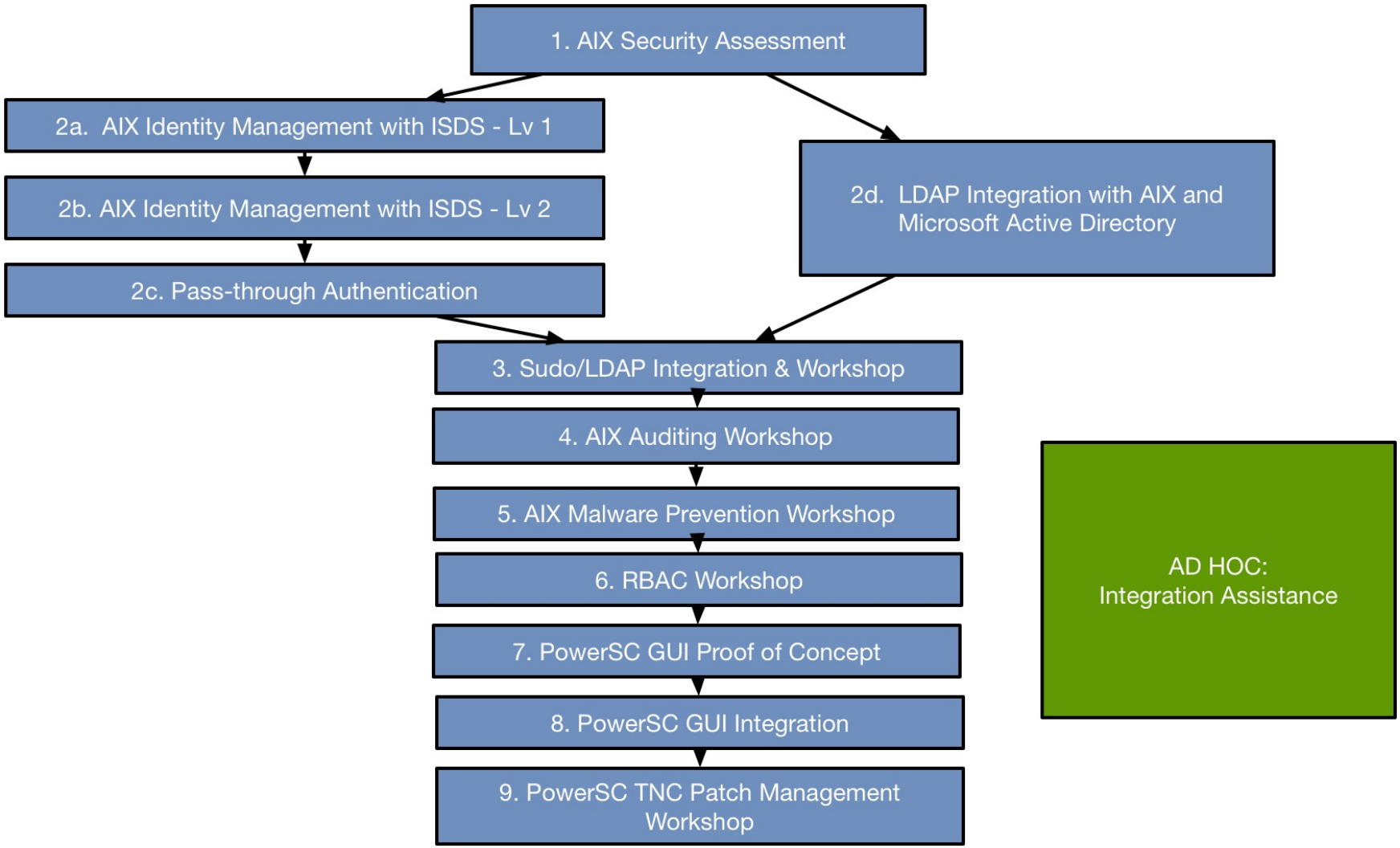
AIX Security Services Roadmap



AIX Security Assessment with PCI 3.2

Overview:

Companies frequently and unknowingly can employ weak security practices that are exposing their company to high risk. The ramifications of a security breach could be unforeseeable litigation, identity theft, the bringing down of networks, and harm to a company's brand. As described by the Jericho Forum, a company shouldn't solely depend on perimeter security for their security. The AIX Security Assessment is the best way to identify weak AIX security practices that may be exposing your company to high risk. This assessment is a comprehensive assessment of how you are implementing AIX security.

- At least one AIX or VIOS partition is assessed
- A set of documents detail the results of the assessment
- The assessment details how the security settings correspond to PCI 3.2
- Learn about AIX solutions available to reduce operational expense
- Learn about PowerSC solutions available to assist you with security & compliance
- Short overviews can be provided to help the customer understand recommended solutions, such as RBAC and LDAP
- Customers wanting to learn about securing VIOS partitions
- The assessment only reads existing security settings --- no settings are altered on the assessment partition

WHO benefits from this assessment and WHY?

- Customers wanting to improve their AIX Security configurations
- Customers wanting to stay abreast of the latest AIX security solutions
- Customers wanting a security baseline for defining standard builds
- Clients wanting to learn about ways to simplify the management of their AIX security environment

Duration

- At least 1 day on-site

Phase 1 – Preparation (remote):

Conference calls are held prior to the service to validate the scope, agenda, schedule and required materials.

- Client provides overview of their current AIX Security environment
- IBM team prepares the service agenda/schedule
- IBM team details security data collection process
- IBM team provides customer security questionnaire
- Identify required materials / Finalize key players

Phase 2 – AIX Security Assessment (on-site):

Review the Results of the Assessment with Customer
Example Tasks

- Consultant reviews the results of the security assessment with customer staff
- Customer reserves conference room with projector and invites relevant staff
- Customer staff can ask questions about the details of the assessment
- Customer staff can ask questions about the security recommendations
- Additional presentations can be provided to expound upon various technologies that may be recommended

Deliverables – Detailed AIX Security Assessment Findings document, Heat Map, Executive Summary

References:
The Jericho Forum:
http://en.wikipedia.org/wiki/Jericho_Forum

Terms and Conditions: Actual Tasks, Deliverables, Service Estimates,,and travel requirements vary with each client's environment. When we have reached a final agreement on the scope of your initiative and our level of assistance, a formal document describing our proposed work effort, costs, etc, will be presented for your approval and signature.

