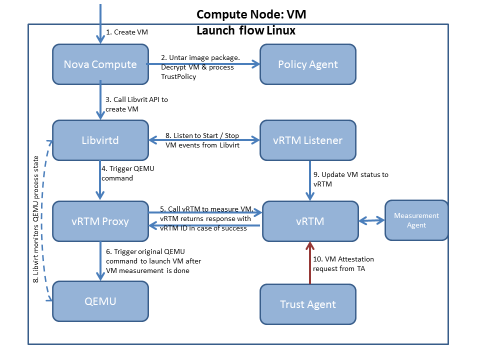
CIT Windows VM Attestation

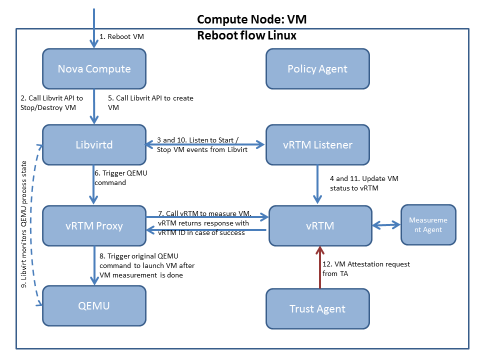
This document entails design specification, and modification from current VM attestation flow on Linux environment, for VM attestation support on windows platform.

# Design

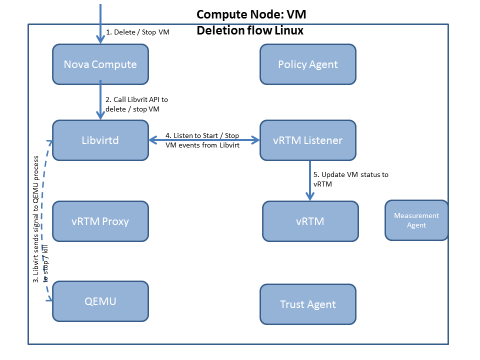
* VM launch Flow on Linux



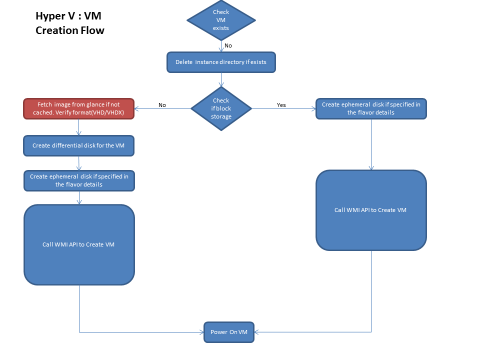
* VM Reboot flow Linux



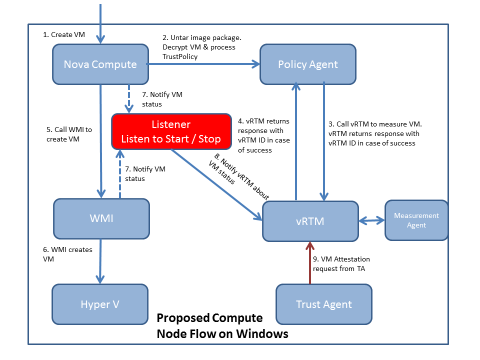
* VM Deletion flow linux



* Hyper-V VM launch flow



* VM launch on windows assisted with CIT



**Control Flow of VM launch on Windows platform:**

1. On VM launch from Horizon request comes to nova-compute.
2. Nova-compute invokes Policy Agent, it untar the image package, decrypt the VM disk and process trust policy. If launch is encrypted launch, it will copy the disk of VM on encrypted partition and make link to it at Openstack default location. Further it will create a directory for this instance under trustreports directory and copies the trustpolicy.xml and manifest.xml in it.
3. It will make api call to vrtmcore with disk path and trustpolicy location for measurement of vm.
4. vRTM will measure the VM and return the response greater than 0 in case of success to PA. Based on policy PA will decide whether it proceeds the request further or drop it.
5. If PA allows the launch control comes back to nova-compute and normal VM launch procedure will continue.
6. In step 9, nova-compute triggers the request of VM report generation by asking report from MtW. Request will be propagated to vrtmcore via MtW and TA, vrtmcore generates report and give path of generated report to TA back in response. Thus, report will propagated back to nova-compute via same path. Result will reflected on horizon whether VM is trusted or not.

# Modifications in windows attestation wrt present CIT components:

1. **vRTM and Measurement Agent ( verifier):** Both has been ported for windows platform. Significant changes are mentioned below-

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Library or Utility | Previous version Usage | Current version Usage | Source Code usage for build/ dll usage | Current Version License |
| Pthread | Pthread | POSIX thread for windows | Not used, dll used at runtime | LGPL |
| Libxml | Same | Same | Used to generate dll, dll is also used at runtime | MIT |
| Log4cpp | Same | Same | Used to generate dll, dll is used at run time | LGPL |
| Openssl | Open-ssl | CNG APIs | Bcrypt.dll and Bcrypt.lib | Comes with msvc |
| Ext2 File system dirver | Not used | Ext2Fsd | Not used, Just executable is used | GPL v2 |
| Linux-Utility Binaries | Grep, rm, cp, find etc. | Replaced these utilites with windows utilites | Not used | Comes with Windows platform |
| Socket | POSIX socket | Winsock 2 | Ws2\_32.lib and Ws2\_32.dll | Comes with msvc |
| Make | make | msbuild | Not used | Comes with Visual studio |

1. **PA:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Library or Utility | Previous version Usage | Current version Usage | Source Code usage | Current Version License |
| Utility to encrypt the disk | dmcrypt | Bitlocker | Not used | Comes with Windows platform |
| Make | Not used | msbuild | Not used | Comes with Visual studio |

1. **TCB Protection:** Earlier TCB protection on Linux uses initramfs (initrd) for measurement of host before it get booted. But initramfs is not available on windows, so in initramfs stead boot driver is used which have same logic of MA (verifier) for measurement of host. For more info please refer the [**Host\_TCB-Protection\_Procedure\_windows.docx]**
2. **Listener replacement:** On Linux vm launch assisted by libvirt(KVM) inform registered listeners about state of change of VMs. But Windows uses Hyper-V for vm launch and it does not expose any API for registering such listener in order get VM state change notification. So, instead of listener a poller is used, which checks periodically if state of VM registered with vrtmcore is changed on Hyper-V. For more info please refer [**VMLifecyclemanagementinvRTM.docx**]