Security management solutions
To support your IT objectives

Tivoli. software

Learn how 10 reports can help you address the most pressing privileged user monitoring and auditing challenges.

While most organizations have concentrated their network security initiatives on neutralizing outside hackers and intruders, the fact is that threats from inside may represent a more significant source of damage.

Even if it isn't practical to deny privileged users access, monitoring their activities is critical — because both accidental and malicious violations by "insiders" can cause considerable harm to your enterprise. IBM Tivoli® Compliance Insight Manager includes powerful tools for fighting insider threats, including the top 10 best-practice reports for monitoring and auditing privileged user activity in your enterprise.

By providing acute visibility into insider threat activity, the Tivoli Compliance Insight Manager reporting engine for audit and compliance initiatives could be an invaluable asset in maintaining network security.

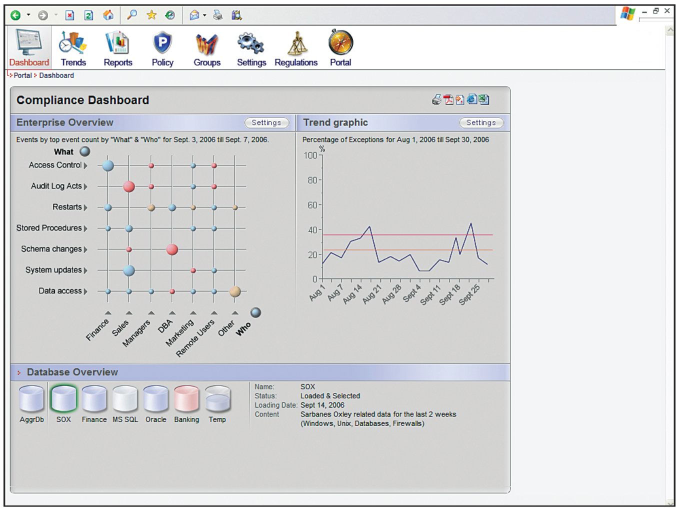
Who is more likely to damage your network — an outside hacker, or an authorized employee, customer, partner or outsourcer? The answer is, perhaps surprisingly, the latter. Regulatory and auditing requirements make it clear that existing security technology's emphasis on network-level, externally oriented threats is misplaced. The far more likely suspects are the privileged users inside your enterprise — who are on your network every day and may cause damage not only of a malicious nature but also accidentally.

In addition, Payment Card Industry Data Security Standard (PCI DSS), Sarbanes-Oxley (SOX), Gramm-Leach-Bliley Act (GLBA) and Health Insurance Portability and Accountability Act (HIPAA) audits make it clear that the activities of privileged users (such as administrators and network managers) are a legitimate concern.

Regulations and auditors are both likely to raise these questions, for which you must have ready answers:

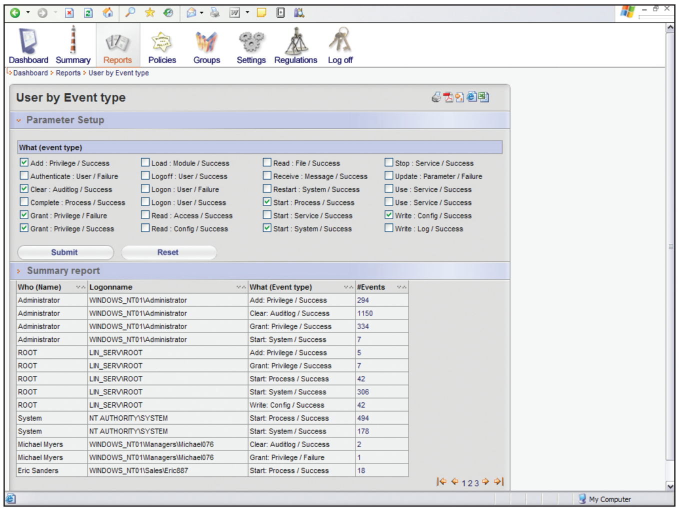
- **What are administrators, database administrators and root users doing on your network?**
- **Were system changes authorized?**
- **Was privileged access used to violate separation of duties?**
- **Did a disgruntled administrator make an attempt at identity theft?**
- **Has confidential or regulated data been viewed by administrators?**

Turn the page to see how the top 10 reports for privileged user activity monitoring in Tivoli Compliance Insight Manager can help ensure that you have quick and suitable answers to all these questions — and more.



Name: SOX
Status: Loaded & Selected
Loading Date: Sept 14, 2006
Content Sarbanes Oxley related data for the last 2 weeks (Windows, Unix, Databases, Firewalls)

The enterprise dashboard gives you insight into all activities on the system. In this case, someone classified as a manager is performing audit log actions and administrators are accessing data — both clear violations of acceptable use guidelines.



