

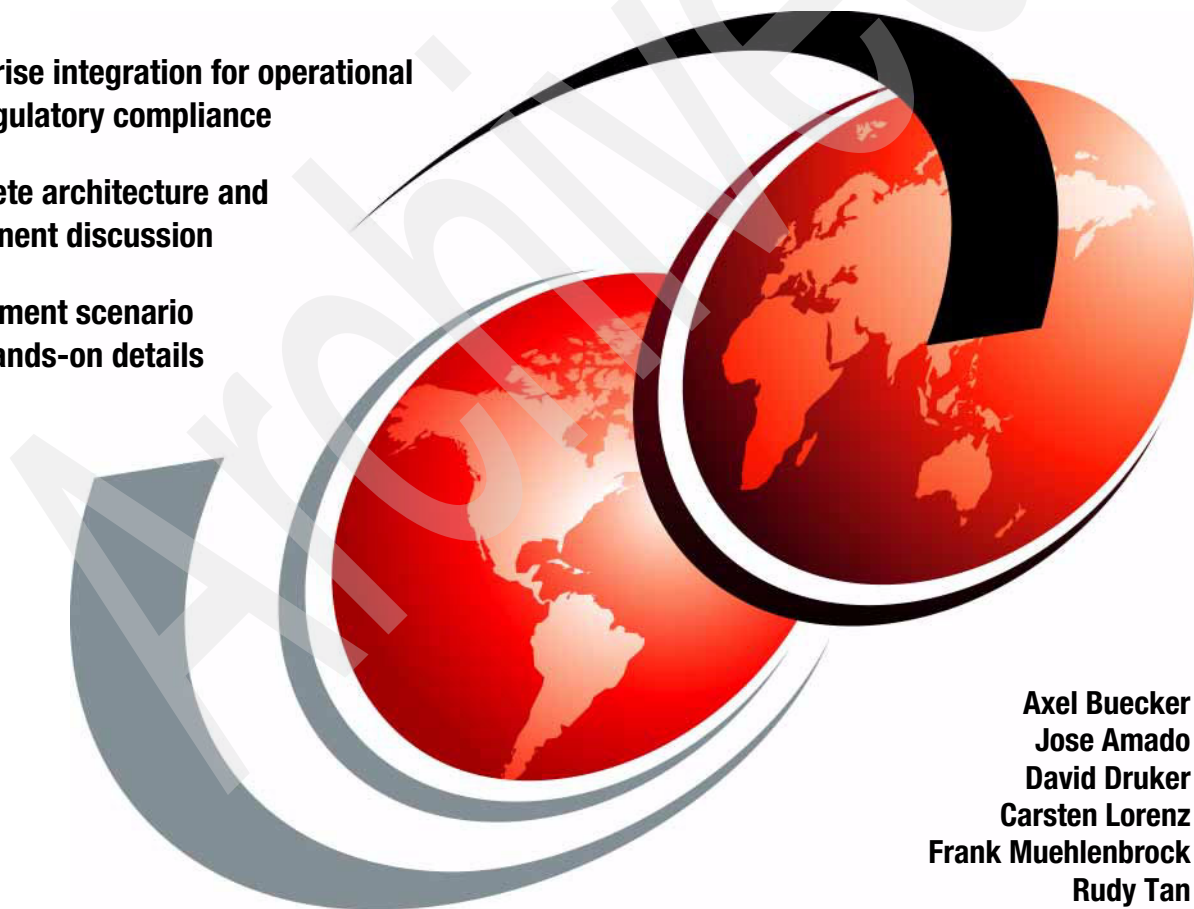
IT Security Compliance Management Design Guide

with IBM Tivoli Security Information and Event Manager

Enterprise integration for operational
and regulatory compliance

Complete architecture and
component discussion

Deployment scenario
with hands-on details



Axel Buecker
Jose Amado
David Druker
Carsten Lorenz
Frank Muehlenbrock
Rudy Tan



International Technical Support Organization

**IT Security Compliance Management Design Guide
with IBM Tivoli Security Information and Event
Manager**

July 2010

Archived

Note: Before using this information and the product it supports, read the information in “Notices” on page ix.

Archived

Second Edition (July 2010)

This edition applies to Version 2.0 of IBM Tivoli Security Information and Event Manager.

© Copyright International Business Machines Corporation 2010. All rights reserved.

Note to U.S. Government Users Restricted Rights -- Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Notices	ix
Trademarks	x
Preface	xi
The team who wrote this book	xi
Now you can become a published author, too!	xiv
Comments welcome	xiv
Stay connected to IBM Redbooks	xv
Summary of changes	xvii
July 2010, Second Edition	xvii
Part 1. Architecture and design	1
Chapter 1. Business context for IT security compliance management ...	3
1.1 Introduction to IT security compliance management	4
1.2 Business drivers for IT security compliance management	7
1.3 Business drivers for log management	9
1.4 Criteria of an IT security compliance management solution	9
1.5 Recent challenges for IT security compliance management	12
1.6 Conclusion	14
Chapter 2. Designing an IT security compliance management solution .	15
2.1 Security Information and Event Management architecture	16
2.1.1 Event types	20
2.2 Solution architecture	22
2.2.1 Projection of an IT security compliance solution	22
2.2.2 Definition of an IT security compliance solution	23
2.2.3 Design of an IT security compliance solution	24
2.3 Conclusion	25
Chapter 3. Introducing the IBM Security Information and Event Management solution	27
3.1 Introducing the IBM SIEM solution	28
3.1.1 IBM Security SiteProtector	28
3.1.2 IBM Guardium	29
3.1.3 IBM Tivoli Security Compliance Manager	30
3.1.4 IBM Tivoli Security Operations Manager	31
3.1.5 IBM Tivoli Security Information and Event Manager	33

3.2	The IBM SIEM architecture	36
3.2.1	Log Management	38
3.2.2	Compliance reporting, alerting, and basic event correlation	42
3.3	Real-time event correlation and alerting	46
3.4	SIEM integration scenarios	48
3.4.1	User personas	48
3.4.2	Typical issues encountered	48
3.4.3	SIEM scenario 1 solution	48
3.4.4	SIEM scenario 2 solution	49
3.4.5	SIEM scenario 3 solution	49
3.4.6	SIEM scenario 4 solution	50
3.4.7	SIEM scenario 5 solution	50
3.5	Conclusion	51
Chapter 4. IBM Tivoli Security Information and Event Manager component structure		53
4.1	Logical components	54
4.1.1	Log Management Base Component	54
4.1.2	Normalization Component	58
4.1.3	Forensics Component	61
4.1.4	Consolidation Component	62
4.1.5	LaunchPad	63
4.1.6	Agents	63
4.2	Data flow	71
4.2.1	Agent-based data flow log collection	71
4.2.2	SSH-based data flow log collection	74
4.2.3	Log Management reporting data flow	75
4.2.4	Normalization process data flow	76
4.3	Physical components	78
4.3.1	Centralized user management using LDAP	78
4.3.2	Functional components	81
4.3.3	Server types	82
4.3.4	Agent	84
4.3.5	Compliance modules	85
4.4	Deployment architecture	85
4.4.1	Log Management Server configuration	85
4.4.2	Single server configuration	86
4.4.3	Cluster configuration	86
4.5	Conclusion	87
Chapter 5. Compliance management solution design		89
5.1	Functional design and configuration	90
5.1.1	Phase 1: Discovery and analysis	91

5.1.2	Phase 2: Project definition and planning	94
5.1.3	Phase 3: Implementation	102
5.1.4	Phase 4: Product use	103
5.2	Operational design and configuration	103
5.2.1	Monitoring, maintenance, and availability	104
5.2.2	Archiving and information retention	112
5.2.3	Performance and scalability	115
5.2.4	Tivoli Security Information and Event Manager limits	116
5.2.5	Support	116
5.3	Conclusion	117
Part 2.	Customer environment	119
Chapter 6.	Introducing X-Y-Z Financial Accounting	121
6.1	Organization profile	122
6.2	Current IT infrastructure	122
6.3	Security compliance business objectives	126
6.3.1	Complying to security requirements in the industry	126
6.3.2	Maintaining and demonstrating management control	127
6.3.3	Integrating monitoring across a multi-platform environment	128
6.3.4	Harvesting and structuring information to specific needs	129
6.3.5	Establishing a cost-efficient and future-proofed solution	130
6.4	Conclusion	130
Chapter 7.	Compliance management design	131
7.1	Business requirements	132
7.2	Functional requirements	133
7.2.1	Business requirement 1	133
7.2.2	Business requirement 2	134
7.2.3	Business requirement 3	135
7.2.4	Business requirement 4	136
7.2.5	Business requirement 5	137
7.2.6	Business requirement 6	139
7.3	Design approach	140
7.3.1	Creating an implementation plan	140
7.4	Implementation approach	143
7.4.1	Determining what reports to generate	143
7.4.2	Monitoring target assets for reports	145
7.4.3	Identifying the data to be collected from each event source	146
7.4.4	Ensuring Tivoli Security Information and Event Manager's ability to monitor audit trails from that event source	146
7.4.5	Prioritizing the target systems and applications	147
7.4.6	Planning deployment	148
7.4.7	Dividing the tasks into phases	149

7.5 Conclusion	150
Chapter 8. Basic auditing	151
8.1 Phase one auditing	151
8.2 Installing the cluster	153
8.2.1 Installing an Enterprise Server	153
8.2.2 Installing a Standard Server	153
8.3 Phase one reporting requirements	154
8.4 Enabling and configuring auditing	155
8.4.1 Auditing settings for the Windows Security log	155
8.4.2 Active Directory audit policy settings	156
8.4.3 File server settings: Object access auditing	159
8.5 Configuring Standard Server for new event sources	164
8.5.1 Creating the Reporting Database	165
8.5.2 Creating system group and add Windows machines	166
8.5.3 Adding event sources	173
8.6 Installing an agent on the target machine	179
8.7 Configuring W7 groups	184
8.7.1 Configuring a new policy with W7 rules	194
8.8 Compliance Dashboard	213
8.8.1 Policy Exceptions	214
8.8.2 Special Attentions	217
8.8.3 Reports	219
8.9 Self-auditing	225
8.10 Conclusion	228
Chapter 9. Extending auditing to other supported platforms	229
9.1 IT environment	230
9.2 Basic approach	231
9.3 Auditing AIX 6.1 systems	231
9.3.1 Configuring auditing for AIX systems	231
9.3.2 Adding the AIX event source to Tivoli Security Information and Event Manager	236
9.3.3 The results	245
9.3.4 AIX auditing conclusion	249
9.4 Auditing Lotus Domino R6 systems	249
9.4.1 Configuring auditing for Domino systems	250
9.4.2 Adding the Domino event source	250
9.4.3 The results	253
9.5 Auditing SAP systems	259
9.5.1 Configuring auditing for SAP systems	260
9.5.2 Adding the SAP event source	261
9.5.3 The results	263

9.5.4	SAP R/3 auditing conclusion	266
9.6	Adding syslog receiver for any type of messages	266
9.6.1	Creating a Ubiquitous syslog receiver on AIX	267
9.6.2	Preparing the syslog file to be collected	270
9.6.3	Using the Log Management Depot Investigation tool	270
9.6.4	Result	275
9.7	Conclusion	275
Chapter 10. Customized and regulatory reporting		277
10.1	Producing customized reports	277
10.1.1	Creating a customized report	278
10.1.2	Distributing reports	284
10.2	Using compliance management modules	291
10.2.1	Tool-based regulatory compliance reporting	291
10.2.2	Running compliance reports	292
10.3	Conclusion	294
Chapter 11. System z integration		295
11.1	Reporting requirements	297
11.2	Audit settings	299
11.3	Implementation	304
11.3.1	Implementing the Standard Server	305
11.3.2	Implementing the Actuator	307
11.3.3	Basel II compliance management module implementation	327
11.4	Conclusion	350
Chapter 12. Custom event source integration		351
12.1	Introduction to custom event sources	352
12.1.1	Event source definition	352
12.1.2	Custom event source definition	352
12.2	Ubiquitous event source	353
12.3	W7Log event source	354
12.3.1	W7Log configurations	354
12.3.2	Transforming Quantwave log files into a valid W7Log format	357
12.3.3	Creating external event logs into the W7Log file format	362
12.3.4	Importing external event logs	374
12.4	The Generic ExtendIT event source	380
12.4.1	The collect script	381
12.4.2	Reusing existing collect scripts	383
12.4.3	The mapper files	385
12.4.4	Grouping files	386
12.4.5	Example of Generic ExtendIT event source	386
12.5	Custom event source methods comparison table	393
12.5.1	Ubiquitous event source pros and cons	394

12.5.2 W7Log event source pros and cons	394
12.5.3 Generic ExtendIT Pros and Cons	395
12.6 Creating a custom UIS using Generic ExtendIT	395
12.6.1 Example of custom UIS.	396
12.7 Conclusion.	402
Appendix A. Corporate policy and standards	403
Standards, practices, and procedures	405
Practical example	405
External standards and certifications	406
Industry specific requirements	407
Product or solution certifications	408
Nationally and internationally recognized standards.	409
Data Privacy Laws	409
Summary	410
Appendix B. Additional material	411
Locating the Web material	411
Using the Web material	412
How to use the Web material	412
Glossary	415
Related publications	427
IBM Redbooks publications	427
Other publications	427
Online resources	428
How to get IBM Redbooks publications	429
Help from IBM	429
Index	431

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:
IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504-1785 U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.


COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

Trademarks

IBM, the IBM logo, and [ibm.com](http://www.ibm.com) are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. These and other IBM trademarked terms are marked on their first occurrence in this information with the appropriate symbol (® or ™), indicating US registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at <http://www.ibm.com/legal/copytrade.shtml>

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

AIX®	Lotus®	Redbooks (logo)  ®
AS/400®	MVS™	System i®
CICS®	Notes®	System Storage®
DB2®	OS/390®	System z®
Domino®	OS/400®	Tivoli®
i5/OS®	Proventia®	WebSphere®
IBM®	RACF®	z/OS®
iSeries®	Redbooks®	
Lotus Notes®	Redpaper™	

The following terms are trademarks of other companies:

Snapshot, and the NetApp logo are trademarks or registered trademarks of NetApp, Inc. in the U.S. and other countries.

SAP R/3, SAP, and SAP logos are trademarks or registered trademarks of SAP AG in Germany and in several other countries.

Oracle, JD Edwards, PeopleSoft, Siebel, and TopLink are registered trademarks of Oracle Corporation and/or its affiliates.

Snapshot, and the Network Appliance logo are trademarks or registered trademarks of Network Appliance, Inc. in the U.S. and other countries.

Java, and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Microsoft, Windows NT, Windows, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.

Preface

To comply with government and industry regulations, such as Sarbanes-Oxley, Gramm Leach Bliley (GLBA), and COBIT (which can be considered a best-practices framework), organizations must constantly detect, validate, and report unauthorized changes and out-of-compliance actions within the Information Technology (IT) infrastructure. Using the IBM® Tivoli® Security Information and Event Manager solution organizations can improve the security of their information systems by capturing comprehensive log data, correlating this data through sophisticated log interpretation and normalization, and communicating results through a dashboard and full set of audit and compliance reporting.

In this IBM Redbooks® publication, we discuss the business context of security audit and compliance software for organizations and describe the logical and physical components of IBM Tivoli Security Information and Event Manager. We also present a typical deployment within a business scenario.

This book is a valuable resource for security officers, administrators, and architects who want to understand and implement a centralized security audit and compliance solution.

The team who wrote this book

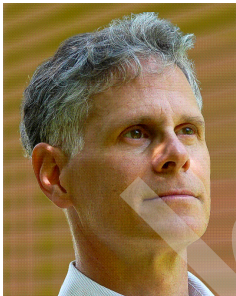
This book was produced by a team of specialists from around the world working at the International Technical Support Organization (ITSO), Austin Center.



Axel Buecker is a Certified Consulting Software IT Specialist at the ITSO, Austin Center. He writes extensively and teaches IBM classes worldwide about areas of software security architecture and network computing technologies. He has a degree in Computer Science from the University of Bremen, Germany. He has 23 years of experience in a variety of areas related to workstation and systems management, network computing, and e-business solutions. Before joining the ITSO in March 2000, Axel worked for IBM in Germany as a Senior IT Specialist in Software Security Architecture.



Jose Amado is a Senior Level 2 Support Engineer and consultant. He is the Tivoli Security Information and Event Manager and Tivoli Compliance Insight Manager Level 2 Technical Team lead. He works for IBM US in Guatemala. Jose has 12 years of experience with IT security solutions, and he has several certifications. For six years he has worked with Tivoli Security Information and Event Manager-related products and has been part of many international deployment projects for Security Information and Event Management (SIEM) solutions. Jose participated in beta testing of various versions of the product and worked on networking infrastructure designs for customers.



David Druker is an IBM Security Architect and works with IBM customers in central and western United States. He is known worldwide as an expert in IBM Tivoli Directory Integrator and has designed many solutions around this product. He has over 20 years of broad technology experience in security, programming, and enterprise architecture. David is a Senior Certified IT Specialist and holds a Ph.D. in Speech and Hearing Science from the University of Iowa.



Carsten Lorenz is a certified Senior Managing Consultant at IBM in the United Kingdom (UK). He manages security solutioning in large and complex IT infrastructure outsourcing engagements for customers throughout Europe, Middle-East and Africa. He has more than 10 years of experience in the security and compliance field, specializing in the areas of Security Management, IT Risk Assessment, Governance, and Operational Risk Management. Carsten performs consulting engagements with IBM customers in various industries, ranging from fortune 500 to small-to-medium sized businesses. Carsten is a CISSP, CISM, and a CISA, and he has a Bachelors Degree in European Studies from the University of Wolverhampton, UK, and a Diploma in Business Science from the University of Trier, Germany.



Frank Muehlenbrock is an IBM Information Security Manager with international experience in IT Security, Data Privacy and Risk and Compliance Management. He has 23 years of experience in the IT industry. Frank developed and implemented many IT security policies, processes, and procedures. He also conducted physical and logical security audits on a European scale. Frank has an Information Management degree from the Fachhochschule Reutlingen, Germany. He has a CISM certification of the ISACA organization and an MCSE and MCT. Frank co-authored three previous IBM Redbooks publications about IBM Tivoli Compliance Insight Manager. He also published technical articles in German journals and a book about implementing security guidelines. He is currently working on another book for the ISACA German chapter about the “Usage of Forensics in an Audit Organization”.



Rudy Tan is a Senior IT-Specialist who works as a technical course developer in the IBM Tivoli Lab in Delft, Netherlands. He has 17 years of experience in the IT industry with a focus on security. In the past 12 years, Rudy worked at Consul as a Tivoli Compliance Insight Manager developer, consultant, and trainer.

Thanks to the authors of the first edition of this book.

- ▶ The authors of the first edition, *IT Security Compliance Management Design Guide*, published in December 2007, were:

Ann-Louise Blair, Franc Cervan, Werner Filip, Scott Henley, Carsten Lorenz, Frank Muehlenbrock, and Rudy Tan

Thanks to the following people for their contributions to this project:

KaTrina Love-Abram, Technical Editor
International Technical Support Organization

Nick Briers, Rick Cohen
IBM

Now you can become a published author, too!

Here's an opportunity to spotlight your skills, grow your career, and become a published author - all at the same time! Join an ITSO residency project and help write a book in your area of expertise, while honing your experience using leading-edge technologies. Your efforts will help to increase product acceptance and customer satisfaction, as you expand your network of technical contacts and relationships. Residencies run from two to six weeks in length, and you can participate either in person or as a remote resident working from your home base.

Find out more about the residency program, browse the residency index, and apply online at:

ibm.com/redbooks/residencies.html

Comments welcome

Your comments are important to us!

We want our books to be as helpful as possible. Send us your comments about this book or other IBM Redbooks publications in one of the following ways:

- ▶ Use the online **Contact us** review Redbooks form found at:

ibm.com/redbooks

- ▶ Send your comments in an email to:

redbooks@us.ibm.com

- ▶ Mail your comments to:

IBM Corporation, International Technical Support Organization
Dept. HYTD Mail Station P099
2455 South Road
Poughkeepsie, NY 12601-5400

Stay connected to IBM Redbooks

- ▶ Find us on Facebook:
<http://www.facebook.com/IBMRedbooks>
- ▶ Follow us on Twitter:
<http://twitter.com/ibmredbooks>
- ▶ Look for us on LinkedIn:
<http://www.linkedin.com/groups?home=&gid=2130806>
- ▶ Explore new Redbooks publications, residencies, and workshops with the IBM Redbooks weekly newsletter:
<https://www.redbooks.ibm.com/Redbooks.nsf/subscribe?OpenForm>
- ▶ Stay current on recent Redbooks publications with RSS Feeds:
<http://www.redbooks.ibm.com/rss.html>

Archived

Summary of changes

In this section, we describe the technical changes made in this edition of the book and in previous editions. This edition might also include minor corrections and editorial changes that are not identified.

Summary of Changes
for SG24-7530-01
for IT Security Compliance Management Design Guide
as created or updated on July 14, 2010.

July 2010, Second Edition

This revision reflects the addition, deletion, or modification of new and changed information.

New information

- ▶ Tivoli Security Information and Event Manager V2 introduced a new Log Manager component to allow organizations to start small by centrally collecting log information. Refer to Chapter 4, “IBM Tivoli Security Information and Event Manager component structure” on page 53.
- ▶ Tivoli Security Information and Event Manager V2 provides a new consolidated web-based Graphical User Interface (GUI) that consolidates all functions for the different Tivoli Security Information and Event Manager use cases in a single GUI. It is based on the Tivoli Integration Portal. Information about the new GUI is dispersed throughout the book.

Changed information

- ▶ Since our first release of this book the industry term Security Information and Event Management (SIEM) underwent some minor changes—the actual discussion in Part I of the book reflects those changes.
- ▶ Several smaller changes are incorporated in the Tivoli Security Information and Event Manager V2 product and are reflected throughout the book.

Archived




Part 1

Architecture and design

In part 1, we discuss the overall business context for security compliance management of IT systems and explain the general business requirements for a security compliance management solution. We then describe a framework for providing security compliance functionality throughout an organization. In addition to this, we introduce the high-level components and new concepts for the design of a compliance management solution using Tivoli Security Information and Event Manager.

Additionally, we provide an understanding of the high-level product architecture of Tivoli Security Information and Event Manager. At the end of this part, we introduce the IBM Security Information and Event Management solution.

Archived



Business context for IT security compliance management

In this chapter, we discuss the overall *business context* for IT security compliance management of IT systems. After a short definition of the necessary terms, we describe the factors that influence *why* and *how* IT security compliance management must be conducted in a given business context. Further, we explain the general *business requirements* for an IT security compliance management solution.

1.1 Introduction to IT security compliance management

The process that an organization operates in accordance with expectations is called *compliance management*. For the area of IT security, the expectations are formulized as requirements in the IT security policies and can include requirements from the individual mission statement of an organization (like ethical behavior or business conduct guidelines) and requirements that are derived from external laws and regulations, such as¹:

- ▶ Sarbanes-Oxley
- ▶ Basel II
- ▶ Food and Drug Administration (FDA)
- ▶ NERC-CIP
- ▶ Health Insurance Portability and Accountability Act (HIPAA)
- ▶ Federal Information Security Management Act (FISMA)
- ▶ Gramm-Leach-Bliley Act (GLBA)
- ▶ Payment Card Industry Data Security Standard (PCI DSS)
- ▶ ISO 27001 / 27002

Information security defines the level of protection for information assets of an organization and summarizes all activities around the *security controls* that are applied to achieve a desired level of confidentiality, integrity, and availability of information assets. In a best practice approach, the desired level is derived by determining the balance between risks that result from a compromised information security and the benefit that is aligned with the information asset. It is a good business practice to minimize the security risk to information in proportion to the importance of such information to the business. *Security controls* are usually defined in a security policy framework.

A *security policy framework* is organized hierarchically. It starts with a top level organizational *security policy*, which is directly derived from the business context, defines the requirements rather broadly, and leaves room for interpretation. The next level consists of refining policies per business unit or department to implement the top level policy. Depending on the size of an organization, there might be several layers of security policies with increasing precision from top to bottom. At one point, the policies start to define technology requirements at a high level and are often referred to as *IT security standards*. There can be multiple levels of standards. Besides these standards about security requirements in technical terms, you can find *IT security procedures* and *IT security practices* that describe process details and work instructions to implement the security requirements.

¹ For a detailed description of the listed laws and regulations, refer to the glossary.

The benefit of a policy framework is the reduction of interpretation to a minimum, the translation of broad business directions into corresponding work instructions for processes and technical settings for systems, and the provision of extensive editable records about management direction on information security. There is more information about this discussion in Appendix A, “Corporate policy and standards” on page 403.

Bringing both definitions together, *IT security compliance* is understood as the process that safeguards that the operations of an organization meet the requirements that are defined in the IT security policies, which consolidate legal and regulatory obligations and management direction. IT security compliance management requires the ability to identify compliance criteria and to assess, to analyze, to consolidate, and to report on the previous, the current, and the expectable compliance status of security controls.

Security controls exist at the *organizational*, *process*, and *technical* levels:

- ▶ An *organizational* level security control can be a concept, such as separation of duties, for example, ensuring that someone who changes something is not the same person who controls the business need and proper execution of the change. This type of security control might require an organizational setup where those two employees report to multiple managers.
- ▶ A *process* level security control can be a concept, such as the four eyes principle, where a specific authorization requires two signatures (or passwords) to be presented before a transaction can be completed. As a result, this process step always requires two employees to be available for execution.
- ▶ A simple *technical* security control can be a required length for a password or specific permissions that are defined for accessing an operating system resource or business data. Operating systems and applications provide configuration settings that allow the administrator to specify minimum password lengths so that the system itself can enforce this control. A more complex technical security control can be the requirement to run an antivirus service (with up-to-date virus definition files) on a computer system or a correctly configured port filter.

Technical security controls are the easiest to monitor because computer systems save audit trails and configuration files, which can be checked for fulfillment of requirements. Security controls on the organizational and the process level (especially, when process steps are not performed with the help of technology) are harder to check and to control because they are less persistent, and audit trails are not created automatically and are easier to manipulate.

Compliance management versus IT security compliance management: In the context of this book, we intentionally distinguish between *compliance management* and *IT security compliance management*.

A *compliance management system* represents the practice that an organization applies to manage the entire compliance process, such as the audit compliance functions, which are independently testing the organization's compliance program and includes adherence to all policies, procedures, and applicable laws and regulations.

An *IT security compliance management system* represents a method that can help an organization to prove that their IT systems and infrastructure are being operated according to all policies, procedures, and applicable laws and regulations. This proof can be achieved by continually and consistently collecting log information to document and report on who accessed important IT resources, and when those accesses occurred.

An IT security compliance management system can be helpful in several situations, for example, to create audit reports, to prevent or to clarify IT security incidents, or just to gather evidence for future compliance activities.

Audit reports can document the level of compliance to any internal policy, external regulation, or applicable law, which applies to any type of audit you can think of:

- ▶ An *internal audit report* can document compliance or non-compliance to internal policies on internal systems.
- ▶ A *supplier audit report* can state the level of compliance to the management system, procedures, or processes as part of an assurance process that is required by customers.
- ▶ The third report type is driven by a *3rd party audit*, such as a 27001 certification or a regulation or law that your organization must adhere to.

For IT security incident management, compliance solutions can help to identify potential security breaches, support preliminary system screening, and perform risk assessments. If a system is compromised, it can be helpful to resolve the IT security incident by having a proper log management system in place and past SIEM activities as part of a compliance management system.

An organization must implement a well-defined log management system along with their overall IT security compliance management solution. The log management system can provide flexible analysis capabilities that you can use to identify threats, better understand future trends, and provide storage for gathered evidence.

1.2 Business drivers for IT security compliance management

While the traditional factors of production are defined as natural resources, capital goods, and labor, today's economy relies on information as a fourth factor of production. Because of the large amount, frequent update, and fast aging of information, most businesses today rely heavily on their information technology to better use information. Information has become so critical that damage incurred to this information can force an organization out of business, for example by reduced availability caused by downtime of systems processing this information. The protection of information and the technology that is used to process it has become essential, and many organization's compliance management focus, to a significant extent, is on the compliance of underlying information technology.

Compliance management today is driven by multiple initiatives:

► Compliance towards commercial laws and industry regulation

Compliance management can be *externally driven* to keep up with the changing global regulatory and business environment, which requires on-going audit capabilities. Regulations, which translate into security control requirements, are:

- Data privacy laws: Applicable for any organization that deals with personally identifiable information
- Basel II: For organizations that provide financial services
- HIPAA: For organizations that are involved in activities with potential impact to public health and hygiene
- PCI DSS: For organizations that process credit card information

As outlined in 1.1, "Introduction to IT security compliance management" on page 4, there might be more regulations that you must adhere to.

► Compliance to objected performance and efficiency targets

Compliance management can be *internally driven* by the intent for organizations to stay in business and to be profitable. Driven by the fact that compliance requirements must be fulfilled to meet legal and regulatory obligations, companies want to maximize the benefits of compliance management by also using the process to identify not only risks, but also opportunities to increase efficiency, which can ultimately lead to competitive advantage.

Customer compliance responsibilities: Customers are responsible for ensuring their own compliance with various laws and regulations, such as those mentioned in the previous bulleted list. It is the customer's sole responsibility to obtain the advice of competent legal counsel regarding the identification and interpretation of any relevant laws that can affect the customer's business and any actions that the customer might need to take to comply with such laws. IBM does not provide legal, accounting, or auditing advice, or represent that its products or services ensure that the customer is in compliance with any law.

The trend to use compliance management beyond its initial purpose is reflected in several of the regulations, for example in Basel II, the excellence of risk management for IT systems, which is part of the operational risk complex, has an impact on the competitive advantage of banks. The level of excellence determines how much money a bank can use to provide credits to their customers and how much it has to keep in reserve to cover for risks, which affects the interest rates that a bank can offer its customers. So today, even the external regulation itself develops further from a basic approach of *compliance versus non-compliance* towards approaches in the area of *control versus non-compliance*, where compliance is the highest level of control possible.

Compliance versus Control: If you have ever been audited (or if you have audited someone), you probably know that there is a difference between being in compliance and being in control:

- ▶ When you are in *compliance*, all your systems and processes are operated and delivered according to the security policies and standards (and you have evidence for compliance).
- ▶ When you are in *control*, you know what is in compliance and what is not, you know why, and you have a plan of action (and you have evidence for control).

Now, which is more important? Being in control is more important because you can be in compliance by accident. Further, if you are compliant but not in control, chances are high that you will not stay compliant for very long.

If you are in control, you will end up being compliant eventually, or at least you will have it on record why you are not compliant.

In addition, if you are not compliant and not in control, gaining control must be your primary goal, which is why more and more often regulations shift from compliance to control objectives.

Most organizations do not stop after they meet the basic principles set out in their policies because they want to understand how efficiently this level of compliance was achieved or even exceeded. Customers also want to identify indicators about how stable and consistent the current compliance achievement is and whether the state of compliance can be maintained.

1.3 Business drivers for log management

The knowledge of *where* the assets of an organization are has become a major business concern in many industry segments. But also knowing *who* is working in the network or *what* network resources employees have access to drives the business to implement a log management system that tells who does what, where, and when.

Log management, therefore, is an integral part of an IT security compliance management system. For the period of retaining the logs, it is ensured that the necessary information is available and can be analyzed or interpreted to a level that can help management to better investigate security incidents or comply with external regulation or laws.

As outlined in 1.2, “Business drivers for IT security compliance management” on page 7, compliance is a key business driver today. Log management must be a part of every IT security compliance management solution, but it can also be implemented alone as an initial step towards a larger IT security compliance initiative. Many international standards and regulatory controls require logging to be enabled and implemented. Also, these logs must be analyzed periodically and stored for a specific period of time, depending on the particular standard or regulatory control.

1.4 Criteria of an IT security compliance management solution

While having IT security compliance management in place is generally a good security practice, there are several factors that influence if and how IT security compliance management is implemented in a specific environment. The main dimensions of IT security compliance management include:

- ▶ Selection of IT security controls

The intention to check technical IT security controls and IT security controls in processes and on the organizational level.

- ▶ Spot check versus duration check

Defines the intention to either check the IT security configuration of systems, of network devices, or of applications at any given point in time (or multiple points in time) or monitor the behavior over a period of time that might cause a non-compliant configuration (and might even prevent this result, if the behavior is analyzed early enough to counteract).

- ▶ Number of IT security controls

Defines which and how many IT security controls are checked. Do you only check IT security settings in configuration files, or do you check log entries too? Do you check only operating system level controls or are application level controls checked also? Which operating systems, middleware, and business applications need to be supported?

- ▶ Frequency of checks

Defines how often an IT security compliance check is performed. This frequency does not only define how often the configuration settings are collected from the environment but also the frequency in which system administrators are called upon to fix or investigate identified deviations.

- ▶ Follow up time frame

Defines how fast reported deviations must be fixed.

- ▶ Scope of IT security compliance checking

Defines which business processes and their supporting IT systems are required to be checked for compliance and what level of control is required for these IT systems. Because security is always concerned about the weakest link, related infrastructure systems must be included too.

- ▶ Level and depth of reporting

Concerned with organizations having to fulfill obligated external reporting requirements and individual reporting to fulfill needs that are inside of the organization, for example, towards the board of directors, internal accounting, the security operations management, or even towards specific compliance-related projects. The reporting can differ in detail and range from reporting technical details to highly-aggregated business level reporting. Also, the reporting can be discrete, for example, on a predefined time frame or continuous (despite the checks still being performed non-continuously). The latter is often referred to as *dashboard*.

- ▶ Level of automation

Concerned with an IT security compliance management solution that relies on automated checks, which requires higher investments in technology or on manual checks, which requires more human effort and skills or a combination of both. Also, the level of automation can be limited by technological

limitations, for example, compliance tools that do not support every system, that must be checked for compliance, or the system itself not providing enough functionality to provide information about its compliance.

These key dimensions can be derived by considering the following secondary factors:

- ▶ Business environment of the organization

Is corporate espionage or other business crime an issue? Does the organization use outsourcing services? How dependent is the business on its IT systems?

- ▶ Regulatory and legal obligations

In which industry is the business operating? In which countries is the business operating? Which laws and regulatory requirements exist in each country for this industry with influence on information security? What level of scrutiny is executed by the regulators?

Note: It is useful to keep in mind that an IT security compliance management system can provide a lot of evidence about the level of executive control.

- ▶ Organizational complexity

The size and setup of the organization influences the speed of the reaction to deviations from the desired security level. Further, it has a significant impact on the requirements on an IT security compliance management solution, such as the administration approach.

- ▶ Technological complexity

Obviously, the existing IT environment defines the scope of the operating system, middleware, and business applications that must be supported by any IT security compliance management solution. Also, the level of standardization, centralization, and consolidation has significant influence on the IT security compliance management solution.

- ▶ IT security policy framework maturity

Mature organizations create and shape security policies, standards, work practices, and procedures from the policy level, for example, this enables them to define general security control requirements at the standards level, which can provide platform-specific security settings to meet the security control requirements on any given platform. A mature policy framework like this can also help implement the standards and guide in situations where the standard cannot be applied because of specific technical requirements of a given system.

1.5 Recent challenges for IT security compliance management

Even if the goal for IT security compliance is clear and defined by precise policies and standards, the task of IT security compliance management for a larger number of systems bears the following major challenges in addition to the requirements that result from the factors that we already discussed:

- ▶ Maintenance of compliance over time

Even in a stable environment systems are constantly changed because patches must be applied, updates must be installed, or additional packages require a change in configuration of the underlying operating environment. Also, the ever increasing requirements of regulations require companies to keep up with these changes to retain compliance.

- ▶ Complexity of the environment

Few businesses can claim that their environment is homogenous and centralized. Heterogeneous, geographically distributed systems in large numbers is the norm, with not only systems from multiple vendors, but also running several versions of operating systems simultaneously. Complexity is growing and today's more complex applications and moves toward *service-oriented architectures* (SOA) takes operations management to new levels of complexity.

- ▶ Complexity of the IT security compliance criteria

Checking the IT security controls of managed systems ensures that a system does not degrade in its IT security controls posture because of changes on the system after it is installed. Let us take, for example, changes made in conjunction with resolving a problem, during installing or upgrading a new application or middleware, or due to an attacker changing the configuration to hide his tracks or to compromise the system.

- ▶ Performance efficiency and cost pressure

Organizations always try to do more with less. Because IT security compliance is a matter of quality, there is a requirement for IT security compliance to be delivered for less cost. Because labor costs are considered one of the major operation expenses for organizations, the aim is to automate IT security compliance management as much as possible.

- ▶ Cloud computing and compliance²

Processing data in a cloud-based IT environment does have its advantages. However, managing IT security compliance to adhere to policies, regulations, and laws might not be a simple task. These policies, regulations, and laws often assume that everything is controlled within predefined borders—mostly

represented by the network boundaries of an organization. These boundaries can be extended to an external partner of the organization who then gets audited through, for example, SAS70³ reviews.

Organizations require visibility into the security posture of their cloud environment, which includes broad-based visibility into change, image, and incident management, and incident reporting for tenants and tenant-specific log and audit data. Visibility can be especially critical for compliance. Many regulators or European privacy laws require comprehensive auditing capabilities. Because public clouds are by definition a *black box* to the subscriber, potential cloud subscribers might not be able to demonstrate compliance. (A private or hybrid cloud, on the other hand, can be configured to meet those requirements.) In addition, providers sometimes are required to support third-party audits, and their clients can be directed to support forensic investigations when a breach is suspected, which adds even more importance to maintaining proper visibility into the cloud.

Organizations want to evolve from the traditional compliance checking, which focuses on collecting the compliance status information at a given point in time, towards controlling the non-compliant events at any point in time:

- ▶ Organizations want to be able to react on indicators that suggest a future status of non-compliance.
- ▶ Organizations want to identify what causes a status of non-compliance to avoid it in the future.

To achieve both, organizations want to extend the scope of compliance, checking from technical configurations of the operating environment towards the behavior of actors in this environment, including or even especially the users and administrators. It is not the IT systems that choose to become non-compliant over time; instead, it is the actions of people on and to IT systems that can cause non-compliance accidentally or on purpose.

Shifting the focus from resulting status to evoking pro behavior puts the focus closer to the root cause.

² Also refer to the Redpaper™ *Cloud Security Guidance: IBM Recommendations for the Implementation of Cloud Security*, REDP-4614. There is also a Whitepaper about Cloud Security from IBM with the title *IBM Point of View: Security and Cloud Computing*, published November 2009. In addition to that, the following hyperlink gives a lot of information about cloud computing: <http://www.ibm.com/ibm/cloud/>

³ Statement on Auditing Standards (SAS) No. 70 is an auditing standard developed by the American Institute of Certified Public Accountants (AICPA). For more information about AICPA, refer to <http://www.aicpa.org>. For a more detailed explanation of the SAS70 standard, refer to <http://www.sas70.com>.

1.6 Conclusion

As a result of the influencing factors that we discussed here, a security compliance management solution must provide a flexible yet comprehensive framework that can be configured and customized to the specific organization in question and takes a holistic approach on collecting and controlling the information security compliance of an organization. Such business requirements for compliance management set the boundaries for functional and operational requirements of a technical compliance management solution.

The increased pressure on organizations to demonstrate better control and compliance and the ever-increasing complexity of the business and the technical environment demands integrated and automated solutions for compliance management to prevent the organization spending more time for managing compliance than for its primary objectives.

In the remainder of this book, we discuss the implementation of such an automated solution based on the IBM Tivoli Security Information and Event Manager and other supporting technologies and products.



Designing an IT security compliance management solution

An *architecture* is designed to be strategic and is meant to have a longer life than a blue print, design specification, topological map, or configuration. If an architecture is too specific, it becomes constrained by current circumstances. If it is too broad or general, it cannot provide direction and guidance. An architecture assists in making decisions that are related to the identification, selection, acquisition, design, implementation, deployment, and operation of security elements in an organization's environment.

An architecture also must support many communities and represent the long-term view of a technical direction. IT security compliance architectures, in particular, must allow for multiple implementations depending on the *realities of the moment*. An organization must exercise caution to prevent the IT security compliance architecture from becoming a blueprint for a specific implementation.

In this chapter, we describe a framework for providing IT security compliance functionality throughout the organization. An IT security compliance architecture must be flexible and open to deal with the changing environment that an organization might face in the future.

The primary factors that require a modification to an architecture are:

- ▶ A change to the requirements in the regulatory environment on which the organization operates.
- ▶ A change to the requirements of the organizational and process environment.
- ▶ A change to the technology environment requirements.

We describe these points intentionally in this order. Although all three issues can arise independently, either internally or externally, a change to the regulatory requirements can always have an impact on organizational and process requirements and the technology environment.

To adapt to changing environments, a security compliance architecture must focus on *event sources* of compliance information, such as collection points (databases), data processing, and reporting, as well as to consider various event types, such as settings, people events, and network events.

2.1 Security Information and Event Management architecture

Security Information and Event Management, abbreviated as *SIEM*, helps an organization to gather security data from many divergent information systems. The volume of security log data is growing over time with more and more systems being connected to an organization's infrastructure. Having all this information in a centralized storage helps an organization to better analyze the data and respond to auditors' requests during reviews and audits.

Many organizations are struggling with three major problems that they cannot completely, or even partially, fulfill:

- ▶ Demonstrating compliance to regulatory requirements.
- ▶ Ensuring appropriate protection of intellectual capital and privacy information.
- ▶ Managing security operations securely and effectively.

An SIEM system can collect data from log files and alerts from a variety of infrastructure components, such as firewalls, routers, anti-virus systems, servers, and many others. It can inform IT teams about unusual behavior on these systems, and then these teams can decide whether and what kind of further investigation to take.

An SIEM architecture can be broken down into two elements:

► Security Information Management (SIM)

The SIM component provides reporting and analysis of data primarily from host systems and applications and secondarily from security devices to support regulatory compliance initiatives, internal threat management, and security policy compliance management. It can be used to support the activities of the IT security, internal audit, and compliance organizations.

► Security Event Management (SEM)

The SEM component improves security incident response capabilities. It processes near-real-time data from security devices, network devices, and systems to provide near-real-time event management for security operations. It helps IT security operations personnel be more effective in responding to external and internal threats.

An SIEM solution must provide log data capturing capabilities. Aggregated information must be securely stored. Also, archived data faces the requirement of having to reside in a database format that allows for accurate and expedient reporting and viewing capabilities.

Market definition and description:

The SIEM market is driven by customer needs to analyze security event data in real time (for threat management, primarily focused on network events) and to analyze and report on log data (for security policy compliance monitoring, primarily focused on host and application events).

SIM provides reporting and analysis of data primarily from host systems and applications and secondarily from security devices to support security policy compliance management, internal threat management, and regulatory compliance initiatives. SIM supports the monitoring and incident management activities of the IT security organization, and supports the reporting needs of the internal audit and compliance organizations.

SEM improves security incident response capabilities. SEM processes near real-time data from security devices, network devices, and systems to provide near real-time event management for security operations. SEM helps IT security operations personnel be more effective in responding to external and internal threats.

Now let us extend the SIEM definition and the approach that IBM took.

The SIEM realm is defined as the interaction between the offering of, and need for a software product that can:

- ▶ Collect and archive log data in a reliable manner for regulatory compliance.
- ▶ Analyze and report on archived log data for regulatory compliance.
- ▶ Analyze event information in real time for threat management.

The SIEM realm typically discriminates between two sets of functionality. The first two items define the capabilities that are required for the SIM segment offering. The last item defines the capabilities required that are offered in the SEM segment of the market.

To fully utilize the capability of both SIM and SEM you also need a strong supporting security *log management* function. The SEM solution can process the collected log data as soon as it is archived. Ideally the log data collection and archiving happens when the log data is generated by the source systems.

For our purposes and in alignment with how market analysts describe SIEM (see the Market Definition introduced in 2.1, “Security Information and Event Management architecture” on page 16), we refer to the combination of these capabilities (SIM and SEM) as an *SIEM solution*.

Figure 2-1 on page 19 depicts a typical SIEM architecture.

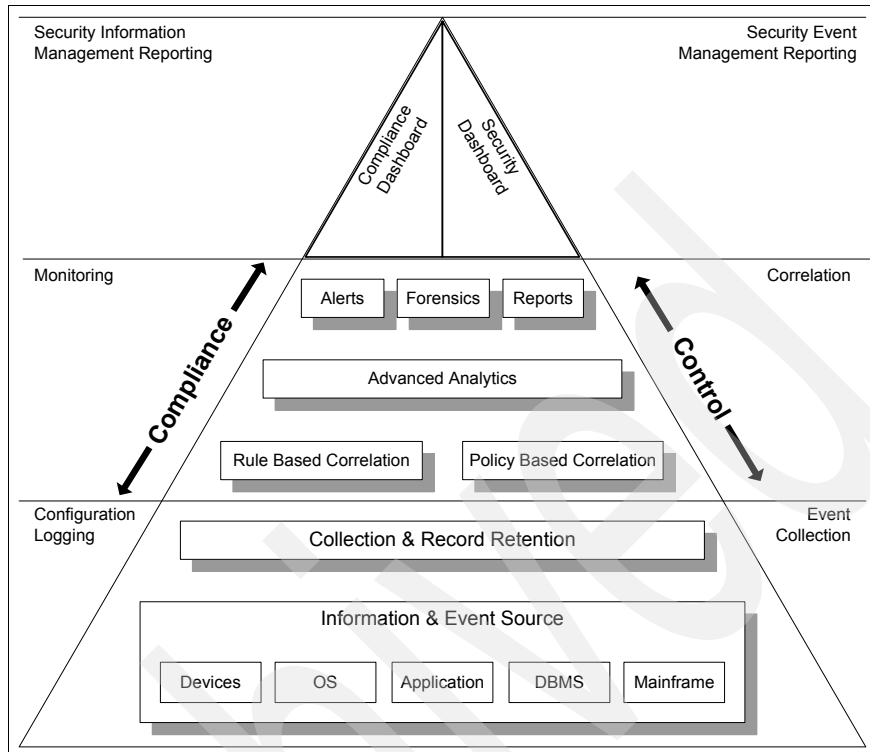


Figure 2-1 The SIEM architecture

The bottom third of Figure 2-1 shows the basic event collection and record retention capabilities. This retained data is then used for monitoring and correlation tasks (middle of Figure 2-1). The top third of the figure shows that the analyzed data can be reported in either security information driven or security event driven reports. You can find more details about SIEM architecture in 3.2, “The IBM SIEM architecture” on page 36. In Gartner’s research paper *Magic Quadrant for Security Information and Event Management, 1Q07*, there is an industry-wide standard definition of SIEM.¹

SIEM provides more effective security management and compliance with regulatory requirements. We do not address side effects, such as rapid return of investment and ongoing savings on equipment and manpower, but these benefits are also valid business reasons to implement an SIEM architecture.

¹ *Magic Quadrant for Security Information and Event management, 1Q07*, 9 May 2007, ID number G00147559.

2.1.1 Event types

Generally, there are four event types that must be monitored to be and stay fully compliant.

- ▶ Settings, policies, and standards
- ▶ People-related events
- ▶ Device-related and network-related events
- ▶ Asset-related events

Examples of events that are logged include, but are not limited, to:

- ▶ All successful and failed sign-on attempts.
- ▶ All successful and failed attempts to access sensitive resources.
- ▶ Rejected access attempts to all resources.
- ▶ Use of privileged user-IDs.
- ▶ User-IDs with system privileges allocated.
- ▶ All changes in the access control system that are carried out by an administrator.
- ▶ All access attempts to databases storing definitions, passwords, and so on that belong to the access control system.

Settings, policies, and standards

Every organization must provide documentation to its employees that clearly states the guidelines about how to use the organization's IT systems. This documentation is usually referred to as the *Information Security Policy*. It can also communicate to the employees what is prohibited and which mandatory processes are to be followed. There is a variety of interpretations of policies, standards, procedures (working instructions), or guidelines. In this book, we concentrate on *policies* and *standards*.

Security policies are defined by the executive board and provide a clearly stated security direction for the overall organization. They can also be named the *security constitution*.

Security standards are the next level of security rules adherence. Security standards are metrics that define allowable boundaries. A standard must provide sufficient parameters that a procedure or guideline can unambiguously be met.

Standards, in comparison to policies, change if requirements or technologies change. Policies remain static. There might be multiple standards for one policy. You can find more discussion on this topic in 1.1, "Introduction to IT security

compliance management” on page 4 and in Appendix A, “Corporate policy and standards” on page 403.

A good example of a standard is password rules. This standard documents the allowed minimum password length, the maximum password age, or whether a new user must change a password after the first access.

When talking about standards, security compliance in larger organizations cannot be maintained manually. How can this be accomplished for hundreds or even thousands of IT systems with multiple operating environments, database servers, Internet-facing systems, and more? IBM Tivoli Security Compliance Manager helps you to check security compliance automatically. For more details refer to 3.1.1.3, “IBM Tivoli Security Compliance Manager” on page 30.

People-related events

IT security compliance can only be accomplished if the people working within the IT environment adhere to the policies. Organizations must identify roles and responsibilities within the environment and define *who* uses *what* resources, and *how* they use the resources. Another defining parameter must specify *what activities* are performed within the IT environment. These roles can vary from privileged administrative tasks, database administration, or just accessing a specific file on a file share. There must be defined roles and responsibilities documented within the IT environment.

Why is user-related behavior such an issue? Almost every publicly provided analysis about internal incidents shows that most of the problems are caused by the technically savvy or privileged users of an organization. The numbers vary from 70% to 90%, showing that the highest risk comes from inside of an organization. Many of these incidents are inadvertent violations of a change management process or acceptable use policy. However, there are also incidents that are deliberate due to revenge or negative events, such as demotions or mergers.

Regardless of the why, the issue is too costly to ignore. Experts, analysts, auditors, and regulators are imploring organizations to start monitoring for this threat.

Device-related and network-related events

You must have a complete overview of your current IT environment that both the assets and users operate in. In this context, we talk about the technology environment on which the solution is implemented. You must consider the type of devices that people work with, and you have to ensure that these devices are compliant in accordance with enterprise policies.

Event data from various network security devices are required and then must be normalized, filtered, and transmitted to a centralized management system.

Asset-related events

An organization must continuously monitor access to high-value databases by privileged users, such as administrators, outsourced personnel, but also unauthorized users. To stay in control, these databases:

- ▶ Must be protected against fraud
- ▶ Enforce change controls
- ▶ Identify database vulnerabilities

The IT security compliance management solution must also streamline the compliance processes with centralized and automated controls for database management platforms. These automated controls must include the ability to trace all database activities to the real application user.

2.2 Solution architecture

In this section, we discuss the solution architecture for SIEM. Basically, there are three steps:

1. Projection of an IT security compliance solution
2. Definition of an IT security compliance solution
3. Design of an IT security compliance solution

2.2.1 Projection of an IT security compliance solution

Most projects involve business tasks, such as cost-benefit analysis and budgeting, project management tasks, such as scheduling, resource allocation and risk management, and technical tasks, such as design, build, test, and deploy. The projects are also driven by business requirements, which we explained in 1.2, “Business drivers for IT security compliance management” on page 7 and in 1.3, “Business drivers for log management” on page 9. We restrict our discussion to the technical tasks that are associated with the production of the architecture and design document. For redundancy reasons, we do not explain the project phases in this section. Refer to our detailed explanation of the multiple project phases for deploying a security compliance solution in our scenario in Chapter 5, “Compliance management solution design” on page 89.

2.2.2 Definition of an IT security compliance solution

The project definition and planning phase documents the project in detailed steps. It involves the following tasks:

1. Analyze the existing environment.
2. Describe the problem at hand.
3. Document the detailed requirements for the solution.

The initial project definition is based on the documentation that triggered the project, such as the IT architecture, security architecture, and request for proposal (RFP) or equivalent. All of these documents identify the business background and the business needs for the solution and document the business and technical requirements for the solution. For a security compliance solution, the following (unordered) areas must be defined in this phase:

▶ Regulatory requirements

What are the regulatory requirements that the organization must adhere to? For example, is the enterprise listed at the New York Stock Exchange (NYSE)? If that is the case, it must be compliant to the Sarbanes-Oxley Act (SOX). Other regulatory requirements apply depending on the industry in which the organization is operating, such as compliance to PCI DSS, HIPAA, or FDA, just to name a few.

▶ Security policies

What does the corporate security policy define for users, accounts, passwords, access control, and so on? It is important to follow the organization's security policies because they ensure the correct handling of IT resources. They are the foundation of information security within an organization.

▶ Monitored environment

- Target users: Who are the users who must be monitored? Examples are privileged users, database administrators, executives, and so on.
- Target systems: What are the components in your system environment that must be monitored? Examples include operating systems, databases, applications, the network, firewalls, physical locations, and so on.

▶ Reports

To demonstrate continuous evidence of compliance, it is mandatory to show compliance reports.

▶ Processes

Although we focus purely on designing a security compliance solution, the outcome of designing such a solution does not only result in a technical toolset and an infrastructure that must be implemented. To create a

comprehensive solution, we must develop supporting processes and put those processes into production, such as:

- Patch management process
- User identity revalidation process
- Problem and change management process
- Incident management process

There are many more processes that can be added to this list. Basically, for every IT related task, you need a process in place.

2.2.3 Design of an IT security compliance solution

The design of a security compliance solution is a schematic diagram that represents the governing ideas and candidate building blocks of the architecture. It provides an overview of the main conceptual elements and relationships in the architecture.

The main purpose of the design is communication. Thus, it is more important for the design diagram to be simple, brief, clear, and understandable rather than comprehensive or accurate in all details. Consequently, the diagram uses an informal rich picture notation. It typically includes supporting text that explains the main concepts of the architecture. This type of diagram can be produced at differing levels (in accordance to what we address in Chapter 1, “Business context for IT security compliance management” on page 3):

► At the organizational level

At an *organizational level*, a design diagram is often produced as part of an overall IT strategy. In this instance, it describes the vision of the business and IT capabilities that are required by an organization. It provides an overview of the main conceptual elements and relationships including data stores, users, external systems, and a definition of the key characteristics and requirements.

At an *organizational level*, a design diagram is often produced as part of an overall IT strategy. In this instance, it describes the vision of the business and IT capabilities that are required by an organization. It provides an overview of the main conceptual elements and relationships, which includes data stores, users, external systems, and a definition of the key characteristics and requirements.

► At the system level

At a *system level*, the design diagram is produced very early in a project and influences the initial component model and operational model. It is not intended that design commitments be based on this overview until the (more formal) component model and operational model are developed and validated.

- ▶ At the process level

The last level is the *process level*. This document most likely is not ready before the solution is deployed. Only after deployment is it possible to identify, develop, and implement the processes that are needed to become and stay in control of the security compliance solution.

Subsequently, the component model and operational model are the primary models, and the design diagram is a derivable view, which is revised if there are changes to the main concepts and relationships.

Chapter 5, “Compliance management solution design” on page 89 describes the design of a security management solution in depth.

2.3 Conclusion

In this chapter, we shed light into the necessary steps to plan an IT security compliance management solution. After we investigated several compliance-related event types that must be collected, we described a general solution architecture.

In the next chapter, we introduce the IBM Tivoli Security Information and Event Manager logical and physical component structure and discuss several deployment options.

Archived



Introducing the IBM Security Information and Event Management solution

In this chapter, we introduce the IBM Security Information and Event solution to meet the overall SIEM requirements, as we discussed in 2.1, “Security Information and Event Management architecture” on page 16.

The SIM part of the requirement can be completely covered by the IBM Tivoli Security Information and Event Manager and IBM Guardium. The SEM part is covered by IBM Security SiteProtector¹, IBM Tivoli Security Operations Manager, and IBM Tivoli Security Compliance Manager. In this chapter, we provide a functional overview of these products, and we spend more time on the details around Tivoli Security Information and Event Manager v2.0. We also provide more details about the Tivoli Security Operations Manager product and its relationship to Tivoli Security Information and Event Manager.

¹ Formerly IBM Proventia® Management SiteProtector

3.1 Introducing the IBM SIEM solution

The IBM SIEM solution addresses the characteristics of an SIEM solution.

The IBM SIEM solution offers the following products:

- ▶ IBM Security SiteProtector
- ▶ IBM Guardium
- ▶ IBM Tivoli Security Compliance Manager
- ▶ IBM Tivoli Security Operations Manager
- ▶ IBM Tivoli Security Information and Event Manager

IBM Security SiteProtector and Tivoli Security Operations Manager cover real-time threat management requirements. We look closer into Tivoli Security Operations Manager in the following sections. To learn more about IBM Security SiteProtector, review the IBM Redbooks deliverable *Enterprise Security Architecture using IBM ISS Security Solutions*, SG24-7581. IBM Guardium² is an SIEM tool for databases that can support real-time threat mitigation and prevention in combination with database auditing and log data archiving. It can support real-time database protection, vulnerability and configuration assessment, and database monitoring and auditing.

3.1.1 IBM Security SiteProtector

IBM Security SiteProtector can help alleviate the complex burden and high costs that are associated with security management through comprehensive, centralized control of an organization's various network security components. This unique capability can enable companies to achieve more effective security, cut costs significantly, maximize business uptime and continuity, and maintain regulatory compliance standards.

IBM Security SiteProtector centrally manages the broadest array of technical security controls, thereby unifying management of network, server, and desktop protection. This central management can enable organizations to control, monitor, analyze, and report on their enterprise security posture from a central console with minimal staff resources.

Although no one technology can demonstrate comprehensive compliance, IBM Security SiteProtector facilitates enterprise compliance efforts by documenting security processes and keeping organizations ahead of the rising standard of due care.

² For more information about IBM Guardium, visit:

<http://www-304.ibm.com/jct09002c/gsdod/solutiondetails.do?solution=28088&expand=true&lc=en>

IBM Security SiteProtector can perform four basic functions:

- ▶ *Manage* security environment and asset data:
 - Perform consolidation of security agents
 - Integrate with existing IT framework
 - Help in mitigation of risk
 - Remediate assets and vulnerabilities
- ▶ *Monitor* the core assets and the network:
 - Help in detecting threats
 - Help in conducting forensics
 - Help in ensuring uptime.
- ▶ *Measure* compliance with policies and standards that the organization set as its goals.
- ▶ Provide a single point of real-time *command and control*.

3.1.2 IBM Guardium

IBM Guardium can provide a robust solution for safeguarding your entire application and database infrastructure, which includes:

- ▶ Real-time *database activity monitoring* (DAM) to proactively identify unauthorized or suspicious activities.
- ▶ Auditing and compliance solutions for simplifying SOX, PCI DSS, and data privacy processes.
- ▶ Change control solutions for preventing unauthorized changes to database structures, data values, privileges, and configurations.
- ▶ Vulnerability management solutions for identifying and resolving vulnerabilities.
- ▶ Database leak prevention for locating sensitive data and thwarting data center breaches.

IBM Guardium provides the most widely-used solution for ensuring the integrity of corporate information and preventing information leaks from the data center.

The enterprise security platform can prevent unauthorized or suspicious activities by privileged insiders, potential hackers, and end-users of enterprise applications, such as Oracle EBS, PeopleSoft, SAP, Business Intelligence, and other in-house systems.

At the same time, the solution optimizes operational efficiency with a scalable, multi-tier architecture that can automate and centralize compliance controls across the entire application and database infrastructure. Figure 3-1 on page 30

shows the IBM Guardium functionality that support part of our complete SIEM requirements.



Figure 3-1 IBM Guardium SIEM requirements coverage

3.1.3 IBM Tivoli Security Compliance Manager

Tivoli Security Compliance Manager is a centralized repository for archiving native audit trails to observe and to report on security compliance policies. Tivoli Security Compliance Manager deploys predefined policies onto managed systems and provides a central repository for automated reporting purposes and data mining.

The architecture of the Tivoli Security Compliance Manager is based on a client/server model. The Tivoli Security Compliance Manager client acts as an agent that collects data from the client subsystem on a predefined schedule or on request of the Tivoli Security Compliance Manager server. After the client collects the data, it is sent to the server.

Let us take a look at the activities that the server and client perform:

- ▶ Tivoli Security Compliance Manager server
 - Tivoli Security Compliance Manager provides an interface for defining policies that specify the conditions that must exist on a client. On the Tivoli Security Compliance Manager server, you schedule when the security compliance data is collected on the clients and which clients collect what kind of data.

- The Tivoli Security Compliance Manager server stores the security compliance data that is received from the clients in a central database and provides the available data to users through an administration console and administration commands.
- The server provides security violation details as a basis for compliance reporting.
- ▶ Tivoli Security Compliance Manager client
The client collects information about its environment that is required to assess compliance with the security policy at a predefined schedule using several collectors. This data is sent back to the Tivoli Security Compliance Manager server.

You can find more information about Tivoli Security Compliance Manager in *Deployment Guide Series: IBM Tivoli Security Compliance Manager, SG24-6450* and *Building a Network Access Control Solution with IBM Tivoli and Cisco Systems, SG24-6678*.

The Tivoli Security Information and Event Manager and the Tivoli Security Compliance Manager are complementary tools that can provide an overall view of IT systems compliance. Tivoli Security Information and Event Manager collects audit trail data and real-time events and reports user behavior and user threats against an acceptable use policy. It is an event audit product.

The Tivoli Security Compliance Manager collects system configuration data and reports on systems' compliance against a security policy. It is a status audit product.

3.1.4 IBM Tivoli Security Operations Manager

Network and IT resource availability is absolutely critical to business and service assurance. Organizations, federal agencies, and service providers can lose millions of dollars per year as a result of worms, trojans, and other types of malware that bring down corporate resources and organization-facing services.

The Tivoli Security Operations Manager is an SIEM platform that is designed to improve the effectiveness, efficiency, and visibility of security operations and information risk management. Tivoli Security Operations Manager can enable the enterprise to automate the following tasks:

- ▶ Log aggregation, correlation, and analysis
- ▶ Recognition, investigation, and response to incidents
- ▶ Incident tracking and handling
- ▶ Monitoring and enforcement of policy
- ▶ Comprehensive reporting for compliance efforts

Tivoli Security Operations Manager automates many repetitive and time-intensive activities that are required for effective security operations.

Data mining, historical reporting, self-auditing, and tracking capabilities provide critical information for understanding security trends. Tivoli Security Operations Manager supplies standard and customizable report templates, an automated report scheduler, and export functionality of all graphs and charts. It draws on information that is stored in a security event database to deliver historical reporting and trending on demand.

The event collectors can send data to a single central management server, or an organization can use multiple servers to maximize availability.

Tivoli Security Operations Manager can also be used as a *managed security services* (MSS) platform. It can help the MSS provider to reduce operational costs by offering a high degree of automation. In addition, it can demonstrate service levels and value to organizations through its comprehensive reporting capabilities.

It centralizes and stores security data from throughout the IT infrastructure to improve security operations and information risk management. It provides automated log aggregation, correlation, and analysis as well as recognition, investigation, and response to IT security incidents.

Tivoli Security Operations Manager succeeds the IBM Tivoli Risk Manager product, which is discontinued to be provided by IBM.

For more information about Tivoli Security Operations Manager, refer to the IBM Redbooks publications *Deployment Guide Series: IBM Tivoli Security Operations Manager 4.1*, SG24-7439 and *Enterprise Security Architecture Using IBM Tivoli Security Solutions*, SG24-6014.

Tivoli Security Information and Event Manager and Tivoli Security Operations Manager are complementary tools to provide a view of real-time external threats, network-based threats, user behavior, and insider threat across applications, databases, and operating systems. Tivoli Security Operations Manager collects and analyzes information in real-time from security devices across the network. Through advanced correlation capabilities, Tivoli Security Operations Manager can identify and prioritize security incidents and enables your organization to respond to these external threat incidents automatically. Tivoli Security Information and Event Manager leverages the resulting information to present a comprehensive enterprise-wide view of the compliance, audit, and insider threat integrated with real-time external security threat identification.

The Tivoli Security Operations Manager is not part of Tivoli Security Information and Event Manager V2.0. Tivoli Security Operations Manager continues to be

offered as a stand-alone product for organizations that specifically need to focus on external threat management.

3.1.5 IBM Tivoli Security Information and Event Manager

An SIM solution requires log management and audit functionality and must generate reports on collected log data that refers to security policies to identify policy violations.

In addition, the solution must offer real-time incident management, which can require using correlation rules to identify more details about the incident. Ideally, the solution must offer real-time mitigation for and alerting of incidents, but strictly speaking, this type of real-time functionality is typically addressed in an SEM realm.

A combination of the Tivoli Security Information and Event Manager and Tivoli Security Operations Manager products can meet all requirements in which Tivoli Security Operations Manager adds real-time incident management to the Tivoli Security Information and Event Manager solution. In addition, the Tivoli Security Information and Event Manager solution offers other capabilities that are often key decision factors for organizations that are looking for these types of technologies. Among these additional factors are:

- ▶ A rapid and scalable deployment and support process

The SIEM solution is modular and flexible and includes the capability to start an implementation small to address key aspects of SIEM requirements and then grow to encompass the complete SIEM requirements of an organization at a later time.

The SIEM implementation can start to address the log management functionality first and address the other SIEM functionality over time, in phases. Sometimes organizations that deploy SIEM solutions place emphasis in their evaluations on their vendor providing an appliance type solution.

IBM provides the flexibility of a rapidly deployable software solution that can be installed on the most appropriate hardware configuration to meet the log data collection, archiving and reporting requirements, and custom IT hardware requirements, such as brand, type, and configuration. The installation of a Tivoli Security Information and Event Manager solution can take less than an hour on the various hardware and operating system platforms that it supports; therefore, an organization can focus on the configuration activities that are more important during project implementation.

Typically, appliance-based solutions do not offer much flexibility, for example, for growth you only have the option of buying more appliances. With the Tivoli Security Information and Event Manager solution, you have options to

increase the amount of hardware or the capacity of the hardware that you have and to change the operating system platform to a more scalable approach.

- ▶ Reliable and secure log collection and archiving

Tivoli Security Information and Event Manager 2.0 offers the possibility to begin an SIEM implementation with log data collection and archiving only. Tivoli Security Information and Event Manager 2.0 can process up to 30,000 syslog messages or SNMP traps per second and archive these using a FIPS-certified communication protocol.

- ▶ Capability to collect and archive any type of log data

Today IT departments in many organizations must support business processes with customized software or with in-house developed software. Because these highly customized systems typically support essential business processes, their log data is subject to audit and analysis, to reduce the business risks or, at least, prove that these sensitive business processes are monitored continually. Custom built applications can be integrated with Tivoli Security Information and Event Manager to collect any type of log data and archive it using the FIPS certified communication layer.

- ▶ Integration with identity and access management solutions

Tivoli Security Information and Event Manager supports integration with a large amount of user directory types. The user and group/role/profile information that is maintained in these user directories can be applied to the security policy compliancy reports to show user behavior that does not follow the proper user's profile/role. These reports can be used for role life cycle management and to automate remediation of user directory configuration errors.

- ▶ Built-in best practice reporting and analysis of log data

Deployment of an SIEM tool can sometimes be delayed because there is no clear idea what reports can help to lower operational risks. Tivoli Security Information and Event Manager provides many existing reports that can help to monitor business processes following best practice recommendation for the IT audit field. These reports can help lower the operational risk that is related to use of privileged user accounts. These reports are available when Tivoli Security Information and Event Manager is deployed as an SIEM solution. In case Tivoli Security Information and Event Manager is deployed as a Log Management only solution, similar reports can be generated to search the log data for suspicious events.

- ▶ Pre-defined audit and regulatory compliance reports cover the following standards and regulations:
 - SOX
 - FISMA

- HIPAA
- PCI DSS
- BASEL II
- GLBA
- ISO 17991
- ISO 27001
- COBIT
- NERC

The reports that are needed to support the regulatory compliancy process are in some cases predefined and in other cases they rely on the implemented security controls in an organization. Tivoli Security Information and Event Manager provides built-in reports for regulations with specific requirements. For other, more flexible requirements, Tivoli Security Information and Event Manager uses the *ISO Code of Practice for Information Security Management* as the framework for reporting. When an organization decides they must comply with an IT-related regulation, they might not have defined the necessary security controls that are required for the monitoring and audit process yet. Tivoli Security Information and Event Manager can help the organization by providing a best practice starter set of reports. Gradually the organization can create and tune its own set of regulatory compliance reports that it can use to support the compliancy claim.

- ▶ Capability to normalize any type of log data for audit and regulatory compliancy processing

Collecting and archiving log data from software that is developed in-house is possible with Tivoli Security Information and Event Manager. But, most of the time, collecting and archiving this log data is not good enough because this log data can contain information that is crucial for effectively monitoring the sensitive business processes. Therefore, being able to compare this log data with business process rules, such as IT security policies, is essential. Tivoli Security Information and Event Manager provides a normalization library that allows organizations to create scripts that can normalize any type of log data into a database model. This data can then be used for reports to facilitate a comparison of the log data against the IT security policy and business process rules. Tivoli Security Information and Event Manager has built-in normalization scripts for over 300 various types of log data that are generated by well-known operating systems, databases, applications, data management systems, and network devices.

- ▶ IBM Mainframe integration

Amongst the well-known supported operating systems is IBM z/OS® for System z® servers. Tivoli Security Information and Event Manager covers a wide range of SMF types and subtypes, including SMF records that are generated by DB2® and CICS®, in addition to RACF® events. When a System z is used in an IT environment, this system probably manages

business critical data, and therefore, these systems are most likely audited and monitored.

- ▶ High performance syslog and SNMP collector

Many IT systems that support an overall IT infrastructure, such as routers and firewalls, historically do not have a sophisticated subsystem for auditing and monitoring. Operational logs that are generated by such systems are mostly stored on syslog-enabled host machines. The syslog protocol was originally designed for system maintenance messages and the protocol itself does not support a guaranteed message delivery mechanism. Environments where large amounts of syslog messages must be analyzed will therefore require a syslog-enabled host that can process high volumes of syslog messages. Tivoli Security Information and Event Manager uses a high performance syslog collector that can process 30,000 events per second. This system is not restricted to syslog messages but can also process SNMP traps at the same rate. The Tivoli Security Information and Event Manager syslog collector is software based and does not require dedicated hardware, which makes it very scalable.

- ▶ Real time event correlation and incident response functionality

Tivoli Security Information and Event Manager can process the collected and archived log data in near real time and perform basic event correlation to identify a possible security breach. Security incidents can trigger Tivoli Security Information and Event Manager alerts using SMTP, SNMP, or executables to process the security incident's information. If more extensive rule-based, real-time threat management is required, you can extend Tivoli Security Information and Event Manager with Tivoli Security Operations Manager.

Tivoli Security Operations Manager can provide security operations functions, including dashboard views that are suitable for an operations center, security incident management and service level reporting capabilities, and integration with leading ticketing systems. In addition, it can provide security operators with the ability to be greatly more effective by capturing their knowledge and incorporating it into threat and risk management practices and allowing automation and remediation.

3.2 The IBM SIEM architecture

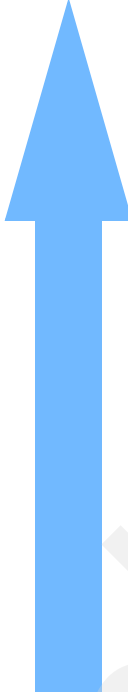
Best practice IT security standards and IT regulatory compliance require a highly sophisticated audit and monitoring process. Although many people in an organization still do not realize this process to be a critical component, the groups that are responsible for business processes understand that auditing and monitoring is required on every business level and for every business type.

With IT gaining more and more importance in various types of business environments, it is obvious that the footprint for IT auditing and monitoring is growing too. The reason why people do not see it as critical is because the additional processes typically do not increase efficiency and productivity of the business. The effects are not easily measured in terms of savings and increased efficiency simply because the added value of auditing and monitoring can be expressed in *reliability, trust, and prevention*. In the case of prevention, for example an insider threat, you can imagine that people who are constantly being audited and monitored develop a heightened awareness of being caught.

It is easy to explain to people that it is beneficiary to be warned when suspicious behavior is recognized and that it can be mitigated automatically, for example, a typical security measure, that is widely implemented, is to lock an account after someone repeatedly tries to logon without any success. Many people believe that these types of measures must be extended to include more complex suspicious behavior, such as advanced outsider attacks or unapproved IT security modifications. To implement these kinds of measures, more complex event correlation and automatic mitigation functionality is required. Ideally, threat mitigation must happen in real time because it can then prove that risk management is more effective simply because the real time process might prevent an identified vulnerability that is being exploited.

It is not a surprise that organizations look for event correlation and log management first before they understand that proper IT security best practices also require solid audit and monitoring to close the risk management process loop, which we can visualize, as shown in Table 3-1 on page 38.

Table 3-1 General SIEM requirements versus IBM SIEM solution

Increasing Value	SIEM Capability	IBM SIEM Capability
	Exception Reporting and Meeting compliance head on	<ul style="list-style-type: none"> ▶ Report when a privileged user is doing something suspicious ▶ Privileged user monitoring and audit reporting ▶ Reporting on compliance exceptions
	Alerting and Reacting to risk	<ul style="list-style-type: none"> ▶ Near real-time analytics ▶ Threshold alerting ▶ “Alert me when someone fails to logon multiple times to my Oracle application”
	Log Management and Checkbox compliance	<ul style="list-style-type: none"> ▶ Reliable, verifiable log management ▶ Log management reporting ▶ Collect original log data
	Threat Aware	<ul style="list-style-type: none"> ▶ Intrusion Detection and Intrusion Prevention Systems ▶ Appliance based ▶ Reacting to and protecting from threat

The IBM SIEM solution addresses:

- ▶ Log Management
- ▶ Compliance reporting, alerting, and basic event correlation

The Tivoli Security Information and Event Manager product covers the SIM requirements. It can be deployed to focus on Log Management only or to cover Log Management plus compliance reporting and alerting. In the next paragraphs, we look at these two configuration options from a functional point-of-view.

3.2.1 Log Management

The Tivoli Security Information and Event Manager Log Management solution provides the ability to collect log data in its original format using a FIPS-certified secure protocol. The original log data is stored in a secure, reliable, and verifiable way.

Verification of the log collection occurs on two levels in Tivoli Security Information and Event Manager 2.0:

- ▶ Verification of successful archiving
- ▶ Verification of log completeness

Regulatory compliancy requires that log data that is being collected and Tivoli Security Information and Event Manager Log Management produces reports to prove that the required log data was indeed archived successfully. Besides this proof, the Log Management component can also demonstrate that the archived log data is complete.

Figure 3-2 shows the Log Management Dashboard report that can help prove to auditors that the log data archiving process is effective and that the log data archive is complete, which means that the original log data is captured and was not tampered with after it was archived.

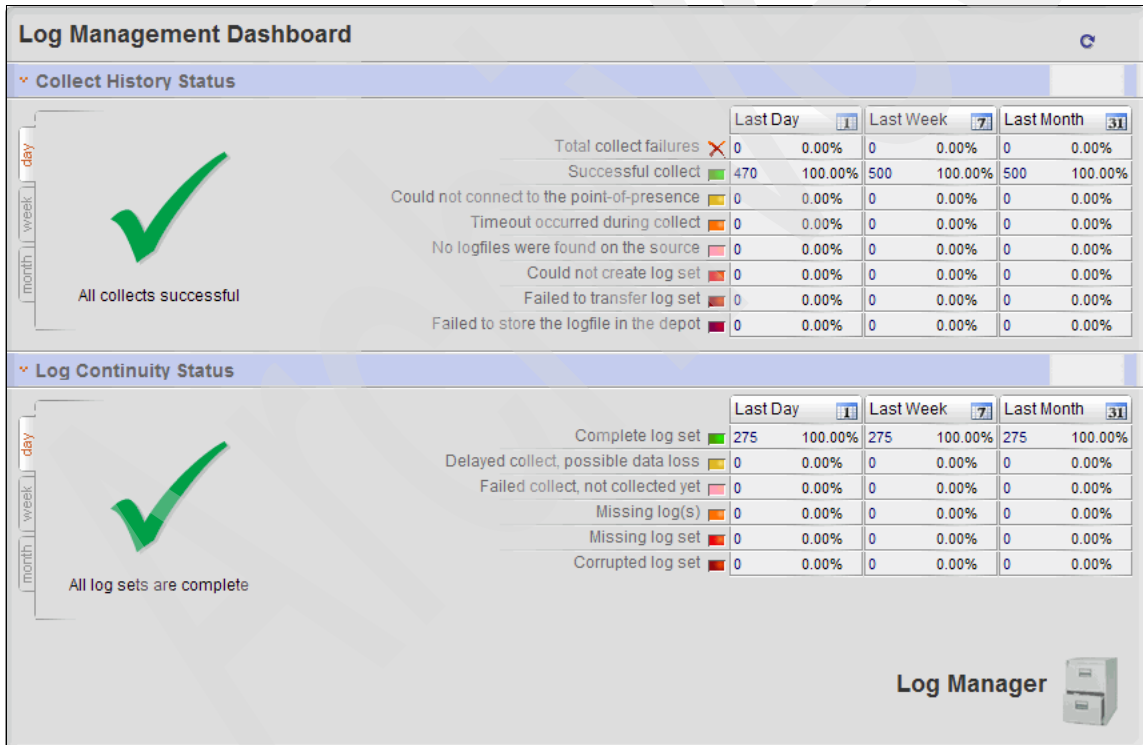


Figure 3-2 Log Management Dashboard

Integration with an IBM DR550 system storage device is possible for enhanced security and availability. You can find more information about the IBM DR550 in

the IBM Redbooks publication *IBM System Storage DR550 V4.5 Setup and Implementation*, SG24-7091.

Tivoli Security Information and Event Manager Log Management includes the capability to perform content searches across the entire Log Management Depot when it is important to find critical information in the raw logs. Original log data analysis is possible in two ways:

- ▶ Forensic search

The original log data can be analyzed by running user-defined search queries. Like in a SQL query, the user defines the search criteria and the filed types that must be displayed from the result set of log records. Figure 3-3 on page 41 shows an example of using the Tivoli Security Information and Event Manager forensic search tool.

Log Management Depot Investigation Tool

Query Builder

Step 1. Time Period

from: month: February | day: 26 | year: 1985 | till: month: February | day: 27 | year: 2010

Step 2. Event Source

Server	Point of presence	Audited machine	Event source type
tsiement01	NOTEXIST tsiement01	10.10.1.4 159.140.176.24 159.140.177.220 159.140.177.221 159.140.177.228 159.140.33.12 159.140.33.13 159.140.33.7 192.168.210.122	CheckPoint FireWall-I CheckPoint FireWall-I (OP Cisco PDX SNMP receiver Cisco PDX syslog receive Cisco Router SNMP rece Cisco VPN syslog receiv Generic ExtendIT HP-UX syslog receiver IBM ADX 5.1-6.1 audit tra

Step 3. Select Fieldnames

Refresh Fieldname List

Select All Fields

<input type="checkbox"/> #Fields__TABLENAME	<input type="checkbox"/> #record	<input type="checkbox"/> /SMF/ACCOUNT/COMPCODE
<input type="checkbox"/> /SMF/DIVOBJ/SUBTYPE	<input type="checkbox"/> /event/info	<input type="checkbox"/> /event/onwhat@name
<input type="checkbox"/> /event/onwhat@path	<input type="checkbox"/> /event/onwhat@type	<input type="checkbox"/> /event/outcome@reason
<input type="checkbox"/> /event/policy/description	<input type="checkbox"/> /event/policy/name	<input type="checkbox"/> /event/policy/type
<input type="checkbox"/> /event/starttime	<input type="checkbox"/> /event/stoptime	<input type="checkbox"/> /event/target/azn/perm
<input type="checkbox"/> /event/taroe/azn/qualifier	<input type="checkbox"/> /event/taroe/azn/result	<input type="checkbox"/> /event/what@noun

Step 4. Content Search

eventmainclass:Logon

Search Information

Search Summary

Audited machine	Event source	Event source type	Total records	Relevance

Figure 3-3 Tivoli Security Information and Event Manager forensic tool

► Best practice log analysis reports

Tivoli Security Information and Event Manager has the following built-in log analysis best practice reports that require minimal configuration:

- Chunk Continuity Report
- Detail Database Activity
- Detail Events by Type
- Detail Logon Failures by User
- Detail User Activity
- Summary Events by Type
- Summary Logon failures by User
- Summary User Activity

Use the Tivoli Security Information and Event Manager Portal and navigate to **Tivoli Security Information and Event Management** → **Log Management** → **Reports** → **Report Set**, as shown in Figure 3-4.

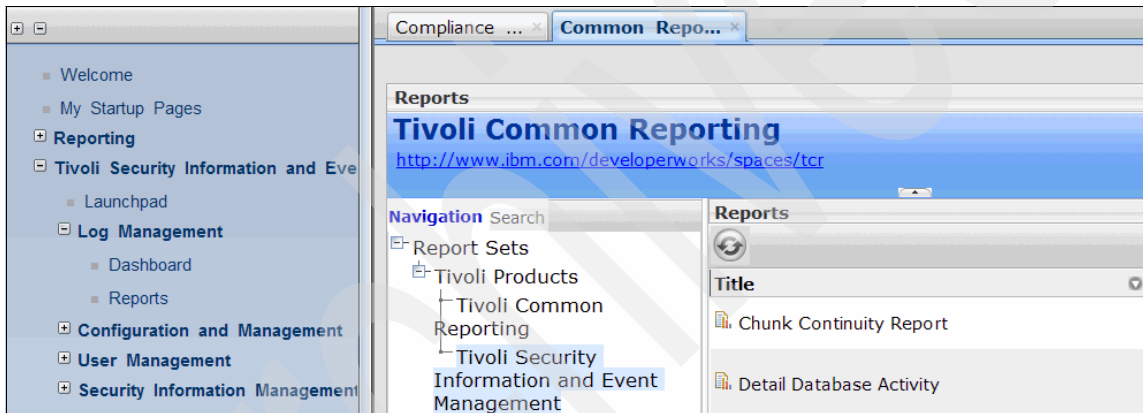


Figure 3-4 Best practice log analysis reports

The reports are implemented using the Tivoli Common Reporting framework.

The report examples in this section demonstrate that the Tivoli Security Information and Event Manager Log Management can make log data collection and archiving manageable. In addition, it can provide reports for log data analysis.

3.2.2 Compliance reporting, alerting, and basic event correlation

As suggested in 3.2.1, “Log Management” on page 38, the Tivoli Security Information and Event Manager Log Management component can be deployed separately, providing centralized log data archiving and log data analysis. If an organization needs to adhere to regulatory compliance or security policy

guidelines, a SIM module must be added to provide normalization of original log data. For a comprehensive deployment, Tivoli Security Information and Event Manager offers three types of servers:

- ▶ Log Manager Server

This server implements the base Log Management components and log analysis reports.

- ▶ Standard Server

This server provides base Log Management components and compliance reporting.

- ▶ Enterprise Server

This server provides base Log Management components, compliance reporting, and log analysis reporting.

Tivoli Security Information and Event Manager compliance reporting requires that the log data is normalized. Both a Standard and Enterprise Server can be used to normalize the log data. This normalization process is depicted in Figure 3-5 (using the Standard Server as an example).

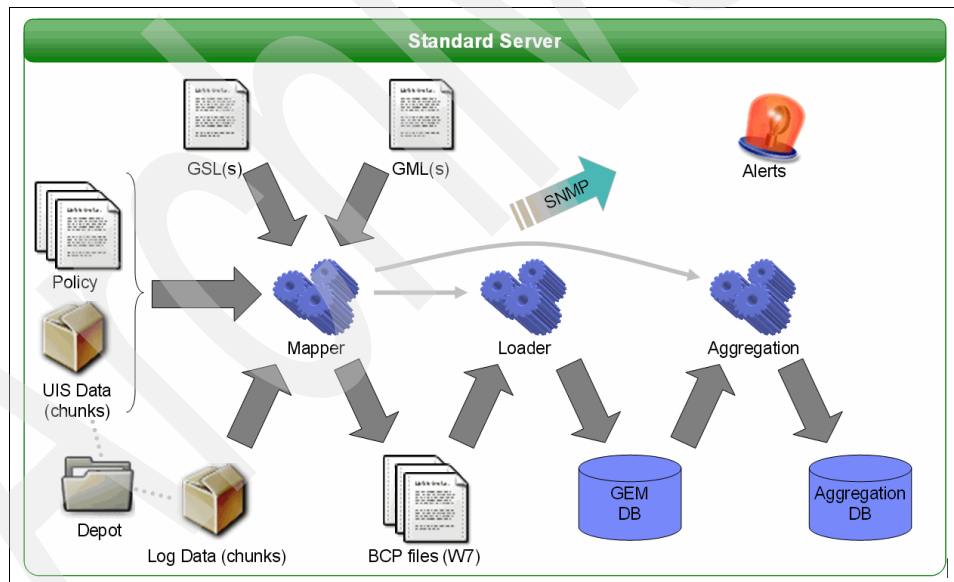


Figure 3-5 Normalization process

Log data is normalized using *General Scanning Language* (GSL) and *Generic Mapping Language* (GML) scripts. Next, the normalized events are combined with the *User Information Source* (UIS data), which is collected from the *user directories* and the *policy rules*. Both UIS data and policy rules are represented

in Tivoli Security Information and Event Manager's *W7 model*, which is a classification scheme that uses the following categories:

- ▶ Who
- ▶ When
- ▶ What
- ▶ Where
- ▶ Onwhat
- ▶ Whereto
- ▶ Wherefrom

Elements of the normalized events are categorized and assigned to a class within the category. The classes are either taken from the user directories or created by the user. The purpose of these classes is to be able to represent corporate assets in the *W7 model* and thus be able to specify relations between the assets. Let us take a look at an example.

W7 example

Let us use an example to look at a business rule and how this business rule can be translated into a *W7* rule.

Business rule

Here is a typical business rule.

Contractors are only allowed to access the IT resources during the regular workday hours.

This translates into a W7 rule

The translation can be mapped into *W7* language in the following way:

Who	Contractors
When	Workdays
What	Access
Onwhat	IT resources
Where	*
Whereto	*
Wherefrom	*

The *W7* model that can represent this business rule will, in addition to the classes, also contain definitions to specify which values of the log data are considered to represent an IT resource. The same mechanism is used to assign log data values to the contractor's class.

The *mapper process* normalizes the log data and applies the *W7* model to the events. The normalized events are stored temporarily as *bulk-copy* (BCP) files before the *loader process* loads them into a physical database. If certain

normalized events are identified as alerts, these events are sent out as SNMP or e-mail messages. But they can also trigger custom scripts. Tivoli Security Information and Event Manager Standard and Enterprise Servers can also support *basic event correlation* that can trigger alerts. These types of event correlation rules are platform independent and are limited to correlate single types of events on the time aspect of the event, for example, you can create a correlation rule that aggregates logon failure events when they occur more than five times within five minutes by specific users or any other W7 categories. These correlation rules are applied after the log data is collected and normalized. In cases where more complex real time rule-based event correlation and alerting is required to be processed by a Security Operations Center (SOC), a separate Tivoli Security Operations Manager module must be integrated with the Tivoli Security Information and Event Manager deployment.

After the normalized events are loaded into a physical database, post processing takes place and statistics are computed on the number of normalized events that match a W7 rule. Every normalized event will at least match one W7 rule because every event is categorized and the values are assigned to appropriate classes. These statistical results are loaded into a separate database called the *aggregation database*. An example of information that can be found in the aggregation database is:

When	Work days
Who	Contractors
What	Access
Onwhat	IT resources
#Events	1034

This result can be interpreted as *Contractors have accessed the IT resources 1034 times on regular working days.*

This statistical information is available on a Tivoli Security Information and Event Manager Standard or Enterprise Server and is computed based on the normalized data that the server generated. From a compliance reporting perspective, there is little difference between a Standard and an Enterprise Server, but from an architectural perspective there is a difference. Tivoli Security Information and Event Manager servers can be clustered to share the log archive between each other. A Tivoli Security Information and Event Manager cluster is comprised of one or multiple Standard Servers and one Enterprise Server. The log archive on the Standard Servers are shared with the Enterprise Server. The Enterprise Server provides a log analysis component that can use the log data that is collected by the Standard Servers in the same cluster. Therefore, the forensic search tool and the Tivoli Common Reporting reports on the Enterprise Server can also search the log archives of the Standard Servers.

Besides this added functionality of a Tivoli Security Information and Event Manager cluster, the statistical data that is kept in the aggregation databases on each Standard Server are copied to the statistical database on the Enterprise Server. This copying process enables a user to generate a single report that shows a summary of all events that are processed by each Standard Server in the cluster. Not only does such a report inform about the number of times a specific action happened, but it also informs about how many events violated the security policy or triggered an alert message. In general, this type of single report can be used to proof overall compliance across multiple Standard Servers.

3.3 Real-time event correlation and alerting

If there is a need for real-time event correlation and alerting, you must integrate Tivoli Security Information and Event Manager with Tivoli Security Operations Manager. Alerts that are identified by either of the products can be exchanged between them. Tivoli Security Information and Event Manager can be informed about both identification and mitigation of threats by Tivoli Security Operations Manager. This information sharing allows Tivoli Security Information and Event Manager to generate the proof through compliance reports that incident management is effective and also archive the evidence that supports the claim. We already explained the Tivoli Security Information and Event Manager architecture from a functional perspective. In this section, we briefly discuss the Tivoli Security Operations Manager functional views. For a more detailed understanding of this product, refer to the IBM Redbooks publications *Enterprise Security Architecture Using IBM Tivoli Security Solutions*, SG24-6014 and *Deployment Guide Series: IBM Tivoli Security Operations Manager 4.1*, SG24-7439.

The Tivoli Security Operations Manager architecture uses a multi-phased approach to event correlation and analysis called *deterministic threat analysis*. This type of threat analysis gives a security team the ability to detect known and unknown attacks, internal misuse, misconfigurations, and other anomalous activity. Using deterministic threat analysis, every event goes through both computational (policy based) and rule-based correlation, which establishes a base line from which any change is detected.

Computational correlation engine

Computational correlation involves using algorithms to assign values to events or groups of events based on factors, such as the severity of the event or the weighting that is assigned to a particular asset. These values are derived from your security policies and standards.

The Tivoli Security Operations Manager architecture uses two distinct techniques to perform computational correlation on events gathered by the system:

- ▶ *Impact correlation* relates to the calculations performed on individual events.
- ▶ *Statistical correlation* determines the trends that are created by groups of events.

Together, these two methods of calculating threats provide a highly accurate and surprisingly easy to administer method of prioritizing incidents of your network infrastructure without needing to configure rules.

The Tivoli Security Operations Manager architecture makes it possible to consolidate information from the network or insider attack that compromised the portal with the out of policy database changes. Analysts that use Tivoli Security Operations Manager can see the effects of an attack on applications and data and details of when the attack occurred, what user identities were used, and how it was accomplished. Using the comprehensive graphical interface, a non-technical user can focus on a specific event that occurred on the database. They can extend their analysis to view all activity by a particular user around the time of that event, including activity on other systems. They can drill down in to the details about a specific event or database operation and look at all events on the database or events for a user on other systems around the time of a specific policy violation or alert. They can open reports, such as one on the actions of system administrators, to obtain how a user was granted privileges and who granted them. These capabilities allow auditors and administrators to determine not only which user performed an action on a database, device, mail server, or other infrastructure component but the actions that were performed by privileged users to grant that user the privileges that they needed to perform actions that violated policy.

The Tivoli Security Operations Manager component adds real-time, rule-based threat management to the Tivoli Security Information and Event Manager solution. This component provides the following correlation techniques:

- ▶ Rule-based correlation
- ▶ Vulnerability correlation
- ▶ Statistical correlation
- ▶ Susceptibility correlation

Identified threats and their possible automatic mitigation can be picked up as events by Tivoli Security Information and Event Manager for integration into compliancy reporting.

With Tivoli Security Operations Manager added to it, Tivoli Security Information and Event Manager can cover the complete SIEM requirement spectrum from real-time threat and log management to regulatory and security policy compliancy reporting.

3.4 SIEM integration scenarios

In this section, we describe user personas and the typical issues that they face combined with the appropriate high-level SIEM solution that can be applied today. Today the integration is performed using the features that are integral to the two components.

3.4.1 User personas

Here are the user personas who might be interested in information that an SIEM solution provides:

- ▶ Network operations
- ▶ Network administrators
- ▶ Security administrators
- ▶ Database administrators
- ▶ Chief Information Security Officer
- ▶ Internal auditors
- ▶ External auditors

3.4.2 Typical issues encountered

Some of the typical issues that these groups might face are:

- ▶ Real-time threat management
- ▶ Network management
- ▶ Failed audit
- ▶ Requirements to comply with a new regulation

3.4.3 SIEM scenario 1 solution

In scenario 1, the personas are the database administrators, security administrators, Chief Information Security Officer, internal auditors, and external auditors. They all recognize that log data must be generated, collected, and analyzed in case of a security incident. Analysis occurs on demand, and there is no IT security policy or regulation that requires use of the contents of the log data to proof compliance. For them, the solution is implemented using a number of Tivoli Security Information and Event Manager Log Manager Servers for log data archiving and log data analysis. The Log Manager Server history and continuity reports address the requirements from the auditors as the forensic search tool and the Tivoli Common Reporting reports provide the database administrators and Chief Information Security Officer with sufficient material to investigate security incidents.

3.4.4 SIEM scenario 2 solution

In scenario 2, the personas are the security administrators, Chief Information Security Officer, and internal audit teams. The objective is to perform internal audits and be able to react to internal security incidents. A security policy is used as a reference to check the log data for security policy violations and incidents. Because there is no need and no business infrastructure for real time mitigation of incidents, an eight hour time-window is acceptable for incident mitigation. A Tivoli Security Information and Event Manager base solution can address all requirements for its compliance reporting functionality and basic event correlation and alerting engine.

3.4.5 SIEM scenario 3 solution

There is a growing need for regulatory compliance and organizations that want to be and stay compliant and that need to prove that the security controls that are required by the external audit body are in place and effective. The proof is based on two arguments:

- ▶ First it is required to show that the controls indeed prevented, that the security policy was violated, and in case of a violation that an effective mitigation occurs.
- ▶ Second it is required to show that security-relevant actions are being monitored.

Ideally a security policy and supporting security controls are customized completely for the type of business and the organization, but most of the times a security framework is used as a best practice reference to implement security controls and security policies, which applies to most of the IT security regulations. Tivoli Security Information and Event Manager provides compliance management modules for the major IT security regulations and these come with best practice frameworks for security policies and monitoring. These compliance management modules can help organizations to rapidly implement a proper set of compliance reports for best practice security controls and monitoring.

3.4.6 SIEM scenario 4 solution

In this scenario, an organization wants all of the aspects that were identified as part of a complete SIEM solution, for example they want:

- ▶ Security information management reporting
- ▶ Security event management reporting, which includes security dashboards, and compliance dashboards
- ▶ Monitoring and correlation (both rules-based and policy-based correlation)
- ▶ Minimization of the creation of specific rules
- ▶ Forensic capabilities
- ▶ Log management, which includes:
 - Record retention
 - Event collection across all platforms, both network and applications tiers
- ▶ Security and network operations convergence
- ▶ Support for IT best practices, such as IBM Service Management capabilities
- ▶ Integration with best of breed network management products, identity, and access management capabilities
- ▶ Incident and threat management capabilities

These requirements require a solution where Tivoli Security Information and Event Manager is integrated with Tivoli Security Operations Manager.

3.4.7 SIEM scenario 5 solution

In this scenario, an organization is required to collect, archive, and report on log data from more than 7000 machines, generating more than 200 GB of log data per day. Reports must be generated on a daily basis and must demonstrate overall compliance according to internal IT policies and regulations. A single Tivoli Security Information and Event Manager server can collect and report on approximately 60 GB of original log data per day and each server can collect and process log data from up to 5000 separate event sources. To process 200 GB per day, the organization must deploy three Standard Servers. To demonstrate overall compliance, a single Enterprise Server is needed to provide the centralized compliance overview. Therefore a cluster is the appropriate solution for this scenario.

3.5 Conclusion

In this chapter, we:

- ▶ Explored the requirements that are inherent for an SIEM solution
- ▶ Introduced the IBM products that address those requirements
- ▶ Described the architecture of Tivoli Security Information and Event Manager
- ▶ Explained how Tivoli Security Information and Event Manager addresses log management, compliance reporting, and alerting
- ▶ Extended the functionality of Tivoli Security Information and Event Manager to also cover real-time incident management by integrating it with Tivoli Security Operations Manager
- ▶ Showed certain basic use cases and the way that they can be addressed with both Tivoli Security Information and Event Manager and Tivoli Security Operations Manager

The remainder of this book describes how Tivoli Security Information and Event Manager meets many of the requirements of an SIEM solution in the context of a business case. Let us continue by introducing the logical and physical components of the IBM Tivoli Security Information and Event Manager product.

Archived



IBM Tivoli Security Information and Event Manager component structure

In this chapter, we explain in detail the logical and physical components of Tivoli Security Information and Event Manager. We also provide an architecture deployment overview.

4.1 Logical components

Tivoli Security Information and Event Manager consists of four main components that can be combined and implemented for various scenarios on one or more physical machines. Understanding these functional components in detail is necessary to properly estimate and size a scalable solution.

The Tivoli Security Information and Event Manager four main components are:

- ▶ Log Management Base Component
- ▶ Normalization Component
- ▶ Forensics Component
- ▶ Consolidation Component

Next to those four main components the product relies on the following two components as well:

- ▶ LaunchPad
- ▶ Agents

4.1.1 Log Management Base Component

The *Log Management Base* securely collects log data that is relevant to security auditing and compliance monitoring on a central server. The collected log data is stored on disk in its native (raw) format, as shown in Figure 4-1 on page 55. The raw log data store is referred to as the *Log Management Depot* or *Depot* for short.

The Log Management Base core relies on the *collect process*, which we explain later in this chapter.

The Log Management Base also acts as a Tivoli Security Information and Event Manager Agent, which means that it also contains the necessary components to remotely collect log information from other end points through SSH, ODBC, and other protocols.

The Log Management Base is deployed as part of either a *Log Management Server*, a *Standard Server*, or an *Enterprise Server*. These three types of servers are further explained in 4.3.3, “Server types” on page 82.

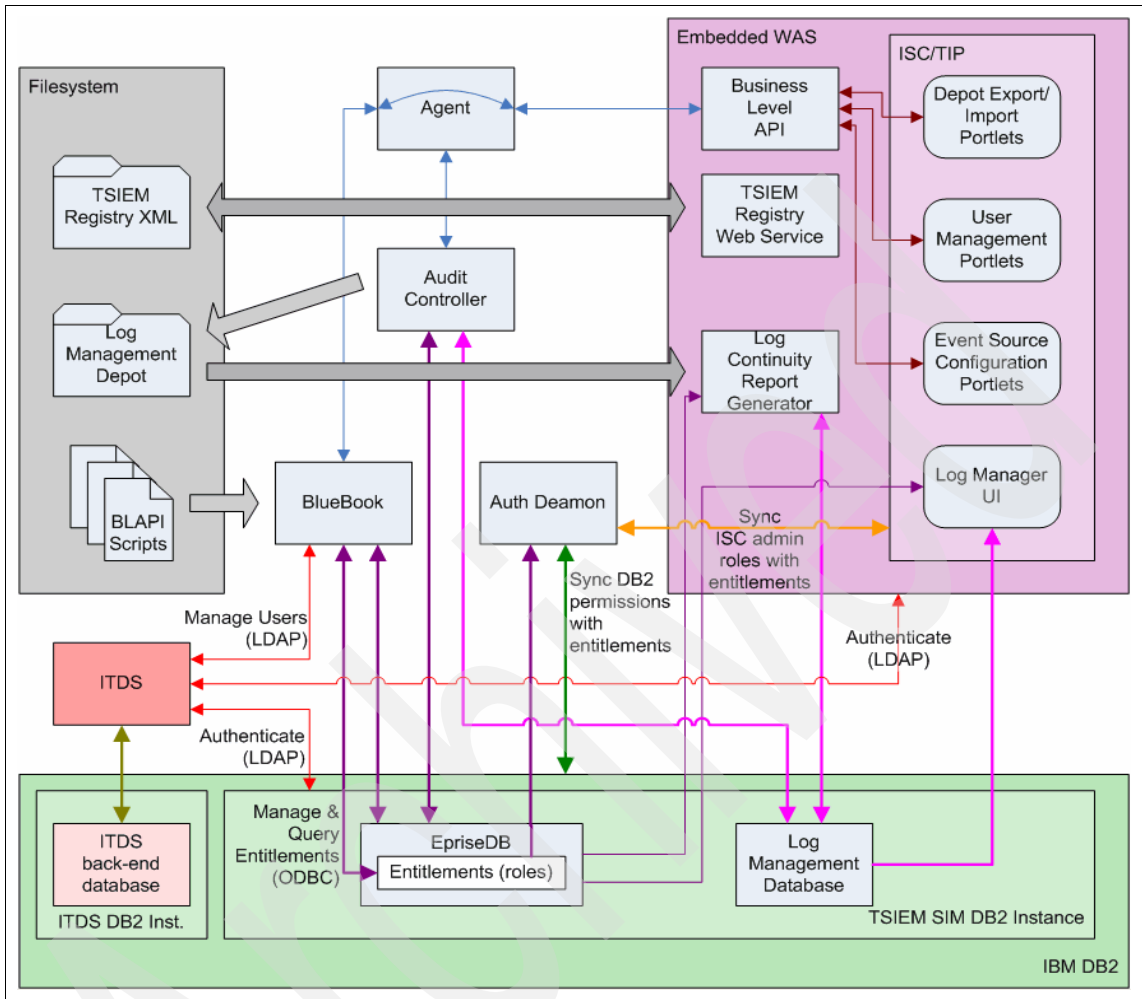


Figure 4-1 Log Management Base components relationship

The Log Management Base (LMBase) is the component that is responsible for initiating the log data collection, storing the data in the Log Management Depot, and monitoring the condition of the Depot. We describe the major component elements in the sections that follow.

Audit controller

The audit controller initiates the collection of log data and ensures that it is stored in the Log Management Depot. Normally, log data collection operations are triggered on a user-defined schedule.

The audit controller also records the attempted collected operations in the Log Management Database, which indicates success or failure. This information is used by the *Collect History* and *Log Continuity* reports.

Auth daemon

The *auth daemon* grants and revokes permissions to objects in the DB2 instance based on the application roles that are assigned to the Tivoli Security Information and Event Manager users. Every minute the auth daemon checks if the roles that are assigned to a user on the Security Server changed. If so, it grants or revokes the necessary permissions in the local DB instance. The auth daemon also synchronizes TIP roles with Tivoli Security Information and Event Manager application roles.

Bluebook

The *bluebook* makes calls to various features, such as the Policy Generator and the SEAMAN installation tool that is used for the remote installation of Windows® Agents. The bluebook also communicates with the Business Level API component (BLAPI). The BLAPI makes calls to the bluebook to perform management operations, for example, the GUI calls the BLAPI, the BLAPI calls the bluebook, and the bluebook performs the necessary configuration updates.

Business Level API component

The *Business Level API* component (BLAPI) is comprised of a set of APIs that the Tivoli Integrated Portal invokes to perform various tasks, such as event source configuration and user and role management.

IBM DB2

The database engine for the Tivoli Security Information and Event Manager product is *IBM DB2*. There are two DB2 instances: one for the Tivoli Directory Server (LDAP) and one for Tivoli Security Information and Event Manager. The Tivoli Security Information and Event Manager DB2 Instance is configured to authenticate against Tivoli Directory Server using the LDAP protocol.

IBM Tivoli Directory Server (ITDS)

Tivoli Security Information and Event Manager uses *Tivoli Directory Server* for user ID management and authentication. For a user to access the Tivoli Security Information and Event Manager application, the user must have a user ID in the Tivoli Directory Server. DB2 access is authenticated against the Tivoli Directory Server as well.

Tivoli Integrated Portal (TIP)

The *Tivoli Integrated Portal* runs on the embedded IBM WebSphere® Application Server that ships with Tivoli Security Information and Event Manager. Single sign-on capabilities within the Tivoli Integrated Portal environment are used to access all Tivoli Security Information and Event Manager features from within the same Tivoli Integrated Portal session.

