Table of Contents

Executive Summary

Never before has computer-based information been so critical to our nation's war fighting capacity. The use of computer-based information to gain a strategic advantage has been embodied in the doctrine of "Network Centric Warfare". To address the newfound importance that information management plays, and provide a framework for its protection, the Department of Defense (DoD) has implemented the Information Assurance Vulnerability Alert (IAVA) program. The goal of IAVA is to decrease security risk by providing a process for vulnerability notification, correction and reporting.

The current IAVA process provides a solid environment for information assurance. It spans from the DoD Computer Emergency Response Team (CERT) to local site system administrators. The process sets guidelines for acknowledging notification, assessing risk, and reporting corrective actions. However, the process does not address a critical factor: improving the local administrators' ability to more rapidly identify and resolve security vulnerabilities.

In order to minimize security threats across DoD assets, attention must be paid to the local administrators. These individuals are often lacking in the latest system and/or security training and in the latest commercial management tools. Commercial technologies exist that could greatly enhance their ability to maintain operational *and* secure systems. Properly implemented management tools would decrease the time and expertise required to locate and resolve Information Assurance Vulnerability Alerts ("IAVAs"). When these management tools are standardized across a command, C/S/A or DoD, benefits from economy of scale would be seen. The DoD community as a whole will be able to communicate security-related solutions and process improvements more readily and share their implementation experiences. However, the net result would be an increase in the security of our nation's IT resources.

Trinity Solutions believes the best management technologies for the IAVA process are found in the Tivoli Enterprise suite of products. These products would enable local administrators to maintain a database of the hardware and software configuration of their systems, perform tasks using a graphical interface to correct IAVAs on multiple, remote machines, and produce accurate, timely compliance reports. Tivoli Enterprise products have been proven to increase the security configuration and decrease the cost of managing DoD computer assets.

This paper presents how the current IAVA process may be streamlined and improved by adding Tivoli Enterprise products. To illustrate this, this document will present the current IAVA process and its challenges, a new streamlined process based on the addition of management technologies, the benefits of this approach, and a description of a Tivoli Enterprise-based solution.

Background

Purpose of IAVA

The Information Assurance Vulnerability Alert (IAVA) process was instituted in 1998 to “provide positive control of vulnerability notification and corresponding corrective action within DoD.” This program was a direct result of two factors: an increase in the reliance on Information Technology (IT) resources and an increase in the number, frequency, and severity of discovered vulnerabilities to these resources. These vulnerabilities could be exploited to decrease performance of or deny access to critical military systems – severely degrading our nation’s warfighting capacity.

To combat this threat, DoD leaders implemented the IAVA process across all of the Commanders-in-Chief (CINCs), Military Services and Defense Agencies (C/S/As). The IAVA process was put in place to ensure that DoD organizations are notified of new threats, their severity, and their corrective actions and are held accountable for the elimination and/or mitigation of these risks within their domains. Ultimately, the goals of the process are to ensure our warfighters’ ability to access and protect information and, therefore, ensure their ability to control future battlefields.

Current Process

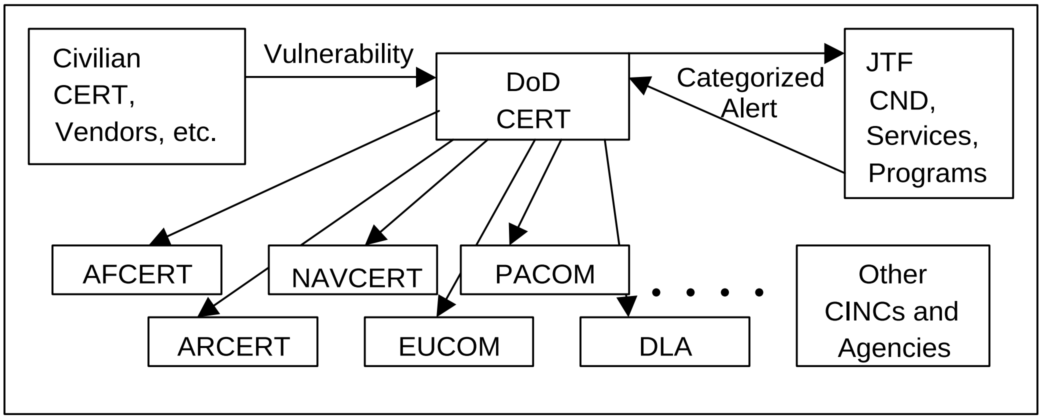
The current IAVA process is a major step toward safeguarding the nation’s systems and networks. The process identifies key organizations and points of contact and provides a set of parameters and guidelines for them to follow. The following are key components of the IAVA process:

DoD CERT

The Defense Information Systems Agency (DISA) was selected to oversee the IAVA process. In this capacity, DISA is responsible for disseminating network, system, and application vulnerabilities to the C/S/As and for providing a means for these organizations to acknowledge receipt of and report compliance with the announcements. As the owner of the process, DISA’s DoD Computer Emergency Response Team (CERT) has categorized vulnerabilities into three levels: an alert (IAVA), a bulletin (IAVB), and a technical advisory. The following table illustrates the importance and required response of each level:

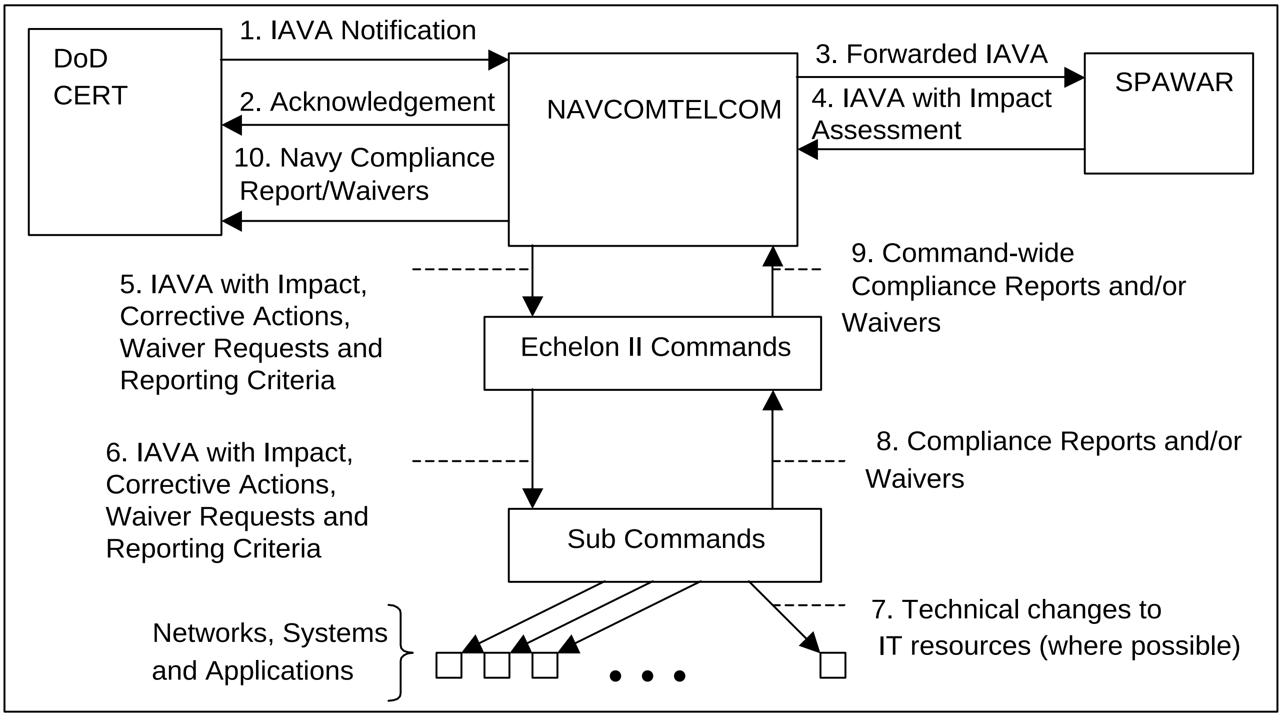
Vulnerability Level	Implication	Response
Alert	Immediate, critical threat	C/S/As must acknowledge receipt and compliance with corrective action
Bulletin	No immediate threat, but may hold future significance	C/S/As must acknowledge receipt
Technical Advisory	Low risk now and in the future	No response action required

In order to identify and categorize vulnerabilities, DoD CERT works with other DoD organizations, technology vendors and civilian CERTs. Once a new vulnerability is received, DoD CERT assesses the impact by considering factors such as what systems may be affected and what could be the effects resulting from a compromise. The initial categorization is sent to the Joint Task Force for Computer Network Defense (JTF-CND), to the Service CERTs and to program managers of joint DoD systems (e.g., Global Command and Control System) for comments and verification. At this stage, the C/S/As are notified of the vulnerability and directed to visit the DoD CERT web site for technical information and fix actions.



CINCs, Services, and Agencies

Once DoD CERT has categorized and sent notice of an IAVA, the next step in the process is for the C/S/As to distribute the alerts within their domains and to take action toward mitigating any risk caused by the vulnerability. Once a notification is received by a C/S/A, the organization's point of contact has five days to acknowledge the message. The C/S/A is the responsible organization for disseminating the alert to its subcomponents and reporting back to DoD CERT on compliance (within 30 days for IAVA and IAVB). The C/S/As will perform a technical assessment to determine the ramifications on their resources. Local system and security administrators receive alerts and are responsible for taking any appropriate corrective actions. The onus of this stage of the process is on the C/S/A and, therefore, the exact details of the process may vary. The illustration below displays an example of how the second stage of the IAVA process is applied by the Navy.



