Securing the Cloud through Comprehensive Identity Management Solution

Millie Mak
Senior IT Specialist
What is Cloud Computing?

A user experience and a business model
- Cloud computing is an emerging style of IT delivery in which applications, data, and IT resources are rapidly provisioned and provided as standardized offerings to users over the web in a flexible pricing model.

An infrastructure management and services delivery methodology
- Cloud computing is a way of managing large numbers of highly virtualized resources such that, from a management perspective, they resemble a single large resource. This can then be used to deliver services with elastic scaling.
An Effective Cloud Deployment is Built on a Dynamic Infrastructure ….

...leveraging virtualization, standardization and automation to free up operational budget for new investment.
Customer Concerns with Cloud Computing *

- **LOSS OF GOVERNANCE:**
  - Customer *relinquishes some control over the infrastructure.*
  - **TRUST in the provider** is paramount. Providers’ experience with outsourcing provides evidence of trust.

- **COMPLIANCE RISKS:**
  - Ability to achieve compliance depends on providers’ operational characteristics.

- **ISOLATION FAILURE:**
  - Multi-tenancy and shared resources are defining characteristics of cloud computing.
  - This risk category covers the *failure of mechanisms separating storage, memory, routing and even reputation between different tenants* (e.g., so-called guest-hopping attacks).

* 2009 European Network and Information Security Agency (ENISA)
Cloud Computing: Benefits, risks and recommendations for information security

© 2010 IBM Corporation
Customer Concerns with Cloud Computing *

- **DATA HANDLING**
  - **DATA PROTECTION:**
    - Demonstrable assurance to the customer that their data is maintained securely from other tenants of the cloud
  - **INSECURE or INCOMPLETE DATA DELETION:**
    - Ensure that data is deleted in a manner that does not allow leakage upon re-allocation

- **MANAGEMENT INTERFACE COMPROMISE:**
  - Increased risk as management interface accessible through Internet and mediate access to larger sets of resources (than traditional hosting providers), when combined with remote access and web browser vulnerabilities

- **MALICIOUS INSIDER:**
  - New tier of highly privileged user in cloud infrastructure
  - Providers’ operations, monitoring and incident handling build trust with the customer. Providers’ history of running outsourcing contracts also builds trust.

* 2009 European Network and Information Security Agency (ENISA)
Cloud Computing: Benefits, risks and recommendations for information security

© 2010 IBM Corporation
What are the Primary Data Protection Requirements?

- Data will be
  - Stored in **multi-tenant environments**, spanning multiple layers in the cloud stack
  - Accessed by various parties of **different trust levels** (users, tenants, privileged cloud admins)
  - **May not be located at customer’s site**
  - Enforced by **various contractual obligations and SLAs**
  - Governed by **various regulations and industry best practices**
  - Secured by **multiple technologies and services**

- Cloud users expect
  - High degree of **agility and flexibility**
  - Very **simple and standardized security management**
  - **Easy integration** with existing enterprise security management and infrastructure
  - Appropriate level of **control and assurance**
IBM Security Framework
– Business-oriented framework on security concerns

Built to meet four key requirements:

- Provide **Assurance**
- Enable **Intelligence**
- Automate **Process**
- Improve **Resilience**

Identity Management Requirements in Cloud environment

• **Web Access Control**
  - Shared Web access control Infrastructure for multiple web applications in the Cloud
  - Policy-based Access Control across wide range of Web resources
  - Single Sign-On for multiple Web Applications in the Cloud
  - Multi-tenant support

• **Federated Identity / On-boarding**
  - Coordinating authentication and authorization with enterprise or third party systems
  - Trust between SOA-based initiatives by connecting users to services across business domains
  - Standards-based Single Sign-On across web domains

• **Life-cycle Identity Management**
  - Enables common model of identity, entitlements, obligations and policy
  - Automatic role based user access life-cycle management
  - Periodic policy validation
  - Auditing of all user provisioning operations
Identity Management Requirements in Cloud environment

