Belarc & Microsoft System Center

Belarc's products and Microsoft's System Center (SC) product were designed around very different architectures and for different purposes. In many ways these products are excellent complements to help IT organizations manage their distributed IT assets.

Belarc's BelManage product is a "best of breed" IT asset management system which automates the discovery of software, hardware and security configuration data and automatically creates a central repository of this data. Belarc's Data Analytics module automates the software licensing process, by combining this configuration data with our customer's purchase records and the product licensing rules, to create detailed software licensing reports.

System Center (SC) 2012 has moved from being primarily focused on deploying Microsoft Windows software and patches, to a more general IT management system with eight modules, including App Controller, Data Protection Manager, Operations Manager, Service Manager, Configuration Manager, Endpoint Protection, Orchestrator and Virtual Machine Manager.[1] As a result SC now competes in many arenas and against many different products such as BMC (Service Manager), EMC (Data Protection Manager), McAfee and Symantec (Endpoint Protec-

1 Click here for details on System Center 2012 modules.

tion), and VMware (Virtual Machine Manager), for example. As a result, IT management staff may wish to consider the pros and cons of using a one size fits all approach to IT management, or whether there are best of breed products which have unique benefits and can be cost effectively used in conjunction with System Center.

This paper will focus primarily on System Center Configuration Manager (SCCM), although other modules such as Operations Manager, Endpoint Protection and Virtual Machine Manager will also come into the discussion. The paper will include a comparison of Belarc's and SCCM's architectural differences and the resulting pros and cons, followed by discussions on how both products are used in IT management functions such as software license management, upgrade planning, software compliance, service desk, security audits and more.

SCCM - Traditional hierarchal architecture

SCCM is based on a traditional hierarchal architecture. SCCM requires multiple site servers including Central Administration Site, Primary Sites, and Secondary Sites. Each Site consists of a site server and one or more site system roles, including Management point, Distribution point, Software update point, Fallback status point, Application Catalog points and System Health Validator point. The site server runs the SCCM server and the site systems run the various system roles[2].

Prior to deployment and when networks and systems are reconfigured, IT managers must deal with issues such as site system boundaries, site types and hierarchies based on network bandwidth availability, site system role requirements, and much more. After deployment, each SCCM site typically requires the attention of at least one qualified SCCM Administrator to maintain and administer the system.

SCCM's architecture is based on a traditional hierarchal structure like that shown in Fig 1.

Because the network bandwidth required by SCCM is large, often > 1 MB per client, it requires separate servers and databases for each network or Domain. In order for this information to be available to enterprise IT

2 Site system roles for SCCM include, Site Server, Site Database Server, Component Server, Distribution Point, Management Point, Reporting Point, Software Update Point, State Migration Point, System Health Validator Point, Application Catalog point, Asset Intelligence synchronization point, Certificate registration point, and others. For details, click here.

