Interested in learning more about security?

SANS Institute InfoSec Reading Room

Security Administration Solution or Why We Implemented An Identity Management/Account Provisioning T

Account provisioning is a fairly new buzz word. Account provisioning, also known as employee-provisioning, or EUA (enterprise-user administration), is one of the terms used to describe the creation, maintenance, and deletion of user accounts, password maintenance, and the administration of user access rights. "By 2004, 40 percent of enterprises will implement EUA products to manage their entire business-transaction flow and user-access requirement for Web and non- Web applications according a recent Gartner report."1 I...

Security Administration Solution or Why We Implemented An Identity Management/Account Provisioning Tool (A Case Study)

GIAC Security Essentials Certification (GSEC)
Version 1.4b
Suzette Franklin

Table of Contents

ABSTRACT

Account provisioning is a fairly new buzz word. Account provisioning, also known as employee-provisioning, or EUA (enterprise-user administration), is one of the terms used to describe the creation, maintenance, and deletion of user accounts, password maintenance, and the administration of user access rights. "By 2004, 40 percent of enterprises will implement EUA products to manage their entire business-transaction flow and user-access requirement for Web and non-Web applications according a recent Gartner report."[1]

I will present a case study of how our company took the challenge and implemented an account provisioning solution. In order to understand why we decided to seek a provisioning provider, I will start with a brief background on how our company created the 'data security' department. Next, I will guide you through data security's timeline and research that led to the selection of a provisioning tool. I will then provide you with how we tested and implemented the tool. And, finally, I will give a synopsis of where we are today.

BACKGROUND

Over the years, many companies have been challenged with the task of managing the identities of their employees. This identity management includes creating, deleting and updating employee accounts, ensuring that employees have the proper accesses to the company's various applications and systems that will allow them to perform their jobs, and a password management solution. With the influx of many new operating systems and database applications, this challenge has increased. Employees continue to move from one position to another and require new accesses and roles and oftentimes their old accesses are not revoked. "One of the greatest administrative and security challenges within every IT and HR organization is provisioning— providing users with appropriate access to enterprise information and technology resources. This is especially true in today's volatile business environment, where employee turnover, cost cutting and consolidation are all constant occurrences."[2]

Our company's environment was no different. A few years ago, we had what was considered a decentralized security environment. Each platform or application had its own administrators who administered user access for their own systems. Along with the decentralized environment were several issues. One of the issues was not knowing all the applications and accesses an employee had, since access was provided in a vacuum. With a variety of operating systems and

[1] http://www.networkcomputing.com/1317/1317f1.html

[2] http://www.epresence.com/capabilities/provisioning.html

databases, and over 800 security components that control access to our business systems, it was very difficult to ensure that proper access was provided. Access rights were also limited to the security consciousness of these administrators. If a network administrator was lazy, he may have provided a user with full access just because it was convenient or easy. And that same administrator may not remember to delete or revoke an account when an employee was terminated.

We also had password issues. Since an employee needed passwords for several different applications, they would frequently use weak passwords that were easy to remember. There was also the employee who infrequently accessed some systems and had to contact the Help Desk to reset their passwords. Eighty percent of our Help Desk calls were password related. Many administrators set passwords never to expire on certain platforms since this was easy for them to administer. There were employees who had been with the company for several years and still had the same password since they first started at our company. The enforcement of periodic password change was impossible.

Our company decided to put an emphasis on data security and we slowly started centralizing our access security. The Data Security department started with just two individuals, and I was one of them. We were responsible for the security access of only two platforms: Lotus Notes and the mainframe (ACF2). My main focus or area of subject matter expertise was Lotus Notes and the other individual's major focus was ACF2.

The company's direction for data security shifted quite rapidly; a team leader was added, and we were given other platforms and applications to administer which included Oracle database, Oracle applications, Novell, NT, Unix and home grown applications. Along with the access administration of these platforms, came other responsibilities such as monitoring and reporting access rights to management.

