Privileged Identity Management

Nick Briers, WW Tivoli Product Manager

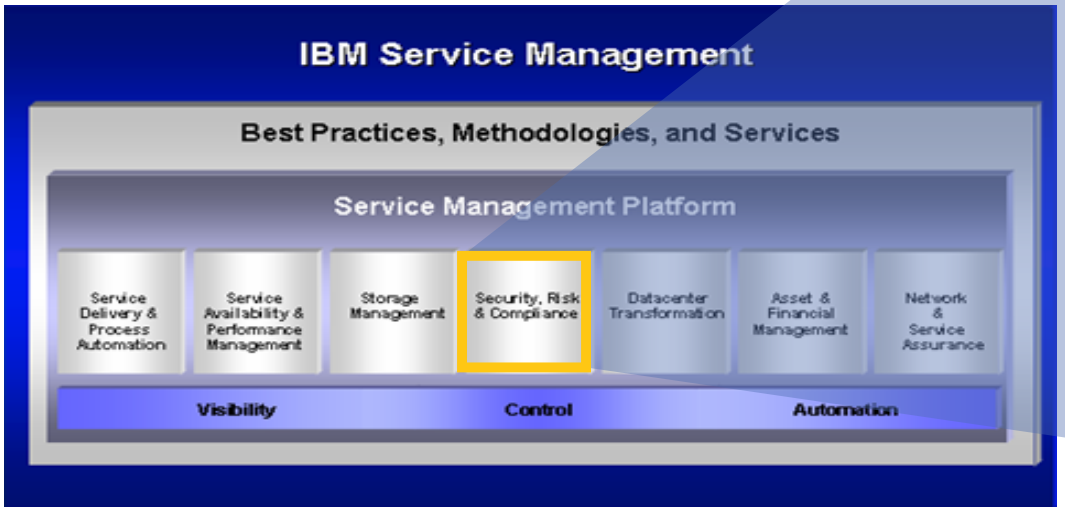
http://www.ibm.com/software/tivoli/solutions/security

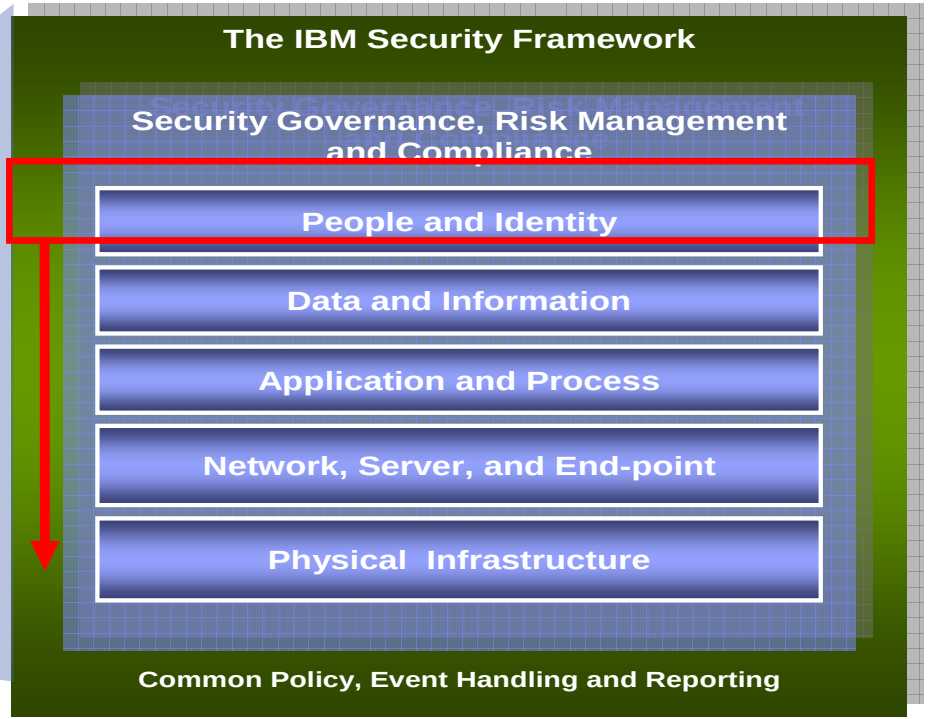
Agenda

- What is a privileged identity
- What are the management challenges for privileged identities
- Putting it all together with Tivoli Solutions to manage privileged identities
- Summary

IBM delivers a new approach to Security Management

IBM's approach is to strategically manage risk end-to end across all risk areas within an organization.





Privileged Identity Management

- What is a privileged identity
  - Not owned by an individual user
  - Have access to sensitive resources
  - Required by virtually all platforms although modern platforms have more capabilities for separating PIM from real user access
  - Example
    - Root
    - Administrator
    - WebServer Accounts
    - Oracle Financials Admin
    - Windows Admin
    - Unix File Shares Admin
    - SQL Server Admin
    - FileNet Admin
    - AD Domain Admins
    - SAP Admin
    - Etc.

What is a ‘privileged user’?