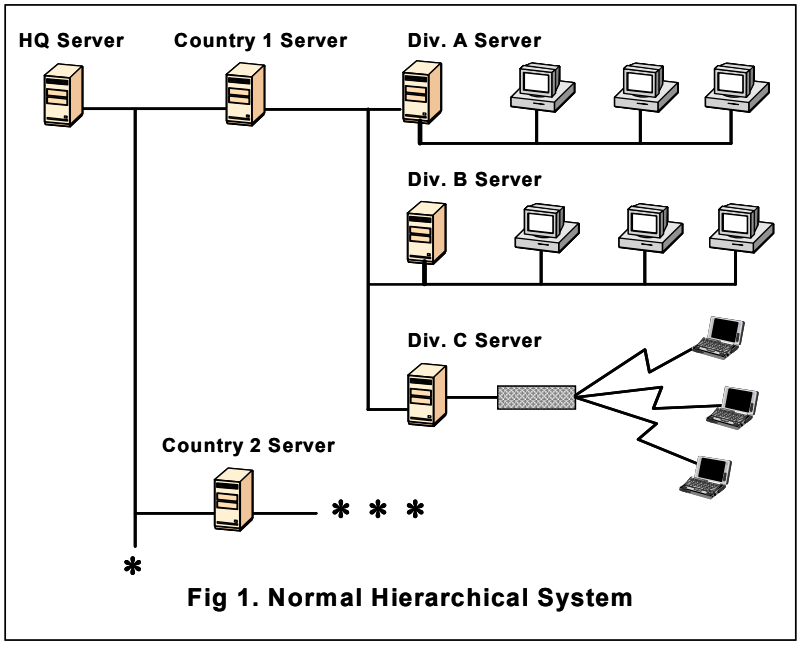

Fig 1. Normal Hierarchical System

personnel, these databases are required to be replicated and synchronized at the next level in the hierarchy and eventually reside on a corporate HQ server. Remote systems create further complications since they require configuration of Internet client servers.

Belarc's WAN Architecture

Belarc's system was designed to operate over the enterprise's WAN. Belarc's WAN architecture is based on lightweight data-gathering agents which use the enterprise's Intranet and requires only one server and a single database (see Fig 2). The agents communicate directly with a single Belarc server, avoiding the need for a hierarchy of servers and replicating databases.

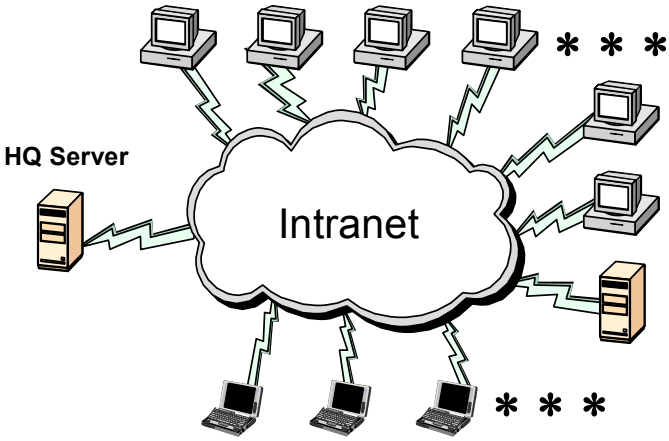

Fig 2. Belarc WAN Architecture

Benefits of WAN architecture

Belarc's WAN architecture allows for very easy system roll out and extremely low ongoing maintenance.[3] This is because there is no need to install and maintain local servers and databases. Belarc's products also use the existing TCP/IP network and standard protocols[4], so that there is no need to manage special router settings across our customer's network. There are also substantial automation features built into Belarc's products which eliminate the need for the manual efforts required by other systems.[5]

Mobile devices are becoming ever more useful and pervasive in today's enterprises. Belarc's WAN based architecture is ideally suited for mobile devices because these devices natively use the WAN to communicate with the enterprise's IT resources. For example, when remote laptops connect to the enterprise network, Belarc's client will automatically

3 The U.S. Marine Corps, who run BelManage enterprise wide on over 120,000 IT assets, on two separate networks distributed throughout the world, require only one-half full time equivalent to run their BelManage system. See Proof Positive section below for details.

4 Belarc's systems use standard protocols, http (port 80) and https (port 443) to upload profiles to the BelManage server. Typical profile size is under 40 KB.

upload their profiles to the enterprise's Belarc server. No additional infrastructure or setup is required.

Another major benefit of Belarc's WAN architecture is that it automatically creates a central repository, or Configuration Management Database (CMDB). Belarc's CMDB is automatically updated, usually on a daily basis, with accurate and complete information. This obviates the need for gathering data from multiple sources as with a federated CMDB approach[6].

Enterprise-wide scalability

A properly designed WAN-based system with instrumented end-points, or agents, can scale to any enterprise's size. What helps make this architecture successful for the enterprise are the following:

- Use of the enterprise's existing Intranet network, which is usually pervasive throughout the organization. This allows configuration data to automatically upload to a central server and repository without the need to manually configure firewalls and routers.
- Small payloads of configuration data. Naturally if an application is using the WAN it needs to be very efficient and limit its use of network resources.[7]
- Efficient database storing and retrieving. With a single central repository actively receiving and storing hundreds of thousands of configuration profiles each day, the repository can become a bottleneck, unless it's properly designed.

