NOLABNOPARTY

Informatica applicata per l'azienda

procedure e guide step-by-step

Procedure informatiche orientate per un ambito aziendale documentate in maniera dettagliata e chiara illustrando tutti i passaggi richiesti con figure e descrizioni.

http://nolabnoparty.com

Titolo: Informatica applicata per l'azienda
Autore: Paolo Valsecchi
Distribuzione: nolabnoparty.com

http://nolabnoparty.com

Blog di informatica applicata per l'azienda

Email: nolabnoparty@gmail.com

Condizioni di utilizzo

Note

Alla data di scrittura dei capitoli, alcune versioni dei software utilizzati potrebbero essere differenti da quelle riportate.

Salvo stravolgimenti nelle nuove release, le procedure descritte non dovrebbero subire variazioni di rilievo.

Indice

Servizi Windows

Configurare Remote Assistance in Windows 2008 R2 tramite GPO

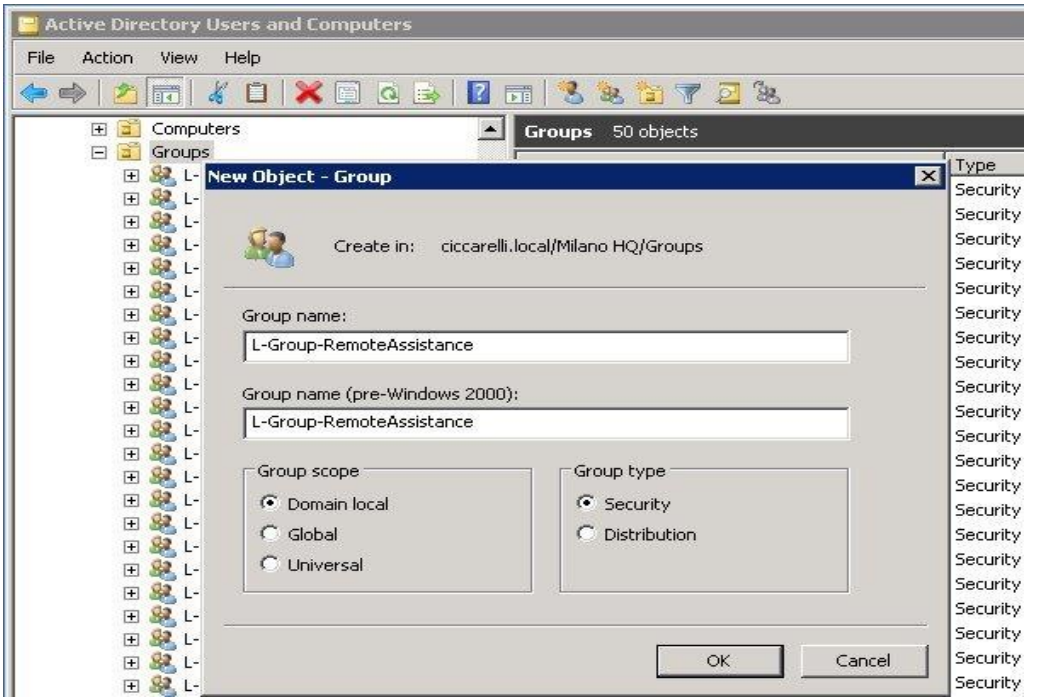
Il servizio di *Remote Assistance* è un ottima soluzione a costo zero per fornire il supporto IT remoto agli utenti della rete restando comodamente seduti davanti al proprio computer.

Il servizio è presente in *Windows* già da tempo ma con l'avvento di *Windows Server 2008 R2 / Windows 7* qualcosa è cambiato nella configurazione creando un po' di confusione.

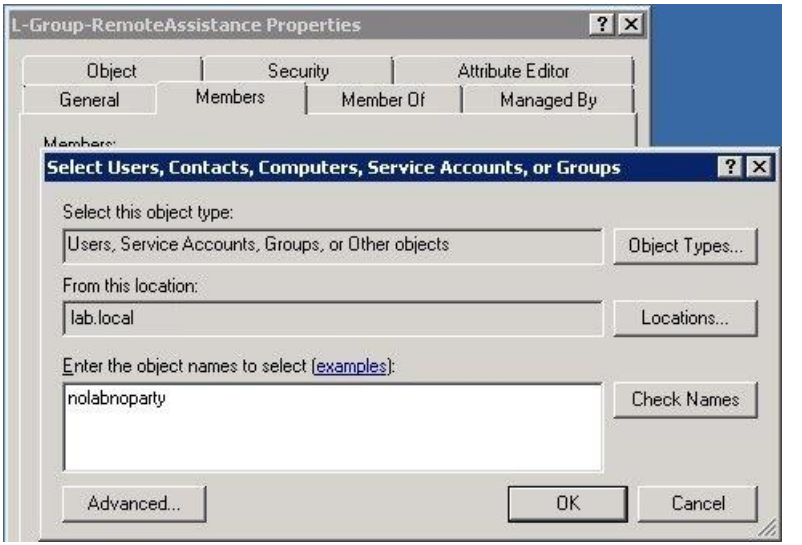
Per la configurazione di Remote Assistance in un ambiente di Active Directory, ci si avvale delle GPO che permettono di **processare i client di rete** in modo efficiente.

Procedura

Come prima cosa bisogna definire quali account/group devono avere i diritti sui client per fornire il servizio di help desk. Creare un nuovo Security Group in *Active Directory*.



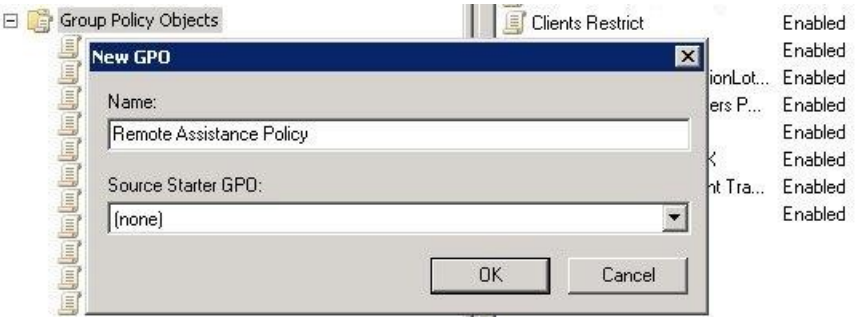
Assegnare al gruppo creato gli account che hanno l'incarico di fornire il supporto di *Remote Assistance*.



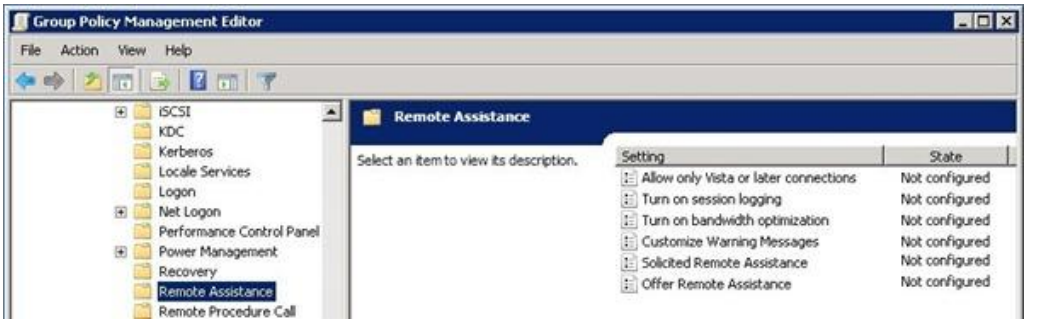
Abilitare Remote Assistance

Operando in un ambiente di rete *Active Directory*, per configurare i client ci si affida alle GPO. Aprire la console *Group Policy Management* e creare una nuova GPO.

Specificare il nome della Policy e cliccare su OK.

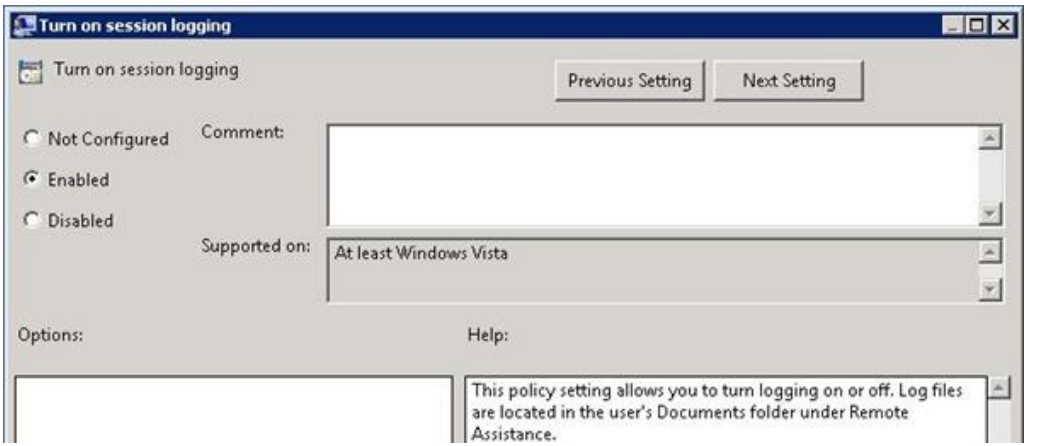


Editare la nuova GPO per procedere con la configurazione dei parametri. Dal *Group Policy Management*, selezionare Computer Configuration –> Policies –> Administrative Templates –> System –> Remote Assistance.

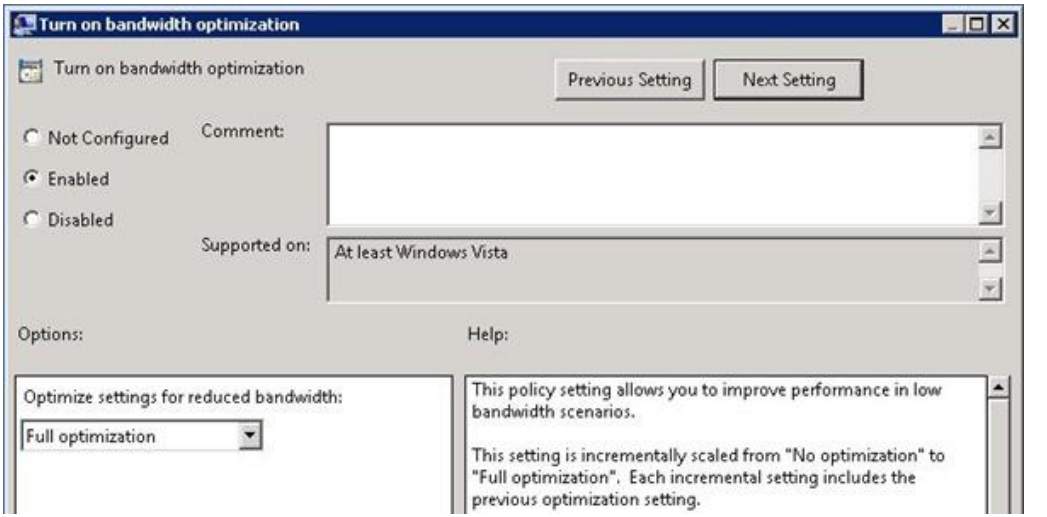


Editare la prima opzione Allow only Vista or later connection. Abilitare o meno questo parametro a seconda dei client presenti nella rete. Click su Next Setting.

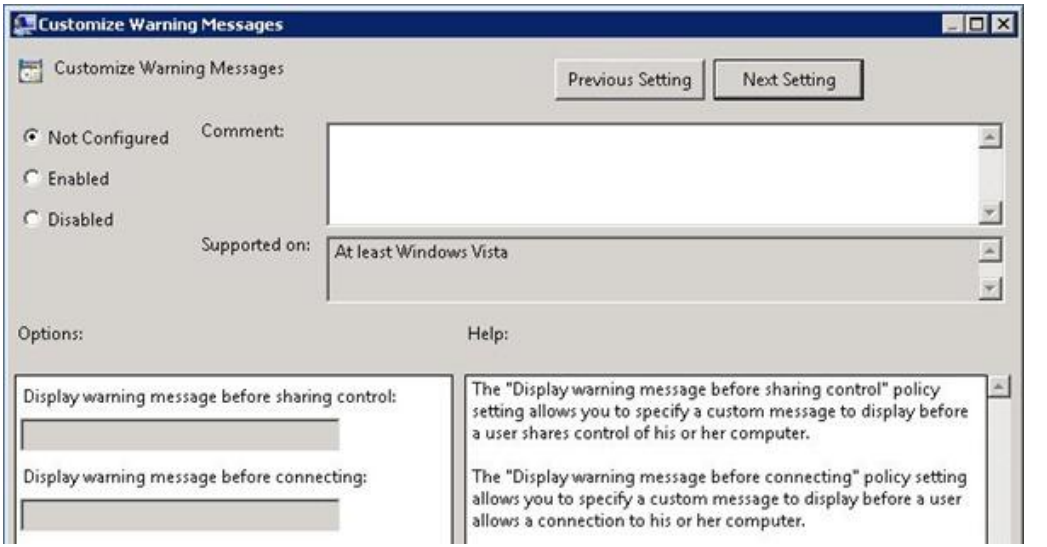
Impostare Turn on session logging come Enabled. Click su Next Setting.



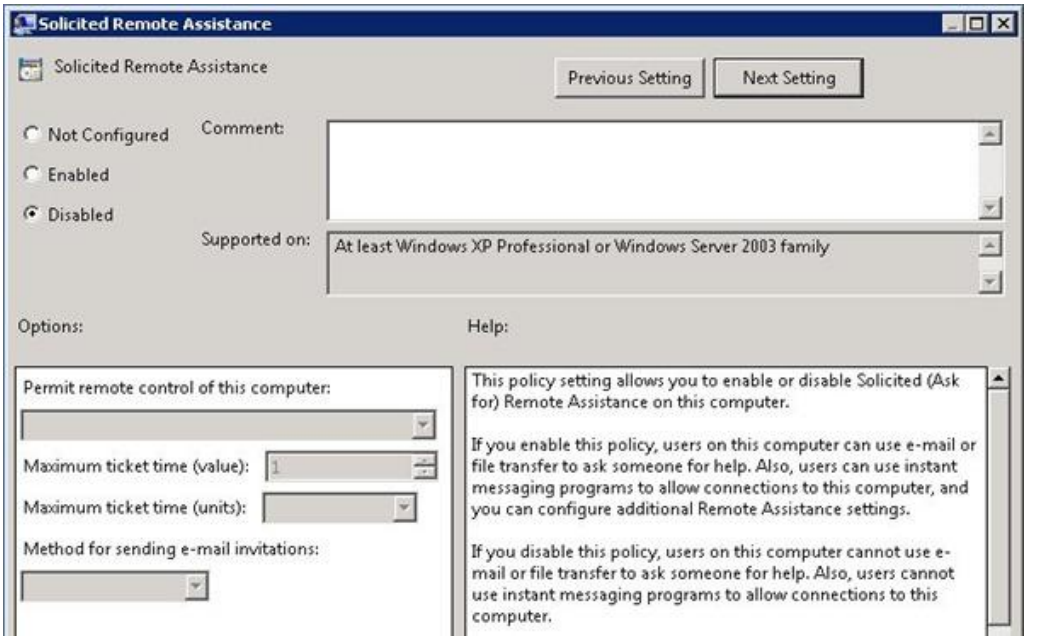
Impostare Turn on bandwidth optimization come Enabled selezionando il valore Full optimization nel campo Optimize settings for reduced bandwidth. Click su Next Setting.



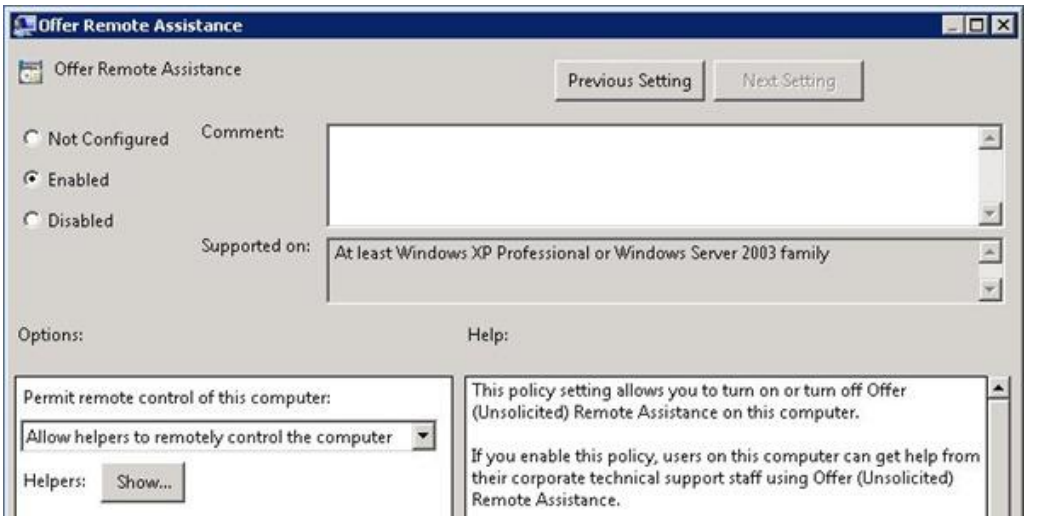
Customize Warning Messages visualizza dei messaggi custom sovrascrivendo quelli di default. Click su Next Setting.



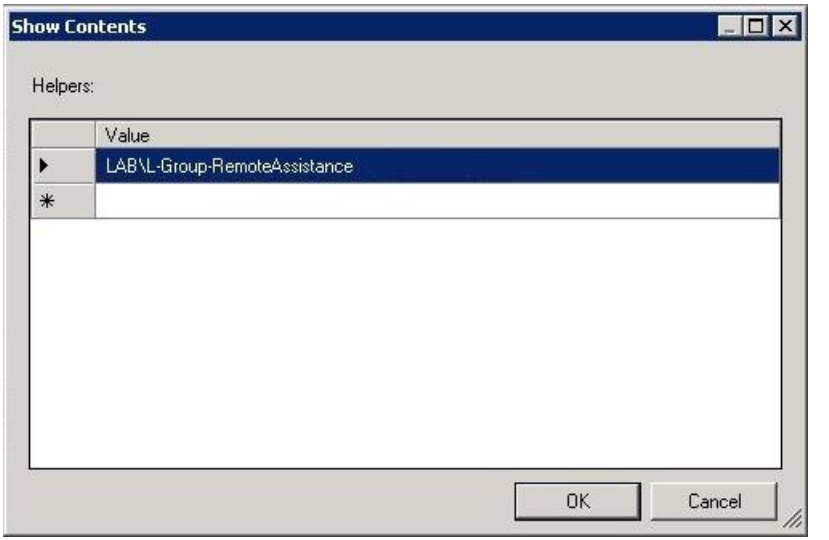
Impostare Solicited Remote Assistance come Disabled. Click su Next Setting.



Impostare Offer Remote Assistance come Enabled. Selezionare nel campo Permit remote control of this computer il valore Allow helpers to remotely control the computer. Cliccare sul bottone Show per indicare gli account da abilitati.



Specificare nel formato *DOMAIN\Group* il gruppo precedentemente creato e cliccare su OK.

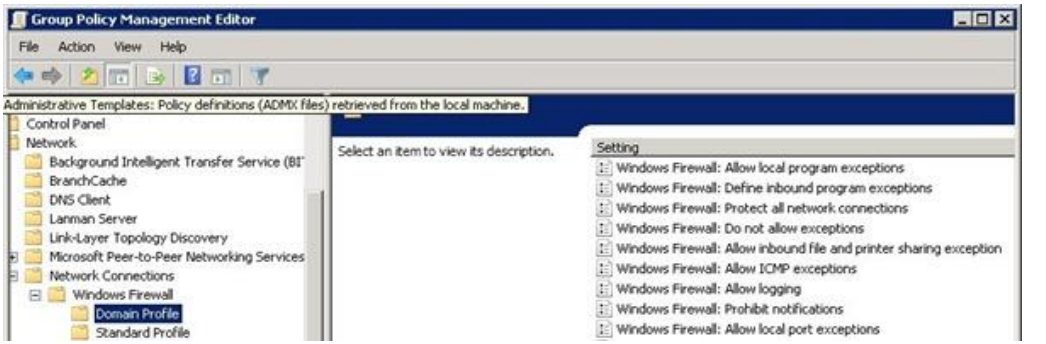


Cliccare su **Apply** per salvare le impostazioni.

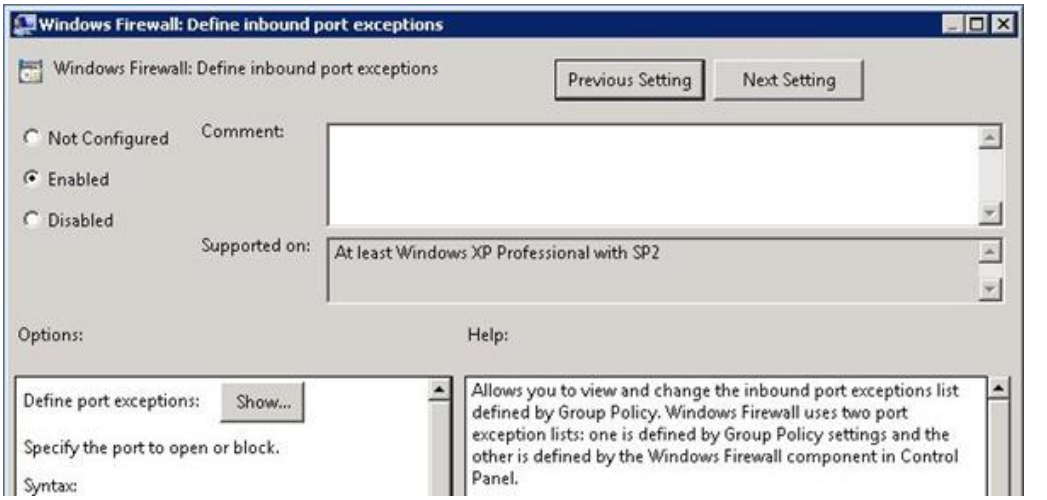
Configurazione del firewall

Mentre per Windows 7 in un ambiente basato su *Active Directory* l'opzione *Remote Assistance exception* è abilitata di default, in Windows XP è necessario configurare alcuni parametri del firewall per il corretto funzionamento.

Dal *Group Policy Management*, selezionare Computer Configuration -> Policies -> Administrative Templates -> Network -> Network Connections -> Windows Firewall -> Domain Profile.

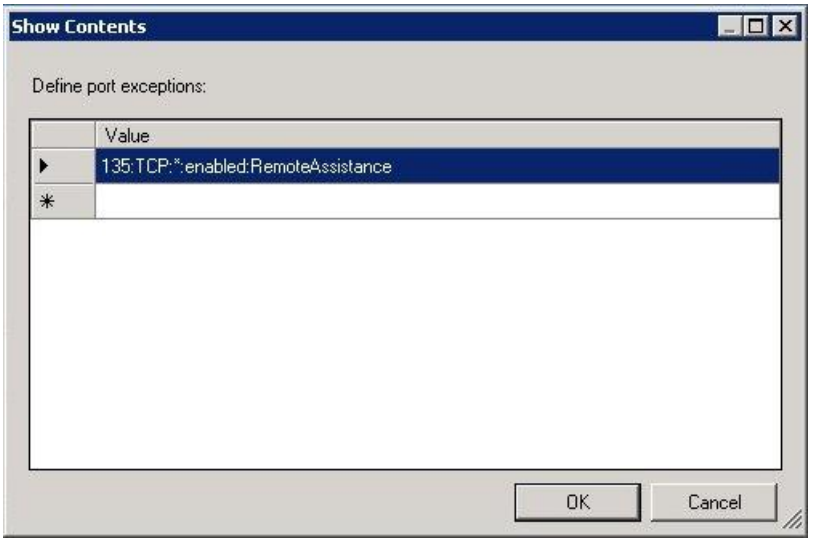


Editare l'opzione Define Inbound port exceptions impostandola come Enabled. Impostare il campo Define port exceptions cliccando sul bottone Show.

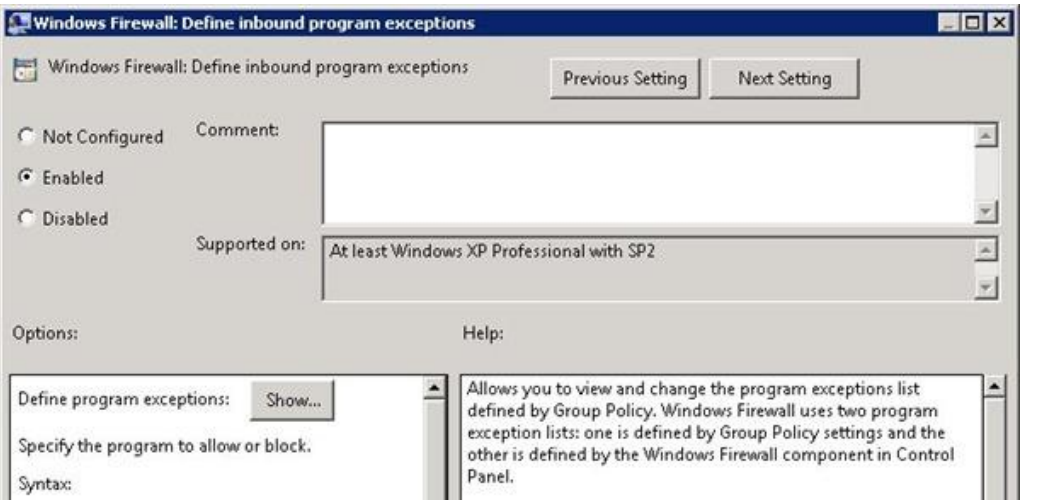


Inserire come Value la stringa:

```
135:TCP:*:enabled:RemoteAssistance
```

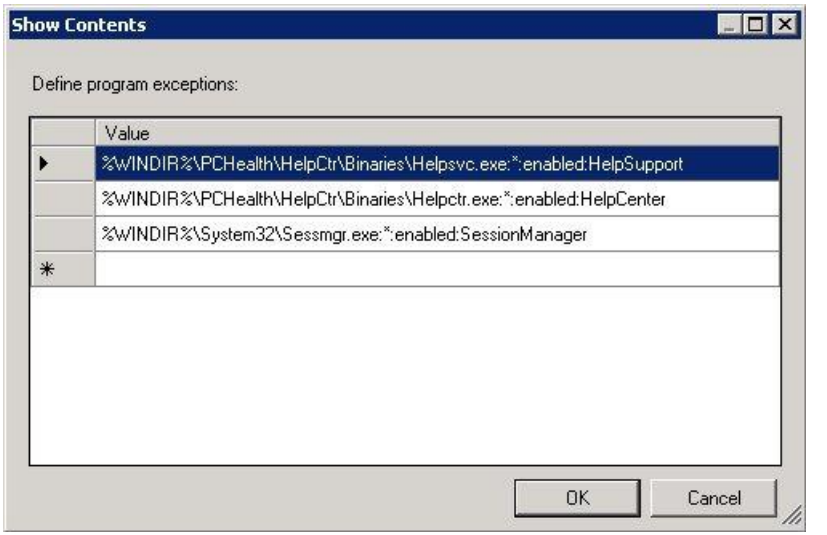


Editare l'opzione Define Inbound program exceptions impostandola come Enabled. Impostare il campo Define program exceptions cliccando sul bottone Show.



Inserire come Value le stringhe:

- %WINDIR%\PCHealth\HelpCtr\Binaries\Helpsvc.exe:*:enabled:HelpSupport
- %WINDIR%\PCHealth\HelpCtr\Binaries\Helpctr.exe:*:enabled:HelpCenter
- %WINDIR%\System32\Sessmgr.exe:*:enabled:SessionManager



Testare Remote Assistance

Una volta configurata la GPO e processata dai client di rete, testare se la procedura appena effettuata funziona come dovrebbe. Dalla *command line* digitare i seguenti comandi:

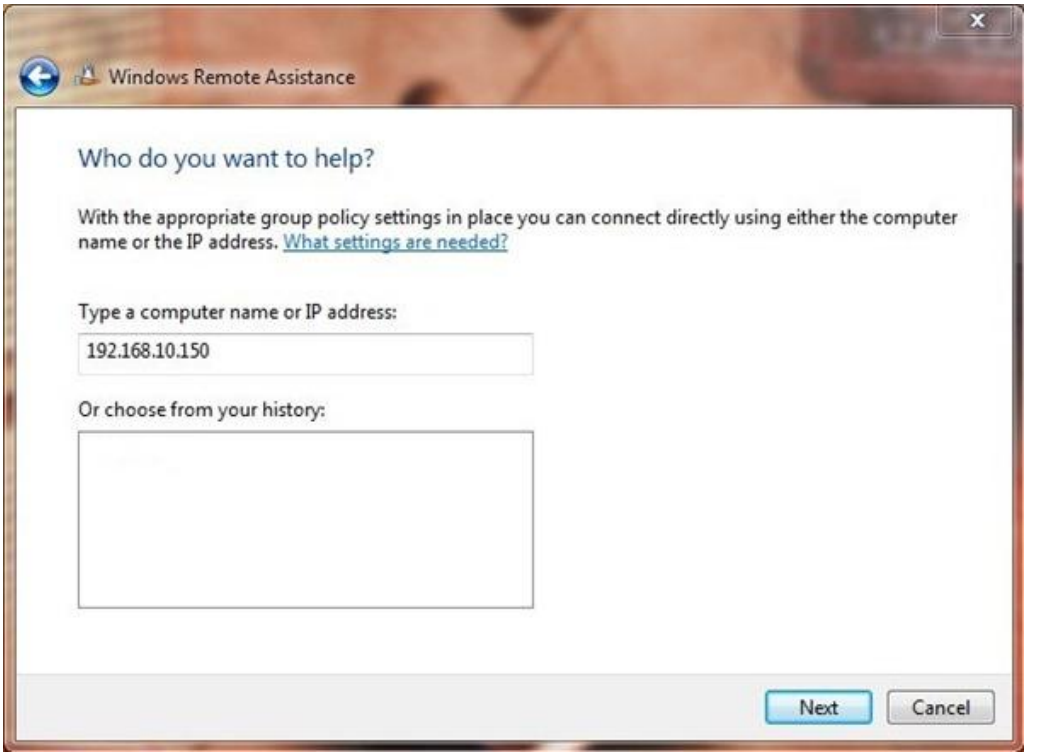
Windows 7

```
%windir%\system32\msra.exe /offerRA
```

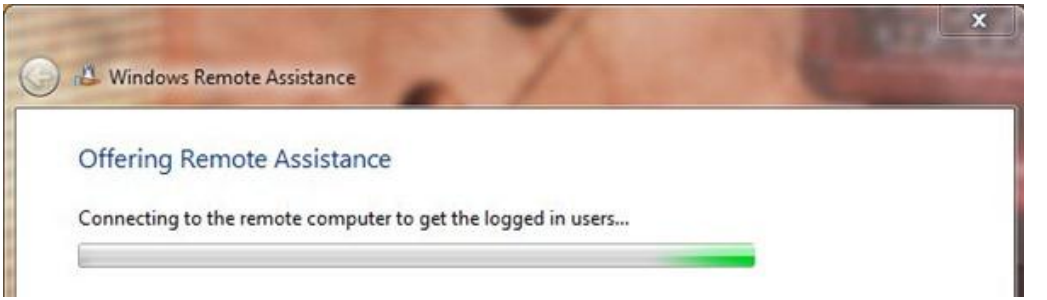
Windows XP

```
hcp://CN=Microsoft%20Corporation,L=Redmond,S=Washington,C=US/Remote%
20Assistance/Escalation/Unsolicited/unsolicitedrcui.htm
```

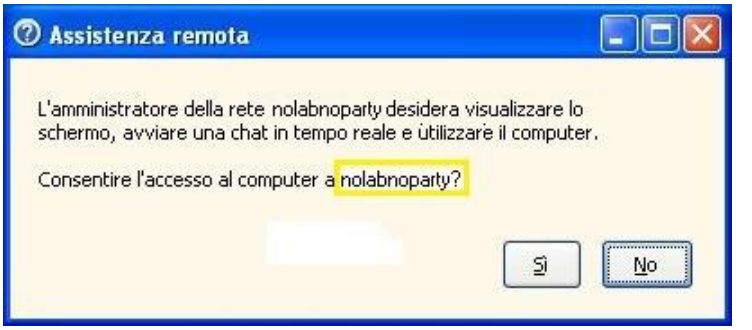
Si apre la finestra Windows Remote Assistance. Digitare l'indirizzo IP o il computer name e cliccare su Next.



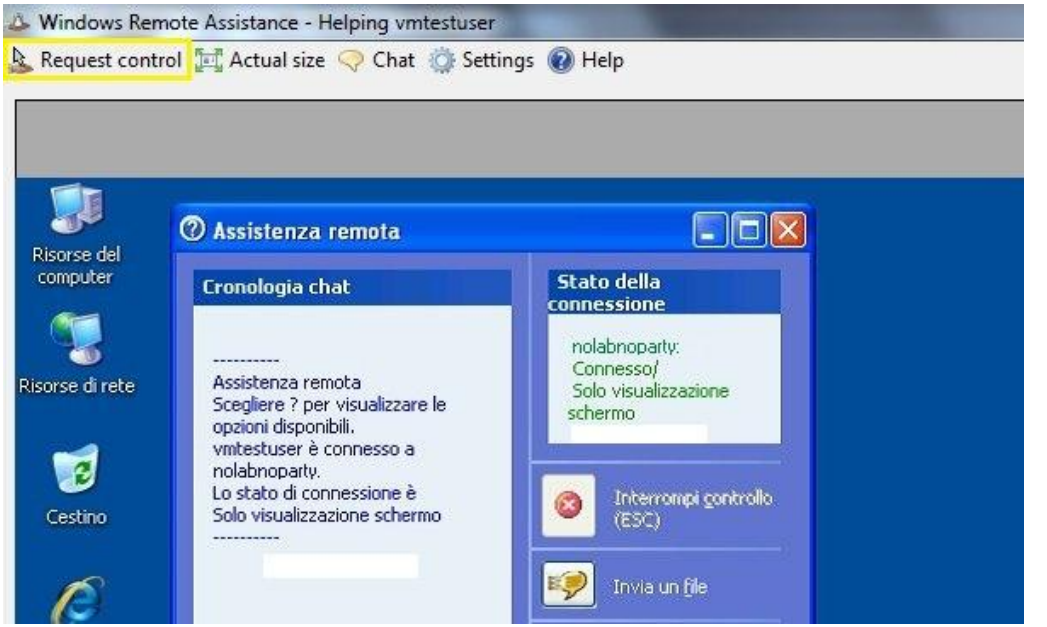
Il sistema effettua la connessione con il client specificato.



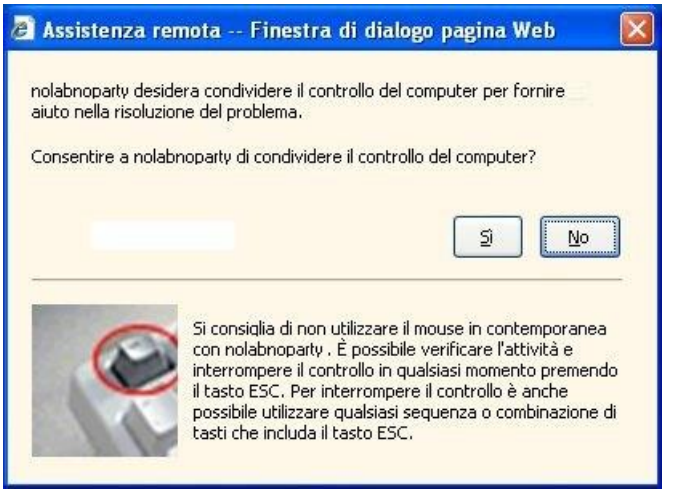
L'utente che ha richiesta assistenza vede comparire nel proprio Desktop la finestra di avviso con il nome dell'helpdesker che sta effettuando la connessione. Cliccando su Si viene data da parte dell'utente l'autorizzazione ad accedere al proprio computer.



