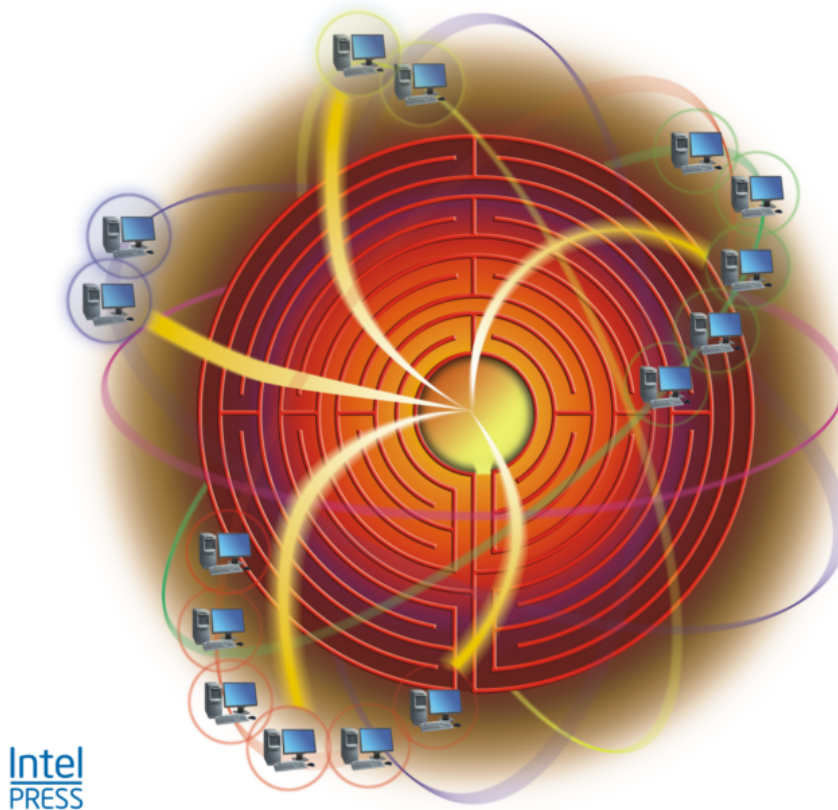


IT Best Practices Series

Active Platform Management Demystified

Unleashing the power of Intel® vPro™ Technology

By Arvind Kumar, Purushottam Goel, and Ylian Saint-Hilaire



Chapter 1 - Introduction to Platform Manageability

- Platform Manageability
- System Manageability
- Manageability Problems
 - Asset Inventory
 - Computer Repair
 - Computer Security
 - Power Savings
- Possible Solutions
- In-band versus Out-of-band
- Management Agents
 - Out-of-band and Agent-less
 - Management in Low Power States
- Summary

Chapter 2 - History of Manageability

- Protocol and Data Model
- Simple Network Management Protocol
- Desktop Management Interface
- Wired for Management
- Intelligent Platform Management Interface
- Alert Standard Format
- Common Information Model
- Abstraction and Classification
- Object Inheritance
- Ability to Depict Dependencies, Component and Connection Associations
- Standard, Inheritable Methods
- Summary

Chapter 3 - Manageability Standards

- Common Information Model (CIM)
 - UML Diagram
 - Managed Object Format (MOF)
- CIM Object Manager (CIMOM)
- CIM Profiles
- Web-Based Enterprise Management (WBEM)
- WS-Management
- Summary

Chapter 4 - Overview of Intel® vPro™ Platforms

- Intel® vPro™ Value Vectors
- Intel® vPro™ Ingredients
 - Intel® Core™2 Processor with vPro™ Technology
 - Chipsets
 - Gigabit Ethernet
 - Platform BIOS
 - Software Applications
- Key Intel® vPro™ Technologies
 - Intel® Virtualization Technology (Intel® VT)
 - Intel® Trusted Execution Technology (Intel® TXT)
- Summary

Chapter 5 - Intel® Active Management Technology Overview

- Key Characteristics
 - Out of Band Access
 - Low Power Operation
 - Operation in Various System States
 - OS-Independent Agent-less Solution
 - Tamper-Resistant Solution
- Discover, Heal, and Protect
- Key Capabilities
 - Hardware Inventory
 - Software Inventory
 - Hardware Health and Platform Sensors
 - Remote Power Control
 - Boot Control
 - Text Console Redirection
 - Disk Redirection
 - Persistent NVRAM Log

- Alerts
- Third Party Data Store (3PDS)
- Agent Presence
- System Defense
- Endpoint Access Control
- Interfaces and Protocols
 - Network Access
 - Local Access
- Intel® AMT and Enterprise Infrastructure
 - Active Directory Integration
 - Setup and Configuration Server
 - Management Consoles
 - Certificate Server
 - BIOS
 - Routers, Access Points, and Servers
 - DHCP and DNS
 - Wi-Fi Access Points
 - Security Compliance Suites
- Summary

Chapter 6 - Solving End User Problems with Intel® vPro™ Manageability

- Protect from a Worm Outbreak
- Tracking Hardware Assets
- Fixing a “Blue Screen”
- Compliance Network Alert
- Tracking Power Usage
- Changing BIOS Settings Remotely
- Remote Platform Diagnostics
- Lockup Detection and Power Control
- Summary

