# Trusted Compute Pools Feature in oVirt

Oct 22, 2013

Gang Wei, gang.wei@intel.com

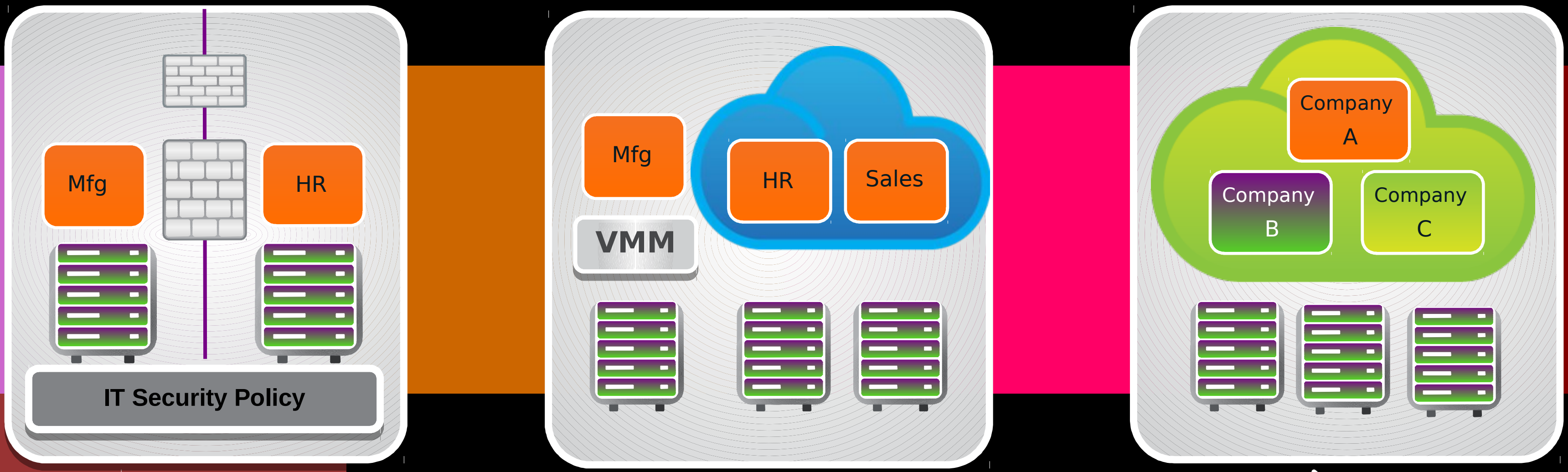
Haitao Shan, haitao.shan@intel.com

# Agenda

- Background
- Architecture
- Implementation Details
- Summary

# Background

# Datacenter Virtualization Drives New Security Needs



Traditional Data Center

Virtualized and Private Cloud Data Center

Public Cloud Data Center

## Challenges

- **Reduced physical control, visibility**
- **Increased multi-tenancy**
- **Reduced effectiveness/efficiency of existing security toolbox**
- **Increased attack surface**

## IT Pro survey of key concerns:

**61%**
**Lack of visibility** inhibiting *private* cloud adoption1

**55%**
**Lack of control over data** key concern for *public* cloud adoption1

**57%**
**Avoid putting workloads** with compliance mandates in cloud1

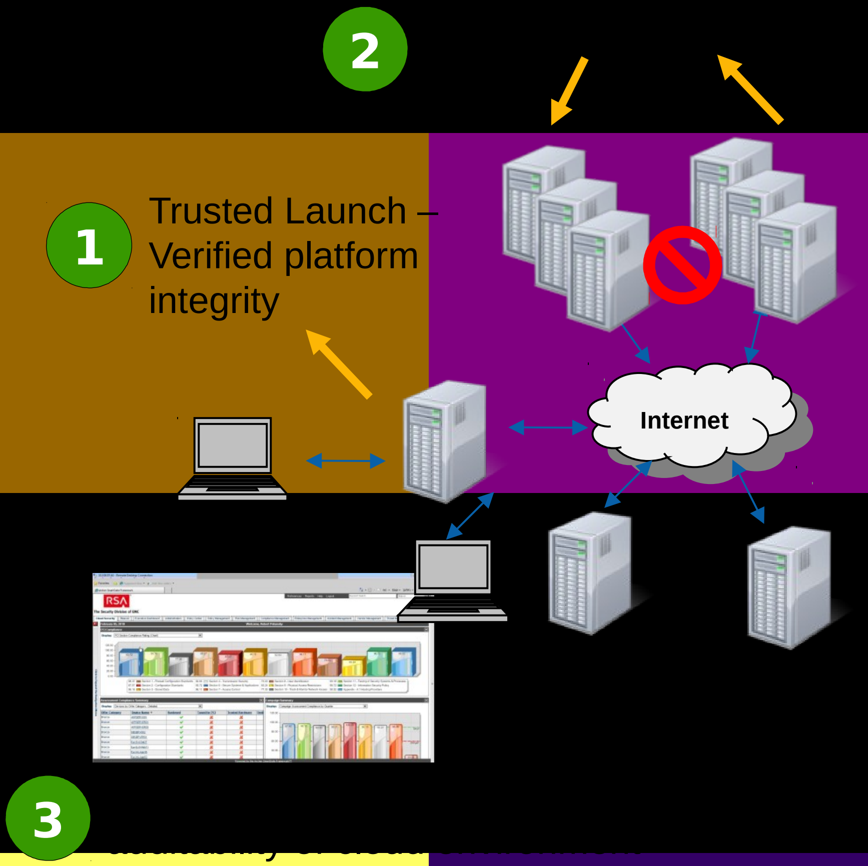
1 source: McCann "what's holding the cloud back?" cloud security global IT survey, sponsored by Intel, May 2012

