Trusted Geolocation in the Cloud

Based on NIST Interagency Report 7904 - Trusted Geolocation in the Cloud: Proof of Concept Implementation

Agenda

- Definition of cloud computing
- Trusted Geolocation in the Cloud use case model
- NIST IR7904: Trusted Geolocation in the Cloud: Proof of Concept Implementation
- Evolution of use case to include data protection
- References

A Working Definition of Cloud Computing

- Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.
- This cloud model promotes availability and is composed of five essential **characteristics,** three **service models**, and four **deployment models**.

Trusted Geolocation in the Cloud

Business Opportunities

- Cloud benefits
  - Agility
  - Flexibility
  - Dynamic Resources
- Cloud Challenges
  - Multi-tenancy and shared hosted infrastructure
  - Lack of physical boundaries
  - Lack of visibility of workloads
  - Integrity of the hosted virtual compute environment
  - Hardware based enforcement mechanism
  - Data protection of the workloads

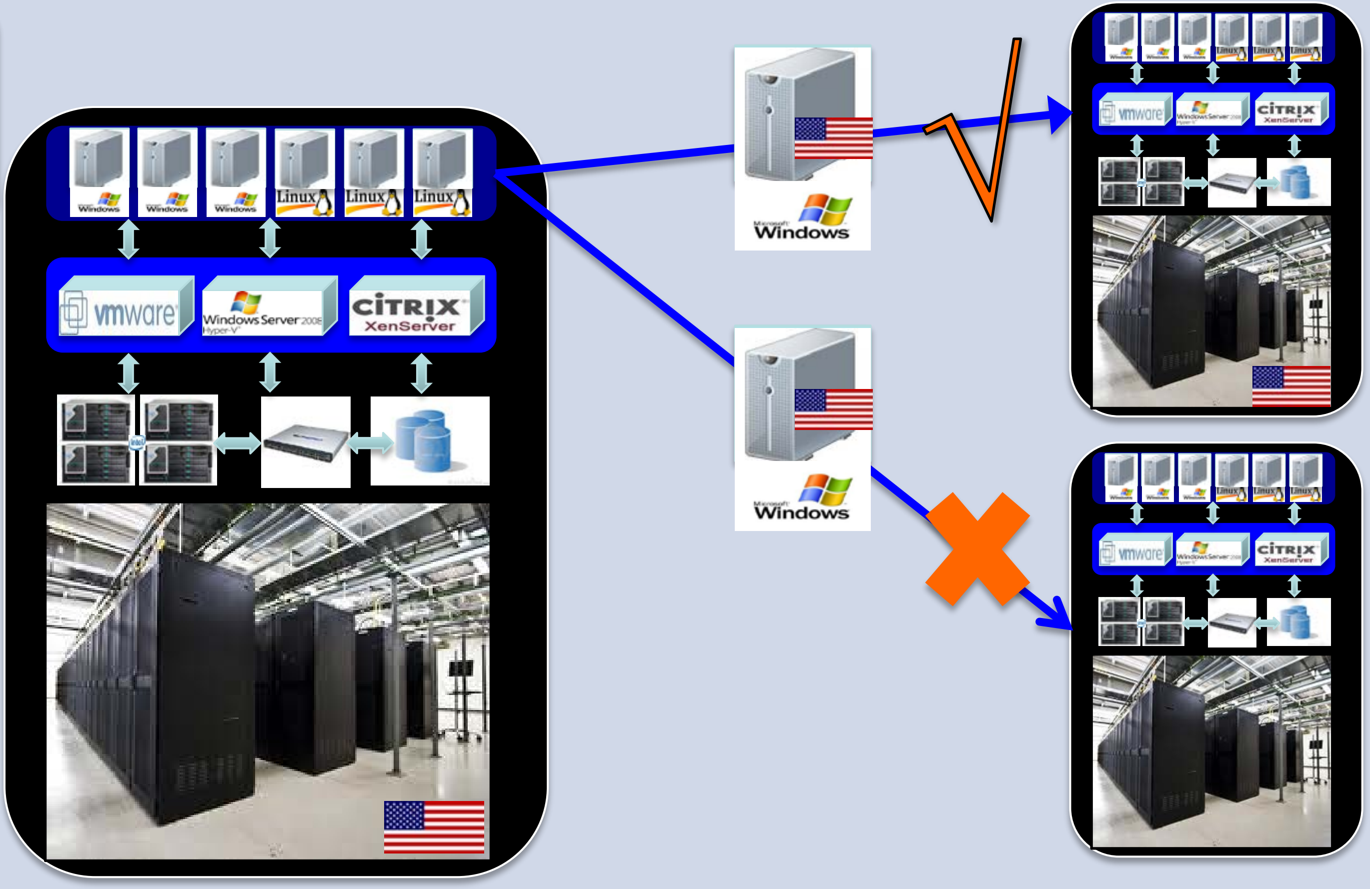
Trusted Geolocation in the Cloud

Security Requirements