- Someone with IT permissions to:
  - Access highly sensitive data
  - Change critical IT systems
  - Conduct high value transactions
  - Cover their tracks in the audit trail
- As viewed by Analysts:
  - Forrester: PUPM (Privileged User and Password Management)
  - Burton: “The seedy underbelly” – PAM (Privileged Account Management)
- Who is a privileged user?

IT Administrators

System Accounts

C Level Executives

?

What damage can be done?

- Privileged identities may be used to define new user definitions
  - to perform work as a userid which is un-noticed by identity management policy enforcement
- Privileged identities may be used to change other user's capabilities
  - inadvertent escalation of privilege to other users
  - create other privileged users
  - deny access to services required by a user
- Privileged identities may be used to access sensitive information
  - copy, modify, or destroy
- Privileged identities may be used to change audit logs
  - remove or modify file-based audit logs
  - modify audit log records
- Privileged identities may, by their intent, “own” a system

Privilege Identity Concerns

- Top of audit findings
  - Compliance awareness of organisations
  - Audit focus
- Used everywhere
  - By definition almost every systems, and sub-system/ application has one or more
- Lack of control
  - Many people know the id and password to do their jobs
  - Difficult to audit – “administrator” always did it!

Who cares about privileged identities?

Malicious insiders care…

THE WALL STREET JOURNAL.

The Online Journal GET 2 WEEKS FREE SUBSCRIBE NOW | The Print Journ GET 2 WEEKS FRE SUBSCRIBE NO

As of Friday, January 25, 2008

News | Today's Newspaper | My Online Journal | Multimedia & Online Extras | Mark

OTHER FREE CONTENT FROM THE WALL STREET JOURNAL

EDITORS' PICKS

Retiring Abroad
Texting for Votes
If You Knew Sushi
Tree Hugger
Airline Champs of 2007
Beautiful Country
MORE EDITORS' PICKS

BLOGS

Most Popular Posts

1. Giants Win Super Bowl, Leaving Pats at 18-1
2. Motorola: Death of an American Icon?
3. Clinton Aims Barbs at Obama, McCain
4. On Eve of Super Tuesday, Obama Lowers Expectations

SEE ALL BLOGS

MORE FREE CONTENT

-- Personal Journal
-- Personal Finance
-- Leisure
-- Markets Data Center
-- Video
-- Blogs
-- Forums
-- Interactives
-- Autos

THE WALL STREET JOURNAL. GET FULL ACCESS TO ALL ONLINE JOU

PAGE ONE

French Bank Rocked by Rogue Trader

Société Générale Blames
$7.2 Billion in Losses
On a Quiet 31-Year-Old

By DAVID GAUTHIER-VILLARS, CARRICK MOLLENKAMP and ALISTAIR MACDONALD
January 25, 2008; Page A1

PARIS -- The rogues' gallery of banking has a new candidate for membership: 31-year-old trader Jérôme Kerviel.

In one of the banking world's most unsettling recent disclosures, France's Société Générale SA said Mr. Kerviel had cost the bank €4.9 billion, equal to $7.2 billion, by making huge unauthorized trades that he hid for months by hacking into computers. The combined trading positions he built up over recent months, say people close to the situation, totaled some €50 billion, or $73 billion.

The loss -- dwarfing the $1.3 billion Nick Leeson cost British bank Barings in 1995 -- has forced Société Générale to seek a capital infusion. It is expected to try to raise €5.5 billion, chiefly from its existing shareholders.

The problem:

- 3 of the Top 10 Threats to Enterprise Security are insider related:
  - Employee error
  - Data stolen by partner/employee
  - Insider Sabotage
- Insider driven fraud costs US enterprises over $600 Billion annually

Who cares about privileged identities?

