Tivoli software

IBM

IBM Tivoli Compliance Insight Manager 8.0 Introduction

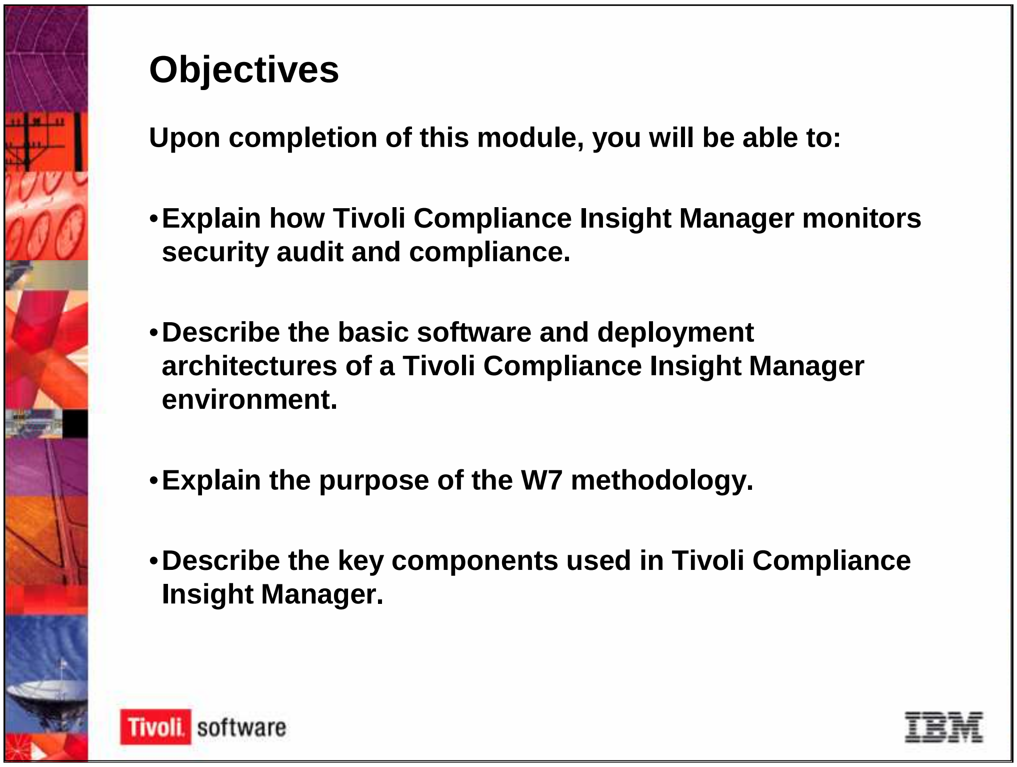
e business software

IBM Software Group

Welcome to the Tivoli Compliance Insight Manager v. 8.0 Overview Course.

This course provides a basic understanding of Tivoli Compliance Insight Manager and may be used as a stand-alone course or as a prerequisite to the Tivoli Compliance Insight Manager Administration and Tivoli Compliance Insight Manager Installation courses.

This course provides a high-level discussion of the Tivoli Compliance Insight Manager Suite. It reviews the architecture, network deployment, and main functionalities while also introducing the key concepts and terms used in Tivoli Compliance Insight Manager.



Objectives

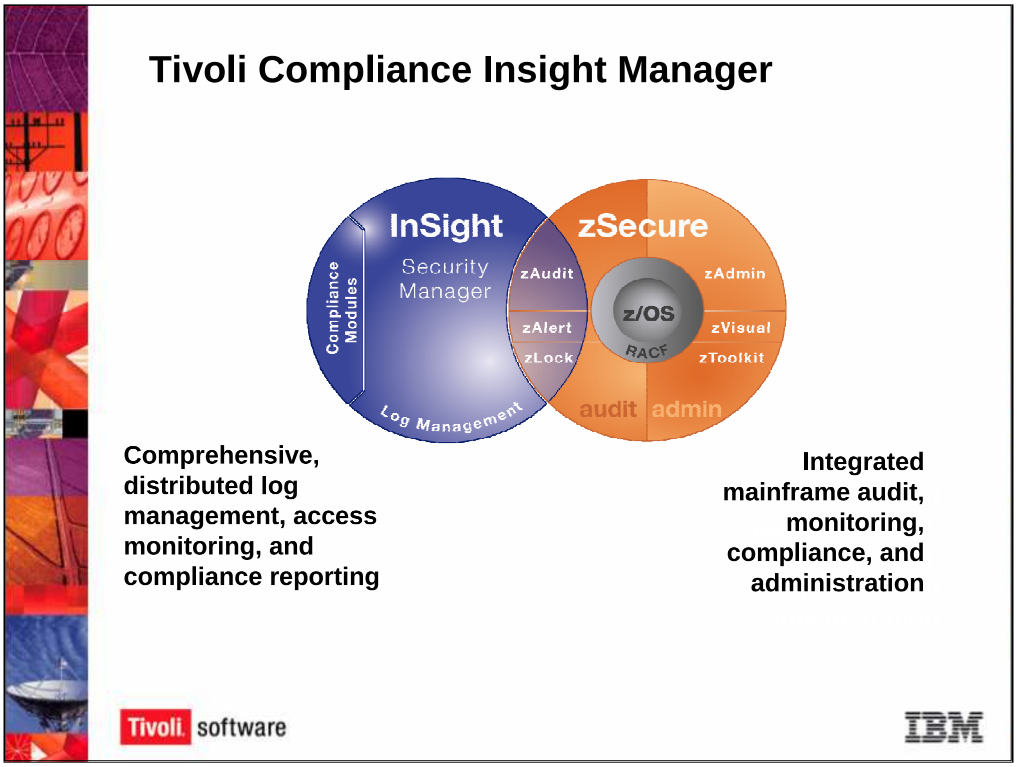
Upon completion of this module, you will be able to:

- **Explain how Tivoli Compliance Insight Manager monitors security audit and compliance.**
- **Describe the basic software and deployment architectures of a Tivoli Compliance Insight Manager environment.**
- **Explain the purpose of the W7 methodology.**
- **Describe the key components used in Tivoli Compliance Insight Manager.**

The purpose of the Overview course is to:

- Explain how the Tivoli Compliance Insight Manager Suite monitors security audit and compliance.
- Describe how Tivoli Compliance Insight Manager operates by discussing the software's collection processes and the network deployment architecture (Enterprise Server, Standard Server, clusters).
- Introduce the W7 methodology.
- Describe the key components used in Tivoli Compliance Insight Manager.

After taking the Tivoli Compliance Insight Manager Overview course, you should be able to identify the purpose of Tivoli Compliance Insight Manager, explain how it works at a high-level, and understand the product's concepts and vocabulary.



Tivoli Compliance Insight Manager

Comprehensive, distributed log management, access monitoring, and compliance reporting

Integrated mainframe audit, monitoring, compliance, and administration

The Consul product line includes the **Tivoli Compliance Insight Manager Suite**, represented by the blue circle on the left, and the **zSecure Suite**, represented by the orange circle on the right.

Consul was founded in 1986 as a mainframe security company specializing in z/OS and RACF. Consul branched out into the network security audit and compliance field with the Tivoli Compliance Insight Manager Suite, which provides comprehensive, distributed log management, access monitoring, and compliance reporting for enterprise networks. The **Tivoli Compliance Insight Manager Suite** includes the **Tivoli Compliance Insight Manager Security Manager**, **Log Manager**, and **Compliance Modules**.

Tivoli Compliance Insight Manager's purpose is to automate log collection and analysis, making it easier for you to manage your network security and respond to audits. The product's reports and compliance modules enable you to be audit-ready at all times.

Tivoli Compliance Insight Manager's Capabilities Include:

•Secure, reliable log capture from any platform

•Automatic collection of syslogs and audit trails

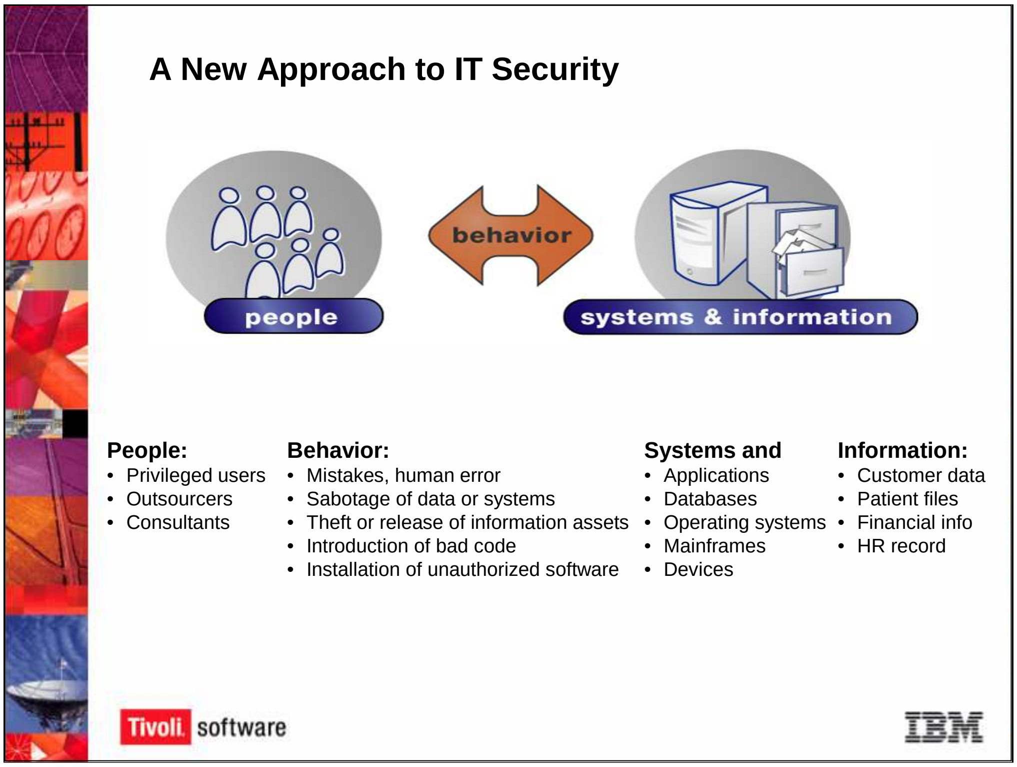
•Full support for native log collection

•Store in an efficient, compressed depot

•Easy access to data when needed

•Forensic search across all logs

•Reports to prove complete collection


behavior
people
systems & information

A New Approach to IT Security

People:
- Privileged users
- Outsourcers
- Consultants

Behavior:
- Mistakes, human error
- Sabotage of data or systems
- Theft or release of information assets
- Introduction of bad code
- Installation of unauthorized software

Systems and
- Applications
- Databases
- Operating systems
- Mainframes
- Devices

Information:
- Customer data
- Patient files
- Financial info
- HR record

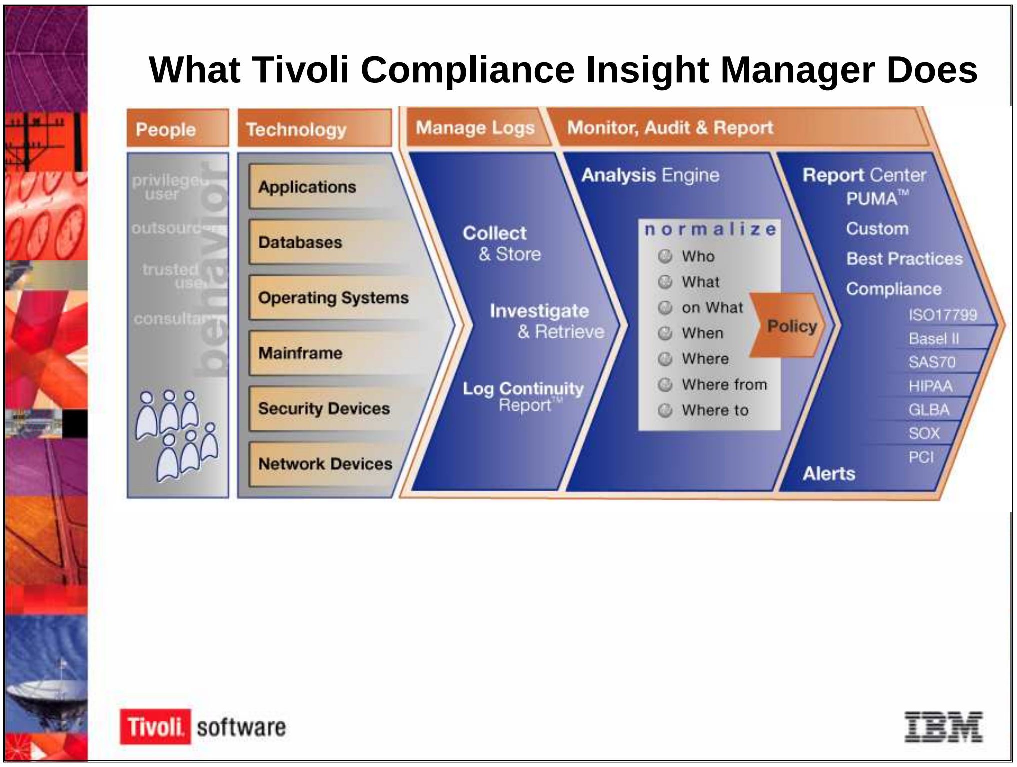
Tivoli Compliance Insight Manager takes a new approach to IT security: it puts log data and security events into a real-world context.

It views IT security as a function of **people** and their **interaction** with your **systems** and **information**.

Due to high-profile corporate data breaches and national and industry data security regulations, organizations must monitor how their employees and other insiders use their networks. Are users taking advantage of their access credentials to inappropriately access confidential information? For example, is a database administrator (DBA) taking advantage of having root access to change payroll data?

Your employees, outsourcers, and business partners have legitimate business reasons to access your network resources -- conducting business -- so controls and limits must not impede their daily work. But at the same time, you need to ensure that their network activities comply with company acceptable use and security policies and with national and industry regulations. In addition, you must be able to show auditors that your company is complying with the standards.

In order to adequately protect your network, you need to be able to see who is interacting with which systems and which data, and what they are doing.