The data security department expanded to six administrators. Because of the speed at which we acquired the administration of the various platforms, there was not a lot of time or money allotted for training. Expert knowledge was almost impossible for any one platform. We received just enough training to perform our tasks. There was not much time to truly understand all the security related to all the platforms and applications.

After many months of struggling with the environment and trying to ensure that the proper access was provided, we decided to address this situation by automating our user account administration.

THE EVOLUTION

The journey to automate our user accounts started more than four years ago. That was about the time that we were transitioning from a decentralized security environment to one that was centralized. Even though our data security department grew from two to six people, that still was not enough to keep up with the daily workload. Our workload was directly tasked by employee turnover, organizational realignment, and accelerated application deployment. This was also compounded by the need for our staff to regularly provide confused employees over-the-phone training sessions on how to access our systems.

The Data Access Request Form (DAR)

A Lotus Notes form, the Data Access Request form or DAR, was created. This form was our first attempt at trying to automate the process. The form grew as our access requirements grew. It was a basic request form that initially included our major platforms and applications. Using the DAR, anyone could request access to any application or resource and manager approval was required. Once the request was approved, it was routed to our data security team and placed in a queue. Someone on the team would complete the request.

This system posed several challenges. One of the biggest challenge was the authorization process. Even though approval was required, there was no mechanism to determine if the approver was actually a manager. Even when managers did approve, oftentimes they would have their secretary complete the form. Data Security had to manually check to ensure that the authorization and approvals were correct. Another challenge was that there were times when time-sensitive requests were not completed on schedule. We eventually had to assign someone from our team to monitor the queue and assign the requests to team members. We tried having each team member focus on one platform and become the 'subject matter expert' (SME), meaning that person would focus on mainframe access, or one would focus on Unix, etc. As a result there were times when more than one security administrator would handle a single request.

The DAR soon became inefficient for several other reasons including:

- No way to automatically reroute the DAR if it required additional approval or to be sent to an alternate approver
- If SME was not in the office, depending on the access requested, the requests had to wait until that person returned
- Even though the DARs were stored in a database, unless the security administrator made notations on the form, it was often hard to determine what accesses were actually given the employee
- The information was saved as a form and it was hard to search the database for a particular request
- The completion of the DARs was inconsistent
- The process of providing user access was manual

Access Database

Our next step was to start profiling our employees. We thought that if we created meaningful profiles, we would be able to speed up the time it would take to process accounts and administer access rights. Many of our company's accesses are cross-divisional and we do not utilize a standard organizational chart. We started by interviewing the various functional units.

We devised a standard naming convention for the profiles and created an access database to input the data for the profiles. The profiles included most of the resources that each department or functional unit accessed. As a departmental profile was completed, it was added to the DAR. Due to the number of different profiles, the DAR became even more unmanageable. The creation of user IDs was still manual and unfortunately our environment was changing faster than we could keep up and input the data.

The access database soon became inefficient because:

- Employees still had to use the DAR to request access
- Not all accesses were recorded in the database and many times the request for access had to be researched to determine what was needed
- The information entered in the database was not consistent. Many applications have multiple names and one team member would enter it in one way and another would enter it in a different way. This would make searching and sorting by application almost impossible.
- Applications were rapidly rolled out and often faster than the information could be added to the database
- The process of providing user access was still manual

EVALUATION

It was now time to start evaluating companies that had provisioning solutions. I was given the task of helping with the search and later the technical lead for the testing and implementation. At the time we started looking, there were very few options. We took a detailed look at our environment and gathered the criteria we wanted from a provisioning provider. We started by assembling information about the various platforms and applications that our employees access. We had to gather information for not only those resources that our security department administered, but all resources within our company because even though they were not currently part of our duties, if a provisioning tool could help, then that would be beneficial. Also, as history would have it, sooner or later if an application involved security, our data security team would eventually take over those functions.

