Alfonso Ponticelli

Tivoli Security Specialist

La soluzione IBM per la gestione dei log e l'audit degli accessi alle risorse elaborative

Le domande più frequenti

Le domande dell'IT e del Business management:

- Siamo in grado di controllare se esistono manipolazioni di info sensibili?
- Possiamo verificare le attività degli outsourcers?
- Possiamo ottenere segnalazioni a fronte di attività non autorizzate?
- Riusciamo a dimostrare la validità della segregation of duties?
- Possiamo investigare su quanto accaduto in modo tempestivo?

Le domande dell'IT e del Business management:

- Vengono tracciati e visionate i log di applicazioni, database, S.O. e device?
- Sono le attività dei system administrator, DBA e system operator tracciate nei log e verificate in maniera regolare?
- Sono tracciati gli accessi a dati sensibili – incluso root/administration e i DBA – nei vari log?
- Esistono dei tool automatici per i processi di audit?
- Sono gli incidenti di sicurezza o attività sospette analizzate al fine di intraprendere delle azioni correttive?

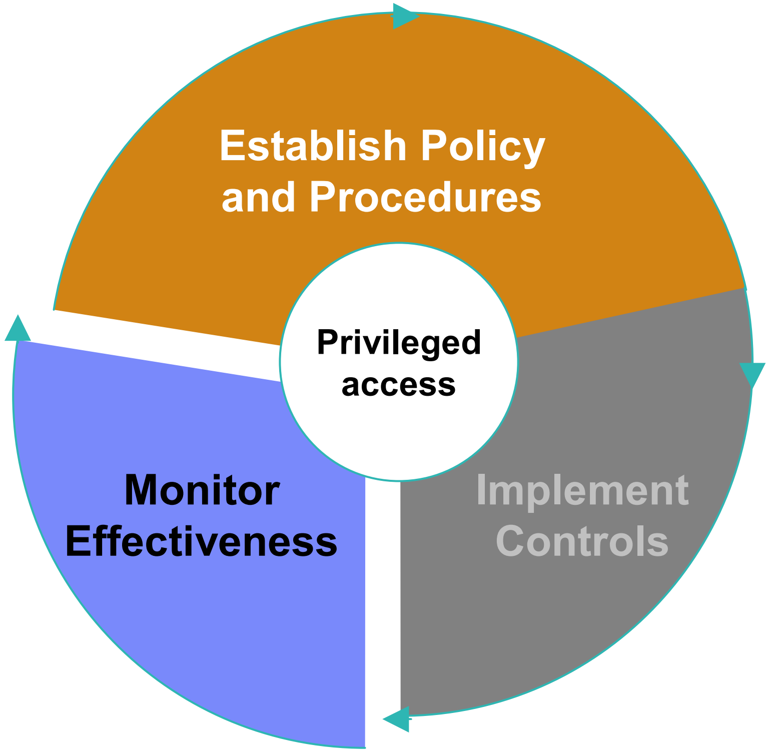
Cosa è rilevante ?

Categoria	Descrizione
Eventi di autenticazione	Eventi di logon / logoff
Eventi di gestione	Start di server, stop, back-up, restore
Change management	Modifiche di configurazione, modifiche sui processi di auditing, modifiche sulla struttura dei database, attività di manutenzione
Gestione utenze	Creazione di nuove utenze, modifica dei privilegi utente, attività di cambio password
Diritti di accesso	Comportamento di tutti i DBA includendo gli accessi ai dati, DBCC (Database Console Command), call a stored procedure
Accesso ai dati sensibili	Tutti gli accessi ai dati sensibili immagazzinati nei database e quindi operazioni di: select, insert, update, delete

La soluzione: la gestione degli utenti

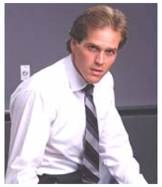
Le difficoltà

- Ogni sorgente ha la sua sintassi
- Non basta archiviare ma bisogna poter effettuare interrogazioni
- Enorme quantità di dati
- Interpretazione degli eventi



Quali sono gli ambiti per i quali serve aiuto ?

Problema

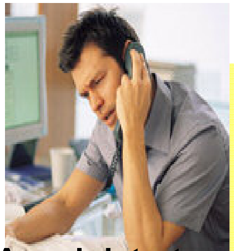


CFO/CIO

Dimostrare la compliance con le regolamentazioni

CISO/Audit

Proteggere la proprietà intellettuale ed assicurare correttamente la privacy



Amministratore della Sicurezza

Gestire la sicurezza operativa in maniera efficiente ed efficace

Funzionalità della Soluzione TSIEM

Dashboard per la Security compliance e reporting

1. Compliance dashboard
2. Regulatory reporting

Audit del comportamento degli utenti

3. Privileged user monitoring and audit (PUMA)
4. Audit di Database ed applicazioni
5. Audit di sistemi operativi e mainframe
6. Integrazione con strumenti di identity management

Security Operations Management

7. Incident mgt e dashboard per la sicurezza operativa
8. Log management e reporting
9. Correlazione di eventi real time
10. Integrazione con IT Operations

