Deploying Intel's ASF Solution

Intel's ASF Solution: an end-to-end manageability solution for today's corporate network

White Paper

Abstract

ASF is a standards based technology that allows the IT administrator to manage network nodes without regard to system state. The DMTF sponsored initiative allows the IT administrator to not only identify platform events but also provides the ability to securely perform corrective actions that address these alerts. Further, ASF allows the IT administrator to manage client systems in both the OS present and OS absent state.

The paper explores Intel's support for industry standard tools that enable the IT administrator to easily deploy Intel's ASF solution within a Microsoft Windows* environment.

Intel Corporation • 2111 NE 25th Ave. • Hillsboro, OR 97124 • USA

Contents

References

1) Introduction to Microsoft Intellimirror*

http://www.microsoft.com

2) Overview of Windows Installer (Platform SDK)

http://www.microsoft.com

3) Deploying Windows Installer Setup Packages with Systems Management Server 2.0

http://www.microsoft.com

4) The Official InstallShield* for Windows Installer Developer's Guide

http://www.installshield.com

5) ASF Specifications

http://www.dmtf.org

6) Platform Event Trap Specification, v1.1 (PET)

ftp://download.intel.com/design/servers/ipmi/

7) *SMBus Control Method Interface Specification*, v1.0,
http://www.smbus.org/specs/index.html

Introduction

With IT organizations facing increasing pressure to manage more systems with fewer resources, they are forced to re-examine their tools and procedures. Suppliers to the IT community are also impacted – they need to identify how they can differentiate their products and add value for their end customers by making systems management cheaper and easier. As a result, Total Cost of Ownership (TCO) initiatives have received significant focus in the market place. Alerting technology in general and ASF specifically is well suited to contribute to the manageability problem. So, what is the Alerting Standards Forum (ASF) and why is its alerting technology different?

While many network management solutions have been available and deployed for many years, a standards-based approach which provides functionality in the low power and OS absent state has not been available. Typically, software-based management solutions require a healthy OS and application to function. Ironically, when the IT manager most needs to retain access to a remote system for diagnosis and recovery, the OS or an application is most likely to be unavailable or unstable. ASF is designed to address this problem.

ASF is a standards-based alerting technology that enables the IT administrator to manage network nodes without regard to the OS state. ASF not only provides remote alerting of key environmental events such as temperature, electrical, fan, and chassis-intrusion that are detected by sensors, it also provides system status using system heartbeats. These same environmental events and system status events can be monitored in the operating-system-absent environment. ASF also monitors failure-to-boot indications. When an event occurs, a Platform Event Trap (PET) is sent to the management console. Management consoles provide remote control functionality that allows the administrator to take corrective actions based on the alerts.

However, without the ability to be deployed and configured by industry standard tools, the effort required to install and configure *any* ASF solution in an enterprise environment would exceed the benefits of the solution itself. This paper explores Intel's ASF solution and how its deployment model is ideally suited to work well with industry standard tools and Microsoft's IntelliMirror initiatives – initiatives designed to increase the availability and reduce the overall cost of supporting Windows users.

Mircosoft's Intellimirror management technologies use policy-based *Change and Configuration management* to enable users' data, software and settings to follow them in a distributed computing environment[1]. While an Intel ASF solution need not *require* all of the Intellimirror technologies, Intellimirror

provides an excellent backdrop for the technology and tools that the Intel ASF solution does support.

Deployment

Historically, network installations have typically supported two basic methodologies – the pull install and the push install. In the pull install scenario, the software application is advertised to the end user who determines if they wish to use the application. The push scenario, however, provides the end user with no choice – the application is pushed to their computer. Within the context of ASF, the intent of the solution is to monitor the system so the software should always be pushed to the desktop. Further, the ASF solution is system based and not end user based. For the purposes of this paper, unless otherwise noted, installs refer to push installs and policies are system specific rather than end user specific.

The Intel ASF installation is based on the Microsoft Installer (MSI) technology, a core component of the Intellimirror initiative. Windows Installer provides consistent and reliable methods to customize installations, update and upgrade applications, and resolve configuration problems[2].

Within the context of mass deployment, there several relevant features that MSI supports – administrative installs, resiliency and advertising - that are relevant.