# Trusted Compute Pools Usage Models

1 **Trusted Boot:** Hardware-based root enforcement of launched environments – reduces malware threat

2 **Trust Based Policy Enforcement:** Control VMMs based on platform trust (and more) – better data protection

3 **Infrastructure Audit and Compliance Reporting:** Hardware-enforced compliance reporting



Trusted Launch – Verified platform integrity

**Trusted Compute Pools:**
**Helps meeting new security needs**

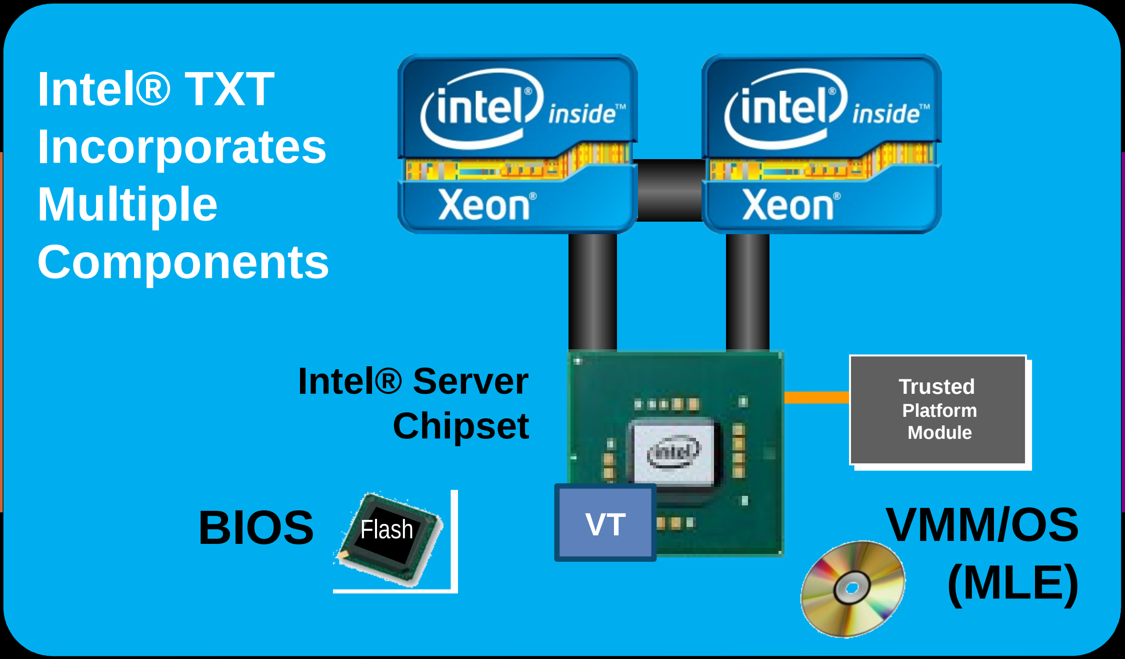
# Trusted Compute Pools Key Components

- Hardware assisted platform integrity measurement
  - H/W platforms with Intel® Trusted Execution Technology support
  - tboot + OS/VMM supporting measured boot based on Intel® TXT
- Remote attestation service providing platform trustworthiness based on platform integrity
  - OpenAttestation providing attestation service & host agent
- Management tools enhanced with Trusted Compute Pools feature

# Intel® Trusted Execution Technology (Intel® TXT)

tamper detection in boot process

- Complements runtime protections
- Reduces support and remediation costs
- Hardware-based increases assura compliance
- Trust status usab
- Trusted Boot(Tbo verified launch of OS kernel/VMM.