We knew that we wanted the provisioning solution to be able to create and revoke user IDs and to be able to have group association. But we also had additional criteria that included:

- ✓ Enable users to synchronize passwords across 100% of our most commonly used platforms
- ✓ Ensure appropriate access is provided to each employee and customer through established profiles
- ✓ Reduction of security administrator's response time for profiled access
- ✓ The ability to provide a complete view of each user's access
- ✓ Ease and speed of deployment and implementation
- ✓ The ability to integrate with our legacy systems

Acceptance Test

We presented our criteria to several provisioning companies. After many presentations and conversations, we finally found what we thought was a good match. We decided to do an acceptance test and selected BMC's CONTROL-SA. We had 13 supported platforms and each had its own unique administration. Our major platforms consisted of the following:

- Netware 5.0
- NT (3 domains and over 80 servers)
- ACF2
- Solaris (10 servers)
- AIX (14 servers)
- Lotus Notes
- Oracle Databases (over 20)
- Oracle Applications
- DB2
- IDMS
- Informix
- Sybase
- SQL Server
- Various Banking Software Applications
- Home-grown applications

None of the companies we looked at had solutions for all our platforms, however BMC had the most. During our 'proof of concept' period, we tested agents on Netware, NT, ACF2, Solaris, AIX, Lotus Notes, and Oracle Databases. These platforms are where a majority of our users have access.

The testing as well as implementation of this enterprise-wide solution required getting many departments involved. We had to solicit help from our Network Administrators, DBAs, Unix Administrators, Server Support team, Lotus Notes Administrators, and Mainframe Administrators. We not only needed to get their buy in for our tool, we also needed their assistance with the implementation on the various platforms. We scheduled meetings with each support department to give an overview of CONTROL-SA and to ensure that they were on board with the acceptance testing and the implementation plan.

What is CONTROL-SA?

CONTROL-SA is a provisioning tool that allows organizations to manage users and user access from a single point. It is scalable thus making it a tool of choice for small organizations such as ours or larger organizations. "CONTROL-SA has been successfully tested at customer sites totaling over one million users. Through dedicated CONTROL-SA/Agents, CONTROL-SA is capable of managing user access rights for more than thirty platforms, systems and applications including legacy systems, midrange and network operating systems, and Web applications."[3]

Key Features & Benefits[4]

- Enables end-to-end identity management and resource provisioning from a central location
- Cuts operational costs with high-level automation
- Tightens security with full accountability, auditing and reporting capabilities
- Reduces help desk password reset and access-rights administration through automation capabilities
- Increases employee productivity by providing access to resources in minutes not days
- Simplifies password management for users by reducing the number of passwords that need to be remembered

CONTROL-SA Components

"The CONTROL-SA server, with its central security repository, functions as the central point of control over managed security systems throughout the enterprise. CONTROL-SA/Agent software modules communicate between the CONTROL-SA server and the user databases of enterprise platforms and applications, providing real-time synchronization. From the CONTROL-SA GUI, security administrators can monitor, control and audit authorized access to all managed systems, at the enterprise level."[5]

[3] http://www.bmc.com/products/documents/78/45/7845/100031016/index.htm

[4] http://www.bmc.com/products/proddocview/0,,0_0_0_1587,00.html

[5] http://www.bmc.com/products/documents/92/38/9238/100034088/index.htm

Figure 1 below is a simplified diagram showing the various components of CONTROL-SA . They include:

- ✓ A central security administration database or Enterprise SecurityStation (ESS) database
- ✓ GUI interface for security administration
- ✓ ESS gateways
- ✓ SA-Agents
- ✓ Resident Security System (RSS) – the native security of an operating system

