SMI-S Deployment Best Practices

Make sure customers love it from the start!

Paul von Behren, Symantec

Duane Baldwin, IBM

Deployment Background

- SMI-S is a standard for Storage Management
- SMI-S solutions started shipping 2002 - 2003
- A couple years later
  - Vague reports of installation and configuration issues
  - Frustration from folks doing the installations
- Many spec improvements related to installability
- In 2006, SNIA's Storage Management Initiative (SMI) started investigating "deployment issues"

Background (continued)

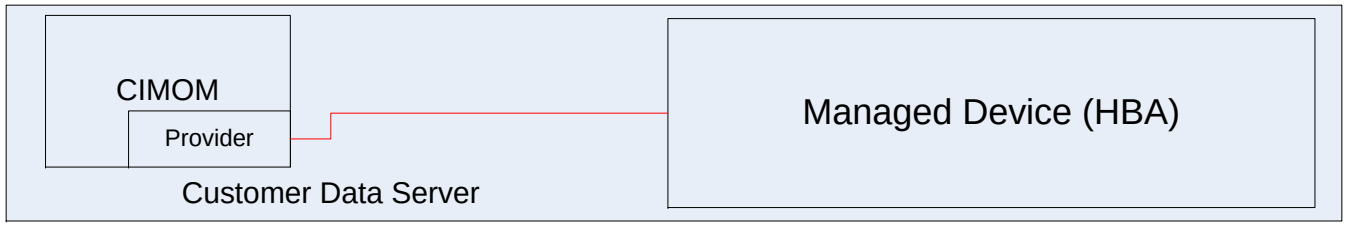
- In 2007, SMI started the "Production Ready Task Force". This task force:
  - Finds themes in reports of deployment issues
  - Investigates root causes
  - Includes spec developers, product developers, product installers
  - Developing installation checklist (for installers) and best practices (for developers)
    - This presentation is based on the best practices

Motivation

- CIM/SMI-S nearly always involves 3rd-party CIMOMs
  - May not be as well integrated or documented as vendor-developed components
  - Some open-source CIMOMs were poorly supported – have disappeared – but impacted early products
- CIM/SMI-S involves multiple vendors
- Bad customer experiences during initial installation and configuration can cause perception of problems in all CIM/SMI-S solutions
  - Hence, the motivation to educate developers
  - Make sure customers love SMI-S installations!

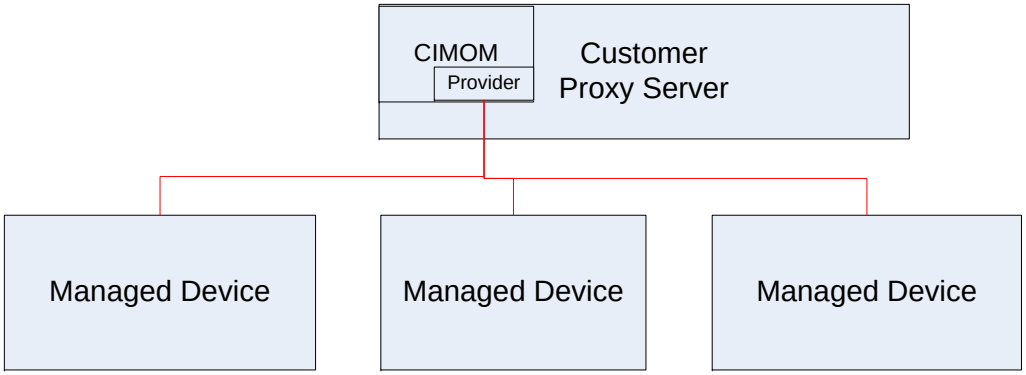
Deployment Options

- Developers have several options for deploying CIM providers for storage
- The choices made for where providers are deployed influence a variety of issues related to installation experiences
- Consider several common approaches to deployment:
  - For host-based components (HBAs, filesystems, …), providers run in a CIMOM running on the *data server*

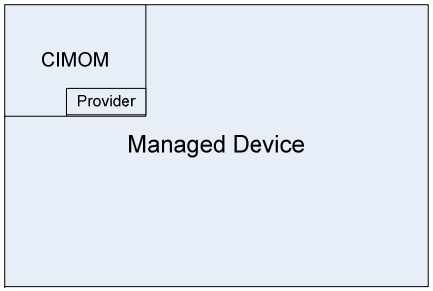


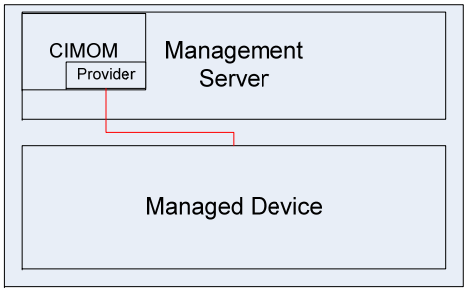
Deployment Options

- For external devices (storage arrays, tape libraries, …)
  - Providers could run on a *proxy* server



