A Multi-tiered Approach to Enterprise Support Services*

Coimbatore S. Chandersekaran and William R. Simpson

Institute for Defense Analyses, 4850 Mark Center Dr., Alexandria, Virginia 22311

Abstract. The Enterprise Support Desk (ESD) is the combination of people, hardware, deployed software agents, and software displays, which maintain the health of the enterprise service based operations. It is both pro-active and re-active. It is required to be integrated with hardware and software health monitoring systems deployed by the enterprise services provider. The objective of this paper is to provide the basic architecture being employed by the USAF enterprise system.

Keywords: Help Desk, enterprise, support services, information sharing.

1 Introduction

The Enterprise Support Desk (ESD) is the combination of people, hardware, deployed software agents, and software displays, which maintain the health of the enterprise SOA operations. It is both pro-active and re-active. It is required to be integrated with hardware and software health monitoring systems deployed by the Area Processing Center (APC) or enterprise services provider. The ESD attempts to resolve 90% of customer issues within 20 minutes, and average less than 15 minutes resolution for all issues. The ESD in this case consists of four basic levels and three separate groups:

1. Level 0: Client Self-help. Assistance is provided to the client in the form of Knowledge Repository (KR) access, frequently asked questions (FAQ), and diagnostic software. Failure to resolve issues at this level leads to a call to the help desk.
2. Level 1 - customer support and help desk. A client may ask for assistance through a help desk phone number, e-mail, or web form entry. This is the unit that will develop a Trouble Report (TR) and see most through to completion.
3. Level 2 – Proactive monitoring of services. This unit will monitor network activities and the performance of services using a testing tool, and a series of embedded agents. This level will assist level 1 when resolution of help desk requests has not been completed at that level. It may also generate TRs before clients call to report problems.

* The publication of this paper does not indicate endorsement by the Department of Defense or IDA, nor should the contents be construed as reflecting the official position of these organizations.

A. Marcus (Ed.): Design, User Experience, and Usability, Pt I, HCII 2011, LNCS 6769, pp. 388–397, 2011.

4. Level 3 – Active monitoring and security. This unit will monitor all security alerts sent by agents and based upon heuristics developed within the enterprise will perform remote desk audits and dispatch a security monitoring team for physical audit of indicated desktops. This level will assist level 1 and level 2 when resolution of help desk requests have not been able to resolve the issue.

In order to facilitate all three units a series of agents on desktops and service machines, a knowledge base system, display work stations, and alert policies are needed. These requirements are varied and must be integrated with hardware and operating system health monitoring data. For this reason, all three units will use service monitoring software, which is flexible, configurable, expandable, and adaptable to include information from health state monitoring activities. Further, every desktop or laptop within the Air Force Enterprise will have embedded agents for self help and repair of common problems as well as software (TBD) that will allow ESD principals to take control of the hardware unit for the purpose of auditing hardware and software configurations and provide troubleshooting assistance. Figure 1 shows the architecture of agents for the services management. There are separate agents for hardware health monitoring and two types of agents for each service. The first agent is embedded in the service itself for provision of alerts and internal logging of service data. The second agent is installed on the server and provides a sweep of log files, either periodically or on demand. At least one vendor (Amberpoint) [21] provides both such agents.