Intel® TXT Incorporates Multiple Components

**Hardens and Helps Control the Platform**

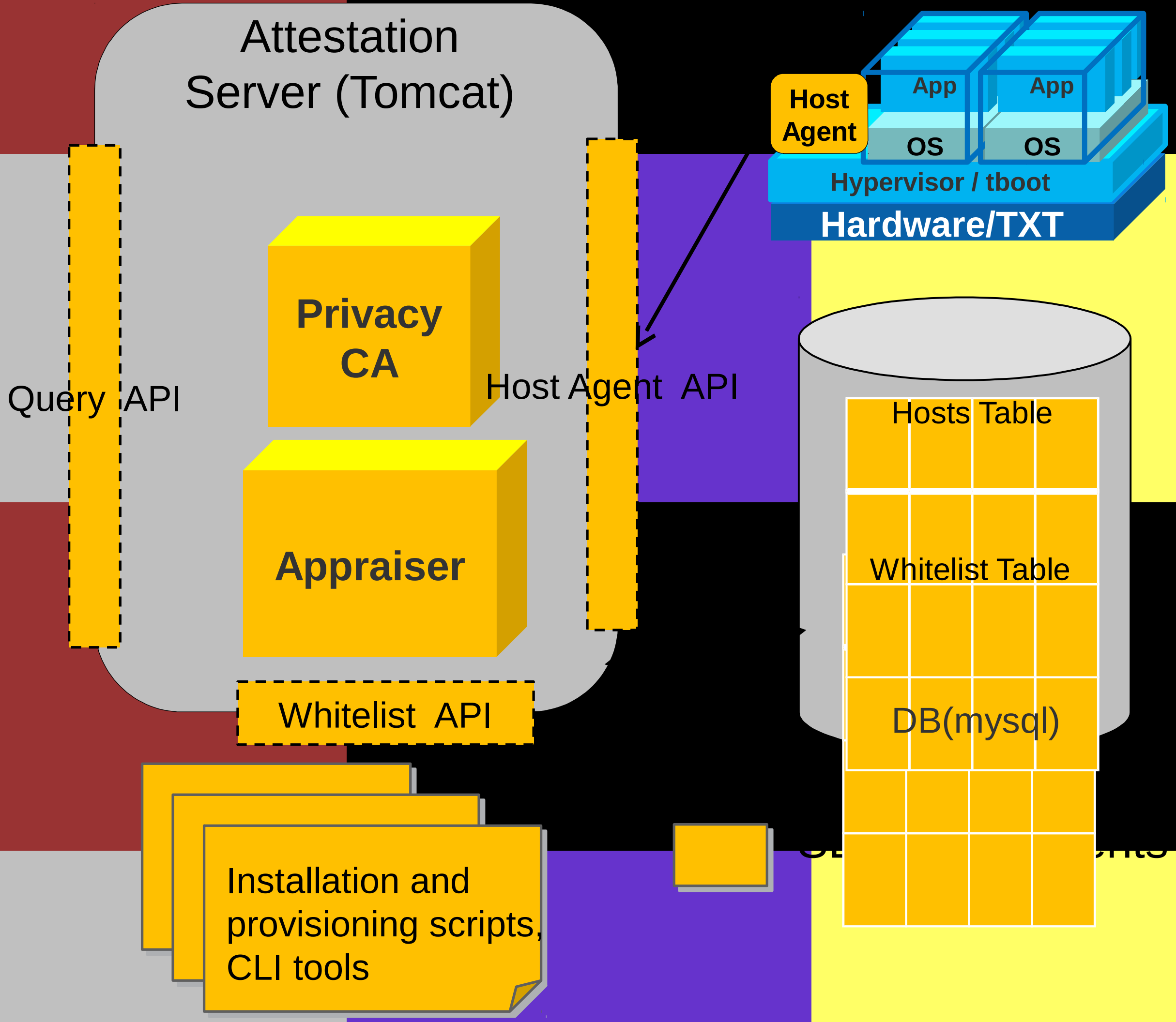
# OpenAttestation (OAT)

- SDK for managing host integrity verification.
- Use TCG-defined remote attestation protocol.
- Target at cloud and enterprise management tools.

https://github.com/OpenAttestation/OpenAttestation.git

- Open Source project established by Intel in Q1’12, v1.6 released in Q4’12, v2.0 released in Q3’13

