Provvedimento sugli Amministratori di sistema

Spunti di discussione per l'adeguamento tecnico

Paolo Giardini - Resp. Relazioni OPSI
Osservatorio Nazionale Privacy e Sicurezza delle Informazioni

Distinguiamo due linee principali di sistemi(*)

1) Sistemi Windows
2) Sistemi *NIX

(*)Esistono altri sistemi, ovviamente, con i relativi problemi e strumenti ma esulano dalle mie competenze.

1) Sistemi Windows

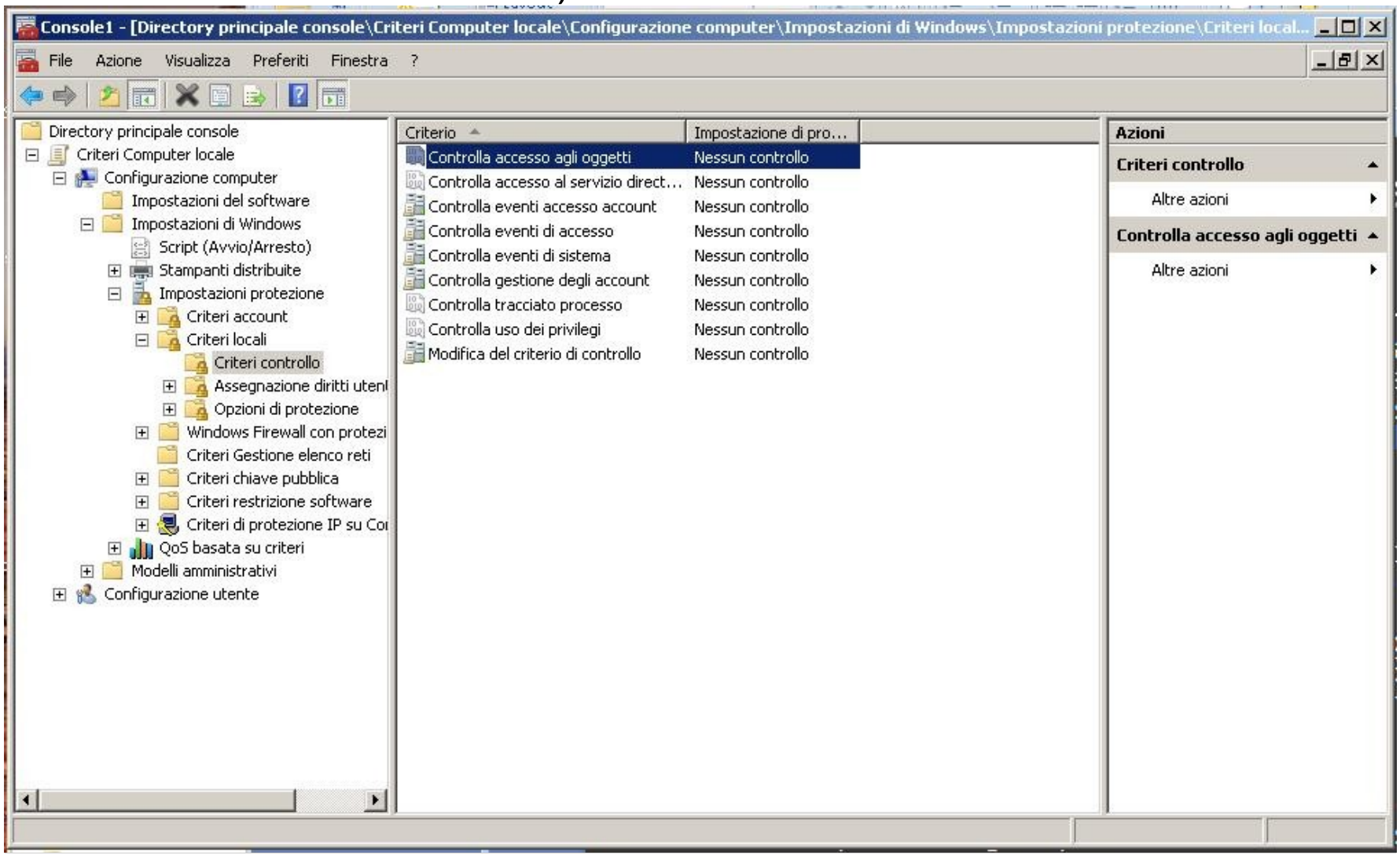
Si distinguono due casi:

a) Computer stand alone o in gruppo di lavoro
b) Computer inserito in un dominio

In entrambi i casi esiste il sistema di log interno di Windows, “Event log”, che memorizza gli eventi in file in formato proprietario “.evt” localizzati, in genere, nella cartella:

c:\windows\system32\config.