Depot export and import options

The most common use of the depot export and import functionality is to support archiving of old log data.

Event source configuration portlets

Using the *event source configuration portlets* you can add an event source or an agent and change a collect schedule. Using the portlets you can assign event sources to Reporting Databases only if the Normalization Component is deployed. For more details about the Normalization Component, refer to 4.1.2, “Normalization Component” on page 58.

Log Management Continuity report generator (LCRG)

The *Log Management Continuity report generator* performs a daily analysis on the Log Management Depot to generate information for the Log Management Continuity report.

Log Manager user interface

The *Log Manager user interface* provides access to Log Management reports to verify the state of the log collection and completeness of the Depot. The Log Manager also provides Log Management Depot Investigation and Log Management Retrieval capabilities.

User management

The *user management* functions support user IDs and entitlements (role assignments), creation and deletion of users, and changing permissions for the Tivoli Security Information and Event Manager users.

Registry Web service

The Tivoli Security Information and Event Manager registry is a general purpose repository for storing information that is related to Tivoli Security Information and Event Manager Servers. The information that is stored in the registry includes the name and the description of the Tivoli Security Information and Event Manager Servers, the URL for launching the Tivoli Security Information and Event Manager Server's GUI, and a list of capabilities (such as LMBase, Standard Server, Enterprise Server, and so on) of the individual servers.

The Registry Web service provides a centralized repository. It is part of the Log Management Base, but it is installed only on one Tivoli Security Information and Event Manager Server in the Security Group.

The Tivoli Security Information and Event Manager registry is accessed using the Launchpad, explained in 4.1.5, “LaunchPad” on page 63. The Launchpad provides options to access other Tivoli Security Information and Event Manager Servers within the Security Group.

4.1.2 Normalization Component

The *Normalization Component* is responsible for W7 normalization and compliance reporting. Figure 4-2 on page 59 depicts the Normalization Component’s relationship.

The Normalization Component is deployed as part of a Tivoli Security Information and Event Manager Standard Server and Enterprise Server and is always deployed together with the Log Management Base. We explain all of the Normalization Components in the sections that follow.

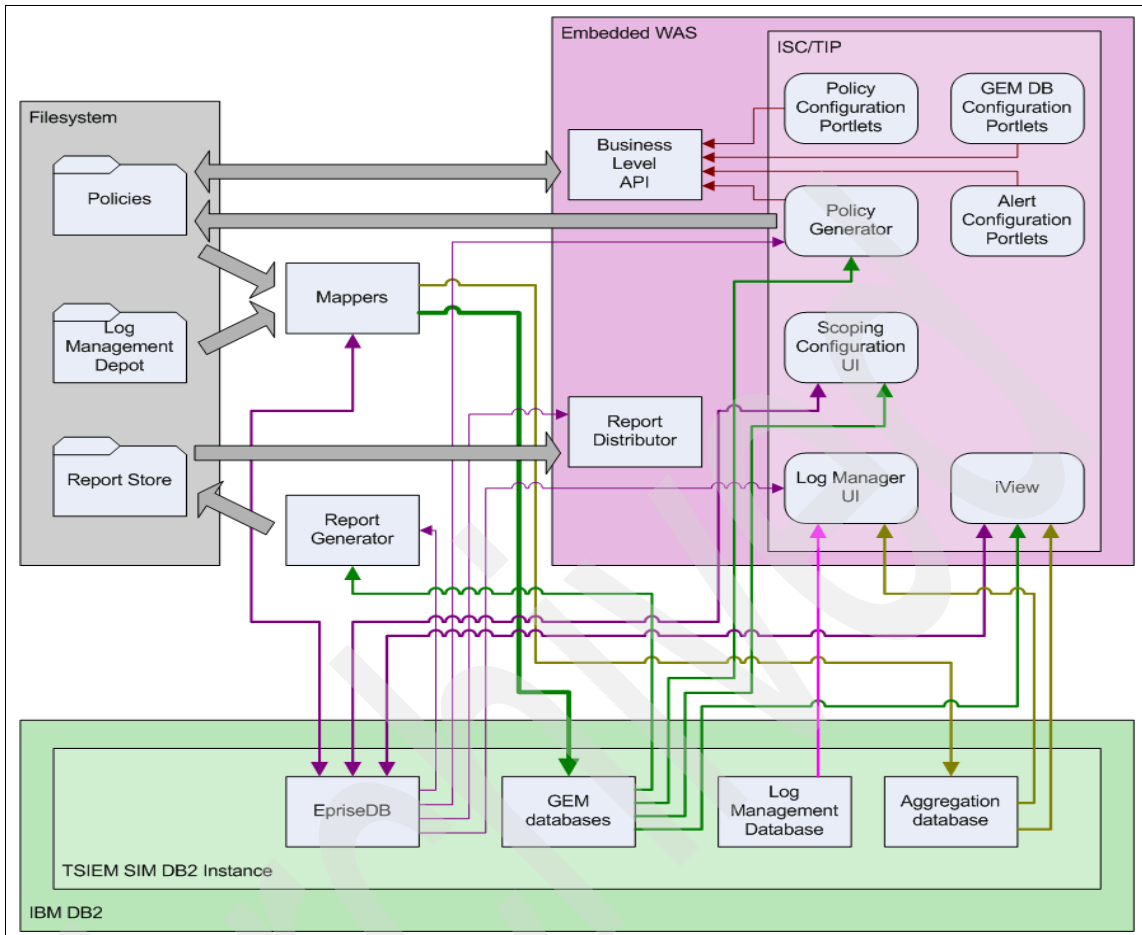


Figure 4-2 Normalization Component's relationship

Alert configuration portlets

Alert configuration portlets set up alerting rules. The mapper process sends out alerts during W7 normalization using SNMP, e-mail, or a custom distribution mechanism.

The Reporting Database configuration portlets

Using the *Reporting Database (GEM DB) configuration portlets* you can change a load schedule, assign event sources to GEM databases, and remove a GEM database.

Compliance Dashboard

The *Compliance Dashboard* provides reporting and data mining capabilities for normalized, W7-based data.

Mappers

The *mapper* component is the data analysis engine. It is responsible for W7 normalization and policy analysis. Normalized events are loaded into a Reporting Database, and a summary is loaded into the aggregation database.

Policy configuration portlets

The *policy configuration portlets* add, delete, and configure the Tivoli Security Information and Event Manager security policy.

Policy generator

The *policy generator* is an initial system configuration tool that can propose a W7 audit policy based on access patterns observed in actual log data from Windows machines and CheckPoint firewalls. On multiplatform environments, this is not a recommended method. This feature is mostly used for demo purposes.

Report distributor

The *report distributor* distributes compliance or custom reports as e-mail attachments in multiple formats, such as XLS, CSV, PDF, and HTML.

Report generator

The *report generator* component is executed by the mapper, generates W7 reports, and stores them in the file system. In a later step, the reports can be sent as e-mail attachments by the report distributor component.

Scoping configuration user interface

You can use the *scoping configuration user interface* to set up content-based access restrictions on W7 data so that multiple users can see W7 events based on their ownership of the resources that are reported on.

4.1.3 Forensics Component

The *Forensics Component* provides consolidated log management reporting, and runs the indexing and searching processes that are required to support the Depot Investigation tool, which enables keyword searches on the data in the Log Management Depot. Figure 4-3 illustrates the Forensics Component's elements, and we describe the elements in the subsections that follow.

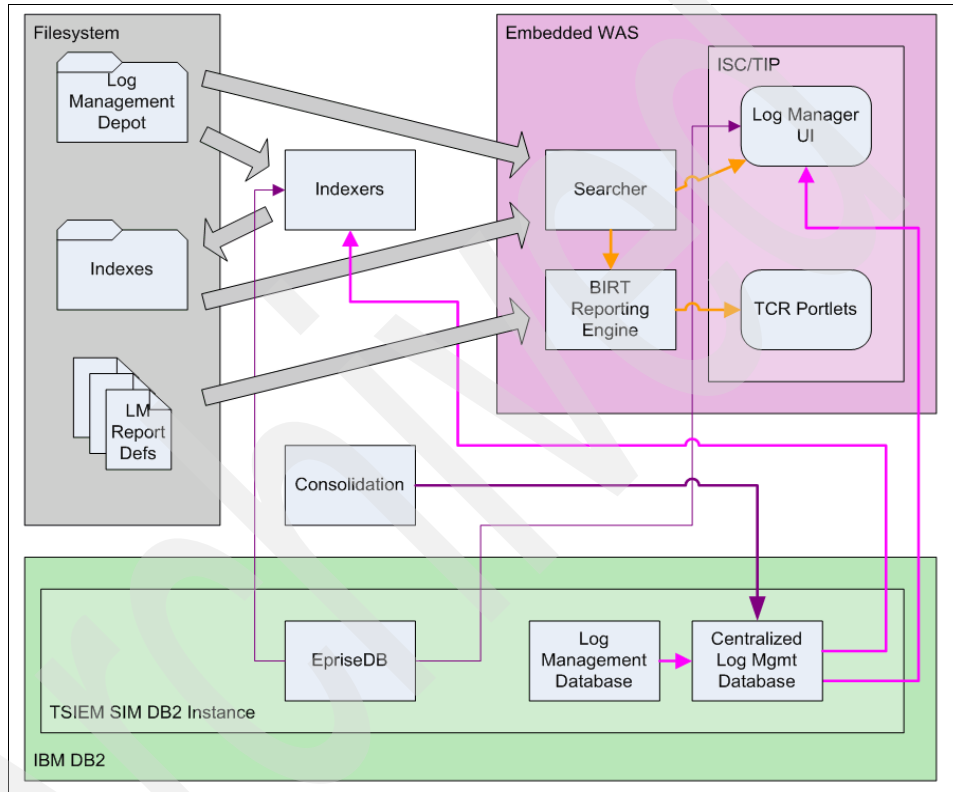


Figure 4-3 Forensics Components relationship

Centralized Log Management Database

The centralized *Log Management Database* on the Tivoli Security Information and Event Manager Enterprise Server provides a consolidated view of the information that is kept in the Log Management Databases on attached Standard Servers.

Data in remote Log Management Databases is read on demand using the DB2 Federated Database feature.

Indexers

The *indexer* processes on the Log Management Server and Enterprise Server and creates indexes of the data in Log Management Depots on attached Standard Servers. This process enables fast keyword searches on log data.

A separate indexer process is launched for each attached Standard Server.

Remote file access is used to access the Log Management Depots on the attached Standard Servers from the Enterprise Server.

Searcher

The *searcher* functionality runs in the context of the Log Manager Web application, but it is only available on a Log Management Server and Enterprise Server. The searcher provides keyword search of collected log data on all attached Standard Servers. Some of the Tivoli Common Reporting reports also use the searcher.

Tivoli Common Reporting

Tivoli Common Reporting (TCR) supports the Log Management Reporting feature. This feature provides reports on the content of the files in the Log Management Depot without doing full W7 normalization. It makes use of the forensic search functionality to accomplish this.

4.1.4 Consolidation Component

The *Consolidation Component* consolidates and summarizes normalized W7 data from a number of attached Standard Servers and provides consolidated W7 reporting. The Consolidation Component is deployed as part of the Enterprise Server, as shown in Figure 4-4 on page 63.

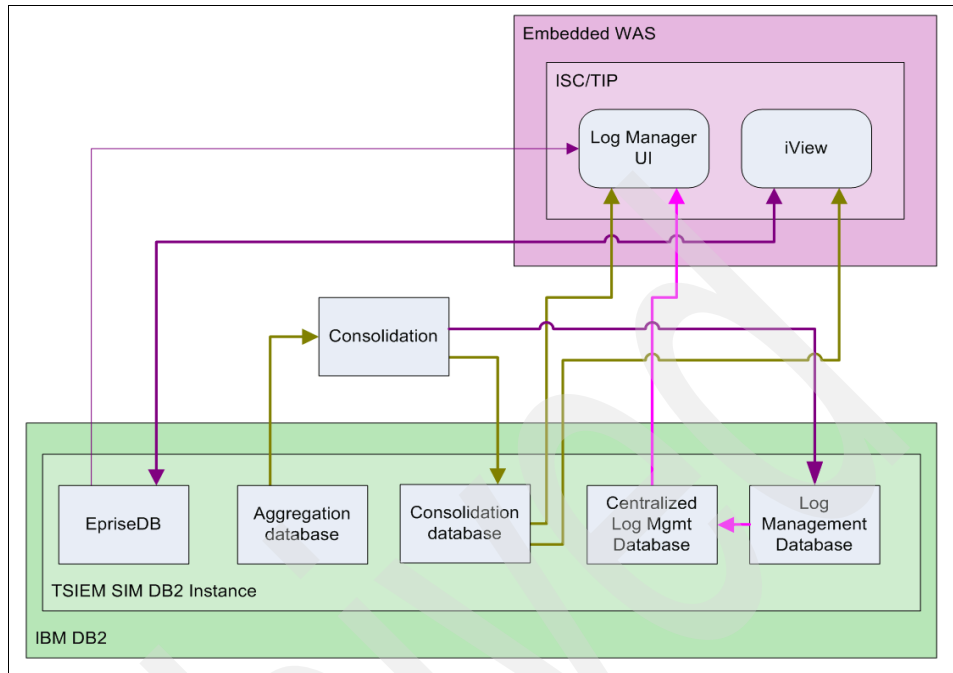


Figure 4-4 Consolidation Component relationship

Consolidation process

The *consolidation process* runs on the Tivoli Security Information and Event Manager Enterprise Server. It consolidates historical information that is stored in the aggregation databases on attached Standard Servers into the consolidation database on the Enterprise Server.

4.1.5 LaunchPad

By default, the *launchpad* is deployed on all Tivoli Security Information and Event Manager servers. It offers a list of all installed Tivoli Security Information and Event Manager servers in the same Security Group. The launchpad provides you with an interface to navigate between the various deployed Tivoli Security Information and Event Manager servers.

4.1.6 Agents

Depending on the platform, *agent* software is installed on end points as a *service* or *daemon*. Each agent consists of an agent and one or more *actuator scripts*. The agent is responsible for maintaining a secure communication channel with

the agents that are running on the server and other end points. Tivoli Security Information and Event Manager uses FIPS certified encryption protocols. The actuator scripts are invoked by the agent (at the request of the server) to collect log data, as shown in Figure 4-5.

The transmission mechanism exploits the Tivoli Security Information and Event Manager secure communication protocol (CSSL) in the Agent process.

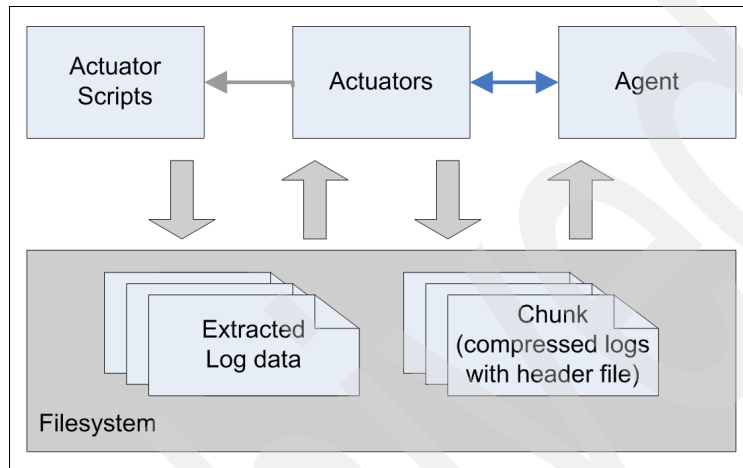


Figure 4-5 Agent components relationship

Actuator scripts

The *actuator scripts* are part of the endpoint data collection process. They extract log data that was not previously collected from an event source. Any number of protocols can be used to access the data, either locally or remotely. The choice of protocol depends on the nature and capabilities of the endpoint, the audited machine, the machine that is hosting the agent, and so on.

Actuators

On request of the *audit controller*, which is running on the server as, explained in 4.1.1, “Log Management Base Component” on page 54, the *actuator* process, which is part of the agent, invokes an actuator script to extract log data. The actuator compresses the extracted log data and adds a descriptive header file. A separate actuator process is launched for each event source.

Agent

The *agent* process provides a secure communication path between a server and the attached agents. Log file data is collected through this secure channel.

The most common mechanism for retrieving security log data is through a process called *batch collect*. A security log is created on an audited machine by the application, system, or device that is audited. In general, such logs contain records of many events, which all get processed. The Tivoli Security Information and Event Manager server initiates the collection of security logs from the audited machines. This action is either triggered by a set schedule or manually through the Tivoli Integrated Portal. After receiving the security logs, the Tivoli Security Information and Event Manager server archives the security logs in the Depot.

Event data is collected using a variety of methods to establish the consolidated archive stored in the Depot. Events can be collected in numerous ways, including:

- ▶ Logs
- ▶ Syslog
- ▶ SNMP
- ▶ NetBIOS
- ▶ ODBC
- ▶ External APIs
- ▶ SSH

There are two methods of data collection:

- ▶ Locally installed software (Tivoli Security Information and Event Manager agent) on the target machine.
- ▶ Agent-less collection, which is achieved by either:
 - A remote Tivoli Security Information and Event Manager agent installation that allows you to collect the application security log that is located on a another host machine.
 - A Tivoli Security Information and Event Manager server that acts as an agent to collect data. By design, a Tivoli Security Information and Event Manager server can act as an agent to collect from end points.
 - The collect process from end points where security data was generated by either Syslog or SNMP. This collect method is considered agent-less.

Let us take a closer look at these two distinct methods.

Data collection using agents

A typical Tivoli Security Information and Event Manager network consists of one or more Tivoli Security Information and Event Manager servers and a number of machines that must be audited. These machines can be running one or more applications, each of which can be audited by the Tivoli Security Information and Event Manager. These machines are often referred to as the *audited systems*.

The Tivoli Security Information and Event Manager agent is comprised of an agent itself and numerous actuator scripts. The actuators or collect scripts facilitate the data collection process. The server where the actuator is installed is referred to as a Tivoli Security Information and Event Manager agent, it can collect and forward security logs for the operating system, applications, databases, or devices on which it is installed. Every application that generates security audit log data is referred to as an endpoint.

Each endpoint that is monitored uses an associated actuator collect script, for example, the security log on a Sun Solaris server is collected by the actuator for the Solaris endpoint. The same server that is running Oracle can use the same actuator to collect and monitor the Oracle security log. There is a distinct actuator script for every supported type of event, so the actuator can process logs for several endpoints. In this example scenario, the actuator is collecting the logs from two endpoints, Solaris and Oracle for Solaris.

The agent continuously listens on a reserved port for collect requests that the Tivoli Security Information and Event Manager server issues. When a request is received, the agent invokes the appropriate script to gather the logs. After the actuator collects the security audit log for a particular event source, the agent compresses and transfers the logs to the centralized Tivoli Security Information and Event Manager Depot. The agent maintains an encrypted channel for all communication between the target machine and the Standard Server. That is, it provides a secure and guaranteed transmission service. Figure 4-6 depicts a step-by-step collection process.

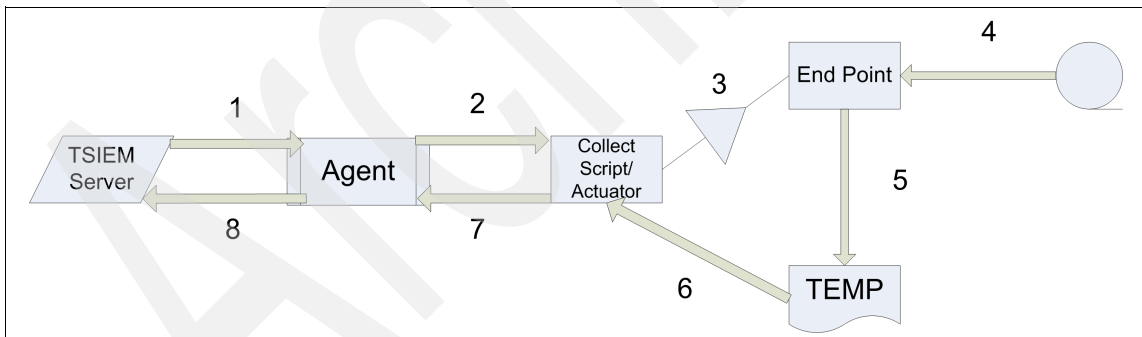


Figure 4-6 Collect step by step

Let us explain these individual steps in Figure 4-6:

1. The Tivoli Security Information and Event Manager server sends a collect command to the agent.
2. The agent invokes the collect script and propagates the endpoint properties that are defined in the Tivoli Integrated Portal for that endpoint.

3. The collect script executes the file, which is referred to in the *Program Path* property of the endpoint. This field is not available for all endpoints.
4. The collect script reads the audit records.
5. The collect script writes the audit records to temporary files.
6. The collect script creates a chunk from the temporary files.
7. The agent compresses this chunk.
8. The agent encrypts the chunk and sends it to the server where it is stored in the Depot.

Important: For practical terminology reasons, the actuator and agent terms are combined to agent in most of the product documentation. For a better understanding, we still use the concept of an actuator, which helps us to understand how the collect mechanism for multiple endpoints takes place using various collect scripts (actuators).

Agent-less data collection

Tivoli Security Information and Event Manager supports agent-less collection on Microsoft® Windows, Novell, IBM System i® (formerly known as AS/400® or iSeries®), and UNIX® platforms. When using agent-less remote collection, the picture is slightly different than agent-based collection, but the steps remain the same. The agent establishes the secure connection to the Tivoli Security Information and Event Manager server and sends all agent-less collected data securely to the Depot. Agent-less data collection reduces the operational overhead compared to an agent-based approach. The SSH approach with UNIX provides a secure connection. For databases, the agent-less collect method can be either through ODBC or an SSH connection to the base Operating System, either UNIX or Linux®.

Network devices that generate either Syslog or SNMP security data are also considered agent-less endpoints.

Let us take a look at a few of the agent-less data collection environments:

- ▶ Microsoft Windows 2008 and Microsoft Vista agent-less collection

The most common implementation of *remote collect* is on a Microsoft Windows system. Figure 4-7 on page 68 shows the typical configuration that is used to perform an agent-less collect when the audited systems are Windows machines.

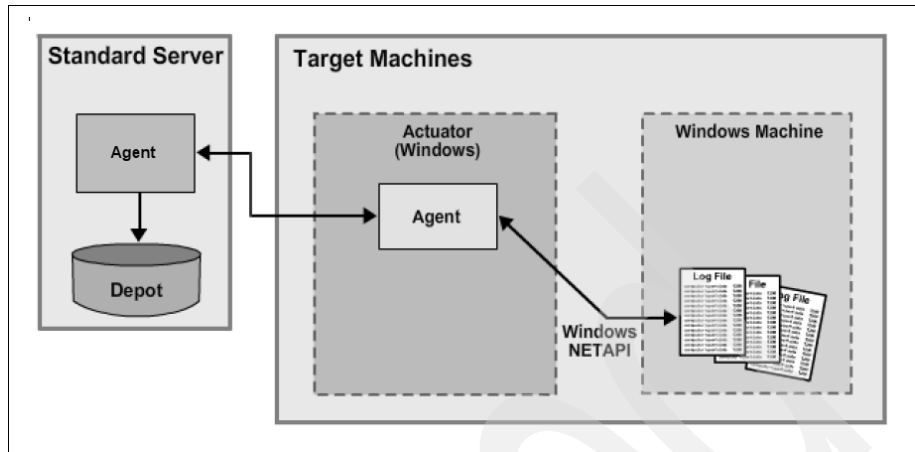


Figure 4-7 Windows agent-less collect mechanism

Windows agent-less collection follows these steps:

- a. The collect schedule is automatically triggered based on site-specific settings. Alternatively, a manual collect command can be given to the Tivoli Security Information and Event Manager server through the Tivoli Integrated Portal.
- b. The server issues a collect log command to the agent, which can be the server itself. This command activates the collect script.
- c. The agent uses a Windows NETAPI call, which connects to the endpoint through a link to the Administrative Share ADMIN\$.
- d. The Tivoli Security Information and Event Manager agent reads the security log from the remote server(s) using the Windows API, generates a dump of that file, and collects only those new events since the last collection cycle or the last 48 hours of activity, if it is a first time collect.
- e. The log data is processed and sent to the Depot on the Tivoli Security Information and Event Manager server.
- f. This collect event is registered as a *successful collect* on the Tivoli Security Information and Event Manager Configuration Database from where it is taken to generate *collect history* and *continuity* reports.

Important: The agent-less collect mechanism for Windows 2008 requires that a user, either local or domain, is granted administrative rights on the server. This requirement is due to the method that is used for the collection mechanism based on the administrative share, which must be reachable from the server or agent that is executing the collect. Security devices that are placed in line of this communication path must be opened to allow access to the ADMIN\$ share.

► UNIX and Linux agent-less collection

Tivoli Security Information and Event Manager also supports agent-less collect for UNIX and Linux servers. It uses the SSH protocol to perform the collect so that it is secure.

Tivoli Security Information and Event Manager uses a PuTTY client to establish the SSH connection, which must be appropriately configured. The PuTTY client can be installed on one of the Tivoli Security Information and Event Manager servers or on any Windows-based agent, as depicted in Figure 4-8 on page 70. The UNIX server must be running an SSH daemon. A user ID must be available on the UNIX machine that was granted the permissions to establish the connection and to read the audit trails.

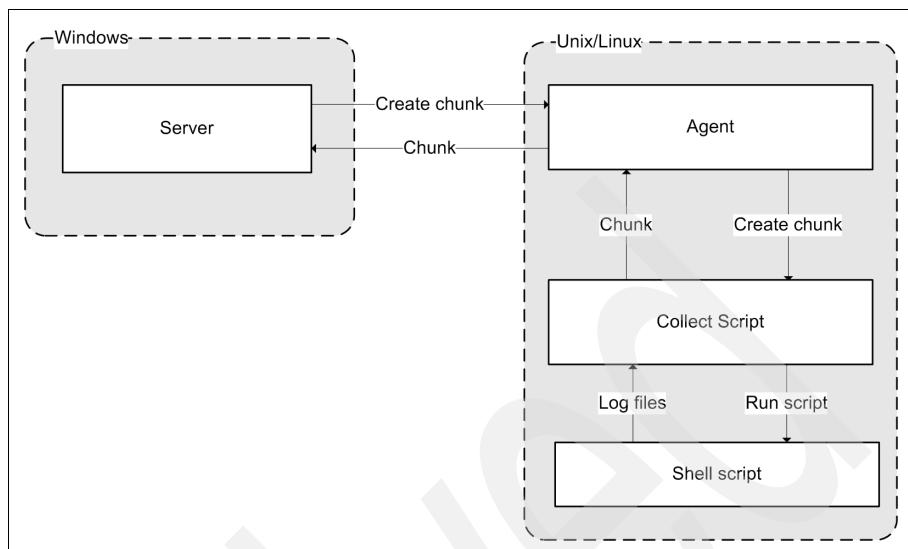


Figure 4-8 SSH collect for UNIX or Linux

► Syslog and SNMP collect

Tivoli Security Information and Event Manager can process and analyze security events that are collected through the Syslog and SNMP network logging mechanisms. The support for Syslog and SNMP messages is achieved in one of the following scenarios:

- Syslog or SNMP end points sending messages to an AIX® agent-based machine.
- Syslog or SNMP end points sending messages to a Syslog-NG receiver.
- Syslog or SNMP end points sending messages to a Tivoli Security Information and Event Manager server.
- Syslog or SNMP end points sending messages to a Tivoli Security Information and Event Manager agent on Microsoft Windows.

In environments with high volumes of SNMP or Syslog security data, the preferred method is to send the SNMP and Syslog messages to an AIX-based agent. Tests that are executed in this kind of environment demonstrated a capacity to manage up to 30,000 transactions per second (TPS).

Even though the Tivoli Security Information and Event Manager server or the agent on Microsoft Windows can also be Syslog and SNMP receivers, they have limitations and can be used for demonstration and test purposes or in environments with very low demand, for example, less than 800 TPS is considered low.

- ▶ Ubiquitous log collection

Tivoli Security Information and Event Manager can collect logs from any source. In several cases, no normalization is available for a specific source.

The ubiquitous endpoint is designed to collect logs from any unsupported platform. They can be used in particular situations where an organization only needs to collect and store the security log data.

If that log data must be analyzed or searchable, indexers can be built for forensic analysis.

- ▶ CSSL

The CSSL protocol is used to communicate between servers and attached Tivoli Security Information and Event Manager agents.

CSSL supports compression and encryption algorithms that are used when data is transmitted between servers and agents. The communication between servers and agents complies with FIPS-certified encryption protocols.

Generally, there are two communication paths in a Tivoli Security Information and Event Manager installation: between servers and agents and between agents and end points. CSSL is the communications methodology that is used between servers and agents. However, other agent to endpoint communications that transmit over the network might rely on other technologies, such as PuTTY and OpenSSH, which are not FIPS compliant. To be FIPS compliant, you either do not use SSH collect or use OpenSSH server and client custom builds that are linked to a FIPS-certified OpenSSL build.

4.2 Data flow

We divided this data flow section into the following parts:

- ▶ Agent-based data flow log collection
- ▶ SSH-based data flow log collection
- ▶ Log Management reporting data flow
- ▶ Normalization process data flow

4.2.1 Agent-based data flow log collection

To better understand the agent-based data flow log collection we begin with looking into the Log Manager data process flow.

Figure 4-9 on page 72 shows the Log Manager data process flow, where the overall log management functionality is depicted in the LM column of the figure.

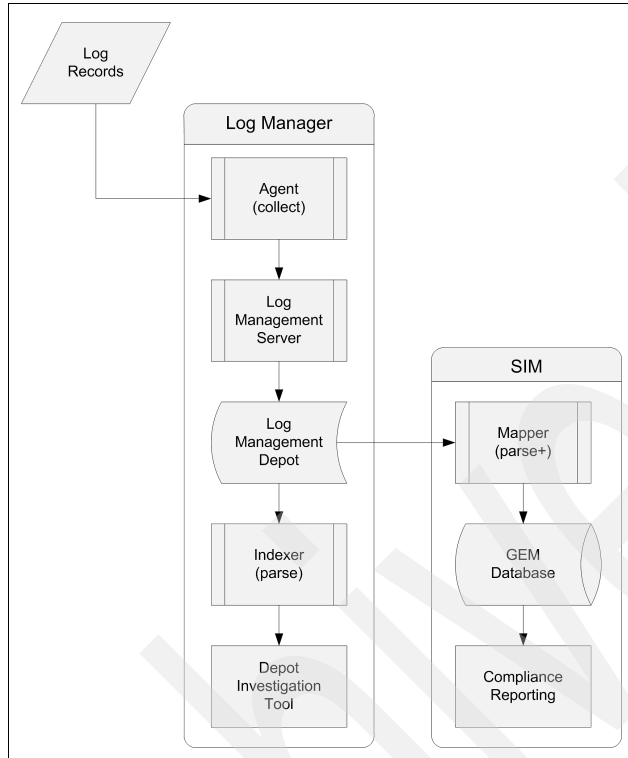


Figure 4-9 Log Manager data process flow

The Tivoli Security Information and Event Manager *Log Manager* collects the *log records* through an *agent* to provide reliable and secure collection. The *Log Management Server* saves the records in the archive. After the log records are stored in the *Log Management Depot*, an *indexer* processes the log records to enable log record analysis. The *Depot investigation tool* then uses the indexes to optimize the performance of the search query.

Because log records are indexed when they are archived and the forensic search tools use the indexes to generate the result sets, these tools still work even after the archive is cleaned up to free up disk space. Typically, original log data is kept in the Tivoli Security Information and Event Manager Log Management Server for 90 days. Log data that is older can then be moved from the Log Management Server to external storage. The size of the log records in the archive are approximately 15% of their original size because the Log Management Server compresses the log data as it collects it.

It is important to realize that the collected log data might come either directly from the native audit subsystems, or it can be routed through the Syslog protocol

or SNMP first. If large amounts of Syslog messages or SNMP traps must be collected, archived, and reported upon, an additional Tivoli Security Information and Event Manager component can be added that collects these messages and traps in real-time. This high performance Syslog collector processes this information for the Tivoli Security Information and Event Manager agents to collect them in the regular manner. The Tivoli Security Information and Event Manager Syslog collector is available for AIX, Linux, and Windows platforms. Figure 4-10 shows the real-time Syslog and SNMP data processing flow.

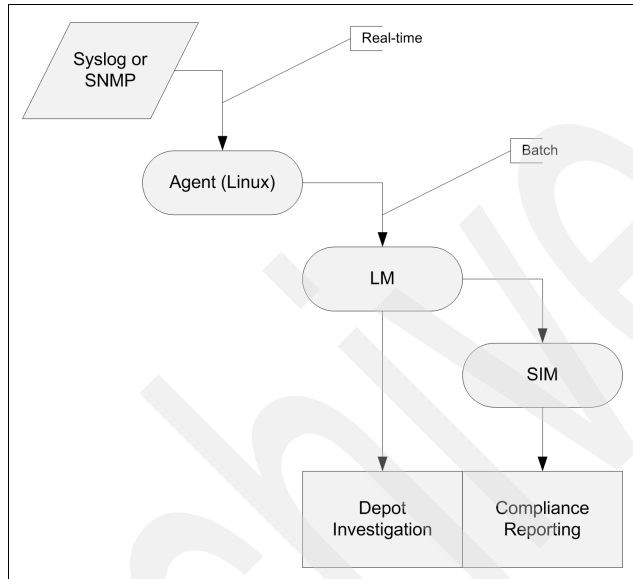


Figure 4-10 Syslog and SNMP data processing flow

With this general understanding, we can now take a closer look at the data flow for agent-based log collection. Figure 4-11 on page 74 depicts the general data flow for collecting log data from an audited machine. The data flows through an agent into the Depot on the Standard Server.

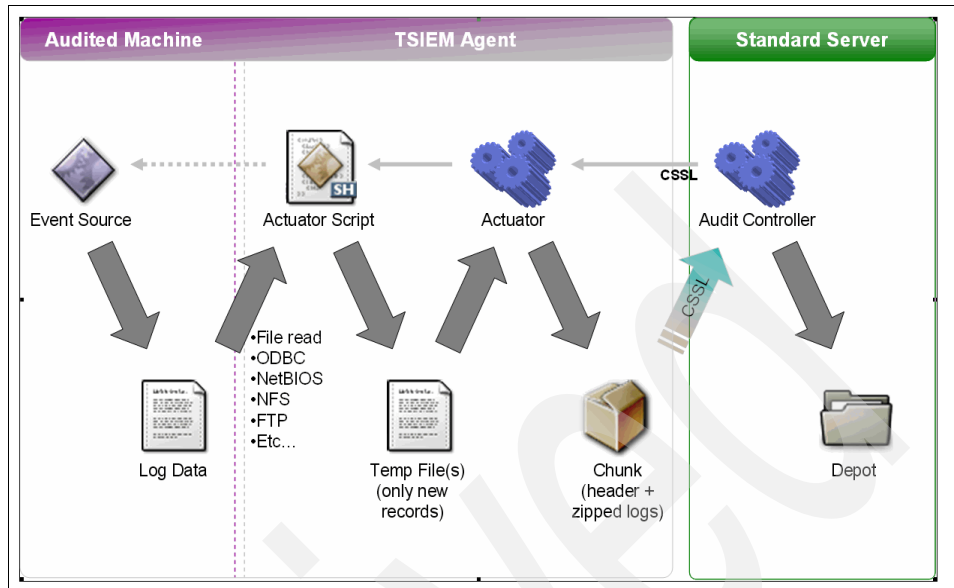


Figure 4-11 Agent based data flow

The *audited machine* represents the machine that is monitored, which is where the events are collected. The *Tivoli Security Information and Event Manager agent* is deployed on the audited machine. The agent packages and transmits the log files to the Standard Server using the secure communication protocol (CSSL).

4.2.2 SSH-based data flow log collection

In this section, the actuator process packages the actuator script and everything it needs to collect remotely, sends it to the audited machine using SSH, executes the script, and retrieves the results using SSH, as depicted in Figure 4-12 on page 75.

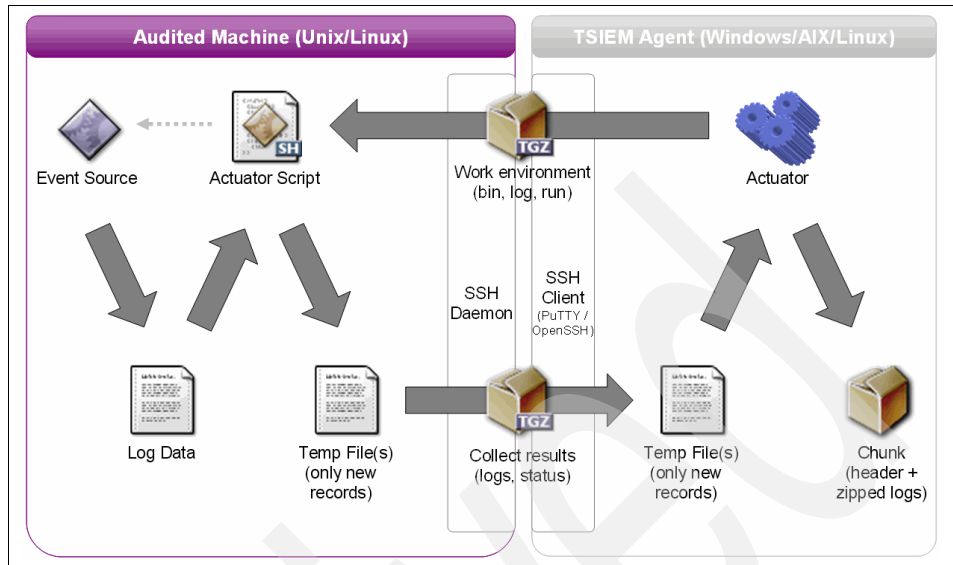


Figure 4-12 SSH-based data flow log collection

4.2.3 Log Management reporting data flow

The Log Management reports are based on data that is retrieved from the raw log files that are collected from event sources on audited machines. The reports run in the Tivoli Common Reporting (TCR) environment, which is included as part of TIP, and use the Eclipse Business Intelligence and Reporting Tools (BIRT) infrastructure to define and render the reports, as shown in Figure 4-13 on page 76.

The Log Management reports can provide additional reporting functionality. This functionality is provided by the Forensics Component, which is only deployed as part of a Log Management Server and Enterprise Server. The Log Management reports provide summary reports, which have links to drill down into more detailed reports.

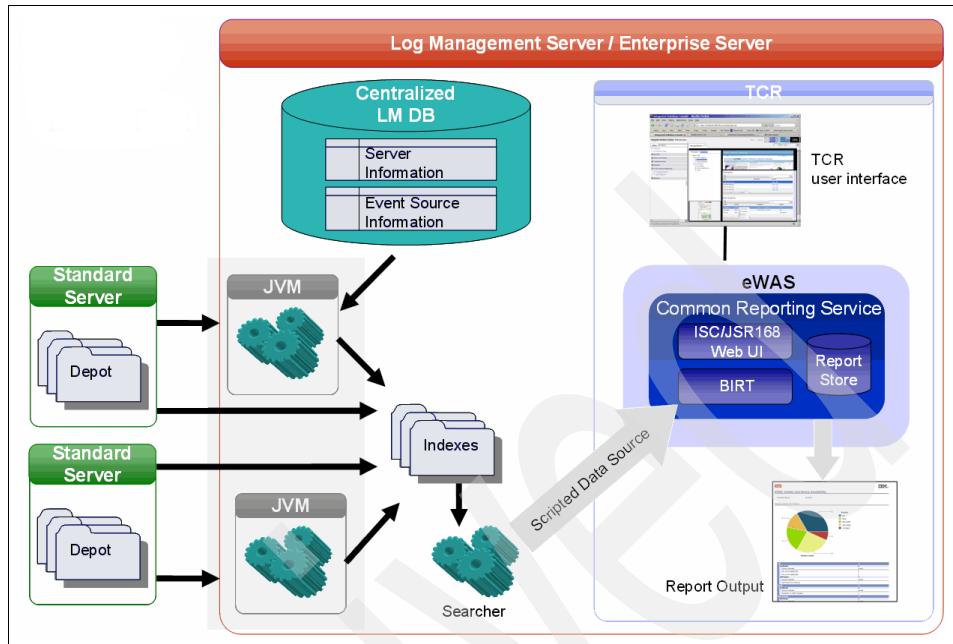


Figure 4-13 Log Management reporting data flow

4.2.4 Normalization process data flow

In Figure 4-14 on page 77, we show the normalization process data flow. Raw log data is read from the Log Management Depot, normalized to W7, and loaded into a Reporting Database (GEM).

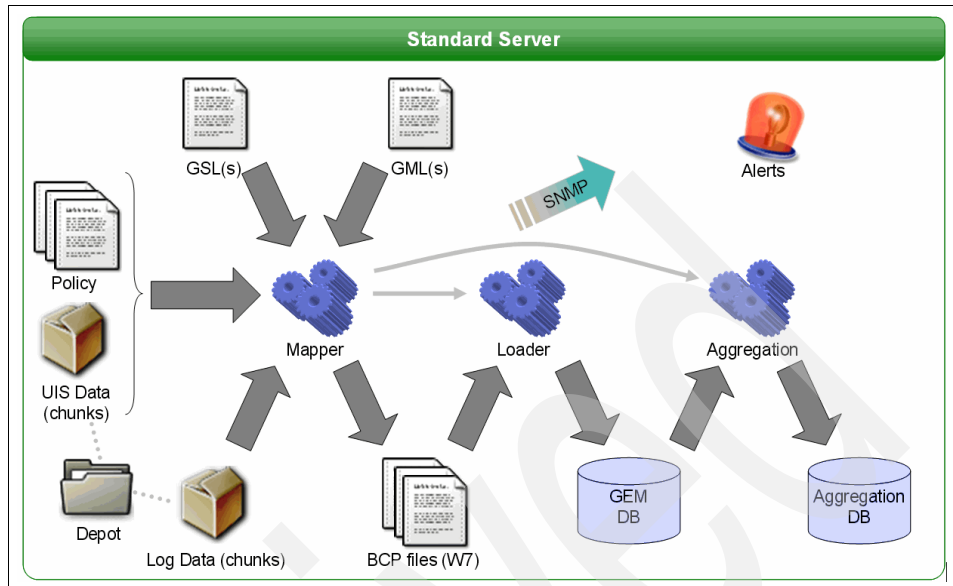


Figure 4-14 Normalization process data flow

The *mapper* component acts as the data analysis engine. It is responsible for normalization and policy analysis. *General Scanning Language* (GSL) and *Generic Mapping Language* (GML) files contain, respectively, log parsing and normalization rules that are used by the mapper to transform the raw log data into W7 events.

GSL and GML are event-source specific and are created during development of a new event source.

As further input, the mapper takes the configured *W7 policy* and the *log data* to be normalized and analyzed. The W7 policy used during analysis is put together from two sources: the W7 policy groups and rules as configured by the Tivoli Security Information and Event Manager policy administrator using the Tivoli Integrated Portal and a set of automatically collected W7 group definitions, for example, Who groups can be automatically created by interrogating an Active Directory server.

The parsing and normalization rules in the GSL and GML files can be written to drop events if they are not compliance relevant.

The mapper writes its output to a set of files called *bulk-copy (BCP) files*, which are simply 1-on-1 representations of the tables in the Reporting Database. When data normalization is complete, these files are loaded into the *Reporting*

Databases by the loader. Optionally, the mapper can send out alerts as it analyzes the data, which is useful for early signaling of critical issues.

As the final step in the normalization flow, the *aggregation* process summarizes the newly loaded W7 events into the *aggregation database* schema. More specifically, it:

- ▶ Maintains statistics of how many events, policy exceptions, special attention events, and failure events occurred over time, by hour and by W7 group combination. This feature enables the creation of trending charts spanning long periods of time (years, potentially).
- ▶ Maintains a history of all high-severity events. By default, all policy exceptions and special attention events that are found during policy analysis are copied to the aggregation database, where they are retained indefinitely (Reporting Databases normally only contain events for a seven-day sliding window). The data volume of high severity events going into the aggregation database is limited by an algorithm that combines similar events into a single summarized event, sacrificing detail only when necessary.

4.3 Physical components

To learn about the physical components of Tivoli Security Information and Event Manager we want to separate this topic into two sections covering the *security* and *functional* views.

For the security point-of-view, we discuss the centralized user management option with the Tivoli Directory Server based LDAP, and from the functional point of view, we discuss the various types of servers, the agent, and the different compliance modules based on the main logical components, as explained in 4.1, “Logical components” on page 54.

4.3.1 Centralized user management using LDAP

While defining the Tivoli Security Information and Event Manager topology and the type of servers (Log Management, Standard, and Enterprise) to be included in a solution, also consider a centralized user management option. This configuration can be implemented using the IBM Tivoli Directory Server, which is based on the Lightweight Directory Access Protocol (LDAP). Tivoli Directory Server gets deployed as an optional component during the Tivoli Security Information and Event Manager installation. You must carefully plan the type of configuration and role assignments because there is no roll back option.

You can manage, for example, create, modify, and delete, user IDs using the Tivoli Security Information and Event Manager user management task.

To utilize the centralized user management option, a *Security Group* is created. This Security Group is a logical concept that includes at least one *Security Server* and one or more *Grouped Servers*.

4.3.1.1 Security Server

The Security Server is a Tivoli Security Information and Event Manager server where the Tivoli Directory Server software is installed. This server provides the user repository and entitlement center, and it authenticates the other servers within the Security Group.

The Security Server role can be assigned to any type of server, Log Management, Standard Server, or Enterprise Server. Decide the type of server prior to the initial deployment because there is no roll-back procedure; instead, you must reinstall the software to choose another option.

4.3.1.2 Grouped Server

A Grouped Server is any Tivoli Security Information and Event Manager server that is a member of a Security Group but is not the Security Server of that group. During the installation of a Grouped Server, you can specify which Security Server to use for authentication and authorization.

4.3.1.3 Cluster and Security Group relationship

In large scale environments, where two or more Tivoli Security Information and Event Manager clusters are deployed, one single Security Server can serve as a Centralized User Management server.

One Tivoli Security Information and Event Manager cluster does not restrict centralized user management to one Security Group. Take time to investigate the multi-cluster environment with a single Security Server, which we show in Figure 4-15 on page 80.

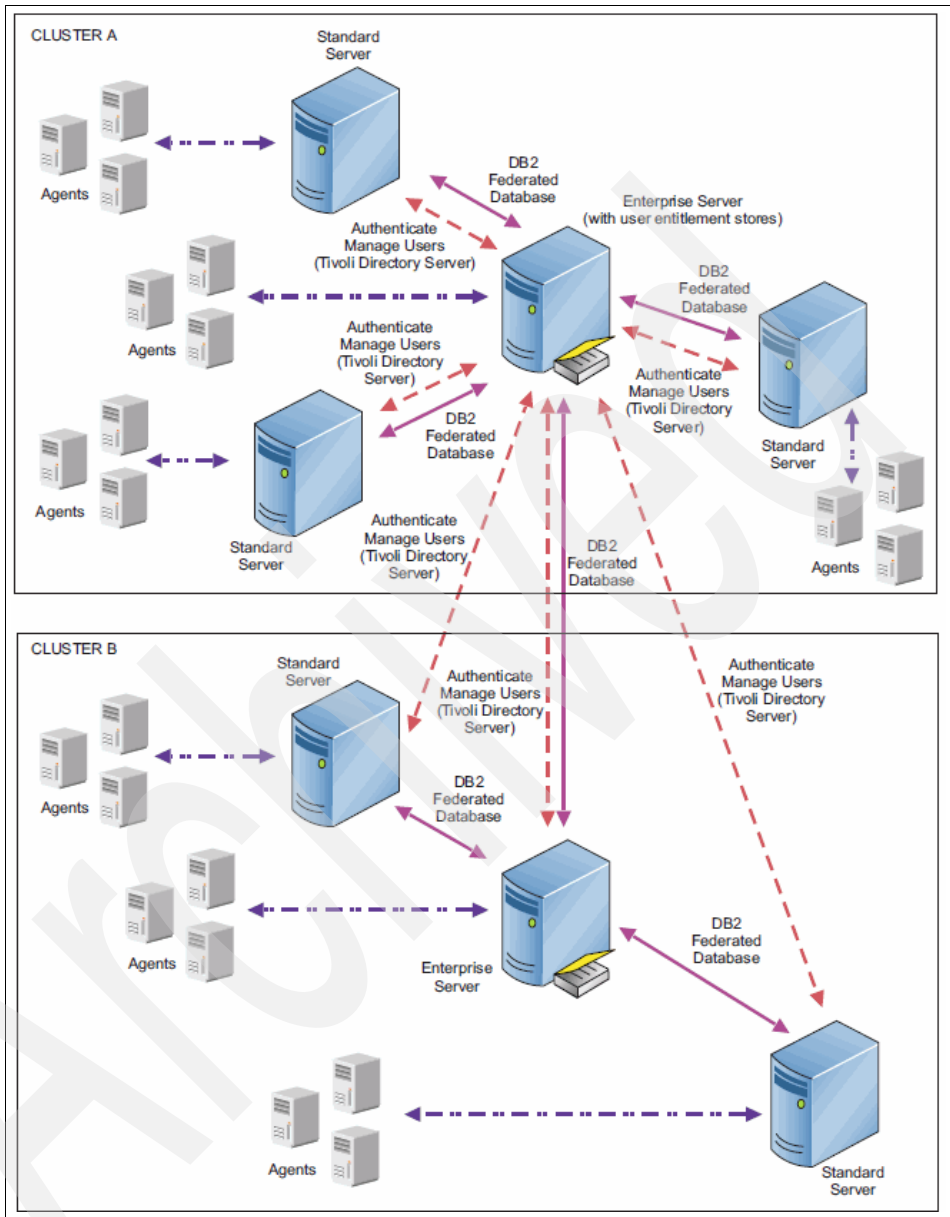


Figure 4-15 Multi-cluster environment with single Security Server

4.3.2 Functional components

From a functionality view, the Tivoli Security Information and Event Manager server software is divided in a number of separate components, total of four, which can be deployed in multiple combinations on one or more physical machines. Each component delivers a set of functionality. These components are:

- ▶ Log Management Base
- ▶ Normalization
- ▶ Forensics
- ▶ Consolidation

Log Management Base

The *Log Management Base* component encompasses the basic functionality that is needed to collect chunks, store them in the Depot, and monitor this process.

Normalization

The *normalization* component extends the functionality of the Log Management Base with log normalization and security policy matching. This component contains the mappers, policies, alert management, and report distribution element. It also allows you to view the normalized data and provides GUIs to administrate the normalization and the policy. The normalization component also adds trend analysis and activity reports.

Forensics

The *forensics* component can be placed on top of the Log Management Base and adds log management functionality to the Tivoli Security Information and Event Manager deployment, such as the indexer and searcher, which provide reporting over the data inside the collected chunks. The forensics component also adds the centralized log management DB so that Log Manager reports from multiple Tivoli Security Information and Event Manager servers can be viewed in a single report.

Consolidation

The *consolidation* component can be placed on top of the normalization component. It provides consolidation of the trend analysis data so that trend reports from multiple Standard Servers can be viewed in a single report.

Figure 4-16 on page 82 depicts these components in the context of the various server types.

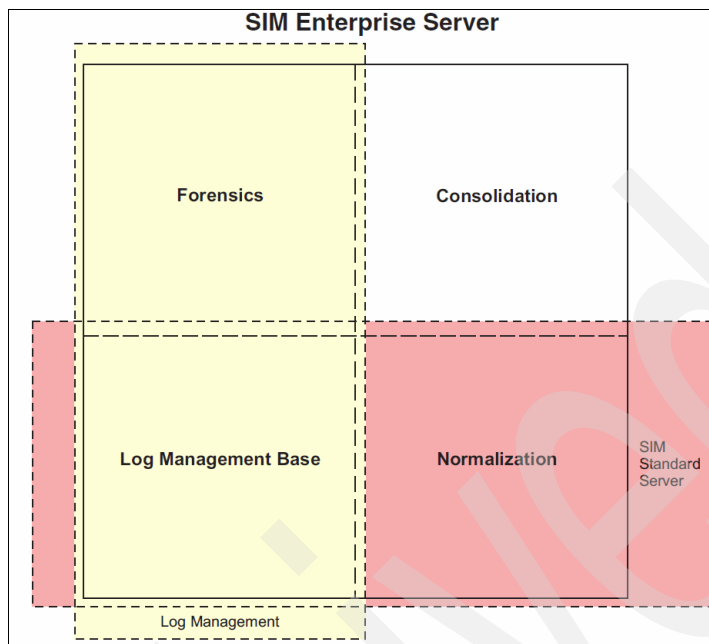


Figure 4-16 Relationship between components and types of servers

4.3.3 Server types

The combination of the four components shown in Figure 4-16 yields three types of servers.

- ▶ Log Management Server
- ▶ Standard Server
- ▶ Enterprise Server

Log Management Server

The *Log Management Server* is composed of the Log Management Base and forensics component. It provides all log management functionality, including log collection, log storage, log retrieval, forensic search, and log management reports.

Data is stored in the Depot where it is indexed for future queries that can be executed for forensic purposes against the raw data.

The Log Management Server also ensures the completeness and continuity of data collection and demonstrates the effectiveness and control by providing *collect history* and *continuity* reports.

Standard Server

The *Standard Server* is composed of the Log Management Base and normalization component. It provides log collection, log storage, log retrieval, W7 normalization and compliance reporting.

Compliance Modules, such as Sarbanes Oxley and PCI DSS, can be deployed along with this type of server.

The Standard Server's strength is focused on the W7 component and its reporting capabilities. Alerts can be sent in case any high severity security event is detected.

Enterprise Server

The *Enterprise Server* is composed of the entire four components: Log Management Base, normalization, forensics, and consolidation component. It provides all Log Management Server functionality and all W7 normalization and compliance reporting.

In environments with low volumes of data, one single Enterprise Server can potentially be used for all of the functionalities—up to 15 GB of original log data collection per day is considered manageable. Beyond that point, use a dedicated server for forensics and consolidation components. This kind of Tivoli Security Information and Event Manager deployment is considered a *cluster*. A preliminary analysis of the deployment environment typically dictates the required quantity and type of servers.

While you are investigating other IBM materials, such as the *IBM Tivoli Security Information and Event Manager Version 2.0 Administrators Guide*, SC23-9688 or *IBM Tivoli Security Information and Event Manager Version 2.0 Installation Guide*, GI11-8778¹, you might encounter two other terms:

- ▶ Log Management Module

The *Log Management Module* is referring to a Log Management Server type that, as mentioned before, is composed of the Log Management Base and forensics components and can be deployed as a stand-alone solution.

- ▶ SIM Module

The *SIM Module* provides after-the-fact policy-based analysis and compliance reporting on the event logs that are collected by the Log Management Base component. The SIM Module consists of the Log Management Base and normalization components.

¹ The online documentation for Tivoli Security Information and Event Manager is located at: <http://publib.boulder.ibm.com/infocenter/tivohelp/v2r1/topic/com.ibm.tsiem.doc/welcome.html>

In other words:

- ▶ The Log Management Server is itself a Log Management Module.
- ▶ The Standard Server is itself a SIM Module.
- ▶ The Enterprise Server is a Log Management Module and SIM Module altogether.

Be aware as you read, and distinguish between the words *Module* and *Component*.

During the installation of Tivoli Security Information and Event Manager, the embedded WebSphere Application Server (eWAS), the Integrated Solution Console (ISC), the Tivoli Integrated Portal (TIP), which is based upon the ISC and eWAS, IBM DB2, and Tivoli Directory Server are automatically configured for use with Tivoli Security Information and Event Manager.

4.3.4 Agent

To establish *event monitoring* in Tivoli Security Information and Event Manager, you must deploy one or more end points. After Tivoli Security Information and Event Manager is installed, you have the capability for across-the-board activity monitoring in your network environment.

Tivoli Security Information and Event Manager supports agent-based collection on Microsoft Windows, HP-UX, Sun Solaris, IBM AIX, and IBM z/OS systems.

After an agent is installed on a platform, Tivoli Security Information and Event Manager can collect from one or more agents, for example, an agent running on a Windows system can collect data from the operating system, Microsoft Exchange, and Oracle applications that are running on the system at the same time.

AIX agent as Syslog and SNMP collector

Tivoli Security Information and Event Manager can support up to 30,000 transactions per second (TPS). Every transaction represents one collected event that originates from either Syslog or SNMP sources. This agent must be installed on an AIX machine.

Definition: An *event source* can be a database, an application, an operating system, a network device, or any other IT-related platform that records its events in logs and to which Tivoli Security Information and Event Manager has access to collect a selection of security-relevant logs for event monitoring and reporting.

4.3.5 Compliance modules

From the boardroom to information technology departments, rules and regulations are placing ever-increasing demands on organizations of all sizes. In the middle are IT security managers and auditors who face the overwhelming task of understanding the regulations and implementing a wide array of compliance measures.

Tivoli Security Information and Event Manager has plug-in Management Modules available that provide optionally installable sets of capabilities to allow you to monitor and maintain compliance with a selected standard. These modules include sample policies and compliance report templates to assist you to meet regulatory requirements.

Regulations underscore the need to understand who is touching the most crucial corporate data and whether this behavior complies with security policy. You can use Tivoli Security Information and Event Manager to monitor all security events and audit them versus security policy:

- ▶ SOX
- ▶ FISMA
- ▶ HIPAA
- ▶ PCI DSS
- ▶ BASEL II
- ▶ GLBA
- ▶ ISO 17799
- ▶ ISO 27001
- ▶ COBIT
- ▶ NERC

4.4 Deployment architecture

In this section, we discuss the ways to deploy Tivoli Security Information and Event Manager and cover the following aspects:

- ▶ Log Management Server configuration
- ▶ Single server configuration
- ▶ Cluster configuration

4.4.1 Log Management Server configuration

The *Log Management Server* receives events and collects logs, which are stored in the Log Management Depot ready to provide log management reports and Depot investigation, also known as forensic search.

This server is typically used by organizations that only need to collect the data and prove to auditors that logs are continuously archived without any interruptions. In these situations further log data normalization is not required (W7 reports).

In a larger scale environment, multiple Log Management Servers might be necessary to handle the log file indexing workload. In these cases, the organization can choose to either run each Log Management Server independently, with its own user management, or configure the servers to use a centralized user management using LDAP, which requires a Security Group configuration.

4.4.2 Single server configuration

On a small business scale, deployment of a single Tivoli Security Information and Event Manager server can suffice to audit all of the IT systems. This single *Standard Server* contains all of the Tivoli Security Information and Event Manager product components and required middleware.

You must investigate the number of end points and the amount of data that those end points generate on a daily basis to ascertain if a single server is sufficient to fulfill the audit requirements. A single server can also be a starting point to a larger deployment that might end up in a cluster configuration, which we explain in the next section.

4.4.3 Cluster configuration

Medium-to-large environments might require the deployment of more than one Tivoli Security Information and Event Manager server that are logically connected. This type of deployment is considered a *cluster*.

A typical cluster configuration can consist of one Enterprise Server and up to three Standard Servers, where the Standard Servers are *attached* to the Enterprise Server.

The segregation of roles in a Tivoli Security Information and Event Manager cluster focuses the Standard Servers on log collection, W7 normalization, and compliance reporting, where the Enterprise Server is focused on forensics, consolidation, and log management of the entire cluster.

The log management reporting and consolidation functions for the cluster are located on the Enterprise Server.

In a cluster environment, it is not recommended that the Enterprise Server collects data from end points; instead, Standard Servers fulfill this role.

A cluster configuration can reduce your operational overhead, and it can provide a single view for auditors to examine the complete log history. Figure 4-17 illustrates a typical cluster configuration.

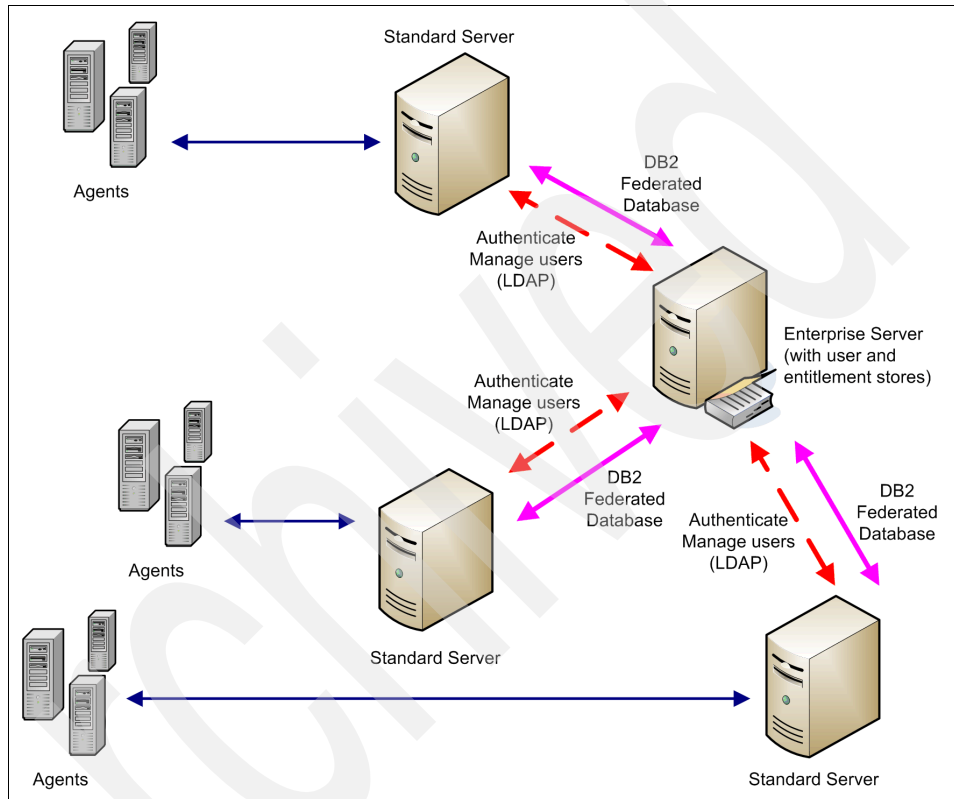


Figure 4-17 Typical cluster configuration

4.5 Conclusion

Tivoli Security Information and Event Manager gathers audit information from across the organization and compares activity to the acceptable use policies that both your organization and regulators define. The core of Tivoli Security Information and Event Manager is based on a secure, reliable, and robust log collection engine that supports effective, complete log collection, and fast, efficient query and retrieval.

By focusing on security from the inside, it uses the W7 methodology (Who, did What, on What, When, Where, Where from, and Where to) to consolidate, normalize, analyze, and report on vast amounts of user behavior and system activity. As a result, organizations can reveal quickly and easily who touched what within the organization (with alerts and proactive reports) and compare that activity to an established internal policy or external regulations.

Numerous organizations rely on the policy-based approach of Tivoli Security Information and Event Manager to simplify the process of monitoring the activities of privileged users, such as administrators and outsourcers, which improves security auditing, compliance monitoring, and enforcement for heterogeneous environments that range from super servers to the desktop.



Compliance management solution design

In this chapter, we discuss Tivoli Security Information and Event Manager solution design from two aspects.

In the context of the implementation process, we first discuss the functional design and configuration, which is directly related to the functional requirements. Next, we discuss the aspects of Tivoli Security Information and Event Manager solution design that are related to operational aspects of implementing and maintaining Tivoli Security Information and Event Manager deployment, such as monitoring and maintenance, archiving and information retention, performance, and scalability.

5.1 Functional design and configuration

In this section, we discuss Tivoli Security Information and Event Manager solution design as an important part of and in the context of the Tivoli Security Information and Event Manager implementation process. We do not go into details of the Tivoli Security Information and Event Manager implementation process here; instead, we cover this topic briefly as a part of the big picture.

Tivoli Security Information and Event Manager provides visibility into your security posture, controls the cost of demonstrating compliance, and reduces the complexity of managing a heterogeneous IT infrastructure through using centralized log management, event correlation, a policy compliance dashboard, and a reporting engine.

The Tivoli Security Information and Event Manager Version 2.0 Installation Guide, GI11-8778-00, provides a high-level overview of the Tivoli Security Information and Event Manager installation process with detailed instructions for deploying the Tivoli Security Information and Event Manager system components and configuring the network environment. In addition, that publication explains how to upgrade from IBM Tivoli Compliance Insight Manager 8.5.

So, what does it take to implement Tivoli Security Information and Event Manager from start to finish? The process is fairly simple and consists of four key phases:

- ▶ Discovery and analysis
- ▶ Project definition and planning
- ▶ Implementation
- ▶ Product use

The most critical piece of information that is needed for any successful implementation are the reporting requirements. These requirements tell you what data you need to capture and report on which leads you to the overall amount of data that you to collect on a daily basis, how much hardware you need, and so on. Based on this information, you can design and size your solution.

We describe each phase of the implementation in more detail in the following sections.

5.1.1 Phase 1: Discovery and analysis

In this first phase, you:

- ▶ Analyze and evaluate reporting requirements
- ▶ Discover and learn about the implementation environment
- ▶ Provide audit settings that support reporting requirements for every event source on every platform

Reporting requirements

You identify the reports that you need based on specified objectives in terms of regulatory compliance, internal security policies, operational efficiency, audit concerns, and so on. The design approach, based on risk assessment, addresses *privileged user monitoring and auditing* first, and then expands the solution to address other objectives.

Risk assessment: A *risk assessment* takes into account the sensitivity and criticality of the data and defines the assets that can be considered *high risk*. The risk assessment, therefore, must be controlled. The controls put into place for these assets are most important and must be addressed first, if possible, by Tivoli Security Information and Event Manager. The set of administrative or high privilege accounts form an asset that has high priority.

To meet reporting requirements, you also must:

- ▶ Identify collection types (near-real-time or batch).
- ▶ Decide on information grouping (by geographic location, platform, business unit, and so on).
- ▶ Specify the time frame for data to be maintained in the Log Management Depot (for example, one, two, or three months or years) and in the Reporting Database (GEM), for example, from one-to-seven days.
- ▶ Determine the time frame (for example, one, two, or three months or years) and location (for example, SAN or DVDs) to archive the data.

Installation environment

You must assess and document the computing environment to prepare for the Tivoli Security Information and Event Manager implementation. Identify existing audit settings (if fine tuned, not to generate excessive amount of log data), data capture, and network topology (communication settings, firewalls, locations, and so on) to identify solution constraints or limitations, estimated log volume, data storage (type and location), and so on.

Audit settings

You must specify the audit data that you must collect to support the reporting requirements. The audit settings that are used are always a trade-off between security and system performance and the disk space that is used. In most cases, auditing every single action is not an option. Thus, you analyze the audit subsystem and determine, evaluate, and document or provide audit settings that support the reporting requirement for every event source on every supported platform, for example, in the Windows audit subsystem, all logons on the platforms are captured by the audit categories *account logon* and *logon*. To generate the same report on Solaris, you must activate the audit class *lo* in the system-wide audit file.

Figure 5-1 and Figure 5-2 on page 93 illustrate a basic example of the Windows audit settings that are required for privileged user monitoring and auditing reporting on actions performed by IT administrators. Examples of actions that are performed by IT administrators are creating, modifying, or deleting administrator accounts and password resets, logon and logoff successes and failures, and so on.

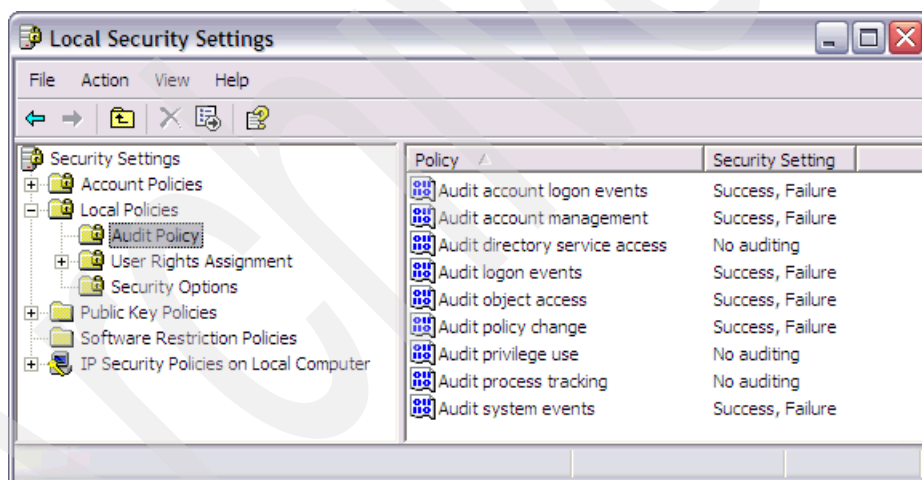


Figure 5-1 Privileged user monitoring and auditing Audit Policy settings

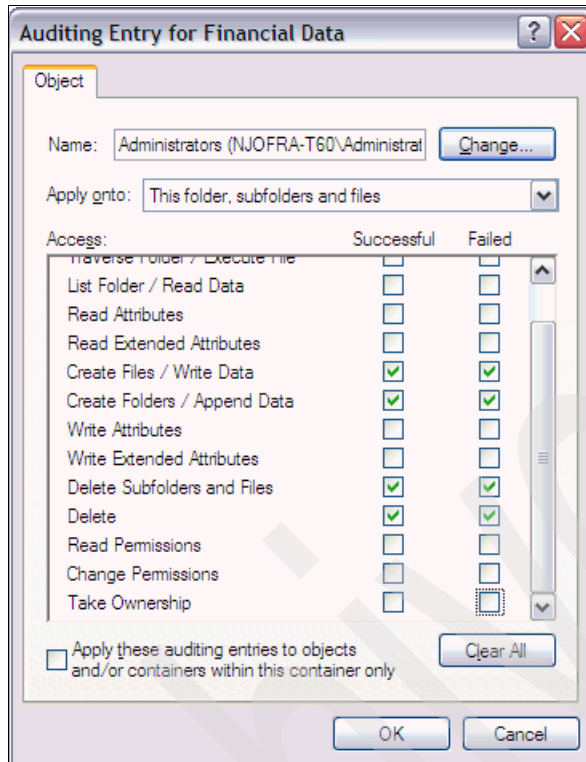


Figure 5-2 Privileged user monitoring and auditing Object Access settings

We suggest three levels of default auditing for Windows:

- ▶ *Low setting* on production systems where performance and disk space are critical.
- ▶ *Medium setting* in most other cases.
- ▶ *High setting* on servers that contain confidential data and object access auditing for the directories that contain the confidential data.

For more details about Windows audit recommendations from Microsoft and independent third party and auditing configuration for all supported event sources, see *Tivoli Security Information and Event Manager Version 2.0 Installation Guide, G111-8778*.

We provide more details about various audit settings in our scenario in the second part of the book starting in Chapter 8, “Basic auditing” on page 151.

5.1.2 Phase 2: Project definition and planning

At this point, you:

- ▶ Acquired base information from discovery and analysis about reporting requirements, the installation environment, and audit settings.
- ▶ Next, you implement a pre-planning worksheet, based on target platforms (with server names, platforms and versions, daily log sizes, server location, database groupings, and so on).
- ▶ Then, you define a draft project plan with an initial project schedule, reporting requirements, and installation environment information. This plan is based on the typical Tivoli Security Information and Event Manager implementation design architecture (number and location of Tivoli Security Information and Event Manager servers, hardware specifications, and so on) and installation prerequisites (software and platform versions, audit settings, ports, and protocols that are needed to install Tivoli Security Information and Event Manager).

The Tivoli Security Information and Event Manager implementation design architecture is a result of information that is gathered in previous phases, product capabilities, and planning. Therefore, for a successful implementation, it is very important that we discuss project definition and planning in more detail in the next subsections.

We explain general logical (conceptual) and physical (system) architecture in the Tivoli Security Information and Event Manager product documentation and in Chapter 4, “IBM Tivoli Security Information and Event Manager component structure” on page 53. In this section, we focus on the various design layouts and the reasons behind those layouts. We start with functional design and configuration.

Design and configuration

There are common network models for security architectures where components with similar security requirements are grouped into zones. Using Figure 5-3 on page 95, think of these areas as uncontrolled, controlled, restricted, secured, and externally controlled. A client uses the network to access applications and data. This client can be from either within your organization or outside of it.

Firewall: In Figure 5-3 on page 95, the breaks between each network zone indicate the use of a firewall that clearly delineates each perimeter from the next.

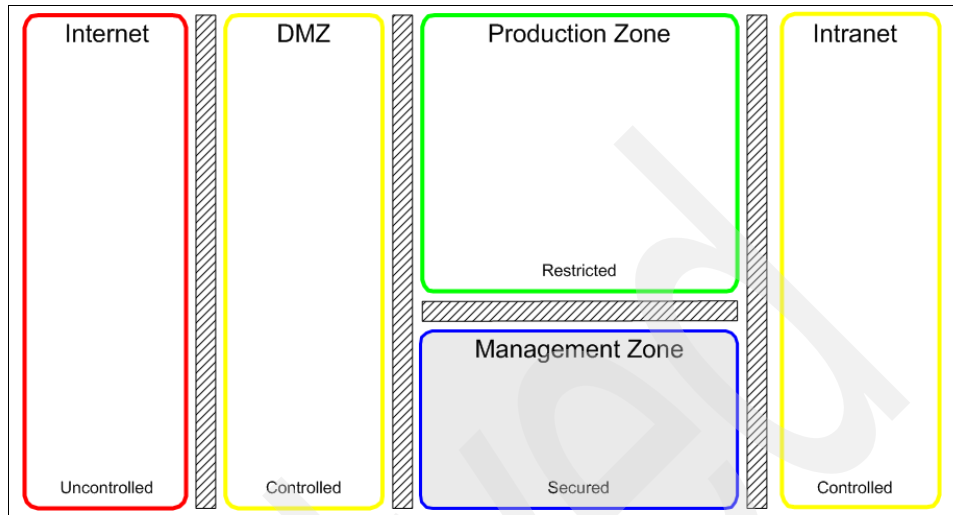


Figure 5-3 Network zone concept

Using this concept you can translate Figure 5-3 into a more targeted deployment decomposition, as shown in Figure 5-8 on page 98.

Tivoli Security Information and Event Manager supports up to eight audit configurations, as shown in Figure 5-4 on page 96 through Figure 5-7 on page 97, where dashed lines represent the system boundary. The layout of Tivoli Security Information and Event Manager components, data flow from audited system to server, and the control of data flow from audited to target system define the actual audit configuration.

Note: The number of audit configurations supported on a specific platform varies from one event source to another.

This configuration is sufficient for auditing multiple event sources on systems that run unlike operating systems. For more information about deploying Tivoli Security Information and Event Manager event sources, see *IBM Tivoli Security Information and Event Manager Event Source Guide, SC23-9687*.

Figure 5-4 on page 96 shows the audit configuration with all components separated.

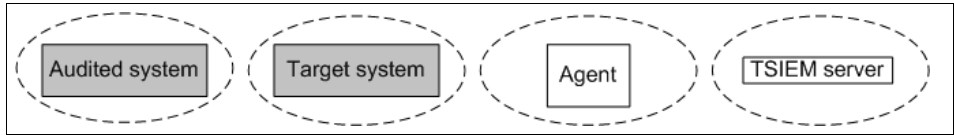


Figure 5-4 Tivoli Security Information and Event Manager audit configuration 1

Figure 5-5 shows audit configurations where either left, middle, right or left, and right pair of components share the same system.

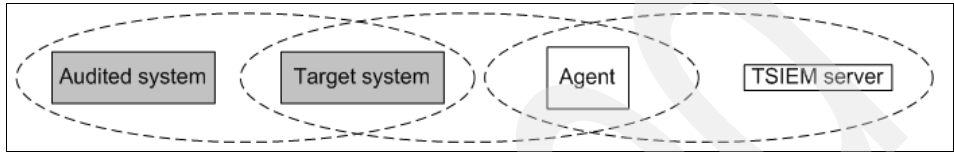


Figure 5-5 Tivoli Security Information and Event Manager audit configurations 2, 3, 4, and 5

Agents: The Tivoli Security Information and Event Manager Enterprise Server can act as an agent in configurations. If this is the case, no agent needs to be installed, because it is already included in the server installation. Otherwise, you must install an agent that corresponds to the operating system that runs on the agent.

Note: The audited system can act as the target system for event sources.

Figure 5-6 shows audit configurations where only the audited system or the server is on its own system.

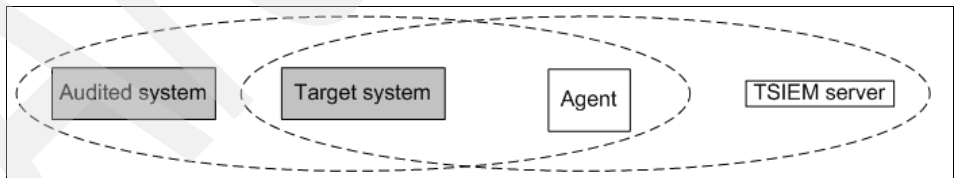


Figure 5-6 Tivoli Security Information and Event Manager audit configurations 6 and 7

Figure 5-7 on page 97 shows the simplest audit configuration with all components on the same system.

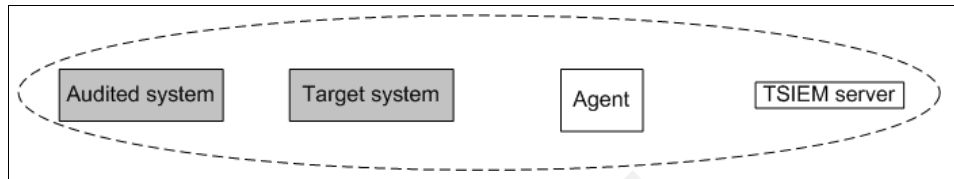


Figure 5-7 Tivoli Security Information and Event Manager audit configuration 8

To exchange information among its components, Tivoli Security Information and Event Manager uses a network of agents that maintain encrypted communication channels. This network runs on the TCP/IP layers of the existing organizational network.

The actual collection process can involve multiple mechanisms in a variety of configurations. A system audited through remote collect does not need to run the Tivoli Security Information and Event Manager software. Instead, event data is forwarded to the server by an agent with direct access to the audited system. To audit several systems in a Windows domain, only one must be configured as an agent and have an Actuator installed. For more information about Tivoli Security Information and Event Manager concepts and typical configurations, see the *IBM Tivoli Security Information and Event Manager Version 2.0 User Guide*, SC23-9689.

In Figure 5-8 on page 98, we place components of Tivoli Security Information and Event Manager into separate network zones to show many, but not all, possible audit configurations and collect mechanisms.

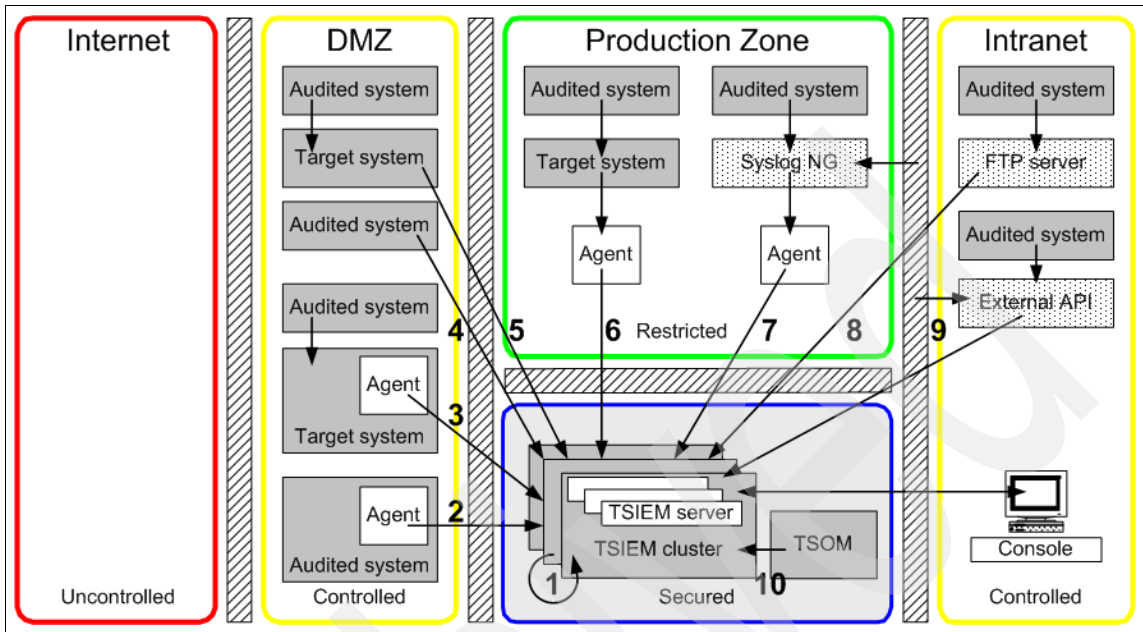


Figure 5-8 Tivoli Security Information and Event Manager deployment options

For Tivoli Security Information and Event Manager to operate, at a minimum the database engine and one server must be deployed. Optionally, one or more servers can be added to enhance storage and logging capabilities. The server component must be placed into the management zone because chunks are stored there and they are the most important asset because they hold crucial data for any forensic or reporting activity.

Agents can be located in other network segments to suite the performance and scalability needs and requirements of direct or remote data collection from audited systems.

Let us explain the examples of possible audit configurations and collect mechanisms, numbered from 1 to 10, in Figure 5-8:

1. Example 1 shows the most simple collect configuration. The agent and the audited instance of the event source are located on the server system. In other words, Tivoli Security Information and Event Manager collects data directly from the server itself. Tivoli Security Information and Event Manager controls the transfer of data.
2. Example 2 shows a configuration where the agent and the audited instance of the event source are located on the same system, and the server is hosted by

another system. In other words, Tivoli Security Information and Event Manager collects data directly from an agent (not equal to server).

3. Example 3 shows a configuration that is similar to the previous one, but this time the user arranges to transfer data from an audited system to an agent (not equal to server), where the data is collected.
4. Example 4 shows the remote collection for a Windows configuration, where the audited instance of the event source is hosted by a system other than the agent, and the server system acts as an agent for this event source. In other words, Tivoli Security Information and Event Manager collects data directly from a remote system. The *remote collect* does not require a running agent on the audited system. Remote collect involves a remote data retrieval mechanism from an independent vendor. The most common configuration is used for event sources that are based on the Windows log mechanism using the Windows event management API.
5. Example 5 shows SSH collect, similar to the previous example, but this time the user arranges to transfer data from the audited system to a remote target system (not equal to server), from where the server collects the data. SSH collect is another variation of remote collect. It can be used with event sources that are based on UNIX and Linux. The configuration is similar to Windows remote collect; however, the data retrieval mechanism utilizes an SSH connection from the agent to the audited system.
6. Example 6 shows Syslog and SNMP collection—the Tivoli Security Information and Event Manager capability to process and analyze security events that are collected through the Syslog and SNMP network logging mechanisms. To collect network events, a component listens in the network and receives all incoming events.

The Tivoli Security Information and Event Manager agent has a built-in listening component that can be activated on any Windows agent and can receive both SNMP and Syslog messages. The agent, server, and the audited instance of the event source are all hosted by distinct systems. In other words, Tivoli Security Information and Event Manager collects data that is directly from a remote audited system through an agent (not equal to server). When the target system component is also present, a user arranges the data transfer to a remote system (not equal to the agent), from where an agent (not equal to server) collects the data.

7. Example 7 is similar to the previous one, but for high volume Syslog processing, a Microsoft Windows-based receiver might not deliver the necessary performance. In these situations, you might want to use a Linux-based Syslog receiver that provides better performance, such as Syslog NG, which is an open source Syslog implementation.
8. Example 8 shows a custom collection mechanism FTP collect. If no other suitable collect mechanism is available, a script is scheduled on the platform

of the event source. The log data is put into a folder where it can be picked up by the agent.

9. Example 9 shows a collection using external APIs. Frequently, obtaining security event data involves using an API that has a specific API event source. Whenever such an API works across a network link, this action influences the configuration. A common example is auditing network appliances. A network appliance usually comes with a management console or other external component that interacts with it. That component also provides the API to obtain the event data.
10. Example 10 shows the integration with IBM Tivoli Security Operations Manager. We discuss the integration in more detail in Chapter 3, “Introducing the IBM Security Information and Event Management solution” on page 27.

Based on the various Tivoli Security Information and Event Manager deployment options that are shown in Figure 5-8 on page 98 and the various collect configuration examples, we can show what a small, medium, and large solution design might look like. We start with an example of a small solution in Figure 5-9.

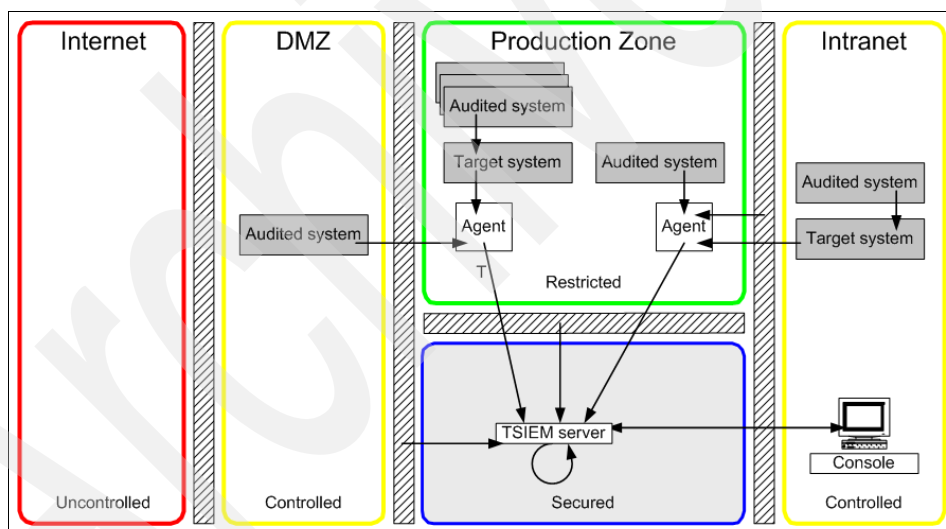


Figure 5-9 Small Tivoli Security Information and Event Manager deployment

A small Tivoli Security Information and Event Manager deployment is best suited for a homogenous environment. We assume a fairly simple environment with a small number of audited systems, which can all be monitored remotely. There is also no need for forensic log search capability, and Syslog performance is low. A single server deployment can handle all of the needs in such an environment.

For a more advanced environment with more audited systems and log forensics requirements, we design a cluster of servers for better performance and to implement log search capability. We also assume that the environment is heterogeneous. Thus, we cannot cover all audited systems remotely any more but must implement certain agents with Actuators.

Figure 5-10 illustrates how a medium Tivoli Security Information and Event Manager deployment might look.

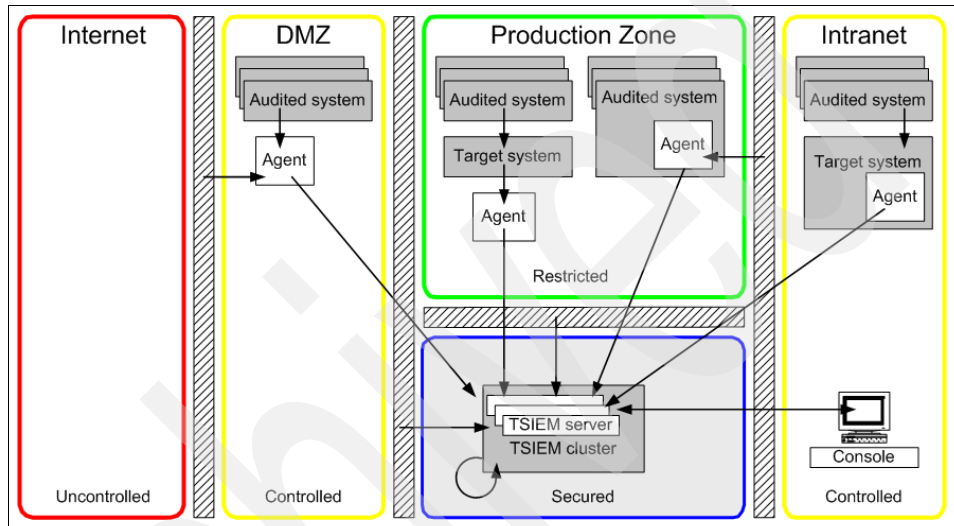


Figure 5-10 Medium Tivoli Security Information and Event Manager deployment

Most demanding environments can involve multiple heterogeneous environments with high performance, availability, and scalability requirements, communication across dispersed locations, and so on. Figure 5-11 shows one possible Tivoli Security Information and Event Manager deployment for such requirements.

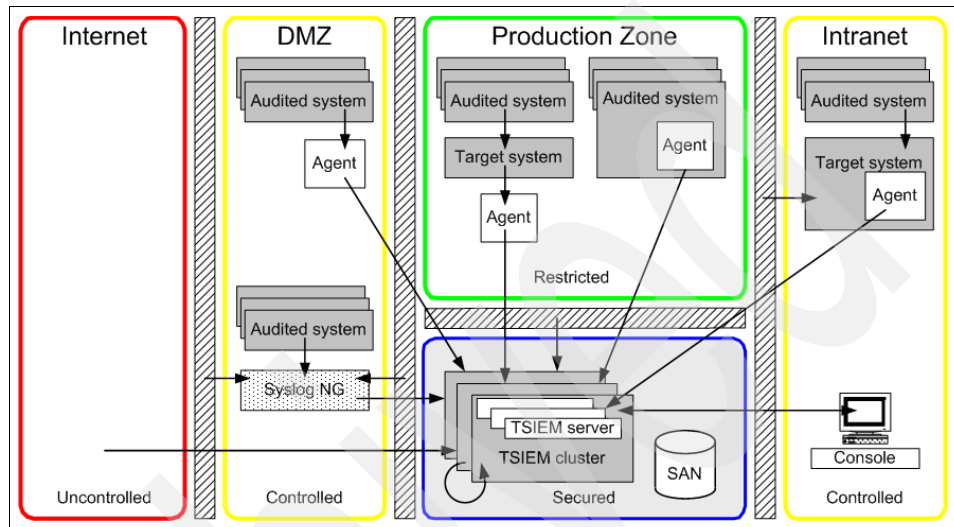


Figure 5-11 Large Tivoli Security Information and Event Manager deployment

For high scalability and performance, there are multiple clusters deployed with multiple agents serving multiple clusters. As shown in Figure 5-11, with the line coming from the Internet zone, there is consolidation among several locations and regions in place. For high Syslog performance, the Syslog receiver is implemented in the DMZ zone. For high availability, all Tivoli Security Information and Event Manager servers are connected to a Storage Area Network (SAN).

We discuss the design approach for our specific scenario in more detail in the second part of the book in 7.3, “Design approach” on page 140.

5.1.3 Phase 3: Implementation

Before you begin the implementation, verify that the recommended audit settings are in place and that all systems are configured as suggested in the prerequisites (verify Tivoli Security Information and Event Manager servers hardware, software and platform versions, audit settings, TCP/IP connectivity, and so on).

Implementation steps

Here is a simple outline of the implementation steps:

1. Install servers.
2. Install necessary agents per platform type.
3. Activate the event sources.
4. Activate auditing for all event sources.
5. Collect and load the data.
6. Build the W7 model, policy, and attention rules.
7. Configure the alerts.
8. Create or code the reports.
9. Configure report distribution.
10. Repeat step 6 to 7 for all reports, per event source.

For details about the product installation and configuration, see the *IBM Tivoli Security Information and Event Manager Version 2.0 Installation Guide*, GI11-8778.

We discuss the implementation approach for our specific scenario in more detail in the second part of the book in 7.4, “Implementation approach” on page 143.

5.1.4 Phase 4: Product use

During the product use phase, you face the security improvement cycle. In this cycle, you monitor and adjust the policy exceptions for improvement. The effectiveness of the controls is reported and translated back to the security objectives. Policies and reporting are adjusted constantly to reflect changes in the organization or changes of assets. Policies are fine tuned to eliminate events that belong to normal processes. Groups are modified on an as-needed basis and all changes and settings are documented.

5.2 Operational design and configuration

In this section, we discuss the aspects of Tivoli Security Information and Event Manager solution design that are not directly related to the functional requirements. We present the considerations to take into account when designing the non-functional and operational aspects of implementing and maintaining Tivoli Compliance Insight Manager deployment.

5.2.1 Monitoring, maintenance, and availability

In this section, we discuss general monitoring and maintenance procedures for Tivoli Security Information and Event Manager to verify the overall state of the environment on a daily, weekly, and monthly basis.

Daily checks

On a daily basis, all logons to the system and the status of the collected data must be verified.

Logon

You login to the Tivoli Integrated Portal of the Tivoli Security Information and Event Manager by providing the following URL:

`http://hostname/ibm/console` or `https://hostname/ibm/console`

In the URL, host name is the name or the IP address of the system where Tivoli Security Information and Event Manager Server is installed. The Tivoli Integrated Portal supports both HTTP (Hypertext Transfer Protocol) and HTTPS (Hypertext Transfer Protocol Secure) for transmitting data to the Web browser.

The Tivoli Integrated Portal is displayed, as shown in Figure 5-12.

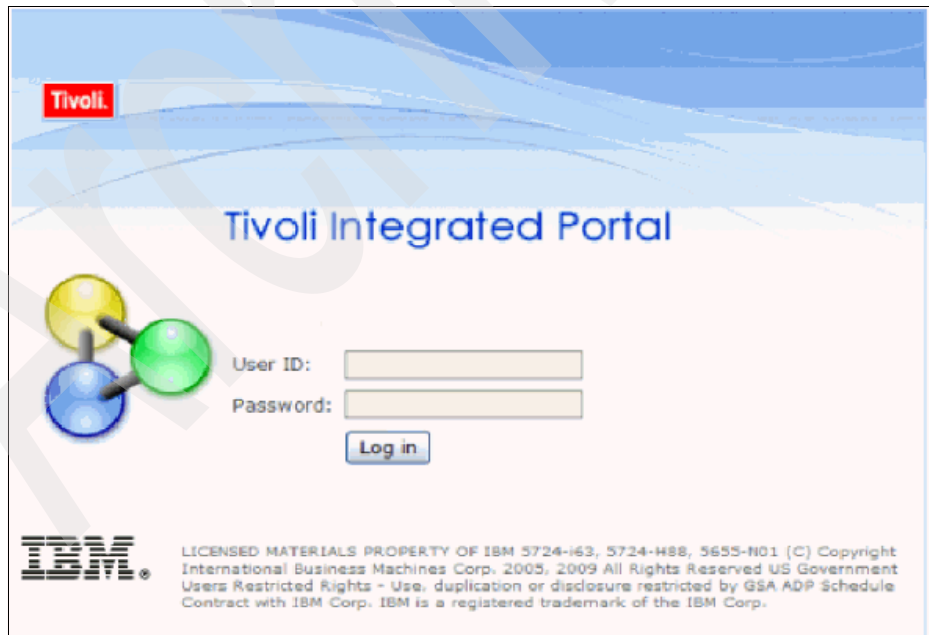


Figure 5-12 The Tivoli Integrated Portal logon window

To successfully logon to the Tivoli Integrated Portal:

1. In the User ID field, enter your user ID.
2. In the Password field, type your password.
3. Click **Log in**.

If the logon was successful, the Tivoli Security Information and Event Manager Welcome Page is displayed. If logon was not successful, verify that you entered the correct user ID and password.

When you finish using Tivoli Security Information and Event Manager, log out and close your Web browser session to maintain the security of the information.

Tivoli Security Information and Event Manager components and functions are protected by user roles, which govern the permissions that a user has. Specific user roles are required to view the user interfaces and perform administrative functions. If you do not have the appropriate user role, you cannot view certain Tivoli Security Information and Event Manager components or perform certain tasks.

Ask the administrator to verify that you have the necessary user roles. For more information about user roles, see the "Configuring Users" chapter in the *IBM Tivoli Security Information and Event Manager Administrators Guide Version 2.0*, SC23-9688.

The Tivoli Security Information and Event Manager user interface

The Tivoli Integrated Portal is organized into two sections:

- ▶ The navigation panel is on the left side of the window.
- ▶ The main part of the window, on the right side, displays the Welcome page when you first log in to Tivoli Security Information and Event Manager.

The navigation panel allows you to open separate tools and pages in Tivoli Security Information and Event Manager. You can expand topics that have a bold typeface by clicking the (+) icon. When a topic is expanded, the icon changes to a (-) icon.

You can collapse expanded topics by clicking the (-) icon. You can adjust the relative size of the navigation panel or the main panel by sliding the divider to the left or to the right.

You can close or open the navigation panel by clicking the arrow on the divider. Figure 5-13 on page 106 shows the Tivoli Security Information and Event Manager Welcome page.

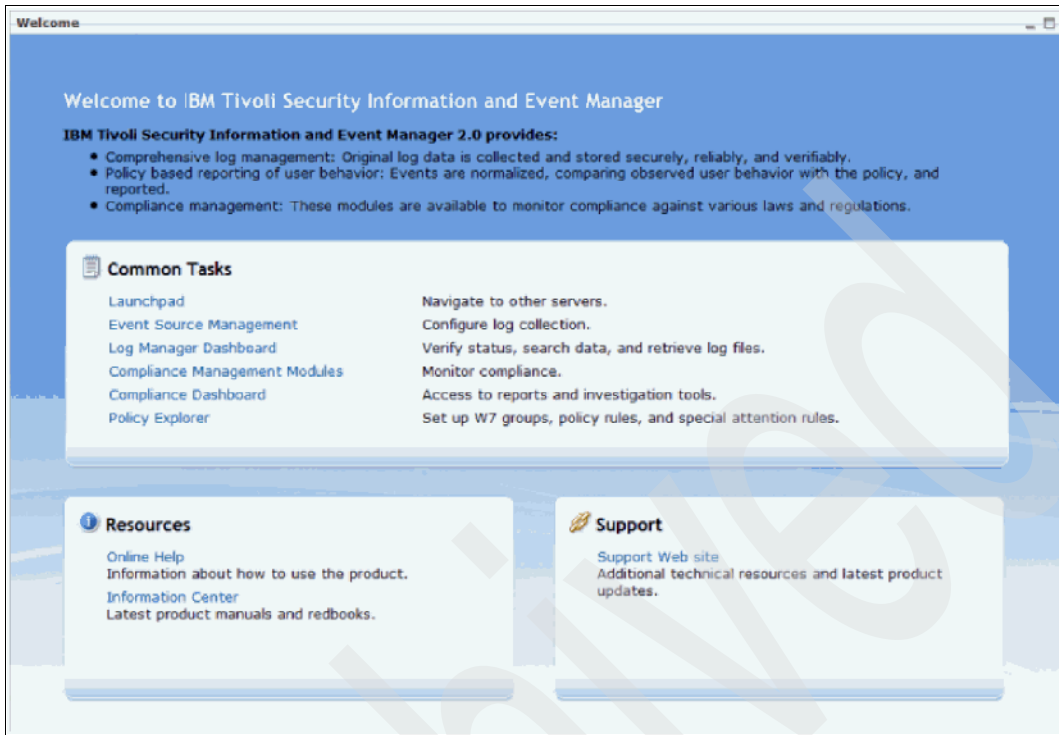
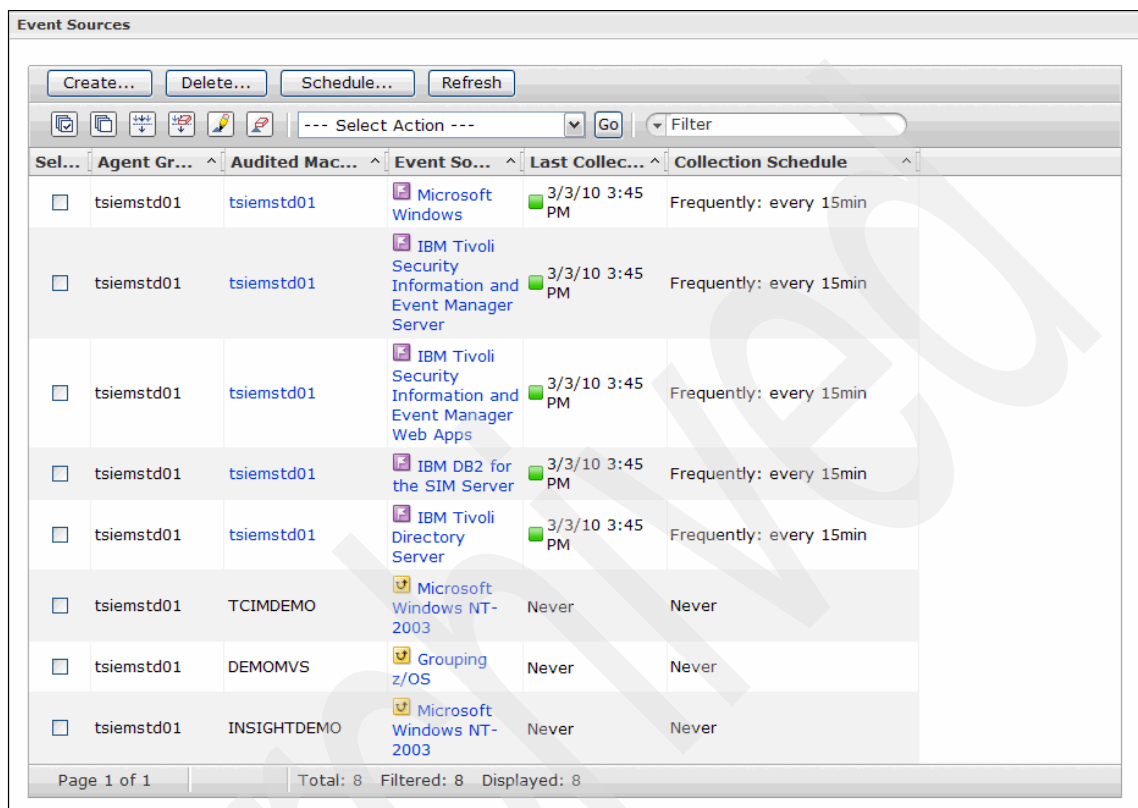


Figure 5-13 The Tivoli Security Information and Event Manager Welcome page

Data collection

To verify the data collection, check the time stamp in the Last Collect column. Figure 5-14 shows how a possible list can look.



Sel...	Agent Gr...	Audited Mac...	Event So...	Last Collec...	Collection Schedule
<input type="checkbox"/>	tsiemstd01	tsiemstd01	Microsoft Windows	3/3/10 3:45 PM	Frequently: every 15min
<input type="checkbox"/>	tsiemstd01	tsiemstd01	IBM Tivoli Security Information and Event Manager Server	3/3/10 3:45 PM	Frequently: every 15min
<input type="checkbox"/>	tsiemstd01	tsiemstd01	IBM Tivoli Security Information and Event Manager Web Apps	3/3/10 3:45 PM	Frequently: every 15min
<input type="checkbox"/>	tsiemstd01	tsiemstd01	IBM DB2 for the SIM Server	3/3/10 3:45 PM	Frequently: every 15min
<input type="checkbox"/>	tsiemstd01	tsiemstd01	IBM Tivoli Directory Server	3/3/10 3:45 PM	Frequently: every 15min
<input type="checkbox"/>	tsiemstd01	TCIMDEMO	Microsoft Windows NT-2003	Never	Never
<input type="checkbox"/>	tsiemstd01	DEMOMVS	Grouping z/OS	Never	Never
<input type="checkbox"/>	tsiemstd01	INSIGHTDEMO	Microsoft Windows NT-2003	Never	Never

Page 1 of 1 Total: 8 Filtered: 8 Displayed: 8

Figure 5-14 Tivoli Security Information and Event Manager data collection

The column shows the time of the oldest log record available in the last collected chunk. In normal conditions, the last collect time is a multiple of the collect schedule. Verify this information for each event source that has a collect schedule defined.

Database check

The database can be in one of the following four states, which you can check in the Management Console:

- ▶ Error
- ▶ Loaded
- ▶ Loading
- ▶ Cleared

The failure message and database contents are in the Tivoli Integrated Portal, as shown in Figure 5-15.