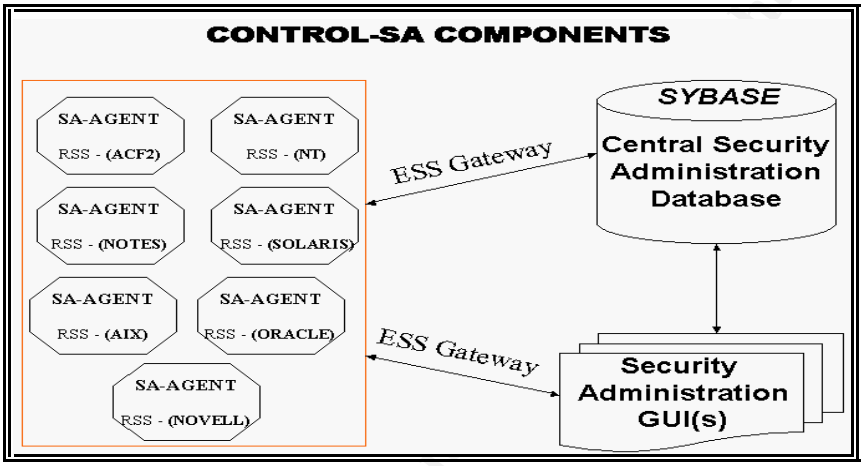

Figure 1

IMPLEMENTATION

After an acceptable 'proof of concept' testing, we were able to move forward with implementation. After strategizing, we decided to implement CONTROL-SA in three phases; installation of application, password synchronization, and job codes (profiles).

Installation

With the help of BMC's Professional Services and our Unix Administrators, we began with the installation of the master (Enterprise SecurityStation) database. At the time of purchase, Sybase was the only available database, supported by BMC, for their CONTROL-SA product. Even though our company no longer supported Sybase as a standard database application, we purchased the Sybase version of CONTROL-SA with the understanding that we would convert to Oracle as soon as BMC had the Oracle database version available. As technical lead of the project, I filled the DBA role for the project and maintained the database. BMC also offered to provide database support for Sybase until we did move to Oracle.

One of the major components of CONTROL-SA is the enterprise user. The enterprise user manages a person's access to all their connected platforms and

resources. Each enterprise user account is unique and it is this account that is used to administer users from a single point of reference.
After the database was created, we had an option of creating a new enterprise user account for all our employees or to leverage off user ids that we already had in place. Our user accounts were consistent across many of our platforms, therefore we opted to use our current user id schema. We imported our employee, contractor, and consultant user accounts from a Lotus Notes database and populated the enterprise user account table in the ESS database. Once we imported that data, any new employees, consultants, or contractors had to have an enterprise user account created in the ESS database

The next step was to install the ESS GUI on all data security desktops. The GUI is what we use to create new enterprise users, RSS users and user groups, and to connect these users to profiles. We are also able to do a snapshot view of groups, resources, and other connected entities.

Once the database was populated with the enterprise users and the GUIs were installed, we were ready to start installing the agents and adding the Resident Security System (RSS) data into our ESS database. As we downloaded each platform, it was easy to see how the database grew and how the various entities connected.

We started with our Unix platforms and installed CONTROL-SA agents on eleven Sun Solaris servers, ten AIX servers and one mainframe LPAR. We installed the CONTROL-SA agent for NT on three domain controllers; our web, production and development domains. We also wanted to administer our local NT user accounts so we installed the CONTROL-SA NT agent on over eighty NT servers.

The Oracle database CONTROL-SA API was next. This API was added for over forty Oracle databases. Novell and Lotus Notes were our last two platforms. The CONTROL-SA Novell agent worked in conjunction with the NT agent. By installing the Netware API, we were able to manage users in our entire Novell tree. The CONTROL-SA Lotus Notes API was the last platform that we installed.