• **Privileged User Monitoring**
  • Especially privileged administrators of Cloud provider
    - Logging Activities
    - Physical Monitoring
    - Background Checking

• **Security Governance, Risk Management and Compliance**
  • 3rd-party audit (ISO27001, PCI-DSS, etc)
  • Client access to tenant-specific log and audit data
  • Effective incident reporting for tenants
  • Visibility into change, incident, image management, etc.
  • SLAs, option to transfer risk from tenant to provider
  • Support for forensics
Integrated Identity Management Service on Cloud

Access Management
- Enterprise Access Management
- Web Access Management
- Federated Access Management
- OS/Network Resource Access

Identity Management
- Provisioning/De-provisioning
- Entitlement Management
- Recertification, Reconciliation
- User Self Service
- Role Management
- Privileged User Management

Audit and Compliance Reporting
- Automated Log Management
- Privileged User Monitoring
- Compliance Management Modules
- Reporting

Legend
- Multi-tenants, Web Based Administration
People and Identity – Access Management

**Tivoli Access Manager for e-business (TAMeb)**

**Summary:** Access management and single sign-on solution that manages the difficulty of executing security policies across a wide range of Web and application resources.

**Cloud Use Case:** Provides validation and processing of user identity information. Addresses the need of authentication of users within the cloud ecosphere. Defines and manages centralized authentication, access and audit policy with access management.

![Diagram showing the interaction between Service Requestor, Service Provider, TAMeb, Service Management, Systems and Image Management, Computing Infrastructure, Systems, Storage, and Network.](image-url)
Tivoli Access Manager for e-business

*An integrated security platform for Web-based e-business*

- **Authentication**: Lets the right people in with support to strong authentication mechanisms
- **Authorization**: Controls access to applications and data
- **Single sign-on (SSO)**: to Web-based applications
- **Integration** with Web, J2EE, and .Net application environments
- **Unified, policy-based administration**
  - Users, access, portals, Web applications, custom applications
- **Audits** all logins and resource access
- **High availability** for critical online and multi-enterprise deployments
- **Multi-tenant** Support
People and Identity – Access Management

Tivoli Federated Identity Manager (TFIM)

**Summary:** TFIM enables trust between SOA-based initiatives by connecting users to services across business domains and helps enterprises strengthen and automate user access rights.

**Cloud Use Case:** In massively parallel, cloud-computing infrastructures, which involve enormous pools of external users constantly logging in to leverage IT services, TFIM’s many authentication management features deliver significant business value.
Tivoli Federated Identity Manager Architecture

**Federated Single Sign-On**
- Secure user interaction
  - Web Portal
  - Web Application

**Federated Web Services**
- Secure application interaction
  - Portal
  - App
  - Gateway

**Federated Provisioning**
- Provisioning System
- Database
- Provisioning System

**Trust infrastructure**
- Business agreements
- Legal agreements
- Technical implementation
  - Transport: SSL/TLS, WS-Sec
  - Message: sign/encrypt
  - Tokens: sign/encrypt
Federated Single Sign-On

- **Identity Provider (IdP)**
  - creates, maintains, and manages identity information for users and provides user authentication to other service providers within a circle of trust.

- **Service Provider (SP)**
  - provides services and/or goods to users.
Federated Web Services

- Key security requirements for both inbound & outbound requests:
  - Security Token Mapping
  - Identity Mapping
Current federated provisioning deployments typically involve non real-time solutions for provisioning
   – E.g. weekly tapes, daily ftp of files.

New cloud business models will require closer to real-time provisioning and just-in-time provisioning solutions

Standards bodies have recently taken up provisioning related issues
   – WS-Provisioning / WS-Notification
   – SPML V2.0
   – Liberty
Summary: Tivoli Identity Manager provides policy-based identity life-cycle management of systems and applications. It manages user entitlements ensuring policy compliance of user access.