The screenshot shows the 'Status of the database' section with a database icon and a table of details. Below it is the 'Data in this database' section with a table of platform data.

Where (Platform)	Start time	End time	#Chunks	#Events
NWRD (z/OS)	Wed Aug 22 2007 00:10:00 GMT+00:00	Sat Aug 25 2007 00:10:00 GMT+00:00	2	585189

Figure 5-15 Tivoli Security Information and Event Manager database status

The *End time* for each platform shown in the Tivoli Integrated Portal is close to the latest scheduled collect that is relative to the *Last Load* time stamp in the Database View, as shown in Figure 5-16. If this is not the case, either the event source failed to collect the latest log records or no log records were produced between the end time and the collection time for that platform.

Compare the time in the Last Load column with the Load Schedule frequency. The last load time stamp is a multiple of the load frequency defined in the load schedule and as close as possible to the current time.

The screenshot shows a table with columns: Sel..., Database N..., Sta..., Audited Mach..., and Last Load. The table contains two rows: SELFAUDIT (Loaded) and QUANT (Not Loaded).

Sel...	Database N...	Sta...	Audited Mach...	Last Load
<input type="radio"/>	SELFAUDIT	Loaded	tciemstd01	3/3/10 12:00...
<input type="radio"/>	QUANT	Not Loaded		

Figure 5-16 Tivoli Security Information and Event Manager database load

Database load problems can occur during the three phases of preparing the reports in the GEM database:

- ▶ Mapping
- ▶ Loading
- ▶ Post-processing

Weekly checks

On a weekly basis, you must check disk space, Depot, and Tivoli Security Information and Event Manager services.

Disk space

The device where the Tivoli Security Information and Event Manager server is installed must have at least 25 GB of free space.

Depot

The time stamps of the latest collected chunks should be as close to the current time with relation to the defined collect schedules.

Services

All Tivoli Security Information and Event Manager services of startup type *Automatic* must be running. The Tivoli Security Information and Event Manager server service spawns additional tasks that you can see in the task manager.

In very rare cases it might be necessary to stop and restart the Tivoli Security Information and Event Manager services. Refer to the *IBM Tivoli Security Information and Event Manager Version 2.0 Troubleshooting Guide*, SC23-9690, and the *IBM Tivoli Security Information and Event Manager Version 2.0 Administrators Guide*, SC23-9688 for further information about how to manage services.

Configuration tasks

There are several tasks to be considered in a Tivoli Security Information and Event Manager environment.

Some of the tasks relate to synchronization between the Enterprise and the Standard Servers and others relate to the collection of data and generation of reports. The Standard Servers in a Tivoli Security Information and Event Manager cluster are responsible for collecting the log files and generating reports and alerts. Both collection and report generation are normally scheduled and managed through the Tivoli Integrated Portal.

Before you can configure any of these tasks, you must, after the installation, register the Standard Servers with the Enterprise Server and configure the schedule for the Consolidation Server to aggregate data. By performing these tasks, you enable the Enterprise Server to consolidate the data from all the Standard Servers in the Tivoli Security Information and Event Manager cluster.

You must register each Standard Server with the Enterprise Server so that the Enterprise Server can consolidate data from Standard Servers and perform centralized log management.

Before the Enterprise Server can consolidate data from the Standard Servers, the indexer and searcher processes in the Enterprise Server must have access to the depots of all Standard Servers in the cluster. Therefore, you must share the Depot of each Standard Server before you register that Standard Server with the Enterprise Server. Perform this step on the Enterprise Server for each Standard Server in the cluster.

Both, the *IBM Tivoli Security Information and Event Manager Version 2.0 Users Guide*, SC23-9689 and the *IBM Tivoli Security Information and Event Manager Version 2.0 Administrators Guide*, SC23-9688, provide more details about how to configure tasks, collect data, and generate reports.

Logs

In certain cases, you might not be able to solve a problem by troubleshooting the symptoms. In such cases, you must collect more diagnostic data. Before you begin to collect data for a problem report, install and run the IBM Support Assistant for best results. This troubleshooting tool includes a console that you can use to gather the required data. Refer to the *IBM Tivoli Security Information and Event Manager Version 2.0 Troubleshooting Guide*, SC23-9690, on how to install the IBM Support Assistant. This guide also shows you how to configure log file settings.

We discuss the following three types of log files, which are available when log tracing is enabled:

- ▶ Installation logs
- ▶ Message logs
- ▶ Trace logs

Installation logs

When Tivoli Security Information and Event Manager components are installed, the installation process creates log files.

The installation program creates log files in three locations:

- ▶ The installation graphical user interface (GUI) logs are called `TSIEM_install-*.log`. These logs are in the home folder of the user who installs Tivoli Security Information and Event Manager (for example, `C:\Documents and Settings\Administrator\TSIEM_install-00.log`).
- ▶ The main log file of the installation engine is located in `%TSIEM_HOME%_uninst\TSIEMInstall\plan\install\MachinePlan_localhost\logs`. The name of the main log file starts with `MachinePlan_localhost_` and is followed by a time stamp.
- ▶ When the installation program calls a subprogram, the resulting logs are written to `%TSIEM_HOME%\log` (for example, `C:\IBM\TSIEM2010\log`).

These installation logs are helpful in resolving any problems that you encounter during installation.

Message logs

Message logs are text files in which the operations of the system are recorded. The following types of messages are recorded by default:

- Informational messages** Indicates conditions that are worthy of noting but that do not require you to take any precautions or perform an action.
- Warning messages** Indicates that a condition was detected that you must be aware of but does not necessarily require that you take any action.
- Error messages** Indicates that a condition occurred that requires you to take action.

Using the Tivoli Integrated Portal, you can configure settings of the logs, such as the location, name, maximum size of the log files, and the levels of severity that you want to log.

By default *JVM message logs* are located in the following directory, where *install_location* is the location where Tivoli Security Information and Event Manager is installed. By default this is `c:\IBM\TSIEM:`

```
install_location\tip\profiles\TIPProfile\logs\server_name\SystemOut.log
```

IBM Service Log logs are installed in the following default location, where *install_location* is the location where Tivoli Security Information and Event Manager is installed. By default this is `c:\IBM\TSIEM:`

```
install_location\tip\profiles\TIPProfile\logs\server_name\activity.log
```

Console message logs are saved in the message log directories of the WebSphere Application Server node where the administrative console is installed.

Trace logs

Trace logging, or tracing, provides you with additional information relating to the condition of the system at the time a problem occurred. In contrast to message logs, where records are made of noteworthy events that occurred, trace logs capture transient information about the current operating environment when a component or application fails to operate as intended.

Trace logging is not enabled by default because in certain circumstances it can cause large amounts of data to be collected in a short amount of time and might result in significant performance degradation.

By default, the trace log is located in the following directory, where *install_location* is the location where Tivoli Security Information and Event Manager is installed. By default this is `c:\IBM\TSIEM`:

```
install_location\tip\profiles\TIPProfile\logs\server_name\trace.log
```

Console trace logs are saved in the trace log directories of the WebSphere Application Server node where the administrative console is installed.

Viewing logs

The format of the logs determines how they can be viewed:

▶ JVM logs

To view the JVM logs, you can use the WebSphere Application Server administrative console, which supports viewing from a remote machine, or use a text editor on the machine where the log files are stored. In the WebSphere Application Server Information Center for more information, search on viewing JVM logs.

▶ IBM service logs

The service logs are written in binary format. To view the log, you can use tools that are part of WebSphere Application Server. In the WebSphere Application Server Information Center for more information, search on viewing the service log.

▶ Trace logs

Trace data is generated as plain text in basic, advanced, or log analyzer format. On an application server, trace data can be directed to a file or an in-memory circular buffer. If the circular buffer is used, the data must be dumped to a file before you can view it.

5.2.2 Archiving and information retention

Archiving and information retention is imperative when you want to capture and preserve information for compliance reasons. Archive information must be managed, retained, and protected effectively and then disposed of properly when it is no longer needed. We can discuss Tivoli Security Information and Event Manager archiving and information retention from many perspectives: disaster recovery, high availability, regulatory, and so on.

There are no internal Tivoli Security Information and Event Manager tools that you can use for full disaster recovery, but you can implement any existing technology outside of Tivoli Security Information and Event Manager, such as Tivoli Storage Manager.

High availability is not an issue for Tivoli Security Information and Event Manager because data is not collected in real time but instead based on a collection schedule. When the system or network is not available at the time the collection of the logs is attempted, Tivoli Security Information and Event Manager always begins log collection from where it was last successful, which keeps log data from being missed because of network or other system problems.

Using Tivoli Security Information and Event Manager you can store all of the event data in a compressed format on a Windows file system as individual chunks of log information in a log Depot. As a result, Tivoli Security Information and Event Manager is easy to integrate with a SAN archival system for long term storage. From a regulatory perspective, it is important that the log Depot is also monitored by Tivoli Security Information and Event Manager itself, and as a result any access to the raw log data is logged and reports can be run to ensure that only proper access occurred to the log data. The raw data remains in the log Depot in an unaltered format. As a result, the data can be used in legal proceedings if required. We suggest that you use secure log management solutions together with Tivoli Security Information and Event Manager, such as the IBM System Storage® DR550 or IBM System Storage DR550 Express, to meet most stringent requirements on secure transmission and storage of regulatory audit data:

- ▶ Encryption and integrity verification in transit (Tivoli Security Information and Event Manager)
- ▶ Encryption and immutability at rest (DR550)
- ▶ Audit reports on continuity of logs (Tivoli Security Information and Event Manager)

The DR550 File System Gateway is designed to offer file archiving capability without requiring any application enablement, and to provide Network File System (NFS) and Common Internet File System (CIFS) file system access to applications. You can obtain more information about DR550/DR550 Express on the Web at the following locations:

<http://www.ibm.com/systems/storage/disk/dr>

<http://www.ibm.com/systems/storage/disk/dr/express/>

<http://www.redbooks.ibm.com/cgi-bin/searchsite.cgi?query=dr550>

For more information about backup and restore of the Tivoli Security Information and Event Manager, refer to the *IBM Tivoli Security Information and Event Manager Version 2.0 Administrators Guide*, SC23-9688.

Export and import

Using the export and import functionality in the Tivoli Integrated Portal you can back up data from the Depot. The Tivoli Integrated Portal offers a tool for defining a backup schedule and a target destination for the backup, as shown in Figure 5-17.

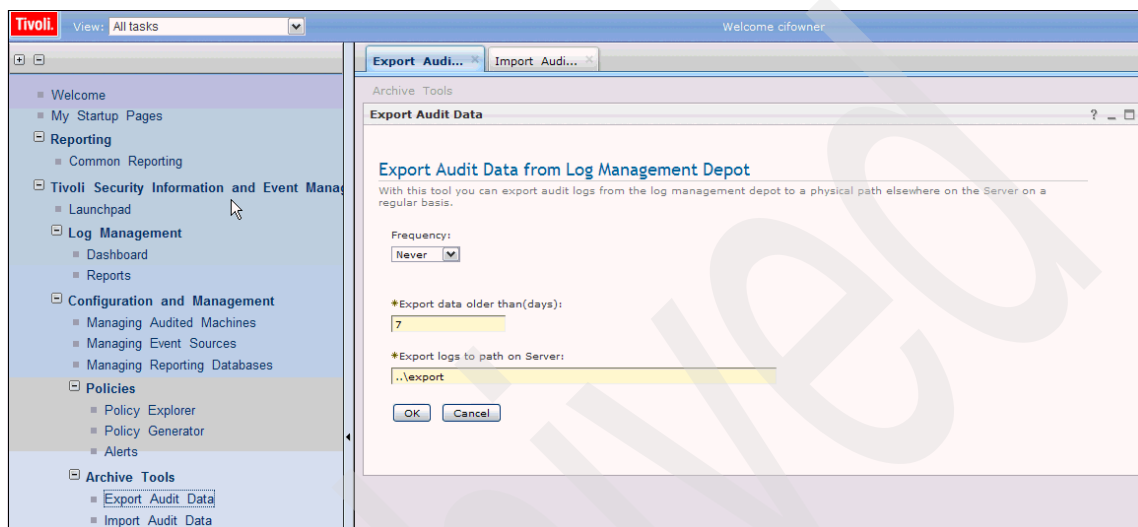


Figure 5-17 Tivoli Security Information and Event Manager backup

The idea behind this backup is that it moves the archived security data (chunks) from the Depot to the backup media, which means that the moved chunks are no longer available for selection when creating reports. To do this the chunks must be imported again.

When you export data from the Depot it is flagged in the Log Manager as *data exported*. So, if you want to retrieve the original log data, you can easily see that the data is not in the Depot and needs to be imported.

The export schedule is defined using the Tivoli Integrated Portal, and the backup is performed by the Tivoli Security Information and Event Manager server. Transferring security data helps to maintain enough disk space on the Tivoli Security Information and Event Manager server, and because all chunks are registered within Tivoli Security Information and Event Manager, the tables in the database are also cleaned up.

After the security data is backed up using the export facility in the Tivoli Integrated Portal, it is not available for reporting until it is imported again using the Tivoli Integrated Portal.

5.2.3 Performance and scalability

Tivoli Security Information and Event Manager scales in any direction, from a very small installation to extremely large sites. Data is collected and loaded into databases. You can organize data collections organization-wide, by platform, by application, by department, by region, or any other segmentation that is meaningful and specific to your organization. Tivoli Security Information and Event Manager can be configured to run on a single system for smaller installations or can use multi-processor threaded and clustered systems for larger sites.

For scalability reasons Tivoli Security Information and Event Manager servers can be deployed as multiple clusters, as shown in Figure 5-11 on page 102, but for best performance, it is recommended not to put more than four Tivoli Security Information and Event Manager servers into a single Tivoli Security Information and Event Manager cluster.

The Tivoli Security Information and Event Manager log collection architecture automatically takes into account the possibility of high levels of log traffic and even network and system outages. The collection method allows the native system to generate log messages at its own rate, and then we collect the logs on a schedule as needed.

This architecture not only eliminates the possibility of our solution impacting the native system log generation process, but also provides for when the system or network is not available at the time collection of the logs is attempted. The Tivoli Security Information and Event Manager always begins log collection from where it was last successful, which keeps log data from being missed due to network or other system problems. Using the log continuity dashboard, we can show any logs with collection problems or where log information contains time gaps.

Log collection is almost exclusively dependent on available network resources and the disk subsystem performance at the collection point. Tivoli Security Information and Event Manager provides several options for collecting Syslog data that is dependent upon the requirements for performance:

- ▶ Internal Syslog collector for mid range performance where message rates are less than a thousand messages per second
- ▶ External collection through the Syslog daemon, suitably configured, for scalable, reliable high performance where message rates are in the tens of thousands of events per second up to hundreds of thousands of events per second, as shown in Figure 5-11 on page 102

For better system performance and report distribution results, match database load and report distribution task schedules. For more information about Tivoli

Security Information and Event Manager reporting, see the *IBM Tivoli Security Information and Event Manager Version 2.0 User Guide*, SC23-9689.

5.2.4 Tivoli Security Information and Event Manager limits

There are limits in a typical Tivoli Security Information and Event Manager deployment that you must consider, for example, there are limits on the amounts of data that can be processed and the number of Standard Servers in a Tivoli Security Information and Event Manager cluster. Table 5-1 shows the Tivoli Security Information and Event Manager limits.

Table 5-1 Tivoli Security Information and Event Manager limits

Description	Limit
Maximum number of Standard Servers in one Tivoli Security Information and Event Manager cluster	3
Maximum number of event sources that can be added to one Tivoli Security Information and Event Manager cluster server	5,000
Maximum number of processes that can be loaded in parallel on a two-processor core	1
Maximum amount of uncompressed original data in depot processed daily (mapping/loading/aggregation) in GB	60 GB
Maximum amount of uncompressed original data in Depot processed per minute by Tivoli Common Reporting reports in MB	40 MB
Maximum number of messages that can be collected in real time per second (syslog, SNMP, and so on)	30,000
Max number of real-time event sources per server with * as source address	10

5.2.5 Support

There are numerous options to find support for Tivoli Security Information and Event Manager. If you encounter an issue, you want it resolved quickly. You can search the available knowledge bases to determine whether a resolution was encountered and is already documented.

IBM provides extensive documentation in an information center that can be installed on your local computer or on an intranet server. You can use the search function of this information center to query conceptual information, instructions for completing tasks, reference information, and support documents.

If you cannot find an answer to your question in the information center, you can also search the Internet for the latest, most complete information that might help you resolve your problem.

A product fix might resolve your issue. To determine fixes that are available for your IBM software product, check the product support on the IBM Software support site:

<http://www.ibm.com/software/support>

For more information about Tivoli Security Information and Event Manager support, see the *IBM Tivoli Security Information and Event Manager Version 2.0 Installation Guide*, GI11-8778.

Whether you are building a skills plan or simply looking for educational resources, we can help you define a software skills program that is right for you. Select from a wide variety of training options from a comprehensive training portfolio, and take advantage of an extensive list of skills, resources, and communities and verify skill level through role-based certification. For more information, visit the Training and Certification Web site at:

<http://www.ibm.com/software/sw-training>

5.3 Conclusion

You must consider how compliance design objectives can be realized using Tivoli Security Information and Event Manager. The goal is to produce a plan that contains a phased set of implementation steps where the end result satisfies the functional requirements and therefore also satisfies the original business requirements.

While business and functional requirements are the main parts of the security design objectives, you also must consider other nonfunctional requirements and constraints. These can include objectives that are necessary to meet general business requirements or practical constraints on designing the compliance solution.

Prioritizing the monitoring and reporting requirements of the target systems and applications is important because the priorities are one of the primary factors used to decide which implementation tasks are done in which phase of the project. It is rare that a compliance management solution can be created as a single deliverable that satisfies every requirement on all targets. It is far more likely that it is delivered in phases and the highest priority requirements must be included in the earliest phases.

After mapping the requirements to Tivoli Security Information and Event Manager features and creating a list of implementation tasks, you can use the priorities of each target and the implementation effort for each target to decide how to break up the project into phases. The goal of breaking the project into phases is to quickly deliver solutions to high-priority requirements, which allows the organization to begin seeing a return on their investment as lower priority and more difficult tasks are still executed.

Archived



Part 2

Customer environment

In this part of the book, we illustrate a scenario about a fictional financial institution and describes the implementation of security compliance management with Tivoli Security Information and Event Manager.

Archived



Introducing X-Y-Z Financial Accounting

To illustrate the implementation of security compliance management with Tivoli Security Information and Event Manager, we now want to discuss a scenario about a fictional financial institution called X-Y-Z Financial Accounting. In this chapter, we provide an introduction to the overall structure of X-Y-Z, including its organization profile, its current IT architecture and infrastructure, and its medium-term business vision and objectives with regard to security compliance management.

Note: All names and references for organization and other business institutions used in this chapter are fictional. Any match with a real organization or institution is coincidental.

6.1 Organization profile

X-Y-Z Financial Accounting is a leading financial services organization with headquarters in Europe and operates in the European Union and in the United States of America. X-Y-Z offers private banking and insurance products.

X-Y-Z started as a privately held organization and was recently acquired by a large universal bank in England that intends to make an initial public offering for X-Y-Z in six months on the New York stock exchange. X-Y-Z provides insurance products to more than 500,000 European households and performs wealth management for more than 61,000 private investors.

Note: In the following sections, we describe organization information that is relevant to a security compliance management solution and use an existing Tivoli Security Operations Manager implementation. We assume that all of the systems to be monitored are already up and running. It is not intended to provide a complete description of the organization nor do the subsequent chapters intend to cover all necessary activities surrounding the actual implementation tasks.

6.2 Current IT infrastructure

X-Y-Z Financial Accounting has an IT environment with common elements for financial services institutions, as shown in Figure 6-1 on page 123. As with other banks, X-Y-Z has a long history of computing and today still performs a majority of the processing of banking data on the mainframe. However, X-Y-Z also entered the client-server era. The organization deployed MS Windows XP workstations to all branches and manages them with Active Directory. Also, utility servers that are used for print and file services run on MS Windows 2003, and X-Y-Z today runs business applications, such as SAP R3, on an Oracle Database on a Microsoft Windows environment.

The most critical application that the organization uses in all of their branches was developed by their own IT department as a Web-enabled DB2 application. This application is called *Quant Unlimited Access Network for Traders* or short *QUANT*. It manages the organization's liquidity and investments. The models that are used by this service are highly secret and largely determine the success of the organization to thrive on the competitive financial market. The nature of this service requires that it is always available and accessible by all corporate traders, regardless of where they are located. It is therefore required that access to and usage of the QUANT system must be restricted and tightly monitored as

access to the front office QUANT Web Access Value Exchanger system, which is the Web-based application, is allowed to all corporate traders. Depending on their profile, the traders are granted access only to the latest models that apply to the type of market that they trade on.

Due to the prediction that Internet attacks against financial institutions might be used to destabilize nations, X-Y-Z will establish its own security operations center in London, which will operate on a 24 hour, 7 day schedule. X-Y-Z wants to use a Tivoli Security Operations Manager deployment as its core to manage network security devices on the corporate network perimeter and on key points in the internal network infrastructure. Overall, the organization stores approximately 246 Terabytes of data from its business operations. Figure 6-1 depicts the overall IT infrastructure of X-Y-Z Financial Accounting.

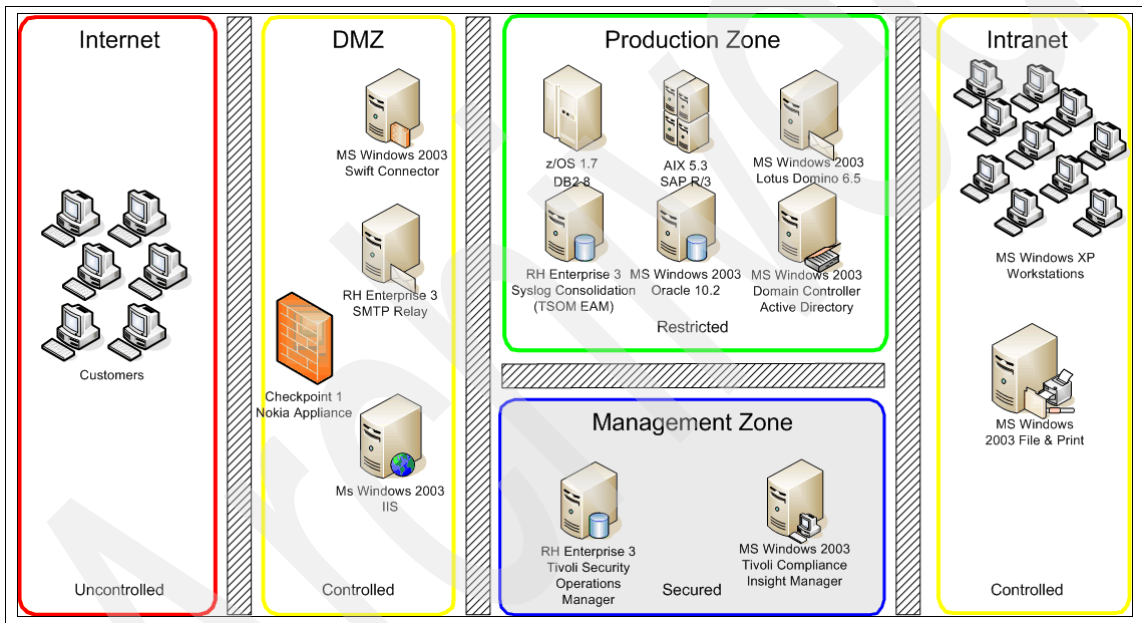


Figure 6-1 IT infrastructure of X-Y-Z

X-Y-Z uses one pair of fully resilient data centers in London, United Kingdom, for their European operations. These centers are also hosting the mainframe system and a fully mirrored Storage Area Network for 150 Terabytes of data. The organization also runs two smaller data centers in Newark, New Jersey, United States (US) to support US operations, which host 70 Terabytes of data. The organization uses two dedicated local data centers in Zurich because regulatory restrictions in Switzerland used to prohibit export of banking customer data outside of Switzerland. The remaining storage of 26 Terabytes is allocated to these data centers. A Cloud Computing-based solution is being considered for

the QUANT service, but the concern is that the organization wants to have an absolute, verifiable assurance that the secrecy and integrity of the QUANT software is maintained.

Figure 6-2 shows the geographical distribution of X-Y-Z Financial Accounting Services.

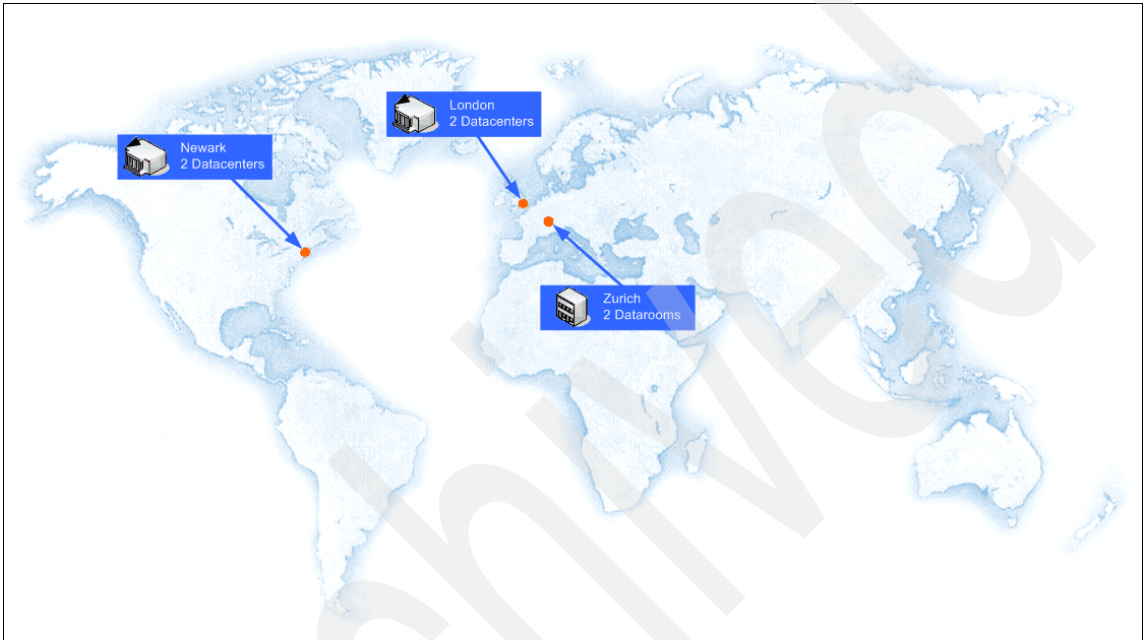


Figure 6-2 Geographical distribution of X-Y-Z Financial Accounting Services

X-Y-Z stores customer information, internal financial data, and HR data in all of these locations, and they intend to monitor their compliance status in more detail. In a first step, the organization's IT operations consolidated a table that lists all major infrastructure assets and their average log size per day, as can be seen in Table 6-1 on page 125. This is equivalent to roughly one million events per hour.

Note: Table 6-1 only shows an excerpt from X-Y-Z's compiled infrastructure assets. The intent here is to provide you with an overview of their initial IT asset analysis.

Table 6-1 Major infrastructure assets and average log size per day

Application	Platform	Server name	Log in MB/day	Zone	Server location
File & Print	MS Windows 2003	EUHQ-FP	100	Intranet	London
File & Print	MS Windows 2003	BR1-FP	100	Intranet	London
File & Print	MS Windows 2003	BR2-FP	100	Intranet	London
File & Print	MS Windows 2003	AM1-FP	100	Intranet	Frankfurt
File & Print	MS Windows 2003	AM2-FP	100	Intranet	Frankfurt
...
Workflow	MS Windows 2003	EUHQ-DO	10	Production	London
Workflow	IBM Lotus® Domino®	EUHQ-DO	100	Production	London
...
Database	Oracle Enterprise	LU-DB	500	Production	Zurich
Database	MS Windows 2003	USHQ-DB	10	Production	Newark HQ
Database	Oracle Enterprise	USHQ-DB	750	Production	Newark HQ
SAP	AIX 5, 3	EUHQ-SP	1000	Production	London HQ
SAP	MS Windows 2003	EUHQ-SP	100	Production	London HQ
SAP	AIX 5, 3	LU-SP	750	Production	Luxembourg 1
QUANTWAVE	AIX 6.1, 64 bit, TL02	COLLAPSE		Production	London
QUANT	AIX 6.1, 64 bit, TL02	STRANGE		Production	London
QUANT	AIX 6.1, 64 bit, TL02	CHARM		Production	London
IBM DB2 9.7	AIX 6.1, 64 bit, TL02	UP		Production	London
IBM DB2 9.7	AIX 6.1, 64 bit, TL02	DOWN		Production	London
IBM DB2 9.7	AIX 6.1, 64 bit, TL02	TOP		Production	London
IBM DB2 9.7	AIX 6.1, 64 bit, TL02	BOTTOM		Production	London
Database application	AIX 6.1, 64 bit, TL02	COLLAPSE		Production	London
Database application	AIX 6.1, 64 bit, TL02	STRANGE		Production	London
Database application	AIX 6.1, 64 bit, TL02	CHARM		Production	London
Database application	AIX 6.1, 64 bit, TL02	UP		Production	London
Database application	AIX 6.1, 64 bit, TL02	DOWN		Production	London
Database application	AIX 6.1, 64 bit, TL02	TOP		Production	London

Application	Platform	Server name	Log in MB/day	Zone	Server location
Database application	AIX 6.1, 64 bit, TL02	BOTTOM		Production	London
...
MF COREBANK	z/OS LPAR1	EU-ANIT	3000	Production	London HQ
MF BRATELLER	z/OS LPAR2	EU-ASRU	2000	Production	London HQ
MF EBANKING	z/OS LPAR3	EU-AZEN	1500	Production	London HQ
SOC	RH Linux Enterprise	EUHQ-SO	10	Management	London HQ
SOC	IBM Tivoli SOM	EUHQ-SO	2500	Management	London HQ
...
Compliance	IBM Tivoli CIM	EUMF-SC	200	Management	London HQ
Compliance	MS Windows 2003	LU-SC	10	Management	Zurich 1
Compliance	IBM Tivoli CIM	USHQ-SC	400	Management	Newark HQ
SWIFT Connect	MS Windows 2003	EUHQ-SW	250	DMZ	London HQ
MAIL Connect	RH Linux Enterprise	USHQ-MR	100	DMZ	Newark HQ
...
WEB Connect	MS Windows 2003	EUHQ-WW	100	DMZ	London HQ
WEB Connect	MS Windows 2003	LU-WW	60	DMZ	Zurich 1
WEB Connect	MS Windows 2003	USHQ-WW	100	DMZ	Newark HQ
Network Device	Nokia, Cisco	various	25	Various	Various
Workstation	Windows XP	various	2	Various	Various

Table 6-1 on page 125 already includes the systems that are reserved for Tivoli Security Information and Event Manager, which are listed under the application category *Compliance*. Table 6-1 on page 125 does not list the shadow systems in the respective backup data centers.

6.3 Security compliance business objectives

X-Y-Z tries to achieve objectives in the area of Security Information and Event Management (SIEM) that are very similar to other financial organizations and are summarized in the next sections.

6.3.1 Complying to security requirements in the industry

As a leading European financial institution, X-Y-Z is obliged to protect the confidentiality, integrity, and availability of customer banking information. This

obligation makes effective security monitoring of its IT environment essential. To protect the security of the customer information appropriately, the organization focuses on establishing and maintaining a secure IT environment.

IT security was mostly implemented by the organization's local IT administrators. Some security functionality is also integrated into their applications by IT development. This type of security highly depends on personal preferences, knowledge about individual products, and personal preferences about the purpose of IT security. Now that the organization is acquired, its IT security is revisited and it is being integrated with the IT security model of the acquiring organization. Their IT security and risk management practice reached the point where the security controls are implemented and now they must be managed.

A secure IT environment is achieved by implementing and enforcing a comprehensive security policy framework that matches the IT infrastructure and its surrounding processes, such as system administration, infrastructure monitoring, and frequent performance of auditing. Daily administration, authentication, and authorization to systems that handle customer banking information are common security elements of their everyday procedures. Due to the workload and the present cost constraints, proper monitoring is limited and audit is often postponed. Besides customer banking data, X-Y-Z Financial Accounting also must protect its own business information, partially, because this is legally required, but primarily for its own interest in protecting its intellectual capital and assets. X-Y-Z achieved its success mostly using its QUANT service, and this service is identified as the major key asset. Protecting its integrity and availability is of the highest priority. To maintain its value as a public division, X-Y-Z must be able to prove that this asset is guarded and maintained. The security policy framework designed for X-Y-Z addresses this and compliance with this policy is their main objective.

6.3.2 Maintaining and demonstrating management control

When X-Y-Z started taking IT security serious, they bought a tool that helped them to collect the syslog messages operating systems, applications and devices sent out. Through the years this tool accumulated several TB worth of syslog messages, and the initial idea was to use these logs for compliance reporting. The syslog messages were also used by the tool for real time incident management, but it proved to be very difficult to implement effective correlation rules that were helpful, up-to-date, and did not generate too many false positives. But most important was that the QUANT software did not support the syslog protocol, and developers did not want to implement it for auditing and monitoring purposes because of the following stacked reasons:

- ▶ High volume of system logs from large application deployments can easily overwhelm *classic* syslog and its UDP transport mechanism.

- ▶ These problems might encourage IT developers to either not create several of the logs or to frequently roll them over and discard old log messages.
- ▶ Even when used as much and as good as possible, UDP-based syslog provides no integrity or security features.
- ▶ These problems now make it difficult to conduct investigations of computer-related crime and related incidents because the collected data might be unreliable and incomplete.

The alternative was to deploy software agents on the monitored machines, but tests show that the agents that the tool provided were very intrusive.

Since then, X-Y-Z's external compliance auditors require that X-Y-Z archives the original log data because forensic investigation requires that the information that is being delivered in their reports can be traced back to the original data because it was generated by the individual event sources.

To achieve a high level of control, X-Y-Z management wants security compliance monitoring to be able not only to see *what happened* but also *how it happened*. Exceptions to defined security policy requirements must be identified, logged, and communicated to management in automatically generated reports. X-Y-Z already uses a well-known security management solution. "However, this is more network-focused and does not meet the requirement of automatically reporting exceptions on operating systems and middle-ware components of the infrastructure," states X-Y-Z Chief Information Security Officer (CISO). "Monitoring and reporting creates too high of a daily manual workload. Various staff members are already tracking logs, but with a million server events, it is possible to monitor only a few systems," he explains. Alternatively, he is well aware, that oversight has become essential for management today and a solution must be found.

6.3.3 Integrating monitoring across a multi-platform environment

X-Y-Z wants the ability to detect and to deter unauthorized use of IT systems and access to customer and financial data within the corporate perimeter because non-repudiation of transactions is essential for financial institutions. X-Y-Z does envision a tool that enables them to collect and review the monitored data in a standardized language, one that can present this data in a comfortable, accessible way.

The internal audit department of X-Y-Z wants all IT systems to be audited. As a leading financial institution, they must be sure that everything is done by the rules and that no data can be misused by falling into the hands of unauthorized users. "We need to know what is happening in the IT environment. I want to monitor all our assets at all times!" the X-Y-Z CISO says.

For X-Y-Z, this means that all platform events must be centrally collected and reported. Having a fully automated tool that can monitor and report across all of X-Y-Z's systems, where classified information is handled, is a key requirement for the solution.

6.3.4 Harvesting and structuring information to specific needs

X-Y-Z's CISO states that they need a proven set of capabilities that are very stable in operation and that require only minor daily attention. The solution must be able to expose potential security breaches on their systems that require more detailed attention. At this time, the X-Y-Z staff can only monitor a very limited numbers of events, and if they spot exceptions, they are often unable to trace their root causes. According to X-Y-Z CISO, "Our solution needs to enable us to guarantee the high level of security that is fundamental for a organization in the financial business."

He continues, "The actual collected data needs to be correlated in a way, that allows easy grouping and filtering, so that we can monitor it more effectively, investigate it thoroughly if required. Above all, the software must be able to report the collected data in an aggregated manner to business people who are not necessarily experts in understanding bits and bytes! We want to see our reports being almost identical for all platforms."

The solution must be highly flexible and capable of supplying the required data in a form that can be routinely utilized every day, without problems. The solution must fit in with X-Y-Z's own way of working. The solution also must be able to help supporting any future and current reporting requirements that are derived from regulations, such as Basel II, Sarbanes-Oxley, and PCI.

According to the X-Y-Z CISO, "When monitoring the last seven days we expect to see upwards of 50 million events per week. It is paramount that any solution allows us to regularly update the exception qualifications to save the auditors' work. We want to be able to refine our security policy on an ongoing basis and be able to easily adapt the solution to reflect these changes."

The solution must help X-Y-Z with the task of formalizing security policy requirements on the technical level by providing support for the formalization of rules in accordance to requirements in their IT security policy framework. It must give X-Y-Z the possibility to classify events as exceptions to these requirements during the continuous monitoring process.

6.3.5 Establishing a cost-efficient and future-proofed solution

X-Y-Z wants to have comprehensive monitoring of all security events with automatic identification of potential security violations and extensive reporting of the security posture. Besides these objectives, X-Y-Z intends to establish a solution, which is cost efficient and flexible to fit for future growth of the organization and its IT infrastructure. Ideally, the solution does not require more headcount than the IT security and audit departments have today, but the new solution can drive the efficiency of these resources.

According to X-Y-Z CISO, “Daily manual workload of our four compliance employees of the IT security team must be reduced substantially. These colleagues are working one full-time eight-hour shift, but only monitor our QUANT, DB2, domain controllers, SAP, and AIX servers in the time frame. To monitor all systems without a solution in place means an unfeasibly large increase in staff. Also, we want to have a solution that can keep pace with the growth of the organization and also with the ever-increasing regulatory boundaries. We want to be able to easily organize our Basel II and Sarbanes-Oxley compliance on the IT level. We also envision that the solution can help to distinguish mistakes signaled as unintentional errors from the malicious activities.”

6.4 Conclusion

In this chapter, we introduced the X-Y-Z Financial Accounting Corporation, a fictional financial institution that serves as an example scenario for the Tivoli Security Information and Event Manager implementation outlined in the following chapters. We discussed the organization profile, the current IT infrastructure, and the objectives with regard to security compliance management. We use this information to design and to implement an appropriate compliance management solution.

Compliance management design

In this chapter, we describe the design approach that X-Y-Z takes to design a compliance management solution that meets all of their regulatory requirements. We divide the discussion into the following sections:

- ▶ Business requirements
- ▶ Functional requirements
- ▶ Design approach
- ▶ Implementation approach

As we described in Chapter 6, “Introducing X-Y-Z Financial Accounting” on page 121, X-Y-Z plans to list with the U.S. Stock Exchange in six months, and they want to be prepared to meet their auditing and reporting compliance needs within that time period. Using Tivoli Security Information and Event Manager as the basis for their compliance management solution, X-Y-Z can meet these regulatory requirements.

7.1 Business requirements

X-Y-Z wants to implement a compliance management solution that they can customize for their environment. Furthermore, they want a solution that can help them to meet any future regulatory requirements that might be introduced, including Sarbanes-Oxley and PCI compliance.

Keeping regulatory compliance in mind, the CIO and the Information Security team identified three primary business requirements for their solution:

- ▶ Implement processes to help achieve regulatory compliance. In particular, monitor and report on user access to sensitive organization assets. The sensitive assets that must be protected include the organization's financial data, confidential customer data that is stored on their servers, and critical applications.
- ▶ Monitor and audit the actions taken by privileged users for internal purposes. The X-Y-Z security representatives recognize the need to monitor privileged users and their activities on key corporate systems and data to ensure that confidentiality, integrity, and the availability of systems is properly maintained. This monitoring and auditing can help prevent costly damages or outages due to inadvertent mistakes or malicious actions of powerful users.
- ▶ A centralized logging mechanism is needed. To meet regulatory requirements, the IT security team wants to automate rapid, reliable log file collection and management throughout their distributed IT environment, which includes a variety of applications, operating systems, and databases. The centralized logging mechanism must meet the following requirements:
 - This logging mechanism must be configurable so that it can change as the corporate requirements and reporting needs evolve.
 - Historical log data must be accessible to get a global view of compliance.
 - The existing syslog collection tool must be replaced by Tivoli Security Information and Event Manager.
 - Syslog data that was archived with the existing tool must become available for investigation in Tivoli Security Information and Event Manager too.

Supporting business requirements also include:

- ▶ Reduce the costs of monitoring and auditing user access to organization resources by automating the process. This automated process must notify key IT security personnel of certain situations, which includes policy violations. As a result, the manual processes and the costs that are associated with them can be minimized.

- ▶ The compliance management solution must have multi-platform support so that it can monitor systems across X-Y-Z's distributed IT environment. The automated monitoring process must allow the corporate IT security policies to be defined and refined on an ongoing basis, for example, when new systems are introduced to the IT environment.
- ▶ The CIO wants to be able to gain an overview of the corporate security compliance posture quickly. The security IT staff needs the ability to generate reports quickly and easily that cover the internal security processes, including the actions of privileged users. Reports must be able to compare user activities and security events to regulatory and acceptable use frameworks.

7.2 Functional requirements

X-Y-Z extracts functional requirements by mapping business requirements to their underlying reasons. It expands the reasons in increasing detail until it finds issues that can be solved using the capabilities of Tivoli Security Information and Event Manager. The functional requirements tie the low-level reasons for each business requirement to a capability of the compliance management solution that can be used to fulfill that business requirement.

In this section, we examine each business requirement and then search for reasons and the functional requirements.

7.2.1 Business requirement 1

To be prepared for future regulatory requirements, X-Y-Z must monitor user access to all sensitive organization assets. This monitoring is important because:

- ▶ The threat of employees misusing the data and breaching privacy. Employees can fraudulently access or disclose confidential information.
- ▶ The primary issue of data integrity. It is essential that the organization ensure that their data records are accurate and complete. Therefore, X-Y-Z must be able to detect if someone tampers with critical data.
- ▶ The integrity of the QUANT software and model must be guaranteed.
- ▶ Usage of QUANTWAVE must be visible.
- ▶ Current SMF support, which is limited to type 80 events, must be extended to include z/OS system events.

X-Y-Z outlined corporate IT security policies to help prevent the misuse of sensitive assets. To enforce these IT security policies, they want to audit the logs of critical systems and applications.

The sheer volume of logged events that are generated each day on these assets means that monitoring the logs manually is not possible. X-Y-Z wants to implement a compliance management solution that enables total monitoring of all system events, with automatic identification and reporting of potential security breaches.

The required log data can be generated by disparate targets that are located on distributed systems across X-Y-Z's IT environment. Therefore, the compliance management solution must have multi-platform support to collect data from the critical systems, including the mainframe.

Extracting relevant information from the raw logs manually can be difficult because the format of logs is often quite incomprehensible. This issue can be overcome by implementing a compliance management solution that can process the log data and transform it into a standardized format that is easier to read. As we described in Chapter 6, "Introducing X-Y-Z Financial Accounting" on page 121, X-Y-Z ideally wants to be able to view this data through a Web-based portal. They also want the ability to generate meaningful reports to display the compliance information.

Table 7-1 lists the key functional requirements for monitoring user access to sensitive organization assets.

Table 7-1 Functional requirements for monitoring user access to sensitive assets

Requirement	Description
A	The corporate IT security policies can be mapped into policies within the compliance management solution.
B	Use of organization assets are continuously monitored, with automatic detection and reporting of potential security breaches.
C	The compliance management solution must have multi-platform support, which includes mainframes, so that it can adapt to X-Y-Z's unique IT environments.
D	The compliance management solution must transform the data that is extracted from the logs into a readable, easy to comprehend format for the user, which must be available through a Web-based portal.
E	The user must be able to easily generate reports regarding user access to corporate assets.

7.2.2 Business requirement 2

Monitoring and auditing the actions of privileged users is important. The reasons for this monitoring are very similar to those that we described in 7.2.1, "Business

requirement 1” on page 133. A special focus on monitoring privileged users is necessary because privileged users have more authority than regular users to perform actions on corporate systems. The IT security staff must know that privileged users are managing data and systems as expected. Powerful users can mistakenly or deliberately damage systems or information assets, which can be costly.

Theft or release of information assets is also one of the main drivers for this monitoring, for example, if a senior executive is leaving the organization to go to a competitor, the IT security team might want to generate a report on that individual’s actions on confidential corporate data over the past month. In this context, any modifications made to the QUANT software and input parameters must be verifiable.

X-Y-Z must be able to verify that the privileged users are behaving as expected and not violating the organization’s internal IT security policies.

Table 7-2 describes the functional requirements for monitoring and auditing the actions of privileged users.

Table 7-2 Functional requirements for monitoring and auditing privileged users

Requirement	Description
F	The administrators of the compliance management solution can define the group of privileged users to be monitored.
G	The administrators of the compliance management solution can specify which corporate data systems and assets contain critical data.
H	Policies can be configured to describe the access rights for privileged users and the actions they are allowed to perform.
I	Reports can be generated automatically regarding privileged users and their actions over a period of time.

7.2.3 Business requirement 3

A centralized logging mechanism must be the heart of the compliance management solution. X-Y-Z deployed hundreds of points across the enterprise that generate log events. Regulators and auditors require these log files to be captured and retained. Additionally, X-Y-Z wants to be able to investigate any events that can represent internal or external threats. Time and cost constraints mean that this log file management must be fast and affordable. This logging requirement is closely linked to the previous two requirements, which rely on using logs to monitor the actions of users.

To be fast and affordable the logging mechanism must have the ability to automatically collect logs on a predefined schedule. The mechanism must also have a backup and archival process in place to ensure that no logs are lost. Auditors require the history of logs to be available to prove that the log data is continually captured and to allow old events to be investigated. The historical log data can be used to obtain an overall view of compliance.

X-Y-Z already collects the syslog messages from various platforms using another tool. This collection tool must be replaced by Tivoli Security Information and Event Manager and the syslog messages that are already collected must be made available for investigation within Tivoli Security Information and Event Manager.

Table 7-3 shows the functional requirements for the compliance management logging mechanism.

Table 7-3 Functional requirements for logging mechanism

Requirement	Description
J	Automatic log collection can be scheduled.
K	The logging mechanism must have a backup and archival process.
L	Logs must be retained so that the continuity of the logs can be proven.

7.2.4 Business requirement 4

X-Y-Z wants to reduce the costs of monitoring and auditing user access to organization resources. This requirement is also related to all of the other business requirements. As previously mentioned, to monitor all systems manually, a large, infeasible increase in staff is necessary due to the following issues:

- ▶ Amount of log data generated
- ▶ Platform specific expertise required
- ▶ Complexity of extracting meaningful information from each log
- ▶ Time taken to compare each logged event with the corporate IT security policies to identify any policy exceptions
- ▶ Effort required to manually present the results in a meaningful report

X-Y-Z decided to implement an *automated* compliance management solution to overcome these issues. This compliance management solution must be flexible enough to cater to X-Y-Z's unique IT architecture and security policies. To minimize the manual labor required, this automated process must send an e-mail

to members of X-Y-Z's IT security team to notify them of suspicious activities, including policy violations.

Table 7-4 lists the functional requirements to minimize the costs of monitoring and auditing user actions.

Table 7-4 Functional requirements to reduce the manual labor required to monitor logs

Requirement	Description
M	Send an e-mail alert to IT security team when suspicious events, including policy violations, occur.
N	All system events can be monitored and reported on automatically with minimal manual labor required.

7.2.5 Business requirement 5

The compliance management solution must be flexible enough to adapt to X-Y-Z's unique IT environment. The IT environment can be expected to evolve continuously over time. There are a few main aspects of the IT environment that, when modified, can impact the compliance management solution:

- ▶ Changes to the IT architecture
- ▶ Changes to the IT personnel
- ▶ Changes to the internal IT security policies that govern the use of the organization assets

The architecture of X-Y-Z's IT environment changes regularly as new systems are acquired, new uses are applied to existing systems, and old systems are retired. Therefore, it is essential that when these changes occur, the compliance management solution can be configured to access the logged audit data that is available on each of the IT systems in use. To do this, it must have multi-platform support, as we previously mentioned (refer to Table 7-1 on page 134). Similarly, it is important that the compliance management solution can collect and process logs from a wide variety of event sources on those target systems. Ideally, it must be flexible enough to monitor and process logs from *any* event source, provided that those logs contain sufficient data in an appropriate format.

The compliance management solution is limited by what data is logged by each of the event sources. Therefore, appropriate audit settings must be identified and configured on the target systems. The auditing on each target system can be referred to as an *audit subsystem*.

Changes to the IT personnel might include existing staff changing roles, new staff being hired, and staff leaving the organization. Any of these personnel changes

must be reflected in the structure of the compliance management solution, which must compare the behavior of these users with the defined security policies of allowable actions.

The corporate IT security policies themselves also need to be defined and refined on an ongoing basis as the business grows, for example, when new regulatory requirements are introduced, the business must be able to create new policies and modify the existing policies. Similarly, when new assets are introduced into the system, a new audit-subsystem must be established on the target system and new policies must be established to monitor and audit the use of the new asset.

Because the compliance management solution is reliant on the individual audit subsystems to obtain its data, it is important to maintain data integrity in the logs on the target systems. To ensure that the integrity is maintained, X-Y-Z needs their compliance management solution to audit the actions that are performed on the audit subsystems.

The configuration of the compliance management solution is extremely important to ensure that the correct log data is audited. Therefore, only a restricted list of privileged users can be authorized to change the compliance management solution itself, and these changes must be audited. This capability is referred to as *self-auditing*.

Reliability, integrity, and availability of the QUANT service is of the highest priority. It is therefore that X-Y-Z decided to use IBM Guardium to monitor the DB2 databases used by QUANT. IBM Guardium is non-intrusive and will therefore not slow down the performance of the DB2 database servers. Guardium can handle incident management for and prevent illegal access to the DB2 databases. Guardium can generate audit logs for Tivoli Security Information and Event Manager that are converted to the Tivoli Security Information and Event Manager W7SDK format using Tivoli Directory Integrator.

In this way, Tivoli Security Information and Event Manager can be used to report on security incidents that IBM Guardium finds. But because the QUANT application has its own account and access management and uses anonymous dedicated DB2 administrative accounts to access DB2, it is necessary to include the QUANTWAVE logs to identify the users who accessed QUANT. A Tivoli Security Information and Event Manager event source is created in combination with a Tivoli Security Information and Event Manager QUANT mapper to integrate the QUANTWAVE logs into the compliance auditing process.

Table 7-5 on page 139 describes the functional requirements for the flexibility of the compliance management solution.

Table 7-5 Functional requirements for flexibility in the compliance management solution

Requirement	Description
O	Be flexible enough to monitor and audit logs from <i>any</i> event source, provided the log contains sufficient data in an appropriate format.
P	Policies can be created, modified, and deleted by the administrator of the compliance management solution.
Q	The compliance management solution must monitor the audit subsystems.
R	The compliance management solution must have self-auditing capability.

7.2.6 Business requirement 6

The compliance management solution must have extensive reporting capabilities. After the log data is collected and stored, it must be analyzed to get an overview of X-Y-Z's compliance, for example, the logged events must be compared with the IT security policies to find any violations and other potential threats.

Rather than a manual process, X-Y-Z wants to automatically generate reports to display meaningful compliance information that is extracted from the logged data. These reports can assist the organization to demonstrate their SOX compliance.

Because X-Y-Z wants to be prepared to introduce SOX and PCI compliance in the future, sample report templates for the various regulatory requirements, such as SOX, can be a very useful starting point. X-Y-Z must determine exactly which reports they want to generate for their unique IT environment and exactly how they want them presented. The compliance management solution must allow new customized reports to be created so that X-Y-Z can create reports that are useful for their IT security staff. These customized reports allow the organization to enforce their security policies actively and meet their regulatory requirements.

Table 7-6 shows the functional requirements for reporting.

Table 7-6 Functional requirements for reporting

Requirement	Description
S	Sample report templates will be available to assist with meeting regulatory requirements, such as SOX, in the future.
T	The compliance management solution will have the ability to customize reports.

7.3 Design approach

Let us now consider how compliance design objectives can be realized using Tivoli Security Information and Event Manager. The goal is to produce a plan that includes a phased set of implementation steps, where the end result satisfies the functional requirements and, therefore, also satisfies the original business requirements.

While business and functional requirements are the main parts of the security design objectives, X-Y-Z also must consider other non-functional (also called operational requirements) requirements and constraints, which can include objectives that are necessary to meet general business requirements or practical constraints on designing the compliance solution.

Tivoli Security Information and Event Manager implementations often include operational requirements relating to the following areas:

- ▶ High availability
- ▶ Backup and recovery
- ▶ Performance and capacity
- ▶ Change management
- ▶ Existing infrastructure
- ▶ Budget and staffing

For further information about these compliance management non-functional requirements, refer to *IBM Tivoli Security Information and Event Manager Version 2.0 Administrators Guide*, SC23-9688.

Non-functional requirements are outside of the scope of the scenario implementation that we discuss in this book. We focus on using Tivoli Security Information and Event Manager to meet the functional requirements for the scenario, as outlined in 7.2, “Functional requirements” on page 133.

We describe the steps that are involved in producing an implementation plan in this section. Steps 1 through 5 encompass the *Discovery and Analysis* phase of design, and steps 6 and 7 are required as part of the *Project Definition and Planning* phase. We describe these phases in Chapter 5, “Compliance management solution design” on page 89.

7.3.1 Creating an implementation plan

To produce an implementation plan:

1. Determine what reports must be generated for X-Y-Z to monitor their compliance.

Reports: The reports that are needed are based on the existing IT security policies that are in place. Tivoli Security Information and Event Manager provides component modules with sample report templates and policy rules to assist with requirements for regulations, such as Basel II and Sarbanes-Oxley, in the future. These templates can be customized for X-Y-Z's specific needs.

2. Decide which target assets must be monitored to produce these reports.
3. Identify what data is to be collected from each event source on the target machines and whether the auditing on that system can be configured to log the required event details.

Note: If it is not possible for sufficient data to be captured in the target system logs, then it is not possible to audit and report on that type of event.

4. Ensure that Tivoli Security Information and Event Manager can monitor audit trails from that event source.

Event sources: You can find a complete list of supported event sources for Tivoli Security Information and Event Manager at:

http://www.ibm.com/support/docview.wss?rs=3285&context=SS22KN&q1=1282770&uid=swg21282770&loc=en_US&cs=utf-8&lang=en

If the event source is not supported, consider using the W7LogSDK toolkit to create logs that Tivoli Security Information and Event Manager can process. We describe the W7LogSDK in 12.3, "W7Log event source" on page 354.

5. Prioritize the monitoring and reporting requirements for the various target systems and applications.
6. Complete a pre-planning worksheet to cover all of the target event sources.
7. Divide the tasks into phases.

Prioritizing the monitoring and reporting requirements of the target systems and applications is important because the priorities are one of the primary factors that are used to decide which implementation tasks are done in which phase of the project. It is rare that a compliance management solution can be created as a single deliverable satisfying every requirement on all targets. It is far more likely that it is delivered in phases, and the highest priority requirements must be included in the earliest phases.

Assigning priorities to the requirements is often difficult because *they are all important*. You can compare the priorities of the target systems and applications more easily by performing a *risk assessment*.

Risk management: To learn more about risk management, refer to *Risk Management Guide for Information Technology Systems* from the NIST, which is available at:

<http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>

You can also read the IT Security Cookbook, which is available at:

<http://www.boran.com/security/index.html>

The targets that are identified as being a high risk can then be treated as the highest priority. A simple way to calculate risk is to use the following formula:

$$\text{Risk} = \text{Impact} * \text{Likelihood}$$

The *Impact* component must be a one through 10 rating that represents the *impact* or *consequence* for the business if a threat is realized. The impact must be judged by business experts and must take into account both the short-term and the long-term effect on the business.

The *likelihood* of a threat occurring can also be rated on a 10 point scale, with one indicating that it is extremely unlikely to occur and 10 indicating that the event is very likely to occur on a daily basis. The technical experts are probably in the best position to evaluate the likelihood of each threat.

Asking yourself questions that gauge the positive and negative impacts of the requirements for each target can also help you with your prioritization:

- ▶ How much money can be saved by automating the auditing of this target?
- ▶ How sensitive is the data stored on this target?
- ▶ Are there existing mechanisms or processes in place for auditing the target, which will be sufficient for now?
- ▶ What is the complexity of monitoring this target? Does Tivoli Security Information and Event Manager provide an agent that supports this event source?

After mapping the requirements to Tivoli Security Information and Event Manager features and creating a list of implementation tasks, you can use the priorities of each target and the implementation effort for each target to decide how to break up the project into phases. The goal of breaking the project into phases is to quickly deliver solutions to high-priority requirements, which allows the

organization to begin seeing a return on their investment, as lower priority and more difficult tasks are still being executed.

7.4 Implementation approach

In this section, we apply the design approach that we described, in 7.3, “Design approach” on page 140, to X-Y-Z’s specific requirements. It is beyond the scope of this book to show the full design and analysis for X-Y-Z. The remainder of this chapter summarizes the result of applying the design analysis to X-Y-Z’s environment and describes the overall phased implementation plan.

7.4.1 Determining what reports to generate

In this section, we determine which reports to generate. First, we look at the various report requirements.

Internal IT security policies

We describe the logging requirements for the IT security policy in Chapter 6, “Introducing X-Y-Z Financial Accounting” on page 121:

- ▶ All logon attempts, both successful and failed
- ▶ All attempts to access classified resources
- ▶ All denied attempts to access all resources
- ▶ Use of privileged user ID
- ▶ Use of user ID with system privilege
- ▶ Administrator’s actions in the access control system
- ▶ All attempts to access resources belonging to access control systems
- ▶ All access to QUANTWAVE
- ▶ All access to DB2 databases used by QUANT

Regulatory requirements

Being a financial corporation, X-Y-Z wants to initially align its reporting with Basel II. However, the organization also wants to be able to adjust their reports and policies in the future to accommodate other regulations, such as SOX and PCI, when necessary.

Table 7-7 lists the set of reports that were identified as a starting point for the organization. You notice that many of these reports can be generated from the data that is collected for the internal IT security policy requirements (the numbers in the brackets refer to sections in ISO 17799).

Table 7-7 Initial Basel II reporting goals

Basel II report	Description
Security alert (6.3, 8.1.3)	Alerts sent in response to policy exceptions or special attention exceptions.
Operational change control (8.1.2)	Changes to the operating environment such, as system updates, DBA activity, and so on.
Operator log (8.4.2)	Actions that the IT administration staff performs.
Review of user access rights (9.2.4, 9.7)	Actions that administrators perform on users.
System access and use (9.2.4.c, 9.7)	Successes and failures against key assets.
User responsibilities and password use (9.3)	Logon failures and successes either locally or remotely.
User identification and authentication (9.5.3)	Logon and logoff successes and failures.
Application access control (9.6)	Actions, Exceptions, and events on HR Data, Sensitive Data, User Sensitive Data, System, Financial Data, Proprietary Data, and General Data.
Information access restrictions (9.6.1)	Who accessed sensitive or private data successfully or unsuccessfully.
Sensitive system isolation (9.6.2)	Exceptions and failures against sensitive systems data in asset groups User, HR Data, Source Code, and Financial Data.
Logging and reviewing events (9.7.2.3)	Exceptions and failures that the Tivoli Security Information and Event Manager system recorded.
Control of operational software (10.4.1)	Exceptions and failures caused by the updating or changing of critical system components.
Data access (12.1.4)	Exceptions and failures against HR, Sensitive, and Proprietary data.

7.4.2 Monitoring target assets for reports

For reports to be meaningful, it is important that X-Y-Z identify the target systems and applications for which each of the reports must be generated.

Table 7-8 shows the classifications of X-Y-Z's current assets.

Table 7-8 Classification of X-Y-Z's systems and event sources

Event source	Classification	Monitor with Tivoli Security Information and Event Manager?
Windows XP workstations	Internal use: Non confidential. It is organization policy not to store confidential data on workstations. Deemed a low risk.	No
File & Print W2K3 servers	Internal use: In intranet zone.	Yes
Tivoli Security Operations Manager servers	Confidential: In Management zone.	Yes
Tivoli Security Information and Event Manager servers	Confidential: In Management zone.	Yes
DMZ machines	Demilitarized zone: No confidential data is stored on these servers. Some confidential data will pass through these machines, but it is deemed low risk because of controls that are already in place.	No
z/OS mainframe	Confidential data, which includes customer, HR, and financial data in DB2.	Yes
DB2 on z/OS	Confidential data, which includes customer, HR, and financial data.	Yes
QUANT	Access to QUANT.	Yes
QUANTWAVE	Access to QUANTWAVE.	Yes
AIX	Confidential corporate data in SAP.	Yes
SAP (on AIX)	Confidential data.	Yes
W2K3 servers (Lotus Domino hosts)	Sensitive data in Domino.	Yes
Domino	Sensitive data in internal emails.	Yes
syslog consolidation	Syslog messages gathered from any system must be searchable on demand.	Yes

Event source	Classification	Monitor with Tivoli Security Information and Event Manager?
W2K3 server (Oracle hosts)	Confidential data in Oracle.	Yes
Oracle	Confidential corporate data.	Yes
Win2K3 Domain Controllers	Sensitive corporate data.	Yes
Active Directory	Sensitive corporate data.	Yes

7.4.3 Identifying the data to be collected from each event source

Each of the individual reports must be analyzed, and identify a list of the event details that are needed from each event source. After the list of required attributes is determined, the audit subsystem of the target system can be investigated to determine whether audit settings exist that will produce logs that contain the required details.

If it is not possible to generate the required log data, that report cannot be produced for that particular system.

X-Y-Z analyzed the audit subsystems for all of the event sources that Tivoli Security Information and Event Manager is to monitor (as described in Table 7-8 on page 145). It is possible to collect sufficient data from each of these audit subsystems for the purposes of monitoring and reporting on these event sources.

7.4.4 Ensuring Tivoli Security Information and Event Manager's ability to monitor audit trails from that event source

X-Y-Z must look through the list of event sources and compare it against the list of supported Tivoli Security Information and Event Manager event sources, as shown in Table 7-9.

Table 7-9 Tivoli Security Information and Event Manager support for event sources

Event Source	Tivoli Security Information and Event Manager Support for TOFT's environment
AIX OS	Yes: IBM AIX audit logs
QUANTWAVE	Yes: W7SDK
QUANT	Yes: Generic Event Source

Event Source	Tivoli Security Information and Event Manager Support for TOFT's environment
W2K3 OS	Yes: Microsoft Windows Security Event Log
Active Directory	Yes: Active Directory is supported by the Windows agent
Syslog	Yes: Any type syslog
Mainframe	Yes: IBM z/OS
DB2	Yes: IBM DB2 on z/OS
Oracle	Yes: Oracle DBMS on Windows
SAP	Yes: SAP R/3 on AIX and Windows
Domino	Yes: IBM Lotus Domino Server on Windows
Tivoli Security Operations Manager	Yes: Tivoli Security Information and Event Manager/Tivoli Security Operations Manager integration capabilities
Tivoli Security Information and Event Manager	Yes: Self-audit capabilities

7.4.5 Prioritizing the target systems and applications

The set of administrative or high privileged accounts can be viewed as an asset that has a high impact when compromised. The systems are quite vulnerable to privileged access because they are only protected by a user ID, password, and account locks and are exposed to anyone who is using the system. The privileged user accounts must therefore be monitored with high priority.

The set of sensitive business data when compromised also has a high impact, but they are less vulnerable because they are protected by ACLs, encryption, and authentication. The exposure is also lower because you do not know where these assets are physically located and how to access them. Therefore monitoring the controls that manage these sensitive assets is of a lower priority.

As a result, X-Y-Z wants to prioritize monitoring the privileged users asset controls first with Tivoli Security Information and Event Manager and then expand the monitoring to address all access to sensitive assets based on the results of the corporate risk assessment.

X-Y-Z also spent time prioritizing the multiple event sources. The existing controls that are in place on the various systems helped them to determine which systems and applications were the highest priority, for example, the Windows

servers were deemed to be a high priority because of their exposure. The Windows servers contain confidential information and are used consistently by all employees. With only limited access controls and monitors currently in place, the Windows servers are classified as a relatively high risk. Meanwhile, z/OS was not considered as high a risk. The mainframe does contain highly confidential data, but because the IT security team already has strong controls and processes in place for restricting and monitoring access to this resource, it was deemed a lower risk than other systems. This process of comparing the risks that are associated with individual event sources helped X-Y-Z in planning their phased Tivoli Security Information and Event Manager deployment.

7.4.6 Planning deployment

X-Y-Z completed a pre-planning worksheet for all of the event sources that are going to be monitored using Tivoli Security Information and Event Manager. The worksheet helped them to plan their compliance management solution.

Based on the data that was captured during this planning phase, X-Y-Z determined that for their current IT architecture, they will use a Tivoli Security Information and Event Manager cluster that is comprised of two Standard Servers and one Enterprise Server. This decision was based on the fact that each Standard Server can process up to 60 GB of log data per day. You can refer back to Chapter 6, “Introducing X-Y-Z Financial Accounting” on page 121, for details about the expected amount of log data from each of X-Y-Z’s event sources.

One Standard Server will be used for the z/OS and DB2 event sources, and the other Standard Server will process the other event sources.

Figure 7-1 on page 149 shows the planned high-level design for X-Y-Z’s compliance management solution. As you can see, certain systems in the Production Zone are audited through locally installed agents, and other auditing occurs through agentless and remote collections depending on which event source is being monitored.

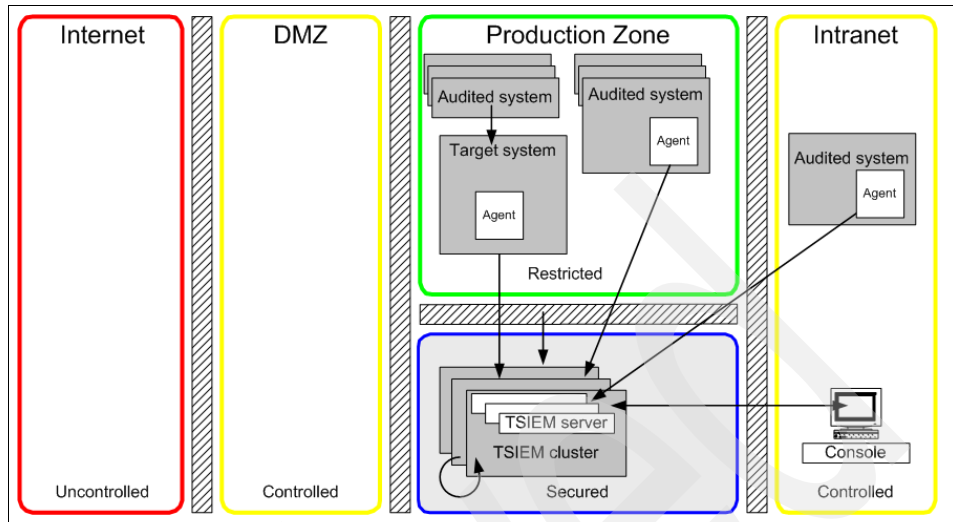


Figure 7-1 Planned Tivoli Security Information and Event Manager solution design

7.4.7 Dividing the tasks into phases

After completing the planning phase and undertaking a comprehensive risk assessment of X-Y-Z's IT environment, the implementation of the compliance management solution was divided into five separate phases, which Table 7-10 outlines. With each new phase, X-Y-Z will expand their compliance management solution.

Table 7-10 Implementation phases

Phase number	Name	Description
1	Windows Basic Auditing	Initially, X-Y-Z wants to implement basic log management and auditing functionality for their Windows event sources with basic reporting.
2	Extended Auditing	Phase 2 expands the centralized log management and auditing to include AIX, SAP, Domino, and (existing) syslog messages with basic reporting.
3	Reporting requirements	In this phase, we introduce more extensive reporting, which includes report distribution. The reports that are created in this phase are focused on presenting data for the purposes of demonstrating regulatory compliance.

Phase number	Name	Description
4	System z integration	The System z servers that store critical data also must be compliant. Therefore, we want the centralized Tivoli Security Information and Event Manager solution to include these machines.
5	QUANT and QUATWAVE integration	The critical QUANT environment must be audited using custom event source techniques.
6	Tivoli Security Operations Manager integration	X-Y-Z wants to realize the full benefits of using both Tivoli Security Information and Event Manager and Tivoli Security Operations Manager by integrating the two products to fulfill their compliance needs.

7.5 Conclusion

In this chapter, we described the design approach that X-Y-Z took to design their compliance management solution using Tivoli Security Information and Event Manager.

We outlined the business requirements and the associated functional requirements. After these requirements were identified, the design approach was outlined. When applied to their unique IT environment, this process of design and analysis helped X-Y-Z to devise an implementation plan.

X-Y-Z decided to deploy their Tivoli Security Information and Event Manager solution through five phases of implementation:

1. Basic auditing of Windows event sources.
2. Extended auditing of AIX, SAP, Domino, and syslog.
3. Implement reporting requirements.
4. System z integration.
5. Integration of QUANT and QUANTWAVE.
6. Tivoli Security Operations Manager integration.

The remaining chapters of this book describe each of these implementation phases in detail.

Basic auditing

In this chapter, we describe the implementation for phase one of X-Y-Z's compliance management solution using Tivoli Security Information and Event Manager.

As outlined in Chapter 7, "Compliance management design" on page 131, in phase one, X-Y-Z plans to install a Tivoli Security Information and Event Manager cluster. For this phase, they monitor the actions of their Windows domain users by installing local Windows agents and configuring a Microsoft Windows event source for each Windows server. They also configure an Active Directory event source on the Windows Domain Controllers. The audit subsystem on each Windows server must be configured to generate sufficient log information. Appropriate W7 groups and rules are established through the Policy Explorer, and ultimately the Compliance Dashboard is used to monitor user actions.

8.1 Phase one auditing

Figure 8-1 on page 152 shows the initial IT architecture for X-Y-Z's compliance management solution using Tivoli Security Information and Event Manager. We described this architecture in detail in Chapter 6, "Introducing X-Y-Z Financial Accounting" on page 121.

In phase one, the Tivoli Security Information and Event Manager servers are installed and configured, and the Windows 2003 servers, including the Active

Directory server, are monitored. In Figure 8-1, these server groups are highlighted in bold, underlined text.

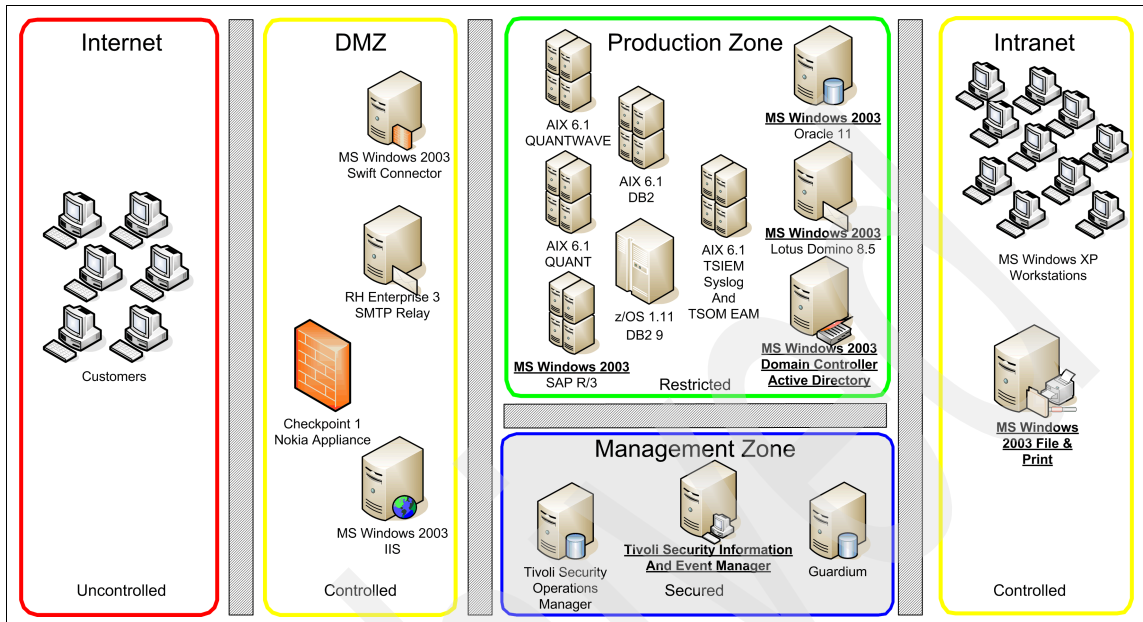


Figure 8-1 X-Y-Z IT architecture

Auditing must be configured on each of the Windows 2003 target machines. As we described in Chapter 7, “Compliance management design” on page 131, X-Y-Z initially wants to focus their audit on the actions of privileged users as a result of the risk assessment. In particular, they want to monitor the logons, both successful and failed, and access to critical data shares.

User logons must be monitored on all of the Windows servers. Additionally, Active Directory must be monitored as a separate event source on the Active Directory servers.

The critical data shares reside on the Windows 2003 file and print servers that are shown in the intranet zone of Figure 8-1. The following share folders were identified to be audited:

- ▶ C:\Finance
- ▶ C:\HR
- ▶ C:\CustomerData
- ▶ Print Share: C:\WINDOWS\system32\spool

Finally, the Tivoli Security Information and Event Manager servers must be enabled for self-auditing.

8.2 Installing the cluster

For phase one, X-Y-Z will deploy an Enterprise Server with a single Standard Server belonging to it. Therefore, both of these Tivoli Security Information and Event Manager servers will be installed and configured on Windows 2003 64-bit Enterprise Edition servers, which we show in the Management Zone of Figure 8-1 on page 152.

8.2.1 Installing an Enterprise Server

To install the Enterprise Server:

1. Install the database engine that is provided with Tivoli Security Information and Event Manager.
2. Install the desired Tivoli Security Information and Event Manager components for the Enterprise Server.
3. Configure the Enterprise Server.

Note: X-Y-Z uses mostly the default values when installing the server, but we opted to change the default *OS account* and *database account* user names, as shown here:

- ▶ OS Account: *cifadmin_os*
- ▶ Database Account: *cifdbadmin_db*

Refer to the *IBM Tivoli Security Information and Event Manager Version 2.0 Installation Guide*, GI11-8778 for more information about the Enterprise Server installation process.

8.2.2 Installing a Standard Server

Installing the Standard Server is very similar to installing the Enterprise Server. To install a Standard Server:

1. Install the database engine that is provided with Tivoli Security Information and Event Manager.
2. Install the desired Tivoli Security Information and Event Manager components for the Standard Server.
3. Register the Standard Server with the Enterprise Server.

For more details about each of these steps, refer to the *IBM Tivoli Security Information and Event Manager Version 2.0 Installation Guide*, GI11-8778.

8.3 Phase one reporting requirements

X-Y-Z identified the key reporting requirements, shown in Table 8-1, to aid in their compliance management (the numbers in the brackets refer to sections in ISO 17799).

Table 8-1 Initial Basel II reporting goals

Basel II report	Description
Security alert (6.3, 8.1.3)	Alerts sent in response to policy exceptions or special attention exceptions.
Operational change control (8.1.2)	Changes to the operating environment, such as system updates, DBA activity, and so on.
Operator log (8.4.2)	Actions that the IT administration staff performs.
Review of user access rights (9.2.4, 9.7)	Actions that the administrators perform on users.
System access and use (9.2.4.c, 9.7)	Successes and failures against key assets.
User responsibilities and password use (9.3)	Logon failures and successes, either locally or remotely.
User identification and authentication (9.5.3)	Logon and logoff successes and failures.
Application access control (9.6)	Actions, Exceptions and events on HR Data, Sensitive Data, User Sensitive Data, System, Financial Data, Proprietary Data, and General Data.
Information access restrictions (9.6.1)	Who accessed sensitive or private data successfully or unsuccessfully.
Sensitive system isolation (9.6.2)	Exceptions and failures against sensitive systems' data in asset groups: User, HR Data, Source Code, and Financial Data.
Logging and reviewing events (9.7.2.3)	Exceptions and failures that the Tivoli Security Information and Event Manager system recorded.
Control of operational software (10.4.1)	Exceptions and failures caused by updating or changing critical system components.
Data access (12.1.4)	Exceptions and failures against HR, Sensitive, and Proprietary data.

8.4 Enabling and configuring auditing

All of the Windows 2003 servers must have appropriate audit policies configured so that the Windows Security logs contain sufficient information. In this section, we describe the settings that are configured for all of the Windows 2003 servers and settings specific to the Active Directory and file and print servers.

8.4.1 Auditing settings for the Windows Security log

The Microsoft Management Console (MMC) can be used to set the Audit Policy for the Windows servers. To configure the policy on the Windows servers:

1. Go to **Start** → **All Programs** → **Administrative Tools** → **Local Security Policy**.
2. In the left menu, navigate to **Local Policies** → **Audit Policy**.
3. Set the Audit Policy to log appropriate events. For X-Y-Z's reporting requirements, the audit policy shown in Figure 8-2 is configured on each Windows 2003 Server.

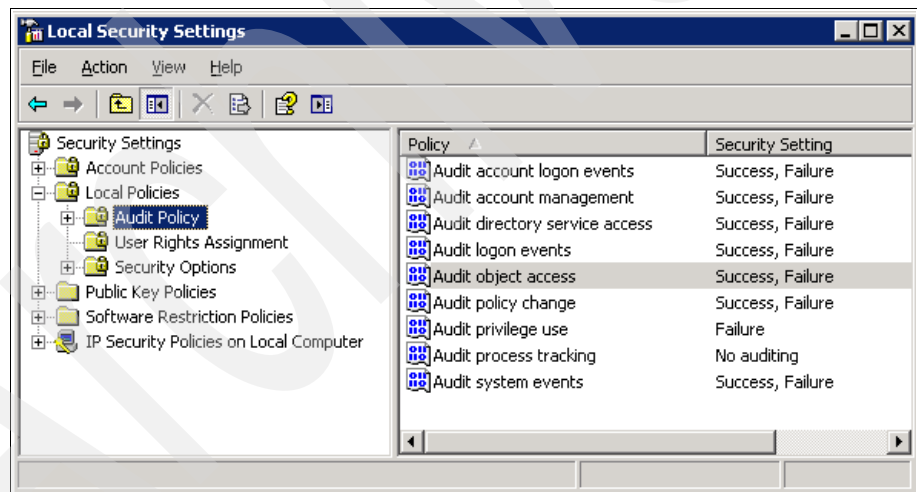


Figure 8-2 Local Audit Policy settings

The Audit object access option: The Audit object access option is only set to *Success/Failure* on the file and print servers that host confidential file shares. On the other Windows servers in X-Y-Z's environment the Audit object access option is set to *No auditing*.

8.4.2 Active Directory audit policy settings

The X-Y-Z Active Directory servers are hosted on Windows 2003. The Windows local audit policy settings are configured on the Active Directory servers. Configure appropriate settings through **Administrative Tools** → **Domain Security Policy and Administrative Tools** → **Domain Controller Security Policy**.

X-Y-Z wants to closely monitor the actions of their domain users. Figure 8-3 displays the domain security audit policy settings that are used on the Windows 2003 Active Directory servers. The same auditing is also configured in the Default Domain Controller security settings.

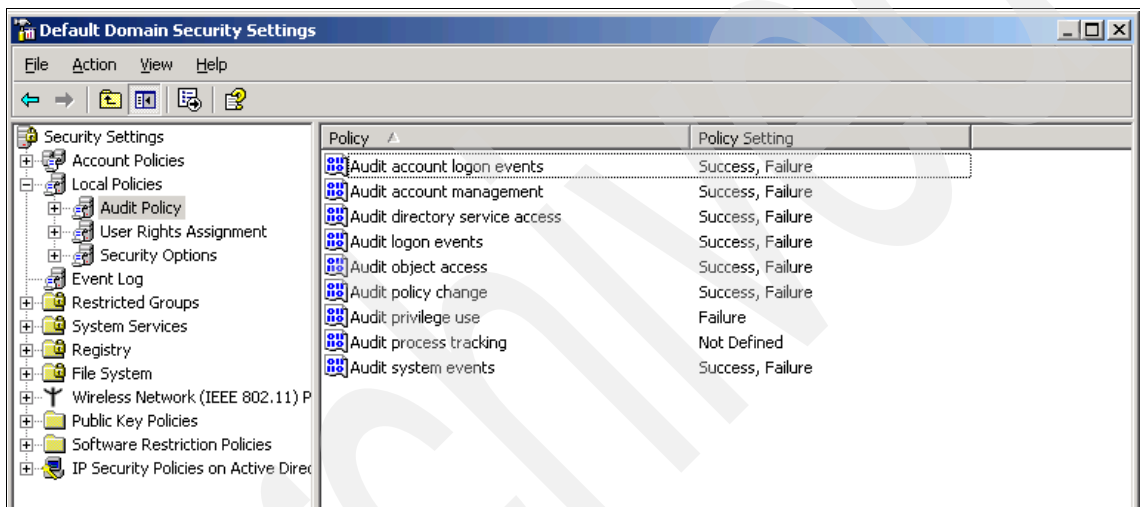


Figure 8-3 Domain security settings

By default, the Active Directory is configured to log critical and error events only. Change this behavior only if a detailed investigation is needed because extensive logging of events can quickly consume data storage space.

The following types of events that can be written to the event log are defined in the Active Directory:

- ▶ Knowledge Consistency Checker (KCC)
- ▶ Security Events
- ▶ ExDS Interface Events
- ▶ MAPI Events
- ▶ Replication Events
- ▶ Garbage Collection
- ▶ Internal Configuration

- ▶ Directory Access
- ▶ Internal Processing
- ▶ Performance Counters
- ▶ Initialization/Termination
- ▶ Service Control
- ▶ Name Resolution
- ▶ Backup
- ▶ Field Engineering
- ▶ LDAP Interface Events
- ▶ Setup
- ▶ Global Catalog
- ▶ Inter-Site Messaging

Microsoft defined the following levels of diagnostic logging for the Active Directory:

- 0 - (None)** Only critical events and error events are logged at this level.
- 1 - (Minimal)** Very high-level events are recorded in the event log at this setting.
- 2 - (Basic)** Events with a logging level of two or lower are logged.
- 3 - (Extensive)** Events with a logging level of three or lower are logged.
- 4 - (Verbose)** Events with a logging level of four or lower are logged.
- 5 - (Internal)** All events are logged, including debug strings and configuration.

X-Y-Z decided to perform a high level of logging on Security Events and Directory Access. To apply these settings through the registry:

1. On the Active Directory target machine, run `regedit.exe`.
2. Navigate to the following registry subkey:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Diagnostics

3. Assign a value from zero through five for each of the available REG_DWORD values in this Diagnostics subkey. Figure 8-4 on page 158 shows the values that are configured for X-Y-Z's Active Directory servers.

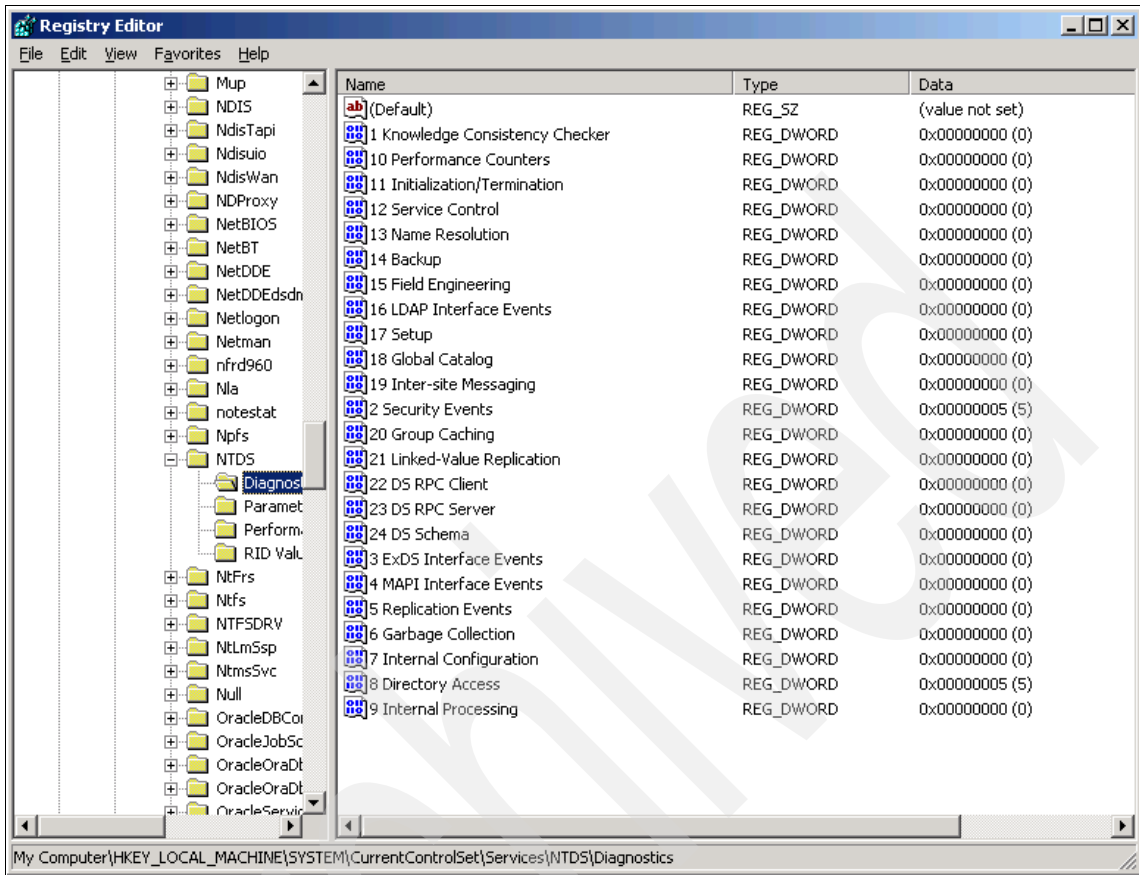


Figure 8-4 Registry settings for Active Directory diagnostic event logging

4. Close regedit.

Active Directory forest: X-Y-Z uses an Active Directory forest. The example in this chapter describes the monitoring of a single Active Directory server only. In reality, to complete the Tivoli Security Information and Event Manager compliance management solution for X-Y-Z, the process for monitoring the single Active Directory server in this chapter must be repeated for each member of the forest.

8.4.3 File server settings: Object access auditing

As we described in 8.1, “Phase one auditing” on page 151, the following Windows 2003 file shares contain sensitive data that must be monitored:

- ▶ C:\Finance
- ▶ C:\HR
- ▶ C:\CustomerData
- ▶ Print Share: C:\WINDOWS\system32\spool

In this section, we describe how to monitor and audit one of these file shares (C:\Finance). X-Y-Z has to repeat this process for all of the shared folders that must be audited.

To enable and configure auditing of access to the C:\Finance folder, complete the following steps on the target file and print servers.

1. Open Windows Explorer, right-click the shared folder, and select **Properties**, as shown in Figure 8-5.

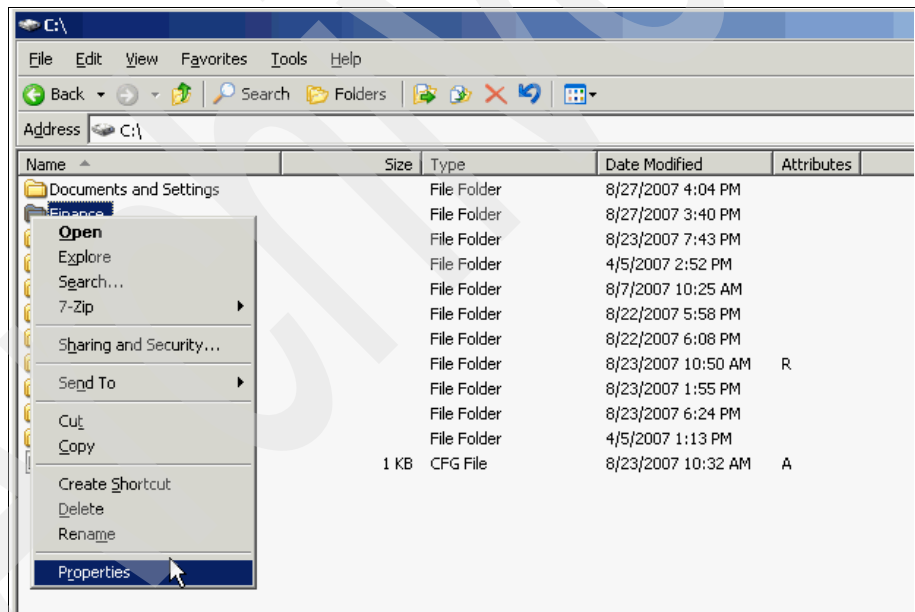


Figure 8-5 Folder properties

2. Go to the Security tab, and click **Advanced**, as shown in Figure 8-6.

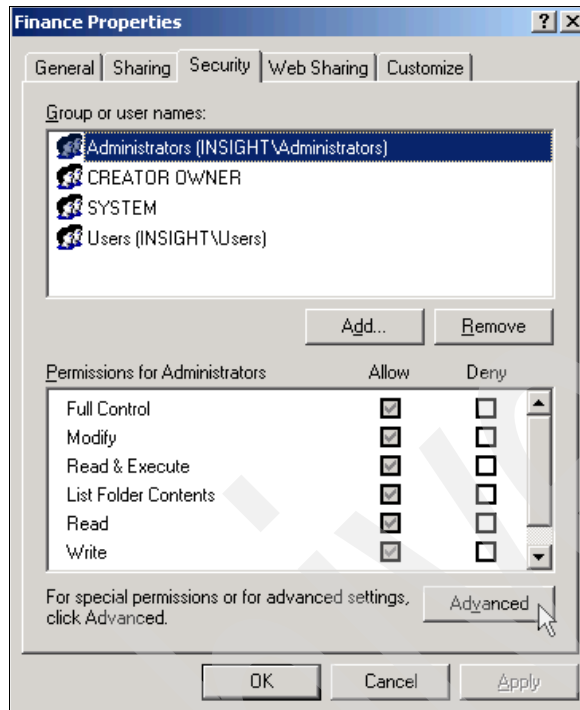


Figure 8-6 Advanced Security options

3. Go to the Auditing tab. Figure 8-7 shows the default contents of this tab.

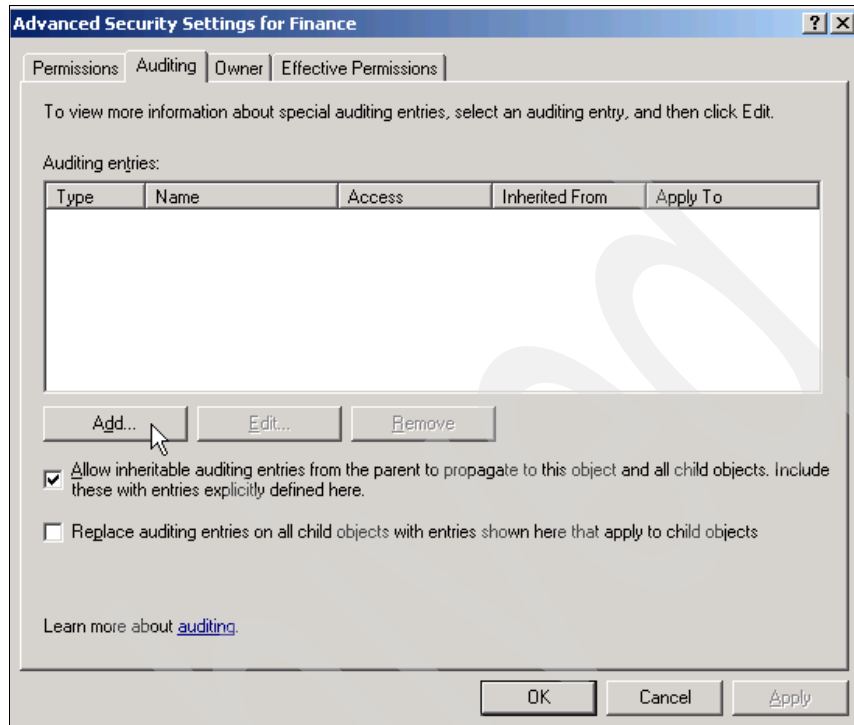


Figure 8-7 Auditing Security settings for a windows folder

4. Configure auditing for a new user or group by clicking **Add**. An input box opens. Enter the name of the user group to be monitored, and click **OK**. In Figure 8-8, the Domain Users group is added because all authenticated users of the X-Y-Z systems are contained in this group.

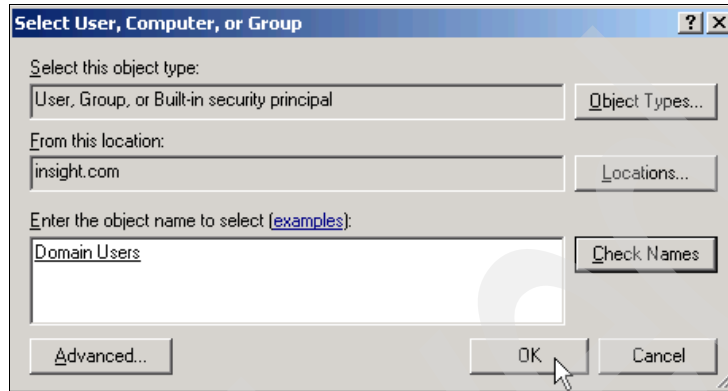


Figure 8-8 Select User, Computer or Group input box

5. An Auditing Entry window for the selected folder opens. In the Apply onto field, select **This folder, subfolders and files** using the available pull-down menu. Set the appropriate Access options before clicking **OK**. As shown in Figure 8-9 on page 163, X-Y-Z elected to monitor the create, read, write, and delete access to this folder and all subfolders and files.

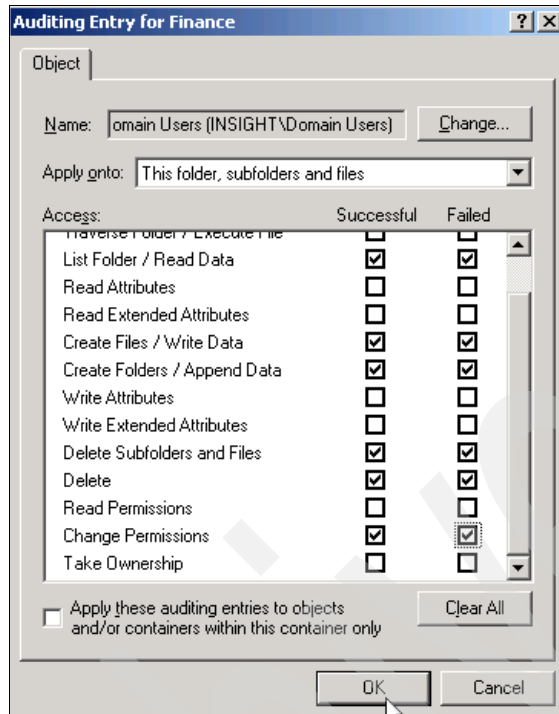


Figure 8-9 Auditing Entry window

6. The new auditing entry now displays in the Advanced Security Settings window, as shown in Figure 8-10. Click **OK** to close.

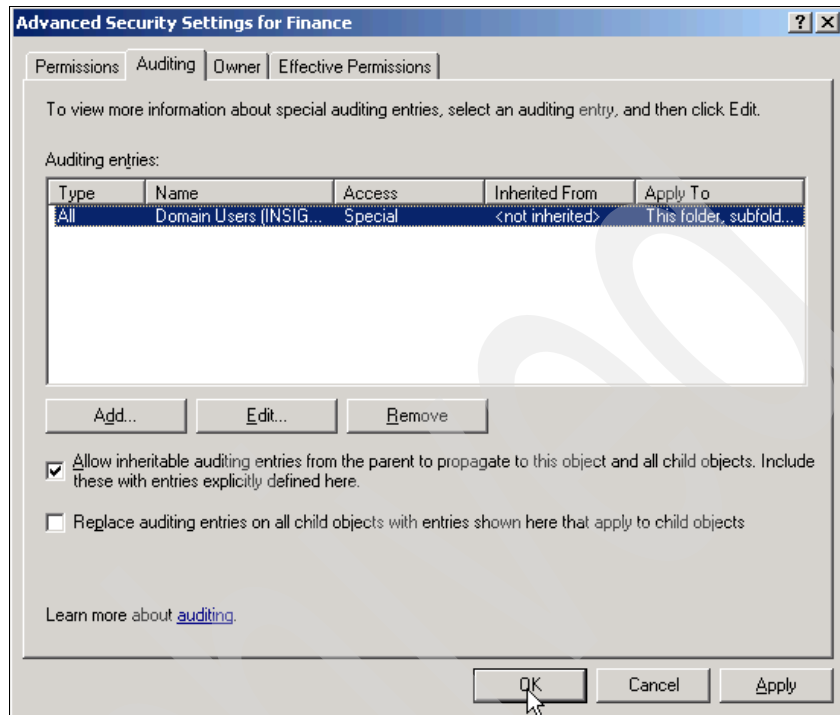


Figure 8-10 The new auditing entry displays in the Advanced Security Settings window

7. Repeat steps 1 through 6 for the other involved file shares.

8.5 Configuring Standard Server for new event sources

Now that the audit subsystems are configured on the target machines, the Tivoli Security Information and Event Manager Standard Server must be configured to monitor the Windows targets. This configuration involves the following high-level steps in the Tivoli Security Information and Event Manager Web portal:

1. Create a Reporting Database to store the event data.
2. Create a Windows Machine Group, and add the machines to be audited.
3. Add the individual event sources for each target machine.

8.5.1 Creating the Reporting Database

To create a new Reporting Database for loading Windows event data:

1. In the Reporting Database view of the Tivoli Security Information and Event Manager portal, navigate to **Portal** → **Tivoli Security Information and Event Manager** → **Configuration and Management** → **Managing Reporting Databases**.
2. Open the Tivoli Security Information and Event Manager Portal.
3. Open the Tivoli Security Information and Event Manager menu.
4. Open the Configuration and Management menu.
5. Open the Managing Reporting Databases page.
6. Choose the Create option from the Select Action pull-down menu, as shown in Figure 8-11.

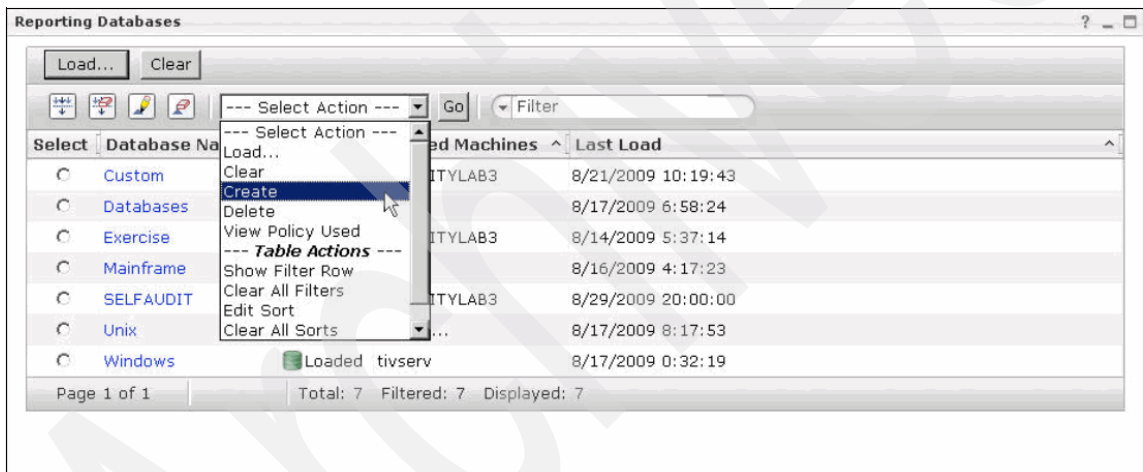
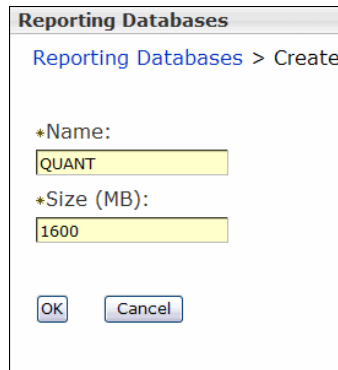


Figure 8-11 Add Reporting Database

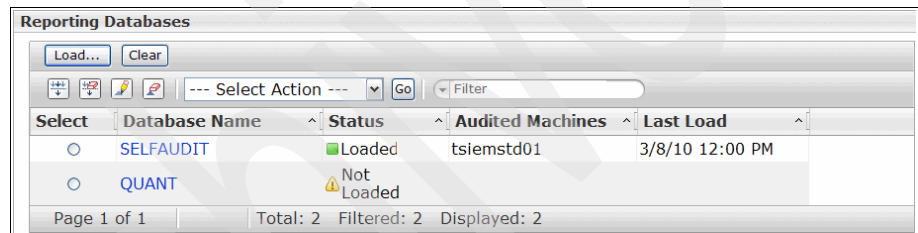
7. As shown in Figure 8-12, enter a name and initial size for the database.



The screenshot shows a dialog box titled "Reporting Databases" with a breadcrumb "Reporting Databases > Create". It contains two input fields: "*Name:" with the value "QUANT" and "*Size (MB):" with the value "1600". There are "OK" and "Cancel" buttons at the bottom.

Figure 8-12 Define name and initial size

Figure 8-13 depicts the page showing the newly created Reporting Database.



The screenshot shows a table with the following data:

Select	Database Name	Status	Audited Machines	Last Load
<input type="radio"/>	SELF-AUDIT	Loaded	tsiemstd01	3/8/10 12:00 PM
<input type="radio"/>	QUANT	Not Loaded		

Page 1 of 1 | Total: 2 | Filtered: 2 | Displayed: 2

Figure 8-13 Reporting Database created

8.5.2 Creating system group and add Windows machines

For Tivoli Security Information and Event Manager to monitor one or more event sources on a particular machine, the audited machine must be registered in the Tivoli Security Information and Event Manager Portal. If desired, the registered machines can be grouped together into *agent groups* to organize the audited systems.

X-Y-Z wants to group their audited Windows machines into a system group called *WindowsSystems* in the Audited Machines view of the Web portal.

Creating Windows system group

To create a system group from the Managing Audited Machines page:

1. From the Tivoli Security Information and Event Manager Portal, select **Tivoli Security Information and Event Manager** → **Configuration and Management** → **Managing Audited Machines**.

- From the pull-down menu, select the **Organize Agent Groups** option, as shown in Figure 8-14.

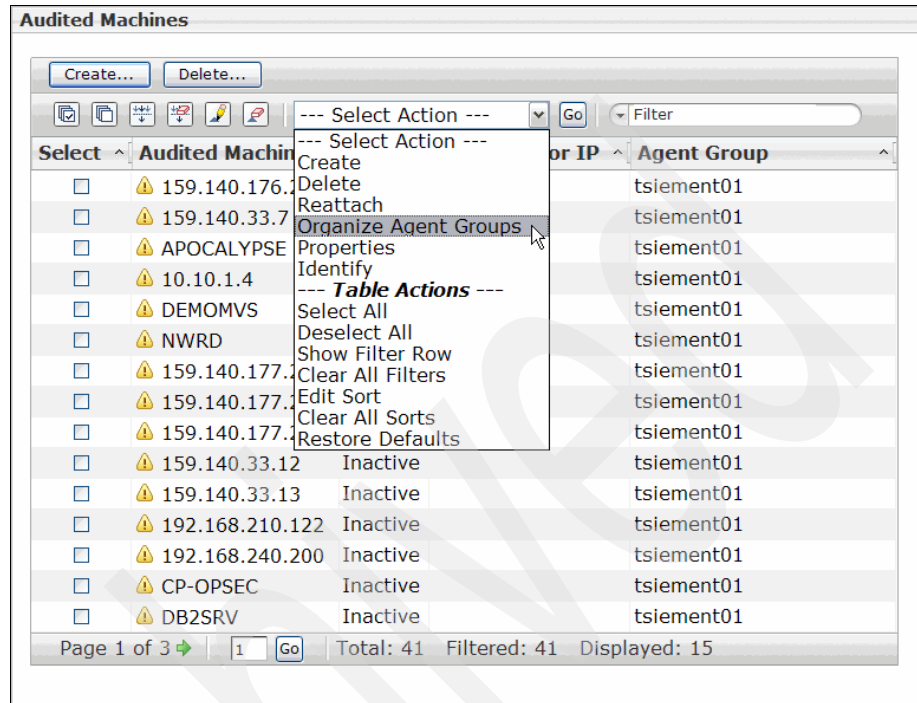


Figure 8-14 Managing Audited Machines

- In the New group name field, Figure 8-15, enter a name for the new machine group. Click **OK**.