What Tivoli Compliance Insight Manager Does

People | Technology | Manage Logs | Monitor, Audit & Report

privileged user
outsourcer
trusted user
consultant
behavior

Applications
Databases
Operating Systems
Mainframe
Security Devices
Network Devices

Collect & Store
Investigate & Retrieve
Log Continuity Report™

Analysis Engine
normalize
- Who
- What
- on What
- When
- Where
- Where from
- Where to

Policy

Report Center
PUMA™
Custom
Best Practices
Compliance
ISO17799
Basel II
SAS70
HIPAA
GLBA
SOX
PCI
Alerts

Tivoli. software

IBM

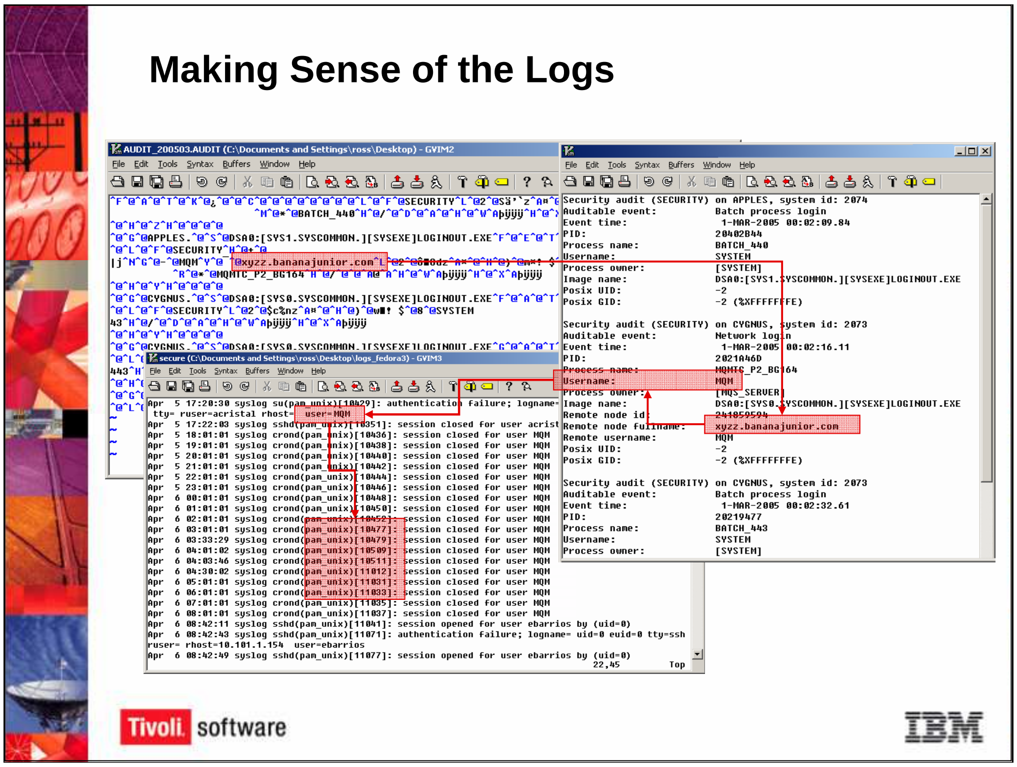
Consul's perspective starts with the people who use the network and their behavior.

When you monitor network security, you are monitoring what people – your privileged users, outsourcers, trusted users, and consultants – are doing with your technology – your applications, databases, operating systems, and devices.

All of your devices, or event sources, generate reams of log data documenting their activity. Tivoli Compliance Insight Manager automatically collects these logs, storing the original logs in a secure depot, and processes the logs using its analysis engine, where logs are normalized into an easy-to-understand W7 language so you can easily search for logs and events.

Once Tivoli Compliance Insight Manager has analyzed the logs, it generates numerous reports showing you the security and compliance gaps. Who is not complying with company acceptable use policy? Or with change management policy? Who is touching data that he or she should not have access to? Tivoli Compliance Insight Manager alerts on policy exceptions, where a policy has definitely been violated, and on special attentions, where something happened that requires extra attention.

The reports can be used to address compliance breaches and used to prove to auditors that the organization has implemented the appropriate compliance policies. Using the W7 language, which puts cryptic log terms into everyday, business terms such as who, what, and where, Tivoli Compliance Insight Manager generates reports on network activity that anyone in your organization can understand. You do not have to be network security expert to understand what policy violation occurred and who did it. Tivoli Compliance Insight Manager's Compliance Modules generate regulation-specific reports so that you can easily answer auditors' questions about your company's compliance efforts with national and industry regulations such as Basel II and the Sarbanes Oxley Act (SOX).



Making Sense of the Logs

AUDIT_200503.AUDIT (C:\Documents and Settings\ross\Desktop) - GVIM2
File Edit Tools Syntax Buffers Window Help

```
^F^@^A^@^T^@^K^@¿^@^@^C^@^@^@^@^@^@^@^@^L^@^F^@SECURITY^L^@2^@Sä'`z^A¤^@
                       ^M^@*^@BATCH_440^H^@/^@^D^@^A^@^H^@^W^Aþÿÿÿ^H^@^X
^@^H^@^Z^H^@^@^@^@
^@^G^@APPLES.^@^S^@DSA0:[SYS1.SYSCOMMON.][SYSEXE]LOGINOUT.EXE^F^@^E^@^T
^@^L^@^F^@SECURITY^H^@+^@
|j^N^G^@-^@MQM^Y^@ ^@xyzz.bananajunior.com^L^@2^@ô■0dz^A*^@^H^@)^@m*! $
          ^R^@*^@MQMTC_P2_BG164^H^@/^@^@^A@^A^H^@^W^Aþÿÿÿ^H^@^X^Aþÿÿÿ
^@^H^@^Y^H^@^@^@^@
^@^G^@CYGNUS.^@^S^@DSA0:[SYS0.SYSCOMMON.][SYSEXE]LOGINOUT.EXE^F^@^A^@^T
^@^L^@^F^@SECURITY^L^@2^@$c%nz^A¤^@^H^@)^@w■! $^@8^@SYSTEM
43^H^@/^@^D^@^A^@^H^@^W^Aþÿÿÿ^H^@^X^Aþÿÿÿ
^@^H^@^Y^H^@^@^@^@
^@^G^@CYGNUS.^@^S^@DSA0:[SYS0.SYSCOMMON.][SYSEXE]LOGINOUT.EXE^G^@^A^@^T
^@^L^
443^H
^@^H^
^@^G^
^@^L^
~
~
~
~
```

secure (C:\Documents and Settings\ross\Desktop\logs_fedora3) - GVIM3
File Edit Tools Syntax Buffers Window Help

```
Apr  5 17:20:30 syslog su(pam_unix)[10429]: authentication failure; logname=
 tty= ruser=acristal rhost=  user=MQM
Apr  5 17:22:03 syslog sshd(pam_unix)[10351]: session closed for user acrist
Apr  5 18:01:01 syslog crond(pam_unix)[10436]: session closed for user MQM
Apr  5 19:01:01 syslog crond(pam_unix)[10438]: session closed for user MQM
Apr  5 20:01:01 syslog crond(pam_unix)[10440]: session closed for user MQM
Apr  5 21:01:01 syslog crond(pam_unix)[10442]: session closed for user MQM
Apr  5 22:01:01 syslog crond(pam_unix)[10444]: session closed for user MQM
Apr  5 23:01:01 syslog crond(pam_unix)[10446]: session closed for user MQM
Apr  6 00:01:01 syslog crond(pam_unix)[10448]: session closed for user MQM
Apr  6 01:01:01 syslog crond(pam_unix)[10450]: session closed for user MQM
Apr  6 02:01:01 syslog crond(pam_unix)[10452]: session closed for user MQM
Apr  6 03:01:01 syslog crond(pam_unix)[10477]: session closed for user MQM
Apr  6 03:33:29 syslog crond(pam_unix)[10479]: session closed for user MQM
Apr  6 04:01:02 syslog crond(pam_unix)[10509]: session closed for user MQM
Apr  6 04:03:46 syslog crond(pam_unix)[10511]: session closed for user MQM
Apr  6 04:30:02 syslog crond(pam_unix)[11012]: session closed for user MQM
Apr  6 05:01:01 syslog crond(pam_unix)[11031]: session closed for user MQM
Apr  6 06:01:01 syslog crond(pam_unix)[11033]: session closed for user MQM
Apr  6 07:01:01 syslog crond(pam_unix)[11035]: session closed for user MQM
Apr  6 08:01:01 syslog crond(pam_unix)[11037]: session closed for user MQM
Apr  6 08:42:11 syslog sshd(pam_unix)[11041]: session opened for user ebarrios by (uid=0)
Apr  6 08:42:43 syslog sshd(pam_unix)[11071]: authentication failure; logname= uid=0 euid=0 tty=ssh
ruser= rhost=10.101.1.154  user=ebarrios
Apr  6 08:42:49 syslog sshd(pam_unix)[11077]: session opened for user ebarrios by (uid=0)
                                                                      22,45         Top
```

```
Security audit (SECURITY) on APPLES, system id: 2074
Auditable event:          Batch process login
Event time:                1-MAR-2005 00:02:09.84
PID:                      20402B44
Process name:             BATCH_440
Username:                 SYSTEM
Process owner:            [SYSTEM]
Image name:               DSA0:[SYS1.SYSCOMMON.][SYSEXE]LOGINOUT.EXE
Posix UID:                -2
Posix GID:                -2 (%XFFFFFFFE)

Security audit (SECURITY) on CYGNUS, system id: 2073
Auditable event:          Network login
Event time:                1-MAR-2005 00:02:16.11
PID:                      2021A46D
Process name:             MQMTC_P2_BG164
Username:                 MQM
Process owner:            [MQS_SERVER]
Image name:               DSA0:[SYS0.SYSCOMMON.][SYSEXE]LOGINOUT.EXE
Remote node id:           241859594
Remote node fullname:     xyzz.bananajunior.com
Remote username:          MQM
Posix UID:                -2
Posix GID:                -2 (%XFFFFFFFE)

Security audit (SECURITY) on CYGNUS, system id: 2073
Auditable event:          Batch process login
Event time:                1-MAR-2005 00:02:32.61
PID:                      20219477
Process name:             BATCH_443
Username:                 SYSTEM
Process owner:            [SYSTEM]
```

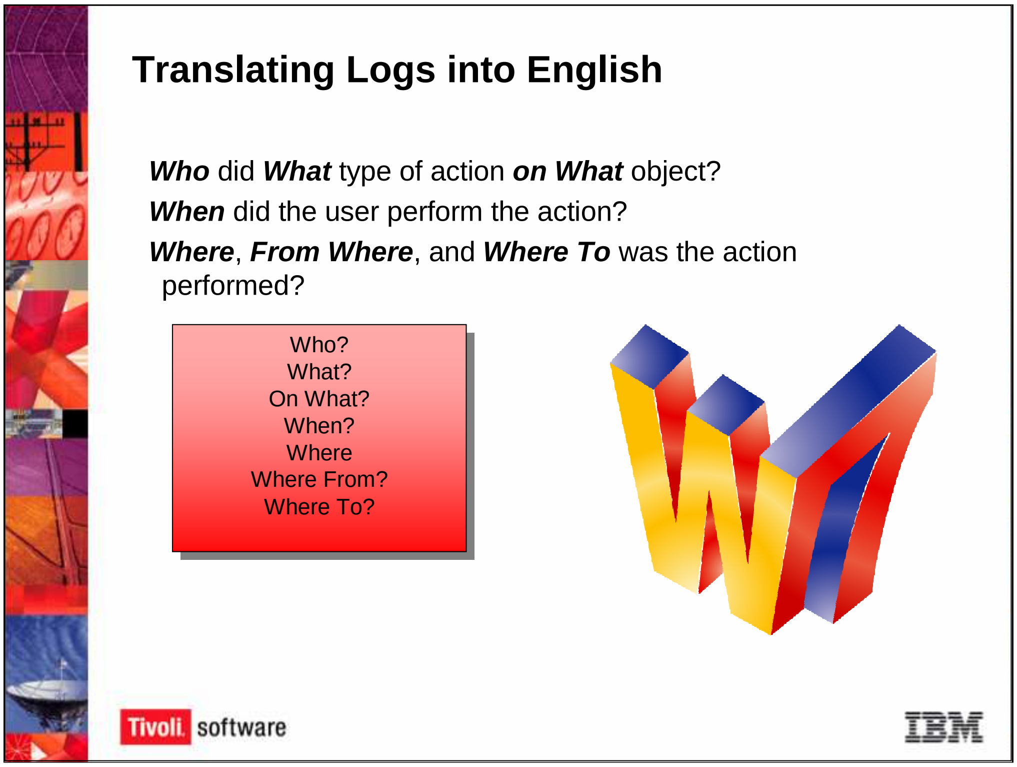
Tivoli software

IBM

Making Sense of the Logs

When Tivoli Compliance Insight Manager’s analysis engine analyzes the log data, it normalizes the log data that it collects into an English-based language called W7.

Different platforms and systems call the same action by different names. One operating system calls it “logging on,” while another OS calls it “login.” One system asks for a “userid;” another system asks for a “username.” Unless you’re an expert in all of the different systems that your company uses, it is very difficult to search across the enterprise’s log files manually and find all instances of a given action or user.



Translating Logs into English

Who did ***What*** type of action ***on What*** object?

When did the user perform the action?

Where, ***From Where***, and ***Where To*** was the action performed?

Who?
What?
On What?
When?
Where
Where From?
Where To?

Tivoli software

IBM

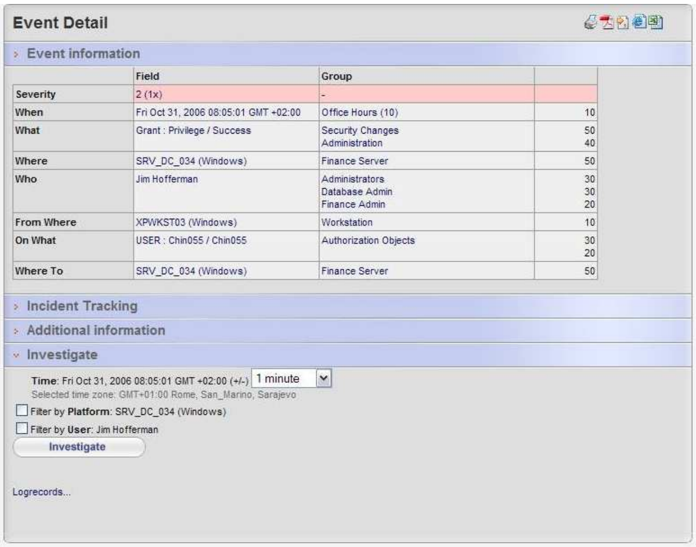
Consul recognized this problem at our customer sites and designed the W7 language to solve it. W7 normalizes cryptic log data into an easy-to-understand, English language of Who, What, When, Where, On What, Where To, and Where From.

In other words, Who does What, and Where? Which user does which action to which system? When does this event happen? From Where – from which IP address? To Where – to which IP address? W7 takes the mystery out of the logs.

W7 Answers These Questions:

- Who: Who is the user?
- What: What action occurred?
- On What: On which machine did the action occur?
- When: When did the action occur?
- Where: Where is the action occur physically?
- Where From: What was the source IP address?
- Where To: What was the destination IP address?