Erin M. Hansen - *PowerCare Opportunity Manager* erinh@us.ibm.com
Linda Hoben – *Opportunity Manager* hoben@us.ibm.com 1-720-395-0556
Stephen Brandenburg – *Opportunity Manager* sbranden@us.ibm.com 1-301-240-2182

AIX Identity Management with ISDS - Level 1

Overview:

The best form of identity management for AIX systems is implemented using LDAP directory services. LDAP can save a great amount of time, effort, and energy by simplifying the task of supporting users and groups as a business grows. This type of centralized management allows you to remove the need of synchronizing passwords and accounts for users and groups across multiple AIX systems. This service provides an on-site workshop that will equip the customer with all the essential elements needed to deploy LDAP directory services using IBM's Security Directory Server (ISDS):

- Provide presentations to help the customer staff understand LDAP
- Installation and configuration of LDAP Server and Clients using ISDS
- Install and configure the web-based GUI administration tool
- Learn how to tune your LDAP client configuration for optimal performance
- Learn how to migrate local users and groups from an AIX partition to an LDAP Directory. N**OTE**: this service does not provide migration of users and groups with inconsistent UIDs and GIDs from multiple partitions to LDAP, but we will provide guidance on how migration is accomplished with inconsistent UIDs and GIDs
- See and understand why ISDS is the best identity management solution for AIX
- Learn why ISDS configured with RFC2307AIX Schema doesn't have the numerous limitations found with other LDAP solutions, like Microsoft Active Directory (MSAD)

WHO benefits from this workshop and WHY?

- Clients with limited skills or experience with LDAP
- Clients needing a solution to simplify password and user/group administration
- Clients wanting to simplify the management of other AIX security services like RBAC, EFS, AIX Security Expert, Trusted Execution

Duration

- 2-3 days on-site

Phase 1 – Preparation (remote):

Conference calls are held prior to the service to validate the scope, agenda, schedule and required materials.

- Client provides overview of their current AIX identity management
- IBM team prepares the service agenda/schedule
- Identify required materials / Finalize key players

Phase 2 – LDAP Workshop – Level 1 (on site):

Installation and configuration of LDAP Client and Server
Example Tasks

- Learn how to add/delete new users to the LDAP directory from AIX
- Learn how to install and configure the LDAP Client and Server

Deliverables – Step-by-step install and configuration document, Understanding LDAP Presentation, AIX/LDAP Name attribute mapping document, LDAP user and group master templates files

Installation and Configuration of LDAP Web Admin Tool
Example Tasks

- Install and configure the Embedded WebSphere Application Server package used for Web-based LDAP GUI administration
- Learn how to customize access to the Web Administration for multiple administrators
- Learn how to manage users and groups from the Web admin interface
- Learn how to migrate pre-existing users from AIX systems to LDAP

Deliverables – Step-by-step install and configuration document, LDAP Workshop slides

LDAP Demo
Example tasks

- At conclusion of the service, provide customer staff a demo of the implemented LDAP ISDS solution
- Provide a general Q&A session
- Provide preview of AIX Identity Management with ISDS – Level 2
- Provide preview of the Pass-through Authentication Service

Terms and Conditions: Actual Tasks, Deliverables, Service Estimates,,and travel requirements vary with each client's environment. When we have reached a final agreement on the scope of your initiative and our level of assistance, a formal document describing our proposed work effort, costs, etc, will be presented for your approval and signature.

Erin M. Hansen - *PowerCare Opportunity Manager* erinh@us.ibm.com
Linda Hoben – *Opportunity Manager* hoben@us.ibm.com 1-720-395-0556
Stephen Brandenburg – *Opportunity Manager* sbranden@us.ibm.com 1-301-240-2182

AIX Identity Management with ISDS - Level 2

Overview:

This service is a follow-on service to the AIX Identity Management with ISDS – level 1 service. The best way of ensuring the security and reliability of LDAP directory services is to provide a fail-over LDAP Server and to encrypt all LDAP related communication. This service provides an on-site workshop that will equip the customer with all the essential elements needed to integrate SSL and LDAP replication with IBM's Tivoli Directory Server running on AIX:

- Provide presentations to help the customer staff understand LDAP replication
- Install and configure SSL with AIX LDAP Clients and the ISDS LDAP Server on AIX
- Install and configure SSL for the ISDS web-based GUI administration tool
- Learn how to configure Master-Slave replication with 2 ISDS LDAP Servers running on AIX
- Learn how to configure AIX LDAP Clients for LDAP Server failover

WHO benefits from this workshop and WHY?

- Customers with limited skills or experience with LDAP
- Customers needing to secure and provide a reliable LDAP solution for their production AIX LDAP Client systems
- Customers needing a secure method for administering their LDAP server

Duration

- 2-3 days on-site

Phase 1 – Preparation (remote):

Conference calls are held prior to the service to validate the scope, agenda, schedule and required materials.

- Customer provides overview of their current AIX identity management
- IBM team prepares the service agenda/schedule
- Identify required materials / Finalize key players

Phase 2 – SSL & Replication Workshop – Level 2 (on site):

Installation and configuration of SSL LDAP Client and Server
Example Tasks

- Learn how to create self-signed certificates
- Learn how to install the GSKIT for SSL integration
- Learn how to create a Key Database file
- Learn how to add, delete and modify a secured directory

Deliverables – Step-by-step SSL install and configuration documents and any related presentation slides

Installation and Configuration of Master-Slave LDAP Replication
Example Tasks

- Learn how to configure an LDAP Server as a Replication Master
- Learn how to configure an LDAP Server as a Replication Slave
- Learn how to export a master directory to a slave securely

Deliverables – Step-by-step Replication install and configuration document and any related presentation slides

LDAP Demo
Example tasks

- At conclusion of the service, provide customer staff a demo of the implemented SSL LDAP ITDS solution
- Provide a demo of the LDAP replication using a failover scenario
- Provide a general Q&A session

Terms and Conditions: Actual Tasks, Deliverables, Service Estimates,,and travel requirements vary with each client's environment. When we have reached a final agreement on the scope of your initiative and our level of assistance, a formal document describing our proposed work effort, costs, etc, will be presented for your approval and signature.

