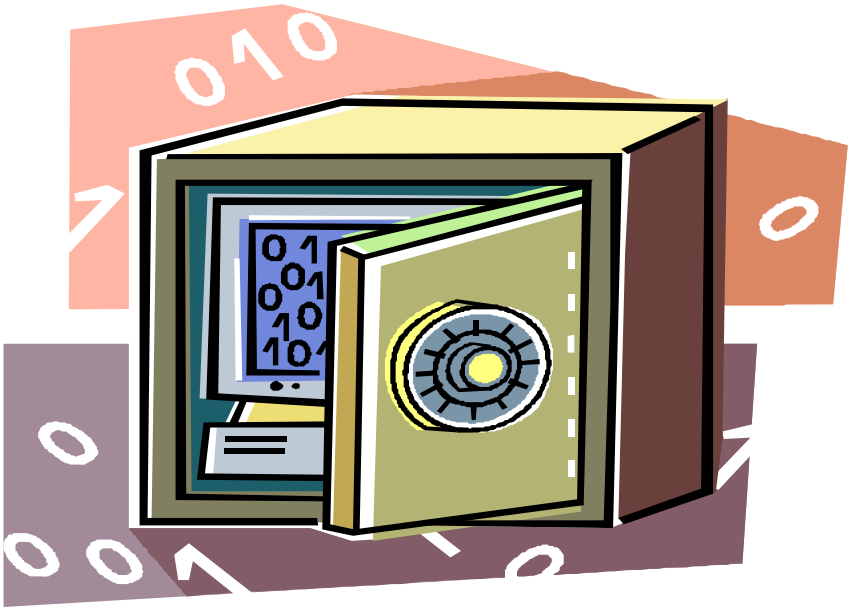
Tendances Logicielles

L'architecture pour répondre aux besoins métier

Pierre Noël

Worldwide Executive, Information Security & Risk Management

Comment Sécuriser entièrement votre système informatique?



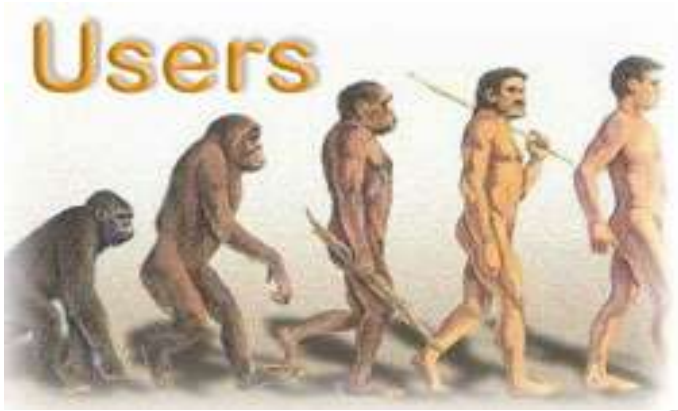
Facile!

Là où ça ce complique

Les Règles de Bases pour sécuriser un environnement informatique

- Qui est-ce?
- A-t-elle le droit?
- Les murs ont-ils des oreilles?
- Sommes-nous conformes aux règles?

Evolution de la sécurité des systèmes



Systèmes propriétaires

TCPIP

Internet

SOA

Evolution

- Ouverture / interopérabilité / Standards
- Besoin d'Authentification Explicite – environnement ouvert
- Retour vers la centralisation des autorisations
- Intégrité et Confidentialité Explicite – environnement ouvert
- Le nombre d'intervenants dans une transaction détermine la complexité d'audit / conformité

Gestion des Identités sous SOA

QUI EST-CE?

Problème d'intégration des identités…

Partners using WS-Federation

Partners using Liberty

Partners using SAML in their Portal or Web

Partners using WS-Security

"Identité"

"Identité"

"Identité"

"Identité"

Multi Protocol Federation Gateway

"Identité"

"Identité"

"Identité"