Cloud Use Case: Allows fast and accurate policy-based user access provisioning from privileged users to end users of cloud computing services, with comprehensive auditing to ensure compliance.
Tivoli Identity Manager
- Automate user privileges life-cycle across IT infrastructure

Reduce Costs
- Self-service password reset
- Automated user provisioning

Simplify Complexity
- Consistent security policy
- Quickly integrate new users & apps

Address Compliance
- Closed-loop provisioning
- Access rights audit & reports

• Know the **people** behind the accounts and **why** they have the access they do
• Fix non-compliant accounts
• Automate user privileges life-cycle across entire IT infrastructure
• Match your workflow processes

Detect and correct local privilege settings
Accounts on different types of Systems Managed, Managed, Plus, In-House Systems & portals

© 2010 IBM Corporation
### Tivoli Security Information and Event Manager (TSIEM)

**Summary:** Tivoli Security Information and Event Manager enables corporations to compile event and log files from network, applications and operating systems, as well as security technologies, into one seamless platform – administered from an easy-to-use Web portal.

**Cloud Use Case:** Improves the speed of conducting security investigation and archives forensically-sound data, admissible as evidence in a court of law, for a period up to seven years.

---

#### Cloud Computing Infrastructure

- **Systems**
- **Storage**
- **Network**
- **Apps**

---

#### Tivoli Security Information and Event Manager

© 2010 IBM Corporation
Tivoli Security Information and Event Manager

The IBM Tivoli SIEM Solution

People
- privileged users
- outsourcers
- trusted users
- consultants
- intruders

Technology
- Applications
- Databases
- Operating Systems
- Mainframe
- Security Devices
- Network Devices
- Desktop

Manage Logs
- Collect & Store
- Investigate & Retreive
- Log Continuity Report™
- Real Time Collection

Monitor, Audit & Report
- User Activity Monitoring
- Security Event Correlation

Compliance Dashboard
- Custom
- Best Practices
- Compliance

Policy

Management Modules
- ISO27001
- BASEL II
- PCI-DSS
- HIPAA
- GLBA
- SOX
- FISMA

Security Operations Dashboard

© 2010 IBM Corporation
Log Continuity Report
Instant proof to auditors and regulators that your log management program is complete and continuous.
# TSIEM Policy Management

## Policy Template

Download this template to use in the management console.

<table>
<thead>
<tr>
<th>Policy Rules</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Who group</strong></td>
<td><strong>What group</strong></td>
</tr>
<tr>
<td>Sales Management</td>
<td></td>
</tr>
<tr>
<td>Administrators</td>
<td></td>
</tr>
<tr>
<td>Marketing</td>
<td>Office Hours</td>
</tr>
<tr>
<td>HR Management</td>
<td>Out of Office Hours</td>
</tr>
<tr>
<td>Logon</td>
<td></td>
</tr>
<tr>
<td>HR Staff</td>
<td>Office Hours</td>
</tr>
<tr>
<td>Managers</td>
<td>Office Hours</td>
</tr>
<tr>
<td>System Operations</td>
<td></td>
</tr>
<tr>
<td>System Processes</td>
<td></td>
</tr>
<tr>
<td>Users</td>
<td>Office Hours</td>
</tr>
<tr>
<td>Sales Staff</td>
<td>Office Hours</td>
</tr>
<tr>
<td>Finance Staff</td>
<td>Office Hours</td>
</tr>
<tr>
<td>IT</td>
<td></td>
</tr>
</tbody>
</table>