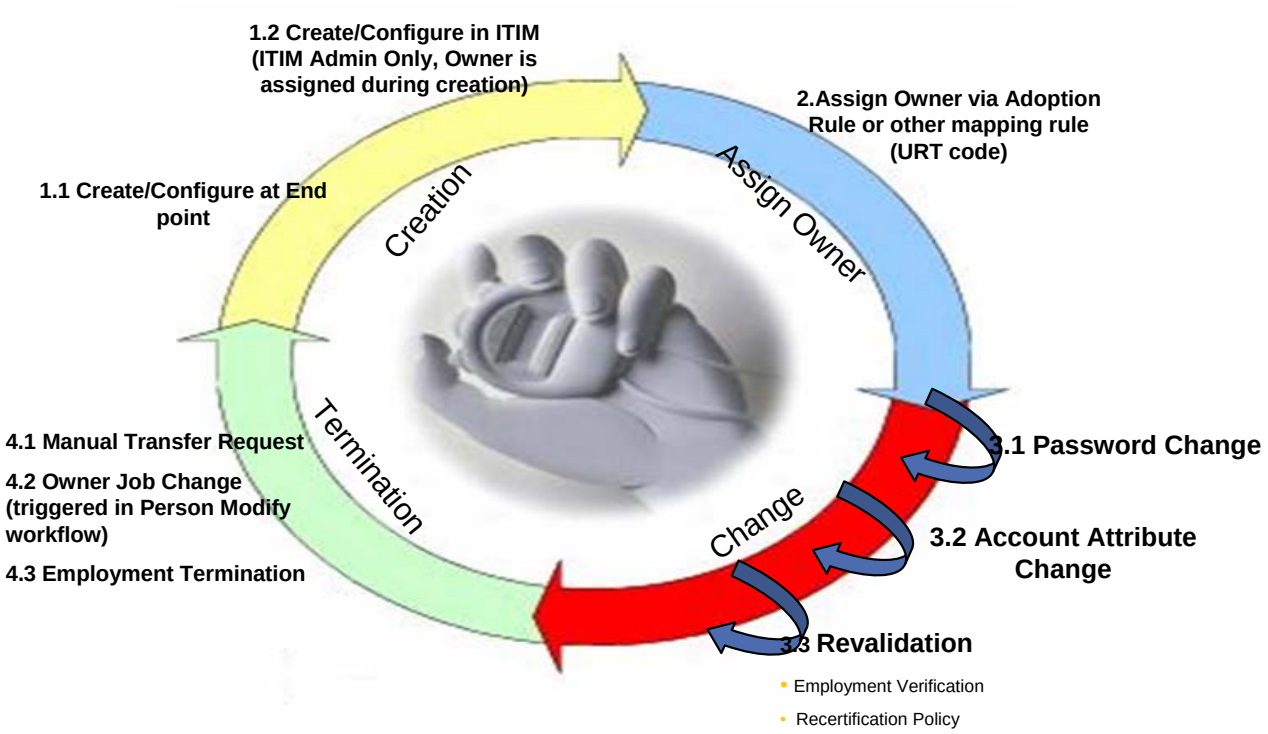
Your auditors care…

Regulatory Compliance Initiative	Relation to Privileged Account Controls
Payment Card Industry (PCI) Data Security Standard (DSS)	**Protect stored cardholder data (#3)** **Develop and maintain secure systems and applications (#6)** **Restrict access to cardholder data by business need-to-know (#7)** **Insufficient internal controls over privileged accounts would negatively impact an organization's capability to meet all of these requirements.**
California Senate Bill 1386 (now California Civil Code 1798)	**SB 1386 requires organizations that lose private information of California residents to report the loss to affected individuals.** **Unauthorized users of privileged accounts can bypass the access control mechanisms and audit controls of most systems to access private information without the organization knowing about it.**
Sarbanes-Oxley Act (SOX) Section 404	**Requires corporate management to take responsibility for establishing and maintaining an adequate internal control structure and procedures for financial reporting** **Requires management to assess and report the effectiveness of the internal control structure and procedures for financial reporting.** • **Insufficient internal controls over privileged accounts negatively impact an organization's capability to meet these requirements.**

Challenges with today's scenario

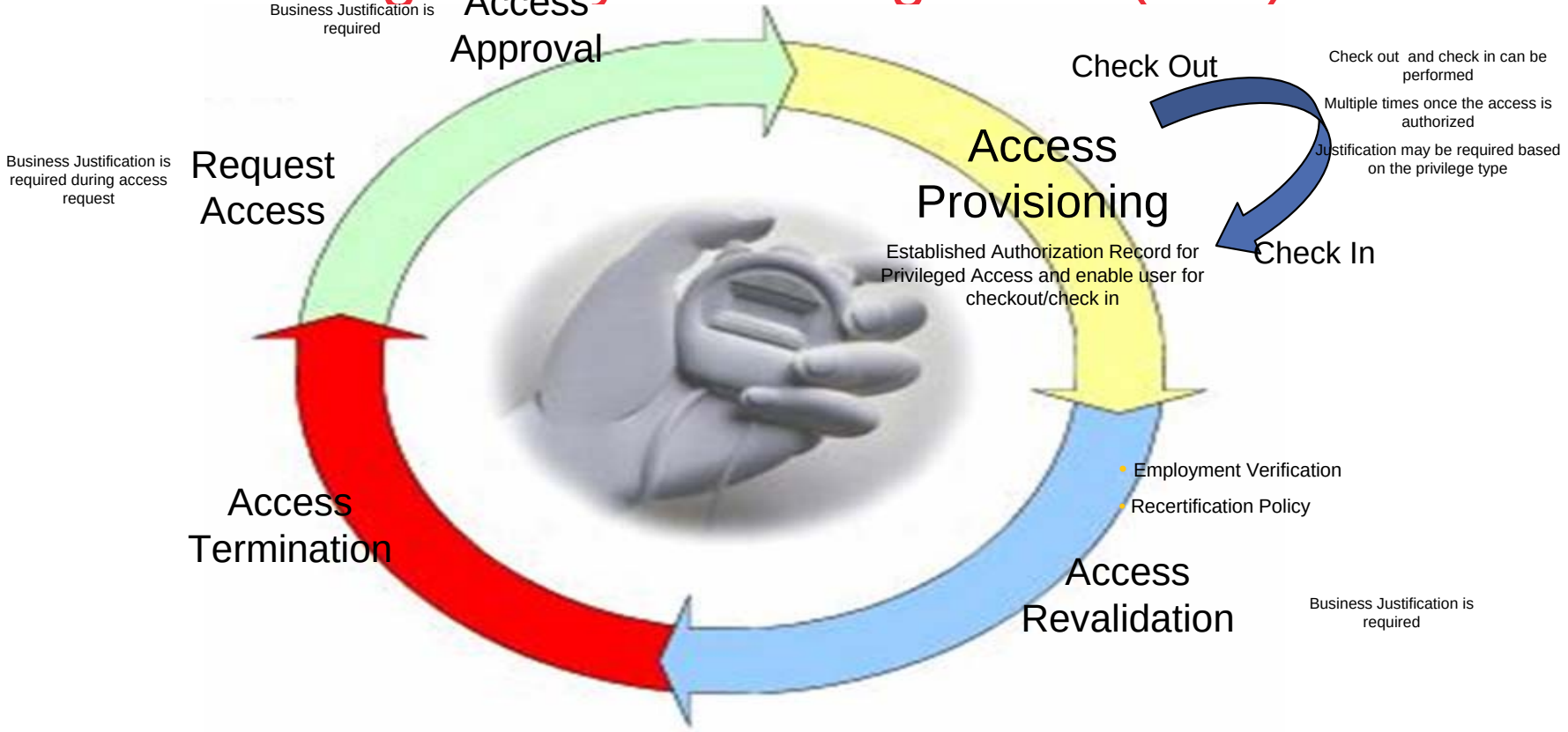
- Privileged identities are shared
- Manually intensive
- No audit trail – Joe signed on to work station but administrator signed on to SAP for example
- Difficult to manage good practices
  - For example changing passwords frequently requires all sharers to be informed