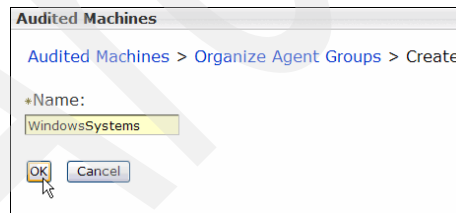


Figure 8-15 Create machine group

The new Machine Group is now displayed in the Machine View window.

Adding Windows target machines

Each of the Windows 2003 servers to be audited must be added as a new machine. X-Y-Z places each of its Windows targets into the new

WindowsSystems group. In this section, we show the setup and configuration for auditing one of X-Y-Z's domain controller servers (FSPDC). X-Y-Z must repeat this process for adding the other Windows target machines.

To add each Windows target machine:

1. In the Tivoli Security Information and Event Manager Portal, go to the Manage Audited Machines page, and click **Create**. The Create Machine Wizard starts, as shown in Figure 8-16.

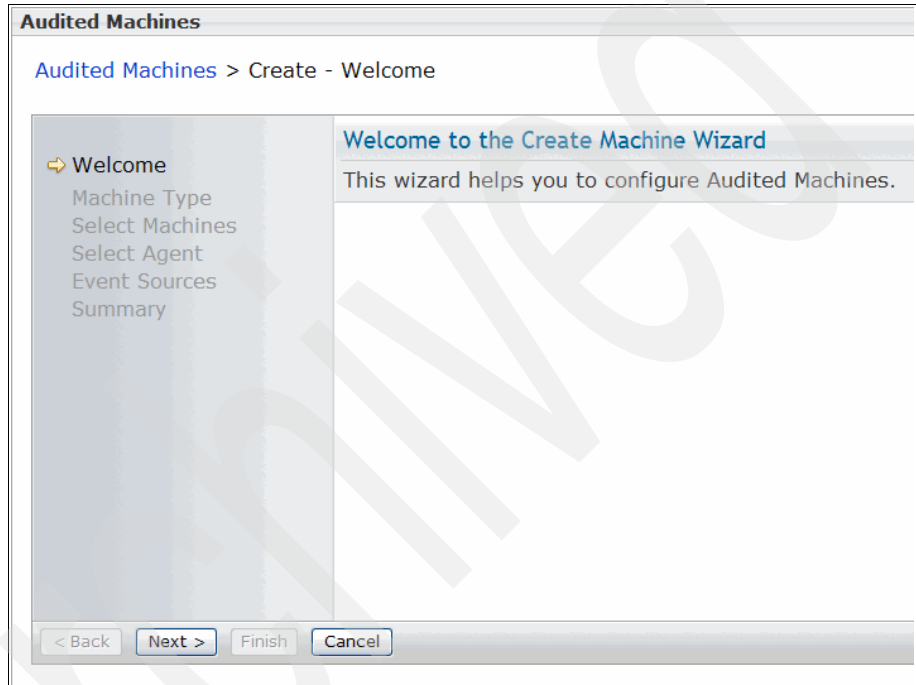


Figure 8-16 Create Machine Wizard

2. Select the Audited Machine Type from the available pull-down menu. For X-Y-Z's Windows 2003 servers, the correct machine type is *Microsoft Windows*, which is highlighted in Figure 8-17. Select **Next**.

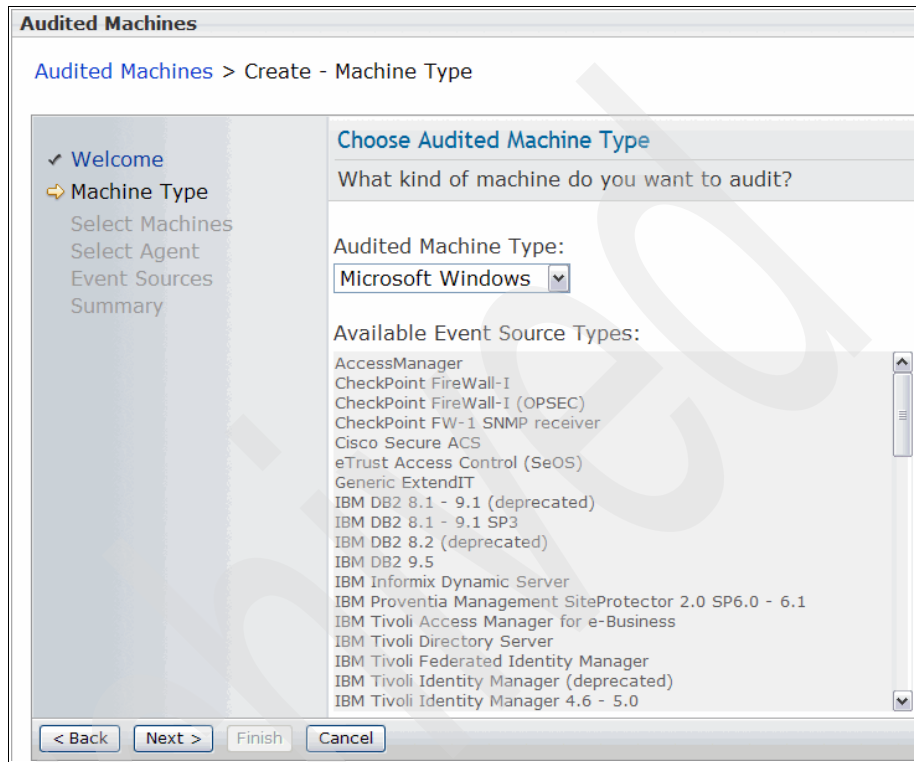


Figure 8-17 Choose Machine Type

3. Enter the name of the target machine or machines to be audited in the Name input box within the Machine frame, and click **Add**. As illustrated in Figure 8-18 on page 170, the machine name now displays in the selected frame. Click **Next**.

Watch the detail: Selecting **Show Event Source Types** causes the Event Source Type panel to display, which allows you to browse the supported event sources for the type of machine that you are adding.

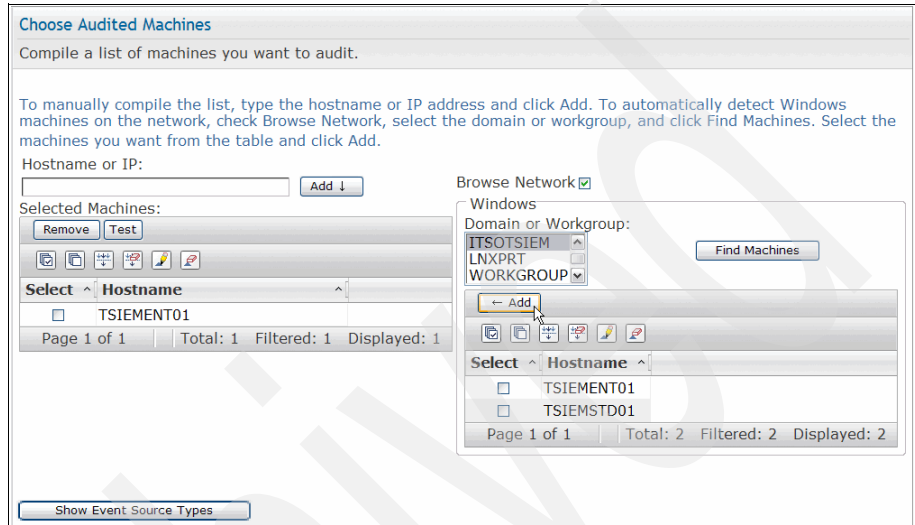


Figure 8-18 Choose Audited Machines

4. A local agent is installed on each of the target machines. This option is selected in Figure 8-19. Click **Next**.

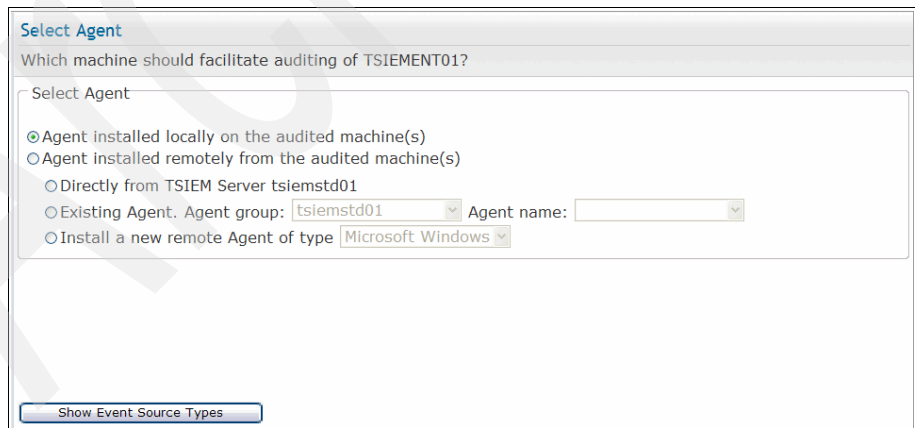


Figure 8-19 Select agent

- The default port that is used for the agent is 5992. Check the availability of the configured port by clicking **Test Port**. In this window, you can choose to perform either an *Automatic* or a *Manual* install.

For demonstration purposes, we show a manual agent installation on a single Windows 2003 target system (TSIEMENT01), as shown in Figure 8-20. When adding the remaining Windows 2003 server machines in Tivoli Security Information and Event Manager, X-Y-Z can use the option of automatically installing the Windows agents on the targets.

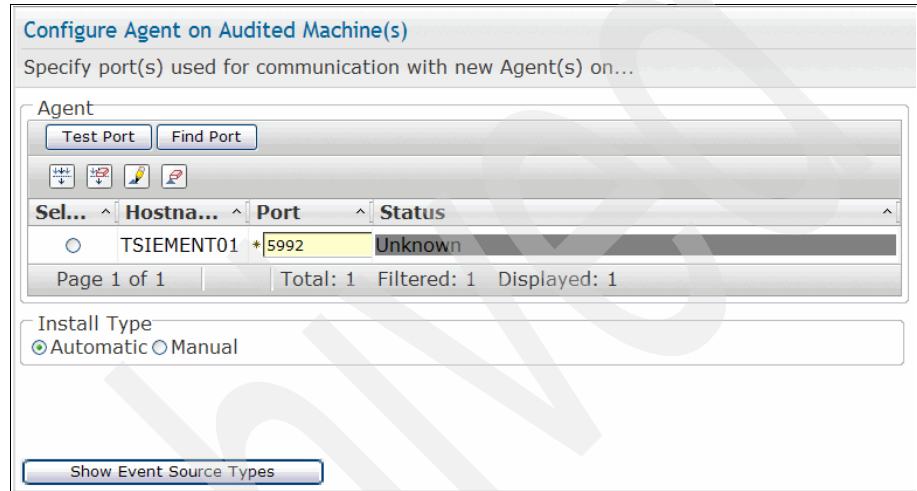


Figure 8-20 Configure new agent

- The port we configured is available, so the message box that is shown in Figure 8-21 displays. Click the Test Port message box, and click **Next** in the New agent window to advance the Wizard.

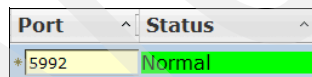


Figure 8-21 Test Port success

- The Choose Event Source Type window opens. For the TSIEMENT01 machine, which is an Active Directory Domain controller, both Microsoft Active Directory and Microsoft Windows are selected, as shown in Figure 8-22 on page 172. Select **Next**.

Watch the detail: When adding the Windows 2003 server machines that are not Active Directory servers, only the Microsoft Windows event source are selected.

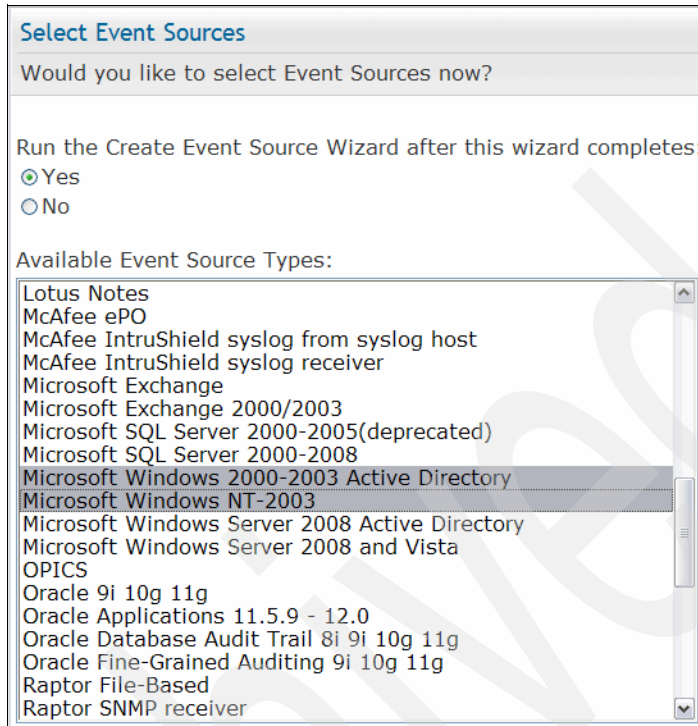


Figure 8-22 Choose event source type

- Figure 8-23 shows the Completing the Create Machine Wizard window that appears. Click **Finish** to complete the Add Machine setup.



Figure 8-23 Complete Create Machine Wizard

Important: During the Create Machine Wizard, a configuration file is created. This file is needed when you install the agent on your target machines.

8.5.3 Adding event sources

Immediately after the Add Machine wizard completes, the Event Source Wizard automatically runs one time for each event source that you selected in step 7, in the previous section “Adding Windows target machines” on page 167.

For the TSIEMENT01 domain controller that was just added, the wizard runs twice: one time for Microsoft Active Directory and one time for Microsoft Windows.

In this section, we illustrate how to complete the Add Event Source Wizard for the Microsoft Active Directory event source on the TSIEMENT01 Windows server. The wizard for the Microsoft Windows event source on TSIEMENT01 is similar and so are the wizards for each of X-Y-Z’s other Windows server event sources.

To complete the Microsoft Active Directory event source wizard for the TSIEMENT01 server, follow these steps:

1. On the Event Source Wizard welcome window, shown in Figure 8-24, click **Next**.

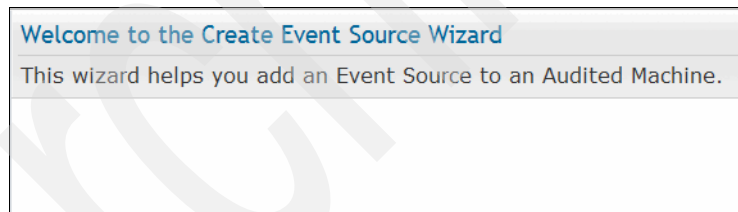
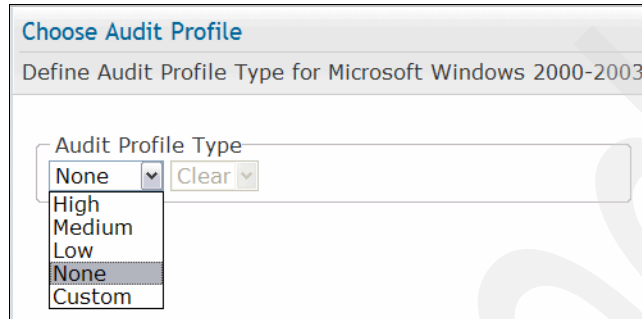


Figure 8-24 Add Event Source Wizard

- The Choose Audit Profile window opens. X-Y-Z already configured the audit subsystems on each of the target machines and wants Tivoli Security Information and Event Manager to leave those existing settings. Therefore, the option **None** is selected in Figure 8-25. Click **Next**.



Choose Audit Profile

Define Audit Profile Type for Microsoft Windows 2000-2003

Audit Profile Type

None Clear

High

Medium

Low

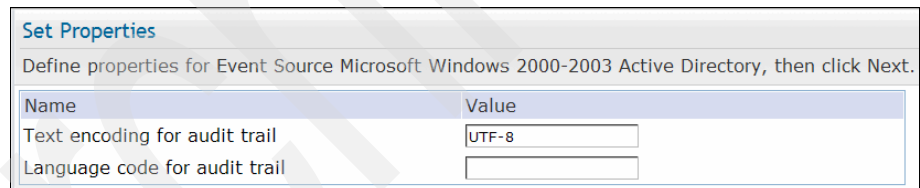
None

Custom

Figure 8-25 Choose an Audit Policy Profile

- Next, you must configure the event source properties. The set of properties differ from event source to event source. The *IBM Tivoli Security Information and Event Manager Version 2.0 Event Source Guide, SC23-9687* explains for each event source what properties can be configured.

You must set the properties, as shown in Figure 8-26.



Set Properties

Define properties for Event Source Microsoft Windows 2000-2003 Active Directory, then click Next.

Name	Value
Text encoding for audit trail	UTF-8
Language code for audit trail	

Figure 8-26 Set event source properties

Tivoli Security Information and Event Manager supports English, German, Spanish, French, Italian, Japanese, Korean, Brazilian, Portuguese, Simplified Chinese, Traditional Chinese, Russian, Hungarian, and Polish language codes.

The contents of audit data, which can be gathered from various target platforms and applications, might depend on the language or locale settings that are set on the target systems. Every event source attempts to automatically determine the proper encoding and language in use for the collected log data. If the encoding or language is not correctly determined by the event source, you can use these two event source properties to specify the desired value.

If the automatic detection returns no results, the settings default to English language data.

Important: Ensure that these properties are set appropriately, they have crucial significance on the correctness of log data being interpreted, processed, and displayed by all Tivoli Security Information and Event Manager components.

If the data that is displayed in reports and in the Tivoli Integrated Portal does not appear to be correct or is unreadable, the automatic detection might have failed. If this condition occurs, set these properties manually to the correct values. Changing these values does not affect data that was already collected. To correct data that was already collected, manual updates to the log set header files is required, which can be a time consuming process.

– Text encoding for audit trail

This setting specifies the text encoding of the text data for collected log data sets. The default value is the empty string, which indicates that the event source must automatically determine the text encoding for the collected data. If the encoding is not correctly determined by the event source, you can specify that a specific text encoding be applied.

Default values: This event source property is only available for those event sources that do not already have a text encoding-type property defined. For the following event sources, the default value is predefined as UTF-8 and does not need to be changed:

- ▶ Microsoft Exchange 2000/2003
- ▶ Microsoft Windows 2000 - 2003 Active Directory
- ▶ Microsoft Windows NT® - 2003
- ▶ Oracle 9i 10g 11g
- ▶ ScanMail for Microsoft Exchange

– Language code for audit trail

This setting specifies the language code of the text data for collected log data sets. The default value is the empty string, which indicates that the event source automatically determines the language that is used for the collected data. In Table 8-2, we list the valid language code values that can be specified for this property.

Table 8-2 Language codes

Language	Code
Arabic	ar

Language	Code
Brazilian Portuguese	pt BR
French	fr
German	de
Hebrew	iw
Hungarian	hu
Italian	it
Japanese	ja
Korean	ko
Polish	pl
Russian	ru
Simplified Chinese	zh CN
Spanish	es
Traditional Chinese	zh TW

4. In Figure 8-27 on page 177, we choose a *collect schedule*. A collect schedule must be tuned to prevent audit trail loss because the event log overwrites itself. Configure the desired schedule, and click **Next**.

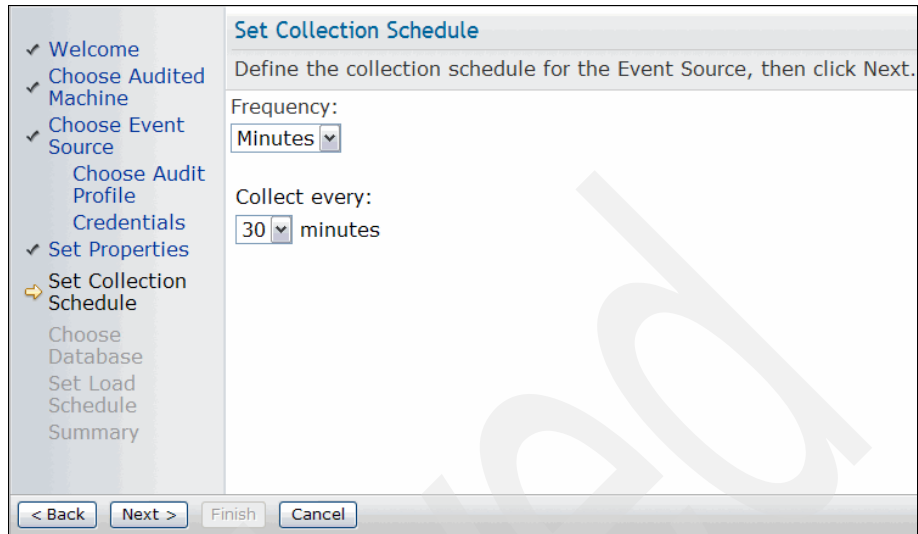


Figure 8-27 Choose a Collection Schedule

- In Figure 8-28, you select the Reporting Database where the data collected from this event source is loaded. X-Y-Z loads all Windows events in the Reporting Database called GENERAL that was created in 8.5.1, “Creating the Reporting Database” on page 165. We select Windows, as shown in Figure 8-25 on page 174. Click **Next**.

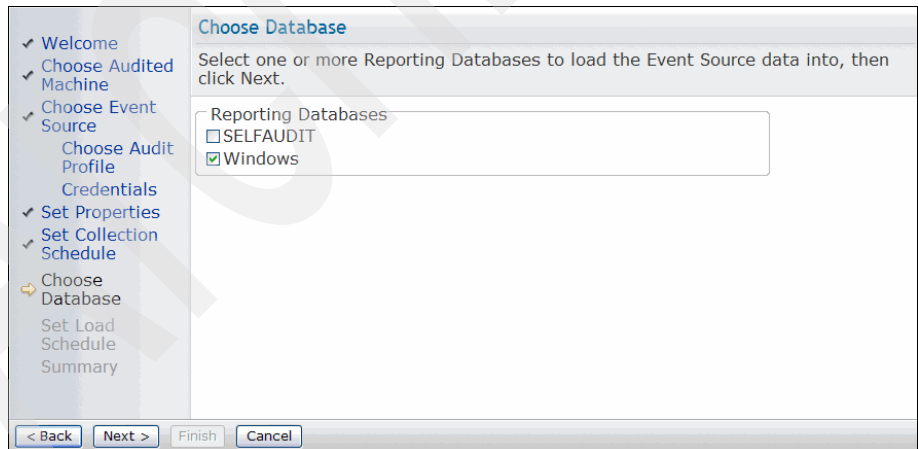


Figure 8-28 Choose a Reporting Database

More details: Data collected from your TSIEM01 machine is first stored in the Depot. At load time it is loaded into the Reporting Database, which here is Windows.

6. In Figure 8-29, you configure a Load schedule for loading the data from the event source into the Windows Reporting database. The Load schedule must be related to the Collect schedule that we configured in step 3. Configure the Load schedule, and click **Next**.

Configuration tip: In general, set load frequency to an interval as long as or longer than the collect schedule interval, for example, data might be collected hourly and loaded twice a day. It is unlikely that you want to collect data twice a day, and load it hourly.

Set the load schedule time at least 15 minutes after each scheduled collection time. This delay ensures that Tivoli Security Information and Event Manager loads the most recently collected data into the database.

Set Database Load Schedule

Define the schedule for Event Source data to be loaded into the Windows Reporting Database.

Frequency: Daily

Load every:
 Working day
 Day

Data that is:
 New data
 Last 1 days of data

+Starting at:
1:54 PM

< Back Next > Finish Cancel

Figure 8-29 Choose a Load Schedule

- The Event Source Wizard is now complete and the final window, shown in Figure 8-30, is displayed. Click **Finish**.

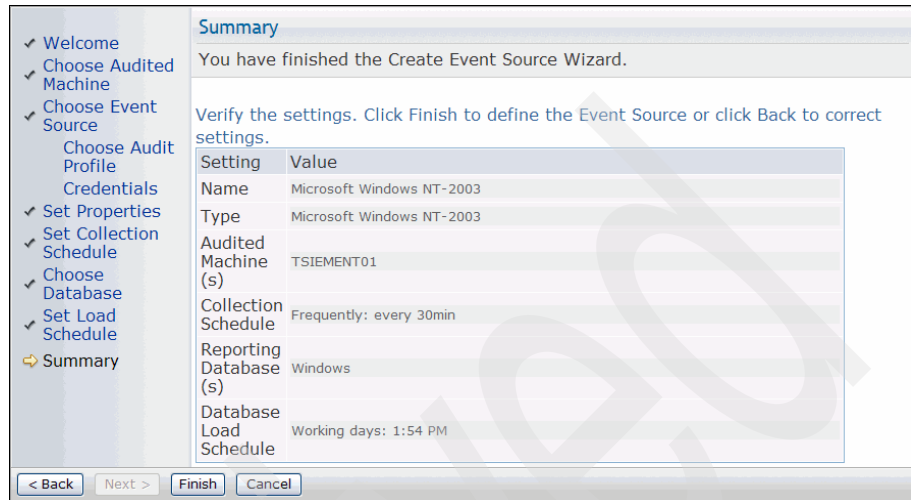


Figure 8-30 Complete the Add Event Source Wizard

8.6 Installing an agent on the target machine

We selected the *manual* install type when we added the machine through the Add Machine wizard in step 5 of “Adding Windows target machines” on page 167. Therefore, the Windows agent must be installed manually on the FSPDC Windows server.

To install the agent locally on the Windows 2003 server:

1. On the TSIEM x86_nt_4 CD, start the installation wizard. The Setup.exe file is located in the x86_nt_4 directory. The Welcome window in Figure 8-31 is displayed. Click **Next**.

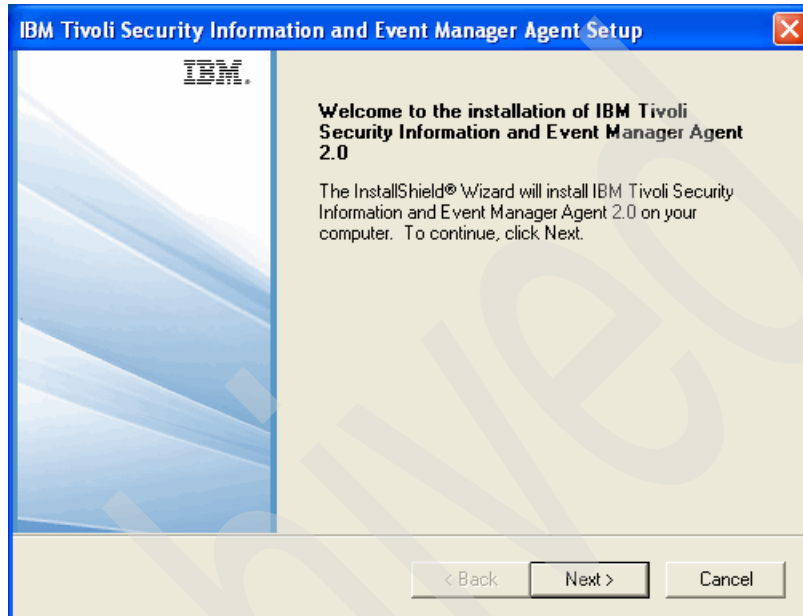


Figure 8-31 Welcome window of installation Wizard

2. Enter the path to the installation directory. The default location C:\IBM\TSIEM is being used on the target machine, as shown in Figure 8-32. Click **Next**.

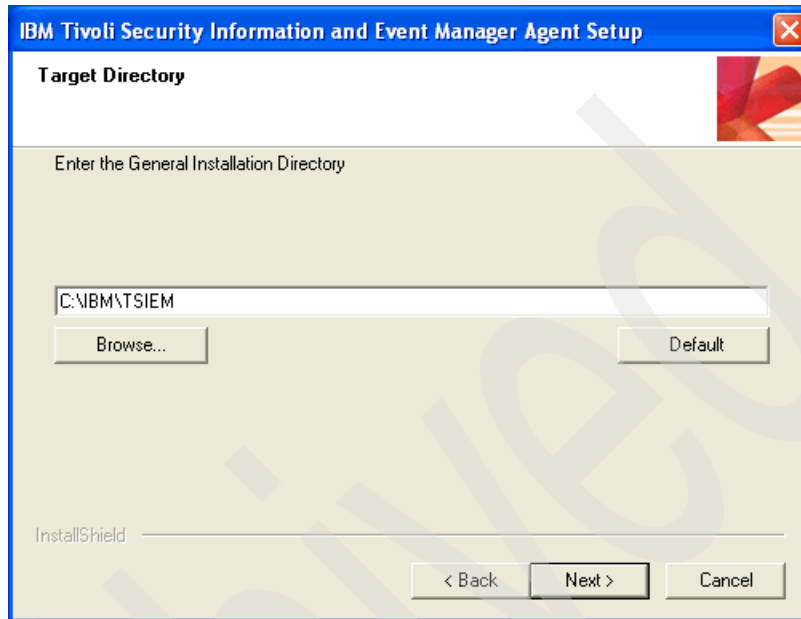


Figure 8-32 General Installation Directory

3. The Select Configuration File window displays, as shown in Figure 8-33 on page 182. To complete this window, the configuration file, that was created when running the Add Machine Wizard, must be made available to the target machine.

Configuration details: The default location for this configuration file on the Tivoli Security Information and Event Manager Standard Server is:

```
<TSIEMHomeDir>\Server\config\machines\<TSIEMServerName>.cfg
```

Copy this configuration file to the target machine, enter the complete path to the file locally, and click **Next**.

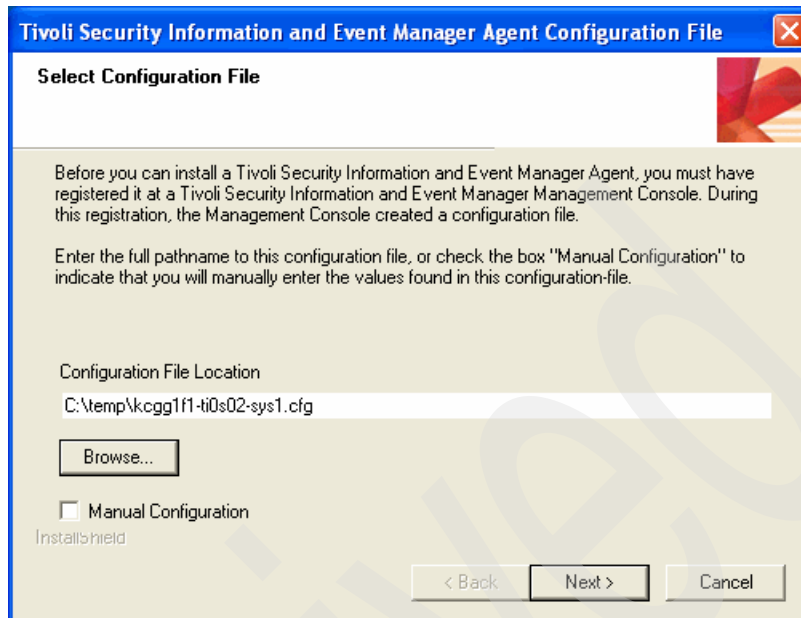


Figure 8-33 Select Configuration File

4. In the Enter OS Account window, Figure 8-34, you can configure an operating system account that will be used to run the Tivoli Security Information and Event Manager agent service. X-Y-Z is using an account called *cearoot_os*. Click **Next**.

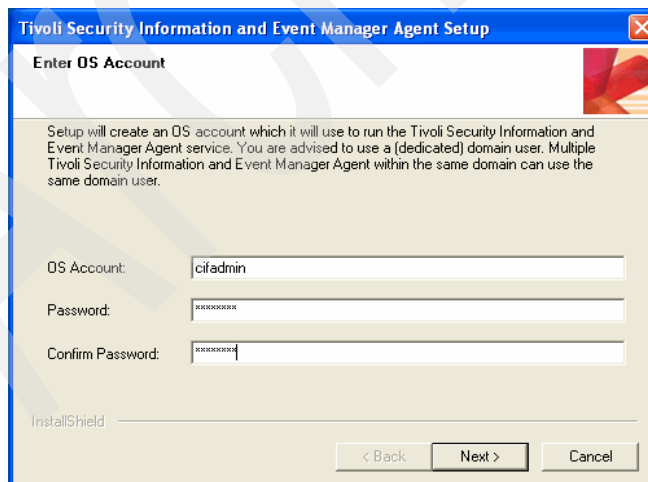


Figure 8-34 Enter OS Account

Configuration details: In this case, we are using a local account, however you can also use a Domain account.

The set up process is performed. A Setup Status window displays to monitor the progress of the setup tasks, as shown in Figure 8-35.

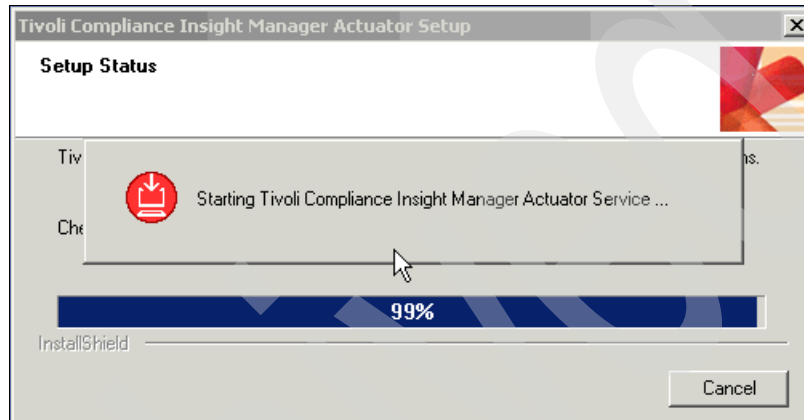


Figure 8-35 Setup Status

The agent Installation Wizard is now complete and the Setup Finished window opens, as shown in Figure 8-36. Click **Finish**.

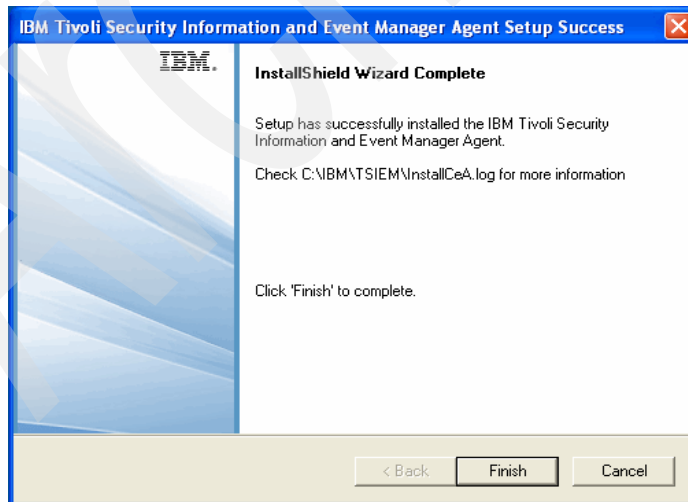


Figure 8-36 Setup Completion

8.7 Configuring W7 groups

Now that the audit subsystems are configured on the Windows servers and the event sources are registered with Tivoli Security Information and Event Manager, the W7 rules can be configured on the Standard Server. In particular, the groups must be defined along with appropriate W7 policy and attention rules.

In this section, we describe the process of setting up the W7 rules for X-Y-Z's Windows event sources.

Adding User Information Source

To create meaningful policy and attention rules, it is important to define W7 groups that represent the structure of your IT environment. To assist with creating these W7 groups, using Tivoli Security Information and Event Manager you can import grouping data from an existing User Information Source (UIS).

X-Y-Z imports the user information from Active Directory to simplify the creation of their W7 grouping definitions.

To import this UIS data:

1. Open the System menu, and select **Add** → **User Information Source**, as shown in Figure 8-37 on page 185.

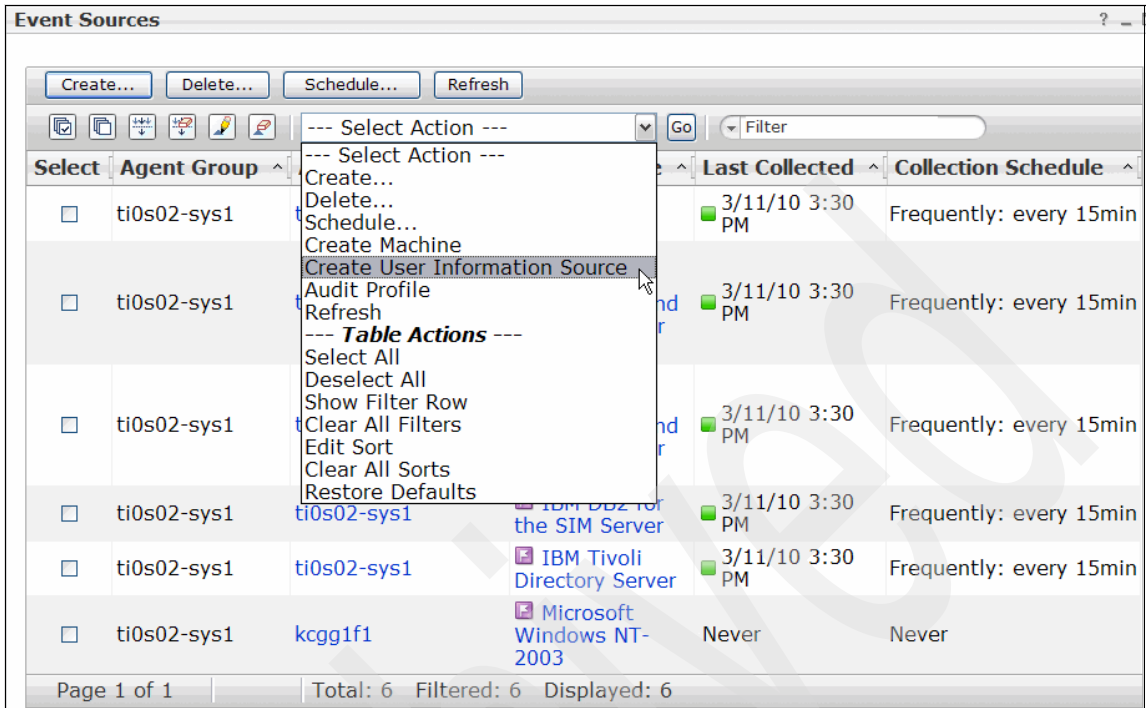


Figure 8-37 Add User Information Source

2. The Add User Information Source Wizard starts. On the welcome window, click **Next**, as shown in Figure 8-38 on page 186.

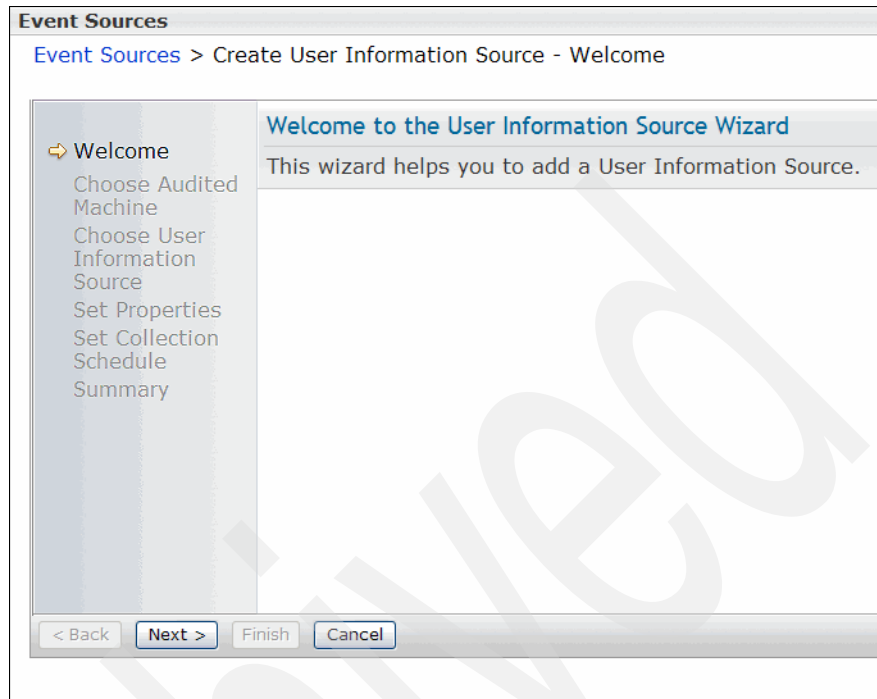


Figure 8-38 Add User Information Source Wizard welcome window

3. In the next window that displays, you can select the machine where the User Information Source resides. Figure 8-39 on page 187 shows that for this example, the AD server is selected. Click **Next**.

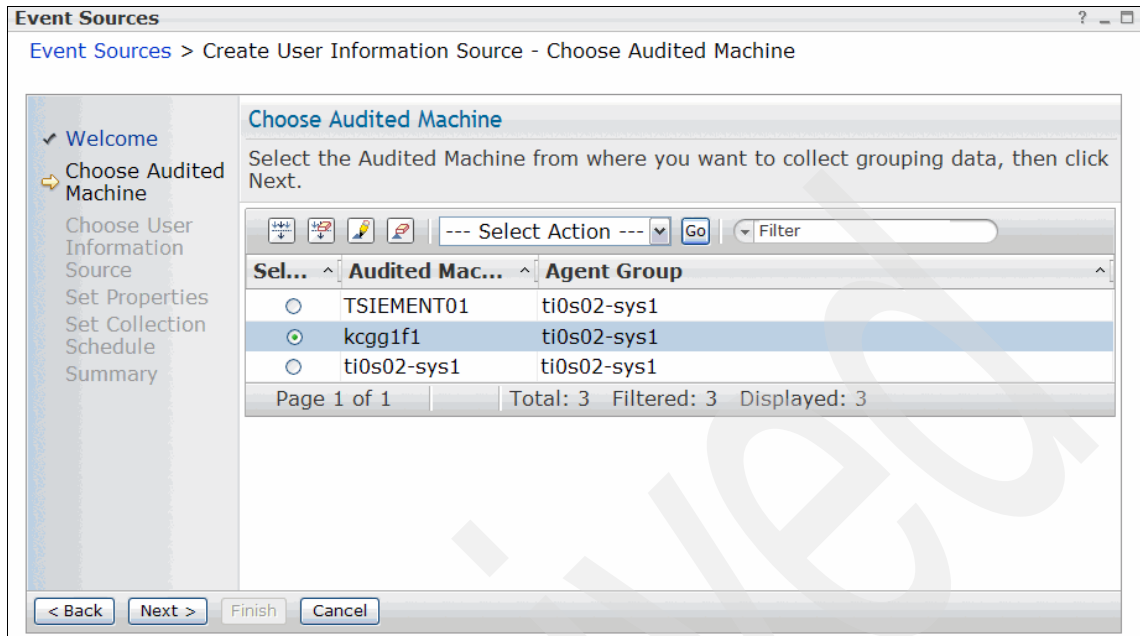


Figure 8-39 Choose a Machine

- The Choose a User Information Source window displays. As shown in Figure 8-40 on page 188, you choose to import the Active Directory groupings from the AD server, and click **Next**.

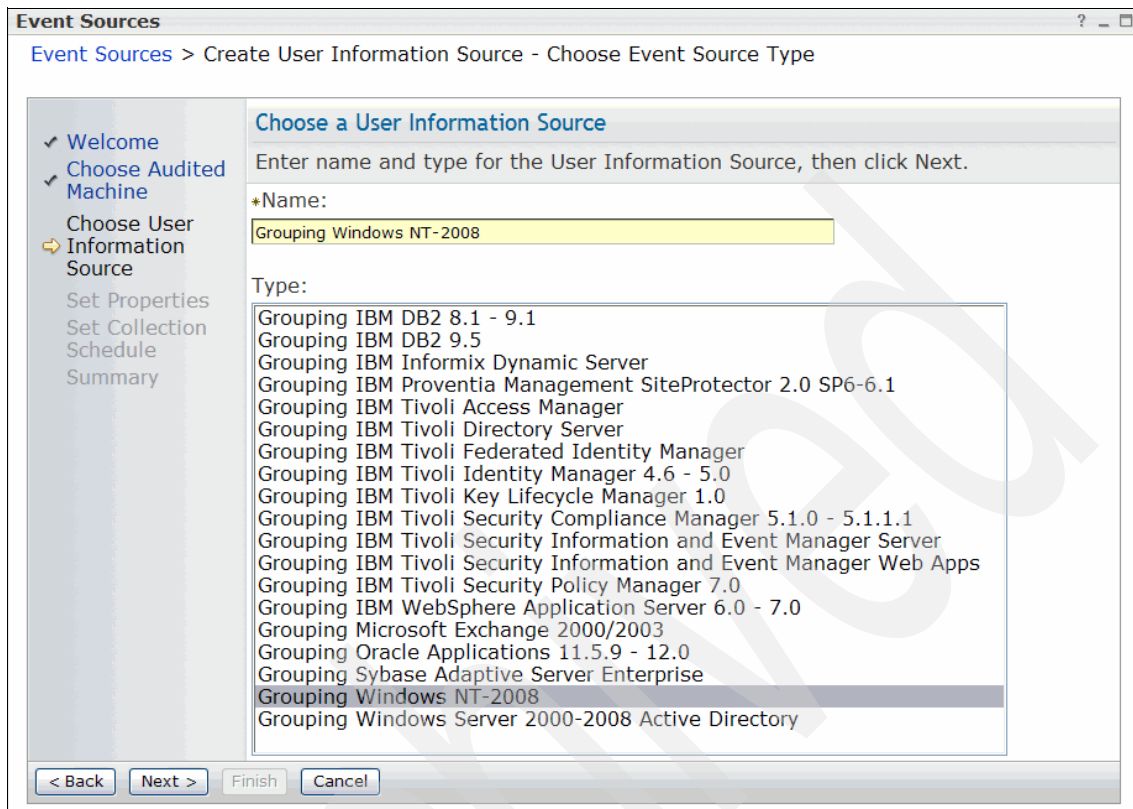


Figure 8-40 Choose a User Information Source

5. The User Information Source properties are displayed on the next window, as displayed in Figure 8-41 on page 189. Click **Edit** to modify the Domain name.

Configuration details: The difference between Grouping ActiveDirectory and Grouping Windows is that Grouping ActiveDirectory is for Active Directory on Windows 2000 and Windows 2003 and Grouping Windows is for Windows NT domains.

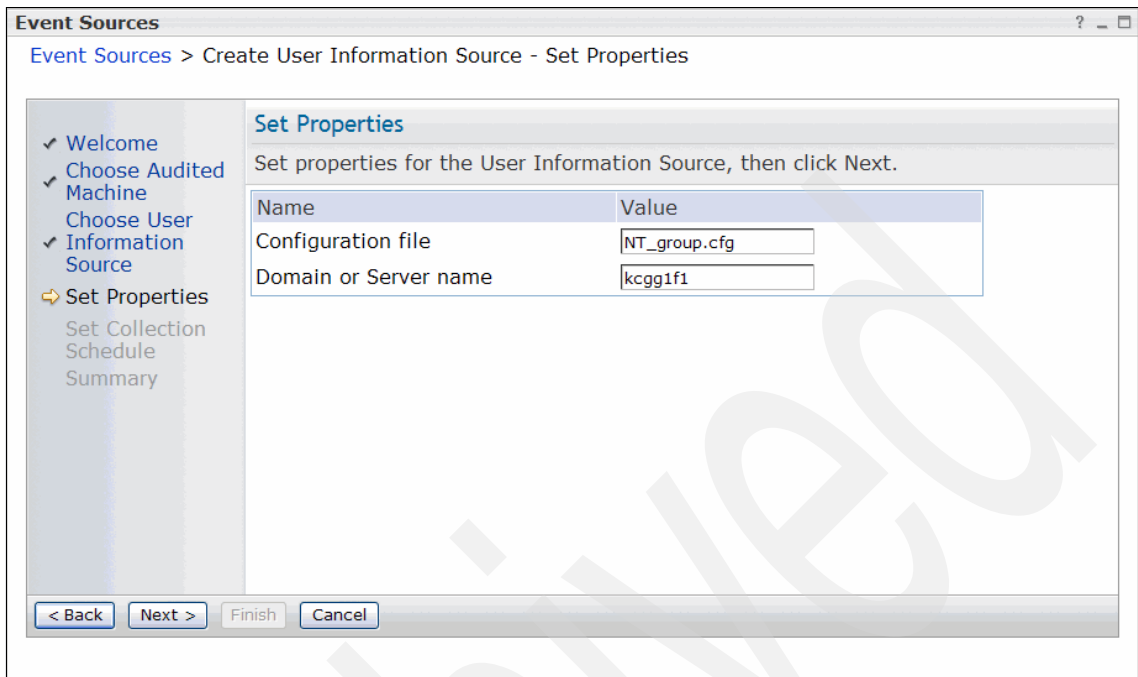


Figure 8-41 User Information Source Properties

6. You can now enter the name of the Active Directory domain, as shown in Figure 8-42. X-Y-Z used the domain name INSIGHT to represent all of its users who are being monitored by Tivoli Security Information and Event Manager. Click **Next**.

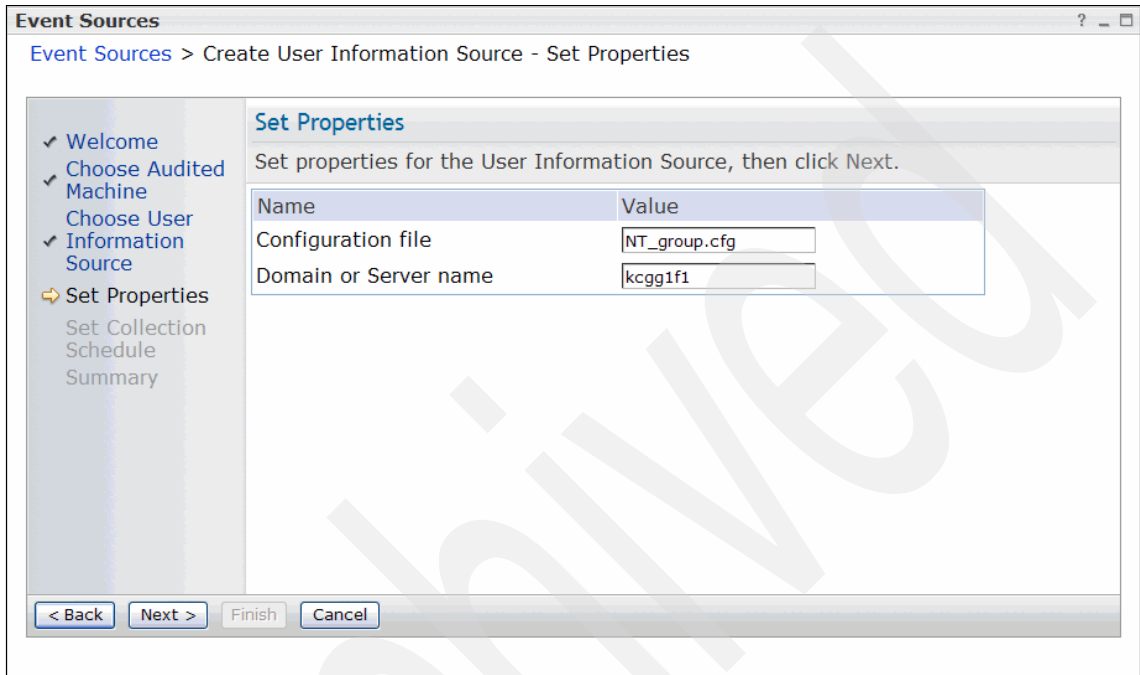


Figure 8-42 Define User Information Source

- Now, choose a collect schedule for extracting information from the specified UIS, as shown in Figure 8-43. Click **Next** to continue.

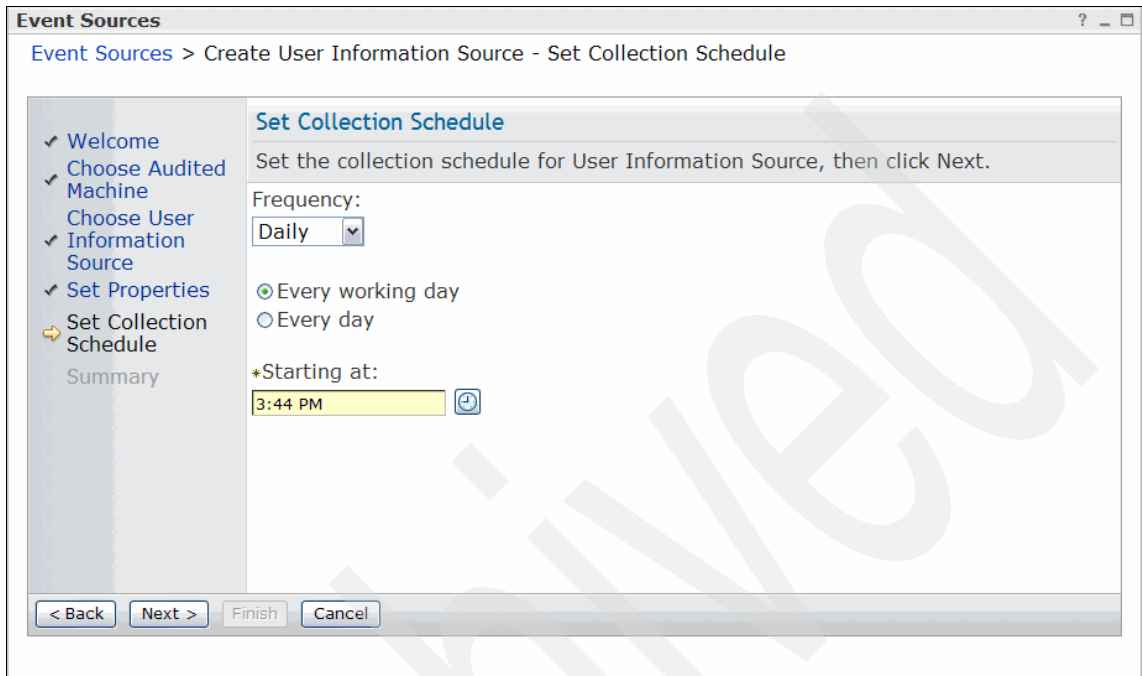


Figure 8-43 UIS Collect Schedule

- The Add User Information Source completion window displays. You must collect the UIS data before the (last) collection of the audit trail occurs. In that way you are sure that the UIS data is applied to the chunks that are analyzed. Click **Finish** to complete the process, as shown in Figure 8-44.

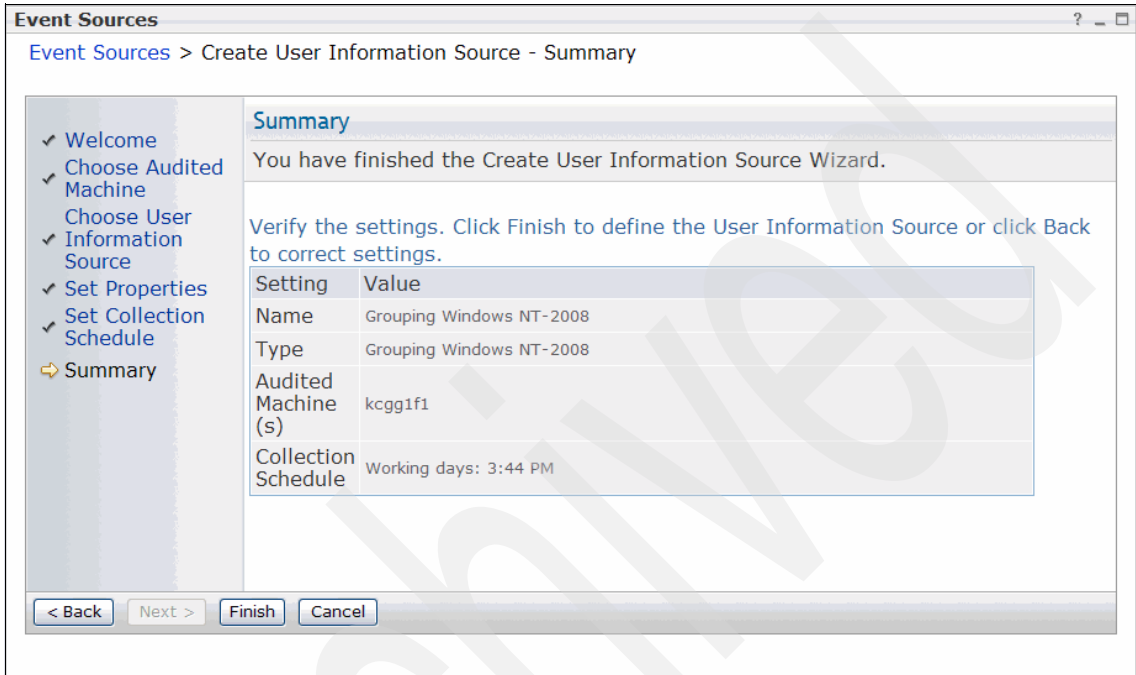


Figure 8-44 Completing the Add User Information Source Wizard

The new User Information Source displays in the event sources view of the Web portal, as shown in Figure 8-45 on page 193.

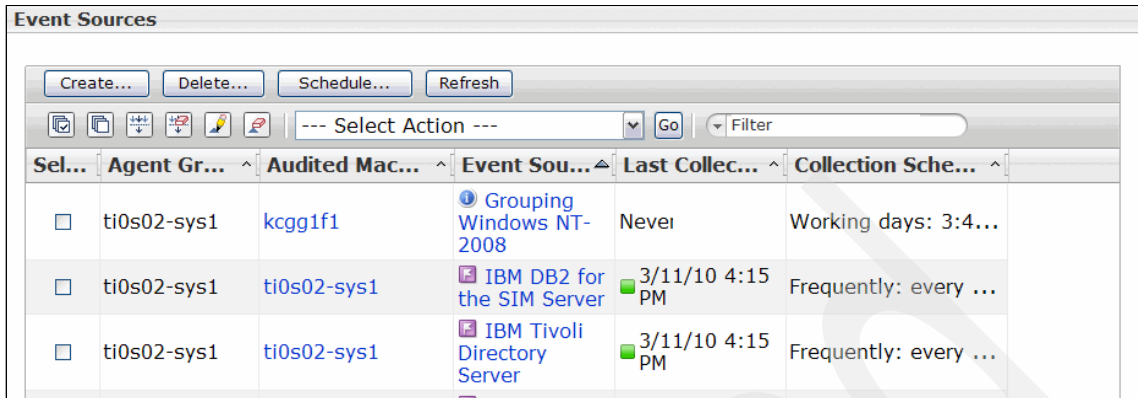


Figure 8-45 Grouping ActiveDirectory UIS is available in the Web portal

Viewing the User Information Source

When the first scheduled UIS collection is complete, we can view the user information grouping definitions that were collected.

Select **Policies** → **Policy Explorer** → **Show Automatic**, and choose the current time to get the most recent grouping definition.

Configuration details: If there is more than one UIS defined in the Web portal, you have the option to select which Automatic Policy you want to view. Each UIS will show the name of the machine being used to collect the UIS data.

Figure 8-46 shows how to view the automatic policies.

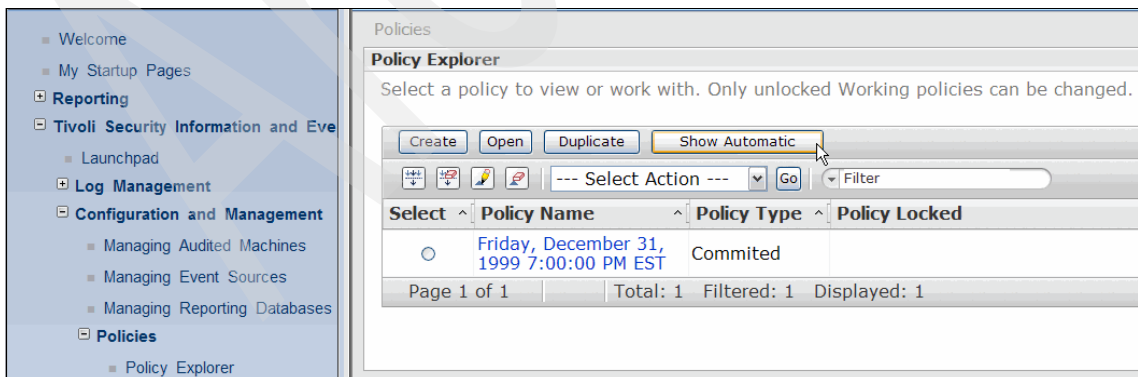


Figure 8-46 View the automatic policies created by the UIS

8.7.1 Configuring a new policy with W7 rules

Policy building is a crucial part of using Tivoli Security Information and Event Manager to effectively monitor your environment. Policy building is essentially the combination of W7 groups. You can combine W7 elements to create policy and attention rules.

As described in Chapter 4, “IBM Tivoli Security Information and Event Manager component structure” on page 53, if the rule is added to the set of policy rules, this rule marks all normalized events that match it as *normal* events. Therefore, events that match policy rules are not displayed in policy exception reports. Meanwhile, if the rule is added to the set of attention rules, all normalized events that match the attention rule are marked as attention events. These attention events show up in the special attention reports.

The following process can be used to create a new policy for X-Y-Z that includes grouping and policy rules for the Windows event sources that are being monitored for phase one:

1. Duplicate the latest committed policy to create a new working policy.
2. The new working policy can be used for customizing the W7 group definitions. The Group Definition Set from the UIS can be imported into this policy.
3. Policy building. Create appropriate W7 policy rules and attention rules.
4. Load the database using this working policy.
5. Commit the policy when the W7 rules are producing the desired results.

Let us describe each of these five steps in more detail now.

Creating a new work policy

X-Y-Z is going to use the default committed policy that is installed with Tivoli Security Information and Event Manager as the foundation for the policy that they must develop.

To create a *Work* policy in the Tivoli Security Information and Event Manager Portal Policies:

1. Select the most recent committed policy, and select **Duplicate**, as shown in Figure 8-47 on page 195.

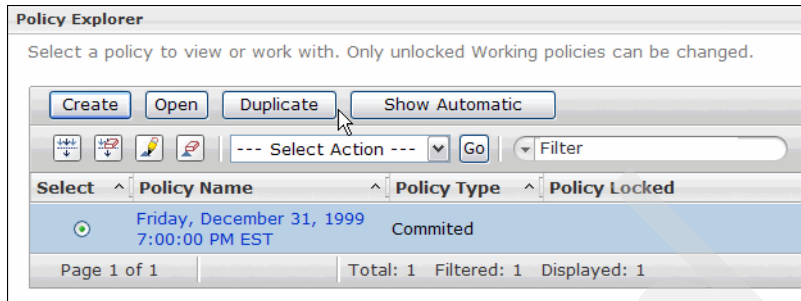


Figure 8-47 Create a new working policy

2. Assign a new name to the duplicate policy, as shown in Figure 8-48.

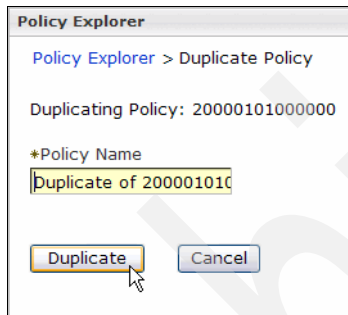


Figure 8-48 Duplicate policy

A new policy appears under the Work folder as shown in Figure 8-49.

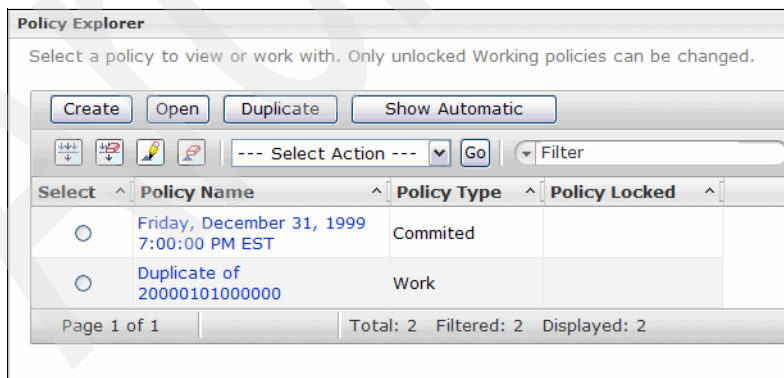


Figure 8-49 Work policy

Customizing group definitions

We also must create other grouping rules to describe sensitive organization assets. As an example, the following figures show how X-Y-Z describes the Windows locations of their confidential financial data. In 8.1, “Phase one auditing” on page 151, we explained that the Windows file servers have a number of directories that contain sensitive corporate data. The financial data is stored within the C:\Finance directory.

A W7 rule must be created in the new Tivoli Security Information and Event Manager policy to describe this corporate asset. The default policy that was used as the basis for this working policy already has a number of predefined groups that are initially empty. X-Y-Z decided to use the existing FinancialData - Medium group to represent the C:\Finance file share on the Windows servers. In the future, they can decide to have more fine-grained control of financial assets by adding rules to classify financial assets as either *High*, *Medium*, or *Low*.

To specify a W7 group definition to describe the Financial file share on the Windows servers:

1. After opening the work that needs to be adjusted, choose the Manage Groups option, as shown in Figure 8-50.

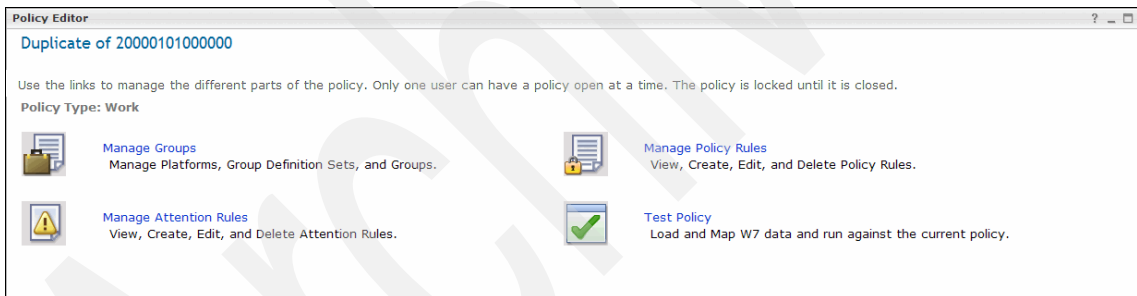


Figure 8-50 Choose the action on the work policy

2. Open the NT group definitions, as shown in Figure 8-51 on page 197.

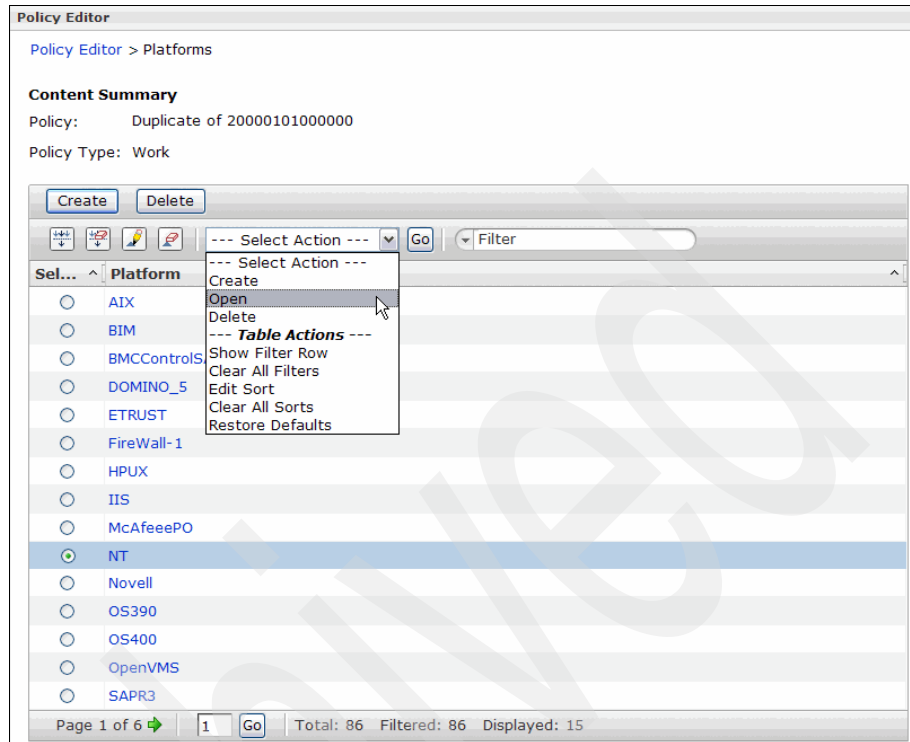


Figure 8-51 Open the platform type folder

3. After opening the appropriate platform type folder, continue with opening the grouping file, as shown in Figure 8-52 on page 198.

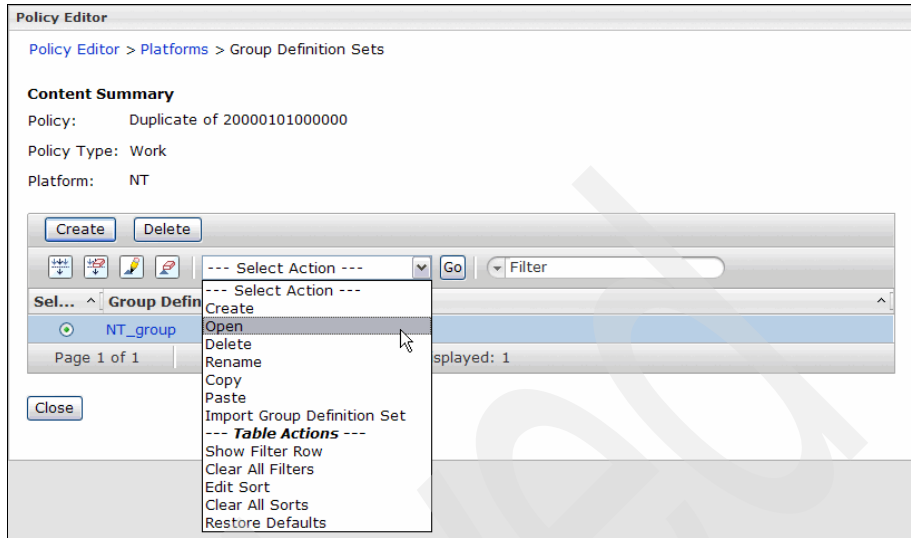


Figure 8-52 Open the group file

4. You can create a new group, as shown in Figure 8-53, by clicking **Create**.

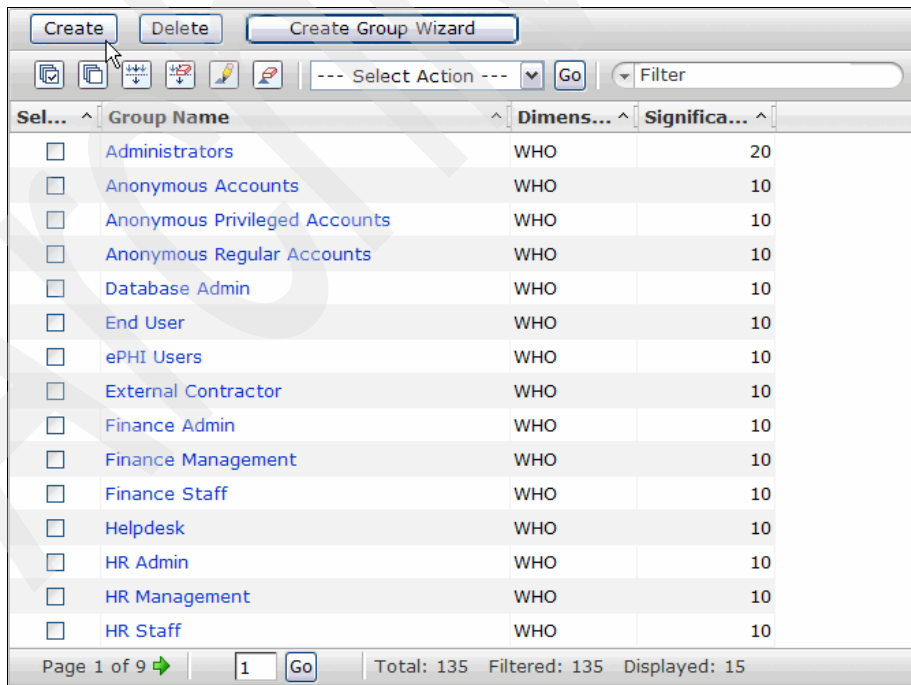


Figure 8-53 Create a new group

- Alternately, you can find the group in the list by filtering on the name, as shown in Figure 8-54.

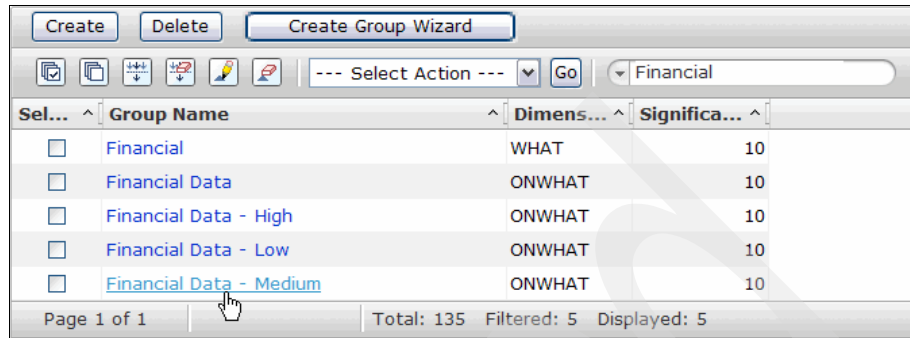


Figure 8-54 Find an existing group

- Open the group, and create a new requirement, as shown in Figure 8-55.

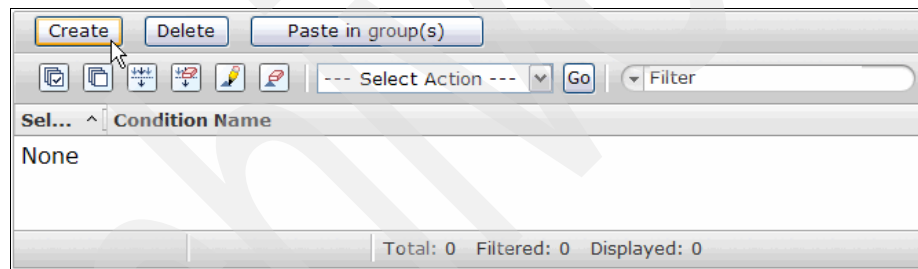


Figure 8-55 Create new requirement

- Object access auditing was configured in 8.4.3, “File server settings: Object access auditing” on page 159. These configured audit settings on the target machine result in user actions on the C:\Finance folder (and its contents) being logged by Windows. These logged events describe actions on the finance share. When mapped by Tivoli Security Information and Event Manager, these events have a W7 Object Path value that starts with C:\Finance.

Therefore, the requirement *Object Path starts with C:\Finance* is configured, as shown in Figure 8-56 on page 200.

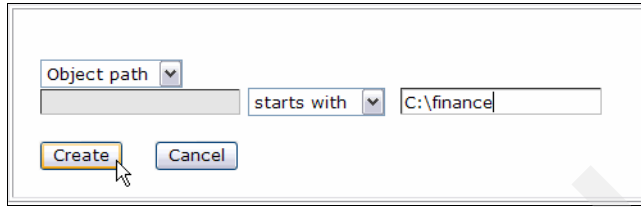


Figure 8-56 Specify condition for asset to be classified as FinancialData: Medium

The new requirement is now complete and can be seen in the Grouping panel, as shown in Figure 8-57.

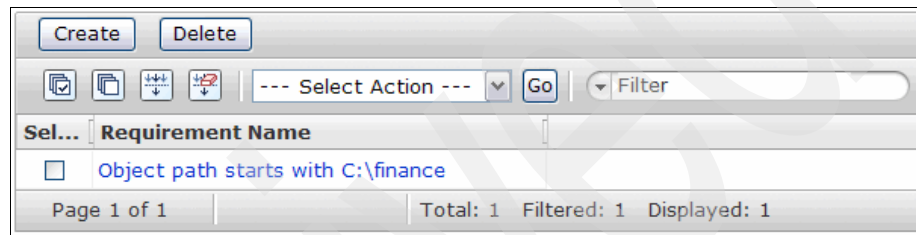


Figure 8-57 W7 group definition for the Windows financial data file share

X-Y-Z now repeats the process of creating appropriate grouping definitions, with associated conditions and requirements, for the rest of their Windows environment, for instance, they include the other confidential file shares (including C:\HR, C:\CustomerData, and the print share) into W7 onWhat groups. Additionally, extra group conditions and requirements are added into the other W7 groups: Who, What, When, and Where.

Showing all of these grouping definitions for X-Y-Z is beyond the scope of this book.

Creating W7 policy rules

The grouping definitions that were created can now be used to formulate W7 policy rules that describe the set of permissible W7 events.

The default committed policy that was used as the basis for the current working policy contains a number of predefined policy rules and attention rules. X-Y-Z analyzes these existing policy and attention rules to ensure that they are all appropriate to their IT environment. Where appropriate, these pre-existing rules are edited.

New rules are also created to customize the rules to meet X-Y-Z's needs. In this section, we describe the process of creating one of the policy rules. Table 8-3 defines the rule.

Table 8-3 New W7 policy rule

W7 Category	Who	What	Where
Value	System	System Operations	XYZ_AD

For this policy rule to be useful, X-Y-Z ensured that the W7 Who group, called System, effectively describes the permitted *system* users with appropriate requirements and conditions defined. Similarly, the W7 Where group called XYZ_AD was created to represent all of the Windows servers being monitored in the XYZ_AD domain.

To create the new policy rule from the Policy Editor in the Web portal:

1. Ensure that the Policy tab is selected, and right-click in the Policy Rules panel. Select **New Rule**, as shown in Figure 8-58.

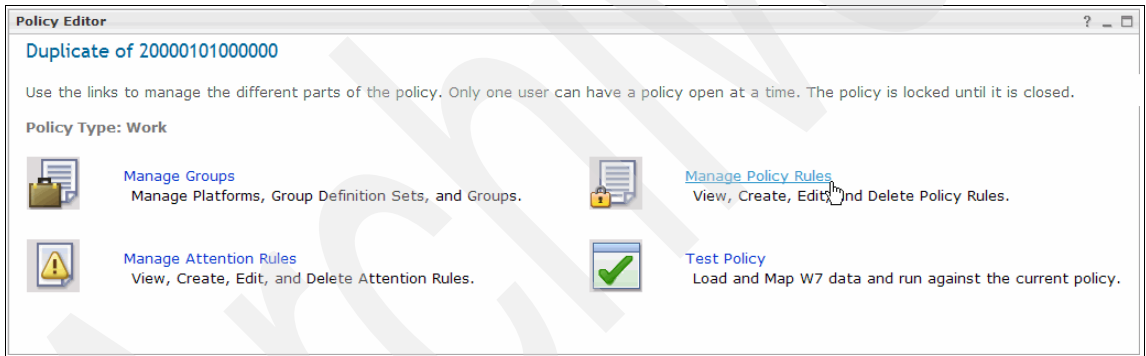


Figure 8-58 Create a new policy rule

2. As you can see in Figure 8-59, an **Edit Rule** window opens where you can enter the W7 groups that specify the new rule. Click **OK**.

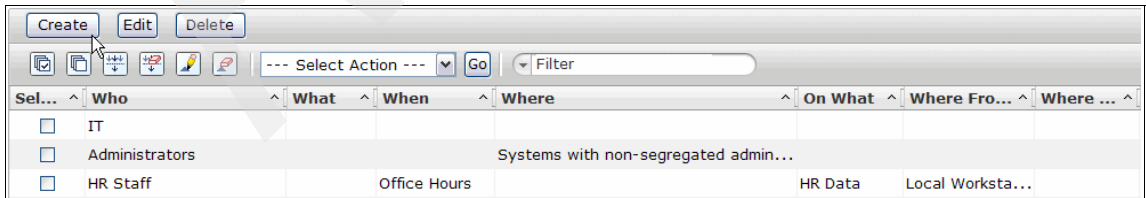


Figure 8-59 Edit rule window

- Specify the W7 groups for the rule. Pick them from a grouping file or enter the name manually, as shown in Figure 8-60.

The screenshot shows the 'Policy Editor' window with the breadcrumb 'Policy Editor > Policy Rules > Create Rule'. The policy is identified as 'Duplicate of 20000101000000' with a type of 'Work'. The dialog contains several input fields, each with a 'Select Group' button: 'Who', 'What', 'When', 'Where', 'On What', 'Where From', and 'Where To'. A 'Description' field is also present. At the bottom are 'OK' and 'Cancel' buttons. A mouse cursor is pointing at the 'Select Group' button for the 'Who' field.

Figure 8-60 New policy rule

- The groupname that is required for the W7 rule can be obtained from an existing grouping file. Click **Select** to navigate to the grouping file, as shown in Figure 8-61.

The screenshot shows the 'Policy Editor' window with the breadcrumb 'Policy Editor > Policy Rules > Create Rule > Select WHO Group'. It features a 'Select a Platform:' dropdown menu set to 'NT'. Below this is a table with columns for selection, group name, and group definition. The 'System' group is selected. At the bottom are 'Select' and 'Cancel' buttons. A mouse cursor is pointing at the 'Select' button.

Sel...	Group Na...	Group Definitio...
<input checked="" type="radio"/>	System	NT_group
<input type="radio"/>	Systems A...	NT_group

Page 1 of 1 | Total: 35 | Displayed: 2

Figure 8-61 Select appropriate grouping file

The new rule appears in the Policy Rules list, as shown in Figure 8-62 on page 203.

Policy Editor

Policy Editor > Policy Rules > Create Rule

Policy: Duplicate of 20000101000000 Policy Type: Work

Who:

What:

When:

Where:

On What:

Where From:

Where To:

Description:

Figure 8-62 List of policy rules

After the new policy rules are defined, they will display in the policies page, as shown in Figure 8-63.

Additional information: For phase 1 of the implementation, X-Y-Z also wanted to create policy rules to capture the allowed operations on the confidential file shares, for example, a policy rule that specifies that the W7 Who group called *Finance* can perform operations on objects in the W7 onWhat group called *FinancialData* and so on.

Sel...	Who	What	Wh...	Where	On What	Where Fr...	Where ...	Descript...
<input type="checkbox"/>	Systems Admin - Produ...	CreateDelete ...		Production Sys...	CreateDelete Sensitive Data - Pro...			
<input type="checkbox"/>	Systems Admin - Test	Read Data		Test Systems	Read Sensitive Data - Test			
<input type="checkbox"/>	Systems Admin - Test	Write Data		Test Systems	Write Sensitive Data - Test			
<input type="checkbox"/>	Systems Admin - Test	CreateDelete ...		Test Systems	CreateDelete Sensitive Data - Test			
<input type="checkbox"/>		Read Data			Non-confidential Write Sensitive Data			
<input type="checkbox"/>	System			XYZ_AD	System Operations			

Page 2 of 2 | 2 | Go | Total: 21 Filtered: 21 Displayed: 6

Figure 8-63 Policy rule shows

Creating W7 attention rules

Attention rules also must be created in the working policy. The W7 attention rules represent events that you are interested in monitoring.

After reviewing the predefined attention rules, the IT security staff at X-Y-Z proceeds to identify attention rules, for example, the IT security staff are interested in being notified whenever confidential financial data is deleted. In this section, we outline the configuration in Tivoli Security Information and Event Manager to configure an attention rule for these deletion events.

Here, it is important to highlight that a *W7* group was defined to represent the deletions that are performed by a user in a Windows environment. Figure 8-64 shows this group definition.

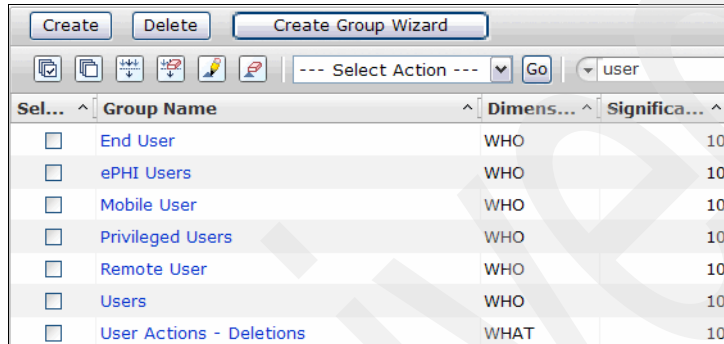


Figure 8-64 *W7* What group: User Actions: Deletions

Figure 8-65 shows the content of the User Actions - Deletions group.

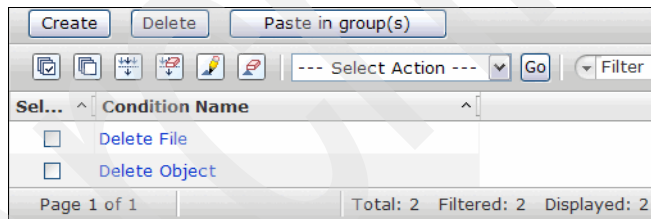


Figure 8-65 Conditions of the group

This *What* group can now be used in the new attention rule.

To create the new attention rule for capturing any deletion events on the Windows financial data file shares:

1. Select the **Attention** tab, and right-click in the Attention Rules panel. Select the **New Rule** option shown in Figure 8-66 on page 205.

Policy Editor > Attention Rules > Create Rule

Policy: Duplicate of 20000101000000 Policy Type: Work

Who	<input type="text"/>	Select Group
What	<input type="text"/>	Select Group
When	<input type="text"/>	Select Group
Where	<input type="text"/>	Select Group
On What	<input type="text"/>	Select Group
Where From	<input type="text"/>	Select Group
Where To	<input type="text"/>	Select Group
Severity (1-99)	*30	
Rule ID	<input type="text"/>	
Description	<input type="text"/>	

OK Cancel

Figure 8-66 Create new attention rule

- Figure 8-67 on page 206 shows the Edit Rule window that opens. The new attention rule is defined as: *Any user performing a deletion (W7 What = User Actions - Deletions) on objects in the financial file shares (W7 onWhat = Financial Data).*

X-Y-Z opted to assign an ID to this attention rule so that it can be managed easily. Tivoli Security Information and Event Manager allows these rule IDs to be used to create alerts for individual attentions. That is, an alert can be configured in the future to send an e-mail to an IT security administrator when events that match this attention rule are detected by Tivoli Security Information and Event Manager. In “Creating e-mail alerts” on page 206, we describe how to create an e-mail alert.

Important: The rule ID is a single word that consists of letters and numbers only.

Policy Editor > Attention Rules > Create Rule

Policy: Duplicate of 20000101000000 Policy Type: Work

Who

What

When

Where

On What

Where From

Where To

Severity (1-99)

Rule ID

Description

Figure 8-67 Edit attention rule window

3. Click **OK**. The new attention rule opens in the Attention Rules panel, as shown in Figure 8-68.

Sel...	Who	What	Wh...	Whe...	On What	Where Fr...	Where ...	Seve...	Rule ID	Description
<input type="checkbox"/>		User Actions - Transaction			Administration Obj...			40 medium		Requires atte...
<input type="checkbox"/>		User Actions - File			Administration Obj...			40 medium		Requires atte...
<input type="checkbox"/>		User Actions - Deletions			Financial Data			70 Delete Finan...		

Page 1 of 1 | Total: 44 | Filtered: 3 | Displayed: 3

Figure 8-68 Attention rule for deletions on FinancialData

Creating e-mail alerts

X-Y-Z wants to configure an alert that sends an e-mail to the IT security administration staff when deletions are performed on objects in the confidential file shares.

To create an e-mail alert for the Windows finance file share:

1. In the Web portal, open the Alerts page. Click **Create**, as shown in Figure 8-69.



Figure 8-69 Alert Maintenance window

2. The Edit Alert window opens. Configure the alert to send an e-mail to the recipient *SecAdmin@x-y-z.org* when events that match the attention rule with ID *DeleteFinancials* occur, as shown in Figure 8-70. Click **OK**.

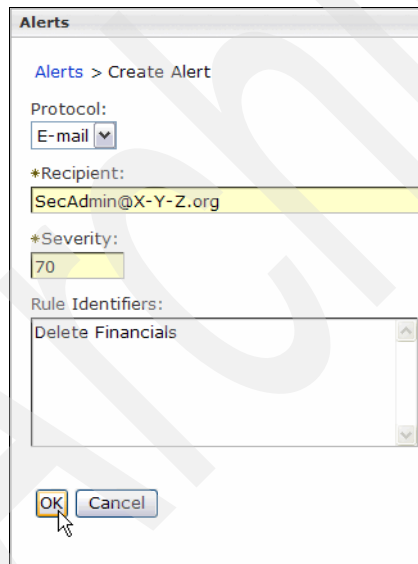


Figure 8-70 Edit Alert options

- The alert is updated with the new configured settings. Click **Protocol**, identified in Figure 8-71, to configure the protocols in use. Protocol settings apply to all alerts that are sent using the same protocol.

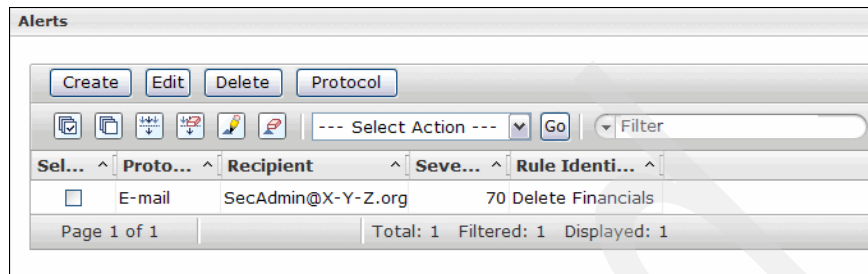


Figure 8-71 Alert Maintenance windows displays the modified alert

- The Protocol Settings window opens, as shown in Figure 8-72. Configure the e-mail settings for the environment, and click **OK**.

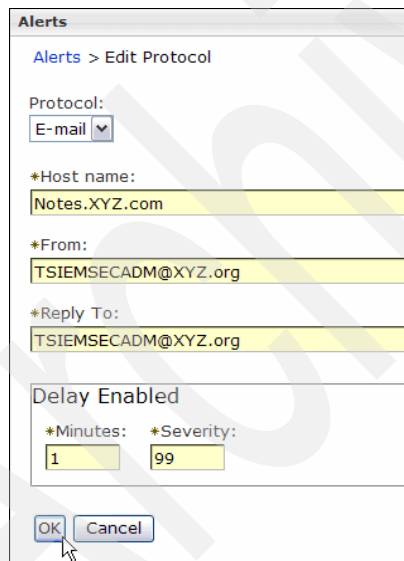


Figure 8-72 Protocol Settings window

The alert is now configured.

Loading the database

Now that the Tivoli Security Information and Event Manager environment is configured for the Windows event sources and a working policy is created, you can collect and load data from the target systems. After the data is loaded, the

Compliance Dashboard can be used to view the data and the effect of the policy mapping process.

You can wait for the next scheduled collect and load to occur. Alternatively, you can temporarily cancel the scheduled load and manually load the database instead.

Configuration details: In a production environment, we do not recommend that you temporarily cancel scheduled loads.

To perform manual loads, we recommend that you create a Reporting Database for that sole purpose.

Performing manual loads on scheduled loads changes the appearance of the dashboard, and statistics information is not well calculated. Additionally, the Last Load Date field is updated.

To manually load the database:

1. Locate the database that you plan to load in the Reporting Database page of the Web portal. Right-click and select **Load** as shown in Figure 8-73.

Reporting Databases

Reporting Databases > Reporting Database Details

Reporting Database Properties

Database Name: **General**

Load Status

⚠ Not Loaded
Schedule: Never

Load... Clear Schedule...

Event Sources

Database Name: **General**

Add... Remove

--- Select Action --- Go Filter

Sel...	Agent Gr...	Audited Mac...	Event Sou...	Last Coll...	Collection Schedule
<input type="checkbox"/>	ti0s02-sys1	ti0s02-sys1	Microsoft Wi...	3/12/10 3:0...	Frequently: every 15min
<input type="checkbox"/>	ti0s02-sys1	kcg1f1	Microsoft Wi...	3/12/10 7:4...	Never
<input type="checkbox"/>	ti0s02-sys1	ti0s02-sys1	QUANTWAVE	3/12/10 7:4...	Never

Page 1 of 1 Total: 3 Filtered: 3 Displayed: 3

Figure 8-73 Start the Load process

The Load Database Wizard Welcome window opens, as shown in Figure 8-74.

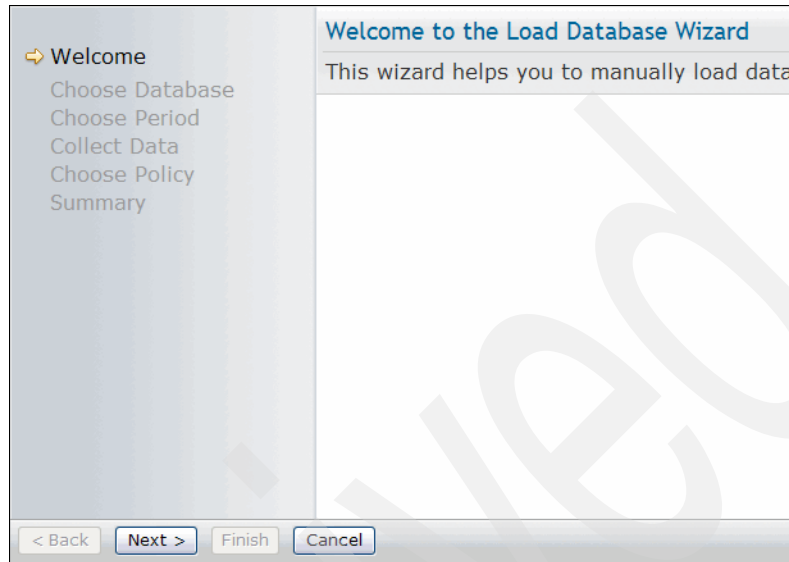


Figure 8-74 Welcome to the Load Database Wizard

2. As highlighted in Figure 8-75, select the **GENERAL** database, and click **Next**.

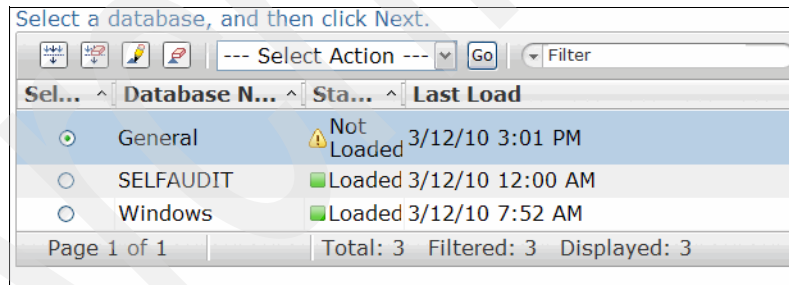


Figure 8-75 Choose a database to load

3. Specify a period of time for which the collected data is to be loaded, as shown in Figure 8-76, and click **Next**.

Choose a Period

From which period of time should data be loaded into database General?

Select a period, and then click Next.

From: *8/24/07 [calendar icon] *3:07 AM [dropdown icon]

Until: *8/28/07 [calendar icon] *11:59 PM [dropdown icon]

Figure 8-76 Data collection period

4. On the next window, decide whether to perform a data collection now or whether to use the data that was already collected through an earlier collect process, as shown in Figure 8-77.

Collect Data

Should data be collected for the Event Sources associated with database General?

Do you want to collect the latest log data before starting the load?

Yes, collect the data first.

No, just load the database.

Choose one of the options, and then click Next.

Figure 8-77 Specify whether to collect before the load

5. Because you are performing a manual load, the wizard prompts you to specify which policy to use to map the data. To test the policy that you have been working on, select the fixed policy option, and navigate to the correct policy in the work folder, as shown in Figure 8-78 on page 212. Click **Next** to proceed.

Choose a Policy

Which Policy should be applied to the data loaded into General?

Choose a Policy, and then click Next.

- Matching: The policy that matches best the selected time period.
- Newest: The latest committed Policy.
- Fixed: An explicit choice from the following collection:

Sel...	Policy Name	Type
<input type="radio"/>	Friday, December 31, 1999 7:00:00 PM EST	<input checked="" type="checkbox"/> Committe
<input checked="" type="radio"/>	Duplicate of 20000101000000	<input checked="" type="checkbox"/> Working

Page 1 of 1 Total: 2 Filtered: 2 Displayed: 2

Figure 8-78 Select a policy to be applied to the loaded data

6. On the completion window for the wizard, click **Finish**, as shown in Figure 8-79.

Completing the Load Database Wizard

Are all settings correct?

You are now ready to request the manual load.
The database load will be queued for execution on the Server.

Setting	Value
Reporting Database	General
Period	From Aug 24, 2007 3:07:00 AM until Aug 28, 2007 11:59:00 PM
Collect first	Yes
Policy	Duplicate of 20000101000000

To close this wizard and start the load request, click Finish.

Figure 8-79 Complete the Load Database Wizard

The status for the database changes to the value *Loading* to signify that the load process started. When the load is complete, the status is *Loaded*, and the time and date of the last load is updated.

Committing the policy

Now that the database is loaded using the policy that we worked on, the IT security team must review the data that was collected and how it is presented in the Compliance Dashboard reports. In 8.8, “Compliance Dashboard” on page 213, we describe how to navigate through the Compliance Dashboard to view the data.

Reviewing the data can lead to modifications to the groupings and rules that are defined in the policy. After any policy changes, the data can be re-loaded and mapped using the policy so that the new effect of the rules can be reviewed. When the team is satisfied that the policy is configured as desired, the policy can be committed. The most recently committed policy is the policy that will automatically be applied to scheduled database loads.

To commit the working policy, select the work policy, and select the action **Commit**. When the policy is committed it appears as *Committed*.

8.8 Compliance Dashboard

To open the Compliance Dashboard:

1. Navigate to **Tivoli Security Information and Event Manager** → **Security Information Management** → **Compliance Dashboard**. The Compliance Dashboard is displayed.
2. Scroll down to the Database Overview section at the bottom of the page, and click the **GENERAL** database icon that is shown in Figure 8-80.

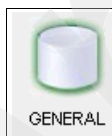


Figure 8-80 GENERAL database icon

The database summary for the GENERAL database displays. Figure 8-81 shows an example of this summary page. You can see an events summary section on the right side of the window that includes Total Events, Policy Exceptions, Special Attentions, and Failures. There are Event List icons and Event Summary Report icons to link through to more specific event details.

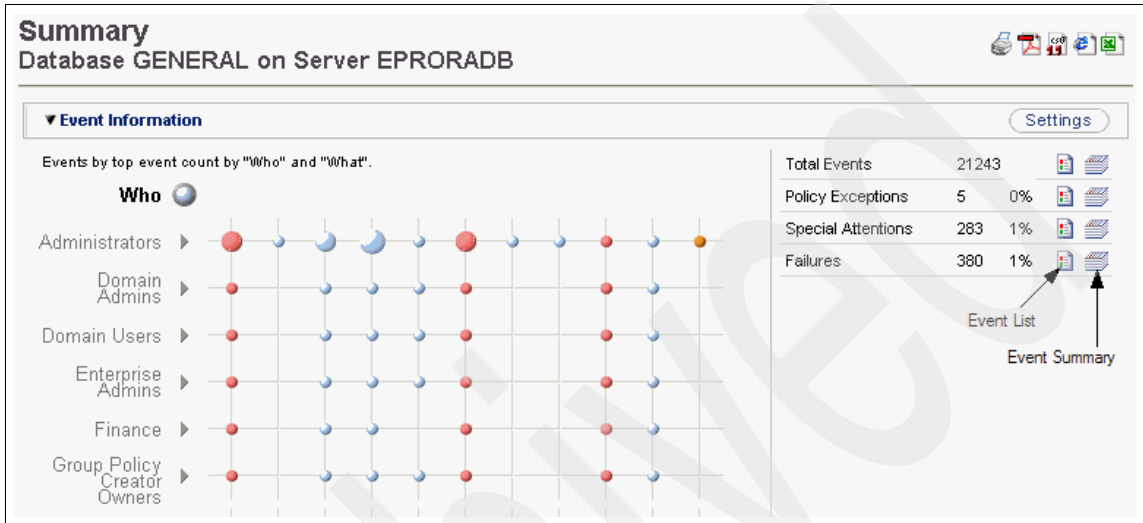


Figure 8-81 Summary of the GENERAL Database

Let us now look in more detail at mapped events. In particular, we explore the *Policy Exceptions* and *Special Attentions*.

8.8.1 Policy Exceptions

To review policy exceptions:

1. Click the **Event Summary Report** link for the Policy Exceptions. The Policy Exception Summary window displays, as shown in Figure 8-82.

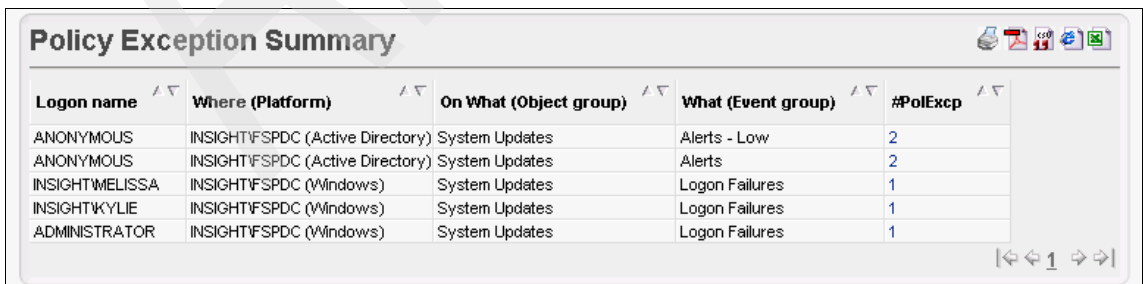


Figure 8-82 Policy Exception Summary

This view shows a summary of the exceptions that occurred with the number of each type of exception in the last column.

- For a view of all the individual policy exception events, from the GENERAL database summary page, click the **Policy Exception Event List** icon (rather than the Policy Exception Summary icon). Clicking this icon displays all of the individual Policy Exception events, as shown in Figure 8-83.

Setup:

Month Day Year Hour Min.
 Start time August 24 2007 12 0
 End time August 28 2007 10 7

Execute Reset

Time zone: Event time zone

Severity	Date / Time	#	What (detail)	Where (detail)	Who (detail)	Where from (detail)	On what (detail)	Where to (detail)
20	Fri Aug 24 2007 13:21:53 GMT-05:00	1	Start : System / Success	INSIGHT\FSPDC (Active Directory)	ANONYMOUS	INSIGHT\FSPDC (Active Directory)	SYSTEM : - / FSPDC	INSIGHT\FSPDC (Active Directory)
20	Mon Aug 27 2007 12:09:42 GMT-05:00	1	Start : System / Success	INSIGHT\FSPDC (Active Directory)	ANONYMOUS	INSIGHT\FSPDC (Active Directory)	SYSTEM : - / FSPDC	INSIGHT\FSPDC (Active Directory)
30	Mon Aug 27 2007 16:06:05 GMT-05:00	1	Logon : User / Failure	INSIGHT\FSPDC (Windows)	Melissa	INSIGHT\FSPDC (Windows)	SYSTEM : . / INSIGHT	INSIGHT\FSPDC (Windows)
30	Mon Aug 27 2007 16:06:15 GMT-05:00	1	Logon : User / Failure	INSIGHT\FSPDC (Windows)	Kylie	INSIGHT\FSPDC (Windows)	SYSTEM : . / INSIGHT	INSIGHT\FSPDC (Windows)
30	Mon Aug 27 2007 16:06:22 GMT-05:00	1	Authenticate : User / Failure	INSIGHT\FSPDC (Windows)	Administrator	127.0.0.1 (Windows)	SYSTEM : INSIGHT / FSPDC	INSIGHT\FSPDC (Windows)

Figure 8-83 Policy Exception Event List

- To look at an individual event in more detail, click one of the values in the Date/Time column, which is a hyperlink to the event detail view. Figure 8-84 on page 216 shows the event detail for the event selected in Figure 8-83.