SAP Platform

WebSphere Platform

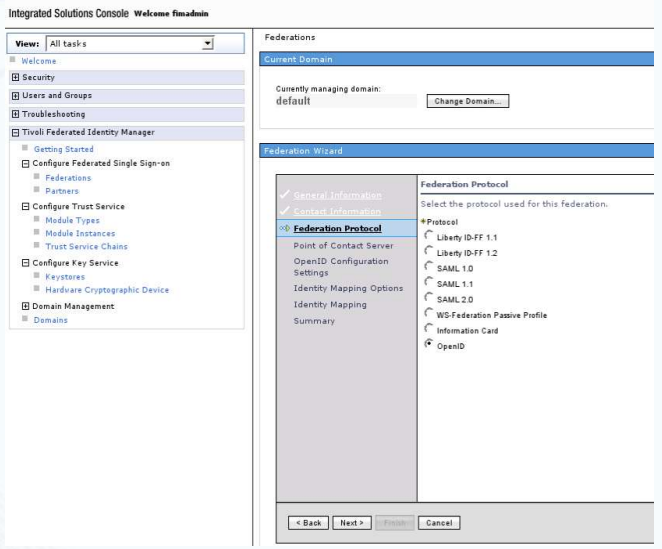
MS .NET Platform

La Gestion des Identités est nécessaire dans le cadre des interactions intra et inter métiers

Tivoli Federated Identity Manager

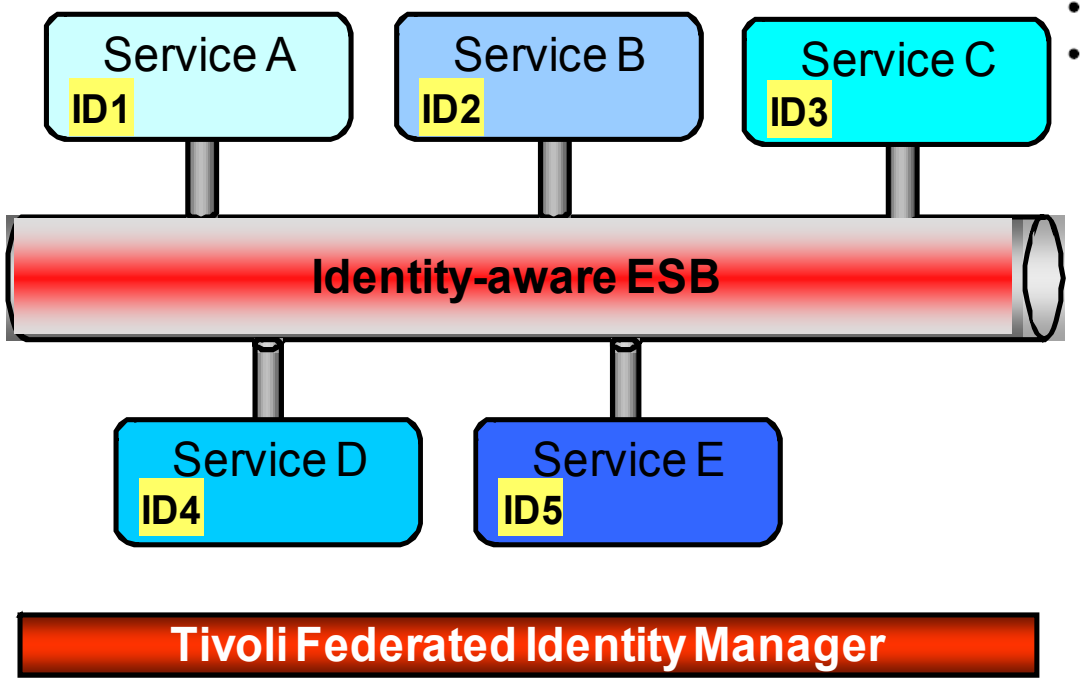
Services de Sécurité et d'Identité pour environnement SOA

- **Single Sign-On (SSO)**
  - Browser-based SSO fédéré
  - Médiateur d'identités pour Services Web
    - Médiation d'identités entre domaines
    - Conversion de formats entre domaines
    - Interface vers les systèmes d'autorisation
- **Service de Gestion des Identités**
  - Security Token Service (STS) basé sur WS-Trust
  - Gestion intégrée des identités, formats et protocoles entre demandeurs de services et fournisseurs de services



La Solution IBM Tivoli Federated Identity Manager

IBM Tivoli Federated Identity Manager fournit un modèle simple de gestion des identités et d'accès aux ressources



