**PUSL2010**

**PART B - Implementation Brief**

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.

**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].