- **Trusted resource pool** based on hardware-based secure technical measurement capability
    - **Platform attestation and safer hypervisor launch** - Provide integrity measurement and enforcement for the compute nodes
    - **Trust-based secure migration** - Provide geolocation measurement and enforcement for the compute nodes
    - **Trust-based data protection of workloads** – Provide trust measurements and policy for release of workload encryption/decryption keys
- Workloads instantiation in a trusted resource pool
- Dynamic workloads migration and enforcement between trusted resource pools
- Visibility and transparency in periodic measurement, reporting, and auditing of the workloads to support governance, risk, and compliance requirements
- Industry recommended practices for deploying a secure virtualized infrastructure

Trusted Migration

Use Case



Trusted Migration

Trusted Migration:

1 Servers use hardware measurement engine to perform measured launch and store values in cryptoprocessor.

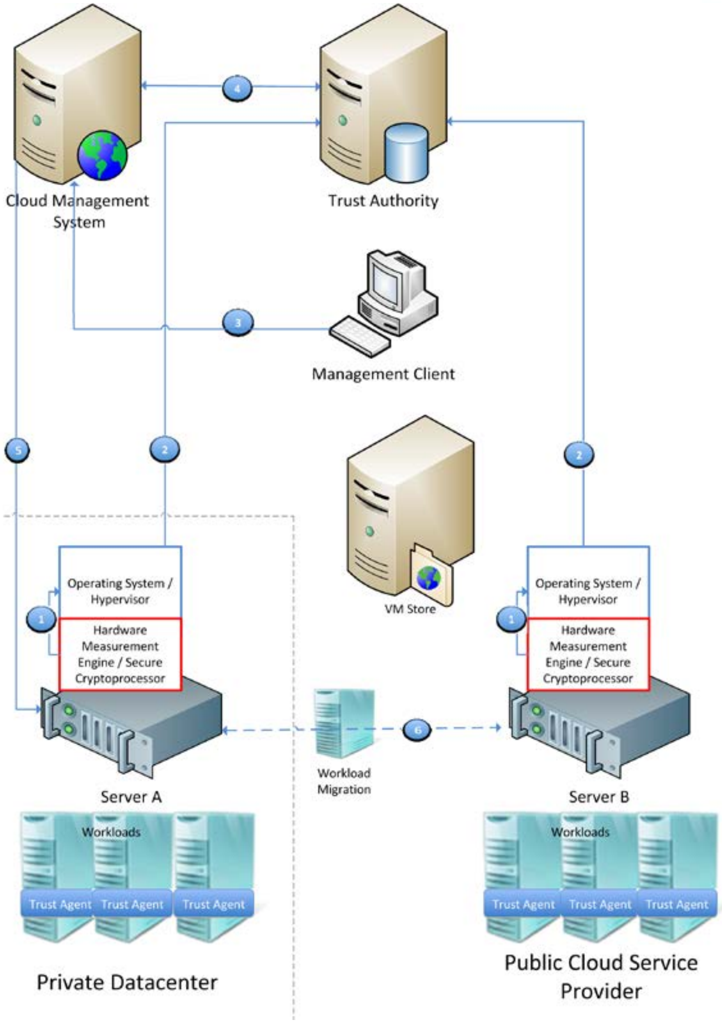
2 Servers send measured launch quotes to the Trust Authority.