Very little customization was required to accommodate a user ID lookup. The enterprise user account as you recall is what was created in the CONTROL-SA ESS database from an import of one of our Lotus Notes databases. This ID is used to manage many of the user's associated RSS user IDs. CONTROL-SA was configured so that when RSSs are downloaded, the RSS user IDs are connected to enterprise users. If there is no existing enterprise user, the RSS user ID is connected to an "UNKNOWN" enterprise user. In our environment, since our user IDs are the same on many of our platforms, when we downloaded the RSS data, CONTROL-SA was able to quickly match the enterprise user ID with the RSS user ID. The only platforms where we needed to modify were Lotus Notes since the user ID is first name and last name, and Novell since the user ID

is the fully qualified user ID which includes the user's organizational units, i.e., yyp01.Hawaii.home.

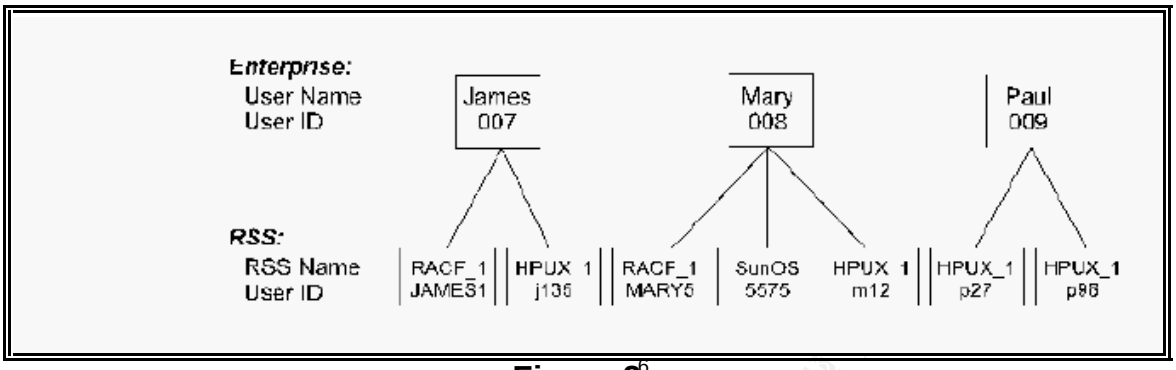

Figure 2[6]

Figure 2 above depicts how the enterprise user and the RSS users are connected. Changes, such as password synchronization and account revocation, can easily be managed from a central point, once all the RSSs are attached to an enterprise user.

Password Synchronization

Phase two of our provisioning implementation was enabling password synchronization. After all the agents were installed and all the data was downloaded into the ESS database, the enterprise users now had their appropriate RSS IDs attached to their enterprise user account.

As an example, I had an ID on over seventy different resources. Before password synchronization, it took a considerable amount of effort and time for me to change all those passwords on a regular basis. There were many platforms that I did not use on a regular basis so frequently I had to contact another team member to either reset the password or unlock the account. Other employees did not have as many IDs but they still had the same issues that I experienced with passwords. When I did chose a password, it was usually a weak one or one that I was sure to remember. As security conscience as I was, I was still guilty of inappropriate password management. "Password strength is also problematic for organizations. Hackers possess effective tools and techniques for cracking poorly constructed passwords. Organizations desire to enforce stronger password formation rules across the enterprise but must balance that desire against poor end-user experience and increases in forgotten passwords."[7]

[6] Enterprise SecurityStation Administration Guide (Windows GUI), Version 3.2.00, December 9, 2001, p 1-16.
[7] ftp://ftp.software.ibm.com/software/tivoli/buyers-guides/bg-ident-mgmt.pdf

We had to evaluate our platforms and determine a password syntax that would satisfy all our resources before we could implement password synchronization. We researched the password syntax for our various platforms and determined the common denominator or the proper syntax that would be sufficient for all platforms. For future planning, we also had to take into consideration the platforms that were not included with the current implementation of CONTROL-SA. We found that in our environment, ACF2 had the greatest constraints for passwords and we were not able to make any modifications to these rules. After checking all the various syntax rules, a password policy was written and adopted. This policy was distributed company-wide prior to activating password synchronization. Below are some of our password syntax rules. I have placed in italics why the rule was chosen.