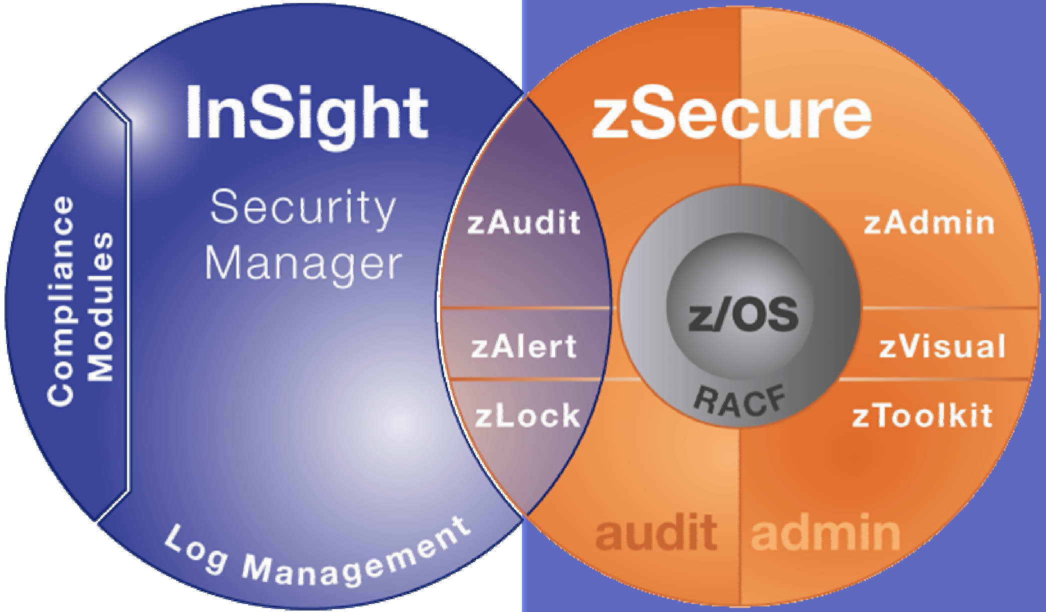
Tivoli Compliance Insight Manager

TCIM

Tivoli Compliance: soluzione

Consul **InSight**™ Suite

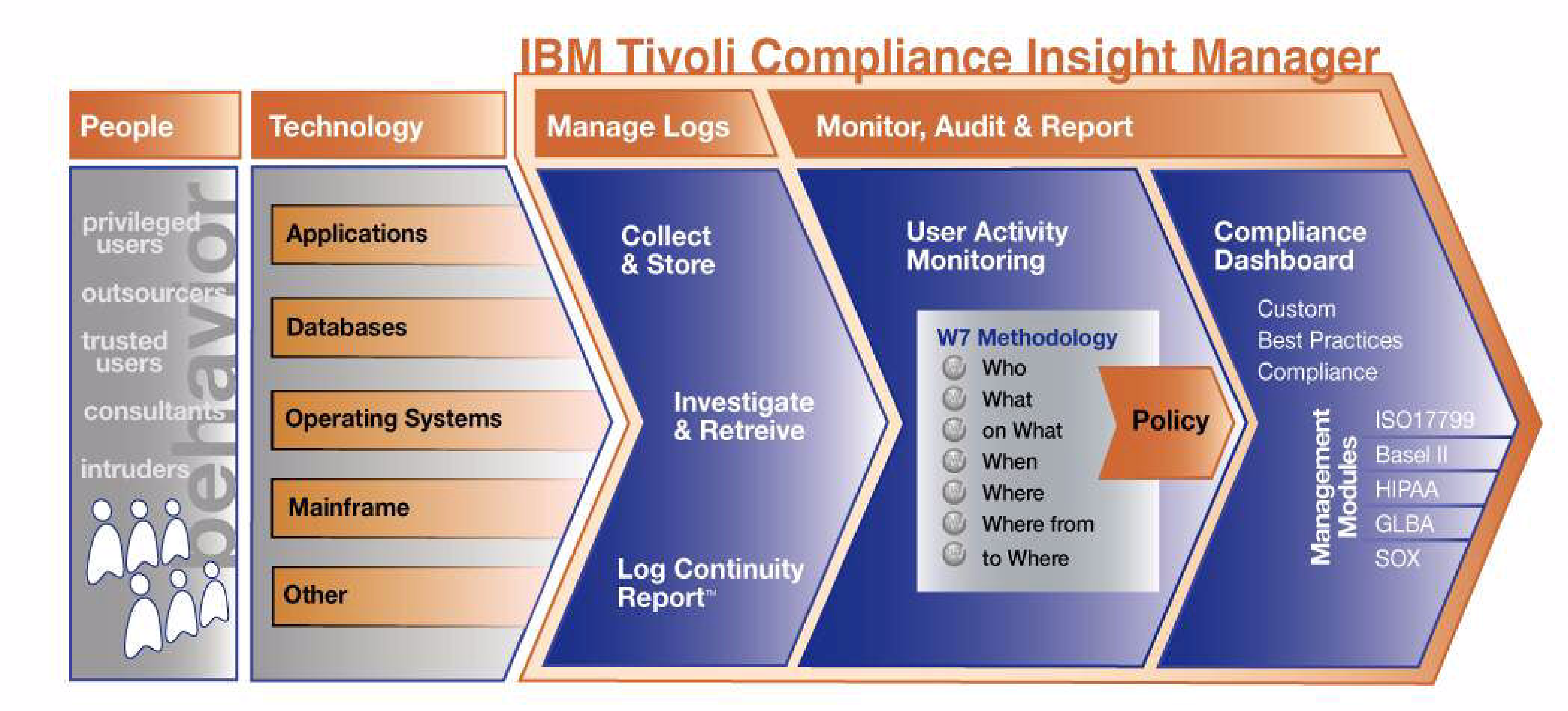
Consul **zSecure**™ Suite



Amministrazione completa dei log, Monitoringdegli accessi ai sistemi e Reporting per la compliance

Integrazione di audit, monitoring, compliance ed amministrazione del mainframe

La soluzione delle 3 C (Capture – Comprehend – Communicate)



IBM Tivoli Compliance Insight Manager

People

behavior

privileged users

outsourcers

trusted users

consultants

intruders

Technology

Applications

Databases

Operating Systems

Mainframe

Other

Manage Logs

Collect & Store

Investigate & Retreive

Log Continuity Report™

Monitor, Audit & Report

User Activity Monitoring

W7 Methodology

- Who
- What
- on What
- When
- Where
- Where from
- to Where

Policy

Compliance Dashboard

Custom

Best Practices

Compliance

Management Modules

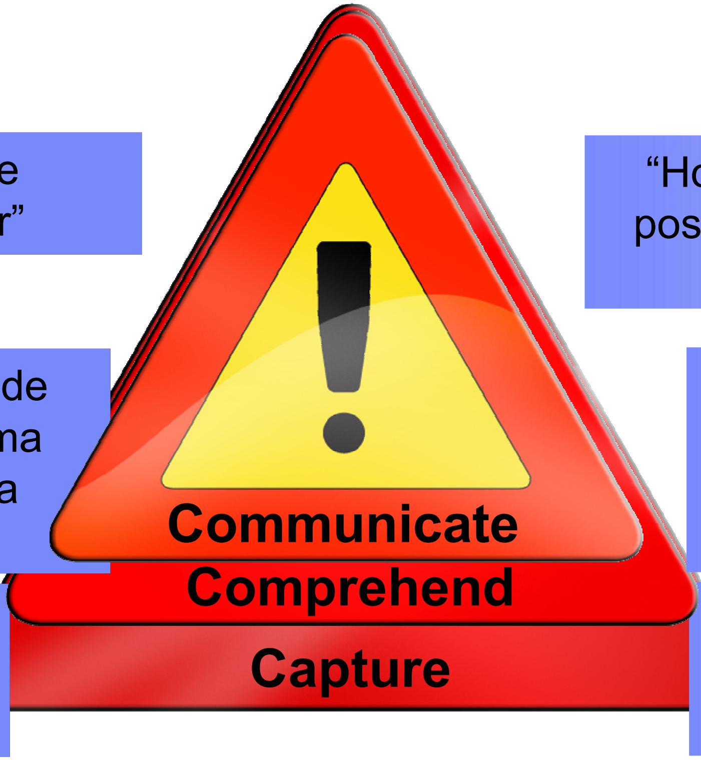
- ISO17799
- Basel II
- HIPAA
- GLBA
- SOX

TCIM: i problemi che aiuta a risolvere

“Ho bisogno di produrre report per i miei auditor”

“Il mio staff non possiede tempo ed esperienza ma necessita di eseguire la scansione dei logs”

“Ho bisogno di storicizzare i log per analisi forense”

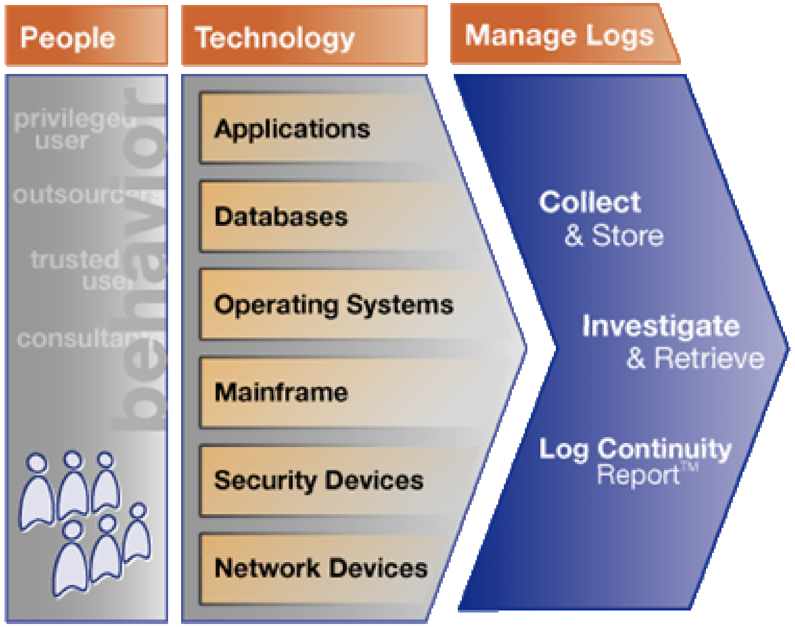


“Ho bisogno di dimostrare di possedere una struttura di IT security controls”

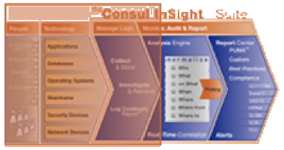
“Sono interessato ad individuare i privilegi che permettono determinate azioni”

“Non ho idea di quale log collezionare e come farlo”

Enterprise Log Management



Capture



Funzionalità:

- Sicuro, affidabile accentratore di log da qualunque piattaforma
- Cattura in automatico i syslogs
- Pieno supporto su attività di collect di eventi da log nativi
- Immagazzina in modo efficiente e compresso i dati in un depot
- Accesso ai dati quando necessario
- Ricerca su tutti i log
- Reports sui dati raccolti