Viene stabilita la connessione con il client ma in modalità di solo visualizzazione. Per poter operare sul client bisogna effettuare una richiesta di controllo all'utente tramite il bottone Request control.



L'utente deve cliccare sul bottone Si per dare il controllo del proprio computer all'helpdesker.

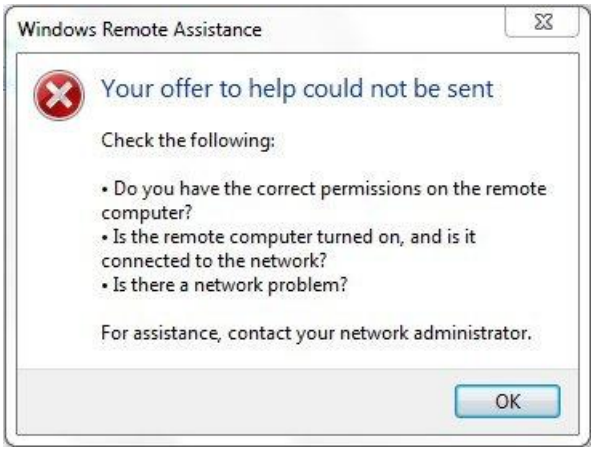


Lo stato della connessione della finestra *Assistenza remota* diventa Connesso/In controllo. Il supporto IT può ora operare sul client fornendo l'assistenza richiesta.

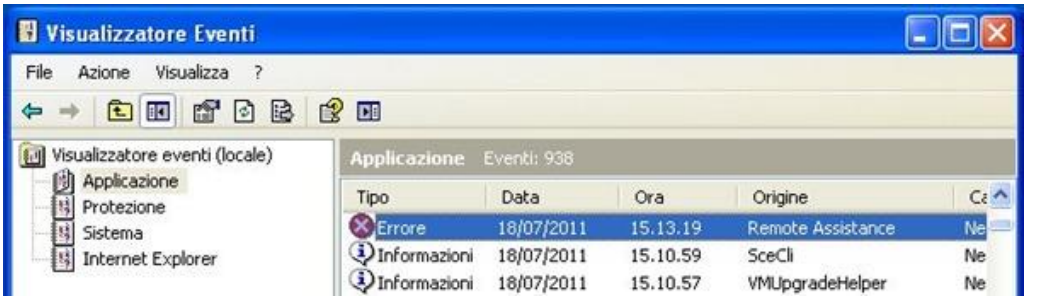
Tramite GPO è quindi possibile configurare il servizio di Remote Assistance in modo veloce e funzionale facilitando il supporto IT nel fornire l'assistenza agli utenti della rete.

Troubleshooting

Può verificarsi che la connessione con il client non venga stabilita e il sistema visualizza una finestra di warning.

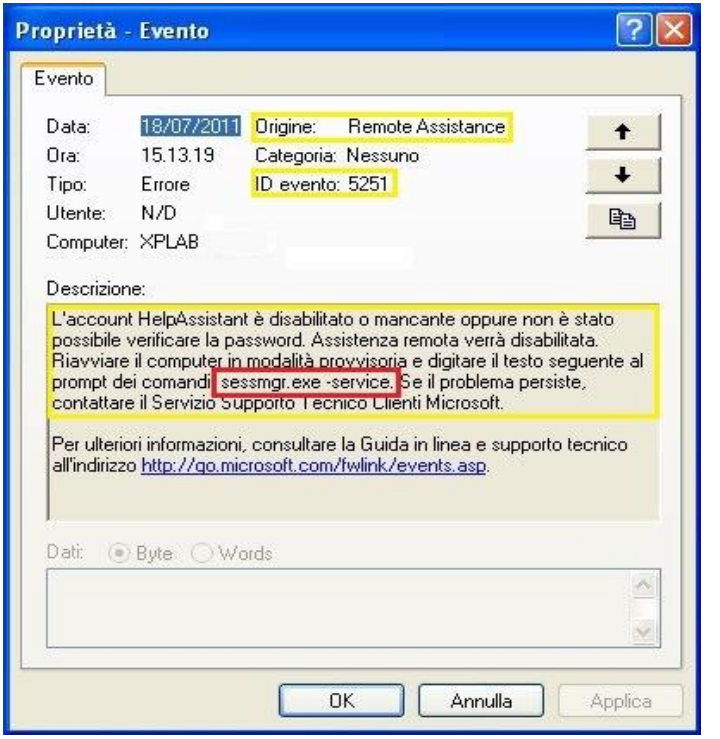


Per capire il motivo del problema, la consultazione dell'*Event Viewer* può dare delle indicazioni significative. Dal client con il quale è stata tentata la connessione, accedere all'*Event Viewer*. Si presenta una segnalazione di errore relativa a *Remote Assistance*.



Facendo doppio click sull'errore, viene visualizzata dal sistema la descrizione della possibile causa del problema che si è verificato. Un esempio può essere il seguente:

- Origine: Remote Assistance
- ID Evento: 5251
- Descrizione: L'account HelpAssistant è disabilitato o mancante oppure non è stato possibile verificare la password.



Questo problema si verifica in genere se viene cambiato il SID del computer utilizzando prodotti come newSID, GhostWalker, etc. Come suggerito nella Descrizione, la soluzione al problema si ottiene avviando Windows in safe mode e lanciando da console il comando:

```
sessmgr.exe -service
```

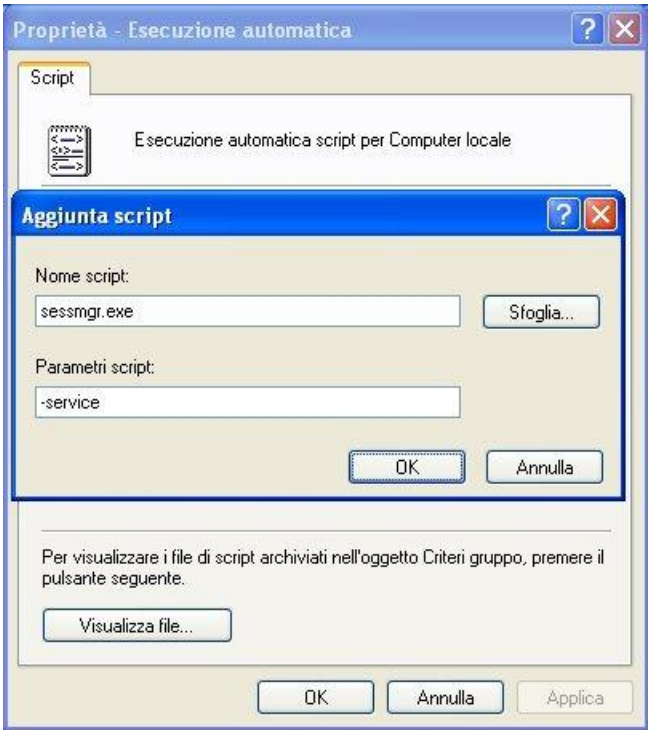
Poichè questa operazione potrebbe richiedere tempo per l'esecuzione in *safe mode*, è possibile lanciare il comando tramite GPO o tramite script.

GPO

Dal client cliccare su Start –> Run e digitare il comando gpedit.msc. Aggiungere i parametri nella sezione Computer Configuration –> Policies –> Windows Settings –> Scripts –> Startup.

Dalla finestra Startup Properties, cliccare sul bottone Add ed impostare i campi della finestra Add a Script con i seguenti valori:

- Script Name: sessmgr.exe
- Script Parameters: -service

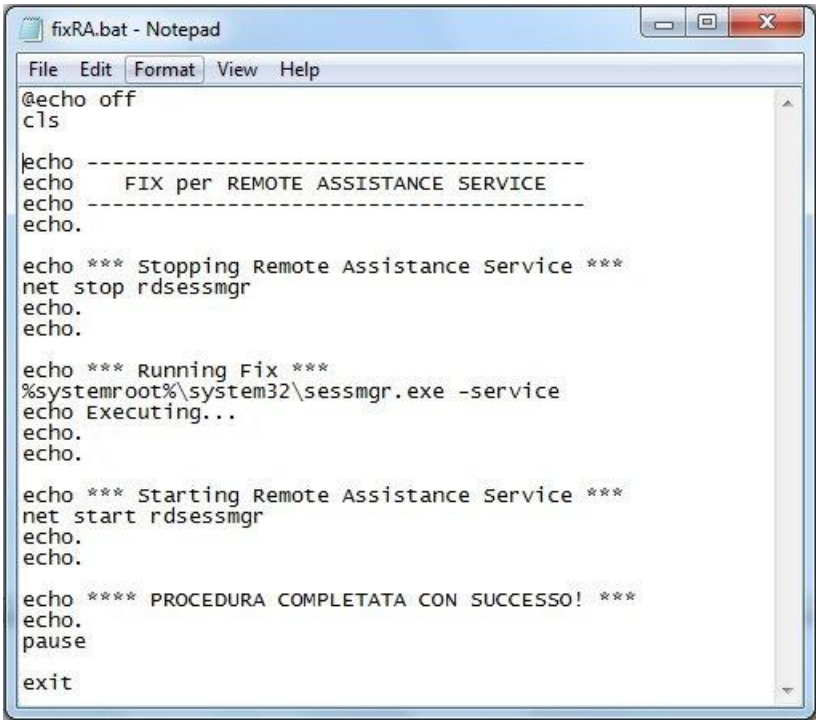


Script

Creare un file batch contenente le seguenti istruzioni:

```
net stop rdsessmgr
%systemroot%\system32\sessmgr.exe -service
net start rdsessmgr
```

Lo script viene eseguito cliccando sul file .bat creato.



Dopo aver eseguito il comando tramite GPO o script, effettuare il reboot del client e provare ad effettuare nuovamente una connessione in *Remote Assistance*.

Il problema relativo all'errore 5251 dovrebbe essersi risolto.

Bloccare l'accesso a Internet a certi utenti tramite GPO

Spesso come policy aziendale, l'accesso a Internet è permesso solo a determinati utenti della rete. Il problema sorge nell'individuare la soluzione ideale per bloccare l'accesso a chi non è autorizzato.

Le soluzioni che si possono implementare sono diverse con diversi gradi di complessità (proxy, firewall, etc.).

Dove il budget disponibile non permette l'implementazione di soluzioni onerose per il portafoglio, è possibile utilizzare una semplice configurazione utilizzando le GPO di *Active Directory*.

Prerequisiti

Per utilizzare al meglio questa soluzione, sono necessari:

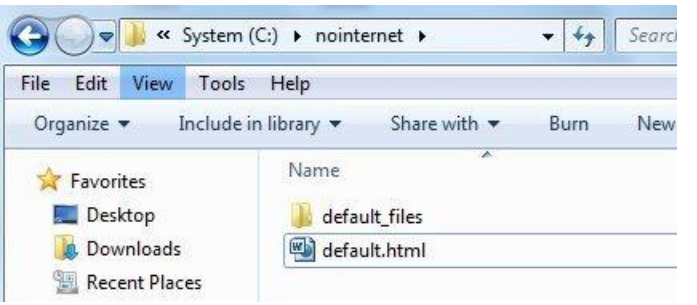
- La presenza nella rete di un *Server IIS*
- Gli utenti non devono avere i diritti di *Local Administrator*

Procedura

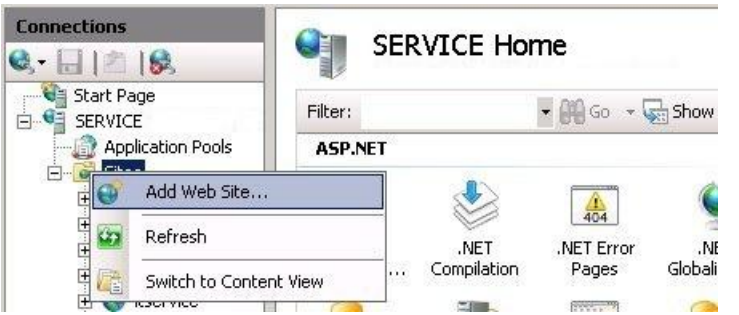
Tramite un html editor (Word ad esempio) creare un file .html in cui viene visualizzato il messaggio di connessione non permessa e salvarlo con nome default.html.

ACCESSO A INTERNET NON AUTORIZZATO

Sul server IIS creare una directory "nointernet" e copiare al suo interno il file *default.html* precedentemente creato assegnando correttamente i permessi di lettura al sistema.



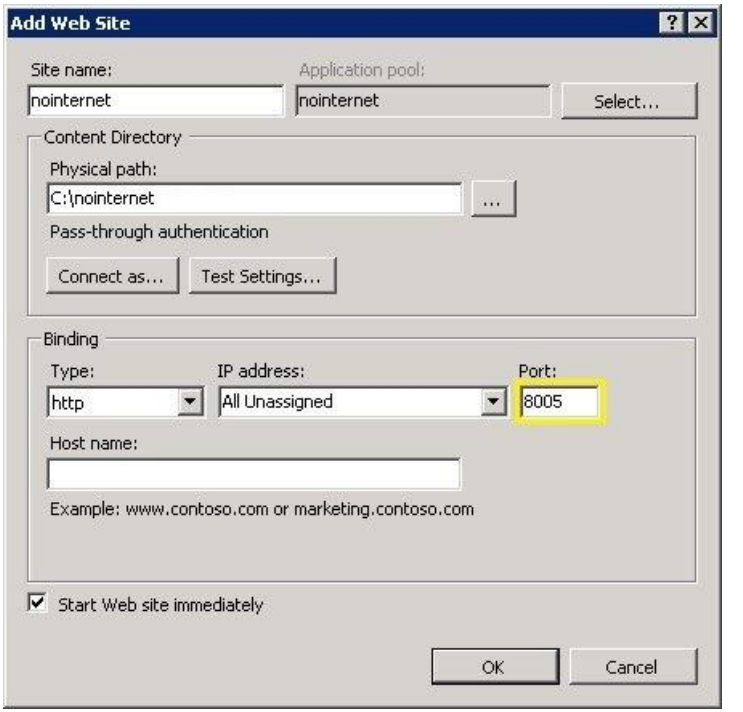
Dal server, aprire Start –> Administrative Tools –> Internet Information Services (IIS) Manager. Click col tasto destro del mouse su *Sites* e selezionare l'opzione Add Web Site.



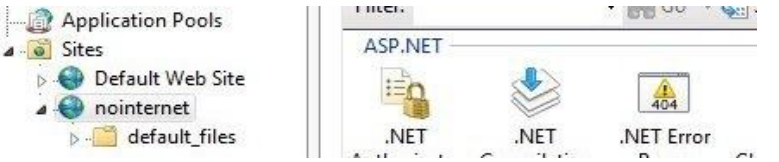
Digitare nei campi i valori precedentemente configurati ed assegnare una porta (*8005* nell'esempio) per il *Binding*.

- Site name: nointernet
- Physical path: C:\nointernet
- Port: 8005 (verificare nel server IIS che la porta impostata non sia già in uso)

Cliccare su OK per creare ed avviare il nuovo sito web.

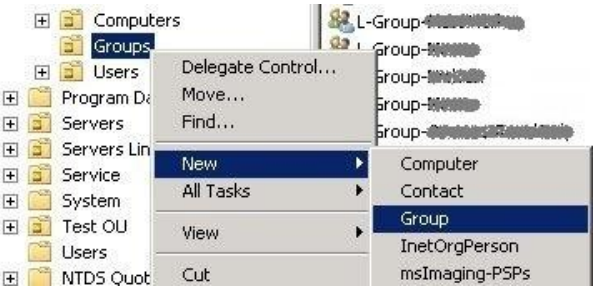


Il sito appena creato compare nella lista dei Sites del sistema.

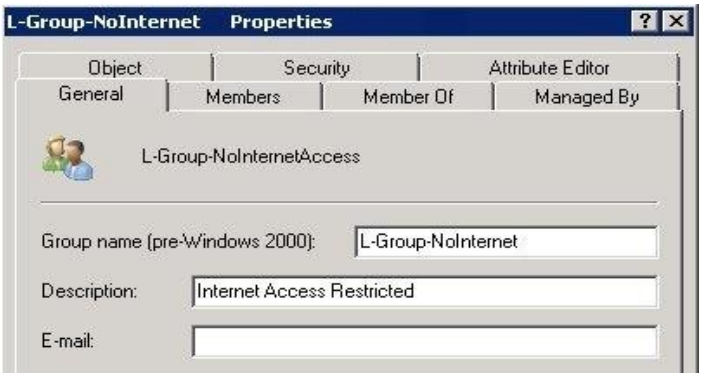


Verificare che il sito sia raggiungibile dai client della rete digitando dal browser di Internet l'indirizzo http://IP_server_iss:8005.

Poichè per bloccare determinati utenti viene utilizzata una Group Policy di *Active Directory*, è necessario utilizzare un security group per contenere la lista di utenti a cui deve essere negato l'accesso a Internet.

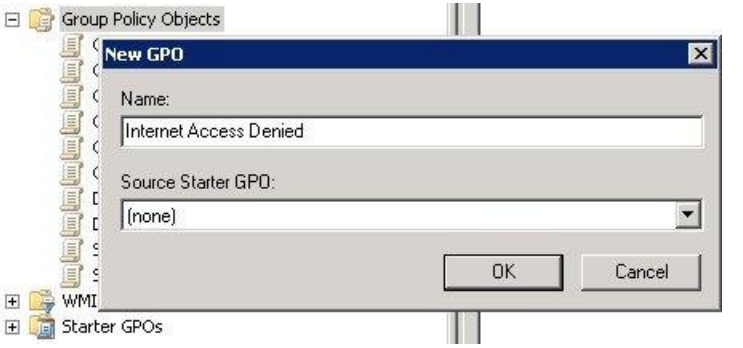


Creare un nuovo gruppo AD dando il nome, ad esempio, L-Group-NoInternet.

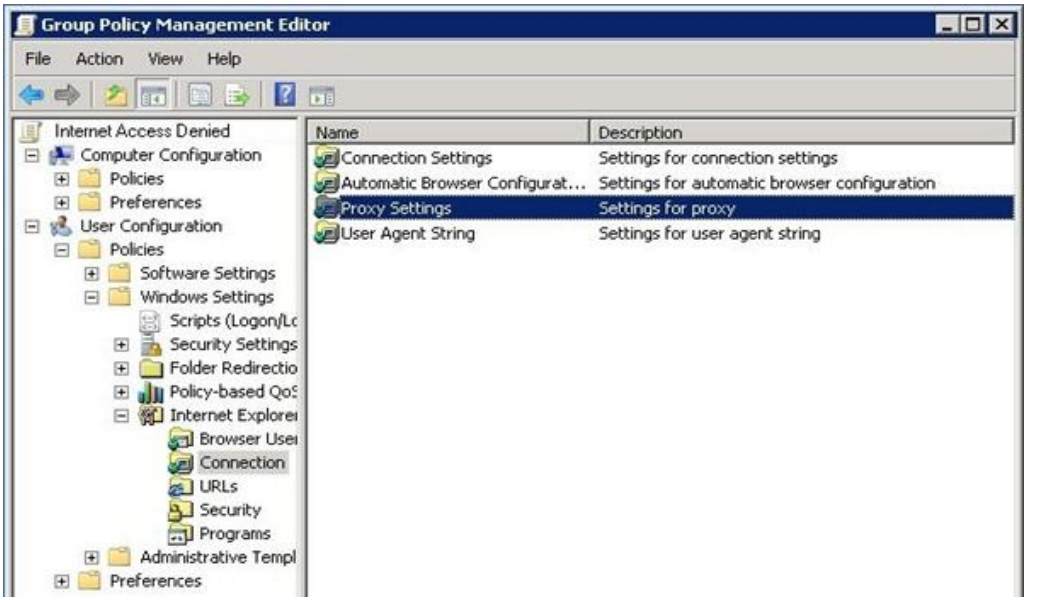


Dal server utilizzato per gestire le GPO, aprire Start –> Administrative Tools –> Group Policy Management.

Sulla voce *Group Policy Objects* fare click col tasto destro del mouse e selezionare New. Dare un nome alla nuova GPO e cliccare su OK.

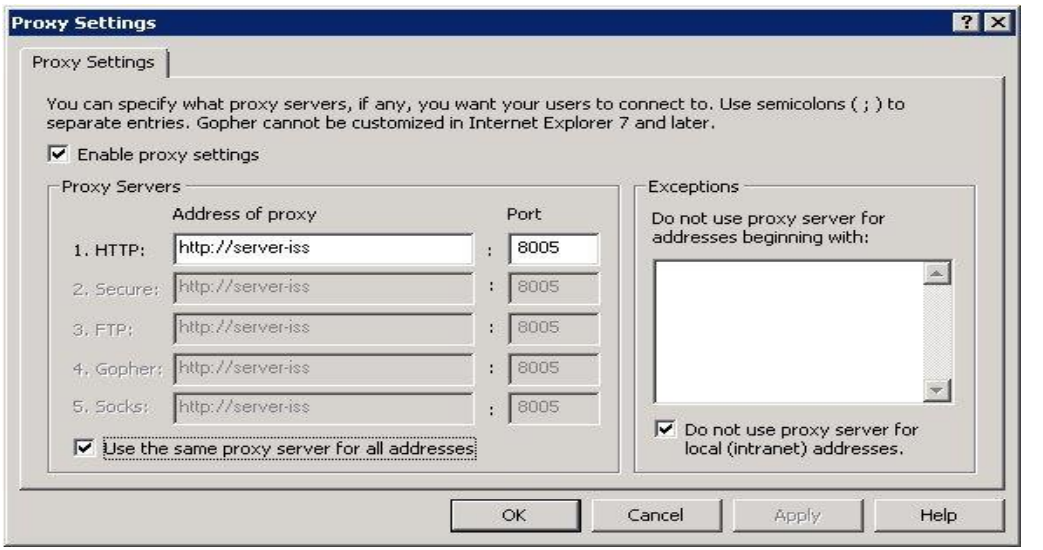


Dal *Group Policy Management Editor*, selezionare la GPO appena creata, cliccare col tasto destro del mouse e selezionare l'opzione Edit. Selezionare User Configuration –> Windows Settings –> Internet Explorer –> Connection –> Proxy Settings.



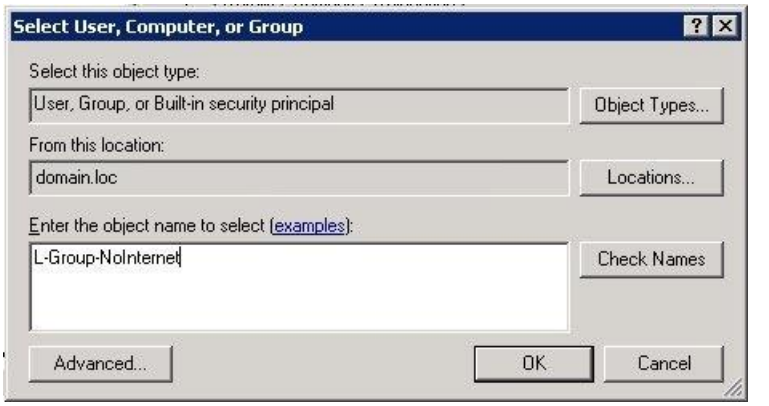
Impostare i Proxy Settings con i valori che riflettono la configurazione della rete e cliccare su OK.

- HTTP: http://IP_Server_ISS
- Port: 8005

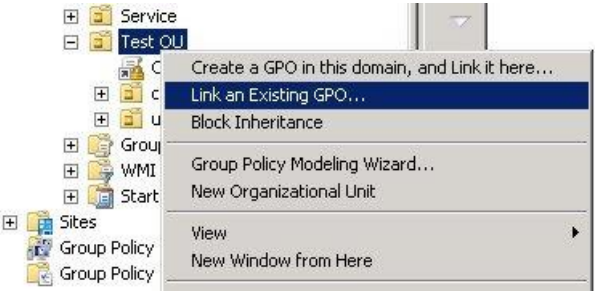


Selezionare la nuova GPO da *Group Policy Object* e cliccare su Add in modo da assegnare la policy al gruppo precedentemente creato.

Specificare quindi il gruppo AD *L-Group-NoInternet* e cliccare su OK.



Infine assegnare la GPO all'OU desiderata tramite la voce Link an Existing GPO.



A questo punto non rimane che assegnare gli utenti a cui si vuole bloccare l'accesso a Internet al gruppo *L-Group-NoInternet*. I membri appartenenti a questo gruppo non saranno più in grado di accedere ad Internet.

Configurare il servizio SNMP in Windows 2008 R2

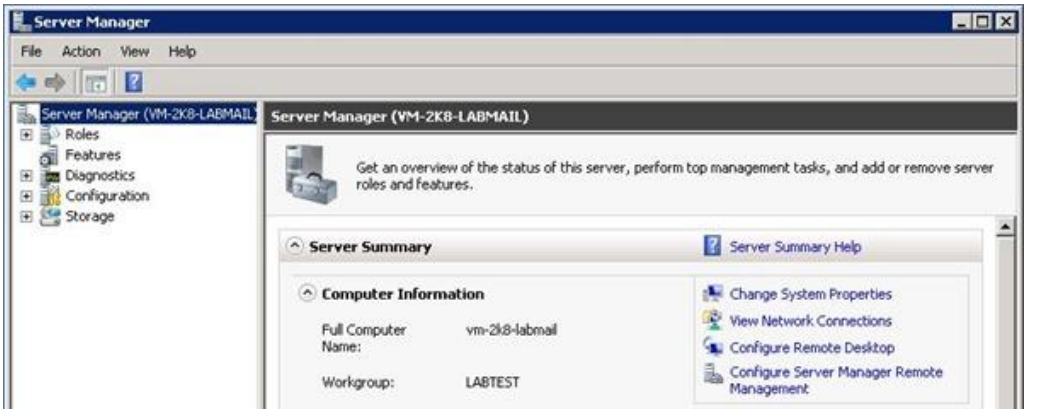
Il servizio SNMP (Simple Network Management Protocol) è un protocollo utilizzato per gestire i vari device (router, switch, server, etc.) su reti IP.

E' utilizzato principalmente in sistemi di monitoraggio dei sistemi (*Nagios* ad esempio).

Anche i server Windows possono essere monitorati tramite il servizio SNMP che però deve essere prima installato e configurato per poter essere utilizzato.

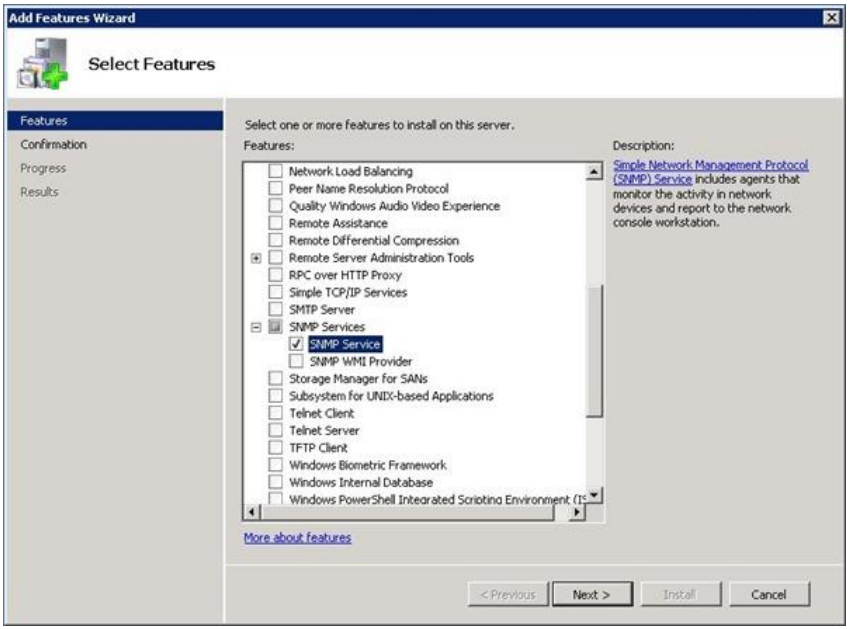
Procedura

L'installazione del servizio avviene tramite l'utility Server Manager.

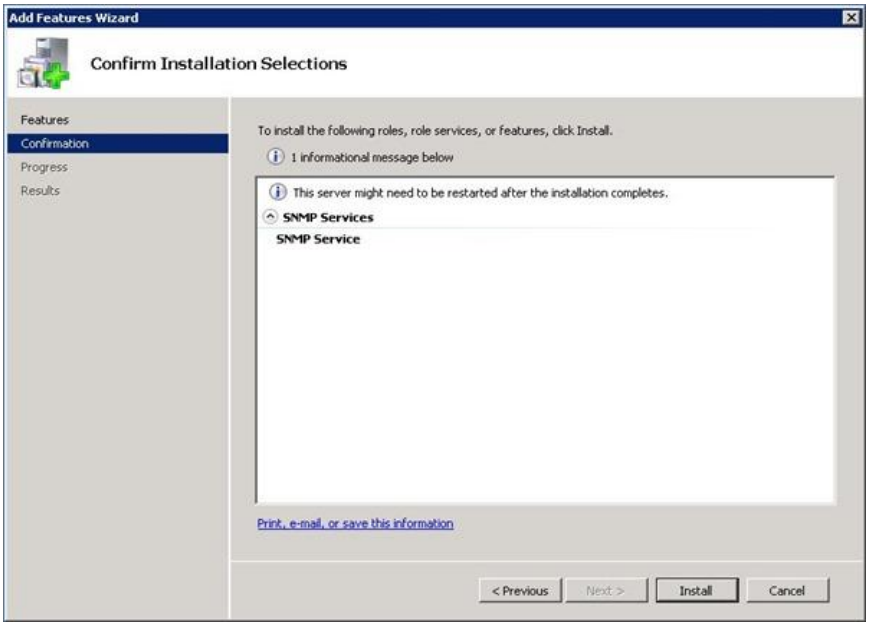


Analizzando la sezione Features Summary, non sono presenti servizi installati.

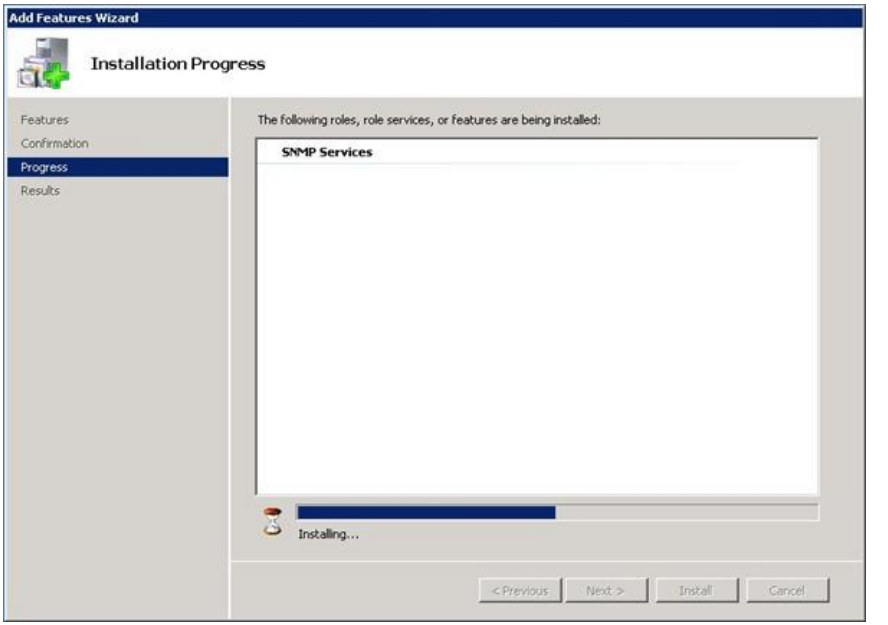
Espandere la voce SNMP Services e selezionare l'opzione SNMP Service. Click su Next.



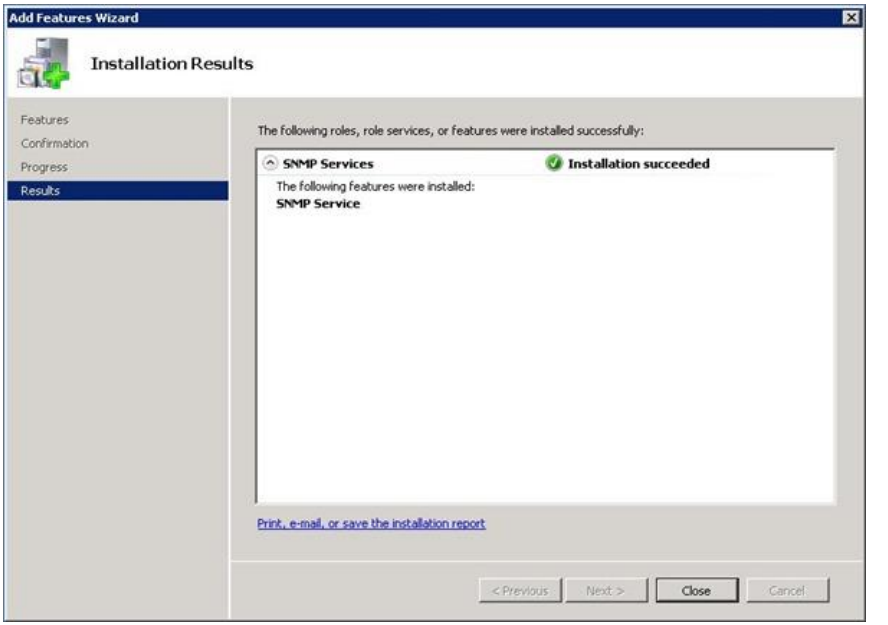
Cliccare su Install per Iniziare l'installazione del servizio.



L'installazione del servizio SNMP inizia.

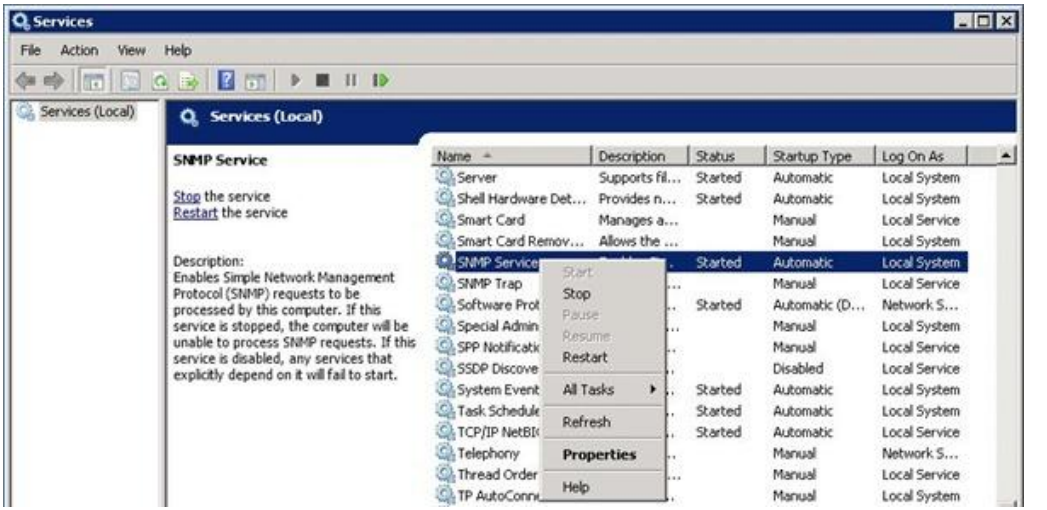


Terminata la procedura viene visualizzata una finestra riepilogativa dei servizi installati.