Current Tools

While the IAVA process is comprehensive, the tools that are used to execute it are not. Current tools focus mostly on providing the ability to send, acknowledge, and report on the compliance of IAVA notifications. These tools do not address the organizations' ability to electronically verify the configuration of their systems or the administrator's ability to apply technical corrections to affected systems. The following list describes many of the tools currently utilized:

- DoD CERT uses the Automatic Digital Network (AUTODIN), the Defense Message System (DMS) and mailing lists for delivery of the IAVA notifications. The automated message does not contain specific details about the IAVA beyond its ID and required reporting timelines. Once received, the receiver must manually check the CERT web site to find detailed information about the problem and its corrective action.

- DoD CERT provides a web site that can be entered via login IDs and passwords for acknowledgement and reporting at the C/S/A level. Once authorized, C/S/A POCs can acknowledge the notification and report on their compliance status.

- The C/S/As may or may not utilize tools for the acknowledgment and reporting of their second echelon commands. Some are operating similar web sites that allow local systems administrators (SAs) to manually update the status of their systems with respect to IAVAs. The implementation and usage of these tools is dependent on the specific command.

- The C/S/As have little tools to *verify* the configuration of their resources. On a local level, some administrators may have tools to scan and report on the configurations of certain machines (e.g., Microsoft's Systems Management Server (SMS)for Windows NT systems). These tools are often not able to identify vulnerabilities associated with specific IAVAs.

- The C/S/As may or may not utilize tools for applying system corrections. Usually, the corrective actions are performed on a manual basis by local administrators (e.g., installation of an operating system patch on a local machine). Some actions are automated via locally developed scripts. However, in many cases, the corrective actions require a senior level of expertise relating to the affected type of computing resource (e.g., Solaris, Oracle, etc.).

Challenges

The current IAVA environment is heavily reliant on human input and action. This reliance is in large part due to a lack of management tools that can optimize the process and can translate administrator knowledge into automated capabilities. As a result, three main challenges have risen to the forefront: decreasing the time and expertise required to identify systems at risk, decreasing the time and expertise required to perform corrective actions, and ensuring the validity of compliance reports. These challenges are described more fully below.

Identifying Systems at Risk

The current environment does not provide tools capable of quickly *and* accurately locating systems that are vulnerable to specific IAVAs. An administrator must check DoD CERT for technical specifics of an IAVA and then manually check each system they manage to determine risk. When considering the number and complexity of IT resources throughout our military installations, this task is extremely costly and requires a very high level of expertise.

For example, assume that an IAVA is issued because there is a bug found in Solaris 2.X that can be exploited to gain "root" access to a system. As a result, it is determined that every system that does not have Solaris patch 1234 installed is vulnerable. An administrator would have to check each Solaris system by logging on to it and performing root level commands to test for compliance.

This scenario presents some interesting problems. First, in order to respond to the IAVA, the administrator(s) need root access. This limits the number of people who can perform the action and therefore makes a unit more reliant on senior technicians. Second, the verification is done by human inspection and is inherently more prone to error. This brings doubt into the validity of risk assessments and compliance reports. Third, the administrator(s) need to go through the manual process of checking each system sequentially. This lengthens the time it takes to correct vulnerable systems and, therefore, increases the risk (amount of exposure time) from the IAVA.

Performing Corrective Actions

The current environment does not provide tools capable of quickly *and* accurately correcting vulnerable systems. An administrator must check DoD CERT for a description of the corrective action and then apply that action to each affected system. The result is an increase in the time and expertise it takes to fix vulnerabilities.

Using the same example as above, assume the administrator identified 35 servers in three locations that are vulnerable. Solaris patch 1234 must be downloaded and installed on each system sequentially. Without management tools, this process requires the administrator to log on to each server and to perform Solaris administration commands as the root user to install the patch.

This scenario presents the same problems as the previous one: senior administrator levels for access and expertise required to perform the fix, and a lengthy amount of time required to perform the fix on multiple, distributed systems.

Producing Valid Compliance Reports

A main goal of the current IAVA process is to measure the compliance level of commands as new alerts are issued. Currently, this is heavily dependent on the local administrators who have to manually check system configurations for IAVA characteristics and then manually maintain and forward a report that details affected systems, percentage of systems corrected, etc. As with any process, human interaction may lead to errors. As a result, reports that are sent to senior leadership/management may be inaccurate.