Password Syntax Rules

- Passwords must be 7 character or 8 characters in length - no shorter or longer. (*ACF2 requires a password of no more than eight characters and our Windows platform was set to require a password of no less than six characters.)*
- Passwords are case sensitive. *(This is a general rule across most of our platforms regardless of any other syntax rule.)*
- Passwords can contain these special characters: @ $ #. *(ACF2 only allows certain special characters. We wanted to make sure that if our users did use a special character that they would use one of the three listed. This would ensure that the password would work.)*
- Passwords should be alpha/numeric but not start with a numeric or special character *(AFC2 allows for the usage of a number as part of the password however, that number can not be the first character. In other words you can not use a phone number or social security number as a password.)*
- Cannot reuse your last eight passwords. *(Password aging of eight is set on the Windows platform.)*

BMC's CONTROL-SA password synchronization is designed where a password change can initiate on any number of platforms. Among these are NT, AIX, ACF2, and Oracle database. This means that if password synchronization is activated on these platforms, when a password change occurs on any of those platforms, synchronization would be triggered across all resources attached to the enterprise user. We decided to activate password synchronization on only one platform, NT, since everyone had an NT account. Also, it would be a single point of focus when troubleshooting.

An announcement was made prior to activating password synchronization. We reiterated the new password syntax and explained that in the near future password synchronization would be activated. We started with a small pilot group for testing. After a successful pilot period, we were ready to activate password synchronization company-wide.

We activated password synchronization by department and notified each department at least two days prior to activation. Working with CONTROL-SA's batch run process, we developed scripts that ran the night before activation. These scripts reset the user's password to a predetermined password, set the flag on the NT account so that the user was prompted to change his/her password at next login, and activated password synchronization within CONTROL-SA. As the users logged in the morning after the scripts ran, they were prompted to change their password and synchronization occurred.

Job Codes

The final phase of our provisioning solution was the implementation of job profiles or job codes. A job code is created when an enterprise user is connected to user groups from his/her connected RSSs. Job codes grant users access rights based on certain conditions and user characteristics assigned to a defined profile. Each job function or task is related to a job code. Job codes assist with access rights accountability.

> Tracking precisely who has access to what information across your organization is a critical function of the provisioning system. Not only does it allow control of sensitive systems but it exposes all accounts that have unapproved authorizations or are no longer necessary. These inappropriate accounts pose one of the most serious threats to corporate security because they cannot be detected as a traditional cyber attack – they are valid, active accounts. Access rights accountability provides configuration control over all accounts and their specific authorities.[8]

While CONTROL-SA was being installed on the various platforms, job codes were constantly being discussed. As we added more and more resources to the ESS database, we started to formalize a plan as to the best way to develop job codes. We had to be sure that they would be flexible enough to accommodate the constant changing of our environment.

We conducted additional departmental interviews. Since many departments were already profiled, this interview process was to compare the previous information we collected and to make any necessary changes to ensure that the profiles were accurate and updated. We started by creating departmental job codes. We quickly realized that in many instances just one departmental job code would not work. There were very few departments that had only one job code or only one job function. In some cases, a job code had to be created for almost everyone in the department because their job functions were too diverse. We also started creating functional job codes as well as application job codes. A functional job code was associated with a function such as clerk or account

[8] http://www.bmc.com/products/documents/92/38/9238/100034088/index.htm

executive. Application job codes were created for applications such as VPN or access to a home-grown application. Currently we have over 700 job codes.

WHERE WE ARE TODAY

CONTROL-SA is installed on all of our major platforms. As our platforms and environment change, so will CONTROL-SA. Since our initial implementation of our provisioning tool, the following changes have already occurred:

- Our headquarters was physically relocated to a new location
- We eliminated Novell from our environment
- We implemented Active Directory and rolled out new PCs company-wide
- We upgraded our Unix AIX platform to AIXR5
- We upgraded our Solaris platform to 2.8
- We are in the process of upgrading our Oracle Databases to 9i
- We added the CONTROL-SA Oracle Applications agent
- We are considering moving from Lotus Notes to Exchange
- We are considering implementing a workflow product that will automate the approval process.