Erin M. Hansen - *PowerCare Opportunity Manager* erinh@us.ibm.com
Linda Hoben – *Opportunity Manager* hoben@us.ibm.com 1-720-395-0556
Stephen Brandenburg – *Opportunity Manager* sbranden@us.ibm.com 1-301-240-2182

Pass-through Authentication

with Microsoft Active Directory and IBM Security Directory Server

Overview:

For most AIX customers, Pass-through Authentication (PTA) is the key to providing the best general solution for centralized password and user/group management for AIX systems.

When AIX systems are configured as LDAP clients pointing to a centralized ISDS LDAP server, ISDS can provide the PTA mechanism to redirect authentication requests to a different LDAP server, in this case MSAD. This PTA mechanism allows AIX users to use a single Windows network login password for both Windows and AIX system login.

With PTA, ISDS will still be used to manage and store AIX user and group information. By storing user and group information on ISDS, full compatibility with AIX systems is maintained because ISDS implements the RFC2307AIX LDAP Schema. Not all LDAP servers, such as MSAD, provide this as a default implemented schema. In the case of MSAD, the schema support that is provided by default for UNIX systems can prove to be difficult to use, limiting and less functional. Fortunately, all of these issues are eliminated by centrally storing and managing user and group information on ISDS.

If an application server running on an AIX LDAP client utilizes OS security, PTA provides the additional benefit of centralizing application authentication to MSAD, even if the application clients are running on different operating systems. This is an additional method of how PTA eliminates the use of multiple passwords and centralizes authentication to the single MSAD-based password for not only AIX login access, but also AIX application access. Please see the PTA Topology diagram on the next page for an illustration of this using DB2.

Duration

- 2-6 days on-site

WHO benefits from this workshop and WHY?

- Clients needing a solution to greatly simplify password and user/group administration
- Clients wanting to allow AIX users to authenticate to their AIX partitions using their Windows network login password

Phase 1 – Preparation (remote):

Conference calls are held prior to the service to validate scope, agenda, schedule and required materials.

- Customer provides overview of their current AIX password and user/group management
- IBM team prepares the service agenda, schedule, etc.

Phase 2 – PTA Workshop (on-site)

Configuration of PTA

Example Tasks

- Configure PTA using the ITDS Web-based Administration Tool
- Learn how PTA can enable an AIX user to login to AIX, whether his username is identical or not to his Windows network login name
- Learn how multiple AIX logins can be mapped to the same Windows password
- Learn how PTA is configured as an option on a per user basis

Deliverables – Step-by-step PTA configuration document & all slides

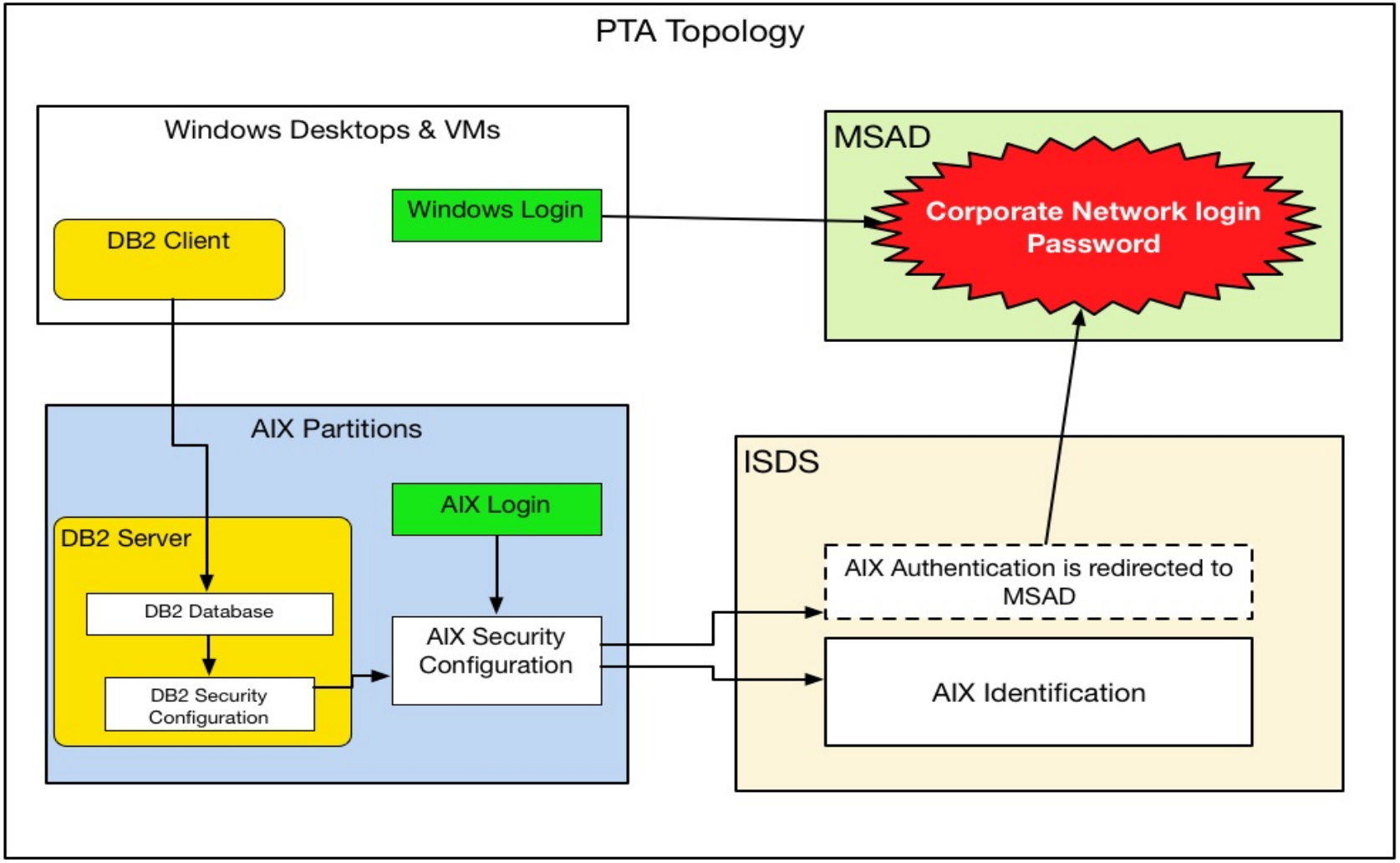
***NOTE**: This PTA solution requires the use of server-side authentication. Therefore SSL (see the Level 2 service) must be implemented with AIX LDAP Clients and Servers.*