---

5 Belarc's automation features are extensive and include the following: automatic grouping based on AD OUs, IP subnets, user names, or any other data in the computer's profile; multiple user types and logins based on need to know; support for CAC/PKI login credentials; control of upload times and statistical spreading of uploading if necessary; automatic profile deletion based on recent upload dates; customized reporting such as software compliance reports, etc.

6 A CMDB is an integral part of the Information Technology Infrastructure Library (ITIL). ITIL is a set of best practice processes to allow organizations to offer high quality and cost effective IT services. For details, click here or here.

7 Each client's profile is typically under 40 KB. While the frequency to upload this to the BelManage server is controlled by the administrator, the default setting is daily.

Ease of deployment and maintenance

To deploy a WAN-based system only requires setting up the central server and database, and deploying the agents. Since the agents are small (< 1 MB) they can be deployed using Active Directory Group Policies, SCCM, or any other means that the organization uses to install small files.

Once the server is set up and the agents are deployed there is no ongoing maintenance by the local admins and very little by the HQ personnel. This is in sharp contrast to SCCM, which requires substantial ongoing support in cases where the network topology changes, or new desktops, servers or laptops are added, for example.

Access to data

SCCM data is only available to the SCCM administrators. If other groups, such as ITAM or ITSM, need access to this data they must ask the SCCM administrators to supply it. Belarc's BelManage data is published as Web based reports and are available to all authorized users[8] based on their need to know, whether they are local admins, HQ personnel or auditors.

SCCM reports are based on SQL Server report builder, and although there are a fair number of standard reports, it helps to know SQL to modify or link additional information to these reports. In addition the reports can only be opened on a computer that has SQL Server reporting services and the proper rights.[9]

Belarc's system publishes it's information on the Belarc server as Web-based reports. This architecture also allows for easy sharing and access to the information by both local administrators and regional and headquarters IT management. The contents of the reports are automatically tailored based on each user's login, so that the user will only see information relevant to their area of responsibility.

From a practical point of view, SCCM data is only available to the SCCM administrators. If any other group such as ITAM or service desk, wishes to use this data, they must ask the SCCM administrator to supply it. This is in contrast to Belarc's BelManage system which automatically publishes this data for both local admins and HQ personnel.[10] Belarc also

8 CAC/PKI secure logins are supported and operate with the DoD and U.S. Federal government CAC/PKI standards.

9 For additional information on reporting in SCCM, click here.

publishes the database schema so it is readily available to other applications such as purchasing or service desk.

Automatic Grouping

Automatic grouping is a very powerful feature in BelManage, and almost required for any large number of IT assets. This feature allows for reports and login access based on the end user's business structure. For example reports and logins can be automatically grouped based in AD OUs, IP subnets, user names, or any combination of the elements in the host's profile. This means that the BelManage data can be quickly put into it's proper context by both HQ personnel and local admins.

In contrast SCCM requires the admin to run queries to group by devices or users, but not both. In practice this often means that grouping by AD OUs is all that is available.[11]

Network Discovery

Belarc's BelManage system has an automated built-in network discovery feature that uses lightweight network protocols to discover all network attached devices such as printers, switches, routers, IP phones, mobile devices, and of course desktops, laptops and servers.[12] BelManage uses this information to automatically create reports on these devices and also identifies computers that do not have detailed configuration data in BelManage's repository. BelManage can also easily audit standalone or non-network connected computers.

By default SCCM discovers profile data for machines in it's Active Directory. If for some reason a system is not in active directory, such as a printer, server or roaming laptop, it will likely not be in SCCM's profile reports. SCCM also does not have a practical way to audit non-network connected computers.

---

10 Using automatic grouping and user login rights, BelManage automatically publishes web based reports based on a user's need to know basis. In addition Belarc has developed automated links to service desk applications such as BMC's Remedy.