Event Detail		
	Field	Group
Severity	30	This is a policy exception.
When	Mon Aug 27 2007 16:06:22 GMT-05:00	Office Hours (10)
What	Authenticate : User / Failure	Logon Failures (30)
Where	INSIGHT\FSPDC (Windows)	Systems with non-segregated administration (10) insight.com (10) More...
Who	Administrator	Other Sources (10)
From Where	127.0.0.1 (Windows)	Systems with non-segregated administration (10)
On What	SYSTEM : INSIGHT / FSPDC	System Updates (10)
Where To	INSIGHT\FSPDC (Windows)	Systems with non-segregated administration (10) insight.com (10) More...

Figure 8-84 Event Detail

- Click **This is a policy exception** to go to the page shown in Figure 8-85, where the Policy Exception event is explained further. Here you can see the W7 rule that the individual event was mapped to during the load process.

A security policy consists of policy rules that describe allowed behavior.

A policy exception is an event that does not comply with the security policy, because it does not match any of the policy rules.

Whether an event matches a policy rule, is determined by comparing the attributes of the event (W7) with the conditions specified by the policy rule.

A policy rule can specify conditions for each event attribute.

If all conditions are met, the event matches the rule and it complies with the security policy.

event:	When group : Period	What group : Event type	Where group : Platform	Who group : Source	From Where group : Origin	On What group : Object	Where To group : Target
	Mon Aug 27 2007 16:00:00 GMT-05:00	Authenticate : User / Failure	INSIGHT\FSPDC (Windows)	Administrator	127.0.0.1 (Windows)	SYSTEM : INSIGHT / FSPDC	INSIGHT\FSPDC (Windows)
groups:	When group : Period group	What group : Eventtype group	Where group : Platform group	Who group : Source group	From Where group : Origin group	On What group : Object group	Where To group : Target group
	Office Hours (10)	Logon Failures (30)	Systems with non-segregated administration (10) insight.com (10) INSIGHT (10)	Other Sources (10)	Systems with non-segregated administration (10)	System Updates (10)	Systems with non-segregated administration (10) insight.com (10) INSIGHT (10)

Figure 8-85 Explanation of Policy Exception

8.8.2 Special Attentions

We can review the special attention events in a similar way. Figure 8-86 shows the Special Attention Summary for the data that was loaded into the GENERAL database.

Special Attention Summary					
Severity	Logon name	Where (Platform)	On What (Object group)	What (Event group)	#SpecAtt
50	INSIGHT\KATIE	INSIGHT\FSPDC (Windows)	Financial Data	User Actions - File	141
50	INSIGHT\KATIE	INSIGHT\FSPDC (Windows)	Financial Data - Medium	User Actions - File	141
50	INSIGHT\KATIE	INSIGHT\FSPDC (Windows)	User Actions - File	User Actions - File	141
50	INSIGHT\ADMINISTRATOR	INSIGHT\FSPDC (Windows)	Financial Data	User Actions - File	69
50	INSIGHT\ADMINISTRATOR	INSIGHT\FSPDC (Windows)	Financial Data - Medium	User Actions - File	69
50	INSIGHT\ADMINISTRATOR	INSIGHT\FSPDC (Windows)	User Actions - File	User Actions - File	69
50	INSIGHT\LACHLAN	INSIGHT\FSPDC (Windows)	Financial Data	User Actions - File	58
50	INSIGHT\LACHLAN	INSIGHT\FSPDC (Windows)	User Actions - File	User Actions - File	58
50	INSIGHT\LACHLAN	INSIGHT\FSPDC (Windows)	Financial Data - Medium	User Actions - File	58
50	INSIGHT\LACHLAN	INSIGHT\FSPDC (Windows)	Financial Data	Administration	5
50	INSIGHT\LACHLAN	INSIGHT\FSPDC (Windows)	User Actions - File	Security Changes	5
50	INSIGHT\LACHLAN	INSIGHT\FSPDC (Windows)	User Actions - File	Administration	5
50	INSIGHT\LACHLAN	INSIGHT\FSPDC (Windows)	Financial Data - Medium	Security Changes	5
		INSIGHT\FSPDC			

Figure 8-86 Special Attention Summary

You can click any values in the #SpecAtt column to link through to a breakdown of that group of events. After clicking the number 141 (as seen in Figure 8-86), the details for that group of Special Attention events are displayed. Figure 8-87 on page 218 shows the Special Attentions for events classified as *User Actions - File* (W7 What group) on Financial Data (W7 onWhat group) by user INSIGHT\Katie (W7 Who Group) located at INSIGHT\FSPDC (W7 Where group).

Time zone:

Severity	Date / Time	#	What (detail)	Where (detail)	Who (detail)	Where from (detail)	On what (detail)	Where to (detail)
50	Mon Aug 27 2007 17:42:18 GMT-05:00	7	Read : File / Success	INSIGHT\FSPDC (Windows)	Caitlyn Hay	INSIGHT\FSPDC (Windows)	FILE : C:\finance / Figures	INSIGHT\FSPDC (Windows)
50	Mon Aug 27 2007 17:42:17 GMT-05:00	9	Read : File / Success	INSIGHT\FSPDC (Windows)	Caitlyn Hay	INSIGHT\FSPDC (Windows)	FILE : C:\finance / Figures	INSIGHT\FSPDC (Windows)
50	Mon Aug 27 2007 17:42:11 GMT-05:00	6	Read : File / Success	INSIGHT\FSPDC (Windows)	Caitlyn Hay	INSIGHT\FSPDC (Windows)	FILE : C:\finance / Figures	INSIGHT\FSPDC (Windows)
50	Mon Aug 27 2007 17:42:11 GMT-05:00	2	Read : File / Success	INSIGHT\FSPDC (Windows)	Caitlyn Hay	INSIGHT\FSPDC (Windows)	FILE : C:\finance / Figures	INSIGHT\FSPDC (Windows)
50	Mon Aug 27 2007 17:42:04 GMT-05:00	4	Read : File / Success	INSIGHT\FSPDC (Windows)	Caitlyn Hay	INSIGHT\FSPDC (Windows)	FILE : C:\finance / Figures	INSIGHT\FSPDC (Windows)
	Mon Aug 27 2007		Read : File /	INSIGHT\FSPDC		INSIGHT\FSPDC	FILE : C:\finance /	INSIGHT\FSPDC

Figure 8-87 Special Attention Events of User Actions

You can get further event details about a particular item that is listed by clicking the link in the Date/Time field. The Event Detail page shown in Figure 8-88 is displayed.

Event Detail

Field	Group
Severity	50 (7x) This is a special attention event.
When	Mon Aug 27 2007 17:42:18 GMT-05:00 Office Hours (10)
What	Read : File / Success User Actions - File (10)
Where	INSIGHT\FSPDC (Windows) Systems with non-segregated administration (10) insight.com (10) More...
Who	Caitlyn Hay (INSIGHT\KATIE) Administrators (20) IT (10) More...
From Where	INSIGHT\FSPDC (Windows) Systems with non-segregated administration (10) insight.com (10) More...
On What	FILE : C:\finance / Figures Financial Data (10) Financial Data - Medium (10) More...
Where To	INSIGHT\FSPDC (Windows) Systems with non-segregated administration (10) insight.com (10) More...

Figure 8-88 Event Detail for selected special attentions

In Figure 8-88 on page 218, click **This is a special attention event** to see an explanation of why the event was classified as a Special Attention event. You can see from Figure 8-89 that in this case, the Special Attention event for *IT* personnel (W7 Who group) performing an action on the *Financial Data - Medium* objects (w7 onWhat group) was triggered.

event:								
When group : Period	What group : Event type	Where group : Platform	Who group : Source	From Where group : Origin	On What group : Object	Where To group : Target		
Mon Aug 27 2007 17:30:00 GMT-05:00	Read : File / Success	INSIGHT\FSPDC (Windows)	Caitlyn Hay (INSIGHT\KATIE)	INSIGHT\FSPDC (Windows)	FILE : C:\finance / Figures	INSIGHT\FSPDC (Windows)		
groups:								
When group : Period group	What group : Eventtype group	Where group : Platform group	Who group : Source group	From Where group : Origin group	On What group : Object group	Where To group : Target group		
Office Hours (10)	User Actions - File (10)	Systems with non-segregated administration insight.com (10) INSIGHT (10)	Administrators (20) IT (10) Finance (10) Domain Users (10) TCIMAdmin (10)	Systems with non-segregated administration insight.com (10) INSIGHT (10)	Financial Data (10) Financial Data - Medium User Actions - File (10)	Systems with non-segregated administration insight.com (10) INSIGHT (10)		
This is a Special Attention because it matches the rule:								
Who (Source group)	What (Event group)	When (Period group)	Where (Platform group)	On What (Object group)	fromWhere (Origin group)	WhereTo (Target group)	Description	Severity
IT	_ANY_	_ANY_	_ANY_	Financial Data - Medium	_ANY_	_ANY_	Requires attention	50
The severity defined by the rule is 50, therefore the Event Severity is 50.								

Figure 8-89 Explanation of Special Attention event

8.8.3 Reports

You can use the Compliance Dashboard Reports page to generate online reports based on the loaded data. To open this page, on the Database Summary page, click Reports (refer back to Figure 8-81 on page 214).

The Compliance Dashboard Reports is divided into the following main categories:

- ▶ Configuration Tools
- ▶ Daily Verification
- ▶ Detailed Investigation
- ▶ Firewall Reports

Each of these categories contain predefined reports for you to analyze the events that were captured. We describe examples from these categories in the remainder of this section.

Configuration Tools reports

Figure 8-90 shows a snapshot from the Compliance Dashboard Reports window. Run the Events by Rule report to delve into the data that is currently loaded in the GENERAL database.



The screenshot shows the Compliance Dashboard interface. At the top, there are navigation tabs: Dashboard, Trends, Reports (selected), Regulations, Policy, Groups, Distribution, and Settings. Below the tabs, the breadcrumb path is 'CIFDB > SELFAUDIT > Reports'. The main heading is 'My reports', with buttons for 'Import custom reports' and 'Add custom reports'. A section titled 'Configuration tools' contains a table with the following data:

Type	Title	Description	Action
	Events by rule	List of events that comply with a W7 rule	
	Events by type	Summary of audited event types	
	Policy Settings	List of events that comply with the policy rules	
	Policy Wizard	Tool to help define a policy and to verify the existing policy	
	W7 Summary	Summary of all events	

Below the table is a section for 'Daily verification'.

Figure 8-90 Configuration Tools - Events by Rule report

The icon in the shape of a tick in the Action column in the row of Events by Rule indicates that to run this report user input is required and that various parameters are needed to determine the scope of the report. You are prompted to configure the W7 rule for which you want the matching events to display. Configure the report to include all events that are classed as user actions on a file containing financial data. That is, you are filtering the events using the W7 What group *User Actions - File* and the W7 onWhat group *Financial Data*, as displayed in Figure 8-91.

What (Event group)	When (Period group)	Where (Platform group)	On What (Object group)
User Actions - File	[_ANY_]	[_ANY_]	Financial Data

Figure 8-91 A part of the Events by Rule report configuration

When this report is submitted, a list of events that match this W7 rule are created. As shown on the previous event list reports, it is possible to navigate through Web links to find individual event details, where desired.

Daily verification reports

The daily verification reports include a number of useful reports to check events that are detected on the audited systems.

As described in 8.3, “Phase one reporting requirements” on page 154, there are a number of Basel II reports that X-Y-Z is particularly interested in generating.

One of the desired reports is based on user responsibilities and password use. Therefore, one of the daily verification reports that is of interest to X-Y-Z is the *Logon Failure Summary* report.

You can generate the Logon Failure Summary report by clicking the appropriate link, as shown in Figure 8-92.

▼ Daily verification				
Type	Title	Description	Action	
	Alerts	List of Alerts by Priority		
	All Exposures	List of Exposures by Priority		
	DBA Activity	List of changes to databases		
	Events by type	Summary of audited event types		
	Failed System Operations	List of failed operator and configuration commands		
	Failed System Services	List of system processes that ended with (security) error condition		
	Failed Transactions	List of failed transactions (SAP, Oracle)		
	Impersonation	List of Users who caused events under another name		
	Logon Failure Summary	Summary of logon failures		

Figure 8-92 Daily Verification Reports: Logon Failure Summary

A list of the failed logon events and their associated details are displayed in the browser. Refer to Figure 8-93 for an example Logon Failure Summary report.

Logon Failure Summary				
Platform	Logon ID	Name	Location	#Events
INSIGHT\FSPDC	FSPDCADMINISTRATOR	Administrator	INSIGHT\FSPDC	7
INSIGHT\FSPDC	INSIGHT\ DAN	Daniel Roberts	INSIGHT\FSPDC	2
INSIGHT\FSPDC	INSIGHT\KATIE	Katie	INSIGHT\FSPDC	2
INSIGHT\FSPDC	INSIGHT\CHAY	Chay	INSIGHT\FSPDC	2

Figure 8-93 Logon Failure Summary Report

Detailed investigation

In 8.1, “Phase one auditing” on page 151, we outlined X-Y-Z’s desire to monitor actions that are performed on their confidential file shares. So, let us now view the detailed investigation report called *Object Audit*.

Figure 8-94 on page 222 is an example of a report that requires parameters to be specified before it can be generated. Select which *W7 onWhat* group you want to audit.

▼ Detailed investigation			
Type	Title	Description	Action
	Administration	List of administrative actions	
	Administration per user	List of administrative actions by user	
	Help Desk Activity	List of helpdesk security commands (enable/disable user)	
	In Period group by Users	List of Users with events inside the specified Period groups	
	Logon History by Platform	List of Platforms with logon events	
	Logon History by User	List of platform Users with logon events	
	Object Audit	List of important Objects to Audit	
	Object H <u>List of important Objects to Audit</u>	List of all Objects with events	
	Out of Office Hours Activity	List of logons outside office hours	
	Platform Events Summary	Summary of events reported by platform	

Figure 8-94 Detailed Investigation Reports - Object Audit

As shown in Figure 8-95, select to audit the Financial Data.

EPRORADB » GENERAL » Reports » Object Audit

Object Audit

Setup:

On What (Object group)

- Administration
- Database Operations
- Financial Data
- Financial Data - Medium
- Other Objects
- Process
- System Operations
- System Processes
- System Updates
- User Actions - File
- User Actions - Process

Figure 8-95 Financial Data Object Audit

When you click **Submit** the report is generated. The window shown in Figure 8-96 shows the output for this report.

Object Audit

Setup:

On What (Object group)

- Administration
- Database Operations
- Financial Data
- Financial Data - Medium
- Other Objects
- Process
- System Operations
- System Processes
- System Updates
- User Actions - File
- User Actions - Process

[Submit](#) [Reset](#)

On What (Object)	WhereTo (Target)	#Events
FILE : C:\finance*	INSIGHT\FSPDC (Windows)	26
FILE : C:\finance\figures*	INSIGHT\FSPDC (Windows)	40
FILE : C:\finance\figures\2007projections.xls	INSIGHT\FSPDC (Windows)	16
FILE : C:\finance\figures\2007q1results.xls	INSIGHT\FSPDC (Windows)	81
FILE : C:\finance\figures\2007q2results.xls	INSIGHT\FSPDC (Windows)	46
FILE : C:\finance\figures\2007q3results.xls	INSIGHT\FSPDC (Windows)	18
OBJECT : C:\finance\figures\2007q3results.xls	INSIGHT\FSPDC (Windows)	1
FILE : C:\finance\Figures	INSIGHT\FSPDC (Windows)	194
FILE : C:\finance\reports\July2007.xls	INSIGHT\FSPDC (Windows)	10
FILE : C:\finance\reports\June2007.xls	INSIGHT\FSPDC (Windows)	27
FILE : C:\finance\figures\New text document.txt	INSIGHT\FSPDC (Windows)	15
FILE : C:\finance\reports\New wordpad document.doc	INSIGHT\FSPDC (Windows)	5
FILE : C:\finance\Reports	INSIGHT\FSPDC (Windows)	59

Figure 8-96 Object Audit Report

As with all of the online reporting in Tivoli Security Information and Event Manager, you can examine the finer details of these events by clicking the desired links.

Let us obtain more about the Object Deletion event that is listed in the Object Audit Report by clicking the 1 in the #Events column. The W7 details of the event are displayed, as shown in Figure 8-97.

Time zone:

Severity	When	#	What	Where	Who	From Where	On What
50	Mon Aug 27 2007 17:42:22 GMT-05:00	1	Delete : Object / Success	INSIGHT\FSPDC	System (NT AUTHORITY\SYSTEM)	INSIGHT\FSPDC	OBJECT : C:\finance\figures\2007q3results.xls

Figure 8-97 Object Audit Event List

By clicking the available link in this window, you can obtain the event details given in Figure 8-98 on page 224.

Event Detail		
	Field	Group
Severity	50	This is a special attention event.
When	Mon Aug 27 2007 17:42:22 GMT-05:00	Office Hours (10)
What	Delete : Object / Success	User Actions - Deletions (80)
Where	INSIGHT\FSPDC (Windows)	Systems with non-segregated administration (10) insight.com (10) More...
Who	System (NT AUTHORITY\SYSTEM)	Administrators (20) IT (10)
From Where	INSIGHT\FSPDC (Windows)	Systems with non-segregated administration (10) insight.com (10) More...
On What	OBJECT : C:\finance\figures / 2007q3results.xls	Financial Data (10) Financial Data - Medium (10) More...
Where To	INSIGHT\FSPDC (Windows)	Systems with non-segregated administration (10) insight.com (10) More...

Figure 8-98 Event Detail

Analyzing Trends with the Compliance Dashboard

The trends part of the Compliance Dashboard presents the aggregated data from all of the databases. The Trends section opens by default with the All Events of the last seven days. You can see this view in Figure 8-99 on page 225. You can click **Last Month** to view events of the last month. Using the pull-down menu you can choose between policy exceptions, special attention events, and failures, or get a percentage view of the three options.

If the diagram represents the last week, click **Previous** to return to the previous week. Click **Next** to go forward one time period. If no data is available, the control is unavailable.

Below the bar graph in this view there are seven list boxes for each W7 group types. You can configure all possible W7 group combinations using these pull-down menus. If you select **Go** (located at the bottom of these seven list boxes) then the diagram displays data for the selected groups. There is a table at the bottom of the window with a description of every bar in the diagram. You can click its number of events to get its event list.

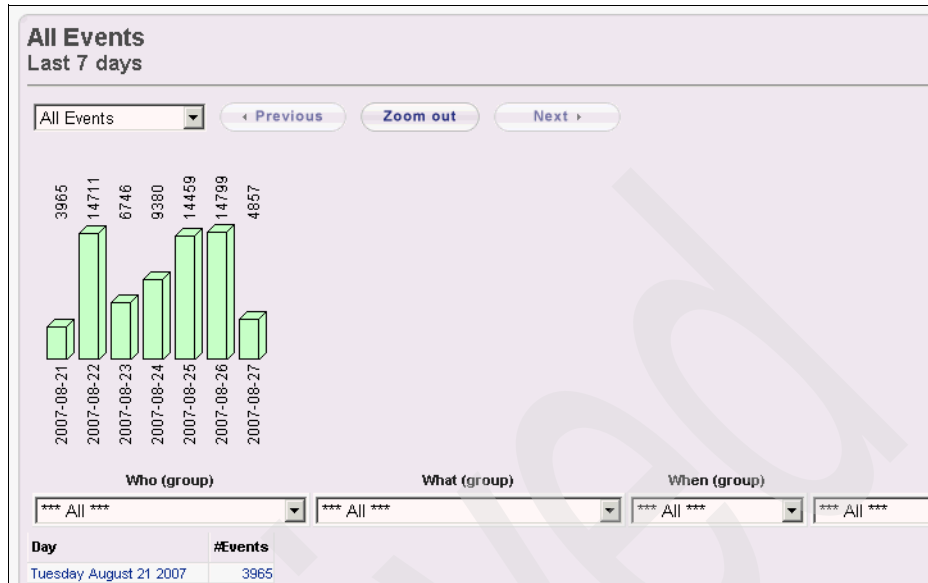


Figure 8-99 Trend data

8.9 Self-auditing

When installed, the Tivoli Security Information and Event Manager servers configure and schedule *self-audits* automatically. You might have noticed in certain diagrams throughout this chapter that there is a database called *SelfAudit* that is configured by default on the Tivoli Security Information and Event Manager server. In the Reporting Database page of the Web portal, shown in Figure 8-100 on page 226, you can see that this database also has a daily load schedule that is associated with it when the server is initially installed. That is, a Tivoli Security Information and Event Manager Server starts self-auditing automatically from the moment it is first installed.

Reporting Databases			
Load... Clear			
<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>		--- Select Action --- Go Filter	
Sel...	Database N...	Sta...	Audited Machi... Last Load
<input checked="" type="radio"/>	SELFAUDIT	<input checked="" type="checkbox"/> Loaded	ti0s02-sys1 3/12/10 12:0...
<input type="radio"/>	Windows	<input checked="" type="checkbox"/> Loaded	kcgg1f1... 3/12/10 7:52...
<input type="radio"/>	General	<input type="checkbox"/> Not Loaded	kcgg1f1...

Page 1 of 1 Total: 3 Filtered: 3 Displayed: 3

Figure 8-100 SelfAudit database and schedule

Auditing the Tivoli Security Information and Event Manager environment is important so that the IT security staff is aware of user actions that affect X-Y-Z's compliance management solution.

Figure 8-101 shows the Daily Verification Report called *Logon Failure Summary* that is run against the SelfAudit database.

Compliance Dashboard							
Dashboard	Trends	Reports	Regulations	Policy	Groups	Distribution	Settings
CIFDB > SELFAUDIT > Reports > Logon Failure Summary							
Logon Failure Summary							
Platform	Logon ID	Name	Location	#Events			
WIN-5KJQA18QOX7	WIN-5KJQA18QOX7\SYSTEM	WIN-5KJQA18QOX7\SYSTEM	WIN-5KJQA18QOX7	8			
ti0s02-sys1	TI0S02-SYS1\SYSTEM	TI0S02-SYS1\SYSTEM	ti0s02-sys1	2			

Figure 8-101 Self-Audit Logon Failure Summary

Figure 8-102 and Figure 8-103 show the results of using the Compliance Dashboard to display further details about the login failure event.

Logon Failure Summary Event list on ti0s02-sys1 by TI0S02-SYS1\SYSTEM from ti0s02-sys1 Database SELFAUDIT on Server CIFDB								
Time zone: <input type="text" value="Event time zone"/>								
Severity	When	#	What	Where	Who	Where From	On What	Where To
30	3/11/10 10:16:44 AM (-0500)	1	Logon : User / Failure	ti0s02-sys1	TI0S02-SYS1\SYSTEM	ti0s02-sys1	USER : - / Administrator	ti0s02-sys1
30	3/11/10 2:44:18 PM (-0500)	1	Logon : User / Failure	ti0s02-sys1	TI0S02-SYS1\SYSTEM	ti0s02-sys1	USER : - / administrator	ti0s02-sys1

Figure 8-102 SelfAudit Logon Failure Event List

Event Detail		
	Field	Group
Severity	30	This is a policy exception
When	3/11/10 10:16:44 AM (-0500)	Office Hours (10)
What	Logon : User / Failure	Logon Failures (30)
Where	ti0s02-sys1 (Microsoft Windows Server 2008/Vista)	Systems with non-segregated administration (10)
Who	TI0S02-SYS1\SYSTEM	Other Sources (10)
Where From	ti0s02-sys1 (Microsoft Windows Server 2008/Vista)	Systems with non-segregated administration (10)
On What	USER : - / Administrator	Administration (10)
Where To	ti0s02-sys1 (Microsoft Windows Server 2008/Vista)	Systems with non-segregated administration (10)

Figure 8-103 Logon Failure Event Detail

There are other useful self-audit reporting capabilities, for instance, the report that is displayed in Figure 8-104 on page 228 shows all of the events that are contained in the SelfAudit database that are classified as *Configuration Changes*. As you can see, by default Configuration Change events include user actions, such as creating policies, committing policies, aggregating log data, and so on.

Events by rule:

Rule:

Who (Source group) Any Group

What (Event group) Configuration Changes

When (Period group) Any Group

Where (Platform group) Any Group

On What (Object group) Any Group

Where From (Origin group) Any Group

Where To (Target group) Any Group

Submit Reset

Time zone: Event time zone

Severity	When	#	What	Where	Who	Where From	On What	Where To
50	3/11/10 5:37:40 AM (-0500)	1	Complete : Load / Success	ti0s02-sys1	Anonymous	ti0s02-sys1	DATABASE :- / SELFAUDIT	ti0s02-sys1
50	3/11/10 5:37:40 AM (-0500)	1	Complete : Load / Success	ti0s02-sys1	Anonymous	ti0s02-sys1	DATABASE :- / SELFAUDIT	ti0s02-sys1

Figure 8-104 Event List of Configuration Changes - SelfAudit Database

8.10 Conclusion

Phase one of X-Y-Z's implementation plan is now complete. In this chapter, we described the process that we used to install and configure a Tivoli Security Information and Event Manager cluster. X-Y-Z now has their Tivoli Security Information and Event Manager environment set up to monitor the actions of their Windows domain users. To achieve this monitoring, Windows agents were installed on the Windows servers in the IT environment. Microsoft Windows event sources and Active Directory event sources were configured for the appropriate servers.

The audit subsystems on each server were also configured to ensure that sufficient log information is generated on the target machines. Appropriate W7 groups and rules were defined and encapsulated in a Tivoli Security Information and Event Manager policy that was committed. Scheduled loads can now be performed on the GENERAL database to collect the data from these Windows event sources. The Compliance Dashboard can be used to monitor user actions by reporting on the loaded events.

In the next phase, X-Y-Z is going to expand their deployed compliance management solution by using Tivoli Security Information and Event Manager to audit more platforms and applications in their environment. In particular, in phase two, they begin monitoring AIX, SAP, Domino, and syslog.



Extending auditing to other supported platforms

In this chapter, we discuss how X-Y-Z expands their deployed compliance management solution by using Tivoli Security Information and Event Manager to audit more platforms and applications in their environment. In particular, in phase two, they begin monitoring AIX, SAP, Domino, and (existing) syslog messages.

9.1 IT environment

Figure 9-1 shows the IT architecture for X-Y-Z's compliance management solution using Tivoli Security Information and Event Manager. We described this architecture in detail in Chapter 6, "Introducing X-Y-Z Financial Accounting" on page 121. In Figure 9-1, the system groups that we address in this phase of the project are highlighted in bold underlined text.

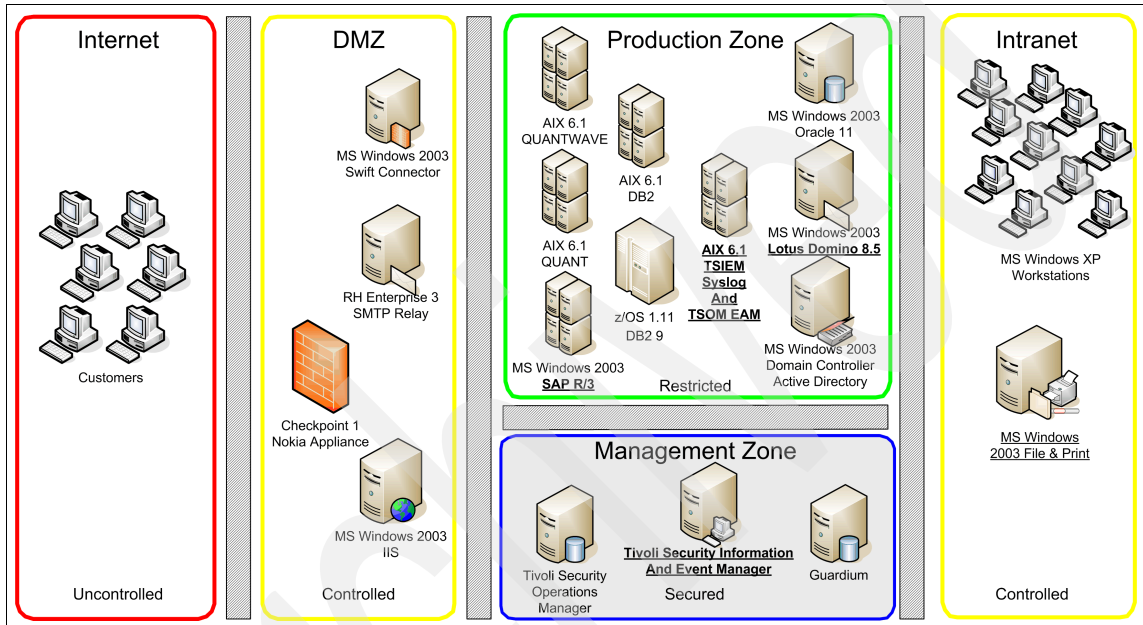


Figure 9-1 X-Y-Z IT architecture components for phase 2

Specifically in this phase of the project, we implement log management and basic audit reporting for the following types of systems:

- ▶ AIX 6.1 systems
- ▶ Domino 8.5
- ▶ SAP R/3 System
- ▶ Syslog messages

We use the Standard Server that was installed as part of phase one of the project as our Tivoli Security Information and Event Manager server. You can find details about how to install a Standard Server and add it to a Tivoli Security Information and Event Manager cluster in the *IBM Tivoli Security Information and Event Manager Version 2.0 Installation Guide*, GI11-8778.

9.2 Basic approach

As with all Tivoli Security Information and Event Manager event sources, the basic approach to collect audit data can be encompassed in the following steps:

1. Configure the target system so that it generates the audit data that you need.
2. Create a Tivoli Security Information and Event Manager event source for that target system using either a local or remote agent.
3. If the agent is remote, you also must configure the target system to make the audit data available to Tivoli Security Information and Event Manager. For many systems, this means that you must create a user account, configure the system so that the user account can access the audit data, and configure a collection mechanism (a typical collection method is to use SSH because we use it for our AIX systems later in this section).
4. Configure the appropriate policy groups and rules.

9.3 Auditing AIX 6.1 systems

For each of the target systems, you must configure auditing using whatever mechanism is appropriate for that environment. We discuss the basic steps for configuring auditing for these platforms in the installation guide and fully elaborated in this section.

9.3.1 Configuring auditing for AIX systems

On the AIX system, you use the audit subsystem to create useful audit information and to collect the standard files that AIX uses to capture login and failed login information.

AIX standard login files

By default, logins and failed logins on AIX are captured in the files `/var/adm/wtmp` and `/etc/security/failedlogin`. You do not need to configure AIX any further to generate these files. By default, the `wtmp` file is readable by any user; however, the `failedlogin` file is, by default, located in a directory that is not accessible by all users. Thus, when you configure the user ID that Tivoli Security Information and Event Manager uses to collect this log data, you must ensure that it is a member of a group that was granted access to this file.

AIX audit subsystem

The audit subsystem on AIX is highly configurable; however, exploring every audit setting and configuration option is outside the scope of this book. For our purposes, we explain basic concepts and configuration options.

The AIX audit subsystem uses the two information collection modes *BIN* and *STREAM*. We use the *BIN* mode.

The basic commands to control the audit subsystem (these commands are located in the */usr/sbin* directory by default) are:

audit start	Starts the audit subsystem.
audit shutdown	Stops the audit subsystem and flushes the bin files.
audit off	Suspends the audit subsystem temporarily.
audit on	Resumes the audit subsystem after suspension.
audit query	Displays the current audit subsystem status.

The following commands are useful when interacting with the AIX audit subsystem:

auditcat	Used to write bin files that the subsystem produces to an audittrail file.
auditpr	Used to format and print audit records in a human readable format.

The AIX audit subsystem is controlled by the following files (by default these files are located in the */etc/security/audit* directory):

► **Config file**

The config file contains the key stanzas that control the auditing subsystem. The stanzas include:

Start	Specifies the audit collection method. Tivoli Security Information and Event Manager typically uses the bin method.
Bin	Specifies how the bin mode audit collection method is configured.
Stream	Specifies how the stream mode audit collection method is configured.

Classes	Defines audit classes. An audit class is a specific set of AIX events. Classes can be assigned to a single user, a user group, or to all.
Users	Specifies to which users event auditing applies and which audit classes are captured for that user. Using the user default applies the collection policy to all users.

Example 9-1 shows an abbreviated example of a Tivoli Security Information and Event Manager config file. The *IBM Tivoli Security Information and Event Manager Version 2.0 Event Source Guide, SC23-9687*, has a complete example that you can study more closely.

Example 9-1 The AIX audit subsystem config file

```
start:
    binmode = on
    streammode = off

bin:
    trail = /audit/trail
    bin1 = /audit/bin1
    bin2 = /audit/bin2
    binsize = 10240
    cmds = /etc/security/audit/bincmds
    freespace = 65536

stream:
    cmds = /etc/security/audit/streamcmds

classes:
eprise = PROC_Delete, PROC_Execute, PROC_RealUID, PROC_AuditID,
PROC_RealGID, PROC_Environ, PROC_Privilege, PROC_Settimer,
FILE_Link, FILE_Unlink, FILE_Rename, FILE_Owner, FILE_Mode,
FS_Mount, FS_Unmount, FILE_Acl, FILE_Privilege, FS_Chroot,
TCPIP_Config, TCPIP_host_id, TCPIP_route, TCPIP_connect,
TCPIP_access, TCPIP_set_time, TCPIP_kconfig, TCPIP_kroute,
TCPIP_kconnect, TCPIP_kcreate, USER_Login, PORT_Locked, SYSCK_Check,
SYSCK_Update, SYSCK_Install, USER_Check, USER_Logout, PORT_Change,
USER_Change, USER_Remove, USER_Create, USER_SetGroups, USER_SetEnv,
USER_SU, GROUP_User, GROUP_Adns, GROUP_Change, GROUP_Create,
GROUP_Remove, PASSWORD_Change, PASSWORD_Flags, PASSWORD_Check,
PASSWORD_Ckerr, SRC_Start, SRC_Stop, SRC_Addssys, SRC_Chssys,
SRC_Addserver, SRC_Chserver, SRC_Delssys, SRC_Delserver,
ENQUE_admin, ENQUE_exec, SENDMAIL_Config, SENDMAIL_ToFile,
AT_JobAdd, AT_JobRemove, CRON_JobRemove, CRON_JobAdd, CRON_Start,
```

CRON_Finish, NVRAM_Config, DEV_Configure, DEV_Change, DEV_Create, DEV_Start, INSTALLP_Inst, INSTALLP_Exec, UPDATEP_Name, DEV_Stop, DEV_UnConfigure, DEV_Remove, LVM_ChangeLV, LVM_ChangeVG, LVM_CreateLV, LVM_CreateVG, LVM_DeleteVG, LVM_DeleteLV, LVM_VaryoffVG, LVM_VaryonVG, BACKUP_Export, BACKUP_Priv, RESTORE_Import, USER_Shell, TCBCCK_Check, TCBCCK_Update, PROC_SetGroups

Points of interest include:

- Our start: Stanza, where we specify the bin mode collection.
- Our bin: Stanza defines the default locations for the audit trail information. In the class: stanza, we defined the event classes in which we are interested. We arbitrarily picked the label eprise.
- Last, and probably most important, we defined our users: Stanza, where we indicated that we want to collect the events labelled with eprise for *all* users, for example, the default for all users is the event list that the label eprise specified.

► Bincmds file

This file contains the commands that are used by the audit daemon (auditbin) when it is flushing the audit bin files to the audit trail. For our purpose, the bincmds file is as described in Example 9-2.

Example 9-2 The bincmds file entries for Tivoli Security Information and Event Manager

```
# the next line removes our previous temporary work audit trail
# in case we did not clean up properly previously.
/usr/bin/rm -f /var/log/eprise/working

# the next line uses the auditcat tool to output the audit trail
# into the location /var/log/eprise/working. The $bin
# parameter will be expanded to the path /audit/trail from
# our config file.
/usr/sbin/auditcat -o /var/log/eprise/working $bin

# The next line appends the flushed data to a date and hour stamped
# file in /var/log/eprise e.g. trail.2007083115. This is the file
# which TCIM is looking for when it collects audit data.
/usr/bin/cat /var/log/eprise/working >>
    /var/log/eprise/trail.`date +"%Y%m%d%H"`

# The next line allows us to maintain the full audit trail in the
# /audit/trail location (this is not required by TCIM but local
# practice may be that this should be the full audit trail).
```

```
/usr/bin/cat /var/log/eprise/working >> /audit/trail  
  
# last we remove our temporary working file as it is no longer  
# required.  
/usr/bin/rm -f /var/log/eprise/working
```

► **Events file**

The events file is where you define the event formatting options. We want to get audit entries for objects that are being read, written, and executed, so we add the entries in Example 9-3 to the end of the events file. Notice that comments in the event file are preceded with the asterisk (*) character.

Example 9-3 The events file entries for Tivoli Security Information and Event Manager

```
* Object Audit Event Definitions needed  
* for Tivoli Security Information and Event Manager  
Obj_READ = printf "%s"  
Obj_WRITE = printf "%s"  
Obj_EXECUTE = printf "%s"
```

► **Objects file**

The objects file defines the system objects that you specifically want to monitor access to. For this to work, you must have previously, in the events file, defined the events that you want to receive. For our purposes, we want to see people who access a directory that contains our sensitive data in the file /home/sensitivedata. Thus, we add the lines in Example 9-4 to the end of the /etc/security/audit/objects file.

Example 9-4 The objects file entries for Tivoli Security Information and Event Manager

```
/home/sensitivedata:  
r = "Obj_READ"  
w = "Obj_WRITE"
```

Preparing the AIX system for audit data collection using SSH

For Tivoli Security Information and Event Manager to perform remote collection of audit data:

1. Create a user for Tivoli Security Information and Event Manager to use. In our case, we create a user named *insight*.
2. Ensure that the user has the correct permissions to access the audit data, for example, the user must have full permissions for the /var/log/eprise directory and its contents, read permissions for the failedlogin file

(/etc/security/failedlogin), read and execute permissions for the /etc and /etc/security directories, read permissions for the wtmp file (/var/log/wtmp), and read and execute permissions for the /var and /var/log directories. We achieved this by adding the insight user to the system, audit, and security groups on the AIX target system.

3. Configure the system so that the Tivoli Security Information and Event Manager server can perform an SSH collect from the AIX system using the new user ID. The basic steps to perform this are covered in the chapter on enabling Collect using SSH event sources in the *IBM Tivoli Security Information and Event Manager Version 2.0 Installation Guide*, G111-8778. The steps that are required are:
 - a. Create ssh public and private keys.
 - b. Copy the public key to the insight user's ssh/authorized_keys file.
 - c. Save the private key to the Tivoli Security Information and Event Manager servers SSHKeys directory (typically C:\IBM\SIM\server\run\sshkeys).
 - d. Perform one Putty-based ssh login from the Tivoli Security Information and Event Manager server to the target platform using your Tivoli Security Information and Event Manager user.

Now that we configured and prepared the AIX system so that its audit subsystem generates the information that we want and so that Tivoli Security Information and Event Manager can use SSH to collect that information, we can configure Tivoli Security Information and Event Manager to collect the audit information.

9.3.2 Adding the AIX event source to Tivoli Security Information and Event Manager

Perform the following steps to configure Tivoli Security Information and Event Manager to collect the AIX audit data using SSH:

1. From the Tivoli Security Information and Event Manager Portal, invoke the Add Machine Wizard. Select **Managing Audited Machines**, which opens the wizard shown in Figure 9-2 on page 237.

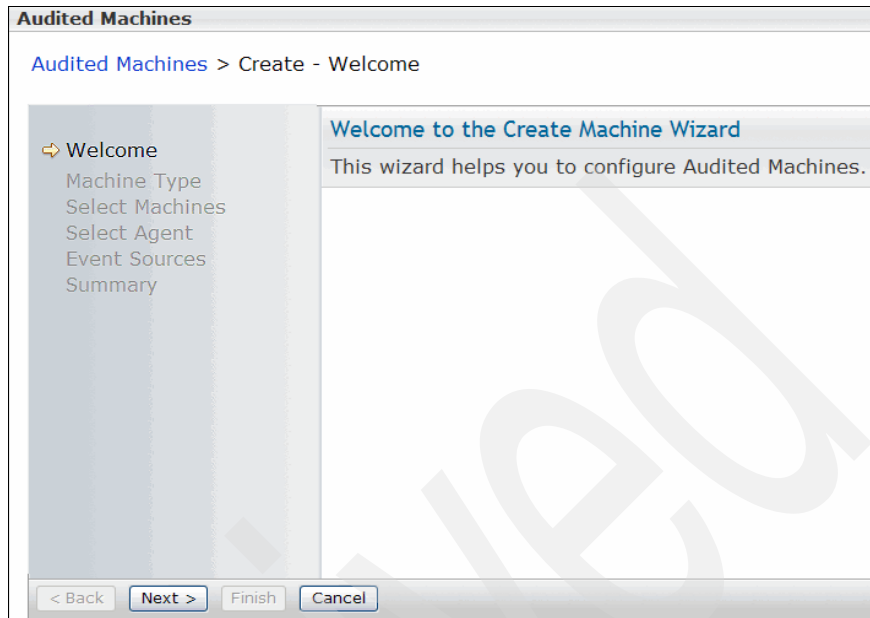


Figure 9-2 Add Machine Wizard

- From the audited machine type, select **IBM AIX**, as shown in Figure 9-3.

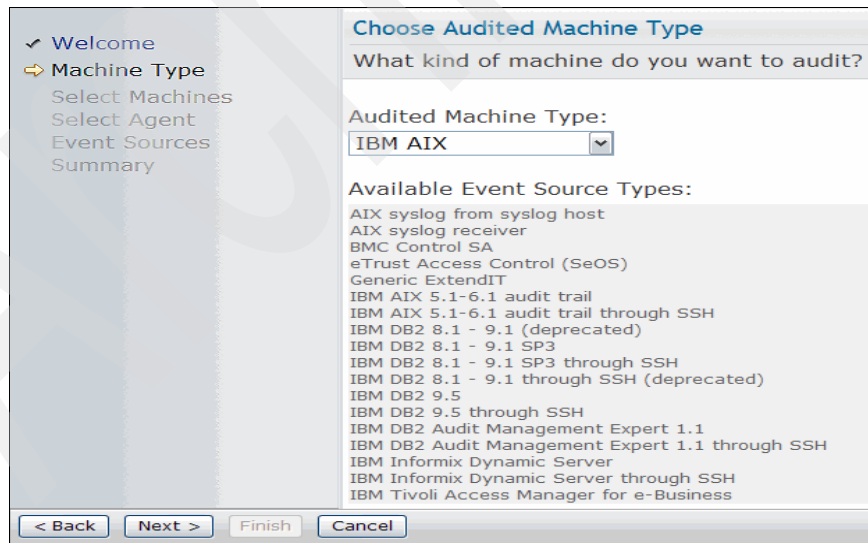


Figure 9-3 Audited machine type

3. Select your machine, as shown in Figure 9-4 (in our case, our AIX system is named FINSYS).

Choose Audited Machines

Compile a list of machines you want to audit.

To manually compile the list, type the hostname or IP address and click Add. To automatically detect Windows machines on the network, check Browse Network, select the domain or workgroup, and click Find Machines. Select the machines you want from the table and click Add.

Hostname or IP: Browse Network

Selected Machines:

Sel...	Hostname
	None

Total: 0 Filtered: 0 Displayed: 0

Figure 9-4 Choose the machine

4. Choose the agent that performs the collection, as shown in Figure 9-5.

Select Agent

Which machine should facilitate auditing of FINSYS?

Select Agent

Agent installed locally on the audited machine(s)

Agent installed remotely from the audited machine(s)

Directly from TSIEM Server ti0s02-sys1

Existing Agent. Agent group: Agent name:

Install a new remote Agent of type

Figure 9-5 Select the agent

5. Select the event source type of AIX Audit trail through SSH, as shown in Figure 9-6.

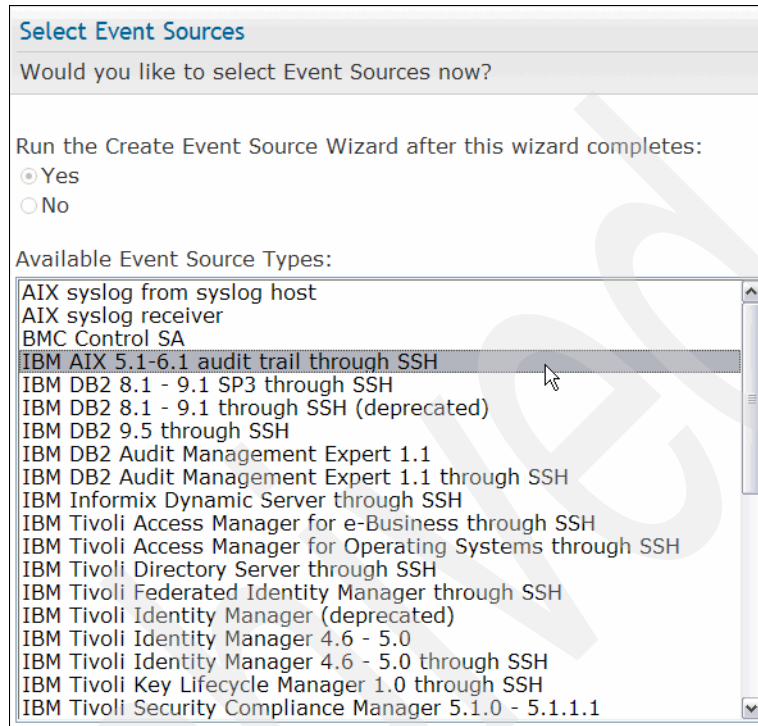


Figure 9-6 Event source type

6. At this stage, you completed the Add Machine Wizard, as shown in Figure 9-7. Select **Finish**, which automatically invokes the Add Event Source Wizard.

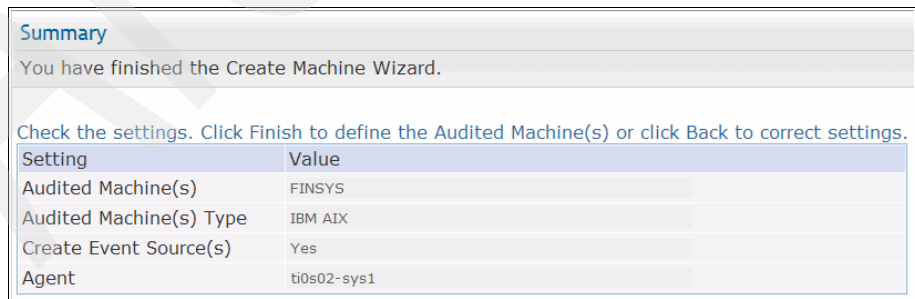


Figure 9-7 Add machine wizard complete

- In the Add Event Source Wizard, select **Next**, as shown in Figure 9-8.

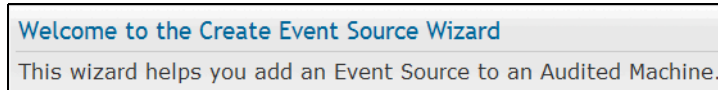


Figure 9-8 The Add Event Source Wizard

- Configure the event source properties, as shown in Figure 9-9 and described in the following list:

Audit trail directory	/var/log/eprise Directory where our audit information is located.
Audit trail prefix	trail Prefix for the log files we collect (see Example 9-2 on page 234 where we defined this).
SSH KeyFile	finsys.ppk Private key we use to connect to the AIX system.
SSH Port	22 Default SSH port.
SSH User	insight User ID that we created on the AIX system for collection.

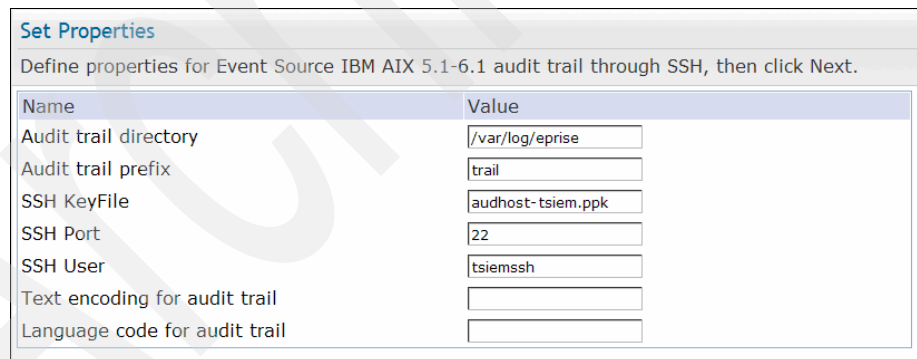


Figure 9-9 AIX event source properties

- Choose a collection schedule. In our case, we are testing and will trigger the collection manually. So, we can change the schedule later date.
- Choose a Reporting Database to store the collected data. In our case, we chose the GENERAL database so that we can apply the same policies to our AIX systems that we applied to the rest of our environment.
- Complete the Add Event Source Wizard.

Our AIX system is now configured to both generate appropriate audit data and for Tivoli Security Information and Event Manager to collect and report on that data. In the next section, we load and display the results of that load manually.

To install the Tivoli Security Information and Event Manager AIX event source software:

1. The software is available on the distribution package CZE8AEN, and the AIX software package is located in the subdirectory CZE8AEN/usr/sys/inst.images, and the name is ibm.tsiem.actuator. Upload this package to the AIX machine.
2. Make sure that the AIX machine meets the requirements that are described in the *IBM Tivoli Security Information and Event Manager Version 2.0 Event Source Guide*, SC23-9687. Following the installation instructions of that same guide, the installation of the software is shown in Figure 9-10 on page 242.

```

# installp -acgNq -X -d . ibm.tsiem.actuator
+-----+
+-----+
+-----+
+-----+
+-----+
Pre-installation Verification...
+-----+
+-----+
Verifying selections...done
Verifying requisites...done
Results...
SUCSESSES
-----
Filesets listed in this section passed pre-installation verification
and will be installed.

Selected Filesets
-----
ibm.tsiem.actuator 2.0.0.0 # IBM Tivoli Security Informat...
<< End of Success Section >>

FILESET STATISTICS
-----
1 Selected to be installed, of which:
  1 Passed pre-installation verification
-----
1 Total to be installed

Filesystem size changed to 524288
+-----+
+-----+
+-----+
Installing Software...
+-----+
+-----+
installp: APPLYING software for:
         ibm.tsiem.actuator 2.0.0.0

. . . . . << Copyright notice for ibm.tsiem >> . . . . .
IBM TivoliSecurity Information and Event Manager Actuator
Copyright (c) IBM Corp. 1998,2009. All Rights Reserved.
. . . . . << End of copyright notice for ibm.tsiem >>. . . . .

Finished processing all filesets. (Total time: 14 secs).
+-----+
+-----+
Summaries:
+-----+
+-----+

Installation Summary
-----
Name                                Level            Part            Event           Result
-----
ibm.tsiem.actuator                  2.0.0.0         USR             APPLY           SUCCESS
ibm_tsiem_actuator                  2.0.0.0         ROOT           APPLY           SUCCESS

```

Figure 9-10 Installing the AIX software

After the software is successfully installed, you can activate the AIX agent, which requires that you copy the configuration file from the Tivoli Security Information and Event Manager server to the AIX machine. If you use FTP to do this, make sure that the transfer mode is set to `ascii`. The activation step is shown in Figure 9-11 on page 243.

```
# ./install/setup.sh /tmp/TSIEM/aix.cfg_
```

Figure 9-11 Activate the AIX event source

The path to the configuration file must be the absolute path.

The activation result is shown in Figure 9-12 on page 244.

Archived

```

using agent ID 12.1.106 and TCP port base 5992
This is an AIX version 5 and release 3 machine
/var/log/eprise does not exist, so creating it.
chmod: /opt/IBM/tsiem/actuator/bin/genact-etrust: A file or directory in the path
name does not exist.
Creating databases
../bin/genasc ../actuator.ini 12.1.106 9.42.171.249 5992 12.1.1 ti0s02-sys1 5992
"Thu Mar 18 09:38:45 EST 2010 AIX ti0s02-sys4 3 5 0006910F4C00 /usr/bin:/etc:/u
sr/sbin:/usr/ucb:/usr/bin/X11:/sbin:/usr/java14/jre/bin:/usr/java14/bin" /var/lo
g/eprise/trail
CRMLOG, Validation test of stream
<20100318 14:38:45 utc> P261M902V0.0.1L335A5S0E10:Crm: Opened default log: stdou
t. Product: actuator.app. Version: 2.0. Builddate: 2010/02/09/19:51. Local time:
Thu Mar 18 09:38:45 2010.
<20100318 14:38:45 utc> P261M902V0.0.1L502A5S0E15:Crm: Closed default log: stdou
t
CRMLOG, Validation test of stream
<20100318 14:38:45 utc> P261M902V0.0.1L335A5S0E10:Crm: Opened default log: stdou
t. Product: actuator.app. Version: 2.0. Builddate: 2010/02/09/19:51. Local time:
Thu Mar 18 09:38:45 2010.
<20100318 14:38:45 utc> P261M902V0.0.1L502A5S0E15:Crm: Closed default log: stdou
t
CRMLOG, Validation test of stream
<20100318 14:38:45 utc> P261M902V0.0.1L335A5S0E10:Crm: Opened default log: stdou
t. Product: actuator.app. Version: 2.0. Builddate: 2010/02/09/19:51. Local time:
Thu Mar 18 09:38:45 2010.
<20100318 14:38:45 utc> P261M902V0.0.1L502A5S0E15:Crm: Closed default log: stdou
t
CRMLOG, Validation test of stream
<20100318 14:38:45 utc> P261M902V0.0.1L335A5S0E10:Crm: Opened default log: stdou
t. Product: actuator.app. Version: 2.0. Builddate: 2010/02/09/19:51. Local time:
Thu Mar 18 09:38:45 2010.
<20100318 14:38:46 utc> P261M902V0.0.1L502A5S0E15:Crm: Closed default log: stdou
t
CRMLOG, Validation test of stream
<20100318 14:38:46 utc> P261M902V0.0.1L335A5S0E10:Crm: Opened default log: stdou
t. Product: actuator.app. Version: 2.0. Builddate: 2010/02/09/19:51. Local time:
Thu Mar 18 09:38:46 2010.
<20100318 14:38:46 utc> P261M902V0.0.1L502A5S0E15:Crm: Closed default log: stdou
t
CRMLOG, Validation test of stream
<20100318 14:38:46 utc> P261M902V0.0.1L335A5S0E10:Crm: Opened default log: stdou
t. Product: actuator.app. Version: 2.0. Builddate: 2010/02/09/19:51. Local time:
Thu Mar 18 09:38:46 2010.
<20100318 14:38:46 utc> P261M902V0.0.1L502A5S0E15:Crm: Closed default log: stdou
t
CRMLOG, Validation test of stream
<20100318 14:38:46 utc> P261M902V0.0.1L335A5S0E10:Crm: Opened default log: stdou
t. Product: actuator.app. Version: 2.0. Builddate: 2010/02/09/19:51. Local time:
Thu Mar 18 09:38:46 2010.
<20100318 14:38:46 utc> P261M902V0.0.1L502A5S0E15:Crm: Closed default log: stdou
t
The actuator should now be installed and started.

```

Figure 9-12 AIX activation result

The AIX agent process shows up in the process list, as shown in Figure 9-13.

```
# ps -efad | grep agent
  root  5360      1  0 09:38:46 pts/0    0:08  ../bin/agent 12.1.106  ../log/clie
nt.log 74FF17706B
  root 14906 19374  0 09:39:56 pts/0    0:00  grep agent
# _
```

Figure 9-13 AIX agent process

When collections are initiated, actuator processes also show up in the process list. Each event source initiates a separate actuator process.

The agent sets up a secure channel with the Tivoli Security Information and Event Manager server, and if it succeeds, it shows a log entry in the agent's client.log file, which is found in the log subdirectory, as shown in Figure 9-14.

```
<20100318 14:38:54 utc> P261M902V0.0.1L2327A6S0E1110:TCP/IP Conn: a connection to
ti0s02-sys1:5992 is established
<20100318 14:38:54 utc> P261M902V0.0.1L280A4S0E80:LCM: Initial certification com
pleted successfully
<20100318 14:38:55 utc> P261M902V0.0.1L115A4S0E160:LCM: PKEP1...
<20100318 14:38:55 utc> P261M902V0.0.1L115A4S0E160:LCM: PKEP1.
```

Figure 9-14 Initial certification completed successfully

This log entry indicates that initial setup of the secure channel was successful and the collection mechanism for the event sources can be activated.

9.3.3 The results

The next time a collection and a database load are performed for the GENERAL Reporting Database, Tivoli Security Information and Event Manager uses the event source that we configured to logon remotely to the AIX server using SSH to collect the various audit files that we documented. After the collection is performed, the data is parsed and mapped to the W7 model and can be reported on in the iView portal. Figure 9-15 on page 246 shows that we collected and mapped the data successfully from our AIX system into the W7 model.



Figure 9-15 AIX events displayed in the Compliance Dashboard

Figure 9-16 shows the policy exceptions. We can see that we have a number of policy exceptions for our root user showing failed logon attempts.

Policy Exception Summary

Logon name	Where (Platform)	On What (Object group)	What (Event group)	#PolExcp
System	FINSYS (AIX)	Other Objects	User Actions - Process	6
INSIGHT.COM\FSPDC\$@INSIGHT.COM	INSIGHT\FSPDC (Windows)	Administration	Administration	6
INSIGHT.COM\ADMINISTRATOR@INSIGHT.COM	INSIGHT\FSPDC (Windows)	Other Objects	Security Changes	6
INSIGHT.COM\FSPDC\$@INSIGHT.COM	INSIGHT\FSPDC (Windows)	Administration	Security Changes	6
root	FINSYS (AIX)	System	Logon Failures	5
UNKNOWN_USER	FINSYS (AIX)	System	Logon Failures	5
ANONYMOUS	INSIGHT\FSPDC (Active Directory)	User Actions - File	User Actions - File	3
FSPDC\ADMINISTRATOR	INSIGHT\FSPDC (Windows)	System Updates	Logon Failures	3
SYSTEM	INSIGHT\FSPDC (Active Directory)	User Actions - File	User Actions - File	3
root	FINSYS (AIX)	Files	User Actions - File	2
INSIGHT\CEAROOT_OS	INSIGHT\FSPDC (Windows)	Administration	User Actions - File	2
INSIGHT.COM\ADMINISTRATOR@INSIGHT.COM	INSIGHT\FSPDC (Windows)	Administration	Security Changes	2
INSIGHT.COM\ADMINISTRATOR@INSIGHT.COM	INSIGHT\FSPDC (Windows)	Administration	Administration	2
NT AUTHORITY\NETWORK SERVICE	INSIGHT\FSPDC (Windows)	User Actions - Process	User Actions - Process	2
NT AUTHORITY\SYSTEM	INSIGHT\FSPDC (Windows)	User Actions - Process	Security Changes	2

Figure 9-16 Policy exceptions summary including our AIX system

Figure 9-17 shows further detail about the AIX system and shows object audit events for the root user who is attempting to access sensitive data, which can be further defined as a policy breach and can result in Tivoli Security Information and Event Manager generating an attention alert.

Severity	Date / Time	#	What (detail)	Where (detail)	Who (detail)	Where from (detail)	On what (detail)	Where to (detail)
10	Fri Aug 31 2007 13:56:11 GMT-05:00	1	Complete : Process / Success	FINSYS (AIX)	nobody	FINSYS (AIX)	SYSTEM : ./ Logon	FINSYS (AIX)
10	Fri Aug 31 2007 14:25:55 GMT-05:00	1	Read : Object / Success	FINSYS (AIX)	root	9.3.4.136 (Host)	Object : /home / sensitivedata	FINSYS (AIX)
10	Fri Aug 31 2007 14:25:55 GMT-05:00	1	Read : Object / Success	FINSYS (AIX)	root	9.3.4.136 (Host)	Object : /home / sensitivedata	FINSYS (AIX)
10	Fri Aug 31 2007 14:25:55 GMT-05:00	1	Read : Object / Success	FINSYS (AIX)	root	9.3.4.136 (Host)	Object : /home / sensitivedata	FINSYS (AIX)
10	Fri Aug 31 2007 14:25:55 GMT-05:00	1	Read : Object / Success	FINSYS (AIX)	root	9.3.4.136 (Host)	Object : /home / sensitivedata	FINSYS (AIX)
10	Fri Aug 31 2007 14:26:39 GMT-05:00	1	Read : File / Success	FINSYS (AIX)	root	FINSYS (AIX)	File : /etc/security / passwd	FINSYS (AIX)
10	Fri Aug 31 2007 14:26:39 GMT-05:00	1	Read : File / Success	FINSYS (AIX)	root	FINSYS (AIX)	File : /etc/security / passwd	FINSYS (AIX)
10	Fri Aug 31 2007 14:30:00 GMT-05:00	1	Read : File / Success	FINSYS (AIX)	root	FINSYS (AIX)	File : /etc/security / passwd	FINSYS (AIX)

Figure 9-17 root user accessing sensitive data

Figure 9-18 shows how to change the sensitive data significance in our policy so that it highlights unusual attempts to access sensitive data. Of course, the significance value must align with the results of your risk analysis.

Policy: Duplicate of 2000010... Platform: AIX
 Policy Type: Work Group Definition Set: AIX_group

Create Delete Create Group Wizard

--- Select Action --- Go Sensitive data - user we gave the group a significance of 99

Sel...	Group Name	Dimensi...	Significa...
<input type="checkbox"/>	Sensitive Data - User	ONWHAT	99

Page 1 of 1 Total: 139 Filtered: 1 Displayed: 1

Figure 9-18 Highlighting access to sensitive data on our AIX server

Figure 9-19 on page 248 shows the results of applying this policy.

Severity	Date / Time	#	What (detail)	Where (detail)	Who (detail)	Where from (detail)	On what (detail)	Where to (detail)
99	Fri Aug 31 2007 14:25:55 GMT-05:00	1	Read : Object / Success	FINSYS (AIX)	root	9.3.4.136 (Host)	Object : home / sensitivedata	FINSYS (AIX)
99	Fri Aug 31 2007 14:25:55 GMT-05:00	1	Read : Object / Success	FINSYS (AIX)	root	9.3.4.136 (Host)	Object : home / sensitivedata	FINSYS (AIX)
99	Fri Aug 31 2007 14:25:55 GMT-05:00	1	Read : Object / Success	FINSYS (AIX)	root	9.3.4.136 (Host)	Object : home / sensitivedata	FINSYS (AIX)
99	Fri Aug 31 2007 14:25:55 GMT-05:00	1	Read : Object / Success	FINSYS (AIX)	root	9.3.4.136 (Host)	Object : home / sensitivedata	FINSYS (AIX)
30	Thu Aug 30 2007 09:25:05 GMT-05:00	1	Authenticate : User / Failure	FINSYS (AIX)	UNKNOWN_USER	HMC1.ITSC.AUSTIN.IBM.COM (Host)	SYSTEM : FINSYS / Logon	FINSYS (AIX)
30	Thu Aug 30 2007 09:25:06 GMT-05:00	1	Authenticate : User / Failure	FINSYS (AIX)	UNKNOWN_USER	HMC1.ITSC.AUSTIN.IBM.COM (Host)	SYSTEM : FINSYS / Logon	FINSYS (AIX)

Figure 9-19 Policy applied

In Figure 9-20, we further refine this policy by defining a special attention alert that can notify security officers about attempts to access sensitive data.

Policy Editor

Policy Editor > Attention Rules > Create Rule

Policy: Duplicate of 20000101000000 Policy Type: Work

Who

What

When

Where

On What

Where From

Where To

Severity (1-99) *99

Rule ID

Description

Figure 9-20 Our special attention alert definition

Figure 9-21 on page 249 shows the results of this special attention alert when access to sensitive data is detected.

Special Attention Summary					
Severity	Logon name	Where (Platform)	On What (Object group)	What (Event group)	#SpecAtt
99	root	FINSYS (AIX)	Sensitive Data - User	User Actions - File	4
99	root	FINSYS (AIX)	Sensitive Data	User Actions - File	4
20	Unavailable	FINSYS (AIX)	System	Alerts - Low	1
20	Unavailable	FINSYS (AIX)	System	Alerts	1

Figure 9-21 Special attentions when sensitive data has been accessed

9.3.4 AIX auditing conclusion

In this section, we showed you how to configure Tivoli Security Information and Event Manager to collect audit data from the AIX platforms and how policies can be applied to this data.

Also, refer to the use of the `aixpert` command in the AIX 6.1 security document. The command helps you to set up auditing to a certain IBM recommended level.

In the next sections, we cover additional platforms. Our coverage is not as detailed because the basic steps are very similar. Key aspects that we highlight in the following sections are:

- ▶ How to set up auditing on the target system
- ▶ What the event source configuration options must be to collect from those event sources

9.4 Auditing Lotus Domino R6 systems

IBM Lotus Domino is the premier collaborative and e-mail environment from IBM. As such, it often hosts important and sensitive information. In this part of the project, X-Y-Z extends their audit capabilities to incorporate the audit information that is contained in the Domino Administration Requests Database.

9.4.1 Configuring auditing for Domino systems

A default installation of Domino creates and uses two main databases that are used by Tivoli Security Information and Event Manager for audit monitoring. These databases are:

- | | |
|-------------------|---|
| log.nsf | This database contains Miscellaneous Domino system events and mail routing events and generally holds these events for the last seven days worth of activity. Both of these event types are extracted and collected by Tivoli Security Information and Event Manager. |
| admin4.nsf | This is the Domino administration requests database. It contains all of the administrative requests for a Domino domain and is the primary place that administrative actions are logged in Domino. |

No further configuration of Domino is required because both of these databases are created by default when you install Domino. Our next step is to configure Tivoli Security Information and Event Manager to capture this information and store it in the Tivoli Security Information and Event Manager repository.

9.4.2 Adding the Domino event source

Tivoli Security Information and Event Manager requires an agent with the Lotus Notes® client installed on it. The Lotus Notes client is used by the agent to access the audit information that we previously described. Prior to configuring the Domino event sources in Tivoli Security Information and Event Manager, you must install the Lotus Notes client on the target system.

After you install the Notes client, you can test that it can access the audit data by performing the following steps:

1. Logon to the target system as the Administrator user that Tivoli Security Information and Event Manager is using to collect data. In our case, this user was *cearoot_os* (the default user is *cifadmin*).
2. Start the Lotus Notes client, and logon to Notes using the Notes user that Tivoli Security Information and Event Manager will use to access the Notes client.
3. From within the Lotus Notes client, open the Notes Log (*log.nsf*) and Administration Requests (*admin4.nsf*) databases on the Domino server. If this is successful, the Notes client is configured correctly for Tivoli Security Information and Event Manager to use.

When you confirm that the Lotus Notes client on the target system can access the Domino audit data, you can create the new Tivoli Security Information and Event Manager Domino event source. This function is performed in the same way as other event sources were added to Tivoli Security Information and Event Manager. The basic steps are:

1. To start the Add Event Source Wizard, in the Tivoli Security Information and Event Manager portal, select **Managing Event Sources**.
2. When the wizard asks you for a machine on which the application runs that you want to audit, Figure 9-22, select the machine on which the Notes client is installed (this machine should already be an agent, and if it is not, you must install the appropriate agent on that machine prior to commencing execution of the Add New Event Source Wizard). In our case, the machine is already being audited for Windows events, so it previously had a Windows agent installed.

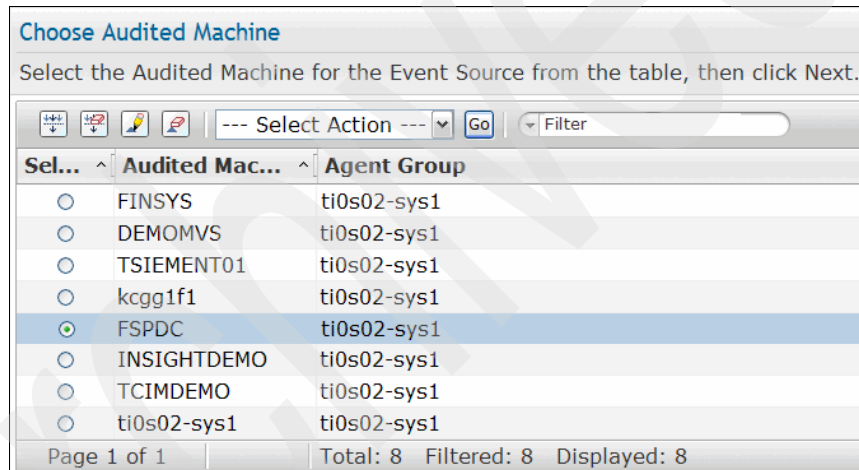


Figure 9-22 Select the Domino audit machine

3. When asked to choose the event source type, select the Lotus Notes event source, as shown in Figure 9-23.

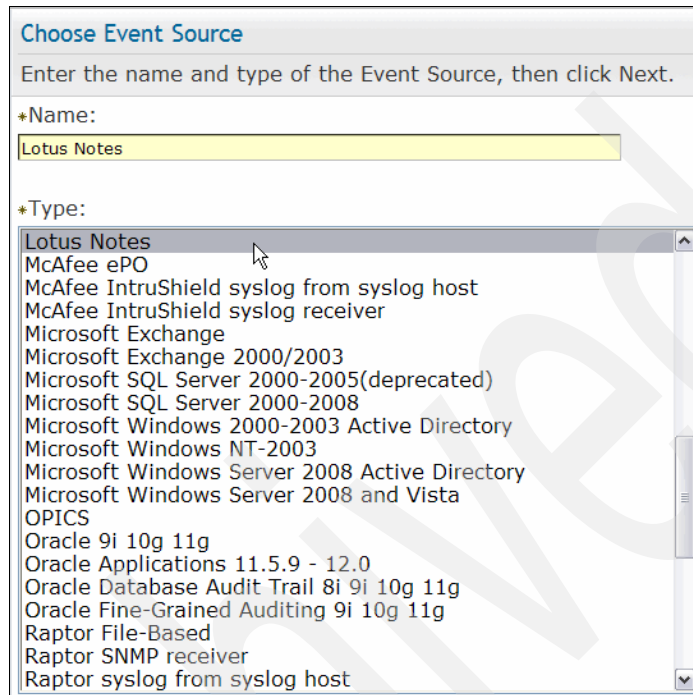


Figure 9-23 Select the Lotus Notes event source

4. Define the event source properties, as shown in Figure 9-24. In this dialog box, enter the details for the Domino server that you want to audit, for example, the entries are for the Server name (fspdc in our case), Logfile (which remains the same), Password (you are asked for the current password and to create a new password for the Notes user), and the Admin Requests database file name (which you should not need to change).

Name	Value
1 - Server	FSPDC
2 - Logfile	log.nsf
3 - Password	
4 - Admin Requests	admin4.nsf
Text encoding for audit trail	
Language code for audit trail	

Figure 9-24 Defining the Domino event source properties

5. Next, define the collection and load schedules and complete the Event Source Definition Wizard. The next time you perform a scheduled collection and load, you will have collected audit data from the Lotus Domino event source.

In this section, we described the process of adding the Lotus Domino event source to our Tivoli Security Information and Event Manager implementation. In the next section, we show the results of this process.

9.4.3 The results

After you define the auditing configuration and configured the event source, you now have collected Lotus Domino audit event data within the Tivoli Security Information and Event Manager repository, as shown in Figure 9-25 on page 254.

▼ Data in this database				
Where (Platform)	Start time	End time	#Chunks	#Events
INSIGHT\FSPDC (Active Directory)	Sat Sep 01 2007 02:50:24 GMT-05:00	Mon Sep 03 2007 02:50:24 GMT-05:00	1	14
fspdc (DOMINO)	Wed Aug 22 2007 18:00:19 GMT-05:00	Mon Sep 03 2007 13:11:44 GMT-05:00	5	1267
FINSYS (AIX)	Tue Jul 24 2007 10:27:37 GMT-05:00	Mon Sep 03 2007 12:43:43 GMT-05:00	2	1181
INSIGHT\FSPDC (Windows)	Fri Aug 31 2007 17:22:53 GMT-05:00	Mon Sep 03 2007 13:33:04 GMT-05:00	11	14572

Our new Domino audit data

Figure 9-25 Domino audit data within Tivoli Security Information and Event Manager

Now, you must apply the appropriate policy, and create appropriate attention alerts. To illustrate what is possible here, we highlighted two cases.

In the first case, Lotus Domino captures a lot of information in its `admin4.nsf` and `log.nsf` databases. This information is captured and stored in the Tivoli Security Information and Event Manager repository. However, much of this information is just about business as usual within our policy guidelines and must not be highlighted as a policy breach. After our first data collect and load, we noticed the results in Tivoli Security Information and Event Manager shown in Figure 9-26, which show a lot of policy violations that were generated by the data collected from the Notes Domino system.

Policy Exception Summary				
Logon name	Where (Platform)	On What (Object group)	What (Event group)	#PolExcp
Unavailable	fspdc (DOMINO)	Database Objects	User Actions - File	1114
nobody	FINSYS (AIX)	Other Objects	User Actions - Process	256
root	FINSYS (AIX)	Files	User Actions - File	240
root	FINSYS (AIX)	System Files	User Actions - File	240
root	FINSYS (AIX)	TCB	User Actions - File	240
root	FINSYS (AIX)	Other Objects	User Actions - Process	114

Policy Exceptions

Figure 9-26 Domino policy exceptions

On closer inspection, the majority of these events appear to be related to a Domino function called *journaling*, as shown in Figure 9-27 on page 255.

Lotus Domino journaling: Lotus Domino journaling is a function where each mail item is inspected, and those mail items that match predefined rules have a copy retained.

Severity	Date / Time	#	What (detail)	Where (detail)	Who (detail)	Where from (detail)	On what (detail)
10	Thu Aug 23 2007 01:00:20 GMT-05:00	1	Modify : Object / Success	fspdc (DOMINO)	Unavailable	fspdc (DOMINO)	DBOBJECT : Mail Journaling (6) / Entry
10	Thu Aug 23 2007 01:00:20 GMT-05:00	1	Modify : Object / Success	fspdc (DOMINO)	Unavailable	fspdc (DOMINO)	DBOBJECT : Mail Journaling (6) / Entry
10	Thu Aug 23 2007 01:00:20 GMT-05:00	1	Modify : Object / Success	fspdc (DOMINO)	Unavailable	fspdc (DOMINO)	DBOBJECT : Mail Journaling (6) / Entry
10	Thu Aug 23 2007 01:00:20 GMT-05:00	1	Modify : Object / Success	fspdc (DOMINO)	Unavailable	fspdc (DOMINO)	DBOBJECT : Mail Journaling (6) / Entry
10	Thu Aug 23 2007 01:00:20 GMT-05:00	1	Modify : Object / Success	fspdc (DOMINO)	Unavailable	fspdc (DOMINO)	DBOBJECT : Mail Journaling (6) / Entry
10	Thu Aug 23 2007 01:00:20 GMT-05:00	1	Modify : Object / Success	fspdc (DOMINO)	Unavailable	fspdc (DOMINO)	DBOBJECT : Mail Journaling (6) / Entry
10	Thu Aug 23 2007 01:00:20 GMT-05:00	1	Modify : Object / Success	fspdc (DOMINO)	Unavailable	fspdc (DOMINO)	DBOBJECT : Mail Journaling (6) / Entry
10	Thu Aug 23 2007 01:00:20 GMT-05:00	1	Modify : Object / Success	fspdc (DOMINO)	Unavailable	fspdc (DOMINO)	DBOBJECT : Mail Journaling (6) / Entry
10	Thu Aug 23 2007 01:00:20 GMT-05:00	1	Modify : Object / Success	fspdc (DOMINO)	Unavailable	fspdc (DOMINO)	DBOBJECT : Mail Journaling (6) / Entry
10	Thu Aug 23 2007 01:00:20 GMT-05:00	1	Modify : Object / Success	fspdc (DOMINO)	Unavailable	fspdc (DOMINO)	DBOBJECT : Mail Journaling (6) / Entry

Figure 9-27 Domino policy exceptions

We determined that this was not a policy exception, so we changed our policy definitions, which we further describe in the next paragraphs.

First, we created an On What group definition called *Journaling*, as shown in Figure 9-28 on page 256. We defined a group to highlight Database Object operations where the object path contains the value *Journal*. This group was assigned a very low significance because operations on this object are considered to be low risk.

Content Summary

Policy:	Duplicate of 2000010...	Group Definition Set:	DOMINO_5_group
Policy Type:	Work	Group:	Journalling
Platform:	DOMINO_5	Dimension:	ONWHAT

Condition Table

Select the condition you want to work with. Changes are saved only when you click the OK or Apply button.

Create Delete Paste in group(s)

--- Select Action --- Go Filter

Filter	Condition Name
<input type="checkbox"/>	Database Objects
<input type="checkbox"/>	Journal

Page 1 of 1 Total: 2 Filtered: 2 Displayed: 2

Figure 9-28 Group definition for journaling

We then created a policy that indicated that journaling actions were within our policy, as shown in Figure 9-29.

Policy Editor

Policy Editor > Policy Rules > Create Rule

Policy: Duplicate of 20000101000000 Policy Type: Work

Who Select Group

What Select Group

When Select Group

Where Select Group

On What Journalling Select Group

Where From Select Group

Where To Select Group

Description System access to journals

OK Cancel

Figure 9-29 Our journaling policy

The results are a massive reduction in the number of policy violations that Tivoli Security Information and Event Manager reports, as shown in Figure 9-30 on page 257.

Policy Exception Summary				
Logon name	Where (Platform)	On What (Object group)	What (Event group)	#PolExcp
Unavailable	fspdc (DOMINO)	Dbc Actions	Administration	100
Unavailable	fspdc (DOMINO)	Dbc Actions	Security Changes	100
fspdc	fspdc (DOMINO)	System	Alerts	30
IT	fspdc (DOMINO)	Dbc Actions	Administration	5
fspdc	fspdc (DOMINO)	System	Alerts - Low	30
IT	fspdc (DOMINO)	Dbc Actions	Security Changes	5
Agent Manager	fspdc (DOMINO)	Process	Warnings	4
Agent Manager	fspdc (DOMINO)	Processes	Warnings	4

Figure 9-30 Reduced Domino policy exceptions

In our case, we were also particularly concerned about users or administrators who accessed a mail box named *Sensitive Mail*. So, our next step was to create the appropriate policy groups and attention rules to highlight attempts to access the Sensitive Mail box. We did this by adding a requirement to the On What policy group that defines anything that contains the string *Sensitive* in its object name to be Sensitive data, as shown in Figure 9-31.

Requirement Table

Select the requirement you want to work with.

Sel...	Requirement Name
<input type="checkbox"/>	Object name contains sensitive

Figure 9-31 The Sensitive data - User policy group definition

We also wanted special attention alerts if someone attempts to access this mailbox out of hours, so we defined a special attention rule, as shown in Figure 9-32 on page 258.

Although we already highlighted the difference between a policy rule and a special attention rule several times throughout this book, we think it is worth describing again. Normal policy rules define what is allowed, anything else is a policy exception. A special attention rule is the opposite of the normal policy and specifically defines what is *not* allowed.

Policy Editor

Policy Editor > Attention Rules > Edit Rule

Policy: Duplicate of 20000101000000 Policy Type: Work

Who

What

When

Where

On What

Where From

Where To

Severity (1-99) *

Rule ID

Description

Figure 9-32 Our Domino special attention rule

Figure 9-33 and Figure 9-34 on page 259, respectively, show the result of creating this policy grouping definition and special attention rule.

Severity	Date / Time	#	What (detail)	Where (detail)	Who (detail)	Where from (detail)	On what (detail)	Where to (detail)
99	Mon Sep 03 2007 12:35:02 GMT-05:00	1	Create : Database / Success	fspdc (DOMINO)	IT	fspdc (DOMINO)	DATABASE : / / roaming/SensitiveMailbox\names.nsf	fspdc (DOMINO)
99	Mon Sep 03 2007 12:35:04 GMT-05:00	1	Create : Database / Success	fspdc (DOMINO)	IT	fspdc (DOMINO)	DATABASE : / / roaming/SensitiveMailbox\bookmark.nsf	fspdc (DOMINO)
99	Mon Sep 03 2007 12:35:06 GMT-05:00	1	Create : Database / Success	fspdc (DOMINO)	IT	fspdc (DOMINO)	DATABASE : / / roaming/SensitiveMailbox\journal.nsf	fspdc (DOMINO)
99	Mon Sep 03 2007 13:02:18 GMT-05:00	1	Modify : User / Success	fspdc (DOMINO)	Sensitive Mailbox/TCIM	fspdc (DOMINO)	SYSTEM : fspdc / CN=Sensitive Mailbox/O=TCIM	fspdc (DOMINO)
99	Mon Sep 03 2007 13:01:22 GMT-05:00	1	Receive : Mail / Success	fspdc (DOMINO)	Router	fspdc (DOMINO)	EMAIL : / / Sensitive Mailbox/TCIM	fspdc (DOMINO)
50	Thu Aug 23 2007 01:00:02 GMT-05:00	1	Add : Database / Success	fspdc (DOMINO)	Unavailable	fspdc (DOMINO)	DATABASE : / / AgentRunner.nsf	fspdc (DOMINO)

Figure 9-33 Policy exceptions for users accessing our Sensitive mail file

Setup:

Month Day Year Hour Min.
 Start time August 1 2007 10 27
 End time September 3 2007 13 7

Execute Reset

Time zone: Event time zone

Severity	Date / Time	#	What (detail)	Where (detail)	Who (detail)	Where from (detail)	On what (detail)	Where to (detail)
99	Mon Sep 03 2007 02:35:06 GMT-05:00	1	Create: Database / Success	fspdc (DOMINO)	IT	fspdc (DOMINO)	DATABASE: ./roaming/SensitiveMailbox/journal.nsf	fspdc (DOMINO)
99	Mon Sep 03 2007 02:35:04 GMT-05:00	1	Create: Database / Success	fspdc (DOMINO)	IT	fspdc (DOMINO)	DATABASE: ./roaming/SensitiveMailbox/bookmark.nsf	fspdc (DOMINO)
99	Mon Sep 03 2007 02:35:02 GMT-05:00	1	Create: Database / Success	fspdc (DOMINO)	IT	fspdc (DOMINO)	DATABASE: ./roaming/SensitiveMailbox/notes.nsf	fspdc (DOMINO)
99	Mon Sep 03 2007 03:01:22 GMT-05:00	1	Receive: Mail / Success	fspdc (DOMINO)	Router	fspdc (DOMINO)	EMAIL: ./Sensitive Mailbox/TCIM	fspdc (DOMINO)
99	Mon Sep 03 2007 03:02:18 GMT-05:00	1	Modify: User / Success	fspdc (DOMINO)	Sensitive Mailbox/TCIM	fspdc (DOMINO)	SYSTEM: fspdc / CN=Sensitive Mailbox/O=TCIM	fspdc (DOMINO)
20	Wed Aug 22 2007 18:10:13 GMT-05:00	1	Start: Server / Success	fspdc (DOMINO)	fspdc	fspdc (DOMINO)	SYSTEM: - / fspdc	fspdc (DOMINO)

Figure 9-34 Special attention alerts for users accessing our Sensitive mailbox out of business hours

In this section, we discussed how to add Lotus Domino to your audited environment using Tivoli Security Information and Event Manager and how X-Y-Z created basic policies and attention alerts for their Domino audit data. In the next section, we extend our auditing to the SAP platform.

9.5 Auditing SAP systems

As part of phase two of X-Y-Z's implementation of Tivoli Security Information and Event Manager, we extend auditing to the SAP R/3 systems that are running on Windows. The steps that are required to configure Tivoli Security Information and Event Manager to audit SAP R/3 are similar to the other systems, for example, we must:

1. Configure the target system to produce appropriate auditable information.
2. Set up the target so that Tivoli Security Information and Event Manager can collect that audit information.
3. Configure the new event source within Tivoli Security Information and Event Manager.
4. Create or modify policies that are required for the SAP system.

In this section, we talk about the major steps that are required to archive these goals.

9.5.1 Configuring auditing for SAP systems

Release 4.0 and later of SAP R/3 supports an internal auditing system called the *Security Audit Log*. Each SAP application server maintains its own daily audit log file. You can specify the name and location of the Security Audit Log using the `rsau/local/file` profile parameter. We took the information in this section from the *IBM Tivoli Security Information and Event Manager Version 2.0 Installation Guide*, GI11-8778, which describes the various parameters that can be set, as e Table 9-1 shows.

Table 9-1 Audit log parameter settings for SAP

Audit Log Parameter	Set value to...
<code>rsau/enable</code>	1
<code>rsau/local/file</code>	path to audit log file
<code>rsau/max_diskspace/local</code>	maximum space to allocate for the audit files
<code>rsau/selection_slots</code>	3
<code>rec/client</code>	ALL

Configuration details: The `rsau/local/file` parameter contains the entire path name to the audit logs and the file name. The file name must include the plus symbol (+) to include a variable date part. Do not include a file extension in the file name. Here are examples for clarification:

- ▶ This example shows a valid path and file name:

```
/usr/sap/machine1/log/audit_++++++
```

- ▶ This example shows an invalid path and file name. The file name does not include a date part:

```
/usr/sap/machine1/log/audit
```

- ▶ This example shows an invalid path and file name. The file name includes a file extension:

```
/usr/sap/machine1/log/audit_++++++.aud
```

After you configure the basic audit settings, you must specify the events to audit and log. Start SAP transaction SM19 to specify the events to log in the Audit Security Log. The installation guide for Tivoli Security Information and Event Manager provides suggested settings to specify the events that you log and the audit settings for each of those events.

Another point to note is that SAP R/3 logging is not circular, which means that when the log reaches the size that is specified by the `max_disksize` parameter, the audit process stops. To prevent this from happening, you can set the `max_disksize` parameter to a reasonable size and schedule an operating system job to delete old SAP R/3 audit logs. Alternatively, there is an SAP transaction SM18 that can do this task for you.

After you configure the SAP R/3 event source to produce appropriate audit logs, you are ready to add the event source to the Tivoli Security Information and Event Manager installation.

9.5.2 Adding the SAP event source

Prior to adding the SAP event source, you must install an agent on the system where SAP resides. Then, adding an SAP R/3 event source is handled the same way as adding any other Tivoli Security Information and Event Manager event source.

To add the SAP event source:

1. Start the Add Event Source Wizard, and select the agent machine that collects the SAP audit logs and the Reporting Database to take the records.
2. Select the event source type, as shown in Figure 9-35 on page 262. Click **Next**.

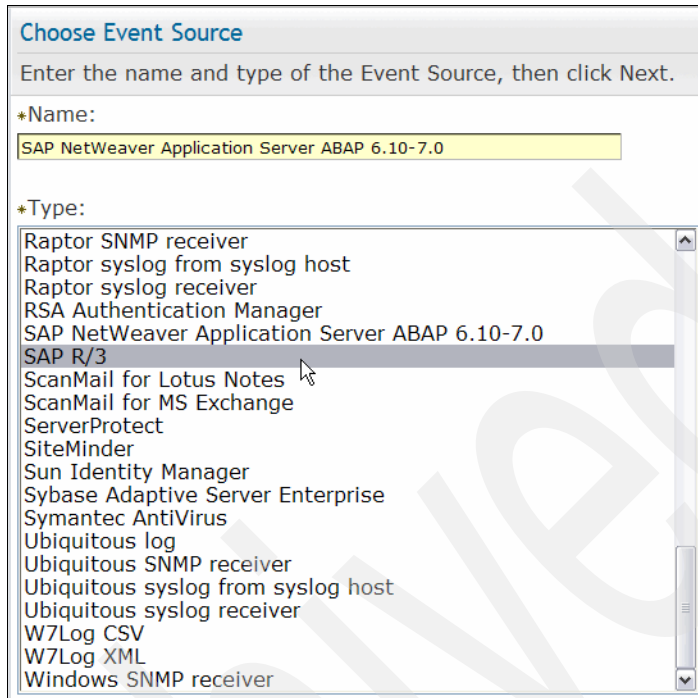


Figure 9-35 Select the SAP R/3 event source type

3. Define the event source properties, as shown in Figure 9-36. The details that are required here are the prefix for the SAP Log Name (audit_ by default), the SAP Log Directory, and the SAP Version. Click **Next**.

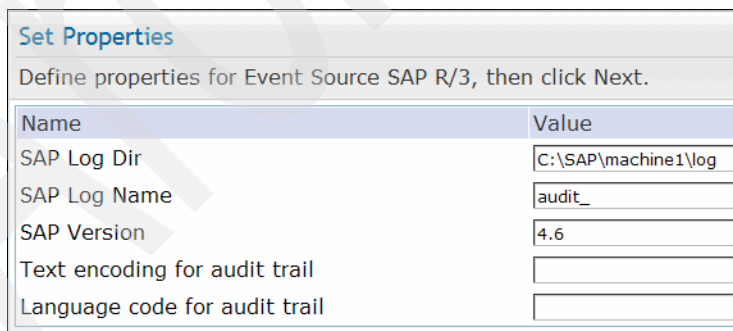


Figure 9-36 Define the event source properties

4. Define a collection schedule.
5. After you complete the Add Event Source Wizard, you can configure Tivoli Security Information and Event Manager to collect your SAP R/3 audit data.

In the next section, we show the results of this data collection.

9.5.3 The results

After you perform the steps that are outlined in the previous sections, you have configured Tivoli Security Information and Event Manager to collect audit data from SAP R/3. This configuration results in Tivoli Security Information and Event Manager collecting the SAP R/3 audit data from the Windows system that hosts the SAP R/3 instance and then mapping it to the W7 format and loading the data into the specified Reporting Database.

Figure 9-37 and Figure 9-38 show how the SAP R/3 data looks when it is loaded into the Reporting Database.

▼ Data in this database					
Where (Platform)	Start time	End time	#Chunks	#Events	
800 (SAP R/3)	Fri Aug 31 2007 10:36:08 GMT-06:00	Wed Sep 5 2007 5:05:22 GMT-06:00	5	6713	
000 (SAP R/3)	Fri Aug 31 2007 10:51:45 GMT-06:00	Wed Sep 5 2007 14:18:05 GMT-06:00	4	17054	

Figure 9-37 SAP R/3 data in Tivoli Security Information and Event Manager

Severity	Date / Time	#	What (detail)	Where (detail)	Who (detail)	Where from (detail)	On what (detail)	Where to (detail)
50	Mon Mar 31 2003 10:36:08 GMT-06:00	1	Modify : Auditpolicy / Success	800 (SAP R/3)	THIMMEL	p42554	SYSTEM : 800 / Audit	800
50	Mon Mar 31 2003 10:36:08 GMT-06:00	1	Modify : Auditpolicy / Success	800 (SAP R/3)	THIMMEL	p42554	SYSTEM : 800 / Audit	800
2	Mon Mar 31 2003 10:38:02 GMT-06:00	1	Logon : User / Success	800 (SAP R/3)	HAUSER	800	SYSTEM : 800 / Logon	800
10	Mon Mar 31 2003 10:38:41 GMT-06:00	1	Call : Function / Success	800 (SAP R/3)	THIMMEL	p42554	FUNCTION : SH19 / STREE_UPDATE_INDX_GENER	800
10	Mon Mar 31 2003 10:38:43 GMT-06:00	1	Call : Function / Success	800 (SAP R/3)	THIMMEL	p42554	FUNCTION : SH19 / STREE_UPDATE_INDX_GENER	800
2	Mon Mar 31 2003 10:43:03 GMT-06:00	1	Logon : User / Success	800 (SAP R/3)	HAUSER	800	SYSTEM : 800 / Logon	800
10	Mon Mar 31 2003 10:46:43 GMT-06:00	1	Stop : Audit / Success	800 (SAP R/3)	THIMMEL	p42554	SYSTEM : 800 / Audit	800
50	Mon Mar 31 2003 10:49:51 GMT-06:00	1	Start : Audit / Success	800 (SAP R/3)	THIMMEL	p42554	SYSTEM : 800 / Audit	800
50	Mon Mar 31 2003 10:49:51 GMT-06:00	1	Modify : Auditpolicy / Success	800 (SAP R/3)	THIMMEL	p42554	SYSTEM : 800 / Audit	800

Figure 9-38 SAP R/3 platform history event list

You can now apply a policy to this data in the same way that you applied policies to each of the other audit event data sources, for example, in our environment, we want to highlight users who modified an SAP system audit policy. To do this,

we use the policy group definition using the standard SAP R/3 Tivoli Security Information and Event Manager provided groupings shown in Figure 9-39.

Content Summary

Policy: Duplicate of 2000010... Platform: SAPR3
 Policy Type: Work Group Definition Set: SAPR3_group

Buttons: Create, Delete, Create Group Wizard

Change Significance: [dropdown] Go [system up]

Sel...	Group Name	Dimensi...	Significa...
<input checked="" type="checkbox"/>	System Updates	WHAT	75

Page 1 of 1 | Total: 145 | Filtered: 1 | Displayed: 1

Figure 9-39 Modify significance of the System Updates What action

We can then create simple policy rules to emphasize what is considered normal activity within the policy, such as user actions in office hours, system administration during office hours, report runs outside of office hours, and so on, as illustrated in Figure 9-40.

Sel...	Who	What	When	Where	On What
<input type="checkbox"/>	Systems Admin - Produ...	Write Data		Production Systems	Write Sensitive Data - Production
<input type="checkbox"/>	Systems Admin - Produ...	CreateDelete...		Production Systems	CreateDelete Sensitive Data - Pro...
<input type="checkbox"/>	Users		Office Hours	SAP	
<input type="checkbox"/>	System Administrators		Office Hours	SAP	
<input type="checkbox"/>				SAP	Reports
<input type="checkbox"/>	Administrators			Systems with non-segregated admin...	

Figure 9-40 Our SAP policy rules

We also create several attention rules that can alert us if certain actions are performed that are not in accordance with our policy, for example, someone modifies our audit policy, as shown in Figure 9-41.

Sel...	W...	What	Wh...	Where	On W...	Where Fr...	Where ...	Seve...	Rule ID
<input type="checkbox"/>				Customer Inform...					40 access me...
<input type="checkbox"/>		Modify Auditpolicy		SAP					75

Page 4 of 4 | 4 | Go | Total: 47 | Filtered: 47 | Displayed: 2

Figure 9-41 Special attention definition for change of SAP audit policy

These policy and attention definitions result in a dashboard that looks like Figure 9-42. This dashboard groups all of the events according to our policy groupings and highlights events that are associated with changes to the SAP audit policies. It also shows the special attentions.



Figure 9-42 SAP Compliance Dashboard

Clicking the intersection of the Ordinary Users and System Updates grid (this intersection is highlighted in red because it contains high severity policy violations) shows us all of the events for Ordinary Users performing System Update activities, as shown in Figure 9-43 on page 266.

Time zone: Event time zone

Severity	When	#	What	Where	Who	From Where	On What	Where To
75	Mon Mar 31 2003 10:36:08 GMT-06:00	1	Modify / Auditpolicy : Success	800	THIMMEL	p42554	SYSTEM : 800 / Audit	800
75	Mon Mar 31 2003 10:36:08 GMT-06:00	1	Modify / Auditpolicy : Success	800	THIMMEL	p42554	SYSTEM : 800 / Audit	800
75	Mon Mar 31 2003 10:49:51 GMT-06:00	1	Start / Audit : Success	800	THIMMEL	p42554	SYSTEM : 800 / Audit	800
75	Mon Mar 31 2003 10:49:51 GMT-06:00	1	Modify / Auditpolicy : Success	800	THIMMEL	p42554	SYSTEM : 800 / Audit	800
75	Mon Mar 31 2003 10:49:51 GMT-06:00	1	Modify / Auditpolicy : Success	800	THIMMEL	p42554	SYSTEM : 800 / Audit	800
75	Mon Mar 31 2003 10:49:51 GMT-06:00	1	Modify / Auditpolicy : Success	800	THIMMEL	p42554	SYSTEM : 800 / Audit	800
75	Tue Apr 01 2003 14:18:23 GMT-06:00	1	Modify / Auditpolicy : Success	800	THIMMEL	p45757	SYSTEM : 800 / Audit	800
75	Tue Apr 01 2003 14:19:26 GMT-06:00	1	Modify / Auditpolicy : Success	800	THIMMEL	p45757	SYSTEM : 800 / Audit	800
75	Tue Apr 01 2003 14:18:23 GMT-06:00	1	Modify / Auditpolicy : Success	800	THIMMEL	p45757	SYSTEM : 800 / Audit	800
75	Tue Apr 01 2003 14:19:26 GMT-06:00	1	Modify / Auditpolicy : Success	800	THIMMEL	p45757	SYSTEM : 800 / Audit	800
75	Mon Mar 31 2003 10:36:08 GMT-06:00	1	Modify / Auditpolicy : Success	800	THIMMEL	p42554	SYSTEM : 800 / Audit	800
75	Mon Mar 31 2003 10:36:08 GMT-06:00	1	Modify / Auditpolicy : Success	800	THIMMEL	p42554	SYSTEM : 800 / Audit	800
75	Mon Mar 31 2003 10:49:51 GMT-06:00	1	Start / Audit : Success	800	THIMMEL	p42554	SYSTEM : 800 / Audit	800
75	Mon Mar 31 2003 10:49:51 GMT-06:00	1	Modify / Auditpolicy : Success	800	THIMMEL	p42554	SYSTEM : 800 / Audit	800
75	Mon Mar 31 2003 10:49:51 GMT-06:00	1	Modify / Auditpolicy : Success	800	THIMMEL	p42554	SYSTEM : 800 / Audit	800
75	Mon Mar 31 2003 10:36:08 GMT-06:00	1	Modify / Auditpolicy : Success	800	THIMMEL	p42554	SYSTEM : 800 / Audit	800
75	Mon Mar 31 2003 10:36:08 GMT-06:00	1	Modify / Auditpolicy : Success	800	THIMMEL	p42554	SYSTEM : 800 / Audit	800
75	Mon Mar 31 2003 10:49:51 GMT-06:00	1	Start / Audit : Success	800	THIMMEL	p42554	SYSTEM : 800 / Audit	800

Figure 9-43 High severity policy exceptions displayed

Clicking the special attention summary icon shows us that the user THIMMEL is our culprit, as shown in Figure 9-44.

Special Attention Summary					
Severity	Logon name	Where (Platform)	On What (Object group)	What (Event group)	#SpecAtt
75	THIMMEL	800 (SAP R/3)	System Objects	System Updates	31

Figure 9-44 Special attention summary: Highlighting THIMMEL

9.5.4 SAP R/3 auditing conclusion

In this section, we extended the Tivoli Security Information and Event Manager implementation to cover audit data from the SAP R/3 systems. We added a new event source type and then applied policies and special attention rules to the data that Tivoli Security Information and Event Manager captured.

9.6 Adding syslog receiver for any type of messages

Before deploying Tivoli Security Information and Event Manager, X-Y-Z used a log collection tool that heavily relied on the syslog protocol. It was used for several years to receive, archive, and report on multiple types of syslog messages that were generated by a major number of platforms that X-Y-Z used. It was decided that the QUANT tool must not be audited using the syslog protocol

because its reliability is insufficient to properly address XYZ's business requirements.

Another reason to quit using the syslog message collection is because several regulations and certain auditors require compliance reports for X-Y-Z's IT environment that cannot easily be produced using the syslog protocol. Finally, X-Y-Z was notified by the auditors that the syslog messages that the platforms generated are typically not the events that are generated by the native audit subsystems and therefore are deemed not reliable.

The current tool also offers the possibility to collect native audit trails, but extensive tests uncovered that this process is too intrusive on the target machines. The sum of these issues motivated X-Y-Z to choose Tivoli Security Information and Event Manager. But X-Y-Z must be able to report on the syslog messages that are already archived by the other tool. In this section, we show the steps you take to include existing syslog files.

The first step to take is to create a new event source on a *Log Manager* or an *Enterprise Server* that can receive up to 30,000 syslog messages per second using an AIX agent. We expect that many syslog message types cannot be normalized using the Tivoli Security Information and Event Manager mapper. Therefore we will rely on the forensic search capability that is available on the Log Manager and Enterprise Server, which provides basic normalization of the various syslog messages that can then be searched.

Perform the following steps on a Log Manager or Enterprise Server.

9.6.1 Creating a Ubiquitous syslog receiver on AIX

To create a Ubiquitous syslog receiver on AIX:

1. Select the AIX machine that will receive the syslog messages. Choose the event source **Ubiquitous syslog receiver**, as shown in Figure 9-45 on page 268.

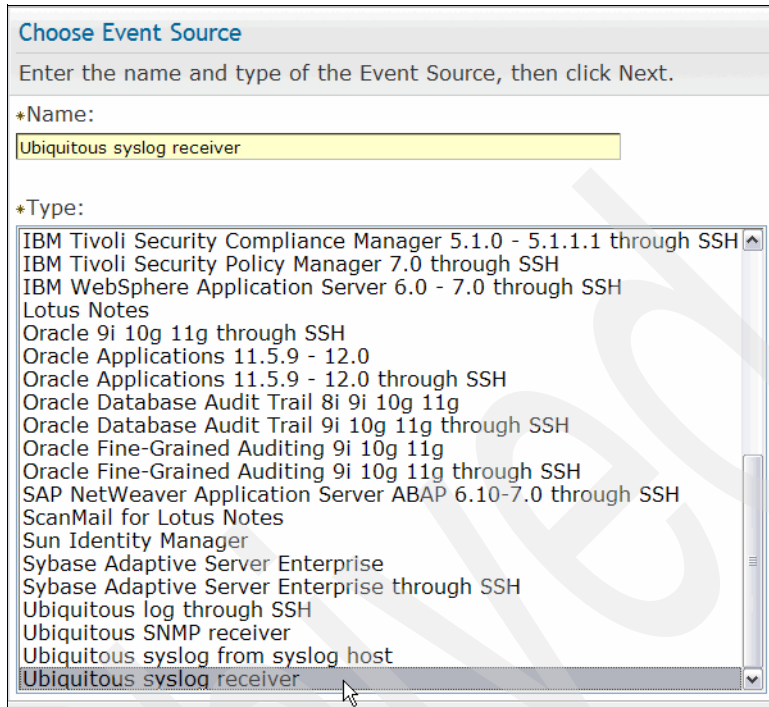


Figure 9-45 Select the Ubiquitous syslog receiver event source

This event source can receive any type of syslog message at a maximum rate of 30,000 messages per second.

2. You must define from which machines the new event source will receive the messages. You can specify a single IP-address or a range of IP-addresses using wild cards. In the example shown in Figure 9-46, the event source receives messages from any event source.

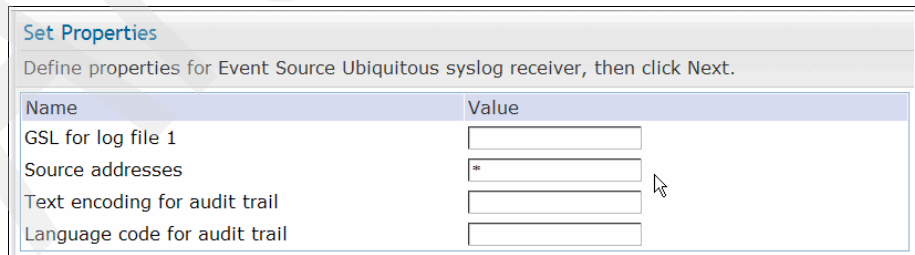


Figure 9-46 Ubiquitous event source properties

The objective is to include previously collected syslog messages in Tivoli Security Information and Event Manager. We assume that the syslog messages are stored in text files, which we will now archive using this newly created Tivoli Security Information and Event Manager event source.