Terms and Conditions: Actual Tasks, Deliverables, Service Estimates,,and travel requirements vary with each client's environment. When we have reached a final agreement on the scope of your initiative and our level of assistance, a formal document describing our proposed work effort, costs, etc, will be presented for your approval and signature.

Stephen Dominguez – WW LBS AIX Security Lead - sdoming@us.ibm.com
Linda Hoben – *Opportunity Manager* hoben@us.ibm.com 1-720-395-0556
Stephen Brandenburg – *Opportunity Manager* sbranden@us.ibm.com 1-301-240-2182

Pass-through Authentication Network Topology

with Microsoft Active Directory and IBM Security Directory Server



LDAP Integration with AIX and Microsoft Active Directory

Overview

A popular LDAP server option for AIX is using Microsoft Active Director as the LDAP server for your AIX LDAP clients.. MSAD can provide basic centralized user, group, and password management options for your AIX systems by leveraging your existing MSAD environment.

When AIX systems are configured as LDAP clients to an MSAD server, AIX users may use their Windows network login password for both Windows and AIX system login.

MSAD can be used to manage and store AIX user and group information without needing to install any additional software or schema extensions. In our service we will provide knowledge transfer, so you will understand how to enable your existing MSAD user and group accounts to support AIX authentication and user/group management.

WHO benefits from this workshop and WHY?

- Clients needing a solution to greatly simplify password and user/group administration
- Clients wanting to allow AIX users to authenticate to their AIX partitions using their Windows network login password
- Clients wanting to leverage MSAD-based authentication for HMC and VIOS systems

Duration

3-9 days on-site, depending on the level of assistance requested

Phase 1 – Preparation (remote)

- Conference calls are held prior to the service to validate scope, agenda, schedule and required materials
- Customer provides overview of their current AIX password and user/group management
- IBM team prepares the service agenda, schedule, etc.

Phase 2 – Workshop (on-site)

- Work with the MSAD and AIX customer staff to install and configure your AIX systems as LDAP Clients to your Active Directory infrastructure
- Provide assistance with mapping AIX LDAP attributes with MSAD defined attributes
- Provide assistance with SSL certificate requirements and verification
- Learn how AIX can be used to authenticate users with MSAD but use local AIX accounts for user and group information
- Learn about additional advanced AIX LDAP client configuration options

Deliverables – Step-by-step AIX configuration documents & all slides

***NOTE**: This service requires the use of server-side authentication with SSL/TLS Therefore a trusted root certificate must be provided by the MSAD customer staff in order for the AIX LDAP clients systems to be able to communicate with MSAD environment over SSL/TLS*

Terms and Conditions: Actual Tasks, Deliverables, Service Estimates,,and travel requirements vary with each client's environment. When we have reached a final agreement on the scope of your initiative and our level of assistance, a formal document describing our proposed work effort, costs, etc, will be presented for your approval and signature.

Stephen Dominguez – WW LBS AIX Security Lead - sdoming@us.ibm.com
Linda Hoben – *Opportunity Manager* hoben@us.ibm.com 1-720-395-0556
Stephen Brandenburg – *Opportunity Manager* sbranden@us.ibm.com 1-301-240-2182

Sudo/LDAP Integration & Workshop

Overview:

Sudo is a popular tool for delegating privileged access to general user accounts on Unix systems, including AIX. Although AIX's Enhanced RBAC is the most secure form of delegating access to AIX privileged commands, sudo maintains its popularity due to its common interface across Unix platforms. Sudo also provides a subset of access options not possible with AIX's Enhanced RBAC.

Sudo's access control rules are defined in the /etc/sudoers configuration file. The configuration file contains detailed information such as users and groups, the commands (and command arguments) they can run, the user/group a command will run as, etc. Host aliases and commands aliases can also be defined to facilitate the access control.

The sudo/LDAP integration workshop is designed to help you centralize the sudoers rules using an LDAP directory. This will reduce the complexity and effort of managing the /etc/sudoers configuration file on each and every AIX partition. This is just a sampling of what is provided during the workshop:

- LDAP server preparation for sudoers support
- Local /etc/sudoers file export/migration to LDAP server
- LDAP sudoers rules prioritization/ordering
- Configuration of sudo for LDAP sudoers lookup
- Mixed mode of sudoders lookup through /etc/sudoers file and LDAP

WHO benefits from this workshop and WHY?

- Clients who wants to simplify sudo rules management
- Clients who wants to reduce errors associated with hundreds of sudoers files in their data center
- Customers wanting a PoC installation of sudo with LDAP support before deploying it to the production environment

Duration

- 3 days on-site (assuming client has functional LDAP server already)

Phase 1 – Preparation (remote):

Conference calls are held prior to the service to validate the scope, agenda, schedule and required materials.

- Client provides the overview of its current AIX security environment and the sudo usage
- Client shares its LDAP server status
- IBM team prepares the service agenda/schedule
- Identify required materials / Finalize key players

Phase 2 – Sudo/LDAP Integration Workshop (on site):

Tasks

- Identifying the LDAP server type
- Installing and configuring the proper Sudo LDAP schema
- Designing the sudoers rule architecture in LDAP
- Examining local /etc/sudoers files
- Migrating sudoers rules to LDAP
- Enabling sudo LDAP lookup on AIX
- Testing/verifying sudo functions with LDAP integration
- Resolving client specific sudo/LDAP integration issues

Deliverables

- Step-by-step configuration document

Terms and Conditions: Actual Tasks, Deliverables, Service Estimates,,and travel requirements vary with each client's environment. When we have reached a final agreement on the scope of your initiative and our level of assistance, a formal document describing our proposed work effort, costs, etc, will be presented for your approval and signature.

