Deploying Enterprise Management in Tactical Networks

Michael Martone
Booz·Allen & Hamilton Inc.
151 Industrial Way East
Eatontown, NJ 07724

Andy Wyckoff
Booz·Allen & Hamilton Inc.
151 Industrial Way East
Eatontown, NJ 07724

Enterprise Management (EM) has become a big part of industry Information Technology (IT) focus. It is being implemented in large and medium-size corporations and being tied to the business processes. The US military has both similar issues to corporate IT infrastructure, and unique tactical requirements. EM technology and best practices from industry deployments can be leveraged to improve tactical operations and IT deployment. This article describes how EM technology deployed in tactical infrastructures can help avoid increasing personnel while adding new systems and capabilities, reduce training costs, and decrease the level of knowledge and experience an operator requires to maintain the tactical infrastructure. There is a description of how EM technology can specifically improve the areas of network management, systems management, software distribution, inventory/configuration management, troubleshooting, user administration and security in a tactical environment.

Definition of Enterprise Management

Enterprise Management is policy-based management of the entire IT infrastructure. This includes telecomm networks (i.e. voice), servers, mainframes, applications, databases, and desktops. Enterprise Management is being implemented in commercial corporations, the Federal Government, and in DoD sustaining base installations. Enterprise Management changes the paradigm from stove-piped functional management (e.g., network management, systems management, etc.) to comprehensive, consistent solutions for managing an integrated enterprise. They provide a common underlying data object repository, as well as a common GUI.

EM Functional Areas

The key functional areas of EM include:

- Inventory & Asset Management
- Software distribution
- Security and User administration
- Remote control of desktops
- Distributed monitoring of systems, applications, and databases
- Fault management with rules-based event correlation.

There are other functional areas associated with EM that are more applicable to sustaining base situations including help desk operations, archive management, and others. This paper focuses on the first six functional areas as they would have the greatest impact in a tactical deployment.

The inventory function allows a system administrator to view and record hardware and software installed on remote systems. This will allow a complete baseline of the tactical network and its components to be maintained. It will allow an administrator to determine if any configuration changes have been. Inventory queries can be developed that look for assets or conditions which correspond to very specific criteria. For example, a tactical application may have been upgraded with a

0-7803-5538-5/99/$10.00 © 1999 IEEE

mission critical feature. This upgrade may require a certain amount of memory available on each server in the tactical network. An inventory query can be performed which identifies all servers without adequate memory, and start actions required to install that memory upgrade to those specific machines.

These queries can be performed by an operator trained only in the use of the enterprise management framework. The different operating systems become transparent to the individual performing the query. The inventory task can be performed across echelons or applications if needed, allowing the inventory function to be performed by a single individual. This will significantly reduce training requirements.

Enterprise Management will allow software to be automatically distributed, installed and updated across a network. Software distribution can also be subjected to which define the appropriate set of conditions under which the software should be installed for targeted devices. As in the previous example, one could distribute a new application only to machines which have sufficient memory available. EM frameworks can be used to distribute the various segmented components of Defense Information Infrastructure (DII) Common Operating Environment (COE). As upgraded software components are shown to be DII COE compliant, they can be distributed to the tactical applications and systems.

User administration functions can be functionally organized versus application specific. Access to data and applications for all users within the tactical network can be controlled by a single interface. EM frameworks allow system administration tasks to be performed in a consistent manner, without the need to learn the specifics of each application or operating system employed within the network. This reduces training cost and enforces consistent security policies across all applications within the tactical network.

EM Frameworks provides the capability for remote control of operator consoles, desktop systems, servers, and distributed applications over the tactical network. Specific technical expertise can be brought directly to the warfighter, and mission critical resources can be brought on line from a centralized location.

Distributed monitoring of tactical network resource and services provides valuable information about the health of the network. Thresholds for critical parameters can be set. Warnings and cautions can be brought to the attention of appropriate personnel for proactive solutions to network problems prior to failure.

Management messages and alarms come from a variety of sources within the tactical network.. Event correlation and root cause analysis is accomplished by a rules-base which takes automated action in accordance with policies established for the network. This significantly reduces troubleshooting time and the skill level required to resolve the problem.

Enterprise Management Benefits

EM can bring many advantages even to tactical networks. These benefits include reduced training and required skill levels, consistent management framework for all systems and communications, reduced troubleshooting time and notification of problems, automation of maintenance procedures, and enforcement of policies.