What (event type)

☑ Add : Privilege / Success
□ Authenticate : User / Failure
☑ Clear : Auditlog / Success
□ Complete : Process / Success
☑ Grant : Privilege / Failure
☑ Grant : Privilege / Success
□ Load : Module / Success
□ Logoff : User / Success
□ Logon : User / Failure
□ Logon : User / Success
□ Read : Access / Success
□ Read : Config / Success
□ Read : File / Success
□ Receive : Message / Success
□ Restart : System / Success
☑ Start : Process / Success
□ Start : Service / Success
☑ Start : System / Success
□ Stop : Service / Success
□ Update : Parameter / Failure
□ Use : Service / Success
□ Use : Service / Success
☑ Write : Config / Success
□ Write : Log / Success

Who (Name)	Logonname	What (Event type)	#Events
Administrator	WINDOWS_NT01\Administrator	Add: Privilege / Success	294
Administrator	WINDOWS_NT01\Administrator	Clear: Auditlog / Success	1150
Administrator	WINDOWS_NT01\Administrator	Grant: Privilege / Success	334
Administrator	WINDOWS_NT01\Administrator	Start: System / Success	7
ROOT	LIN_SERV\ROOT	Add: Privilege / Success	5
ROOT	LIN_SERV\ROOT	Grant: Privilege / Success	7
ROOT	LIN_SERV\ROOT	Start: Process / Success	42
ROOT	LIN_SERV\ROOT	Start: System / Success	306
ROOT	LIN_SERV\ROOT	Write: Config / Success	42
System	NT AUTHORITY\SYSTEM	Start: Process / Success	494
System	NT AUTHORITY\SYSTEM	Start: System / Success	178
Michael Myers	WINDOWS_NT01\Managers\Michael076	Clear: Auditlog / Success	2
Michael Myers	WINDOWS_NT01\Managers\Michael076	Grant: Privilege / Failure	1
Eric Sanders	WINDOWS_NT01\Sales\Eric887	Start: Process / Success	18

1 2 3

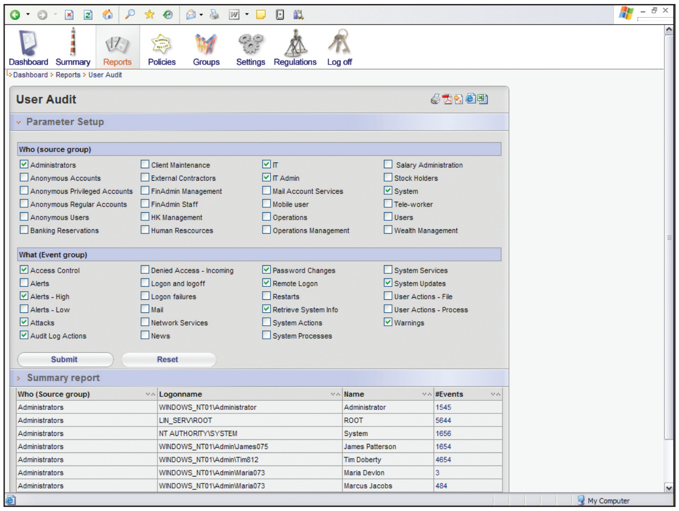
The user by event type report gives you a quick, comprehensive view of administrative activities across your enterprise and who is performing them. Here you can quickly ascertain if any nonadministrators made privileged changes on the system — a topic your auditor will surely be interested in.

1. Enterprise dashboard

The Tivoli Compliance Insight Manager enterprise dashboard allows you to view all activities on the system, including people, activities and objects. The size of each circle correlates to the amount of activity it represents, while color indicates the level of compliance. Red circles indicate areas of particular risk — cases in which your acceptable use policy is being violated. The lower portion of the screen juxtaposes people and activities, highlighting potential violations.

2. User by event type

It's important to be able to home in on all administrative activities across your enterprise and see who performed them. The user by event type report in Tivoli Compliance Insight Manager allows you to do just that, by showing each person who conducted an activity and the types of activities conducted. Greater detail on the activities in question is just a click away.