Erin M. Hansen - *PowerCare Opportunity Manager* erinh@us.ibm.com
Linda Hoben – *Opportunity Manager* hoben@us.ibm.com 1-720-395-0556
Stephen Brandenburg – *Opportunity Manager* sbranden@us.ibm.com 1-301-240-2182

AIX Auditing Workshop

Overview:

The AIX Auditing subsystem provides comprehensive recording of security-related AIX events that can be used to alert you about potential or actual violations to the system security policy.

AIX Auditing allows you to track user activities critical to preventing, detecting or minimizing the impact of a security breach. The implementation of auditing allows thorough tracking, alerting, and analysis if something goes wrong. Additionally, determining the cause of a compromise is extremely difficult or impossible without the critical forensic information that AIX Auditing provides.

Proper auditing is typically mandatory for being able to meet various regulatory security compliance standards. This workshop provides the following:

- Presentations provided to help customer staff quickly understand AIX Auditing
- Learn how AIX Auditing can be coupled with PowerSC Trusted Logging to provide tamper-proof logging
- Learn how to plan for Production deployment
- Deploy a running PoC of AIX Auditing & PowerSC Trusted Logging
- Learn how AIX Auditing can be optimized and streamlined with the use of AIX's Enhanced Role Based Access Control (RBAC)

WHO benefits from this workshop and WHY?

- Customers with limited or no experience with AIX Auditing
- Customers wanting to properly monitor AIX systems to prevent security breaches
- Customers wanting an auditing solution to help meet regulatory compliance
- Customers wanting a PoC installation of AIX Auditing in a sandbox environment before deploying AIX Auditing to their production environment

Duration

- At least 1 day on-site

Phase 1 – Preparation (remote):

Conference calls are held prior to the service to validate the scope, agenda, schedule and required materials.

- Client provides overview of their current AIX auditing environment
- IBM team prepares the service agenda/schedule
- Identify required materials / Finalize key players

Phase 2 – AIX Auditing Workshop (on-site):

Configuration of AIX Auditing

- Learn how to configure AIX Auditing
- Learn how to configure RBAC-based AIX Auditing
- Learn about configuration options for saving on disk space and CPU cycles

Deliverables – Step-by-step AIX Auditing and configuration documents, AIX Auditing Workshop slides

Installation and configuration of PowerSC Trusted Logging
Example Tasks

- Learn how to install and configure PowerSC Trusted Logging
- See how AIX Auditing and Trusted Logging can provide tamper-proof auditing logs

Deliverables – Step-by-step PowerSC Trusted Logging install and configuration documents, PowerSC Trusted Logging Slides

AIX Auditing Demo
Example tasks

- At the conclusion of the service, a demo of AIX Auditing & PowerSC Trusted Logging will be provided
- Final general Q&A session provided

Terms and Conditions: Actual Tasks, Deliverables, Service Estimates,,and travel requirements vary with each client's environment. When we have reached a final agreement on the scope of your initiative and our level of assistance, a formal document describing our proposed work effort, costs, etc, will be presented for your approval and signature.

Erin M. Hansen - PowerCare Opportunity Manager erinh@us.ibm.com
Linda Hoben – *Opportunity Manager* hoben@us.ibm.com 1-720-395-0556
Stephen Brandenburg – *Opportunity Manager* sbranden@us.ibm.com 1-301-240-2182

AIX Malware Prevention Workshop

with AIX Trusted Execution


CNET › News › Security & Privacy › Target confirms malware used on point-of-sale terminals

Target confirms malware used on point-of-sale terminals

During an interview with CNBC, retailer's CEO defends four-day delay ir notifying customers of security breach as necessary for the investigation and preparation for consumer reaction.

by Steven Musil | January 12, 2014 7:15 PM PST

Follow

THE WALL STREET JOURNAL. | BUSINESS

TOP STORIES IN BUSINESS 1 of 12 Twitter Seeks More Ad Credibility

2 of 12 From Saks, the High and Low

BUSINESS

Malware Lurked for Months Inside Neiman

Credit-Card Stealing Software Worked From July 16 to Oct. 30.

Overview:

Companies frequently and unknowingly fail to deploy proper security countermeasures for malware, which exposes these companies to high risk of a security breach leading to numerous harmful effects, such as damage to a company's brand, huge financial losses, identity theft, costly litigation, etc.

Fortunately, IBM has provided a powerful solution, AIX Trusted Execution (TE), to drastically reduce the risk posed by malware, and IBM Lab Services has provided a service to help you quickly deploy this indispensable tool for preventing malware on AIX networks.

Workshop Description:

In this workshop, we will look at the nuts and bolts of Trusted Execution (TE) deployment and work through several TE lab exercises in order to gain experience in addressing the most critical elements of TE deployment

Phase 1 – Preparation (remote):

Conference calls are held prior to the service to validate scope, agenda, schedule and required materials.

- Customer provides overview of their current malware prevention tooling, (if possible)
- IBM team prepares the service agenda, schedule, etc.

Phase 2 – AIX Malware Prevention Workshop (on-site):

Example Tasks

- Learn how to prevent and detect the various types of malware, such as: viruses, rootkits, trojan horses, etc using TE
- Learn how to generate TE logging reports
- Learn how TE can be used to satisfy regulatory standards, such as PCI, HIPAA, NERC-CIP,DoD STIG, SOX-COBIT
- Learn how to install and configure TE
- Learn how to prevent scripts and applications from being infected or altered by malware

Deliverables – Step-by-step configuration documents & all slides

Duration:

2 days on-site

Terms and Conditions: Actual Tasks, Deliverables, Service Estimates,,and travel requirements vary with each client's environment. When we have reached a final agreement on the scope of your initiative and our level of assistance, a formal document describing our proposed work effort, costs, etc, will be presented for your approval and signature.