Tactical Issues

Unlike most sustaining base infrastructures, tactical networks have specific issues related to the battlefield environment. These include:

- Mobility and re-affiliation
- Security
- Low bandwidth links (i.e. < 56Kbps)
- Unreliable/intermittent links

Many tactical network users, as well as the network itself, are mobile and change position. This may result in accessing the network at different physical points, even during the same data conversation (e.g. FTP session). Also, the user may change affiliation (e.g. IP address, host name, role) and subsequently there will be a change in the Tactical DNS and possibly the configuration of the computer or application(s).

Security, of course, is an important concern in a military network. In addition to standard computer security issues there are multiple security classifications (e.g. SBU, Secret) that are managed separately, and security mechanisms such as firewalls.

Most of the links in the tactical environment have actual throughputs of less than 56Kbps. In addition, these links are in high contention due to digitizing the battlefield, thereby reducing the amount of traffic any individual application or user can access. This limits the amount of bandwidth that should be used for managing and maintaining the network.

Many of the tactical communication links are wireless (e.g. LOS, UAV, etc.) and subject to atmospheric interference, ECM, and adjacent radio interference. This increased Bit Error Rate reduces the actual throughput of data. Also, as units move and create ad-hoc network enclaves certain communication links may temporarily or permanently disappear.

Current EM Solutions to Tactical Issues

Enterprise Management Frameworks have capabilities to distribute software while managing the limited resources available of the tactical Wide Area Network (WAN). These capabilities include fan-out for parallel distribution, staging, network bandwidth tuning and throttling, difference-based distributions that transmit only changes, and compression. This approach makes distributions fast and efficient, enabling them to take optimal advantage of network bandwidth. For example, you can efficiently fan-out software over Windows NT and UNIX servers using the IP protocols to tens of thousands of client systems with a single management action. You can use robust scheduling capabilities to take advantage of network capacity fluctuations and specify the number of automatic retries.

Enterprise Management Frameworks can address scalability and bandwidth issues by employing a multi-tiered architecture. The operator consoles and servers are endpoints managed by the Enterprise Management framework. They receive software distributions, execute tasks, run monitors, and send events. Gateways performs all communications with assigned endpoints without requiring additional communications with the Enterprise Management server. An endpoint manager establishes and maintains the relationship between an endpoint and a gateway and is automatically created on the Enterprise Management server during server installation.

The chief advantage of endpoints is scalability. Each gateway can manage thousands of endpoints, and each Enterprise Management server can manage hundreds of gateways. As a result, you can gather required management information from thousands of endpoint machines and remotely manage those machines with very little overhead. Also, because an endpoint installation typically requires less than 1 MB of disk space, endpoints consume few computer resources. After the initial installation process, all endpoint communications are handled by a gateway, instead of the Enterprise Management server. Shifting a share of the management processes to the gateway reduces computing demand on the Enterprise Management server.

Protecting tactical network resources is critical to mission success. Heterogeneous platform security has always been a difficult challenge, requiring detailed security knowledge of all platforms in use, constant system monitoring, application of vendor patches to newly discovered breaches, and contin-

ual editing of configuration files. Enterprise Management Frameworks provide comprehensive solutions to the prevention of attacks to systems. The primary goal of security management is to provide an open solution for role-based distributed client/server security management. Enterprise Management Frameworks incorporate, integrate, exploit and extends the best aspects and features of systems management and application-specific security products. They provide centralized role-based security administration across many types of UNIX systems and the NT operating system.

Summary

Current COTS implementations of EM software address many of the unique management problems of the tactical infrastructure. There are however, some areas which still require more development, such as security. Also, some issues will need to be addressed not technically, but from an operational and policy-level. The EM framework can also be integrated into other areas of technology and policies including Information Assurance and C2 Protect.

One of the keys to successful application of an EM framework is to define an implementation strategy based on high level policies and lower level requirements. It is estimated that over 70% of EM implementations have failed; and the number one reason for these failures has been improper strategy planning and execution.

A properly implemented EM system can provide many benefits including reduced troubleshooting time and automation of maintenance activities. Many of the previous problems associated with managing a tactical infrastructure such as mobility, security, and lack of bandwidth can be addressed to a greater extent today with EM technology than ever before.