User Audit

Parameter Setup

Who (source group)

☑ Administrators
☐ Anonymous Accounts
☐ Anonymous Privileged Accounts
☐ Anonymous Regular Accounts
☐ Anonymous Users
☐ Banking Reservations
☐ Client Maintenance
☐ External Contractors
☐ FinAdmin Management
☐ FinAdmin Staff
☐ HK Management
☐ Human Rescources
☑ IT
☑ IT Admin
☐ Mail Account Services
☐ Mobile user
☐ Operations
☐ Operations Management
☐ Salary Administration
☐ Stock Holders
☑ System
☐ Tele-worker
☐ Users
☐ Wealth Management

What (Event group)

☑ Access Control
☐ Alerts
☑ Alerts - High
☐ Alerts - Low
☑ Attacks
☑ Audit Log Actions
☐ Denied Access - Incoming
☐ Logon and logoff
☐ Logon failures
☐ Mail
☐ Network Services
☐ News
☑ Password Changes
☑ Remote Logon
☐ Restarts
☑ Retrieve System Info
☐ System Actions
☐ System Processes
☐ System Services
☑ System Updates
☐ User Actions - File
☐ User Actions - Process
☑ Warnings

Submit Reset

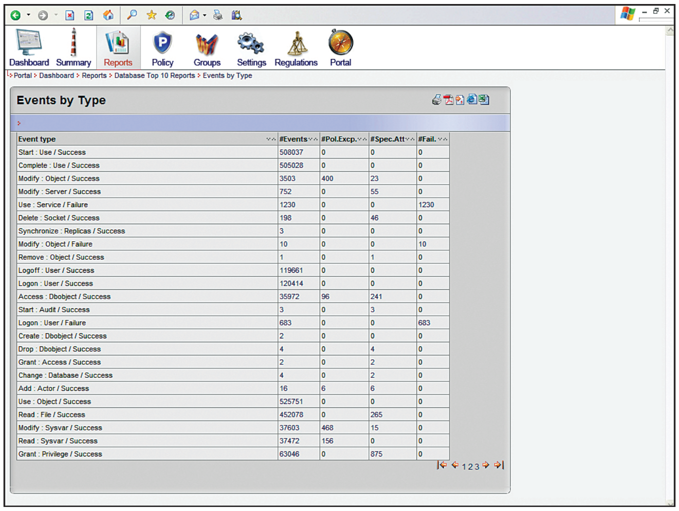
Summary report

Who (Source group)	Logonname	Name	#Events
Administrators	WINDOWS_NT01\Administrator	Administrator	1545
Administrators	LIN_SERV\ROOT	ROOT	5644
Administrators	NT AUTHORITY\SYSTEM	System	1656
Administrators	WINDOWS_NT01\Admin\James075	James Patterson	1654
Administrators	WINDOWS_NT01\Admin\Tim812	Tim Doberty	4654
Administrators	WINDOWS_NT01\Admin\Maria073	Maria Devlon	3
Administrators	WINDOWS_NT01\Admin\Maria073	Marcus Jacobs	484

The user audit report shows who is conducting administrative activities and how often.

3. Overview of select users and their activities

The user audit report in Tivoli Compliance Insight Manager is the ideal report for use in a PCI, HIPAA or ISO compliance audit. This report allows you to select administrators, then select specific activities that are of the most concern.


Dashboard
Summary
Reports
Policy
Groups
Settings
Regulations
Portal
Portal > Dashboard > Reports > Database Top 10 Reports > Events by Type