La solution la plus complète sur le marché

- Liberty ID-FF 1.x (Compliant), SAML 1.0, 1.1, 2.0, WS-Federation

Support natif pour les principales plateformes du marché

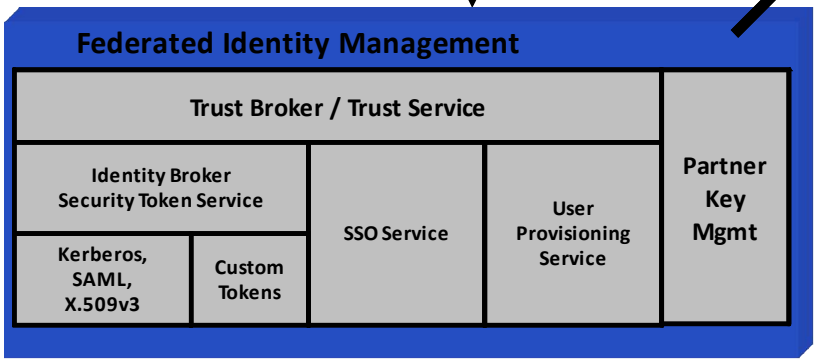
- z/OS support y inclus RACF PassTicket pour CICS et transactions IMS
- Microsoft .NET et SharePoint
- Support SAML certifié pour SAP

Caractéristiques

- Complète la sécurité entre systèmes et architectures différentes
- Meilleure intégration utilisateurs et augmentation de la productivité
- Automatise l'intégration des identités entre différentes plateformes
- Simplifie les aspects d'audits et conformité
- Réduit le coût en relation avec la gestion des identités (y compris appels help desk)

Scénario d'utilisation

Federated SSO – .NET et WebSphere Application Server



Scénario

- [1]L'utilisateur s'authentifie sur MyHR.com et accède à des services à travers le portail
- [2]La gestion des identités dans l'environnement MyHR est gérée par TFIM
- [3]Dans le cadre de sa session, l'utilisateur accède à un site externe – Options.com
- [4]TFIM génère et communique les informations d'authentification de manière sécurisée afin que Options.com puisse prendre des décisions d'autorisation

Intégrité et Confidentialité sous SOA

LES MURS ONT-ILS DES OREILLES?

XS40 XML Security Gateway

Intégrité et Confidentialité sous SOA

- Périphérique réseau conçu ad hoc par quelques-uns des plus grands experts mondiaux XML afin d'aider à sécuriser les transactions à base de XML et de services Web, XS40 met à disposition un jeu complet de fonctions comme
  - la prise en charge de WS-Security
  - la cryptographie XML
  - un pare-feu et des filtres XML/SOAP
  - la signature numérique du XML
  - la validation par schéma XML
  - le SSL à deux voies
  - le contrôle des accès XML, XPath et la journalisation détaillée.

Gestion des Autorisations et Accès sous SOA

A-T-ELLE LE DROIT?

Tivoli Security Policy Manager V7.0

Pour les architectes, les développeurs et responsables entité métier

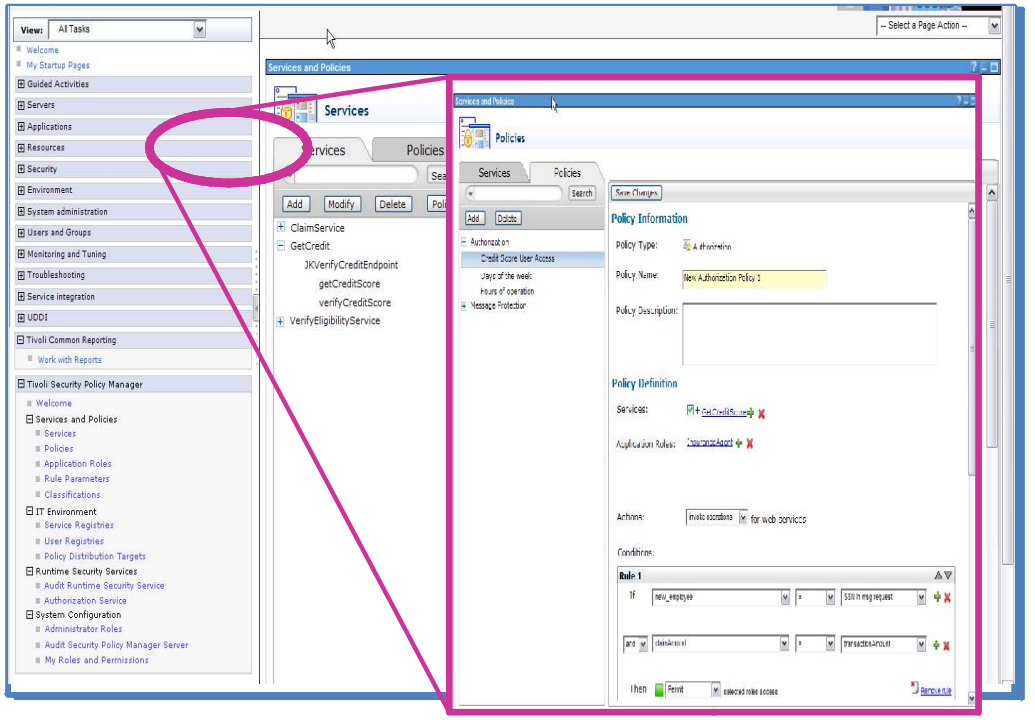
- La gestion des autorisations et accès se fait de manière centralisée
- Simplification des procédures d'audit et conformité