# OAT Architecture

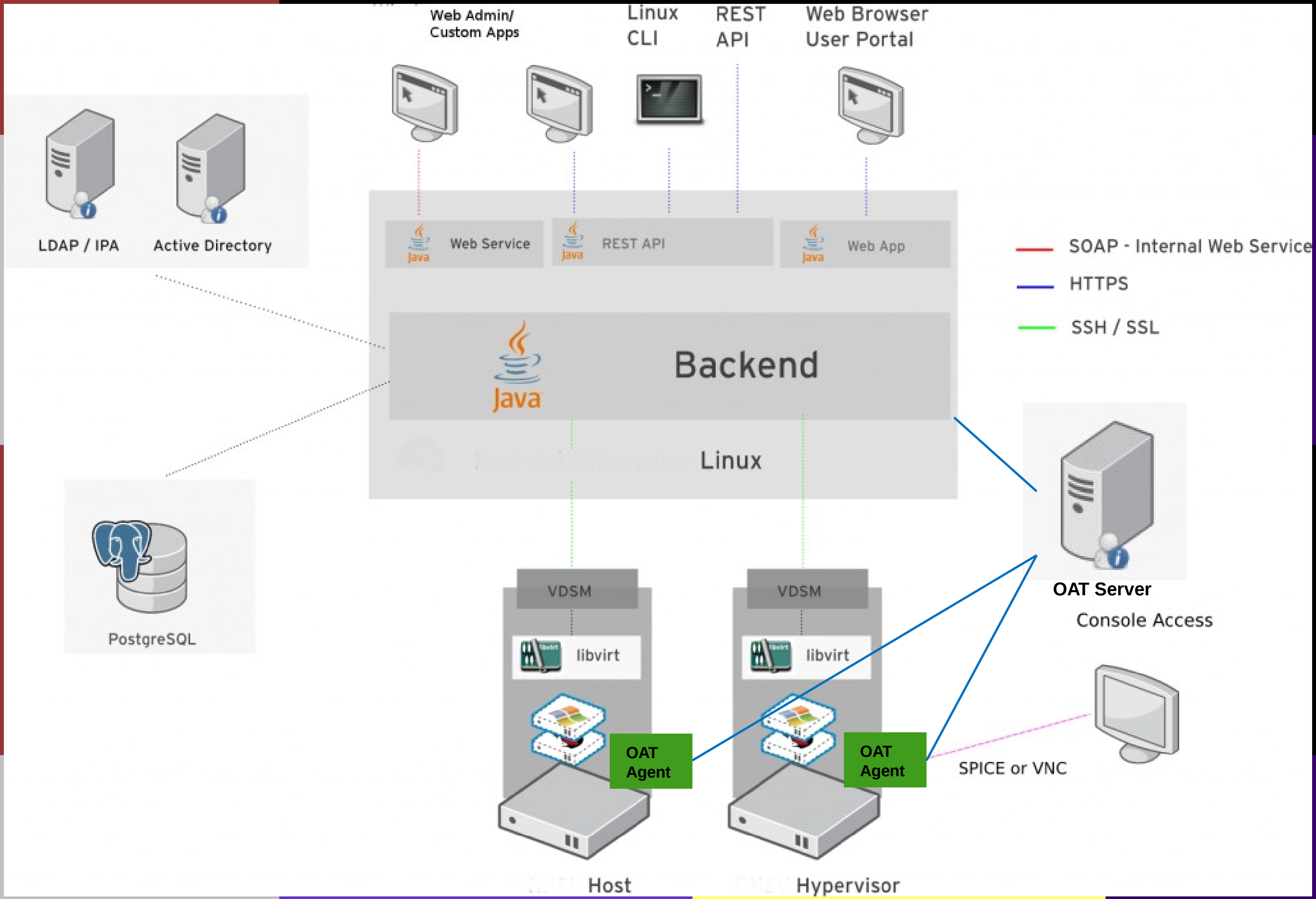


- Privacy Certificate Authority (Privacy CA), Appraiser, Host Agent are Java*
- Host Agent accesses TPM through TrouSerS

