

# AUDIT ACCESSI AMMINISTRATIVI

---

SOLUZIONE PER L'OTTEMPERANZA ALLE DISPOSIZIONI DEL  
GARANTE SULLA PRIVACY

© 2009 Progel S.r.l. Tutti i diritti sono riservati.

Questo documento contiene informazioni proprietarie che sono coperte da copyright. Tutti i diritti sono riservati. Nessuna parte di questo documento può essere fotocopiata, riprodotta o tradotta in altra lingua senza il preventivo consenso scritto di Progel S.r.l.

Le informazioni contenute nel presente documento rappresentano la posizione corrente di Progel S.r.l. in merito all'oggetto discusso alla data della pubblicazione. Ogni procedura, politica od altra indicazione fornita si intendono accettati dal cliente al momento dell'applicazione delle stesse.

Dal momento che Progel S.r.l. deve rispondere alle mutevoli condizioni di mercato e fornire indicazioni su strumenti non direttamente sotto il proprio controllo, le informazioni qui vi esposte sono da ritenersi valide alla data di pubblicazione e nessuna garanzia esplicita o implicita viene fornita sull'accuratezza di quanto esposto dopo tale data.

Mythos è un marchio registrato Progel.

Altri prodotti o ditte menzionate possono essere marchi registrati dei rispettivi possessori.

Progel srl • Via Due Ponti, 2 • 40050 Argelato (BO) • Italy • [www.progel.it](http://www.progel.it) • [info@progel.it](mailto:info@progel.it) • Tel. +39 051 6639411 • Fax +39 051 6639412  
Registro delle Imprese di Bologna n. 03791100377 – Registro Ditte: 316517 – P.Iva 00662101203 CF 03791100377 – Capitale Sociale: 100.000 Euro I.V

Data	Versione	Autore	Modifiche
15-10-2009	1.10	DG	Versione definitiva

## CONTENUTI

<b>Auditing degli accessi amministrativi .....</b>	<b>4</b>
Introduzione .....	4
L'Architettura proposta .....	4
Risposte alle richieste del garante .....	5
Outsourcing selettivo del servizio .....	5
Hosting dei dati di security .....	6
Tecnologia e prerequisiti .....	6
Gestione di piattaforme non Microsoft .....	6
Servizi possibili per le piattaforme non Microsoft .....	8
Gestione di logging esterno al security log .....	8
Capacity planning.....	8
Attività previste .....	9
Reports.....	10



Sebbene l'architettura implementata sia in grado di collezionare qualsiasi evento presente nel security log dei sistemi Windows, l'intervento mira esclusivamente a raccogliere gli eventi di logon, e dove possibile di logoff, così come richiesto dalla disposizione del garante e successivi chiarimenti.

Dopo una fase di assessment per l'individuazione delle device e dei sistemi interessati saranno applicate le opportune politiche di auditing implementate direttamente dal cliente

## RISPOSTE ALLE RICHIESTE DEL GARANTE

La soluzione basata sul modulo ACS di System Center Operations Manager 2007 risponde alle seguenti richieste del garante:

- **Completezza:** garantita dal security log delle macchine Windows e dal fatto che i log sono immediatamente collezionati dall'agente. Se l'amministratore decidesse di cancellare il security log, questo evento sarebbe comunque collezionato mettendo in evidenza l'operazione.
- **Inalterabilità:** per inalterabilità del dato si intende l'impossibilità per gli amministratori oggetto di auditing di modificare il dato raccolto. L'inalterabilità si ottiene prima di tutto grazie alla raccolta "near real time" delle informazioni dai security log e dalla loro trasmissione in modo cifrato sulla rete fino a raggiungere il repository. La scelta di quale livello di compliance raggiungere in termini di inalterabilità è lasciato al cliente. Le strategie possibili sono:
  - Il repository può essere messo in sicurezza in modo tale da impedire che gli amministratori vi possano accedere (hardening)
  - L'intera infrastruttura di raccolta può essere realizzata in un contesto amministrativo (Active Directory Forest) separata da quella oggetto di auditing
  - Un'opportuna politica di backup può garantire lo stoccaggio dei nastri in modo che non siano alterabili.
  - Possono essere adottate misure di archiviazione su supporto non riscrivibile.
  - Possono essere adottate strategie di hashing dei dati raccolti e di firma con marca temporale (esempio posta certificata)
- **Integrità:** la verifica dell'integrità del dato può essere ottenuta tramite un'opportuna politica di backup che, salvando in modo inalterabile i dati, permetta un loro restore e/o una verifica degli stessi con i dati online
- **Mantenimento** per almeno 6 mesi: può essere ottenuto sia conservando online i dati sul database SQL, sia tramite un'opportuna politica di backup, sia tramite un prodotto di archiviazione evoluta.

