

Approfondimenti

dott. Stefano D. Fratepietro

steve@stevelab.net



CIRSFID
Università degli studi di Bologna



stevelab.net

Creative Commons license Stefano Fratepietro - www.stevelab.net

1



Contenuti

- **Modello client server**
- Utenti e gruppi
- Task Manager
- Event view
- Personalizzazione del sistema

Creative Commons license Stefano Fratepietro - www.stevelab.net

2

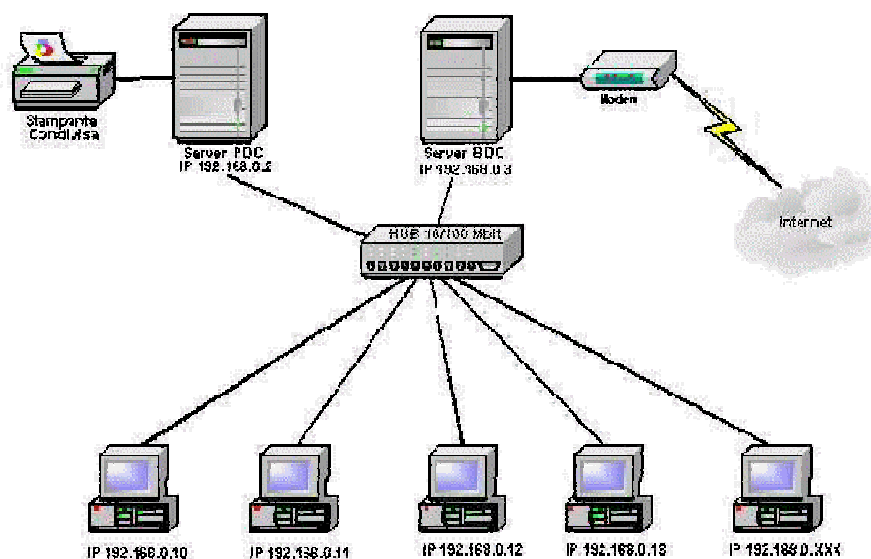


Modello Client Server I

- Un'applicazione client-server è semplicemente un'iterazione tra due o più computer dove uno dei computer fornisce un servizio, gli altri ne usufruiscono
- Formalmente, è un tipo di applicazione di rete nel quale un computer client istanzia l'interfaccia utente di un'applicazione connettendosi ad una server application o ad un sistema di database



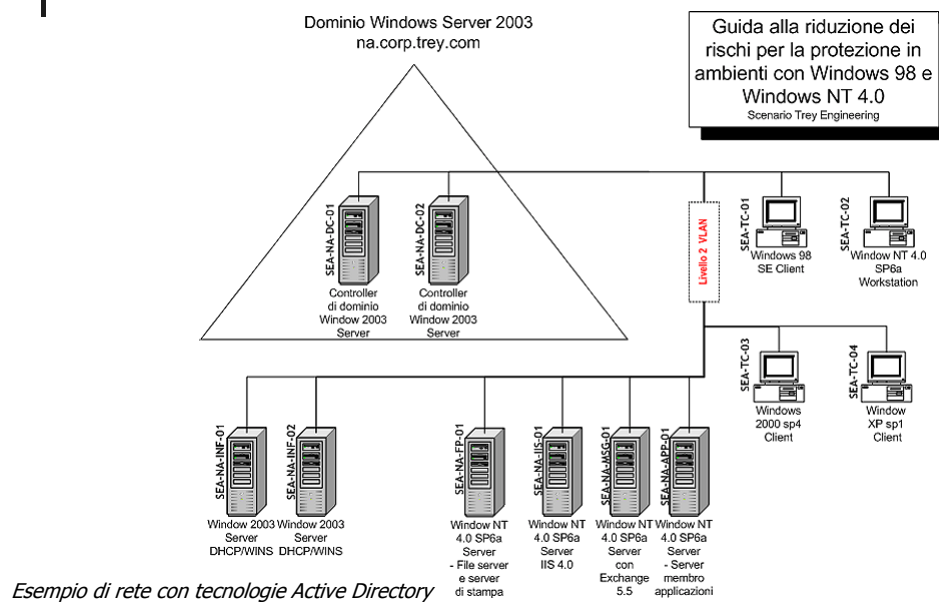
Modelo Client Server II



Esempio di rete con tecnologia Domini NT



Modello Client Server III



Modello Client Server IV





Modello Client Server V

- Esempi applicazioni client server:
 - Autenticazione in reti Active Directory
 - Iterazione con database
 - Condivisione di file all'interno di una rete
 - Trasferimento di immagini tra due o più computer collegati in diverse reti