Pour la gestion des opérations

- Augmentation de la sécurité et gouvernance opérationnelle avec un système de gestion des politiques de sécurité unifié

Interopérabilité et conformité aux standards

- XACML pour la gestion des accès.
- WS-Policy, WS-SecurityPolicy pour la sécurité SOA



Visibilité

- Vue unique des rôles, autorisations et accès (data level) au niveau de l'entité métier (Line of Business)

Contrôle

- Système de gestion des règles et politiques centralisé

Automatisation

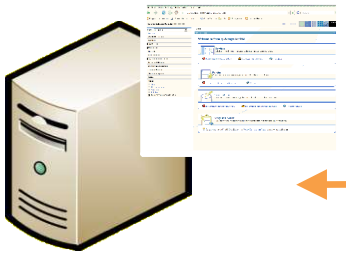
- Elimine le besoin de coder les règles et gestion d'accès au niveau applicatif – gestion centralisée

Scenario 1 – Enabling Application Owners to Easily Implement Entitlements for New Applications

Examples: Business Policy

- Doctors in the role of a Primary Care Physician (PCP) can view/update only their patient's record.
- Insurance Agents as claims approver (*role*) during business hours (*environment*) for their own clients (*identity*) if the value of the claim is less than approved limit (*service-level*) and the claim is approved by the fraud detection rules-based system (*external rule*).

1



• ***Author*** *and* ***manage*** *entitlements*
• *Authorization (XACML)*

Application Owner

Tivoli Security Policy Manager

Authorization service acts as ***policy decision point***

Security policies are distributed to Application Server

2

Enforce *the updated policy locally using TSPM run-time security service (RTSS)*

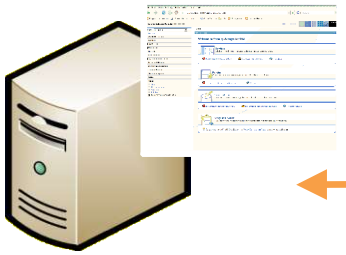
Application Server
(e.g. WAS, .NET, BEA…)

"Ability to manage & enforce entitlements consistently"

Scenario 2 – Enabling IT Operations to Centrally Manage Web Services Access Control and Drive Governance and Compliance

Examples: Services Policy

- Which service can a user access?
- All incoming messages need to be signed, and tokens encrypted
- Need to validate and authenticate users with diverse user credentials

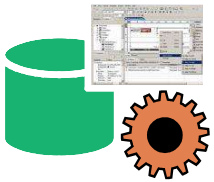


- ***Author*** *&* ***manage*** *security policies & configuration*
  - *For message security (WS-SecurityPolicy)*

IT Operations

Tivoli Security Policy Manager

Obtain ***service definition and metadata*** *from WSRR*



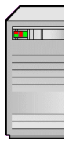
WebSphere Service Registry and Repository

Authorization service acts as ***policy decision point***

Security policies are distributed to DataPower

DP queries RR and configures itself

Enforce *the updated policy*



Service Consumer
(e.g. FinancialAgents)