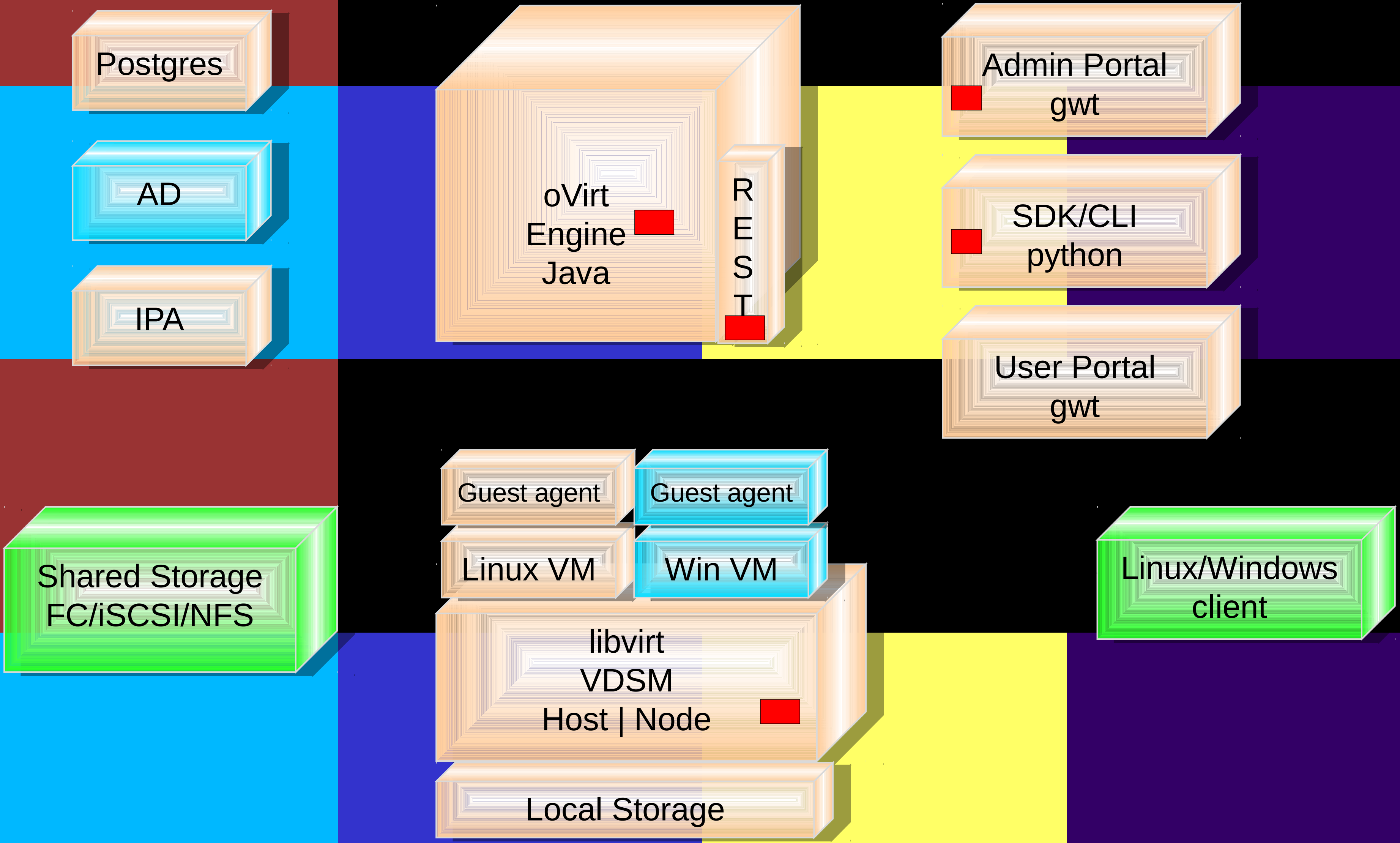
**OAT provides standard RESTful API interfaces**

