Reference Architecture:

PrivateCore vCage and Puppet Enterprise

Overview

Compromising or misconfiguring one node of a server cluster can jeopardize the security of the entire infrastructure. The combination of Puppet Enterprise and PrivateCore vCage Manager enables enterprises to enforce consistency from applications down to the server infrastructure layer. Puppet Labs Puppet Enterprise with Razor enforce consistency in systems and applications while PrivateCore vCage extends consistency checking to the hardware infrastructure. vCage Manager validates trustworthiness and avoids misconfiguration to protects OpenStack servers and applications from persistent threats.

This reference architecture integrates Puppet Razor and PrivateCore vCage Manager so that enterprises can enroll Trusted Platform Modules on server hardware and attest the integrity of the server before allowing applications to run on such infrastructure.

Architecture System Requirements

- Puppet Enterprise with Razor
- PrivateCore vCage Manager
- x86 servers supporting Intel® Trusted Execution Technology (Intel® TXT) and provisioned with Trusted Platform Modules (TPMs).

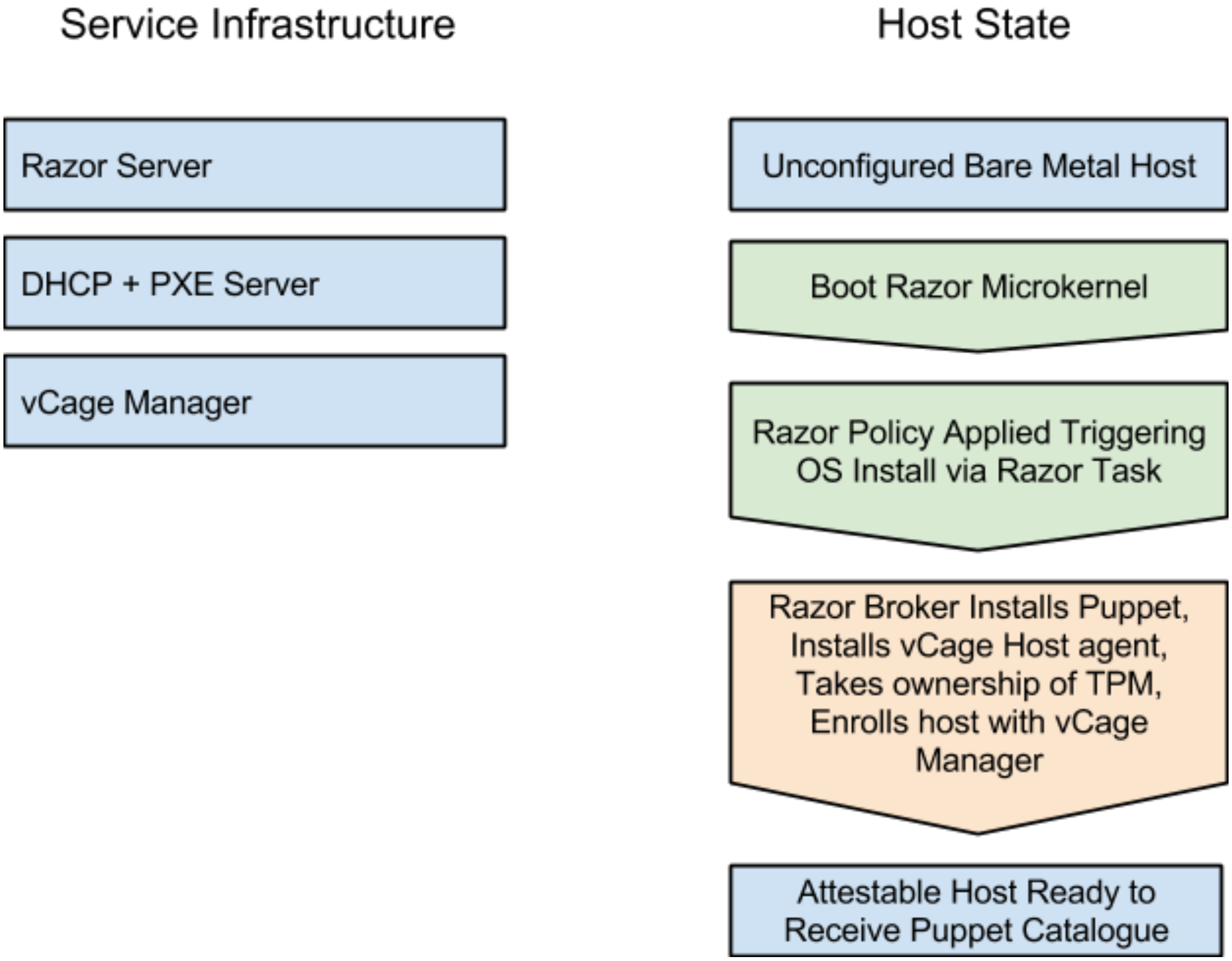
Puppet/Razor Integration Architecture

Razor installs Ubuntu, configures vCage Host Agent, takes ownership of a TPM, and enrolls the host with vCage Manager.

Requirements

Take advantage of Razor to ease enrollment of new/repurposed bare-metal with PrivateCore vCage Manager.