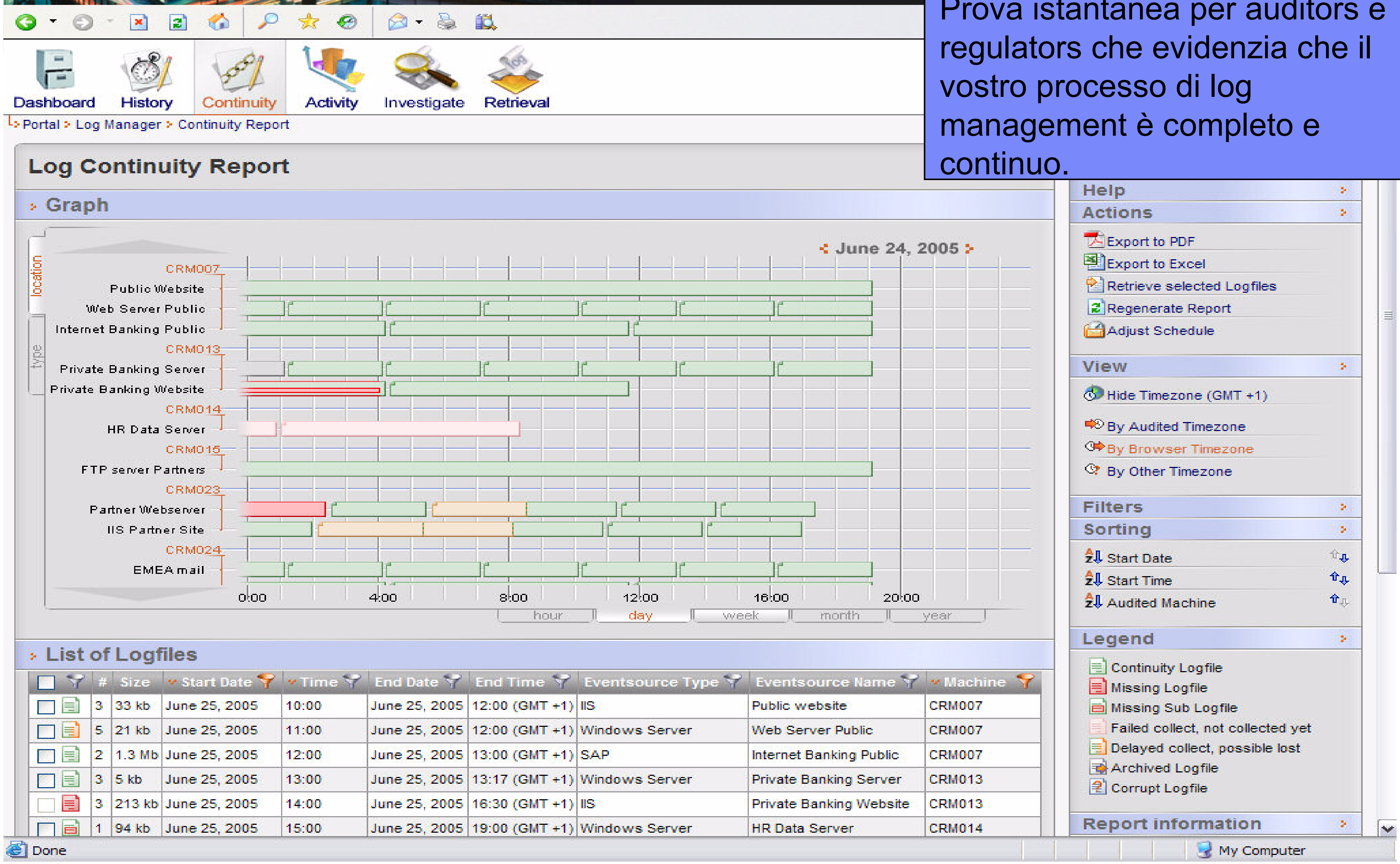
Benefici:

- Riduzione dei costi grazie all’automatizzazione e centralizzazione del collect dei dati
- Essere sempre “audit ready”!

Implementation time: plug and play.

Log Continuity Report

Prova istantanea per auditors e regulators che evidenzia che il vostro processo di log management è completo e continuo.



Portal > Log Manager > Continuity Report

Log Continuity Report

Legend:

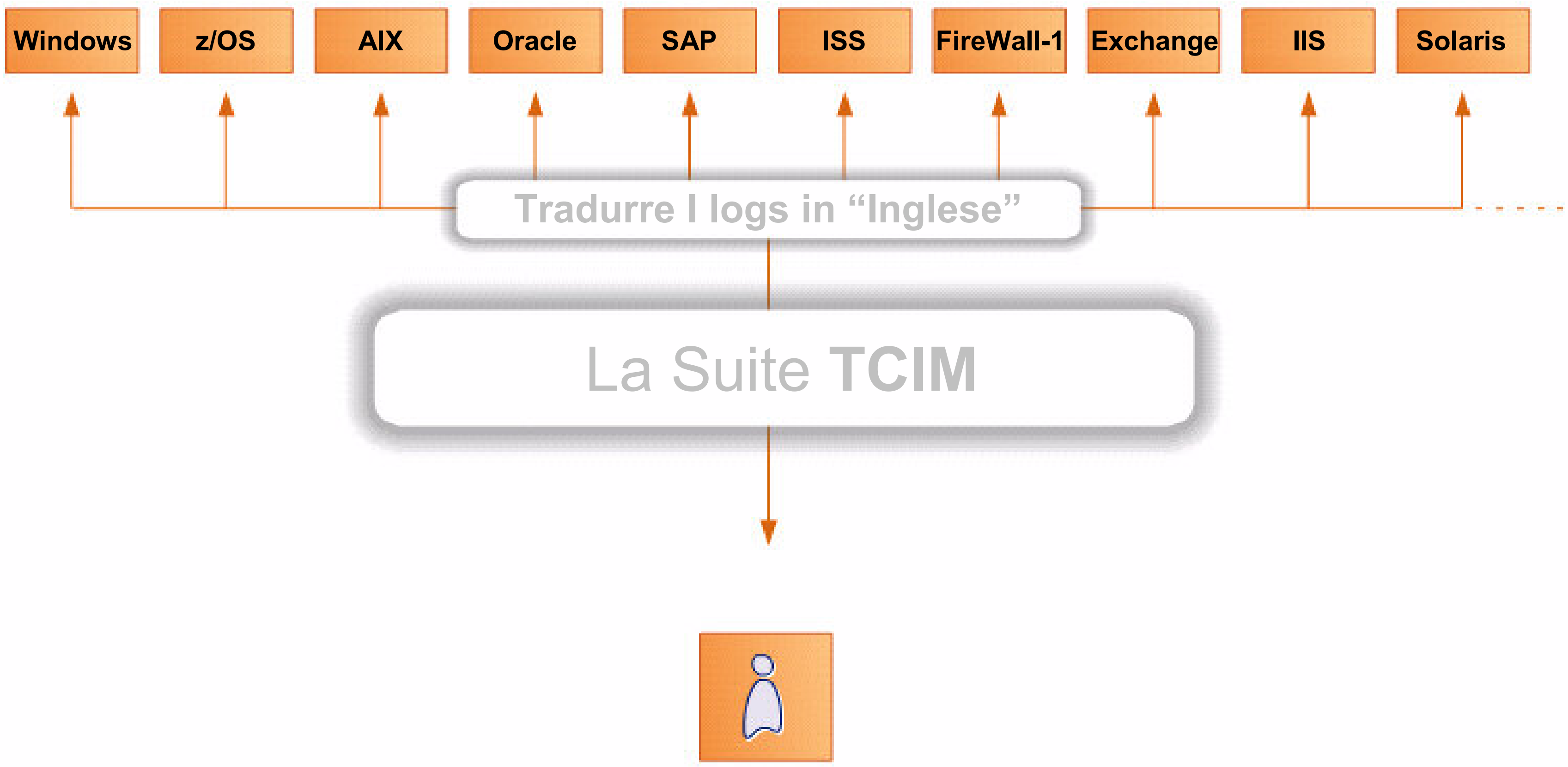
- Continuity Logfile
- Missing Logfile
- Missing Sub Logfile
- Failed collect, not collected yet
- Delayed collect, possible lost
- Archived Logfile
- Corrupt Logfile

List of Logfiles

□	#	Size	Start Date	Time	End Date	End Time	Eventsource Type	Eventsource Name	Machine
□	3	33 kb	June 25, 2005	10:00	June 25, 2005	12:00 (GMT +1)	IIS	Public website	CRM007
□	5	21 kb	June 25, 2005	11:00	June 25, 2005	12:00 (GMT +1)	Windows Server	Web Server Public	CRM007
□	2	1.3 Mb	June 25, 2005	12:00	June 25, 2005	13:00 (GMT +1)	SAP	Internet Banking Public	CRM007
□	3	5 kb	June 25, 2005	13:00	June 25, 2005	13:17 (GMT +1)	Windows Server	Private Banking Server	CRM013
□	3	213 kb	June 25, 2005	14:00	June 25, 2005	16:30 (GMT +1)	IIS	Private Banking Website	CRM013
□	1	94 kb	June 25, 2005	15:00	June 25, 2005	19:00 (GMT +1)	Windows Server	HR Data Server	CRM014

Ora tutti i log della vostra azienda in un unico linguaggio

Comprehend



Windows

z/OS

AIX

Oracle

SAP

ISS

FireWall-1

Exchange

IIS

Solaris

Tradurre I logs in “Inglese”

La Suite **TCIM**

TCIM storicizza levostre informazioni di security e compliance risparmiando tempo esoldi attraverso l’automatizzazione di processi di monitoring sull’azienda.