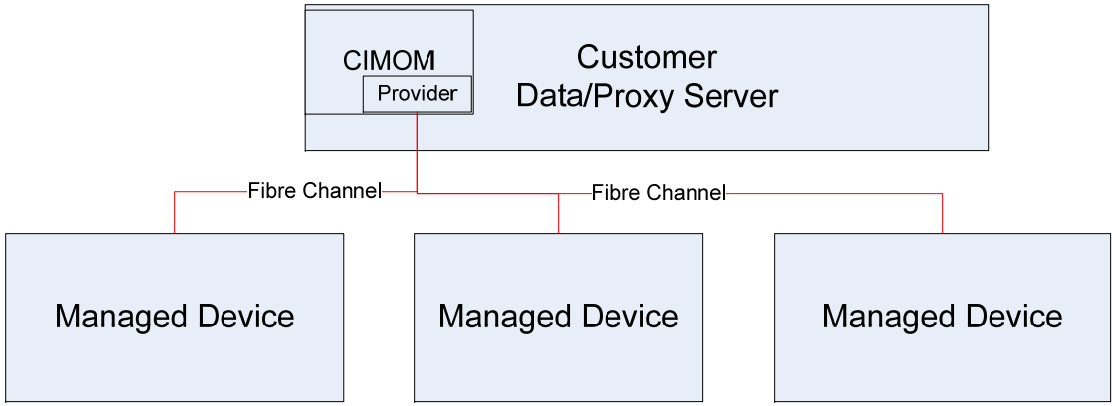
  - Providers and CIMOM could be *embedded* in devices either acting as an integral component or as a management server possibly supporting multiple devices.





Deployment Options

- If the device uses the *datapath* (as opposed to Ethernet) for management communication, then the deployment may be a merge of the Data and Proxy Server approaches



Data Server Deployment
Best Practices

- Consider integrating with the OS and/or platform vendors
  - If the SMI-S instrumentation is "just there", many installation issues disappear
  - If this is not possible, make sure that your CIMOM infrastructure coexists with others
    - Make sure you look for potential conflicts with TCP ports
    - Make sure customer knows which ports are actually in use
    - Don't change the port number later (clients probably have it persisted)

Proxy Server Deployment
Best Practices

- Provide guidelines on scalability
  - Number of devices per reference proxy server configurations
  - Impact (if any) of adding memory
- Provide proxy server software requirements
  - versions, options, middleware
- Smart installer
  - Handle installation of JRE, CIMOM, providers, provider support SDKs if necessary
  - Rather than forcing people to determine when this installations are necessary

Embedded Deployment
Best Practices

- Consider customer reaction to device unavailability due to management software upgrades
  - Consider embedded architectures where the management components can be restarted with no impact to data availability
- Consider scalability
  - In most devices, not an issue – the configuration scales up via multiple devices
  - For network switches, a large network may result in too much management activity for resources of one switch

Datapath Communication
Best Practices

- Documentation on HBA and HBA firmware requirements
- Even if your vendor documentation is sub-optimal, customers may be able to troubleshoot Ethernet connectivity issues
  - But customers are likely to be less familiar with datapath trouble-shooting tools
  - Consider more-detailed trouble-shooting documentation

Post Installation Configuration

- In many systems, the configuration of resources is separate from the installation
  - Make sure installer realizes that additional steps are needed to make the device manageable by clients
  - Document the steps needed to configure devices using serial ports, … to make the device usable with SMI-S
  - Document requirements for middleware (such as APIs) on the server hosting the providers

Compatibility with Device

- Avoid requiring the installer to know the compatibility matrix
  - Have provider validate the device has appropriate firmware level
  - Have provider validate the device is configured as needed
  - Have provider validate the device model is supported

Deployment-independent
Best Practices

- Make sure software and documentation is easy to locate
  - Consider third-party installations (from integrators, client vendors)
- Make sure CIM components scale up to the maximum supported configuration
  - Consider view classes
  - Consider client pull operations
- Make sure software elegantly deals with situation where installer configures second proxy to manage the same device

Standard Provider APIs

- Considering using a standard provider API (such as CMPI or JSR48)
  - In the future there may be a need to switch to a different CIMOM
  - Use of a standard may make it possible to offer customers a choice between open-source and commercially supported CIMOMs

CIMOM Coexistence

- Don't disallow customer installing multiple CIMOMs on same server
- Most vendors do not want to allow customer installs of providers in a pre-existing CIMOM
  - Concerns about stability
- Multiple CIMOMs may not perform optimally
- But customer may have a few small CIM configurations
  - Several CIMOMs on one server – with possible performance bump – may be more attractive than several servers

CIMOM Coexistence

Best Practices

- Make sure your CIMOM startup elegantly deals with another running CIMOM
- Make sure your CIMOM is able to handle TCP port conflicts
- Make sure your CIMOM is not using the same /var/run/whatever.pid file name or Windows service name as a previously installed CIMOM

SLP (for Client Developers)

- SMI-S requires support of SLP as a initial discovery mechanism
  - It appears that CIMOMs have SLP working fairly well
    - Thought developers may need to enable SLP support
  - SLP uses both unicast and multicast
    - Clients do not need a user to provide multicast IP address
      - But multicast often limited by administrators due to potential issues in security and bandwidth
    - But uncast SLP still useful
      - Client makes unicast request to CIMOM servers to discover supported TCP ports, schemes, interop namespace name, and profiles
      - Eliminates the need to ask user for this info

Security Best Practices

- Document information on how to install certificates (if supported)
  - Sometime this is simply a matter of copying certificate files to a known location
- Consider 3rd Party Authentication and Authorization
  - For example, allow devices to use an Active Directory server
- Consider Supporting Mutual Authentication for indications

Questions?