For example, using the Solaris patch scenario, assume that the local administrator has 150 Solaris systems to check for the vulnerability. As described above, this process without management tools can be very complex and arduous. One possibility could be that, in order to save time, the administrator checks one machine and finds that it is not vulnerable to the IAVA. He then assumes that, since all the systems were installed and configured by the same group of five administrators, they must have the same configuration. Therefore, he reports his site at 100 percent compliant. But this could be a mistake. What if one machine had to be reinstalled since the original configuration and the patch wasn't applied to it after the install? What if that machine happens to be a critical database server that is accessed by multiple commands? The ramifications of not accurately identifying and reporting the vulnerability could be severe.

This scenario illustrates the dependence of the current IAVA process on human actions. This dependence can and will lead to errors in vulnerability identification, risk assessment, and vulnerability correction. All of these factors will increase the possibility of critical DoD networks being compromised.

Streamlined IAVA

Future Process

The key to minimizing DoD's threat from IT vulnerabilities is to minimize the time and expertise required by local administrators to identify and correct computing assets at risk.

With the current IAVA environment laying the groundwork for protecting DoD IT assets, the next step should be to streamline the process. The addition of enterprise management tools would decrease the time required to locate and resolve vulnerabilities by DoD components and increase the accuracy of compliance reports and risk assessments on the command, C/S/A, and DoD levels. The end result would be increased information assurance and, therefore, increased ability to defend our nation and its interests. To illustrate a new approach to IAVA, this document will outline the process starting from the local level (e.g., a Base Network Control Center) and move up to the DoD CERT.

Local Network Control Center

In each C/S/A, multiple organizations exist that perform daily management and monitoring of IT resources. While these organizations have many different names, for the sake of discussion, they will be referred to as Network Control Centers (NCCs). The NCCs perform general systems, network, and security administration.

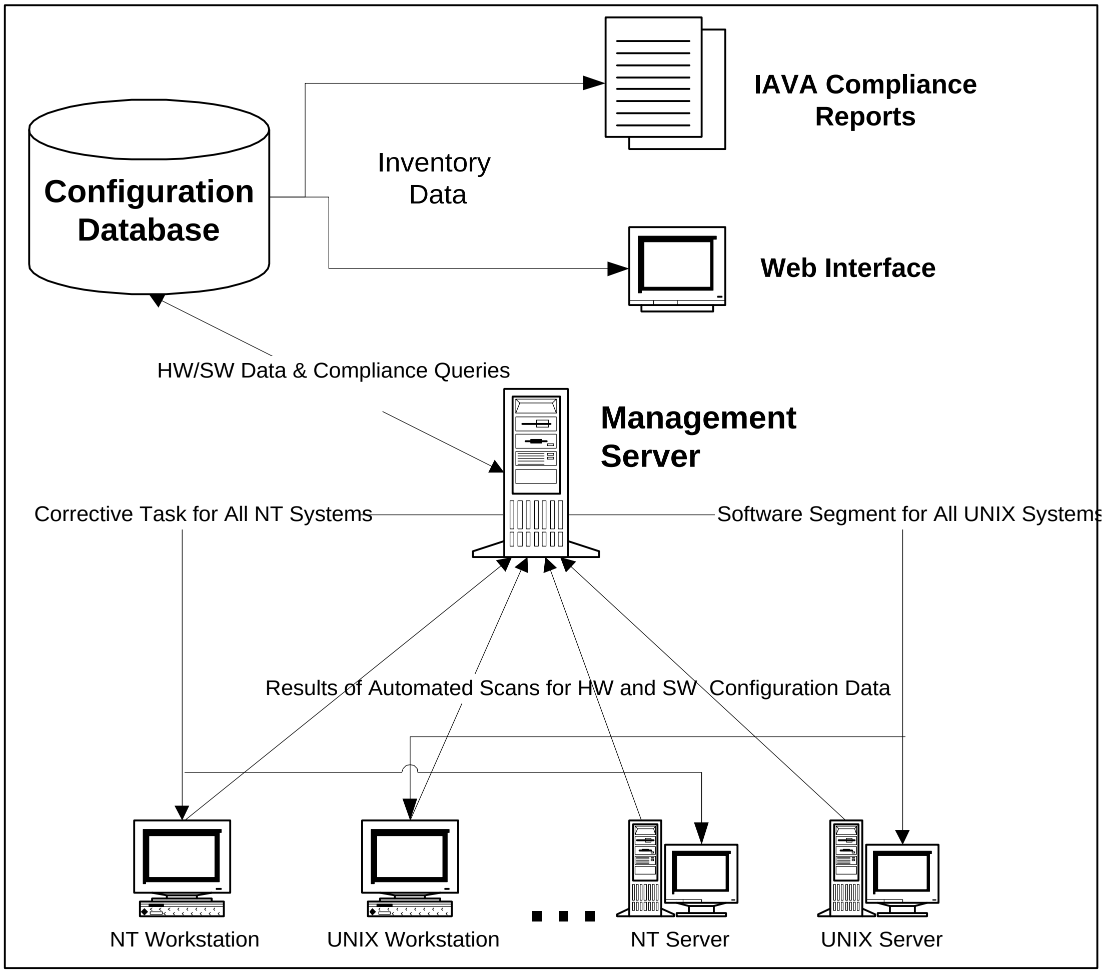
Personnel in the NCCs can vary from highly trained (e.g. someone with years of experience on the system) to novice (e.g. someone who came from a PC background and is now responsible for UNIX administration on the GCCS). The systems they manage range from Windows NT desktops to UNIX servers running Government-Off-The-Shelf (GOTS) applications to Oracle databases storing critical information. In short, they are heterogeneous and complex.