Putting Events into Context with W7



Event Detail

Event information

	Field	Group	
Severity	2 (1x)	-	
When	Fri Oct 31, 2006 08:05:01 GMT +02:00	Office Hours (10)	10
What	Grant : Privilege / Success	Security Changes Administration	50 40
Where	SRV_DC_034 (Windows)	Finance Server	50
Who	Jim Hofferman	Administrators Database Admin Finance Admin	30 30 20
From Where	XPWKST03 (Windows)	Workstation	10
On What	USER : Chin055 / Chin055	Authorization Objects	30 20
Where To	SRV_DC_034 (Windows)	Finance Server	50

Incident Tracking

Additional information

Investigate

Time: Fri Oct 31, 2006 08:05:01 GMT +02:00 (+/-) 1 minute

Selected time zone: GMT+01:00 Rome, San_Marino, Sarajevo

□ Filter by **Platform**: SRV_DC_034 (Windows)

□ Filter by **User**: Jim Hofferman

Tivoli software

IBM

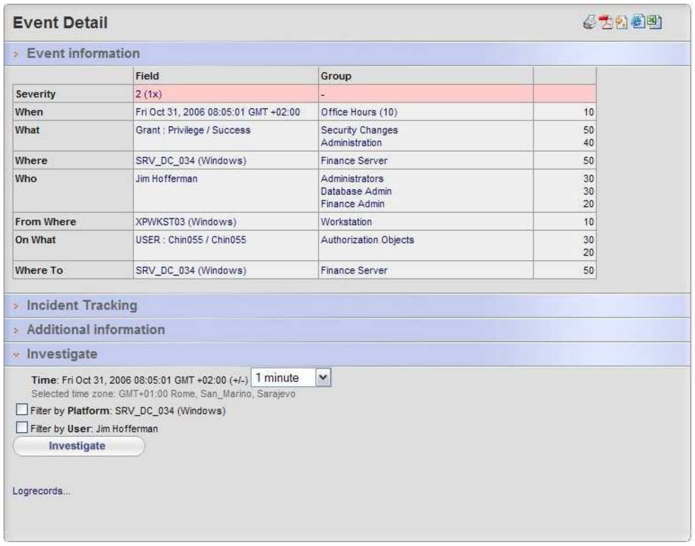
Let’s look an example of W7 in the context of an event. Tivoli Compliance Insight Manager lets you drill down from a high-level summary of IT activity to the individual events and logs themselves. This slide shows the Event Detail for a particular event.

The W7 attributes are shown in the leftmost column, and the other columns provide information on the field and the groups affected by the event. The field column shows event attributes from the log data. The group column shows which group the attribute is associated with.

W7 groups allow you to categorize your network devices, users, and compliance policies. For example, you may want to assign the hours from 9 a.m. to 5 p.m. (0900-1700 hours) as office hours and from 5 p.m. to 9 a.m. as after hours (1700-0900 hours). Network activity that occurs during office hours is acceptable, but activity that occurs during after hours is unacceptable. So you could set up these groups and configure Tivoli Compliance Insight Manager to issue a policy exception and an alert when something happens during after hours. You can setup groups for different categories of users, such as your database administrators and your finance staff, or for different categories of machines, such as workstations or application servers, and so on.

We’ll go to the next slide to discuss the W7 example in detail.

W7 Example



Event Detail

› Event information

	Field	Group	
Severity	2 (1x)	-	
When	Fri Oct 31, 2006 08:05:01 GMT +02:00	Office Hours (10)	10
What	Grant : Privilege / Success	Security Changes Administration	50 40
Where	SRV_DC_034 (Windows)	Finance Server	50
Who	Jim Hofferman	Administrators Database Admin Finance Admin	30 30 20
From Where	XPWKST03 (Windows)	Workstation	10
On What	USER : Chin055 / Chin055	Authorization Objects	30 20
Where To	SRV_DC_034 (Windows)	Finance Server	50

› Incident Tracking

› Additional information

› Investigate

Time: Fri Oct 31, 2006 08:05:01 GMT +02:00 (+/-) 1 minute

Selected time zone: GMT+01:00 Rome, San_Marino, Sarajevo

□ Filter by **Platform**: SRV_DC_034 (Windows)

□ Filter by **User**: Jim Hofferman

Investigate

Logrecords...

Tivoli software IBM

Let’s look at this event and find out what happened on the evening of Friday, October 31, 2006.

The **When row** tells us the date and time when the event occurred. This event took place during office hours.

The **What** row identifies that someone successfully granted privileges.

The **Where** row shows that the privileges were granted on a Windows machine, SRV_DC_034, that is part of the finance servers.

The **Who** row tells us that Jim Hofferman, who belongs to the Administrators, Database Admin, and Finance Admin groups, made the change.

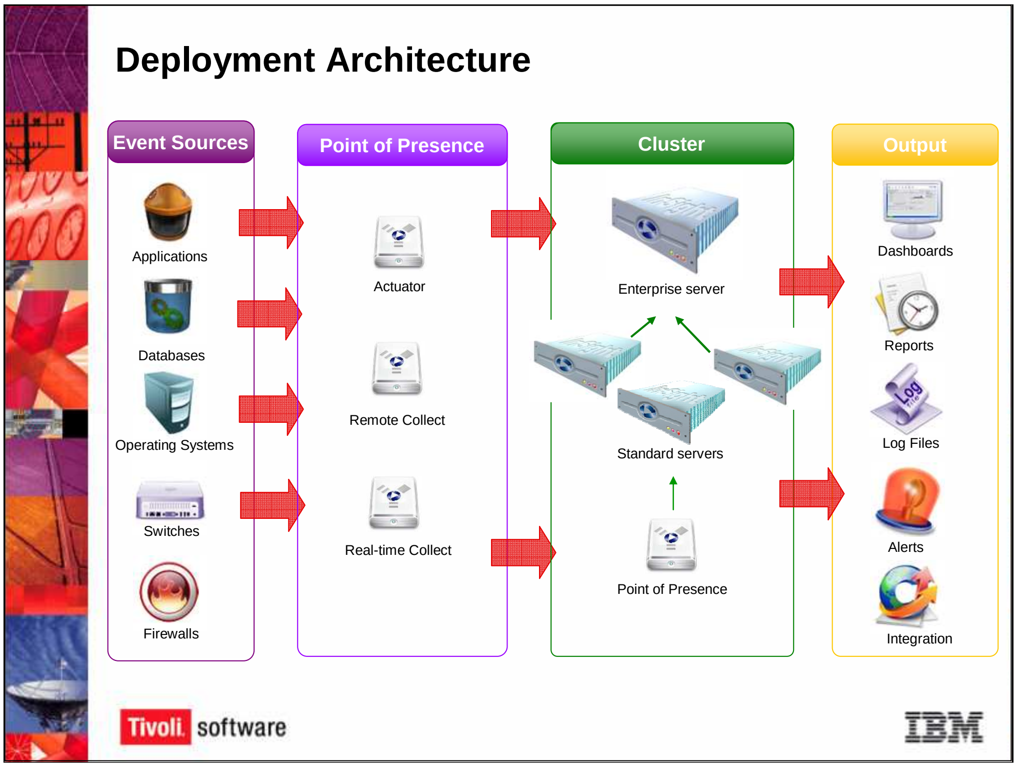
The **From Where** row tells us the source machine that was used to make the change. The source machine was a Windows machine in the Workstation group.

The **Where To** row tells us the destination machine, which was the target of the change. The destination machine was a Windows machine, SRV_DC_034, that is part of the finance servers.

The **On What** row identities the object of the event. In this case, the object is a user “Chin055.”

So, what happened? This event shows that a DBA, Jim Hofferman, granted privileges to a user account, Chin055, thus allowing Chin055 to access a finance server.

The W7 methodology puts events in context. For example, if Chin055 is a new accountant who legitimately needs to access the finance servers, then this event is an acceptable action. If Jim the DBA is a disgruntled employee who is using the alias Chin055 to change financial data, then this event is very serious. In this case, the severity metrics tells us that this event was a 2, which means that it is a low severity event.



Deployment Architecture

Event Sources
Applications
Databases
Operating Systems
Switches
Firewalls

Point of Presence
Actuator
Remote Collect
Real-time Collect

Cluster
Enterprise server
Standard servers
Point of Presence

Output
Dashboards
Reports
Log Files
Alerts
Integration

Tivoli. software

IBM

How Tivoli Compliance Insight Manager is Deployed in the Network

Tivoli Compliance Insight Manager is a software application that runs in the network to collect, analyze, and report on log data. It is loaded on a dedicated machine, the **Tivoli Compliance Insight Manager server**, which aggregates and analyzes the log data that is collected from the audited machines in the network.

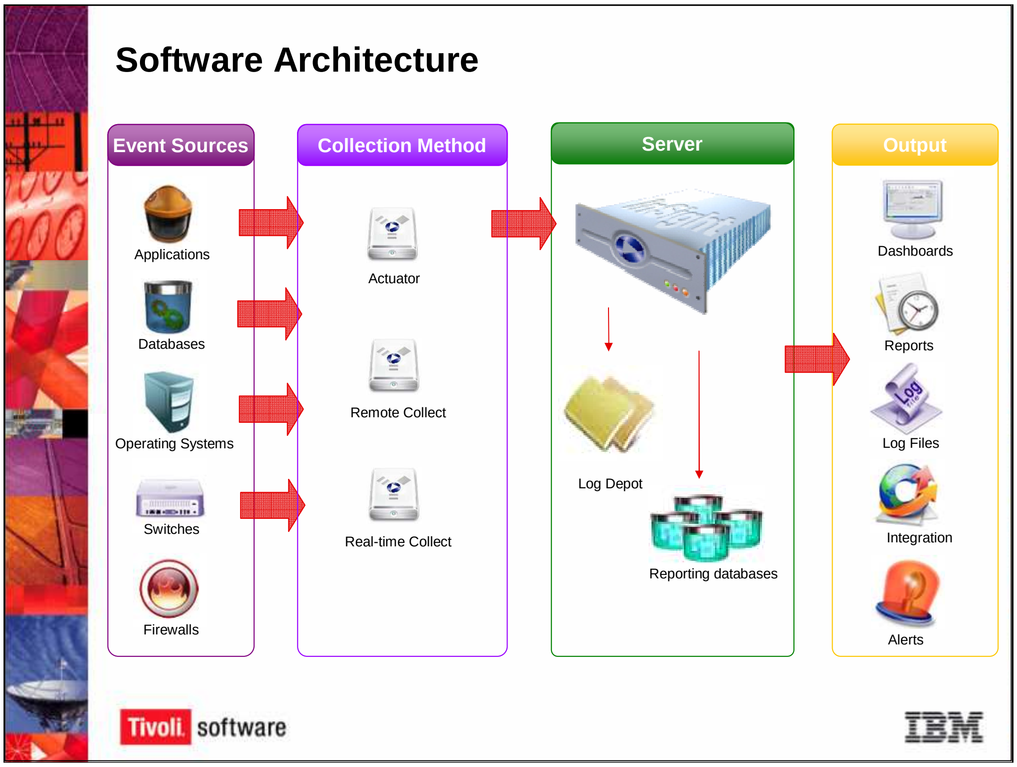
The audited machines are also known as **event sources**. An event source is any machine, device, or application that is a source of log data.

Tivoli Compliance Insight Manager can collect logs from a wide variety of operating systems, applications, and devices, and it can collect logs in several ways. One way Tivoli Compliance Insight Manager collects logs is through a **Point-of-Presence (PoP)**. The PoP is a piece of software, called an **actuator**, that is installed on the device and collects the logs from the event source and transmits the logs to the Tivoli Compliance Insight Manager server. Tivoli Compliance Insight Manager can also run an **agent-less collect**, or **remote collect,** using ssh or NetBios for Windows. Agent-less collect is only available on certain platforms. In addition, Tivoli Compliance Insight Manager can collect logs from a **syslog collector** or from **SNMP traps**.

The Tivoli Compliance Insight Manager server is used to collect, store, and analyze the log data. There are different classes of Tivoli Compliance Insight Manager servers, depending on your needs and the size of the network: the **Standard Server** and the **Enterprise Server**. The **Tivoli Compliance Insight Manager Standard Server** is used to gather log data. The **Tivoli Compliance Insight Manager Enterprise Server** can be used in conjunction with one or more Standard Servers to provide enterprise-wide coverage. A combination of up to three standard servers and one enterprise server is called an **Tivoli Compliance Insight Manager cluster**.

After collecting and analyzing the data, Tivoli Compliance Insight Manager presents its analyses through its online dashboards and reports, generates alerts, and enables you to search and retrieve log data and to integrate its analysis into other third-party systems.

We'll discuss the deployment of an Tivoli Compliance Insight Manager cluster and the capabilities of the standard server and enterprise server shortly.



Software Architecture

Event Sources

Applications

Databases

Operating Systems

Switches

Firewalls

Collection Method

Actuator

Remote Collect

Real-time Collect

Server

Log Depot

Reporting databases

Output

Dashboards

Reports

Log Files

Integration

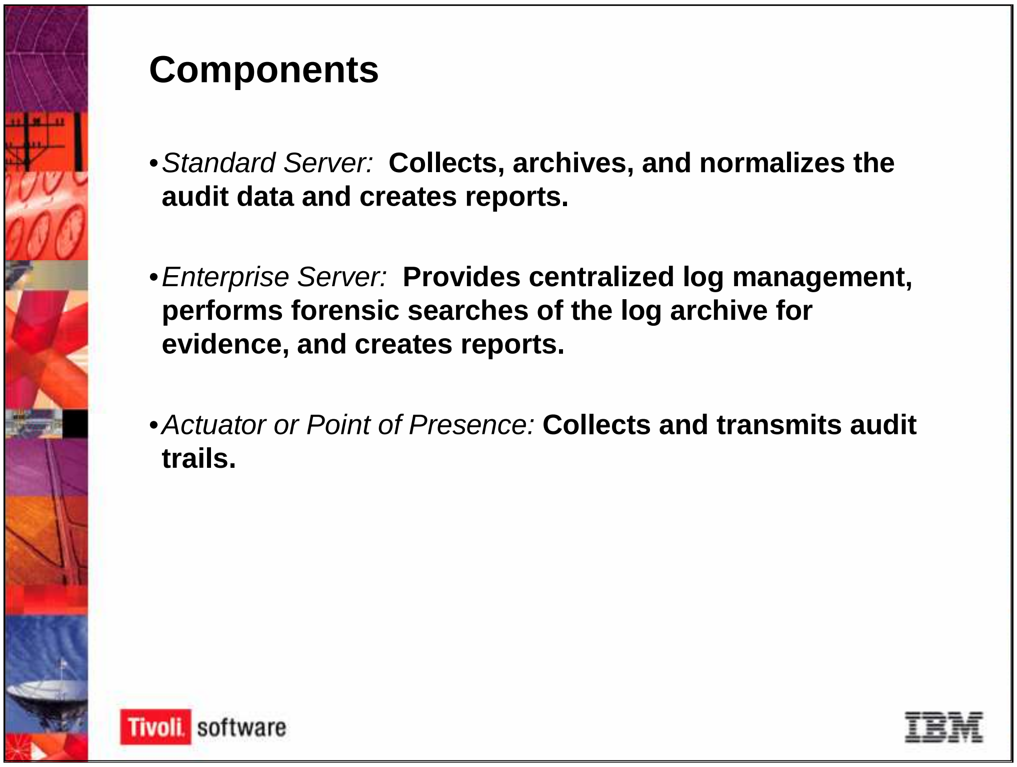
Alerts

As Tivoli Compliance Insight Manager collects logs from the event sources, it stores the original logs in its secure **depot** and normalizes the log data using the **W7 methodology**. Tivoli Compliance Insight Manager analyzes the logs by comparing the logs against the **policies** you have created, determining whether the user behavior reflected in the logs complies with your company's acceptable use policies.

If the user behavior does not comply, then Tivoli Compliance Insight Manager generates a **policy exception event,** and optionally generates an **alert**, notifying you that a policy violation occurred. Of course, sometimes users do things that are not exactly policy violations, but are things that you want to pay attention to. In this case, Tivoli Compliance Insight Manager can generate a **special attention**, which notifies you that something happened that requires your attention.

Tivoli Compliance Insight Manager also enables the user to filter the audit trails to search for specific types of events. Once these events are found, you can drill down deeper into the event details, even to the level of the original platform record that caused the event. The reports are displayed in our web-based user interface and can be printed, saved, and emailed as a PDF, HTML, Microsoft Excel, or CSV file.

We'll discuss Tivoli Compliance Insight Manager's reports more in a moment.



Components

- *Standard Server:* **Collects, archives, and normalizes the audit data and creates reports.**
- *Enterprise Server:* **Provides centralized log management, performs forensic searches of the log archive for evidence, and creates reports.**
- *Actuator or Point of Presence:* **Collects and transmits audit trails.**

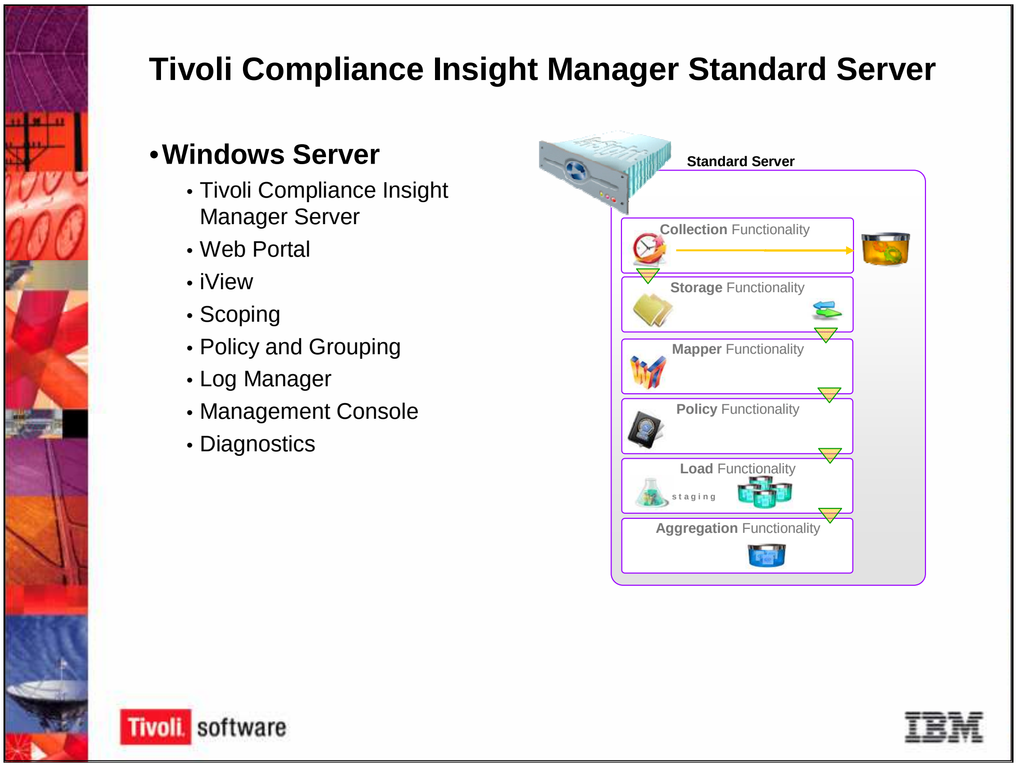
Tivoli. software
IBM

There are two key components of Tivoli Compliance Insight Manager's deployment in the network: the **Tivoli Compliance Insight Manager server** and the **actuator** (also called the **point-of-presence)**.

The **Tivoli Compliance Insight Manager server** houses the Tivoli Compliance Insight Manager applications and collects, archives, and normalizes the log data, and creates reports.

The **actuator** is the mechanism for gathering the log data from the audited machines, or event sources. As we discussed earlier, the actuator can work using the point-of-presence actuator software, or it can work remotely, using ssh or by other means.

There are two types of Tivoli Compliance Insight Manager servers, the **Standard Server** and the **Enterprise Server**. A standard server is that part of a Tivoli Compliance Insight Manager cluster collects and archives the audit trails. The enterprise server in an Tivoli Compliance Insight Manager cluster adds centralized log management.

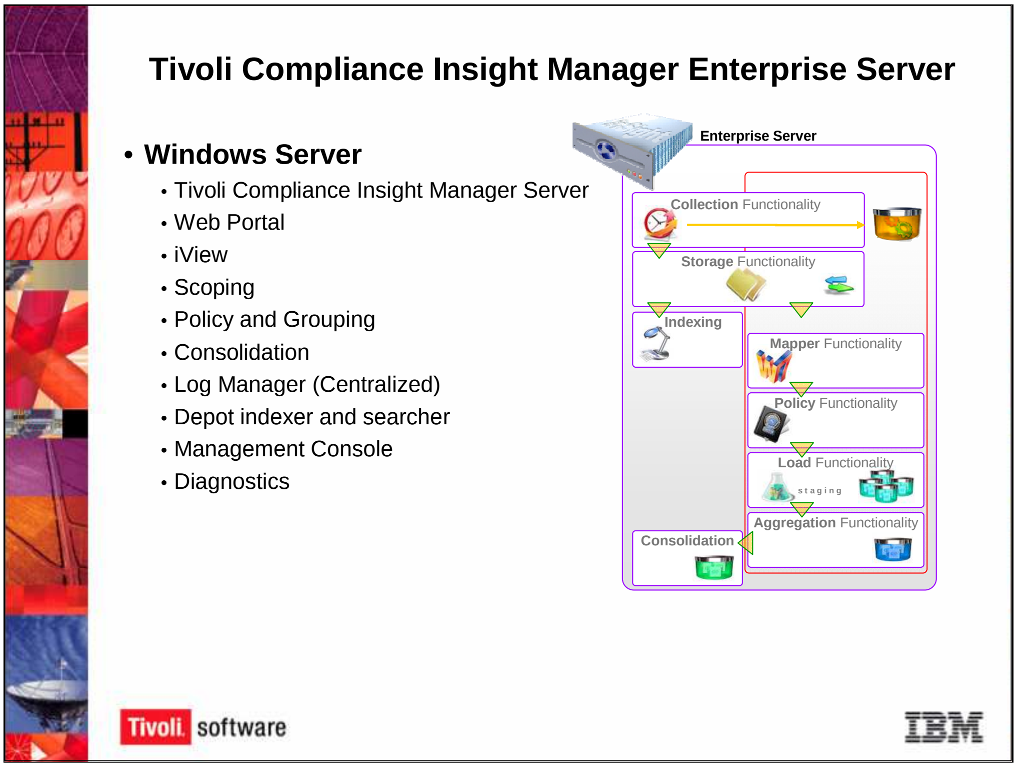


Tivoli Compliance Insight Manager Standard Server

- **Windows Server**
  - Tivoli Compliance Insight Manager Server
  - Web Portal
  - iView
  - Scoping
  - Policy and Grouping
  - Log Manager
  - Management Console
  - Diagnostics

The **Tivoli Compliance Insight Manager Standard Server** provides the Tivoli Compliance Insight Manager Engine, Server, Single Sign-On Portal, iView, Policy and Grouping functionalities, Scoping, Management Console, and Diagnostics. We’ll discuss these functionalities in more detail as we go through the presentation.

The standard server can be deployed by itself or in combination with other standard servers and an enterprise server to form an Tivoli Compliance Insight Manager Cluster.



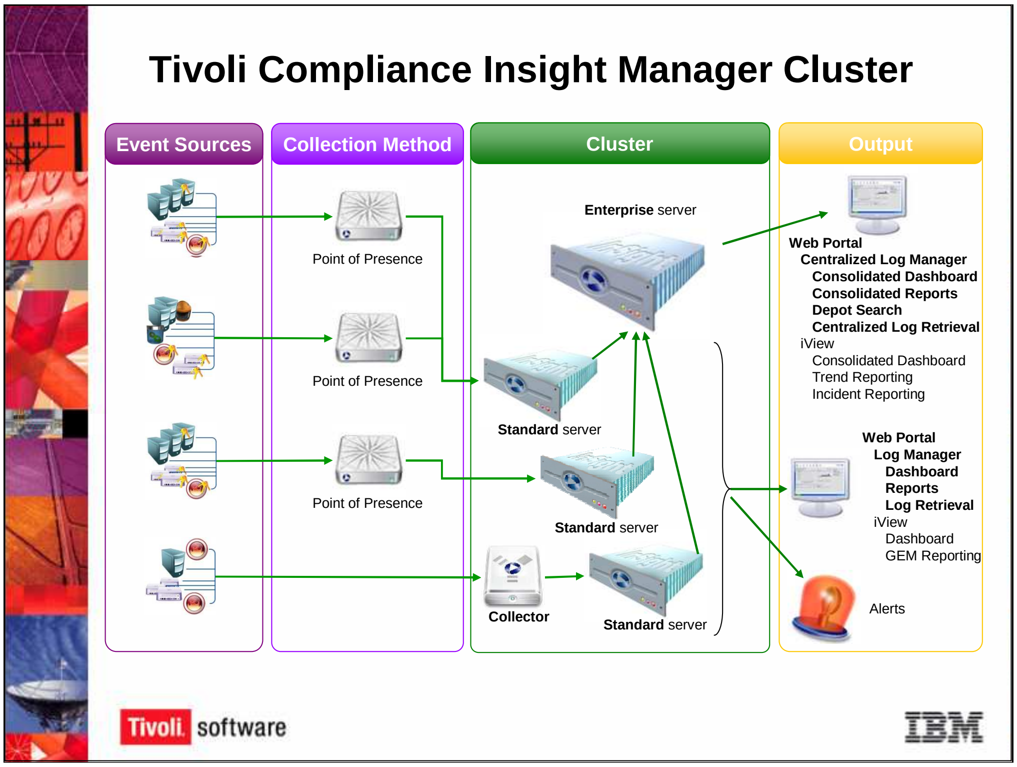
Tivoli Compliance Insight Manager Enterprise Server

- **Windows Server**
  - Tivoli Compliance Insight Manager Server
  - Web Portal
  - iView
  - Scoping
  - Policy and Grouping
  - Consolidation
  - Log Manager (Centralized)
  - Depot indexer and searcher
  - Management Console
  - Diagnostics

Tivoli software

IBM

The **InSight Enterprise Server** offers all of the functionality of the Standard Server in addition to the centralized log management functionality, depot indexer, and log forensics tools. The Enterprise Server is often used in combination with a maximum of three Standard Servers to create an Tivoli Compliance Insight Manager Cluster.



Tivoli Compliance Insight Manager Cluster

Event Sources

Collection Method

Cluster

Output

Point of Presence

Point of Presence

Point of Presence

Enterprise server

Standard server

Standard server

Collector

Standard server

Web Portal
- **Centralized Log Manager**
  - **Consolidated Dashboard**
  - **Consolidated Reports**
  - **Depot Search**
  - **Centralized Log Retrieval**
- iView
  - Consolidated Dashboard
  - Trend Reporting
  - Incident Reporting

Web Portal
- **Log Manager**
  - **Dashboard**
  - **Reports**
  - **Log Retrieval**
- iView
  - Dashboard
  - GEM Reporting

Alerts

Tivoli. software

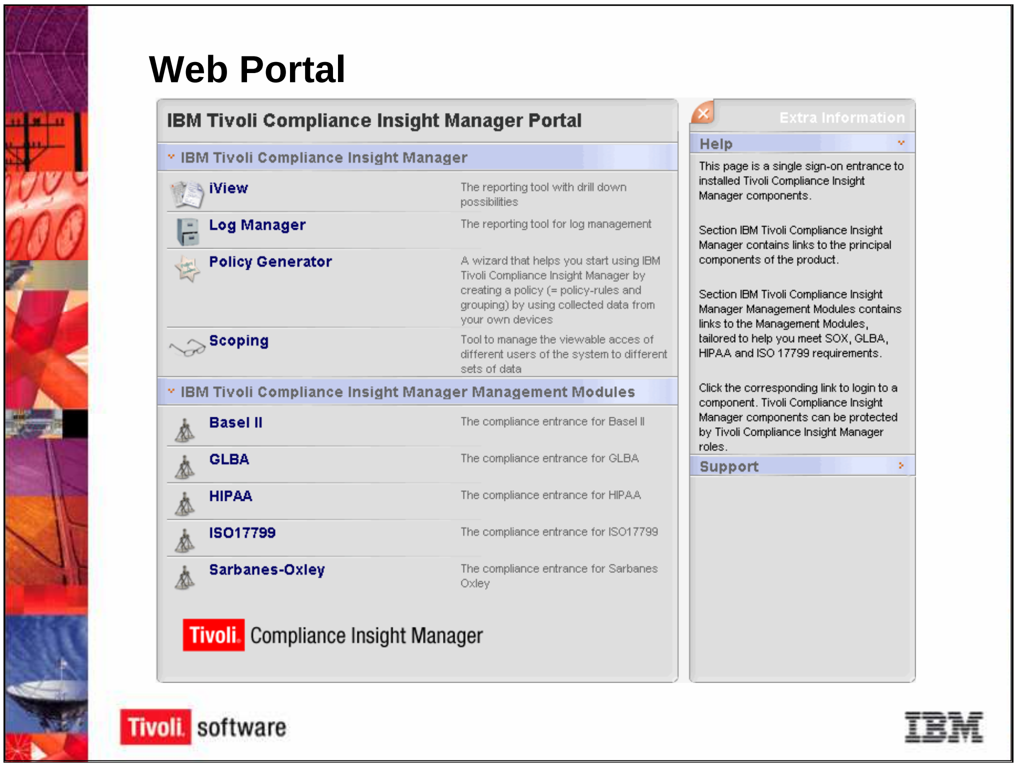
IBM

An **Tivoli Compliance Insight Manager cluster** is the name for the network of up to three standard servers and one enterprise server. An Tivoli Compliance Insight Manager cluster is used for scaling to larger or distributed network environments.

In an Tivoli Compliance Insight Manager cluster, the standard servers send the data to the enterprise server, which analyzes the log management data and compliance statistics and provides an enterprise-level view of the level of IT-security through the Tivoli Compliance Insight Manager Portal. In this configuration, the enterprise server typically does not collect any audit trails other than the ones used for self-auditing, but does provide centralized log management for the audit trails collected by the standard servers.

The **Tivoli Compliance Insight Manager Portal** is a single sign-on web interface that shows you all of the dashboards and reports for monitoring your network. We'll talk more about the Tivoli Compliance Insight Manager Portal in a moment.

In addition, each of the standard servers analyzes the data it contains and provides information on its environment through the Tivoli Compliance Insight Manager Portal. As a result, you can see what's happening throughout the enterprise using the enterprise server's aggregated view, or you can see into part of the network using the respective standard server.



Web Portal

IBM Tivoli Compliance Insight Manager Portal

IBM Tivoli Compliance Insight Manager

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 Compliance Insight Manager Management Modules

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

Tivoli. Compliance Insight Manager

Extra Information

Help

This page is a single sign-on entrance to installed Tivoli Compliance Insight Manager components.

Section IBM Tivoli Compliance Insight Manager contains links to the principal components of the product.

Section IBM Tivoli Compliance Insight Manager Management Modules contains links to the Management Modules, tailored to help you meet SOX, GLBA, HIPAA and ISO 17799 requirements.

Click the corresponding link to login to a component. Tivoli Compliance Insight Manager components can be protected by Tivoli Compliance Insight Manager roles.

Support

Tivoli. software

IBM

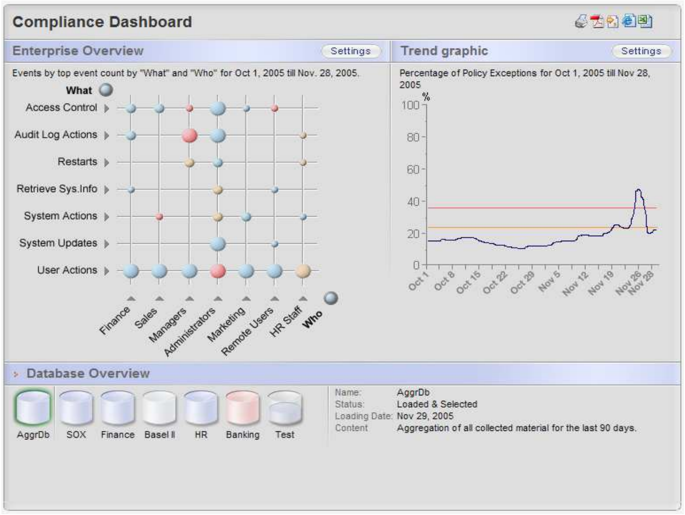
The **Tivoli Compliance Insight Manager Portal** is a single sign-on web-based user interface. If you login to a standard server, then the Tivoli Compliance Insight Manager Portal only displays the information for that server. If you login to an enterprise server, then the Tivoli Compliance Insight Manager Portal displays the information from the attached standard servers.

From the Portal, you can access:

- **iView**, Tivoli Compliance Insight Manager's compliance and reporting interface.
- **Log Manager**, Tivoli Compliance Insight Manager's log management and reporting interface.
- **Policy Generator**, Tivoli Compliance Insight Manager's policy configuration and management interface.
- **Scoping**, Tivoli Compliance Insight Manager's viewer manager, which lets you limit the visibility individual users and groups of users have into the system.
- **Compliance Modules**, which enable you to run reports showing your company's compliance with a given regulation or standard, such as Sarbanes Oxley or ISO17799.

We'll go through each of these interfaces in detail in the upcoming slides.

iView and the Compliance Dashboard



Compliance Dashboard

Enterprise Overview

Events by top event count by "What" and "Who" for Oct 1, 2005 till Nov. 28, 2005.

Trend graphic

Percentage of Policy Exceptions for Oct 1, 2005 till Nov 28, 2005

Database Overview

Name: AggrDb
Status: Loaded & Selected
Loading Date: Nov 29, 2005
Content Aggregation of all collected material for the last 90 days.

Tivoli. software

IBM

iView is the compliance and reporting interface. In iView's **Compliance Dashboard**, you can see whether your network is in compliance with company policy. You can also see any policy exceptions and special attentions, and you can generate reports on the W7 groups and also drill down into security events.

The **Enterprise Overview** is the graph on the left of the screen. It shows you the compliance status for every database in Tivoli Compliance Insight Manager, using information from the **Aggregation Database**.

The **compliance dashboard** identifies policy exceptions and special attentions. On the X and Y axes are two of the W7 groups. In this example, we show What – what action – on the Y axis and Who – which user groups – on the X axis. You can configure it to show different W7 groups.

The bubble at the intersection of these two groups indicates who is doing what. The size of the bubble indicates the number of log records. If the number of log records increases, then the bubble gets bigger. The color of the bubble indicates the level of compliance. If the bubble is large and blue, then there were many instances of a given action but those instances were in compliance with policy. If the bubble is red, then this indicates that a user's actions are not in compliance with the policy. An orange bubble indicates a middle ground between the highest severity level, indicated by red, and the lowest severity level, indicated by blue.

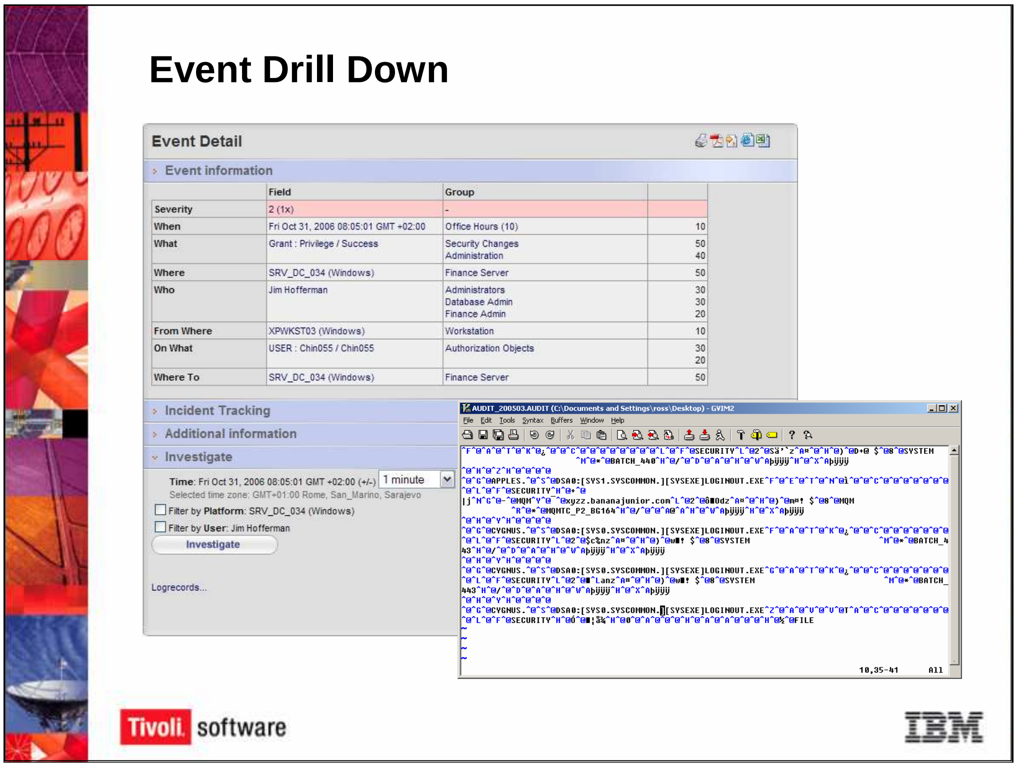
You can drill down by clicking on the bubble. Tivoli Compliance Insight Manager will show you all of the event details related to this incident, and you can create a report and document the incident for further action.

The **Trend Graphic** on the right side of the screen shows you your compliance levels over time and compares the actual number of policy exceptions and special attentions with your desired number of policy exceptions and special attentions. It's a quick way to see where you are, compared with where you would like to be.

Logs are stored in the **depot** and processed in the Tivoli Compliance Insight Manager Server. The **Database Overview**, at the bottom of the screen, shows you what has been loaded into each of the databases, enabling you to have a partitioned view of certain network or business functions. You can select a database and see the compliance dashboard for only that database, or you can select the Aggregation database and see information from all of the databases.

Each individual database is called a **Generic Event Module Database**, or **GEM Database**. For example, you could create a database for all financial records. Using Tivoli Compliance Insight Manager's **compliance dashboard**, you could drill into the database and see the level of compliance and run reports. This is a good way to perform a self-audit to check your policy compliance.

You can define as many databases as you would like. By default, Tivoli Compliance Insight Manager comes with one predefined database, the **Aggregation Database**. The Aggregation Database, or AggrDb, as it is abbreviated, shows you an enterprise-wide view of network activity.



Event Drill Down

Event Detail

Event information

	Field	Group	
Severity	2 (1x)	-	
When	Fri Oct 31, 2006 08:05:01 GMT +02:00	Office Hours (10)	10
What	Grant : Privilege / Success	Security Changes Administration	50 40
Where	SRV_DC_034 (Windows)	Finance Server	50
Who	Jim Hofferman	Administrators Database Admin Finance Admin	30 30 20
From Where	XPWKST03 (Windows)	Workstation	10
On What	USER : Chin055 / Chin055	Authorization Objects	30 20
Where To	SRV_DC_034 (Windows)	Finance Server	50

Incident Tracking

Additional information

Investigate

Time: Fri Oct 31, 2006 08:05:01 GMT +02:00 (+/-) 1 minute

Selected time zone: GMT+01:00 Rome, San_Marino, Sarajevo

□ Filter by **Platform**: SRV_DC_034 (Windows)

□ Filter by **User**: Jim Hofferman

Investigate

Logrecords...

AUDIT_200503.AUDIT (C:\Documents and Settings\ross\Desktop) - GVIM2

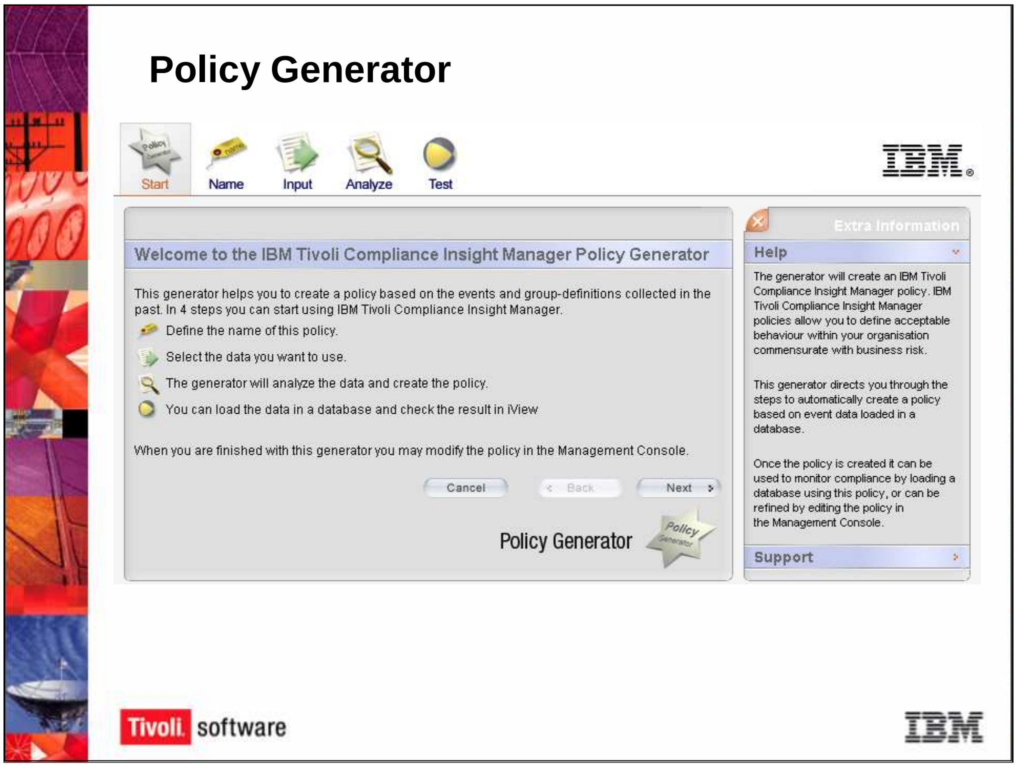
```
^F^@^A^@^T^@^K^@¿^@^@^C^@^@^@^@^@^@^@^@^L^@^F^@SECURITY^L^@2^@Sä'`z^A¤^@^H^@)^@D+@ $^@8^@SYSTEM
           ^M^@*^@BATCH_440^H^@/^@^D^@^A^@^H^@^W^Aþÿÿÿ^H^@^X^Aþÿÿÿ

^@^H^@^Z^H^@^@^@^@
^@^G^@APPLES.^@^S^@DSA0:[SYS1.SYSCOMMON.][SYSEXE]LOGINOUT.EXE^F^@^E^@^T^@^N^@ì^@^@^C^@^@^@^@^@^@^@
^@^L^@^F^@SECURITY^H^@+^@
|j^N^G^@-^@MQM^Y^@¯^@xyzz.bananajunior.com^L^@2^@ô■Odz^A¤^@^H^@)^@m¤! $^@8^@MQM
     ^R^@*^@MQMTC_P2_BG164^H^@/^@^@^A@^A^H^@^W^Aþÿÿÿ^H^@^X^Aþÿÿÿ

^@^H^@^Y^H^@^@^@^@
^@^G^@CYGNUS.^@^S^@DSA0:[SYS0.SYSCOMMON.][SYSEXE]LOGINOUT.EXE^F^@^A^@^T^@^K^@¿^@^@^C^@^@^@^@^@^@^@
^@^L^@^F^@SECURITY^L^@2^@$c%nz^A¤^@^H^@)^@w■! $^@8^@SYSTEM                 ^M^@*^@BATCH_4
43^H^@/^@^D^@^A^@^H^@^W^Aþÿÿÿ^H^@^X^Aþÿÿÿ
^@^H^@^Y^H^@^@^@^@
^@^G^@CYGNUS.^@^S^@DSA0:[SYS0.SYSCOMMON.][SYSEXE]LOGINOUT.EXE^G^@^A^@^T^@^K^@¿^@^@^C^@^@^@^@^@^@^@
^@^L^@^F^@SECURITY^L^@2^@■^Lanz^A¤^@^H^@)^@w■! $^@8^@SYSTEM                 ^M^@*^@BATCH_
443^H^@/^@^D^@^A^@^H^@^W^Aþÿÿÿ^H^@^X^Aþÿÿÿ
^@^H^@^Y^H^@^@^@^@
^@^G^@CYGNUS.^@^S^@DSA0:[SYS0.SYSCOMMON.][SYSEXE]LOGINOUT.EXE^Z^@^A^@^V^@^V^@T^A^@^C^@^@^@^@^@^@^@
^@^L^@^F^@SECURITY^H^@Ó^@■¦å¾^H^@0^@^A^@^@^@^H^@^A^@^A^@^@^@^H^@½^@FILE
~
~
~
~
                                                              10,35-41      All
```

Event Drill Down: Find Out What Happened and Who Did It

You can drill down into events from the Compliance Dashboard and from the reports. The Event Detail shows you the severity level and W7 event information, showing you what happened, who did it, when, and so on. You can even drill down into the logs themselves using the forensic search capabilities of the Log Manager.

You can distribute this report by printing it or by converting it into PDF, CSV, HTML, or Microsoft Excel file.

Policy Generator



Welcome to the IBM Tivoli Compliance Insight Manager Policy Generator

This generator helps you to create a policy based on the events and group-definitions collected in the past. In 4 steps you can start using IBM Tivoli Compliance Insight Manager.

- Define the name of this policy.
- Select the data you want to use.
- The generator will analyze the data and create the policy.
- You can load the data in a database and check the result in iView

When you are finished with this generator you may modify the policy in the Management Console.

Help

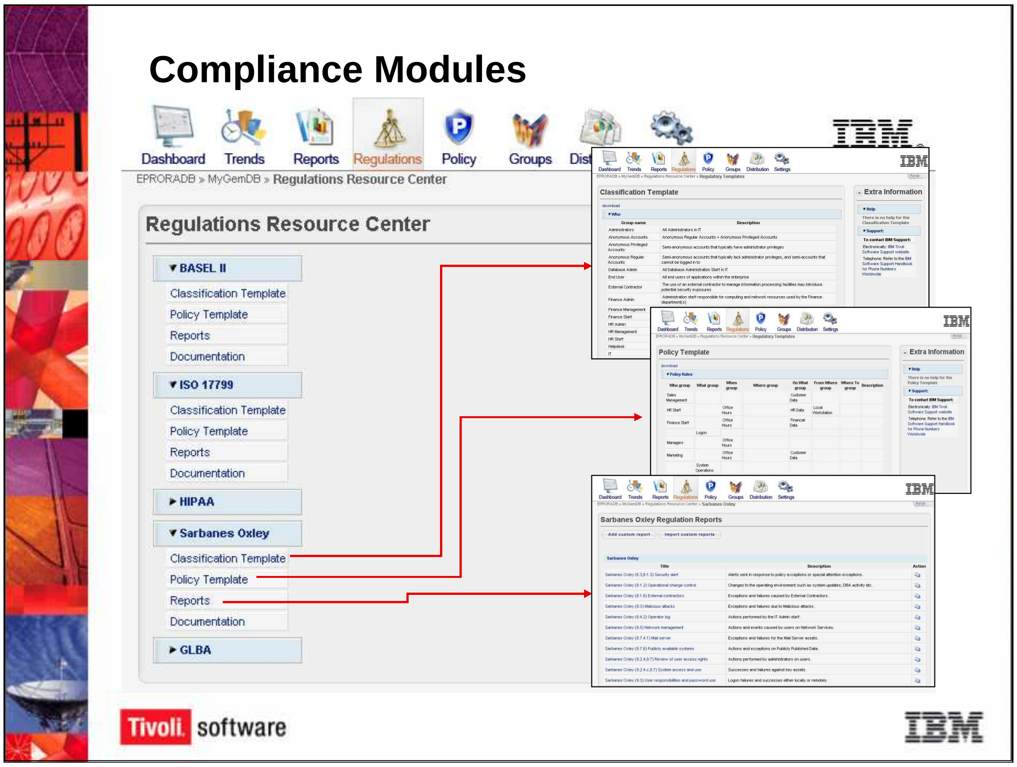
The generator will create an IBM Tivoli Compliance Insight Manager policy. IBM Tivoli Compliance Insight Manager policies allow you to define acceptable behaviour within your organisation commensurate with business risk.

This generator directs you through the steps to automatically create a policy based on event data loaded in a database.

Once the policy is created it can be used to monitor compliance by loading a database using this policy, or can be refined by editing the policy in the Management Console.

Tivoli Compliance Insight Manager determines whether your users' network behavior is in compliance with your company's security and acceptable use policies by comparing the log records to the stored policies. The **Policy Generator** allows you to create policies from existing logs. If your current network activity is acceptable to you, you can use the Policy Generator to load the data from Windows files servers and Check Point firewalls, apply heuristics, and generate policies using the logs as a baseline. You can also define policies manually.

Tivoli Compliance Insight Manager also includes **policy templates** that define acceptable use according to the regulations and standards that your company needs to comply with. For example, if you need to comply with Sarbanes Oxley (SOX), then you would employ the SOX policies and run reports against that criteria.



Compliance Modules

Dashboard
Trends
Reports
Regulations
Policy
Groups
Distribution
Settings
EPRORADB » MyGemDB » Regulations Resource Center » Regulatory Templates
Portal

Classification Template

download

▼Who

Group name	Description
Administrators	All Administrators in IT
Anonymous Accounts	Anonymous Regular Accounts + Anonymous Privileged Accounts
Anonymous Privileged Accounts	Semi-anonymous accounts that typically have administrator privileges
Anonymous Regular Accounts	Semi-anonymous accounts that typically lack administrator privileges, and semi-accounts that cannot be logged in to
Database Admin	All Database Administration Staff in IT
End User	All end users of applications within the enterprise
External Contractor	The use of an external contractor to manage information processing facilities may introduce potential security exposures
Finance Admin	Administration staff responsible for computing and network resources used by the Finance department(s)
Finance Management	
Finance Staff	
HR Admin	
HR Management	
HR Staff	
Helpdesk	
IT	

Extra Information

▼Help

There is no help for the Classification Template

▼Support:

To contact IBM Support:

Electronically: IBM Tivoli Software Support website

Telephone: Refer to the IBM Software Support Handbook for Phone Numbers Worldwide

Dashboard
Trends
Reports
Regulations
Policy
Groups
Distribution
Settings
EPRORADB » MyGemDB » Regulations Resource Center » Regulatory Templates
Portal

Policy Template

download

▼Policy Rules

Who group	What group	When group	Where group	On What group	From Where group	Where To group	Description
Sales Management				Customer Data			
HR Staff		Office Hours		HR Data	Local Workstation		
Finance Staff		Office Hours		Financial Data			
	Logon						
Managers		Office Hours					
Marketing		Office Hours		Customer Data			
	System Operations						

Extra Information

▼Help

There is no help for the Policy Template

▼Support:

To contact IBM Support:

Electronically: IBM Tivoli Software Support website

Telephone: Refer to the IBM Software Support Handbook for Phone Numbers Worldwide

Sarbanes Oxley Regulation Reports

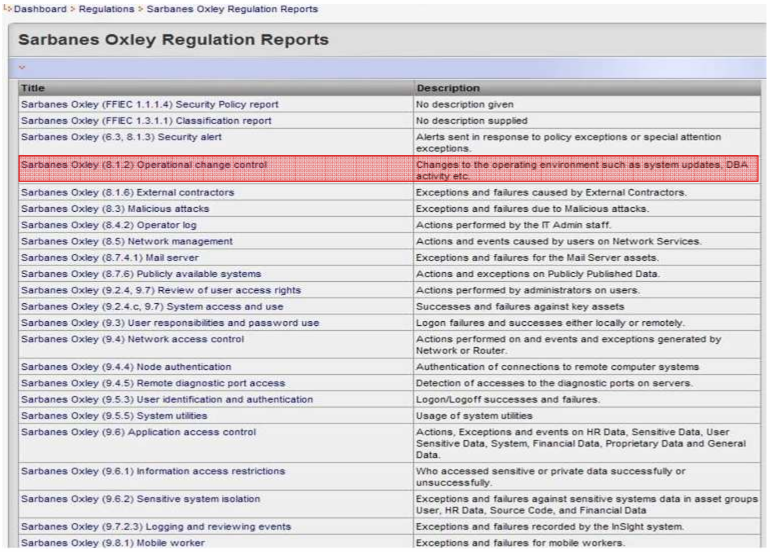
Sarbanes Oxley

Title	Description	Action
Sarbanes Oxley (6.3,8.1.3) Security alert	Alerts sent in response to policy exceptions or special attention exceptions.	
Sarbanes Oxley (8.1.2) Operational change control	Changes to the operating environment such as system updates, DBA activity etc.	
Sarbanes Oxley (8.1.6) External contractors	Exceptions and failures caused by External Contractors.	
Sarbanes Oxley (8.3) Malicious attacks	Exceptions and failures due to Malicious attacks.	
Sarbanes Oxley (8.4.2) Operator log	Actions performed by the IT Admin staff.	
Sarbanes Oxley (8.5) Network management	Actions and events caused by users on Network Services.	
Sarbanes Oxley (8.7.4.1) Mail server	Exceptions and failures for the Mail Server assets.	
Sarbanes Oxley (8.7.6) Publicly available systems	Actions and exceptions on Publicly Published Data.	
Sarbanes Oxley (9.2.4,9.7) Review of user access rights	Actions performed by administrators on users.	
Sarbanes Oxley (9.2.4.c,9.7) System access and use	Successes and failures against key assets.	
Sarbanes Oxley (9.3) User responsibilities and password use	Logon failures and successes either locally or remotely.	

The **Compliance Modules** listed in the Tivoli Compliance Insight Manager Portal include whichever modules that you purchased.

Consul offers numerous modules designed to correspond to specific regulations and industry standards, including the Sarbanes Oxley Act (SOX), Health Information Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA), ISO 17799, among others. The Compliance module goes through the regulation and reports on the company's level of compliance with each item. Customers can also work with IBM Tivoli Professional Services staff to develop **custom reports**.

Compliance Reports



Dashboard > Regulations > Sarbanes Oxley Regulation Reports

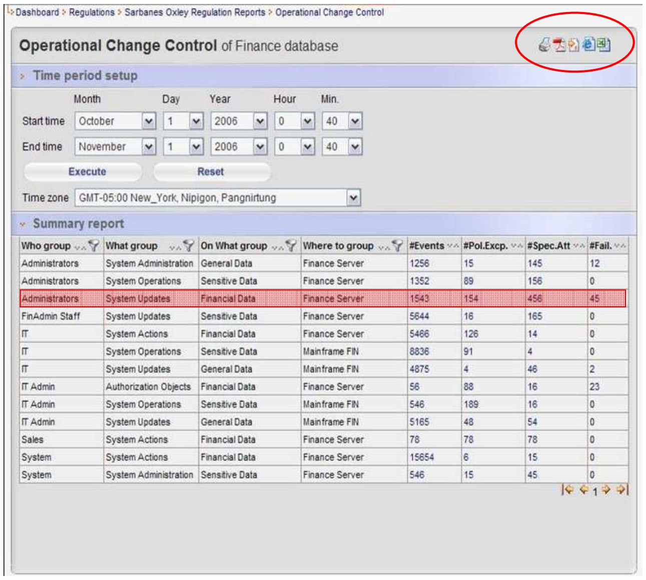
Sarbanes Oxley Regulation Reports

Title	Description
Sarbanes Oxley (FFIEC 1.1.1.4) Security Policy report	No description given
Sarbanes Oxley (FFIEC 1.3.1.1) Classification report	No description supplied
Sarbanes Oxley (6.3, 8.1.3) Security alert	Alerts sent in response to policy exceptions or special attention exceptions.
Sarbanes Oxley (8.1.2) Operational change control	Changes to the operating environment such as system updates, DBA activity etc.
Sarbanes Oxley (8.1.6) External contractors	Exceptions and failures caused by External Contractors.
Sarbanes Oxley (8.3) Malicious attacks	Exceptions and failures due to Malicious attacks.
Sarbanes Oxley (8.4.2) Operator log	Actions performed by the IT Admin staff.
Sarbanes Oxley (8.5) Network management	Actions and events caused by users on Network Services.
Sarbanes Oxley (8.7.4.1) Mail server	Exceptions and failures for the Mail Server assets.
Sarbanes Oxley (8.7.6) Publicly available systems	Actions and exceptions on Publicly Published Data.
Sarbanes Oxley (9.2.4, 9.7) Review of user access rights	Actions performed by administrators on users.
Sarbanes Oxley (9.2.4.c, 9.7) System access and use	Successes and failures against key assets
Sarbanes Oxley (9.3) User responsibilities and password use	Logon failures and successes either locally or remotely.
Sarbanes Oxley (9.4) Network access control	Actions performed on and events and exceptions generated by Network or Router.
Sarbanes Oxley (9.4.4) Node authentication	Authentication of connections to remote computer systems
Sarbanes Oxley (9.4.5) Remote diagnostic port access	Detection of accesses to the diagnostic ports on servers.
Sarbanes Oxley (9.5.3) User identification and authentication	Logon/Logoff successes and failures.
Sarbanes Oxley (9.5.5) System utilities	Usage of system utilities
Sarbanes Oxley (9.6) Application access control	Actions, Exceptions and events on HR Data, Sensitive Data, User Sensitive Data, System, Financial Data, Proprietary Data and General Data.
Sarbanes Oxley (9.6.1) Information access restrictions	Who accessed sensitive or private data successfully or unsuccessfully.
Sarbanes Oxley (9.6.2) Sensitive system isolation	Exceptions and failures against sensitive systems data in asset groups User, HR Data, Source Code, and Financial Data
Sarbanes Oxley (9.7.2.3) Logging and reviewing events	Exceptions and failures recorded by the InSight system.
Sarbanes Oxley (9.8.1) Mobile worker	Exceptions and failures for mobile workers.

In this example, we look at the Sarbanes Oxley (SOX) Compliance Module. There are several reports for different issues monitored by SOX, such as the Security Alert Report, which shows whether alerts are issued to notify security administrators about policy exceptions or special attentions, and the Operational Change Control Report, which shows changes made to the operating environment such as system updates or database administrator activity.

You can run all of the reports or just the reports that your auditor asks for. The main benefit of the Tivoli Compliance Insight Manager Compliance Modules is that you can easily and quickly report on your network controls and answer auditor questions without interrupting the business.

SOX Operation Change Control Report



Dashboard > Regulations > Sarbanes Oxley Regulation Reports > Operational Change Control

Operational Change Control of Finance database

Time period setup

	Month	Day	Year	Hour	Min.
Start time	October	1	2006	0	40
End time	November	1	2006	0	40

Time zone: GMT-05:00 New_York, Nipigon, Pangnirtung

Summary report

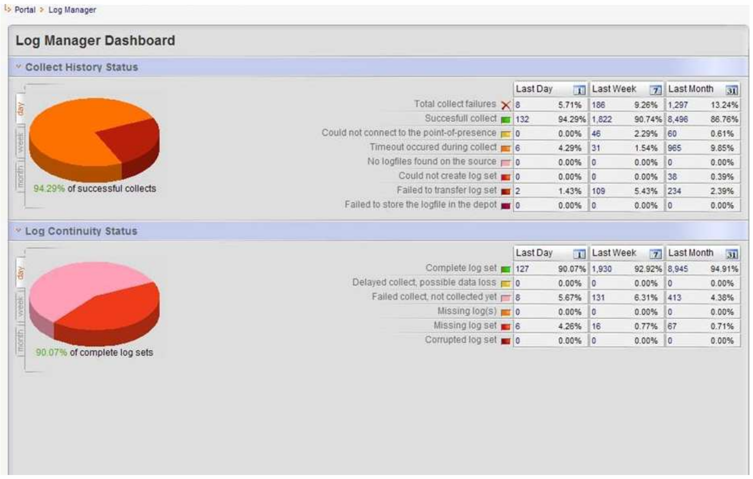
Who group	What group	On What group	Where to group	#Events	#Pol.Excp.	#Spec.Att	#Fail.
Administrators	System Administration	General Data	Finance Server	1256	15	145	12
Administrators	System Operations	Sensitive Data	Finance Server	1352	89	156	0
Administrators	System Updates	Financial Data	Finance Server	1543	154	456	45
FinAdmin Staff	System Updates	Sensitive Data	Finance Server	5644	16	165	0
IT	System Actions	Financial Data	Finance Server	5466	126	14	0
IT	System Operations	Sensitive Data	Mainframe FIN	8836	91	4	0
IT	System Updates	General Data	Mainframe FIN	4875	4	46	2
IT Admin	Authorization Objects	Financial Data	Finance Server	56	88	16	23
IT Admin	System Operations	Sensitive Data	Mainframe FIN	546	189	16	0
IT Admin	System Updates	General Data	Mainframe FIN	5165	48	54	0
Sales	System Actions	Financial Data	Finance Server	78	78	78	0
System	System Actions	Financial Data	Finance Server	15654	6	15	0
System	System Administration	Sensitive Data	Finance Server	546	15	45	0

As mentioned before, each compliance module contains numerous reports and that correspond to each reporting item in the regulation.

Here is an example of the Operational Change Control Report from the Sarbanes Oxley Compliance Module. The Operation Change Control Report shows all operational changes made by different groups within the organization. You can drill down into the events, policy exceptions, special attentions, and failures to see details on the specific events summarized in this report.

You can also distribute this report by printing it or by converting it into a PDF, CSV, HTML, or Microsoft Excel file.

Log Manager



Log Manager Dashboard

Collect History Status

	Last Day		Last Week		Last Month	
Total collect failures ✗	8	5.71%	186	9.26%	1,297	13.24%
Succesfull collect 🟩	132	94.29%	1,822	90.74%	8,496	86.76%
Could not connect to the point-of-presence 🟨	0	0.00%	46	2.29%	60	0.61%
Timeout occured during collect 🟧	6	4.29%	31	1.54%	965	9.85%
No logfiles found on the source	0	0.00%	0	0.00%	0	0.00%
Could not create log set 🟥	0	0.00%	0	0.00%	38	0.39%
Failed to transfer log set 🟥	2	1.43%	109	5.43%	234	2.39%
Failed to store the logfile in the depot 🟥	0	0.00%	0	0.00%	0	0.00%

Log Continuity Status

	Last Day		Last Week		Last Month	
Complete log set 🟩	127	90.07%	1,930	92.92%	8,945	94.91%
Delayed collect, possible data loss 🟨	0	0.00%	0	0.00%	0	0.00%
Failed collect, not collected yet	8	5.67%	131	6.31%	413	4.38%
Missing log(s) 🟧	0	0.00%	0	0.00%	0	0.00%
Missing log set 🟥	6	4.26%	16	0.77%	67	0.71%
Corrupted log set 🟥	0	0.00%	0	0.00%	0	0.00%

Tivoli. software IBM

The **Log Manager** is Tivoli Compliance Insight Manager's log management interface, which includes the **Log History** and **Log Continuity Reports** that show you which logs have been collected and whether those log collections were successful. The Log Manager also enables you to investigate logs using a Boolean search tool called the **Depot Investigation Tool**.

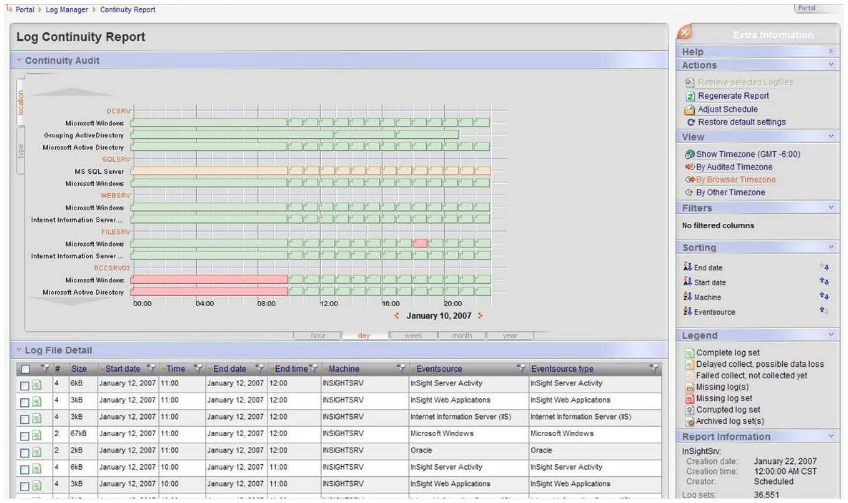
Tivoli Compliance Insight Manager can collect almost any log from any type of machine or platform. It can prove that it has collected the logs and report on the status of those log collection events in the Log Manager interface.

The **Log Manager Dashboard** summarizes information about your log collection efforts. It shows both the **log collection status** and the **log continuity status** on the same page, so that you can immediately see the status of your log collection and management efforts.

On the left side of the screen is a pie chart. The chart shows the status of the log collection history and the log continuity status. If the log collection events were successful, the pie chart is green. If some of the log collection events were unsuccessful, i.e., the collection was delayed or some other problem occurred, then Tivoli Compliance Insight Manager diagnoses the problem. Each status is represented by a different color.

On the right side of the screen is a table showing the number of log collection events for the last day, last week, and last month. The table breaks down the log collection events by their status or event diagnosis. You can click on the blue hyperlinked numbers in the table to drill down into the collection events. Typically, if a log collection event fails, it indicates a physical problem affecting the link between the Tivoli Compliance Insight Manager server and the audited machine, such as a disconnected router. The diagnosis helps you remediate any problems, so that the logs can be consistently and reliably collected.

Log Continuity Report



□	#	Size	Start date	Time	End date	End time	Machine	Eventsource	Eventsource type
□	4	6kB	January 12, 2007	11:00	January 12, 2007	12:00	INSIGHTSRV	InSight Server Activity	InSight Server Activity
□	4	3kB	January 12, 2007	11:00	January 12, 2007	12:00	INSIGHTSRV	InSight Web Applications	InSight Web Applications
□	4	3kB	January 12, 2007	11:00	January 12, 2007	12:00	INSIGHTSRV	Internet Information Server (IIS)	Internet Information Server (IIS)
□	2	67kB	January 12, 2007	11:00	January 12, 2007	12:00	INSIGHTSRV	Microsoft Windows	Microsoft Windows
□	2	2kB	January 12, 2007	11:00	January 12, 2007	12:00	INSIGHTSRV	Oracle	Oracle
□	4	6kB	January 12, 2007	10:00	January 12, 2007	11:00	INSIGHTSRV	InSight Server Activity	InSight Server Activity
□	4	3kB	January 12, 2007	10:00	January 12, 2007	11:00	INSIGHTSRV	InSight Web Applications	InSight Web Applications

InSightSrv:
Creation date: January 22, 2007
Creation time: 12:00:00 AM CST
Creator: Scheduled
Log sets: 36,551

As logs are collected, Tivoli Compliance Insight Manager stores the logs in the depot as **chunks**. Each time a collection occurs, Tivoli Compliance Insight Manager collects a chunk of information, that is, the amount of information that was generated since the last time Tivoli Compliance Insight Manager collected the audit trail from the machine. The **chunk** is the delta of the audit trail.

The Log Continuity Report shows the **Continuity Audit** graph, where each bar represents a chunk. The longer the bar, the longer the time between the log collections. Using the Management Console, you can setup the automated collection schedule.

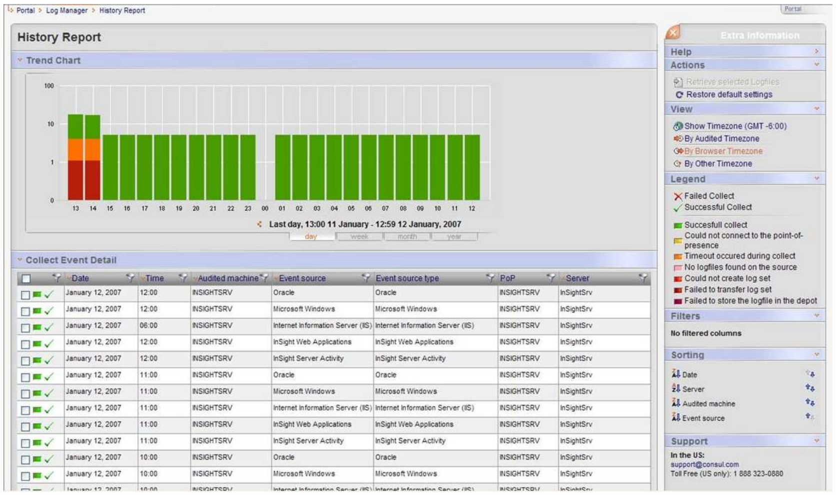
The Continuity Audit graph shows the different platforms, systems, applications, and services that are being audited on the left. You can see the continuity status for each system.

Color coding shows the status of the log chunks. Green indicates that the log chunks were collected in entirety as scheduled. If a problem occurred that affected the log collection, then the color coding reports what happened. For example, the Microsoft SQL Server is shown in yellow because the collection was delayed, indicating possible data loss.

As we mentioned earlier, if a collection event fails, then there is typically a physical problem with the connection between the Tivoli Compliance Insight Manager server and the audited machine. In addition, Tivoli Compliance Insight Manager is self-healing. Our product will continue to attempt to collect the logs and if it is able to successfully connect to the audited machine, then it will collect all of the logs generated since the last collect.

At the bottom half of the screen is the Log File Detail table, which provides information about each log file. This is useful for investigating continuity problems, because you can see if problems are occurring on certain platforms or at certain times, and so on.

Log History Report



Last day, 13:00 11 January - 12:59 12 January, 2007

Collect Event Detail

□	Date	Time	Audited machine	Event source	Event source type	PoP	Server
□ 🟩 ✓	January 12, 2007	12:00	INSIGHTSRV	Oracle	Oracle	INSIGHTSRV	InSightSrv
□ 🟩 ✓	January 12, 2007	12:00	INSIGHTSRV	Microsoft Windows	Microsoft Windows	INSIGHTSRV	InSightSrv
□ 🟩 ✓	January 12, 2007	06:00	INSIGHTSRV	Internet Information Server (IIS)	Internet Information Server (IIS)	INSIGHTSRV	InSightSrv
□ 🟩 ✓	January 12, 2007	12:00	INSIGHTSRV	InSight Web Applications	InSight Web Applications	INSIGHTSRV	InSightSrv
□ 🟩 ✓	January 12, 2007	12:00	INSIGHTSRV	InSight Server Activity	InSight Server Activity	INSIGHTSRV	InSightSrv
□ 🟩 ✓	January 12, 2007	11:00	INSIGHTSRV	Oracle	Oracle	INSIGHTSRV	InSightSrv
□ 🟩 ✓	January 12, 2007	11:00	INSIGHTSRV	Microsoft Windows	Microsoft Windows	INSIGHTSRV	InSightSrv
□ 🟩 ✓	January 12, 2007	11:00	INSIGHTSRV	Internet Information Server (IIS)	Internet Information Server (IIS)	INSIGHTSRV	InSightSrv
□ 🟩 ✓	January 12, 2007	11:00	INSIGHTSRV	InSight Web Applications	InSight Web Applications	INSIGHTSRV	InSightSrv
□ 🟩 ✓	January 12, 2007	11:00	INSIGHTSRV	InSight Server Activity	InSight Server Activity	INSIGHTSRV	InSightSrv
□ 🟩 ✓	January 12, 2007	10:00	INSIGHTSRV	Oracle	Oracle	INSIGHTSRV	InSightSrv
□ 🟩 ✓	January 12, 2007	10:00	INSIGHTSRV	Microsoft Windows	Microsoft Windows	INSIGHTSRV	InSightSrv
□ 🟩 ✓	January 12, 2007	10:00	INSIGHTSRV	Internet Information Server (IIS)	Internet Information Server (IIS)	INSIGHTSRV	InSightSrv

Legend

- ✗ Failed Collect
- ✓ Successful Collect
- 🟩 Succesfull collect
- 🟨 Could not connect to the point-of-presence
- 🟧 Timeout occured during collect
- ▭ No logfiles found on the source
- 🟥 Could not create log set
- 🟥 Failed to transfer log set
- 🟥 Failed to store the logfile in the depot

No filtered columns

In the US:
support@consul.com
Toll Free (US only): 1 888 323-0880

The Log History Report enables you to prove to auditors that you have in place a regular and consistent log collection program.