## Attention Rules

<table>
<thead>
<tr>
<th>Attention Rules</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Who group</strong></td>
<td><strong>What group</strong></td>
</tr>
<tr>
<td>HR Management</td>
<td>Office Hours</td>
</tr>
<tr>
<td>Intrusion - Medium</td>
<td></td>
</tr>
<tr>
<td>Customer Information Systems</td>
<td></td>
</tr>
<tr>
<td>Administrators</td>
<td>HR - Medium</td>
</tr>
<tr>
<td>Administrators</td>
<td>Financial - Medium</td>
</tr>
<tr>
<td>Administrators</td>
<td>Customer Data - High</td>
</tr>
<tr>
<td>Administrators</td>
<td>Financial - Low</td>
</tr>
</tbody>
</table>

© 2010 IBM Corporation
Compliance Dashboard
Logs after W7 – Billions of log files summarized on one overview graphic!
Regulation specific modules with tailored reports to jumpstart your compliance efforts – saving you staff time and reducing audit costs

<table>
<thead>
<tr>
<th>Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sarbanes Oxley (FFIEC 1.1.1.4) Security Policy report</td>
<td>No description given</td>
</tr>
<tr>
<td>Sarbanes Oxley (FFIEC 1.3.1.1) Classification report</td>
<td>No description supplied</td>
</tr>
<tr>
<td>Sarbanes Oxley (6.3. 8.13) Security alert</td>
<td>Alerts sent in response to policy exceptions or special attention exceptions.</td>
</tr>
<tr>
<td>Sarbanes Oxley (8.1.2) Operational change control</td>
<td>Changes to the operating environment such as system updates, DBA activity etc.</td>
</tr>
<tr>
<td>Sarbanes Oxley (8.1.6) External contractors</td>
<td>Exceptions and failures caused by External Contractors.</td>
</tr>
<tr>
<td>Sarbanes Oxley (8.3) Malicious attacks</td>
<td>Exceptions and failures due to Malicious attacks.</td>
</tr>
<tr>
<td>Sarbanes Oxley (8.4.2) Operator log</td>
<td>Actions performed by the IT Admin staff.</td>
</tr>
<tr>
<td>Sarbanes Oxley (8.4.5) Remote diagnostic port access</td>
<td>Detection of accesses to the diagnostic ports on servers.</td>
</tr>
<tr>
<td>Sarbanes Oxley (8.5.3) User identification and authentication</td>
<td>Login/Logoff successes and failures.</td>
</tr>
<tr>
<td>Sarbanes Oxley (8.5.5) System utilities</td>
<td>Usage of system utilities</td>
</tr>
<tr>
<td>Sarbanes Oxley (9.6) Application access control</td>
<td>Actions, Exceptions and events on HR Data, Sensitive Data, User Sensitive Data, System, Financial Data, Proprietary Data and General Data.</td>
</tr>
<tr>
<td>Sarbanes Oxley (9.6.1) Information access restrictions</td>
<td>Who accessed sensitive or private data successfully or unsuccessfully.</td>
</tr>
<tr>
<td>Sarbanes Oxley (9.6.2) Sensitive system isolation</td>
<td>Exceptions and failures against sensitive systems data in asset groups User, HR Data, Source Code, and Financial Data.</td>
</tr>
<tr>
<td>Sarbanes Oxley (9.7.2.3) Logging and reviewing events</td>
<td>Exceptions and failures recorded by the InSight system.</td>
</tr>
<tr>
<td>Sarbanes Oxley (9.8.1) Mobile worker</td>
<td>Exceptions and failures for mobile workers.</td>
</tr>
</tbody>
</table>
Operational Change Control Report
See a summary of all the operational changes made by different groups.
Event List
Zoom in into the all actions that IT admin did on the financial Server and see the creation of the user account of Chin055

