason for security is we upgraded all VM were possible to latest hosts and setup paths for regular patches and patch protection by notification recalls, polices for encryption and roles and access rights, robust we meant allows the system to function without problems of its own by vApp we setup sturdier mechanics for VM operations and inbuilt configuration for reliable storage allocation and enabled DRS for almost 100% even when high priority maintenances are required. Considering all facts this infrastructure becomes liable to support and sustain the business at its best.

**NIDULA**

**ISHAN**

**Bibliography –**

Docs.vmware.com. 2020. *Configuring And Viewing Notifications*. [online] Available at: <https://docs.vmware.com/en/VMware-vSphere/6.7/com.vmware.vsphere.update\_manager.doc/GUID-0454B3CD-F3EE-424D-AA5F-BEC433D38CFF.html> [Accessed 2 May 2020].

Docs.vmware.com. 2020. *Types Of Update Manager Notifications*. [online] Available at: <https://docs.vmware.com/en/VMware-vSphere/6.7/com.vmware.vsphere.update\_manager.doc/GUID-AD4FA8A3-5FED-4F83-8262-EFF567DBC08C.html> [Accessed 2 May 2020].

**References -**