Log Management per gli accessi degli Amministratori di Sistema

Il Garante sulla Privacy ha prescritto l'adozione di specifiche misure tecniche e organizzative, da parte di enti e società, che agevolino la verifica sull'attività dell'amministratore di sistema da parte di chi ha la titolarità delle banche dati e dei sistemi informatici (***Provvedimento del Garante sulla Privacy sugli Amministratori di Sistema***, *del 27-11-08, pubblicato sulla G.U. n.300 del 24-12-08).*

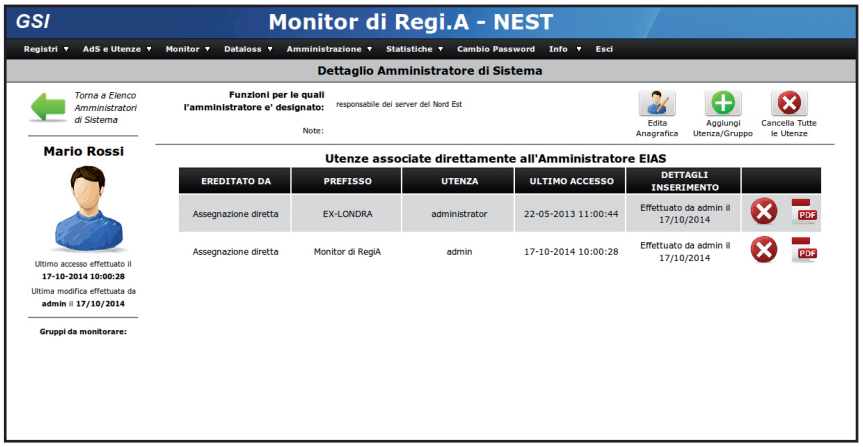
Regi.A è la soluzione di GSI Srl che permette di ottemperare alle esigenze della normativa ed è stata già scelta da moltissime realtà italiane operanti in diversi settori di business.

Cosa richiede il Garante

- Registrazione degli accessi logici (log on/log off) completi, inalterabili e integri, da conservarsi per almeno 6 mesi.
- Identificazione degli Amministratori di Sistema (AdS).
- Verifiche periodiche delle attività e dei privilegi degli AdS.

Cosa prevede Regi.A

- **Relay** per la registrazione degli accessi e l'inoltro degli eventi.
- **Server di raccolta** centrale su cui vengono registrati e conservati i log.
- **Elenco degli Amministratori di Sistema** e correlazione con utenze e log.
- **Monitor** per l'analisi in tempo reale degli eventi raccolti, per le ricerche e verifiche periodiche.



Monitor di ***Regi.A***

Regi.A

Relay

Per ogni sistema interessato dalla registrazione dei log è previsto un Relay.

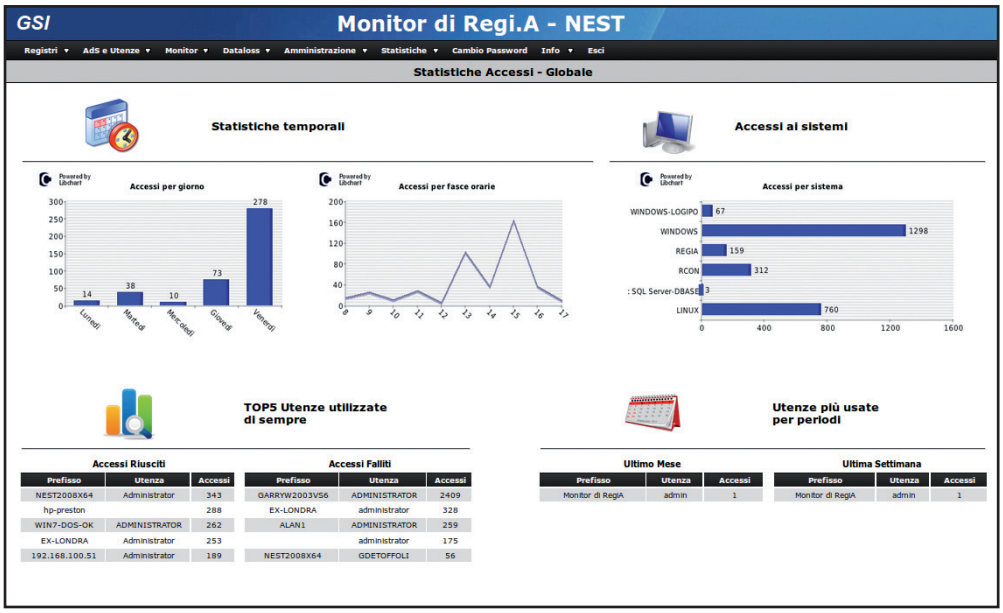
I Relay registrano gli eventi e li inoltrano al server di raccolta in formato signed syslog.