Tradurre i Log in Inglese – con la metodologia Consul W7

Comprehend

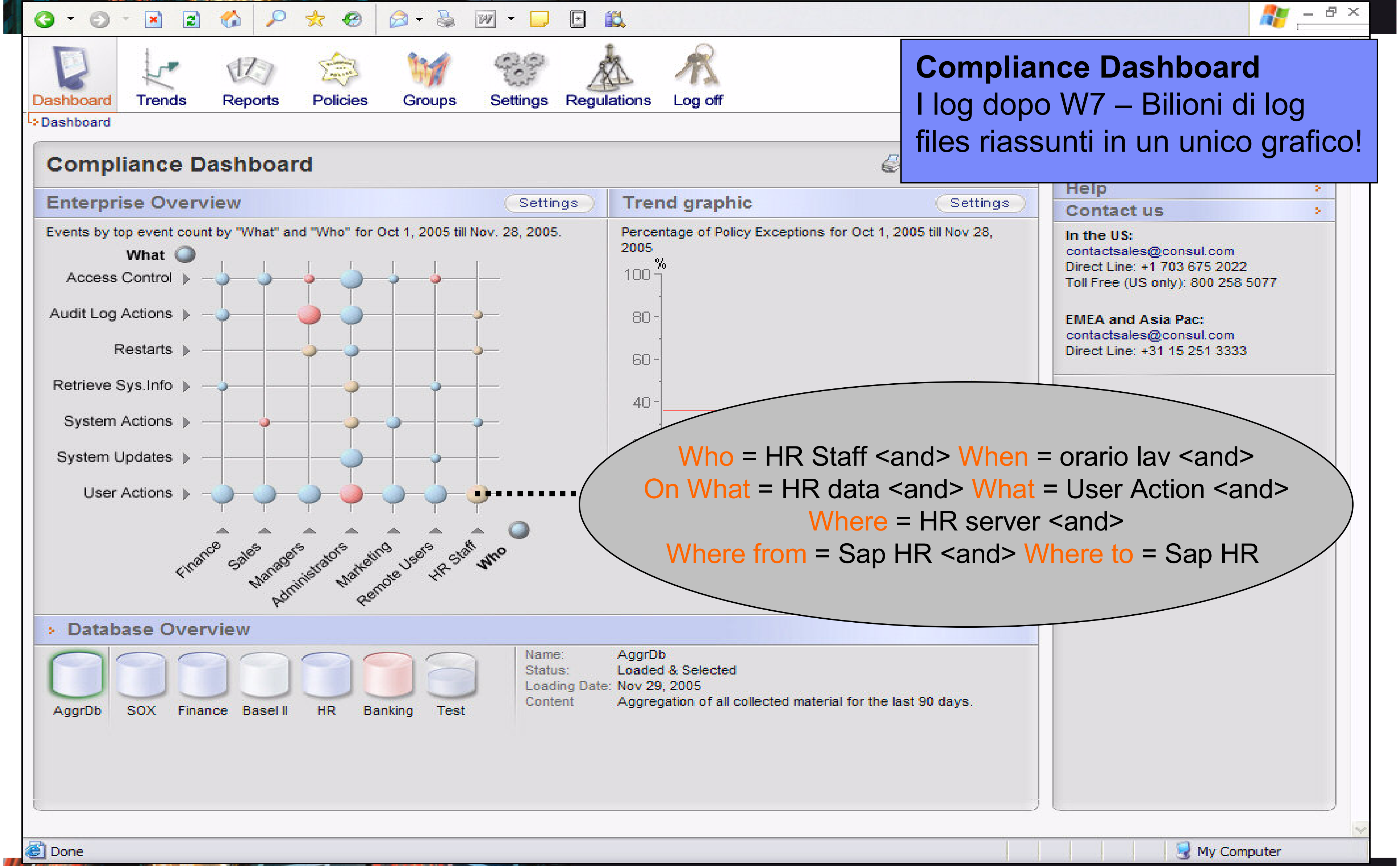
Who l’ha fatto **What** tipo di azione **on What**?

When l’ha fatto e **Where**, **From Where** e **Where To**?

We do the hard work, so you don’t have to!!

Compliance Dashboard

I log dopo W7 – Bilioni di log files riassunti in un unico grafico!



Dashboard

Compliance Dashboard

Enterprise Overview Settings

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

Trend graphic Settings

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

Help

Contact us

In the US:
contactsales@consul.com
Direct Line: +1 703 675 2022
Toll Free (US only): 800 258 5077

EMEA and Asia Pac:
contactsales@consul.com
Direct Line: +31 15 251 3333

Database Overview

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

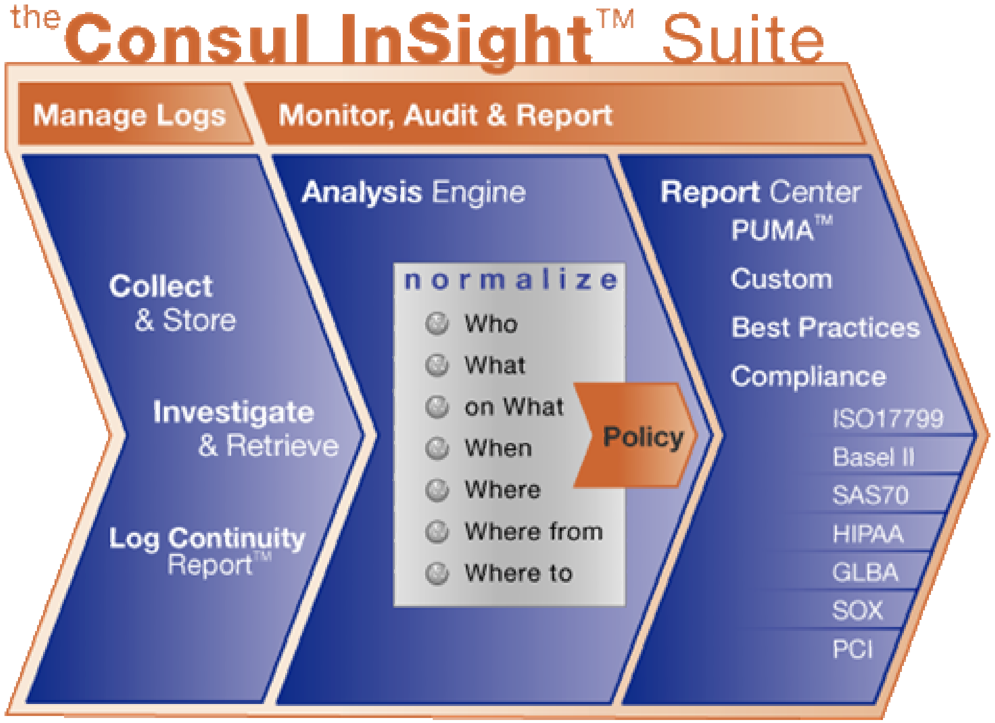
Done

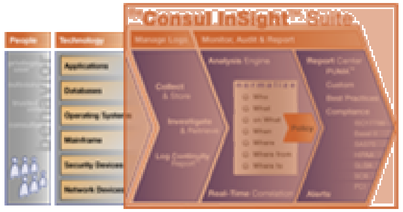
My Computer

Who = HR Staff <and> When = orario lav <and>
On What = HR data <and> What = User Action <and>
Where = HR server <and>
Where from = Sap HR <and> Where to = Sap HR