<table>
<thead>
<tr>
<th>Severity</th>
<th>When</th>
<th>#</th>
<th>What</th>
<th>Where</th>
<th>Who</th>
<th>from Where</th>
<th>on What</th>
<th>Where to</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Tue Oct 24 2006 14:32:44 GMT+02:00</td>
<td>1</td>
<td>Grant: Privilege / Success</td>
<td>SRV_DC_034 (Windows)</td>
<td>Mike Bonfire</td>
<td>WS_03442 (Windows)</td>
<td>USER: David088 / David088</td>
<td>SRV_DC_034 (Windows)</td>
</tr>
<tr>
<td>2</td>
<td>Tue Oct 24 2006 16:09:39 GMT+02:00</td>
<td>1</td>
<td>Grant: Privilege / Success</td>
<td>SRV_DC_034 (Windows)</td>
<td>Mike Bonfire</td>
<td>WS_03442 (Windows)</td>
<td>USER: David088 / David089</td>
<td>SRV_DC_034 (Windows)</td>
</tr>
<tr>
<td>2</td>
<td>Tue Oct 24 2006 16:20:49 GMT+02:00</td>
<td>1</td>
<td>Grant: Privilege / Success</td>
<td>SRV_DC_034 (Windows)</td>
<td>Jim Hoffman</td>
<td>WS_03442 (Windows)</td>
<td>USER: Administrator / Administrator</td>
<td>SRV_DC_034 (Windows)</td>
</tr>
<tr>
<td>2</td>
<td>Tue Oct 24 2006 16:20:52 GMT+02:00</td>
<td>1</td>
<td>Grant: Privilege / Success</td>
<td>SRV_DC_034 (Windows)</td>
<td>Jim Hoffman</td>
<td>WS_03442 (Windows)</td>
<td>USER: Administrator / Administrator</td>
<td>SRV_DC_034 (Windows)</td>
</tr>
<tr>
<td>2</td>
<td>Sat Oct 28 2006 11:21:26 GMT+02:00</td>
<td>1</td>
<td>Grant: Privilege / Success</td>
<td>SRV_DC_034 (Windows)</td>
<td>Jim Hoffman</td>
<td>SRV_DC_034 (Windows)</td>
<td>USER: Administrator / Administrator</td>
<td>SRV_DC_034 (Windows)</td>
</tr>
<tr>
<td>2</td>
<td>Sat Oct 28 2006 11:21:49 GMT+02:00</td>
<td>1</td>
<td>Grant: Privilege / Success</td>
<td>SRV_DC_034 (Windows)</td>
<td>Mike Bonfire</td>
<td>SRV_DC_034 (Windows)</td>
<td>USER: Administrator / Administrator</td>
<td>SRV_DC_034 (Windows)</td>
</tr>
<tr>
<td>2</td>
<td>Tue Oct 31 2006 08:03:02 GMT+02:00</td>
<td>1</td>
<td>Grant: Privilege / Success</td>
<td>SRV_DC_034 (Windows)</td>
<td>Max Doane</td>
<td>SRV_DC_034 (Windows)</td>
<td>USER: Richard019 / Richard019</td>
<td>SRV_DC_034 (Windows)</td>
</tr>
<tr>
<td>2</td>
<td>Tue Oct 31 2006 08:03:02 GMT+02:00</td>
<td>1</td>
<td>Grant: Privilege / Success</td>
<td>SRV_DC_034 (Windows)</td>
<td>Max Doane</td>
<td>SRV_DC_034 (Windows)</td>
<td>USER: Richard019 / Richard019</td>
<td>SRV_DC_034 (Windows)</td>
</tr>
<tr>
<td>2</td>
<td>Tue Oct 31 2006 08:05:01 GMT+02:00</td>
<td>1</td>
<td>Grant: Privilege / Success</td>
<td>SRV_DC_034 (Windows)</td>
<td>Jim Hoffman</td>
<td>SRV_DC_034 (Windows)</td>
<td>USER: Chin055 / Chin055</td>
<td>SRV_DC_034 (Windows)</td>
</tr>
<tr>
<td>2</td>
<td>Tue Oct 31 2006 08:05:01 GMT+02:00</td>
<td>1</td>
<td>Grant: Privilege / Success</td>
<td>SRV_DC_034 (Windows)</td>
<td>Jim Hoffman</td>
<td>SRV_DC_034 (Windows)</td>
<td>USER: Chin055 / Chin055</td>
<td>SRV_DC_034 (Windows)</td>