Chapter 7 - The Components of Intel® Active Management Technology

- Hardware Architecture
 - Intel® Manageability Engine (Intel ME)
 - Memory for the Intel® ME
 - Nonvolatile Storage for the Intel® ME
 - Network Access to Intel® ME
 - Protected Clock
 - True Random Number Generator
 - Chipset Fuse Key
- Firmware Architecture
 - Intel® ME ROM
 - Intel® ME Kernel
 - Intel® ME Common Services
 - Intel® AMT Firmware Applications
- Software Architecture
 - Intel® AMT BIOS Component
 - Local Software Components
 - Remote Software Components
- Power Management States of Intel® AMT
- Summary

Chapter 8 - Discovery of Platforms and Information

- Network Scanning for Intel® AMT
- Obtaining Intel® AMT Features
- Obtaining Management Information
- Asset Inventory
 - Intel® AMT Event Log
 - Intel® AMT Network Alerts
 - Event Log and Alert Filters
 - Computer's Power, Battery, and Lockup State
- Third Party Data Storage (3PDS)
- 3PDS Allocation System
- Summary

Chapter 9 - Healing the Platforms

- Remote IDE (IDE-R)
 - IDE-R Protocol
 - IDE-R Speed
 - Booting a Recovery OS
- Serial-over-LAN (SOL)
 - Serial-over-LAN Protocol
 - Serial-over-LAN Speed
 - BIOS Using Serial-over-LAN
 - OS Applications Using Serial-over-LAN
 - Building a Serial-over-LAN Terminal
 - Advanced Uses of Serial-over-LAN
- Summary

Chapter 10 - Protecting the Platforms

- System Defense
 - Network Filters
 - Network Policies
 - Anti-Spoofing Filter
 - Rate Throttling Filter
- Heuristic Filter
 - Heuristic Policy
 - Heuristic Filter Demonstration
 - Heuristic Filter Limitations
- Agent Presence
 - Application Heartbeat
 - Taking Action
- Summary

Chapter 11 - Connecting and Communicating with Intel® Active Management Technology

- Connection
 - Port Usages
 - Authentication and Authorization
 - Environment Detection
 - Intel® AMT VPN Flag
- Local Host Access
 - Implementation of the VPN Flag
- Summary

Chapter 12 - Internet Platform Management

- Environment Detection
- Intel® Fast Call for Help Protocol
- Intel® Fast Call for Help Policies
 - Connection Triggers
- Fast Call for Help Network Routing
- Fast Call for Help Security and Authentication
- Fast Call for Help Connection
- Intel® vPro™ enabled Gateway
- Manageability DTK and Fast Call for Help
- Fast Call for Help Network Speed
- Fast Call for Help Considerations
- Summary

Chapter 13 – Using Intel® Active Management Technology in Small and Medium-Sized Businesses

- Installation
- Manageability Commander
- Connecting
- Remote display
- Intel® System Defense
- Summary

Chapter 14 - Securing Intel® Active Management Technology from Attacks

- Threats to an Intel AMT Computer
 - Local Attacks
 - Remote Attacks
 - Intel® AMT Process and Memory Isolation
 - Intel® AMT Nonvolatile Storage Isolation
 - Firmware Security
 - Intel® AMT BIOS Security
 - Securing the Communication with Intel® AMT
 - Authentication to Intel® AMT
 - Access Control in Intel® AMT
 - Trusted Time in Intel® AMT
- Summary

Chapter 15 - Advanced Security Mechanisms in Intel® Active Management Technology

- True Random Number Generator
- Secure Storage of Sensitive Data – Blob Service
 - Chipset Fuse Key
 - Monotonic Counters
- Measured Launch of Intel® AMT Firmware
- Security Audit Logs
 - Separation of Duties
 - Audit Log Records
 - Posting an Event to the Log
 - Auditing Policy
 - The Audit Trail
- Summary

Chapter 16 - Privacy Protections in Intel® Active Management Technology

- Privacy in the World of Technology
 - Privacy in the Workplace
 - What Constitutes Private Information?
 - The Legal Aspect of Privacy
- Importance of Privacy in Intel® AMT
- Privacy Protection Mechanisms in Intel® AMT
 - Opt-in and Opt-out
 - Secure Local Configuration
 - End-user Notification
 - Private Data Storage Protection
 - Secure Communication of Information
 - Mitigating the Rogue Administrator
- Summary 13

Chapter 17 - Deploying and Configuring Intel® Active Management Technology

- What Is Setup and Configuration for Intel® AMT?
- Deployment Scenarios
 - Factors to Consider
- Intel® AMT Setup and Configuration Overview
- Intel® AMT Web Based Configuration
- Intel® AMT Enterprise Configuration Methods
 - Pre-shared Key TLS-based Configuration Protocol
 - Asymmetric Key TLS-based Configuration Protocol
 - Configuring Enterprise Data
 - Configuration Audit Record
 - Bare Metal Configuration
- Summary

Chapter 18 - Developing Solutions for Intel® Active Management Technology

- Complete Re-use
- Supporting Serial-over-LAN
 - Selecting a Terminal
- Selecting a Software Stack
 - Selecting a WSMAN Stack
- Using the WSMAN Translator
- Using the Manageability DTK Stack
- Manageability Stack Services
- Certificate Operations
- Kerberos Support
- Summary

Chapter 19 - Support for WS-Man and CIM Profiles

- WS-Management Support in Intel® AMT
 - Intel® AMT Data Model
 - DASH Profiles
 - Intel® AMT Extension Profiles
- Summary

Appendix A - Quick Intel® Active Management Technology Setup

Identify If You Have an Intel® vPro™ System

Setup Intel® AMT System

Configure a Browser to Connect

Connect and Explore

Notables

Summary