Shared Privileged ID Account Lifecycle Management in Tivoli Identity Manager (TIM)

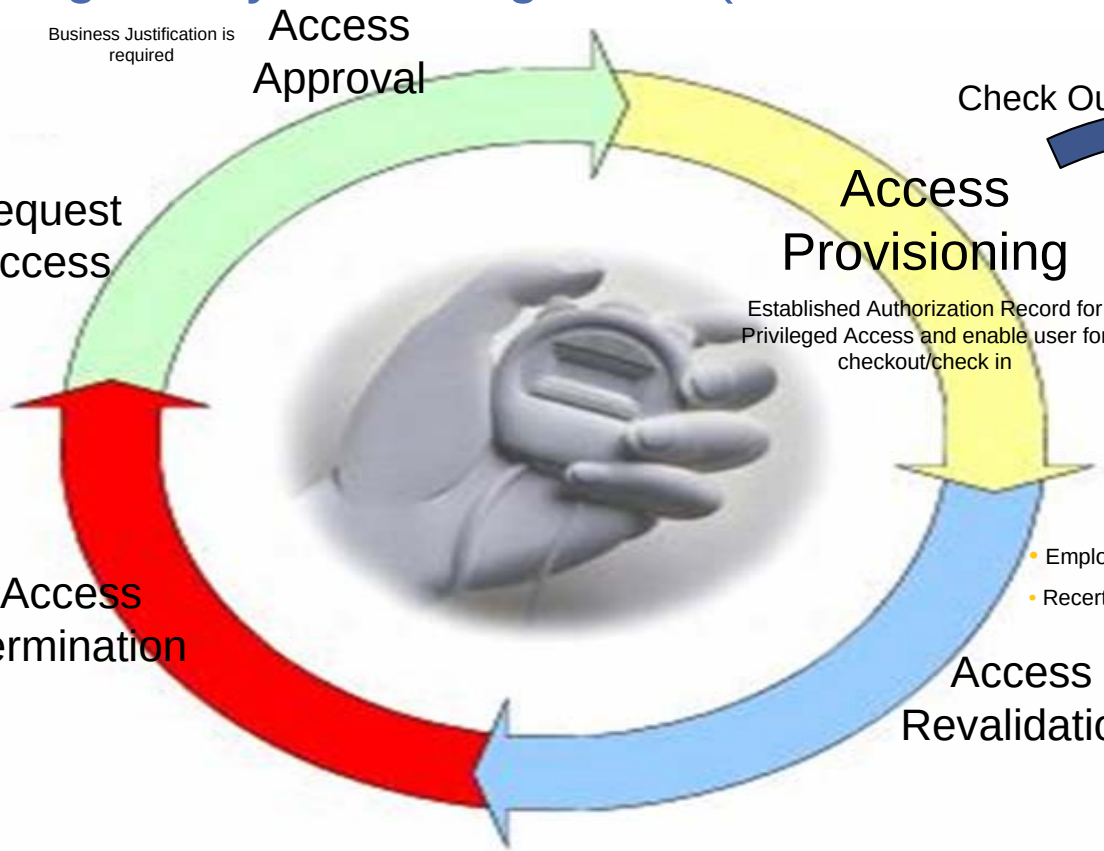


- Privileged ID accounts in ITIM are flagged and can be enabled for sharing.
- Specific Access Control is required for Privileged ID via ITIM ACI
- Specific Lifecycle workflows are required for lifecycle change events of shared ID (Create/Modify/PasswordChange/Suspend/Delete)
- Password Change needs to support privilege sharing