</tr>
<tr>
<td>2</td>
<td>Tue Oct 31 2006 08:05:01 GMT+02:00</td>
<td>1</td>
<td>Grant: Privilege / Success</td>
<td>SRV_DC_034 (Windows)</td>
<td>Joe Security</td>
<td>SRV_DC_034 (Windows)</td>
<td>USER: Sean031 / Sean031</td>
<td>SRV_DC_034 (Windows)</td>
</tr>
<tr>
<td>2</td>
<td>Tue Oct 31 2006 08:05:01 GMT+02:00</td>
<td>1</td>
<td>Grant: Privilege / Success</td>
<td>SRV_DC_034 (Windows)</td>
<td>Joe Security</td>
<td>SRV_DC_034 (Windows)</td>
<td>USER: Sean031 / Sean031</td>
<td>SRV_DC_034 (Windows)</td>
</tr>
<tr>
<td>2</td>
<td>Tue Oct 31 2006 08:10:00 GMT+02:00</td>
<td>1</td>
<td>Grant: Privilege / Success</td>
<td>SRV_DC_034 (Windows)</td>
<td>Mike Bonfire</td>
<td>SRV_DC_034 (Windows)</td>
<td>USER: Rick053 / Rick053</td>
<td>SRV_DC_034 (Windows)</td>
</tr>
<tr>
<td>2</td>
<td>Tue Oct 31 2006 08:10:00 GMT+02:00</td>
<td>1</td>
<td>Grant: Privilege / Success</td>
<td>SRV_DC_034 (Windows)</td>
<td>Mike Bonfire</td>
<td>SRV_DC_034 (Windows)</td>
<td>USER: Rick053 / Rick053</td>
<td>SRV_DC_034 (Windows)</td>
</tr>
<tr>
<td>2</td>
<td>Tue Oct 31 2006 08:30:00 GMT+02:00</td>
<td>1</td>
<td>Grant: Privilege / Success</td>
<td>SRV_DC_034 (Windows)</td>
<td>Mike Bonfire</td>
<td>SRV_DC_034 (Windows)</td>
<td>USER: Rabh037 / Rabh037</td>
<td>SRV_DC_034 (Windows)</td>
</tr>
<tr>
<td>2</td>
<td>Tue Oct 31 2006 08:30:00 GMT+02:00</td>
<td>1</td>
<td>Grant: Privilege / Success</td>
<td>SRV_DC_034 (Windows)</td>
<td>Mike Bonfire</td>
<td>SRV_DC_034 (Windows)</td>
<td>USER: Rabh037 / Rabh037</td>
<td>SRV_DC_034 (Windows)</td>
</tr>
</tbody>
</table>
An Event Detail Report
Even drill down into that specific event and see all the event details, and we can even go to the raw log-file.
Tivoli Information and Event Manager Capability in the Cloud

“I need to store logs for forensics”

“I have no idea which logs to collect or how”

“Comprehend: My staff lacks the time, expertise, and desire to scan logs”

“I’m concerned about privileged actions”

“I need to provide reports to my auditors and regulators”

“I need to prove that I have effective IT security controls”

“I have no idea which logs to forensics or how”

Gain Control, Achieve Compliance

© 2010 IBM Corporation
Why IBM for Identity Management in Cloud environment?

**Because IBM solution**
- Delivers integrated security management solution
- Simplifies administration through a unified identity management solution
- Provides rapid deployment of consistently secure applications based on a single security model in the Cloud
- Improves governance and simplifies compliance management
- Delivers common security management best practices and industry leadership

**Tivoli Security Management Solution for Cloud Infrastructure**

**Intelligent Management Software that Integrates and Automates**