Il Garante, nei chiarimenti alla disposizione, indica che:

*"...anche i **client**, intesi come "postazioni di lavoro informatizzate", sono compresi tra i sistemi per cui devono essere registrati gli accessi degli AdS."*

Se i dati protetti sono contenuti solo su sistemi server e se su questi è possibile tracciare i logon tramite rete (e non solo quelli interattivi - sempre possibile per sistemi Microsoft Windows), nel rispetto dello spirito della direttiva, è a nostro parere inutile raccogliere i logon dai client stessi, essendo tracciato ogni logon per l'accesso ai dati protetti sui sistemi server. La soluzione permette comunque di collezionare anche i dati di auditing dei sistemi client.

In tutti i casi è l'ufficio o il consulente legale dell'azienda a dover definire l'estensione dell'auditing e i relativi requirement. Si ricorda inoltre che il Documento Programmatico per la Sicurezza (DPS) e il Regolamento Informatico interno devono essere aggiornati con il dettaglio delle scelte effettuate. Progel srl fornisce unicamente consulenza tecnologica e non legale.

## OUTSOURCING SELETTIVO DEL SERVIZIO

Per i clienti che non vogliono gestire direttamente la raccolta dei dati di auditing, Progel propone un servizio di outsourcing selettivo lasciando sistemi e dati presso il cliente.

Il servizio può essere erogato in due forme:

- 1) Outsourcing dell'intera soluzione
- 2) Outsourcing della gestione dei soli dati di security

L'outsourcing dell'intera infrastruttura prevede la sottoscrizione di un contratto Remote Systems Management (RSM) e Progel Patch Service (PPS) per i sistemi coinvolti. Rimane a carico dell'infrastruttura del cliente la realizzazione dei backup, il cui corretto funzionamento sarà comunque controllato da Progel.

Nel caso di outsourcing del solo repository dati, attivabile in caso di hardening e di sistema dedicato, il servizio si occupa di:

- Verificare il corretto funzionamento della raccolta dei security log tramite un monitor centralizzato presso Progel
- Verificare l'esecuzione dei backup e in caso di errore notificarlo al cliente (l'infrastruttura di backup dovrà essere messa a disposizione del cliente)
- Manutenere i server necessari alla raccolta in termini di patching e fixing con cadenza mensile

## HOSTING DEI DATI DI SECURITY

Progel è in grado di garantire l'hosting dei dati di auditing raccolti dalla soluzione proposta. Il servizio prevede la memorizzazione dei dati presso server di Progel per un periodo non inferiore ai 6 mesi e ne garantisce backup e recovery con una finestra di massima scopertura di 24h (RPO).

La tariffazione è per GB memorizzato e la fattibilità tecnica dipende dal link di collegamento disponibile tra Progel ed il cliente e dal volume dei dati raccolti.

Progel fornisce anche un servizio di archiviazione che prevede però l'utilizzo da parte del cliente della soluzione di archiviazione Secure Vantage.

L'hosting dei dati può essere combinato con l'outsourcing selettivo del servizio.