# Architecture

# Overall Architecture



# oVirt Components Requiring Changes

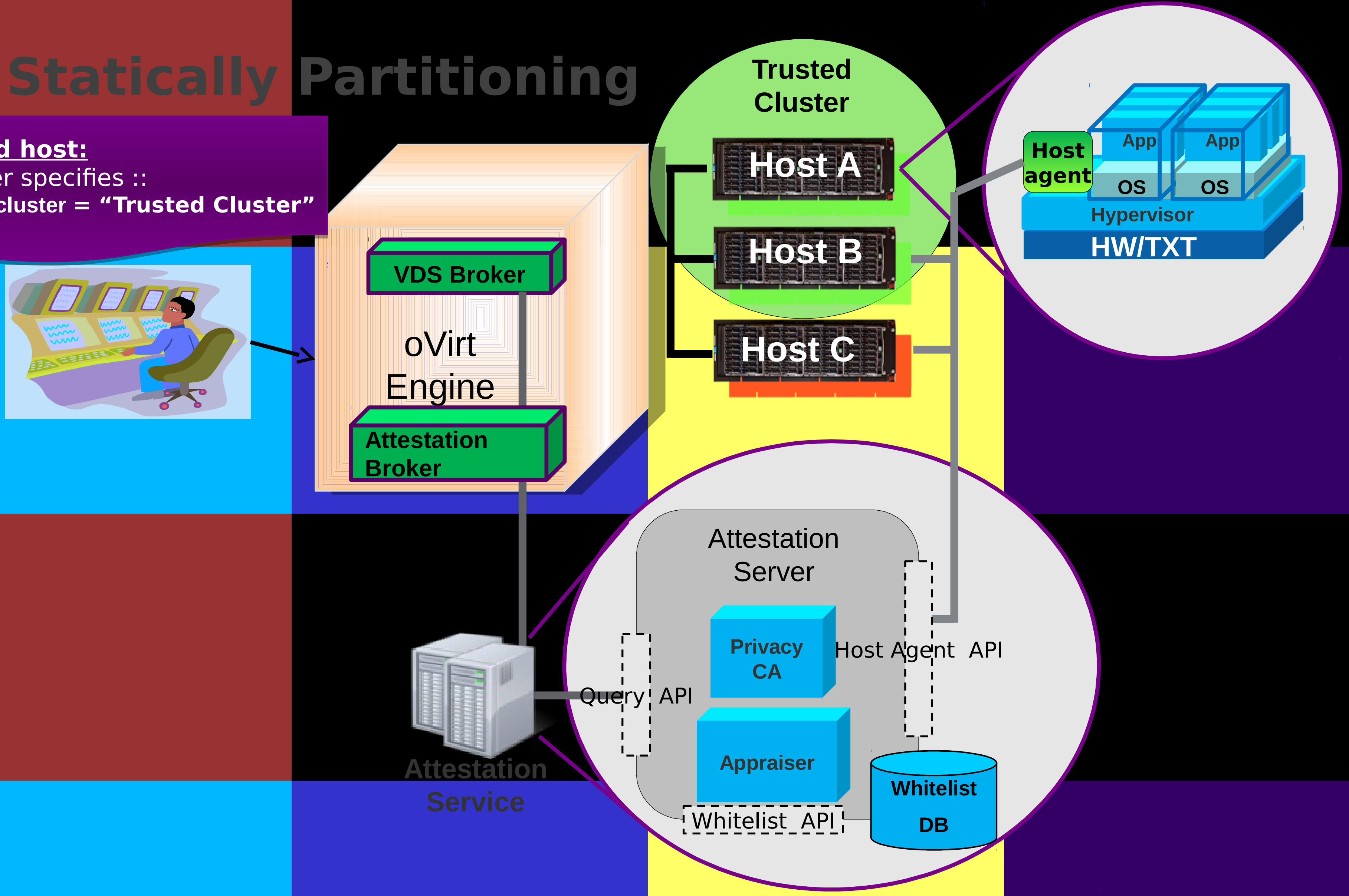


# Statically Partitioning

**Add host:**

User specifies ::

**cluster = "Trusted Cluster"**



# Key advantages

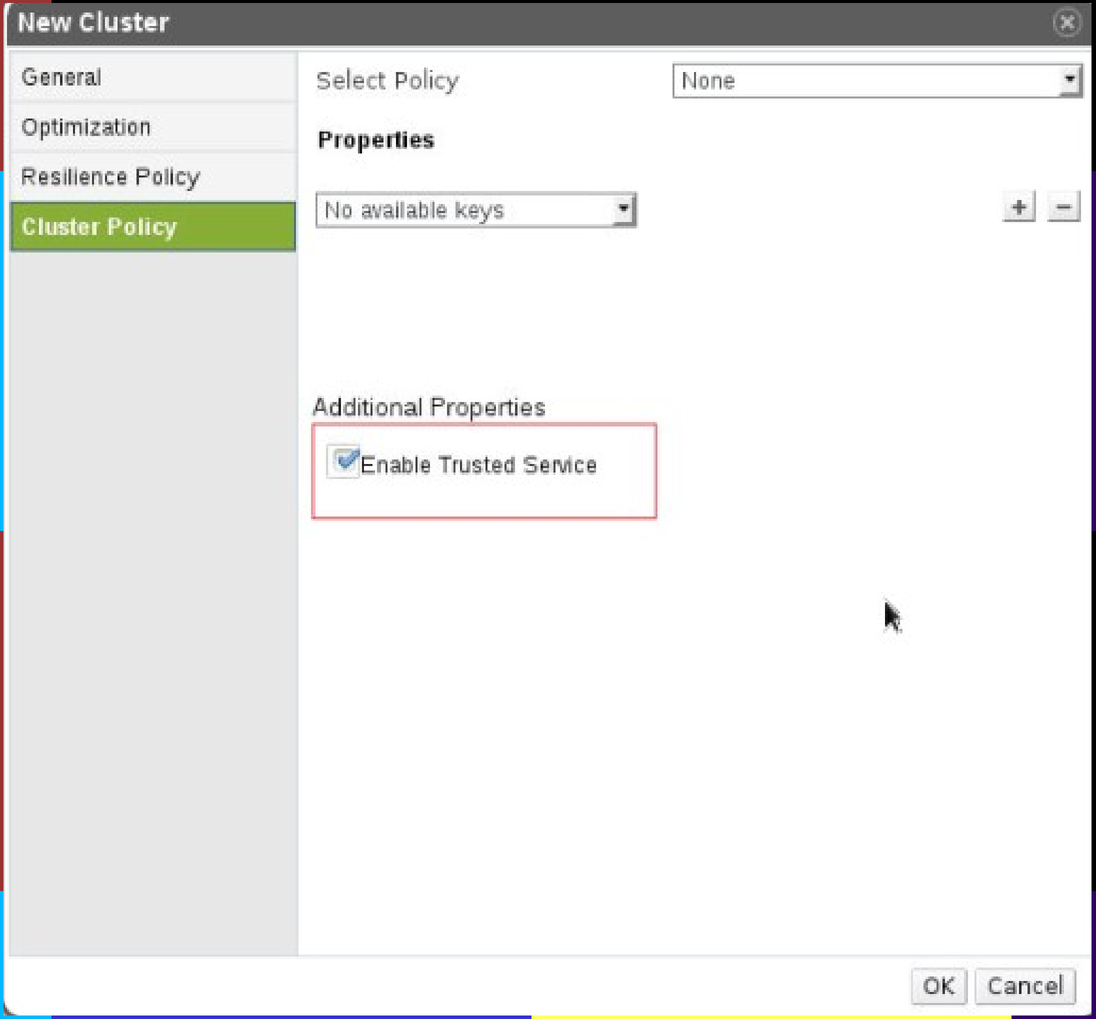
- No migration support issue
- No additional scheduling performance lost