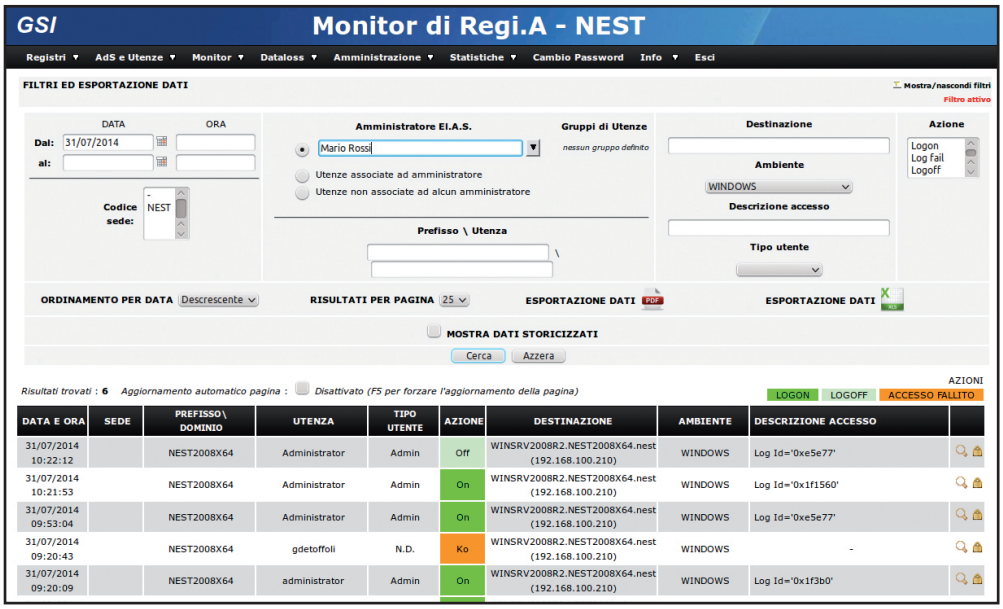
Sistema di raccolta e veicolazione dei log

E' stato scelto lo standard internazionale syslog, nella forma definita da IETF come syslog-signed, che garantisce compatibilità e omogeneità di formato.

Sistemi supportati

Regi.A è compatibile con tutti i principali sistemi diffusi nelle aziende, quali Windows, Linux/Unix, AS400, Mac e apparati di rete compatibili con syslog standard.





Caratteristiche e vantaggi

- **Filtro alla fonte**
  Riduce drasticamente i costi di archiviazione e semplifica le ricerche
- **Completamento dei dati alla fonte**
  Identifica con precisione gli accessi amministrativi
- **User-friendly**
  Sintesi delle informazioni utili, fruibile anche da non tecnici
- **Certificazione alla fonte**
  Gli eventi sono firmati, resi inalterabili e identificabili univocamente
- **Bufferizzazione**
  Riduce al minimo il traffico di rete e gestisce le indisponibilità delle rete o dei server di raccolta
- **Correlazione tra accessi, utenze e amministratori**
  Collega i log alle utenze che li hanno generati e all'amministratore di sistema
- **Integrazione dei dati**
  Integrazione dei dati degli amministratori di più sistemi
- **Formato standard e aperto**
  Syslog-signed, standard IETF per garantire l'interoperabilità con i migliori software di mercato

GSI
Gestione Servizi Informatici
Contrà Riale, 6 • 36100 Vicenza • Italy
Tel.: +39 0444 1788069 • Fax: +39 0444 1788051 • info@gsionline.net

ZAP TECHNOLOGY
Distribuito da:
Zap Technology Srl
Largo Marco Gerra, 3
42124 Reggio Emilia • Italy
Tel.: +39 0522 1486805
Fax: +39 0522 1486782
info@zapsrl.com