11 For details on grouping (collections) in SCCM, click here.

12 BelManage assigns one client per IP Subnet to accomplish the lightweight network discovery. These results are then sent to the central repository on the client's regular schedule. The reporting system then aggregates these IP subnets to create enterprise wide network map reports.

Timeliness

How up to date is the configuration data? BelManage updates all of its host's profiles daily by default, even for the largest enterprises with over 100K IT assets. It can be set to update more frequently if desired. SCCM says it updates every seven days by default, but from our experience this is unlikely to occur in larger enterprises because of the large amount of network bandwidth required for profile updates and database replication. In addition the demand on the hosts to create a profile is often substantial too.

This means that the data in BelManage is always up to date and can be used at any time. No need to wait for a data call. However SCCM may need to run through its paces for a few weeks before its data is usable.

Belarc & SCCM - Roles in IT management

Enterprises today are becoming more geographically distributed, are adding ever more computer systems, using multiple operating systems, and are placing new demands on their IT staffs. Much of this is driven by new security, corporate governance and compliance requirements. These requirements are in addition to traditional IT management tasks such as software license management, hardware and operating system refreshes, patching, software deployment, lifecycle management and others. In this environment, management tools need to move from primarily supporting the local administrators, to offering an enterprise wide view of the IT infrastructure.

In addition enterprises deploy multiple operating systems and can greatly reduce the complexity of their management tasks by using one system which automatically gathers data from multiple operating systems into a single central repository[13].

SCCM is a powerful tool for the local administrator, particularly when used to deploy Windows software and patches. However because of its architecture, it is not well suited for enterprise wide IT decision support. The following scenarios give examples where Belarc's products can complement and enhance an SCCM system.

13 BelManage supports all versions of Windows, Linux, Apple OSX and Solaris (x86). An Android app called the Security Advisor is also available.

Software License Management

Many organizations today are overlicensed, especially in their most common software (Microsoft, Adobe, Oracle)[14]. With the proper data Belarc's customers have been able to achieve significant software licensing and annual maintenance savings by correctly identifying their installed software, hardware platforms and whether the software is not just installed but actually being used.[15]

In order to accomplish this, enterprises need to have a software license management process which is automated, accurate and detailed. The alternative is to invest much manpower in local data calls, special SCCM scripts, and then aggregating the data on an enterprise wide basis. The benefits of an automated enterprise wide data collection system far outweigh the costs, because without accurate data, the enterprise is at the mercy of software vendors in the event of an audit. Alternatively once an organization has accurate, up-to-date enterprise wide information, it can often easily qualify for reduced software license and annual maintenance costs, due to un-used software or over licensing.

SCCM does software discovery by first setting the file types to be discovered, i.e. exes or dlls, for example. It then joins these discovered files to the Asset Intelligence Catalog to try to determine the correct software package and version that is actually installed.[16] There are a number of problems with this approach as follows:

- There will be an enormous number of files returned for each client, but this will be relatively meaningless unless the exact file is also in the Asset Intelligence Catalog downloaded from Microsoft. This is unlikely to be the case for any custom or GOTS software, so these packages will be very difficult to identify.
- SCCM does not discover any license keys or IDs, which can be very helpful in software license management, to determine who purchased the software and the rights associated with that purchase.

---

14 FAST Ltd, a UK authority in software asset management, estimates that over 40% of UK businesses are over licensed on their software and that they are on average over spending $310 (BP 200) per host device.

15 Please request our Software License Management white paper for details, by sending an email to: info@itamsoft.com

16 SCCM Software Inventory settings details are here.

It is one thing to discover that a software package or suite is installed, but it is equally important to discover whether the software package has been used or not. Why pay for more licenses if the organization has ones that are unused? Why pay for ongoing maintenance or SA on software that is not being used? Knowing whether a software package has been used and when is very important to better managing software and maintenance, an increasingly large part of most IT outlays. SCCM calls this software metering, and it requires the administrator to specify the file to be monitored and then wait for six, nine or twelve months to see the results for that file. Hardly encouraging when you need an answer today.