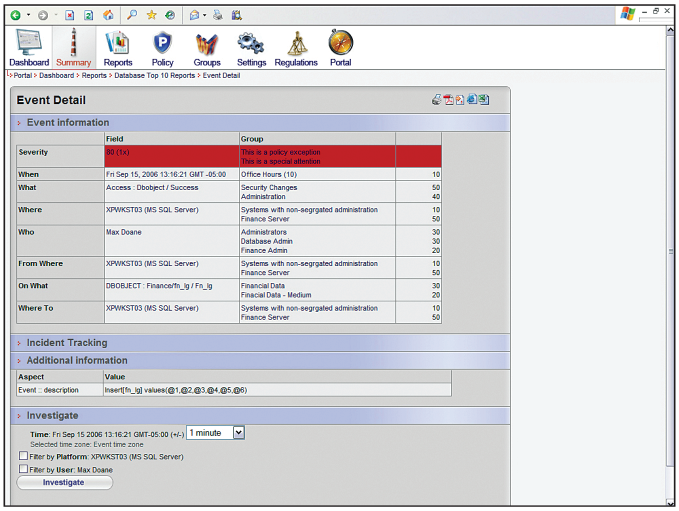
Events by Type

Event type	#Events	#Pol.Excp.	#Spec.Att	#Fail.
Start : Use / Success	508037	0	0	0
Complete : Use / Success	505028	0	0	0
Modify : Object / Success	3503	400	23	0
Modify : Server / Success	752	0	55	0
Use : Service / Failure	1230	0	0	1230
Delete : Socket / Success	198	0	46	0
Synchronize : Replicas / Success	3	0	0	0
Modify : Object / Failure	10	0	0	10
Remove : Object / Success	1	0	1	0
Logoff : User / Success	119661	0	0	0
Logon : User / Success	120414	0	0	0
Access : Dbobject / Success	35972	96	241	0
Start : Audit / Success	3	0	3	0
Logon : User / Failure	683	0	0	683
Create : Dbobject / Success	2	0	0	0
Drop : Dbobject / Success	4	0	4	0
Grant : Access / Success	2	0	2	0
Change : Database / Success	4	0	2	0
Add : Actor / Success	16	6	6	0
Use : Object / Success	525751	0	0	0
Read : File / Success	452078	0	265	0
Modify : Sysvar / Success	37603	468	15	0
Read : Sysvar / Success	37472	156	0	0
Grant : Privilege / Success	63046	0	875	0

The events by type report lets you examine how many events have occurred, how many violated your security policies and how many sets of attention alerts and actions failed.

4. Events by type

The Tivoli Compliance Insight Manager events by type report provides a focused view of activities on your network, and helps demonstrate to auditors that you have sufficient insight into them.


Dashboard
Summary
Reports
Policy
Groups
Settings
Regulations
Portal
Portal > Dashboard > Reports > Database Top 10 Reports > Event Detail

Event Detail

Event information

	Field	Group	
Severity	80 (1x)	This is a policy exception This is a special attention	
When	Fri Sep 15, 2006 13:16:21 GMT -05:00	Office Hours (10)	10
What	Access : Dbobject / Success	Security Changes Administration	50 40
Where	XPWKST03 (MS SQL Server)	Systems with non-segrgated administration Finance Server	10 50
Who	Max Doane	Administrators Database Admin Finance Admin	30 30 20
From Where	XPWKST03 (MS SQL Server)	Systems with non-segrgated administration Finance Server	10 50
On What	DBOBJECT : Finance/fn_lg / Fn_lg	Financial Data Finacial Data - Medium	30 20
Where To	XPWKST03 (MS SQL Server)	Systems with non-segrgated administration Finance Server	10 50

Incident Tracking

Additional information

Aspect	Value
Event :: description	Insert[fn_lg] values(@1,@2,@3,@4,@5,@6)

Investigate

Time: Fri Sep 15 2006 13:16:21 GMT-05:00 (+/-) 1 minute

Selected time zone: Event time zone

☐ Filter by **Platform**: XPWKST03 (MS SQL Server)

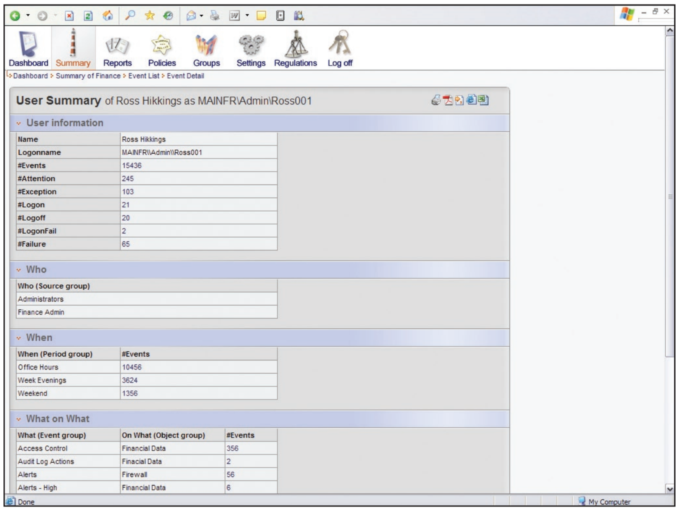
☐ Filter by **User**: Max Doane

Investigate

The event detail report allows you to "zoom in" on every detail of an incident, escalate it to a workflow system through tracking and continue your investigation in even greater detail.

5. Detailed incident investigation

The event detail report in Tivoli Compliance Insight Manager provides all the documentation available on any incident, up to and including details such as the time and origin of the incident. In fact, the detailed incident investigation report provides all the details, at a field level and with the policy groups.