The example shows how to archive a single file, and this process must be repeated for all files and preferably for each platform from which the messages were received. These steps are necessary because XYZ wants to be able to search the syslog messages by event source. If this is not required, you can concatenate all individual files into one and collect that file. Preferably this file should not be bigger than 500 MB to prevent unnecessary load in the network.

3. Because the logfile(s) are only collected, a collect schedule is needed that runs after, as shown in Figure 9-47.

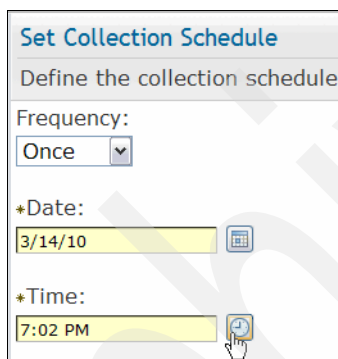
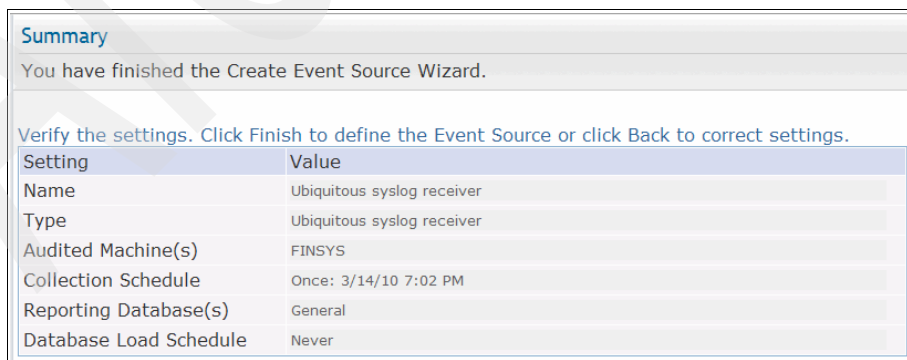


Figure 9-47 Set a collect schedule

After the event source is defined, the configuration should be similar to the example in Figure 9-48.



Setting	Value
Name	Ubiquitous syslog receiver
Type	Ubiquitous syslog receiver
Audited Machine(s)	FINSYS
Collection Schedule	Once: 3/14/10 7:02 PM
Reporting Database(s)	General
Database Load Schedule	Never

Figure 9-48 Event source summary

9.6.2 Preparing the syslog file to be collected

To prepare the syslog file to be collected:

1. After the event source is created, a logfile is found in the log subdirectory of the agent on which the event source was defined. The file is named `splitter.log` and from its contents we can see the name of the logfile that the event source will eventually collect. In the example in Figure 9-49, you can see that the logfile is called `rtlog15.1.113`. The event source expects this log file in the agent's run directory.

```
:Subscribing in inactive single mode 0
}:adapter 15.1.113 subscribed for Syslog messages from *
}:rotated log file for 15.1.113 to rtlog15.1.113.collect
```

Figure 9-49 Determine the name of logfile from the `splitter.log`

2. To execute the collect and archive process, we must copy the syslog file into the run directory of the agent and rename it to the filename shown in the `splitter.log`. Figure 9-50 shows the renamed file in its location.

```
03/19/2009 11:56 AM 164,936 rtlog15.1.113.log
1 File(s) 164,936 bytes
```

Figure 9-50 Rename the syslog file

9.6.3 Using the Log Management Depot Investigation tool

The result of these steps is that the archived syslog files can now be searched using the forensic search tool, as shown in Figure 9-51 on page 271.

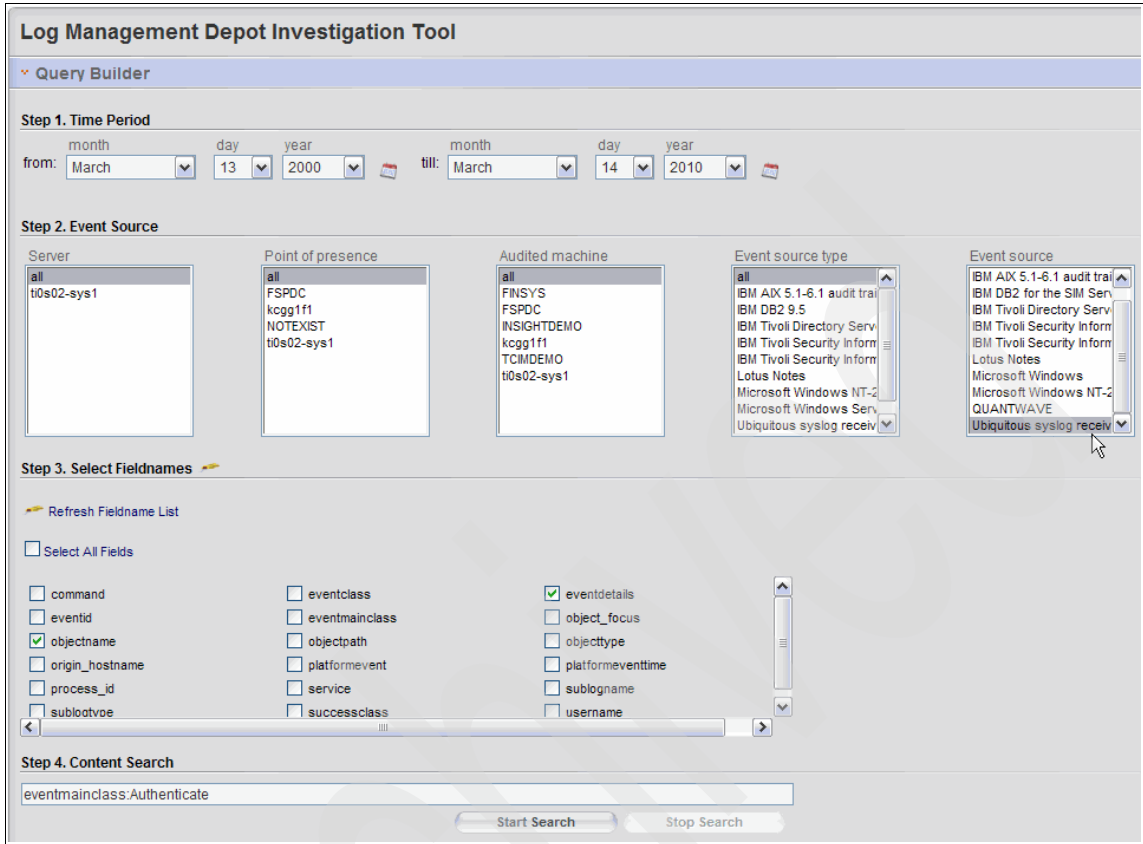


Figure 9-51 First step of forensic search

Figure 9-52 on page 272 shows the result set.

Search Information					
Status:	100%	Logfiles:	1		
Creation Time:	00:00 minutes	Events:	4		
Search Summary					
Audited machine	Event source	Event source type	Total records	Relevance	Difficulty
ti0s02-sys1	Ubiquitous syslog receiver	Ubiquitous syslog receiver	110000	36%	■■

Search Results					
<input type="checkbox"/>	Audited machine	Event Source	Timestamp	objectname	eventdetails
<input type="checkbox"/>	ti0s02-sys1	Ubiquitous syslog receiver	Tue Mar 09 15:30:20 2010	Logon	authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=
<input type="checkbox"/>	ti0s02-sys1	Ubiquitous syslog receiver	Wed Mar 10 15:29:39 2010	Logon	authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=
<input type="checkbox"/>	ti0s02-sys1	Ubiquitous syslog receiver	Thu Mar 11 15:29:39 2010	Logon	authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=
<input type="checkbox"/>	ti0s02-sys1	Ubiquitous syslog receiver	Fri Mar 12 15:29:59 2010	Logon	authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=

Figure 9-52 Result set of a search through a ubiquitous event source's log

Besides using the investigation tool, Tivoli Security Information and Event Manager ships with Tivoli Common Reporting (TCR) reports for log investigation, as shown in Figure 9-53.

Reports																	
Tivoli Common Reporting http://www.ibm.com/developerworks/spaces/tcr																	
Navigation Search <ul style="list-style-type: none"> Report Sets <ul style="list-style-type: none"> Tivoli Products <ul style="list-style-type: none"> Tivoli Common Reporting Tivoli Security Information and Event Management 	Reports <table border="1"> <thead> <tr> <th>Title</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Log Management Collect History Report</td> <td>collection events for a reporting period in the past</td> </tr> <tr> <td>Summary Database Activity</td> <td>Summary of events for Database Event Source Types.</td> </tr> <tr> <td>Summary Event Source Activity</td> <td>Summary of events by Event Source Type on each Audited Machine.</td> </tr> <tr> <td>Summary Events by Type</td> <td>Summary of event types.</td> </tr> <tr> <td>Summary Host Activity</td> <td>Summary of events by event type on each audited machine.</td> </tr> <tr> <td>Summary Logon Failures by Host</td> <td>Summary of Logon failure events for each audited machine.</td> </tr> <tr> <td>Summary Logon Failures by User</td> <td>Summary of Logon failure events by User.</td> </tr> </tbody> </table>	Title	Description	Log Management Collect History Report	collection events for a reporting period in the past	Summary Database Activity	Summary of events for Database Event Source Types.	Summary Event Source Activity	Summary of events by Event Source Type on each Audited Machine.	Summary Events by Type	Summary of event types.	Summary Host Activity	Summary of events by event type on each audited machine.	Summary Logon Failures by Host	Summary of Logon failure events for each audited machine.	Summary Logon Failures by User	Summary of Logon failure events by User.
Title	Description																
Log Management Collect History Report	collection events for a reporting period in the past																
Summary Database Activity	Summary of events for Database Event Source Types.																
Summary Event Source Activity	Summary of events by Event Source Type on each Audited Machine.																
Summary Events by Type	Summary of event types.																
Summary Host Activity	Summary of events by event type on each audited machine.																
Summary Logon Failures by Host	Summary of Logon failure events for each audited machine.																
Summary Logon Failures by User	Summary of Logon failure events by User.																

Figure 9-53 TCR reports for Log Manager depot investigation

The report demonstrated searches through the original log data and presents the information in a normalized format. The reports can be configured, as shown in Figure 9-54 on page 273.

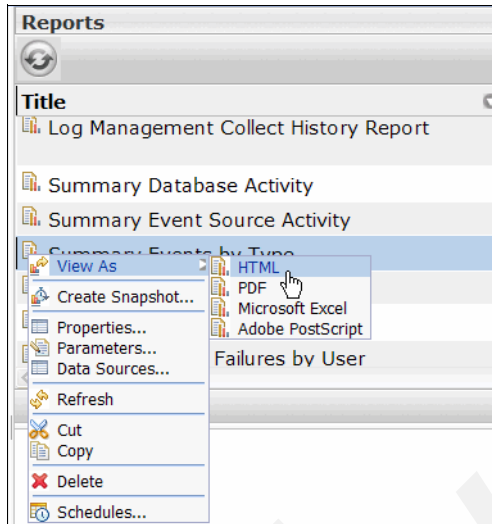


Figure 9-54 The report formats

The report can be prepared in many date formats and the report query can also be configured, as shown in Figure 9-55.

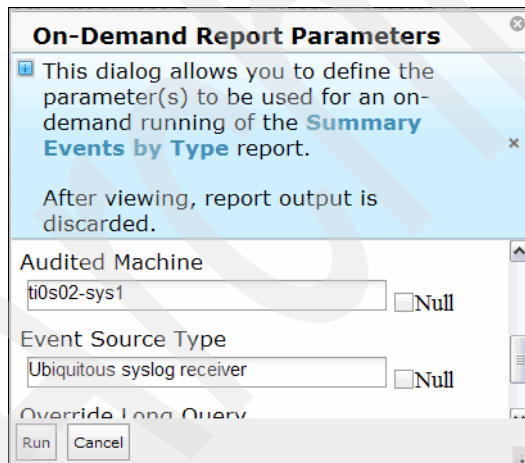


Figure 9-55 TCR report parameters

Figure 9-56 on page 274 shows the result set of this report's run.

Events by Type Summary Report

Summary Period

Report Period	Last 24 hours	End Date	Mar 15, 2010
Start Date	Mar 14, 2010	Event Source Type	Ubiquitous syslog receiver
Audited Machine	ti0s02-sys1		

Events by Type Summary Table

Event Type	Event Count
Logon	135
Logoff	135
Total	270

This report shows the summary of event types for events retrieved by Log Manager over a period of time.

March 15, 2010 9:23:47 AM EDT

1 / 1

Figure 9-56 Result set of TCR report

Because we decided to generate the report as an HTML page, the report contains hyperlinks for drill down, as shown in Figure 9-57 on page 275.

Events by Type Activity Detail Report

Report Input Parameters

Start Date	Mar 14, 2010	End Date	Mar 15, 2010
Event Type	Logon		
Event Source Type		Audited Machine	
Event Range Begin	0	Maximum Number of Events To Show	10000

Events for Event Type "Logon"

Showing event 1 to 135 of 135

Date and Time	Event Type	Result	Audited Machine	Event Source Type	User	Object
3/14/10 5:30:08 AM	Logon	Success	ti0s02-sys1	Ubiquitous syslog receiver	root	dmgprd2:sshd
3/14/10 5:37:33 AM	Logon	Success	ti0s02-sys1	Ubiquitous syslog receiver	root	dmgprd2:sshd
3/14/10 5:37:33 AM	Logon	Success	ti0s02-sys1	Ubiquitous syslog receiver	root	dmgprd2:sshd
3/14/10 5:37:33 AM	Logon	Success	ti0s02-sys1	Ubiquitous syslog receiver	root	dmgprd2:sshd

Figure 9-57 Drill down of a TCR report

9.6.4 Result

Tivoli Security Information and Event Manager can import and archive the syslog messages that were archived by a previous tool. After the messages are archived, they can also be analyzed using the Log Management Depot Investigation Tool or Tivoli Common Reporting, which demonstrates the flexibility of Tivoli Security Information and Event Manager to integrate with or replace existing log management processes.

9.7 Conclusion

In this chapter, we discussed how to add new event sources to a Tivoli Security Information and Event Manager implementation. After you configure the event sources, you can create audit policies to report on the captured data. We also showed how to create policy rules and how to apply these rules with basic modifications to the underlying policy groupings across all aspects of the infrastructure.

In the next chapter, we extend these themes by showing how to create custom reports using the Tivoli Security Information and Event Manager custom report tool.

Archived



Customized and regulatory reporting

In this chapter, we discuss how X-Y-Z can use the Tivoli Security Information and Event Manager for reporting on compliance towards business regulations that apply to the organization (for example Basel II).

10.1 Producing customized reports

In Chapter 8, “Basic auditing” on page 151 and Chapter 9, “Extending auditing to other supported platforms” on page 229, we discussed how to implement standard reporting with the Tivoli Security Information and Event Manager, choosing from its variety of predefined reports. Organizations can use these reports to perform investigations, root cause analysis, and quick reporting to the IT department. However, in certain cases, a more advanced presentation of the data might be required. To answer specific requests from various stakeholders, which are not covered by the standard reports, Tivoli Security Information and Event Manager provides a custom reporting functionality that allows companies to present the event information that is collected with the software product filtered by custom criteria. Also, custom reporting allows an organization to add a graphical representation of the data in common chart formats.

The X-Y-Z security policy framework requires the performance of a *systematic attack detection*, which is defined in the X-Y-Z security policies as the monitoring of logon failures, if they happen more than five times in a minute, because this might indicate not a simple user error but a malicious activity against a user account using a brute force attack.

The CIO office thus asks that a custom report is created for systematic attack detection and sent by e-mail on a daily basis. This custom report can be performed automatically by Tivoli Security Information and Event Manager.

10.1.1 Creating a customized report

Tivoli Security Information and Event Manager comes with standard reporting on logon failures. However, this standard report does not consider organization-specific thresholds, nor does it provide a graphical representation of the events, which can help to directly catch the account that might be under attack.

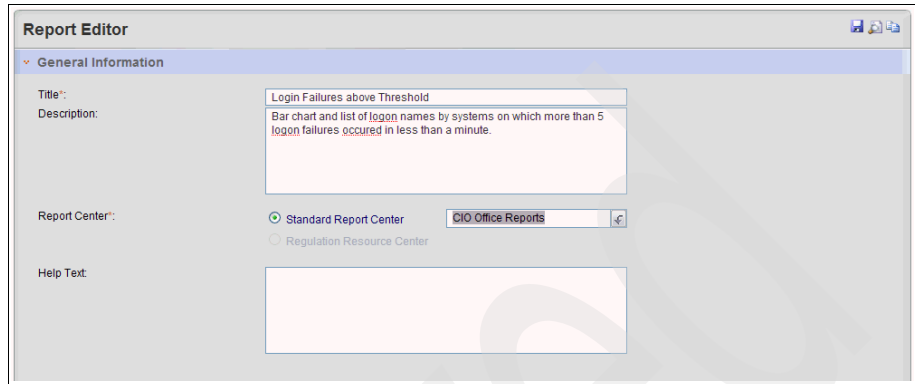
To create a custom report:

1. Open the Tivoli Integrated Portal, and navigate to **Security Information Management** → **Reporting**. Depending on your general databases, a similar window to the one in Figure 10-1 is displayed. Click **Add custom reports**.



Figure 10-1 Adding a custom report

2. The Report Editor page is opened, which consists of multiple sections. First complete the fields in the General Information section, as shown in Figure 10-2.



The screenshot shows the 'Report Editor' window with the 'General Information' section expanded. The 'Title' field contains 'Login Failures above Threshold'. The 'Description' field contains 'Bar chart and list of *login* names by systems on which more than 5 *login* failures occurred in less than a minute.' The 'Report Center' section has two radio buttons: 'Standard Report Center' (selected) and 'Regulation Resource Center'. A dropdown menu next to 'Standard Report Center' is open, showing 'CIO Office Reports'. The 'Help Text' field is empty.

Figure 10-2 Filling in the General Information section

The information in this section provides:

- A unique name to the report
 - A description with a maximum length of 150 characters
 - The Report Center, which defines either the tap under which the report shows in the list of all reports in the standard report center or the Compliance Management Module to which the report is allocated
3. Complete the Report Layout section of the report editor shown in Figure 10-3 on page 280. In the Report Type section, select **Threshold Report**, and configure it to use a threshold of five events in one minute. This threshold means that the report only shows events that occur together with at least another four events of the same kind in the chosen time window of one minute.

For the understanding of report results, it is important to realize that this report type basically summarizes every five *log events* and replaces them with one respective *threshold event* in the report.

Report Layout

Report Type

Select the types of report you would like to create. Mouse over the name to see an example.

Event List
 Summary Report
 Top-N Report
 Threshold Report

a report summarized and only showing results if something happened more than N times in a defined time period.

Number
 Event Type ▼
 Period minutes.

Column selection

Select the columns you want to see in the report from the list on the left. (Use the field boxes to add the aspects of that W7). The selected columns will appear in the box on the right. Here you can sort them by dragging them into the correct order.

When items

Who items

Who group

Who detail

Who: Logon name

Who: Real name

Aspect:

What items

On What items

Where items

Where group

Where detail

Where: Platform name

Where: Platform type

Aspect:

Where From items

Where To items

Selected Columns

Where: Platform name

Who: Logon name

Aggregator: Number of Events

Figure 10-3 Filling report type and column selection of the report layout

4. After you define the report type, select the columns that you want to see in the report by clicking the W7 items on the left side of the mask. The columns to be displayed in the report are the platform name, where the event occurred, and the logon name that was used in the event. By default, the number of events is selected and already shown on the right side of the mask. This item cannot be deleted because we specified in the report type that we want a threshold report on events.

As the last item for the layout of the report, we want to include a bar chart, which means that we want to have a bar showing the number of threshold events, added by platform and by logon name used. Figure 10-4 shows the necessary selections.

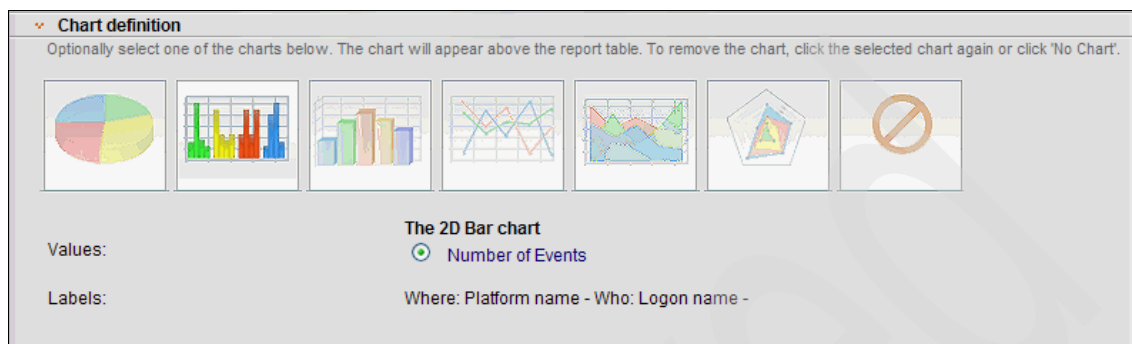


Figure 10-4 Filling the chart definition of the report layout section

5. Finally, before the report definition is complete, you must select the events that are to be reported on in the threshold report. Define the data criteria of the report, as shown in Figure 10-5.

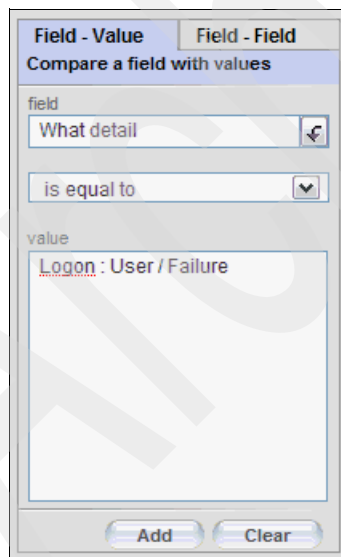


Figure 10-5 Filling the data criteria section

Because we selected a threshold report type and defined events as the threshold source, we cannot change the event selection of the data criteria

section, so it is predefined and greyed out. We must add a condition so that only logon failures are taken into account for the report. Logon failure is an activity that is described as a *what* in W7 terminology, and the corresponding detail description of a logon failure in the model is *Logon: User / Failure*.

- After entering the conditions on the left side of the mask, click **Add**. The rule displays on the right side of the mark. The mask now looks as shown in Figure 10-6.

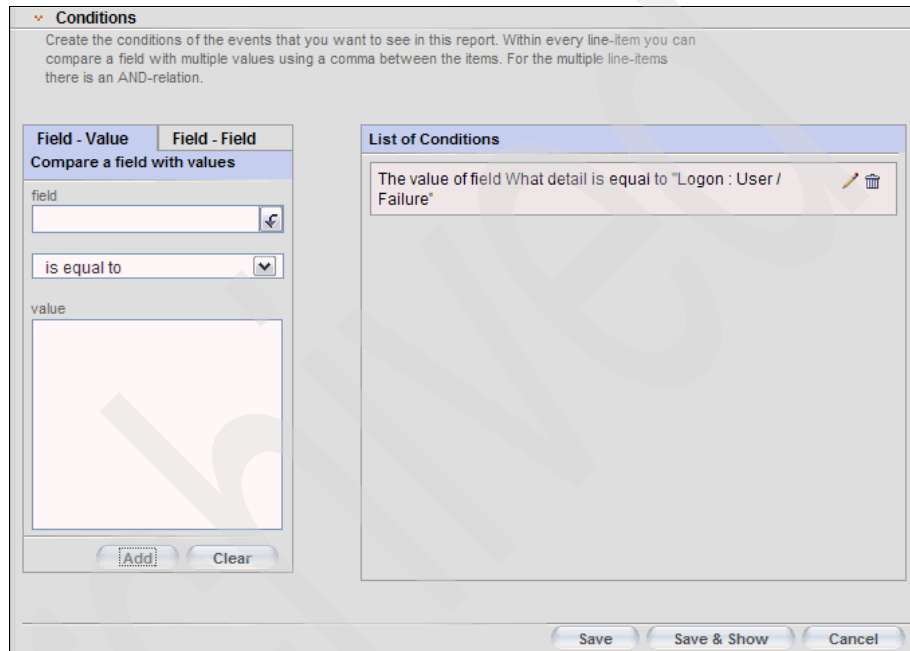


Figure 10-6 Completed criteria section

- After we finish the Report Editor, on the bottom of the mask click **Save**, and you can see the custom report at the end of the report list in the new section *CIO Office Reports* together with the short description that you gave it in the Report Editor, as shown in Figure 10-7.



Figure 10-7 New defined custom report and description at end of report list

The report list is sorted alphabetically by report groups, in which the reports are shown in alphabetical order; therefore, a custom report might not show at the end of the list but in the middle of it depending on the report group that you used.

The report list, including the new report, must be reloaded from the server. To see the new report on another system displaying the report list, on your browser, click **Refresh**. So there is no need to panic, in case you cannot find a newly defined report directly.

8. Finally, click the report to test the report. We can see that the result matches the requirements and that the content of the report indicates a possible brute force attack against six user identifiers, as shown in Figure 10-8.



Figure 10-8 Result of the custom report on Logon Failures

The report shows that six logon failures must have occurred against the user identifier *TSIEMSTD01\$* on workstation *TSIEMSTD01*. Remember, that the report shows the number of threshold violations, not the actual number of events. Also, on the same workstation, threshold violations were caused in conjunction with the other user identifiers. By selecting the violations in the list, you can review the events and their details—just like with the standard reporting.

As we can see, the custom report is working as expected and as required. Now, we must set up the distribution for the report so that the CIO office receives it in their mailbox every day. We show you how to configure distribution for the report in the next section.

10.1.2 Distributing reports

The CIO office wants to have an update on the custom report *Logon Failures above Threshold* on a daily basis to be in control and to be able to trigger investigations, such as checking whether the user to whom a user identified belongs is still employed or whether the user might have called the helpdesk reporting an issue to log on.

A Tivoli Security Information and Event Manager administrator can schedule a report to run on a periodic basis and configure Tivoli Security Information and Event Manager to automatically send the results to specified e-mail addresses.

To set up a scheduled distribution of the custom report, we must first check, whether the intended recipient of the e-mail is a registered Tivoli Security Information and Event Manager user because only these users are allowed to receive reports. To set up a scheduled distribution of the custom report:

1. On the left pane, open **User Management**, and click **Users and Roles** to invoke the user management dialog, as shown in Figure 10-9.

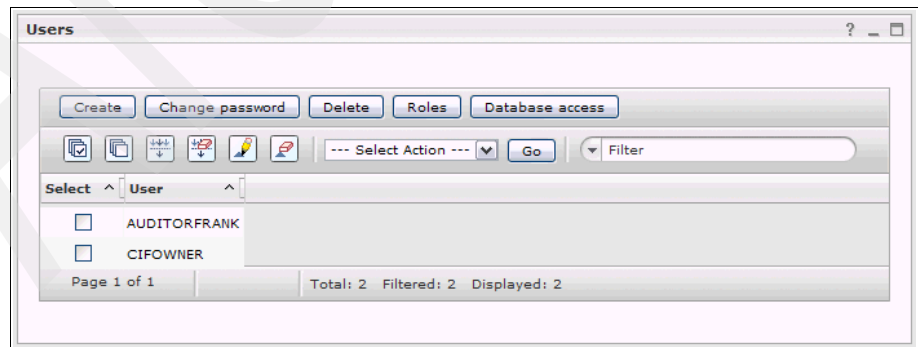
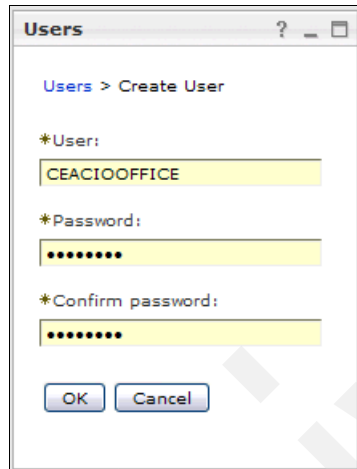


Figure 10-9 User Management Dialog in Management Console

2. Click **Create** to create the user *CEACIOFFICE* and provide rights to log on to the portal to create and edit custom reports and to use (view) custom reports. Thus, the CIO office can access the portal and investigate violations in reports that are received by e-mail. Figure 10-10 shows how to create the user.

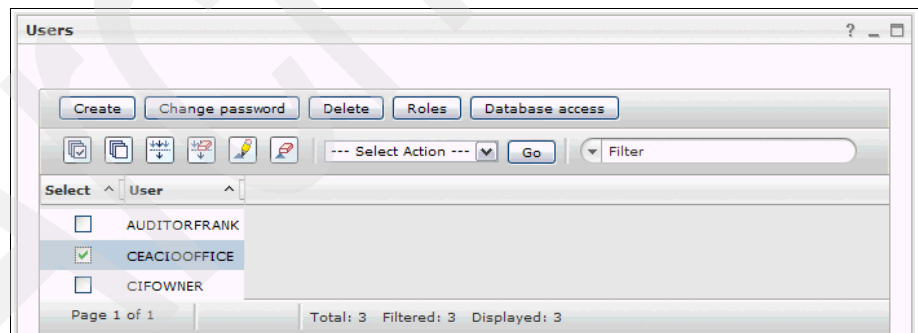


The screenshot shows a window titled "Users" with a breadcrumb "Users > Create User". It contains three labeled input fields: "*User:" containing "CEACIOFFICE", "*Password:" containing seven dots, and "*Confirm password:" containing seven dots. At the bottom are "OK" and "Cancel" buttons.

Figure 10-10 Creating a user

Click **OK**. The user is created with the credentials that you entered.

3. Assign roles to the user that you just created, as shown in Figure 10-11.



The screenshot shows a window titled "Users" with a toolbar containing "Create", "Change password", "Delete", "Roles", and "Database access". Below the toolbar is a table with columns "Select" and "User". The table lists three users: "AUDITORFRANK", "CEACIOFFICE" (with a checked checkbox), and "CIFOWNER". At the bottom, the status bar shows "Page 1 of 1", "Total: 3", "Filtered: 3", and "Displayed: 3".

Figure 10-11 Select the created user

4. To assign roles, click **Roles**. Figure 10-12 on page 286 shows the dialog that appears next. For our scenario, you assign the roles to create or edit custom reports and view custom reports.

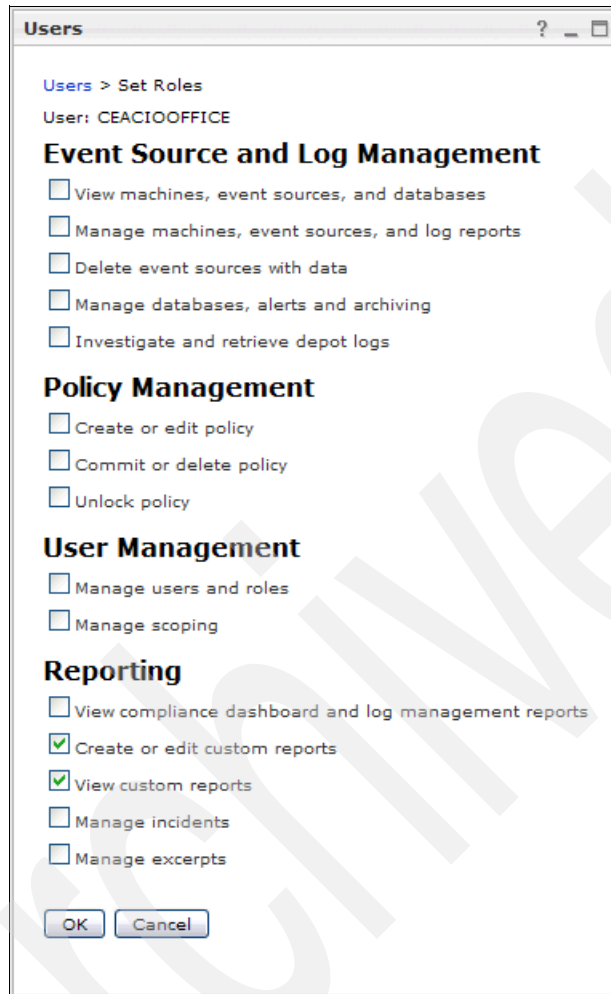


Figure 10-12 Assigning roles to users

5. When you click **OK**, the roles are assigned to the user. Return to the Compliance Dashboard, and click **Distribution** to configure the e-mail settings that the distribution engine uses to send out the reports.

Configuration details: Tivoli Security Information and Event Manager assumes that the mail server that is provided in the field *Mail-host* does not require authentication when the Tivoli Compliance Insight Manager server connects to the SMTP service, for example, an internal relay server, ideally set up for system management activities, such as report distribution, can be used.

It must be clear that the sensitivity of the distributed data is high so that the mail engine must only be used for *internal* mail distribution and not for mail distribution over the Internet.

- Complete the appropriate e-mail address of the CIO office next to the user *CEACIOOFFICE*, as shown in Figure 10-13.

Automated Report Distribution

[Add distribution task](#)

▼ Distribution Task

Title	Run time	Recurrence	Start date	Action
-------	----------	------------	------------	--------

▼ Email Settings

▼ Sender

These settings will be used by every Automated Report Distribution task.

From email name:

From email address:*

Reply-to email address:

Mail-host:*

* Required field

▼ Notification

Every Automated Report Distribution task will send a notification email to this address. A notification email contains details of every report sent by Automated Report Distribution, including successes, failures, or empty reports. If left empty, a notification will not be sent.

Notification email address:

▼ Manage Users

User Name	E-mail Address
<input type="checkbox"/> AUDITORFRANK	<input type="text"/>
<input type="checkbox"/> CEACIOOFFICE	<input type="text" value="ceaciooffice@yourcompany.com"/>
<input type="checkbox"/> CIFOWNER	<input type="text"/>

[Save](#) [Cancel](#)

Figure 10-13 Automated Report Distribution setup

7. You can configure the distribution of the logon failures threshold report by clicking **Add distribution task**, which invokes the Edit Automated Distribution Task dialog box shown in Figure 10-14.

Edit Automated Report Distribution Task

▼ **General Information**

▼ **Email**

Title:* Logon Failures above Threshold

Body:* Daily reporting to CIQ Office about logon failures above threshold.

* Required field

Report Format: PDF CSV

Also send reports when they contain no data:

▼ **Schedule**

Start date: month day year
March 12 2010

Run time: hour minutes
11 : 15

Recurrence: Inactive Daily Weekly Monthly

Daily recurrence pattern
 Every 1 day(s) Every weekday

▼ **Reports**

▼ **Addresses**

Save Cancel

Figure 10-14 General information section of the automated report distribution editor

To establish a daily automated report distribution for the X-Y-Z Logon Failure Threshold Report, in the general information section shown in Figure 10-14, specify the:

- Email title
- Body of the e-mail
- Format of the report—either PDF or CSV
- Schedule
- Recurrence
- Run time (determines when the event query to the database is performed)

The report is sent directly thereafter.

Important: Because querying the event database can be time consuming depending on the amount of data and in case you want to have the report every day (for example, always including the events of the last 24 hours), the schedule for the loading of the event databases and schedule for the report distribution must be matched properly, for example, the database loading for a given database must complete before the report is run.

8. In the report section of the editor, from the pull-down list, select the **Tivoli Financial Accounting Services Logon Failures Above Threshold** report, as shown in Figure 10-15.

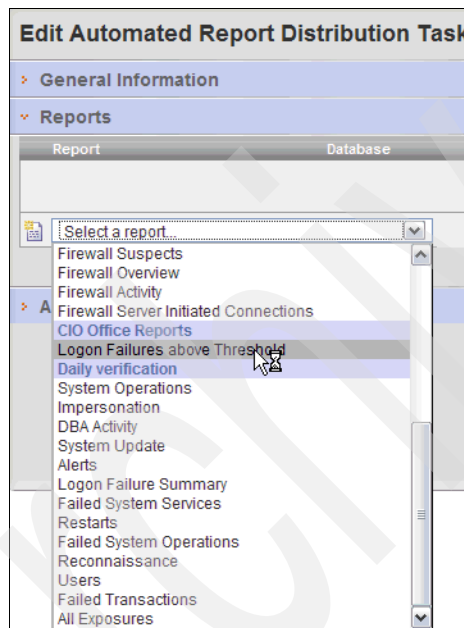


Figure 10-15 Report section of report distribution editor

9. Add the user *CEACIOOFFICE* to the list of recipients in the addressees section of the editor, as shown in Figure 10-16 on page 290.

Edit Automated Report Distribution Task

- General Information
- Reports
- Addresses

User Name	E-mail Address
-- There are no users selected for this Distribution Task. --	

Select a username...

Select a username...

AUDITORFRANK (email: auditorfrank@yourcompany.com)

CEACIOFFICE (email: ceacioffice@yourcompany.com)

CIFOWNER (email: cifowner@yourcompany.com)

Figure 10-16 Addressees section of report distribution editor

10. Close the editor by selecting **Save**, and return to the Automated Report Distribution main page, which now shows that the distribution task is defined, as shown in Figure 10-17.

Automated Report Distribution

- Distribution Task

Title	Run time	Recurrence	Start date	Action
Logon Failures above Threshold	11:15:00 AM GMT-05:00	Every 1 day(s)	Mar 12, 2010	
- Email Settings
 - Sender

These settings will be used by every Automated Report Distribution task.

From email name:

From email address:*

Reply-to email address:

Mail-host:*

* Required field
 - Notification

Every Automated Report Distribution task will send a notification email to this address. A notification email contains details of every report sent by Automated Report Distribution, including successes, failures, or empty reports. If left empty, a notification will not be sent.

Notification email address:
- Manage Users

User Name	E-mail Address
AUDITORFRANK	<input type="text" value="auditorfrank@yourcompany.com"/>
CEACIOFFICE	<input type="text" value="ceacioffice@yourcompany.com"/>
CIFOWNER	<input type="text" value="cifowner@yourcompany.com"/>

Figure 10-17 Automated Report Distribution main page with defined task

Now the X-Y-Z CIO Office will receive one e-mail every day with a report in PDF format that shows the logon failures that exceed the defined threshold.

10.2 Using compliance management modules

Tools, such as Tivoli Security Information and Event Manager, cannot automate the interpretation of regulatory compliance into functional terms. It is wrong to assume that an organization can automatically become compliant by deploying and configuring an IT security compliance management tool.

There are *compliance management modules* for Tivoli Security Information and Event Manager that each provide a set of predefined reports. These reports are aligned to the structure or sections of several given regulatory standards. By this, the reports indicate a mapping between the security events, which are logged in the IT infrastructure and consolidated by Tivoli Security Information and Event Manager and the requirement of the given standard.

Tivoli Security Information and Event Manager compliance management modules are currently available for the following regulatory and security standards:

- ▶ Basel II
- ▶ COBIT
- ▶ FISMA
- ▶ GLBA
- ▶ HIPAA
- ▶ ISO27001
- ▶ NERC CIP
- ▶ PCI DSS
- ▶ Sarbanes-Oxley

Organizations can use these compliance management modules for Tivoli Security Information and Event Manager as one cornerstone to demonstrate control over the mapped requirements of a given regulatory standard to the extent that these requirements address the technical security infrastructure and can be monitored with the respective logging mechanisms.

10.2.1 Tool-based regulatory compliance reporting

Before diving into the compliance reporting features of Tivoli Security Information and Event Manager, it is important to confirm the correct understanding about what tools can and cannot provide towards regulatory compliance.

For regulations to become binding to organizations, they must be put into *laws*, which predominate in a sovereign territory in which the organizations are based. Because the intent is to preserve the uniformity of laws to a high extent and prevent the changes of the laws, for example, with every advance in technology, regulatory clauses in laws formulate rather broad requirements.

Regulatory authorities usually provide further guidance about how to meet these requirements in more functional terms, which, again, are still somewhat distant from technical terms. The actual interpretation into functional and even technical terms retains with the organization. Therefore, two companies that fall under the same regulatory requirements can have very distinctive ways to meet these requirements and also to report on them, yet still both be able to meet the requirements.

Further, it is important to choose the right moment to *go public* with reporting that is performed by automated tools. When you have such tools running, they become part of your official knowledge and—in case they are not properly configured, so that they might show incompliant despite the fact that you might be compliant—can push you into a lot of arguing with your auditors. Such tools, including Tivoli Security Information and Event Manager, are powerful, so you must use them with care.

Finally, tools, such as Tivoli Security Information and Event Manager, address detective security controls primarily. They do not provide—for systems other than itself—preventive security controls. If a given regulatory standard does require preventive security controls and you do not have them deployed, Tivoli Security Information and Event Manager might help you to detect and monitor these security controls. Thus, you are at least in control of the non-compliance, which the product cannot fix. To conclude this topic, regulatory standards might require security controls, which fall outside of the technical remit and must be taken care of on the business level.

10.2.2 Running compliance reports

Tivoli Security Information and Event Manager provides a set of predefined reports. These reports are grouped to follow the chapters, sections, or other structure of a given standard.

As one example of the usefulness of the compliance reports for X-Y-Z, we discuss the requirement that X-Y-Z wants to comply to ISO27001.

X-Y-Z processes their financial transactions with the help of information technology; therefore, they must be able to prove that a transaction was not manipulated on the IT infrastructure level. This process makes a log collection and storage of systems which processes financial transactions essentially.

The Tivoli Security Information and Event Manager ISO27001 Compliance Management Module provides a predefined report that addresses the ISO27001 requirement.

You can access this module in the left pane by clicking **Compliance Management Modules**.

When selecting the report Log Collection, the report shows the event source, the planned schedule for the log collection, the last collection date, and the events collected in the last collection. Figure 10-18 shows the result for the X-Y-Z infrastructure.

Compliance Management Modules

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

CIFDB > SELFAUDIT > ISO 27001 > Log collection

Log collection

Time zone:

Event source	Schedule	Last collect	#Collect
tsiemstd01 Microsoft Windows	Frequent: 15 minutes	3/12/10 4:00:00 PM (-0500)	193
tsiemstd01 IBM Tivoli Security Information and Event Manager Server	Frequent: 15 minutes	3/12/10 4:00:00 PM (-0500)	193
tsiemstd01 IBM Tivoli Security Information and Event Manager Web Apps	Frequent: 15 minutes	3/12/10 4:00:00 PM (-0500)	192
tsiemstd01 IBM DB2 for the SIM Server	Frequent: 15 minutes	3/12/10 4:00:00 PM (-0500)	193
tsiemstd01 IBM Tivoli Directory Server	Frequent: 15 minutes	3/12/10 4:00:00 PM (-0500)	193

Page 1 | << < > >> | Jump to page [Paragraph 10.10.1](#)

▼ Help

The Log Collection report shows you - by platform - when logs were collected. This report is used to ensure coverage of all assets.

▼ Background

Figure 10-18 ISO27001 report on log collection

Similar to this, clicking the Log storage report provides an overview of the log storage files that are created together with the storage data and the event source, of which the log data is taken from the log database into storage. Figure 10-19 on page 294 shows the example report for the X-Y-Z infrastructure.

System z integration

In Chapter 6, “Introducing X-Y-Z Financial Accounting” on page 121, we described X-Y-Z’s profile and high-level requirements. To summarize, we must institute controls over data access and use within the corporate perimeter on many distinct platforms. We discussed the distributed environment in Chapter 8, “Basic auditing” on page 151, Chapter 9, “Extending auditing to other supported platforms” on page 229, and Chapter 10, “Customized and regulatory reporting” on page 277. The next step for X-Y-Z to implement a compliance management solution and to fulfill the business requirements is System z integration.

Keeping compliance in mind, the business requirements that we identified in Chapter 7, “Compliance management design” on page 131 addressed the implementation processes to help achieve regulatory compliance and to reduce operational risk. In particular, we identified monitoring and reporting on high-privilege user accounts and activities, access to sensitive organization assets, including financial and business data, and confidential customer data that is stored on their servers, as highest priority processes to implement.

By mapping identified business requirements to the underlying reasons and expanding the reasons in increasing detail, we extracted functional requirements for multi-platform support, from data collection from the critical systems to Basel II reporting, including System z. One of the outstanding capabilities of Tivoli Security Information and Event Manager is to collect data from distributed systems, such as UNIX, Linux, and Windows, together with midrange event data and System z.

In our scenario, certain business critical applications run on System z, such as the corporate banking transaction system, the branch bank teller, and customer online home banking applications. These applications exploit CICS to process sensitive financial, business, and customer data that is stored on the DB2 back end system. We do not go into details here, but X-Y-Z's network deployment from Chapter 6, "Introducing X-Y-Z Financial Accounting" on page 121 is shown again for reference in Figure 11-1 with System z highlighted in bold in the production zone.

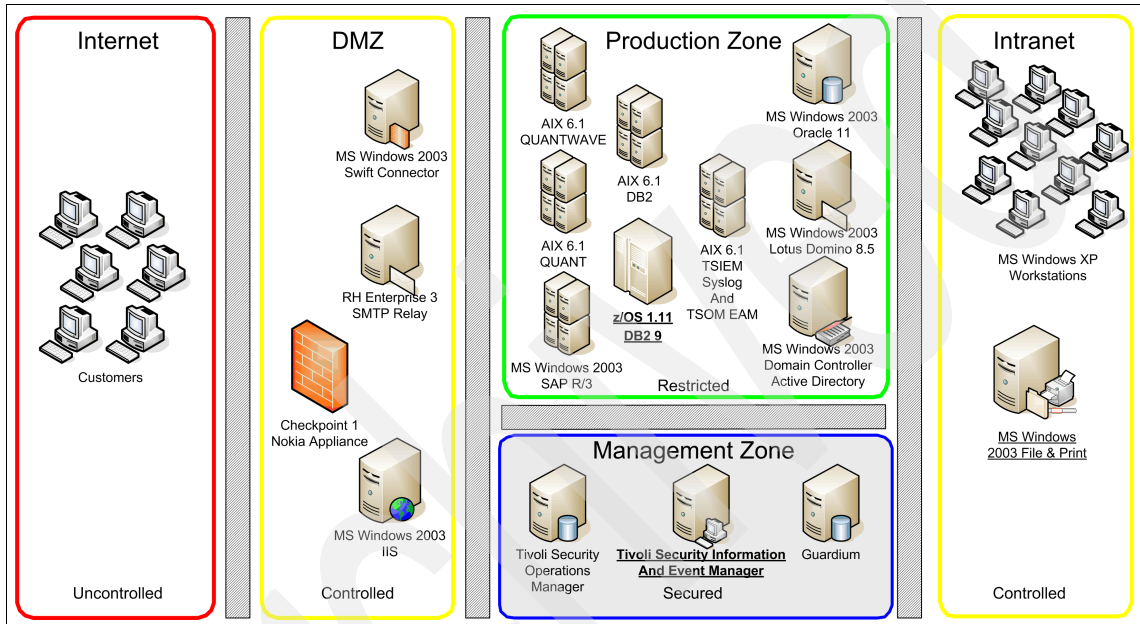


Figure 11-1 X-Y-Z System z deployment

In the following sections, we show the System z integration based on our general design discussion in Chapter 5, "Compliance management solution design" on page 89 and the scenario-specific design discussion in Chapter 7, "Compliance management design" on page 131. We also apply the same approach for log collection and management, policies, reporting, and regulatory requirements as the approach shown in the distributed environment. We start with reporting requirements as a first step in the analysis phase.

11.1 Reporting requirements

The most critical piece of information that we need for any successful implementation are *reporting requirements*. They tell us what data we must capture and how we need to report that data.

Measuring IT security as part of operational risk is easiest when you use a common standard. Tivoli Security Information and Event Manager's Basel II Compliance Management Module uses the embedded ISO17799 security standard and offers dozens of reports on compliance to IT security.

To show that the controls are in place, active, and working, we defined the example set of Basel II reports shown in Table 11-1 (the numbers in the brackets refer to sections in ISO 17799).

Table 11-1 System z Basel II reporting requirements example

Basel II report	Description
Security alert (6.3, 8.1.3)	Alerts sent in response to policy exceptions or special attention exceptions.
Operational change control (8.1.2)	Changes to the operating environment, such as system updates, DBA activity, and so on.
Operator log (8.4.2)	Actions performed by the IT administration staff.
Review of user access rights (9.2.4, 9.7)	Actions performed by administrators on users.
System access and use (9.2.4.c, 9.7)	Successes and failures against key assets.
User responsibilities and password use (9.3)	Logon failures and successes either locally or remotely.
User identification and authentication (9.5.3)	Logon and logoff successes and failures.
Application access control (9.6)	Actions, Exceptions, and events on HR Data, Sensitive Data, User Sensitive Data, System, Financial Data, Proprietary Data, and General Data.
Information access restrictions (9.6.1)	Who accessed sensitive or private data successfully or unsuccessfully.
Sensitive system isolation (9.6.2)	Exceptions and failures against sensitive systems data in asset groups User, HR Data, Source Code, and Financial Data.
Logging and reviewing events (9.7.2.3)	Exceptions and failures recorded by the Tivoli Security Information and Event Manager system.

Basel II report	Description
Control of operational software (10.4.1)	Exceptions and failures that are caused by updating or changing critical system components.
Data access (12.1.4)	Exceptions and failures against HR, Sensitive, and Proprietary data.

Here are additional comments about the Basel II reports from this table:

- ▶ **Operational change control (8.1.2):** The system update report shows changes to key system components. Using this report, with the incident tracking report, you can monitor, record, and track changes using an external incident tracking system.
- ▶ **Operator log (8.4.2):** Basel II requires that operational staff maintain logs of their activities. Using this report, you can verify the activities of the IT administration staff against this log, for example, actions include creating, modifying, deleting administrator accounts, resetting password, logon and logoff successes, and so on.
- ▶ **Review of user access rights (9.2.4, 9.7):** This report shows accesses by users to key resources and shows success and failures. Failures indicate that the user rights are not sufficient to access the resource. These failures must be reviewed to determine whether the user has a legitimate need to access this data. Similarly, successful accesses must be reviewed on a regular basis to determine if these users can still have the right to access this resource and if not have the access revoked or changed.
- ▶ **System access and use (9.2.4.c, 9.7):** This report shows accesses by users to key resources and shows success and failures. Failures indicate that the user rights are not sufficient to access the resource. These failures must be reviewed to determine where the user has a legitimate need to access this data. Similarly, successful accesses must be reviewed on a regular basis to determine if these users are still permitted access rights to this resource and if not have their access revoked or changed.
- ▶ **User responsibilities and password use (9.3):** This report shows failed attempts to logon to the systems and services in the network. Failed logons can be as simple as someone having forgotten a password to an attempted breach of security. This report is an excellent starting point for someone looking to determine an appropriate use of user information or identity theft.
- ▶ **User identification and authentication (9.5.3):** This report shows successful logon and logoff events based on event data that is collected from systems and services throughout the enterprise. Using this event data, you can see all user IDs that are currently in use, determine whether these user IDs and passwords are being used responsibly, and do a visual inspection to ensure

that the user IDs do not reveal the user's role or responsibility in the enterprise.

- ▶ Information access restrictions (9.6.1): Monitoring access to key information systems and access success and failures is key. This report shows who accessed which key systems.
- ▶ Sensitive system isolation (9.6.2): This report shows accesses by users to key resources and shows success and failures. Groups HR DATA, Sensitive Data, Source code, financial data, and proprietary data are monitored with this report. Failures indicate that the user rights are not sufficient to access the resource. These failures must be reviewed to determine if this user does have legitimate needs to access this data. Similarly, review successful accesses on a regular basis to determine if these users can still have rights to access this resource and if not have the access revoked changed.
- ▶ Logging and reviewing events (9.7.2.3): Basel II requires that logs be collected and that these logs not be tampered with. Using this report, you can see, through the Tivoli Security Information and Event Manager self-audit events, whether any actions were taken that can compromise this event data. This report requires a valid Tivoli Security Information and Event Manager policy that represents the X-Y-Z's security policy.
- ▶ Control of operational software (10.4.1): Control of change and update to system files and resources is essential to control risk. This report shows who accessed and changed which system resources. Modifications that are made to the audit subsystem must be reported because any modification affects the level of information in any of the other reports that we discussed.
- ▶ Data access (12.1.4): The data access report monitors access to key data resources. The report shows access to resources that are defined in the HR_DATA, SENSITIVE_DATA, PROPRIETARY_DATA, FINANCIAL_DATA and GENERAL_DATA, who accessed the data, and from where.

We show real data from our scenario for a few of these reports later in “Reports” on page 332.

Our next step is to specify the audit data to collect to support our reporting requirements. We provide audit settings that support X-Y-Z's Basel II System z required reports in the next section.

11.2 Audit settings

The goal of this task is to specify the audit data to collect to support X-Y-Z's Basel II System z reporting requirements. In most cases, auditing every action is not an option, thus we analyze the audit subsystem and determine, evaluate, and

provide audit settings that support reporting requirements for event sources on the System z platform.

For audit data, Tivoli Security Information and Event Manager uses the event data that is created through normal System Management Facilities (SMF) processing on System z.

SMF is a component that provides a standardized method for writing records of activity to a file (or a *data set* using System z terms). SMF provides full instrumentation of all baseline activities that are running on System z, including I/O, network activity, software usage, error conditions, processor utilization, and so on. It forms the basis for many monitoring and automation utilities. Each SMF record has a numbered type (for example *SMF 120* or *SMF 89*), and operators have great control over how much or how little SMF data to collect.

Based on the reporting requirements examples that we identified in previous sections, we determined that the System z audit settings example needed for our scenario, shown in Table 11-2.

Table 11-2 System z Basel II audit settings example

SOX report	Audit settings
Security alert (6.3, 8.1.3)	None
Operational change control (8.1.2)	SMF 9, SMF 11, SMF 52, SMF 53, SMF 54, SMF 55, SMF 56, SMF 58, SMF 80 events SETROPTS, CHAUDIT, SMF 90 subtypes 1, 3, 4, 6, 16, 18, 19, 20, 21, 22, 23, 24, 25, 27, 28, 29, 31
Operator log (8.4.2)	SMF 9, SMF 11, SMF 14, SMF 15, SMF 17, SMF 18, SMF 52, SMF 53, SMF 54, SMF 55, SMF 56, SMF 58, SMF 61, SMF 62, SMF 64, SMF 65, SMF 66, SMF 80 events SETROPTS, CHAUDIT, ALTDSD, PERMIT, RALTER, RDEFINE, RDELETE, ADDVOL, RENAME, DELETE, DELVOL, DEFINE, DELDSD, ADDSD, ACCESSSMF, SMF 90 subtypes 1, 3, 4, 5, 6, 13, 14, 16, 18, 19, 20, 21, 22, 23, 24, 25, 27, 28, 29, 31, SMF 92 subtypes 10, 11, SMF 118
Review of user access rights (9.2.4, 9.7)	SMF 9, SMF 11, SMF 52, SMF 53, SMF 54, SMF 55, SMF 56, SMF 58, SMF 80 events SETROPTS, CHAUDIT, SMF 90 subtypes 1, 3, 4, 6, 16, 18, 19, 20, 21, 22, 23, 24, 25, 27, 28, 29, 31

SOX report	Audit settings
System access and use (9.2.4.c, 9.7)	SMF 9, SMF 11, SMF 14, SMF 15, SMF 17, SMF 18, SMF 52, SMF 53, SMF 54, SMF 55, SMF 56, SMF 58, SMF 61, SMF 62, SMF 64, SMF 65, SMF 66, SMF 80 events SETROPTS, CHAUDIT, ALTDSD, PERMIT, RALTER, RDEFINE, RDELETE, ADDVOL, RENAME, DELETE, DELVOL, DEFINE, DELDSD, ADDSD, ACCESSSMF, SMF 90 subtypes 1, 3, 4, 5, 6, 13, 14, 16, 18, 19, 20, 21, 22, 23, 24, 25, 27, 28, 29, 31, SMF 92 subtypes 10, 11, SMF 118
User responsibilities and password use (9.3)	SMF 30 subtypes 1, 5, SMF 118 subtype 72, SMF 80 event RACINIT
User identification and authentication (9.5.3)	SMF 30 subtypes 1, 5, SMF 118 subtype 72, SMF 80 event RACINIT
Application access control (9.6)	SMF 9, SMF 11, SMF 14, SMF 15, SMF 17, SMF 18, SMF 52, SMF 53, SMF 54, SMF 55, SMF 56, SMF 58, SMF 61, SMF 62, SMF 64, SMF 65, SMF 66, SMF 80 events SETROPTS, CHAUDIT, ALTDSD, PERMIT, RALTER, RDEFINE, RDELETE, ADDVOL, RENAME, DELETE, DELVOL, DEFINE, DELDSD, ADDSD, ACCESSSMF, SMF 90 subtypes 1, 3, 4, 5, 6, 13, 14, 16, 18, 19, 20, 21, 22, 23, 24, 25, 27, 28, 29, 31, SMF 92 subtypes 10, 11, SMF 118
Information access restrictions (9.6.1)	SMF 9, SMF 11, SMF 14, SMF 15, SMF 17, SMF 18, SMF 52, SMF 53, SMF 54, SMF 55, SMF 56, SMF 58, SMF 61, SMF 62, SMF 64, SMF 65, SMF 66, SMF 80 events SETROPTS, CHAUDIT, ALTDSD, PERMIT, RALTER, RDEFINE, RDELETE, ADDVOL, RENAME, DELETE, DELVOL, DEFINE, DELDSD, ADDSD, ACCESSSMF, SMF 90 subtypes 1, 3, 4, 5, 6, 13, 14, 16, 18, 19, 20, 21, 22, 23, 24, 25, 27, 28, 29, 31, SMF 92 subtypes 10, 11, SMF 118
Sensitive system isolation (9.6.2)	SMF 9, SMF 11, SMF 14, SMF 15, SMF 17, SMF 18, SMF 52, SMF 53, SMF 54, SMF 55, SMF 56, SMF 58, SMF 61, SMF 62, SMF 64, SMF 65, SMF 66, SMF 80 events SETROPTS, CHAUDIT, ALTDSD, PERMIT, RALTER, RDEFINE, RDELETE, ADDVOL, RENAME, DELETE, DELVOL, DEFINE, DELDSD, ADDSD, ACCESSSMF, SMF 90 subtypes 1, 3, 4, 5, 6, 13, 14, 16, 18, 19, 20, 21, 22, 23, 24, 25, 27, 28, 29, 31, SMF 92 subtypes 10, 11, SMF 118
Logging and reviewing events (9.7.2.3)	None
Control of operational software (10.4.1)	SMF 30 subtypes 1, 5, SMF 118 subtype 72, SMF 80 event RACINIT

SOX report	Audit settings
Data access (12.1.4)	SMF 9, SMF 11, SMF 14, SMF 15, SMF 17, SMF 18, SMF 52, SMF 53, SMF 54, SMF 55, SMF 56, SMF 58, SMF 61, SMF 62, SMF 64, SMF 65, SMF 66, SMF 80 events SETROPTS, CHAUDIT, ALTDSD, PERMIT, RALTER, RDEFINE, RDELETE, ADDVOL, RENAME, DELETE, DELVOL, DEFINE, DELDSD, ADDSD, ACCESSSMF, SMF 90 subtypes 1, 3, 4, 5, 6, 13, 14, 16, 18, 19, 20, 21, 22, 23, 24, 25, 27, 28, 29, 31, SMF 92 subtypes 10, 11, SMF 118

Typically, it is the System z system programmers who actually configure SMF audit settings on System z.

Based on the System z Basel II audit settings example in Table 11-2 on page 300, we predict roughly 3 Gb of audit data per day from each Logical Partition (LPAR) on X-Y-Z's System z.

We have the following recommendations for SMF audit settings:

- ▶ To audit logon in RACF we must capture SMF record type 30, subtype 1, which reflects the time of logon for TSO sessions and batch jobs.
- ▶ We must collect RACINIT events in SMF record type 80 to capture logon to CICS, session managers, and so on.
- ▶ Logoff from TSO must be logged to track the end of a session, which is reflected by SMF record type 30, subtype 5.
- ▶ Record type 30, subtype 2 and 4 generate a huge volume but are not relevant for auditing.
- ▶ Data set access is captured in SMF record type 80, ACCESS events. This task requires that the profiles protecting the data sets have AUDIT(ALL(READ)) for confidential data and AUDIT(SUCCESS(UPDATE) FAIL(READ)) for the change of sensitive data.
- ▶ Of fundamental importance is to configure SETROPTS SAUDIT and SETROPTS OPERAUDIT.

For more information about SMF, see *z/OS MVS System Management Facilities (SMF)*, SA22-7630 and *z/OS Security Server RACF Macros and Interfaces*, SA22-7682.

Table 11-2 on page 300 shows the typical SMF records that might be required to monitor z/OS according to the Basel II controls that the report addresses. Tivoli Security Information and Event Manager supports a subset of the z/OS SMF record set. To generate data that is supported by Tivoli Security Information and Event Manager, SMF processing must be turned on and appropriate records that

are supported by Tivoli Security Information and Event Manager must be created and saved.

These required SMF records are 0, 7, 9, 11, 14, 15, 17, 18, 22, 26, 30, 36, 41, 43, 45, 47, 48, 49, 52, 53, 54, 55, 56, 57, 58, 59, 61, 62, 64, 65, 66, 80 (RACF), 80 (Top Secret), the ACF2 record type, 81, 90, most of 92, selected subtypes of 102 (IFCids 4, 5, 6, 7, 8, 9, 10, 22, 23, 24, 25, 55, 83, 87, 90, 92, 107, 140, 141, 142, 143, 144, 145, 169, 177, 219, 220, 258, 314, and 319), the CICS monitoring record type 110 subtype 1, and selected subtypes of 118 and 119.

The exact SMF record selection is specified in the CARLa member C2ELES. This member can be updated by regular maintenance.

To generate SMF records for CICS transactions, CICS monitoring must be enabled and set up. You can set up monitoring by data types and classes, for example, you can monitor the classes for exceptions, performance, and resources.

To use CICS monitoring:

1. Create a DFHMCTxy CICS MCT (Monitoring Control Table).
2. Add MCT=xy to the SIT (System Initialization Table).
3. Run Configuring a z/OS Agent for Tivoli Security Information and Event Manager using the CEMT INQ MON command to confirm or set monitoring on and set classes of monitoring data and options.

For further details, see the CICS Monitoring Facility documentation in the CICS Transaction Server Information Center¹. You can also use the SET MONITOR command to change monitoring classes and options.

For DB2, you must activate the DB2 trace to generate the required SMF records using the following commands:

- ▶ -<subsysname> START TRACE(PERFM) DEST(SMF) CLASS(30) IFCID(6,7,8,9,10,22,90,107,177,314)
- ▶ -<subsysname> START TRACE(STAT) DEST(SMF) CLASS(30) IFCID(258)
- ▶ -<subsysname> START TRACE(AUDIT) DEST(SMF) CLASS(*)

These commands are intended as an example. In your installation, IFCIDs might already be logged to SMF by other traces. Verify and adapt these examples to meet the requirements of your installation.

If you use installation-defined events, make sure to include the SMF records that are required by your CARLa member C2EICES.

¹ This information is at <http://www.ibm.com/software/htp/cics/tserver/v31/library/>

Now that the audit subsystems are configured and activated on the target machines, we can start with Tivoli Security Information and Event Manager implementation for the System z, which we cover in the next section.

11.3 Implementation

Based on our analysis and the System z Basel II audit settings example configuration, a *new Standard Server* will be dedicated for System z and added to the Tivoli Security Information and Event Manager cluster as shown in Figure 11-2, with the System z and Tivoli Security Information and Event Manager cluster highlighted in bold in the production and management zones, respectively.

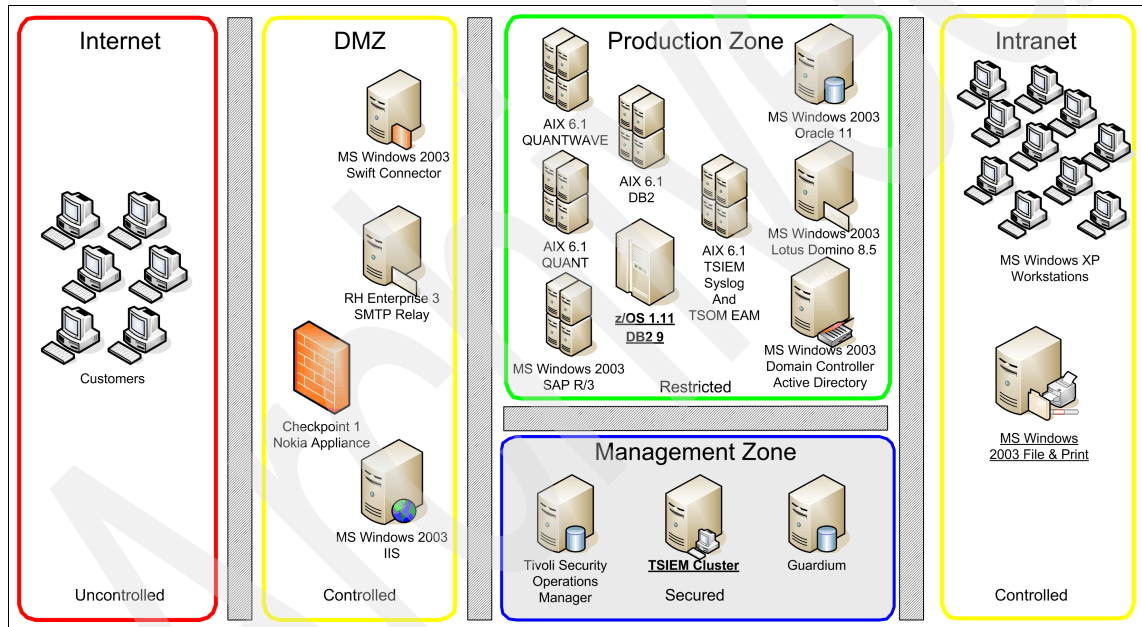


Figure 11-2 X-Y-Z Tivoli Security Information and Event Manager cluster

The Tivoli Security Information and Event Manager Basel II compliance management module integration is also a part of the System z implementation, which we execute in the following steps:

- ▶ Implementing the Standard Server
- ▶ Implementing the Actuator
- ▶ Basel II compliance management module implementation

11.3.1 Implementing the Standard Server

To implement the new Tivoli Security Information and Event Manager Standard Server, we perform an installation before we proceed with the configuration.

Installing the Standard Server

To install the Standard Server:

1. Install the database engine provided with Tivoli Security Information and Event Manager.
2. Install the desired Tivoli Security Information and Event Manager components for the Standard Server.
3. Register the Standard Server with the Enterprise Server.

We do not describe the Standard Server installation and registration to the Enterprise Server here because it is straightforward. For more details about each of these steps, see *IBM Tivoli Security Information and Event Manager Version 2.0 Installation Guide*, GI11-8778.

Configuring the Standard Server

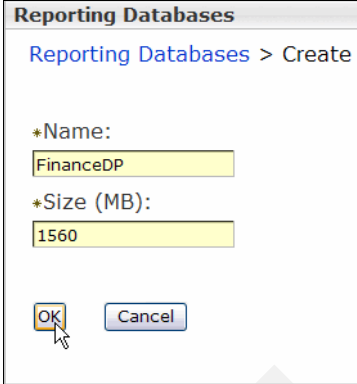
The configuration involves the following high-level steps in the Tivoli Security Information and Event Manager Web portal:

1. Create a Reporting Database to store the event data.
2. Create a System z Machine Group.

We outline each of these steps in the following sections.

Creating a Reporting Database

We create new Reporting Databases for loading all System z-related event data. X-Y-Z will store all System z event data in a database called FinanceDP, as shown in Figure 11-3.

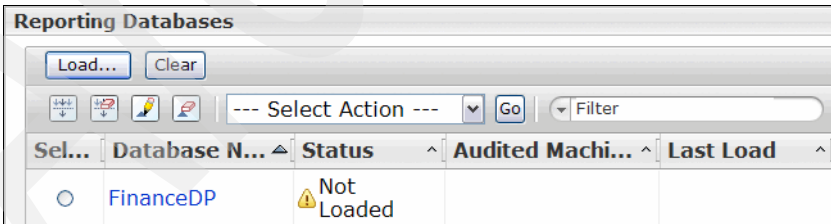


The screenshot shows a dialog box titled "Reporting Databases" with a breadcrumb "Reporting Databases > Create". It contains two input fields: "*Name:" with the value "FinanceDP" and "*Size (MB):" with the value "1560". At the bottom, there are "OK" and "Cancel" buttons. A mouse cursor is pointing at the "OK" button.

Figure 11-3 Add FinanceDP database

Based on the System z Basel II audit settings example in 11.2, “Audit settings” on page 299, we predict roughly 3 Gb of audit data per day from each System z LPAR on X-Y-Z’s System z. We have three LPARs in the System z environment to serve the corporate banking transaction system, branch bank teller, and customer online home banking applications. Therefore, in total we expect roughly 9 Gb of audit data per day. To be on the safe side, we configure the FinanceDP database for 15 Gb (15x1024 Mb), as shown in Figure 11-3.

Figure 11-4 shows how the FinanceDP database appears in the Reporting Database view.



The screenshot shows a table view titled "Reporting Databases". It has a toolbar with "Load..." and "Clear" buttons, and a "Select Action" dropdown menu. The table has columns: "Sel...", "Database N...", "Status", "Audited Machi...", and "Last Load". The "FinanceDP" database is listed with a status of "Not Loaded" and a warning icon.

Sel...	Database N...	Status	Audited Machi...	Last Load
<input type="radio"/>	FinanceDP	Not Loaded		

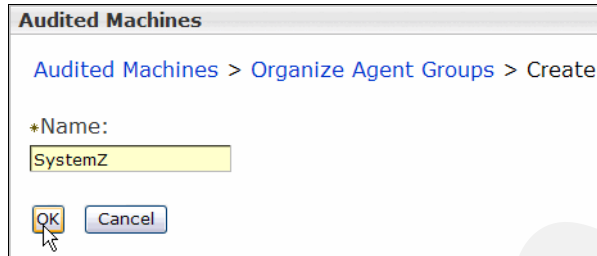
Figure 11-4 X-Y-Z FinanceDP database

Creating a Machine Group

For Tivoli Security Information and Event Manager to monitor one or more event sources on a particular machine, the machine must be registered in the Web portal. You can group the registered machines together into Machine Groups to

organize the audited systems. X-Y-Z wants to group their audited System z machines into a Machine Group called *SystemZ*.

We create a System z group named *SystemZ* in the Web portal, as shown in Figure 11-5.



Audited Machines

Audited Machines > Organize Agent Groups > Create

*Name:
SystemZ

OK Cancel

Figure 11-5 Add SystemZ Machine Group

The new SystemZ Machine Group now displays in the Machine page window, as shown in Figure 11-6.



Agent Groups	Agents
SystemZ ti0s02-sys1	

Create... Rename... Delete Paste Cut

Figure 11-6 X-Y-Z SystemZ Machine Group

After the new Standard Server is installed and registered with the Enterprise Server and both the Reporting Database and Machine Group are prepared, we can focus on our System z target and implement Actuators to start collecting required audit data.

11.3.2 Implementing the Actuator

The Tivoli Security Information and Event Manager Actuator component on System z copies selected SMF data to a file that is stored in UNIX System Services and then passes the data to the Tivoli Security Information and Event Manager Server.

The Actuator consists of the following processes:

▶ The Agent

The Agent provides a secure communication channel to the Tivoli Security Information and Event Manager Server. It is typically started soon after Initial Program Load (IPL) and only stopped in preparation for the next IPL.

▶ The User Information Source Actuator

The User Information Source Actuator collects data from the security data base and from the CKFREEZE data set.

▶ The Event Source Actuator

The Event Source Actuator process reads live or accumulated SMF data and generates an extract available to be used by the Agent. The Event Source Actuator also references the User Information Source data.

SMF records are written to SMF data sets when they are created and are then periodically dumped to sequential files using the SMF Dump Utility (IFASMFDP). IFASMFDP can also be used to split such sequential files and copy them to other files.

Original SMF data: The original SMF data is not deleted, changed, or moved; instead, the data is only copied. Therefore, other processes that use this data to report on specific data and events in the System z environment are not affected by Tivoli Security Information and Event Manager. This process also preserves the originating data for further processing or forensic analysis tasks where it might be required for *chain of evidence* needs.

System requirements

Here is a list of the system requirements on System z for implementing the Actuator:

- ▶ SMF processing must be activated.
- ▶ UNIX System Services must be available.
- ▶ A user ID is needed with the authority to:
 - Define users, groups, directories, and file systems.
 - Define a set of IP ports to be allocated for the Agent.
 - Create and mount recommended HFS or zFS file systems.
 - Set up STARTED or SURROGAT profiles.
 - Update access to one of the procedure libraries of the Job Entry Subsystem.
 - Create entries in the Job Scheduler or Automated Operations.

- ▶ Adjust and synchronize UNIX System Services time zones.
- ▶ Unicode support.
- ▶ TCP/IP security.
- ▶ Tivoli zSecure 1.7.0 at PTF PZ01300 or higher.

Preparation

It is recommended to use separate file systems for the Actuator software and the Agent data.

It is also recommended to create two separate RACF users:

- ▶ One that owns the Actuator software and directories.
- ▶ One that owns the Agent data and directories and has read and execute permission on the Actuator software and directories.

The defaults shown in Table 11-3 are used here.

Table 11-3 System z owners, directories, and file systems

	Software	data
Owning User	C2RUSER	C2EAUDIT
Owning Group	C2RGROUP	C2EGROUP
Directory	/usr/lpp/c2e/vx.y	u/c2eaudit/actuatr1
Mountpoint	/usr/lpp/c2e	u/c2eaudit
File system	OMVS.C2R.HFS	OMVS.C2EAUDIT.HFS
Variable	C2ESW	C2EPATH

Installing the software

To install the software:

1. Run the job C2RZCHFS from the CNRINST library to prepare the location where the software is to be installed. This job must be executed under root authority.
2. The recommended install directory is /usr/lpp/c2e/v8.0. The installation directory is referred to as C2ESW.
3. Upload the file `ibm.tsiem.actuator.pax.Z`, which is part of the IBM Tivoli Security Information and Event Manager distribution package `cfzf02en`, into an HFS or zFS file on System z in binary mode. The file is in the `mvs390_oe_2` directory of the package.

4. Run the job C2EUNPAC from the CNRINST library to unpack the software. This job can be run as:
 - Root, where C2RUSER and C2RGROUP are substituted
 - SURROGAT, where USER=C2RUSER and GROUP=C2RGROUP
5. Provide the location of the `ibm.tsiem.actuator.pax.Z` file and the software installation directory (C2ESW) to the job.

Installing the Agent

To install the Agent:

1. In the zSecure configuration, edit or at least uncomment the Actuator's specific parameter section (default C2R\$PARM of library C2RPARM). Specific parameters are C2ECUST, C2EPATH, C2ESW, C2ELVPFX, and C2ELVLLQ. Only C2EPATH and C2ELVPFX are mandatory.

The parameters are documented in Appendix D in the *IBM Tivoli zSecure Suite: CARLa-Driven Components Installation and Deployment Guide, Version 1.11.0*, SC23-6556-04.

2. In the CNRINST library, run the job C2EZAUSR to create the Agent's owner, group, home directory, and file system, if needed, provided that the z/OS security system is RACF. In case CA Top Secret or CA ACF2 is used, use various jobs. These jobs are also included in the CNRINST library.
3. Change the USER parameter to the user ID that will run the Agent.
4. Include the location of the Agent's typical C2R\$PARM that contains the correct C2EPATH parameter in the C2EJSTRT job.
5. Set the C2ESW parameter to the software installation directory, the default is `/usr/1pp/c2e/V8R0M0`.
6. Run the job C2EAROOT in the SCKRSAMP library to build the Agent's root directory. Among others, this job creates a symbolic link in the root directory called bin to the C2ESW.

Important: Do not start the Agent job or procedure until after you set up the secure connection.

For more information about Software or Agent installation, see the *IBM Tivoli zSecure Suite: CARLa-Driven Components Installation and Deployment Guide, Version 1.11.0*, SC23-6556-04.

Starting the Agent activation

Before starting the Agent activation, let us consider how the following recommendations about performance and multiple LPARs apply to the X-Y-Z System z environment:

- ▶ Generally recommended setup:
 - Separate Agents on each System z LPAR that you want to monitor.
 - Use a Live strategy for the event source, with a schedule as frequent as it corresponds to the demand to have events available on the Tivoli Security Information and Event Manager server in a reasonable time.
 - If the Agent for Tivoli Security Information and Event Manager is the only component of zSecure, also use a Live strategy for the User Information Source. A collect schedule of one time a day is sufficient for most cases.
- ▶ Multiple System z LPARs recommended setup:
 - When processing multiple System z LPARs, the recommended setup is that each System z LPAR has its own Agent, processing SMF, CKFREEZE, and the security database from that System z LPAR. However, when most of the DASD is shared, a performance gain can be achieved by not writing all shared information to all CKFREEZEs.
 - A multiple System z LPAR Agent usually requires more processing than several single Agents because each event source collects references to all User Information Source data, for example: CKFREEZEs and possibly UNLOADs from all System z LPARs are processed during each chunk of SMF collection.
 - In general, multiple System z LPAR Agents are not recommended. If you run with a common SMF accumulation data set and do not want to split that, you might consider setting up a single System z LPAR Agent on each System z LPAR and use a Live event source. This way, each Agent only processes its own System z LPAR's SMF. There is no objection against combining the Live event source with a Poll or Wait User Information Source.

Add each of the LPARs on System z that must be audited as a new machine. X-Y-Z will place each of its System z targets into the new *SystemZ* Machine Group. In this section, the setup and configuration for auditing one of the System z LPARs is shown. X-Y-Z repeats this process for adding other System z LPARs.

To add each System z LPAR:

1. With focus on the SystemZ Machine Group in the Web portal Machine View, start the Add Machine Wizard, as shown in Figure 11-7.

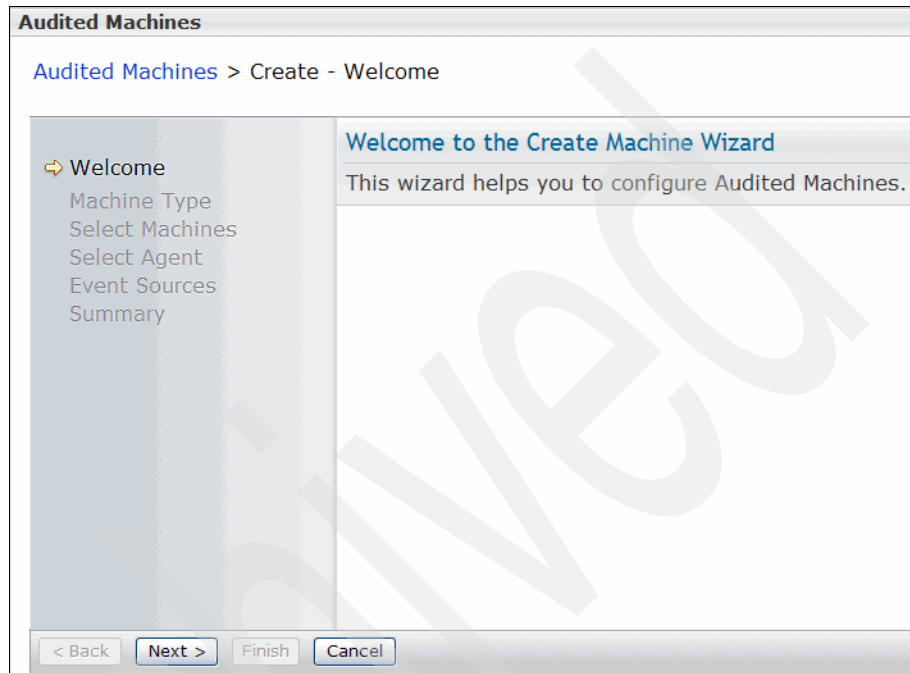


Figure 11-7 Add Machine Wizard

2. In the next window, select the Audited Machine Type from the available pull-down menu. For X-Y-Z's System z, the correct machine type is *IBM z/OS* or *OS/390®*, as shown in Figure 11-8 on page 313.

Figure 11-8 Choose Machine Type

Displaying the Source Type window: Selecting **Show Event Source Types** causes the Event Source Type window to display. Using this option, you can browse the supported event sources for the type of machine you are adding.

3. In the next window, in the Name input box within the Machine frame, enter the name of the target machines to be audited. Figure 11-9 shows our first target on System z, LPAR *ANIT*.

Figure 11-9 Choose Machine

4. Install a local Actuator on each of the target machines, as shown in Figure 11-10.

Select Agent

Which machine should facilitate auditing of ANIT?

Select Agent

Agent installed locally on the audited machine(s)

Agent installed remotely from the audited machine(s)

Directly from TSIEM Server ti0s02-sys1

Existing Agent. Agent group: ti0s02-sys1 Agent name: FSPDC

Install a new remote Agent of type Microsoft Windows

Figure 11-10 Select agent

5. In case the port is available on the z/OS machine, you can leave the default setting as shown in Figure 11-11.

Configure Agent on Audited Machine(s)

Specify port(s) used for communication with new Agent(s) on...

Agent

Test Port Find Port

+++ + - -

Sel...	Hostna...	Port	Status
<input type="radio"/>	ANIT	*5992	Unknown

Page 1 of 1 Total: 1 Filtered: 1 Displayed: 1

Install Type

Automatic Manual

Figure 11-11 Configure agent

As also shown in Figure 11-11, the Install Type is always manual by default for IBM z/OS or OS/390 Machine Type. You might also experience an unexpected side effect of System z, such as dynamic Virtual IP Addressing (VIPA).

With VIPA, the DNS holds the Virtual IP Address of the System z, but this address does not really exist. System z has another network address (physical address) that accepts packages with the main address as destination. When the System z sends packages, they originate from the physical address, which is designed for instant recovery when one of the System z LPARs dies. A backup machine can take over and accepts the packages that are sent to the virtual address.

The Tivoli Security Information and Event Manager server is designed to refuse packages that claim to be from an Agent but have an IP address that does not fit the value in the configuration file. Those messages are dropped.

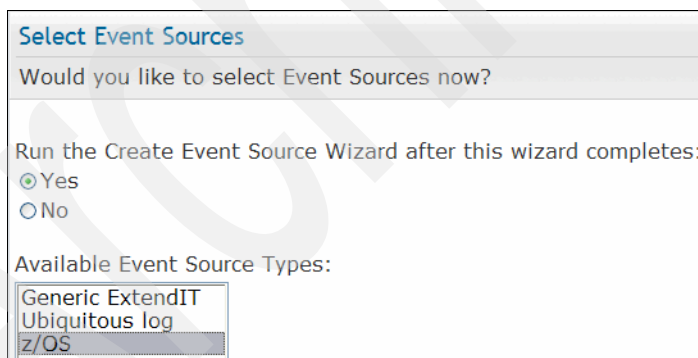
Also, a System z can have several network interfaces, each with a separate IP address. If this is the case, packages received from the System z can have a different address from what the DNS says.

Tip: Specify the IP physical address of the System z LPAR by issuing a **netstat** command on the TSO prompt, and review the *local socket* column.

You might find the IP physical address this way, but there is no absolute guarantee.

Important: Another option is to configure Tivoli Security Information and Event Manager server in a way that it can ignore the IP address of messages that claim to be from the System z Agent, which removes a security feature of the communication layer, so do it with caution.

6. Choose the correct Event Source Type, as shown in Figure 11-12. In our scenario it is *z/OS*.



Select Event Sources

Would you like to select Event Sources now?

Run the Create Event Source Wizard after this wizard completes:

Yes

No

Available Event Source Types:

Generic ExtendIT

Ubiquitous log

z/OS

Figure 11-12 Choose Event Source Type

Figure 11-13 on page 316 shows the final wizard window.

Summary

You have finished the Create Machine Wizard.

Check the settings. Click Finish to define the Audited Machine(s) or click Back to correct settings.

Setting	Value
Audited Machine(s)	ANIT
Audited Machine(s) Type	IBM z/OS or OS/390
Create Event Source(s)	Yes
Agent	ANIT

Connection File

A connection file is saved on the TSIEM server. Click Save when you want to download a copy.

Figure 11-13 Complete Add Machine Wizard

7. Before you finish the configuration, save the configuration file that is needed for Agent activation on a preferred location, or let the wizard save it by default in IBM/TSIEM/SIM/Server/config/machines.
8. Transfer this configuration file in text mode to the Agent root directory on System z (C2EPATH).
9. To initialize the Agent, run the C2ECNNT job that is located in CNRINST under the user ID that owns the Agent install directory (C2EAUDIT). To verify success, check the Agent.log file that is located in the C2EPATH/log directory for the string: LCM: Initial certification completed successfully.

Important: A configuration file is only valid for 24 hours before it expires.

10. Run the C2EJSTOP job in the SC2RJOBS library, again using the C2EAUDIT user ID, to stop the initialization process.
11. Continue to activate the Agent using the C2EJSTRT job in SC2RJOBS library using C2EAUDIT user ID.

Adding event source

Immediately after the Add Machine Wizard completes, the Event Source Wizard runs automatically. In this section, we illustrate how to complete the Add Event Source Wizard for the z/OS Event Source on the *ANIT* System z LPAR.

To add an event source:

1. Continue on the Add Event Source Wizard welcome window that displays, as shown in Figure 11-14 on page 317. Click **Next**.

Welcome to the Create Event Source Wizard

This wizard helps you add an Event Source to an Audited Machine.

Figure 11-14 Create Event Source Wizard

2. Define the z/OS event source properties. Use the default settings with the Live collection strategy as recommended before. Table 11-4 provides the properties explanation.

Table 11-4 Event source properties

Property	Description
Collect past data	Configures the collection of SMF records regardless of the time stamps. This option is intended for recovery of lost SMF intervals and for initially loading a Tivoli Security Information and Event Manager server with SMF data. For normal production, it must be set to NO. When this property is set to NO, SMF intervals that are already collected are not collected again.
Collect strategy	Determines how the collection is executed. The options are Live, Poll, or Wait. Live: SMF data is collected from the System z LPAR where the Agent is running. No more than one event source per Agent must run under the Live strategy. Using the Live strategy (with the SMF switch intercept) guarantees that no SMF records are lost, provided that the SMF data sets are off loaded in the correct order. Poll: Data is collected from the data set that you specify under SMF Data Set Name. If this data set is in use at the moment that the event source collection starts (or, for instance, when the data set resides on tape and all tape drives are in use), this particular event source collection is cancelled. The schedule remains active, and in time a new attempt is made. Wait: Same as Poll strategy with the difference being that if the data set is in use, the event source collection waits (up to half an hour) until the data set is available.
Error retention	Number of days that message log files are kept. Older log files are deleted at the next event source collect.

Property	Description
SMF Data Set Name	Data set from which data is collected when the collect strategy is Poll or Wait. For normal production, specify your SMF accumulation data set here. Often, installations off load their active SMF into a data set that is member of a Generation Data Group (GDG), for instance: off load into SYS2.WEEKLY.SMF(0), and one time a week create SYS2.WEEKLY.SMF(+1). If your installation uses a GDG, you can specify SYS2.WEEKLY.SMF(0), which represents the most recent member of the GDG. Processing ACF2 data by an Agent that runs on a RACF system, or reverse, is not supported. This field must be empty when the collect strategy is Live.
Store raw files	Reserved for future use.

3. Enter the proper Event Source Properties, as shown in Figure 11-15. Click **Next** to continue.

Set Properties

Define properties for Event Source z/OS, then click Next.

Name	Value
Connect String	A:localhost:49152
Collect strategy	LIVE
Store raw files	NO
Error retention	3
SMF Data Set Name	
Collect past data (discouraged)	NO
Text encoding for audit trail	UTF-8
Language code for audit trail	

Figure 11-15 Define event source properties

For better understanding, we depict System z Live as well as Wait and Poll strategies in Figure 11-16 on page 319 and Figure 11-17 on page 319 respectively. In the Live strategy, the Event Source only reads the intercepted SMF data sets.

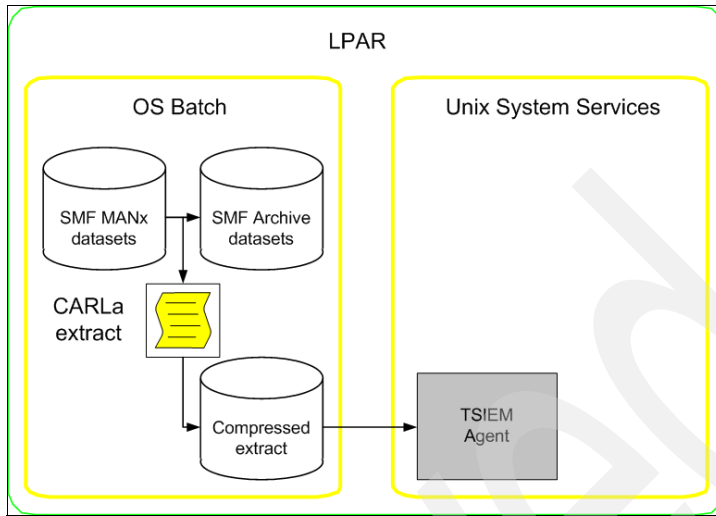


Figure 11-16 System z Live collect strategy

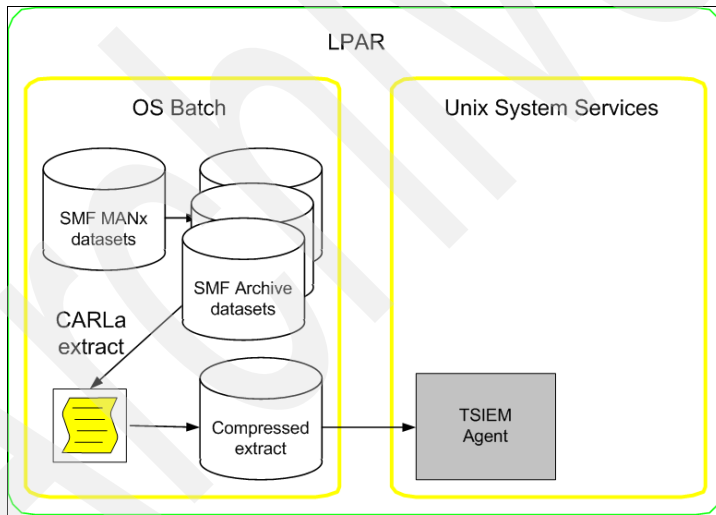


Figure 11-17 System z Wait and Poll collect strategy

4. Choose a Collect Schedule, as shown in Figure 11-18. Click **Next** to continue.

Set Collection Schedule

Define the collection schedule for the Event Source, then click Next.

Frequency:
Daily

Collect every:
 Working day
 Day

*Starting at:
9:00 PM

Figure 11-18 Choose a Collect Schedule

As recommended in the Agent activation section, choose to collect data on a daily basis (at 1 a.m.) when System z utilization is low. Because we expect about 3 Gb of data from each System z LPAR, we plan to provide the system with reasonable time to load this data into the Reporting Database a few hours later.

5. Choose to load audit data into the prepared *FinanceDP* database, as shown in Figure 11-19. Click **Next** to continue.

Choose Database

Select one or more Reporting Databases to load the Event Source data into, then click Next.

Reporting Databases

- FinanceDP
- General
- SELFAUDIT
- Windows

Figure 11-19 Choose a Reporting Database

- For the Load Schedule, choose to load data on a working day basis (at 3 a.m.), as shown in Figure 11-20. Click **Next** to continue.

Set Database Load Schedule

Define the schedule for Event Source data to be loaded into the FinanceDP Reporting Database.

Frequency:

Load every:
 Working day
 Day

Data that is:
 New data
 Last days of data

+Starting at:

Figure 11-20 Choose a Load Schedule

This schedule allows for System z audit data to be collected on time from all System z LPARs and then loaded into the *FinanceDP* Reporting Database. On the other hand, audit data that is collected from Friday to Sunday is loaded as late as Monday morning, but there is no expected high activity during the weekend on System z; therefore, we do not expect the Tivoli Security Information and Event Manager server to be overloaded.

For reporting reasons, we want last week's data available at any time, so we are using a seven-day sliding schedule, as shown in Figure 11-20.

- Complete the Add Event Source wizard, as shown in Figure 11-21. Click **Finish**.

Summary

You have finished the Create Event Source Wizard.

Verify the settings. Click Finish to define the Event Source or click Back to correct settings.

Setting	Value
Name	z/OS
Type	z/OS
Audited Machine(s)	ANIT
Collection Schedule	Working days: 9:00 PM
Reporting Database(s)	FinanceDP
Database Load Schedule	Working days: 11:00 PM

Figure 11-21 Complete Add Event Source Wizard

After you repeat the implementation process to the current point for all three of X-Y-Z's System z LPARs, namely *ANIT*, *ASRU*, and *AZEN*, the Tivoli Security Information and Event Manager Web portal Machine page reflects the status of System z LPARs, as shown in Figure 11-22.

Sel...	Audited Mac...	Type	Hostname o...	Agent Gr...
<input type="checkbox"/>	ANIT	Agent	ANIT	SystemZ
<input type="checkbox"/>	ASRU	Agent	ASRU	SystemZ
<input type="checkbox"/>	AZEN	Agent	AZEN	SystemZ
<input type="checkbox"/>	FINSYS	Agent...		ti0s02-sys1

Figure 11-22 System z Machine View

Similarly, the Event Source page in Tivoli Security Information and Event Manager's Web portal reflects the status of System z event sources, as shown in Figure 11-23.

Sel...	Agent Gr...	Audited Mac...	Event Sou...	Last Collec...
<input type="checkbox"/>	SystemZ	ANIT	z/OS	Never
<input type="checkbox"/>	SystemZ	ANIT	Grouping z/OS	Never
<input type="checkbox"/>	SystemZ	ASRU	z/OS	Never
<input type="checkbox"/>	SystemZ	AZEN	z/OS	Never
<input type="checkbox"/>	SystemZ	ASRU	Grouping z/OS	Never
<input type="checkbox"/>	SystemZ	AZEN	Grouping z/OS	Never
<input type="checkbox"/>	ti0s02-sys1	ti0s02-sys1	Microsoft Windows	3/16/10 2:15 PM

Figure 11-23 System z Event Source page

The Database page in Tivoli Security Information and Event Manager's Web portal reflects the System z FinanceDP database status, as shown in Figure 11-24 on page 323.

Reporting Databases				
Load... Clear				
<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>		--- Select Action --- Go Filter		
Sel...	Database N...	Status	Audited Machines	Last Load
<input type="radio"/>	FinanceDP	⚠ Not Loaded	ANIT...	
<input type="radio"/>	General	✅ Loaded	ti0s02-sys1	3/15/10 4:43...
<input type="radio"/>	SELFAUDIT	✅ Loaded	ti0s02-sys1	3/16/10 12:0...
<input type="radio"/>	Windows	✅ Loaded	kcg1f1...	3/12/10 7:52...
Page 1 of 1		Total: 4 Filtered: 4 Displayed: 4		

Figure 11-24 System z Database page

In the next step, we configure a User Information Source with a Live collect strategy using the Web portal. We must run at least one User Information Source collect before we run any Event Source collect; otherwise, the Event Source collect will fail because the CKFREEZE data set was never written into. Therefore, we postpone loading and testing the FinanceDP database for now.

Adding user information source

It is not always necessary to define the grouping process manually. For System z the Tivoli Security Information and Event Manager server produces the grouping functions for the *Who* and *Where* grammatical form. It reads the user databases for the System z platform and translates the information to a grouping function definitions. These grouping functions are merged with the user defined grouping functions during the grouping process. The merging process looks at the most recent collection time of the chunks that are selected for loading and finds the most recent user information grouping definitions for all supported platforms, created before the most recent chunk is loaded.

The user information source is actually yet another event source that is responsible for collecting the user database information. The collected information is also stored in the Tivoli Security Information and Event Manager server archive as a chunk. The information is already stored as a grouping function definition and is used during a scheduled load of a database.

We add the z/OS user information source using the Web portal to include RACF user and IOCONFIG information in the reports.

In this section, we illustrate how to complete the Add User Information Source Wizard for the z/OS user information source on the *ANIT* System z LPAR:

1. Start with the Add User Information Source Wizard welcome window that is displayed as shown in Figure 11-25 on page 324. Click **Next** to continue.

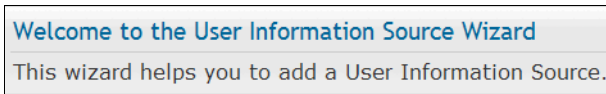


Figure 11-25 Add User Information Source Wizard

2. Choose a machine, as shown in Figure 11-26. Click **Next** to continue.

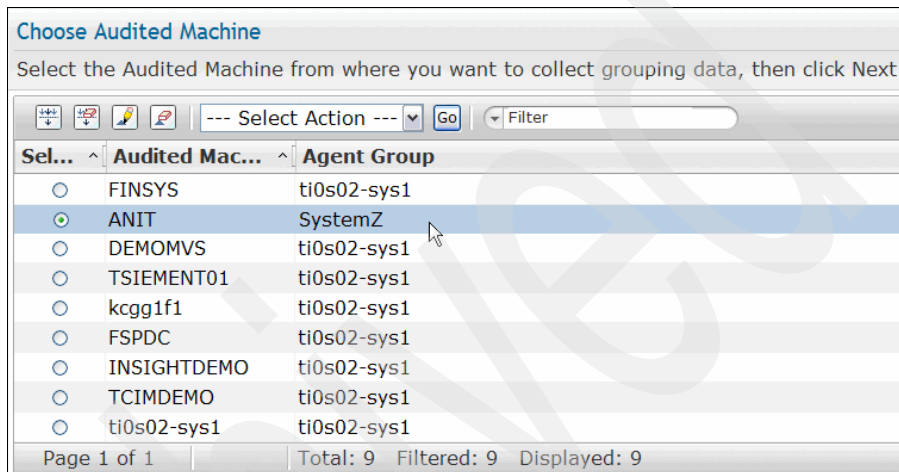


Figure 11-26 Choose a Machine

When loading data into a Reporting Database, Tivoli Security Information and Event Manager uses the group definitions from the user information source in addition to the groups that are defined in the policy. User information from a user information source is applied to all event sources from the same operating system.

3. Chose z/OS grouping for our scenario, as shown in Figure 11-27. Click **Next** to continue.

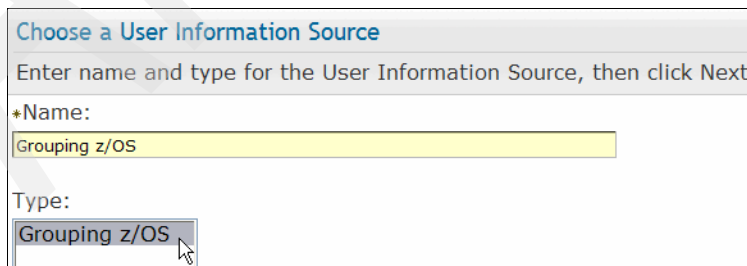


Figure 11-27 Choose a User Information Source

- Define z/OS event source properties, as shown in Figure 11-28. Use the default settings with a Live collection strategy as recommended before. Click **Next** to continue.

Set Properties

Set properties for the User Information Source, then click Next.

Name	Value
Connect String	A:localhost:49152
Configuration file	zOS_group.cfg
Collect strategy	LIVE
Store raw files	NO
Error retention	3
Complex name	
IOCONFIG Data Set Name	
UNLOAD Data Set Name	
System Policy Type	Production
Text encoding for audit trail	UTF-8

Figure 11-28 Define User Information Source Properties

Table 11-5 provides a description of the user information source properties.

Table 11-5 User Information Source properties

Property	Description
Collect strategy	<p>The collection strategy that the agent uses to collect the user information source data. There are three collection strategies:</p> <p>Live: The user data is read from the Primary RACF database as policy relevant data is read from an IOCONFIG data set. The data set creation is triggered by the user information source.</p> <p>Poll: The user data is read from the Primary RACF database, and policy-relevant data is Collect strategy read from an IOCONFIG data set. The data set is defined in the IOCONFIG Data Set Name property. If this data set is being used during collection, an error is returned.</p> <p>Wait: The user data is read from the Primary RACF database, and policy-relevant data is read from an IOCONFIG data set. The data set is defined in the IOCONFIG Data Set Name property. If this data set is being used during collection, the user information source tries to collect again 30 minutes later.</p>

Property	Description
Complex name	Logical name given to a set of System z LPARs that share the same users in a RACF database. All event sources that collect the SMF from this set of System z LPARs prefix the RACF user IDs that are found in the SMF with the Complex name.
Error retention	The number of log files sets to maintain in the C2EPATH/1og/*.props directory for this user information source.
IOCONFIG Data set Name	Name of an existing IOCONFIG data set used by this user information source to obtain system-specific information and to add it to the z/OS grouping file. Leave this field empty when using the Live strategy.
System policy type	Determines in which W7 WHERE group the System z LPAR is categorized, such as Systems with non-segregated administration and Systems with segregated administration.
UNLOAD Data Set Name	Name of an existing unloaded RACF data set that is related to the IOCONFIG Dataset Name parameter. Leave this field empty when using the Live strategy.

- Again, as with the event source and as recommended in “Starting the Agent activation” on page 311, choose to collect data on a daily basis, at midnight as shown in Figure 11-29, when System z utilization is low and before the event source collect begins. Click **Next** to continue.

Figure 11-29 Set a Collection Schedule

6. Complete the Add User Information Source wizard, as shown in Figure 11-30. Click **Finish**.

Summary

You have finished the Create User Information Source Wizard.

Verify the settings. Click Finish to define the User Information Source or click Back to correct settings.

Setting	Value
Name	Grouping z/OS
Type	Grouping z/OS
Audited Machine(s)	ANIT
Collection Schedule	Working days: 8:00 PM

Figure 11-30 Complete Add user Information Source Wizard

This concludes our section about the Actuator implementation. We can begin collecting audit data now. The last step before we can show System z Basel II compliance reports is the Basel II compliance management module implementation.

11.3.3 Basel II compliance management module implementation

Now that we can collect, load, and store needed audit data from the System z machines, we must perform an additional step to be able to report on this data according to Basel II compliance regulations.

A best practice approach for a regulatory compliance life cycle is:

- ▶ Evaluate
- ▶ Install compliance management module
- ▶ Import templates
- ▶ Configure W7 groups
- ▶ Adjust reports
- ▶ Commit policy
- ▶ Re-evaluate

In this section, we go through the life cycle of the Basel II compliance management module, which includes the installation, implementation, and finally Basel II compliance reports as identified in the X-Y-Z requirements. The goal is to produce Basel II compliance reports for its System z environment.

Installation

The *IBM Tivoli Security Information and Event Manager Version 2.0, IBM Tivoli Basel II Management Module Installation Guide, G111-8779* provides an overview and installation information for the IBM Tivoli Basel II compliance management module, so we do not go into details here.

After successful installation from a self-extracting executable on a separate CD, the Basel II compliance management module is displayed in the Tivoli Security Information and Event Manager Management Modules section of the portal, as shown in Figure 11-31.

