Enabling Manageability with Intel® Active Management Technology

Intel IT has started replacing desktop and mobile PCs across the enterprise with client systems enabled with Intel® Core™2 processor with vPro™ technology and Intel® Centrino® with vPro™ technology. These processor technologies include Intel® Active Management Technology (Intel® AMT), which enables out-of-band (OOB) access to PC clients regardless of whether systems are powered down or non-functional. This functionality will help us reduce client management costs and improve IT security and inventory accuracy.

We plan to purchase all new PCs and integrate Intel AMT serial-over-LAN (SOL) and IDE redirect (IDER) down-the-wire management capabilities into our helpdesk responses. To date, we've deployed over 4,000 systems with Intel AMT and successfully introduced and managed multiple versions of Intel AMT in our ecosystem.

Profile: Intel® Active Management Technology

- More than 4,000 desktop and mobile systems deployed in 2007
- Reduces costs of managing client systems
- Improves IT ecosystem security and accuracy of IT inventories

Figure 1. Building an enterprise manageability ecosystem. PCs based on Intel® Core™2 processor with vPro™ technology and Intel® Centrino® with vPro™ technology feature Intel® Active Management Technology, which allows IT staff to remediate problems remotely, reducing operating costs and the time users wait for system repairs.
Implementing Intel® Active Management Technology across the Enterprise

Intel AMT, a hardware component of the Intel Core 2 processor with vPro technology and Intel Centrino with vPro technology, combines remote client management and network protection into an OS-independent and tamper-resistant solution. It enables out-of-band (OOB) access to PC clients regardless of whether systems are operating, powered down, or non-functional. Intel AMT improves system security, asset management, and system manageability.

To gain these benefits corporate-wide, Intel IT started deploying Intel AMT-enabled systems in the second quarter of 2007, as shown in Table 1. Our initial deployments involved controlled releases in training rooms, followed by deployments to our production intranet. We plan to continue the implementation through 2008 by tying it to a rolling, worldwide replacement of all desktop and mobile systems.

Our corporate-wide re-platforming effort includes several compute ecosystem components:
- Intel AMT manageability functions
- Intel® Core™ processor family
- Intel AMT management console
- Intel AMT Setup and Configuration Service

**Table 1. Deployment of Intel® Active Management Technology (Intel® AMT) at Intel**

<table>
<thead>
<tr>
<th>Version</th>
<th>Number of Systems</th>
<th>Timeframe</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intel AMT version 2.0</td>
<td>300</td>
<td>Second quarter, 2007</td>
</tr>
<tr>
<td>Intel AMT version 2.5</td>
<td>200</td>
<td>Third quarter, 2007</td>
</tr>
<tr>
<td>Intel AMT version 2.5</td>
<td>4,000</td>
<td>Fourth quarter, 2007</td>
</tr>
</tbody>
</table>

**Table 2. Intel® Active Management Technology (Intel® AMT) Deployment Guiding Principles**

<table>
<thead>
<tr>
<th>Guiding Principle</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add no user operating system agent.</td>
<td>Simplifies use and reduces agent management requirements.</td>
</tr>
<tr>
<td>Do not pass sensitive data in clear text.</td>
<td>Helps ensure that access to Intel AMT is restricted and secure.</td>
</tr>
<tr>
<td>Integrate solution with existing security capabilities.</td>
<td>Maintains the security of the environment when adding Intel AMT. Adding authentication and authorization tools can increase security risks.</td>
</tr>
<tr>
<td>Integrate deployment steps into current means of building and provisioning systems.</td>
<td>Helps ensure that Intel AMT provisioning will be completed successfully.</td>
</tr>
<tr>
<td>Integrate and handle multiple Intel AMT versions concurrently.</td>
<td>Helps ensure ecosystem manageability and avoids errors that come with complexity.</td>
</tr>
<tr>
<td>Use existing architectural principles for the implementation.</td>
<td>Keeps costs down by reusing existing capabilities, purchasing new capabilities only when necessary, and custom building capabilities as a last resort.</td>
</tr>
</tbody>
</table>

**Deployment Guiding Principles**

As we planned for Intel AMT deployments, we established a set of principles to guide our efforts, outlined in Table 2.

**Aligning ISV Management Products with IT Priorities**

As we planned our implementation, we made sure that ISV console management functions aligned with our IT priorities by making certain that:
- The console offering addresses all high-priority IT functional requirements
- The ISV is committed to quickly enabling new Intel AMT features
- The ISV roadmap shows a transition from software-based management agents to managing the device at the hardware level, regardless of the state of the operating system
- The console integrates with common means of system and user authentication
- The console integrates with Intel IT methods for tracking asset identities
Testing and Developing an Implementation

To make sure that the architecture and services could handle multiple versions of Intel AMT concurrently, we introduced wireless and mobile clients with Intel AMT version 2.5 into an existing Intel AMT version 2.0 environment, shown in Figure 2.

We tested ISV management functions in this mixed environment and found that these functions operated well for both versions of Intel AMT; the SOL and IDER functions worked better with the more recent version.

Results

To date, we’ve successfully deployed over 4,000 client systems with Intel AMT enabled. We found that we could use the same provisioning process for both versions, making deployment more straightforward and efficient, and we encountered no problems managing multiple versions of Intel AMT from a single toolset.

Intel AMT can be deployed in two operational modes: small and medium business (SMB) and enterprise. Enterprise mode offers greater security protection, with encrypted communication and certificate-based access control to meet Intel security policies. In designing our implementation, we initially enabled SMB mode to gain familiarity with Intel AMT capabilities, and then we enabled enterprise mode to meet our environment’s security requirements.

During our implementation, we discovered that some of our processes for handling systems will need to be revised for future deployments. For example, any process that renames a system requires an Intel AMT re-provisioning step.

---

**Figure 2. Environment for testing multiple versions of Intel® Active Management Technology (Intel® AMT).** ISV management functions work well on both versions tested. Intel AMT version 2.5 improved SOL and IDER functionality.
Future Architectural Plans

Our long-term goal is to increase manageability and scalability using a service-oriented architecture (SOA) with Intel AMT, following WS-Management industry specifications (see Figure 3). With this infrastructure, we plan to:

- Create policies that reflect business priorities and practices
- Manage these policies across multiple toolsets
- Translate the policies into product- and tool-specific rules
- Distribute policy rules to domain policy enablers and Intel AMT end-points for execution

Because new toolsets can be integrated with an SOA, we expect our future SOA to increase IT flexibility and improve return on investment.

Conclusion

The widespread deployment of Intel AMT provides Intel with a significant opportunity to reduce the total cost of operation for client systems and increase manageability by taking advantage of the remote management capabilities with improved security and inventory accuracy.

As we move forward in our implementation, we are identifying ways to increase the value of Intel AMT to our organization. We will expand our IDER-based fault response toolset in response to new use cases for down-the-wire diagnostic and repair. We see even greater benefits from aligning Intel AMT with SOA infrastructure for significantly improved scalability, manageability, and return on investment.

Authors

Jay Hahn-Steichen
Bob Bogowitz
David McCray

Acronyms

IDER integrated drive electronics redirect
Intel® AMT Intel® Active Management Technology
OOB out-of-band
SMB small and medium business
SOA service-oriented architecture
SOL serial-over-LAN