User Summary of Ross Hikkings as MAINFR\Admin\Ross001

User information

Name	Ross Hikkings
Logonname	MAINFR\\Admin\\Ross001
#Events	15436
#Attention	245
#Exception	103
#Logon	21
#Logoff	20
#LogonFail	2
#Failure	65

Who

Who (Source group)
Administrators
Finance Admin

When

When (Period group)	#Events
Office Hours	10456
Week Evenings	3624
Weekend	1356

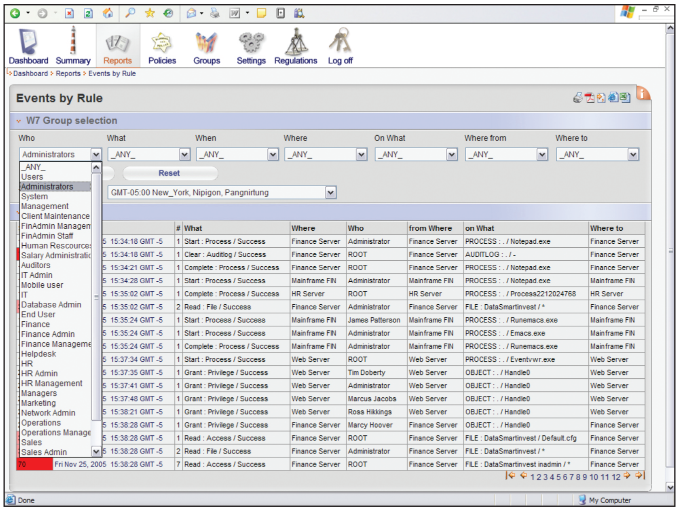
What on What

What (Event group)	On What (Object group)	#Events
Access Control	Financial Data	356
Audit Log Actions	Finacial Data	2
Alerts	Firewall	56
Alerts - High	Financial Data	6

The user summary report allows you to "zoom in" to analyze a suspected user and his or her recent actions.

6. User investigation

When an incident occurs and a privileged user's activities are suspect, it's critical to be able to view the details of that user's recent actions. The Tivoli Compliance Insight Manager user summary report gives you a close-up view into how many events that user created, when they occurred, how many were policy violations, attention alerts or failures and what groups the user belongs to.



Dashboard > Reports > Events by Rule

Events by Rule

W7 Group selection

Who	What	When	Where	On What	Where from	Where to
Administrators	_ANY_	_ANY_	_ANY_	_ANY_	_ANY_	_ANY_

ANY
Users
Administrators
System
Management
Client Maintenance
FinAdmin Managem
FinAdmin Staff
Human Rescource
Salary Administratio
Auditors
IT Admin
Mobile user
IT
Database Admin
End User
Finance
Finance Admin
Finance Manageme
Helpdesk
HR
HR Admin
HR Management
Managers
Marketing
Network Admin
Operations
Operations Manage
Sales
Sales Admin

GMT-05:00 New_York, Nipigon, Pangnirtung

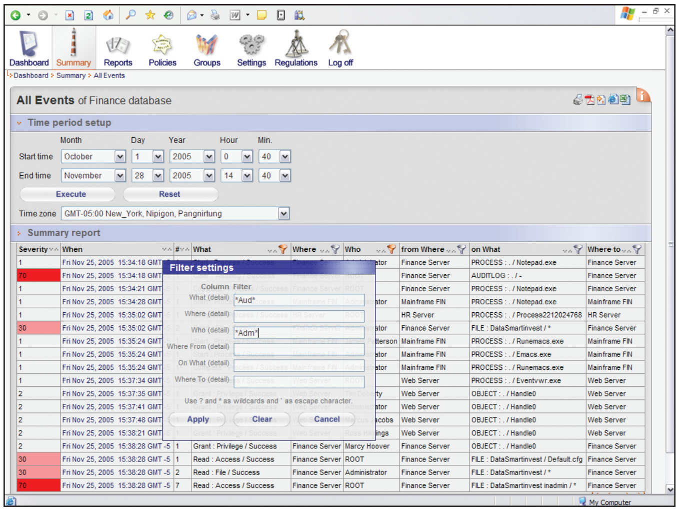
		#	What	Where	Who	from Where	on What	Where to
	5 15:34:18 GMT -5	1	Start : Process / Success	Finance Server	Administrator	Finance Server	PROCESS : . / Notepad.exe	Finance Server
	5 15:34:18 GMT -5	1	Clear : Auditlog / Success	Finance Server	ROOT	Finance Server	AUDITLOG : . / -	Finance Server
	5 15:34:21 GMT -5	1	Complete : Process / Success	Finance Server	ROOT	Finance Server	PROCESS : . / Notepad.exe	Finance Server
	5 15:34:28 GMT -5	1	Start : Process / Success	Mainframe FIN	Administrator	Mainframe FIN	PROCESS : . / Notepad.exe	Mainframe FIN
	5 15:35:02 GMT -5	1	Complete : Process / Success	HR Server	ROOT	HR Server	PROCESS : . / Process2212024768	HR Server
	5 15:35:02 GMT -5	2	Read : File / Success	Finance Server	Administrator	Finance Server	FILE : DataSmartinvest / *	Finance Server
	5 15:35:24 GMT -5	1	Start : Process / Success	Mainframe FIN	James Patterson	Mainframe FIN	PROCESS : . / Runemacs.exe	Mainframe FIN
	5 15:35:24 GMT -5	1	Start : Process / Success	Mainframe FIN	Administrator	Mainframe FIN	PROCESS : . / Emacs.exe	Mainframe FIN
	5 15:35:24 GMT -5	1	Complete : Process / Success	Mainframe FIN	Administrator	Mainframe FIN	PROCESS : . / Runemacs.exe	Mainframe FIN
	5 15:37:34 GMT -5	1	Start : Process / Success	Web Server	ROOT	Web Server	PROCESS : . / Eventvwr.exe	Web Server
	5 15:37:35 GMT -5	1	Grant : Privilege / Success	Web Server	Tim Doberty	Web Server	OBJECT : . / Handle0	Web Server
	5 15:37:41 GMT -5	1	Grant : Privilege / Success	Web Server	Administrator	Web Server	OBJECT : . / Handle0	Web Server
	5 15:37:48 GMT -5	1	Grant : Privilege / Success	Web Server	Marcus Jacobs	Web Server	OBJECT : . / Handle0	Web Server
	5 15:38:21 GMT -5	1	Grant : Privilege / Success	Web Server	Ross Hikkings	Web Server	OBJECT : . / Handle0	Web Server
	5 15:38:28 GMT -5	1	Grant : Privilege / Success	Finance Server	Marcy Hoover	Finance Server	OBJECT : . / Handle0	Finance Server
	5 15:38:28 GMT -5	1	Read : Access / Success	Finance Server	ROOT	Finance Server	FILE : DataSmartinvest / Default.cfg	Finance Server
	5 15:38:28 GMT -5	2	Read : File / Success	Finance Server	Administrator	Finance Server	FILE : DataSmartinvest / *	Finance Server
70	Fri Nov 25, 2005 15:38:28 GMT -5	7	Read : Access / Success	Finance Server	ROOT	Finance Server	FILE : DataSmartinvest inadmin / *	Finance Server