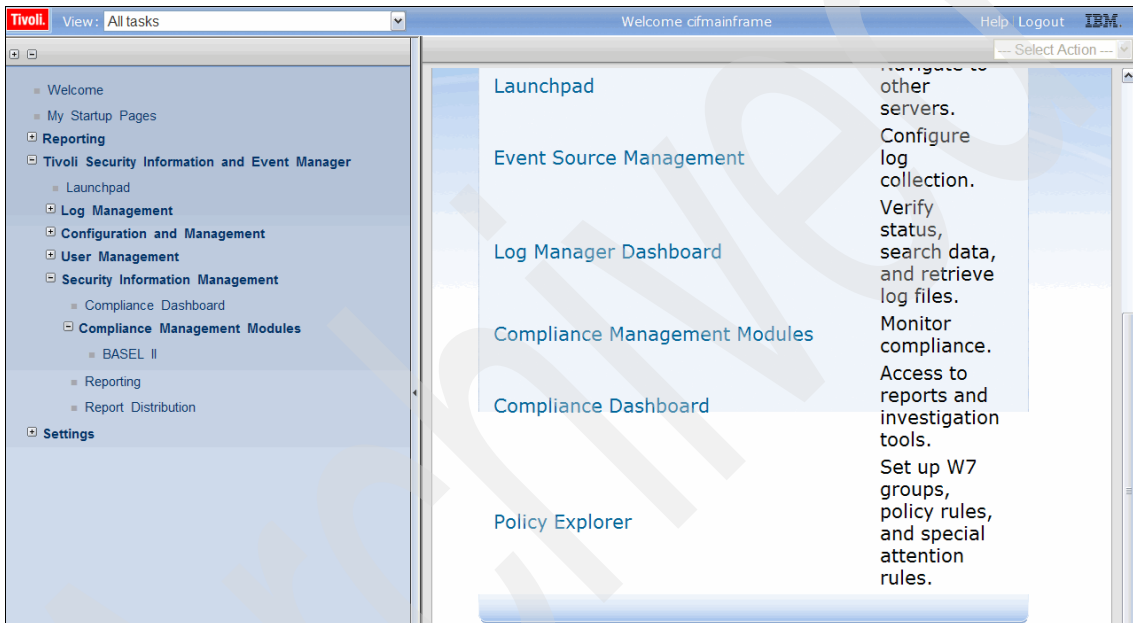


Figure 11-31 Tivoli Security Information and Event Manager Basel II compliance management module

Optionally, the templates, reports, and documentation that are associated with the Basel II compliance management module can be accessed in the Compliance Dashboard Regulations Resource Center, as shown in Figure 11-32.

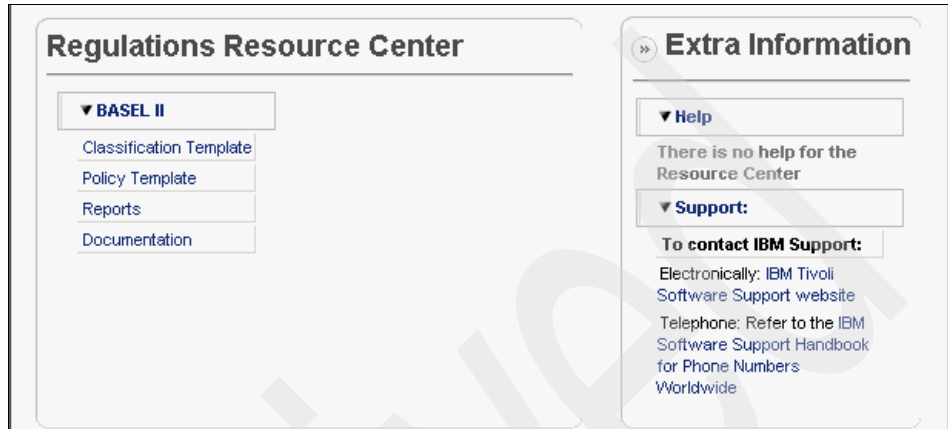


Figure 11-32 Tivoli Security Information and Event Manager regulations

In the next section, we explain those components.

Classification Template

A W7 Classification Template helps us to build W7 groups according to the Basel II regulation.

The Classification Template is a link to the `grouping.cfg` file, which contains a complete list of all group names for each and every W7 category that is used by the Basel II compliance management module report and Tivoli Security Information and Event Manager policy. The template can be exported using the Download button.

Figure 11-33 on page 330 partially shows the *onWhat* category in the Basel II classification template.

Classification Template

download

► Who

► What

▼ onWhat

Group name	Description
Administration Objects	Any object that is used for user or system administration
CreateDelete Sensitive Data - Production	Data where removal or masquerading may compromise a production system
CreateDelete Sensitive Data - Test	Data where removal or masquerading may compromise a test system
Customer Data	All data pertaining to customers including personal information, financial information etc.
Customer Data - High	All data pertaining to customers including personal information, financial information etc. - High Sensitivity
Customer Data - Low	All data pertaining to customers including personal information, financial information etc. - Low Sensitivity
Customer Data - Medium	All data pertaining to customers including personal information, financial information etc. - Medium Sensitivity
Diagnostic Port	Security sensitive system ports
Financial Data	All Financial related data
Financial Data - High	Highly Sensitive Financial Data
Financial Data - Low	Low sensitivity Financial Data
Financial Data - Medium	Medium Sensitivity Financial Data
General Data	General, unspecified data
HR Data	All Human Resources related data
HR Data - High	Highly sensitive Human Resources data
HR Data - Low	Low sensitivity Human Resources data
HR Data - Medium	Medium sensitive Human Resources data

Figure 11-33 Basel II Classification Template

The Classification Template is an empty W7 classification. Containing no references to entities but the description for each groups, it explains what type of entities are to be classified by the group.

Policy Template

The Policy Template contains a set of policy and attention rules based on the regulation's recommendation.

This is the link to the policy.pcy file that is installed with the grouping file that belongs to the Basel II compliance management module. Again, download this file by clicking **Download**.

Figure 11-34 shows Policy Rules from Basel II 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						
	System Processes						
IT							
HR Management		Out of Office Hours		HR Data			
Users		Office Hours		General Data			
Administrators			Systems with non-segregated administration				
Sales Staff		Office Hours		Customer Data			

► Attention Rules

Figure 11-34 Basel II Policy Rules template

The Policy Template contains policy and attention rules that are based on the recommendations in the Basel II regulation. These recommendations were evaluated and translated into the W7 model and included if meaningful coverage can be achieved.

Figure 11-35 shows a partial list of all Attention Rules from the Basel II Policy Template.

Policy Template

download

► Policy Rules

▼ Attention Rules

Who group	What group	When group	Where group	On What group	From Where group	Where To group	ID	Severity	Description
IT				Customer Data - Low			access low	20	Review
IT				Organizational Data			access low	25	Review
	User Actions - File			Administration Objects			medium	40	Requires attention
IT				HR Data - Medium			access medium	50	Requires attention
	Collect Failure						collect_failure	70	Requires immediate attention
IT				Customer Data - Medium			access medium	50	Requires attention
Administrators				Organizational Data			access medium	50	Review
	Intrusion - High						high	70	Requires immediate attention
	Alerts - Medium						medium	50	Requires attention
IT				Proprietary Data			access low	25	Review
IT				Non-Public Data			access low	25	Review

Figure 11-35 Basel II Attention Rules template

As with the grouping.cfg file or Classification Template, the file contents are used in the Tivoli Security Information and Event Manager default policy. When used there, the groups and rules build the dashboard contents in the Compliance Dashboard. The policy rules that are used in the Management Module are derived from the Basel II compliance regulation.

Reports

The reports section contains the reports that are required by the regulation.

The most important link of the Basel II compliance management module is the Reports link. It provides access to the set of reports that are specially defined for the Basel II compliance management module. Every report has a link to a

paragraph in the compliance regulation that discusses the need for information of the type shown in the report.

These reports are built according to the report requirements recognized in the Basel II regulatory compliance document.

Figure 11-36 shows a partial list of Basel II regulation reports.

BASEL II Regulation Reports			
<input type="button" value="Add custom report"/> <input type="button" value="Import custom reports"/>			
BASEL II			
Title	Description	Action	
BASEL II Internal attacks - quarterly trend	Number of exceptions NOT in the Exposure and Intrusion groups quarter over quarter		
BASEL II (.) External attacks - monthly trend	Number of exceptions in the Exposure and Intrusion groups month over month		
BASEL II (.) External attacks - quarterly trend	Number of exceptions in the Exposure and Intrusion groups quarter over quarter		
BASEL II (.) Internal attacks - monthly trend	Number of exceptions NOT in the Exposure and Intrusion groups month over month		
BASEL II (.) Policy Exceptions - monthly trend	Number of exceptions month over month		
BASEL II (.) Policy Exceptions - quarterly trend	Number of exceptions quarter over quarter		
BASEL II (5.2.5.2) Classification	Assets defined to the system.		
BASEL II (6.3.8.1.3,8.1.3) Security alert	Alerts sent in response to policy exceptions or special attention exceptions.		
BASEL II (6.3.4,8.1.3,8.1.3) Incident tracking	Policy exceptions and incident tickets recorded against them.		
BASEL II (8.1.2,8.1.2) Operational change control	Changes to the operating environment such as system updates, DBA activity, and so on.		
BASEL II (8.1.6,8.1.6) External contractors	Exceptions and Failures Caused by External Contractors.		
BASEL II (8.3,8.3) Malicious attacks	Exceptions and failures due to Malicious attacks.		
BASEL II (8.4,9.7.1,9.7.1) Log archive	Log archive dates and locations.		
BASEL II (8.4,9.7.1,9.7.1) Log collection	Log collection schedule and platforms.		
BASEL II (8.4,9.7.1,9.7.1) Log storage	Log storage report for all platforms.		
BASEL II (8.4.2,8.4.2) Operator log	Actions performed by the IT Admin staff.		
BASEL II (8.5,8.5) Network management	Actions and events caused by users on Network Services.		

Figure 11-36 Basel II Reports

The set of reports is partly a set of text files in the `\iView\Srv\reports\nl\consul\regulations\base1\` directory for the Basel II compliance management module. Some reports are hard coded in a Java™ class but most are coded in the `.pearl` files.

Importing

When the compliance management module is installed, you need a working policy. Because we want System z to be compliant to Basel II regulations, we use templates that come with the Basel II compliance management module and customize them to suit X-Y-Z's System z need.

It is a recommended approach in Tivoli Security Information and Event Manager to create a duplicate of X-Y-Z's default predefined policy, which is located in the *committed* folder in `\Server\config\grouping\committed\20000101000000`, and start with that. Although it can be used as a template for all supported systems, at the moment we do not want to deal with anything else but System z.

To create a new working policy:

1. In the *work* directory (`..\Server\config\grouping\work` on hard drive), create a new empty System z policy called *SystemZ*, as shown in Figure 11-37.

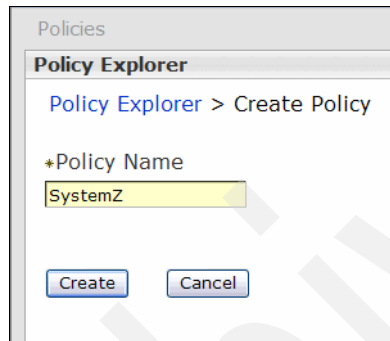


Figure 11-37 Create Basel II policy

Later on, we can merge this policy into a common X-Y-Z policy, where System z plays an integral part.

2. Open the SystemZ policy, and import all needed components. From the Policy Explorer, import the Basel II grouping file `grouping.cfg`, as shown in Figure 11-38 on page 335. The grouping and policy files are in the location: `\IBM\TSIEM\tip\systemApps\isclite.ear\iiview.war\regulations\base1`

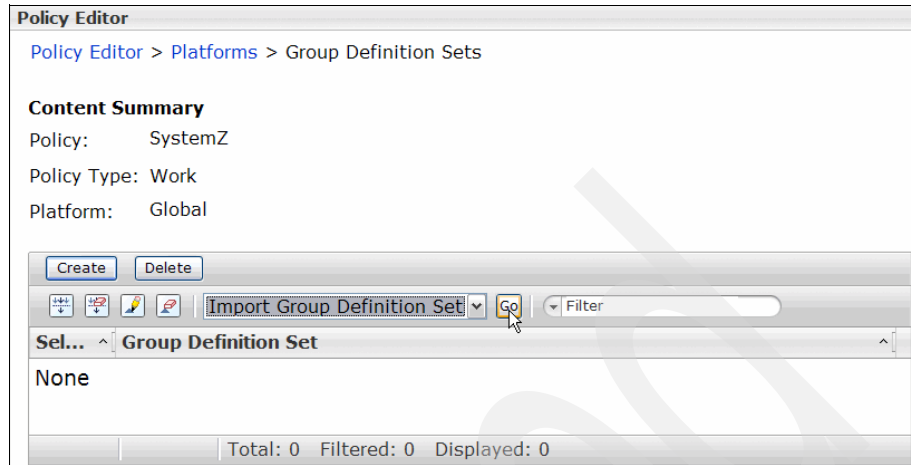


Figure 11-38 Import Basel II grouping

Figure 11-39 shows how to import the .cfg file after it is downloaded through the regulations page.

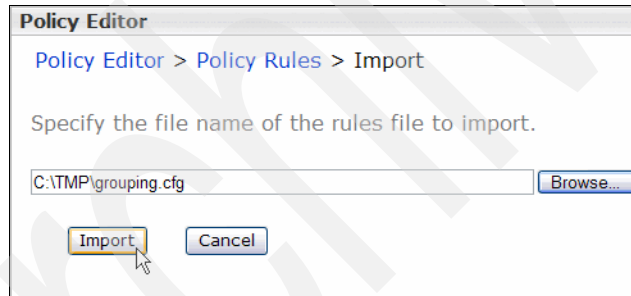


Figure 11-39 Importing a cfg file

3. Import Basel II policy rules and attention rules from the template, as shown in Figure 11-40 on page 336.

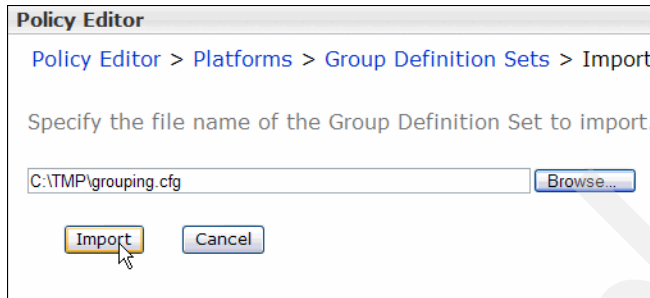


Figure 11-40 Import Basel II rules

When imported, Basel II policy and attention rules display as shown in Figure 11-41 and Figure 11-42 on page 337, respectively.

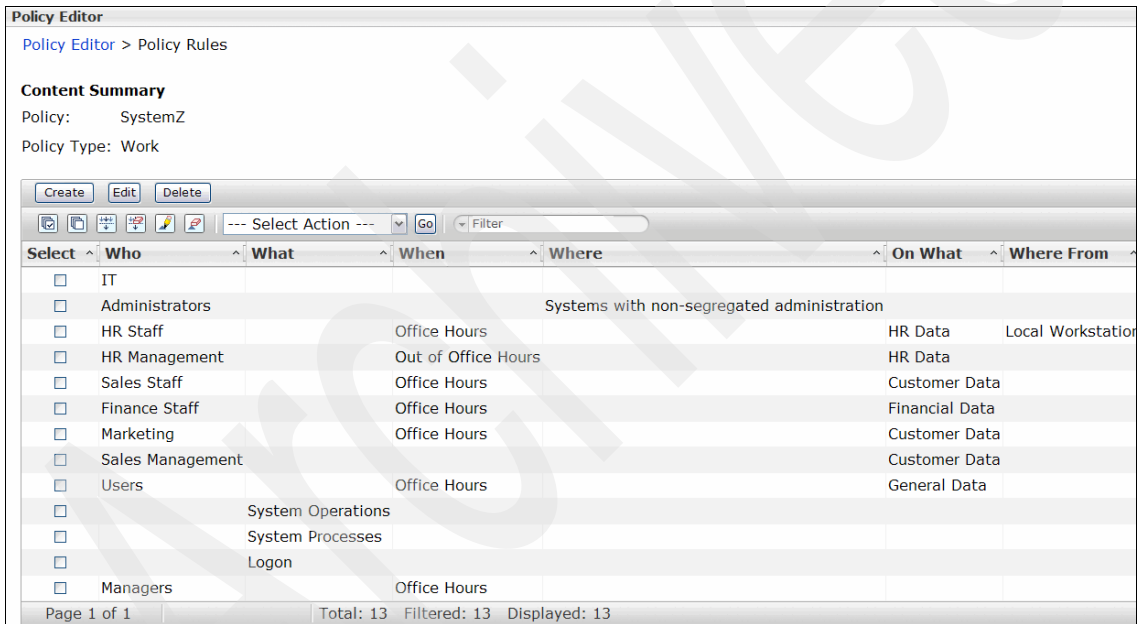


Figure 11-41 Basel II Policy Rules

Attention: Figure 11-42 does not show all Basel II attention rules.

Sel...	Who	What	Wh...	Wh...	On What	Where Fr...	Where ...	Seve...	Rule ID
<input type="checkbox"/>		Alerts - High						70 high	
<input type="checkbox"/>		Collect Failure						70 collect_fail...	
<input type="checkbox"/>		Intrusion - High						70 high	
<input type="checkbox"/>	IT				Customer Data - High			70 access high	
<input type="checkbox"/>	IT				HR Data - High			70 access high	
<input type="checkbox"/>	IT				Financial Data - High			70 access high	
<input type="checkbox"/>	Administra...				Customer Data - High			70 access high	
<input type="checkbox"/>	Administra...				HR Data - High			70 access high	
<input type="checkbox"/>	Administra...				Financial Data - High			70 access high	
<input type="checkbox"/>		Alerts - Medium						50 medium	
<input type="checkbox"/>		Intrusion - Me...						50 medium	
<input type="checkbox"/>	IT				Customer Data - Me...			50 access me...	
<input type="checkbox"/>	IT				HR Data - Medium			50 access me...	
<input type="checkbox"/>	IT				Financial Data - Me...			50 access me...	
<input type="checkbox"/>	Administra...				Customer Data - Me...			50 access me...	

Figure 11-42 Basel II Attention Rules

Now that the policy is in place, we must customize it for X-Y-Z's System z environment. We do not modify any policy and attention rules because they are based on the Basel II regulation recommendations, which were evaluated and translated into the W7 model.

In the next paragraph, we explain how to customize W7 groups for X-Y-Z's System z environment.

W7 groups

First, we assign entities to the classification template groups. When the policy is used, this grouping is merged and used together with the latest grouping from the user information source.

Figure 11-43 shows an example of X-Y-Z's assignment for the W7 category *When* and in part for category *Where* (*Customer Information systems group*).

Content Summary			
Policy:	SystemZ	Group Definition Set:	grouping
Policy Type:	Work	Group:	Office Hours
Platform:	Global	Dimension:	WHEN

Condition Table
Select the condition you want to work with. Changes are saved only when you click the OK or Apply button.

--- Select Action ---

Sel...	Condition Name
<input type="checkbox"/>	from Monday at 7:00 to Monday at 17:59
<input type="checkbox"/>	from Tuesday at 7:00 to Tuesday at 17:59
<input type="checkbox"/>	from Wednesday at 7:00 to Wednesday at 17:59
<input type="checkbox"/>	from Thursday at 7:00 to Thursday at 17:59
<input type="checkbox"/>	from Friday at 7:00 to Friday at 17:59

Page 1 of 1 | Total: 5 | Filtered: 5 | Displayed: 5

Figure 11-43 W7 assignment example

In Figure 11-44 we show another W7 assignment example.

Policy Editor			
Policy Editor > Platforms > Group Definition Sets > Groups > Conditions > Requirements			
Content Summary			
Policy:	SystemZ	Group Definition Set:	grouping
Policy Type:	Work	Group:	Finance
Platform:	Global	Dimension:	WHERE
Requirement Table			
Select the requirement you want to work with.			
Sel...	Requirement Name		
<input type="checkbox"/>	Platform name is ANIT		
<input type="checkbox"/>	Platform name is ASRU		
<input type="checkbox"/>	Platform name is AZEN		

Figure 11-44 The Where group Finance

If you already have a grouping in place, we recommend that you rename the existing groups to the group names that are used in the classification template.

To do this, you must know what the classification groups refer to. The best references are the regulatory reports that make use of these groups.

After you run the report, you can use the *Extra Information* panel to obtain information about:

- ▶ What assets, processes, or actions are monitored by the report (*Background*).
- ▶ Filters used by the report (*Filters*).

Also the group's description in the classification template must provide enough information to determine which entities are to be referred by it. We showed an example in Figure 11-33 on page 330.

- ▶ What the report was meant to be used for (*Help*).

For X-Y-Z, we already described a set of identified Basel II reports in 11.1, “Reporting requirements” on page 297.

After we save our first policy, it is time to load the System z audit data, see the first resulting reports, and make adjustments if necessary.

Reports

To load the System z audit data into the FinanceDP database, we first must disable the existing associated load schedule in the Tivoli Security Information and Event Manager's Web portal, as shown in Figure 11-45 on page 340.

Note: In a production environment, we recommend using a specifically created test Reporting Database so that we do not interrupt any scheduled load or report on our FinanceDP database.

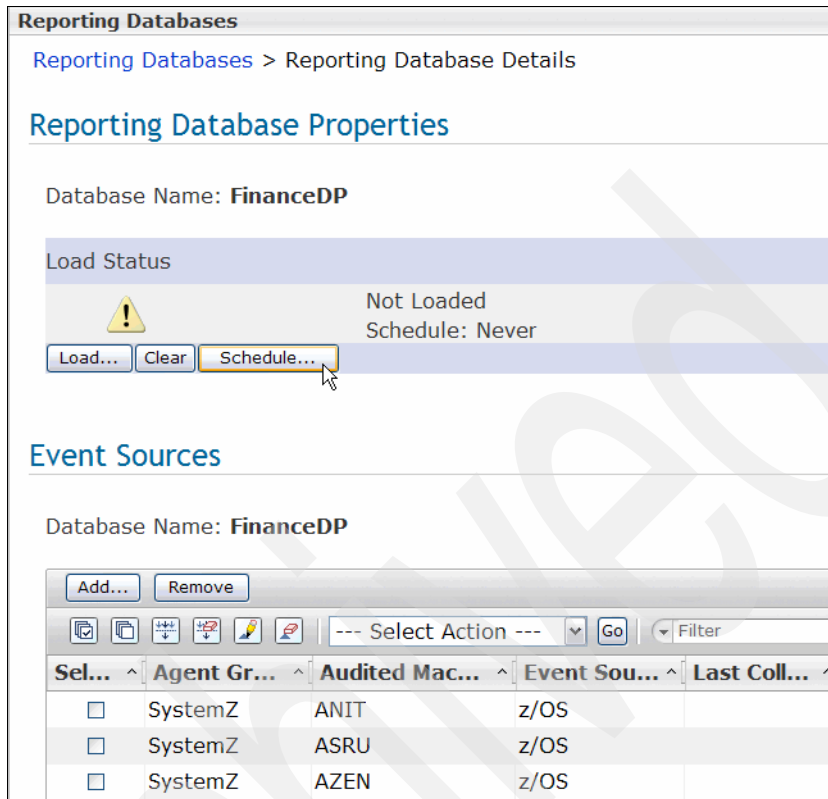


Figure 11-45 Disable load schedule

Start loading the database, using our draft policy:

1. Select the FinanceDP database, and start the Load Database Wizard, as shown in Figure 11-46. Click **Next** to continue.

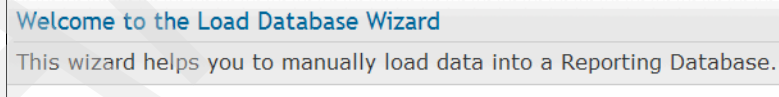


Figure 11-46 Start Load Database Wizard

2. Confirm the preselected database, as shown in Figure 11-47 on page 341. Click **Next** to continue.

Choose a Database

Into which Reporting Database do you want to load data?

Select a database, and then click Next.

--- Select Action --- Go Filter

Sel...	Database N...	Sta...	Last Load
<input checked="" type="radio"/>	FinanceDP	⚠ Not Loaded	3/16/10 11:06 AM
<input type="radio"/>	General	✅ Loaded	3/16/10 4:19 PM
<input type="radio"/>	SELFAUDIT	✅ Loaded	3/17/10 12:00 AM
<input type="radio"/>	Windows	✅ Loaded	3/12/10 7:52 AM

Figure 11-47 Choose database

- For the data that you want to load, specify the time frame, as shown in Figure 11-48. Click **Next** to continue.

Choose a Period

From which period of time should data be loaded into database FinanceDP?

Select a period, and then click Next.

From: * 2/17/10 * 9:44 AM

Until: * 3/17/10 * 11:59 PM

Figure 11-48 Choose time period

- Specify whether you want the latest data from the event sources in addition to audit data that is already present in the Depot, or just the latest, as shown in Figure 11-49. Click **Next** to continue.

Collect Data

Should data be collected for the Event Sources associated with database FinanceDP?

Do you want to collect the latest log data before starting the load?

Yes, collect the data first.

No, just load the database.

Choose one of the options, and then click Next.

Figure 11-49 Collect or load

- Choose the policy to use for this load, as shown in Figure 11-50. Click **Next** to continue.

Choose a Policy

Which Policy should be applied to the data loaded into FinanceDP?

Choose a Policy, and then click Next.

- Matching: The policy that matches best the selected time period.
- Newest: The latest committed Policy.
- Fixed: An explicit choice from the following collection:

Sel...	Policy Name	Type
<input type="radio"/>	Friday, December 31, 1999 7:00:00 PM EST	<input checked="" type="checkbox"/> Committe
<input type="radio"/>	Duplicate of 20000101000000	<input checked="" type="checkbox"/> Working
<input checked="" type="radio"/>	SystemZ	<input checked="" type="checkbox"/> Working

Page 1 of 1 | Total: 3 | Filtered: 3 | Displayed: 3

Figure 11-50 Choose policy

- Complete the Load Database Wizard, as shown in Figure 11-51. Click **Finish**.

Completing the Load Database Wizard

Are all settings correct?

You are now ready to request the manual load.
The database load will be queued for execution on the Server.

Setting	Value
Reporting Database	FinanceDP
Period	From Feb 17, 2010 9:44:00 AM until Mar 17, 2010 11:59:00 PM
Collect first	Yes
Policy	SystemZ

To close this wizard and start the load request, click Finish.

Figure 11-51 Complete Load Database Wizard

We are now ready to request the System z audit data to be loaded into the FinanceDP database.

After a successful load, we open the dashboard to have a first look at X-Y-Z's System z Basel II compliance status, as shown in Figure 11-52.

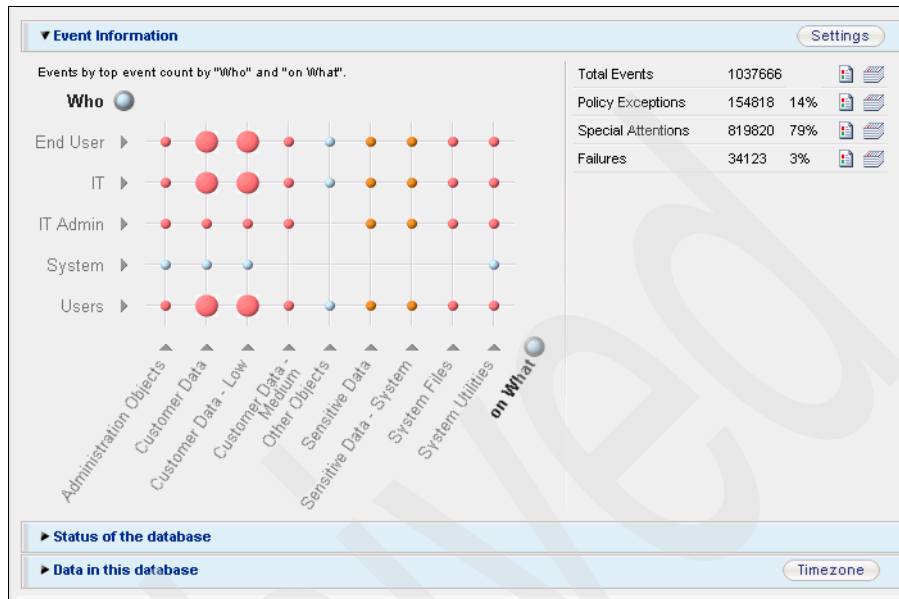


Figure 11-52 X-Y-Z's System z Basel II summary

At a first glance, we see a grid dashboard that clearly indicates that a majority of exceptions are related to customer data on System z. We can also check the status of audit data and the FinanceDP database itself, as shown in Figure 11-53.

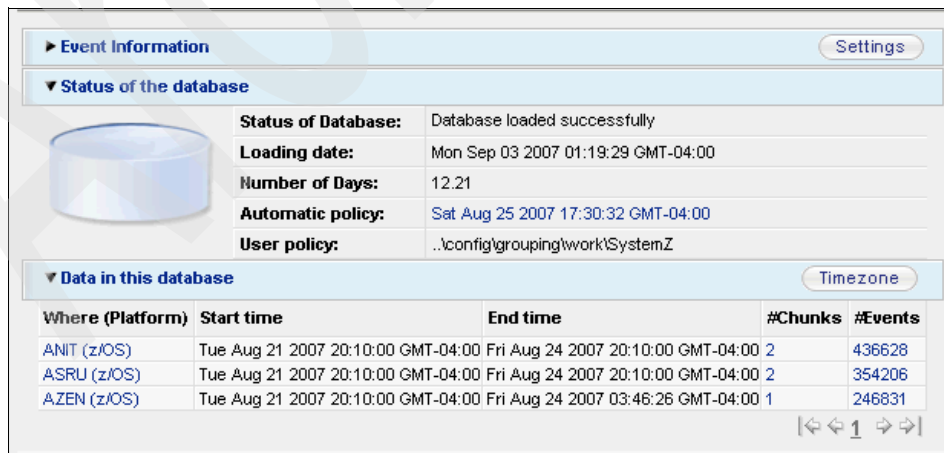


Figure 11-53 FinanceDP database status

We see that the database was loaded successfully with the automated policy used together with our *SystemZ* work policy. We also see the amount of audit data in the database together with the time frame for each of the X-Y-Z's System z LPAR.

We end the Reports section with actual Basel II reports for X-Y-Z's System z, as requested and identified in 11.1, "Reporting requirements" on page 297. These reports are illustrated in Figure 11-54 through Figure 11-62 on page 348.

Setup:

Month Day Year Hour Min.
 Start time August 21 2007 20 10
 End time September 3 2007 1 11

Execute Reset

Time zone: GMT-05:00 Cuba, East-Indiana, Eastern

Who group	What group	On What group	Where To group	When group	#Events	#Pol. Excp.	#Spec. Att	#Fail.
End User	System Actions	Administration Objects	Customer Information Systems	Out of Office Hours	3	3	0	0
End User	System Updates	Administration Objects	Customer Information Systems	Office Hours	18	18	0	0
End User	System Updates	Administration Objects	Customer Information Systems	Out of Office Hours	22	22	0	0
System	System Actions	Administration Objects	Customer Information Systems	Out of Office Hours	3	3	0	0
System	System Updates	Administration Objects	Customer Information Systems	Office Hours	18	18	0	0
System	System Updates	Administration Objects	Customer Information Systems	Out of Office Hours	22	22	0	0
Users	System Actions	Administration Objects	Customer Information Systems	Out of Office Hours	3	3	0	0
Users	System Updates	Administration Objects	Customer Information Systems	Office Hours	18	18	0	0

Figure 11-54 Operational change control (8.1.2)

Setup:

Month Day Year Hour Min.
 Start time August 21 2007 20 10
 End time September 3 2007 1 11

Execute Reset

Time zone: GMT-05:00 Cuba, East-Indiana, Eastern

What group	On What group	When group	Where group	#Events	#Pol. Excp.	#Spec. Att	#Fail.
Administration	Administration Objects	Office Hours	Customer Information Systems	75	0	0	0
Administration	Administration Objects	Out of Office Hours	Customer Information Systems	2	0	2	0
Read Data	Administration Objects	Office Hours	Customer Information Systems	126	0	71	80
Read Data	Administration Objects	Out of Office Hours	Customer Information Systems	6182	0	602	6083
Read Data	Customer Data	Office Hours	Customer Information Systems	994	0	994	0
Read Data	Customer Data	Out of Office Hours	Customer Information Systems	19436	0	19436	0
Read Data	Customer Data - Low	Office Hours	Customer Information Systems	994	0	994	0
Read Data	Customer Data - Low	Out of Office Hours	Customer Information Systems	19436	0	19436	0
Read Data	System Files	Office Hours	Customer Information Systems	27	0	27	0
Read Data	System Files	Out of Office Hours	Customer Information Systems	770	0	770	0
Read Data	System Utilities	Office Hours	Customer Information Systems	126	0	71	80
Read Data	System Utilities	Out of Office Hours	Customer Information Systems	6133	0	577	6081
Write Data	Administration Objects	Out of Office Hours	Customer Information Systems	21	0	2	0
Write Data	Customer Data	Office Hours	Customer Information Systems	565	0	565	0
Write Data	Customer Data	Out of Office Hours	Customer Information Systems	11495	0	11495	3
Write Data	Customer Data - Low	Office Hours	Customer Information Systems	565	0	565	0

Figure 11-55 Operator log (8.4.2)

Setup:

Month Day Year Hour Min.
 Start time August 21 2007 20 10
 End time September 3 2007 1 11

Execute Reset

Time zone: GMT-05:00 Cuba, East-Indiana, Eastern

Who group	On What group	When group	#Events	#Pol. Excp.	#Spec. Att	#Fail.
End User	Administration Objects	Out of Office Hours	3	3	0	0
IT	Administration Objects	Office Hours	75	0	0	0
IT	Administration Objects	Out of Office Hours	2	0	2	0
IT Admin	Administration Objects	Office Hours	75	0	0	0
IT Admin	Administration Objects	Out of Office Hours	2	0	2	0
System	Administration Objects	Out of Office Hours	3	3	0	0
Users	Administration Objects	Out of Office Hours	3	3	0	0

Figure 11-56 Review of user access rights (9.2.4)

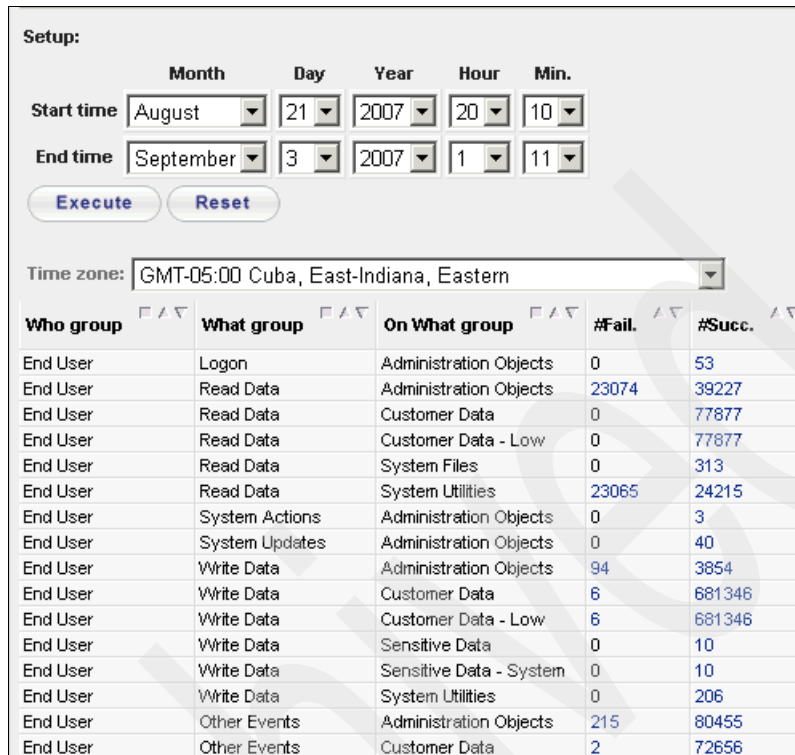


Figure 11-57 System access and use (9.2.4c)

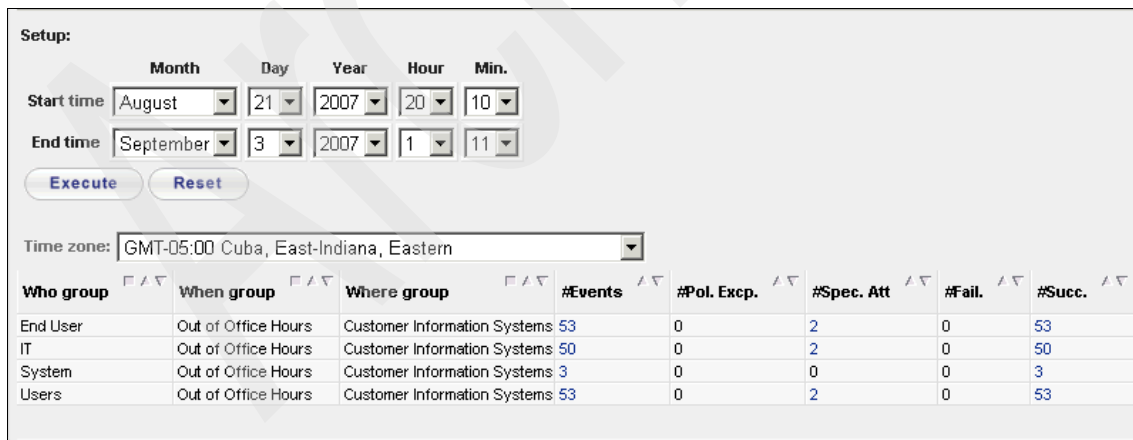


Figure 11-58 User responsibilities and password use (9.3)

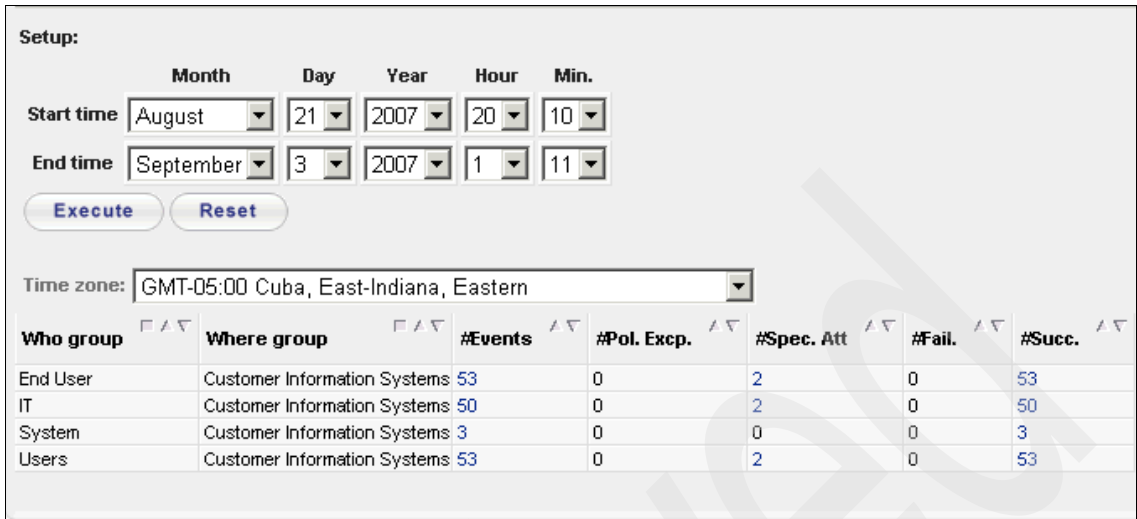


Figure 11-59 User identification and authentication (9.5.3)

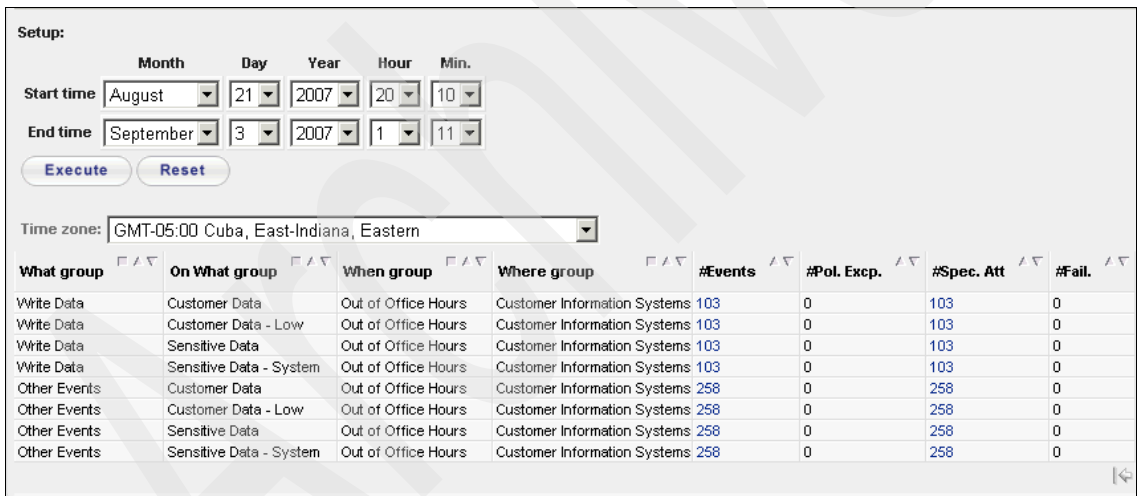


Figure 11-60 Application access control (9.6)

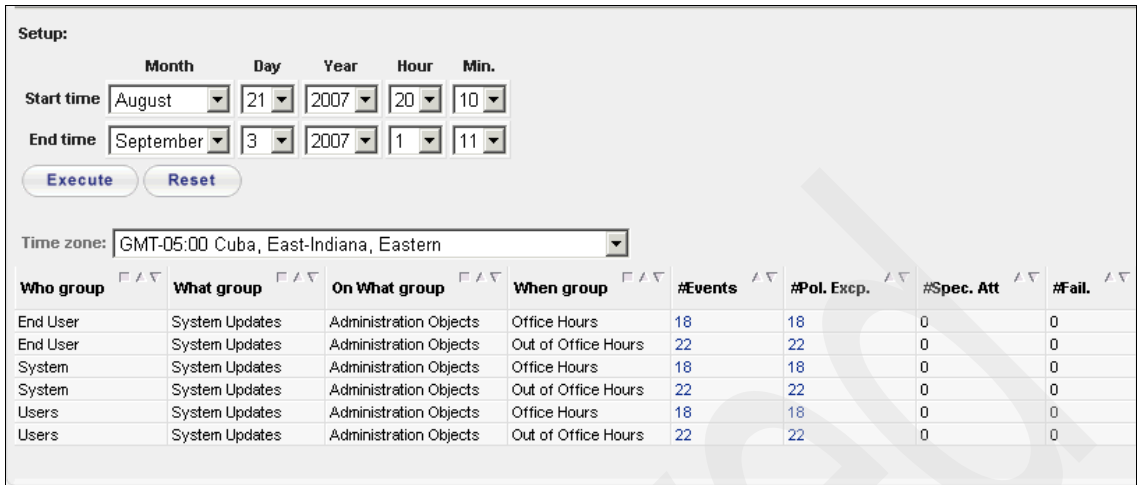


Figure 11-61 Control of operational software (10.4.1)

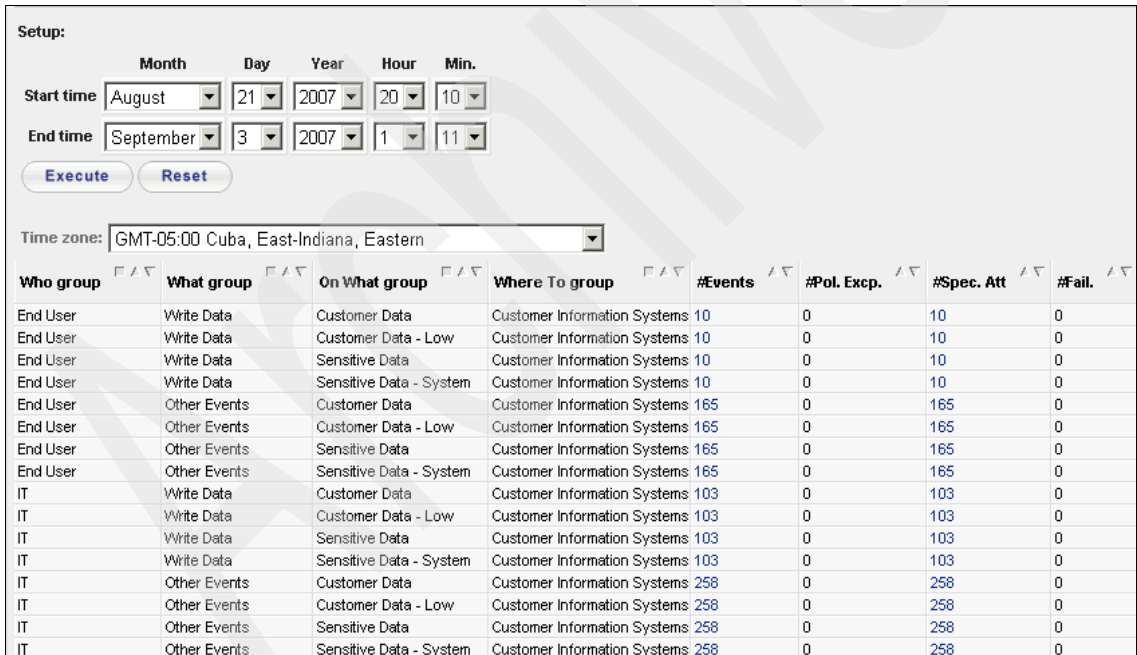


Figure 11-62 Data access (12.1.4)

Committing

We are satisfied with the reports and want to put them into *automatic mode*. To schedule System z audit data load with Basel II policy:

1. Re-enable the load schedule for the FinanceDP database, as shown in Figure 11-63.

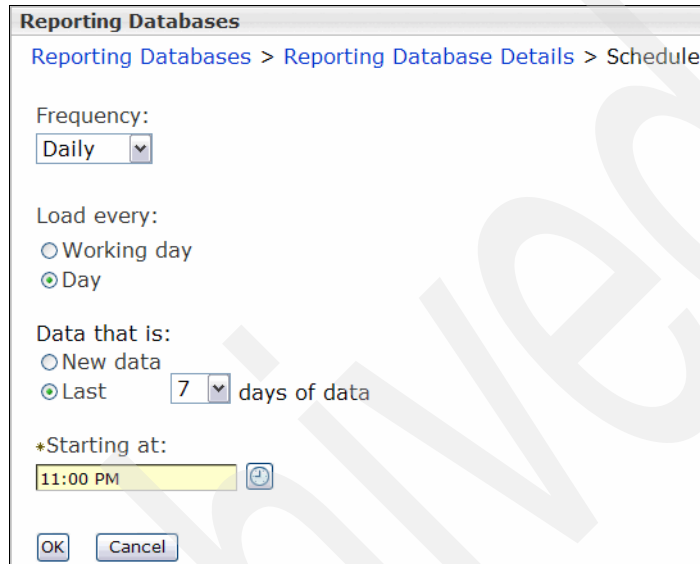


Figure 11-63 Re-enable load schedule

2. Commit the Basel II policy, to be used for subsequent scheduled loads, as shown in Figure 11-64 on page 350.

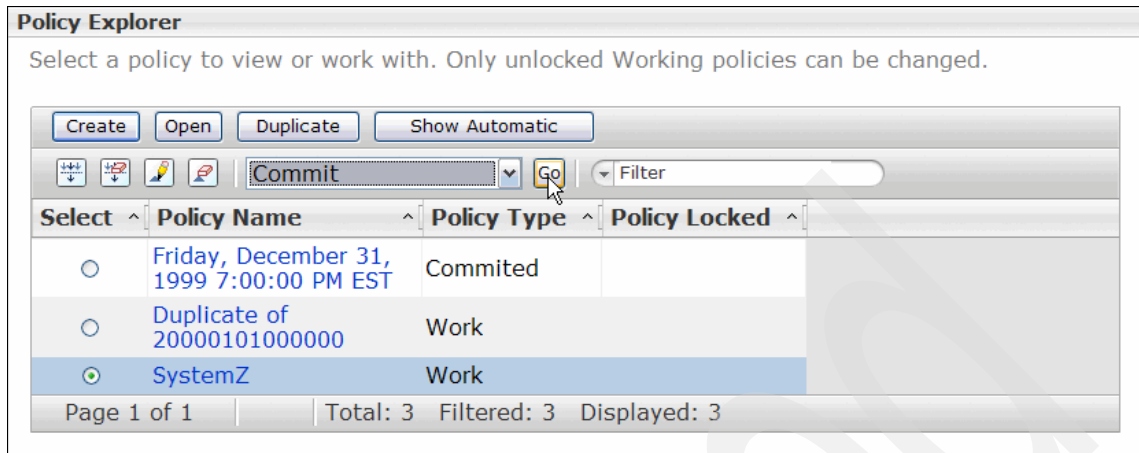


Figure 11-64 Commit policy

This concludes the implementation and Basel II compliance management report section.

11.4 Conclusion

Demonstrating a proper understanding of operational risk is a critical aspect of the complying with the Basel II regulation. In today's business environment, IT security is a critical component of operational risk management. IT security manages a growing number of operational controls and is a repository for evidence of operational incidents, so it becomes critical for IT security to support risk management in its Basel II compliance efforts, which requires implementing a series of mechanisms to monitor, measure, and control risks and incidents. This close interaction between risk management and IT security not only accelerates regulatory compliance but also significantly improves the effectiveness of operational risk management through the enterprise.

X-Y-Z effectively defined and produced Basel II compliance reports for its System z environment, and showed that the controls are in place, active and working.

Custom event source integration

In this chapter, we describe the process to support a new event source. Tivoli Security Information and Event Manager supports more than 300 types of platforms, applications, databases, and network devices that are available in the market. However, in many field deployments there are applications that were modified or developed solely by an organization's developers to achieve specific business needs. Those, so called, in-house applications typically need to demonstrate IT security compliance and be audited. To comply with this requirement Tivoli Security Information and Event Manager offers three different mechanisms to support those *custom event sources*:

- ▶ Ubiquitous event source
- ▶ W7 Log event source
- ▶ Generic ExtendIT event source

We discuss the differences between the three methods and how to create a custom event source and their pros and cons.

We develop two custom event sources for the scenario explained in Chapter 7, "Compliance management design" on page 131, where two of the business requirements are to add support for the QUANTWAVE back office and Web application and add support for the QUANT application.

12.1 Introduction to custom event sources

In this section, we discuss the differences between officially supported event sources and custom event sources.

12.1.1 Event source definition

An *event source* is any source of audit records that describe events that occurred on the system that you plan to monitor. Tivoli Security Information and Event Manager provides support for more than 300 different event source types. When an event source is part of this list you can consider such an event source as officially supported by IBM as a Tivoli Security Information and Event Manager event source.

12.1.2 Custom event source definition

There might be two types of *custom event sources*:

Customized The functionality was changed compared to the one that IBM officially released.

Custom IBM did not release the event source.

You cannot claim official support from IBM, if at least one of these two custom event sources applies.

To process audit records from a particular event source Tivoli Security Information and Event Manager must accomplish the following steps:

1. Collect the audit records from the event source (this step is called *collect*).
2. Parse the audit records. Identify only those values relevant or security related.
3. Map those data values into normalized GEM events.
4. Assign GEM events to normalized groups.
5. Manage the audit records in different locales.

To simplify the understanding, we summarize this process into three main steps:

- ▶ Collect
- ▶ Map
- ▶ Group

Note: While deploying custom event sources, take into account that they might be overwritten by upgrades or fixpack installations.

12.2 Ubiquitous event source

Using the Tivoli Security Information and Event Manager *ubiquitous event source* family you can collect log files from any file-based log sources. Ubiquitous event sources eliminate the necessity for supplying special Tivoli Security Information and Event Manager add-ons for specific platforms, for example, ubiquitous event sources can be used to audit ubiquitous text-based log files that produce a single log record per line. Such files can be collected and retrieved from the Tivoli Security Information and Event Manager Log Management Depot using the Log Retrieval Tool.

The following ubiquitous event sources are provided with Tivoli Security Information and Event Manager:

- ▶ Ubiquitous log

The event source collects files that are locally accessible to a Tivoli Security Information and Event Manager server or agent.

- ▶ Ubiquitous through SSH

The event source collects files from a UNIX or Linux machine through an SSH connection.

- ▶ Ubiquitous log syslog from syslog host

The event source collects *syslog messages* from locally accessible files to a Tivoli Security Information and Event Manager Server or Agent.

- ▶ Ubiquitous syslog receiver

The event source collects real-time *syslog messages* that a Tivoli Security Information and Event Manager server or agent receives.

- ▶ Ubiquitous SNMP receiver

The event source collects real-time *SNMP traps* that a Tivoli Security Information and Event Manager server or agent receives.

Tivoli Security Information and Event Manager provides a forensic investigation capability of the ubiquitous event source collected data. Each line from the audit trail is regarded as a single field. The audit records can be separated into different fields. To do that, you must provide suitable parse rules (GSL code). See the *IBM Tivoli Security Information and Event Manager Version 2.0 Users Guide*, SC23-9689, for more information about how to use ubiquitous event sources.

Important: Ubiquitous event sources do not allow the loading of collected chunks in Reporting Databases. If Tivoli Security Information and Event Manager attempts to load this type of collected data into a Reporting Database, the Reporting Database issues an error. In other words, a ubiquitous event source does not have compliance reporting capabilities through the Compliance Dashboard. However, the data is being securely stored in the Depot, and it can be searched and analyzed using the Forensic tool that is available on a Log Manager Server or an Enterprise Server, and audit trails can also be retrieved.

12.3 W7Log event source

In this section, we describe how the *W7Log event source* is used to add support for various platforms to Tivoli Security Information and Event Manager.

With the W7Log event source, Tivoli Security Information and Event Manager provides support for any software that produces log data running on IBM AIX or any supported Microsoft Windows operating system. This support gives you the ability to collect custom log files. Also, you can map and load data that is available in either *.csv* or *.xml* formats.

To be accepted into the W7Log, the log data must be mapped to a special W7 format. Tivoli Security Information and Event Manager provides tools to validate the format of the adapted log file, which is important, because the mapping process fails if the adapted log file is not in the correct format.

12.3.1 W7Log configurations

Tivoli Security Information and Event Manager can monitor platforms using one of the two following configurations:

- ▶ The adapted log data to be audited is located on a system other than the server. With this, Tivoli Security Information and Event Manager can monitor more than one platform within the network using an agent on each of the monitored systems.
- ▶ The adapted log data to be audited is located on the same system as the Tivoli Security Information and Event Manager Server.

Prerequisites

There are a few conditions that must be satisfied before a platform can be audited by Tivoli Security Information and Event Manager:

- ▶ A Tivoli Security Information and Event Manager server must be up and running.
- ▶ For a system that is not a Tivoli Security Information and Event Manager Server, the agent software must be installed on that system and it must be ensured that the agent is up and running. On this system, there must be system administrator credentials and a working TCP/IP network connection.

For details about how to install the agent, refer to the *IBM Tivoli Security Information and Event Manager Version 2.0 Installation Guide*, GI11-8778.

The log data to be audited must be in the required format and placed on the system to be audited.

Log data requirements

All log files that need to be processed must be placed in a separate designated directory. The path to the directory must be specified in the event source property log files location using the following steps:

1. Under Configuration and Management in the left pane, click **Event Source Management**.
2. In the left pane, the window with all event sources is displayed. Click **QUANTWAVE** to open the event source for our scenario. The Event Source Properties window opens, as shown in Figure 12-1.

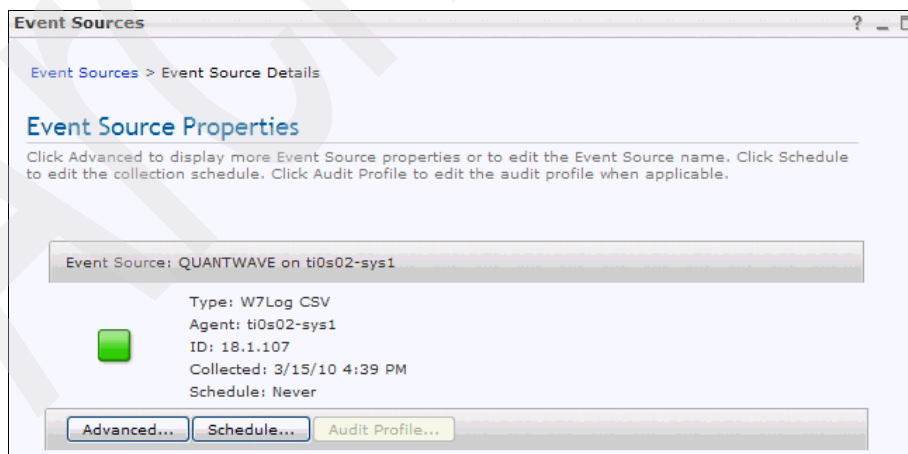


Figure 12-1 Event Source Properties

3. To define the log files location, click **Advanced**. A dialog displays the properties of the event source and allows you to define further advanced properties:
 - Audited Machine
The system that is being monitored. This is a read-only value.
 - Agent
A host where the Tivoli Security Information and Event Manager component (agent or server, if the platform is located on the server), which collects events from this event source, is installed. This is a read-only property and is defined when the event source is created.
 - Type
The event source type, which is either in the *.csv* format or the *.xml* format. This also is a read-only property.
 - Log files location
The path to the adapted log files. There is no default value for this property; instead, you must specify one.

Important: Every *batch collect* deletes all log files from the designated directory, which is specified in the event source property log files location.

- Platform Type
The name of the W7Log platform type. Use the default value W7Log-CSV or W7Log-XML depending on the type of event source that you configured to audit the W7Log platform.
- Text encoding for audit trail
For further information about which values can be entered in this field, refer to the *IBM Tivoli Security Information and Event Manager Version 2.0 Event Source Guide*, SC23-9687. For our scenario, enter UTF-8, which is the Eight-bit UCS Transformation Format.
- Language code for audit trail
Specifies the language code of the text data for collected log data sets. The default value is an empty string, which indicates that the event source must automatically determine the language used for the collected data. Further information about language codes can be obtained from the *Tivoli Security Information and Event Manager Version 2.0 Event Source Guide*, SC23-9687.

Figure 12-2 shows you the entries for advanced event source properties for our scenario.

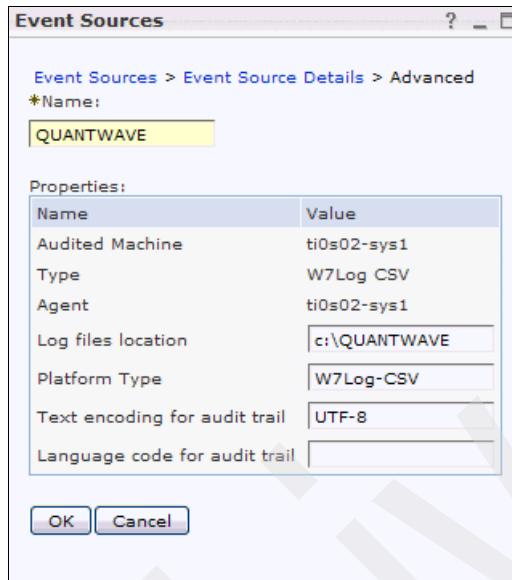


Figure 12-2 Defining advanced properties for event sources

All log files are deleted from the designated directory after they are processed by Tivoli Security Information and Event Manager. Therefore, a backup copy of the logs must be stored in some other directory.

As pointed out, each log file in the designated directory must be in a valid *.csv* or *.xml* format. Also, each log file in the designated directory must contain only complete records. Log records must be written in UTF-8 encoding and during creation of log records, contents of different log files must not overlap.

12.3.2 Transforming Quantwave log files into a valid W7Log format

First, we must discuss mapping the fields that are in the Quantwave log files into the *W7Log .csv format*. This format is the same as Microsoft Excel CSV, which is a file format that is used as a portable representation of a database. Each line represents one entry or record, and the fields in a record are separated by commas or any other delimiter. Blank lines are always ignored.

The header line must list field names, separated by commas in a fixed order, exactly as follows (as a single line):

when,whorealname,whologonname,whatverb,whatnoun,whatsuccess,wheretype,

wherename,wherefromtype,wherefromname,wheretotype,wheretaname,
onwhattype,onwhatpath,onwhatname,info

Record fields can be empty or have only spaces; however, use a single dash (-) for empty values. The size of record fields is not checked. However, the log producer must satisfy the requirements.

Description of W7Log validator log fields

Fields that are used in log records that the W7Log validators generate have the meanings that Table 12-1 shows. The W7Log format requires that the .csv file contains all of the fields and in the order they are listed in the table.

Table 12-1 W7Log log fields

Field Name	Field Description	Value
when	Time, when event occurred. This field is defined as: YYYY-MM-ddTHH:mm:ss:s	<ul style="list-style-type: none"> ▶ YYYY: The year in the Gregorian calendar ▶ MM: The month number (1-12) ▶ dd: The day number (1-31) ▶ T: The literal separator between date and time ▶ HH: The hours number (0-23) ▶ mm: The minute number (0-59) ▶ ss: The second number (0-59) <p>Optional values are fractional seconds in one-to-three decimals.</p>
whorealname, whologonname	Platform-dependent logon ID and logon name of the user who initiated the event. The name of the system process or application can be specified here instead of the name of the actual user.	Defined as arbitrary string values of up to 64 bytes each.

Field Name	Field Description	Value
whatverb, whatnoun, whatsuccess	<p>The triplet of values that indicate what kind of action the event represents:</p> <ul style="list-style-type: none"> ▶ The <i>verb</i> is an action type (for example, logon, create, and so on). ▶ The <i>noun</i> is the refinement of the action type (for example, user, file, and so on). ▶ The value of <i>success</i> can be either <i>success</i> or <i>failure</i>, depending on how the action was run. 	<p>For <i>whatverb</i> and <i>whatnoun</i> an arbitrary string of up to 20 characters.</p> <p>For <i>whatsuccess</i> an arbitrary string of up to eight characters.</p>
wheretype, wherename	<p>The platform (type and name) where the event happened. Examples are "SUN Solaris" or "GATEWAY", and so on.</p>	<p>For <i>wheretype</i> an arbitrary string of up to 20 characters.</p> <p>For <i>wherename</i> an arbitrary string of up to 128 characters.</p>
wherefromtype, wherefromname	<p>Platform (type and name) of the event's origin platform. Examples are "Internet", "192.168.103.104", and so on.</p>	<p>For <i>wherefromtype</i> an arbitrary string of up to 20 characters.</p> <p>For <i>wherefromname</i> an arbitrary string of up to 128 characters.</p>
wheretotype, wheretomname	<p>Platform (type and name) of the event's target platform. Examples are "Microsoft Windows", "WORKSTATION", and so on.</p>	<p>For <i>wheretomtype</i> an arbitrary string of up to 20 characters.</p> <p>For <i>wheretomname</i> an arbitrary string of up to 128 characters.</p>

Field Name	Field Description	Value
onwhattype, onwhatpath, onwhatname	The triplet of values that indicate what object was involved. Examples are file, database, printer, and so on.	<ul style="list-style-type: none"> ▶ <i>onwhattype</i> groups all objects according to some platform-specific event type as an arbitrary string of up to 20 bytes. ▶ <i>onwhatpath</i> groups all objects of the same type into separate names spaces (or directories) as an arbitrary string of up to 110 bytes. ▶ <i>onwhatname</i> identifies objects within each name space (or directory) as an arbitrary string of up to 110 bytes.
info	Provides additional information about an event, for example, you can use this field to provide hyperlinks to external internet resources.	This field is a text field of up to 3900 characters.

We now must map the Quantwave log file contents into the W7Log file format. The Quantwave log file is delimited by tabs and contains 21 fields in the following order:

ID - DOMAIN - SUB_DOMAIN - NAME - USERID - ACTION - START_TIME - DBMS_START_TIME - ELAPSED_TIME - ROW_COUNT - HTTP_USER_AGENT - HTTP_REMOTE_ADDRESS - URL - INFORMATION - LANGUAGE - KEY_1 - KEY_2 - KEY_3 - KEY_4 - KEY_5 - SUBSCRIBER_ID

We do not need all of these fields for the scenario. However, some are important and are listed in Table 12-2.

Table 12-2 Mapping of Quantwave log file into W7Log log file format

W7Log	Quantwave Log File
when	START_TIME
whorealname	USERID
whologonname	USERID
whatverb	see separate table

W7Log	Quantwave Log File
whatnoun	see separate table
whatsuccess	see separate table
wheretype	'-' (a hyphen)
wherename	DOMAIN
wherefromtype	'-' (a hyphen)
wherefromname	HTTP_USER_AGENT
wheretotype	'-' (a hyphen)
wheretname	'-' (a hyphen)
onwhattype	SUB_DOMAIN
onwhatpath	NAME up to the last '/'
onwhatname	NAME from the last '/' to the end
info	The complete record

There might be some cases, where a field in the Quantwave log file does not have an entry. Because the W7Log file format does not accept blank entries, these then must be filled with a '-' (a hyphen).

As outlined in Table 12-1 on page 358, there is a triplet of values that indicates the kind of action the event represents. From scanning the Quantwave log file we identified, that there are eight different actions:

- ▶ Logon
- ▶ Logout
- ▶ Create
- ▶ Delete
- ▶ Edit
- ▶ Execute
- ▶ Search
- ▶ View

We will now map these actions into the W7Log file fields *whatverb*, *whatnoun*, and *whatsuccess*, as shown in Table 12-3 on page 362.

Table 12-3 The “what”-table

ACTION	whatverb	whatsnoun	whatsuccess
Logon	Logon	User	Success
Logout	Logout	User	Success
Create	Add	Model	Success
Delete	Delete	Model	Success
Edit	Modify	Model	Success
Execute	Execute	Model	Success
Search	Search	Data	Success
View	Read	Model	Success

We now fully mapped all Quantwave log file entries into the W7Log file format. The next step is to parse the Quantwave log file contents into a .csv file, which then can be loaded into the Tivoli Security Information and Event Manager.

12.3.3 Creating external event logs into the W7Log file format

With the mapping that we discussed, you can now create a W7Log file in one of the two formats described in “Log data requirements” on page 355. For the scenario in this book, we use a comma separated file (.csv file) that can be loaded into Tivoli Security Information and Event Manager. We use Tivoli Directory Integrator to help us with this. In the following sections, we explain the necessary steps to accomplish this task. You can also refer to the *IBM Tivoli Director Integrator Users Guide, SC23-6561*.

To create external logs into the W7Log file format:

1. Open a workspace, which we call *worksp*. The workspace represents a folder on your computer system, where all data of this project is stored.
2. Create a project in Tivoli Directory Integrator. We call this project *QUANTWAVE*. Figure 12-3 on page 363 shows what the project QUANTWAVE in Tivoli Directory Integrator looks like right after its creation.

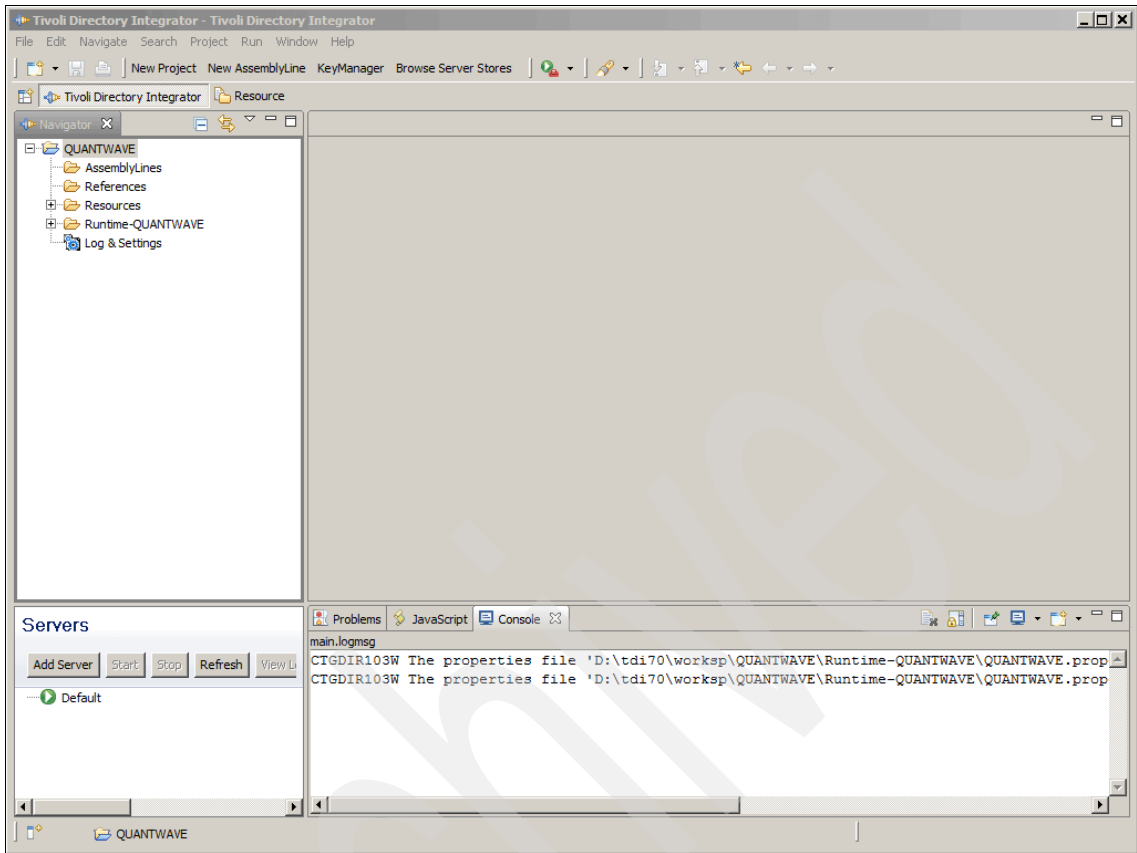


Figure 12-3 Project QUANTWAVE created in Tivoli Directory Integrator

3. The Quantwave log file that we received is called *QuantwaveData.txt*. In this scenario, the file is placed in a folder called *data* within the *QUANTWAVE* project. This file can actually be anywhere on the file system and does not need to be in the workspace location. However, this is one way to manage the artifacts that Tivoli Directory Integrator consume and produce. Figure 12-4 on page 364 shows where the file on the file system is located.

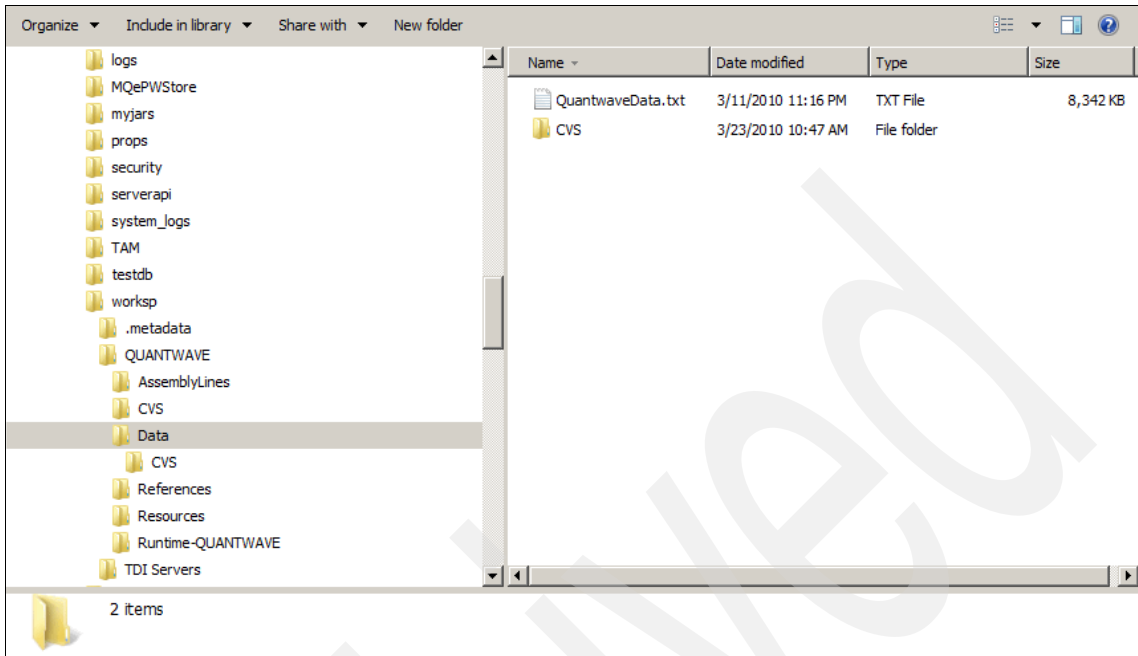


Figure 12-4 Quantwave log file copied to workspace

4. When developing Tivoli Directory Integrator solutions you will often reference information, such as path names, user names, or passwords. Best practice is to store this data in an external properties file. Add properties to the *QUANTWAVE* project and upload them to the server. Figure 12-5 on page 365 shows the properties that must be created for this particular project.

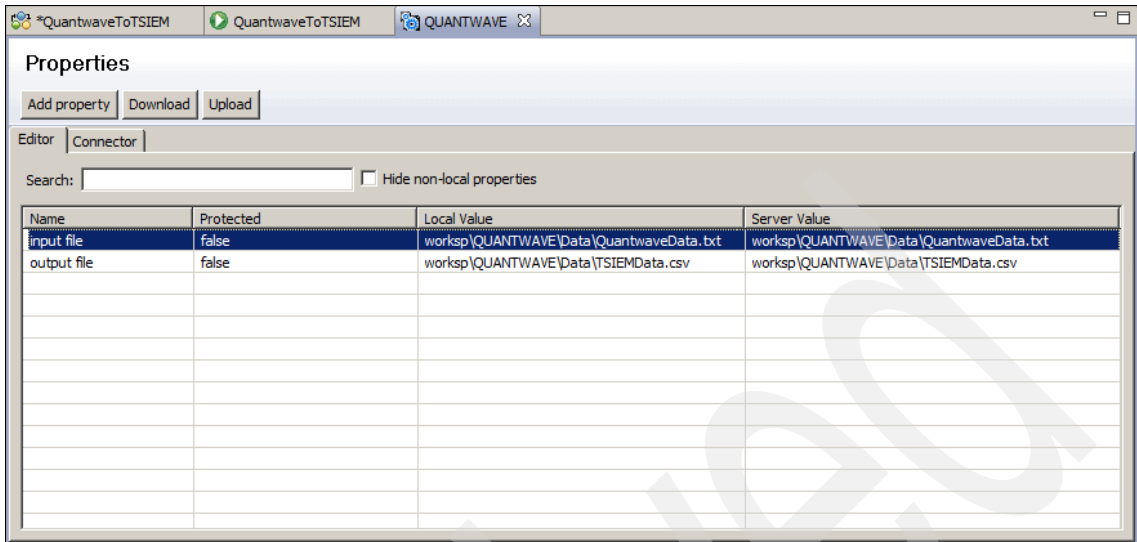


Figure 12-5 Added and uploaded properties of the QUANTWAVE project

5. The next step is to create an *AssemblyLine*, which is a set of components that are strung together to move and transform data. It describes the *route* along which the data passes. The data that is being handled through that journey is represented as an *Entry object*. The AssemblyLine processes with a single *work entry* at a time on each cycle of the AssemblyLine. An AssemblyLine represents a flow of information from one or more data sources to one or more targets. Figure 12-6 shows the created AssemblyLine for the *QUANTWAVE* project.

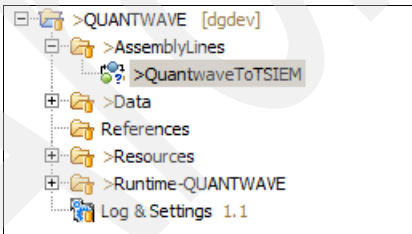


Figure 12-6 AssemblyLine for QuantwaveToTSIEM

6. In Figure 12-7 on page 366, you see that we create a *Connector* from the *File System Connector* template. By clicking **Next**, you are prompted to define the file path, the input file, and to select a *parser*.

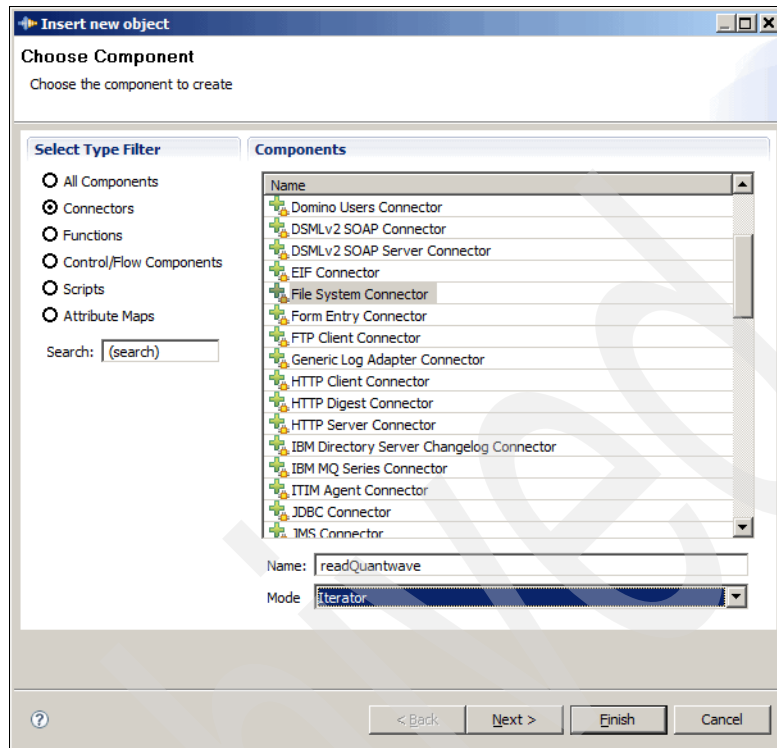


Figure 12-7 Creating the File System Connector in Tivoli Directory Integrator

7. Read the first line of the Quantwave log file, which describes the field names and the order of the fields in the input (log) file. Select all of the schema attributes, and drag them with the mouse onto the left side to map them to the *work attributes*. Figure 12-8 on page 367 shows this step.

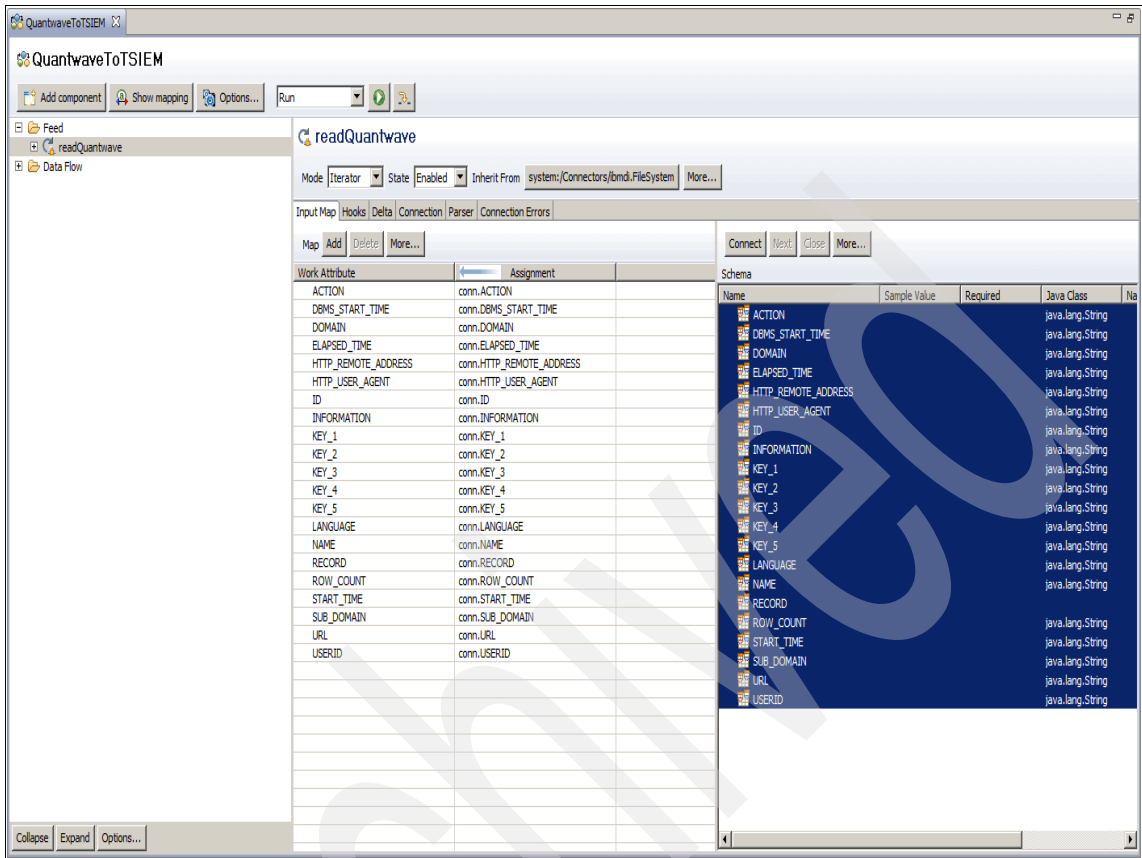


Figure 12-8 Mapping the schema attributes to the work attributes in Tivoli Directory Integrator

- For the reports that must be created, we do not need all fields from the Quantwave log file. However, we want to keep the entire record for possible future expansion of the reports, which is why we store the entire record in the *info* field of the W7Log file format. For that reason, you must create a field, called *Record*, to the schema, and map it to *work*. To capture this record field, create another File System Connector called *readQuantwaveRecord Connector*. This connector is in a passive state. We call it from JavaScript code in the *After GetNext Hook* of the *readQuantwaveRecord Connector* (see Figure 12-9 on page 368).

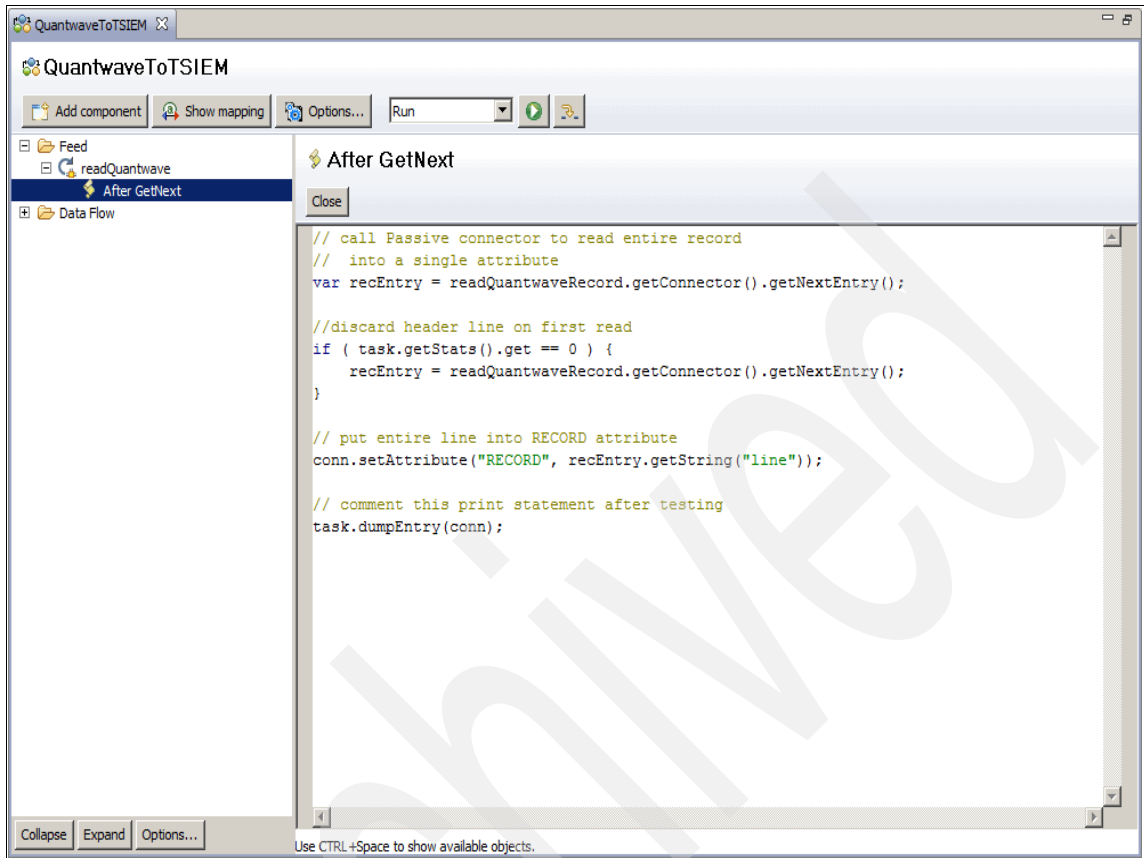


Figure 12-9 Added code to readQuantwaveRecord Connector

9. Add and configure the *writeTSIEM Connector* with a CSV parser and a field separator to “,”. Add the list of field names to the *Advanced* configuration section of the parser, as shown in Figure 12-10 on page 369. These fields must be in the correct order of the W7Log file format to be able to be read from Tivoli Security Information and Event Manager.

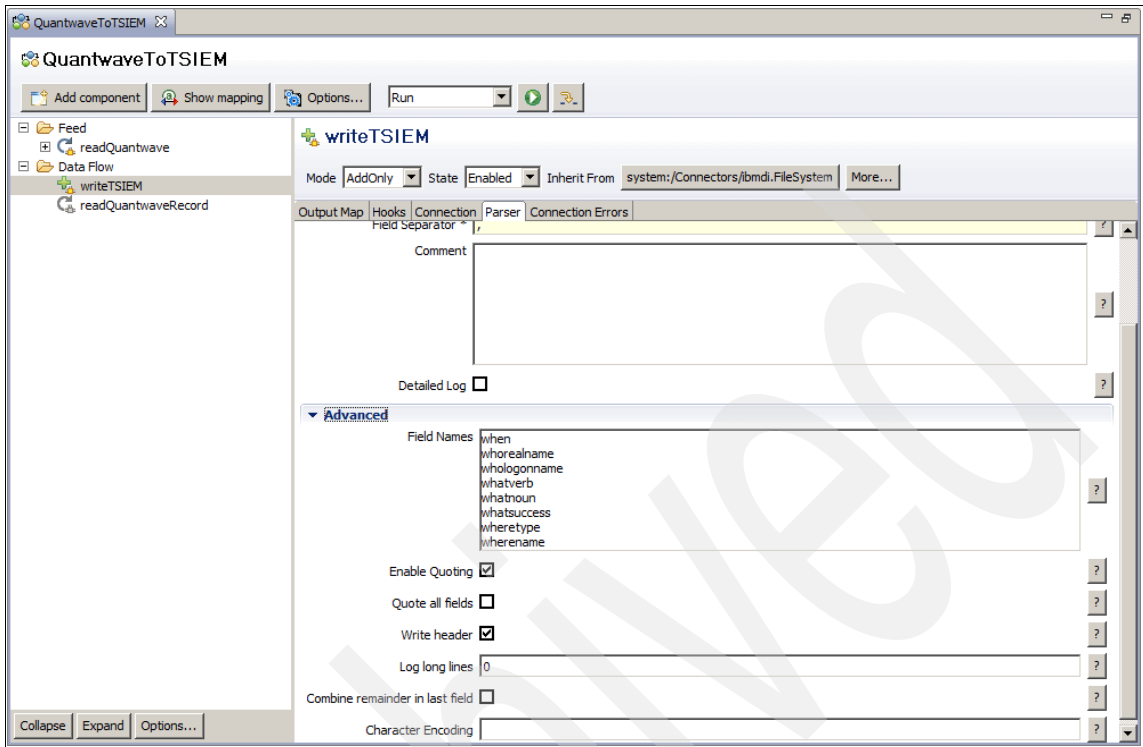


Figure 12-10 The Advanced configuration section of the parser in Tivoli Directory Integrator

10. Figure 12-11 on page 370 shows the window after you drag the work attributes from `readQuantwave` to `writeTSIEM`.

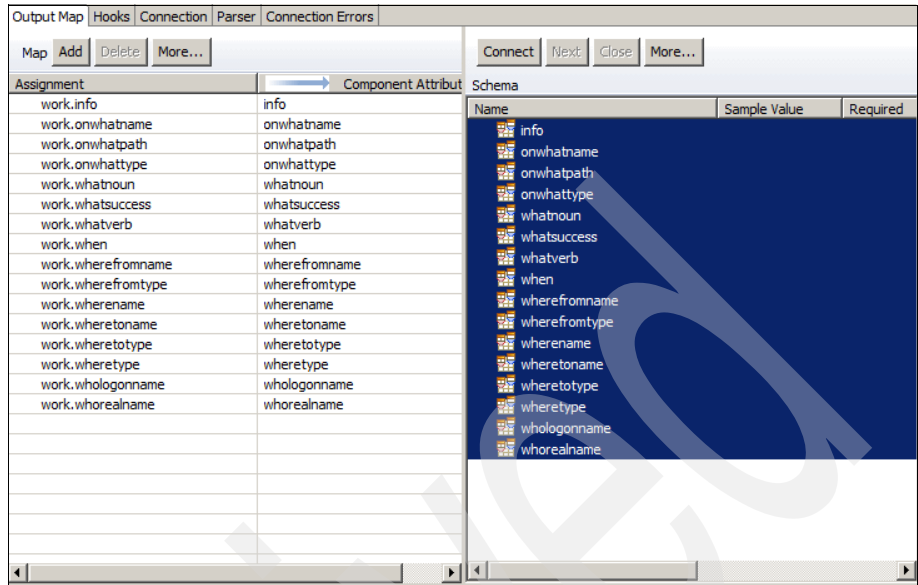


Figure 12-11 Dragging the attributes from readQuantwave to writeTSIEM

11. Complete the detailed mapping, as defined in Table 12-2 on page 360 and Table 12-3 on page 362. Figure 12-12 on page 371 shows the detailed work for the detailed mapping for the *onwhatname* field. You must do this process for each field that the W7Log file format requires.

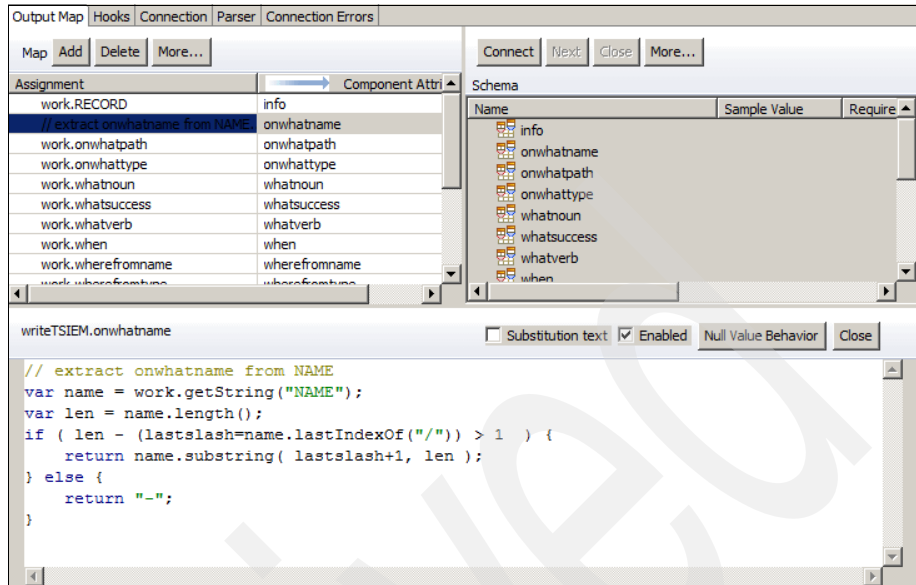


Figure 12-12 Detailed mapping work for the field onwhatname

Figure 12-13 on page 372 shows the detailed work for the data that is explained in Table 12-3 on page 362.

```
/*
   define objects for calculating whatverb, whatnoun and whatsuccess from ACTION
   The AL reads and processes this before executing any iterations
*/

var whatverb = new java.util.HashMap();
whatverb.put("logon","Logon");
whatverb.put("logout","Logoff");
whatverb.put("create","Add");
whatverb.put("delete","Delete");
whatverb.put("edit","Modify");
whatverb.put("execute","Execute");
whatverb.put("search","Search");
whatverb.put("view","Read");

var whatnoun = new java.util.HashMap();
whatnoun.put("logon","User");
whatnoun.put("logout","User");
whatnoun.put("create","Model");
whatnoun.put("delete","Model");
whatnoun.put("edit","Model");
whatnoun.put("execute","Model");
whatnoun.put("search","Data");
whatnoun.put("view","Model");

// whatsuccess is always Success for any non-null action
```

Figure 12-13 Detailed mapping of the fields *whatverb* and *whatnoun*

12. You completed the definition work and are ready to run a first test. In the AssemblyLine settings, set the number of maximum reads to 1, and run the test. Figure 12-14 on page 373 shows the result with which you can examine the test output.

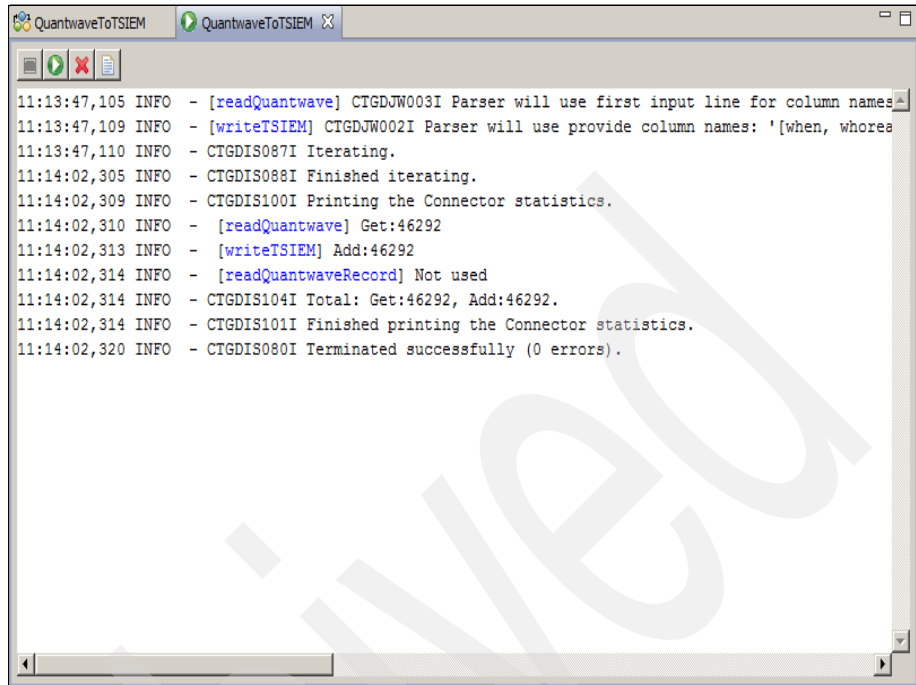
```

QuantwaveToTSIEM  QuantwaveToTSIEM
11:12:28,182 INFO - [readQuantwave] CTGDJW003I Parser will use first input line for column names.
11:12:28,185 INFO - [writeTSIEM] CTGDJW002I Parser will use provide column names: '[when, whorealname, whologonname, wh
11:12:28,188 INFO - CTGDIS087I Iterating.
11:12:28,192 INFO - CTGDIS003I *** Start dumping Entry
11:12:28,193 INFO - Operation: generic
11:12:28,196 INFO - Entry attributes:
11:12:28,200 INFO - KEY_4 (replace): ''
11:12:28,202 INFO - KEY_3 (replace): ''
11:12:28,213 INFO - HTTP_USER_AGENT (replace): '127.0.0.1'
11:12:28,221 INFO - DOMAIN (replace): 'wwc'
11:12:28,226 INFO - KEY_2 (replace): ''
11:12:28,228 INFO - KEY_1 (replace): '226283760132'
11:12:28,228 INFO - HTTP_REMOTE_ADDRESS (replace): ''
11:12:28,230 INFO - SUB_DOMAIN (replace): 'user'
11:12:28,231 INFO - NAME (replace): 'A000000'
11:12:28,231 INFO - URL (replace): ''
11:12:28,232 INFO - LANGUAGE (replace): '11613'
11:12:28,232 INFO - ID (replace): '60169831'
11:12:28,233 INFO - START TIME (replace): '10/10/2002 10:04:06 AM'
11:12:28,233 INFO - DBMS_START_TIME (replace): ''
11:12:28,235 INFO - USERID (replace): 'A000000'
11:12:28,235 INFO - RECORD (replace): '60169831 wwc user A000000 A000000 login 10/10/2002 10:04:06 AM'
11:12:28,236 INFO - INFORMATION (replace): 'us'
11:12:28,237 INFO - ROW_COUNT (replace): 'Mozilla/4.0'
11:12:28,238 INFO - ACTION (replace): 'login'
11:12:28,240 INFO - ELAPSED_TIME (replace): '0'
11:12:28,240 INFO - KEY_5 (replace): '1'
11:12:28,253 INFO - CTGDIS004I *** Finished dumping Entry
11:12:28,257 INFO - CTGDIS091I Ending AssemblyLine after reaching maximum number of entries to read: 1.
11:12:28,262 INFO - CTGDIS100I Printing the Connector statistics.
11:12:28,263 INFO - [readQuantwave] Get:1
11:12:28,265 INFO - [writeTSIEM] Add:1
11:12:28,266 INFO - [readQuantwaveRecord] Not used
11:12:28,267 INFO - CTGDIS104I Total: Get:1, Add:1.

```

Figure 12-14 Test result examination in Tivoli Directory Integrator

13. If the test was not successful, check your settings again until the test result is satisfactory. Next, run the completed AssemblyLine, which produces the output file as a .csv file and shows run statistics, as shown in Figure 12-15 on page 374.



```
11:13:47,105 INFO - [readQuantwave] CTGDJW003I Parser will use first input line for column names
11:13:47,109 INFO - [writeTSIEM] CTGDJW002I Parser will use provide column names: '[when, whores
11:13:47,110 INFO - CTGDIS087I Iterating.
11:14:02,305 INFO - CTGDIS088I Finished iterating.
11:14:02,309 INFO - CTGDIS100I Printing the Connector statistics.
11:14:02,310 INFO - [readQuantwave] Get:46292
11:14:02,313 INFO - [writeTSIEM] Add:46292
11:14:02,314 INFO - [readQuantwaveRecord] Not used
11:14:02,314 INFO - CTGDIS104I Total: Get:46292, Add:46292.
11:14:02,314 INFO - CTGDIS101I Finished printing the Connector statistics.
11:14:02,320 INFO - CTGDIS080I Terminated successfully (0 errors).
```

Figure 12-15 Run the completed AssemblyLine

12.3.4 Importing external event logs

In the previous section, we described how the Quantwave log files are mapped against the W7Log file format and how an adapted .csv file can be created using Tivoli Directory Integrator. In this section, we show how to get this transformed log file data into Tivoli Security Information and Event Manager, as outlined in the following steps:

1. Click **Managing Reporting Databases** in the left pane of the Tivoli Security Information and Event Manager Web portal to list all databases on the right side of the window, as shown in Figure 12-16 on page 375.

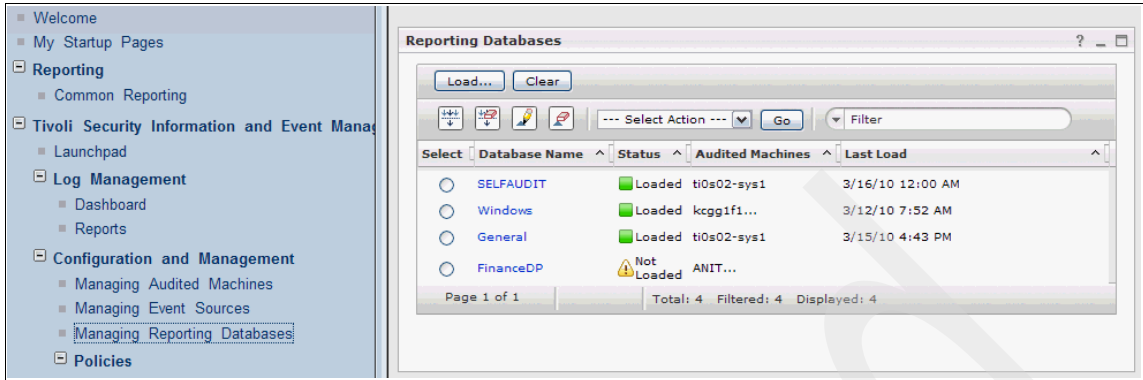


Figure 12-16 Managing Reporting Databases window

- For our scenario, we select the General database. Figure 12-17 shows the window with the properties of the QUANTWAVE database that we selected. It shows that we already loaded the data from the .csv file into the Tivoli Security Information and Event Manager.

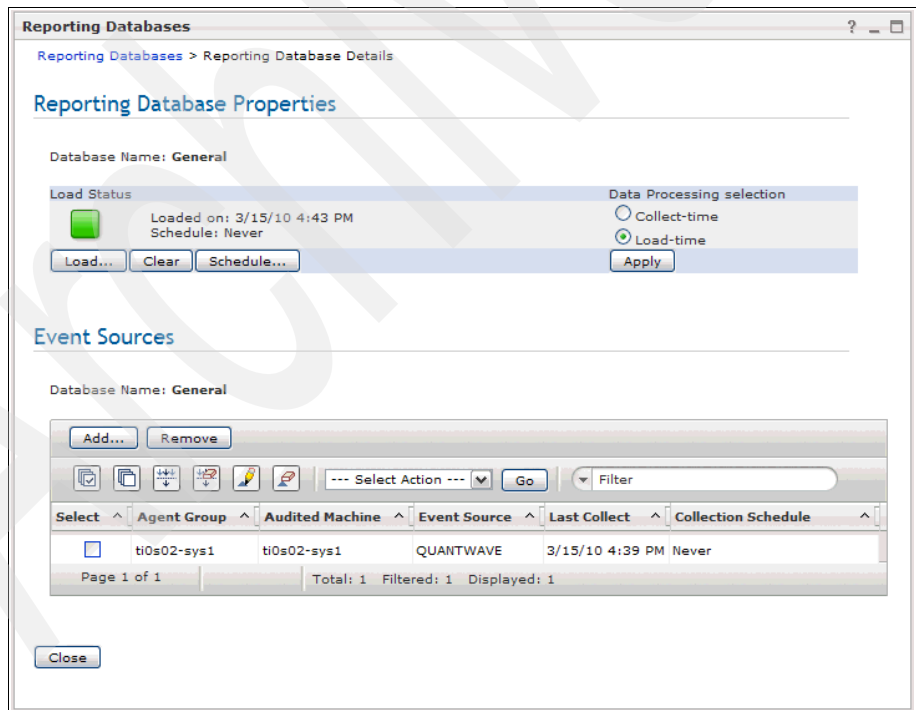


Figure 12-17 The properties of the selected scenario database QUANTWAVE

- The next few steps show how you can proceed if you need to load a new .csv file into Tivoli Security Information and Event Manager. Click **Load** to start the Load Database Wizard, which is shown in Figure 12-18.

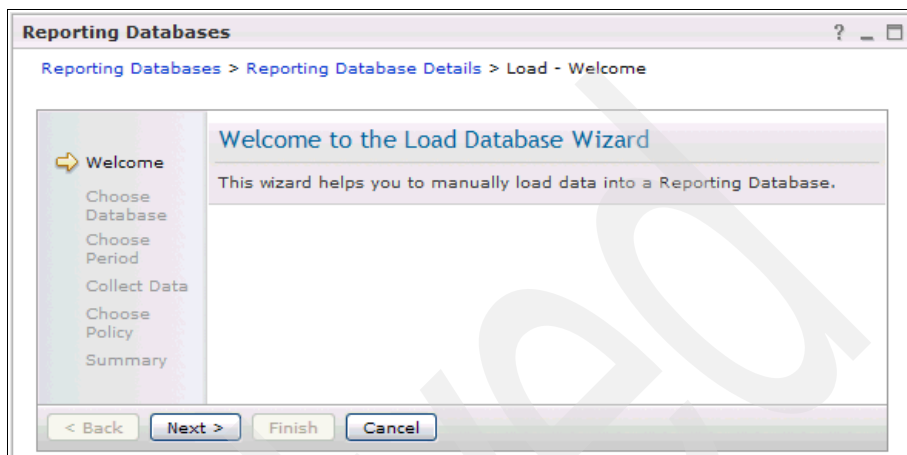


Figure 12-18 The Load Database Wizard

- Click **Next** to choose the General database, as shown in Figure 12-19.