Ultimately, the IAVA process depends on a local resource taking technical action to identify and correct security holes. Clearly, if the local administrator is not able to do this in the most accurate and timely way possible, the IAVA process is either unsuccessful or may merely present a false sense of security. The following steps should be added to the local administrator's process. Each of these steps depends on the addition of Commercial-Off-The Shelf (COTS) management tools:

- **Collect and store hardware and software configuration data** – Regular system scanning can be performed to gather system configuration management or CM data (e.g., version of software installed, type of hardware devices in use, etc.). When stored in a database, CM data can be quickly accessed for comparison with new IAVA notifications and for compliance report generation. Instead of inspecting each machine to determine its OS patch level, a configuration database could be queried in minutes to produce a valid report of all systems at risk.
- **Maintain a set of IAVA compliance reports** – Each systems manager should have the ability to quickly produce a report that describes compliance levels with all previous IAVAs or with a specific IAVA. This will decrease the time required to report on risk levels and provide an efficient means of regularly assessing security validation.
- **Maintain and utilize a collection of IAVA corrective tasks** – The corrective actions for many IAVAs can be automated through graphical tasks. Local personnel should execute these tasks to correct vulnerabilities. Instead of correcting problems via a set of complex system commands on each individual machine, graphical tasks would allow a less experienced technician to correct multiple systems in parallel.

- **Utilize an automated method to perform software installation** – The local administrator can utilize graphical management tools to quickly apply software patches or upgrades to multiple, remote systems. This process would decrease the time currently required by manual steps and would ensure that software modifications are standardized across the enterprise. The software distribution tools will also enable less experienced personnel to install and remove applications.
- **Utilize an automated method of deploying new systems at current operating system and patch levels** – System management tools can more rapidly deploy new systems at the appropriate software revision levels. The newly deployed systems can also automatically be scanned and maintained for CM data within the inventory database.

The figure below shows how management tools can be added to a NCC to streamline the IAVA process.


IAVA Compliance Reports
Configuration Database
Inventory Data
Web Interface
HW/SW Data & Compliance Queries
Management Server
Corrective Task for All NT Systems
Software Segment for All UNIX Systems
Results of Automated Scans for HW and SW Configuration Data
NT Workstation
UNIX Workstation
NT Server
UNIX Server

CINCs/Services/Agencies

Each C/S/A is dependent on its subcomponents to quickly assess their risk for an IAVA. As their ability to do this improves, the entire IAVA process will become more effective. Assuming the process described above for the Network Control Center is in place, the C/S/A would be able to quickly respond to IAVA notifications and accurately assess the associated risk.

An economy of scale would be reached when the entire C/S/A agrees on a set of management tools for the process. These management tools would be implemented across the organization to ensure that each subcomponent has the same ability to secure its resources. The commonality would decrease the amount of integration required to combine information from multiple components and would allow the C/S/A to provide a standard set of IAVA discovery and correction actions for use. The following steps should be added to the IAVA process and performed by the C/S/A. Each step assumes that a common set of management tools is used across all subcomponents and that the functions described above for the NCC are ongoing.

- **Maintain a C/S/A-wide configuration database –** Once the local administrators are collecting and storing configuration data, the C/S/A should maintain a composite database. This would be made up of a subset of data from the local level and would provide instant access to compliance data.
- **Maintain a set of standard C/S/A-wide compliance reports –** The C/S/A configuration database would allow the C/S/A to quickly produce compliance reports and assess risk.
- **Develop standard tasks for identification and resolution of IAVAs -** The C/S/A should maintain a center of excellence that has access to and expertise in the chosen management tools. This center would assess the risk associated with a given IAVA, develop standard tasks to identify and, where possible, develop standard tasks to resolve IAVA vulnerabilities. These tasks would be developed and tested for the use with the standard management tools and distributed to ensure that local administrators can quickly and accurately eliminate vulnerabilities.
- **Develop standard software packages for distribution by local administrators** – Where applicable, the C/S/A should develop and test software packages that can be distributed to remote systems to resolve IAVA notifications. This software package would enable administrators to upgrade multiple systems in parallel.