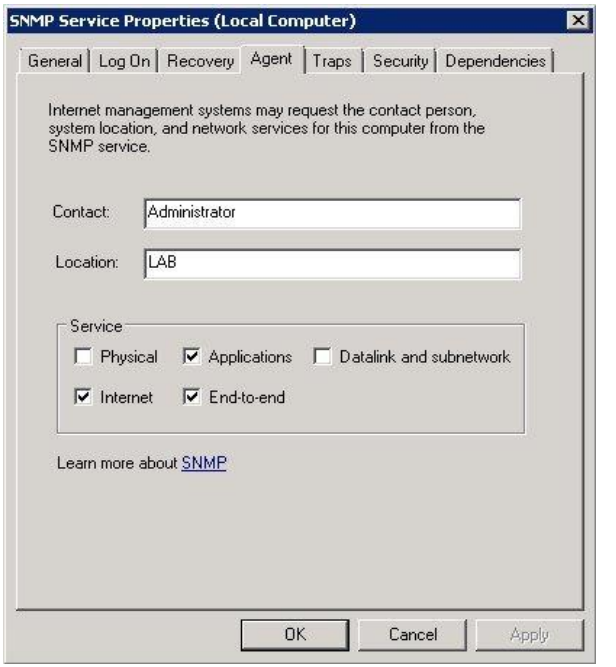


Verificando nuovamente la sezione Features Summary, compare il servizio SNMP appena installato.

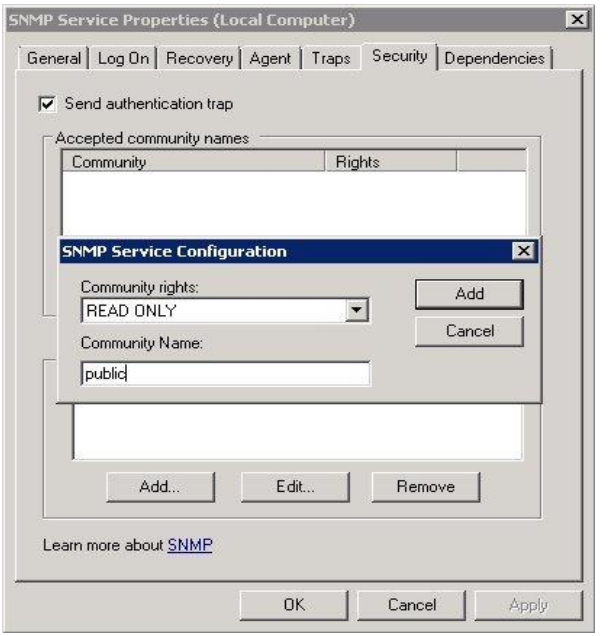
Per accedere alla configurazione del servizio SNMP, cliccare Start -> Administrative Tools -> Services. Cliccare con il tasto destro del mouse sulla voce SNMP Service e selezionare Properties.



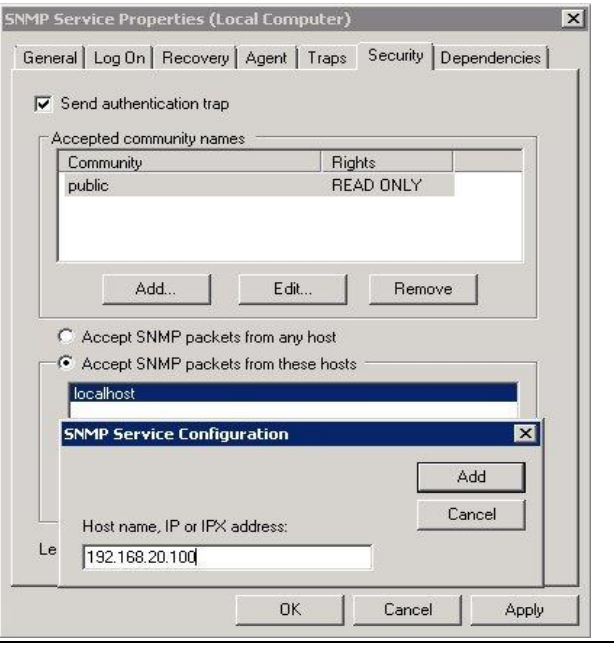
Selezionare la tab Agent, impostare i parametri richiesti.



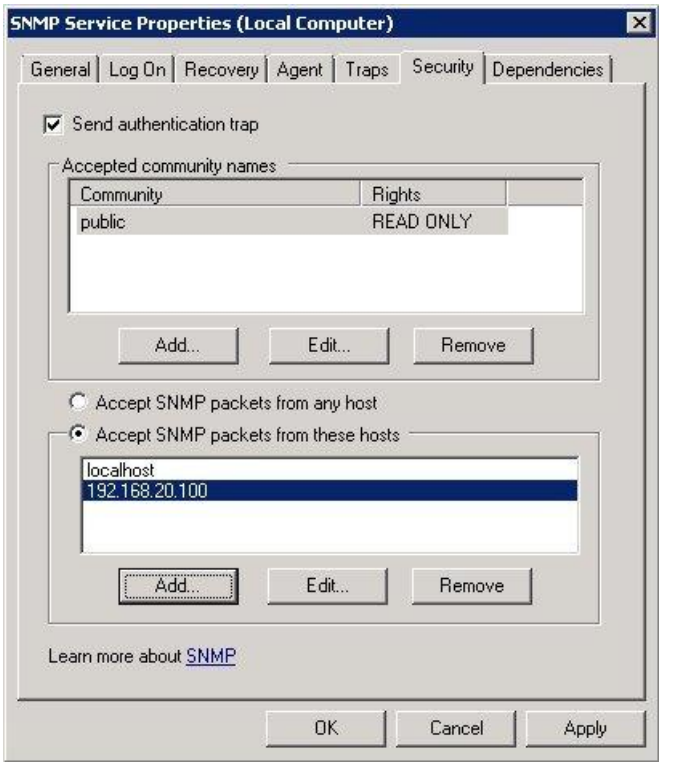
Selezionare la tab Security e cliccare il bottone Add della sezione Accepted community names. Specificare il nome nel campo Community Name e cliccare Add.



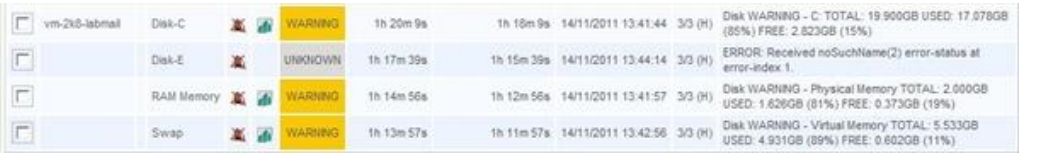
Cliccare sul bottone Add della sezione Accept SNMP packets from these hosts. Impostare l'IP o l'host name del server di monitoraggio in uso e cliccare su Add.



Terminato l'inserimento dei parametri, selezionare l'host specificato per il monitoraggio e cliccare su OK.



Accedendo al sistema di monitoraggio, è possibile vedere lo stato del server utilizzando il protocollo SNMP.



Configurando i parametri più significativi del server, il sistema di monitoraggio permette di avere sotto controllo lo stato del server utile a facilitare l'intervento in caso di necessità.

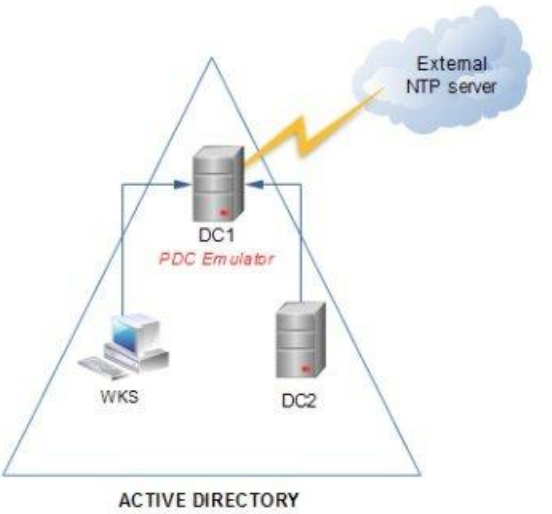
L'importanza di avere tutti i sistemi sincronizzati con la stessa ora è fondamentale per il corretto funzionamento di una rete basata su Active Directory. La sicurezza delle autenticazioni, che avvengono tramite il protocollo kerberos, si affida al *time stamps* della richiesta effettuata dai *client*.

Il non tener conto di questo aspetto può portare a molti problemi di autenticazione poichè se il discostamento degli orologi tra il client e KDC è oltre la soglia di tolleranza, l'autenticazione semplicemente viene rifiutata. E' quindi molto importante fare in modo che all'interno della rete i vari sistemi abbiano tutti la stessa data e ora.

Fortunatamente Windows Server 2008 viene incontro a questa esigenza tramite Windows Time Service (W32Time) che è un servizio con il compito di mantenere gli orologi sincronizzati nei computer della rete utilizzando il protocollo SNTP.

PDC come server NTP

In una topologia di rete basata su Active Directory, W32Time sincronizza gli orologi della *forest* utilizzando una relazione gerarchica che inizia dal PDC Emulator nella *root domain* della forest, considerato per la *AD forest* lo stratum 2 del *time source*.



Se il PDC è sincronizzato tramite un *Internet time server* o un *orologio atomico*, questi ultimi sono considerati nella gerarchia W32Time stratum 1 del *time source*.

Quindi il computer che deve essere configurato come NTP server in Active Directory deve essere il domain controller che ricopre il ruolo di PDC Emulator.

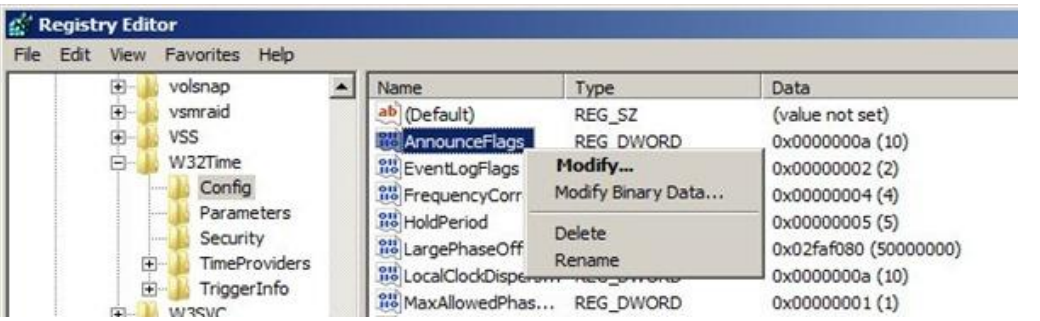
Configurazione del server

La configurazione viene fatta direttamente nel registry di Windows tramite il *Registry Editor*.

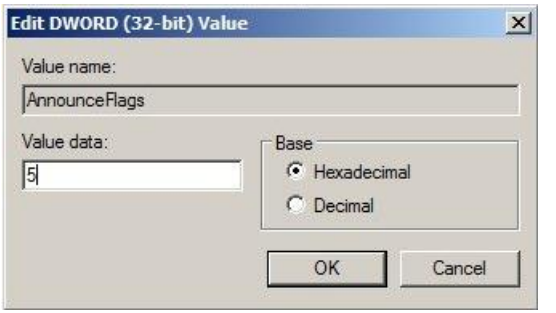
Una volta avviato il Registry Editor tramite il comando *regedit*, identificare la voce di registro:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Config
```

Cliccare con il tasto destro del mouse la voce AnnounceFlags e quindi Modify.



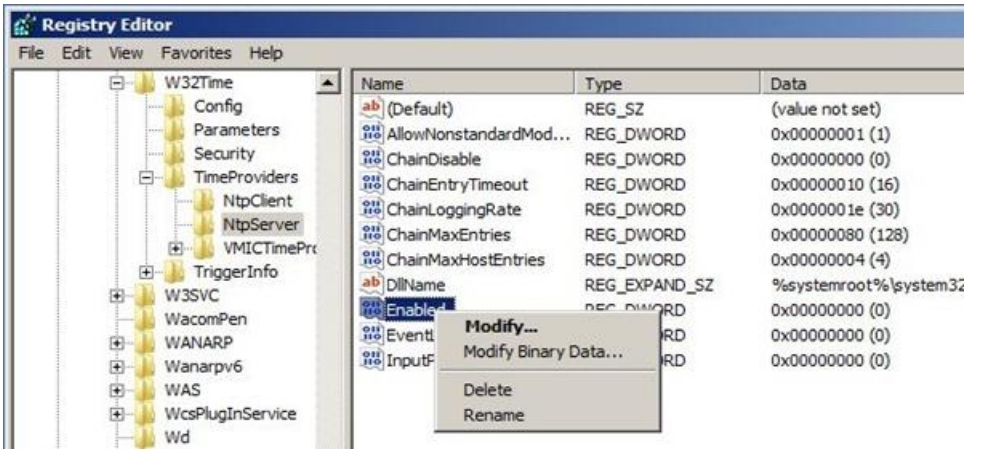
Nel campo Value data digitare 5 e successivamente click su OK.



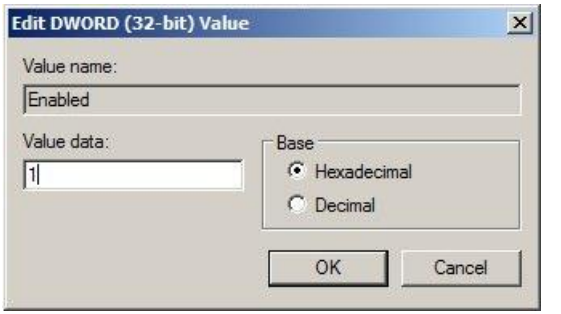
Per abilitare il server NTP, posizionarsi sulla voce di registro:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\
TimeProviders\ NtpServer
```

Cliccare con il tasto destro del mouse la voce Enabled e quindi Modify.



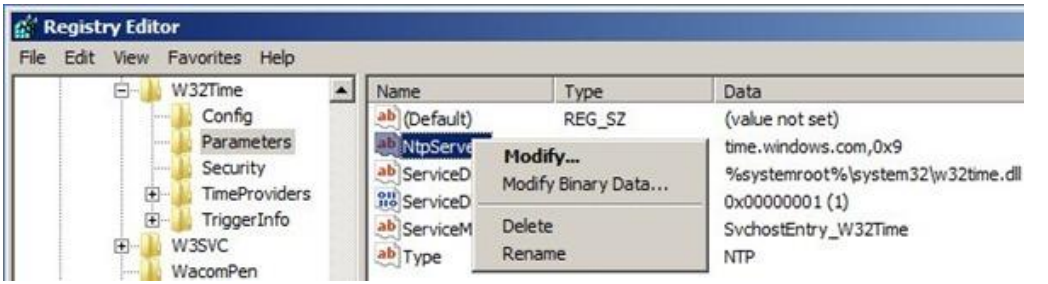
Nel campo Value data digitare 1 e successivamente OK.



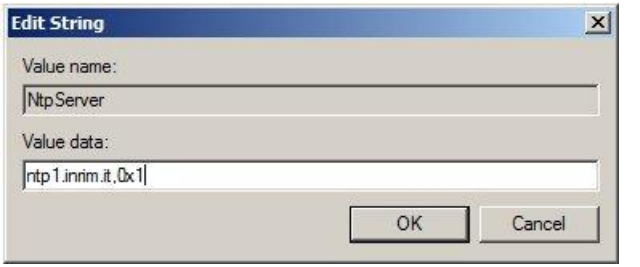
Per impostare con quali server NTP esterni il nostro sistema deve sincronizzarsi, selezionare la voce di registro:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Parameters

Cliccare con il tasto destro del mouse la voce NtpServer e quindi Modify.

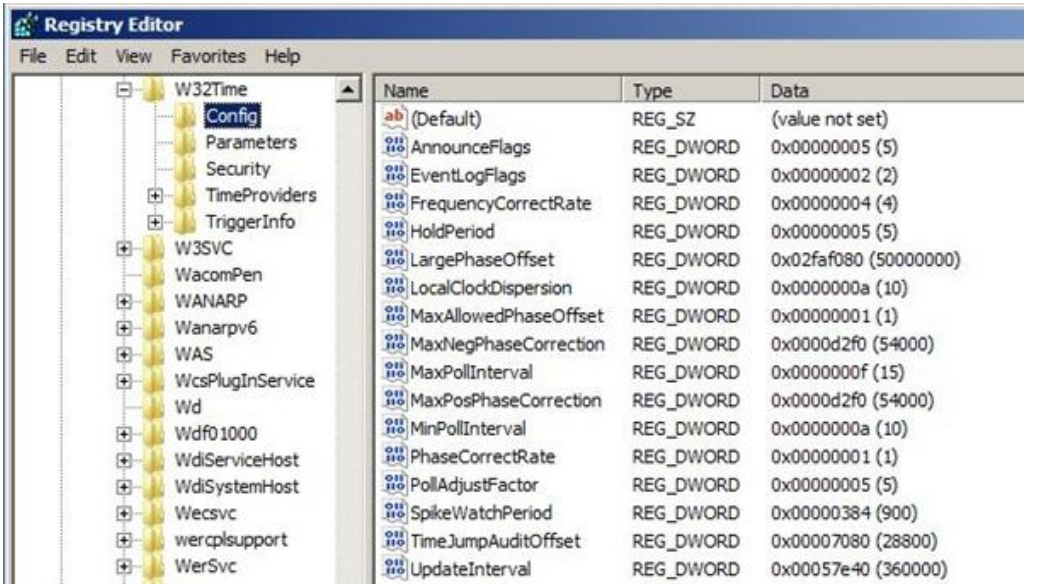


Nel campo Value data impostare il *DNS name* del/i server NTP con i quali effettuare la sincronizzazione seguiti da ,0×1 per ogni valore DNS impostato. Cliccare poi OK.



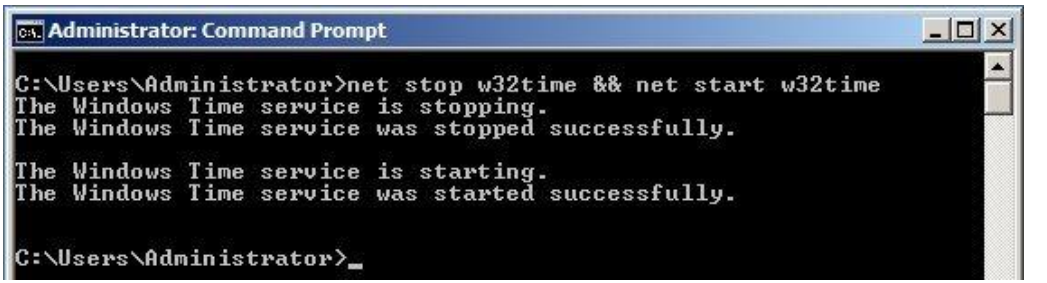
Per impostare il valore di time correction o modificare i parametri di default secondo le proprie esigenze, posizionarsi nella chiave di registro:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Config

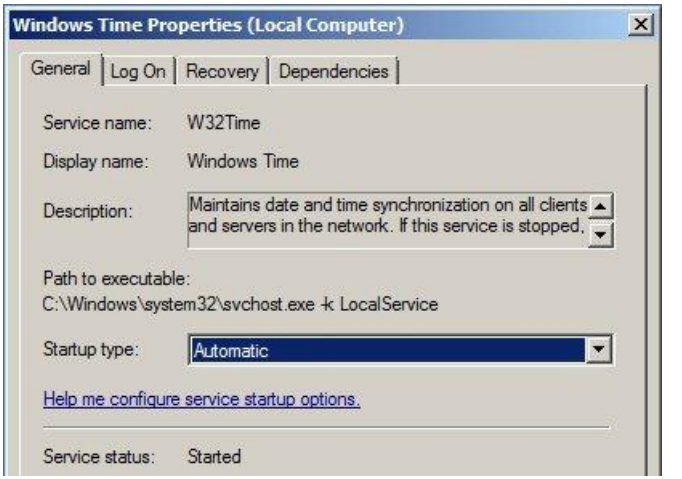


Dopo aver chiuso il *Registry Editor*, l'ultima operazione da effettuare è il riavvio del servizio W32Time dal *Command Prompt* tramite il comando seguente:

```
net stop w32time && net start w32time
```



Per fare in modo di avviare il servizio ad ogni reboot del server, impostare lo Startup type del servizio W32Time in Automatic.



Poichè il servizio utilizza la porta UDP 123 per il suo funzionamento, è necessario aprire la porta nel firewall di Windows.

Configurazione dei client e test del servizio

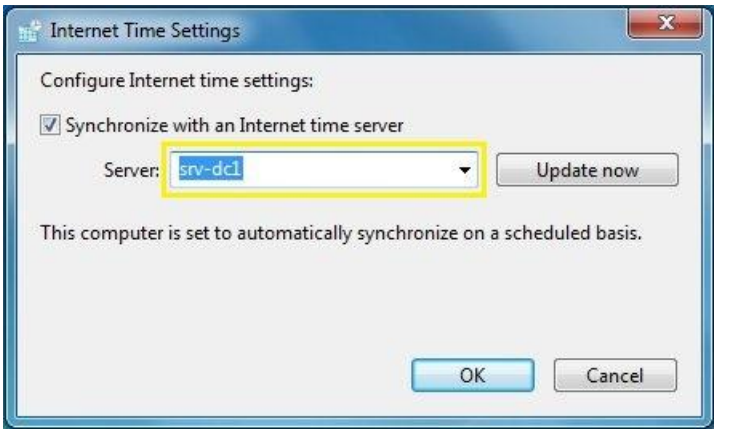
Utilizzando Windows Time (W32Time) service come server NTP è possibile sincronizzare sia client Windows che non-Windows.

Windows 7

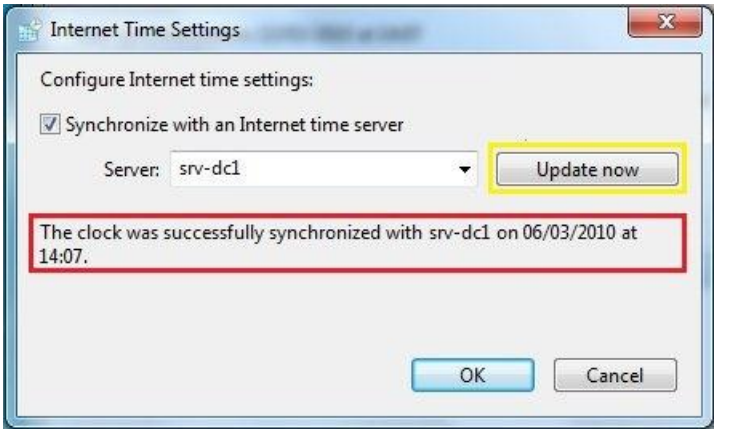
Effettuare un click con il tasto destro sull'orologio in basso a destra del desktop e selezionare Adjust date/time.

All'apertura della finestra, selezionare la voce Internet Time e cliccare sul bottone Change Settings…

Digitare il *DNS name* del server NTP appena impostato (srv-dc1 nell'esempio).



Per effettuare la sincronizzazione manuale cliccare sul bottone Update Now.



Linux

Installare il *daemon ntpd*, renderlo attivo all'avvio del computer ed editare il file di configurazione */etc/ntpd.conf* per impostare il nuovo server NTP di riferimento (srv-dc1 nell'esempio):

```
# yum install ntp
# chkconfig ntpd on
# vi /etc/ntpd.conf
```

```
# Use public servers from the pool.ntp.org project.
# Please consider joining the pool (http://www.pool.ntp.org/join.html).
server srv-dc1
#server 0.centos.pool.ntp.org
#server 1.centos.pool.ntp.org
#server 2.centos.pool.ntp.org
```

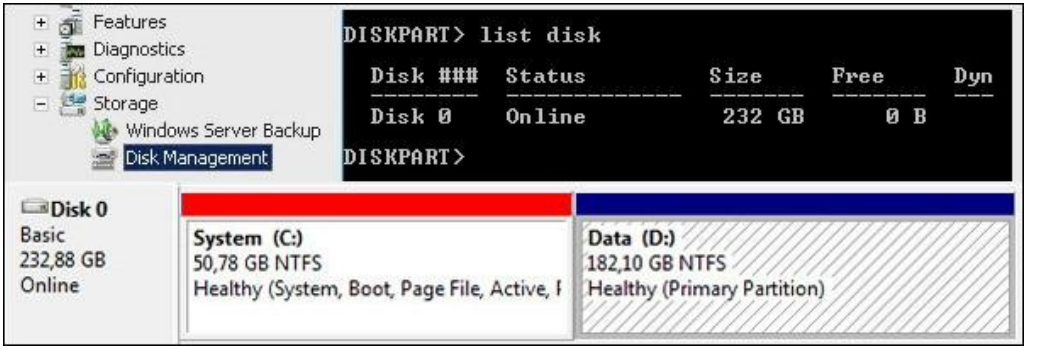
Per testare la sincronizzazione sul client Linux è sufficiente fermare il servizio *ntpd* ed utilizzare il comando *ntpdate*:

```
# service ntpd stop
# ntpdate srv-dc1
```

```
[root@wordpress /]# ntpdate srv-dc1
 8 Mar 09:51:47 ntpdate[6985]: adjust time server 172.16.20.5 offset -0.420902 s
ec
[root@wordpress /]#
```

A questo punto tutti i sistemi possono essere sincronizzati con il nuovo server NTP appena configurato scongiurando potenziali problemi dovuti all'autenticazione in Kerberos.

Estendere la partizione con diskpart in VMware vSphere



Lavorando in ambiente virtuale VMware vSphere (ma il concetto è valido anche per altri sistemi), la gestione delle risorse implica l'applicazione di alcuni criteri specialmente nella configurazione dello spazio disco destinato alle virtual macine.

Assegnare, ad esempio, un disco da 50 GB ad un server che ne utilizza a regime solo 10 GB, è evidente che questo comporta uno spreco di spazio nello storage che potrebbe rivelarsi critico man mano che il numero di virtual machine cresce. Cosa molto facile quando si utilizza questa tecnologia.

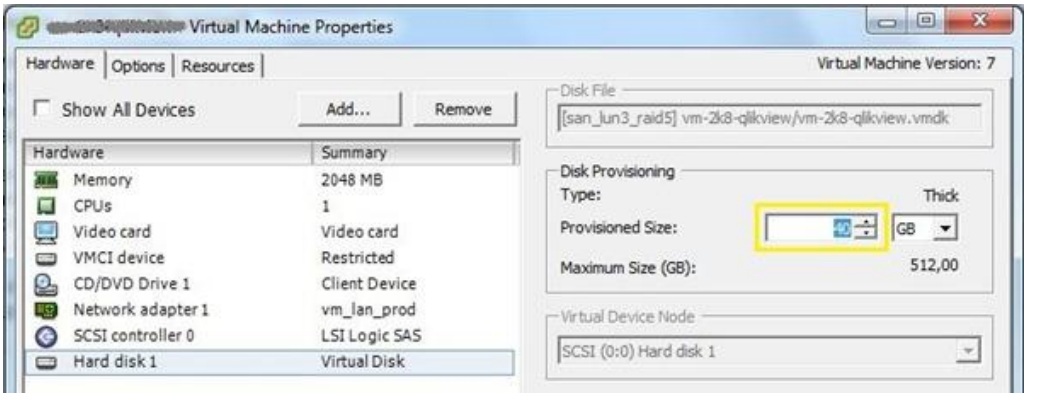
Una buona *best practise* è di allocare uno spazio minimo per le virtual machine (ad esempio per installare Windows 2008 R2, 12 GB sono sufficienti) ed espandere successivamente il disco virtuale man mano che se ne presenta la necessità. Queste operazioni sono in genere molto veloci e richiedono pochi click.

Estendere il disco virtuale

Tramite *vSphere Client* collegarsi al vCenter Server per accedere alla gestione delle virtual machine presenti nell'*inventory*.

Selezionare la virtual machine da modificare, fare click col tasto destro del mouse e selezionare Edit Settings.

Selezionare il *virtual disk* Hard disk1 ed impostare il valore richiesto, ad esempio 40 GB.



Cliccare su OK per confermare la nuova dimensione del disco virtuale.

Estendere la partizione in Windows

L'estensione della partizione è possibile solo nel caso in cui ci sia della spazio non allocato nello stesso disco.

Da *Windows Server 2008 R2*, accedere al Command Prompt.

Come prima cosa visualizzare l'elenco dei dischi attualmente disponibili nel sistema tramite il comando list disk e selezionare il disco che si intende modificare (Disk 0 nell'esempio) tramite il comando select disk.

```
Administrator: C:\Windows\system32\cmd.exe - diskpart

C:\Users\Administrator>diskpart

Microsoft DiskPart version 6.1.7600
Copyright (C) 1999-2008 Microsoft Corporation.
On computer: VM-2K8-DC1

DISKPART> list disk

  Disk ###  Status         Size     Free     Dyn  Gpt
  --------  -------------  -------  -------  ---  ---
  Disk 0    Online           40 GB    20 GB

DISKPART> select disk 0

Disk 0 is now the selected disk.

DISKPART>
```

Prima di procedere con l'estensione della partizione è consigliato visualizzare le partizioni presenti nel disco tramite list partition per evitare di modificare una partizione sbagliata. Identificata la partizione corretta (Partition 2 nell'esempio) selezionarla tramite il comando select partition.

```
Administrator: C:\Windows\system32\cmd.exe - diskpart

DISKPART> list partition

  Partition ###  Type              Size     Offset
  -------------  ----------------  -------  -------
  Partition 1    Primary            100 MB  1024 KB
  Partition 2    Primary             19 GB   101 MB

DISKPART> select partition 2

Partition 2 is now the selected partition.

DISKPART> _
```

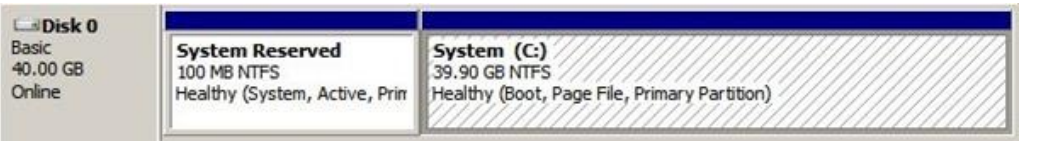
Per procedere con l'effettiva estensione, sono disponibili due opzioni per come definire lo spazio da allocare:

- extend (la partizione viene estesa utilizzando tutto lo spazio disponibile)
- extend size=xx (la partizione viene estesa di xx MB)

```
Administrator: C:\Windows\system32\cmd.exe - diskpart

DISKPART> extend

DiskPart successfully extended the volume.

DISKPART> list partition

  Partition ###  Type              Size     Offset
  -------------  ----------------  -------  -------
  Partition 1    Primary            100 MB  1024 KB
* Partition 2    Primary             39 GB   101 MB

DISKPART> _
```

Tramite list partition è ora possibile verificare il risultato dell'operazione.

Anche dalla GUI del *Disk Management*, la partizione riporta la nuova dimensione.



Tramite diskpart estendere le partizioni delle macchine Windows risulta un'operazione semplice e veloce permettendo una gestione ottimale dello spazio sullo storage presente nell'infrastruttura virtuale.

Servizi Linux

Installare un server FTP con proFTPd + proFTPd Administrator

I continui tagli di budget inflitti ai reparti IT, costringe i sistemisti ad orientare le soluzioni informatiche su prodotti che non incidano pesantemente sui costi cercando di mantenere il più alto fattore di sicurezza/prestazioni.

Un PC considerato obsoleto o poco performante con un sistema operativo Linux può essere molto utile per realizzare un buon server FTP contenendo i costi ed assicurando una certa affidabilità e sicurezza.

Utilizzando il robusto proftpd appoggiato ad un'installazione bare minimum di CentOS 5.4 è possibile implementare un server FTP molto robusto ed efficiente.

Prerequisiti

Per utilizzare proftpd e l'interfaccia web proftpd Administrator, sono richiesti quattro packages principali:

- mysql
- apache
- proftpd
- proftpd administrator

Procediamo con l'installazione dei requisiti di sistema:

```
# yum install mysql-server httpd php php-mysql mod_ssl
```

```
[root@srv-ftp install]# yum install mysql-server httpd php mod_ssl
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * addons: centos.fastbull.org
 * base: centos.bio.lmu.de
 * extras: centos.bio.lmu.de
 * updates: centos.bio.lmu.de
Setting up Install Process
Resolving Dependencies
--> Running transaction check
```

```
# chkconfig mysqld on
# chkconfig httpd on
```

Una volta installato il repository rpmforge, possiamo installare proftpd tramite il comando yum:

```
# rpm -Uvh rpmforge-release-0.3.6-1.el5.rf.i386.rpm
```

```
[root@srv-ftp install]# rpm -Uvh rpmforge-release-0.3.6-1.el5.rf.i386.rpm
warning: rpmforge-release-0.3.6-1.el5.rf.i386.rpm: Header V3 DSA signature: NOKE
Y, key ID 6b8d79e6
Preparing...                ########################################### [100%]
   1:rpmforge-release       ########################################### [100%]
[root@srv-ftp install]#
```

```
# yum install proftpd proftpd-mysql
# chkconfig proftpd on
```

Dal sito http://proftpd-adm.sourceforge.net scarichiamo l'ultima versione di proftpd Administrator e la scompattiamo. La directory sarà poi copiata nella root di Apache impostata in */etc/http/conf/httpd.conf*, nell'esempio */var/www/html/*.

```
# tar -xzvf proftpd_admin_v1.2.tar.gz
# mv proftpd_admin_v1.2 /var/www/html/ftpadmin
```

Impostazioni di mySQL

Per incrementare la sicurezza di mySQL, è opportuno impostare la password di root ed eliminare ciò che non è necessario:

```
# service mysqld start
# mysql_secure_connection
```

impostare la password di root

rimuovere l'utente anonymous

disabilitare l'accesso remoto root

rimuovere il database test

```
Remove anonymous users? [Y/n] Y
 ... Success!

Normally, root should only be allowed to connect from 'localhost'.  This
ensures that someone cannot guess at the root password from the network.

Disallow root login remotely? [Y/n] Y
 ... Success!

By default, MySQL comes with a database named 'test' that anyone can
access.  This is also intended only for testing, and should be removed
before moving into a production environment.

Remove test database and access to it? [Y/n] Y
 - Dropping test database...
 ... Success!
 - Removing privileges on test database...
 ... Success!

Reloading the privilege tables will ensure that all changes made so far
will take effect immediately.

Reload privilege tables now? [Y/n]
```

Una volta installato proftpd, bisogna impostare la password precedentemente assegnata a mySQL root editando il file della struttura del database che sarà importato in mySQL. Da */var/www/html/ftpadmin/misc/database_structure_mysql/*, editiamo le ultime tre righe del file *db_structure.sql*:

```
# cd /var/www/html/ftpadmin/misc/database_structure_mysql/
# vi db_structure.sql
```

```
INSERT INTO grouptable (gid) VALUES (9999);
DELETE FROM grouptable WHERE gid=9999;
INSERT INTO grouptable (groupname, description) VALUES ("admins", "Administrator
s");
INSERT INTO grouptable (groupname, description) VALUES ("users", "Ordinary users
");

GRANT ALL ON usertable TO proftpd@localhost IDENTIFIED BY 'newpassword';
GRANT ALL ON grouptable TO proftpd@localhost IDENTIFIED BY '<database_password>'
;
GRANT ALL ON xfer_stat TO proftpd@localhost IDENTIFIED BY '<database_password>';
```

A questo punto dalla directory */var/www/html/ftpadmin/misc/database_structure_mysql/* importiamo la struttura del database in mySQL:

```
# mysql -u root -p < db_structure.sql
```

```
[root@srv-ftp database_structure_mysql]# mysql -u root -p < db_structure.sql
Enter password:
[root@srv-ftp database_structure_mysql]#
```

Impostazioni di Apache

Configurare Apache */etc/http/conf/httpd.conf* impostando il *ServerName* ed avviare il servizio:

```
# service httpd start
```

Impostazioni di proFTPd

Prima di avviare il servizio, bisogna configurare proftpd per rispecchiare le impostazioni del sistema. Come riferimento è possibile utilizzare il file di esempio *proftpd.conf* incluso nella directory */var/www/html/ftpadmin/misc/sample_config/*.