WebSphere DataPower SOA Appliance

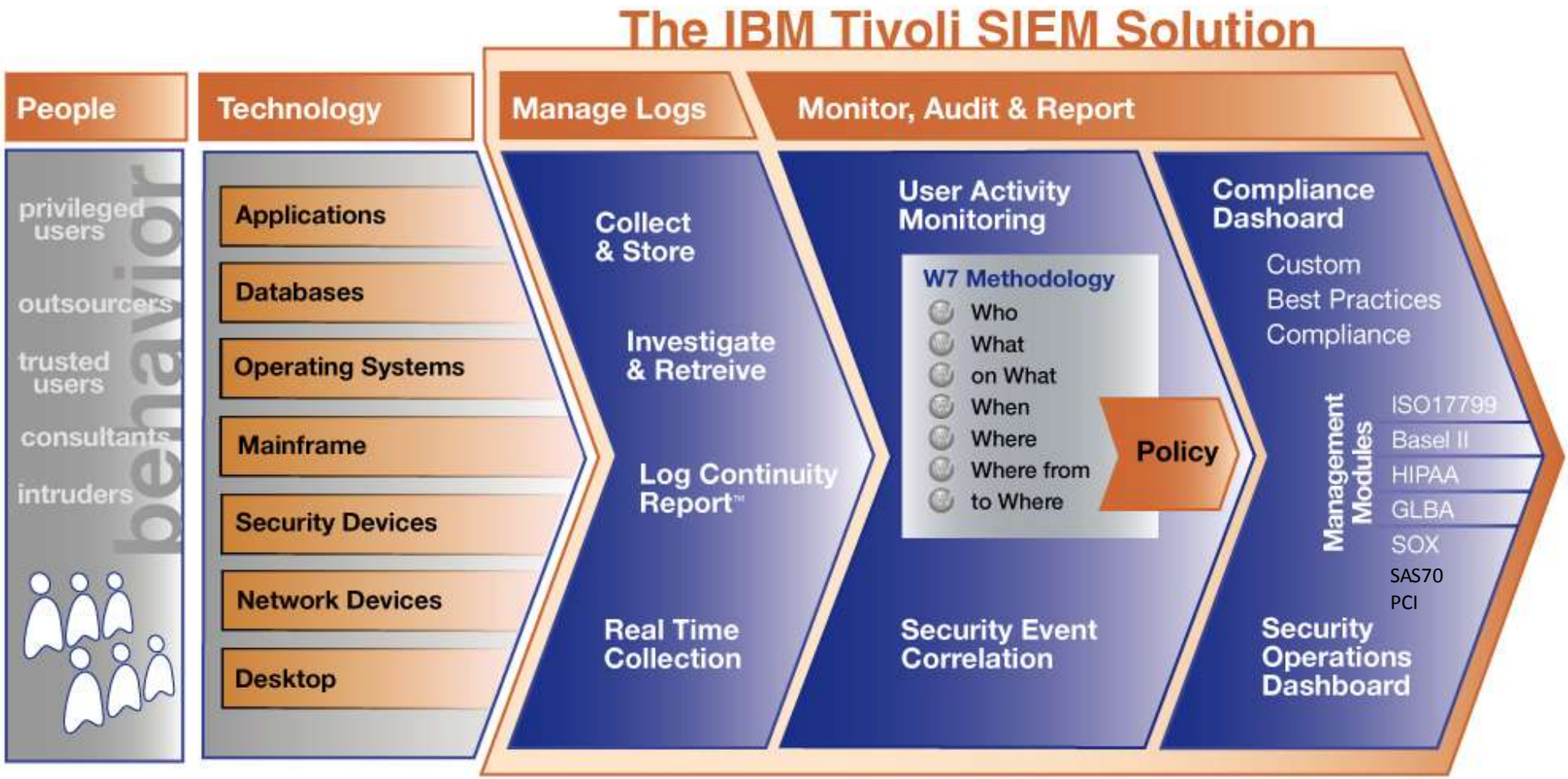
Service Provider
(e.g. Credit Check Service)