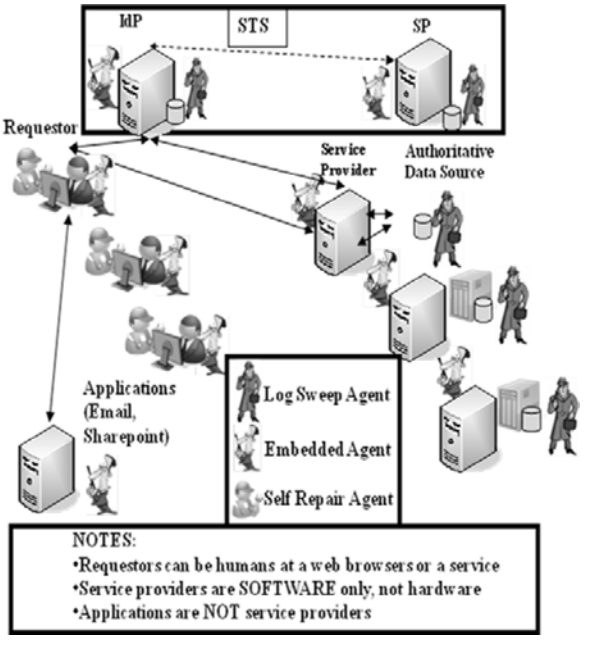

Fig. 1. Deployed Agent Architecture

Each Unit will have an administrator present with specific duties. Each shift will have such an administrator and the team of administrators will meet at a frequency dictated by events to review operations and to modify or create heuristics for ESD usage. Administrator privileges are required for certain tasks. All ESD personnel must abide by enterprise security policies, including bi-lateral authentication and SAML authorization for access control. Figure 2 illustrates how these units work with the monitored data.

2 The Knowledge Repository

The knowledge repository (KR) is a single integrated source of all information on the operation of the enterprise. It will be updated by all three units within the ESD and accessible to all three units within the ESD. Instrumented agents feed the data base on a schedule or on demand. This subsection deals with information requirements for the Unit 2 ESD (SOA Monitoring).

3 Information for SOA Monitoring

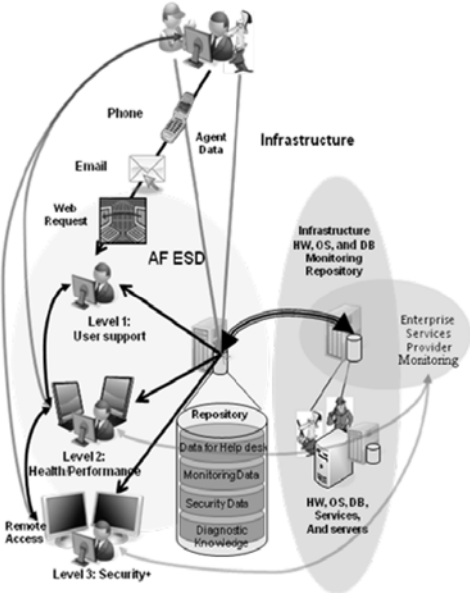

Fig. 2. Support Desk Operations

The knowledge base is where all information related to the enterprise SOA is stored. This will include the following:

- Hardware / software current status from DECC or APC
- Current reports on test activities including response times, frequency of test, etc.
- Current reports of usage data from service agent monitors and service logs, including number of users, session times, response times, etc.
- Hardware / software historical data
- A list of current alerts for the entire enterprise
- Historical data on alerts.

4 Customer Support and Help Desk

After initial self help is unsuccessful, the client will turn to the helpdesk. There are three levels of service provided. Level 1 will be the entry point to the system. At this level a client will call the helpdesk about a problem or other issue. The helpdesk assistant will collect some information, such as name, address, rank, SSN, etc. from the client, verify the client's identity, and attempt to quickly solve the issue using a pre-defined script and access to the KR. If this does not resolve the issue, it is categorized and escalated to the appropriate level (level 2). At level 2 a knowledgeable person will go through a more detailed script to collect information from the client and use the agent based monitoring process to gain more detailed

information about the situation. Level 2 personnel will have more access and privileges, allowing them to make changes and attempt to fix the problem. If Level 2 personnel are able to solve the problem, they will close the TR and update the KR with information about the TR resolution. If the issue cannot be resolved by this level, the TR will be escalated to level 3, where in-depth analysis and coding are involved. If this resolves the issue, any code fixes will be pushed to the patch/Configuration Management (CM) team, and a temporary quick fix will be generated for future issues and added to the KR. This describes the basic helpdesk flow in the figures below.

The rest of the section is structured as follows:

- Levels of service
- Identity Verification System;
- Trouble Report Management System;
- KR System;
- Error reporting;
- Administrator duties, and
- Trouble report scenarios and data requirements.

Details of the agent-based architecture are complex and discussed in a separate paper [20].

5 Levels of Service

As previously described there are four basic levels of support, and three basic units or groups to assist in that support.

5.1 Level 0: Client Self-Help

Before executing the well-structured Help Desk Levels, there is a loosely defined "Level 0," which refers to the client's ability to solve their own issues through the KR or other means. The KR is primarily a helpdesk resource. By developing a culture within the client base of first checking the KR when an issue is encountered, this can further act as a filter, reducing the load on Level 1. The relationship of levels is shown in the next three figures

5.2 Level 1: Basic Information

Level 1 is where most of the TRs are created. All helpdesk requests will be recorded in a help desk TR. The Level 1 operator will follow a simple script, which will involve collecting basic information from the client, entering it into a TR, and creating the TR. At this point, the operator will start to address the client's issue. If the issue is resolved, the method of resolution will be entered in the TR. Often this will involve listing a link to the KR article that helped resolve the issue. Other times, it will be an operator text entry based on information personally provided to the client.

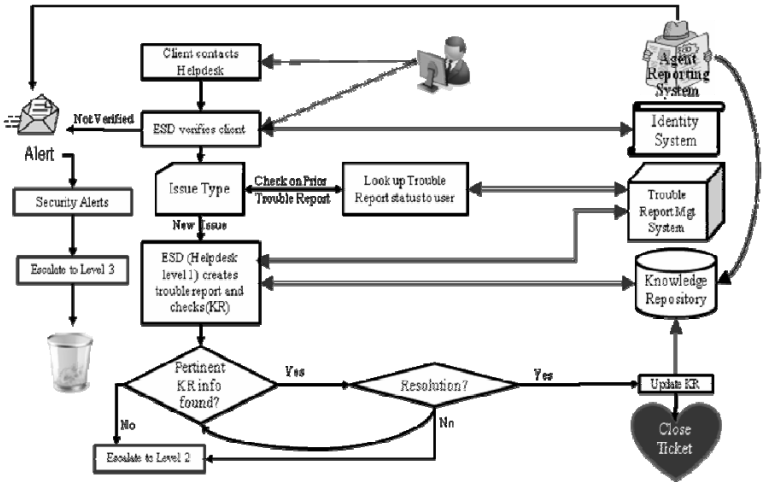

Fig. 3. Help Desk Level 1

This process ensures that all interactions are logged appropriately. An issue that is resolved quickly by a link to the KR is important to document. This provides positive feedback to the higher levels that create and maintain these KR articles. A high frequency of access can indicate that this is an important issue that clients need to understand. As a result, a more client-friendly KR article might be created to reduce call volume to the helpdesk or an enterprise-wide memo might be released addressing the issue. If the article addresses a bug and its workaround, a high access rate might indicate that this is a high priority for a permanent fix. In any case, the proper documentation of client requests, even for seemingly trivial issues, is an important part of the role of Level 1 operators.

In addition to the KR, Level 1 has access to basic live feeds from Units 2 and 3 of the ESD. These feeds indicate the current health, performance, and security situation of the network, and also include hardware and OS failure information. This feed is one-way, providing current information to the Level 1 operators. This information is intended for use when there are significant network issues. If a client calls and asks about a slow connection, this feed could provide a quick answer for that client if there is significant network traffic at the time. The TR could then be closed without escalation by verifying that Unit 2 knows about the issue and is working to fix it.

Not all issues will be resolved by a KR article link at Level 1. For more difficult problems and problems that require an administrator or other access, the TR is escalated to Level 2. Responsibility of the TR is passed to someone in Level 2, and Level 1's obligations for that TR are complete.

5.3 Level 2: Interactive Support

When a TR is escalated to Level 2, it is first scanned to determine the general issue. Although all operators in Level 2 are trained and capable of resolving issues, there will be some areas of expertise that people or levels develop within Level 2, so matching the problem with the person or group addressing it will be helpful for

certain types of TRs. When someone has taken ownership of a TR, they contact the client by phone to authenticate them, confirm the information collected by Level 1, and collect more detailed information to address the issue. This interaction follows a script much like Level 1, but it is more detailed in terms of the authentication steps and the information collected. Level 2 operators all have the ability to remotely access a client's desktop. This is provided by agents running on the clients' desktops, which is part of the AF standard desktop configuration. If needed, the Level 2 operator will access the client's desktop, collect information directly from their desktop, and make changes to the client's desktop. Examples of changes would be software updates, installation of certificates or other security-relevant information, or removal of unauthorized device drivers or other software. All authorized software will be signed and certificated, so detection of unauthorized code should be easily accomplished by an automated scan.

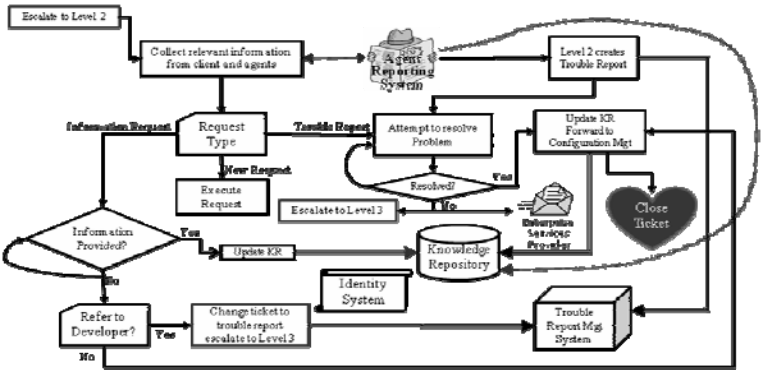

Fig. 4. Help Desk Level 2

The level of expertise at Level 2 is very high. The baseline training for Level 2 operators provides them an ability to resolve almost all issues faced. Specialized training for certain specific issues may be limited to a smaller group within Level 2, but this group will be consulted or given the TR when appropriate. Such specialized training might be for key services, such as the STS, MDE, or AD. Although the issues addressed might be difficult to diagnose and fix, by having these specialized groups within Level 2 for the most common problem area it is possible to avoid the very costly escalation to Level 3. However, sometimes there is just a fundamental problem with the code, either enterprise code or vendor code, or there is a fundamental architectural problem that must be changed, perhaps at the service provider facility not accessible directly from Level 2. In this case, the issue is escalated to Level 3 and/or sent to the service provider.

5.4 Level 3: Security, Serious Bugs and Vendor Support

Level 3 is not as well-defined as Levels 1 and 2. It consists of a collection of developers, security experts, architects, and vendor support channels for all COTS software and hardware. These experts are typically very costly to utilize, but their

expertise and skills can resolve any issue, if properly diagnosed and allocated to them. The goal of the ESD is to address all TRs at the lowest level possible. Essentially, Level 1 acts as a filter to weed out all issues that are a waste of Level 2 resources. Level 2 acts as a further filter to weed out all issues that are a waste of Level 3 resources.

Level 3 does not actually take ownership of any helpdesk TRs. The one exception is security TRs opened by Level 3. The level 3 administrator, in consultation with other level 3 SMEs, may decide to call a Computer Security Incident Response Team (CSIRT) and is responsible for managing this team in its work. Level 3 is contacted by Level 2 when there is a serious issue to resolve, but Level 2 maintains ownership of the TR. Level 3 is treated more like consultants that the Level 2 operator can call on to solve serious problems. Although the TR does not change hands, the Level 2 operator contacts the client before escalating to Level 3 to inform them that their issue is more serious and may take some time to resolve. Level 3 issues are expected to take days or weeks to resolve instead of the minutes or hours expected at Level 1 or Level 2.