Editare il file *proftpd.conf* e settare la stessa password impostata precedentemente in mySQL nella riga dove viene riportato:

SQLConnectInfo proftpd_admin@localhost proftpd newpassword

```
# Set up authentication via SQL
# ===========
AuthOrder               mod_sql.c
SQLAuthTypes            Backend
SQLConnectInfo          proftpd_admin@localhost proftpd newpassword
SQLUserInfo             usertable userid passwd uid gid homedir shell
SQLGroupInfo            grouptable groupname gid members
```

Verifichiamo che non ci siano errori di configurazioni in proftpd lanciando semplicemente il comando:

```
# proftpd
```

Se non viene visualizzato nessun errore, proftpd è pronto per essere avviato.

```
[root@srv-ftp /]# proftpd
[root@srv-ftp /]#
```

```
# service proftpd start
```

Impostazioni di proFTPd Administrator

Precedentemente abbiamo spostato la directory *proftpd_admin* in */var/www/html/ftpadmin*, quindi è qui che sposteremo adesso la nostra attenzione. Per poter configurare il sistema tramite l'interfaccia web e abilitare la scrittura dei log,

dobbiamo assegnare i diritti di scrittura al file *configuration.xml* e alle directory *groups* e *users* in */var/www/html/ftpadmin/logs*:

```
# cd /var/www/html/ftpadmin
# chmod o+w configuration.xml
# chmod 733 logs/*
```

Creiamo il gruppo e l'utente utilizzati dal programma:

```
# groupadd -g 1000 grouptable
# useradd -u 1000 -s /bin/false -d /bin/null -c "proftpd user" -g
grouptable usertable
```

Per come sono le impostazioni di default, creiamo la directory */ftp* nella root di sistema:

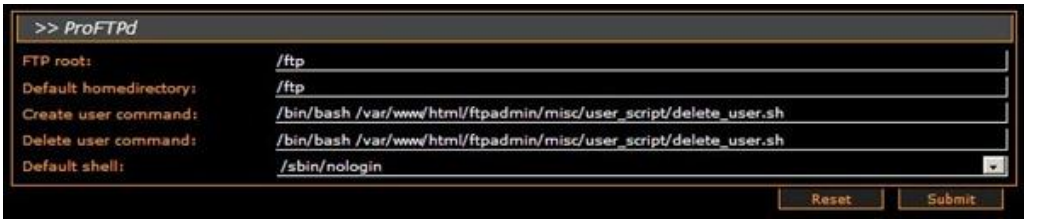
```
# mkdir /ftp
```

Per aumentare la sicurezza del sistema è consigliato creare una partizione dedicata a ftp.

Per configurare correttamente l'ambiente operativo, riavviamo il servizio httpd e richiamiamo dal browser l'interfaccia web di proftpd Administrator tramite *http://ip_address/ftpadmin/configure.php*. Per configurare correttamente i parametri di sistema, cliccare su Configure e impostare i parametri come riportato in figura:

<u>Database</u>

proFTPd



Filepath

Terminata la configurazione, richiamando dal browser l'indirizzo *http://ip_address/ftpadmin* si accede alla Main Page:

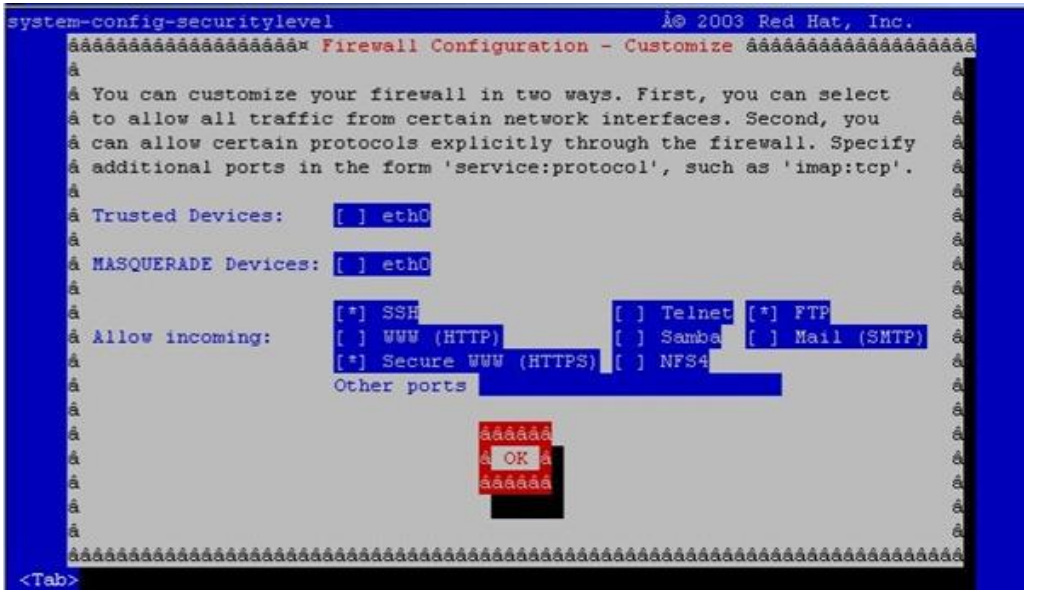
Sicurezza

Poichè presumibilmente il server FTP sarà messo in DMZ, è necessario impostare determinati parametri di sicurezza per garantirne una certa affidabilità contro eventuali tentativi di intrusione.

Tramite il comando *system-config-securitylevel-tui* impostare il firewall come attivo lasciando passare solo i servizi necessari:

- ssh
- ftp
- https

```
# system-config-securitylevel-tui
```



Con l'installazione del modulo *mod_ssl* di Apache, utilizzeremo il protocollo SSL per accedere all'interfaccia web tramite l'indirizzo https://ip_address/ftpadmin.

Non ci resta poi che definire gli utenti con le home directory operative e il server FTP, dopo averlo testato per qualche giorno, è pronto per essere messo in produzione.

Installare un server FTP con vsftpd su CentOS

Per un'azienda e non solo, la condivisione di dati e file di medio/grosse dimensioni (grafica, presentazioni, media, etc.) è una necessità sempre più presente nel business svolto.

Anche se gli utenti si ostinano ad inviare grossi file via email fino a saturare il loro inbox o vedersi respingere il messaggio dal destinatario (per questo gli amministratori mettono le quote sulle caselle!), l'utilizzo di un servizio FTP è spesso la soluzione del problema.

Tra le varie proposte del mercato, uno dei più quotati sistemi FTP in ambiente *Linux* è vsftpd.

Prerequisiti

Per implementare il server FTP, sono richiesti i seguenti componenti:

- Linux CentOS 5.x
- Package vsftpd

Consigliata la creazione di una partizione dedicata home per le home directory

Procedura

Data la tipologia del servizio da implementare, effettuare un'installazione tipo "bare minimum" di *Linux CentOS 5.x*.

Successivamente installare il package vsftpd tramite il comando *yum*.

```
# yum install vsftpd
```

```
================================================================================
Installing:
 vsftpd          i386          2.0.5-16.el5_6.1          updates          141 k

Transaction Summary
================================================================================
Install       1 Package(s)
Upgrade       0 Package(s)

Total download size: 141 k
Is this ok [y/N]: y
Downloading Packages:
vsftpd-2.0.5-16.el5_6.1.i386.rpm                        | 141 kB     00:00
Running rpm_check_debug
Running Transaction Test
Finished Transaction Test
Transaction Test Succeeded
Running Transaction
  Installing     : vsftpd                                                   1/1

Installed:
  vsftpd.i386 0:2.0.5-16.el5_6.1

Complete!
```

Terminata l'installazione, la configurazione risiede nel file */etc/vsftpd/vsftpd.conf*. Per avviare il servizio durante il reboot della macchina, impostare il parametro tramite *chkconfig*.

```
# chkconfig vsftpd on
```

```
[root@FTP ~]# chkconfig vsftpd on
[root@FTP ~]#
```

Nel firewall bisogna aprire la porta TCP 21 per permettere il corretto funzionamento dell'FTP. Utilizzando il comando *system-config-securitylevel-tui* si accede alla configurazione base del firewall.

```
# system-config-securitylevel-tui
```

Abilitare il firewall cliccando nel campo Security Level il parametro Enabled, disabilitare SELinux e cliccare sul bottone Customize.

```
Firewall Configuration

A firewall protects against unauthorized
network intrusions. Enabling a firewall blocks
all incoming connections. Disabling a firewall
allows all connections and is not recommended.

Security Level: (*) Enabled ( ) Disabled

SELinux: Enforcing
         Permissive
         Disabled

OK        Customize        Cancel
```

Nel campo Allow incoming cliccare sulla voce FTP (abilita la porta TCP 21). Lasciare SSH attivo per la connessione remota sulla macchina. Cliccare su OK per impostare.

```
Firewall Configuration - Customize

You can customize your firewall in two ways. First, you can select
to allow all traffic from certain network interfaces. Second, you
can allow certain protocols explicitly through the firewall. Specify
additional ports in the form 'service:protocol', such as 'imap:tcp'.

Trusted Devices:     [ ] eth0  [ ] eth0.bak

MASQUERADE Devices:  [ ] eth0  [ ] eth0.bak

                     [*] SSH                 [ ] Telnet  [*] FTP
Allow incoming:      [ ] WWW (HTTP)          [ ] Samba   [ ] Mail (SMTP)
                     [ ] Secure WWW (HTTPS)  [ ] NFS4
                     Other ports

                                 OK
```

Si ripresenta la finestra precedente. Cliccare sul bottone OK per attivare il firewall.

```
[root@FTP ~]# system-config-securitylevel-tui
/usr/sbin/setenforce: SELinux is disabled
[root@FTP ~]#
```

Editare il file di configurazione *vsftpd.conf* per impostare i parametri di funzionamento.

```
# vi /etc/vsftpd/vsftpd.conf
```

Rimuovere dal file di configurazione il simbolo # dalle varie voci per abilitare le specifiche funzioni.

Per permettere la scrittura, il listing delle directory e assegnare i diritti di read & write alle directory:

local_enable=YES
write_enable=YES
local_umask=022

Per abilitare il chroot degli utenti su determinate directory:

chroot_list_enable=YES
chroot_list_file=/etc/vsftpd/chroot_list

Creare il file */etc/vsftpd/chroot_list* per inserire la lista degli utenti che dovranno essere "jailed" nella loro home directory.

```
# vi /etc/vsftpd/chroot_list
```

```
ftptest
```

Una configurazione tipo di *vsftpd* può essere impostata come riportato in figura.

```
#--------------------------------------------------------------
# VSFTPD configuration file
#--------------------------------------------------------------
anonymous_enable=NO
local_enable=YES
write_enable=YES
local_umask=022
dirmessage_enable=YES

xferlog_enable=YES
xferlog_file=/var/log/xferlog
xferlog_std_format=YES

idle_session_timeout=600
data_connection_timeout=120

ascii_upload_enable=YES
ascii_download_enable=YES
ftpd_banner=Welcome to FTP service.

chroot_list_enable=YES
chroot_list_file=/etc/vsftpd/chroot_list

listen=YES
pam_service_name=vsftpd
userlist_enable=YES
tcp_wrappers=YES
```

Configurato il servizio, non rimane che creare nel sistema gli utenti che utilizzeranno l'*FTP*.

```
[root@FTP ~]# useradd ftptest
[root@FTP ~]# passwd ftptest
Changing password for user ftptest.
New UNIX password:
Retype new UNIX password:
passwd: all authentication tokens updated successfully.
[root@FTP ~]#
```

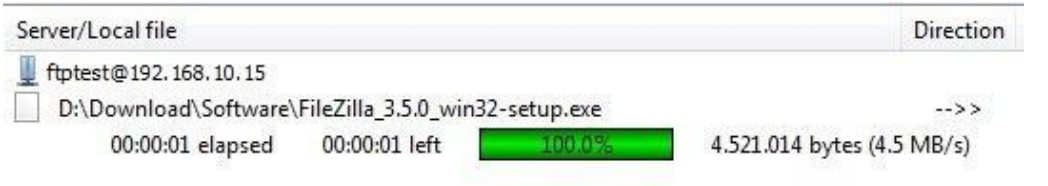
Per rendere operativa la configurazione, riavviare il daemon *vsftpd*.

```
# service vsftpd restart
```

```
[root@wordpress /]# service vsftpd restart
Shutting down vsftpd:                                      [  OK  ]
Starting vsftpd for vsftpd:                                [  OK  ]
[root@wordpress /]#
```

Test del servizio

Per verificare che il tutto funzioni correttamente, utilizzare un client FTP per testare la connessione e provare ad effettuare l'upload di un file.



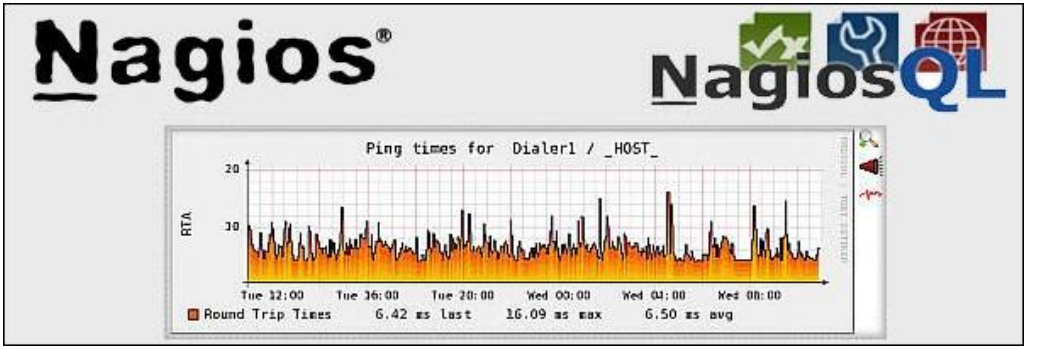
Utilizzando *Internet Explorer* (mezzo utilizzato da molte aziende), connettersi al server FTP ed effettuare il download del file. Digitando l'indirizzo del server FTP, si presenta la finestra di autenticazione. Inserire le credenziali (nell'esempio ftptest) e cliccare su Log on.

Si accede all'area FTP dell'utente (ftptest in questo caso) dove è presente il file precedentemente caricato. Come si nota, l'utente non ha modo di "uscire" dalla propria directory poichè è soggetto a chroot dal sistema.

Il server FTP è adesso operativo e pronto per essere messo in produzione. Generalmente, dato l'utilizzo, è consigliabile posizionare il server FTP nell'area DMZ della rete, configurando opportunamente il firewall.

Monitoraggio rete

Installare Nagios + NagiosQL su CentOS



Il dover controllare quotidianamente che tutti i sistemi siano perfettamente operativi è uno dei compiti più importanti per un sistemista. Il trascurare un'anomalia può portare a dei risvolti a volte drammatici… morto un disco del server in RAID5, il sistema continua a funzionare ma ovviamente il disco deve essere sostituito al più presto per evitare problemi. Ma se non verifichiamo lo stato degli array dei nostri server… cosa succede se oltre al primo, anche un secondo disco del RAID smette di funzionare?… vi consiglio di non sfidare la sorte…

In reti piccole o con pochi apparati, il controllo periodico si può fare "manualmente" ma se la rete presenta un numero importante di dispositivi "in produzione", è opportuno utilizzare un qualche sistema di controllo automatico.

Uno strumento molto funzionale è Nagios, un software con licenza GNU (General Public Licence) che permette il monitoraggio completo della rete.

Essendo uno strumento non semplicissimo come setup, sono nati alcuni tool per rendere la sua configurazione un po' più accessibile… uno di questi è NagiosQL, un'interfaccia web che facilita l'impostazione dei parametri di *Nagios*.

Host	Service	Status	Last Check	Duration	Attempt	Status Information
	FTP	OK	10-13-2008 20:48:06	0d 2h 39m 13s	1/3	FTP OK - 0.098 second response time on port 21 [220 (vsFTPd 2.0.5)]
	ICMP	OK	10-13-2008 20:48:30	0d 2h 38m 49s	1/3	PING OK - Packet loss = 0%, RTA = 48.49 ms
	SMTP	OK	10-13-2008 20:48:55	4d 4h 5m 27s	1/3	SMTP OK - 0.023 sec. response time
	SSH	OK	10-13-2008 20:49:19	0d 2h 38m 0s	1/4	SSH OK - OpenSSH_4.3 (protocol 2.0)
	cpu_load	OK	10-13-2008 20:49:43	0d 2h 37m 36s	1/3	OK - load average: 0.01, 0.01, 0.00
	current_users	OK	10-13-2008 20:50:08	0d 2h 37m 11s	1/3	USERS OK - 1 users currently logged in
	disk_mount_-	OK	10-13-2008 20:50:32	0d 2h 36m 47s	1/3	DISK OK - free space: / 202868 MB (97% inode=99%):
	swap_usage	OK	10-13-2008 20:50:57	0d 2h 36m 22s	1/3	SWAP OK - 100% free (1983 MB out of 1983 MB)
	total_processes	OK	10-13-2008 20:51:21	0d 2h 35m 58s	1/3	PROCS OK: 123 processes
	zombie_processes	OK	10-13-2008 20:51:45	0d 2h 35m 34s	1/3	PROCS OK: 1 process with STATE = Z
[illegible]	FTP	OK	10-13-2008 20:52:10	0d 2h 35m 9s	1/3	FTP OK - 0.046 second response time on port 21 [220 (vsFTPd 2.0.5)]
	ICMP	OK	10-13-2008 20:47:34	0d 2h 34m 45s	1/3	PING OK - Packet loss = 0%, RTA = 20.85 ms
	NTP	OK	10-13-2008 20:47:59	0d 2h 34m 20s	1/3	NTP OK: Offset -0.003712913778 secs

Poichè l'installazione è un po' lunga, ricordarsi tutti i passaggi necessari per il corretto funzionamento del sistema potrebbe non essere immediato. Di seguito viene riportata la procedura adottata per l'installazione del sistema utilizzando come OS Linux CentOS 5.3.

Aggiornamento del sistema

Prima di procedere con l'installazione di Nagios, verifichiamo di avere il nostro Linux aggiornato tramite il comando *yum*.

```
# yum update
```

Aggiunta del repository RPMFORGE

RPMForge è una collaborazione dei più noti packagers (Dag, Dries, etc.) che implementano i moduli rpm delle più note distribuzioni Linux. L'aggiunta di questo repository, ci permette di effettuare l'installazione di Nagios tramite yum.

Verifichiamo innanzitutto quale sia l'ultima release di *rpmforge-release* all'indirizzo http://dag.wieers.com/rpm/packages/rpmforge-release/ e poi procediamo con la sua installazione.

In una cartella precedentemente creata (*/install* nell'esempio), scaricare l'ultima versione:

```
# wget http://dag.wieers.com/packages/rpmforge-release/rpmforge-
release-0.3.6-1.el5.rf.i386.rpm
```

```
Resolving dag.wieers.com... 62.213.193.164
Connecting to dag.wieers.com|62.213.193.164|:80... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: http://dag.wieers.com/rpm/packages/rpmforge-release/rpmforge-release-0
.3.6-1.el5.rf.i386.rpm [following]
--18:43:59--  http://dag.wieers.com/rpm/packages/rpmforge-release/rpmforge-relea
se-0.3.6-1.el5.rf.i386.rpm
Reusing existing connection to dag.wieers.com:80.
HTTP request sent, awaiting response... 302 Found
Location: http://rpmforge.sw.be/redhat/el5/en/i386/rpmforge/RPMS/rpmforge-releas
e-0.3.6-1.el5.rf.i386.rpm [following]
--18:43:59--  http://rpmforge.sw.be/redhat/el5/en/i386/rpmforge/RPMS/rpmforge-re
lease-0.3.6-1.el5.rf.i386.rpm
Resolving rpmforge.sw.be... 130.133.35.16
Connecting to rpmforge.sw.be|130.133.35.16|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 16698 (16K) [application/x-rpm]
Saving to: `rpmforge-release-0.3.6-1.el5.rf.i386.rpm'

100%[=====================================>] 16,698      --.-K/s   in 0.1s

18:44:00 (125 KB/s) - `rpmforge-release-0.3.6-1.el5.rf.i386.rpm' saved [16698/16
698]

[root@monitor install]# _
```

Installare il modulo rpm appena scaricato:

```
# rpm -Uvh rpmforge-release-0.3.6-1.el5.rf.i386.rpm
```

```
[root@monitor install]# rpm -Uvh rpmforge-release-0.3.6-1.el5.rf.i386.rpm
warning: rpmforge-release-0.3.6-1.el5.rf.i386.rpm: Header V3 DSA signature: NOKE
Y, key ID 6b8d79e6
Preparing...                ########################################### [100%]
   1:rpmforge-release       ########################################### [100%]
[root@monitor install]# _
```

Installazione componenti richiesti da Nagios e NagiosQL

I componenti richiesti per il corretto funzionamento sono Linux Apache + MySQL + PHP (acronimo LAMP) che vengono installati tramite il comando *yum.*

```
# yum install httpd mod_ssl php mysql mysql-server php-mysql php-pear
```

Attivare i servizi:

```
# chkconfig httpd on
# service httpd start
# chkconfig mysqld on
# service mysqld start
```

Installazione di Nagios

Installare i componenti di Nagios richiesti per il suo funzionamento:

```
# yum install nagios nagios-devel nagios-plugins nagios-plugins-nrpe
```

```
Installed: nagios.i386 0:3.0.6-1.el5.rf nagios-devel.i386 0:3.0.6-1.el5.rf nagio
s-plugins.i386 0:1.4.13-1.el5.rf nagios-plugins-nrpe.i386 0:2.12-1.el5.rf
Dependency Installed: fping.i386 0:2.4-1.b2.2.el5.rf gd.i386 0:2.0.33-9.4.el5_1.
1 libXpm.i386 0:3.5.5-3 libtool-ltdl.i386 0:1.5.22-6.1 perl-Crypt-DES.i386 0:2.0
5-3.2.el5.rf perl-Digest-HMAC.noarch 0:1.01-15 perl-Digest-SHA1.i386 0:2.12-1.el
5.rf perl-Net-SNMP.noarch 0:5.2.0-1.2.el5.rf perl-Socket6.i386 0:0.23-1.el5.rf p
kgconfig.i386 1:0.21-2.el5
Complete!
[root@monitor install]# _
```

Una volta installato, i componenti di Nagios risiedono nelle seguenti directory:

- cfg files: /etc/nagios
- web interface files: /usr/share/nagios
- log files: /var/log
- CGI files: /usr/lib/nagios/cgi
- plugins: /usr/lib/nagios/plugins

Per l'utilizzo di plugin che utilizzano il protocollo SNMP (tipo *check_hpjd*), è necessario installare ed abilitare il daemon net-snmp:

```
# yum install net-snmp net-snmp-utils
# chkconfig snmpd on
# service snmpd start
```

Configurazione di Apache

Modificare il file di configurazione di Apache impostando come *ServerName* il nome dell'host, supponiamo "*monitor*".

```
# vi /etc/httpd/config/httpd.conf
```

```
### Section 2: 'Main' server configuration

ServerAdmin root@localhost
ServerName monitor_
```

Impostare successivamente la password per accedere a Nagios.

```
# htpasswd -bcm /etc/nagios/htpasswd.users nagiosadmin password
```

```
[root@monitor install]# htpasswd -bcm /etc/nagios/htpasswd.users nagiosadmin pas
sword
Adding password for user nagiosadmin
[root@monitor install]# _
```

Digitare dal browser l'indirizzo http://IP_Address_Nagios per verificare che la pagina sia visualizzata.

Installazione componenti NagiosQL

I componenti richiesti da NagiosQL sono i seguenti:

- Webserver (Apache 1.x o superiore)
- PHP 5 o superiore
- MySQL 4.1 o superiore
- Nagios 2 o superiore
- PEAR Module: HTML_Template_IT 1.1 o superiore
- PHP Extension: mysql
- Javascript enabled nel browser

Installazione template PEAR

L'installazione del template viene effettuata con il comando *pear*:

```
# pear install HTML_Template_IT
```

```
[root@monitor install]# pear install HTML_Template_IT
WARNING: channel "pear.php.net" has updated its protocols, use "channel-update p
ear.php.net" to update
downloading HTML_Template_IT-1.2.1.tgz ...
Starting to download HTML_Template_IT-1.2.1.tgz (21,565 bytes)
........done: 21,565 bytes
install ok: channel://pear.php.net/HTML_Template_IT-1.2.1
[root@monitor install]# _
```

Installazione NagiosQL

Il file di installazione viene prelevato tramite il comando *wget* e lo copiamo nella directory di appoggio precedentemente creata (*/install*).

```
# wget
https://sourceforge.net/project/platformdownload.php?group_id=1343
90
```

```
Resolving puzzle.dl.sourceforge.net... 195.141.111.5
Connecting to puzzle.dl.sourceforge.net|195.141.111.5|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 878361 (858K) [application/x-gzip]
Saving to: `nagiosql303.tar.gz'

100%[===================================================================>] 878,361     45.5K/s   in 23s

20:28:42 (37.3 KB/s) - `nagiosql303.tar.gz' saved [878361/878361]

[root@monitor install]#
```

Scompattare e copiare i files in */var/www/html*.

```
# tar -xzvf nagiosql303.tar.gz
# cp nagiosql3/ /var/www/html/ -R
```

Directory Structure

Come riportato dal sito di NagiosQL, deve essere creata una struttura di directory come riportato nello schema:

- /etc/nagiosql
- /etc/nagiosql/hosts
- /etc/nagiosql/services
- /etc/nagiosql/backup
- /etc/nagiosql/backup/hosts
- /etc/nagiosql/backup/services

Configurazione nagios.cfg

Il file */etc/nagios/nagios.cfg* deve essere corretto per riflettere la *directory structure* appena creata.

```
# OBJECT CONFIGURATION FILE(S)
# These are the object configuration files in which you define hosts,
# host groups, contacts, contact groups, services, etc.
# You can split your object definitions across several config files
# if you wish (as shown below), or keep them all in a single config file.

# You can specify individual object config files as shown below:
#cfg_file=/etc/nagios/objects/commands.cfg
#cfg_file=/etc/nagios/objects/contacts.cfg
#cfg_file=/etc/nagios/objects/timeperiods.cfg
cfg_file=/etc/nagios/objects/templates.cfg


##################################################
# new configs by NagiosQL

cfg_file=/etc/nagiosql/contacttemplates.cfg
cfg_file=/etc/nagiosql/contactgroups.cfg
cfg_file=/etc/nagiosql/contacts.cfg
cfg_file=/etc/nagiosql/timeperiods.cfg
cfg_file=/etc/nagiosql/commands.cfg

cfg_file=/etc/nagiosql/hostgroups.cfg
cfg_file=/etc/nagiosql/servicegroups.cfg

cfg_dir=/etc/nagiosql/hosts
cfg_dir=/etc/nagiosql/services

##################################################
```

Creare i file a cui fare riferimento nel file *nagios.cfg*:

```
# touch /etc/nagiosql/contacttemplates.cfg
# touch /etc/nagiosql/contactgroups.cfg
# touch /etc/nagiosql/contacts.cfg
# touch /etc/nagiosql/timeperiods.cfg
# touch /etc/nagiosql/commands.cfg
# touch /etc/nagiosql/hostgroups.cfg
# touch /etc/nagiosql/servicegroups.cfg
```

Permessi

Per permettere a NagiosQL di leggere e scrivere i file di configurazione di Nagios, bisogna impostare i permessi di accesso.

Nagios Main Configuration Files

```
# chgrp apache /etc/nagios
# chgrp apache /etc/nagios/nagios.cfg
# chgrp apache /etc/nagios/cgi.cfg
# chmod 775 /etc/nagios
# chmod 664 /etc/nagios/nagios.cfg
# chmod 664 /etc/nagios/cgi.cfg
```

NagiosQL Configuration

```
# chmod 6755 /etc/nagiosql
# chown apache.nagios /etc/nagiosql
# chmod 6755 /etc/nagiosql/hosts
# chown apache.nagios /etc/nagiosql/hosts
# chmod 6755 /etc/nagiosql/services
# chown apache.nagios /etc/nagiosql/services
```

NagiosQL Backup Configuration

```
# chmod 6755 /etc/nagiosql/backup
# chown apache.nagios /etc/nagiosql/backup
# chmod 6755 /etc/nagiosql/backup/hosts
# chown apache.nagios /etc/nagiosql/backup/hosts
# chmod 6755 /etc/nagiosql/backup/services
# chown apache.nagios /etc/nagiosql/backup/services
```

Impostare i permessi sui file già esistenti.

```
# chmod 644 /etc/nagiosql/*.cfg
# chown apache.nagios /etc/nagiosql/*.cfg
```

Il file binario Nagios deve essere eseguibile dall'utente di Apache.

```
# chown nagios.apache /usr/bin/nagios
# chmod 750 /usr/bin/nagios
```

L'utente Apache deve poter accedere alla directory */var/www/html/nagiosql3/*.

```
# chown apache:apache /var/www/html/nagiosql3/ -R
```

L'utente Nagios deve poter scrivere il file di comando *nagios.cmd* (verificare che in */etc/nagios/nagios.cfgi* il parametro *check_external_commands* sia impostato a 1):

```
# chown nagios.apache /var/log/nagios/rw/ -R
```

Se la directory rw non esiste, crearla manualmente.

```
# chmod 750 /var/log/nagios/rw/ -R
```

Per verificare se sono necessari ulteriori permessi, eseguire il comando:

```
# nagios -v /etc/nagios/nagios.cfg
```

Creazione file ENABLE_INSTALLER

L'installatione wizard di NagiosQL richiede l'esistenza del file ENABLE_INSTALLER in */var/www/html/nagiosql3/install/*:

```
# touch /var/www/html/nagiosql3/install/ENABLE_INSTALLER
```

Configurazione di NagiosQL

Nel browser digitare l'indirizzo http://IP_Address_Nagios/nagiosql3 per accedere all'installazione guidata.

Cliccare sull'opzione *Start new installation* per procedere con la configurazione di *NagiosQL*.

Il sistema effettua un controllo sull'ambiente operativo.

Dopo aver verificato che la pagina non presenta nessun errore, specificare la password di MySQL, se precedentemente impostata, e del campo "*Initial NagiosQL Password*". Cliccare su Next.

La procedura di setup imposta la configurazione richiesta e visualizza lo stato finale nella maschera Finishing Setup.

Per procedere ulteriormente è necessario rimuovere prima il file precedentemente creato in */var/www/html/nagiosql3/install/ENABLE_INSTALLER.*

```
# rm /var/www/html/nagiosql3/install/ENABLE_INSTALLER
```

Cliccare su Finish, per completare il setup. Si presenta la pagina di login.

A questo punto l'installazione è terminata. Prima di procedere con la configurazione di Nagios, è necessario effettuare alcune modifiche alla configurazione di NagiosQL per farlo funzionare correttamente con *Linux CentOS*.

Procedere in questo modo:

- effettuare il login a NagiosQL
- andare su *Administration -> Domains*
- editare (Modify) la voce localhost

il parametro *Nagios command file* deve avere il path impostato con il seguente valore: /var/log/nagios/rw/nagios.cmd

- il parametro *Nagios binary file* deve avere il path impostato a /usr/bin/nagios
- il parametro *Nagios process file* deve avere il path impostato a /var/nagios/nagios.pid
- cliccare su Save

ricordatevi di effettuare sempre il controllo della configurazione di Nagios tramite NagiosQL per essere sicuri che non ci siano errori. Con NagiosQL si utilizza: *Tools -> Nagios Control -> Check configuration files*.

A questo punto non resta che definire hosts, printers, switches e tutto ciò che si vuole monitorare.

Troubleshooting

1. Errore “Permission Denied”

Tramite il comando *Tools -> Nagios Control -> Check configuration files*, viene visualizzato l’errore:

“*Error: Unable to write to temp_path (‘/var/nagios/spool/checkresults’) – Permission Denied*”

“*Error: Unable to write to check_result_path (‘/var/nagios/spool/checkresults’) – Permission Denied*”

E’ un semplice problema di permessi. Per il fix procedere così:

```
# chown nagios.apache /var/nagios/spool/checkresults/ -R
# chmod 774 /var/nagios/spool/checkresults/ -R
```

2. Viene visualizzato l’errore:

“*Nagios Binary found but not executable, please check permissions!*”

Per risolvere il problema:

```
# chmod +x /usr/bin/nagios
```

Inviare Nagios alerts via email con sSMTP

Sapere tempestivamente se un sistema della nostra rete ha un problema è spesso la chiave per ridurre al minimo i disservizi. Non sempre però gli occhi sono puntati sul monitor per controllare che tutto sia *up & running*, specialmente se la rete è composta da molti dispositivi.

Avere la possibilità di ricevere gli alert via email invece, permette di acquisire l'informazione in tempo reale su diversi dispositivi (pc, blackberry o telefono) senza la necessità di essere fisicamente davanti al monitor di sistema. Questo permette un intervento tempestivo prima di essere sommersi di chiamate da parte degli utenti.

Utilizzando Nagios per monitorare la rete, è utile ricevere le notifiche via email degli alert generati dal sistema al verificarsi di un particolare evento poichè Nagios non ha questa funzione implementata internamente.

Per non complicare troppo il sistema, dotare Nagios del supporto email diventa indolore se ci si affida ad un sistema come ssmtp, un package che permette di inviare in maniera molto semplice le email ad un server SMTP… in pratica effettua il forward delle email generate in automatico ad un indirizzo di posta.

Installazione

Da console procediamo in questo modo:

```
# wget http://download.fedora.redhat.com/pub/epel/5/i386/ssmtp-
2.61-11.8.el5.i386.rpm
```

```
# rpm -Uvh ssmtp-2.61-11.8.el5.i386.rpm
```

```
[root@nagios install]# rpm -Uvh ssmtp-2.61-11.8.el5.i386.rpm
warning: ssmtp-2.61-11.8.el5.i386.rpm: Header V3 DSA signature: NOKEY, key ID 2175
21f6
Preparing...                ########################################### [100%]
   1:ssmtp                  ########################################### [100%]
[root@nagios install]#
```

In CentOS il file eseguibile viene installato in */usr/sbin/*.

Una volta installato il package, bisogna editare il file di configurazione *ssmtp.conf* per impostare i parametri corretti:

```
# vi /etc/ssmtp/ssmtp.conf
```

```
# ====================================================
#  sSMTP config file
# ====================================================

root=mail@gmail.com
mailhub=smtp.gmail.com:587
AuthUser=mail@gmail.com
AuthPass=password
RewriteDomain=domain.loc
Hostname=nagios
FromLineOverride=YES
UseSTARTTLS=YES
```

Testare sSMTP

Per verificare che il tutto funzioni correttamente, inviamo una email di prova nella casella di posta configurata:

```
# ssmtp mail@gmail.com
```

Digitiamo un testo, ad esempio "*Test invio email con ssmtp…*"

- Premiamo INVIO
- Premiamo CTRL+D

```
[root@nagios ~]# ssmtp mail@gmail.com
Test invio email con ssmtp...
[root@nagios ~]#
```

Se tutto funziona, riceveremo nella casella specificata una email da *root* con il testo digitato precedentemente.