1 2 3 4 5 6 7 8 9 10 11 12

With the events by rule report you can conduct investigations more efficiently, simply by selecting only the user groups you want to view. For example, to investigate a privileged user, you simply select the "Administrators" group and begin.

7. Events by rule

Being able to sift quickly through complex information is an attribute of any good report. The Tivoli Compliance Insight Manager events by rule report facilitates a quick understanding of specific events, by letting you select only the groups you want to view.



Dashboard > Summary > All Events

All Events of Finance database

Time period setup

	Month	Day	Year	Hour	Min.
Start time	October	1	2005	0	40
End time	November	28	2005	14	40

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

Summary report

Filter settings

Column Filter
What (detail) *Aud*
Where (detail)
Who (detail) *Adm*
Where From (detail)
On What (detail)
Where To (detail)

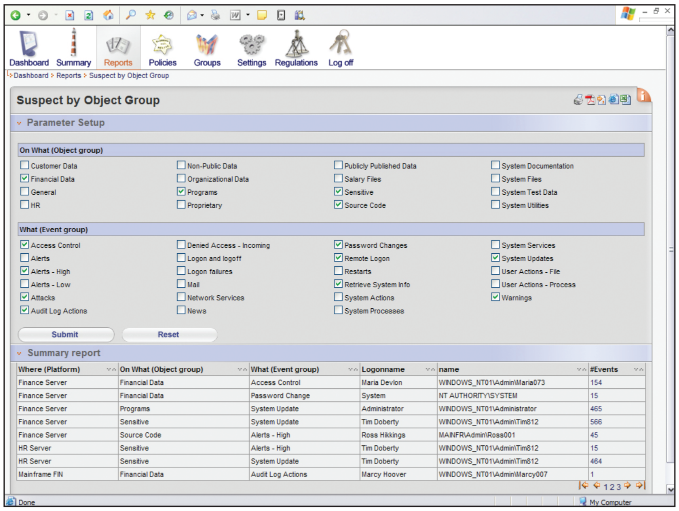
Use ? and * as wildcards and ` as escape character.

