Intel(R) Active Management Technology (Intel AMT)

Prominent usage of the Intel ME Interface is to communicate with Intel(R) Active Management Technology (Intel AMT) implemented in firmware running on the Intel ME.

Intel AMT provides the ability to manage a host remotely out-of-band (OOB) even when the operating system running on the host processor has crashed or is in a sleep state.

Some examples of Intel AMT usage are:
- Monitoring hardware state and platform components
- Remote power off/on (useful for green computing or overnight IT maintenance)
- OS updates
- Storage of useful platform information such as software assets
- Built-in hardware KVM
- Selective network isolation of Ethernet and IP protocol flows based on policies set by a remote management console
- IDE device redirection from remote management console

Intel AMT (OOB) communication is based on SOAP (deprecated starting with Release 6.0) over HTTP/S or WS-Management protocol over HTTP/S that are received from a remote management console application.

For more information about Intel AMT:
https://software.intel.com/sites/manageability/AMT_Implementation_and_Reference_Guide/default.htm

Intel AMT Applications

1. Intel Local Management Service (Intel LMS)

   Applications running locally on the platform communicate with Intel AMT Release 2.0 and later releases in the same way that network applications do via SOAP over HTTP (deprecated starting with Release 6.0) or with WS-Management over SOAP over HTTP. This means that some Intel AMT features can be accessed from a local application using the same network interface as a remote application communicating with Intel AMT over the network.

   When a local application sends a message addressed to the local Intel AMT host name, the Intel LMS, which listens for traffic directed to the host name, intercepts the message and routes it to the Intel MEI. For more information:
   https://software.intel.com/sites/manageability/AMT_Implementation_and_Reference_Guide/default.htm Under "About Intel AMT" => "Local Access"

   For downloading Intel LMS: https://github.com/intel/lms

   The Intel LMS opens a connection using the Intel MEI driver to the Intel LMS firmware feature using a defined GUID and then communicates with the feature using a protocol called Intel AMT Port Forwarding Protocol (Intel APF protocol). The protocol is used to maintain multiple sessions with Intel AMT from a single application.

   See the protocol specification in the Intel AMT Software Development Kit (SDK)
   https://software.intel.com/sites/manageability/AMT_Implementation_and_Reference_Guide/default.htm Under "SDK Resources" => "Intel(R) vPro(TM) Gateway (MPS)" => "Information for Intel(R) vPro(TM) Gateway Developers" => "Description of the Intel AMT Port Forwarding (APF) Protocol"

2. Intel AMT Remote configuration using a Local Agent

   A Local Agent enables IT personnel to configure Intel AMT out-of-the-box without requiring installing additional data to enable setup. The remote configuration process may involve an ISV-developed remote configuration agent that runs on the host. For more information:
   https://software.intel.com/sites/manageability/AMT_Implementation_and_Reference_Guide/default.htm Under "Setup and Configuration of Intel AMT" => "SDK Tools Supporting Setup and Configuration" => "Using the Local Agent Sample"

Intel AMT OS Health Watchdog

The Intel AMT Watchdog is an OS Health (Hang/Crash) watchdog. Whenever the OS hangs or crashes, Intel AMT will send an event to any subscriber to this event. This mechanism means that IT knows when a platform crashes even when there is a hard failure on the host.

The Intel AMT Watchdog is composed of two parts:
1. Firmware feature - receives the heartbeats and sends an event when the heartbeats stop.
2. Intel MEI iAMT watchdog driver - connects to the watchdog feature, configures the watchdog and sends the heartbeats.

The Intel iAMT watchdog MEI driver uses the kernel watchdog API to configure the Intel AMT Watchdog and to send heartbeats to it. The default timeout of the watchdog is 120 seconds.

If the Intel AMT is not enabled in the firmware then the watchdog client won't enumerate on the me client bus and watchdog devices won't be exposed.

--- linux-mei@linux.intel.com