Within the MSI domain advertising is best thought of as install on first use. Consider, Microsoft Word. The installation may be configured such that the dictionary associated with Word is advertised rather than full installed. This capability enables the user to conserve local hard drive space yet be assured that if the need arises, the dictionary is available. Since the Intel ASF agent footprint is very small, no advertising is performed – the entire stack is installed.

MSI also supports the concept of resiliency. Should the user destroy any ASF files, the files can be restored using the repair mechanisms inherent within MSI. The Intel ASF Agent solution supports MSI's repair capability. If a file that is part of the Intel ASF solution is inadvertently deleted, it can easily be restored using MSI's repair mechanisms.

A critical feature for mass deployment is the ability to perform an administrative install – the installation of a source image to a network share. Since Windows Installer requires users to retain access to the source files throughout the life of the applications to enable the MSI application repair and install on demand capabilities, it is critical that the source image be available for these features to work.[3] The Intel ASF solution supports administrative installs.

Many software deployment tools support the concepts of multiple distributions points and resilient sources. In many enterprise environments, the number of systems under management typically requires some form of partitioning. It may be over geographical region or it may be based or organizational functions. To assist with site management, distribution points can be created that allow for the distribution of software to flow from the primary distribution point to these

secondary distribution points before being made available to end users. Resilient sources are administrative installation points that are available to the clients throughout the life of the applications. Distribution points together with resilient sources provide a degree of fault tolerance since client computers can use the resilient sources should the original source become unavailable. Use of these features may require additional steps to configure than the traditional installation. Please consult your software deployment user manual to determine if it supports these features and how to use them.

As noted earlier, Intel ASF installations support the necessary MSI features required in MSI based software deployment tools. The Intel ASF solution can be deployed using tools such as Microsoft Systems Management Server (SMS), Computer Associates TNG Unicenter* (with the software deployment option) and Landesk's Management Suite (LDMS). In short, if the tool supports MSI, it can be used to deploy Intel's ASF solution.

Configuration

Unlike most software applications, the Intel ASF solution requires configuration data before they can become functional. The IP address of the management console, alerting status enabled and the name of the SNMP community string that the management console is monitoring are some of the configuration items that are needed before the Intel alerting solution is functional. There are a myriad of ways that can be used to configure ASF; this section outlines some of the tools that can be used to configure. Ultimately, administrators must decide how to best configure ASF within their own environment.

Installation Tools

Since the Intel ASF install model is MSI based, users can use a database table editor such as Microsoft ORCA, a tool provided with the Windows Installer SDK, to manipulate the install itself. Users can modify items such as the install name, support information, reboot requirements and the default install configuration. Through the use of tools such as ORCA, administrators can create installs that are customized for their organization.

In the case where an organization already has an MSI based installation that they have created, it is worth considering using the Intel ASF merge modules that are provided. So what is a merge module? First, let's provide some background on MSI. MSI supports the notion of features and components. Features represent what the end user sees when they install the product. Components represent the binaries and settings that are required to provide the functionality of a feature. Features need to be associated with one or more components. Merge modules represent a container of binaries and associated files and settings for a given component. Next, consider the case of an organization that has an in-house application that uses an MSI based install. By adding an alerting feature to this pre-existing MSI based install and associating all the of merge modules – the agent, aprov and custom merge modules in the case of the Intel ASF Agent software stack – you can integrate the full Intel ASF stack with minimal effort. More importantly, leveraging the merge modules enables the IT organization to provide the desired ASF functionality without the associated overhead of tracking yet another application. It is worth noting that the current Intel ASF installs follow the aforementioned model – it is essentially a wrapper around the merge modules provided as part of the Intel ASF solution.

Users should be cautioned that modifications to the base install or making use of the merge modules requires a degree of understanding of MSI and its tables. Please consult the MSI SDK for additional support.

Transforms

Consider the case of the base Intel ASF install. The configuration settings of the base install will typically need to be modified for any given organization. MSI provides a mechanism called a transform that allows for modifications of a base installation at install time. Technically, a transform represents a template of the differences between two MSI databases.[4] To generate a transform, administrators can install the Intel ASF solution to a given machine and configure it with their desired settings. Once this is complete, the administrator can use a tool such as Wise's Package Studio* or InstallShield's AdminStudio* to generate a transform. The administrator can then create a package – a package that would include the Intel ASF installation as well as the transform. The package can be deployed throughout the organization. The net result is that organization's client systems would have the Intel ASF solution installed and configured based on the settings of the prototype system.