Severity	When	#	What	Where	Who	from Where	on What	Where to
1	Fri Nov 25, 2005 15:34:18 GMT		Start : Process / Success	Finance Server	Administrator	Finance Server	PROCESS : . / Notepad.exe	Finance Server
70	Fri Nov 25, 2005 15:34:18 GMT -5	1	Clear : Auditlog / Success	Finance Server	ROOT	Finance Server	AUDITLOG : . / -	Finance Server
1	Fri Nov 25, 2005 15:34:21 GMT -5	1	Complete : Process / Success	Finance Server	ROOT	Finance Server	PROCESS : . / Notepad.exe	Finance Server
1	Fri Nov 25, 2005 15:34:28 GMT -5	1	Start : Process / Success	Mainframe FIN	Administrator	Mainframe FIN	PROCESS : . / Notepad.exe	Mainframe FIN
1	Fri Nov 25, 2005 15:35:02 GMT -5	1	Complete : Process / Success	HR Server	ROOT	HR Server	PROCESS : . / Process2212024768	HR Server
30	Fri Nov 25, 2005 15:35:02 GMT -5	2	Read : File / Success	Finance Server	Administrator	Finance Server	FILE : DataSmartinvest / *	Finance Server
1	Fri Nov 25, 2005 15:35:24 GMT -5	1	Start : Process / Success	Mainframe FIN	James Patterson	Mainframe FIN	PROCESS : . / Runemacs.exe	Mainframe FIN
1	Fri Nov 25, 2005 15:35:24 GMT -5	1	Start : Process / Success	Mainframe FIN	Administrator	Mainframe FIN	PROCESS : . / Emacs.exe	Mainframe FIN
1	Fri Nov 25, 2005 15:35:24 GMT -5	1	Complete : Process / Success	Mainframe FIN	Administrator	Mainframe FIN	PROCESS : . / Runemacs.exe	Mainframe FIN
1	Fri Nov 25, 2005 15:37:34 GMT -5	1	Start : Process / Success	Web Server	ROOT	Web Server	PROCESS : . / Eventvwr.exe	Web Server
2	Fri Nov 25, 2005 15:37:35 GMT -5	1	Grant : Privilege / Success	Web Server	Tim Doberty	Web Server	OBJECT : . / Handle0	Web Server
2	Fri Nov 25, 2005 15:37:41 GMT -5	1	Grant : Privilege / Success	Web Server	Administrator	Web Server	OBJECT : . / Handle0	Web Server
2	Fri Nov 25, 2005 15:37:48 GMT -5	1	Grant : Privilege / Success	Web Server	Marcus Jacobs	Web Server	OBJECT : . / Handle0	Web Server
2	Fri Nov 25, 2005 15:38:21 GMT -5	1	Grant : Privilege / Success	Web Server	Ross Hikkings	Web Server	OBJECT : . / Handle0	Web Server
2	Fri Nov 25, 2005 15:38:28 GMT -5	1	Grant : Privilege / Success	Finance Server	Marcy Hoover	Finance Server	OBJECT : . / Handle0	Finance Server
30	Fri Nov 25, 2005 15:38:28 GMT -5	1	Read : Access / Success	Finance Server	ROOT	Finance Server	FILE : DataSmartinvest / Default.cfg	Finance Server
30	Fri Nov 25, 2005 15:38:28 GMT -5	2	Read : File / Success	Finance Server	Administrator	Finance Server	FILE : DataSmartinvest / *	Finance Server
70	Fri Nov 25, 2005 15:38:28 GMT -5	7	Read : Access / Success	Finance Server	ROOT	Finance Server	FILE : DataSmartinvest inadmin / *	Finance Server

The all events report with search filter allows you to narrow your search for violations. Here, a search for administrators tampering with audit settings has uncovered an instance of the audit log being cleared — a clear policy violation.

8. All events with search filter

Tivoli Compliance Insight Manager includes this report to allow you to truly narrow your search while you investigate privileged user activities. The search filter in the all events report uses Boolean search capabilities to eliminate millions of events from your view, retaining only those you are concerned about.



Dashboard > Reports > Suspect by Object Group

Suspect by Object Group

Parameter Setup

On What (Object group)

☐ Customer Data
☑ Financial Data
☐ General
☐ HR
☐ Non-Public Data
☐ Organizational Data
☑ Programs
☐ Proprietary
☐ Publicly Published Data
☐ Salary Files
☑ Sensitive
☑ Source Code
☐ System Documentation
☐ System Files
☐ System Test Data
☐ System Utilities

What (Event group)

☑ Access Control
☐ Alerts
☑ Alerts - High
☐ Alerts - Low
☑ Attacks
☑ Audit Log Actions
☐ Denied Access - Incoming
☐ Logon and logoff
☐ Logon failures
☐ Mail
☐ Network Services
☐ News
☑ Password Changes
☑ Remote Logon
☐ Restarts
☑ Retrieve System Info
☐ System Actions
☐ System Processes
☐ System Services
☑ System Updates
☐ User Actions - File
☐ User Actions - Process
☑ Warnings

