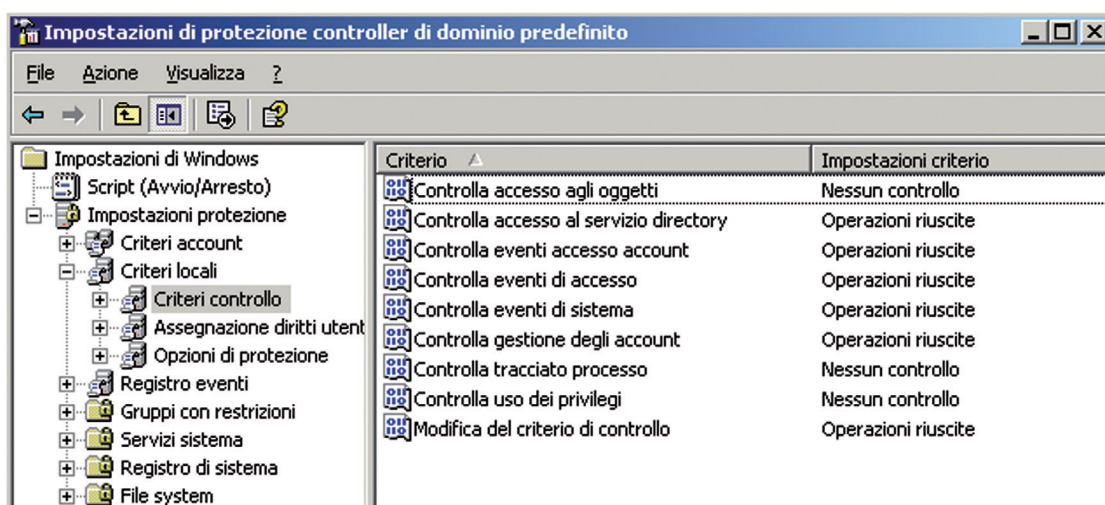


IMPOSTARE I CRITERI DI AUDITING

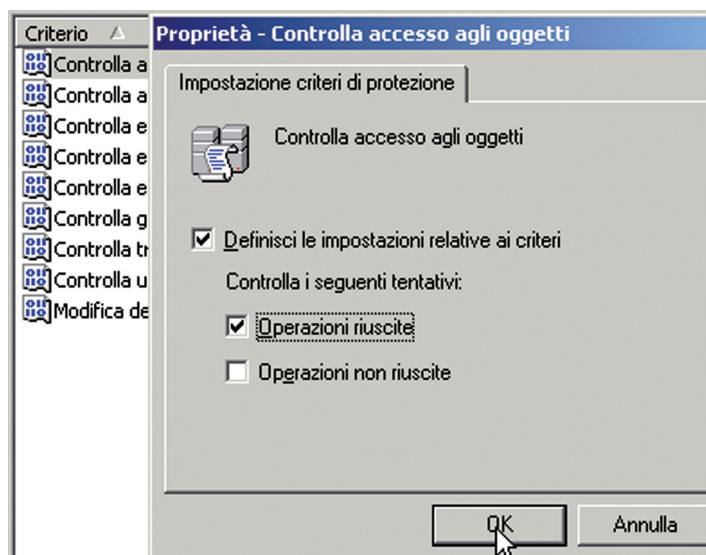
Impostare i criteri di auditing

La seguente procedura illustra come abilitare i **Criteri di Auditing** con Windows versione server:

1. apri la Console negli **Strumenti di Amministrazione**;
2. fai doppio clic su **Criteri locali**, quindi doppio clic su **Criteri di controllo**;



3. fai clic con il tasto destro, nel pannello di destra, sul criterio che vuoi abilitare (in questo caso **Controlla accesso agli oggetti**) e seleziona la voce **Proprietà**. Appare la seguente finestra:



4. spunta la voce **Definisci le impostazioni relative ai criteri** e quindi le voci **Operazioni riuscite** o **Operazioni non riuscite** secondo le esigenze;
5. chiudi la Console.

Per monitorare gli Eventi di Auditing esistono diversi metodi per monitorare gli eventi scritti nel registro eventi. A seconda delle necessità e delle circostanze possiamo scegliere tra quattro metodi principali:

- visualizzatore di eventi;
- script personalizzati;
- Event Comb.
- strumenti completamente automatizzati (ad esempio **Microsoft Operations Manager**).

Visualizzatore di Eventi

È lo strumento più semplice per monitorare gli eventi e permette di:

- vedere i dettagli degli eventi;
- ordinare eventi per tipo, criterio di auditing, data;
- cercare eventi per aree comuni;
- filtrare eventi per aree comuni;
- esportare registri di eventi in formato .evt, .csv, .txt;
- connettersi a computer remoti e gestire il Registro Eventi.



Il Visualizzatore di Eventi non permette l'unione di eventi, possono infatti nascere problemi per eventi registrati su più server, come gli eventi di Accesso ad Account. Il Visualizzatore inoltre non permette la ricerca di dettagli di eventi.

Esportando gli eventi in un file, si possono importare in un database o eseguire script personalizzati da molti computer.

Script Personalizzati


Esistono molti script nati con lo scopo di gestire eventi, vediamo alcuni.

- [Dumpel.exe](#). Riversa e filtra registri eventi in un file di testo separato.
- [Eventlog.pl](#). È uno script scritto in linguaggio Perl che ripulisce e copia file di registro, mostra e modifica le relative impostazioni.
- [Eventquery.vbs](#). È uno script scritto in visual basic che mostra gli eventi di file di registro di Windows Server.
- [LogParser 2.2](#). È un versatile strumento che analizza file basati su testo come i registri di auditing e crea rapporti in linguaggio SQL-like.

Event Comb

L'Event Comb analizza Registri Eventi da più server, generando percorsi distinti di esecuzione per ciascun server incluso nei criteri di ricerca, inoltre permette di mettere insieme eventi da più computer. Inoltre permette di cercare occorrenze di eventi per qualsiasi area negli eventi riuniti, cercare tra i registri archiviati ed seguire ricerche molto specifiche grazie ai parametri offerti.



La maggior parte dei firewall, sia hardware che software, dispone di software di monitoraggio, per l'analisi dettagliata dei log che vengono inviati via mail all'amministratore. Inoltre esistono **software stealth**  che effettuano auditing sui computer client della rete.



Software stealth

I software stealth hanno la capacità di controllare quanto si scrive alla tastiera, i siti web visitati, le eventuali chat, catturare a cicli predefiniti immagini del desktop e inviare il tutto a una cartella su un server, in modo che l'amministratore possa controllare il tutto, come per esempio [SpyAgent](#).