# Implementation Details

# Status

- Feature page: http://www.ovirt.org/Trusted_compute_pools
- Work started since Dec 2012, finished by Aug 2013
- Available in oVirt 3.3(Sep 16, 2013)

# Frontend:



New Cluster

Select Policy: None

**Properties**

No available keys

Additional Properties

☑ Enable Trusted Service

# Backend

- Add attestation check logic in "InitVdsOnUpCommand.java“
  - Trusted host “Up” and untrusted host put as non-operational status
  - Expected trigger conditions:
    - Add a host into a trust cluster
    - Host rebooted
  - Call SetNonOperationalVdsCommand with a new NonOperationalReason
    - Migrate all VMs from the host and then set it non-operational.
- Add aggregated attestation check in Backend.Initialize()
  - Fire a one-time background request from this method to avoid blocking it
  - Do attestation by stages:
    - Configurable max number of attested hosts in stages:
      - Stage 1: FIRST_STAGE_QUERY_SIZE , 10 as default
      - Stage N: SECOND_STAGE_QUERY_SIZE, 20 as default

# Database

- vds_groups table: add a new field, trusted_service.

# RESTful API

```
curl -v -u "admin:password“
    -H “content-type: application/xml“
    -d '<cluster><name>my_cluster</name>
               <trusted_service >true</ trusted_service>
       </ cluster >‘
    'http://engine.***.com:80/api/cluster'
```

- Key relevant modification includes api.xsd and VmMapper.java

# OVF

- A new flag in OVF: trusted_service
  - Record whether the VM is exported from a trusted cluster
- Key relevant classes:
  - OvfTemplate{Reader|Writer}.java
  - OvfVm{Reader|Writer}.java
- Alert for importing a 'trusted' VM into an untrusted cluster
  - Alert via printing event log

# Future Work

- High Availability solution
- Etc.