Per attivare i log è necessario attivare le Group Policy (su Win XP home ci sono dei problemi da risolvere... Sulle versioni home di Vista non ho notizie su come fare.)



•Se il computer fa parte di un dominio si opera sul server, altrimenti l'impostazione va fatta su ogni singolo computer.

•La registrazione può comprendere sia gli eventi riusciti che quelli non riusciti.

•Ogni evento legato ad un computer inserito in un dominio comporta una registrazione sia sul log del server che su quello del computer locale.

•Ovviamente in caso di computer stand-alone la registrazione avviene solo sul pc locale.

•I file .evt possono essere copiati ma essendo in formato proprietario non sono direttamente consultabili (p.e. con un editor di testo). Esistono strumenti messi a disposizione da Microsoft per editing, consultazione, estrazione, backup, inserimento su database:

•LOG Parser:
http://www.microsoft.com/technet/scriptcenter/tools/logparser/default.mspx

•Script appositi in VBS:
http://www.microsoft.com/technet/scriptcenter/scripts/default.mspx?mfr=true

•Eventlog Management Tool (per windows 2000):
http://support.microsoft.com/kb/318763/en-us/

Ad esempio si potrebbe usare uno script (scaricabile dal sito MS) per effettuare una copia remota del log su file o database.

2) Sistemi *NIX

Il log dei sistemi *NIX è in qualche modo più semplice.

•I log vengono creati automaticamente dal sistema syslog nella cartella */var/log* in formato testo.

•Vengono registrati eventi di sistema, accessi e tentativi di accesso.

•Il log può essere facilmente remotizzato con strumenti open source:

Syslog-ng:
http://www.balabit.com/network-security/syslog-ng/
http://www.dia.unisa.it/~ads/corso-security/www/CORSO-0304/Syslog/index.html

Rsyslog
http://freshmeat.net/projects/rsyslog/

Interoperabilità

• Esistono strumenti per registrare su sistemi Windows i log generati da sistemi *NIX, per esempio Kiwi syslog ed altri

http://www.kiwisyslog.com/
http://www.winsyslog.com/en/

•Esistono strumenti per registrare su sistemi *NIX i log generati da sistemi Windows, come ntsyslog

http://sourceforge.net/projects/ntsyslog/
http://troy.jdmz.net/syslogwin/
http://www.jrsoftware.org/isdl.php
http://www.aboutdebian.com/syslog.htm
http://www.syslogserver.com/download.html

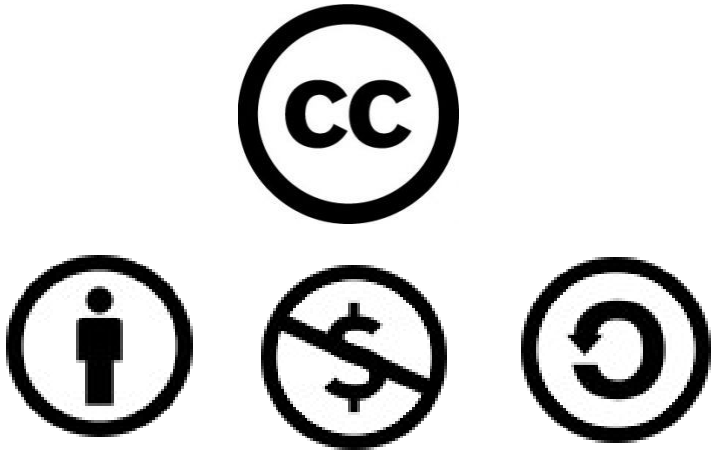
•Altre risorse:

http://www.loganalysis.org/sections/syslog/windows-to-syslog/index.html

Meritano ulteriori riflessioni i seguenti punti:

- **Conservazione**
  - I file di log dovranno essere conservati in modo che non siano alterabili per almeno 6 mesi. In che modo? “Almeno” significa anche “per sempre”?
- **Riferimenti temporali**
  - La data ed ora di sistema devono essere corretti per consentire eventuali correlazioni temporali. Problemi a dimostrare l'esattezza dell'ora della registrazione, al minino serve una sincronizzazione via NTP.
- **Inalterabilità**
  - Copia su cdrom con somma di controllo (MD5, SHA*) ?
  - Con firma digitale e marca temporale?
- **Chi controlla il controllore?**
  - Chi garantisce che l'Amministratore di sistema (o root) ovvero colui che può gestire tutto, (compresi i log), non li modifichi a suo vantaggio?

Questo lavoro viene distribuito sotto licenza
Creative Commons 3.0



Sei libero di copiare, distribuire, trasmettere quest'opera e di modificarla a condizione di: attribuirne la paternità all'autore originale, non usare quest'opera per fini commerciali, condividerla allo stesso modo.