Scripts

Scripts represent another option available to assist configuration of the Intel ASF stack. The Intel ASF solution includes two sample scripts – a VB script and a login script. The scripts should be modified such that the key values suit the needs of the given organization.

VB Scripts

A VB script can be deployed in a number of ways. The script can be run locally or remote. It can incorporated into a software deployment package in much the same fashion as a transform – the Intel ASF base install and the VB script would comprise a complete package. Alternatively, the VB script can be an addendum in the user's login script. Ultimately, the script is used to modify the default base configuration so that the settings conform to the organization's desires.

Login script

The login script leverages the mechanisms of the users pre-existing login environment. The script may be used in conjunction with the user's base login script or it may use some of the login mechanisms supported in tools such as Microsoft SMS. In the end, it is similar to any of the other mechanism previously mentioned – it modifies the default base settings so that they reflect the settings dictated by the organization.

Group Policy

Group Policy allows the administrator to configure groups of users or systems using Active Directory. Through Group policy, Intellimirror centralizes and simplifies change and configuration management.[1] So how does Group Policy work and why is it easier?

The first step in using any Group Policy is to define the group. A group may be a site, a domain or an organization unit. As an example, let's assume that a group has been created that represented all systems within your network that are Intel ASF capable. Next, consider the fact that group policies can be applied on a user or a system basis. Since ASF is solely focused on monitoring a given system and who is actually using the machine is irrelevant, system policies are the only group policies that need to be created for ASF.

Group policy features that support deployment and configuration are then leveraged for the "ASF Group". An installation package is pushed to group members and an administrative template is used to configure the systems. Equally as important, Group Policy allows an administrator to lock down the client system so end users cannot modify configuration settings

ASF 2.0 Key Deployment

In ASF 1.0, the remote control protocol does not support any form of authentication. As a result, any user could generate a RMCP packet that could reboot the system if its remote control capabilities are enabled. To address these concerns, the specification was updated so security is now an integral part of the remote control functionality.

As part of the security initiative, the ASF 2.0 specification requires a symmetrical key – a long term key that is shared by both the agent and the management console - as well as session keys. It also defines the RSP protocol such that the remote control protocols are now secure. The specification framers, however, were mindful of the fact that there is great diversity among organizations in terms of network security infrastructure and security tolerance. With respect to the key exchange between the agent and the management console, the specification for key deployment is sufficiently broad to support the diversity without compromising security. Officially, key exchange requires "an out-of-band mechanism (e.g. local physical access or remote access via a secured connection".

Intel's ASF solution supports a variety of options. The first option is local physical access – placing the keys in each system with an agent and placing the corresponding keys in the management console. Many IT organizations have customized images that they put on new systems upon arrival. As part of this imaging process, organizations may chose to put the ASF key into the system.

However, this option is not suitable for all environments. It does not address the pre-existing systems that do not have keys. If the keys are compromised or lost, the keys must be replaced. It does not scale very well – the effort to get keys to a thousand systems or more is nontrivial. The Intel ASF solution provides a mechanism to do key exchange between the agent and the management console over network. These mechanisms are supported at the WMI layer so they may be invoked from a remote machine. To limit access, the standard WMI security model is used - users are authenticated by their username and password prior to gaining access to WMI. Keys are dynamically generated at the management console and the encrypted keys are sent over the network to the agent system. The agent system decrypts the keys and stores them. Once the keys are available at the agent and the management console, the remote control functions can be performed securely.

Alternatively, organizations may wish to use a secure connection such as those afforded by a public key infrastructure to exchange keys or a secure shell connection. When used in conjunction with Intel's ASF key generation and

load/store functionality, organizations can define a key exchange model for ASF that suits their needs.

Summary

Deployment, configuration and key exchange are critical components of any ASF solution; Intel's ASF solution contains support for best of breed tools and technologies to ensure an easily deployable ASF solution for all types of organizations.