Shared Privilege lifecycle management (TIM)



Shared Privilege lifecycle management (TIM+TAM-ESSO)



Business Justification is required

Access Approval

Check Out

Check out and check in is triggered when user access native system via TAM-ESSO once the access is authorized in ITIM

User does not have to know the iD/password, it is provided by TAM-ESSO

Justification may be required based on the privilege type

Business Justification is required during access request

Request Access

Access Provisioning

Established Authorization Record for Privileged Access and enable user for checkout/check in

Check In

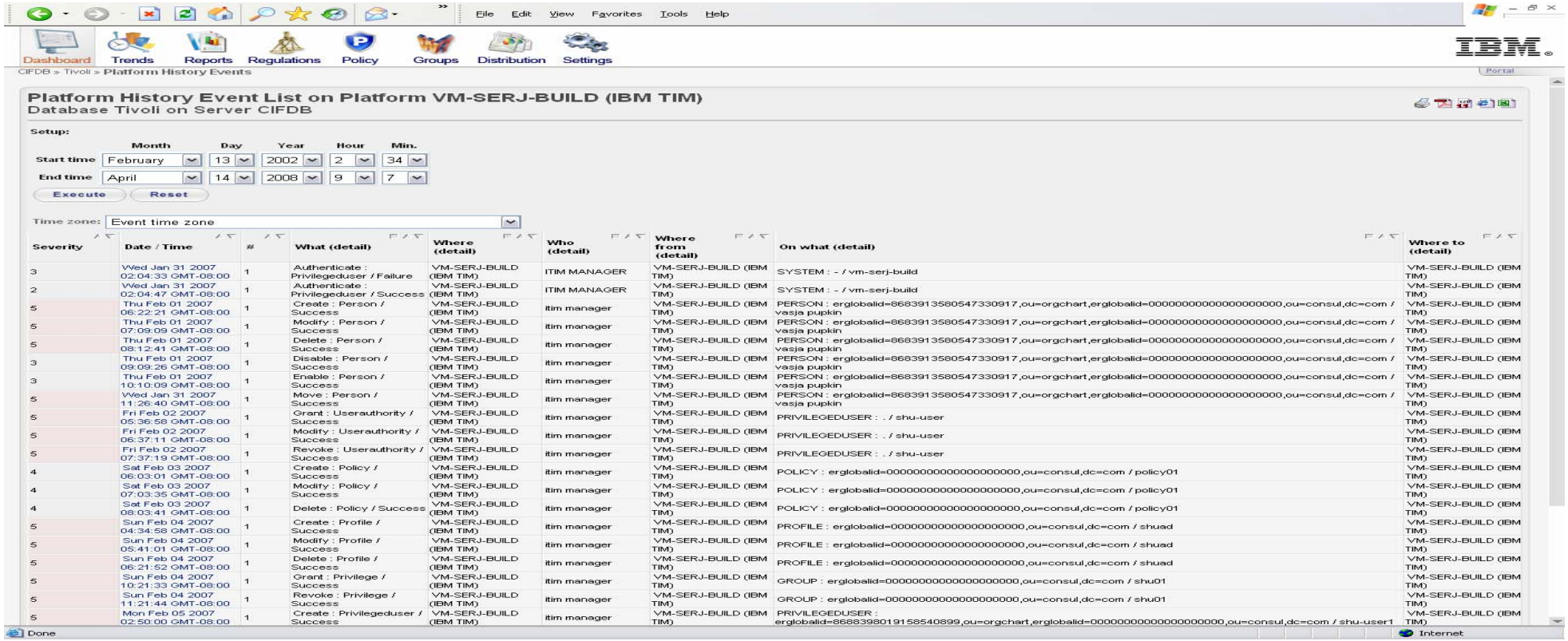
- Employment Verification
- Recertification Policy

Access Termination

Access Revalidation

Business Justification is required

Configuration changes to TIM



File Edit View Favorites Tools Help

Dashboard | Trends | Reports | Regulations | Policy | Groups | Distribution | Settings

CIFDB » Tivoli » Platform History Events

Platform History Event List on Platform VM-SERJ-BUILD (IBM TIM)

Database Tivoli on Server CIFDB

Setup:

	Month	Day	Year	Hour	Min.
Start time	February	13	2002	2	34
End time	April	14	2008	9	7