Mesures et Conformité sous SOA

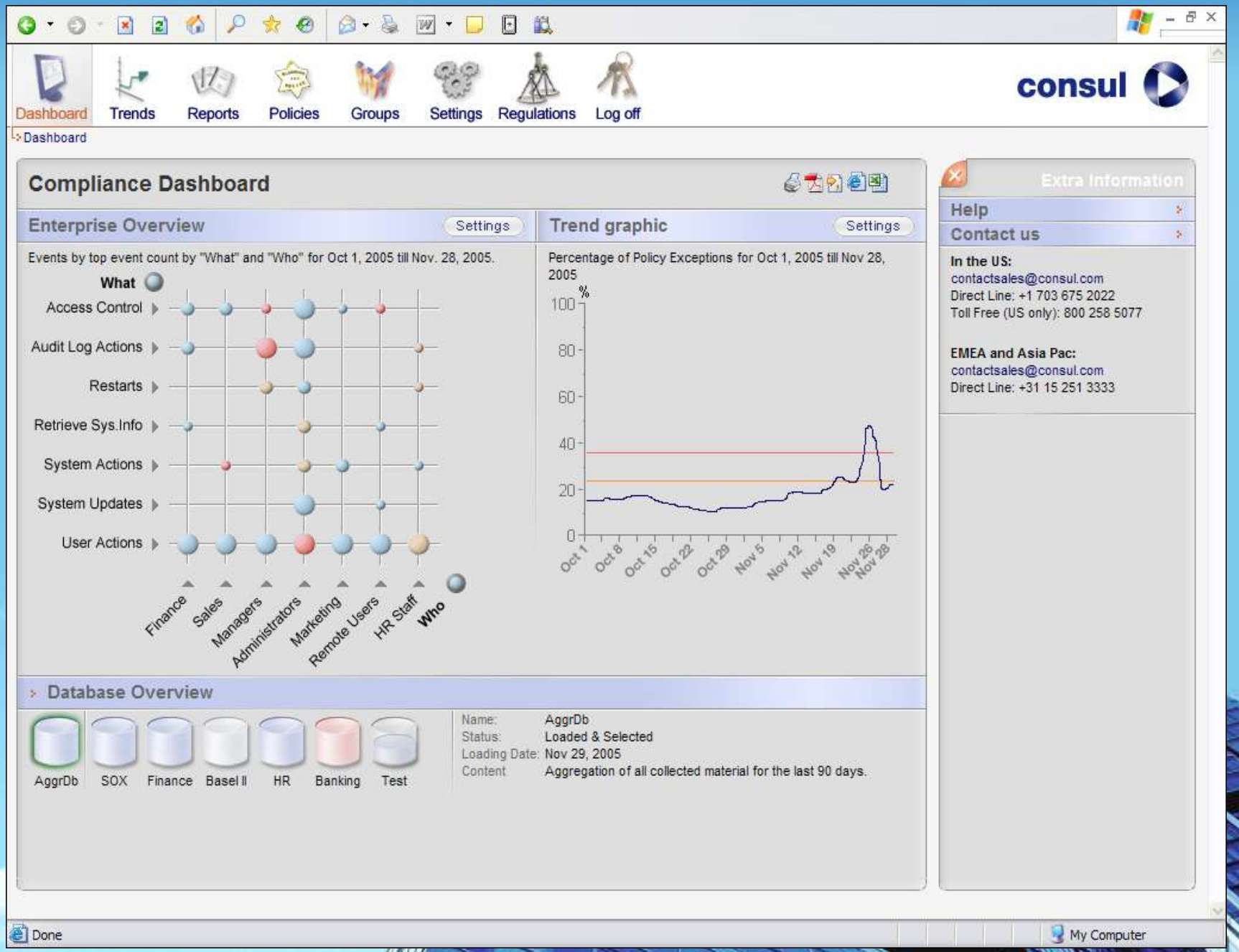
SOMMES-NOUS CONFORMES AUX RÈGLES?

IBM Tivoli Security Information and Event Management - TSIEM

Mesures et Conformité sous SOA



Mesurer et Valider la Conformité



IBM Tivoli Compliance Insight Manager Portal

IBM Tivoli Compliance Portal

iView	The reporting tool with drill down possibilities
Log Manager	The reporting tool for log management
Policy Generator	A wizard that helps you start using IBM Tivoli Compliance Insight Manager by creating a policy (= policy-rules and grouping) by using collected data from your own devices
Scoping	Tool to manage the viewable acces of different users of the system to different sets of data

IBM Tivoli Regulatory Compliance Reports

Basel II	The compliance entrance for Basel II
GLBA	The compliance entrance for GLBA
HIPAA	The compliance entrance for HIPAA
ISO17799	The compliance entrance for ISO17799
Sarbanes-Oxley	The compliance entrance for Sarbanes Oxley

IBM Tivoli Security Operations Portal

Realtime Portal	Open Security Operations Realtime Event Portal
Realtime Reporting Portal	Open Security Operations Realtime Reporting Portal

Tivoli Compliance Insight Manager

Conclusions

Le déploiement d'une architecture SOA sécurisée nécessite une attention particulière afin de maintenir un environnement fluide, efficace et gérable

- Externaliser les services de Sécurité (***Security as a Service***)
  - Gestion des Identités
  - Gestion des Accès
  - Intégrité / Confidentialité
  - Surveillance, Mesures et Conformité
- Utilisation des standards en vue de simplifier les intégrations

Nous avons les technologies et l'expérience, nous pouvons vous aider…

Questions?

Tendances Logicielles

L'architecture pour répondre aux besoins métier

Pierre Noël

Worldwide Executive, Information Security & Risk Management

SG24-7310-01