# Summary

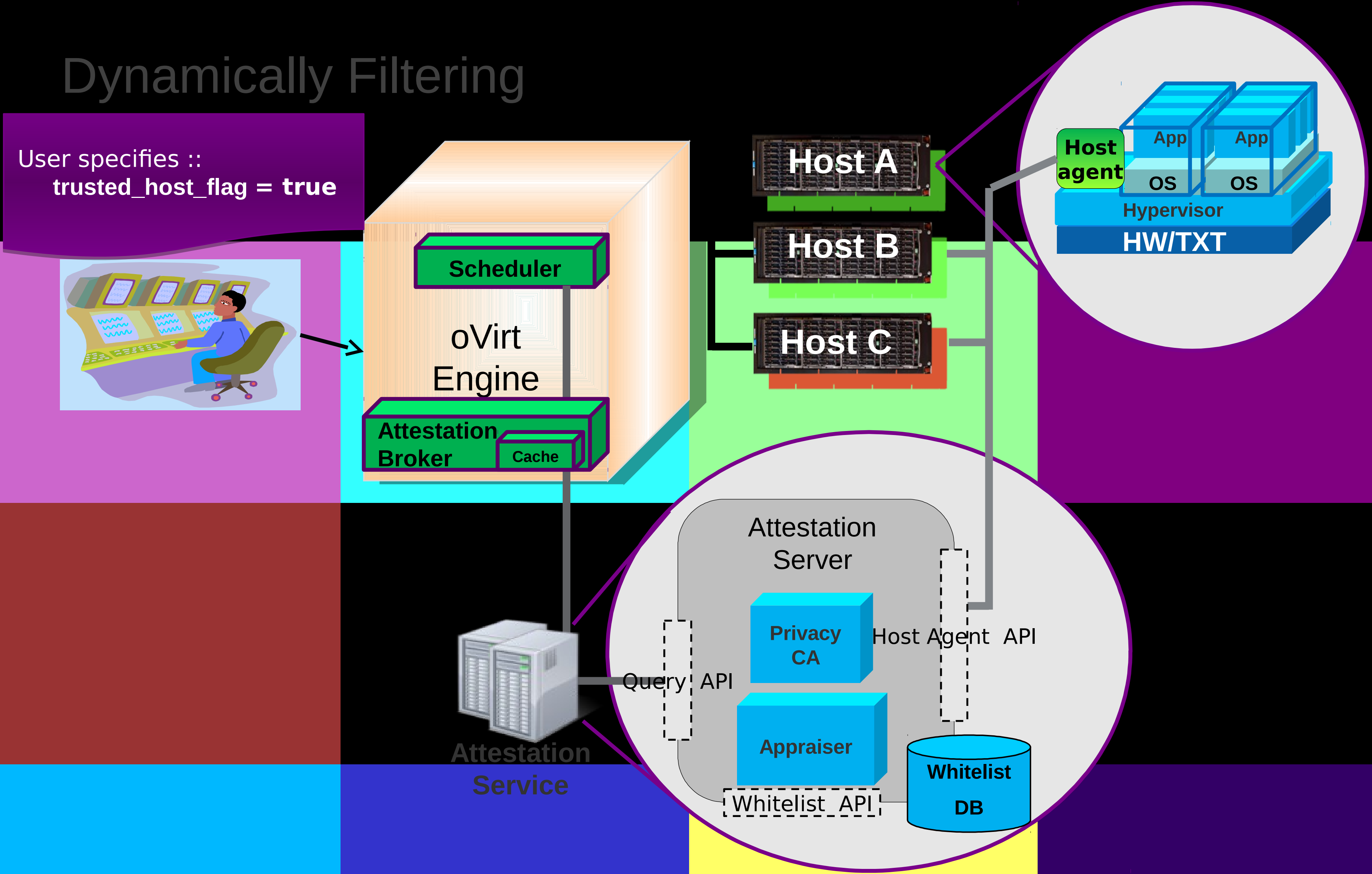
# Trusted Compute Pools Feature in oVirt Summary

- Trusted Compute Pools provides a way for Cloud/Datacenter administrator to deploy VMs on trusted hosts for data protection & service differentiation.
- Intel® TXT provides hardware support for Trusted Compute Pools usage.
- Trusted Boot (tboot) and OpenAttestation (OAT) are two key components for the deployment of Trusted Compute Pools.

# Q&A

# Backup

# Dynamically Filtering



User specifies ::
**trusted_host_flag = true**

# Key issues

- Migration support
- Scheduling performance

# Notices and Disclaimers

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL® PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER, AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL® PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT. INTEL PRODUCTS ARE NOT INTENDED FOR USE IN MEDICAL, LIFE SAVING, OR LIFE SUSTAINING APPLICATIONS.

Intel may make changes to specifications and product descriptions at any time, without notice.

All products, dates, and figures specified are preliminary based on current expectations, and are subject to change without notice.

Intel, processors, chipsets, and desktop boards may contain design defects or errors known as errata, which may cause the product to deviate from published specifications. Current characterized errata are available on request.

No computer system can provide absolute security under all conditions. Intel® Trusted Execution Technology (Intel® TXT) requires a computer with Intel® Virtualization Technology, an Intel TXT-enabled processor, chipset, BIOS, Authenticated Code Modules and an Intel TXT-compatible measured launched environment (MLE). Intel TXT also requires the system to contain a TPM v1.s. For more information, visit http://www.intel.com/technology/security

Intel, Intel logo, Xeon, and Xeon Inside are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

*Other names and brands may be claimed as the property of others.