Full Audit and Compliance Reporting

Communicate



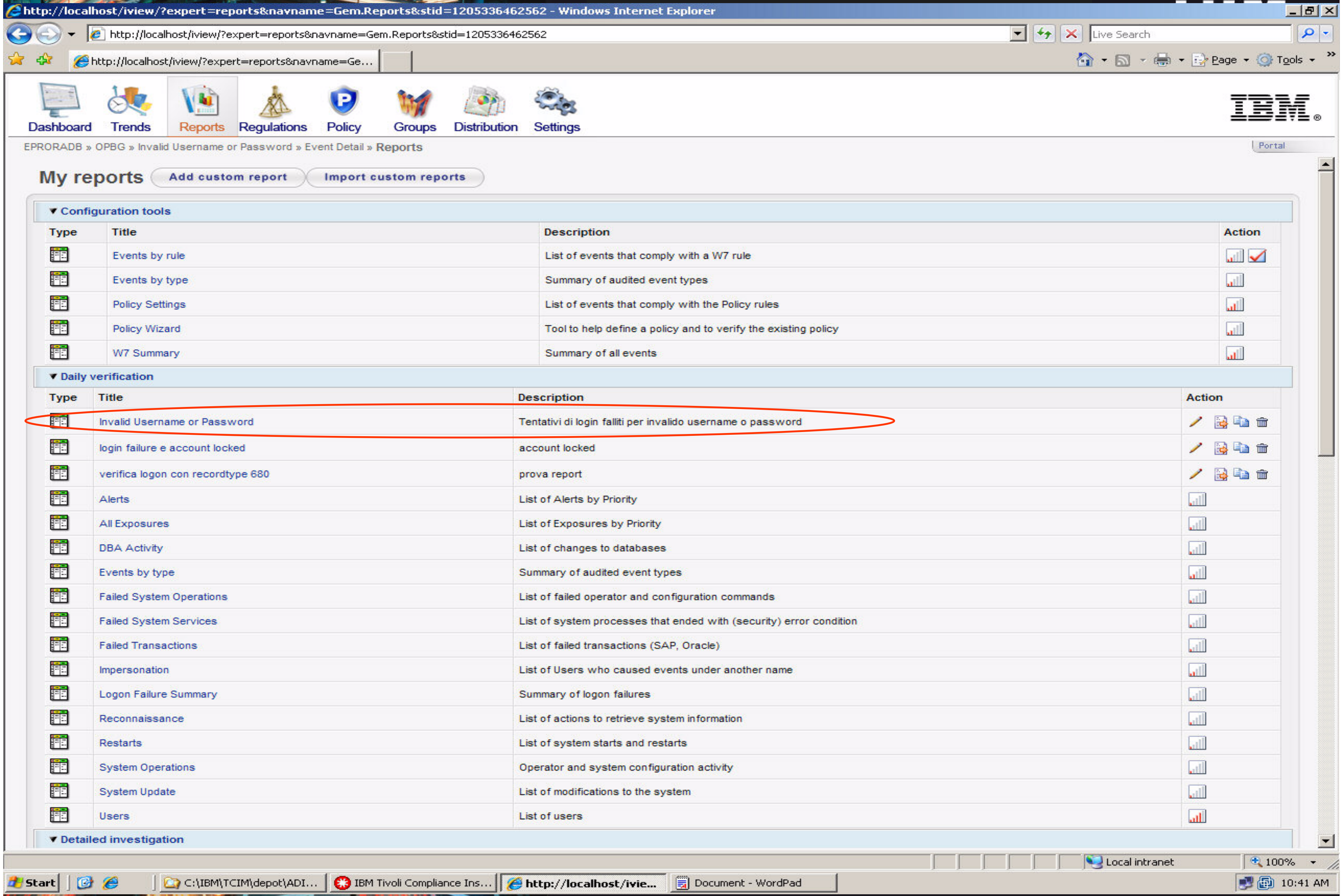


Capabilities:

- Centinaia di reports
- Moduli di Compliance
- Alert di Special attention
- Reports Custom

Benefits:

- Riduce l'impegno richiesto per l'audit
- Reports istantanei, salva tempo
- Riduce i rischi di minacce a dati sensibili:
  - Protezione dei dati
  - Controllo sui change
  - User management


http://localhost/iview/?expert=reports&navname=Gem.Reports&stid=1205336462562 - Windows Internet Explorer
http://localhost/iview/?expert=reports&navname=Gem.Reports&stid=1205336462562
Live Search
http://localhost/iview/?expert=reports&navname=Ge...
Page
Tools
Dashboard
Trends
Reports
Regulations
Policy
Groups
Distribution
Settings
IBM
Portal
Local intranet
100%
Start
C:\IBM\TCIM\depot\ADI...
IBM Tivoli Compliance Ins...
http://localhost/ivie...
Document - WordPad
10:41 AM

EPRORADB » OPBG » Invalid Username or Password » Event Detail » Reports

My reports

Add custom report | Import custom reports

▼ Configuration tools

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	

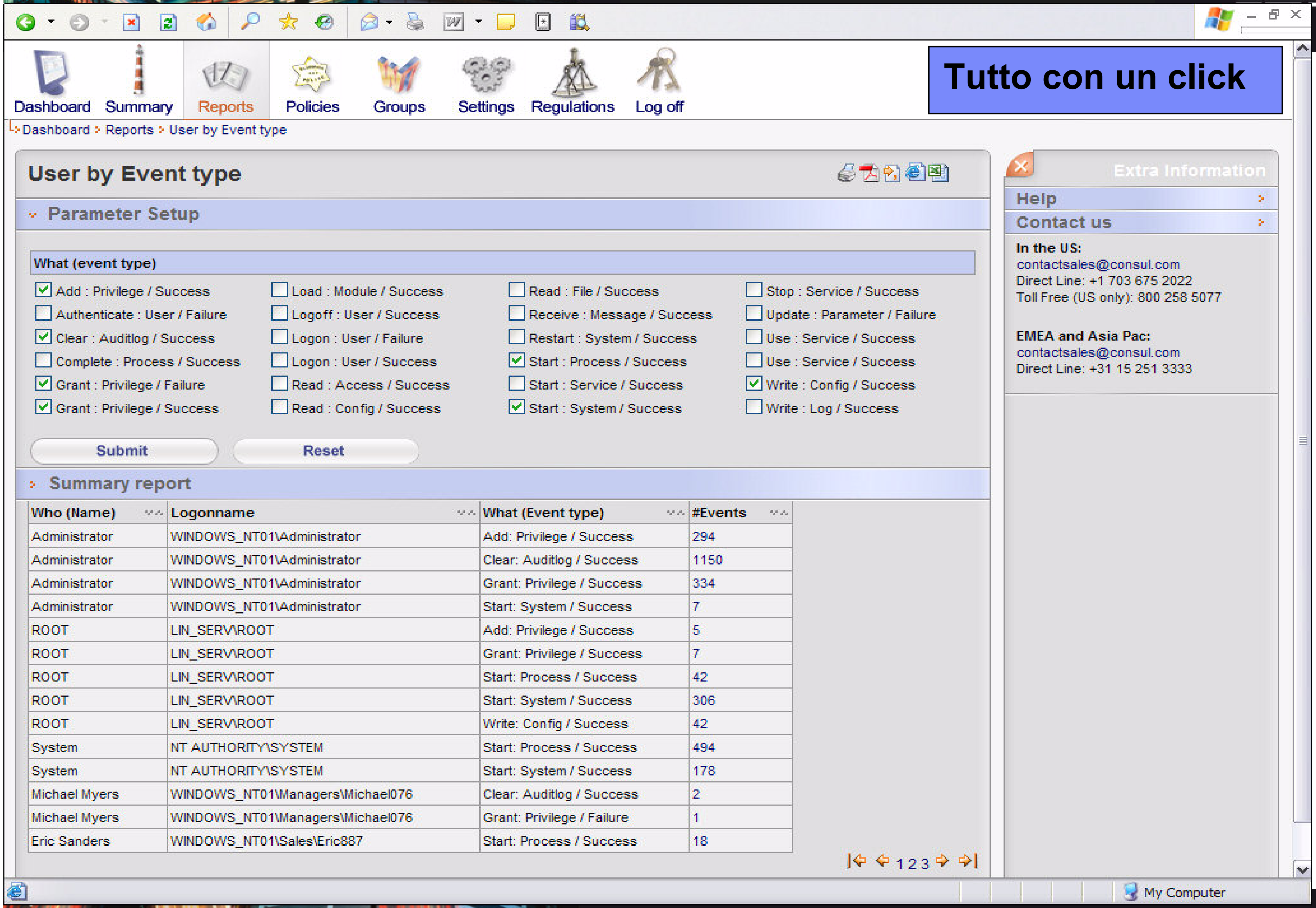
▼ Daily verification

Type	Title	Description	Action
	Invalid Username or Password	Tentativi di login falliti per invalido username o password	
	login failure e account locked	account locked	
	verifica logon con recordtype 680	prova report	
	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	
	Reconnaissance	List of actions to retrieve system information	
	Restarts	List of system starts and restarts	
	System Operations	Operator and system configuration activity	
	System Update	List of modifications to the system	
	Users	List of users	