Summary report

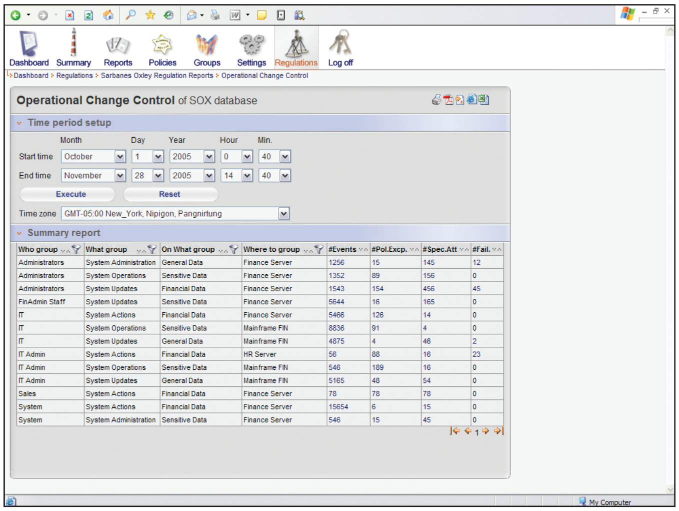
Where (Platform)	On What (Object group)	What (Event group)	Logonname	name	#Events
Finance Server	Financial Data	Access Control	Maria Devlon	WINDOWS_NT01\Admin\Maria073	154
Finance Server	Financial Data	Password Change	System	NT AUTHORITY\SYSTEM	15
Finance Server	Programs	System Update	Administrator	WINDOWS_NT01\Administrator	465
Finance Server	Sensitive	System Update	Tim Doberty	WINDOWS_NT01\Admin\Tim812	566
Finance Server	Source Code	Alerts - High	Ross Hikkings	MAINFR\Admin\Ross001	45
HR Server	Sensitive	Alerts - High	Tim Doberty	WINDOWS_NT01\Admin\Tim812	15
HR Server	Sensitive	System Update	Tim Doberty	WINDOWS_NT01\Admin\Tim812	464
Mainframe FIN	Financial Data	Audit Log Actions	Marcy Hoover	WINDOWS_NT01\Admin\Marcy007	1

1 2 3

Who is tampering with your protected data? The suspect by object group report will answer that question and facilitate further investigation.

9. Sensitive data tampering

The suspect by object group report in Tivoli Compliance Insight Manager provides information on who may be tampering with protected data, such as the data associated with SOX, PCI, HIPAA or GLBA. Simply by selecting the data you want to investigate, then narrowing the search to privileged activities, you can uncover such activity occurring on financial, credit, patient or customer data.



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

Operational Change Control of SOX database

Time period setup

	Month	Day	Year	Hour	Min.
Start time	October	1	2005	0	40
End time	November	28	2005	14	40

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

Summary report

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

1

The operational change control report monitors administrative changes across platforms, reports on administrative activities and allows for "click-through" investigation.

10. Operational change management

Monitoring administrative changes is critical, and the operational change control report lets you get a handle on such changes. This part of Tivoli Compliance Insight Manager follows best-practice advice from ISO, providing an overview of changes made. It also allows you and the auditor to verify that those changes adhere to policy.

Use these 10 ways to achieve network security

Tivoli Compliance Insight Manager and its top 10 reports for privileged user activity monitoring provide a better view of what these users are doing on your enterprise network. By using Tivoli Compliance Insight Manager to monitor and neutralize insider threats to your network, you help significantly enhance network security, while confidently meeting auditor requirements.

For more information

To learn more about how Tivoli Compliance Insight Manager can help your organization monitor and audit privileged user activity, contact your IBM representative or IBM Business Partner, or visit **ibm.com**/tivoli

About Tivoli software from IBM

Tivoli software provides a set of offerings and capabilities in support of IBM Service Management, a scalable, modular approach used to deliver more efficient and effective services to your business. Helping meet the needs of any size business, Tivoli software enables you to deliver service excellence in support of your business objectives through integration and automation of processes, workflows and tasks. The security-rich, open standards–based Tivoli service management platform is complemented by proactive operational management solutions that provide end-to-end visibility and control. It is also backed by world-class IBM Services, IBM Support and an active ecosystem of IBM Business Partners. Tivoli customers and business partners can also leverage each other's best practices by participating in independently run IBM Tivoli User Groups around the world — visit www.tivoli-ug.org

IBM Corporation
Software Group
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
9-07
All Rights Reserved

Disclaimer: The customer is responsible for ensuring compliance with legal requirements. It is the customer's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the reader may have to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer is in compliance with any law or regulation.

TAKE BACK CONTROL WITH Tivoli.