## TECNOLOGIA E PREREQUISITI

La soluzione proposta è basata su Microsoft System Center Operations Manager 2007 R2. La proposta prevede che tutti i prerequisiti al deployment della soluzione siano stati soddisfatti, oltre alle piattaforme supportate e ai prerequisiti di sistema (<http://technet.microsoft.com/en-us/library/bb309428.aspx>).

Il supporto di Progel a fronte di problematiche non può prescindere dalla possibilità di scalare il problema agli autori del software e/o della soluzione. Garantendo comunque il massimo impegno, potrebbe verificarsi che, qualora il cliente decidesse di adottare architetture o soluzioni tecnologiche al di fuori degli ambiti supportati dal fornitore, Progel non sia in grado di farsi pienamente carico delle problematiche o di fornire risposte soddisfacenti.

## GESTIONE DI PIATTAFORME NON MICROSOFT

I sistemi e le device non basate su sistemi operativi Microsoft potranno essere integrate nella soluzione proposta tramite il Secure Vantage Syslog Gateway. Un singolo gateway su un sistema dedicato può supportare fino ad un massimo di 200 device o 1000 eventi al secondo. Il gateway è in ascolto sulla porta 514 UDP (questa impostazione non è modificabile) e risponde ai seguenti assunti:

- Le device o i sistemi da integrare devono essere in grado di veicolare gli eventi di interesse tramite standard syslog
- Il gateway non ha una propria coda di eventi e quindi non ha capacità di recupero in caso di problemi di comunicazione

Il livello di dettaglio e la trascodifica degli eventi syslog in eventi ACS è riassunta dalla seguente tabella:

Syslog Source Data	Event Translation	ACS Sample Event
Facility = 4 Severity = 2 Priority = 34 PriorityName = security.critical TimeStamp = Nov 27 04:49:50 HostName = 192.168.3.81 Message = "This is a test..."	Facility = Attribute1 Severity = Lookup Table Priority = Attribute2 PriorityName = Attribute3 TimeStamp = Attribute4 HostName = MachineName Message = Attribute5	EventID = 3 Severity = Failure MachineName = 192.168.3.81 Attribute1 = Facility Attribute2 = Priority Attribute3 = PriorityName Attribute4 = TimeStamp Attribute5 = Message

TAB. 1 – CODIFICA EVENTI SYSLOG IN ACS

L'architettura risultante è perfettamente integrata con ACS e sfrutta le funzionalità native degli ACS forwarder per far giungere al repository centrale gli eventi collezionati.

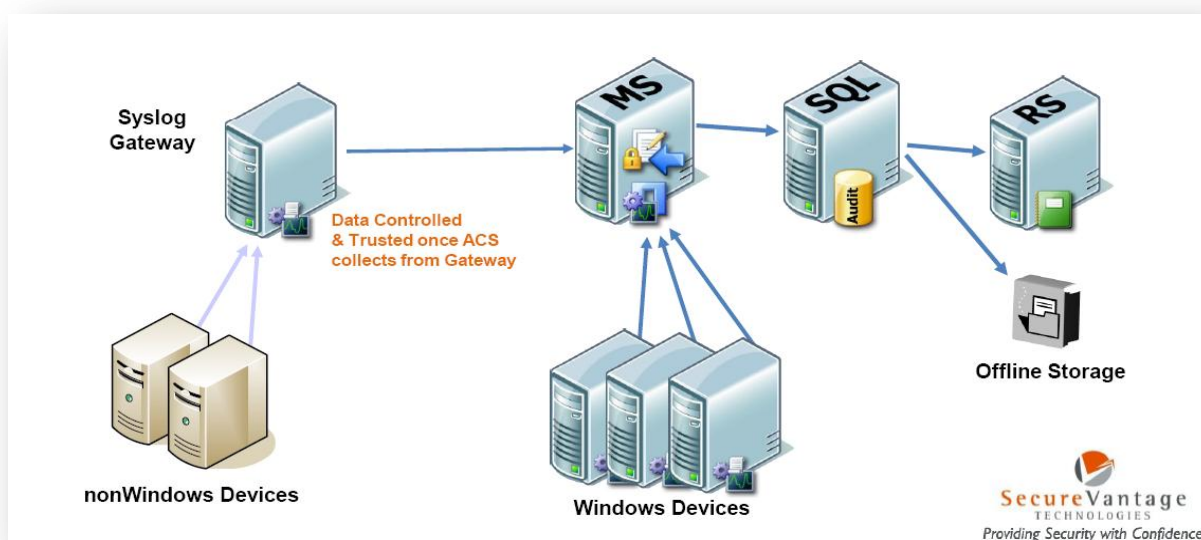


FIG. 2 – INTEGRAZIONE DI SISTEMI NON WINDOWS

È opportuno aggiungere che nei prossimi mesi saranno rilasciati da Microsoft alcuni moduli nativi di integrazione con ACS per le seguenti piattaforme:

- RedHat Enterprise 4, 5
- Novell SLES 9, 10, 11
- Solaris 8, 9, 10
- HPUX 11iv2, 11iv3
- AIX 5.3, 6.1

## SERVIZI POSSIBILI PER LE PIATTAFORME NON MICROSOFT

Progel è in grado di fornire consulenza per la configurazione ai fini di auditing di sistemi non Microsoft laddove il cliente non sia autonomo con proprio personale o consulenti terzi. Data l'eterogeneità dei sistemi che è possibile includere, i servizi Progel su queste piattaforme hanno le seguenti limitazioni:

- Progel si riserva di coinvolgere propri fornitori terzi per la configurazione di questi sistemi
- Si assume che i sistemi siano in grado di raccogliere informazioni di auditing e di veicolarle tramite syslog o nativamente, oppure tramite prodotti disponibili commercialmente che il cliente si impegna ad acquistare.
- Non è previsto lo sviluppo di codice per queste piattaforme

## GESTIONE DI LOGGING ESTERNO AL SECURITY LOG

Alcuni applicativi non sono in grado di scrivere i propri eventi di audit all'interno del security log.

In questi casi è necessario implementare un sistema per la codifica di questi eventi in eventi di security così da poter essere collezionati tramite ACS. A questo fine Progel ha sviluppato il Progel Security Log Gateway che al momento copre SQL Server 2000, SQ Server 2005 e SQL Server 2008 Standard (la versione Enterprise ha la capacità di scrivere nel security log), Oracle DBMS a partire dalla versione 8i, Exchange Server ed ISA Server. Per il momento questo modulo include esclusivamente eventi di logon, ma può essere esteso per gestire altri eventi in base alle esigenze del cliente.

## CAPACITY PLANNING

Il capacity planning della raccolta di eventi di security ha un elevato margine di aleatorietà essendo legato a fattori caratteristici di ogni ambiente (es. numero di logon che ogni utente effettua al giorno, o durata media della password). La stima dovrà dunque essere rivista dopo il primo periodo di esercizio.

Ai fini della proposta si utilizzeranno due modelli:

- 1) Il primo riprende le indicazioni disponibili da parte di Microsoft e può essere considerato come una stima per eccesso, un tetto massimo che molto difficilmente sarà superato
- 2) Il secondo prende spunto da una media registrata, dopo un prolungato periodo di utilizzo, da parte di clienti Progel che hanno già utilizzato la soluzione

Ipotizzando un'infrastruttura con una decina di server, questa è la stima dei dati raccolti mensilmente:

Dato	Microsoft	Stima su clienti
<b>Dimensione database (GB)</b>	50 GB	20 GB
<b>Dimensione log (GB)</b>	3 GB	2 GB
<b>Spazio disco da allocare (GB)</b>	60 GB	25 GB

TAB. 2 – STIMA DATA RACCOLTI MENSILMENTE

La stima mensile deve essere moltiplicata per il periodo durante il quale si intende avere i dati in linea.

La disposizione del Garante prevede almeno 6 mesi (180 giorni) di dati conservati e interrogabili, ma non specifica che questi debbano essere in linea. Se si vuole mantenere in linea meno dei 180 giorni previsti è possibile ricorrere ad un opportuno piano di backup o all'archiviazione di Secure Vantage.

La stima prende in considerazione una raccolta di log non limitata ai soli eventi di logon e logoff, ma allargata alle operazioni amministrative compiute sugli account utente (aggiunta, rimozione, reset della

password, ...). Nel caso il cliente intenda raccogliere solo logon e logoff i volumi saranno inferiori, ma non è possibile darne una stima.

I dati indicati fanno riferimento ai soli sistemi Windows coperti dalla soluzione. Per i sistemi esterni sarà necessario un periodo di raccolta dati prima di poter fornire una stima attendibile.

Tutti i ruoli Operations Manager possono essere virtualizzati su piattaforma Microsoft. Per piattaforme di virtualizzazione non Microsoft rimane valido quanto indicato nella KB 897615 *“Support policy for Microsoft software running in non-Microsoft hardware virtualization software”*. Per questo motivo si daranno indicazioni in termini generici sulle performance richieste per i vari ruoli identificati dal progetto. A carico del cliente la decisione di implementarli tramite virtualizzazione oppure su server fisici, fatto salvo la soddisfazione dei requisiti minimi di performance richiesti.

## ATTIVITÀ PREVISTE

Le attività per la realizzazione della soluzione sono le seguenti:

- Installazione dell'infrastruttura Operations Manager comprensiva di Audit Collector Service (ACS)
- Installazione e configurazione del monitor utile al controllo dell'infrastruttura ACS
- Installazione degli agenti e consulenza nella creazione delle Policy di auditing.
- Integrazione dei nuovi sistemi nell'infrastruttura di backup del cliente assumendo che il sistema di backup in essere sia in grado di fare il backup dei sistemi e delle tecnologie coinvolte
- Pianificazione degli opportuni task di manutenzione sul sistema fornito
- Eventuale installazione del syslog gateway di Secure Vantage per la collezione dei syslog
- Consulenza per l'auditing su piattaforme e device non Microsoft
- Hardening dell'infrastruttura Operations Manager per evitarne l'accesso agli amministratori
- Eventuale installazione e configurazione dei Progel Security Gateway

## REPORTS

La soluzione messa a punto da Progel è corredata dalla personalizzazione di alcuni reports per agevolare le verifiche sulla corretta raccolta dei log di accesso, di cui se ne riporta qualche esempio.

Dal  Al

Utente  Azione

Filtra per data di creazione in security log

1 of 4 100% Find | Next Select a format Export

1988 2008 **20**progel

### Disposizione Garante Privacy Novembre 2008 - Amministratori di sistema - Logon / Logoff per amministratore

Il report mostra tutti gli eventi di logon e logoff registrati dai sistemi operativi e dai provider applicativi per l'utente indicato nella finestra temporale specificata

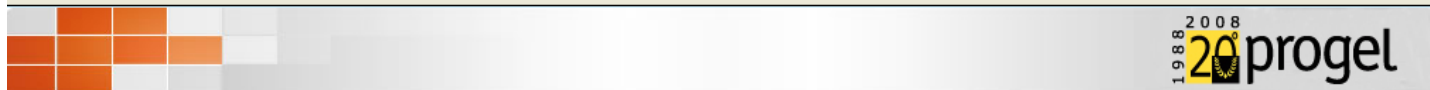
Dal : 12/1/2009 7:38:04 PM  
 Al : 12/2/2009 7:38:04 PM  
 Azione : Logon, Logoff, Logon/Logoff  
 Utente : grandinid  
 Seleziona per data creazione in security log : True

Data	Azione	Sistema	Provider	S/F	Tipo Logon	Evento
12/1/2009 8:18:59 PM	Logon	DC02.pre.lab	Win2k8	S	Network	4624
12/1/2009 8:19:01 PM	Logon	DC02.pre.lab	Win2k8	S	Network	4624
12/1/2009 8:19:01 PM	Logon	DC02.pre.lab	Win2k8	S	Network	4624
12/1/2009 8:19:01 PM	Logon	DC02.pre.lab	Win2k8	S	Network	4624
12/1/2009 8:19:01 PM	Logoff	DC02.pre.lab	Win2k8	S	Network	4634
Sequence		93412105		Collection Time		12/1/2009 8:19:05 PM
Category		Logoff		Creation Time		12/1/2009 8:19:01 PM
Agent		PRE\DC02\$		Source		Win2k8
Header Sid/User/Domain		n/a		n/a		n/a
Primary Sid/User/Domain		n/a		n/a		n/a
Client Sid/User/Domain		n/a		n/a		n/a
Target Sid/User/Domain		S-1-5-21-4185495620-1739196763-3906522881-1171 grandinid		PRE		n/a
Strings		0x490ff615 3		n/a		n/a
12/1/2009 8:19:03 PM	Logoff	DC02.pre.lab	Win2k8	S	Network	4634
12/1/2009 8:19:38 PM	Logoff	DC02.pre.lab	Win2k8	S	Network	4634
12/1/2009 8:20:31 PM	Logoff	DC02.pre.lab	Win2k8	S	Network	4634

TAB. 3 – REPORT DI LOGON-LOGOFF PER AMMINISTRATORE

Dal  Al   
 Sistema  Azione   
 Filtra per data di creazione in security log

of 3581  Find | Next  Export



### Disposizione Garante Privacy Novembre 2008 - Amministratori di sistema - Logon / Logoff per sistema

Il report mostra tutti gli eventi di logon e logoff registrati dai sistemi operativi e dai provider applicativi per l'utente indicato nella finestra temporale specificata

Dal	: 12/1/2009 7:41:13 PM
Al	: 12/2/2009 7:41:13 PM
Azione	: Logon, Logoff, Logon/Logoff
Sistema	: sql2k8.pre.lab
Selezione per data creazione in security log	: True

Data	Azione	Utente	Provider	S/F	Tipo Logon	Evento
12/1/2009 6:41:59 PM	Logon	SYSTEM	PSLG SQL Server	S		30004
12/1/2009 6:42:00 PM	Logon	Administrator	PSLG SQL Server	S		30004
12/1/2009 6:42:00 PM	Logon	Administrator	PSLG SQL Server	S		30004
	Sequence		56883474	Collection Time		12/1/2009 7:42:03 PM
	Category	Logon		Creation Time		12/1/2009 7:42:00 PM
	Agent / System	PRE\SQL2K8\$	sql2k8.pre.lab	Source	PSLG SQL Server	
	Header Sid/User/Domain	S-1-S-19	LOCAL SERVICE	NT AUTHORITY		
	Primary Sid/User/Domain	S-1-S-21-4185495620-1739196763-3906522881-500	Administrator	PRE		
	Client Sid/User/Domain		[CLIENT: <local machine>]			
	Target Sid/User/Domain	n/a	n/a	n/a		
	Strings	2009 12 01 18:42:00	MSSQLSERVER	Administrator	PRE	sql2k8.pre.lab
12/1/2009 6:42:00 PM	Logon	Administrator	PSLG SQL Server	S		30004
12/1/2009 6:42:00 PM	Logon	Administrator	PSLG SQL Server	S		30004
12/1/2009 6:42:59 PM	Logon	SYSTEM	PSLG SQL Server	S		30004
12/1/2009 6:43:00 PM	Logon	Administrator	PSLG SQL Server	S		30004
12/1/2009 6:43:00 PM	Logon	Administrator	PSLG SQL Server	S		30004

TAB. 4 – REPORT DI LOGON-LOGOFF PER SISTEMA