With any changes, and especially those listed above, there are new and different challenges. CONTROL-SA has allowed our Data Security department to keep up with these rapid changes. Without CONTROL-SA, we would have had to double our staff to keep up with these changes.

By enabling password synchronization, a majority of the Help Desk calls that were password related have been eliminated. Prior to password synchronization, our security staff was constantly being interrupted on a daily basis to reset passwords. Due to the training and knowledge required for some of the platforms, it was not feasible to have the Help Desk make these changes. We are now able to delegate this function to our Help Desk staff without having to provide them with administrator access to the various platforms. The Help Desk can change passwords within CONTROL-SA. Even though we have to have a weak password policy to accommodate all our platforms, we are able to enforce a monthly password change.

Through the implementation of job codes, our Data Security department can create a new user account within a matter of minutes and not days. The same is true when we have to terminate an employee. To terminate an employee, we simply revoke the enterprise user account and all attached RSSs IDs are revoked. Due to the design of the job codes, the administrator can look at the job code and determine if the terminated employee has access to any platforms that are not associated with CONTROL-SA, such as VPN or AT&T Global Dialer. Even though these applications have to be manually revoked, by looking at the job codes, we can see in one location all applications associated with a user.

Job codes allow the timely creation and revocation of user IDs, however, the downside is that the job codes have to constantly be updated as quickly as job functions change. Job codes do allow us to provide consistent access to departments, however if a department has standardized job codes, and if a single job function changes, then the job code has to be updated or a new on needs to be created.

Job codes also enable us to update multiple users with just one job code. If an entire department needs a new resource, the job codes only need to be modified and not the individual users. This is especially helpful when departments are consolidated or reorganized.

CONCLUSIONS

"With user populations fluctuating, user communities expanding to include business partners, suppliers and customers, and employee turnover continuing, the need for an efficient way to manage user identities throughout their entire lifecycles has never been more important."[9] Implementing a provisioning tool requires a considerable amount of planning. It is not a task that can be done quickly and once implemented, maintenance is an on going process. When determining the right tool for you, not only does the architect and technology have to be evaluated, you need to also evaluate the various features that the system provides. The tool should be flexible enough to change with your environment.

It has taken us over four years to get to where we are today and two of those have been the implementation of the provisioning tool. Thanks to CONTROL-SA, we now have a good foundation for a secure environment. Our security team can focus on true data security and start working on our policies, security awareness program, and monitoring and access reporting. In looking ahead, as we change our environment, CONTROL-SA will be able to change with us.

[9] ftp://ftp.software.ibm.com/software/tivoli/buyers-guides/bg-ident-mgmt.pdf

REFERENCES

MacVittie, Lori. "Employee Provisioning." Network Computing. August 19, 2002. URL: http://www.networkcomputing.com/1317/1317f1.html (26 Jan. 2003)

"Capabilities: Provisioning." ePresence. (1 Mar. 2003)
URL: http://www.epresence.com/capabilities/provisioning.html

"Central Management and Its Impact on Enterprise Performance – White Paper", BMC Software, Inc. (19 Dec. 2002)
URL: http://www.bmc.com/products/documents/78/45/7845/100031016/index.htm

"Products: CONTROL-SA." BMC Software, Inc. (19 Dec. 2002)
URL: http://www.bmc.com/products/proddocview/0,,0_0_0_1587,00.html

"BMC Software – B2B Solutions for eBusiness System Management." BMC Software, Inc. (19 Jan. 2003)
URL: http://www.bmc.com/products/documents/92/38/9238/100034088/index.htm