Execute Reset

Time zone: Event time zone

Severity	Date / Time	#	What (detail)	Where (detail)	Who (detail)	Where from (detail)	On what (detail)	Where to (detail)
3	Wed Jan 31 2007 02:04:33 GMT-08:00	1	Authenticate : Privilegeduser / Failure	VM-SERJ-BUILD (IBM TIM)	ITIM MANAGER	VM-SERJ-BUILD (IBM TIM)	SYSTEM : - / vm-serj-build	VM-SERJ-BUILD (IBM TIM)
2	Wed Jan 31 2007 02:04:47 GMT-08:00	1	Authenticate : Privilegeduser / Success	VM-SERJ-BUILD (IBM TIM)	ITIM MANAGER	VM-SERJ-BUILD (IBM TIM)	SYSTEM : - / vm-serj-build	VM-SERJ-BUILD (IBM TIM)
5	Thu Feb 01 2007 06:22:21 GMT-08:00	1	Create : Person / Success	VM-SERJ-BUILD (IBM TIM)	itim manager	VM-SERJ-BUILD (IBM TIM)	PERSON : erglobalid=8683913580547330917,ou=orgchart,erglobalid=00000000000000000000,ou=consul,dc=com / vasja pupkin	VM-SERJ-BUILD (IBM TIM)
5	Thu Feb 01 2007 07:09:09 GMT-08:00	1	Modify : Person / Success	VM-SERJ-BUILD (IBM TIM)	itim manager	VM-SERJ-BUILD (IBM TIM)	PERSON : erglobalid=8683913580547330917,ou=orgchart,erglobalid=00000000000000000000,ou=consul,dc=com / vasja pupkin	VM-SERJ-BUILD (IBM TIM)
5	Thu Feb 01 2007 08:12:41 GMT-08:00	1	Delete : Person / Success	VM-SERJ-BUILD (IBM TIM)	itim manager	VM-SERJ-BUILD (IBM TIM)	PERSON : erglobalid=8683913580547330917,ou=orgchart,erglobalid=00000000000000000000,ou=consul,dc=com / vasja pupkin	VM-SERJ-BUILD (IBM TIM)
3	Thu Feb 01 2007 09:09:26 GMT-08:00	1	Disable : Person / Success	VM-SERJ-BUILD (IBM TIM)	itim manager	VM-SERJ-BUILD (IBM TIM)	PERSON : erglobalid=8683913580547330917,ou=orgchart,erglobalid=00000000000000000000,ou=consul,dc=com / vasja pupkin	VM-SERJ-BUILD (IBM TIM)
3	Thu Feb 01 2007 10:10:09 GMT-08:00	1	Enable : Person / Success	VM-SERJ-BUILD (IBM TIM)	itim manager	VM-SERJ-BUILD (IBM TIM)	PERSON : erglobalid=8683913580547330917,ou=orgchart,erglobalid=00000000000000000000,ou=consul,dc=com / vasja pupkin	VM-SERJ-BUILD (IBM TIM)
5	Wed Jan 31 2007 11:26:40 GMT-08:00	1	Move : Person / Success	VM-SERJ-BUILD (IBM TIM)	itim manager	VM-SERJ-BUILD (IBM TIM)	PERSON : erglobalid=8683913580547330917,ou=orgchart,erglobalid=00000000000000000000,ou=consul,dc=com / vasja pupkin	VM-SERJ-BUILD (IBM TIM)
5	Fri Feb 02 2007 05:36:58 GMT-08:00	1	Grant : Userauthority / Success	VM-SERJ-BUILD (IBM TIM)	itim manager	VM-SERJ-BUILD (IBM TIM)	PRIVILEGEDUSER : . / shu-user	VM-SERJ-BUILD (IBM TIM)
5	Fri Feb 02 2007 06:37:11 GMT-08:00	1	Modify : Userauthority / Success	VM-SERJ-BUILD (IBM TIM)	itim manager	VM-SERJ-BUILD (IBM TIM)	PRIVILEGEDUSER : . / shu-user	VM-SERJ-BUILD (IBM TIM)
5	Fri Feb 02 2007 07:37:19 GMT-08:00	1	Revoke : Userauthority / Success	VM-SERJ-BUILD (IBM TIM)	itim manager	VM-SERJ-BUILD (IBM TIM)	PRIVILEGEDUSER : . / shu-user	VM-SERJ-BUILD (IBM TIM)
4	Sat Feb 03 2007 06:03:01 GMT-08:00	1	Create : Policy / Success	VM-SERJ-BUILD (IBM TIM)	itim manager	VM-SERJ-BUILD (IBM TIM)	POLICY : erglobalid=00000000000000000000,ou=consul,dc=com / policy01	VM-SERJ-BUILD (IBM TIM)
4	Sat Feb 03 2007 07:03:35 GMT-08:00	1	Modify : Policy / Success	VM-SERJ-BUILD (IBM TIM)	itim manager	VM-SERJ-BUILD (IBM TIM)	POLICY : erglobalid=00000000000000000000,ou=consul,dc=com / policy01	VM-SERJ-BUILD (IBM TIM)
4	Sat Feb 03 2007 08:03:41 GMT-08:00	1	Delete : Policy / Success	VM-SERJ-BUILD (IBM TIM)	itim manager	VM-SERJ-BUILD (IBM TIM)	POLICY : erglobalid=00000000000000000000,ou=consul,dc=com / policy01	VM-SERJ-BUILD (IBM TIM)
5	Sun Feb 04 2007 04:34:58 GMT-08:00	1	Create : Profile / Success	VM-SERJ-BUILD (IBM TIM)	itim manager	VM-SERJ-BUILD (IBM TIM)	PROFILE : erglobalid=00000000000000000000,ou=consul,dc=com / shuad	VM-SERJ-BUILD (IBM TIM)
5	Sun Feb 04 2007 05:41:01 GMT-08:00	1	Modify : Profile / Success	VM-SERJ-BUILD (IBM TIM)	itim manager	VM-SERJ-BUILD (IBM TIM)	PROFILE : erglobalid=00000000000000000000,ou=consul,dc=com / shuad	VM-SERJ-BUILD (IBM TIM)
5	Sun Feb 04 2007 06:21:52 GMT-08:00	1	Delete : Profile / Success	VM-SERJ-BUILD (IBM TIM)	itim manager	VM-SERJ-BUILD (IBM TIM)	PROFILE : erglobalid=00000000000000000000,ou=consul,dc=com / shuad	VM-SERJ-BUILD (IBM TIM)
5	Sun Feb 04 2007 10:21:33 GMT-08:00	1	Grant : Privilege / Success	VM-SERJ-BUILD (IBM TIM)	itim manager	VM-SERJ-BUILD (IBM TIM)	GROUP : erglobalid=00000000000000000000,ou=consul,dc=com / shu01	VM-SERJ-BUILD (IBM TIM)
5	Sun Feb 04 2007 11:21:44 GMT-08:00	1	Revoke : Privilege / Success	VM-SERJ-BUILD (IBM TIM)	itim manager	VM-SERJ-BUILD (IBM TIM)	GROUP : erglobalid=00000000000000000000,ou=consul,dc=com / shu01	VM-SERJ-BUILD (IBM TIM)
5	Mon Feb 05 2007 02:50:00 GMT-08:00	1	Create : Privilegeduser / Success	VM-SERJ-BUILD (IBM TIM)	itim manager	VM-SERJ-BUILD (IBM TIM)	PRIVILEGEDUSER : erglobalid=8688398019158540899,ou=orgchart,erglobalid=00000000000000000000,ou=consul,dc=com / shu-user1	VM-SERJ-BUILD (IBM TIM)