Stephen Dominguez – *WW LBS AIX Security Lead* - sdoming@us.ibm.com
Linda Hoben – *Opportunity Manager* hoben@us.ibm.com 1-720-395-0556
Stephen Brandenburg – *Opportunity Manager* sbranden@us.ibm.com 1-301-240-2182

RBAC Workshop

Overview:

Starting with AIX 6.1, Enhanced Role Based Access Control (RBAC) on AIX is the most powerful and sophisticated access control tool for AIX. Many UNIX security breaches occur because of excessive access to root. One of the most important ways to protect your AIX environment is to lessen unnecessary root access. RBAC provides a rich set of tools for allowing administrators to gain the access they need to do their jobs without having to grant root access. RBAC is also important for many companies to implement in order to satisfy various regulatory standards.

In this workshop, we will look at the nuts and bolts of RBAC and work through several different RBAC lab exercises in order to gain experience in addressing the most critical elements of RBAC implementation:

- Provide presentations to help the customer staff understand RBAC
- Detailed installation and configuration of RBAC
- Learn how to enable 3rd party scripts and applications for RBAC
- Roadmap for implementing RBAC in production
- Learn why RBAC is far superior to other access control tools, like SUDO
- Learn how to centralize RBAC using existing LDAP Directory Services
- Learn how save disk space and CPU cycles when integrating RBAC with the AIX auditing subsystem

WHO benefits from this workshop and WHY?

- Clients wanting to prevent a security breach
- Clients with limited skills or experience with RBAC
- Clients needing a secure solution for delegated administrative access
- Clients needing to implement separation of duties
- Clients wanting to enable their AIX environment for existing and future AIX applications that implement RBAC roles

Duration

- 2 days on-site

Phase 1 – Preparation (remote):

Conference calls are held prior to the service to validate the scope, agenda, schedule and required materials.

- Client provides overview of their current AIX access control systems
- IBM team prepares the service agenda/schedule
- Identify required materials / Finalize key players

Phase 2 – RBAC Workshop (on site):

Installation and configuration of RBAC
Example Tasks

- Create and customize RBAC roles and authorizations
- Learn how to configure RBAC with AIX Auditing
- Learn how Domain RBAC can be used to add further granularity to your access control design
- Learn how to replace use of dangerous setuid with RBAC
- Learn how to customize your RBAC configuration
- Configure separation of duties using RBAC by requiring multiple administrators for command activation
- Learn the differences between AIX roles, authorizations and privileges
- Configure critical files for access via RBAC roles
- Limit access to critical file systems using Domain RBAC

Deliverables – Understanding RBAC presentation, RBAC Workshop slides, Implementation Guide for integrating RBAC with existing LDAP Services

RBAC Demo
Example tasks

- At conclusion of the service, provide customer staff a demo of RBAC
- Provide a general Q&A session

Terms and Conditions: Actual Tasks, Deliverables, Service Estimates,,and travel requirements vary with each client's environment. When we have reached a final agreement on the scope of your initiative and our level of assistance, a formal document describing our proposed work effort, costs, etc, will be presented for your approval and signature.

Erin M. Hansen - *PowerCare Opportunity Manager* erinh@us.ibm.com
Linda Hoben – *Opportunity Manager* hoben@us.ibm.com 1-720-395-0556
Stephen Brandenburg – *Opportunity Manager* sbranden@us.ibm.com 1-301-240-2182

PowerSC GUI Proof of Concept

Overview:

IBM's PowerSC Security & Compliance Automation tool provides compliance-based profiles and tooling for deploying security hardening for AIX.. Real-time monitoring of these compliance settings is accomplished via PowerSC Real Time Compliance.

Building upon the foundation provided by these two indispensable solutions, the release of PowerSC v1.1.5.0 includes a powerful new solution, the PowerSC Graphical User Interface (GUI), that makes the management of security compliance significantly easier. The PowerSC GUI allows administrators to centrally manage end point security compliance across the entire AIX environment from a web-based GUI, significantly reducing effort, complexity, and potential for human error.

The PowerSC GUI Proof of Concept (POC) service is designed to help customers quickly deploy PowerSC GUI in a customer POC environment. This is a sampling of what is provided during the service:

- GUI server installation and configuration
- Discover and connect the PowerSC managed machines to the GUI server
- Organize and group machines using filtering for simplified management
- Apply, check, and undo compliance settings using both the built in profiles and custom profiles on multiple endpoints simultaneously
- Understand the security compliance of all PowerSC managed systems in an environment from a centralized location

WHO benefits from this POC and WHY?

- Clients wanting to simplify security management and compliance measurement
- Customers wanting reduce the costs of meeting compliance regulations
- Customers wanting to improve audit capabilities for virtualized systems
- Organizations wanting to greatly reduce the effort and complexity of the security management of their Cloud environment

Duration

- 3 days or less (on-site or remote)

Phase 1 – Preparation (remote):

Conference calls are held prior to the service to validate the scope, agenda, schedule and required materials.

- Client provides the overview of their current AIX security environment and the compliance requirements
- Client shares the security policy they want to implement on the AIX servers
- IBM team prepares the service agenda/schedule
- Identify required materials / Finalize key players

Phase 2 – PowerSC UI Proof of Concept (on site):

Tasks

- Installation/configuration of the PowerSC GUI server
- Installation/configuration of end point agents
- Discovery of endpoints
- Use SSL to protect communication between GUI server and end points
- Configure endpoint access controls to securely share administrative access to the PowerSC GUI Server
- Apply profiles, check compliance of endpoints using the GUI Server
- Creation/use of endpoint groups
- Profile management from GUI Server
- Deploy PowerSC Real Time Compliance to complement PowerSC GUI