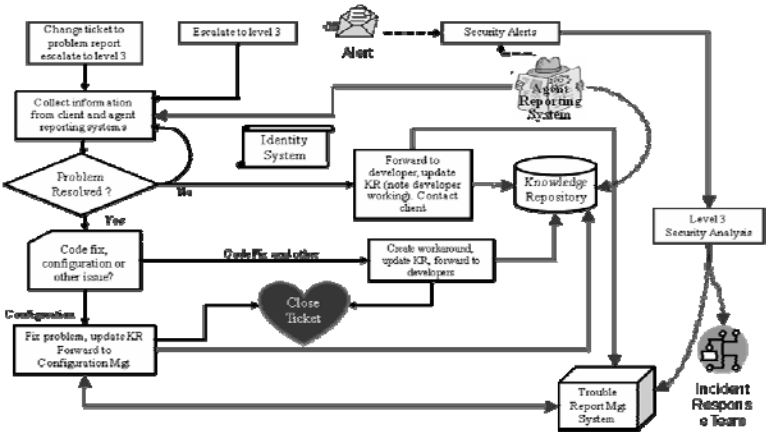

Fig. 5. Help Desk Level 3

6 The Knowledge Repository (KR)

The KR is a single integrated source of all information on the operation of the enterprise. It will be updated by all three units within the ESD and accessible to all three units within the ESD. The KR consists of a data base, and tools to import and categorize agent based data, as well as tools for search and discovery. The KR is access controlled at all levels.

6.1 Information for Help Desk Operations

The KR is where all information related to TRs is stored. This will include the following:

- Hardware/software current status from the service provider
- Hardware/software historical data
- A list of current alerts for the entire enterprise
- Historical data on alerts
- Reference material for all hardware components
- Reference material for all software components
- Reference material for all protocols and standards
- Configuration information
- All closed TRs
- All reference material that closed TRs link to
- Articles useful for setting up HW/SW, troubleshooting, etc.
- Frequently Asked Questions (FAQs)

Configuration information will consists of the standard desktop configuration, service configuration, infrastructure component configuration, and any other hardware, software, protocol, or standards settings or choices that have been established across the enterprise.

Closed TRs will be available in the KR. This will allow the helpdesk to search for similar TRs and use past experience to aid with current issues. Every TR will be added to the KR when it is closed. Access to these closed TRs will be discussed, since this is a potentially sensitive area. However, for now, it is sufficient to note that all closed TRs will be in the KR and available to someone, if not everyone.

In addition to closed TRs, any other documents referenced by the TRs should be included in the KR. Articles written internally by the ESD or other entities within the enterprise will be added to the KR if they would be useful for ESD activity. FAQs will be established and Configuration information will consists of the standard desktop configuration, service configuration, infrastructure component configuration, and any other hardware, software, protocol, or standards settings or choices that have been established across the enterprise. This includes the choice of which ports to open or close, when to use the various WS-* protocols, and which services should run at startup on a Windows Vista machine. For hardware, software, protocol, and standard elements there are an associated set of configurations and settings.

Closed TRs will be available in the KR. This will allow the helpdesk to search for similar TRs and use past experience to aid with current issues. Every TR will be added to the KR when it is closed. Access to these closed TRs will be discussed, since this is a potentially sensitive area.

In addition to closed TRs, any other documents referenced by the TRs should be included in the KR. This should be done not when the TR is closed but when the links are added to the open TR. The data should be added to the KR, then the link should be established, and then when the TR is closed the data and link are already there, so no additional work needs to be done. External links (web sites, etc.) will be captured in some way (like a Google cache) so that access is assured even when network connectivity is limited.

Articles written internally by the ESD or other entities within the enterprise will be added to the KR if they would be useful for ESD activity. FAQs will be established and probably be used when searching for general information on a topic, which might

include KR data as well as other information. The KR search will be more for clients contemplating starting a TR or ESD/ESU personnel who want specific information for an existing TR.

Different levels of access will be established. These would correspond to different groups and roles that determine KR access. For TRs, the following levels are defined:

1. No closed TRs are viewable by callers
2. Callers can only view their own TRs
3. All TRs without any sensitive information are visible.
4. All TRs are visible (exception – security sensitive TRs), but fields designated sensitive blanked out
5. Everything is visible

The ability to update the KR will be restricted to level 2 and level 3 personnel. Level 1 is essentially a firewall for these people, weeding out all the previously solved and documented issues. Because of this, level 1 will only read the KR, much like the enterprise clients. When a new issue is found that cannot be addressed by the existing KR information, it is resolved at level 2 or level 3. After this issue is resolved, the level 2 administrator writes enough information in either the TR or a KR article so that the issue can be discovered in the KR and resolved by level 1 support the next time it happens.