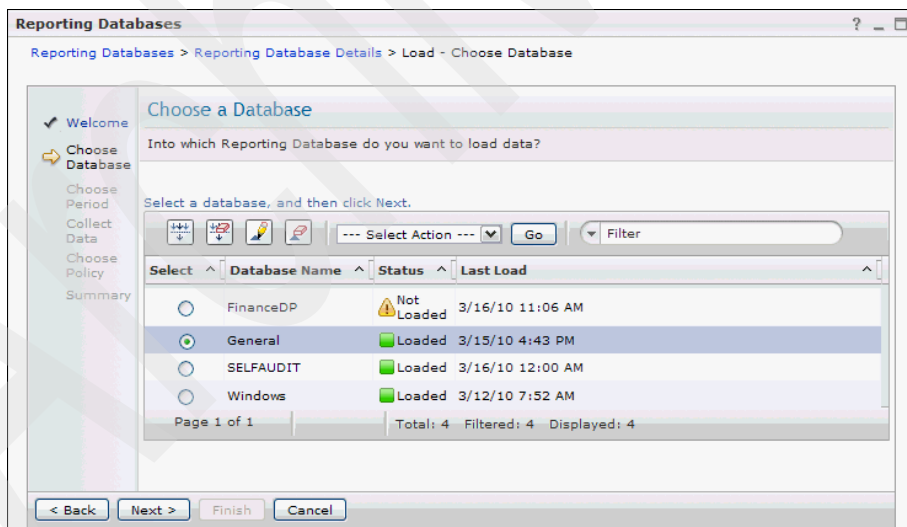


Figure 12-19 Choosing a database

- Click **Next** to choose a period of time from which the data must be loaded, as shown in Figure 12-20 on page 377.

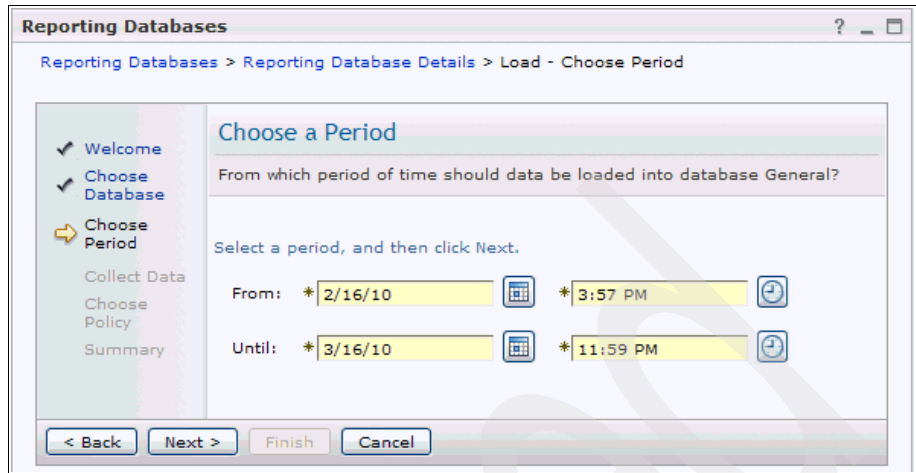


Figure 12-20 Choosing a time period

After clicking **Next**, you can choose from two options:

- a. Yes, collect the data first
- b. No, just load the database

For our scenario, we select the first option, as shown in Figure 12-21.

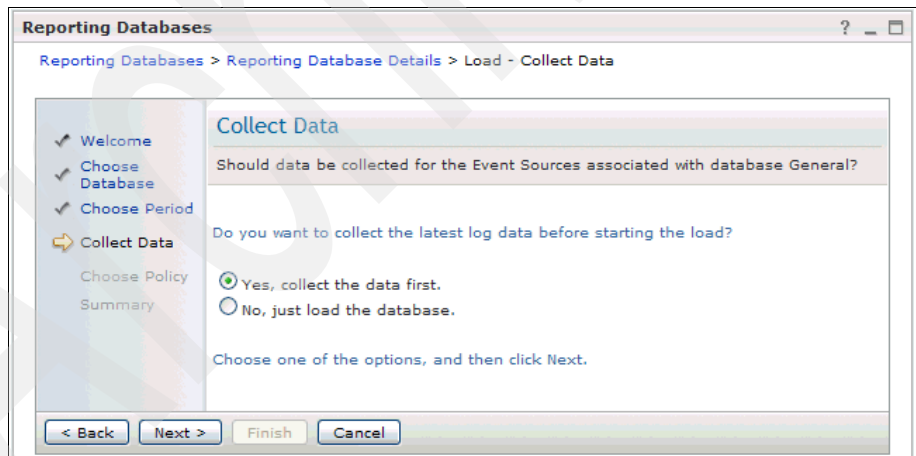


Figure 12-21 Options menu for collecting data

6. Click **Next** to choose which policy applies to the data loaded into the database. Three options are available, as shown in Figure 12-22 on page 378:
 - Matching: The policy that matches best the selected time period.

- Newest: The latest committed policy.
- Fixed: An explicit choice from one of the options shown in a separate window.

Click **Next**.

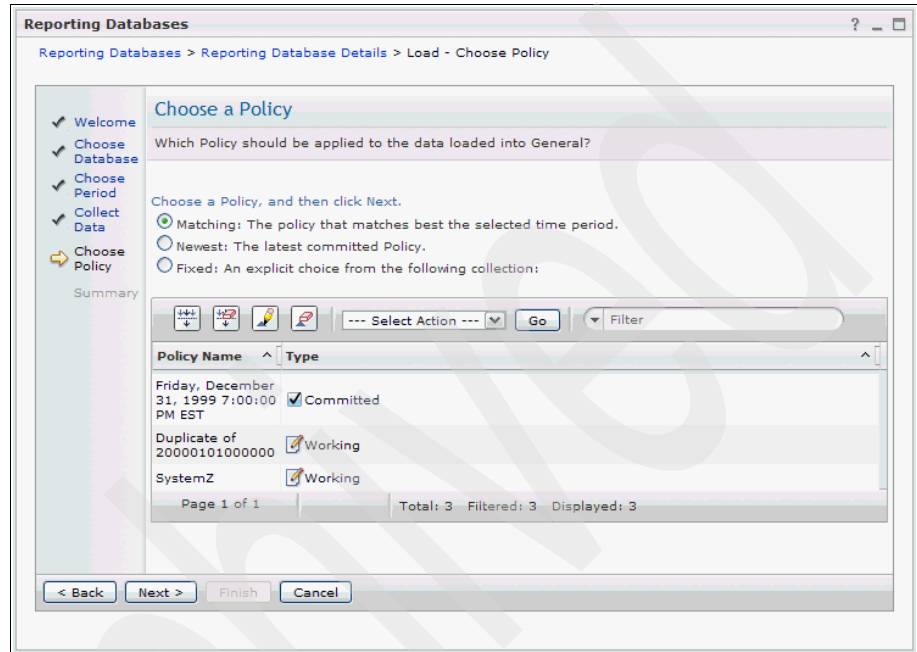


Figure 12-22 Choosing a policy for the data to be loaded

A summary of the definition you just made is displayed, as shown in Figure 12-23 on page 379.

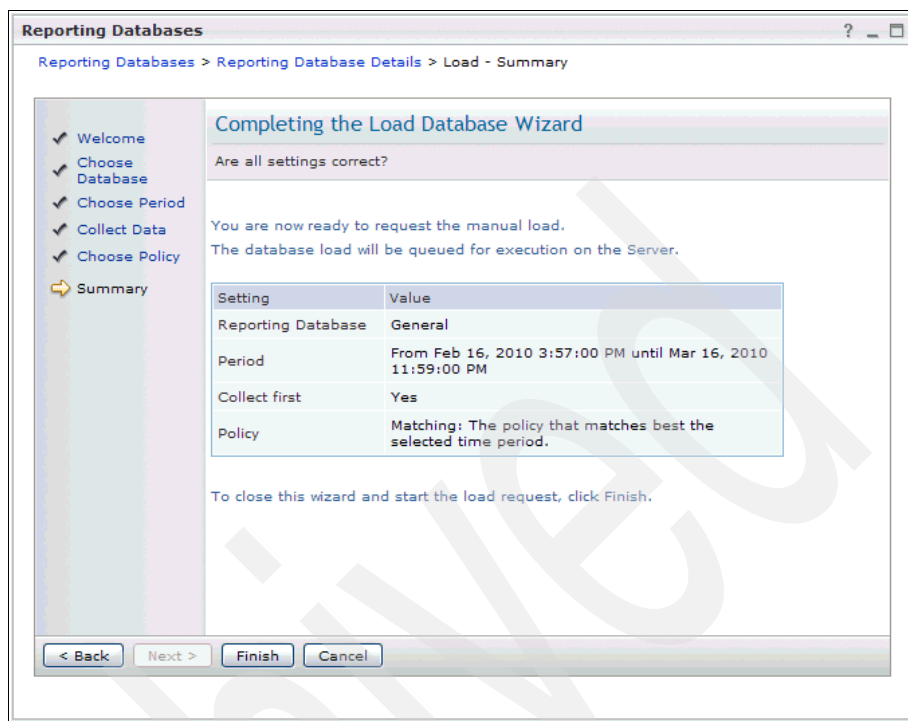


Figure 12-23 Summary page of input for loading external log files

7. Click **Finish** to start the import. After the import finishes, you can create your own reports or use the data on predefined reports.

Log file validation tools

Tivoli Security Information and Event Manager provides tools to validate correct log data format. For both adapted formats, there is one tool available:

- ▶ W7Log CSV Validator tool
- ▶ W7Log XML Validator tool

Both tools are operating-system independent diagnostic tools that are intended for third parties to check the validity of proposed CSV or XML log data for W7Log event sources that are provided in one of the two formats.

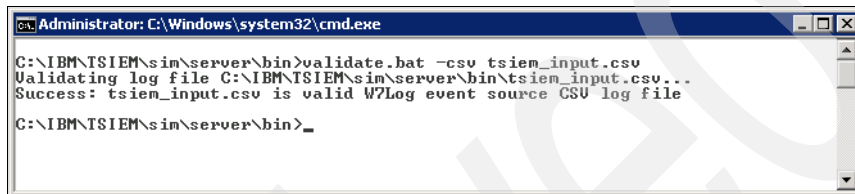
Important: Neither the W7Log CSV Validator nor the W7Log XML Validator check for log data for empty fields or fields that contain only blanks. It is important to not use such values in the log files.

For further information about how to install, configure, and use the validator tools, refer to the *IBM Tivoli Security Information and Event Manager Version 2.0 Event Source Guide*, SC23-9687.

The tool is executed from the `/IBM/TSIEM/sim/server/bin` directory with one of the following parameters:

- ▶ `-csv`: This parameter checks input files with a *.csv file* format.
- ▶ `-xml`: This parameter checks input files with a *.xml file* format.

You also must enter the name of the input file. In Figure 12-24, we show the result of a validation run of a *.csv* file format input file with no errors returned.



```
Administrator: C:\Windows\system32\cmd.exe
C:\IBM\TSIEM\sim\server\bin>validate.bat -csv tsiem_input.csv
Validating log file C:\IBM\TSIEM\sim\server\bin\tsiem_input.csv...
Success: tsiem_input.csv is valid W7Log event source CSU log file
C:\IBM\TSIEM\sim\server\bin>_
```

Figure 12-24 Correct output of a validation run

Tip: The data that we used for this scenario is located in the files that can be downloaded from the IBM Redbooks publications Web page. Refer to Appendix B, “Additional material” on page 411.

12.4 The Generic ExtendIT event source

Using the *Generic ExtendIT event sources* you can collect, parse, and map log files that are not supported by any other standard event source. The Generic ExtendIT event source type contains no built-in collecting or mapping functionality. You must provide that functionality using scripts. Generic ExtendIT can be considered the most flexible custom event source type; however, all of the functionality must be developed within the organization or within IBM services.

Before you start to work on a Generic ExtendIT event source, make sure you gained experience in the following areas:

- ▶ Any scripting or compiled language: Can help you write a collect script to pull and handle the audit trails from the event source.
- ▶ General Scanning Language (GSL) and Generic Mapping Language (GML): You need to parse and map the collected audit trails from the event source.
- ▶ Event source technical details: Which type of events are important or security related.

Generic ExtendIT event sources can be developed for the following agent operating systems: HP-UX, IBM AIX, IBM i (formerly i5/OS®, OS/400®), IBM z/OS, Microsoft Windows, Sun Solaris.

Let us now talk about the details for your Generic ExtendIT event source development:

- ▶ The collect script
- ▶ Reusing existing collect scripts
- ▶ The mapper files
- ▶ Grouping files
- ▶ Example of Generic ExtendIT event source

12.4.1 The collect script

When a new data collection is requested for an event source, the Tivoli Security Information and Event Manager server or agent execute an appropriate *collect script* that is expected to return the collected data in specified files. For supported event sources, IBM provides a collect script that is appropriate for that event source. For Generic ExtendIT event sources, you must specify which collect script to use.

You can use any scripting language (batch files, VBScript, Perl, shell scripts, and so on) or compiled language (Java, C, C++, and so on).

Parameters passed to the main collect script

The collect script is called with a fixed set of parameters, which are provided as properties of the event source in the form of options. The script can call any number of other scripts, as needed.

In practice, the main collect script often is a shell script that calls (third-party) tools with the right subset of parameters to gather the data, especially if multiple audit logs must be collected from the same audited system.

Collect script parameters 1 to 4

The first four parameters let you specify the names of four temporary files in which the collect script must return the collected data from up to four different kind of related log files. The names must be specified relative to the current working directory. It is allowed to use fewer than four temporary files, but the file names that will be ignored must be at the end of the list of four.

Audit data that is of a different type and that cannot be handled by the same set of parse rules must be stored in different temporary files. Likewise, audit data that is of the same type must be stored in the same temporary file even if it was

initially stored in separate files on the target system, for example, if the target system stores its audit data in a new file every day, the collect script must identify audit data from all new audit data files and store it in a single temporary file.

Collect script parameters 5 to 12

These parameters provide eight free-form options that can be used to guide the collection, for example, you can specify the location of the data of interest or credentials that are needed to access that data. The collect script is not required to use any of these eight parameters.

Collect script parameter 13

This parameter defines the name of a state file that is unique to the event source instance. No two event source instances can use the same state file name. This name is useful for defining locations to store instance-specific information that must not be touched, even by other instances of the same event source type that use the same collect script.

Tivoli Security Information and Event Manager server or agent do not actually create the state file, and the collect script is not required to use the name. The state file is typically used to store state information that helps the next collect process avoid collecting the same data again.

Return value

A return value of 0 (zero) from the collect script means that all newly available audit data is successfully stored in temporary files. If there was no new audit data available, the expected temporary files must exist but might be empty. Tivoli Security Information and Event Manager takes the temporary files and turns them into sublogs in a chunk.

A non-zero return value from the collect script means that an error occurred and that no audit data is stored in the temporary files. In that case, Tivoli Security Information and Event Manager does not create a data chunk and reports the problem in the *Compliance Dashboard*. It also writes the error into the Tivoli Security Information and Event Manager logs.

Regardless of the return value, the Tivoli Security Information and Event Manager agent or server deletes the original temporary files after first copying them into a data chunk, if appropriate.

Collect script requirements

There are three requirements a collect script must fulfill:

- ▶ The collect script and any other scripts or tools that the collect script calls must run without any user interaction. Thus, it must never ask for any user input or generate pop-up windows.
- ▶ The collect script must ensure that all data is collected *exactly one time*. The recommended way to achieve this is to store some relevant collect progress information in the state file, as described in “Collect script parameter 13” on page 382. The script must initialize the collect process using the contents of the state file, and write updated information to the state file upon completion. This process must take into account the most recently collected data.
- ▶ All collect scripts must be placed into the `bin` directory of the Tivoli Security Information and Event Manager server or agent on which it runs. For a server on Microsoft Windows, which is installed into the default location, this directory is at `C:\IBM\TSIEM\sim\server\bin`. The collect script is executed in the `run` directory (`../run` relative to the `bin` directory mentioned before) of the server or agent. To avoid any problems, the collect script must not change the current working directory.

12.4.2 Reusing existing collect scripts

Collect scripts that are already written for supported event sources can be reused. It is recommended to set up a proper lab environment and run tests before placing scripts on production systems.

Let us take a closer look and explain the parameters of two existing collect scripts that are currently used by supported event sources.

The `getnewrecs.bat` collect script

This Microsoft Windows batch file retrieves lines that added to a set of logs since the previous run. It assumes that at any time there is only one single active file to which new records get added. After the logging switches to a new active file, the old file is not modified anymore. State information is stored in the registry.

As with all collect scripts, it returns `0` if the collect process was successful and non-zero otherwise. To run this collect script, type:

```
getnewrecs.bat out i1 i2 i3 label logdir pattern
```

Let us check out the parameters.

out	The name of the output file (temporary file) to produce.
i1, i2, i3	Three arguments that are ignored.

label	A unique label that can be used to keep apart state information for different event source instances in the registry. Use the state file name as shown in “Collect script parameter 13” on page 382 for this.
logdir	The directory containing the log files to check for new data.
pattern	A file name pattern that identifies the logs to check for new data. If all of the files in the <i>logdir</i> should be checked, then * can be used for the <i>pattern</i> .

getnewrecs.sh

This UNIX shell script retrieves lines added to a set of logs since the previous run. It assumes that at any time there is only a single active file to which new records get added. After the logging switches to a new active file, the old file is not modified anymore.

As with all collect scripts, it returns 0 if the collect process was successful, and non-zero otherwise. To run this collect script, type:

```
getnewrecs.sh out label logdir pattern state
```

Let us check out the parameters:

out	The name of the output file (temporary file) to produce.
label	A unique label that can be used to keep apart information for different event source instances in the same state file. If each event source instance uses its own <i>state</i> file (for example, by basing <i>state</i> on \${PROPSFILE}), the <i>label</i> can be a fixed value.
logdir	The directory that contains the log files to check for new data.
pattern	A regular expression that identifies the logs to check for new data. If all of the files in the <i>logdir</i> must be checked, .* can be used for the <i>pattern</i> .
state	The name of a state file in which information can be stored that identifies the data that was collected, so the next run will not collect those records again. Use the state file name, as shown in “Collect script parameter 13” on page 382 for this.

12.4.3 The mapper files

After the data is collected from the event source, we must process that data. This process is divided in two parts:

- ▶ Parsing
- ▶ Mapping

Parsing

Audit records come in many different types. Some examples are:

- ▶ Binary
- ▶ Text with one line per record
- ▶ Text with multiples per record
- ▶ Free-format text
- ▶ Text in columns
- ▶ And so on

To understand the different formats in the audit records Tivoli Security Information and Event Manager uses *Log Sources* and *scanners*, which can understand the format of the audit trail and will send this to the *GSL*.

The *GSL* file discards audit records that are not relevant and identifies those audit records that are security related.

A specific set of *Log Sources*, *Scanners*, and *GSL* are used for specific platforms.

The parsing process converts audit records into a stream of *platform events* that are sent to the next phase—*mapping*.

A platform event is a set of key-value pairs that describe the important information that is extracted from an audit record, which was done in the *parsing* phase, and the contents of a platform event are determined by the *GSL*.

Important: To write the *GSL* code for a Generic ExtendIT event source or to customize a supported event source *GSL*, you must understand the audit trail of the audited system and differentiate which events are relevant and which type of data to be discarded.

GSL files are located in the \run folder of the Tivoli Security Information and Event Manager server file system.

Mapping

The mapping phase converts *platform events* into Reporting Database (GEM) Events that are loaded into a Reporting Database. The mapping phase is governed by GML.

A GEM event contains items for the different Reporting Database dimensions according to the W7 Model.

Important: To write GML code for a Generic ExtendIT event source or to customize a supported event source GML you must fully understand the W7 model and GEM Events.

GML files are located in the \run folder of the Tivoli Security Information and Event Manager server file system.

12.4.4 Grouping files

Tivoli Security Information and Event Manager policy rules are defined in terms of GEM Groups. Each GEM (W7) dimension has its own set of GEM Groups.

For a Generic ExtendIT event source, one empty group can be created and based on the information in the Compliance Dashboard we can start to build the grouping file. For instructions about how to handle grouping files, refer to the *IBM Tivoli Security Information and Event Manager Version 2.0 Administrators Guide*, SC23-9688.

12.4.5 Example of Generic ExtendIT event source

For this example, we create support for the QUANT application using a Generic ExtendIT event source.

To accomplish this task we must complete the following steps:

1. Analyzing the audit log.
2. Creating the collect script.
3. Preparing the mapper configuration.
4. Creating the mapper configuration file.
5. Adding the event source.
6. Creating the grouping file.
7. Validating results in the Compliance Dashboard.

Analyzing the audit log

Example 12-1 shows the format of the original log from QUANT.

Example 12-1 Original log output from QUANT

```
Date,Time,AccessDevice,User-Name,Acct-Flags,service,Portname,IP-Address
,QUANT Server,Real Name,Description
3/18/2009,0:01:49,DB2inst\Payroll,DB2Admin,change,shell,tty2,10.26.44.1
24,Q01NTRV,db2 admin,DB2 Administrator
3/19/2009,0:01:55,DB2inst\Payroll,jeremy,change,shell,tty2,10.26.44.125
,Q01NTRV,Jermy,Operator
3/20/2009,0:01:56,DB2inst\Temp,Franco,erase,,tty2,10.26.44.126,Q01NTRV
,Franco,Operator
3/21/2009,0:02:01,DB2inst\HR,Mercy,change,shell,tty2,10.26.44.127,Q01NTRV
, Mercy,Operator
3/22/2009,0:08:15,DB2inst\Temp,Silvia,erase,shell,tty2,10.26.44.128,Q01
NTRV,Silvia,Assistant
3/23/2009,0:08:15,DB2inst\Temp,Patty,erase,,tty2,10.26.44.129,Q01NTRV,
Patty,Assistant
3/24/2009,0:08:15,DB2inst\Temp,ExternalUser,erase,shell,tty2,10.26.44.1
30,Q01NTRV,External User,HelpDesk
3/25/2009,0:15:02,DB2inst\Temp,Contractor,erase,shell,tty2,10.26.44.131
,Q01NTRV,Contractor,HelpDesk
```

Additional information: The original log uses a header to specify the data fields, and each record within the log uses a “,” (comma) to separate those fields. By looking at the original log, we can think about how we are going to translate these fields into W7 dimensions.

Creating the collect script

We use a Windows-based script that is named `getquantlogs.bat` to copy the content of the `audit.log` file located in the folder `c:\Application`. The collect process transforms the content of `audit.log` file into a chunk.

In Example 12-2, we show the content of the collect script.

Example 12-2 Collect script

```
@rem Retrieve event source properties
set TempFile1=%1%
set TempFile2=%2%
set TempFile3=%3%
set TempFile4=%4%
set Option1=%5%
set Option2=%6%
```

```

set Option3=%7%
set Option4=%8%
set Option5=%9%
shift
set Option6=%9%
shift
set Option7=%9%
shift
set Option8=%9%
shift
set Props=%9%
@rem Set progress log name; base on %Props%
@rem to make it unique.
set log=..\log\%Props%
echo %DATE%^ ^%TIME% Start collect >> %log%
echo Using event source properties:
echo Temporary file 1 = %TempFile1% >> %log%
echo Temporary file 2 = %TempFile2% >> %log%
echo Temporary file 3 = %TempFile3% >> %log%
echo Temporary file 4 = %TempFile4% >> %log%
echo >> %log%
echo Option 1 = %Option1% >> %log%
echo Option 2 = %Option2% >> %log%
echo Option 3 = %Option3% >> %log%
echo Option 4 = %Option4% >> %log%
echo Option 5 = %Option5% >> %log%
echo Option 6 = %Option6% >> %log%
echo Option 7 = %Option7% >> %log%
echo Option 8 = %Option8% >> %log%
echo State file: %Props% >> %log%
@rem Invoke an executable for every sublog
echo %DATE%^ ^%TIME% Collect 1st log >> %log%
@rem Remove remnants of previous collect
del %TempFile1%
@rem Collect the whole 'Option 1' file
copy %Option1% %TempFile1%
echo %DATE%^ ^%TIME% End of collect >> %log%
@set errorlevel=0

```

The collect script must be placed in the C:\IBM\TSIEM\sim\server\bin directory.

Preparing the mapper configuration

We use a GSL file to parse the data, a GML file to map it, and a mapper configuration file named `quant.ini` to serve as a point of reference for both GSL and GML.

GSL file

We create a GSL file called `quant.gsl` and save it in the `\run` folder on the Tivoli Security Information and Event Manager server. Example 12-3 shows the structure of the GSL format that understands the original log.

Example 12-3 Structure of the GSL format

```
[table: HeaderLineSource, name, value]
separator = ","
[node: base]
$time = value+Date,lit+" ",value+Time,setflexibletime+default
objectname|m = lit+"-"
objecttype = lit+DBTABLE"
objectpath = value+Access_Device
realname = value+Real_Name
username = value+User_Name
platformname = value+QUANT_Server
platformtype = lit+"QUANT Server"
srcplatformname = value+IP_Address
srcplatformtype = lit+"QUANT Client"
tgtplatformname = value+Access_Device
tgtplatformtype = lit+"QUANT Device"
[item: base.start, value+Acct_Flags="change"]
$type = settype+"start acc"
eventmainclass = lit+"Modify"
eventclass = lit+"DBTable"
successclass = lit+"Success"
[item: base.stop, value+Acct_Flags="erase"]
$type = settype+"stop acc"
eventmainclass = lit+"Delete"
eventclass = lit+"DBTable"
successclass = lit+"Success"
[node: base.others]
### Indexed variables ###
[table: Indexer, oldname, newname]
eventclass = eventclass
eventmainclass = eventmainclass
objectpath = objectpath
objecttype = objecttype
platformname = platformname
```

```
platformtype = platformtype
realname = real_username
successclass = successclass
username = username
$time = platformenttime
objectnameIm = objectname
```

GML file

We create a GML file called `quant.gml` and save it in the `\run` folder on the Tivoli Security Information and Event Manager server. Example 12-4 shows the structure of the GML file that converts the *Platform Events* to *GEM Events* for our Quantum application.

Example 12-4 Structure of the GML file

```
key PlatformRefKey(platformname, platformtype)
key OriginRefKey(platformname, platformtype)
key TargetRefKey(platformname, platformtype)
key ObjectRefKey(objectname, objecttype, objectpath)
key SourceRefKey(logonname, realname)
key StreamRefKey(description)
key EventDetailKey(reason)
initial final state Quant
  platformname := Trim (Quant.platformname, "Unavailable")
  platformtype := Trim (Quant.platformtype, "Quant")
  platform := GetPlatform(PlatformRefKey)
  platformname := Trim (Quant.srcplatformname, "Unavailable")
  platformtype := Quant.srcplatformtype
  origin := GetOrigin(OriginRefKey)
  platformname := Trim (Quant.tgtplatformname, "Unavailable")
  platformtype := Quant.tgtplatformtype
  target := GetTarget(TargetRefKey)
  objecttype := Trim (Quant.objecttype, "*")
  objectpath := Trim (Quant.objectpath, "-")
  objectname := Trim (Quant.objectname, "-")
  object := GetObject(ObjectRefKey)
  logonname := Trim (Quant.username, "Unavailable")
  realname := Trim (Quant.realname, logonname)
  source := GetSource(SourceRefKey)
  description := Quant.platformname
  stream := GetStream(StreamRefKey)
  reason := Quant.reason
  eventmainclass := Quant.eventmainclass
  eventclass := Quant.eventclass
  successclass := Quant.successclass
```

```
eventtimestamp := Quant.platformeventtime
chunk := Quant
event := GetEvent(EventDetailKey)
endstate
```

Creating the mapper configuration file

The GSL and GML files use the mapper configuration file as a point of reference during the load process. The name must be something meaningful, in this case `quant.ini`, and it must be stored in the directory `C:\IBM\TSIEM\sim\server\config\mappers`. Example 12-5 shows the contents.

Example 12-5 Content of `quant.ini`

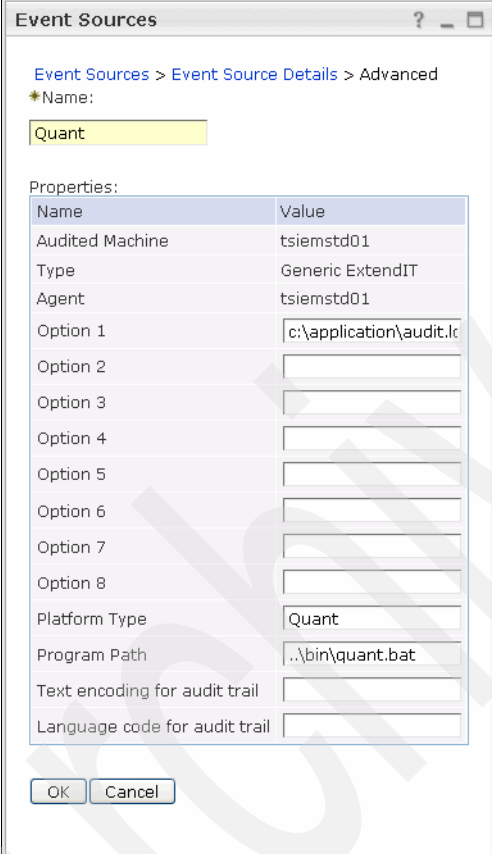
```
[platform:"Quant"]
pre_lm      = yes
grouping = quant_group.cfg
gml = quant.gml
sublogname#1 = Main audit log from quant
original#1 = 1
extension#1 = .log
logsource#1 = HeaderLineSource
scanner#1 = RegexListFile
gsl#1 = quant.gsl
original#1 = 1
```

Additional learning information: The path

`C:\IBM\TSIEM\sim\server\config\mappers` defines the repository for all of the configuration files for this Generic ExtendIT event source project. By looking at the files, you can gain experience and understand how the supported event sources are configured and which files are used to process the data.

Adding the event source

Now that collect script and mapper files are ready, we must add the event source. From the Tivoli Integrated Portal, we add a new event source, Generic ExtendIT type, and fill in the properties, as shown in Figure 12-25.



The screenshot shows a dialog box titled "Event Sources" with a breadcrumb trail: "Event Sources > Event Source Details > Advanced". The "Name" field is set to "Quant". Below this is a "Properties:" section with a table-like structure:

Name	Value
Audited Machine	tsiemstd01
Type	Generic ExtendIT
Agent	tsiemstd01
Option 1	c:\application\audit.lc
Option 2	
Option 3	
Option 4	
Option 5	
Option 6	
Option 7	
Option 8	
Platform Type	Quant
Program Path	..\bin\quant.bat
Text encoding for audit trail	
Language code for audit trail	

At the bottom of the dialog are "OK" and "Cancel" buttons.

Figure 12-25 Properties of Generic ExtendIT type

In Figure 12-25:

- ▶ Option 1 is the path for the original audit logs `c:\application\audit.log`
- ▶ Platform Type specifies the *Quant* name that we selected for the platform
- ▶ Program Path (`..\bin\quant.bat`) points to the file system location where we placed the collect script

Creating the grouping file

This task requires basic skills about *grouping manipulation*. For instructions, refer to the *IBM Tivoli Security Information and Event Manager Version 2.0 Administrators Guide, SC23-9688*.

Validating results in the Compliance Dashboard

To validate your newly created Generic ExtendIT event source you must perform a *collect*, and then *load* and *analyze* the results, as the depicted in Figure 12-26.

Database QuantWeb on Server CIFDB								
Setup:								
	Month	Day	Year	Hour	Min			
Start time	March	19	2010	18	5			
End time	March	19	2010	18	5			
Time zone:		Event time zone						
Severity	Date / Time	#	What (detail)	Where (detail)	Who (detail)	Where From (detail)	On What (detail)	Where To (detail)
10	3/19/10 6:05:48 PM (-0600)	1	Modify : DBTable / Success	Q01NTRSV (QUANT Server)	db2 admin	10.26.44.124 (QUANT Client)	DBTABLE : DB2instlPayroll / -	DB2instlPayroll (QUANT Device)
10	3/19/10 6:05:48 PM (-0600)	1	Modify : DBTable / Success	Q01NTRSV (QUANT Server)	Jermy	10.26.44.125 (QUANT Client)	DBTABLE : DB2instlPayroll / -	DB2instlPayroll (QUANT Device)
10	3/19/10 6:05:48 PM (-0600)	1	Delete : DBTable / Success	Q01NTRSV (QUANT Server)	Franco	10.26.44.126 (QUANT Client)	DBTABLE : DB2instlTemp / -	DB2instlTemp (QUANT Device)
10	3/19/10 6:05:48 PM (-0600)	1	Modify : DBTable / Success	Q01NTRSV (QUANT Server)	Mercy	10.26.44.127 (QUANT Client)	DBTABLE : DB2instlHR / -	DB2instlHR (QUANT Device)
10	3/19/10 6:05:48 PM (-0600)	1	Delete : DBTable / Success	Q01NTRSV (QUANT Server)	Silvia	10.26.44.128 (QUANT Client)	DBTABLE : DB2instlTemp / -	DB2instlTemp (QUANT Device)
10	3/19/10 6:05:48 PM (-0600)	1	Delete : DBTable / Success	Q01NTRSV (QUANT Server)	Patty	10.26.44.129 (QUANT Client)	DBTABLE : DB2instlTemp / -	DB2instlTemp (QUANT Device)
10	3/19/10 6:05:48 PM (-0600)	1	Delete : DBTable / Success	Q01NTRSV (QUANT Server)	External User	10.26.44.130 (QUANT Client)	DBTABLE : DB2instlTemp / -	DB2instlTemp (QUANT Device)
10	3/19/10 6:05:48 PM (-0600)	1	Delete : DBTable / Success	Q01NTRSV (QUANT Server)	Contractor	10.26.44.131 (QUANT Client)	DBTABLE : DB2instlTemp / -	DB2instlTemp (QUANT Device)

Figure 12-26 Results of the Quant collection using the Generic ExtendIT event source

This concludes our Generic ExtendIT event source creation example.

12.5 Custom event source methods comparison table

In the previous chapters, we described and provided examples of the three methods that Tivoli Security Information and Event Manager offers to create custom event sources.

Table 12-4 shows a comparison where we consolidate and describe the main differences. We also share some additional comments to be considered when designing a solution for your organization.

Table 12-4 Custom event source methods comparison

Event source Type	Original audit trail format	Log management	Forensic investigation	Compliance reporting
Ubiquitous	Plain text, one line per record.	Yes	Yes, each line per record. To split the record in more fields a GSL needs to be developed.	No
W7	Supported CSV or XML.	Yes	Yes	Yes, but not normalized by Tivoli Security Information and Event Manager.
Generic Extend IT	Any	Yes	Yes. User must develop parsers.	Yes. User must develop mappers and grouping files.

12.5.1 Ubiquitous event source pros and cons

The ubiquitous method is the most easy type of event source to implement; however, it is limited to plain text only, and it does not offer any compliance reporting capabilities. In other words, an organization cannot analyze reports using the Compliance Dashboard.

Data that is collected using the ubiquitous method can be searched and analyzed through Forensic Investigation and basic reporting using Tivoli Common Reporting.

This type of event source can be utilized for non-supported event sources and where the main requirement is to collect and store the audit logs.

12.5.2 W7Log event source pros and cons

This can be considered the most flexible type of custom event source. The challenge is to convert the original audit trail information from your event source into a supported CSV or XML format. This task can be accomplished using Tivoli

Directory Integrator or a script that can be built in any other programming language.

The converted CSV or XML file should finally be located on a Windows machine with an agent installed, or on the Tivoli Security Information and Event Manager server itself. In other words, if the original audit trail is located on a UNIX machine, you must find a method to transfer the files to a Windows machine or to the Tivoli Security Information and Event Manager server on a regular basis.

There is no normalization with this type of event source, which means that every single record must be converted to a Reporting Database (GEM) event. No classification of the data is being collected. In this case it is recommended to fine tune the audited system to only generate important events.

12.5.3 Generic ExtendIT Pros and Cons

Generic ExtendIT can be used on virtually any type of audit log, including databases. Generic Extend IT can be customized to connect using JDBC or ODBC to pull the data. Generic ExtendIT can also be used in UNIX environments to access audit logs in binary format.

With the implementation of its own GSL and GML files, Generic ExtendIT can classify the data, discard irrelevant events, and process only security related events.

To implement a Generic ExtendIT event source the organization must gain skills in writing GSL and GML code.

12.6 Creating a custom UIS using Generic ExtendIT

A *user information source* (UIS) obtains information about users and groups on the target system. Based on the data that is available on the target system, the user information source returns information, such as:

- ▶ The user account name (the name the user enters when logging on)
- ▶ The internal user ID (such as a numeric user number)
- ▶ The name of the user (as provided in the user registry)
- ▶ The groups that the user is a member of
- ▶ The roles that the user possesses

This information can be used to improve the mapping of audit trails that feature these users. Grouping rules and policy rules can be directly defined in Tivoli Security Information and Event Manager using this information. If the audit record contains only one identifier for a user, for example, the internal user ID,

then the other values, such as user account name or the full name, can be deduced using the data from the user information source.

Tivoli Security Information and Event Manager supports more than 50 different types of user information sources.

Every UIS is associated with a type of platform or application. There is a UIS available for Windows, AIX, Solaris, z/OS, and so on. A complete list is available in the *IBM Tivoli Security Information and Event Manager Version 2.0 Event Source Guide*, SC23-9687.

You might run into situations where you must create a custom UIS event source, either because an officially supported event source does not provide its own UIS or to improve the grouping capabilities of a custom event source.

To create a custom UIS, you must:

1. Obtain access to the user directory on the target system.
2. Convert the user directory information to a Tivoli Security Information and Event Manager supported grouping format.

Preferred method: The preferred method to accomplish this step is by using Tivoli Directory Integrator, which uses its AssemblyLines and connector technology to transform almost any kind of source data on many different target platforms.

3. Create a collect script.
4. Configure the grouping files and event source on the Tivoli Security Information and Event Manager server.

12.6.1 Example of custom UIS

For this section, we create UIS support for the QUANT application that is used in the Generic ExtendIT example in the previous section.

Access to the users directory

QUANT stores its users in the following path `c:\users\store\userlists.txt`. It uses a comma separated value (CSV) file, as shown in Example 12-6.

Example 12-6 QUANT users directory file

```
Membership, logonname, realname, identifier  
End Users,0101022,Charlie,0432176  
End users,0111123,Alice,053445
```

Administrators,0234512,Aaron,987689
Administrators,6782334,Leslie,778321
Contractors,5677772,Joseph,8890322
Contractors,8790223,Adrian,9890001

Converting a user directory file to a grouping file

To convert the userlist.txt file into a supported grouping format we use Tivoli Directory Integrator. You can also use another scripting or compiled language of your choice.

This task must be executed before the collect. After the conversion, the file is in a supported grouping format, as shown in Example 12-7.

Example 12-7 User directory file converted to a supported grouping file

```
[SourceGroup]
"Administrators"
{
  match logonname "6782334"
  match originator "778321"
  match realname "Leslie"
}
{
  match logonname "0234512"
  match originator "987689"
  match realname "Leslie"
}
"End Users"
{
  match logonname "0101022"
  match originator "0432176"
  match realname "Charlie"
}
{
  match logonname "0111123"
  match originator "053445"
  match realname "Alice"
}
"Contractors"
{
  match logonname "5677772"
  match originator "8890322"
  match realname "Joseph"
}
{
```

```
match logonname "8790223"
match originator "9890001"
match realname "Adrian"
}
```

Creating the collect script for a custom UIS

In this next step, we create a Windows-based script called `getquantuis.bat` and place it in the `c:\ibm\tsiem\sim\server\bin` folder. This script is called every time a collect is issued for this event source using the Tivoli Integrated Portal.

Example 12-8 shows our sample collect script.

Example 12-8 Collect UIS script for QUANT

```
@rem Retrieve event source properties
set TempFile1=%1%
set TempFile2=%2%
set TempFile3=%3%
set TempFile4=%4%
set Option1=%5%
set Option2=%6%
set Option3=%7%
set Option4=%8%
set Option5=%9%
shift
set Option6=%9%
shift
set Option7=%9%
shift
set Option8=%9%
shift
set Props=%9%
@rem Set progress log name; base on %Props%
@rem to make it unique.
set log=..\log\%Props%
echo %DATE%^ ^%TIME% Start collect >> %log%
echo Using event source properties:
echo Temporary file 1 = %TempFile1% >> %log%
echo Temporary file 2 = %TempFile2% >> %log%
echo Temporary file 3 = %TempFile3% >> %log%
echo Temporary file 4 = %TempFile4% >> %log%
echo >> %log%
echo Option 1 = %Option1% >> %log%
echo Option 2 = %Option2% >> %log%
echo Option 3 = %Option3% >> %log%
```

```
echo Option 4 = %Option4% >> %log%
echo Option 5 = %Option5% >> %log%
echo Option 6 = %Option6% >> %log%
echo Option 7 = %Option7% >> %log%
echo Option 8 = %Option8% >> %log%
echo State file: %Props% >> %log%
@rem Invoke an executable for every sublog
echo %DATE%^ ^%TIME% Collect 1st log >> %log%
@rem Remove remnants of previous collect
del %TempFile1%
@rem Collect the whole 'Option 1' file
copy %Option2% %TempFile1%
echo %DATE%^ ^%TIME% End of collect >> %log%
@set errorlevel=0
```

Configuring the event source for QUANT custom UIS

From the Tivoli Integrated Portal, we add a new Generic ExtendIT event source and fill in the properties, as shown in Figure 12-27 on page 400.

Event Sources

Event Sources > User Information Source Details > Advanced

*Name:

Properties:

Name	Value
Audited Machine	tsiemstd01
Type	Generic ExtendIT
Agent	tsiemstd01
Option 1	<input type="text" value="quant_group.cfg"/>
Option 2	<input type="text" value="users\store\userlist.txt"/>
Option 3	<input type="text"/>
Option 4	<input type="text"/>
Option 5	<input type="text"/>
Option 6	<input type="text"/>
Option 7	<input type="text"/>
Option 8	<input type="text"/>
Platform Type	<input type="text" value="GROUPING"/>
Program Path	<input type="text" value="..\bin\getquantuis.bat"/>
Text encoding for audit trail	<input type="text"/>
Language code for audit trail	<input type="text"/>

Figure 12-27 Event source details

In Figure 12-27:

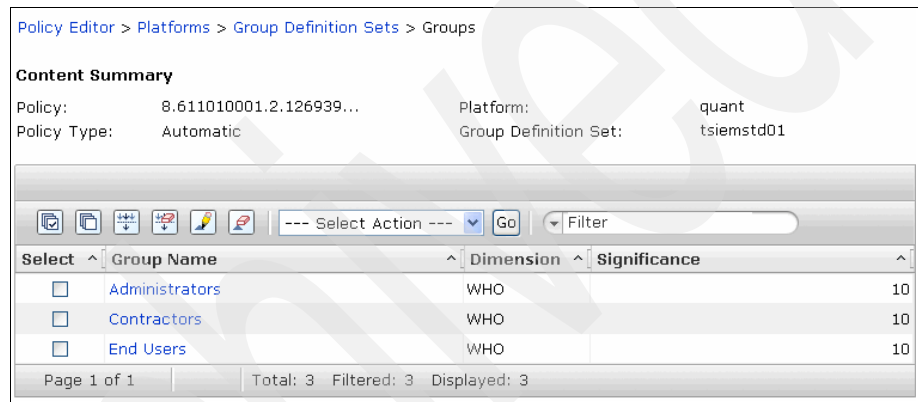
- ▶ Option 1 specifies the grouping file that is associated to the platform that we want to support with this UIS. In this case, it is the QUANT application that uses the `quant_group.cfg` file. This information is taken and registered in the chunk header where it is used as a pointer during the load. No additional steps are required.
- ▶ Option 2 specifies the place where the QUANT application stores the `userlist.txt` file. The Platform Type value must be `GROUPING`, and the Program Path defines the place where the collect process can find the `getquantuis.bat` collect script. It must be located in the `bin` folder on the server.

Validating the new custom UIS for QUANT

To validate that the new custom UIS is working:

1. From the Policy Explorer in TIP, click **Show Automatic**.
2. Specify a date. Not specifying a date retrieves the last collected UIS data. Click **Show Automatic**.
3. Select **Manage Groups**, and then click **quant**.
4. Select the server or agent where the custom UIS was deployed.

The content of the UIS is shown in Figure 12-28. As you can observe, the Platform indicated is *quant*, therefore, the data that will be used during the load is of the type *quant*.



Policy Editor > Platforms > Group Definition Sets > Groups

Content Summary

Policy: 8.611010001.2.126939... Platform: quant
Policy Type: Automatic Group Definition Set: tsiemstd01

Select	Group Name	Dimension	Significance
<input type="checkbox"/>	Administrators	WHO	10
<input type="checkbox"/>	Contractors	WHO	10
<input type="checkbox"/>	End Users	WHO	10

Page 1 of 1 Total: 3 Filtered: 3 Displayed: 3

Figure 12-28 Quant custom UIS result

5. When data is being loaded, the content of the UIS data is merged with the platform grouping file. An entry in the *mainmapper log* also demonstrates that the new custom UIS is working, as shown in Example 12-9.

Example 12-9 Entries in the mainmapper log

```
[Mar 23, 2010 3:09:17 PM] INFO: CIFJG0246I: ID information of 6 users after quant_group.cfg  
[Mar 23, 2010 3:09:17 PM] INFO: CIFJG0507I: STATUS: merged quant_group.cfg for quant
```

Tip: The data we used for this scenario can be downloaded, as described in Appendix B, “Additional material” on page 411.

12.7 Conclusion

In this chapter, we discussed the necessary steps to integrate several custom event sources.

This concludes our customer scenario of X-Y-Z Financial Accounting.

Archived

Corporate policy and standards

Technology must not drive the corporate policy; instead, it should be the other way around. When you know what you need to protect and the potential threats and risks to those assets, you can start protecting them. First, all of the threats and risks are classified in a study based on certain elements, such as:

- ▶ Direct financial loss
- ▶ Indirect financial loss (such as investigation, recovery, and so on)
- ▶ Loss of confidential information
- ▶ Liability
- ▶ Image impact (loss of goodwill, customer loyalty, and so on)
- ▶ Cost of risk mitigation or transfer
- ▶ Accepting residual risk

This study can process the same threats and risks applied to separate assets, but concludes at a different level of liability based on your particular business environment. Next, the decision must be made: accept, mitigate, or transfer the risk. This process can be handled by external consultants, such as IBM Global Services or by an internally appointed team. The process can use both formal and informal methods, but the result is usually a blend of these approaches. The threat identification, as well as this severity study, using a formal approach occurs in conjunction with the organization by applying a standard and a proven methodology.

It is tempting to directly translate the threat analysis into a technical solution, but it must first lead to the corporate policy and standards. These documents highlight the risks and present how they must be handled enterprise wide.

The first document that must be written is therefore the *corporate policy document*. It must outline the high-level directions to be applied enterprise wide. It is absolutely not technical. It is derived from the business of the enterprise and must be as static as possible, as shown in Figure A-1.

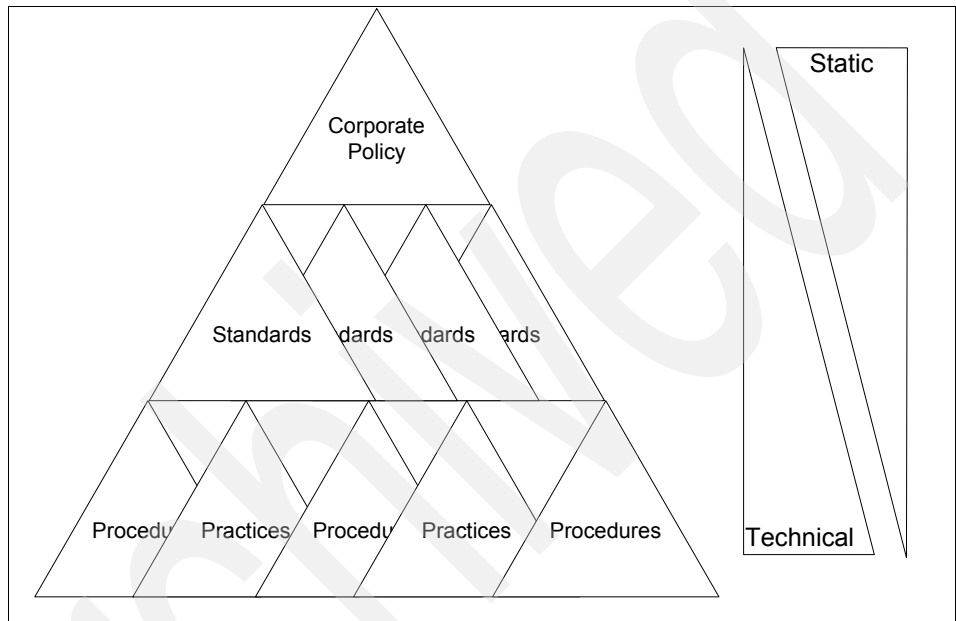


Figure A-1 Dynamics for policy, standards, practices, and procedures

Attention: *Policies* is a very common term, and in many products you find specific policies sections. These are the product-related policies that are covered in the practice or procedure documents. The corporate policy is not related to products and is a high-level document.

Standards, practices, and procedures

Standards are derived from the corporate policy. They are documents that explain how to apply the policy details in terms of *authentication*, *access control*, and so on. They explain how the policy must be applied. Changes in threats or major technology changes can impact them. The standards are then mapped to *practices* or *procedures*.

The practices are descriptions of practical implementations of the standard on an operating system, application, or any other endpoint. They detail precise configurations, such as the services to be installed, the way to set up user accounts, or how to securely install software.

The procedures document the single steps to be applied to requests and the approval and implementation flows. Such a procedure can be the request to access a specific set of sensitive data, where the approval path (system owner, application owners, and so on) and conditions (Virtual Private Network, strong authentication, and so on) are explained in detail.

Approval procedures: Approval procedures are often implemented by sending e-mails or paperwork. The efficiency can be improved by using a computer to handle these repetitive tasks and ensure that changes within the organization are applied quickly to the procedures. As explained later, this can reduce human errors.

Practical example

Here is an example of how a policy is defined and implemented with procedures and practices.

The operations manager has reported an increased workload on the help desk due to problems caused by employees downloading non-business related programs onto their systems.

The problems range from the introduction of viruses to disruption of business processes, with a real financial impact. To address this problem, upper management incorporated, in the corporate policy, the following directive: “The corporate assets might be used only to perform enterprise related tasks”.

First, the policy must be communicated to all employees in the enterprise.

The standards for the networking part explain which services can be allowed on the employee computer. The practice then explains how to set up the Windows or Linux clients according to the standards, and the procedures explain how to

perform a request, the requirements, and the approval paths, to get special services installed on your computer.

The existing clients are updated and controls are performed to verify the compliance in addition to a further audit of the environment.

Figure A-2 summarizes the five steps we went through. It is a common approach that is adopted in many methodologies.

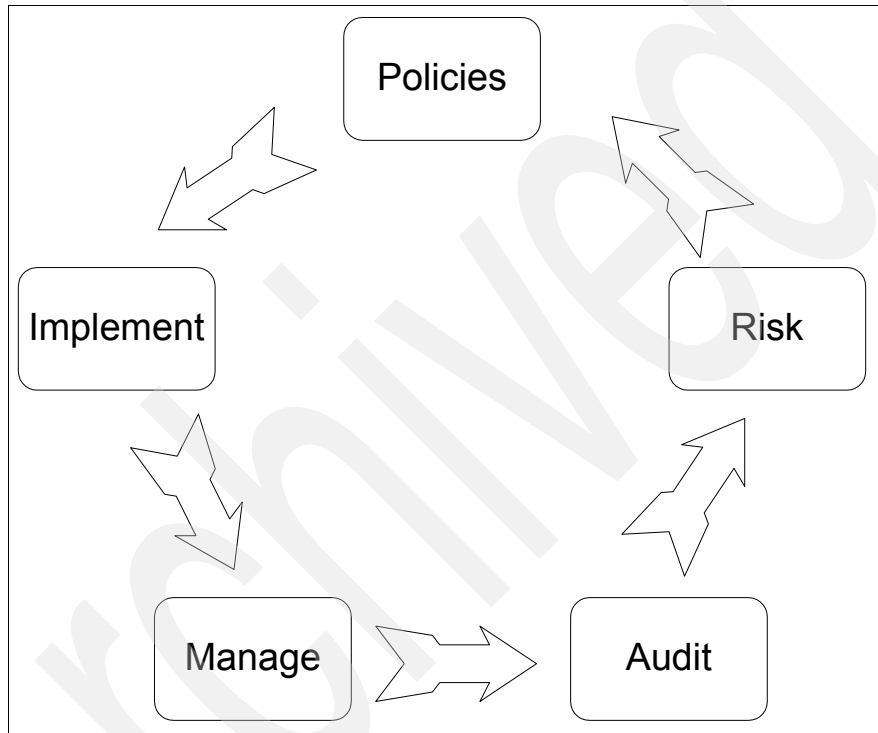


Figure A-2 The five steps in defining your IT security

External standards and certifications

The discussion on corporate policies suggests that internal business needs are the drivers for designing corporate policies. While this is true, there are a number of external factors that can change these business needs and policies. Some of these external pressures can be detailed enough to specify not only policies, but also standards and procedures.

We show examples of these external drivers. The list is not exhaustive, nor is each description complete; instead it is provided as a guide to the type of

standards that might (or might not) apply to your organization and, therefore, several of the external factors you must consider when creating policies.

Many organizations use these external standards as a guide to help them formulate their own corporate policies. It is not uncommon to find organizations using the ISO17799 standards, but without having them externally audited and certified. These standards are seen as a good foundation for security.

Industry specific requirements

Some industry sectors have standards that are specific to that industry sector. Two examples are:

- ▶ The Sarbanes-Oxley Act (SOX)

SOX was established in 2002, a result of corporate scandals about incorrect financial reporting. It aims to protect stakeholders from huge losses and to prevent future shocks to confidence in the financial system in the U. S. Since July 2006, the law applies to all companies that are listed on the U. S. stock exchanges, which includes international or foreign companies.

- ▶ Basel II

Basel II is an accord issued by the Basel Committee on Banking Supervision and provides summarized recommendations on banking laws and regulations with the intent to harmonize banking regulation worldwide. This second accord introduces matters around Operational Risk, which again includes risks in the area of technology, processes, and people.

Any pharmaceutical organization that wants to sell or market its products in America must abide by these rules. Corporate policies, standards, and processes must reflect this requirement.

- ▶ CFR 21 Part 11

21 CFR Part 11 applies to electronic records that are created, modified, maintained, archived, retrieved, or transmitted under any records requirements that are covered by Federal Drug Agency regulations.

Any pharmaceutical organization that wants to sell or market its products in America must abide by these rules. Corporate policies, standards, and processes must reflect this requirement.

- ▶ Health Insurance Portability and Accountability Act (HIPAA)

HIPAA was established in 1996 and contains provisions for USA national standards for the security and privacy of electronic health information. It provides safeguards for the area of administration processes and the physical and technical infrastructure and defines the rights of individuals and the

related obligations for organizations in the health industry with regard to Personal Health Information (PHI).

The requirements of the HIPAA standard have since then been adopted into health industry regulation of many other countries, for example, in Germany.

► **Gramm-Leach-Bliley Act (GLBA)**

GLBA was established in 1999 and deals with the protection of the privacy of customers or financial institutions and the security requirements that financial institutions must meet. The two significant impacts of the act are on one hand the obligation of strict separation between corporate and private banking and insurance activities on financial institutions in the USA in contrast to the widely spread universal banking approach taken by financial institutions in Europe. On the other hand, the act introduces the requirement to take precautions against *Social Engineering*, which is referred to as *Pretexting* in the act. Also, the act requires financial institutions to establish a security framework to protect their own and their customer's financial data.

Product or solution certifications

Some products or solutions can be certified before use so that a potential purchaser has an understanding that the product or solution fits the role that it is needed for.

Common Criteria

This is a set of tests originally based upon the US Orange book and European/Australian ITSEC evaluations. It is currently recognized by 14 countries. There are seven levels of tests. Evaluation Assurance Levels (EAL) 1–4 are usually used in the commercial areas, and the tests that represent the higher EALs 5–7 are reserved for the security testing of highly secure environments.

CAPS UK

In addition to internationally recognized evaluations, there might be local evaluations that impact an organization. The UK Government's Communications-Electronic Security Group (CESG) produced the Assisted Products Scheme in an effort to help commercial product vendors produce cryptographic products suitable for use by the British government. It is called CESG Assisted Product Scheme (CAPS), which is similar in purpose to the FIPS 140 (for the US and Canadian governments) and the Cryptographic Advisory Note (CAN) (for the Australian and New Zealand governments).

Nationally and internationally recognized standards

Some standards bodies publish broad general sets of standards that an organization can implement. These standards can be audited and hence the organization can be sure they are complying.

BS7799, ISO17799, and ISO27001

BS7799 was written in February 1995 and was updated in May 1999 and is the most widely known standard. British Standard (BS) 7799 consists of multiple parts. The first part is intended to serve as a single reference point for identifying a range of security controls, needed for most situations, where information systems are used in industry and commerce within large, medium, and small organizations. This part was lifted onto the international level in 2001 and is called ISO17799 and was updated in 2005. The second part of BS7799 defines the standard against which organizations can be certified for meeting the method and intent of part 1. This second part was internationally adopted as ISO27001. To reduce confusion with the numbering, ISO17799 was recently renumbered as ISO27002.

BS7858

BS7858 is just one example of the other less well-known standards that can affect security policy. Specifically, BS7858 gives recommendations for the security screening of personnel to be employed in an environment where the security of people, goods, or property is a significant feature of the employing organization's operations.

Data Privacy Laws

The privacy laws of the country in which an organization operates are many and diverse. The application of the laws is variable from geography to geography, and it is good to be aware of the impact of them upon corporate security policies. Modern democracies are often fond of creating freedom of information laws. One of the problems with these laws is that they are directly contrary to the same democracies' desire to maintain the privacy of individual information. Besides the the articles of the privacy laws, the actual legal practice and enforcement of the laws is very important. In certain countries, the actual obligations might not be met in a given case, but it might be a widely accepted practice.

Privacy law is, therefore, a growing area. Some examples are:

- ▶ UK Data Protection Act 1998

An act to make new provisions for the regulation of the processing of information relating to individuals, including obtaining, holding, using, or disclosing of such information.

- ▶ European Data Directive 95/46/EC

This directive and others give direction to issues surrounding the protection of individuals with regard to the processing of personal data and on the free movement of such data. The way they interact with national law must also be considered.

Summary

Corporate policies must be thought of as business level requirements. They are primarily internal business drivers, but they might be impacted upon by external factors, so corporate policies must take account of these factors. Subsidiary standards and the procedures and practices that result in turn are also produced.

Corporate policies must be relatively static and technology free and standards, practices, and procedures can be more fluid and technology specific.

Additional material

This appendix refers to additional material that can be downloaded from the Internet as described below.

Locating the Web material

The Web material that is associated with this book is available in softcopy on the Internet from the IBM Redbooks Web server. Point your Web browser at:

<ftp://www.redbooks.ibm.com/redbooks/SG247530>

Alternatively, you can go to the IBM Redbooks Web site at:

ibm.com/redbooks

Select the **Additional materials**, and open the directory that corresponds with the IBM Redbooks form number, SG24-7530.

Using the Web material

The additional Web material that accompanies this book includes the following files:

<i>File name</i>	<i>Description</i>
SG247530.zip	Zipped files for use with the Tivoli Directory Integrator scenario in Chapter 12, “Custom event source integration” on page 351.

How to use the Web material

Create a subdirectory (folder) on your workstation, and unzip the contents of the Web material zip file into this folder.

You will get two separate folders:

- ▶ TDI to W7Log File Format
- ▶ Custom UIS Generic ExtendIT

TDI to W7Log File Format

The TDI to W7Log File Format folder contains the following files:

- ▶ Input.txt
This file contains the simulated log that is used as input for the Tivoli Directory Integrator AssemblyLine.
- ▶ Output.csv
This file contains the output from the Tivoli Directory Integrator AssemblyLine.
- ▶ Quantwave.xml
This file contains the actual Tivoli Directory Integrator AssemblyLine.

Custom UIS Generic ExtendIT

The Custom UIS Generic ExtendIT folder contains the following files:

- ▶ userlist.txt
This file contains the simulated file with user directory and groups that is used as a input for the Tivoli Directory Integrator AssemblyLine.
- ▶ grpCfg.txt
This file contains the output from the Tivoli Directory Integrator AssemblyLine. The extension of this one can be changed to CFG.

- ▶ GroupCfg.xml
This file contains the actual Tivoli Directory Integrator AssemblyLine.
- ▶ GroupCfg.properties
This file contains properties of the connector.

Archived

Archived

Glossary

8-bit UCS/Unicode Transformation Format A variable-length character encoding for Unicode. It is able to represent any character in the Unicode standard, yet the initial encoding of byte codes and character assignments for UTF-8 is consistent with ASCII.

Access Management A discipline that focuses on ensuring that only approved roles are able to create, read, update, or delete data - and only using appropriate and controlled methods. Data governance programs often focus on supporting access management by aligning the requirements and constraints posed by governance, risk management, compliance, security, and privacy efforts.

Agent A piece of software that automates the collection of logs from event sources and transmits the logs to the Depot.

Actuator Scripts The Actuator Scripts also known as collect scripts are invoked by the Agent (at the request of the Tivoli Security Information and Event Manager Server) to collect the log for a particular event source. There is a different script for every supported event type.

Aggregation Database Data and statistics, spanning a longer period, are maintained by a process called aggregation. The aggregation process builds a special database called the aggregation database, which is used for trend and summary reports.

Alerts Messages that Tivoli Security Information and Event Manager sends when a serious or potentially harmful security event has occurred. Alerts allow for a fast response to the event by a systems manager or system administrator.

Assurance Activities designed to reach a measure of confidence. Assurance is different from audit, which is more concerned with compliance to formal standards or requirements.

Audit An independent examination of an effort to determine its compliance with a set of requirements. An audit might be carried out by internal or external groups.

Audit Report A report which shows infrastructure changes that are made to hardware and software and who is responsible for the changes.

Audit Trail A record that can be interpreted by auditors to establish that an activity has taken place. Often, a chronological record of system activities to enable the reconstruction and examination of the sequence of events or changes in an event. An audit trail of system resource usage might include user login, file access, and triggers that indicate whether any actual or attempted security violations occurred.

Audited System A system on which events occur and are recorded in logs which provide the audit data for Tivoli Security Information and Event Manager.

Authentication In computer security, verification of the identity of a user or process and the construction of a data structure that contains the privileges that were granted to the user or process. Contrast with authorization.

Authorization The process of granting a user either complete or restricted access to an object, resource, or function. Contrast with authentication.

Basel II A round of deliberations by central bankers from around the world, under the auspices of the Basel Committee on Banking Supervision (BCBS) in Basel, Switzerland, aimed at producing uniformity in the way banks and banking regulators approach risk management across national borders. The Basel II deliberations began in January 2001, driven largely by concern about the arbitrage issues that develop when regulatory capital requirements diverge from accurate economic capital calculations. Basel II recommends three pillars: risk appraisal and control, supervision of the assets, and monitoring of the financial market, to bring stability to the financial system.

Batch Collect Mechanism for retrieving security log data.

British Standard 7799 A standard code of practice and provides guidance on how to secure an information system. It includes the management framework, objectives, and control requirements for information security management systems.

Can Spam Act of 2003 A commonly used name for the United States Federal law more formally known as S. 877 or the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003. The law took effect on January 1, 2004. The Can Spam Act allows courts to set damages of up to \$2 million when spammers break the law. Federal district courts are allowed to send spammers to jail or triple the damages if the violation is found to be willful.

CCO See Chief Compliance Officer.

CERT See Computer Emergency Response Team.

Certified Server Validation (CSV) A technical method of e-mail authentication intended to fight spam. Its focus is the SMTP HELO-identity of Mail transfer agents.

Change Control A formal process used to ensure that a process, product, service, or technological component is modified only in accordance with agreed-upon rules. Many organizations have formal Change Control Boards that review and approve proposed modifications to technology infrastructures, systems, and applications. Data governance programs often strive to extend the scope of change control to include additions, modifications, or deletions to data models and values for reference/master data.

Chief Compliance Officer (CCO) The officer primarily responsible for overseeing and managing compliance issues within an organization. The CCO typically reports to the Chief Executive Officer. The role has long existed at companies that operate in heavily regulated industries such as financial services and health care. For other companies, the rash of recent accounting scandals, the Sarbanes-Oxley Act, and the recommendations of the U.S. Federal Sentencing Guidelines have led to additional CCO appointments.

Chunk Data structure of the archived log files in the Depot. A chunk consists of a header file and one or more data files.

Client A system entity that requests and uses a service provided by another system entity, called a server. In some cases, the server might itself be a client of some other server. A system entity that requests and uses a service provided by another system entity, called a server. In some cases, the server might itself be a client of some other server.

Cluster (Tivoli Security Information and Event Manager) The combination of a Enterprise Server and up to three Standard Servers.

COBIT See Control Objectives for Information and related Technology.

Collect History Report Tivoli Security Information and Event Manager report that documents log collection events.

Collector A software module that runs on a client system and gathers data. This data is subsequently sent to a server.

Committee of Sponsoring Organizations of the Treadway Commission (COSO) A U.S. private-sector initiative, formed in 1985. Its major objective is to identify the factors that cause fraudulent financial reporting and to make recommendations to reduce its incidence. COSO has established a common definition of internal controls, standards, and criteria against which companies and organizations can assess their control systems.

Common Criteria The Common Criteria is the result of the integration of information technology and computer security criteria. In 1983, the US issued the Trusted Computer Security Evaluation Criteria (TCSEC), which became a standard in 1985. Criteria developments in Canada and European ITSEC countries followed the original US TCSEC work. The US Federal Criteria development was an early attempt to combine these other criteria with the TCSEC, and eventually led to the current pooling of resources towards production of the Common Criteria. The Common Criteria is composed of three parts: the Introduction and General Model (Part 1), the Security Functional Requirements (Part 2), and the Security Assurance Requirements (Part 3). While Part 3 specifies the actions that must be performed to gain assurance, it does not specify how those actions are to be conducted; to address this issue, the Common Evaluation Methodology (CEM) was created for the lower levels of assurance.

Compliance Either a state of being in accordance with established guidelines, specifications, or legislation or the process of becoming so. Software, for example, can be developed in compliance with specifications created by some standards body, such as the Institute of Electrical and Electronics Engineers (IEEE), and might be distributed in compliance with the vendor's licensing agreement. In the legal system, compliance usually refers to behavior in accordance with legislation, such as the United States' Can Spam Act of 2003, the Sarbanes-Oxley Act (SOX) of 2002, or HIPAA (United States Health Insurance Portability and Accountability Act of 1996).

Compliance Check A set of rules used to determine whether a computer or group of computers is compliant or not. There are two types of compliance checks: software and security.

Compliance Dashboard . It displays an easy-to-understand, color-coded matrix that highlights degrees and level of compliance based on user behavior and data access.

Compliance Management Module Tivoli Security Information and Event Manager regulation-specific reporting interface.

Compliance Report A report that provides information about the patch compliance status of all selected target computers.

Compliant State The state that a user wants an object to have.

Computer Emergency Response Team

(CERT) The CERT/CC is a major reporting center for Internet security problems. Staff members provide technical advice and coordinate responses to security compromises, identify trends in intruder activity, work with other security experts to identify solutions to security problems, and disseminate information to the broad community. The CERT/CC also analyzes product vulnerabilities, publishes technical documents, and resents training courses. The CERT/CC is located at the Software Engineering Institute (SEI), a federally funded research and development center (FFRDC) operated by Carnegie Mellon University (CMU).

Configuration Compliance The comparison of known state to a compliant state and can include automated actions. After discovery or scanning is performed, devices are said to be either compliant or noncompliant.

Consolidation Database An Enterprise Server database that delivers enterprise-wide trend and summary reports.

Control A means of managing a risk or ensuring that an objective is achieved. Controls can be preventative, detective, or corrective and can be fully automated, procedural, or technology-assisted human-initiated activities. They can include actions, devices, procedures, techniques, or other measures.

Control Objectives for Information and related Technology (COBIT) is a set of best practices (framework) for information technology (IT) management created by the Information Systems, Audit and Control Association (ISACA), and the IT Governance Institute (ITGI) in 1992. COBIT provides managers, auditors, and IT users with a set of generally accepted measures, indicators, processes and best practices to assist them in maximizing the benefits derived through the use of information technology and developing appropriate IT governance and control in an organization.

COSO See Committee of Sponsoring Organizations of the Treadway Commission.

CSV See Certified Server Validation.

Data Aggregation The ability to get a more complete picture of the information by analyzing several different types of records at the same time.

Data Governance The exercise of decision-making and authority for data-related matters. The organizational bodies, rules, decision rights, and accountabilities of people and information systems as they perform information-related processes. Data governance determines how an organization makes decisions.

Data Mapping The discipline, process, and organizational group that conducts analysis of data objects used in a business or other context, identifies the relationships among these data objects, and creates models that depict those relationships.

Data Privacy The assurance that a person's or organization's personal and private information is not inappropriately disclosed. Ensuring data privacy requires access management, security, and other data protection efforts.

Delta Table A database table used for saving changed data from subsequent runs of a collector.

Deployment The process of reconfiguring and reallocating resources in the managed environment. Deployment occurs in response to deployment requests, created manually by administrators or automatically by the system.

Depot Tivoli Security Information and Event Manager secure storage facility for storing and archiving logs.

Depot Server The component that stores files for distribution. Files are uploaded to a Depot server using a client and stored in a directory that is specified when the Depot server is installed. Depot servers can replicate files to other Depot servers and download files to clients.

Domain A logical grouping of resources in a network for the purpose of common management and administration.

Enterprise Server A server that provides centralized log management, performs forensic searches of the GEM log archives, and creates reports.

Event An observable occurrence in a system or network.

Event source Software module used by Tivoli Security Information and Event Manager to collect log files from an event source. Event Sources are included in the TSIEM distribution for all supported platforms. Custom Event Sources can be added to an existing TSIEM deployment manually.

Extensible Markup Language (XML) is a general-purpose markup language. It is classified as an extensible language because it allows its users to define their own tags. XML is recommended by the World Wide Web Consortium. The W3C recommendation specifies both the lexical grammar, and the requirements for parsing.

File Transfer Protocol (FTP) Used to transfer data from one computer to another over the Internet, or through a network.

Federal Information Security Management Act (FISMA) This is a U.S. federal law enacted in the year of 2002. It outlines the importance of information security to the economic and national security interests of the U.S. Each federal agency is required to implement a program to provide information security for the information and systems where it resides.

Food and Drug Administration (FDA) This is a government agency of the U.S. Department of Health and Human Services. It regulates the safety of foods, dietary supplements, tobacco products, medication (with or without prescription), vaccines, blood transfusions, medical devices, and so on. For more information, please refer to <http://www.fda.gov>.

Forensic Analysis Used to follow up on security incidents and behavioral trends.

FTP See File Transfer Protocol.

General Scanning Language (GSL) A scripting language that enables you to describe the structure and label the attributes contained in the log files of ubiquitous collect event sources. The GSL Toolkit eases the forensic analysis of log data by enabling you to define attributes contained in the log data and to describe the structure of log files.

Reporting Database Contains the logs from different event sources.

Governance, Risk, and Compliance (GRC) An acronym often used by management in financial institutions to acknowledge the interdependencies of these three disciplines in setting policy.

Gramm-Leach-Bliley Act An Act of the United States Congress which repealed the Glass-Steagall Act, opening up competition among banks, security companies and insurance companies. The Glass-Steagall Act prohibited a bank from offering investment, commercial banking, and insurance services.

GRC See Governance, Risk, and Compliance.

GSL See General Scanning Language.

Health Insurance Portability and Accountability Act (HIPAA) is the United States Health Insurance Portability and Accountability Act of 1996. There are two sections to the Act. HIPAA Title I deals with protecting health insurance coverage for people who lose or change jobs. HIPAA Title II includes an administrative simplification section which deals with the standardization of health care-related information systems. In the information technology industries, this section is what most people mean when they refer to HIPAA. HIPAA establishes mandatory regulations that require extensive changes to the way that health providers conduct business.

HIPAA See Health Insurance Portability and Accountability Act.

IETF See Internet Engineering Task Force.

Incident An incident as an adverse network event in an information system or network or the threat of the occurrence of such an event.

Information Quality Management An information technology (IT) management discipline, which encompasses the COBIT Information Criteria of efficiency, effectiveness, confidentiality, integrity, availability, compliance, and reliability. The idea is for companies to have the risks of using a program diminished to protect private and sensitive information definition.

Information Systems Audit and Control Association (ISACA) is an international association for the support and improvement of professionals whose jobs involve the auditing of corporate and system controls.

Information Technology Governance A subset discipline of Corporate Governance focused on information technology (IT) systems and their performance and risk management. The rising interest in IT governance is partly due to compliance initiatives (e.g. Sarbanes-Oxley (USA) and Basel II (Europe)), as well as the acknowledgement that IT projects can easily get out of control and profoundly affect the performance of an organization.

International Compliance The International Standards Organization (ISO) produces international standards such as ISO 27002.

Internet Engineering Task Force (IETF) Develops and promotes Internet standards, cooperating closely with the W3C and ISO/IEC standard bodies; and dealing in particular with standards of the TCP/IP and Internet protocol suite.

ISACA See Information Systems Audit and Control Association.

ISO Name generally applied to quality system standards published by the International Organization for Standardization. ISO certification is provided, on a fee basis, by third party assessors or registrars through an on-site, in-depth audit to determine that an organization's quality system meets the requirements of the standard.

ISO 27002 See SO/IEC 17799.

ISO/IEC27001 An information security standard published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) as ISO/IEC 17799:2005 and subsequently renumbered ISO/IEC 27002:2005 in July 2007, bringing it into line with the other ISO/IEC 27000-series standards. It is entitled Information technology - Security techniques - Code of practice for information security management. The current standard is a revision of the version first published by ISO/IEC in 2000, which was a word-for-word copy of the British Standard (BS) 7799-1:1999.

IT Governance Institute (ITGI) Exists to assist enterprise leaders in their responsibility to ensure that IT goals align with those of the business, it delivers value, its performance is measured, its resources properly allocated and its risks mitigated. Through original research, symposia and electronic resources, the ITGI helps ensure that boards and executive management have the tools and information they need for IT to deliver against expectations.

Compliance Dashboard Tivoli Security Information and Event Manager Web user interface for compliance reporting.

JAAS See Java Authentication and Authorization Service.

Java Authentication and Authorization Service (JAAS) A set of APIs that enable services to authenticate and enforce access controls upon users. It implements a Java technology version of the standard Pluggable Authentication Module (PAM) framework, and supports user-based authorization.

Log Chunk The set of events placed in the Depot by the collect mechanism.

Log Collection Event Each instance of collecting an audit trail, or log chunk, from an audited machine is called a log collection event.

Log Continuity Report Tivoli Security Information and Event Manager report that documents log continuity status.

Log Manager Provides all Log Management functionality, including log collection, log storage, log retrieval, forensic search, and log management reports.

Logs and Audit Trails The system records that documents all activity that occurred on the audited machine.

Metadata Information about a particular data set which might describe, for example, how, when, and by whom it was received, created, accessed, or modified and how it is formatted. Some metadata, such as file dates and sizes, can easily be seen by users; other metadata can be hidden or embedded and unavailable to computer users who are not technically adept. Metadata is generally not reproduced in full form when a document is printed.

National Institute of Standards and Technology (NIST) A unit of the US Commerce Department. Formerly known as the National Bureau of Standards, NIST promotes and maintains measurement standards. It also has active programs for encouraging and assisting industry and science to develop and use these standards.

NERC See North American Electric Energy Corporation.

NIST See National Institute of Standards and Technology.

Normalization The process of standardizing log data by describing them in a single, uniform language.

North American Electric Energy Corporation (NERC) An international, independent, self-regulatory, not-for-profit organization, whose mission is to ensure the reliability of the bulk power system in North America.

Payment Card Industry Data Security Standard (PCI DSS) Developed by the major credit card companies as a guideline to help organizations that process card payments prevent credit card fraud, hacking and various other security issues. An organization that processes, stores, or transmits credit card numbers must be PCI DSS compliant or they risk losing the ability to process credit card payments.

PCI DSS See Payment Card Industry Data Security Standard.

Policy A set of one or more compliance queries used to demonstrate the level of adherence to specific security requirements.

Policy Bundle A file containing the information associated with a policy, such as the compliance queries, the collectors, and the associated schedules. A policy bundle permits the policy to be saved and subsequently applied to other servers.

Policy Exceptions Actions or network activity that violates organization policy.

Policy Generator Tivoli Security Information and Event Manager tool that can be used to create policies using existing logs to set a baseline for acceptable network activity.

Policy Rules A Tivoli Security Information and Event Manager tool that helps a user to generate automatically a set of policy rules or extend an existing policy rule set.

Proxy Relay A special pull client that acts as a relay between the server and one or more clients. A proxy relay is used to reach a limited number of clients that are located behind a firewall, or that are in an IP-address range that is not directly addressable by the server.

Proxy Server A server that acts as an intermediary between a workstation user and the Internet so that the enterprise can ensure security, administrative control, and caching service. A proxy server is associated with or part of a gateway server that separates the enterprise network from the outside network and a firewall server that protects the enterprise network from outside intrusion.

Pull Client A client that permits communication with the server to be initiated by only the server.

Push Client A client that permits communication with the server to be initiated by either the client or the server.

PuTTY A free software SSH, Telnet, rlogin, and raw TCP client. It was originally available only for Windows, but is now also available on various UNIX platforms.

Regulatory Compliance Refers to systems or departments at corporations and public agencies to ensure that personnel are aware of and take steps to comply with relevant laws and regulations.

Agent-less log collection mechanism facilitated by SSH or by NetBIOS for Windows.

Risk The product of the level of threat with the level of vulnerability. It establishes the likelihood of a successful attack.

Risk Assessment The process by which risks are identified and the impact of those risks determined.

Risk Management In a broad sense, to assess, minimize, and prevent negative consequences posed by a potential threat. The term risk management has significantly different meanings that can affect Data Governance programs. At an enterprise level, risk refers to many types of risk (operational, financial, compliance, etc.); managing risk is a key responsibility of Corporate Boards and Executive Teams. Within financial institutions (or in the context of a GRC program), risk management might be a boundary-spanning department that focuses on risk to investments, loans, or mortgages. At a project level, risk management is an effort that should be undertaken as part of project management, focusing on risks to the successful completion of the project. From a compliance/auditing/ controls perspective, risk assessments and risk management are high-effort activities included in the COSO, and COBIT frameworks and required by Sarbanes-Oxley and other compliance efforts. Data governance programs might be asked to support any of these risk management efforts, and might need input from these efforts to resolve data-related issues.

Role Based Access Control Assigns users to roles based on their organizational functions and determines authorization based on those roles.

Sarbanes-Oxley Act (SOX) Legislation enacted in response to the high-profile Enron and WorldCom financial scandals to protect shareholders and the general public from accounting errors and fraudulent practices in the enterprise. The act is administered by the Securities and Exchange Commission (SEC), which sets deadlines for compliance and publishes rules on requirements. Sarbanes-Oxley is not a set of business practices and does not specify how a business should store records; rather, it defines which records are to be stored and for how long. The legislation not only affects the financial side of corporations, but also affects the IT departments whose job it is to store a corporation's electronic records. The Sarbanes-Oxley Act states that all business records, including electronic records and electronic messages, must be saved for not less than five years. The consequences for non-compliance are fines, imprisonment, or both. IT departments are increasingly faced with the challenge of creating and maintaining a corporate records archive in a cost-effective fashion that satisfies the requirements put forth by the legislation.

Scoping Enables you to define limited access for certain users or for certain groups of users.

Secure Shell (SSH) A network protocol that allows data to be exchanged over a secure channel between two computers. Encryption provides confidentiality and integrity of data. SSH uses public-key cryptography to authenticate the remote computer and allow the remote computer to authenticate the user, if necessary.

Security audit A systematic evaluation of the security of an organization's information system by measuring how well it conforms to a set of established criteria. A thorough audit typically assesses the security of the system's physical configuration and environment, software, information handling processes, and user practices. Security audits are often used to determine regulatory compliance, in the wake of legislation (such as HIPAA, the Sarbanes-Oxley Act, and the California Security Breach Information Act) that specifies how organizations must deal with information.

Security Controls Individual security requirements that are categorized into security-related areas. Different organizations must demonstrate the implementation of the security controls through a formal audit process to achieve the respective certification required.

Sensitive Data Data that is private, personal, or proprietary and must be protected from unauthorized access.

Sensitive Information As defined by the federal government, is any unclassified information that, if compromised, could adversely affect the national interest or conduct of federal initiatives.

Server A system where audit data is collected and investigated using Tivoli Security Information and Event Manager.

Shell A UNIX term for the interactive user interface with an operating system. The shell is the layer of programming that understands and executes the commands a user enters. In some systems, the shell is called a command interpreter.

Simple Mail Transfer Protocol (SMTP) The de facto standard for e-mail transmissions across the Internet.

Simple Network Management Protocol (SNMP) Defined by the Internet Engineering Task Force (IETF). SNMP is used by network management systems to monitor network-attached devices for conditions that warrant administrative attention.

SMTP See Simple Mail Transfer Protocol.

Snapshot™ The result of running all of the compliance queries in a policy against a set of clients. A snapshot shows the number of violations and indicates what clients are not adhering to the security requirements being tested by the compliance queries.

SNMP See Simple Network Management Protocol.

SOX See Sarbanes-Oxley Act.

Special Attention Actions or network activities that cannot violate organization policy but are suspicious and require additional attention.

SSH See Secure Shell.

Standard Server The Standard Server is composed of Log Management base and Normalization component. Tivoli Security Information and Event Manager Standard Server provides log collection, log storage, log retrieval, W7 normalization and compliance reporting.

Syslog Often used for both the actual syslog protocol, as well as the application or library sending syslog messages. Syslog is typically used for computer system management and security auditing.

Target System A system to which Tivoli Security Information and Event Manager receives access to the audit data.

Threat A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm.

Threat Assessment The identification of types of threats that an organization might be exposed to.

Tivoli Security Information and Event Manager Cluster The combination of an Enterprise Server, one of the Standard Servers, and a collector in a network deployment.

Tivoli Security Information and Event Manager Server A generic term referring to the Tivoli Compliance Insight Manager engine that collects, and normalizes log data using the W7 methodology. There are two types of Tivoli Compliance Insight Manger servers, Enterprise and Standard.

Tivoli Security Information and Event Manager Suite. Refers to the entire Tivoli Security Information and Event Manager application. This includes the Tivoli Security Information and Event Manager server, Agents, SIM Module, Tivoli Integrated Portal, Log Manager Module, and the Compliance Management Modules.

Tivoli Integrated Portal TIP Tivoli Security Information and Event Manager Web based application for performing administrative, configuration, and reporting functions.

UTF-8 See 8-bit UCS/Unicode Transformation Format.

Vulnerability A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy.

W7 Attributes The following list shows the basic W7 attributes:

1. **Who:** Which user or application initiated the event?
2. **What:** What kind of action does the event represent?
3. **When:** When did the event occur?
4. **Where:** On which system did the event happen?
5. **On What:** What was the object (file, database, printer) involved?
6. **Where from:** From which system did the event originate?
7. **Where To:** Which system is the target or destination of the event?

W7 Methodology Tivoli Compliance Insight Manager patent-pending normalization methodology, which translates log files into an English-based language of who, what, on what, when, where, where from, and where to.

World Wide Web Consortium (W3C) The main international standards organization for the World Wide Web (W3).

XML See Extensible Markup Language.

Archived

Related publications

We consider the publications that we list in this section particularly suitable for a more detailed discussion of the topics that we cover in this book.

IBM Redbooks publications

For information about ordering these publications, see “How to get IBM Redbooks publications” on page 429. Note that some of the documents that we reference here might be available in softcopy only.

- ▶ *Deployment Guide Series: IBM Tivoli Security Compliance Manager*, SG24-6450
- ▶ *Enterprise Security Architecture Using IBM Tivoli Security Solutions*, SG24-6014
- ▶ *Understanding SOA Security Design and Implementation*, SG24-7310
- ▶ *Deployment Guide Series: IBM Tivoli Security Operations Manager 4.1*, SG24-7439
- ▶ *Building a Network Access Control Solution with IBM Tivoli and Cisco Systems*, SG24-6678
- ▶ *Accounting and Auditing on AIX 5L*, SG24-6396
- ▶ *IBM System Storage DR550 V4.5 Setup and Implementation*, SG24-7091

Other publications

These publications are also relevant as further information sources:

- ▶ *IBM Tivoli Security Information and Event Manager Version 2.0 Installation Guide*, GI11-8778
- ▶ *IBM Tivoli Security Information and Event Manager Version 2.0 Users Guide*, SC23-9689
- ▶ *IBM Tivoli Security Information and Event Manager Version 2.0 User Reference Guide*, SC23-9691
- ▶ *IBM Tivoli Security Information and Event Manager Version 2.0 Administrators Guide*, SC23-9688

- ▶ *IBM Tivoli Security Information and Event Manager Version 2.0 Event Source Guide*, SC23-9687
- ▶ *IBM Tivoli Security Information and Event Manager Version 2.0 Troubleshooting Guide*, SC23-9690
- ▶ *IBM Tivoli Security Information and Event Manager Version 2.0, IBM Tivoli Basel II Management Module Installation Guide*, GI11-8779

IBM Tivoli Security Operations Manager related manuals:

- ▶ *IBM Tivoli Security Operations Manager Installation Guide Version 4.1.1*, GC23-6099
- ▶ *IBM Tivoli Security Operations Manager Administration Guide Version 4.1.1*, SC23-6100
- ▶ *IBM Tivoli Security Operations Manager User Guide Version 4.1.1*, SC23-6306

IBM Tivoli Director Integrator related manuals:

- ▶ *IBM Tivoli Director Integrator Users Guide*, SC23-6561

Online resources

These Web sites are also relevant as further information sources:

- ▶ IBM Software support Web site:
<http://www.ibm.com/software/support>
- ▶ To find more information about Basel II, visit this URL:
<http://www.bis.org/pub1/bcbsca.htm>
- ▶ To find more information about the Sarbanes-Oxley Act, visit this URL:
<http://www.soxlaw.com/>
- ▶ To find more information about PCI, visit this URL:
<https://www.pcisecuritystandards.org/>
- ▶ To find more information about HIPAA, visit this URL:
<http://www.hhs.gov/ocr/hipaa/>
- ▶ IBM Training and certification Web site:
<http://www.ibm.com/software/sw-training/>

How to get IBM Redbooks publications

You can search for, view, or download IBM Redbooks, Redpapers, Technotes, draft publications and Additional materials, as well as order hardcopy Redbooks, at this Web site:

ibm.com/redbooks

Help from IBM

IBM Support and downloads

ibm.com/support

IBM Global Services

ibm.com/services

Archived

Archived

Index

A

- Active Directory
 - audit policy settings 155–156
 - diagnostic logging 157
 - event source 151
 - event source configuration 173
 - activity report 81
 - actuator 64
 - script 63
 - System z 307
 - administrative accounts 147
 - agent 63–64, 231
 - data flow log collection 71
 - Domino 250
 - event monitoring 84
 - group 166
 - installation 179
 - SAP 261
 - agentless
 - collect 65
 - collection mechanism 67
 - aggregated information 17
 - aggregation database 60
 - AIX
 - audit subsystem 232
 - event source configuration 236
 - log management 231
 - login files 231
 - alert
 - attention rule 205
 - configuration 59
 - management 81
 - alerting 46
 - functional solution 42
 - rules 59
 - analyzing trends 224
 - antivirus
 - service 5
 - API
 - Windows event management 99
 - architecture 15
 - SIEM 18
 - archival 91
 - archiving 112
 - attention
 - alert 247, 257
 - rule 184, 194, 203
 - SAP 264
 - System z 332
 - audit
 - AIX subsystem 232
 - concerns 91
 - configuration 97
 - controller 55
 - data collection 235
 - approach 231
 - log for SAP 260
 - network appliance 100
 - policy for Windows 2003 Server 155
 - record processing 352
 - settings 91–92, 137
 - System z settings 299
 - trail 5
 - audited
 - machine
 - add to system group 167
 - AIX 237
 - registration 166
 - auditing
 - AIX 231
 - Domino 250
 - System z 295
 - auth daemon 56
- ## B
- Basel II 8, 277, 327, 407
 - compliance management module 291, 297
 - reporting 35
 - reporting goals 144, 154
 - reports 333
 - System z compliance 327
 - batch collect 65
 - bluebook 56
 - brute force attack 278, 283
 - BS7799 409
 - BS7858 409

- business
 - conduct guidelines 4
 - context 3
 - data 147
 - objectives 126
 - requirements 132
 - scenario 121
 - tasks 22
- Business Level API 56

C

- CFR 21 Part 11 407
- change management 24
- Chief Information Security Officer 48, 128
- chunk 98
- CICS
 - logon audit 302
 - monitoring 303
- cloud computing 12
- cluster 83, 86, 304
 - scalability 115
 - scenario configuration 148
- COBIT
 - reporting 35
- Code of Practice for Information Security Management 35
- collect
 - history report 82
 - mechanism 97
 - process 54
 - schedule 107, 176, 311
 - script 381
 - reuse 383
 - strategy
 - System z 317
- collection
 - schedule 113
 - types 91
- Commerical Laws 7
- Common Criteria 408
- compliance 132
 - architecture 15
 - criteria 12
 - dashboard 50, 151, 213, 332
 - reports 219
 - trends 224
- maintenance 12
- management 4

- challenges 12
- criteria 9
 - module 291
- monitoring 128
- report 23
- reporting 58
- scope of checking 10
- solution design 24
- computational correlation 46
- consolidation 81
 - component 62
 - database 63
 - process 63
- Consolidation Server
 - configuration 153
- continuity report 82
- correlation 19, 47
 - ... of real-time events 46
 - engine 46
- cost
 - business requirement 136
 - pressure 12
- CSSL protocol 71
- CSV
 - file format 357
- custom applications 34
- custom event source 351
 - definition 352
- customized report 278

D

- daily verification report 220
- dashboard 36, 213
 - log continuity 115
 - reports 219
 - trends 224
- data
 - analysis engine 60
 - basic collection approach 231
 - collection 107
 - collection methods 65
 - integrity 133
- database
 - administrator 48
 - check 107
 - manual load 209
- DB2 56
 - monitoring 138, 303

- depot 40, 54
 - export 57
 - import 57
 - investigation tool 61, 72, 270
 - weekly check 109
- depth of reporting 10
- design objectives 140
- detailed investigation report 221
- deterministic threat analysis 46
- device events 21
- discovery and analysis 90
- Domino
 - Administration Requests Database 249
 - agent 250
 - attention alerts 257
 - event source configuration 250
 - journaling 254
 - log management 250
 - policy violations 254
- DR550 113
- duration check 10

E

- Enterprise Server 45, 54, 83
 - ... in a cluster configuration 86
 - installation 153
 - Point of Presence 96
- European Data Directive 95/46/EC 410
- event
 - collection 19
 - correlation 36, 45–46
 - functional solution 42
 - log
 - creation with Tivoli Directory Integrator 362
 - monitoring 84
 - type 16, 20
- event source 16, 84
 - Active Directory 151
 - adding an ... 173
 - AIX 236
 - configuration 164
 - configuration portlet 57
 - custom integration 351
 - definition 352
 - Domino 250
 - Generic ExtendIT 380
 - SAP 261
 - ubiquitous 353

- W7Log 354
- external
 - auditor 48
- external API
 - event collection 65

F

- FIPS 34
 - protocol 38, 64, 71
- FISMA
 - reporting 34
- forensic
 - activity 98
 - search tool 45
- forensics 81
 - component 61
- four eyes principle 5
- frequency of checks 10
- FTP
 - collect 99
- functional design 89, 94
- functional requirements 133

G

- Gartner 19
- GEM
 - database 91
 - load problems 108
 - DB configuration 59
- General Scanning Language
 - see GSL
- Generic ExtendIT
 - collect script 381
 - event source 380
 - example 386
 - GML 386
 - grouping files 386
 - GSL 385
 - mapper 385
 - policy rules 386
- Generic Mapping Language
 - see GML
- GLBA
 - compliance management module 291
 - reporting 35
- GML 380
 - example 390
 - Generic ExtendIT 386

- Gramm-Leach-Bliley Act 408
- group
 - definition customization 196
- Grouped Server 79
- grouping file
 - example 393
- GSL 380
 - example 389
 - Generic ExtendIT 385
- Guardium 29

H

- Health Insurance Portability and Accountability Act
 - see HIPAA
- heterogeneous environment 102
- HIPAA 407
 - compliance management module 291
 - reporting 35
- historical log data 132

I

- IBM DB2
 - see DB2
- IBM Guardium 138
 - see Guardium
- IBM Security SiteProtector
 - see Security SiteProtector
- IBM Service Log logs 111
- IBM Support Assistant 110
- IBM System Storage DR550 113
- IBM Tivoli Directory Server
 - see Tivoli Directory Server
- IBM Tivoli Security Compliance Manager
 - see Security Compliance Manager
- IBM Tivoli Security Operations Manager
 - see Security Operations Manager
- identity and access management 34
- identity revalidation process 24
- impact correlation 47
- implementation 90, 102
 - approach 143
 - process 89
- incident
 - management 24, 36
 - response 36
- indexer 62, 72, 110
- Industry Regulation 7
- information retention 112

- Information Security Policy 20
- installation
 - log 110
- internal
 - auditor 48
- investigation 277
- ISO
 - 17799 297, 407, 409
 - compliance management module 291
 - 17991 reporting 35
 - 27001 409
 - reporting 35
 - 27002 409
 - Code of Practice for Information Security Management 35
- IT
 - security compliance 5
 - security policies 5, 143
 - strategy 24

J

- JVM message logs 111

L

- large deployment 102
- launchpad 63
- legal obligations 11
- level
 - of auditing 93
 - of automation 10
 - of reporting 10
- liability 403
- Linux
 - log collection 69
 - SSH collect 99
 - Syslog receiver 99
- load schedule 178
- loader process 44
- log
 - collect process 54
 - collection 34, 115
 - verification 39
 - completeness 39
 - continuity dashboard 115
 - data 113
 - capturing 17
 - normalization 35
 - requirements 355

- event collection 65
- file validation 379
- historical data 132
- management 33, 81, 270
 - ... for AIX 231
 - ... for Domino 250
 - ... for System z 295
- business drivers 9
- continuity report 57
- database 61
- depot 40, 54, 72
 - ubiquitous event source 353
- functional solution 38
- module 83
- reporting 61
- reports 75
- normalization 81
- ubiquitous collection 71
- Log Management Base 54, 81
- Log Management Server 54, 82, 85
- Log Manager
 - data process flow 71
 - user interface 57
- logging
 - business requirement 135
 - requirements
 - IT security policy 143
- login files
 - AIX 231
- Logon Failure Summary report 221
- logs 110

M

- machine group
 - System z 306
- Magic Quadrant for Security Information and Event Management 19
- maintain compliance 85
- maintenance
 - compliance 12
- managed security services 32
- Management Console 114
- mapper 60, 81, 385
 - example 389, 391
 - process 44
- medium deployment 101
- message log 111
- Microsoft Vista

- log collection 67
- Microsoft Windows
 - log collection 67
- monitored environment 23
- monitoring 19, 104
 - compliance 85
 - requirements 117

N

- NERC
 - reporting 35
- NetBIOS
 - event collection 65
- network
 - administrators 48
 - appliance auditing 100
 - models 94
 - operations 48
 - zones 97
- non-functional requirements 103, 140
- non-repudiation 292
- normalization 35, 81
 - component 58
 - process 43
 - data flow 76

O

- ODBC
 - event collection 65
- operational efficiency 91
- operational requirements 103, 140
- Orange book 408
- organizational
 - complexity 11
 - level design 24
 - level security control 5

P

- password
 - length 5
- patch management 24
- PCI DSS 7
 - reporting 35
- people events 21
- performance efficiency 12
- physical components 78
- platform events 385

- Point of Presence
 - Enterprise Server 96
 - port configuration 171
- policies and standards 12
- policy
 - analysis 60
 - breach on AIX 247
 - configuration portlets 60
 - corporate 403
 - definition
 - business requirement 137
 - exception report 194
 - exceptions 214
 - exceptions for AIX 246
 - framework 4
 - generator 60
 - mapping
 - results 209
 - rule 184, 194, 200, 386
 - System z 331
 - violations in Domino 254
- Policy Explorer 151
- practices 4, 405
- priority requirements 117
- privileged accounts 147
- privileged user access 132
- privileged user monitoring and auditing
 - business requirement 134
- problem management 24
- procedures 4, 405
- process
 - changes 16
 - level design 25
 - level security control 5
- processes 23
- processing creditcard information 7
- product support 116
- product use 90, 103
- project
 - analysis 91
 - definition 94
 - definition and planning 90, 94
 - implementation 102
 - management tasks 22
 - planning 94

R

RACF

- logon audit 302
- raw
 - data 113
- real-time event correlation 46
- receiver configuration 267
- Redbooks Web site 429
 - Contact us xiv
- regulatory
 - changes 16
 - compliance 91, 132
 - reporting 291
 - obligations 11
 - requirements 23, 131, 143
- remote collect 99
- report
 - collect history 56, 82
 - continuity 82
 - distributor 60
 - generator 60
 - log continuity 56
- reporting
 - business requirement 139
 - customized 278
 - detailed investigation 221
 - functional solution 42
 - Logon Failure Summary 221
 - policy exception 194
 - requirements 91, 117, 154, 297
- reporting database
 - configuration 59
 - creation 165
 - System z 306
- reports 23, 339
- risk
 - assessment 91, 142
 - management 8
- role 21
- root cause analysis 277
- rule-based correlation 46–47

S

SAN 91, 102, 113

SAP

- agent 261
- attention rules 264
- audit log 260
- event source 261
- Sarbanes-Oxley Act

- see SOX
- scalability 115
- scenario
 - business objectives 126
 - business requirements 132
 - cluster configuration 148
 - compliance monitoring 128
 - design objectives 140
 - functional requirements 133
 - high level design 148
 - implementation approach 143
 - IT environment 122
 - regulatory requirements 131
 - reporting requirements 154
- scope of compliance checking 10
- scoping configuration 60
- searcher 62, 110
- security
 - administrator 48
 - architecture 94
 - compliance architecture 15
 - compliance monitoring 128
 - controls 4–5, 9
 - dashboard 50
 - incident management 36
 - incident response capabilities 17
 - log 65
 - policies 5
 - policy 20, 23, 91
 - compliance management 17
 - policy framework 4, 11
 - policy matching 81
 - practices 4
 - procedures 4
 - risk 4
 - standard 20
 - standards 4, 20
- Security Compliance Manager 30
- Security Event Management
 - see SEM
- Security Group 79
- Security Information and Event Management
 - see SIEM
- Security Information and Event Manager
 - overview 33
- Security Information Management
 - see SIM
- Security Operations Manager 100
 - dashboard 36
 - event collector 32
- Security Server 79
- Security SiteProtector 28
- self audit 138, 225
- SEM 17
 - market definition 17
- separation of duty 5
- server
 - synchronization 109
- service level reporting 36
- service oriented architecture
 - see SOA
- shadow system 126
- SIEM 17
 - architecture 18–19, 36
 - integration scenarios 48
 - market definition 17
 - solution architecture 22
- SIM 17
 - market definition 17
 - Module 83
- small deployment 100
- SMF data 307
- SNMP
 - collection 99
 - collection of log data 70
 - data processing flow 73
 - event collection 65
 - high performance collector 36
 - ubiquitous event source 353
- SOA
 - compliance challenge 12
- Solaris 92
- solution
 - architecture 22
 - constraints 91
 - design 89
- SOX 23, 407
 - business requirement 133
 - compliance management module 291
 - reporting 34
- special attention 217
- spot check 10
- SSH
 - audit data collection 235
 - collection 99
 - data flow log collection 74
 - event collection 65
 - ubiquitous event source 353

- Standard Server 45, 54, 83, 86
 - event source configuration 164
 - installation 153
 - W7 rules configuration 184
- standards 405
- statistical
 - correlation 47
- Storage Area Network
 - see SAN
- successful archiving 39
- support 116
- susceptibility correlation 47
- synchronization
 - ... of servers 109
- syslog 267
 - collection 99
 - collection of log data 70
 - data collection 115
 - data processing flow 73
 - event collection 65
 - high performance collector 36
 - ubiquitous event source 353
- syslog-ng 99
- system level design 24
- System Management Facilities 300
- System z
 - actuator 307
 - Agent installation 310
 - attention rule 332
 - audit settings 299
 - Basel II compliance 327
 - collect schedule 311
 - collect strategy 317
 - event source 316
 - integration overview 35
 - log management 295
 - LPAR recommendations 311
 - policy rule 331
 - reporting requirements 297
 - SMF data 307
- systematic attack detection 278

T

- target
 - system 23
 - user 23
- technical
 - direction 15

- security control 5
- tasks 22
- technological complexity 11
- technology changes 16
- threat
 - analysis 46
 - management 17
- threshold event 279
- Tivoli Common Reporting 62, 75
 - syslog reporting 272
- Tivoli Directory Integrator
 - event log creation 362
- Tivoli Directory Server 56
 - Security Server 79
- Tivoli Integrated Portal 57, 104–105
- trace log 111
- trend analysis 81
- trends 224
- troubleshooting
 - IBM Support Assistant 110
 - installation log 110
 - message log 111
 - trace log 111

U

- ubiquitous
 - event source 353
 - summary 394
 - log collection 71
 - syslog receiver 267
- UK Data Protection Act 1998 410
- UNIX
 - log collection 69
 - SSH collect 99
- user behavior 21
- user information source 184, 395
- user management 57

V

- verification reports 220
- Virtual IP Addressing 314
- vulnerability
 - correlation 47

W

- W7
 - attention rule 203

- Classification Template 329
- groups 151, 184, 194, 337
- log event source 354
 - summary 394
- log format
 - transformation 357
- log validator 358
- methodology 88
- normalization 58, 60, 83
- policy rule 200
- reporting 62
- rules
 - configuration 184, 194
 - example 44
- Windows
 - audit subsystem 92
 - event management API 99
 - levels of auditing 93
- Windows 2003 Server
 - audit policy 155
- work policy
 - creation 194

Z

- z/OS
 - integration overview 35

Archived



Redbooks

IT Security Compliance Management Design Guide with IBM Tivoli Security Information and Event Manager

(1.0" spine)
0.875" <-> 1.498"
460 <-> 788 pages



IT Security Compliance Management Design Guide

with IBM Tivoli Security Information and Event Manager



Enterprise integration for operational and regulatory compliance

Complete architecture and component discussion

Deployment scenario with hands-on details

To comply with government and industry regulations, such as Sarbanes-Oxley, Gramm Leach Bliley (GLBA), and COBIT (which can be considered a best-practices framework), organizations must constantly detect, validate, and report unauthorized changes and out-of-compliance actions within the Information Technology (IT) infrastructure. Using the IBM Tivoli Security Information and Event Manager solution organizations can improve the security of their information systems by capturing comprehensive log data, correlating this data through sophisticated log interpretation and normalization, and communicating results through a dashboard and full set of audit and compliance reporting.

In this IBM Redbooks publication, we discuss the business context of security audit and compliance software for organizations and describe the logical and physical components of IBM Tivoli Security Information and Event Manager. We also present a typical deployment within a business scenario.

This book is a valuable resource for security officers, administrators, and architects who want to understand and implement a centralized security audit and compliance solution.

INTERNATIONAL TECHNICAL SUPPORT ORGANIZATION

BUILDING TECHNICAL INFORMATION BASED ON PRACTICAL EXPERIENCE

IBM Redbooks are developed by the IBM International Technical Support Organization. Experts from IBM, Customers and Partners from around the world create timely technical information based on realistic scenarios. Specific recommendations are provided to help you implement IT solutions more effectively in your environment.

For more information:
ibm.com/redbooks