DoD CERT

In this streamlined IAVA process, DoD CERT would function in much the same manner it does currently. Its mission would still be to identify security threats to DoD systems, categorize these threats, disseminate the information to C/S/As, and to provide consolidated reports on the compliance and risk of DoD systems. The difference would be in the organization's ability to provide compliance reports that are both more accurate and expedient. The result would be greater security for this nation's critical IT resources.

Benefits

Simply put, combining COTS management tools with the current IAVA process would decrease the risk DoD systems face from vulnerability exploitation. The current process provides a solid framework for vulnerability announcements and reporting, but does not help the local administrator verify and correct the security configuration of their resources. The environment described above would aid both the local technician and the high level commander. Complementing the current process with management tools would have the following positive effects:

- Decrease the time *and* expertise needed for local administrators to identify systems that are vulnerable to specific IAVAs.
- Enable administrators to apply standard fixes to hundreds of systems in parallel; therefore, decreasing the time these systems are at risk and saving precious time of administrators.
- Allow commands to maintain a database of their systems' hardware and software configuration for quicker risk assessment and compliance reporting.

- Increase validity of reported risk levels and compliance levels – allowing senior leaders to make more educated decisions.
- And above all, minimize risk to information vulnerabilities.

Tivoli Solution

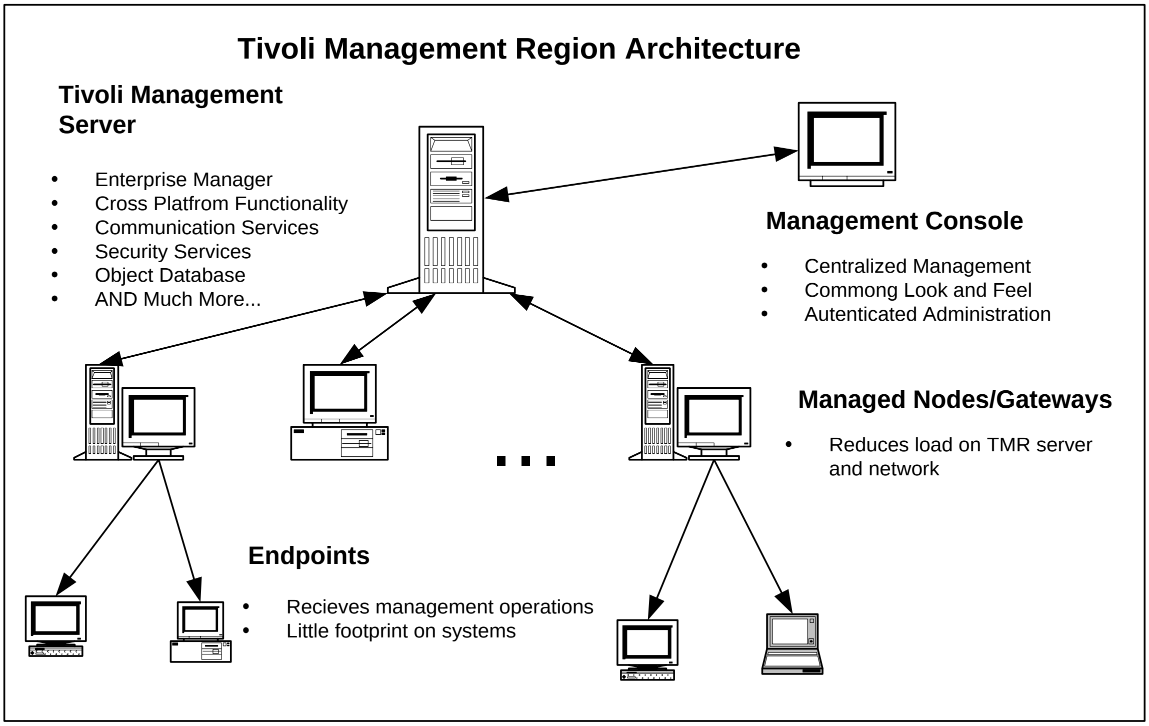
Trinity Solutions believes that the best set of commercial management technologies for the IAVA process is the Tivoli Enterprise suite of products. Both government and commercial customers have successfully deployed Tivoli Enterprise and seen an increase in both the availability and performance of their systems and a decrease in their operational costs. This section describes three of the essential sets of Tivoli Enterprise products relevant for improving IAVA and offers a high level architecture and description of each.