3 Migration command sent from Management Clientto Cloud Management System.

4 Cloud Management System checks Trust Authority for trust status of destination server.

5 If migration is allowed by policy, Cloud Management System sends migrate command to Server A.

6 Server A migrates workload to Server B.

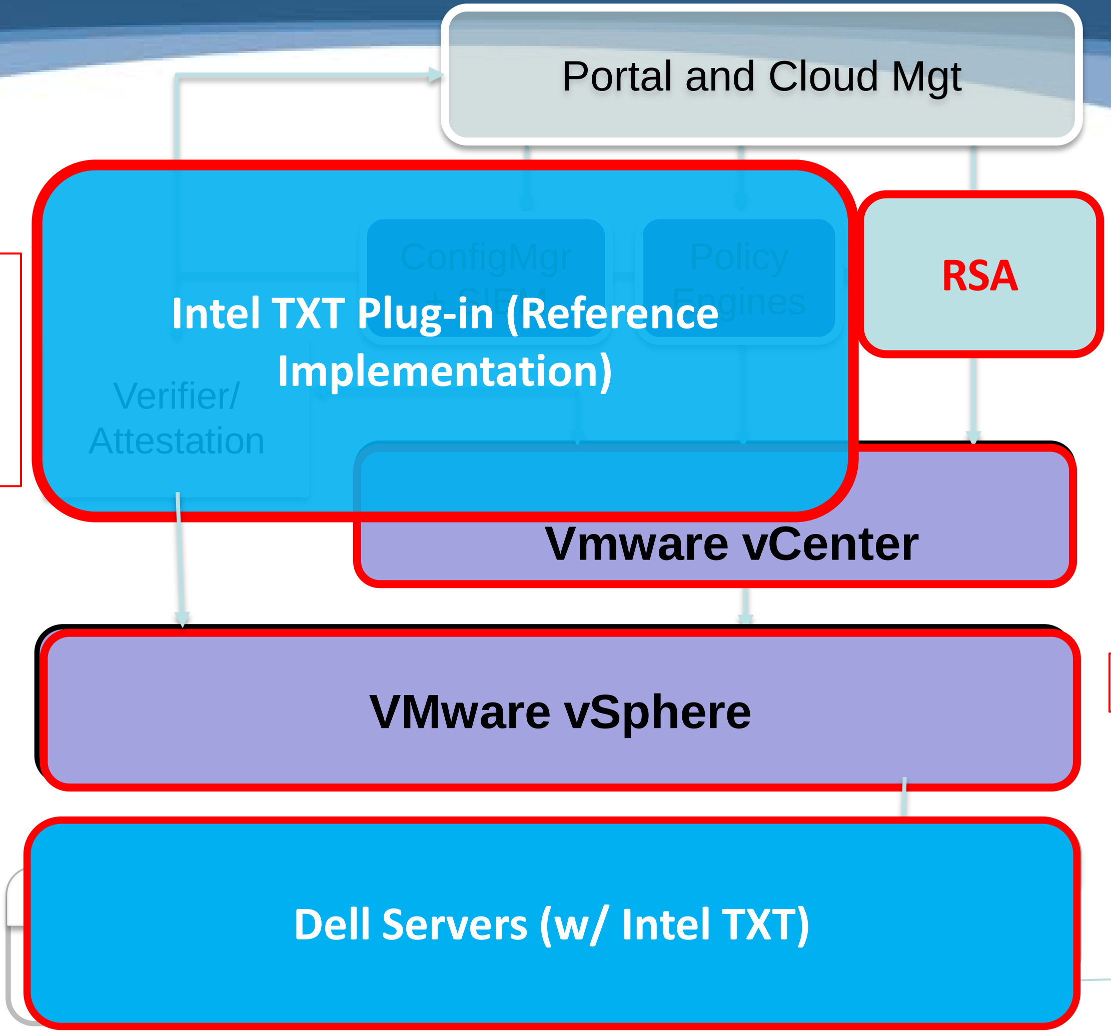


Build

Trusted Cloud Solution
Solution Architecture

Trusted Cloud Solution
NIST Reference Design

- *Basic Policy Mgt*
- *Workload Placement & Migration Control*
- *Basic Trust Attestation*
- *Basic Geo-Location Attestation*