Configurare Nagios

Una volta verificato che le email di test arrivano, bisogna configurare il file *commands.cfg* di Nagios per poter utilizzare ssmtp:

```
# vi /etc/nagios/objects/commands.cfg    (path se installato solo nagios)

# vi /etc/nagiosql/commands.cfg          (path se installato nagiosql)
```

Sostituire */bin/mail* con il comando */usr/sbin/ssmtp*.

```
define command{

command_name notify-host-by-email

command_line /usr/bin/printf "%b" "***** Nagios *****\n\nNotification Type: $NOTIFICATIONTYPE$\nHost: $HOSTNAME$\nState: $HOSTSTATE$\nAddress: $HOSTADDRESS$\nInfo: $HOSTOUTPUT$\n\nDate/Time: $LONGDATETIME$\n" | /bin/mail /usr/sbin/ssmtp -s "** $NOTIFICATIONTYPE$ Host Alert: $HOSTNAME$ is $HOSTSTATE$ **" $CONTACTEMAIL$

}

define command{

command_name notify-service-by-email

command_line /usr/bin/printf "%b" "***** Nagios *****\n\nNotification Type: $NOTIFICATIONTYPE$\n\nService: $SERVICEDESC$\nHost: $HOSTALIAS$\nAddress: $HOSTADDRESS$\nState: $SERVICESTATE$\n\nDate/Time: $LONGDATETIME$\n\nAdditional Info:\n\n$SERVICEOUTPUT$" | /bin/mail /usr/sbin/ssmtp -s "** $NOTIFICATIONTYPE$ Service Alert: $HOSTALIAS$/$SERVICEDESC$ is $SERVICESTATE$ **" $CONTACTEMAIL$

}
```

Al verificarsi di un alert, Nagios invierà una notifica all'indirizzo email specificato nella configurazione di ssmtp.

```
***** Nagios *****

Notification Type: PROBLEM

Service: Printer Status
Host: HP Color LaserJet 5550
Address: 172.16.20.100
State: WARNING

Date/Time: Thu Jan 21 02:47:46 CET 2010

Additional Info:

Toner Low (Powersave on)
```

Questo ci permette di essere avvisati immediatamente al verificarsi di un problema e quindi di poter intervenire tempestivamente limitando i disservizi al minimo.

Troubleshooting

Se *sSMTP* funziona inviando la mail manualmente ma Nagios non riesce ad inviare in automatico, verificare come prima cosa il log.

```
# cat /var/log/nagios/nagios.log
```

```
[1286374724] HOST NOTIFICATION: nagiosadmin;HP-lj3015p;DOWN;notify-host-by-email
;CRITICAL - Host Unreachable (192.168.10.12)
[1286374724] Warning: Attempting to execute the command "/usr/bin/printf "%b" "*
**** Nagios *****\n\nNotification Type: PROBLEM\nHost: HP-lj3015p\nState: DOWN\n
Address: 192.168.10.12\nInfo: CRITICAL - [illegible] (192.168.10.12)\n\nDat
e/Time: Wed Oct 6 16:18:44 CEST 2010\n" | /usr/bin/mail -s "** PROBLEM Host Aler
t: HP-lj3015p is DOWN **" lanadmin@dominio.com [illegible] resulted in a return code of 1
27.  Make sure the script or binary you are trying to execute actually exists...
```

Questo indica che non è stato modificato correttamente il file di configurazione.

```
# vi /etc/nagios/objects/commands.cfg    (path se installato solo
nagios)

# vi /etc/nagiosql/commands.cfg          (path se installato
nagiosql)
```

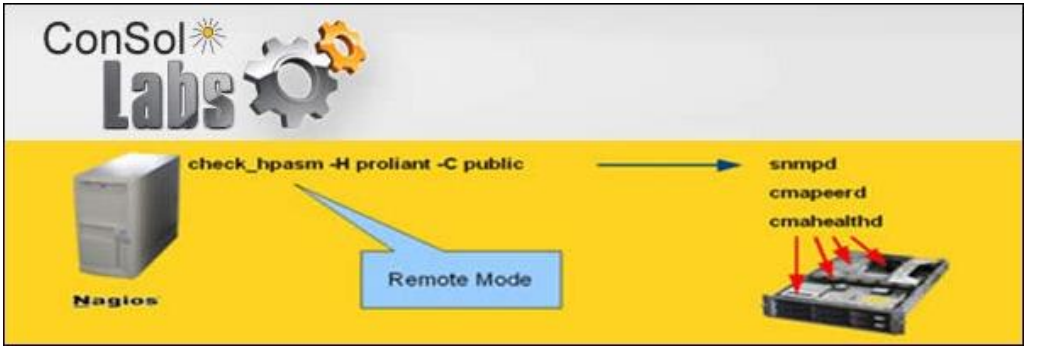
```
define command {
        command_name                            notify-host-by-email
        command_line                            /usr/bin/printf "%b" "***** Nag
ios *****\n\nNotification Type: $NOTIFICATIONTYPE$\nHost: $HOSTNAME$\nState: $H
OSTSTATE$\nAddress: $HOSTADDRESS$\nInfo: $HOSTOUTPUT$\n\nDate/Time: $LONGDATETI
ME$\n" | /usr/bin/mail -s "** $NOTIFICATIONTYPE$ Host Alert: $HOSTNAME$ is $HOS
TSTATE$ **" $CONTACTEMAIL$
}
```

Verificare inoltre la configurazione del file */etc/nagiosql/contacts.cfg*.

```
define contact {
        contact_name                            nagios_administrator
        alias                                   Nagios Admin
        host_notifications_enabled              1
        service_notifications_enabled           1
        host_notification_period                24x7
        service_notification_period             24x7
        host_notification_options               d,u,r
        service_notification_options            w,c,r
        host_notification_commands              notify-host-by-email
        service_notification_commands           notify-service-by-email
        email                                   administrator@dominio.com
        use                                     admin-contact
        }
```

Ricontrollare che SMTP, username, password e l'indirizzo email siano stati inseriti correttamente.

Monitorare i server HP Proliant con Nagios



Sapere se l'hardware di un server funziona correttamente e soprattutto conoscere lo stato dell'array è fondamentale per non rischiare brutte sorprese.

Purtroppo il sistema di monitoraggio Nagios non è provvisto della funzione di check dello stato dell'hardware compatibile con i vari prodotti disponibili sul mercato. Fortunatamente presso il sito http://exchange.nagios.org sono disponibili diversi addon, plugin e altro che permettono di arricchire le funzioni di Nagios e quindi di monitorare diversi brand di hardware.

Utilizzando principalmente server HP Proliant, l'esigenza è di poter monitorare lo stato globale dei server e soprattutto se l'array è integro o in stato di failure… è vero che tendenzialmente è saggio configurare i server con sistemi RAID 5 ma se non siamo al corrente che un disco dell'array è danneggiato e trascuriamo il tutto… provate ad immaginare cosa succederebbe se anche un secondo disco decidesse di passare a miglior vita?

Per poter effettuare il monitoraggio dello stato dell'hardware dei server HP Proliant tramite Nagios, c'è un ottimo plugin che serve proprio a questo scopo: si chiama check_hpasm ed è reperibile presso il sito *http://labs.consol.de*. Per poter utilizzare questo plugin è indispensabile che sui server da monitorare sia attivo l'agent SNMP.

Installazione

Per procedere alla sua installazione, dobbiamo ovviamente scaricare il software per il nostro sistema di monitoraggio, Nagios appunto.

```
# wget http://labs.consol.de/wp-content/uploads/2010/01/check_hpasm-4.1.1.tar.gz
```

```
# tar -xzvf check_hpasm-4.1.1.tar.gz
```

Una volta scompattato l'archivio, impostiamo i parametri per l'installazione su CentOS:

```
# cd check_hpasm-4.1.1
```

```
# ./configure -prefix=/usr/lib/nagios/plugins
```

```
[root@nagios check_hpasm-4.1.1]# ./configure --prefix=/usr/lib/nagios/plugins
checking for a BSD-compatible install... /usr/bin/install -c
checking whether build environment is sane... yes
checking for a thread-safe mkdir -p... /bin/mkdir -p
checking for gawk... gawk
checking whether make sets $(MAKE)... yes
checking how to create a pax tar archive... gnutar
checking build system type... i686-pc-linux-gnu
checking host system type... i686-pc-linux-gnu
checking for a BSD-compatible install... /usr/bin/install -c
checking whether make sets $(MAKE)... (cached) yes
checking for gawk... (cached) gawk
checking for sh... /bin/sh
checking for perl... /usr/bin/perl
configure: creating ./config.status
config.status: creating Makefile
config.status: creating plugins-scripts/Makefile
config.status: creating plugins-scripts/subst
                      --with-perl: /usr/bin/perl
                --with-nagios-user: nagios
               --with-nagios-group: nagios
               --with-noinst-level: unknown
                    --with-degrees: unknown
                 --enable-perfdata: no
             --enable-extendedinfo: no
                  --enable-hwinfo: yes
                 --enable-hpacucli: no
[root@nagios check_hpasm-4.1.1]#
```

Procediamo quindi con l'effettiva installazione tramite il comando *make*:

```
# make
```

```
[root@nagios check_hpasm-4.1.1]# make
Making all in plugins-scripts
make[1]: Entering directory `/install/check_hpasm-4.1.1/plugins-scripts'
/bin/echo "#! #PERL# -w" | gawk -f ./subst > check_hpasm
/bin/echo >> check_hpasm
for m in Nagios/MiniPlugin.pm HP/SNMP/Utils.pm HP/Proliant/Component/Powersupply
Subsystem.pm HP/Proliant/Component/PowersupplySubsystem/CLI.pm HP/Proliant/Compo
nent/PowersupplySubsystem/SNMP.pm HP/Proliant/Component/TemperatureSubsystem.pm
HP/Proliant/Component/TemperatureSubsystem/CLI.pm HP/Proliant/Component/Temperat
ureSubsystem/SNMP.pm HP/Proliant/Component/CpuSubsystem.pm HP/Proliant/Component
/CpuSubsystem/CLI.pm HP/Proliant/Component/CpuSubsystem/SNMP.pm HP/Proliant/Comp
```

Eseguito il comando *make*, nella directory *check_hpasm-4.1.1/plugins-scripts* viene creato il file check_hpasm che è appunto il nostro plugin compilato.

```
[root@nagios plugins-scripts]# ll
total 328
-rwxr-xr-x 1 root root 267780 Mar  5 08:27 check_hpasm
-rw-r--r-- 1 1000 1000   5228 Jan  7 14:15 check_hpasm.pl
drwxrwxrwx 5 1000 1000   4096 Jan  7 14:16 HP
-rw-r--r-- 1 root root  13361 Mar  5 08:24 Makefile
-rw-r--r-- 1 1000 1000   2978 Jan  7 14:15 Makefile.am
-rw-r--r-- 1 1000 1000  12437 Jan  7 14:15 Makefile.in
drwxrwxrwx 2 1000 1000   4096 Jan  7 14:16 Nagios
-rw-r--r-- 1 root root   1430 Mar  5 08:24 subst
-rw-r--r-- 1 1000 1000   1460 Jan  7 14:15 subst.in
[root@nagios plugins-scripts]#
```

Per terminare l'installazione è sufficiente copiare questo file nella directory plugins di Nagios:

```
# cp check_hpasm-4.1.1/plugins-scripts/check_hpasm
/usr/lib/nagios/plugins/
```

Configurazione

Terminata l'installazione, va definito il comando *check_hpasm* che Nagios utilizzerà per effettuare il monitoraggio del server editando il file *command.cfg*:

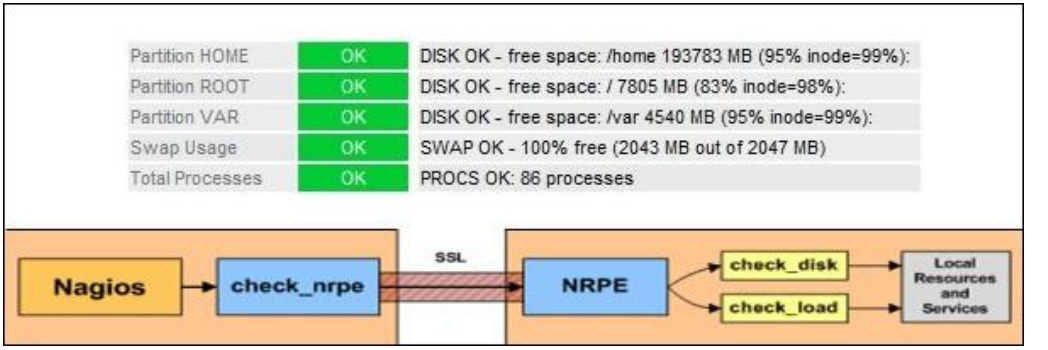
```
# vi /etc/nagios/objects/commands.cfg

define command {
command_name check_hpasm
command_line $USER1$/check_hpasm -H $HOSTADDRESS$ -C $ARG1$ -v -
ignore-fan-redundancy*
}
```

* Il parametro *–ignore-fan-redundancy* va specificato solo se il server non è dotato di fan ridondanti onde evitare continui warning.

Se tutto funziona correttamente, Nagios riporterà come status dell'hardware del nostro server il seguente messaggio:

```
OK - System: 'proliant ml350 g4', S/N: '[redacted]', ROM: 'D17 07/16/2007', hardware working fine, da: 1 logical
drives, 4 physical drives
```

Adesso l'hardware del nostro server è monitorato. Al verificarsi di un qualsiasi problema il sistema genererà un alert.



Come visto nei precedenti post, Nagios è un ottimo sistema per il monitoraggio della rete. Se abbiamo delle macchine in Linux e vogliamo tenere sotto controllo lo stato globale del sistema, dobbiamo installare nei computer nagios-nrpe, un agent di Nagios che permette al sistema di effettuare controlli remoti.

Vediamo i vari passi da effettuare per configurare le nostre macchine remote utilizzando Linux CentOS.

Installazione plugin sulla macchina remota

Per effettuare l'installazione tramite *yum* è necessario aver installato il repository RPMforge.

```
# yum install nagios-nrpe
# chkconfig nrpe on
```

I plug-in vengono installati nella directory */usr/lib/nagios/plugins/*.

Per monitorare le eventuali partizioni presenti nei sistemi Linux della rete, dobbiamo conoscere quante sono le partizioni presenti nelle varie macchine. Tramite il comando *df* è possibile visualizzare le partizioni di un sistema.

```
# df -h
```

```
[admin@[redacted] ~]$ df -h
Filesystem            Size  Used Avail Use% Mounted on
/dev/hda3             9.7G  1.6G  7.7G  17% /
/dev/hda7             208G  8.1G  190G   5% /home
/dev/hda6             996M   57M  888M   6% /tmp
/dev/hda5             5.0G  237M  4.5G   5% /var
/dev/hda1              99M   11M   83M  12% /boot
tmpfs                1005M     0 1005M   0% /dev/shm
```

In questo caso abbiamo cinque partizioni. Questa informazione ci serve per aggiungere i parametri mancanti nel file di configurazione di NRPE.

Configurazione del plugin

Per poter monitorare i nostri sistemi (partizioni, swap, processi, etc.), bisogna editare il file di configurazione *nrpe.conf*. Va specificato l'IP del server Nagios per permettere la corretta comunicazione tra i sistemi e definire i comandi addizionali richiesti non presenti per default nel file di configurazione.

```
# vi /etc/nagios/nrpe.conf
```

log_facility=daemon
pid_file=/var/run/nrpe.pid
server_port=5666
#server_address=127.0.0.1

nrpe_user=nagios
nrpe_group=nagios
allowed_hosts=127.0.0.1,IP_Nagios

dont_blame_nrpe=0
 # command_prefix=/usr/bin/sudo
debug=0
command_timeout=60
connection_timeout=300
#allow_weak_random_seed=1

#include=<somefile.cfg>
#include_dir=<somedirectory>
#include_dir=<someotherdirectory>

 # The following examples use hardcoded command arguments…
command[check_users]=/usr/lib/nagios/plugins/check_users -w 5 -c 10

command[check_load]=/usr/lib/nagios/plugins/check_load -w 15,10,5 -c 30,25,20
command[check_hda1]=/usr/lib/nagios/plugins/check_disk -w 20% -c 10% -p /dev/hda1

 # Aggiungere i comandi in base alle partizioni da monitorare
command[check_hdax]=/usr/lib/nagios/plugins/check_disk -w 20% -c 10% -p /dev/hdax
command[check_sdax]=/usr/lib/nagios/plugins/check_disk -w 20% -c 10% -p /dev/sdax

command[check_zombie_procs]=/usr/lib/nagios/plugins/check_procs -w 5 -c 10 -s Z
command[check_total_procs]=/usr/lib/nagios/plugins/check_procs -w 150 -c 200
command[check_swap]=/usr/lib/nagios/plugins/check_swap -w 20% -c 10%
Avviamo quindi il servizio:

```
# service nrpe start
```

Se tra la macchina remota e il server Nagios c'è un firewall, bisogna aprire la porta TCP 5666 necessaria a Nagios per comunicare con la macchina da monitorare.

Testare la comunicazione

Per verificare che Nagios riesca a comunicare con il daemon NRPE nella macchina remota, da Nagios lanciamo il comando:

```
# /usr/lib/nagios/plugins/check_nrpe -H IP_MacchinaRemota
```

```
[root@nagios /]# /usr/lib/nagios/plugins/check_nrpe -H 192.168.10.10
NRPE v2.12
[root@nagios /]#
```

Per verificare manualmente che il sistema funzioni, proviamo a controllare lo stato della partizione di ROOT della macchina remota:

```
# /usr/lib/nagios/plugins/check_nrpe -H IP_MacchinaRemota -c
check_hda3
```

```
[root@nagios /]# /usr/lib/nagios/plugins/check_nrpe -H 192.168.10.10 -c check_hda3
DISK OK - free space: / 7805 MB (83% inode=98%);| /=1598MB;7932;8924;0;9916
[root@nagios /]#
```

Verificato che il plug-in funziona correttamente, andiamo a definire il comando in Nagios.

Configurare nagios

Una volta configurati i parametri nel file di configurazione di NRPE, non ci resta che editare il file */etc/nagios/commands.cfg* per definire il comando per l'utilizzo del plug-in da parte di Nagios:

```
define command {
command_name check_nrpe
command_line $USER1$/check_nrpe -H $HOSTADDRESS$ -c $ARG1$
}
```

Impostando ad esempio il comando per la verifica dello stato della partizione di ROOT della macchina remota, Nagios è adesso in grado di visualizzare lo stato corrente ed eventualmente generare un alert al presentarsi di un problema.

Partition ROOT	OK	DISK OK - free space: / 7805 MB (83% inode=98%):

Adesso siamo in grado di monitorare i parametri che più ci interessano delle macchine remote Linux presenti nella rete.

Installare Nagios + Centreon su CentOS 6

Monitorare la rete per garantire la funzionalità ottimale dei vari servizi è un aspetto molto importante per uno staff IT.

Sapere se un dato server sta funzionando correttamente, se le stampanti sono tutte operative, se i database sono integri sono tutti fattori che determinano l'efficienza della rete aziendale ed il successo del business svolto.

Tra i vari prodotti disponibili sul mercato, una soluzione funzionale e potenzialmente a costo zero è data dall'abbinare due ottimi prodotti come Nagios e Centreon leader nel monitoraggio dei sistemi.

Installazione componenti CentOS

La procedura utilizza la versione CentOS 6 64-bit minimal installation come OS in modo da risparmiare spazio e non installare inutili package.

Installato il sistema operativo, procedere ad effettuare gli aggiornamenti di *CentOS* tramite il comando *yum*.

```
# yum update
```

Installare i package di sistema che sono richiesti per il corretto funzionamento del sistema *Nagios* + *Centreon*.

```
# yum install system-config-firewall-tui system-config-network-tui
wget ntp perl vixie-cron sudo
```

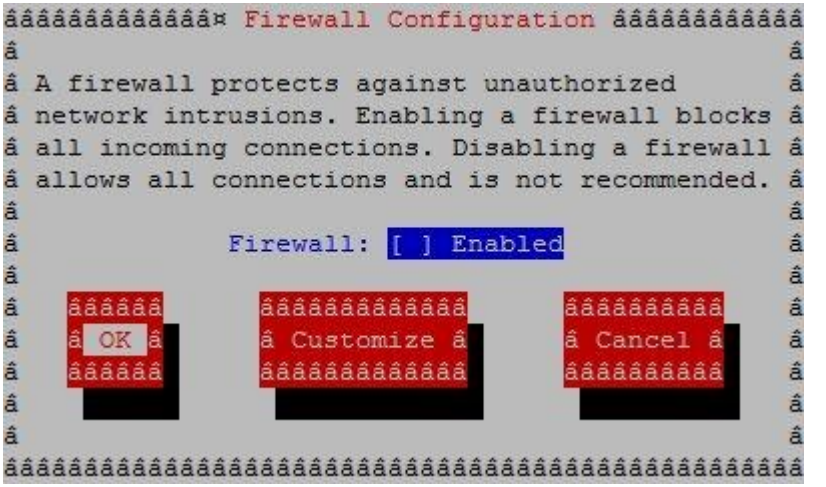
Il sistema richiede che SELINUX sia disabilitato.

```
# vi /etc/sysconfig/selinux
```

```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#     enforcing - SELinux security policy is enforced.
#     permissive - SELinux prints warnings instead of enforcing.
#     disabled - No SELinux policy is loaded.
SELINUX=disabled
# SELINUXTYPE= can take one of these two values:
#     targeted - Targeted processes are protected,
#     mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

Disabilitare anche il firewall per evitare problemi di funzionamento.

```
# system-config-firewall-tui
```



Attivare il client ***ntp*** ed impostare la data corretta del sistema.

```
# chkconfig ntpd on
# ntpdate pool.ntp.org
# service ntpd start
```

```
[root@centos6 ~]# chkconfig ntpd on
[root@centos6 ~]# ntpdate pool.ntp.org
20 Sep 12:29:29 ntpdate[2413]: step time server 212.121.88.250 offset 58.67
3646 sec
[root@centos6 ~]# service ntpd start
Starting ntpd:                                             [  OK  ]
[root@centos6 ~]#
```

Scaricare il package del repository rpmforge.

```
# wget http://packages.sw.be/rpmforge-release/rpmforge-release-
0.5.2-2.el6.rf.x86_64.rpm
```

```
[root@centos6 install]# wget http://packages.sw.be/rpmforge-release/rpmforg
e-release-0.5.2-2.el6.rf.x86_64.rpm
--2011-11-08 12:32:05--  http://packages.sw.be/rpmforge-release/rpmforge-re
lease-0.5.2-2.el6.rf.x86_64.rpm
Resolving packages.sw.be... 78.46.17.228
Connecting to packages.sw.be|78.46.17.228|:80... connected.
```

Effettuare l'installazione del package tramite il comando *rpm*.

```
# rpm -Uvh rpmforge-release-0.5.2-2.el6.rf.x86_64.rpm
```

Installazione mySQL, Apache e PHP

Procedere con l'installazione dei package MySQL, Apache e PHP.

```
# yum install mysql mysql-server mysql-devel httpd mod_ssl php
```

```
[root@centos6 /]# yum install mysql mysql-server mysql-devel httpd mod_ssl p
hp
Loaded plugins: fastestmirror, presto
Loading mirror speeds from cached hostfile
 * base: mirror.mserverz.de
 * extras: centos.intergenia.de
 * rpmforge: ftp-stud.fht-esslingen.de
 * updates: centos.intergenia.de
Setting up Install Process
Resolving Dependencies
--> Running transaction check
---> Package httpd.x86_64 0:2.2.15-5.el6.centos set to be updated
--> Processing Dependency: httpd-tools = 2.2.15-5.el6.centos for package: h
ttpd-2.2.15-5.el6.centos.x86_64
--> Processing Dependency: /etc/mime.types for package: httpd-2.2.15-5.el6.
centos.x86_64
--> Processing Dependency: apr-util-ldap for package: httpd-2.2.15-5.el6.ce
ntos.x86_64
```

Attivare i servizi e renderli avviabili anche al boot del sistema.

```
# chkconfig httpd on
# service httpd start
# chkconfig mysqld on
# service mysqld start
```

Mettere in sicurezza MySQL digitando da console:

```
# mysql_secure_installation
```

Digitare Y a tutte le richieste presentate dal sistema.

- Set root password? [Y/n] **y**
- Remove anonymous users? [Y/n] **y**
- Disallow root login remotely? [Y/n] **y**
- Remove test database and access to it? [Y/n] **y**
- Reload privilege tables now? [Y/n] **y**

Installazione prerequisiti

Come indicato nella documentazione di *Centreon*, alcuni package aggiuntivi sono richiesti per il corretto funzionamento dell'applicativo.

- PHP and Dependencies
- GD Modules
- PERL modules
- DBI Modules
- RRDTool modules
- SNMP and Supporting Packages
- Additional Apps
- PEAR modules

Installazione moduli PHP

```
# yum install php-mysql php-gd php-ldap php-xml php-mbstring php-posix
```

```
[root@centos6 ~]# yum install php-mysql php-gd php-ldap php-xml php-mbstrin
g php-posix
Loaded plugins: fastestmirror, presto
Loading mirror speeds from cached hostfile
 * base: ftp.uni-bayreuth.de
 * extras: mirror.de.leaseweb.net
 * rpmforge: fr2.rpmfind.net
 * updates: mirror.de.leaseweb.net
Setting up Install Process
Resolving Dependencies
--> Running transaction check
---> Package php-gd.x86_64 0:5.3.2-6.el6_0.1 set to be updated
--> Processing Dependency: libpng12.so.0(PNG12_0)(64bit) for package: php-g
d-5.3.2-6.el6_0.1.x86_64
--> Processing Dependency: libpng12.so.0()(64bit) for package: php-gd-5.3.2
-6.el6_0.1.x86_64
--> Processing Dependency: libjpeg.so.62()(64bit) for package: php-gd-5.3.2
-6.el6_0.1.x86_64
```

Installazione moduli GD

```
# yum install gd fontconfig-devel libjpeg-devel libpng-devel gd-devel perl-GD
```

```
[root@centos6 ~]# yum install gd fontconfig-devel libjpeg-devel libpng-deve
l gd-devel perl-GD
Loaded plugins: fastestmirror, presto
Loading mirror speeds from cached hostfile
 * base: ftp.uni-bayreuth.de
 * extras: mirror.de.leaseweb.net
 * rpmforge: fr2.rpmfind.net
 * updates: mirror.de.leaseweb.net
Setting up Install Process
Package gd-2.0.35-10.el6.x86_64 already installed and latest version
Resolving Dependencies
--> Running transaction check
---> Package fontconfig-devel.x86_64 0:2.8.0-3.el6 set to be updated
--> Processing Dependency: freetype-devel >= 2.1.4 for package: fontconfig-
devel-2.8.0-3.el6.x86_64
```

Installazione moduli PERL

```
# yum install perl-Config-IniFiles
```

```
[root@centos6 ~]# yum install perl-Config-IniFiles
Loaded plugins: fastestmirror, presto
Loading mirror speeds from cached hostfile
 * base: ftp.uni-bayreuth.de
 * extras: mirror.de.leaseweb.net
 * rpmforge: fr2.rpmfind.net
 * updates: mirror.de.leaseweb.net
Setting up Install Process
Resolving Dependencies
--> Running transaction check
---> Package perl-Config-IniFiles.noarch 0:2.56-1.el6.rf set to be updated
--> Finished Dependency Resolution
```

Installazione moduli DBI

```
# yum install perl-DBI perl-DBD-MySQL
```

```
[root@centos6 ~]# yum install perl-DBI perl-DBD-MySQL
Loaded plugins: fastestmirror, presto
Loading mirror speeds from cached hostfile
 * base: ftp.uni-bayreuth.de
 * extras: mirror.de.leaseweb.net
 * rpmforge: fr2.rpmfind.net
 * updates: mirror.de.leaseweb.net
Setting up Install Process
Package perl-DBI-1.609-4.el6.x86_64 already installed and latest version
Package perl-DBD-MySQL-4.013-3.el6.x86_64 already installed and latest vers
ion
```

Installazione RRDTOOLS

```
# yum install rrdtool perl-rrdtool
```

```
[root@centos6 ~]# yum install rrdtool perl-rrdtool
Loaded plugins: fastestmirror, presto
Loading mirror speeds from cached hostfile
 * base: ftp.uni-bayreuth.de
 * extras: mirror.de.leaseweb.net
 * rpmforge: fr2.rpmfind.net
 * updates: mirror.de.leaseweb.net
Setting up Install Process
Resolving Dependencies
--> Running transaction check
---> Package rrdtool.x86_64 0:1.3.8-6.el6 set to be updated
--> Processing Dependency: dejavu-sans-mono-fonts for package: rrdtool-1.3.
8-6.el6.x86_64
--> Processing Dependency: dejavu-lgc-sans-mono-fonts for package: rrdtool-
1.3.8-6.el6.x86_64
```

Installazione SNMP

```
# yum install net-snmp net-snmp-utils net-snmp-libs perl-Crypt-DES
perl-Digest-SHA1 perl-Digest-HMAC perl-Socket6 perl-IO-Socket-
INET6 perl-Net-SNMP net-snmp-perl php-snmp dmidecode lm_sensors
```

```
[root@centos6 ~]# yum install net-snmp net-snmp-utils net-snmp-libs perl-Cr
ypt-DES perl-Digest-SHA1 perl-Digest-HMAC perl-Socket6 perl-IO-Socket-INET6
 perl-Net-SNMP net-snmp-perl php-snmp dmidecode lm_sensors
Loaded plugins: fastestmirror, presto
Loading mirror speeds from cached hostfile
 * base: ftp.uni-bayreuth.de
 * extras: mirror.de.leaseweb.net
 * rpmforge: fr2.rpmfind.net
 * updates: mirror.de.leaseweb.net
Setting up Install Process
Package perl-Crypt-DES-2.05-3.2.el6.rf.x86_64 already installed and latest
version
Package perl-Digest-SHA1-2.12-2.el6.x86_64 already installed and latest ver
sion
Package perl-Digest-HMAC-1.01-22.el6.noarch already installed and latest ve
rsion
Package perl-Socket6-0.23-3.el6.x86_64 already installed and latest version
Package perl-Net-SNMP-5.2.0-1.2.el6.rf.noarch already installed and latest
version
Resolving Dependencies
--> Running transaction check
---> Package dmidecode.x86_64 1:2.10-1.30.1.el6 set to be updated
---> Package lm_sensors.x86_64 0:3.1.1-10.el6 set to be updated
--> Processing Dependency: libsensors.so.4()(64bit) for package: lm_sensors
-3.1.1-10.el6.x86_64
```

Attivare il servizio *snmp* e renderlo operativo anche al boot del sistema.

```
# chkconfig snmpd on
# service snmpd start
```

Installazione APPS

```
# yum install fping graphviz
```

```
[root@centos6 ~]# yum install fping graphviz
Loaded plugins: fastestmirror, presto
Loading mirror speeds from cached hostfile
 * base: ftp.uni-bayreuth.de
 * extras: mirror.de.leaseweb.net
 * rpmforge: fr2.rpmfind.net
 * updates: mirror.de.leaseweb.net
Setting up Install Process
Package fping-2.4-1.b2.3.el6.rf.x86_64 already installed and latest version
Resolving Dependencies
--> Running transaction check
---> Package graphviz.x86_64 0:2.26.0-4.el6 set to be updated
--> Processing Dependency: urw-fonts for package: graphviz-2.26.0-4.el6.x86
_64
--> Processing Dependency: libXaw.so.7()(64bit) for package: graphviz-2.26.
0-4.el6.x86_64
--> Processing Dependency: libXmu.so.6()(64bit) for package: graphviz-2.26.
0-4.el6.x86_64
```

Installazione PEAR e moduli richiesti

- I moduli PEAR richiesti da Centreon:
- Auth_SASL
- Date
- DB
- DB_DataObject
- DB_DataObject_FormBuilder
- HTML_Common
- HTML_QuickForm
- HTML_QuickForm_advmultiselect
- HTML_Table
- Image_Canvas
- Image_Color
- Image_Graph
- Image_GraphViz
- Mail_Mime
- MDB2
- Net_Ping
- Net_Traceroute

- Numbers_Roman
- Numbers_Words
- PEAR
- Validate
- XML_RPC

```
# yum install php-pear
```

```
[root@centos6 /]# yum install php-pear
Loaded plugins: fastestmirror, presto
Loading mirror speeds from cached hostfile
 * base: ftp.uni-bayreuth.de
 * extras: mirror.de.leaseweb.net
 * rpmforge: fr2.rpmfind.net
 * updates: mirror.de.leaseweb.net
Setting up Install Process
Resolving Dependencies
--> Running transaction check
---> Package php-pear.noarch 1:1.9.0-2.el6 set to be updated
--> Finished Dependency Resolution
```

```
# pear channel-update pear.php.net
```

```
[root@centos6 /]# pear channel-update pear.php.net
Updating channel "pear.php.net"
Update of Channel "pear.php.net" succeeded
[root@centos6 /]#
```

```
# pear upgrade-all
```

```
[root@centos6 /]# pear channel-update pear.php.net
Updating channel "pear.php.net"
Update of Channel "pear.php.net" succeeded
[root@centos6 /]# pear upgrade-all
Will upgrade channel://pear.php.net/structures_graph
Will upgrade channel://pear.php.net/xml_rpc
Will upgrade channel://pear.php.net/archive_tar
Will upgrade channel://pear.php.net/pear
Will upgrade channel://pear.php.net/console_getopt
WARNING: "pear/XML_RPC" is deprecated in favor of "pear/XML_RPC2"
downloading Structures_Graph-1.0.4.tgz ...
Starting to download Structures_Graph-1.0.4.tgz (30,318 bytes)
.........done: 30,318 bytes
downloading XML_RPC-1.5.5.tgz ...
Starting to download XML_RPC-1.5.5.tgz (31,862 bytes)
...done: 31,862 bytes
```

```
# pear install -o -f –alldeps DB DB_DataObject
DB_DataObject_FormBuilder MDB2 Date Numbers_Roman Numbers_Words
HTML_Common HTML_QuickForm HTML_QuickForm_advmultiselect
HTML_Table Auth_SASL HTTP Image_Canvas Image_Color Image_Graph
Image_GraphViz Mail Mail_Mime Net_SMTP Net_Socket Net_Traceroute
Net_Ping Validate SOAP Auth_SASL Date Validate XML_RPC
```

```
[root@centos6 /]# pear install -o -f --alldeps DB DB_DataObject DB_DataObje
ct_FormBuilder MDB2 Date Numbers_Roman Numbers_Words HTML_Common HTML_Quick
Form HTML_QuickForm_advmultiselect HTML_Table Auth_SASL HTTP Image_Canvas I
mage_Color Image_Graph Image_GraphViz Mail Mail_Mime Net_SMTP Net_Socket Ne
t_Traceroute Net_Ping Validate SOAP Auth_SASL Date Validate XML_RPC
WARNING: "pear/DB" is deprecated in favor of "pear/MDB2"
WARNING: failed to download pear.php.net/Numbers_Words within preferred sta
te "stable", will instead download version 0.16.2, stability "beta"
WARNING: "pear/HTML_Common" is deprecated in favor of "pear/HTML_Common2"
WARNING: "pear/HTML_QuickForm" is deprecated in favor of "pear/HTML_QuickFo
rm2"
WARNING: failed to download pear.php.net/Image_Canvas within preferred stat
e "stable", will instead download version 0.3.3, stability "alpha"
WARNING: failed to download pear.php.net/Image_Graph within preferred state
 "stable", will instead download version 0.8.0, stability "alpha"
```

Installazione sendmail e mailx

```
# yum install sendmail mailx
```

```
[root@centos6 /]# yum install sendmail mailx
Loaded plugins: fastestmirror, presto
Loading mirror speeds from cached hostfile
 * base: ftp.uni-bayreuth.de
 * extras: mirror.de.leaseweb.net
 * rpmforge: fr2.rpmfind.net
 * updates: mirror.de.leaseweb.net
Setting up Install Process
Resolving Dependencies
--> Running transaction check
---> Package mailx.x86_64 0:12.4-6.el6 set to be updated
---> Package sendmail.x86_64 0:8.14.4-8.el6 set to be updated
```

Installazione Nagios e NDOutils

Installare Nagios e i relativi package aggiuntivi richiesti.