Product Description

Tivoli Management Framework

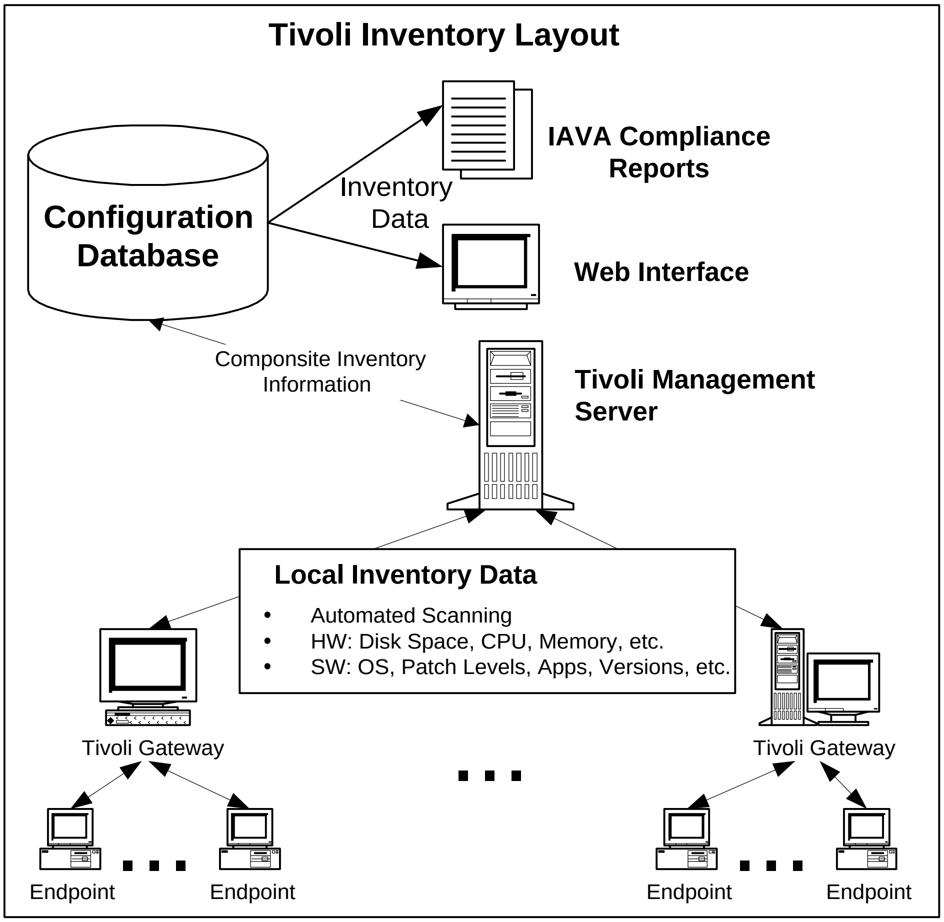
Tivoli's Framework contains a database of management actions and policy, communications services used with the Tivoli Management Environment (TME), a graphical user interface, and other services that are used by subsequent Tivoli modules. It is important to note that the Tivoli Framework will provide functionality that can be used in the IAVA process and in other management domains. For example, the Framework allows administrators to model custom scripts in graphical tasks that can be quickly re-used by other administrators. These tasks could be used to perform various IAVA operations such as checking for a specific vulnerability or to perform other administrative functions (e.g., restarting print servers, removing core files, checking JOPES send queues, etc.).

The following diagram illustrates the Tivoli Enterprise architecture. The architecture is designed to allow administrators to perform operations on multiple heterogeneous systems by using a common interface from a centralized location.