- *Archer*

- *VCenter 4.1*
- *Intel TXT APIs*

- *ESX4.1 U2*

- *Platform Integrity Measurements (Intel TXT)*
- *Geo-Tag*

Trusted Data Protection of Workloads

Workload Data Protection:

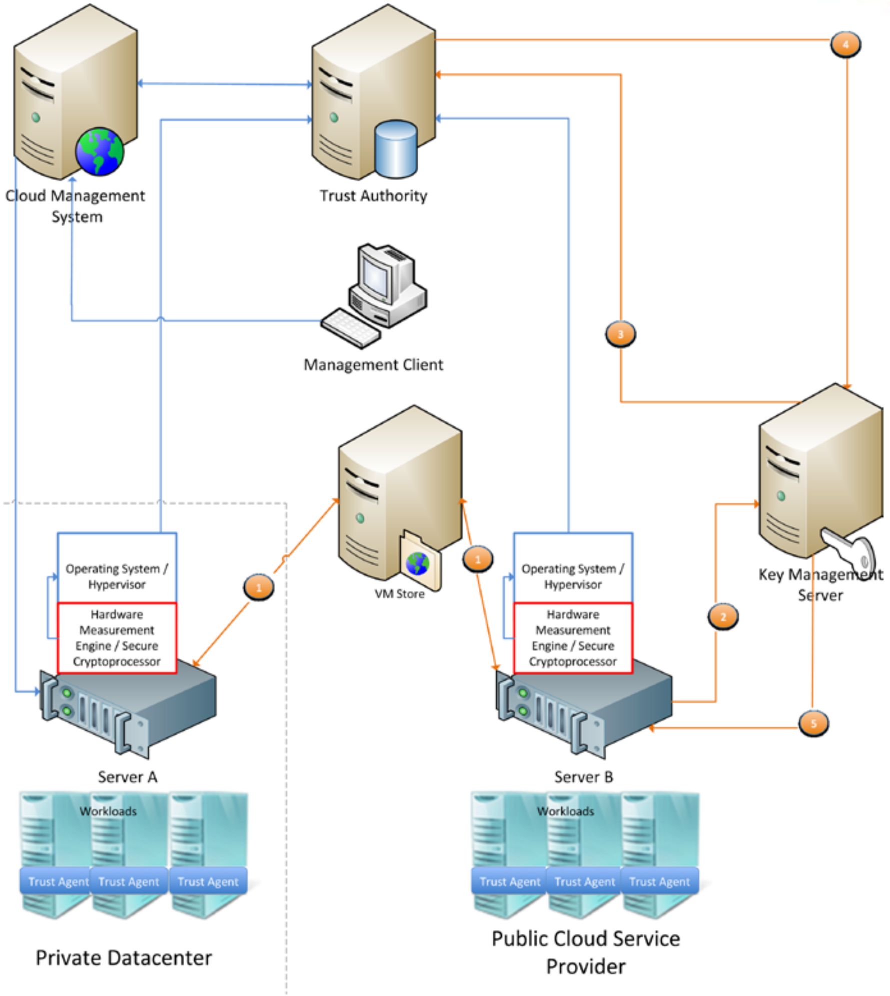
1. Server B accesses workload store that holds encrypted workload image.

2. Server B sends signed request for workload encryption key to Key Management Server.

3. Key Management Server sends host trust attestation request to Trust Authority.

4. Trust Authority sends trust status response to Key Management server.

5. If the host trust status meets policy for workload encryption key, Key Management server sends Server B encryption key for workload encrypted with Server B private key.



References

NIST SP 800-145 The NIST Definition of Cloud Computing

NIST IR 7904 DRAFT Trusted Geolocation in the Cloud: Proof of Concept Implementation.

Yeluri, Raghu and Castro-Leon, Enrique, *Building the Infrastructure for Cloud Security A Solutions Overview*, Apress Media, 2014.