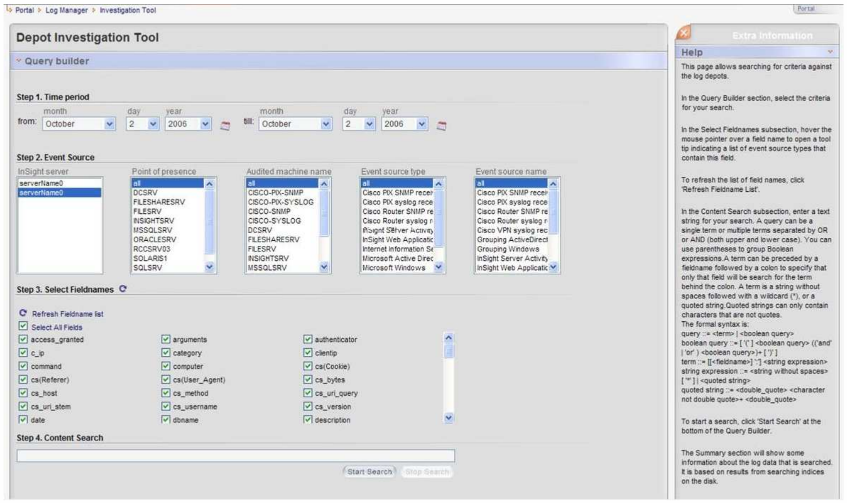
Every time Tivoli Compliance Insight Manager collects a log from an audited machine it is called a **log collection event**. The History Report shows the number of log collection events that occurred during a given time period, such as the past day, week, month, or year. You can change the time period of the report using the tabs at the bottom of the **Trend Chart**.

The History Report enables you quickly to see the results of log collection events (i.e., whether log collections were successful or unsuccessful). As in the Continuity Report, color coding shows the status of the collection event.

For example, on January 11th between 1 and 2 p.m. (1300-1400 hours) there was a timeout during the log collection event, indicated by the orange color. The connection between the Tivoli Compliance Insight Manager server and the audited machine dropped. But Tivoli Compliance Insight Manager reported this, and the technician was able to bring the audited machine online again so the log collection could occur.

At the bottom half of the screen is the Collect Event Detail table, which provides information about each collection event.

Log Investigation and Retrieval



Depot Investigation Tool

Query builder

Step 1. Time period

from: month October, day 2, year 2006 till: month October, day 2, year 2006

Step 2. Event Source

InSight server: serverName0, serverName0

Point of presence: all, DCSRV, FILESHARESRV, FILESRV, INSIGHTSRV, MSSQLSRV, ORACLESRV, RCCSRV03, SOLARIS1, SQLSRV

Audited machine name: all, CISCO-PIX-SNMP, CISCO-PIX-SYSLOG, CISCO-SNMP, CISCO-SYSLOG, DCSRV, FILESHARESRV, FILESRV, INSIGHTSRV, MSSQLSRV

Event source type: all, Cisco PIX SNMP recei, Cisco PIX syslog rece, Cisco Router SNMP re, Cisco Router syslog r, InSight Server Activity, InSight Web Applicatic, Internet Information Se, Microsoft Active Direc, Microsoft Windows

Event source name: all, Cisco PIX SNMP recei, Cisco PIX syslog rece, Cisco Router SNMP re, Cisco Router syslog r, Cisco VPN syslog rec, Grouping ActiveDirect, Grouping Windows, InSight Server Activity, InSight Web Applicatic

Step 3. Select Fieldnames

Refresh Fieldname list

☑ Select All Fields

☑ access_granted
☑ c_ip
☑ command
☑ cs(Referer)
☑ cs_host
☑ cs_uri_stem
☑ date
☑ arguments
☑ category
☑ computer
☑ cs(User_Agent)
☑ cs_method
☑ cs_username
☑ dbname
☑ authenticator
☑ clientip
☑ cs(Cookie)
☑ cs_bytes
☑ cs_uri_query
☑ cs_version
☑ description

Step 4. Content Search

Help

This page allows searching for criteria against the log depots.

In the Query Builder section, select the criteria for your search.

In the Select Fieldnames subsection, hover the mouse pointer over a field name to open a tool tip indicating a list of event source types that contain this field.

To refresh the list of field names, click 'Refresh Fieldname List'.

In the Content Search subsection, enter a text string for your search. A query can be a single term or multiple terms separated by OR or AND (both upper and lower case). You can use parentheses to group Boolean expressions.A term can be preceded by a fieldname followed by a colon to specify that only that field will be search for the term behind the colon. A term is a string without spaces followed with a wildcard (*), or a quoted string.Quoted strings can only contain characters that are not quotes.
The formal syntax is:
query ::= <term> | <boolean query>
boolean query ::= ['('] <boolean query> (('and' | 'or') <boolean query>)+ [')']
term ::= [[<fieldname>] ':'] <string expression>
string expression ::= <string without spaces> ['*'] | <quoted string>
quoted string ::= <double_quote> <character not double quote>+ <double_quote>

To start a search, click 'Start Search' at the bottom of the Query Builder.

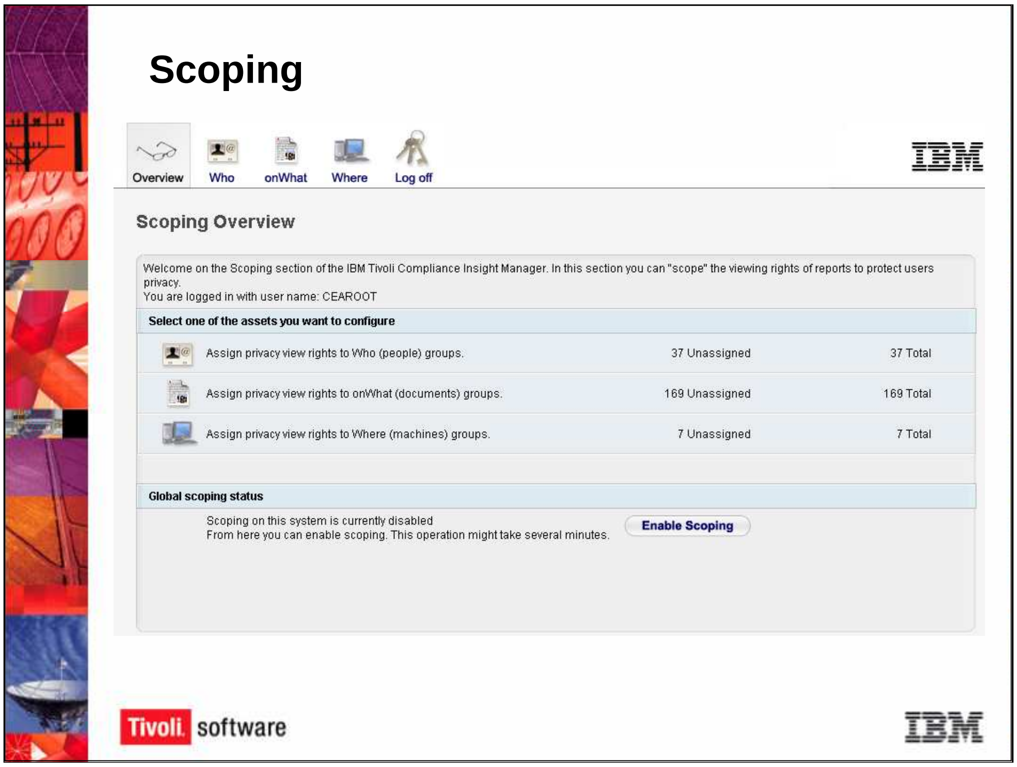
The Summary section will show some information about the log data that is searched. It is based on results from searching indices on the disk.

Tivoli software

IBM

Without an integrated log management program, it is very difficult to sort through the logs and find relevant events. Tivoli Compliance Insight Manager Log Manager makes it easy for you to investigate security incidents, search across the stored logs for events, and retrieve those logs for further investigation.

The **Depot Investigation Tool** uses a simple interface to enable you to build a complex search query. You can select the time period, the event source, and field names, or event attributes, in steps one, two, and three of the **Query Builder**. Step 4 allows you to enter a keyword using a Boolean syntax such as “username=admin”. When you run the search, Tivoli Compliance Insight Manager returns a list of all logs that contain events that match the search criteria. You can further sort the logs to narrow your search and you can download the logs for further analysis.



Scoping

Scoping Overview

Welcome on the Scoping section of the IBM Tivoli Compliance Insight Manager. In this section you can "scope" the viewing rights of reports to protect users privacy.
You are logged in with user name: CEAROOT

Select one of the assets you want to configure

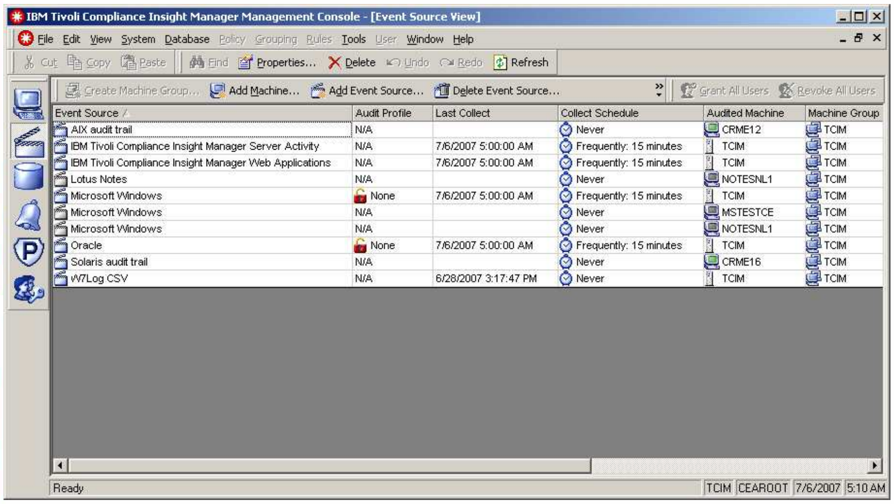
Assign privacy view rights to Who (people) groups.	37 Unassigned	37 Total
Assign privacy view rights to onWhat (documents) groups.	169 Unassigned	169 Total
Assign privacy view rights to Where (machines) groups.	7 Unassigned	7 Total

Global scoping status

Scoping on this system is currently disabled
From here you can enable scoping. This operation might take several minutes.

Tivoli Compliance Insight Manager monitors sensitive information, and, as such, it may not be necessary or appropriate for all users to be able to see all of the data in the system. The **Scoping** interface enables you to restrict viewing rights to protect user privacy. You can grant or limit viewing rights to the following W7 groups: the Who group, the onWhat group, and the Where group.

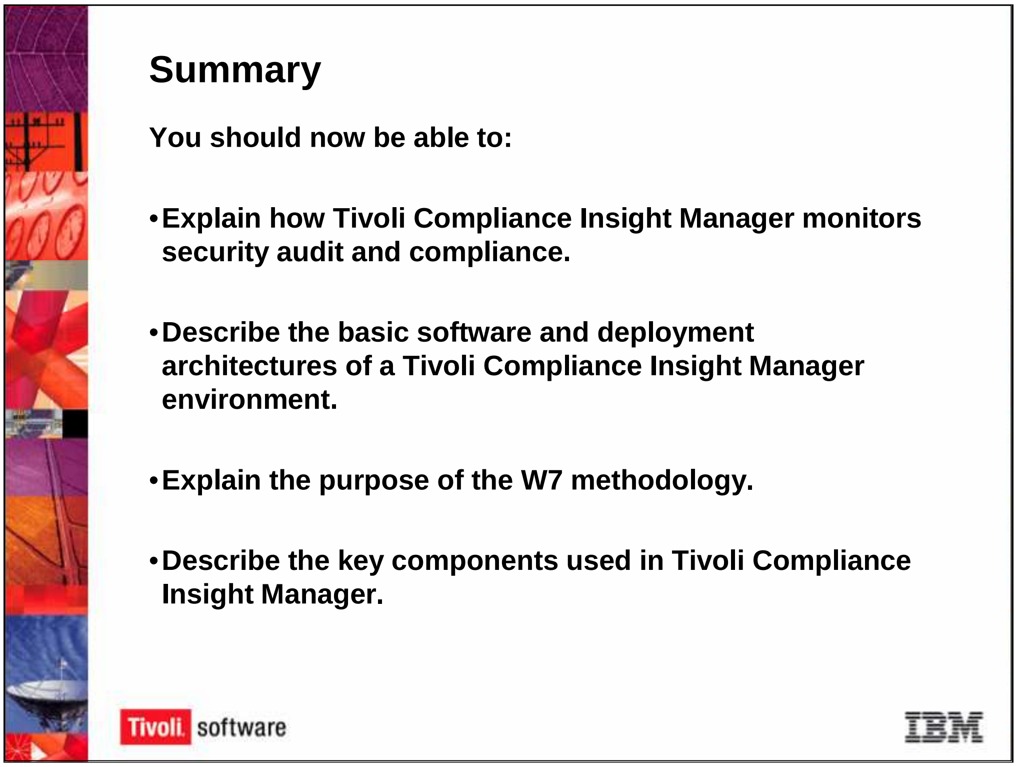
Management Console


IBM Tivoli Compliance Insight Manager Management Console - [Event Source View]
File Edit View System Database Policy Grouping Rules Tools User Window Help
Cut Copy Paste Find Properties... Delete Undo Redo Refresh
Create Machine Group... Add Machine... Add Event Source... Delete Event Source... Grant All Users Revoke All Users
Ready
TCIM CEAROOT 7/6/2007 5:10 AM

Event Source	Audit Profile	Last Collect	Collect Schedule	Audited Machine	Machine Group
AIX audit trail	N/A		Never	CRME12	TCIM
IBM Tivoli Compliance Insight Manager Server Activity	N/A	7/6/2007 5:00:00 AM	Frequently: 15 minutes	TCIM	TCIM
IBM Tivoli Compliance Insight Manager Web Applications	N/A	7/6/2007 5:00:00 AM	Frequently: 15 minutes	TCIM	TCIM
Lotus Notes	N/A		Never	NOTESNL1	TCIM
Microsoft Windows	None	7/6/2007 5:00:00 AM	Frequently: 15 minutes	TCIM	TCIM
Microsoft Windows	N/A		Never	MSTESTCE	TCIM
Microsoft Windows	N/A		Never	NOTESNL1	TCIM
Oracle	None	7/6/2007 5:00:00 AM	Frequently: 15 minutes	TCIM	TCIM
Solaris audit trail	N/A		Never	CRME16	TCIM
W7Log CSV	N/A	6/28/2007 3:17:47 PM	Never	TCIM	TCIM

While the Scoping interface grants and restricts viewing rights, the **Management Console** is used for system administration, user management, and policy creation.

The Management Console enables you to load data into the databases, add new machines and event sources, configure collection and reporting schedules, and add and configure users.



Summary

You should now be able to:

- **Explain how Tivoli Compliance Insight Manager monitors security audit and compliance.**
- **Describe the basic software and deployment architectures of a Tivoli Compliance Insight Manager environment.**
- **Explain the purpose of the W7 methodology.**
- **Describe the key components used in Tivoli Compliance Insight Manager.**

Tivoli. software
IBM

You should now be able to:

•Explain how the Tivoli Compliance InSight Suite monitors security audit and compliance.

• Describe the basic software and deployment architectures of an InSight environment.

• Explain the purpose of the W7 methodology.

• Describe the key components used in Tivoli Compliance Insight Manager.

This concludes the Tivoli Compliance Insight Manager v. 8.0 Overview course.