For example, if a specific configuration must be used to access a particular new service, level 2 will field all calls relating to this issue until a KR article is added or the prior TRs provide enough information for level 1 to solve the problems. As new issues are discovered, the level 2 people will continue to resolve them and add more information to the KR. Eventually, a client attempting to access the service will find a wealth of information either through reading articles specifically about configuration for the service or through reviewing closed TRs with similar problems.

The main goal is to solve problems as few times as possible, since every level an issue is escalated is more costly than the previous one. The most preferable is for clients to solve their own problems through KR articles. When this is not possible, level 1 tries to resolve it. If it is a new issue, level 2 must address it. If it is a fundamental change, level 3 will be involved. However, once an issue makes it to a certain level, it should stop at a lower level the next time it arises, since the expert attention provided last time should be documented in a way that the levels below can use it without escalating the issue again.

Although only level 2 and level 3 can update the KR, anyone can suggest something be added to the KR. A simple way to implement this is through a web page, where any client can enter the information for a KR article, submit it to the appropriate group at level 2, and let the people at level 2 review the article and take the appropriate action. This allows people to provide input on issues they may have that do not get addressed by the KR, perhaps because they are low frequency issues or relate to a specific service that a client not in the ESD happens to know very well. The final say is by the level 2 person, though, since they ultimately are the maintainers of the KR.

7 Summary

This paper has presented a multi-tiered approach to enterprise support services. To our knowledge, it is the first full enterprise service support desk that is integrated with the hardware and operating systems of the support provider. These techniques are currently being implemented by DISA and the USAF in the DISA DECC stand-up of the enterprise solution for the USAF.

References

1. Air Force Information Assurance Strategy Team, Air Force Information Assurance Enterprise Architecture, Version 1.25, SAF/XC, April 11 (2008)
2. AFPD 33-3 Information Management, AF Portal Community of Practice: AF Information & Data Management Strategy – Implementation (Policy), http://www.e-publishing.af.mil/
3. COI Primer, AF Portal Community of Practice: AF Information & Data Management Strategy – Implementation (COI Primer)
4. DoD Directive 8320.2 "Data Sharing in a Net-Centric Department of Defense" and DOD Guidance 8320.2-G "Guidance for Implementing Net-Centric Data Sharing", AF Portal Community of Practice: AF Information & Data Management Strategy – Implementation (Policy)
5. Metadata Concept, AF Portal Community of Practice: AF Information & Data Management Strategy – Implementation (Metadata)
6. Transparency Integrated Product Team (TIPT) information and proceedings AF Portal Community of Practice
7. AFMAN 33-223, Identification and Authentication
8. AFMC Supplement 1, AFMAN 33-223, Identification and Authentication
9. CJCSI 6212.01D, Interoperability and Supportability of Information Technology and National Security Systems
10. DoDD 5000.1, The Defense Acquisition System
11. DoDD 4630.5, Interoperability and Supportability of Information Technology and National Security Systems
12. DoDD 8000.1, Management of DoD Information Resources and Information Technology
13. DoDI 8115.02, Information Technology Portfolio Management Implementation, October 30 (2006)
14. Joint Concept of Operations for Global Information Grid NetOps, Ver. 3, August 4 (2006)
15. Guide to Secure Web Services: Recommendations of the National Institute of Standards and Technology, NIST-US Department of Commerce Publication (August 2007)
16. Middleton, I.: Key Factors in HelpDesk Success (An analysis of areas critical to helpdesk development and functionality. British Library R&D Report 6247 (1996)
17. Service management solutions White paper Deliver service excellence through the unique advantages of IBM Service Management solutions (September 2007)
18. Farrell, J.A., Kreger, H.: Web services management approaches. IBM Systems Journal 41(2) (2002)
19. Managing Information Access to an Enterprise, Information System Using J2EE and Services, Oriented Architecture, IBM Redbook (January 2005)
20. Simpson, W.R., Chandersekaran: CCCT2010. An Agent Based Monitoring System for Web Services, Orlando, FL, April 2011, vol. II, pp. 84–89 (April 2011)
21. Introduction to Amber Point SOA Management System, Software Manual (December 2007)