```
# yum install nagios nagios-devel nagios-plugins nagios-plugins-
setuid nagios-plugins-nrpe ndoutils
```

```
[root@centos6 /]# yum install nagios nagios-devel nagios-plugins nagios-plug
ins-setuid nagios-plugins-nrpe ndoutils
Loaded plugins: fastestmirror, presto
Loading mirror speeds from cached hostfile
 * base: mirror.mserverz.de
 * extras: centos.intergenia.de
 * rpmforge: ftp-stud.fht-esslingen.de
 * updates: centos.intergenia.de
Setting up Install Process
Resolving Dependencies
--> Running transaction check
---> Package nagios.x86_64 0:3.2.3-3.el6.rf set to be updated
--> Processing Dependency: libltdl.so.7()(64bit) for package: nagios-3.2.3-
3.el6.rf.x86_64
---> Package nagios-devel.x86_64 0:3.2.3-3.el6.rf set to be updated
```

Creare utente e password dell'amministratore per accedere a *Nagios*.

htpasswd -bcm /etc/nagios/htpasswd.users *administrator password*

```
# htpasswd -bcm /etc/nagios/htpasswd.users nagiosadmin password
```

```
[root@centos6 /]# htpasswd -bcm /etc/nagios/htpasswd.users nagiosadmin pass
word
Adding password for user nagiosadmin
[root@centos6 /]#
```

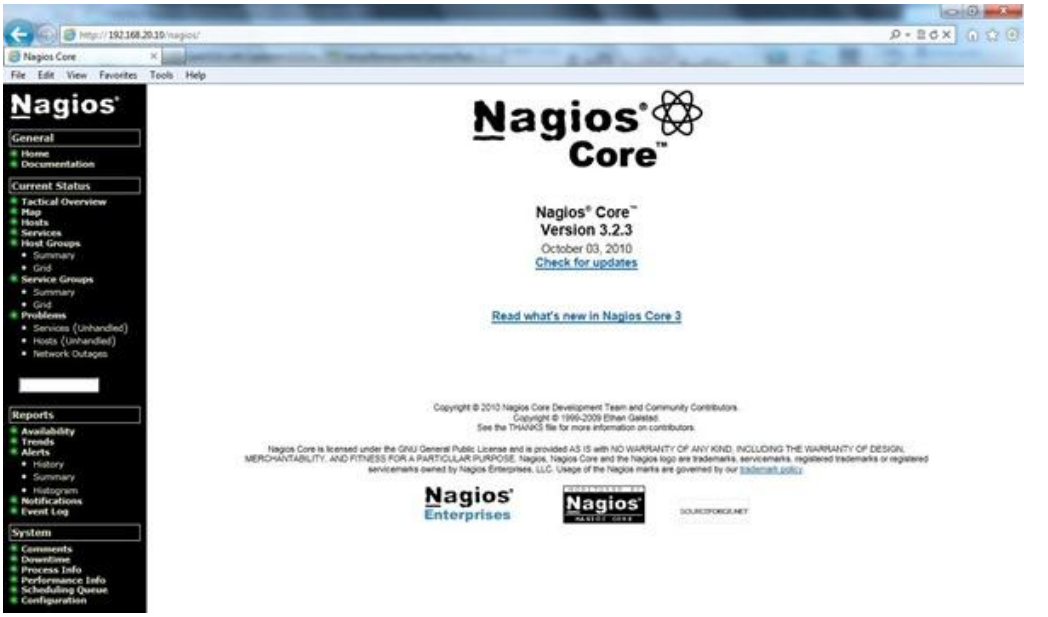
Riavviare il servizio Apache per rendere attiva l'interfaccia web di *Nagios*.

```
# service httpd restart
```

Attivare Nagios al boot del sistema.

```
# chkconfig nagios on
```

Verificare l'accesso a Nagios digitando da browser l'indirizzo http://IP_Address/nagios. Se è stato installato il modulo di Apache *mod_ssl* verificare anche l'accesso tramite https.



L'installazione dei componenti richiesti per il funzionamento del sistema è completa.

Installazione di Centreon

Centreon è un software per il monitoraggio di server, reti e software e la sua l'installazione e configurazione richiede alcuni passaggi.

Prima di procedere con l'installazione di *Centreon*, è opportuno segnarsi i path dei moduli che sono richiesti durante la configurazione dell'applicativo.

- **RRD**: /usr/lib64/perl5/RRDs.pm
- **PEAR**: /usr/share/pear/PEAR.php

NAGIOS:

- nagios: /usr/lib64/nagios
- config: /etc/nagios
- var: /var/nagios
- plugins: /usr/lib64/nagios/plugins
- image: /usr/share/nagios/images/logos
- **NDOMOD**: /usr/libexec/ndomod-3x.o

Scaricare l'ultima versione di Centreon tramite il comando *wget*.

```
# wget http://download.centreon.com/index.php?id=158
```

```
[root@centos6 install]# wget http://download.centreon.com/index.php?id=158
--2011-09-19 14:02:27--  http://download.centreon.com/index.php?id=158
Resolving download.centreon.com... 91.121.53.110
Connecting to download.centreon.com|91.121.53.110|:80... connected.
HTTP request sent, awaiting response... 302 Found
Location: http://download.centreon.com/centreon/centreon-2.2.2.tar.gz [foll
owing]
--2011-11-08 14:02:27--  http://download.centreon.com/centreon/centreon-2.2
.2.tar.gz
Reusing existing connection to download.centreon.com:80.
HTTP request sent, awaiting response... 200 OK
Length: 6351229 (6.1M) [application/x-gzip]
Saving to: âcentreon-2.2.2.tar.gzâ

56% [==================>              ] 3,608,123    119K/s  eta 15s
```

Scompattare il file ed effettuare l'installazione.

```
# tar -zxvf centreon-2.2.2.tar.gz
# cd centreon-2.2.2
# ./install.sh -i -v
```

```
#################################################################################
####
#
   #
#                          Centreon (www.centreon.com)
   #
#                           Thanks for using Centreon
   #
#
   #
#                                    v2.2
   #
#
   #
#                                infos@centreon.com
   #
#
   #
#                    Make sure you have installed and configured
   #
#                    sudo - sed - php - apache - rrdtool - mysql
   #
#
   #
#################################################################################
```

Premere INVIO per proseguire.

```
-------------------------------------------------------------------------
        Checking all needed binaries
-------------------------------------------------------------------------
rm                                                          OK
cp                                                          OK
mv                                                          OK
/bin/chmod                                                  OK
/bin/chown                                                  OK
echo                                                        OK
more                                                        OK
mkdir                                                       OK
find                                                        OK
/bin/grep                                                   OK
/bin/cat                                                    OK
/bin/sed                                                    OK

You will now read Centreon Licence.
        Press enter to continue.
```

Accettare l'EULA digitando Y.

```
                    GNU GENERAL PUBLIC LICENSE
                       Version 2, June 1991

 Copyright (C) 1989, 1991 Free Software Foundation, Inc.
                       51 Franklin St, Fifth Floor, Boston, MA  02110-1301
 USA
 Everyone is permitted to copy and distribute verbatim copies
 of this license document, but changing it is not allowed.

                            Preamble

  The licenses for most software are designed to take away your
...................

Do you accept GPL license ?
[y/n], default to [n]:
> y
```

Inizia l'installazione di *Centreon*. Rispondere Y a tutte le richieste effettuate dal sistema.

```
--------------------------------------------------------------------------
        Please choose what you want to install
--------------------------------------------------------------------------

Do you want to install : Centreon Web Front
[y/n], default to [n]:
> y

Do you want to install : Centreon CentCore
[y/n], default to [n]:
> y

Do you want to install : Centreon Nagios Plugins
[y/n], default to [n]:
> y

Do you want to install : Centreon Snmp Traps process
[y/n], default to [n]:
> y

--------------------------------------------------------------------------
```

Accettare i path proposti compilando solo quelli precedentemente segnalati.

Start CentWeb Installation.

```
-------------------------------------------------------------------------
        Start CentWeb Installation
-------------------------------------------------------------------------

Where is your Centreon directory?
default to [/usr/local/centreon]
>

Do you want me to create this directory ? [/usr/local/centreon]
[y/n], default to [n]:
> y
Path /usr/local/centreon                                    OK

Where is your Centreon log directory
default to [/usr/local/centreon/log]
>

Do you want me to create this directory ? [/usr/local/centreon/log]
[y/n], default to [n]:
> y
Path /usr/local/centreon/log                                OK

Where is your Centreon etc directory
default to [/etc/centreon]
>

Do you want me to create this directory ? [/etc/centreon]
[y/n], default to [n]:
> y
Path /etc/centreon                                          OK

Where is your Centreon generation_files directory?
default to [/usr/local/centreon]
>
Path /usr/local/centreon                                    OK

Where is your Centreon variable library directory?
default to [/var/lib/centreon]
>

Do you want me to create this directory ? [/var/lib/centreon]
[y/n], default to [n]:
> y
Path /var/lib/centreon                                      OK

Where is your CentPlugins Traps binary
default to [/usr/local/centreon/bin]
>
```

```
Do you want me to create this directory ? [/usr/local/centreon/bin]
[y/n], default to [n]:
> y
Path /usr/local/centreon/bin                                    OK

Where is the RRD perl module installed [RRDs.pm]
default to [/usr/lib/perl5/RRDs.pm]
> /usr/lib64/perl5/RRDs.pm
Path /usr/lib64/perl5                                           OK
/usr/bin/rrdtool                                                OK
/bin/mail                                                       OK

Where is PEAR [PEAR.php]
default to [/usr/share/php/PEAR.php]
> /usr/share/pear/PEAR.php
Path /usr/share/pear                                            OK

Where is installed Nagios ?
default to [/usr/local/nagios]
>  /usr/lib64/nagios
Path /usr/lib64/nagios                                          OK

Where is your nagios config directory
default to [/usr/local/nagios/etc]
> /etc/nagios
Path /etc/nagios                                                OK

Where is your Nagios var directory ?
default to [/usr/local/nagios/var]
> /var/nagios
Path /var/nagios                                                OK

Where is your Nagios plugins (libexec) directory ?
default to [/usr/local/nagios/libexec]
> /usr/lib64/nagios/plugins
Path /usr/lib64/nagios/plugins                                  OK
/usr/bin/nagios                                                 OK

Where is your Nagios image directory ?
default to [/usr/local/nagios/share/images/logos]
> /usr/share/nagios/images/logos
Path /usr/share/nagios/images/logos                             OK
/usr/bin/nagiostats                                             OK
p1_file : /usr/bin/p1.pl                                        OK
/usr/bin/php                                                    OK
/usr/bin/perl                                                   OK
Finding Apache group :                                          apache
Finding Apache user :                                           apache
Finding Nagios user :                                           nagios
Finding Nagios group :                                          nagios
```

```
Where is your NDO ndomod binary ?
default to [/usr/sbin/ndomod.o]
> /usr/libexec/ndomod-3x.o
/usr/libexec/ndomod-3x.o                                    OK
```

Configure Sudo.

```
-----------------------------------------------------------------------
        Configure Sudo
-----------------------------------------------------------------------

Where is sudo configuration file
default to [/etc/sudoers]
>
/etc/sudoers                                                OK
Nagios init script                                          OK
Your sudo is not configured

Do you want me to configure your sudo ? (WARNING)
[y/n], default to [n]:
> y
Configuring Sudo                                            OK
```

Configure Apache server.

```
-----------------------------------------------------------------------
        Configure Apache server
-----------------------------------------------------------------------

Do you want to add Centreon Apache sub configuration file ?
[y/n], default to [n]:
> y
Create '/etc/httpd/conf.d/centreon.conf'                    OK
Configuring Apache                                          OK

Do you want to reload your Apache ?
[y/n], default to [n]:
> y
Reloading Apache service                                    OK
Preparing Centreon temporary files
Change right on /usr/local/centreon/log                     OK
Change right on /etc/centreon                               OK
Change right on /usr/share/nagios/images/logos              OK
Install nagios documentation                                OK
Change macros for insertBaseConf.sql                        OK
Change macros for php files                                 OK
Change right on /etc/nagios                                 OK
```

```
Copy CentWeb in system directory
Install CentWeb (web front of centreon)                    OK
Install libraries                                          OK
Copying libinstall                                         OK
Change macros for centreon.cron                            OK
Install Centreon cron.d file                               OK
Change macros for archiveDayLog                            OK
Change macros for centAcl.php                              OK
Install cron directory                                     OK
```

Pear Modules

```
-----------------------------------------------------------------------
Pear Modules
-----------------------------------------------------------------------
Check PEAR modules
PEAR                            1.4.9       1.9.4          OK
DB                              1.7.6                      NOK
DB_DataObject                   1.8.4                      NOK
DB_DataObject_FormBuilder       1.0.0RC4                   NOK
MDB2                            2.0.0                      NOK
Date                            1.4.6                      NOK
HTML_Common                     1.2.2                      NOK
HTML_QuickForm                  3.2.5                      NOK
HTML_QuickForm_advmultiselect   1.1.0                      NOK
HTML_Table                      1.6.1                      NOK
Archive_Tar                     1.1         1.3.7          OK
Auth_SASL                       1.0.1                      NOK
Console_Getopt                  1.2         1.3.1          OK
Net_SMTP                        1.2.8                      NOK
Net_Socket                      1.0.1                      NOK
Net_Traceroute                  0.21                       NOK
Net_Ping                        2.4.1                      NOK
Validate                        0.6.2                      NOK
XML_RPC                         1.4.5       1.5.5          OK
SOAP                            0.10.1                     NOK
Log                             1.9.11                     NOK

Do you want me to install/upgrade your PEAR modules
[y/n], default to [y]:
> y
Upgrading PEAR modules
Installing PEAR modules
DB                              1.7.6       1.7.14         OK
DB_DataObject                   1.8.4       1.9.6          OK
DB_DataObject_FormBuilder       1.0.0RC4    1.0.1          OK
MDB2                            2.0.0       2.4.1          OK
HTML_QuickForm_advmultiselect   1.1.0       1.5.1          OK
HTML_Table                      1.6.1       1.8.3          OK
```

```
Auth_SASL                       1.0.1       1.0.5          OK
Net_SMTP                        1.2.8       1.6.1          OK
Net_Traceroute                  0.21        0.21.3         OK
Net_Ping                        2.4.1       2.4.5          OK
Validate                        0.6.2       0.8.4          OK
SOAP                            0.10.1      0.12.0         OK
Log                             1.9.11      1.12.7         OK
Check PEAR modules
```

Centreon Post Install.

```
-----------------------------------------------------------------------
                Centreon Post Install
-----------------------------------------------------------------------
Create /usr/local/centreon/www/install/install.conf.php    OK
Create /etc/centreon/instCentWeb.conf                      OK
```

Start CentStorage Installation.

```
-----------------------------------------------------------------------
        Start CentStorage Installation
-----------------------------------------------------------------------

Where is your Centreon Run Dir directory?
default to [/var/run/centreon]
>

Do you want me to create this directory ? [/var/run/centreon]
[y/n], default to [n]:
> y
Path /var/run/centreon                                     OK

Where is your CentStorage binary directory
default to [/usr/local/centreon/bin]
>
Path /usr/local/centreon/bin                               OK

Where is your CentStorage RRD directory
default to [/var/lib/centreon]
>
Path /var/lib/centreon                                     OK
Finding Nagios group :                                     nagios
Finding Nagios user :                                      nagios
Preparing Centreon temporary files
/tmp/centreon-setup exists, it will be moved...
install www/install/createTablesCentstorage.sql            OK
Creating Centreon Directory '/var/lib/centreon/status'     OK
Creating Centreon Directory '/var/lib/centreon/metrics'    OK
```

```
Change macros for centstorage binary                        OK
Install CentStorage binary                                  OK
Install library for centstorage                             OK
Change right : /var/run/centreon                            OK
Change macros for centstorage init script                   OK

Do you want me to install CentStorage init script ?
[y/n], default to [n]:
> y
CentStorage init script installed                           OK

Do you want me to install CentStorage run level ?
[y/n], default to [n]:
> y
Change macros for logAnalyser                               OK
Install logAnalyser                                         OK
Change macros for nagiosPerfTrace                           OK
Install nagiosPerfTrace                                     OK
Change macros for purgeLogs                                 OK
Install purgeLogs                                           OK
Change macros for purgeCentstorage                          OK
Install purgeCentstorage                                    OK
Change macros for centreonPurge.sh                          OK
Install centreonPurge.sh                                    OK
Change macros for centstorage.cron                          OK
Install CentStorage cron                                    OK
Create /etc/centreon/instCentStorage.conf                   OK
```

Start CentCore Installation.

```
-----------------------------------------------------------------------
        Start CentCore Installation
-----------------------------------------------------------------------

Where is your CentCore binary directory
default to [/usr/local/centreon/bin]
>
Path /usr/local/centreon/bin                                OK
/usr/bin/ssh                                                OK
/usr/bin/scp                                                OK
Finding Nagios group :                                      nagios
Finding Nagios user :                                       nagios
Preparing Centreon temporary files
/tmp/centreon-setup exists, it will be moved...
Change CentCore Macro                                       OK
Copy CentCore in binary directory                           OK
Change right : /var/run/centreon                            OK
Change right : /var/lib/centreon                            OK
Replace CentCore init script Macro                          OK
```

```
Do you want me to install CentCore init script ?
[y/n], default to [n]:
> y
CentCore init script installed                                OK

Do you want me to install CentCore run level ?
[y/n], default to [n]:
> y
Create /etc/centreon/instCentCore.conf                        OK
```

Start CentPlugins Installation.

```
-----------------------------------------------------------------------
        Start CentPlugins Installation
-----------------------------------------------------------------------

Where is your CentPlugins lib directory
default to [/var/lib/centreon/centplugins]
>

Do you want me to create this directory ? [/var/lib/centreon/centplugins]
[y/n], default to [n]:
> y
Path /var/lib/centreon/centplugins                            OK
Finding Nagios user :                                         nagios
Finding Nagios group :                                        nagios
Preparing Centreon temporary files
/tmp/centreon-setup exists, it will be moved...
Change macros for CentPlugins                                 OK
Installing the plugins                                        OK
Change right on centreon.conf                                 OK
CentPlugins is installed
```

Start CentPlugins Traps Installation.

```
-----------------------------------------------------------------------
        Start CentPlugins Traps Installation
-----------------------------------------------------------------------

Where is your SNMP configuration directory
default to [/etc/snmp]
>
/etc/snmp                                                     OK

Where is your SNMPTT binaries directory
default to [/usr/local/centreon/bin/]
>
/usr/local/centreon/bin/                                      OK
```

```
Finding Nagios group :                                    nagios
Finding Apache user :                                     apache
Preparing Centreon temporary files
/tmp/centreon-setup exists, it will be moved...
Change macros for CentPluginsTraps                        OK
Installing the plugins Trap binaries                      OK
Change macros for snmptrapd.conf                          OK
Change macros for snmptt.ini                              OK
Install : snmptrapd.conf                                  OK
Install : snmp.conf                                       OK
Install : snmptt.ini                                      OK
Install : snmptt                                          OK
Install : snmpttconvertmib                                OK
Create /etc/centreon/instCentPlugins.conf                 OK
hostname: Unknown host
```

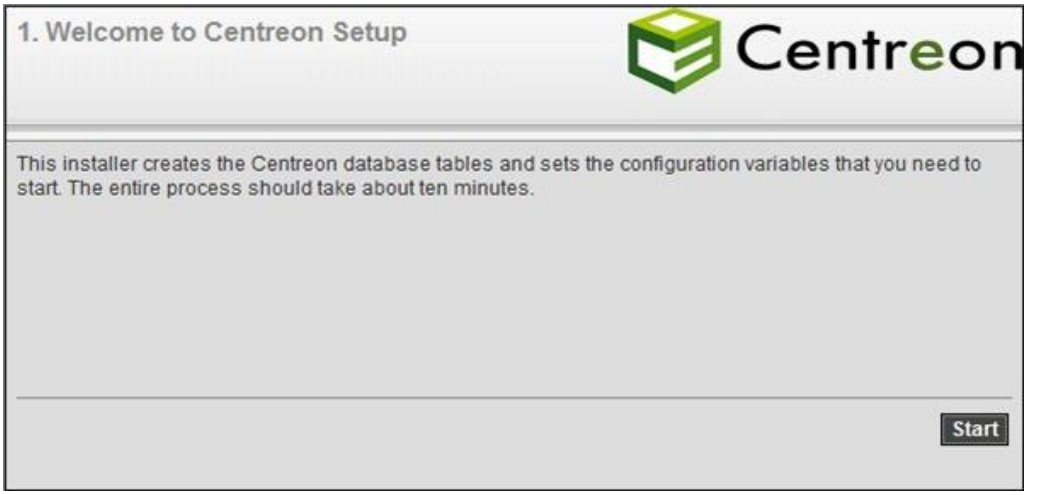
L'installazione termina con la visualizzazione della schermata seguente.

```
#################################################################################
####
#
   #
#                 Go to the URL : http:///centreon/                    #
#                            to finish the setup
   #
#
   #
#                  Report bugs at http://forge.centreon.com
   #
#
   #
#                         Thanks for using Centreon.
   #
#                          -----------------------
   #
#                        Contact : infos@centreon.com
   #
#                          http://www.centreon.com
   #
#
   #
#################################################################################
####
```

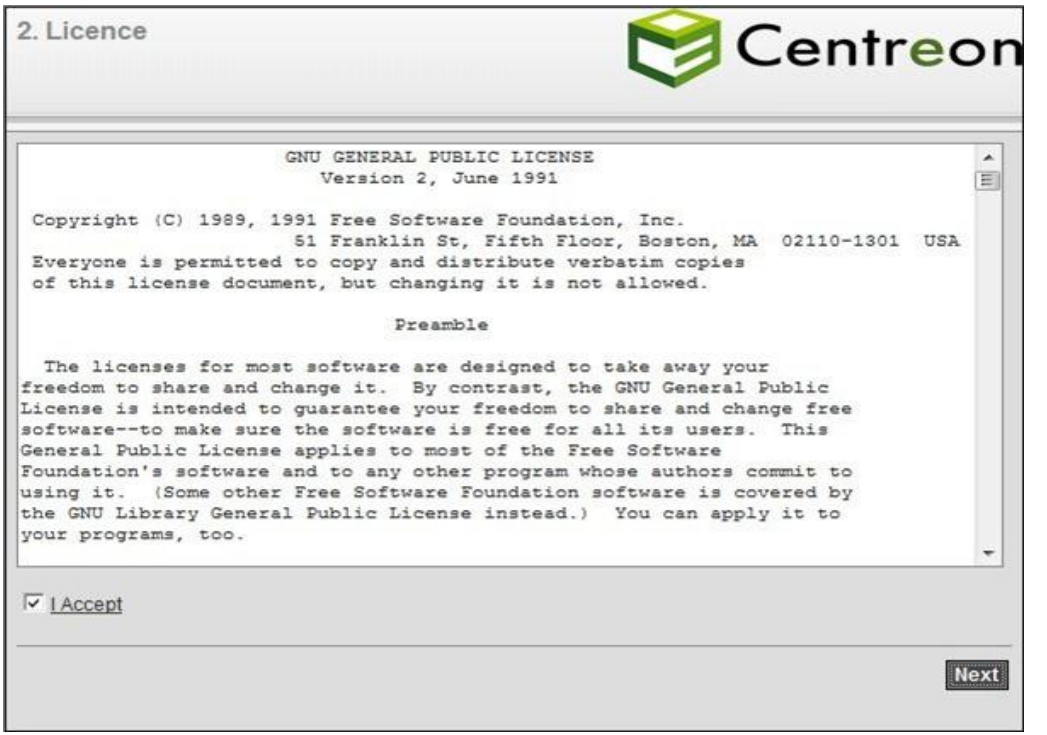
Configurazione di Centreon

Accedere alla configurazione web di *Centreon* digitando da browser l'indirizzo http://IP_Address/centreon.

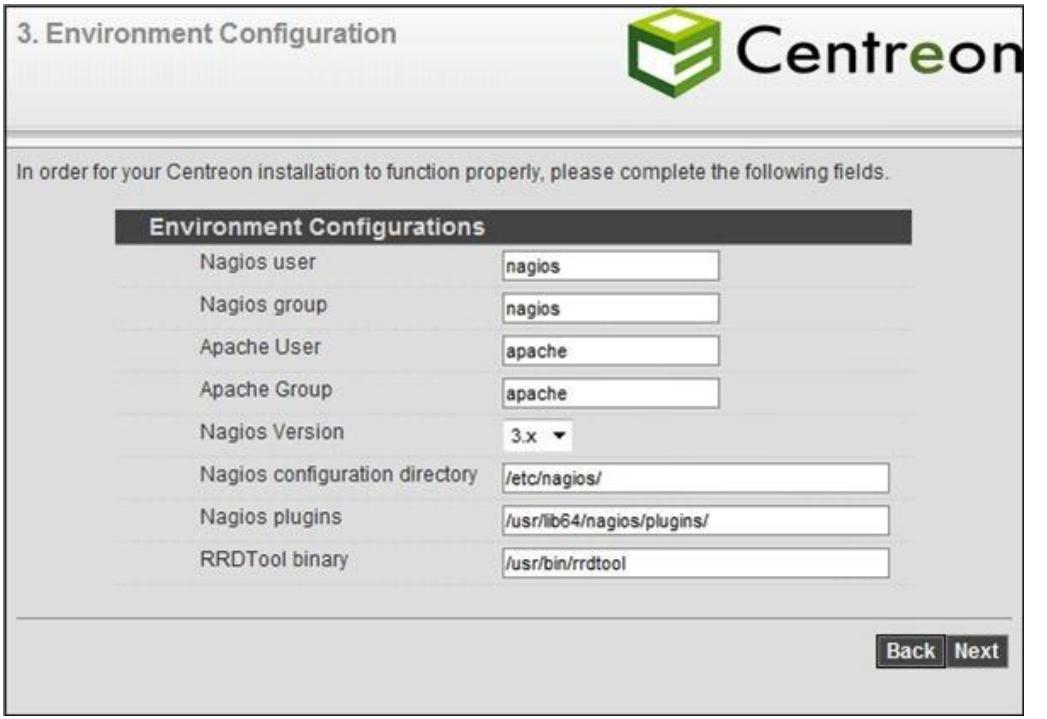
Cliccare su Start per iniziare.



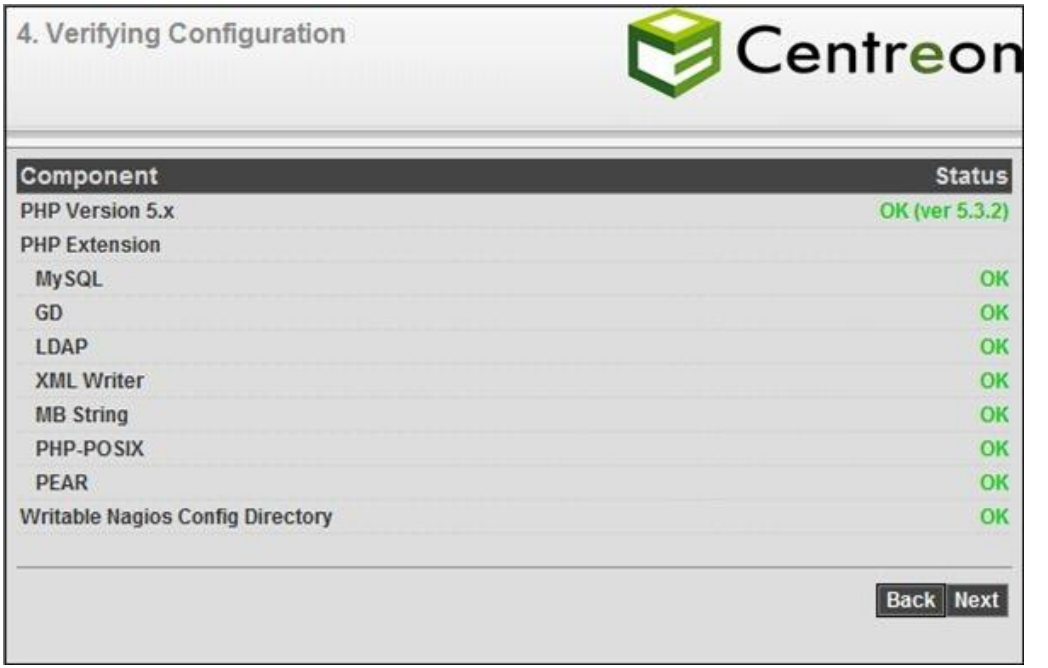
Accettare l'EULA.



Viene presentata la configurazione dell'ambiente mostrando parametri preimpostati presi dall'installazione precedentemente effettuata. Effettuare eventuali correzioni nel caso. Click su Next.



Viene effettuata una verifica della configurazione PHP. Se non ci sono errori, cliccare su Next.



Vengono analizzati i componenti PEAR. Se non sono segnalati errori, cliccare su Next.

5. Verifying PHP Pear Component

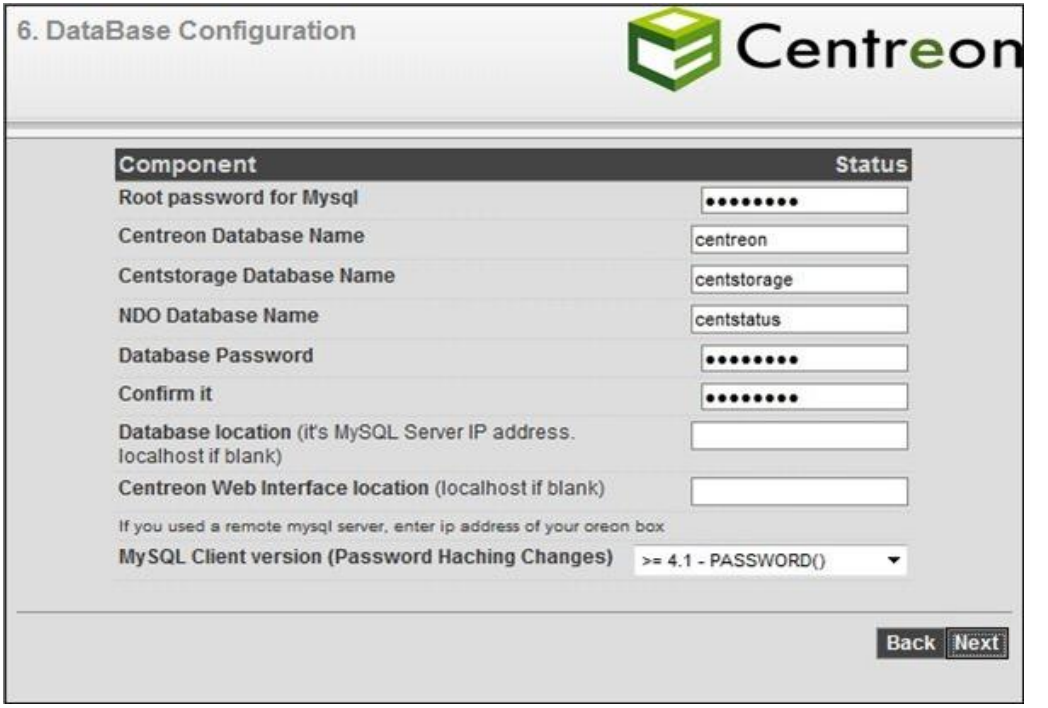
Centreon

Component	Status
PHP Pear Extension	
DB	OK
DB_DataObject	OK
DB_DataObject_FormBuilder	OK
MDB2	OK
Date	OK
HTML_Common	OK
HTML_QuickForm	OK
HTML_QuickForm_advmultiselect	OK
HTML_Table	OK
Archive_Tar	OK
Auth_SASL	OK
Console_Getopt	OK
Net_Socket	OK
Net_Traceroute	OK
Net_Ping	OK
Validate	OK
XML_RPC	OK
SOAP	OK

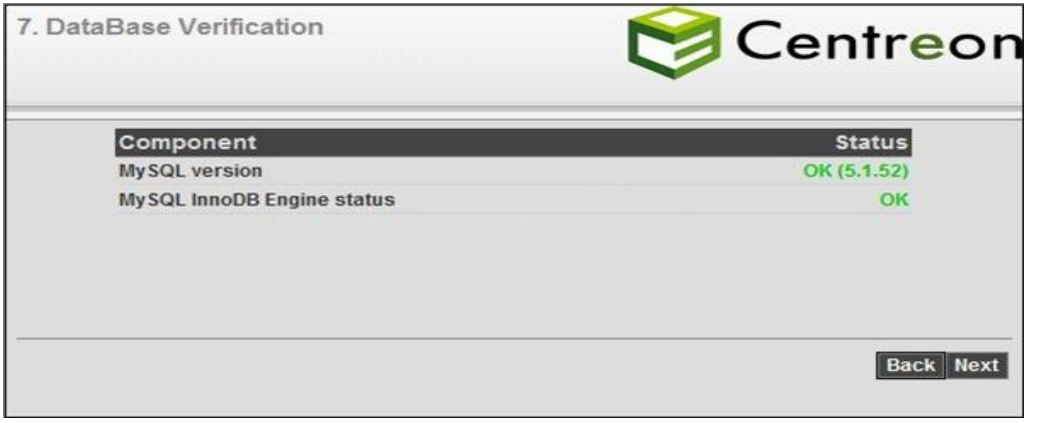
Back Next

Inserire i parametri richiesti per l'accesso ai database e cliccare su Next.

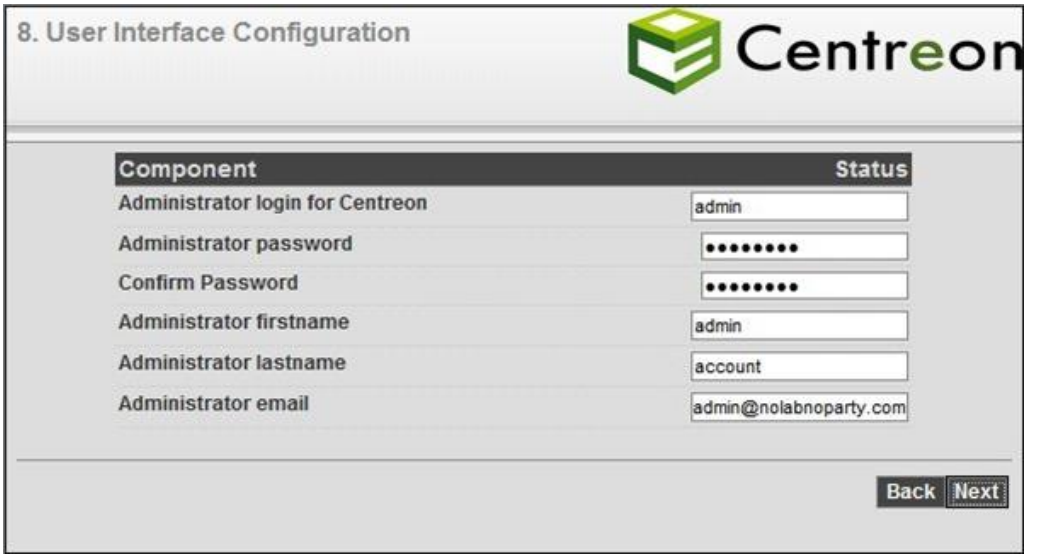
- Root password for MySQL: impostata durante l'installazione di MySQL.
- Database Password: impostare una password



Se le credenziali sono corrette, la verifica del database non mostra errori. Click su Next.

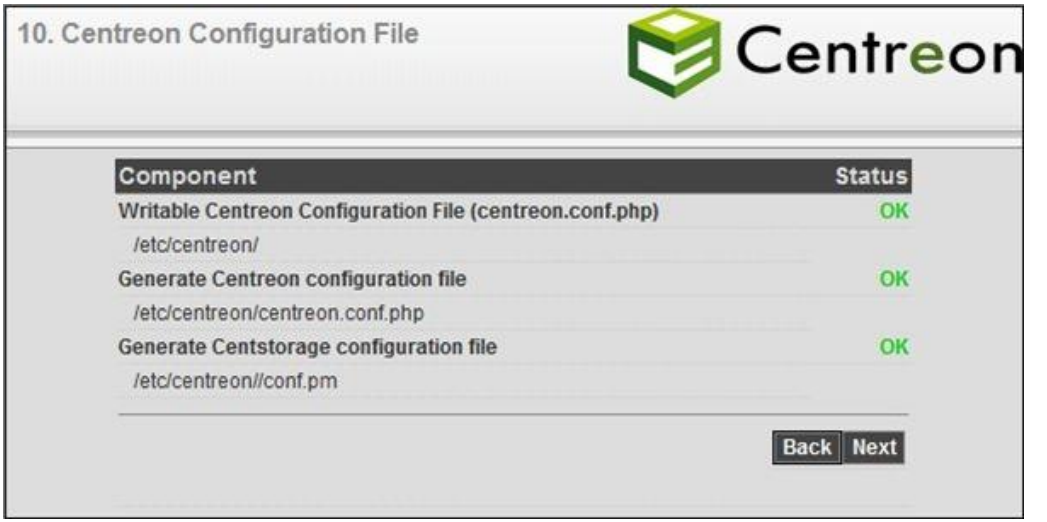


Impostare le credenziali per l'amministratore di Centreon e cliccare Next per proseguire.



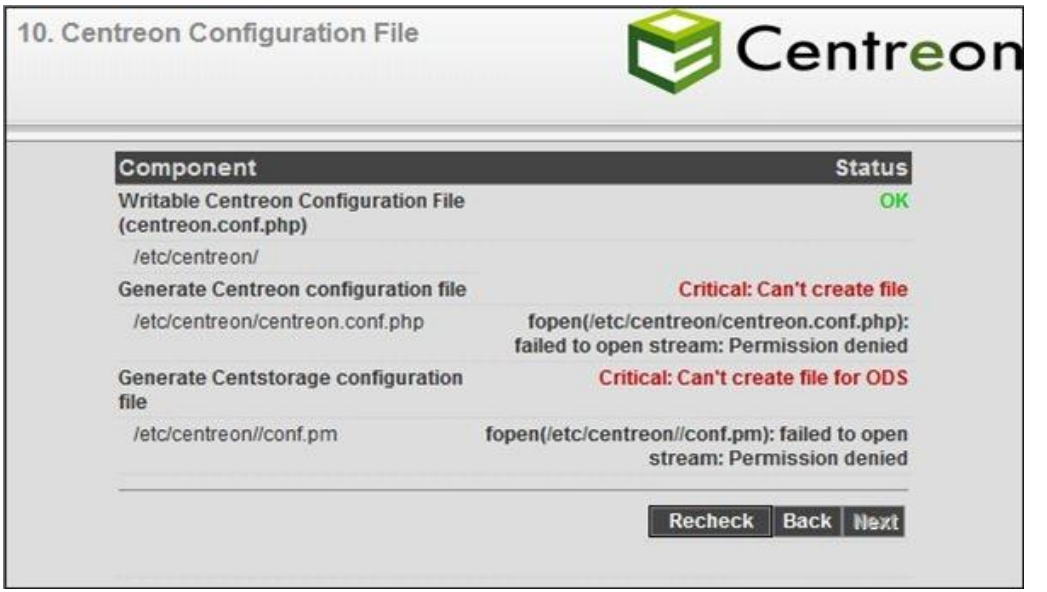
Abilitare l'autenticazione LDAP solo se richiesto dal proprio ambiente di rete. Click su Next.

Viene creato il file di configurazione di Centreon. Click su Next.

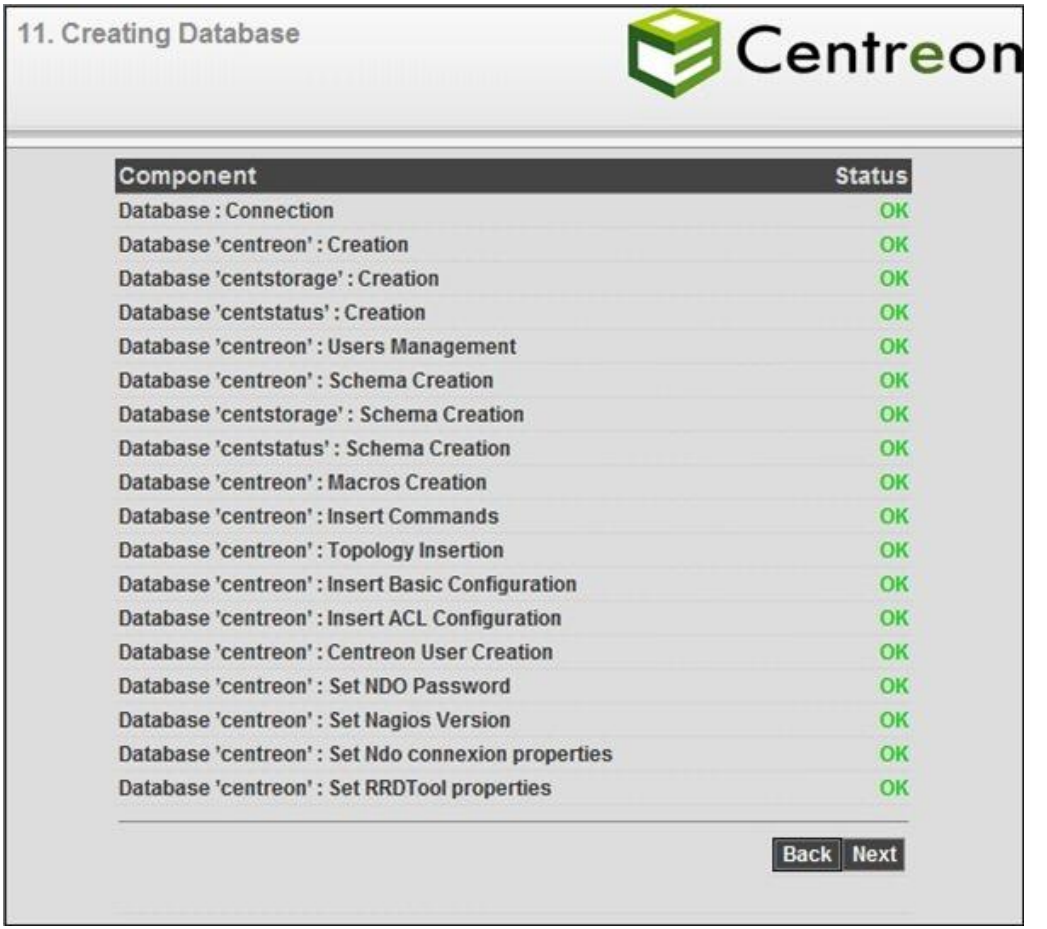


Nel caso venisse mostrata una videata con errori di creazione file (vedi figura), verificare che SELINUX sia stato disabilitato in */etc/sysconfig/selinux*. Per rendere la modifica operativa senza dover riavviare il sistema, digitare da console il comando:

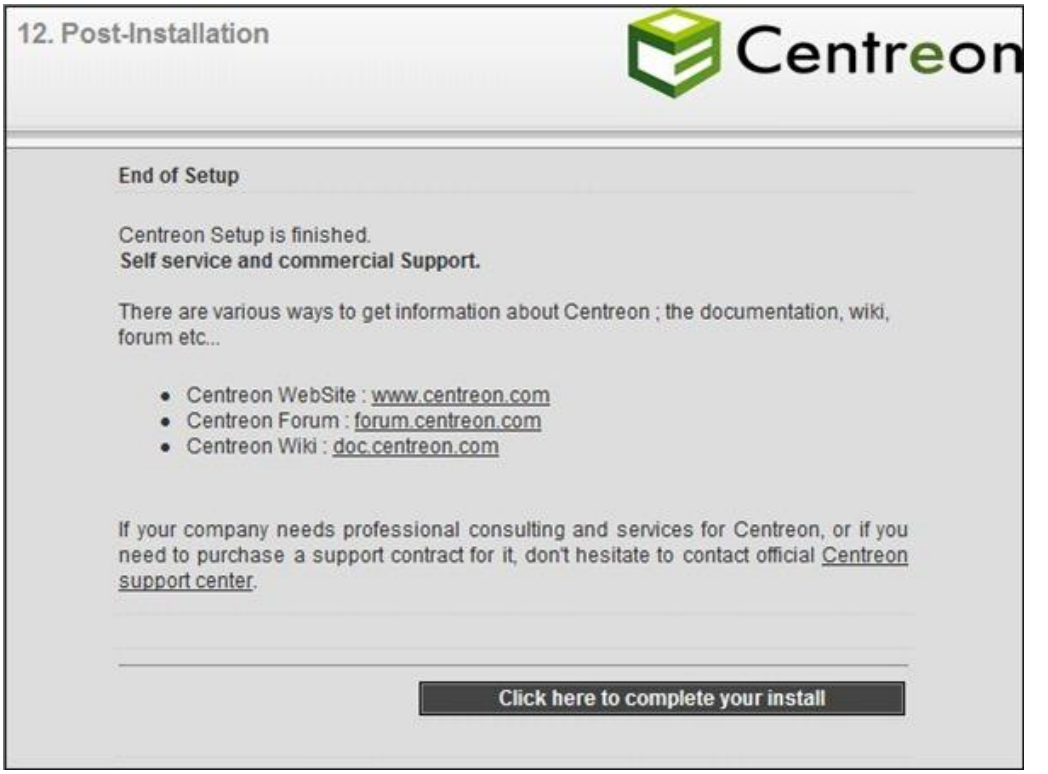
```
setenforce 0
```



Viene creato il database. Click su Next.

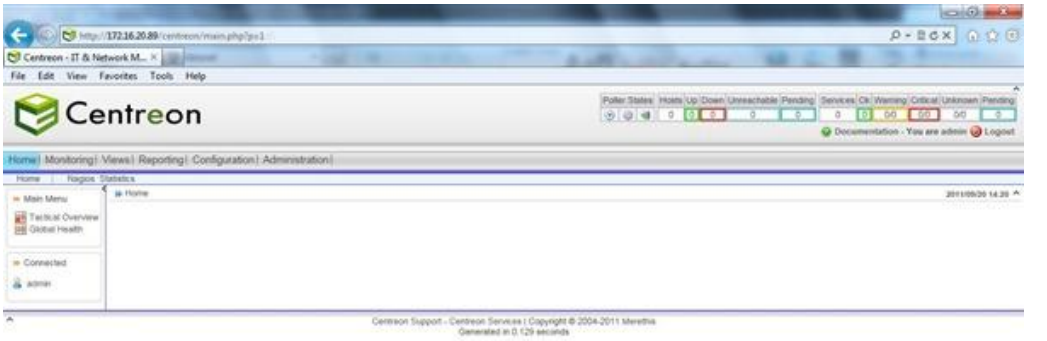


Terminata la configurazione viene presentata una schermata riepilogativa. Cliccare su Click here to complete your install.



La configurazione termina con la presentazione da parte del sistema della videata di login. Accedere come Administrator utilizzando le credenziali definite precedentemente e cliccare su Connect.

Si accede alla pagina principale di *Centreon*.



A questo punto non rimane che definire gli oggetti della rete da monitorare per avere il sistema operativo e funzionale.

Aggiornare Centreon

Per aggiornare Centreon 2.x ad una versione superiore, scaricare la nuova release, scompattarla e digitare da console il seguente comando:

```
# ./install.sh -u "/etc/centreon"
```

L'installazione dell'aggiornamento richiede pochi minuti e richiede di digitare Yes o No per alcuni parametri.

Monitorare server ESX(i) tramite plugin check_esx

check_esx3.pl è un plugin che permette di monitorare i componenti critici dei server ESX(i) tramite il sistema *Nagios*.

Per funzionare correttamente, il plugin necessita del package Perl-SDK di VMware e deve essere installato in un sistema in cui sia presente *Nagios*.

Procedura

Dal sito *VMware* scaricare VMware-vSphere-Perl-SDK versione 4.1 e copiarlo sul sistema di monitoraggio *Nagios*.

```
[root@nagios install]# ll
total 23572
-rw-r--r-- 1 root root 24109045 Nov 28 14:33 VMware-vSphere-Perl-SDK-4.1.0-
254719.i386.tar.gz
[root@nagios install]#
```

```
# tar -xzvf VMware-vSphere-Perl-SDK-4.1.0-254719.i386.tar.gz
# cd vmware-vsphere-cli-distrib
# ./vmware-install.pl
```

L'installazione inizia visualizzando l'EULA. E' necessario scorrerla tutta per procedere.

```
[root@nagios vmware-vsphere-cli-distrib]# ./vmware-install.pl
Creating a new vSphere CLI installer database using the tar4 format.

Installing vSphere CLI.

Installing version 254719 of vSphere CLI


You must read and accept the vSphere CLI End User License Agreement to
continue.
Press enter to display it.
```

Accettare l'EULA digitando yes e premere Invio.

```
terms is found to be invalid or unenforceable, the remaining terms will
continue to be valid and
enforceable to the fullest extent permitted by law.

rev10.24.08


Do you accept? (yes/no) yes
```

Accettare la directory predefinita */usr/bin* e premere Invio.

```
Do you accept? (yes/no) yes

Thank you.

In which directory do you want to install the executable files?
[/usr/bin]

Please wait while copying vSphere CLI files...

The installation of vSphere CLI 4.1.0 build-254719 for Linux completed
successfully. You can decide to remove this software from your system at an
y
time by invoking the following command:
"/usr/bin/vmware-uninstall-vSphere-CLI.pl".

This installer has successfully installed both vSphere CLI and the vSphere
SDK
for Perl.

Enjoy,

--the VMware team

[root@nagios vmware-vsphere-cli-distrib]#
```

Per poter utilizzare il plugin è necessario installare il componente Nagios::Plugin.
L'installazione è possibile farla tramite il comando *yum*.

```
# yum install perl-Nagios-Plugin
```

```
[root@nagios /]# yum install perl-Nagios-Plugin
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: centos.mirror.range-id.it
 * extras: centos.mirror.range-id.it
 * rpmforge: apt.sw.be
 * updates: centos.mirror.range-id.it
base                                                     | 1.1 kB     00:00
extras                                                   | 2.1 kB     00:00
extras/primary_db                                        | 171 kB     00:02
graphviz-stable                                          |  951 B     00:00
rpmforge                                                 | 1.1 kB     00:00
updates                                                  | 1.9 kB     00:00
updates/primary_db                                       | 304 kB     00:02
vmware-tools                                             |  951 B     00:00
Setting up Install Process
Resolving Dependencies
--> Running transaction check
---> Package perl-Nagios-Plugin.noarch 0:0.35-2.el5.rf set to be updated
--> Processing Dependency: perl(Class::Accessor::Fast) for package: perl-Na
gios-Plugin
--> Processing Dependency: perl(Math::Calc::Units) for package: perl-Nagios
-Plugin
```

Scaricare dal sito http://git.op5.org il plugin check_esx3.pl.

```
# wget
"http://git.op5.org/git/?p=nagios/op5plugins.git;a=snapshot;h=1fe4
ba671d29dcdf7c281b686ec39a291632ae4c;sf=tgz" -O check_esx3.pl
```

```
[root@nagios install]# wget "http://git.op5.org/git/?p=nagios/op5plugins.gi
t;a=snapshot;h=1fe4ba671d29dcdf7c281b686ec39a291632ae4c;sf=tgz" -O check_es
x3.pl
--2011-11-28 15:11:09--  http://git.op5.org/git/?p=nagios/op5plugins.git;a=
snapshot;h=1fe4ba671d29dcdf7c281b686ec39a291632ae4c;sf=tgz
Resolving git.op5.org... 193.201.96.29
Connecting to git.op5.org|193.201.96.29|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [application/x-gzip]
Saving to: `check_esx3.pl'

    [     <=>                          ] 195,962      193K/s   in 1.0s

2011-11-28 15:11:10 (193 KB/s) - `check_esx3.pl' saved [195962]

[root@nagios install]#
```

Rendere il file eseguibile tramite il comando *chmod*.

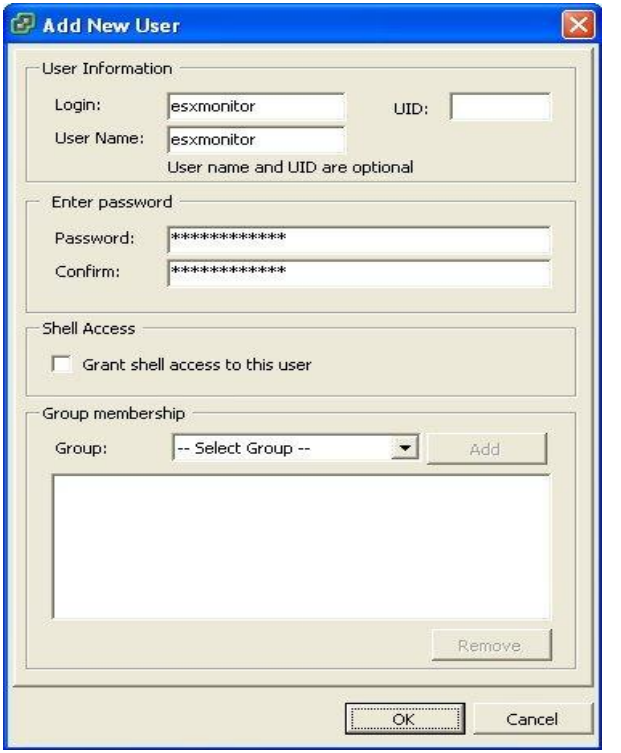
```
# chmod +x check_esx3.pl
```

Copiare il file nella directory */usr/lib/nagios/plugins*.

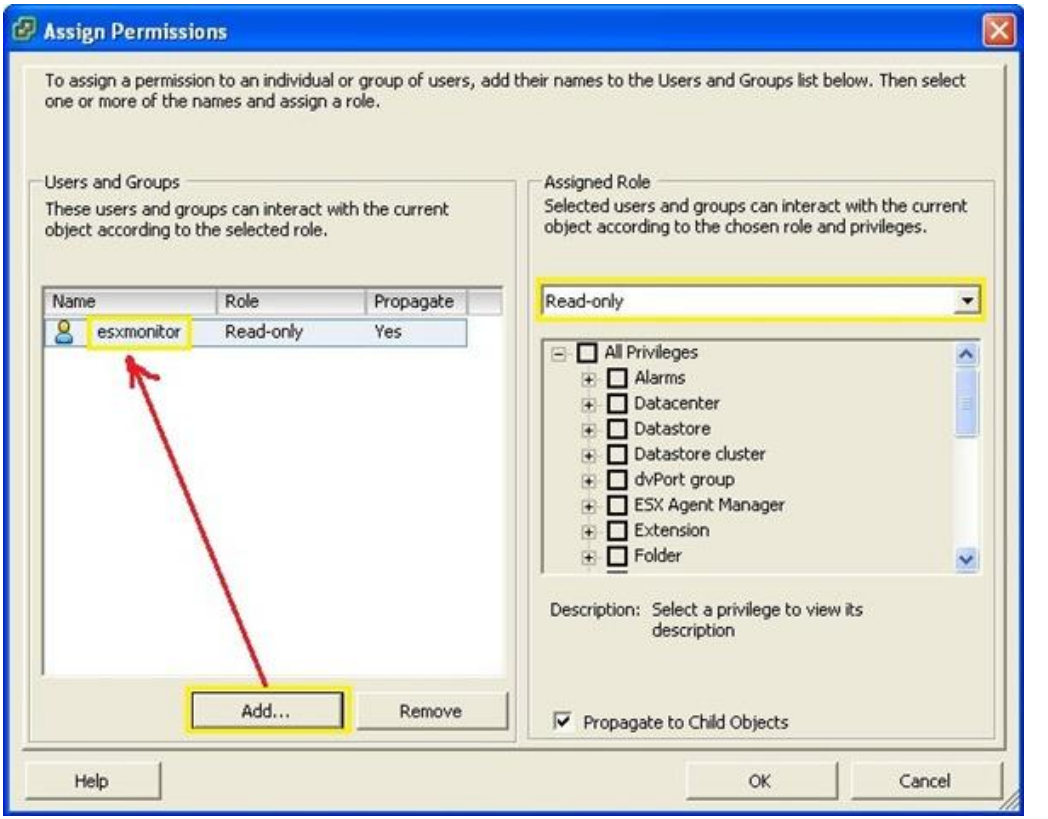
```
# cp check_esx3.pl /usr/lib/nagios/plugins/
```

```
[root@nagios install]# chmod +x check_esx3.pl
[root@nagios install]# ll
total 23772
-rwxr-xr-x  1 root root   195962 Nov 28 15:11 check_esx3.pl
drwxr-xr-x 10 root root     4096 Apr 29  2010 vmware-vsphere-cli-distrib
-rw-r--r--  1 root root 24109045 Nov 28 14:33 VMware-vSphere-Perl-SDK-4.1.0
-254719.i386.tar.gz
[root@nagios install]# cp check_esx3.pl /usr/lib/nagios/plugins/
[root@nagios install]#
```

Tramite vSphere Client –> Local Users & Groups, creare un utente che sarà utilizzato dal plugin per monitorare il sistema. Prestare attenzione al formato della password che richiede certi criteri di password complexity.



In vSphere Client –> Permissions, assegnare il ruolo di Read-only all'utente appena creato e cliccare su OK.



Per testare se il plugin funziona, digitare da console:

```
# cd /usr/lib/nagios/plugins
# ./check_esx3.pl -H IP_Address_ESX -u AccountMonitor -p Password
-l cpu -s usage -w 80 -c 90
```

```
[root@nagios plugins]# ./check_esx3.pl -H esxi1 -u monitor -p password -l cpu -s
usage -w 80 -c 90
CHECK_ESX3.PL OK - cpu usage=6.35 % | cpu_usage=6.35%;80;90
[root@nagios plugins]#
```

Testato che il plugin funziona correttamente, definire il comando check_esx in *Nagios* prestando attenzione alla sintassi. Editare il file */etc/nagios/resource.cfg* ed impostare le variabili dell'utente utilizzato dal plugin per accedere al server ESX(i).

```
USER2$=account
USER3$=password

# vi /etc/nagios/resource.cfg
```

```
$USER1$=/usr/lib/nagios/plugins
$USER2$=monitor
$USER3$=password
```

Per monitorare il carico della CPU, ad esempio, utilizzare la seguente sintassi:

```
$USER1$/check_esx3.pl -H $HOSTADDRESS$ -u $USER2$ -p $USER3$ -l
cpu -s usage -w $ARG1$ -c $ARG2$
```

```
define command{
        command_name    check_esx_cpu
        command_line    $USER1$/check_esx3.pl -H $HOSTADDRESS$ -u $USER2$ -
p $USER3$ -l cpu -s usage -w $ARG1$ -c $ARG2$
}
```

Alcuni esempi di configurazione:

disk

```
command_name check_esx_disk

command_line $USER1$/check_esx3.pl -H $HOSTADDRESS$ -u $USER2$ -p
$USER3$ -l vmfs -w $ARG1$ -c $ARG2$
```

ram

```
command_name check_esx_ram

command_line $USER1$/check_esx3.pl -H $HOSTADDRESS$ -u $USER2$ -p
$USER3$ -l mem -s usagemb -w $ARG1$ -c $ARG2$
```

swap

```
command_name check_esx_swap

command_line $USER1$/check_esx3.pl -H $HOSTADDRESS$ -u $USER2$ -p
$USER3$ -l mem -s swap -w $ARG1$ -c $ARG2$
```

status

```
command_name check_esx_status
command_line $USER1$/check_esx3.pl -H $HOSTADDRESS$ -u $USER2$ -p
$USER3$ -l runtime -s status
```

nic

```
command_name check_esx_nic
command_line $USER1$/check_esx3.pl -H $HOSTADDRESS$ -u $USER2$ -p
$USER3$ -l net -s nic
```

issues

```
command_name check_esx_issues
command_line $USER1$/check_esx3.pl -H $HOSTADDRESS$ -u $USER2$ -p
$USER3$ -l runtime -s issues
```

Altri parametri di configurazione sono disponibili nel sito op5.com.

Configurati i parametri da monitorare, Nagios è in grado di visualizzare lo stato del server ESX(i) specificato.

esxi1	CPU	OK	CHECK_ESX3.PL OK - cpu usage=4.69 %
	Disk	OK	CHECK_ESX3.PL OK - Storages : esxi1-local-storage=68385.00 MB (33.39%)
	Issues	OK	CHECK_ESX3.PL OK - No config issues
	Memory	OK	CHECK_ESX3.PL OK - mem usage=4437.82 MB
	Nic	OK	CHECK_ESX3.PL OK - All 2 NICs are connected
	Ping	OK	OK - esxi1: rta 0.093ms, lost 0%
	Status	OK	CHECK_ESX3.PL OK - overall status=green
	Swap	OK	CHECK_ESX3.PL OK - swap usage=0.00 MB

Un plugin molto comodo che permette di tenere sotto controllo i server ESX(i) diventati ormai i core system in molte aziende.

Monitorare AS/400 con Nagios in CentOS

Nagios è uno dei più efficienti sistemi di monitoraggio rete ma necessita di plugin dedicati per monitorare sistemi specifici come l'AS/400.

Per monitorare l'*AS/400* esiste il plugin check_as400 che opportunamente configurato permette di rilevare lo stato di alcune componenti di questo sistema.

Prerequisiti

Per il corretto funzionamento del plugin, sono necessari tre requisitifondamentali:

Sistema di monitoraggio basato su *Nagios*.

Bisogna creare un utente generico nel sistema *AS/400* con permessi limitati per permettere l'accesso del plugin al sistema. Come riportato dall'autore del plugin, l'utente deve avere accesso a WRKSYSSTS, WRKOUTQ, WRKACTJOB, DSPJOB, DSPSBSD e DSPMSG.

Poichè il plugin è scritto in Java, nel sistema va installata la versione JRE.

Procedura

Scaricare dal sito Oracle la versione JRE 6 di Java e copiarla nel sistema. La versione attualmente disponibile è la Java SE 6 Update 29. Se viene scaricata la versione autoinstallante jre-6u29-linux-i586-rpm.bin. , rendere il file eseguibile tramite il comando *chmod*.

```
# chmod +x jre-6u29-linux-i586-rpm.bin
```

```
[root@nagios install]# ll
total 20616
-rw-r--r-- 1 root root 21080374 Nov 29 11:46 jre-6u29-linux-i586-rpm.bin
[root@nagios install]# chmod +x jre-6u29-linux-i586-rpm.bin
[root@nagios install]# ll
total 20616
-rwxr-xr-x 1 root root 21080374 Nov 29 11:46 jre-6u29-linux-i586-rpm.bin
[root@nagios install]#
```

Procedere con l'installazione di Java.

```
# ./jre-6u29-linux-i586-rpm.bin
```

```
[root@nagios install]# ./jre-6u29-linux-i586-rpm.bin
Unpacking...
Checksumming...
Extracting...
UnZipSFX 5.50 of 17 February 2002, by Info-ZIP (Zip-Bugs@lists.wku.edu).
  inflating: jre-6u29-linux-i586.rpm
Preparing...                ########################################### [10
0%]
   1:jre                    ########################################### [10
0%]
Unpacking JAR files...
        rt.jar...
        jsse.jar...
        charsets.jar...
        localedata.jar...
        plugin.jar...
        javaws.jar...
        deploy.jar...

Done.
[root@nagios install]#
```

Scaricare il plugin da SourceForge e scompattare il file nel sistema.

```
# tar -xzvf as400NagiosPlugin-018.gz
```

```
[root@nagios install]# tar -xzvf as400NagiosPlugin-018.gz
as400NagiosPlugin/
as400NagiosPlugin/check_as400.class
as400NagiosPlugin/check_as400.java
as400NagiosPlugin/check_as400_cmd_vars.class
as400NagiosPlugin/THANKS
as400NagiosPlugin/README
as400NagiosPlugin/install
as400NagiosPlugin/check_as400
```

Creare la directory */usr/lib/nagios/plugins/check_as400* e copiare i file *.class e check_as400 presenti nella directory scompattata del plugin nella nuova directory.

```
# mkdir /usr/lib/nagios/plugins/check_as400
# cd as400NagiosPlugin
# cp *.class /usr/lib/nagios/plugins/check_as400/
# cp check_as400 /usr/lib/nagios/plugins/check_as400/
```

```
[root@nagios as400NagiosPlugin]# cp *.class /usr/lib/nagios/plugins/check_as400/
[root@nagios as400NagiosPlugin]# cp check_as400 /usr/lib/nagios/plugins/check_as
400/
[root@nagios as400NagiosPlugin]#
```

Creare nella directory */usr/lib/nagios/plugins/check_as400/* il file nascosto .as400 dove memorizzare l'utente e la password dell'utente *AS400*.

```
# cd /usr/lib/nagios/plugins/check_as400/
# vi .as400
```

Aggiungere utente e password come indicato:

USER=*account_AS400*
PASS=*password_AS400*

```
USER=account_as400
PASS=password_as400
```

Restringere i diritti di accesso al file *.as400* precedentemente creato.

```
# chmod 700 /usr/lib/nagios/plugins/check_as400/.as400
```

Assegnare l'ownership della directory */usr/lib/nagios/plugins/check_as400/* all'account nagios.

```
# chown -R nagios.nagios /usr/lib/nagios/plugins/check_as400/
```

Editare il file */usr/lib/nagios/plugins/check_as400/check_as400* e verificare ed eventualmente modificare i path di sistema.

Originale

USER=`cat ~~/usr/nagios/libexec/~~.as400 |grep -e USER | cut -d = -f 2`
PASS=`cat ~~/usr/nagios/libexec/~~.as400 |grep -e PASS | cut -d = -f 2`
*~~/usr/lib/java/bin/~~java -cp ~~/usr/nagios/libexec~~ check_as400 -u $USER -p $PASS $**

CentOS

USER=`cat /usr/lib/nagios/plugins/check_as400/.as400 |grep -e USER | cut -d = -f 2`
PASS=`cat /usr/lib/nagios/plugins/check_as400/.as400 |grep -e PASS | cut -d = -f 2`
*/usr/java/jre1.6.0_29/bin/java -cp /usr/lib/nagios/plugins/check_as400 check_as400 -u $USER -p $PASS $**

```
USER=`cat /usr/lib/nagios/plugins/check_as400/.as400 |grep -e USER | cut -d = -f
 2`
PASS=`cat /usr/lib/nagios/plugins/check_as400/.as400 |grep -e PASS | cut -d = -f
 2`
/usr/java/jre1.6.0_29/bin/java -cp /usr/lib/nagios/plugins/check_as400 check_as4
00 -u $USER -p $PASS $*
```

Testare il plugin

Terminata l'installazione e configurazione, non resta che testare il plugin per verificare se il tutto funziona correttamente.

Per testare manualmente la funzionalità, da console digitare l'istruzione seguente per verificare se il plugin riesce a logarsi al sistema *AS/400*.

```
# ./check_as400 -H as400 -v LOGIN
```

```
[root@nagios check_as400]# ./check_as400 -H as400 -v LOGIN
OK - Login completed successfully
[root@nagios check_as400]#
```

Un altro test è verificare il carico della CPU.

```
# ./check_as400 -H as400 -v CPU -w 80 -c 90
```

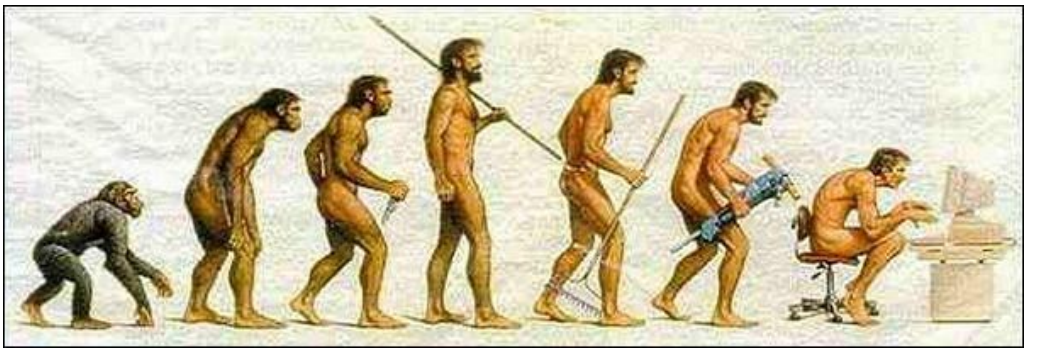
```
[root@nagios check_as400]# ./check_as400 -H as400 -v CPU -w 80 -c 90
OK - CPU Load (0.4%)
[root@nagios check_as400]#
```

Configurato con i parametri *AS/400* da monitorare, il sistema Nagios visualizzerà il risultato dei controlli tramite *check_as400*. Esempi di configurazione sono presenti in *services.example e checkcommands.example* all'interno del file compresso del plugin in.

as400	IBM	Active-Jobs	OK	30-11-2011 11:56:57	0d 0h 11m 46s	1/3	OK - 310 active jobs in system
		CPU	OK	30-11-2011 11:58:05	0d 0h 10m 38s	1/3	OK - CPU Load (4%)
		DB	OK	30-11-2011 11:58:11	0d 0h 14m 22s	1/3	OK - DB Load (0%)
		Disk	OK	30-11-2011 11:55:36	0d 0h 13m 7s	1/3	OK - 96.63 G (54.97%) free of 175,8 G
		Jobs	OK	30-11-2011 11:56:51	0d 0h 11m 52s	1/3	OK - 4485 jobs in system
		Login	OK	30-11-2011 11:58:06	0d 0h 10m 37s	1/3	OK - Login completed successfully
		Ping	OK	30-11-2011 11:54:18	1d 5h 16m 4s	1/3	OK - as400: rta 0.367ms, lost 0%

Il sistema *AS/400* può essere adesso monitorato per prevenire eventuali malfunzionamenti evitando blocchi potenzialmente pericolosi per il business aziendale.

Monitorare i security updates per CentOS 5.x tramite check_yum



Nelle reti moderne i sistemi Linux sono fortemente presenti e anche loro necessitano di essere costantemente aggiornati.

Per monitorare lo stato degli aggiornamenti tramite *Nagios*, è necessario utilizzare un plugin specifico chiamato check_yum.

Prerequisiti

Il plugin richiede la presenza del sistema ***Nagios*** e prevede l'installazione nella macchina da monitorare di due package:

- Sistema *Nagios* operativo
- nagios-nrpe
- yum-security

Procedura

Tramite il comando *yum*, installare il package yum-security e nagios-nrpe (disponibili nel repository *rpmforge*). *yum-security* è disponibile solo per la versione 5.x di CentOS.