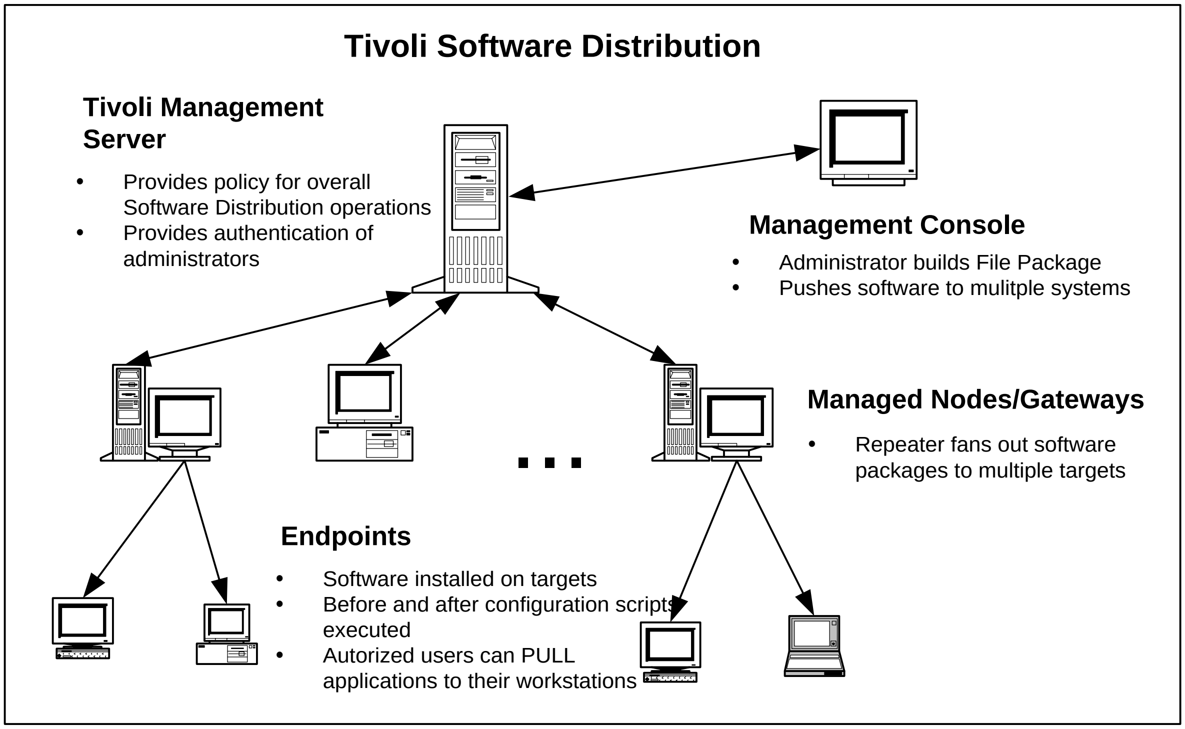
Tivoli Inventory

The Tivoli Inventory module provides automated and scheduled hardware and software inventory collection in an IT enterprise. Inventory data can be collected from UNIX, Windows, OS/390 and NetWare platforms and then stored in a Relational Database Management System (RDBMS). The product utilizes the TIVScan distributed scanning technology to ensure that all system information is collected and the WAN-Smart data collection method to conserve network bandwidth. The diagram below illustrates the Tivoli Inventory architecture.



Tivoli Software Distribution

The Tivoli Software Distribution module provides automated and scheduled distribution and installation of software. Software Distribution is a key for organizations that need to deploy software applications across large, complex enterprises. Software Distribution provides a graphical method for more junior level administrators to deploy software to multiple locations, reducing expertise and time required and, therefore, saving money. Software distribution can use the Inventory data to dynamically build the list of systems to distribute software based on hardware or software requirements. The use of repeater systems decreases the load on network resources. The following diagram illustrates Tivoli Software Distribution.



Tivoli Software Distribution

Tivoli Management Server

- Provides policy for overall Software Distribution operations
- Provides authentication of administrators

Management Console

- Administrator builds File Package
- Pushes software to mulitple systems

Managed Nodes/Gateways

- Repeater fans out software packages to multiple targets

Endpoints

- Software installed on targets
- Before and after configuration scripts executed
- Autorized users can PULL applications to their workstations

It is important to note that there are many other applications in the Tivoli Enterprise suite. These applications utilize the framework and provide added management functionality. Local administrators who have access to the Tivoli framework for the IAVA process would be able to choose additional Tivoli Enterprise applications such as Distributed Monitoring, User Administration, and more. This would give them even greater control over their IT resources and save them time and operational costs.

Benefits of Tivoli-Based Implementation

The Tivoli Enterprise solution has a number of unique benefits to the IAVA process that separate it from other management tools. This section briefly describes these advantages.

Successful Deployments by DoD Organizations

The Tivoli suite of products has been successfully deployed and is in use by a number of DoD organizations. These organizations have a core set of knowledge in both the configuration and operation of Tivoli applications. The knowledge they have gained could be leveraged should Tivoli Enterprise be chosen as a common IAVA management tool. The result would be a faster time to implementation and a lower cost of integration since other management tools would have to be integrated with existing Tivoli implementations. Some examples of organizations and programs utilizing Tivoli Enterprise include: DISA, Air Force Materiel Command (AFMC), Defense Intelligence Agency (DIA), Army Network and Systems Operation Center (ANSOC), and more.

Successful Security Test and Evaluation by the NSA

In the spring of 1999, the Joint Staff Support Center (JSSC) worked with the National Security Agency (NSA) to verify the security configuration of the Tivoli Enterprise products. The test was successful and showed that the products can increase the security configuration of a mission-critical system (the Global Command and Control System). As a result, the JSSC received Joint Staff approval to install and configure Tivoli products on GCCS resources at the National Military Command Center (NMCC) and Alternate National Military Command Center (ANMCC).

Industry Leading Product Attributes

Tivoli is recognized as an industry leading network and systems (or “enterprise”) management product suite. Over 75% of commercial companies with annual revenues of a billion dollars or more utilize Tivoli products. The three Enterprise products described above have many technical characteristics that set them apart from the competition.

- Cross platform functionality
- Common GUI between products and operating systems
- Centralized or decentralized management
- Reduces complexity
- Ensures standardized management
- Multiple administrators can perform multiple management tasks in parallel
- Secure authentication of administrators
- Policy-based management and ability to delegate administration by roles/privileges
- Scaleable to large enterprises
- And many more…