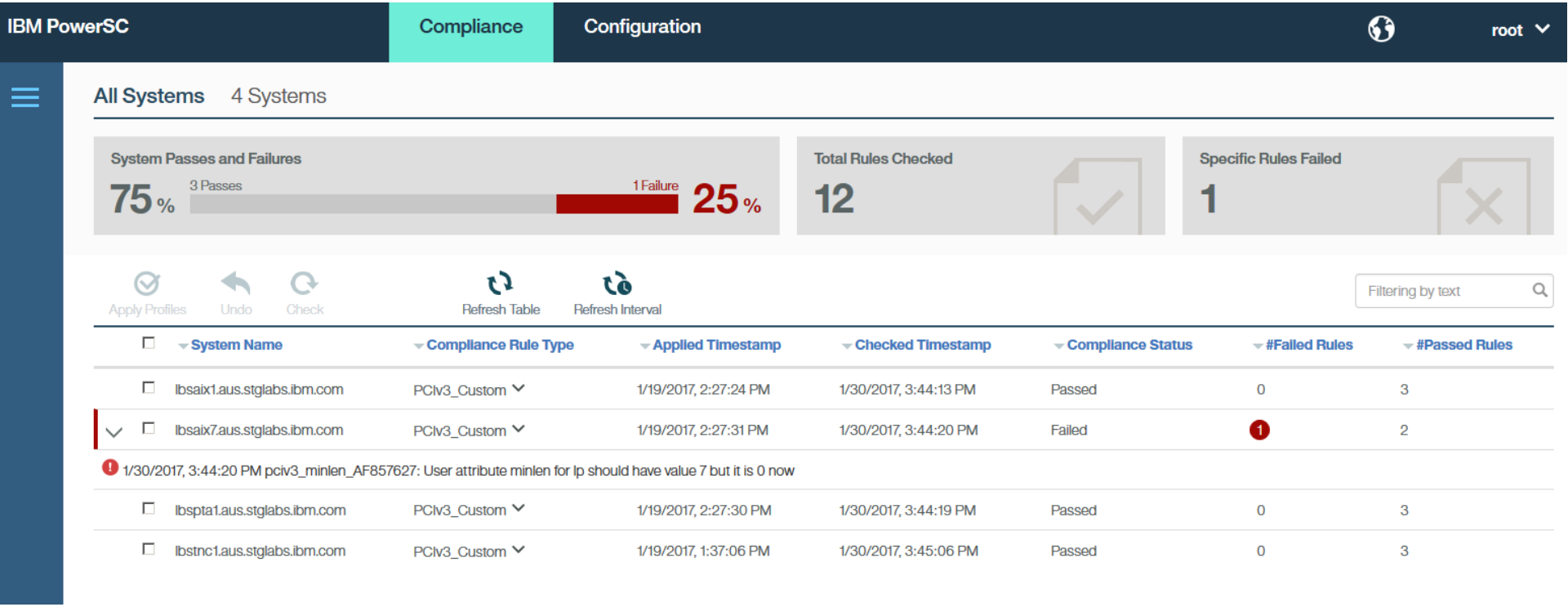
Deliverables

- Step-by-step configuration documents and any supplementary slides
- Customers may have a copy of any material presented

Terms and Conditions: Actual Tasks, Deliverables, Service Estimates,,and travel requirements vary with each client's environment. When we have reached a final agreement on the scope of your initiative and our level of assistance, a formal document describing our proposed work effort, costs, etc, will be presented for your approval and signature.

Erin M. Hansen - *PowerCare Opportunity Manager* erinh@us.ibm.com
Linda Hoben – *Opportunity Manager* hoben@us.ibm.com 1-720-395-0556
Stephen Brandenburg – *Opportunity Manager* sbranden@us.ibm.com 1-301-240-2182

The PowerSC Graphical User Interface



Erin M. Hansen - *PowerCare Opportunity Manager* erinh@us.ibm.com
Linda Hoben – *Opportunity Manager* hoben@us.ibm.com 1-720-395-0556
Stephen Brandenburg – *Opportunity Manager* sbranden@us.ibm.com 1-301-240-2182

PowerSC GUI Integration

Overview:

The PowerSC GUI Integration service is an optional service that follows the PowerSC GUI Proof of Concept service. In the POC service, all of the essential tasks are explained and demonstrated using the customer's POC environment; however, the POC service does not fully integrate PowerSC GUI across the entire customer environment. Some customers may choose to integrate PowerSC GUI on their own; however, other customers may want to simplify and expedite the integration of PowerSC GUI by utilizing this service.

This is a sampling of what is provided during the service:

- PowerSC GUI installation and configuration across customer environments
- Customize profiles to achieve full compliance and compatibility with different types of security compliance requirements, zones, partitions, or Cloud tenants
- Learn how to perform advanced customization options by incorporating your own original security checks within the PowerSC GUI framework

WHO benefits from this service and WHY?

- Customers who have already taken the PowerSC GUI POC service and want additional assistance deploying PowerSC GUI in their production and non-production environments
- Customers wanting to expedite the integration of PowerSC GUI to their environment(s)
- Customers wanting assistance with integrating PowerSC GUI settings in an incremental and methodical approach that minimizes or eliminates application conflicts

Duration

- 1 or more weeks (onsite or local) – actual length will depend on the level of assistance requested and the complexity of the endpoint security requirements

Phase 1 – Preparation (remote):

Conference calls are held prior to the service to validate the scope, agenda, schedule and required materials.

- Client provides the overview of their current AIX security environment and the compliance requirements
- Client shares the security policy they want to implement on the AIX servers
- IBM team prepares the service agenda/schedule
- Identify required materials / Finalize key players

Phase 2 – PowerSC GUI Integration (on site or remote):

Tasks

- Lab Services Consultant develops a plan for integration
- Consultant provides expert knowledge concerning the security settings being deployed with PowerSC GUI in order to expedite integration
- Installation/configuration of PowerSC GUI server
- Installation/configuration of GUI agents
- Verify correct discovery of endpoints
- Consultant helps define configurations that will provide compatibility for the different types of systems the environment may contain
- Consultant aids in the design of endpoint groups

Deliverables

- Step-by-step configuration documents and any supplementary slides
- Customers may have a copy of any material presented
- **Optional**: An AIX/VIOS Security Assessment is taken before and after the GUI integration to be able to compare the improvements made after integrating PowerSC GUI

Terms and Conditions: Actual Tasks, Deliverables, Service Estimates,,and travel requirements vary with each client's environment. When we have reached a final agreement on the scope of your initiative and our level of assistance, a formal document describing our proposed work effort, costs, etc, will be presented for your approval and signature.