Architecture


Service Infrastructure
Host State
Razor Server
DHCP + PXE Server
vCage Manager
Unconfigured Bare Metal Host
Boot Razor Microkernel
Razor Policy Applied Triggering OS Install via Razor Task
Razor Broker Installs Puppet, Installs vCage Host agent, Takes ownership of TPM, Enrolls host with vCage Manager
Attestable Host Ready to Receive Puppet Catalogue

The Razor server uses a custom broker to install the PrivateCore vCage agent and client tools and their dependencies. Once the vCage tools are installed, the broker will send an API call to the vCage Manager, enrolling the system and readying it for attestation.

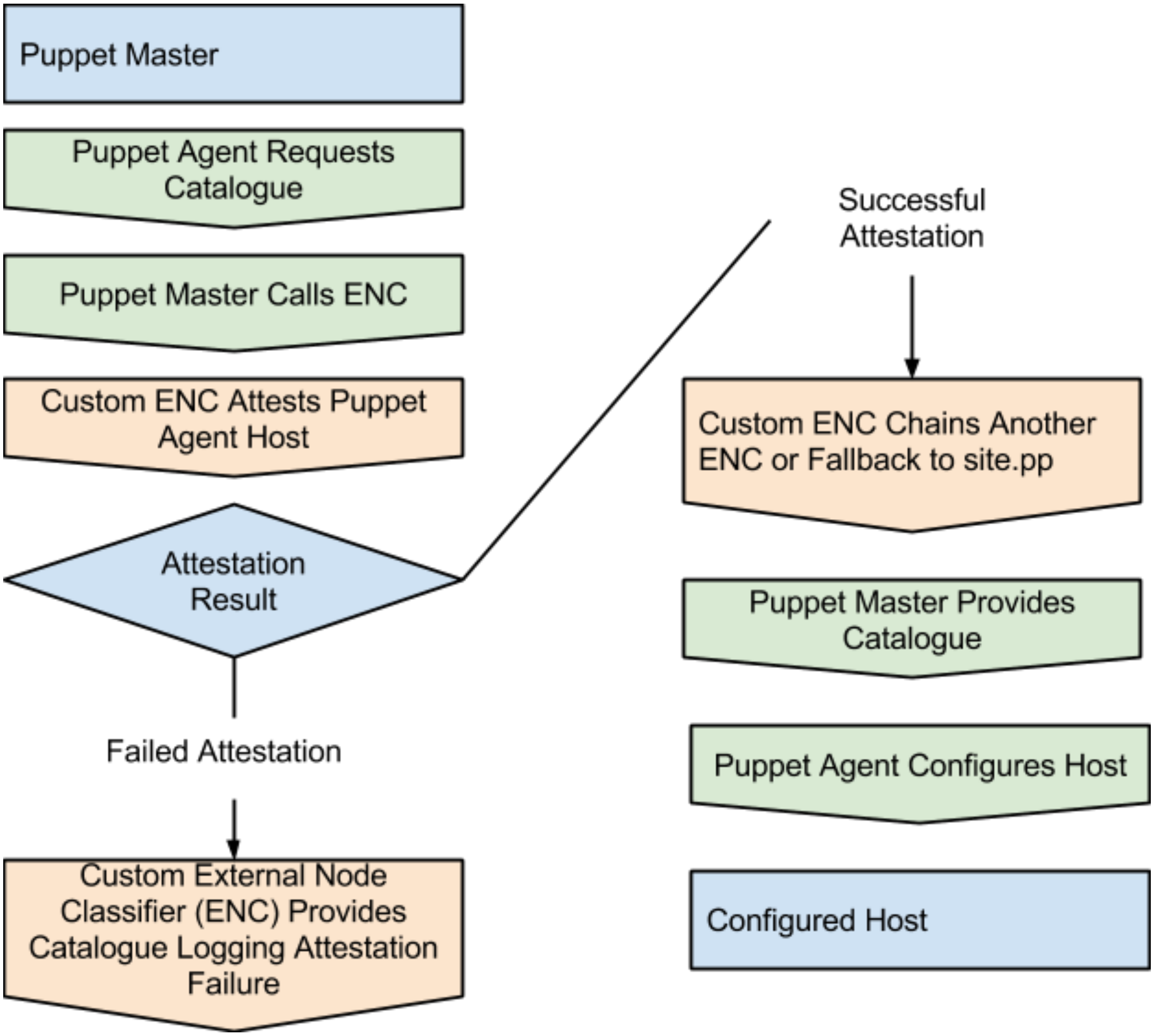
The primary point of integration is a customized Razor broker, otherwise standard Razor tasks and policies are used.

Puppet Agent Host Attestation Using Custom External Node Classifier (ENC)

Requirements

Perform attestation on hosts before providing a Puppet catalogue to Puppet Agents.

Architecture


Puppet Master
Puppet Agent Requests Catalogue
Puppet Master Calls ENC
Custom ENC Attests Puppet Agent Host
Attestation Result
Failed Attestation
Custom External Node Classifier (ENC) Provides Catalogue Logging Attestation Failure
Successful Attestation
Custom ENC Chains Another ENC or Fallback to site.pp
Puppet Master Provides Catalogue
Puppet Agent Configures Host
Configured Host

About PrivateCore

PrivateCore is the private computing company. PrivateCore vCage software validates the integrity of OpenStack servers and secures against persistent malware, malicious hardware devices, and insider threats. PrivateCore was founded in 2011 by security industry veterans from the IDF, VMware and Google. The company is based in Palo Alto, California and has received venture funding from Foundation Capital. For more information, please visit www.privatecore.com.