▼ Detailed investigation

BASTA PARLARE **INIZIAMO A FARE**

Tutto con un click



Dashboard > Reports > User by Event type

User by Event type

Parameter Setup

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

Submit Reset

Summary report

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

Extra Information

Help

Contact us

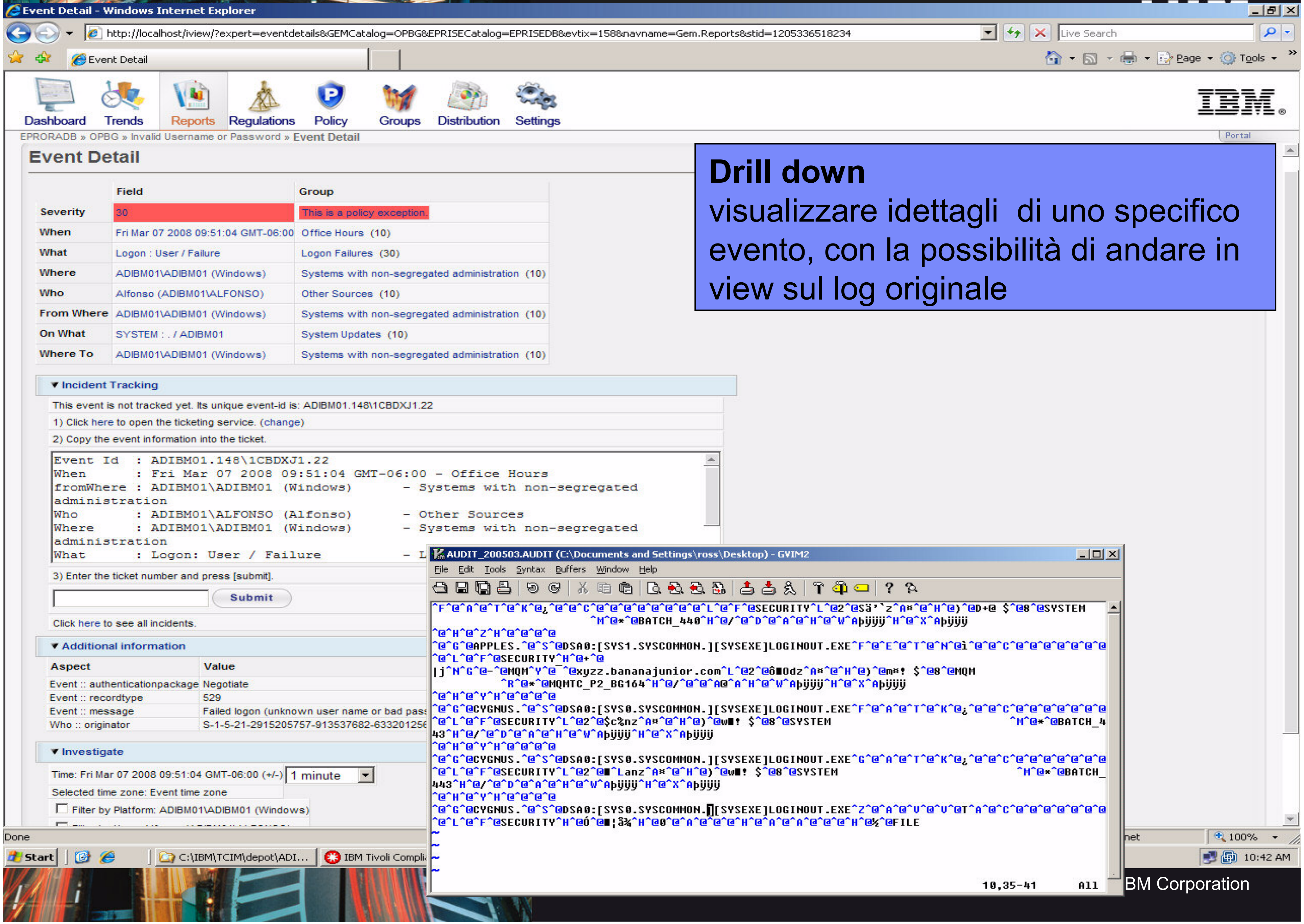
In the US:
contactsales@consul.com
Direct Line: +1 703 675 2022
Toll Free (US only): 800 258 5077

EMEA and Asia Pac:
contactsales@consul.com
Direct Line: +31 15 251 3333

My Computer

Drill down

visualizzare idettagli di uno specifico evento, con la possibilità di andare in view sul log originale



EPRORADB » OPBG » Invalid Username or Password » Event Detail

Event Detail

	Field	Group
Severity	30	This is a policy exception.
When	Fri Mar 07 2008 09:51:04 GMT-06:00	Office Hours (10)
What	Logon : User / Failure	Logon Failures (30)
Where	ADIBM01\ADIBM01 (Windows)	Systems with non-segregated administration (10)
Who	Alfonso (ADIBM01\ALFONSO)	Other Sources (10)
From Where	ADIBM01\ADIBM01 (Windows)	Systems with non-segregated administration (10)
On What	SYSTEM : . / ADIBM01	System Updates (10)
Where To	ADIBM01\ADIBM01 (Windows)	Systems with non-segregated administration (10)

▼ Incident Tracking

This event is not tracked yet. Its unique event-id is: ADIBM01.148\1CBDXJ1.22

1) Click here to open the ticketing service. (change)

2) Copy the event information into the ticket.

```
Event Id   : ADIBM01.148\1CBDXJ1.22
When       : Fri Mar 07 2008 09:51:04 GMT-06:00 - Office Hours
fromWhere  : ADIBM01\ADIBM01 (Windows)       - Systems with non-segregated
administration
Who        : ADIBM01\ALFONSO (Alfonso)       - Other Sources
Where      : ADIBM01\ADIBM01 (Windows)       - Systems with non-segregated
administration
What       : Logon: User / Failure           - L
```

3) Enter the ticket number and press [submit].

Submit

Click here to see all incidents.

▼ Additional information

Aspect	Value
Event :: authenticationpackage	Negotiate
Event :: recordtype	529
Event :: message	Failed logon (unknown user name or bad pass
Who :: originator	S-1-5-21-2915205757-913537682-63320125

▼ Investigate

Time: Fri Mar 07 2008 09:51:04 GMT-06:00 (+/-) 1 minute

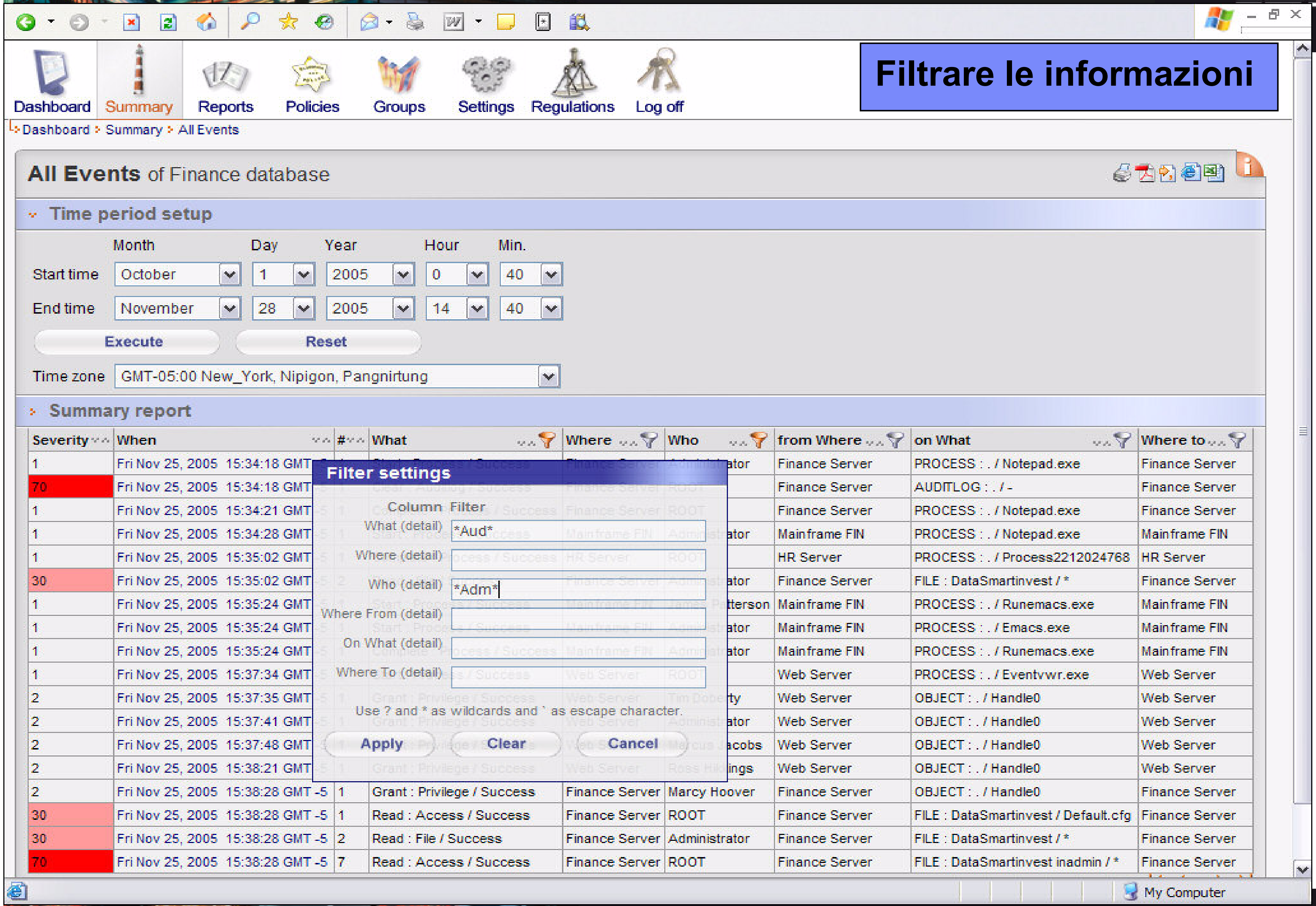
Selected time zone: Event time zone

□ Filter by Platform: ADIBM01\ADIBM01 (Windows)