Belarc's BelManage product automatically discovers the detailed information on all installed software packages and suites, including custom and GOTS software, software keys or IDs if they are installed, and normalizes the data in it's central repository. BelManage does this without using a software catalog, which needs to be constantly updated. In addition, BelManage automatically discovers when all software packages have been last used so that software can be moved or removed.[17]

Belarc's Data Analytics module uses this discovered data to help automate the software license management process. Discovered instances and usage of products such as Microsoft Office, SQL Server, Windows Server, Visio, Project, Oracle, Adobe, etc., are automatically linked to purchase records and the product licensing rules.

Upgrade Planning

All IT organizations are at some point faced with the need to upgrade to a newer operating system or major application. One of the keys to success here is accurate and up-to-date inventory information so that IT can create realistic "Red, Green, Yellow" reports[18]. Without accurate and timely data, the project can easily go over budget and miss deadlines.

Belarc's BelManage system automatically creates an enterprise wide central repository with the correct information to make these cost and project planning decisions.

17 Belarc was awarded patent US 8473607 in June 2013 for "System and method for software usage discovery".

18 Red - machines that need to be retired. Green - machines that can run the upgrade. Yellow - machines that need to have hardware or software enhancements to run the upgrade.

SCCM uses the MIF files on the host system to collect hardware data. The information in these MIF files is often incomplete and must be extended with custom scripts.[19]

Software Compliance

Belarc's BelManage system automatically identifies unused, unlicensed, unauthorized, and obsolete software on an enterprise wide basis. This is true for COTS, GOTS[20] and in-house developed custom software, without the need to update and maintain software signature files, or a catalog.[21]

Belarc´s discovery system automatically collects the correct detailed information about all COTS, GOTS and custom software. It then presents this to the user in an easy to understand format. Powerful automatic drill down shows further details such as on which systems and where these software packages are installed. In addition BelManage has easy to set up Software Compliance reports, which immediately show which systems have non-compliant versions of software installed.

SCCM offers few details on most non-commercial, GOTS and custom software applications. Microsoft's Asset Intelligence module requires each SCCM site to set up its own Catalog with both software and hardware definitions. These must of course be periodically updated and then synchronized to all of the SCCM client sites. Software and hardware unknown to the catalog must be dealt with manually. Click here for details.

Operations & Service Desk

Because Belarc's system automatically creates an accurate, up-to-date central repository, local and HQ IT personnel can easily answer questions like the following:

---

19 For details on SCCM's hardware inventory, click here.

20 COTS (Commercial Off the Shelf Software) and GOTS (Government off the shelf Software) are standardized software packages, in contrast to custom built software.

21 Signature files or catalog. SCCM requires software signature files, called a catalog, to identify standardized and custom software. This is problematic because often unauthorized software is new and may not have a current signature in SCCM. In this case the unauthorized software is mistakenly not identified as being installed. In addition for custom software to be identified, new signatures will need to be created in SCCM.

- Was the latest software update installed on all the required computers?
- Was the memory or HDD upgraded on the requested computers?
- Which local and domain users logged into particular computers?
- Which software applications are good candidates for consolidation?

These are examples of the common IT operations questions that are not easily answered by SCCM on an enterprise wide basis.

In addition Belarc's system can be easily integrated with service desk applications, such as Remedy, Footprints and others. This integration is provided with a Belarc interface module included with every product. This allows the service desk user to simply click on a link to access the Belarc profile and change history reports for the relevant computers. Needless to say, SCCM currently has no such easy interface capability.

Datacenter consolidation

Belarc's products can automatically gather the following data, which are important to successfully implement datacenter consolidation programs:

- Server roles such as File, DNS, Applications (Oracle, Exchange, etc.), Web, WINS, Print, etc.
- Applications and versions running on Windows, Linux and Solaris servers.
- Virtual machine dependency mapping, i.e. which guest operating systems are running on the hosts and their related hardware platforms.[22]

Security Status & Audits

Belarc's system allows users to easily see the status of their missing hotfixs and IAVA[23] status (for Microsoft, Adobe, Apple, Oracle Java applica-

22 BelManage supports discovery and association of VM hosts to guests for a wide variety of host platforms, including Hyper-V, Virtual PC, Windows Virtual PC, vmWare ESXi, vmWare ESX, vmWare Workstation, vmWare Player, vmWare Server.