Done | Internet

Key Solution Functions
Combined Product and Services

- Centralized web-based management of Privileged IDs
  - Provisioning
  - Access management – who can access
  - Change password
  - Password reset
  - De-provisioning
  - Approval workflows
- Single Sign-on with Real-time Privileged ID Access Control
  - On demand check-in/check-out and verification of Privileged IDs
  - Single sign on to all systems with Privileged ID
  - Easy on boarding of applications through visual profiling
- Comprehensive audit trail and reporting
  - SQL logs for password provisioning, change, reset, de-provisioning
  - SQL logs for check in. check out cross by user and application

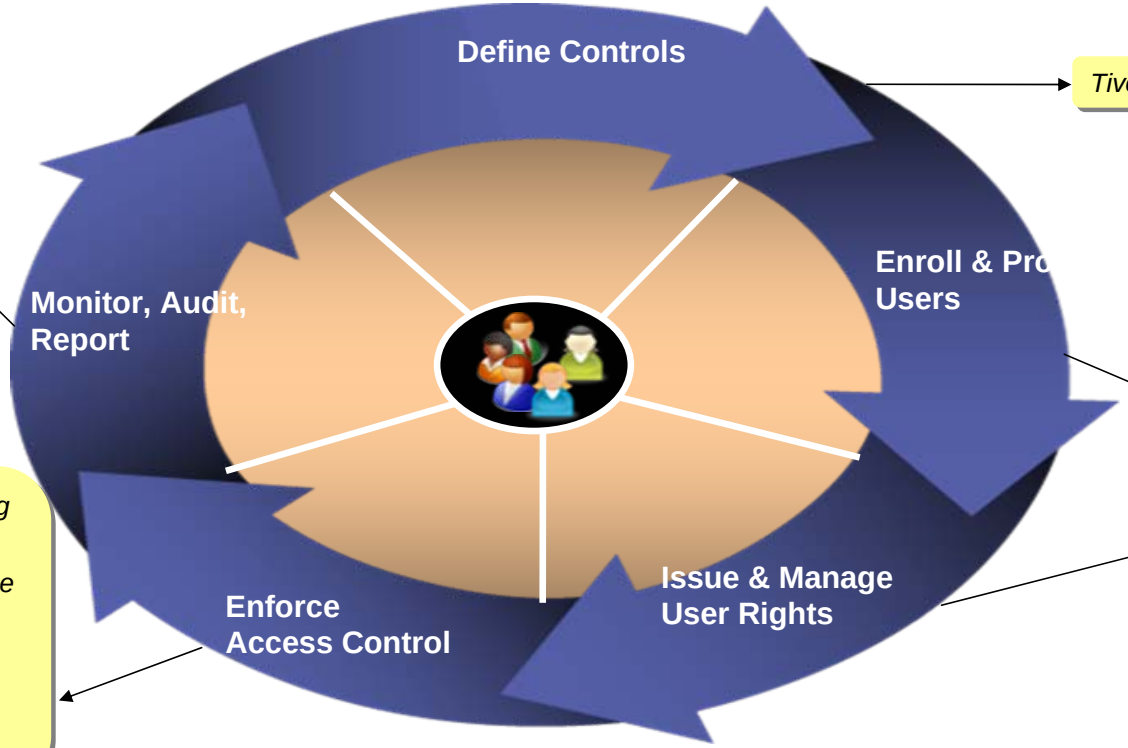
Key Benefits – Solution (TIM + TAM ESSO + Services)