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

```
^F^@^A^@^T^@^K^@¿^@^@^C^@^@^@^@^@^@^@^@^L^@^F^@SECURITY^L^@2^@Sä'`z^A¤^@^H^@)^@D+@ $^@8^@SYSTEM
                ^M^@*^@BATCH_440^H^@/^@^D^@^A^@^H^@^W^Aþÿÿÿ^H^@^X^Aþÿÿÿ
^@^H^@^Z^H^@^@^@^@
^@^G^@APPLES.^@^S^@DSA0:[SYS1.SYSCOMMON.][SYSEXE]LOGINOUT.EXE^F^@^E^@^T^@^N^@ì^@^@^C^@^@^@^@^@^@^@
^@^L^@^F^@SECURITY^H^@+^@
|j^N^G^@-^@MQM^Y^@¯^@xyzz.bananajunior.com^L^@2^@ô■Odz^A¤^@^H^@)^@m¤! $^@8^@MQM
       ^R^@*^@MQMTC_P2_BG164^H^@/^@^@^A@^A^H^@^W^Aþÿÿÿ^H^@^X^Aþÿÿÿ
^@^H^@^Y^H^@^@^@^@
^@^G^@CYGNUS.^@^S^@DSA0:[SYS0.SYSCOMMON.][SYSEXE]LOGINOUT.EXE^F^@^A^@^T^@^K^@¿^@^@^C^@^@^@^@^@^@^@
^@^L^@^F^@SECURITY^L^@2^@$c%nz^A¤^@^H^@)^@w■! $^@8^@SYSTEM                    ^M^@*^@BATCH_4
43^H^@/^@^D^@^A^@^H^@^W^Aþÿÿÿ^H^@^X^Aþÿÿÿ
^@^H^@^Y^H^@^@^@^@
^@^G^@CYGNUS.^@^S^@DSA0:[SYS0.SYSCOMMON.][SYSEXE]LOGINOUT.EXE^G^@^A^@^T^@^K^@¿^@^@^C^@^@^@^@^@^@^@
^@^L^@^F^@SECURITY^L^@2^@■^Lanz^A¤^@^H^@)^@w■! $^@8^@SYSTEM                    ^M^@*^@BATCH_
443^H^@/^@^D^@^A^@^H^@^W^Aþÿÿÿ^H^@^X^Aþÿÿÿ
^@^H^@^Y^H^@^@^@^@
^@^G^@CYGNUS.^@^S^@DSA0:[SYS0.SYSCOMMON.][SYSEXE]LOGINOUT.EXE^Z^@^A^@^V^@^V^@T^A^@^C^@^@^@^@^@^@^@
^@^L^@^F^@SECURITY^H^@Ó^@■¦ã¾^H^@0^@^A^@^@^@^H^@^A^@^A^@^@^@^H^@½^@FILE
~
~
~
~
                                                                   10,35-41      All
```

Filtrare le informazioni



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

Execute Reset

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

Summary report

Severity	When	#	What	Where	Who	from Where	on What	Where to
1	Fri Nov 25, 2005 15:34:18 GMT -5	1	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	[illegible]ocess / Success	HR Server	ROOT	HR Server	PROCESS : . / Process2212024768	HR Server
30	Fri Nov 25, 2005 15:35:02 GMT -5	2	[illegible]	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	[illegible]s / 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 Doherty	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 Hillings	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

Filter settings

Column Filter

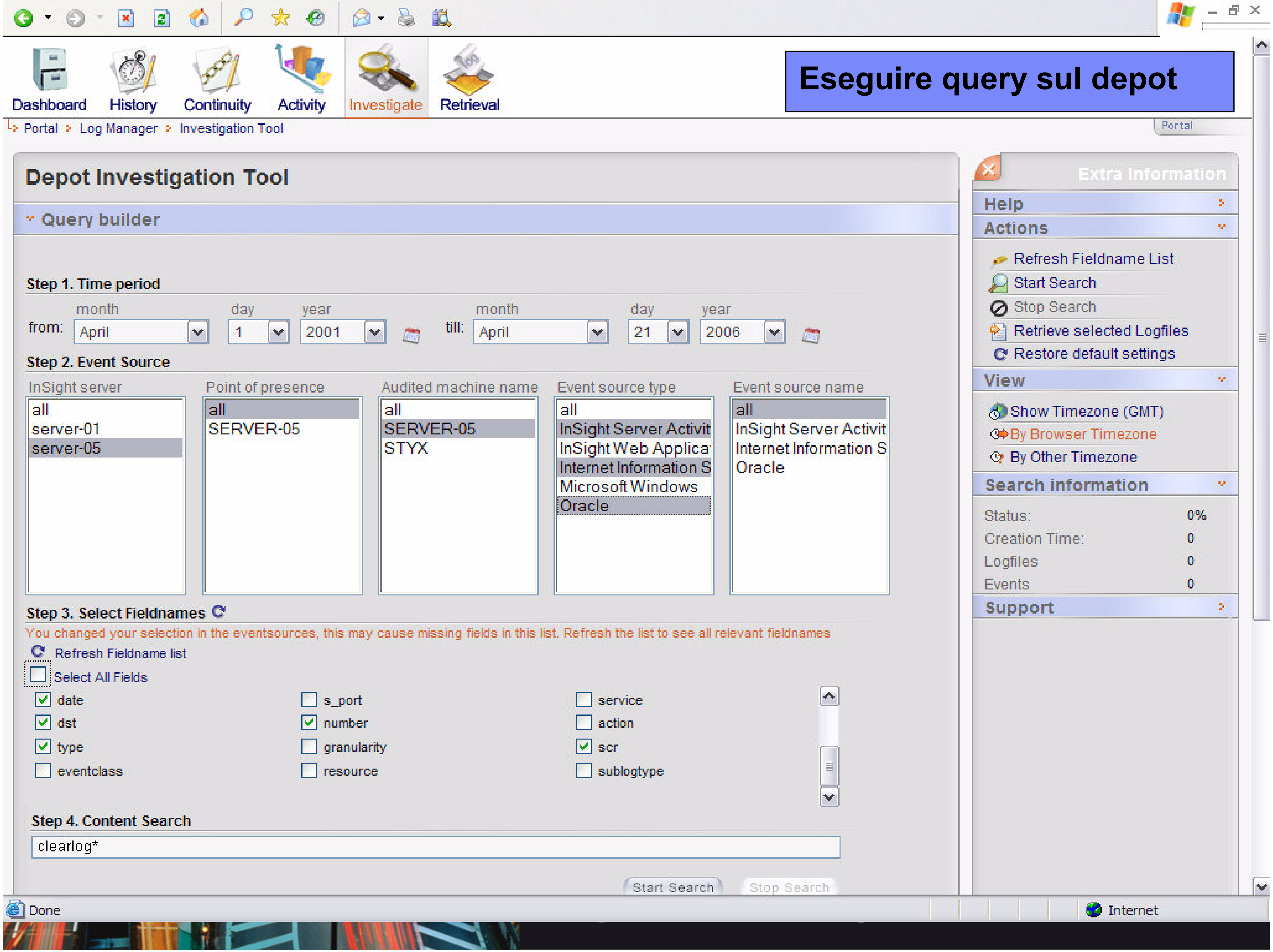
What (detail)	*Aud*
Where (detail)	
Who (detail)	*Adm*
Where From (detail)	
On What (detail)	
Where To (detail)	