"Buyer's Guide for Identity Management." Tivoli Software,IBM. January 2003. p. 6.
URL: ftp://ftp.software.ibm.com/software/tivoli/buyers-guides/bg-ident-mgmt.pdf (6 Mar. 2003)

Fox, Pimm. "Provisioning Can Boost IT Operations." Computerworld. August 19, 2002. (18 Dec. 2002)
URL:
http://www.computerworld.com/managementtopics/management/story/0,10801,73544,00.html

Radcliff, Deborah. "Be Prepared: Laying the Groundwork for Provisioning." Computerworld. April 29, 2002. (18 Dec. 2002)
URL: http://www.computerworld.com/networkingtopics/networking/story/0,10801,70526,00.html

"How BMC Software Uses CONTROL-SA to Manager Security Policies Across Multiple Platforms – White Paper." BMC Software, Inc. November 12, 2002. (16 Jan. 2003)
URL: http://www.bmc.com/products/documents/20/09/22009/22009.pdf

"CONTROL-SA – The Foundation for Secure Identity Management." BMC Software, Inc. (2 Feb. 2003)
URL: http://www.bmc.com/offers/campaign/security/control_sa/

"BMC Software Enhances Provisioning Solution with Increased Scalability and Flexibility." BMC Software, Inc. January 22, 2003. (23 Jan. 2003)
URL: http://www.bmc.com/corporate/nr2003/012203_1.html

BMC Software, Inc. Enterprise SecurityStation Administration Guide (Windows GUI), Version 3.2.00, December 9, 2001, 1-16.

Last Updated: October 19th, 2017

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS San Diego 2017	San Diego, CAUS	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Seattle 2017	Seattle, WAUS	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Gulf Region 2017	Dubai, AE	Nov 04, 2017 - Nov 16, 2017	Live Event
SANS Milan November 2017	Milan, IT	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Amsterdam 2017	Amsterdam, NL	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Miami 2017	Miami, FLUS	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Paris November 2017	Paris, FR	Nov 13, 2017 - Nov 18, 2017	Live Event
Pen Test Hackfest Summit & Training 2017	Bethesda, MDUS	Nov 13, 2017 - Nov 20, 2017	Live Event
SANS Sydney 2017	Sydney, AU	Nov 13, 2017 - Nov 25, 2017	Live Event
GridEx IV 2017	Online,	Nov 15, 2017 - Nov 16, 2017	Live Event
SANS San Francisco Winter 2017	San Francisco, CAUS	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS London November 2017	London, GB	Nov 27, 2017 - Dec 02, 2017	Live Event
SIEM & Tactical Analytics Summit & Training	Scottsdale, AZUS	Nov 28, 2017 - Dec 05, 2017	Live Event
SANS Khobar 2017	Khobar, SA	Dec 02, 2017 - Dec 07, 2017	Live Event
SANS Austin Winter 2017	Austin, TXUS	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Munich December 2017	Munich, DE	Dec 04, 2017 - Dec 09, 2017	Live Event
European Security Awareness Summit & Training 2017	London, GB	Dec 04, 2017 - Dec 07, 2017	Live Event
SANS Bangalore 2017	Bangalore, IN	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS Frankfurt 2017	Frankfurt, DE	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DCUS	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Security East 2018	New Orleans, LAUS	Jan 08, 2018 - Jan 13, 2018	Live Event
SANS SEC460: Enterprise Threat Beta	San Diego, CAUS	Jan 08, 2018 - Jan 13, 2018	Live Event
SANS Amsterdam January 2018	Amsterdam, NL	Jan 15, 2018 - Jan 20, 2018	Live Event
Northern VA Winter - Reston 2018	Reston, VAUS	Jan 15, 2018 - Jan 20, 2018	Live Event
SEC599: Defeat Advanced Adversaries	San Francisco, CAUS	Jan 15, 2018 - Jan 20, 2018	Live Event
SANS Berlin 2017	OnlineDE	Oct 23, 2017 - Oct 28, 2017	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced