**Table of Contents**

[Install CIT compute node](#h.a7sfzjfguyao)

[Prerequisites on Host for creating Baremetal Trustpolicy from TD](#h.rc9n7dh3l44i)

**Introduction**

This document describes the procedure to setup a CIT Compute Node for Windows Server 2012 R2 with Hyper-V environment

Prerequisites:

* Cloud Controller Kilo with Neutron
* CIT Server
* Trust Director

The required installer is located at:

**\\fmcsssan101\CSSShare\Projects\To\_GSLABs\** **CIT\_3.2**

# Install CIT compute node

CIT compute node is a complete installer that installs CIT components in following sequence:

* TrustAgent
* PolicyAgent
* Tbootxm
* vRTM
* Openstack-extension

**Prerequisites for installing CIT compute node**

1. Enable Hyper-V feature
2. Install Openstack Nova-Compute Kilo
3. Install bitlocker with all its features (System will be rebooted once bitlocker is installed)

# Open powershell commandline

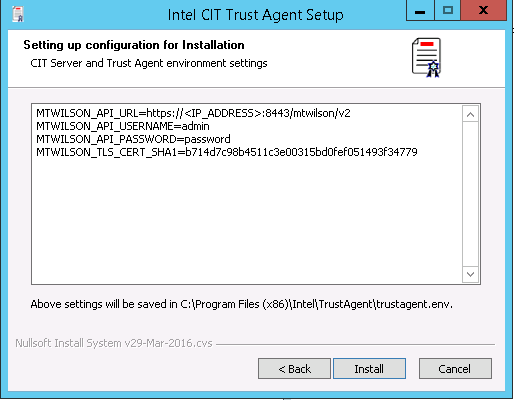
# Execute command

Install-WindowsFeature BitLocker -IncludeAllSubFeature -IncludeManagementTools -Restart

1. Install cygwin at “C:\cygwin64” location. Make sure you select “patchutils” during cygwin installation

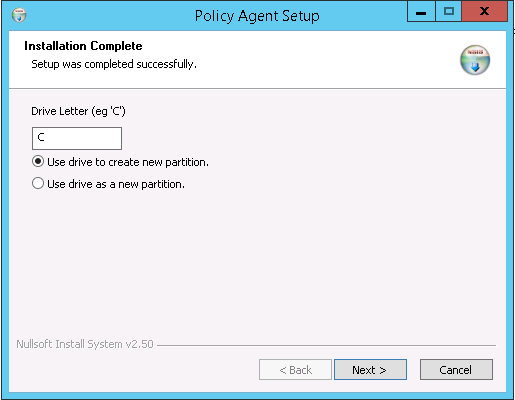
**Installing CIT compute node**

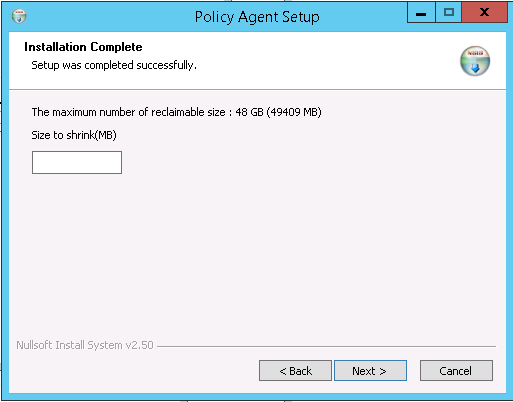
1. Execute CIT compute node installer (cit-compute-node-setup.exe) by double clicking on it.
2. TrustAgent installation will start
   1. During TA installation, provide CIT Server details when installer asks for the same as shown in following snapshot:

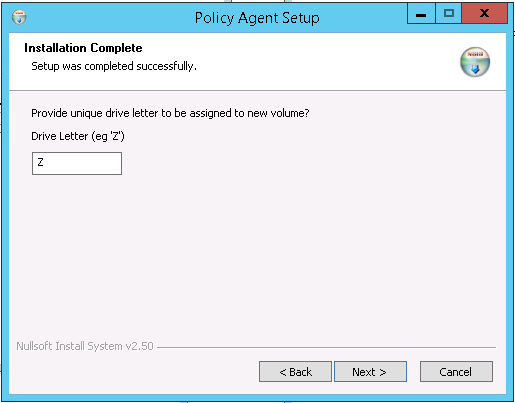


1. PolicyAgent installation will start
   1. During PA installation select any one of the 2 options as shown in following snapshot:
      1. Use drive to create new partition:

This option will use the existing partition to create a new partition out of it and use it for encryption

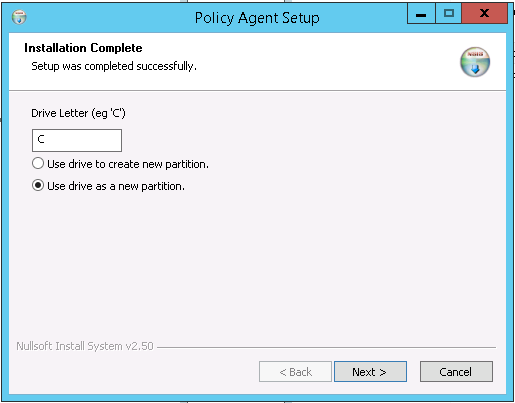






* + 1. Use drive as a new partition

This option will use the already created partition for encryption



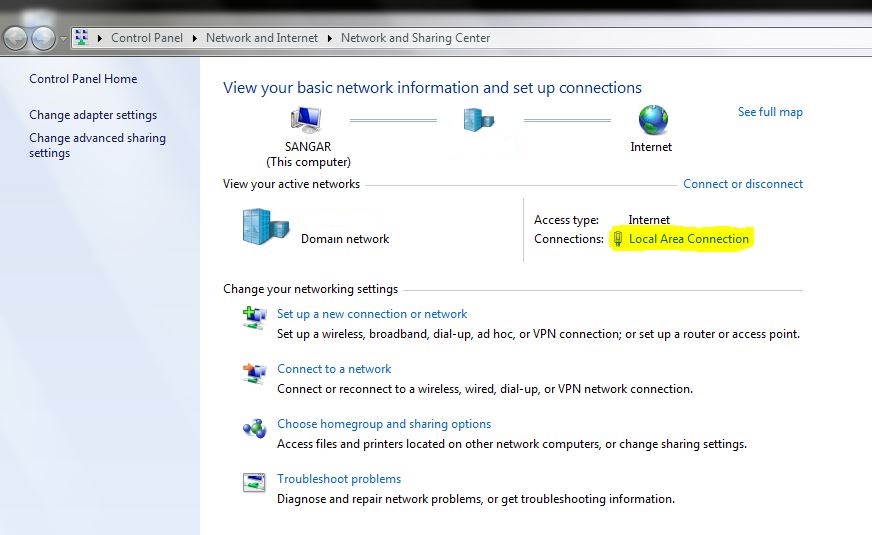
1. Tbootxm installation will start
   1. During installation “tbootxm” driver will be installed and prompt will be displayed for system restart. Select “Restart later” option.
2. vRTM installation will start
3. Openstack-extension installation will start
4. Ensure the following after installation
   1. “Intel CIT Trustagent” service is running
   2. “Intel CIT UnlockDrive” service is running
   3. Unlock icon is displayed on encryption drive that was selected during installation
   4. Create manifest.xml using Trust Director
   5. “tbootxm” driver is installed
   6. “Intel CIT vRTM” service is in running state
5. Create trustpolicy for non-virtualized server using Trust Director
6. After successfull installation of all the CIT components reboot the host system
7. Ensure the following after reboot
   1. Intel CIT TrustAgent service is in running state
   2. Intel CIT vRTM service is in running state
   3. Intel CIT UnlockDrive service is in running state
   4. tbootxm driver is loaded and is in running state
8. Whitelist the host on CIT Server
9. System is now ready to launch instances via Openstack Horizon

# 

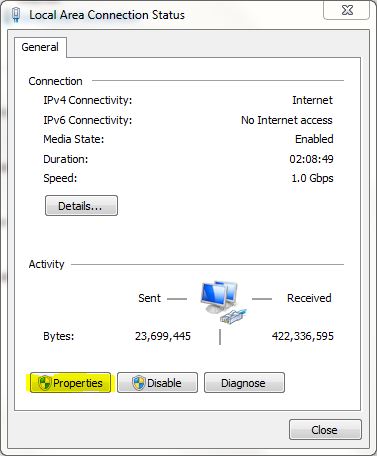
# Prerequisites on Host for creating Baremetal Trustpolicy from TD

**Prerequisites on compute-node/host for creating baremetal trustpolicy**

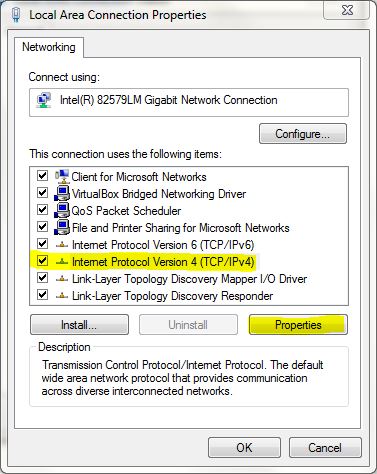
1. Enable **Netbios** setting for network adapter
   1. Open **Network and Sharing Center**
   2. Click on the Network adapter *(“Local Area Connection Status” window will be displayed)* as highlighted in following snapshot



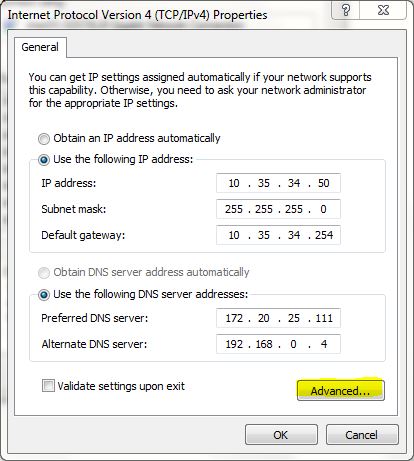
* 1. Click on the **Properties** button on **Local Area Connection Status** window as highlighted in following snapshot



* 1. Select **Internet Protocol Version 4 (TCP/IPv4)** and click on the **Properties** button as highlighted in following snapshot



* 1. Click on **Advanced...** button as highlighted in following snapshot



* 1. Go to **WINS** tab and select **Enable NetBIOS Over TCP/IP** as highlighted in following snapshot