23 Belarc's products automatically report the IAVM (IAVA) status for Microsoft operating systems and Microsoft, Apple, Adobe, Oracle Java applications, based on the latest DISA IAVM-CVE data feed. Click here for details.

tions), anti-virus application status[24], local and domain account user status, USB storage drive usage, HDD disk encryption status, and more. When given access to the BelManage web interface, this information is readily available to local and headquarters administrators and security auditors.

SCCM does not automatically discover the non-Microsoft missing security updates, such as those from Adobe, Apple, Oracle, etc. However SCCM can be used to deploy them once you know where they are needed. This also means that SCCM cannot deliver an IAVA status report.

Complete IT asset view, including switches, routers, printers, IP phones, etc.

Belarc's network discovery feature automatically discovers all network attached devices, such as network switches, routers, printers, IP phones, tablets, and computers with other operating systems, including Apple OSX, Linux, Solaris, Unix, and more. SCCM does not offer a comparable capability.

Most networks contain more than only Windows machines. Knowing where these assets are located and what their configurations are is important for a realistic picture of the IT asset mix.

Secure Configurations

Belarc's products automatically show whether systems are compliant with the NIST secure configuration benchmarks[25]. The U.S. Office of Management and Budget (OMB) has mandated that all Agencies implement a standard set of these secure configurations[26]. The U.S. FFIEC, which sets standards for audits of financial institutions, has also been a long term proponent of configuration benchmarks.

Setting and monitoring configurations based on consensus benchmarks is important to IT security because it is a pro-active way to avoid many successful attacks. The NSA has found that configuring computers with proper security settings blocks over 90% of the existing threats.

---

24 Anti-virus scan engine version, definition file date, real time scanning status, and more.

25 These configurations are also referred to as benchmarks or checklists and have been developed by the National Institutes of Standards and Technology (NIST), the Center for Internet Security (CIS) and the National Security Agency (NSA).

26 For details, please request our white paper titled, "Securing the Enterprise".

Microsoft's Active Directory Group Policies (GP) are often used to implement many of the elements of these secure configurations. However it is also very important to monitor the status of these configuration benchmarks, because GPs do not cover elements such as:

- Security hotfixes and updates for operating systems and applications.
- Anti-virus status such as, engine version, definition date, real-time file scanning on, etc.
- Running unauthorized software such as peer-to-peer file sharing.
- User and Domain accounts, and more.

ITIL & CMDB

Many organizations are looking to follow the ITIL[27] processes for service management, software license management, security management and other IT operations. A requirement for all of these ITIL processes is a central repository consisting of all of the organization's IT assets and their configurations. ITIL calls this a Configuration Management Database, or CMDB. A CMDB consists of Configuration Items (CIs). The CIs can be configuration data of the IT assets, the relationships between the CIs, historical changes in the CIs, ownership of the CIs and sourcing details of the CIs.

Belarc's products automatically create much of the needed CMDB repository data on an enterprise wide basis, thus offering the ITIL project team some early and clear wins. On the other hand, if the ITIL project team relies on SCCM data, they will be forced to specify what data they require from SCCM, federate the data from multiple SCCM sites and then find a way to automate the process so that the CMDB can be kept up to date. More reasons why Belarc has been used by many enterprises that already have SCCM. For details, see the customer cases in the Proof Positive section below.

27 ITIL is a process driven set of best practices for IT Service Management developed under the Office of Government Commerce UK.

Proof Positive

Belarc's products have been successfully used by hundreds of small and large enterprises for over twelve years. Brief descriptions of three of our customers are below.

Agfa Healthcare UK

Agfa Healthcare UK uses Belarc's BelManage product to successfully complete and maintain the ISO 20000 certification required for IT healthcare providers. Agfa Healthcare offers diagnostic image management solutions, and state-of-the-art systems for capturing and processing images in hospitals and healthcare facilities. Belarc's system is used to automatically gather detailed IT configuration data on these systems located throughout the UK on a daily basis. BelManage automatically creates a central repository or CMDB with the latest profile data and changes that have occurred on the systems.