Erin M. Hansen - *PowerCare Opportunity Manager* erinh@us.ibm.com
Linda Hoben – *Opportunity Manager* hoben@us.ibm.com 1-720-395-0556
Stephen Brandenburg – *Opportunity Manager* sbranden@us.ibm.com 1-301-240-2182

PowerSC - TNC Patch Management Workshop

Overview:

The Sony PlayStation Network Security Breach of April 2011 serves as an example of the importance of ensuring that all your virtual machines are properly patched. Trusted Network Connect & Patch Management (TNC) of PowerSC is a new solution designed to prevent your company from experiencing the type of breach that Sony experienced in 2011 by ensuring the end-point integrity of the AIX partitions that are active on your network. TNC enables administrators to securely and easily manage the AIX updates by providing tools to verify the service pack and patch levels of all your AIX systems and generate reports on the partitions that are down level or not compliant. Using NIM and SUMA, TNC also provides capabilities for downloading and installing these updates from your existing NIM server to your NIM clients.

- Provide presentations to help customer staff quickly understand TNC
- Provide planning for Production deployment
- Deploy a running PoC via installation and configuration of TNC Patch Manager, TNC Server, and TNC clients
- Learn how TNC detects and verifies completely new LPARs or partitions that have missed a patch window due to migration or hibernation
- Learn how TNC can help you prioritize security patches based on CVE numbers and CVE severity ratings
- Demonstrate how TNC provides reduced response time to CVE remediation

WHO benefits from this workshop and WHY?

- Customers with limited or no experience with TNC
- Customers wanting to properly patch AIX systems to prevent security breaches
- Customers wanting a solution to verify AIX service pack and patch levels
- Customers wanting a PoC installation of TNC in a sandbox environment before deploying TNC to their production environment

Duration

- 1-2 days on-site

Phase 1 – Preparation (remote):

Conference calls are held prior to the service to validate the scope, agenda, schedule and required materials.

- Client provides overview of their current AIX identity management
- IBM team prepares the service agenda/schedule
- Identify required materials / Finalize key players

Phase 2 – TNC Workshop (on-site):

Installation and configuration of TNC Patch Manager (TNCPM)
Example Tasks

- Learn how to securely configure the TNCPM using an http proxy
- Learn how to install and configure the TNC patch manager
- Learn how TNC can be used to deploy service packs, Security, Hiper, PE, and Enhancement APARs

Deliverables – Step-by-step TNC pre-install document, Understanding TNC Presentation,

Installation and configuration of TNC Server and Clients
Example Tasks

- Learn how to set TNC patch policies for different sets of AIX partitions
- Verify the AIX level for a set of AIX TNC Clients
- Install actual patches on AIX TNC Clients
- Install service packs on AIX TNC Clients
- Learn how to install a multi-TNC server configuration
- Learn about the different TNC email reporting options that are available

Deliverables – Step-by-step TNC install and configuration documents, TNC Workshop Slides

TNC Demo
Example tasks

- At conclusion of the service, provide customer staff a demo of TNC
- Provide a general Q&A session

Terms and Conditions: Actual Tasks, Deliverables, Service Estimates,,and travel requirements vary with each client's environment. When we have reached a final agreement on the scope of your initiative and our level of assistance, a formal document describing our proposed work effort, costs, etc, will be presented for your approval and signature.

Erin M. Hansen - *PowerCare Opportunity Manager* erinh@us.ibm.com
Linda Hoben – *Opportunity Manager* hoben@us.ibm.com 1-720-395-0556
Stephen Brandenburg – *Opportunity Manager* sbranden@us.ibm.com 1-301-240-2182

Integration Assistance

Overview:

Our standard services provide our customers with the essential knowledge transfer and Proof of Concept deployment to enable them to take the next steps from Proof of Concept to Production. The Integration Assistance service is a purely optional service that provides additional assistance to help customers more quickly and easily take that next step from Proof of Concept to Production.

This service is a general technical service that can be requested solely or combined with one or any number of our standard services to assist customers with the deployment of any AIX security related feature to your production environments. For example, 3 weeks of deployment assistance can be added to the one week RBAC workshop in order to assist you with integrating RBAC into your production environment.

This service can also be requested for general technical security assistance with the implementation of any arbitrary security solution. In this type of assistance, we only provide our best effort to assist, since we are providing assistance with possibly a solution with which we might have no prior experience. However, our assistance can greatly expedite and increase the chance of successful implementation since you will be leveraging a highly experienced security technical resource.

Service Highlights:

- Obtain general technical assistance with deploying AIX security related functionality into your production environments
- Can be requested with any of our standard services
- Technical services are provided with whatever combination of local/remote support desired
- Ensure you are deploying security features according to best practice
- Expedite the integration of security features by leveraging a Lab Services consultant who can also leverage an AIX development network

WHO benefits from this service and WHY?

Our workshop services are typically done in a sandbox environment for proof of concept purposes. After you have had a chance to evaluate and learn about the new technology in our workshop service, you may request this service to help you deploy the technology to your production environments.

Duration

1 or more weeks on-site/remote technical assistance

Phase 1 – Preparation (remote):

Conference calls are held prior to the service to validate the scope, agenda, schedule and required materials.

- Client provides overview of their current AIX Security environment
- IBM team prepares the service agenda/schedule
- Identify required materials / Finalize key players

Phase 2 – Security Integration (on-site/remote):

Example Tasks

- Consultant reviews implementation process
- Customer provides guidance with implementing security functionality
- Consultant can resolve complex technical issues leveraging the IBM development network
- Consultant verifies methodology used for integrating security tooling is consistent with best practices
- Consultant provides implementation guidance based upon previous customer environment deployments

Terms and Conditions: Actual Tasks, Deliverables, Service Estimates,,and travel requirements vary with each client's environment. When we have reached a final agreement on the scope of your initiative and our level of assistance, a formal document describing our proposed work effort, costs, etc, will be presented for your approval and signature.

Erin M. Hansen - *PowerCare Opportunity Manager* erinh@us.ibm.com
Linda Hoben – *Opportunity Manager* hoben@us.ibm.com 1-720-395-0556
Stephen Brandenburg – *Opportunity Manager* sbranden@us.ibm.com 1-301-240-2182