- Comprehensive tracking and reporting enhances accountability and compliance
  - Provides technical controls for Individual Accountability by providing an entry log for the following tasks:
    - Check-Out function
    - Automatic log-on
    - Check-In function
    - Password Reset (when needed)
- Single sign on with automatic check in/check out improves user productivity
- Centralized Privileged ID management improves IT control
- Centralized password store enhances security
- SOAP interfaces with visual profiling simplifies deployment

Putting it all together
-Privileged Identity Management Solutions

- Leverage your IAM infrastructure
  - Approval workflows
  - Ensure password management/ regular password changes
  - Centralized ID management and password management and password store improves overall control and security
  - Password Reset
  - Tivoli Identity Manager helps here
- Exploit your SSO infrastructure
  - Utilise check-in/ check-out (see upcoming example)
  - Single sign-on of all privileged IDs
  - TAM ESSO helps here
- Access control
  - Limit the rights of privileged users
  - TAMOS helps here
- Leverage your SIM infrastructure
  - Audit real user access
  - Audit privileged identity access
  - Correlate and report
  - TCIM helps here

IBM Tivoli Identity, Access, and Audit Management Suite provides a complete solution for cost effective privileged identity management



Tivoli Security Policy Manager

Tivoli Compliance Insight Manager

Tivoli Identity Manager

Tivoli zSecure Family

IBM Entity Analytics

IBM RACF

Tivoli Access Manager for Operating Systems

Tivoli Access Manager for Enterprise Single Sign On

Tivoli Federated Identity Manager

Tivoli zSecure Family

IBM RACF

IBM has incorporated privileged identity management into its managed services security portfolio

Provisioning management …

- Delivers audit-ready compliance reports to help drive attestation and provide increased management visibility with **Tivoli Identity Manager 5.0**
- Eliminates the need to maintain expensive identity management and associated middleware skills on staff
- Offers a best-practice deployment model to speed return on investment and lower Total Cost of Ownership (TCO)
- Provides service level-based management to improve customer satisfaction and quality
- Enables enhanced functionality through IBM reusable assets
- Builds the foundation for other identity management initiatives such as single sign-on and federation
- Helps optimize investment using a transaction-based model and IBM financing
- Can plug in privileged monitoring using Tivoli Compliance Manager to see what the highest-risk accounts are doing

Control authorizations to privileged accounts on critical resources

IBM also offers a managed service for monitoring the use of privileged access

Privileged monitoring management …

- Provide centralized and demonstrable automated log collection and storage from heterogeneous sources
- Address demands of regulators and auditors by establishing clear audit trails for incident response, reducing the risks associated with security incidents and data breaches
- Monitor and audit the actions taken by privileged users, helping prevent costly damages or outages due to inadvertent mistakes or malicious actions
- Leverage market-leading technologies with **Tivoli Compliance Insight Manager**, services expertise and proven methodologies to deploy and manage an integrated security solution
- Benefit from lower total cost of ownership, accelerated deployment and simplified management through an extensible platform and scalable solutions

Monitor privileged activities on critical IT resources

IBM also can help clients deploy single sign-on solutions

Authentication management …

- Improve user productivity and enhance security bv decreasing number of passwords users have to remember for applications with **Tivoli Access Manager for Enterprise Single Sign On (E-SSO)**
- Decrease costs by reducing help desk calls
- Manage privileged access to critical devices with centralized policies and controls
- Centralized compliance reporting to include application access by user
- Accountability maintained through roaming desktop support for shared workstations

Manage authentication to privileged resources

IBM's unmatched security investment and worldwide skills deliver innovation and end to end solutions for our customers

InformationWeek
BUSINESS INNOVATION POWERED BY TECHNOLOGY

IBM Launches $1.5 Billion Security Initiative
The program is designed to recalibrate a customer's compliance and security offerings across IBM's five domains of information technology security.

By Thomas Claburn, InformationWeek
Nov. 1, 2007

IBM on Thursday announced a major security initiative encompassing products, services, and research to help businesses manage risk and keep information safe. To support the initiative, IBM said it plans to spend $1.5 billion on security-related projects in 2008. ...

Recent Acquisitions Strengthen Portfolio

SECURITY COMPLIANCE
- Demonstrable policy enforcement aligned to regulations, standards, laws, agreements (PCI, FISMA, etc.)

consul an IBM company

IDENTITY & ACCESS
- Enable secure collaboration with internal and external users with controlled and secure access to data, applications, and assets

ENCENTUATE Security Through Convenience

DATA SECURITY
- Protect and secure your data and information assets

princeton softech an IBM Company

APPLICATION SECURITY
- Continuously manage, monitor and audit application security

watchfire

INFRASTRUCTURE SECURITY
- Comprehensive threat and vulnerability management across networks, servers and end-points

INTERNET SECURITY SYSTEMS™

- 15,000 researchers, developers and SMEs on security initiatives
- 3,000+ security & risk management patents
- 200+ security customer references and 50+ published case studies
- 40+ years of proven success securing the zSeries environment

Questions?