Protocolli Active Directory

- Active Directory utilizza vari protocolli come:
 - LDAP
 - DNS
 - DHCP
 - Kerberos



LDAP

- In Active Directory LDAP viene usato come una base di dati che memorizza in forma centralizzata tutte le informazioni di un dominio di amministrazione, col vantaggio di mantenere le informazioni sincronizzate tra i vari server di autenticazione di accesso alla rete



Contenuti

- Modello client server
- **Utenti e gruppi**
- Task Manager
- Event view
- Personalizzazione del sistema

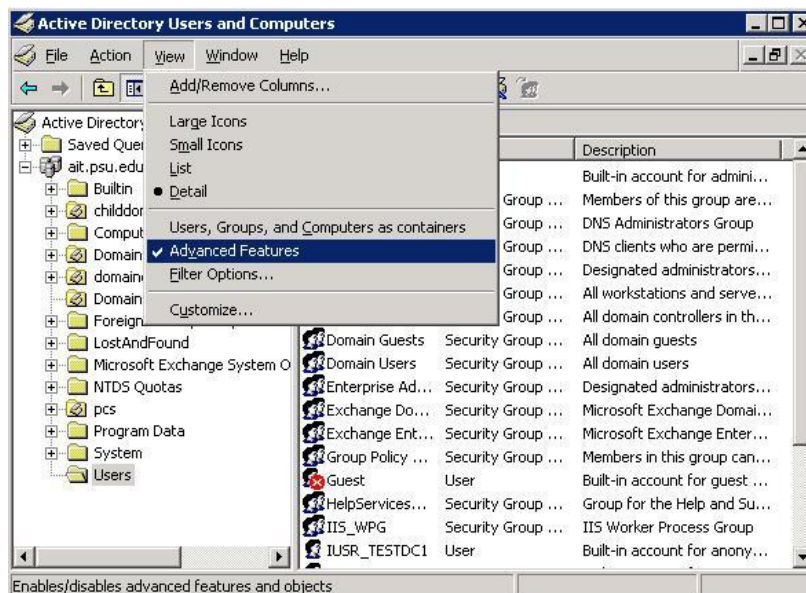


Utenti e gruppi I

- Active Directory è il nome utilizzato da Microsoft per riferirsi alla sua implementazione della sicurezza in una rete distribuita di computer
- Ogni singolo utente può avere un livello di "privilegi" superiore o inferiore rispetto ad un altro utente
- Ogni gruppo di utenti può avere un livello di "privilegi" superiore o inferiore rispetto ad un altro gruppo di utenti
- Questi privilegi sono delle policy di Active Directory applicate direttamente al gruppo o al singolo utente



Utenti e gruppi II





Permessi su file remoti

- Valgono le stesse regole dei permessi su file locali
- Nelle foreste di domini, si possono creare delle limitazioni a seconda del dominio e del gruppo di appartenenza al dominio



Contenuti

- Modello client server
- Utenti e gruppi
- **Task Manager**
- Event view
- Personalizzazione del sistema



Task Manager I

- Nei moderni sistemi operativi ad interfaccia grafica è detto Task manager l'applicazione a livello kernel che permette di monitorare le applicazioni in esecuzione sulla macchina
- Tutti gli utenti utilizzatori del sistema hanno l'autorizzazione per visualizzare a video la lista dei processi delle applicazioni attualmente in utilizzo



Task Manager II

- Sistemi Windows 2000 e XP permettono di monitorare e controllare in modo separato le applicazioni aperte e i processi in esecuzione
- Nei moderni sistemi operativi al task manager è in genere assegnata una combinazione particolare e riservata di tasti, questa combinazione è Ctrl+Alt+Canc, che nei vecchi sistemi DOS attivava il riavvio a caldo della macchina
- Per motivi di sicurezza questa hotkey non può essere in alcun modo alterata o dirottata, essendo controllata direttamente da winlogon.exe, processo di sistema a livello di kernel