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

Apply Clear Cancel

BASTA PARLARE **INIZIAMO A FARE**

Eseguire query sul depot



Depot Investigation Tool

Query builder

Step 1. Time period

from: month April, day 1, year 2001 — till: month April, day 21, year 2006

Step 2. Event Source

InSight server	Point of presence	Audited machine name	Event source type	Event source name
all	all	all	all	all
server-01	SERVER-05	SERVER-05	InSight Server Activit	InSight Server Activit
server-05		STYX	InSight Web Applica	Internet Information S
			Internet Information S	Oracle
			Microsoft Windows	
			Oracle	

Step 3. Select Fieldnames

You changed your selection in the eventsources, this may cause missing fields in this list. Refresh the list to see all relevant fieldnames

Refresh Fieldname list

□ Select All Fields

☑ date
☑ dst
☑ type
□ eventclass
□ s_port
☑ number
□ granularity
□ resource
□ service
□ action
☑ scr
□ sublogtype

Step 4. Content Search

clearlog*

Extra Information

Help

Actions

- Refresh Fieldname List
- Start Search
- Stop Search
- Retrieve selected Logfiles
- Restore default settings

View

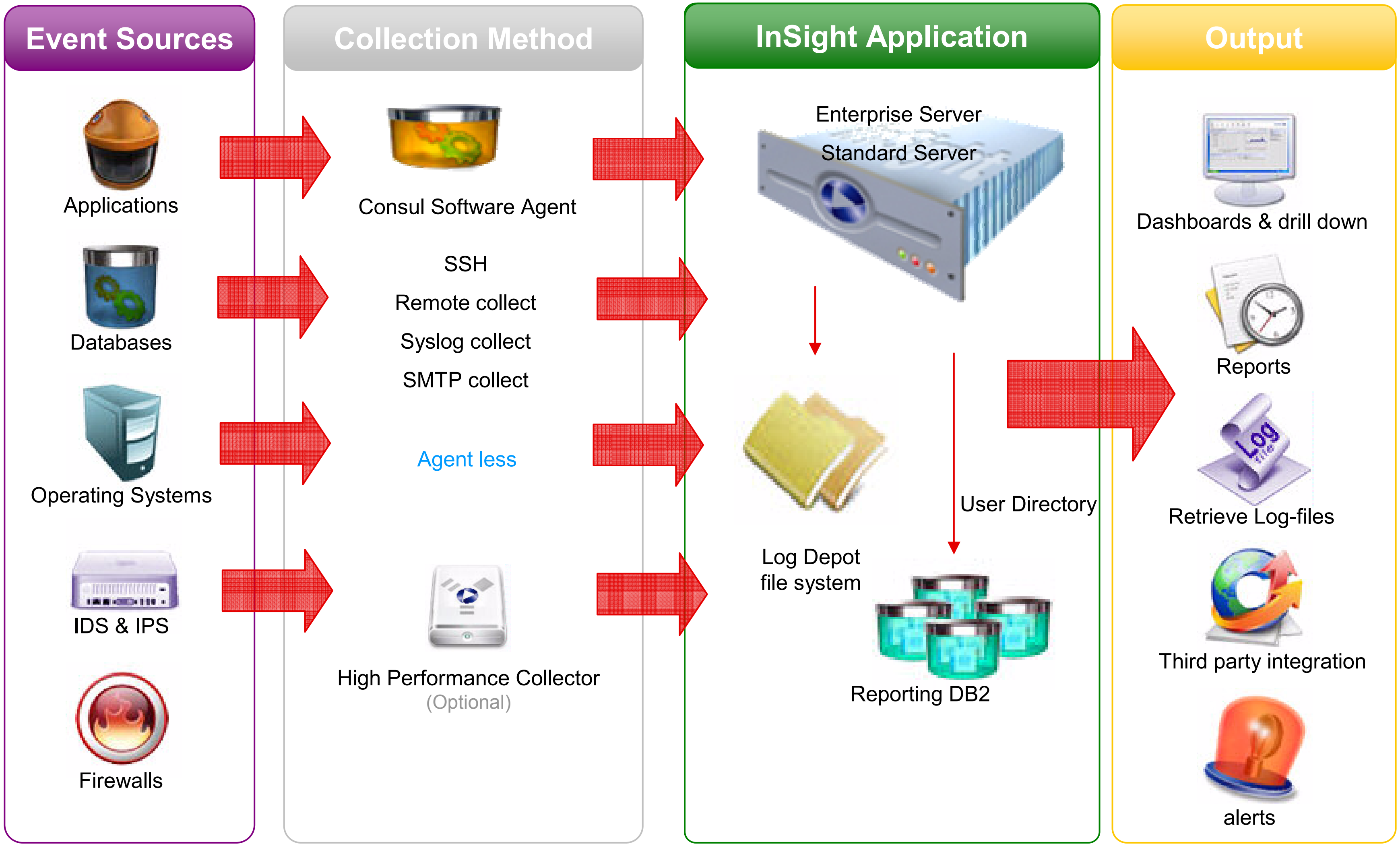
- Show Timezone (GMT)
- By Browser Timezone
- By Other Timezone

Search information

Status:	0%
Creation Time:	0
Logfiles	0
Events	0

Support

Architecture



Event Sources

Applications

Databases

Operating Systems

IDS & IPS

Firewalls

Collection Method

Consul Software Agent

SSH

Remote collect

Syslog collect

SMTP collect

Agent less

High Performance Collector

(Optional)

InSight Application

Enterprise Server

Standard Server

Log Depot file system

User Directory

Reporting DB2

Output

Dashboards & drill down

Reports

Retrieve Log-files

Third party integration

alerts

TCIM Supported event sources

Supported SERVERS:

- IBM AIX Audit logs
- IBM AIX syslog
- IBM OS/400 & i5/OS journals
- Hewlett-Packard HP-UX Audit logs
- Hewlett-Packard HP-UX syslog
- Hewlett-Packard NonStop (Tandem)
- Hewlett-Packard OpenVMS
- Hewlett-Packard Tru64
- Microsoft Windows
- Novell Netware
- Novell NSure Audit
- Novell Audit
- Novell Suse Linux
- RedHat Linux
- Stratus VOS
- SUN Solaris BSM Audit logs
- SUN Solaris syslog

Supported MAINFRAME:

- IBM z/OS + RACF
- IBM z/OS + CA ACF2
- IBM z/OS + CA Top Secret
- CA Top Secret for VSE/ESA

Supported APPLICATIONS:

- Tivoli Identity Manager
- Tivoli Access Manager for OS and for e-Business
- FUTURE (in engineering pipeline): TFIM, TDS, TDI, TSOM
- SAP R/3 on Windows, Solaris, AIX, HP-UX
- Misys OPICS
- BMC Identity Manager
- CA eTrust (Netegrity) SiteMinder
- RSA Authentication Server
- Microsoft Exchange
- IBM Lotus Domino Server on Windows
- Microsoft Internet Information server
- SUN iPlanet Web Server on Solaris

Supported DATABASES:

- IBM DB2 on z/OS
- IBM DB2 / UDB on Windows, Solaris, AIX
- Microsoft SQL Server application logs
- Microsoft SQL Server trace files
- Oracle DBMS on Windows, AIX, Solaris, HP-UX
- Oracle DBMS FGA on Windows, AIX, Solaris, HP-UX
- Sybase ASE on Windows, AIX, Solaris, HP-UX
- FUTURE (in pipeline): DB2 Viper 2, Informix, AME

Supported DEVICES:

- Cisco Router
- Hewlett-Packard ProCurve Switch
- Blue Coat Systems ProxySG Series
- Check Point Firewall-1
- Cisco PIX
- Cisco VPN Concentrator (3000 series)
- Symantec (Raptor) Enterprise Firewall
- ISS RealSecure
- ISS System Scanner
- McAfee IntruShield IPS Manager
- McAfee ePolicy Orchestrator
- Snort IDS
- Symantec Antivirus
- TrendMicro ScanMail for Domino
- TrendMicro ScanMail for MS Exchange
- TrendMicro ServerProtect for Windows

Minimum Requirements:

Tivoli Compliance Insight Manager Standard Server and Enterprise Server

Server dedicato (no virtualization)

Minimum Enterprise Server requirements

Quad Core Intel® Xeon™ 3.0 GHz processor

6 GB RAM + 0.5 GB per scheduled General Event Model (GEM) database

Minimum Standard Server requirements

Duo Core Intel Xeon 3.0 GHz processor

4 GB RAM

Disk space requirements

1.5 * (total GB of daily logs / 10 compression factor) * number of days to keep in repository + 25 GB