Catholic Relief Services

Catholic Relief Services (CRS) has been using BelManage for over eight years, on their 4,000+ IT assets located in 93 countries. Many of these CRS locations are very remote with poor communications. Even in this environment, BelManage has been able to help CRS automate many of their IT asset management tasks, so that they can use their resources to better fulfill their mission to help people in need throughout the world.

USAF 844th CG

The 844th Communications Group covers the Pentagon and Bolling and Andrews AFBs. The 844th CG has been using BelManage for over seven years and currently runs on their 25,000+ IT assets. BelManage was initially deployed in the Pentagon and used for their Microsoft license audit. BelManage helped the 844th CG reduce their Microsoft true-up costs by $2.7 million annually and was nominated for a Best Practice award for Software License Management.[28] In addition BelManage is being used help insure that consistent configurations of software are deployed. This helps improve IT security and reduce service desk calls.

US FAA

The US Federal Aviation Administration (FAA) initially deployed BelManage in two of its divisions, ESC and AQS. Upon the consolidation of the IT department, the FAA AIT deployed BelManage to all of its IT assets, totaling just over 57,000 host machines located throughout the U.S. This was accomplished in under 30 days. The FAA is using BelManage and the

28 Please send us an email to request details of the Best Practice Nomination.

Data Analytics module for software license management, configuration management and IT security purposes.

U.S. Marine Corps (USMC)

The USMC has been using Belarc's BelManage system for over twelve years. BelManage is deployed across the entire USMC world-wide network of over 120,000 computers, including servers, desktops and laptops on both the NIPRNet and SIPRNet[29]. For each network, BelManage runs on a single Windows server and Oracle database, and the profiles are updated daily. The system is accessed by hundreds of remote administrators throughout the world. The HQ IT staff uses BelManage for software license management, security audits, software application consolidation, hardware upgrade planning, server consolidation, and day-to-day management of their computer assets. The USMC has found that less than half of one administrator's time is required by their BelMa-nage system.

29 NIPRNet (Normal IP Routed Network, an unclassified but sensitive DOD network). SIPRNet (Secret IP Routed Network, an isolated more secure DOD network).

Summary

Belarc's products and SCCM have very different architectures and are primarily used for very different purposes. They are in many ways ideal complements to each other. Belarc is based on a WAN architecture, with a single server and database servicing the entire enterprise. SCCM is based on a hierarchical architecture requiring fast LAN speed connections between the managed assets and the local site servers. The local databases are then replicated up to higher level Parent servers and eventually the Central Server.

SCCM is primarily a tool used by local administrators to manage their Windows IT assets and deploy software and patches. Belarc's products are used by enterprise level IT management and local administrators for decision support purposes for multiple operating systems. Areas where Belarc's products are an excellent complement to SCCM include the following:

- Software License Management. Belarc automatically offers an enterprise-wide view of software installed and used to minimize licensing and annual maintenance costs.
- Upgrade Planning. Belarc easily creates Red, Green, Yellow Reports.
- Software Compliance. Belarc automatically identifies unused, unlicensed, unauthorized, obsolete software.
- Operations and Service Desk integration. Belarc quickly answers operations questions. Easily integrates with service desk applications.
- Security Status and Audits. Belarc shows missing hotfixes for multiple applications, AV status, account usage, and more.
- Complete IT Asset View. Belarc automatically discovers network switches, routers, printers and machines running operating systems other than Windows, such as Apple, Linux, Solaris, Unix, and more.
- Secure Configurations. Belarc runs the NIST benchmarks.
- ITIL and CMDB projects. Belarc automatically creates an accurate, complete, up-to-date, enterprise wide central repository.

Contact Us:

For additional information and a briefing of our capabilities, please contact us

.

ITAMSOFT B.V.
Den ilp 8
1127PA Den llp The Netherlands
Tel: (+31(0)20 4822603
Email: info@itamsoft.com
Web: www.itamsoft.com