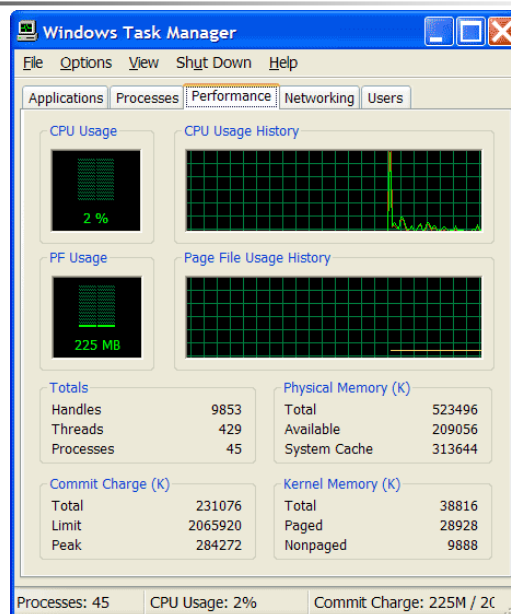


Task Manager III

- E' articolato in quattro sezioni che monitorizzano e gestiscono:
 - Le applicazioni attualmente in utilizzo
 - I processi attualmente in esecuzione
 - La quantità di CPU (in percentuale) e di memoria di sistema utilizzata (Ram)
 - Il traffico dei dispositivi di rete
 - Nelle reti con domini gestiti da Active Directory, vi è la possibilità di vedere gli utenti utilizzatori del sistema (utenti locali e remoti)



Task Manager IV





Contenuti

- Modello client server
- Utenti e gruppi
- Task Manager
- **Event view**
- Personalizzazione del sistema



Event view I

- I file registro eventi contiene i record degli eventi di sistema cioè tutti gli avvisi e tutte le operazioni riuscite e non riuscite durante l'esecuzione dei processi
- E' presente in tutti i sistemi Windows dalla versione 2000 in poi, sia lato client che lato server



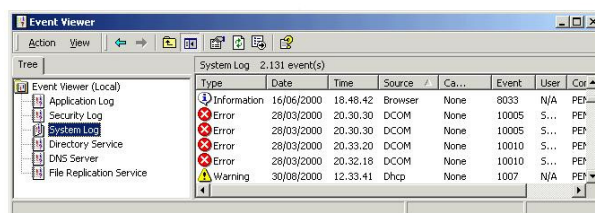
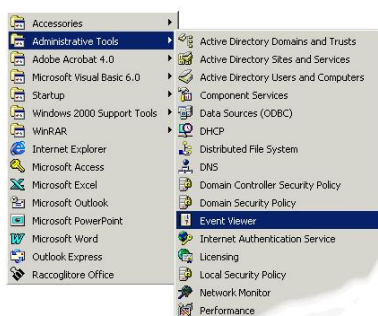
Event view II

Gli eventi vengono registrati in tre tipi di file registro:

- Sistema: (cartellasistema\System32\Config\Sysevent.evt) contiene gli eventi relativi a tutti i componenti del sistema e driver di periferica di Windows NT
- Protezione: (cartellasistema\System32\Config\Secevent.evt) contiene le informazioni sui tentativi di accesso validi e non validi e quelle sull'utilizzo delle risorse, quali la creazione, l'apertura o l'eliminazione di file o di altri oggetti
- Applicazione: (cartellasistema\System32\Config\Appevent.evt) contiene gli eventi generati dalle applicazioni
- Al file registro di protezione possono accedere solamente gli amministratori e va attivato manualmente da User Manager scegliendo Audit dal menu policies e selezionando gli eventi si desidera controllare



Event view III





Status dei messaggi

- Icona rossa con **X**: evento errore
- Icona bianca con **i**: evento informazione
- Icona gialla con **!**: evento di avviso importante



Contenuti

- Modello client server
- Utenti e gruppi
- Task Manager
- Event view
- Personalizzazione del sistema
- Operazioni di manutenzione



Bibliografia

- <http://it.wikipedia.com>
- <http://stevelab.net/didattica.html>
- <http://guide.supereva.it>
- Microsoft Windows 2000 Administrator's Pocket Consultant, Second Edition