```
# yum install yum-security nagios-nrpe
```

```
[root@vm-lx5-mysql ~]# yum install yum-security nagios-nrpe
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: ftp.eutelia.it
 * extras: mirror.fraunhofer.de
 * rpmforge: apt.sw.be
 * updates: swissmirror.silyus.net
base                                                     | 1.1 kB     00:00
extras                                                   | 2.1 kB     00:00
extras/primary_db                                        | 171 kB     00:00
rpmforge                                                 | 1.1 kB     00:00
updates                                                  | 1.9 kB     00:00
updates/primary_db                                       | 397 kB     00:02
Setting up Install Process
Resolving Dependencies
--> Running transaction check
---> Package nagios-nrpe.i386 0:2.12-1.el5.rf set to be updated
--> Processing Dependency: nagios-plugins for package: nagios-nrpe
---> Package yum-security.noarch 0:1.1.16-16.el5.centos set to be updated
```

Scaricare il plugin check_yum dal sito http://exchange.nagios.org/directory/Plugins/Uncategorized/Operating-Systems/Linux/Check_Yum/details ed assegnare i permessi di esecuzione.

```
# chmod 755 check_yum
```

```
[root@vm-lx5-mysql install]# chmod 755 check_yum
[root@vm-lx5-mysql install]# ll
total 24
-rwxr-xr-x 1 admin admin 21816 Dec 13 11:47 check_yum
[root@vm-lx5-mysql install]#
```

Copiare il file *check_yum* nella directory */usr/lib/nagios/plugins*.

```
# cp check_yum /usr/lib/nagios/plugins
```

```
[root@vm-lx5-mysql install]# cp check_yum /usr/lib/nagios/plugins/
[root@vm-lx5-mysql install]# ll /usr/lib/nagios/plugins/check_yum
-rwxr-xr-x 1 root root 21816 Dec 13 15:49 /usr/lib/nagios/plugins/check_yum
[root@vm-lx5-mysql install]#
```

Editare il file nrpe.cfg ed aggiungere l'istruzione:

command[check_yum]=/usr/lib/nagios/plugins/check_yum

```
# vi /etc/nagios/nrpe.cfg
```

```
# The following examples use hardcoded command arguments...
command[check_users]=/usr/lib/nagios/plugins/check_users -w 5 -c 10
command[check_load]=/usr/lib/nagios/plugins/check_load -w 15,10,5 -c 30,25,20

# Yum updates
command[check_yum]=/usr/lib/nagios/plugins/check_yum

# Disk 1
command[check_sda1]=/usr/lib/nagios/plugins/check_disk -w 20% -c 10% -p /dev/sda
1
```

Rendere il servizio *nrpe* avviabile al boot e riavviarlo per acquisire le nuove impostazioni.

```
# chkconfig nrpe on
# service nrpe restart
```

```
[root@vm-lx5-mysql /]# service nrpe restart
Shutting down Nagios NRPE daemon (nrpe):                   [  OK  ]
Starting Nagios NRPE daemon (nrpe):                        [  OK  ]
[root@vm-lx5-mysql /]#
```

Dal sistema da monitorare, testare che il plugin *check_yum* funzioni.

```
[root@vm-lx5-mysql plugins]# ./check_yum
YUM OK: 0 Security Updates Available
[root@vm-lx5-mysql plugins]#
```

Effettuare un test manuale anche da *Nagios*.

```
[root@nagios plugins]# ./check_nrpe -H vm-lx5-mysql -c check_yum
YUM OK: 0 Security Updates Available
[root@nagios plugins]#
```

Configurare ***Nagios*** per rendere operativo il plugin definendo il comando:

command_name nrpe_check_yum
command_line $USER1$/check_nrpe -H $HOSTADDRESS$ -c check_yum

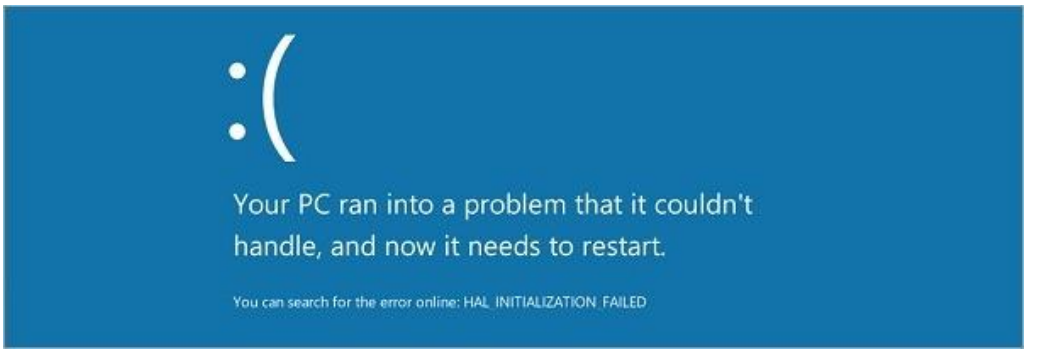
```
define command{
        command_name                    nrpe_check_yum
        command_line                    $USER1$/check_nrpe -H $HOSTADDRESS$ -c c
heck_yum
}
```

Il sistema di monitoraggio è adesso in grado di visualizzare lo stato dei security updates.

vm-lx5-mysql	Memory	OK	Total memory used : 4% ram used : 85%, swap used 1%
	Ping	OK	OK - vm-lx5-mysql: rta 7.962ms, lost 0%
	Security Updates	OK	YUM OK: 0 Security Updates Available. 1 Non-Security Update Available

Con questa implementazione il servizio di monitoraggio fornisce un'informazione in più utile a migliorare la manutenzione dei sistemi.

Monitorare i log di Windows con Nagios tramite check_logfiles



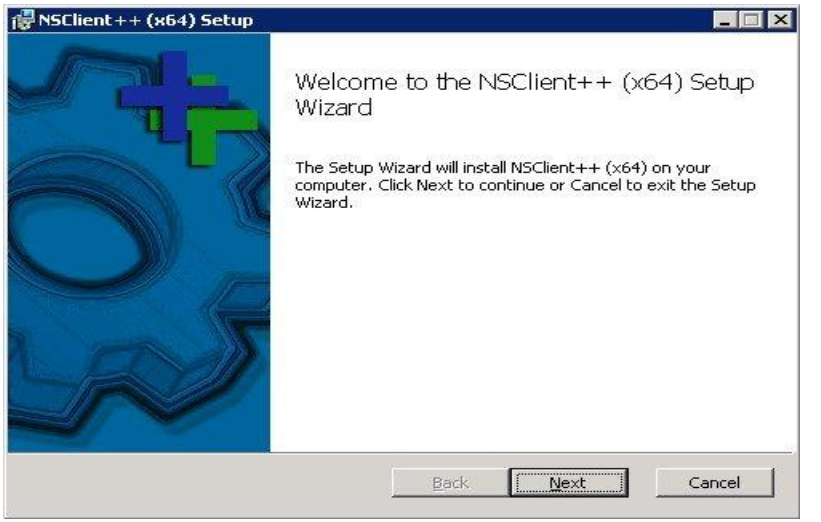
Monitorare i log di *Windows* soprattutto gestendo numerosi server è utile per ridurre al minimo eventuali spiacevoli sorprese.

Affidandoci come sempre al sistema *Nagios*, il monitoraggio dei log di *Windows* viene effettuato da un plugin chiamato check_logfiles sviluppato da ConSol Lab.

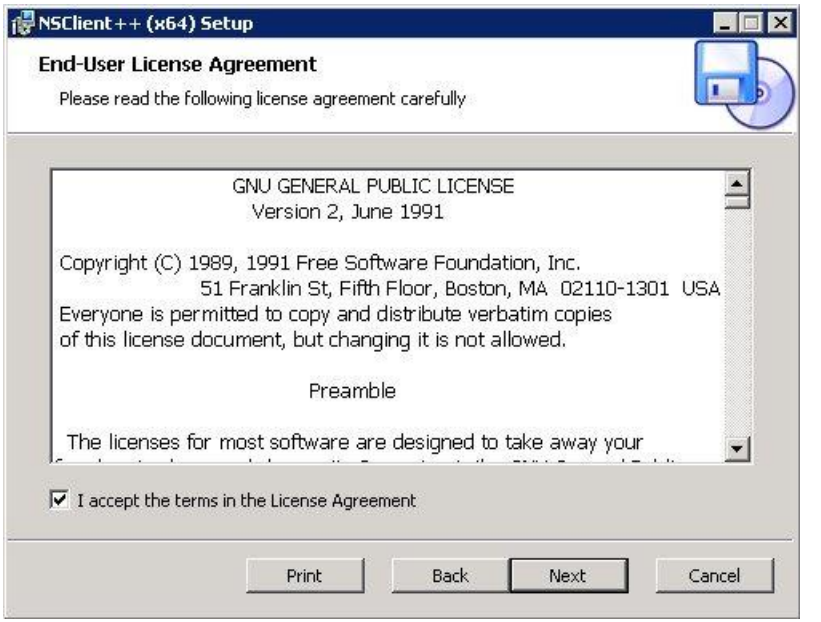
Procedura

Effettuare il download dell'addon NSClient++.

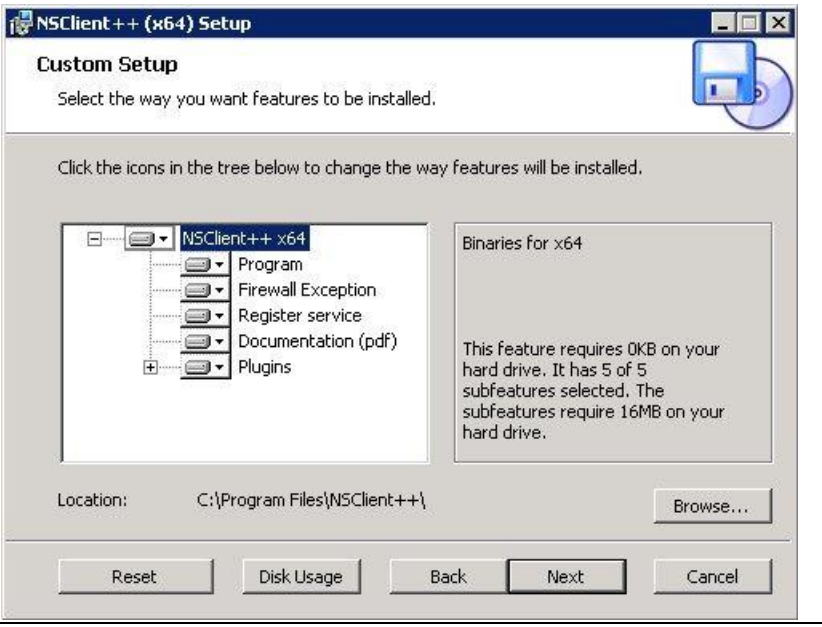
Copiare il file nel server da monitorare e lanciare l'esecuzione. Click Next per continuare.



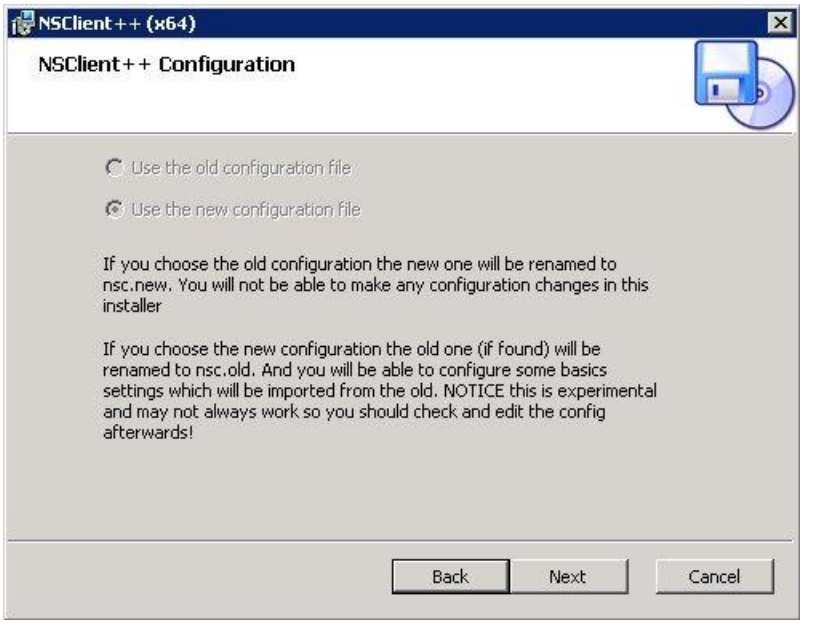
Accettare l'EULA e cliccare su Next.



Modificare le opzioni di installazione in caso di necessità e cliccare Next per proseguire.



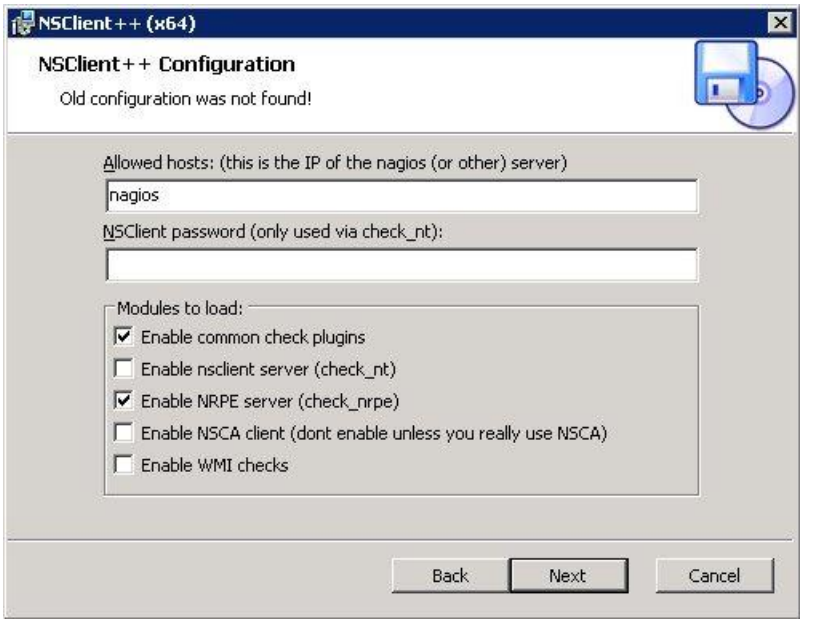
Se non è presente nessuna precedente installazione, viene creato un nuovo file di configurazione. Cliccare su Next per continuare.



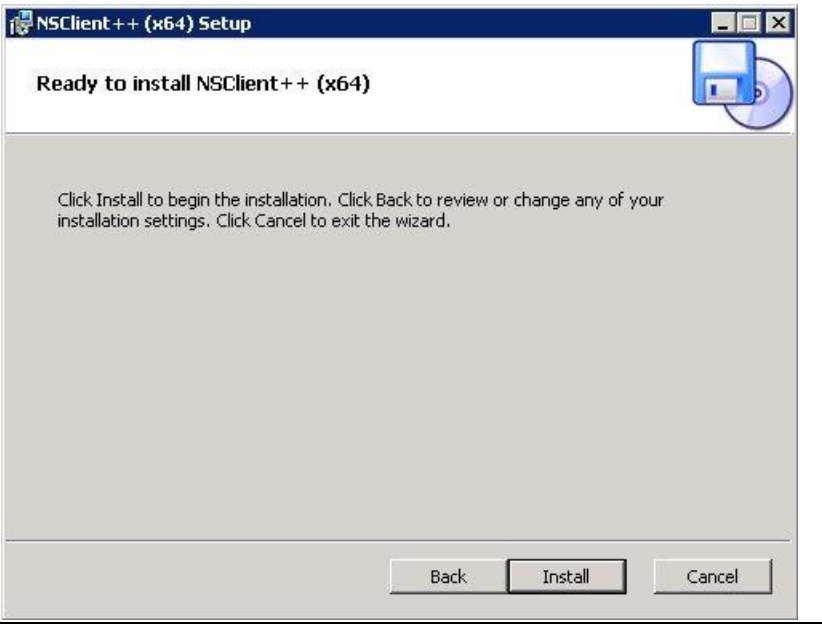
Specificare l'IP o hostname di *Nagios* utilizzato per monitorare il server ed abilitare i moduli:

Enable common check plugin
Enable NRPE server (check_nrpe)

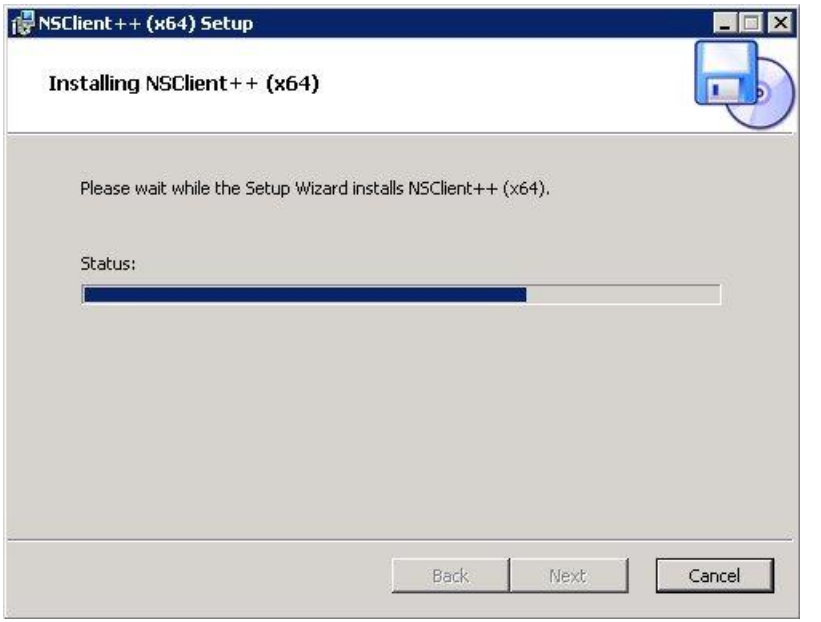
Cliccare Next per proseguire.



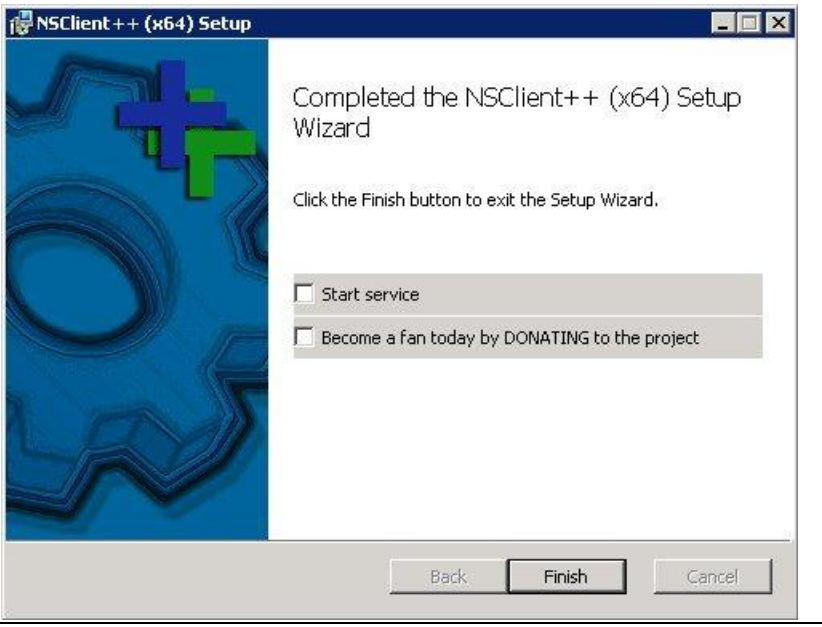
Configurati i vari parametri, cliccare Install per effettuare l'installazione.



La schermata mostra lo status dell'installazione.



Terminata la procedura, cliccare Finish senza abilitare l'opzione Start service.



Durante l'installazione, vengono automaticamente aperte nel firewall di *Windows* le porte TCP e UDP necessarie per permettere il corretto funzionamento.

Editare il file *C:\Program Files\NSClient++\NCS.ini*.

Modificare i parametri come indicato:

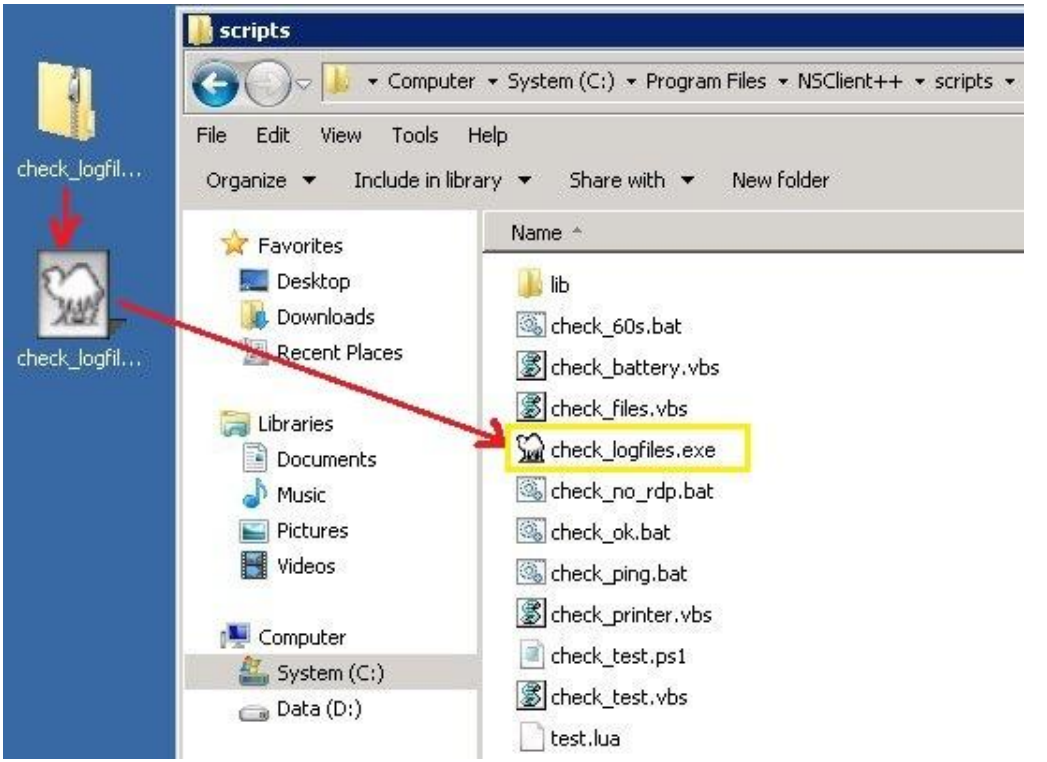
CheckExternalScripts.dll (rimuovere ";")
allow_arguments=1 (impostare il valore a 1)

aggiungere le righe:

[NRPE Handlers]
check_logfiles=scripts\check_logfiles.exe -f scripts\check_logfiles.cfg

```
1  [modules]
2  NRPEListener.dll
3  NSClientListener.dll
4  FileLogger.dll
5  CheckSystem.dll
6  CheckDisk.dll
7  CheckEventLog.dll
8  CheckHelpers.dll
9  ;SysTray.dll
10 ;CheckWMI.dll
11
12 ; Script to check external scripts and/or internal aliases.
13 CheckExternalScripts.dll
14
15 [Settings]
16 ;# ALLOWED HOST ADDRESSES
17 allowed_hosts=nagios
18
19 ;# USE THIS FILE
20 use_file=1
21
22
23 [NRPE]
24 ;# COMMAND ARGUMENT PROCESSING
25 allow_arguments=1
26
27
28 [NRPE Handlers]
29 check_logfiles=scripts\check_logfiles.exe -f scripts\check_logfiles.cfg
30
31
```

Scaricare il plugin check_logfiles dal sito http://labs.consol.de/wp-content/uploads/2011/11/check_logfiles-3.4.5.2.zip, scompattarlo estraendo il file eseguibile e copiarlo in *C:\Program Files\NSClient++\scripts*.



Creare un file di tipo .txt e rinominarlo in check_logfiles.cfg. Editare il file con Notepad o programmi simili.

All'interno di questo file è contenuta la configurazione del plugin.

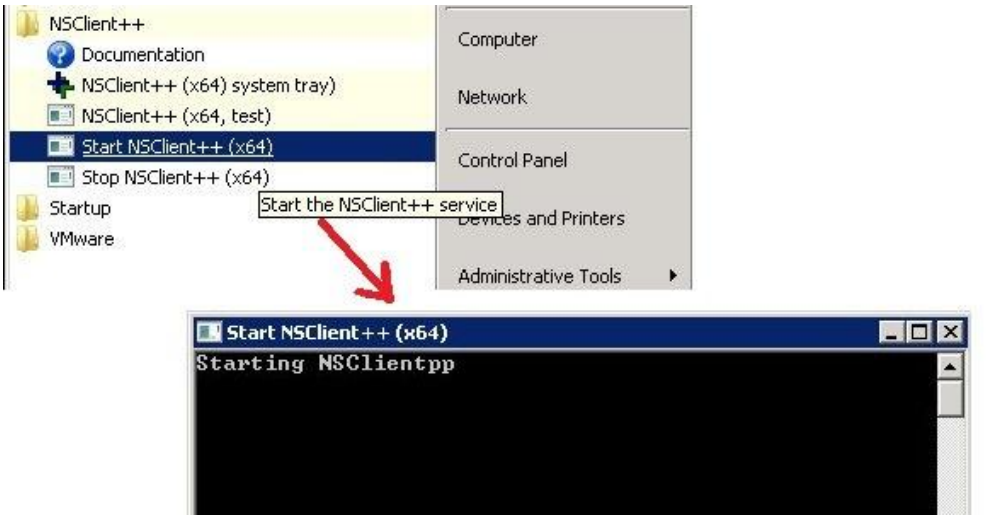
Per ricevere gli alert di tipo Critical, Error, Warning, aggiungere le seguenti righe:

```
@searches = ({
    tag => 'evt_sys',
    type => 'eventlog',
    options => 'winwarncrit',
});
```

```
1  @searches = ({
2    tag => 'evt_sys',
3    type => 'eventlog',
4    options => 'winwarncrit',
5  });
```

Per ulteriori informazioni sui parametri di configurazione, fare riferimento al sito del plugin.

Avviare il servizio *NSClient* da da Start –> All Programs –> NSClient++.



Per testare manualmente il plugin dal server da monitorare, dal *Command Prompt* digitare l'istruzione:

```
C:\> cd \Program Files\NSClient++

C:\Program Files\NSClient++> scripts\check_logfiles.exe -f
scripts\check_logfiles.cfg
```

```
Administrator: Command Prompt
C:\Program Files\NSClient++>scripts\check_logfiles.exe -f scripts\check_logfiles
.cfg
OK - no errors or warnings|evt_sys_lines=0 evt_sys_warnings=0 evt_sys_criticals=
0 evt_sys_unknowns=0

C:\Program Files\NSClient++>_
```

Per fare in modo che il plugin legga tutto il log ("*allyoucaneat*"), aggiungere l'opzione -reset per resettare i dati nel seekfile.

```
C:\Program Files\NSClient++> scripts\check_logfiles.exe -f
scripts\check_logfiles.cfg -reset
```

```
Administrator: Command Prompt
C:\Program Files\NSClient++>scripts\check_logfiles.exe -f scripts\check_logfiles
.cfg
OK - no errors or warnings|evt_sys_lines=0 evt_sys_warnings=0 evt_sys_criticals=
0 evt_sys_unknowns=0

C:\Program Files\NSClient++>scripts\check_logfiles.exe -f scripts\check_logfiles
.cfg -reset
OK

C:\Program Files\NSClient++>scripts\check_logfiles.exe -f scripts\check_logfiles
.cfg
CRITICAL - (51 errors, 36 warnings in check_logfiles.protocol-2012-01-12-15-39-1
4) - 2012-01-12T13:59:04 1500 The SNMP Service encountered an error while access
ing the registry key SYSTEM\CurrentControlSet\Services\SNMP\Parameters\TrapConfi
guration.  ...|evt_sys_lines=7085 evt_sys_warnings=36 evt_sys_criticals=51 evt_s
ys_unknowns=0

C:\Program Files\NSClient++>_
```

Per testare manualmente il plugin da Nagios, digitare da console l'istruzione:

./check_nrpe -H ip_address_server -c check_logfiles

```
# cd /usr/lib/nagios/plugins
# ./check_nrpe -H 192.168.10.200 -c check_logfiles
```

```
[root@nagios plugins]# ./check_nrpe -H 192.168.10.200 -c check_logfiles
OK - no errors or warnings|evt_sys_lines=0 evt_sys_warnings=0 evt_sys_criti
cals=0 evt_sys_unknowns=0

[root@nagios plugins]#
```

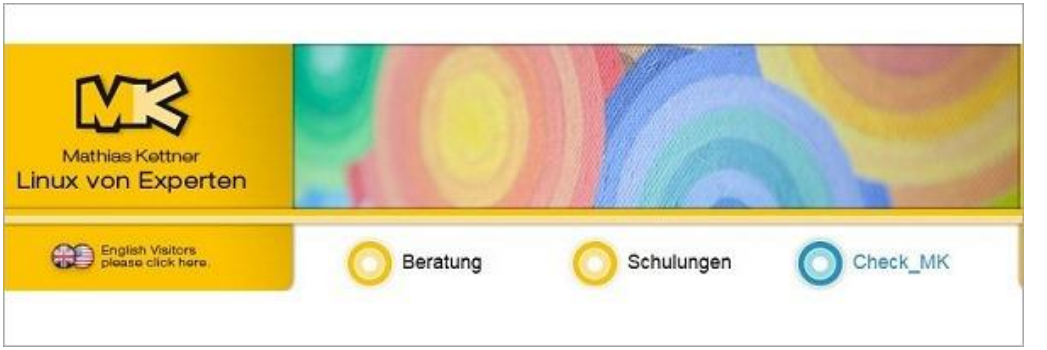
Definire il comando in *Nagios* per effettuare il check dei file di log.

```
define command {
command_name check_nrpe
command_line $USER1$/check_nrpe -H $HOSTADDRESS$ -c $ARG1$
}
```

Effettuato il check, *Nagios* visualizza il risultato tramite il plugin installato.

labmail	CPU	OK	CPU utilization percentage : 1%
	Disk-C	OK	Disk OK - C: TOTAL: 29.899GB USED: 17.796GB (59%) FREE: 12.104GB (41%)
	Disk-E	OK	Disk OK - D: TOTAL: 9.997GB USED: 3.670GB (36%) FREE: 6.327GB (64%)
	LogFiles	CRITICAL	CRITICAL - (51 errors, 36 warnings in check_logfiles.protocol-2012-01-12-16-42-51) - 2012-01-12T13:59:04 1500 The SNMP Service encountered an error while accessing the registry key SYSTEMCurrentControlSetServicesSNMPParametersTrapConfiguration. ...
	Memory	OK	Disk OK - Physical Memory TOTAL: 4.000GB USED: 1.427GB (35%) FREE: 2.573GB (65%)
	Ping	OK	OK - labmail: rta 0.933ms, lost 0%
	Swap	OK	Disk OK - Virtual Memory TOTAL: 7.997GB USED: 4.636GB (57%) FREE: 3.361GB (43%)
	Uptime	OK	OK - Uptime (in day): 0

Con questo plugin anche i log sono sotto controllo rendendo la vita degli amministratori di sistema un po' più semplice.



Check_mk è un plugin per Nagios per effettuare il monitoring della rete e dei sistemi operativi senza utilizzare gli addon *NRPE*, *check_by_ssh*, *NSClient* e *check_snmp*.

I vantaggi più significativi di *check_mk* rispetto ad altre soluzioni sono:

Riduzione del carico sulla CPU di Nagios.

Inventario automatico delle componenti controllate sugli host.

Prerequisiti

Per utilizzare il plugin sono richiesti tre componenti fondamentali:

- Sistema Nagios funzionante
- La presenza del modulo mod_python in Apache
- Il package di sistema xinetd operativo

Per installare *xinetd* e *mod_python*, utilizzare il comando *yum*.

```
# yum install xinetd mod_python
```

```
[root@nagios install]# yum install xinetd mod_python
Loaded plugins: fastestmirror, security
Loading mirror speeds from cached hostfile
 * base: ftp.hosteurope.de
 * extras: mirror.mserverz.de
 * rpmforge: apt.sw.be
 * updates: mirror.mserverz.de
Setting up Install Process
Resolving Dependencies
--> Running transaction check
---> Package mod_python.i386 0:3.2.8-3.1 set to be updated
---> Package xinetd.i386 2:2.3.14-13.el5 set to be updated
--> Finished Dependency Resolution
```

Installazione del plugin

Tramite il comando *wget*, scaricare il plugin *check_MK* dal sito http://mathias-kettner.de.

```
# wget http://mathias-kettner.de/download/check_mk-1.1.12p6.tar.gz
```

```
[root@nagios install]# wget http://mathias-kettner.de/download/check_mk-1.1
.12p6.tar.gz
--2012-01-09 12:31:37--  http://mathias-kettner.de/download/check_mk-1.1.12
p6.tar.gz
Resolving mathias-kettner.de... 87.106.4.132
Connecting to mathias-kettner.de|87.106.4.132|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2782332 (2.7M) [application/x-gzip]
Saving to: `check_mk-1.1.12p6.tar.gz'

100%[=================================>] 2,782,332    180K/s   in 13s

2012-01-09 12:31:50 (209 KB/s) - `check_mk-1.1.12p6.tar.gz' saved [2782332/
2782332]
```

Scompattare il file scaricato ed accedere alla directory.

```
# tar xzf check_mk-1.1.12p6.tar.gz
# cd check_mk-1.1.6p1
```

```
[root@nagios install]# ll
total 2724
-rw-r--r-- 1 root root 2782332 Dec 19 15:46 check_mk-1.1.12p6.tar.gz
[root@nagios install]# tar xzf check_mk-1.1.12p6.tar.gz
[root@nagios install]# cd check_mk-1.1.12p6
[root@nagios check_mk-1.1.12p6]#
```

Lanciare l'esecuzione dell'installazione del plugin tramite il comando *setup.sh*.

```
# ./setup.sh
```

```
Check_MK setup                                    Version: 1.1.12p6

Welcome to Check_MK. This setup will install Check_MK into user defined
directories. If you run this script as root, installation paths below
/usr will be suggested. If you run this script as non-root user paths
in your home directory will be suggested. You may override the default
values or just hit enter to accept them.

Your answers will be saved to /root/.check_mk_setup.conf and will be
reused when you run the setup of this or a later version again. Please
delete that file if you want to delete your previous answers.

* Found running Nagios process, autodetected 19 settings.
```

L'installazione, composta da sei sezioni, richiede la conferma dei vari path delle componenti indicando il valore di default. Confermare i path proposti premendo Invio.

Installation directories of check_mk

```
1) Installation directories of check_mk

Executable programs
Directory where to install executable programs such as check_mk itself.
This directory should be in your search path ($PATH). Otherwise you
always have to specify the installation path when calling check_mk:
( default  --> /usr/bin):

Check MK configuration
Directory where check_mk looks for its main configuration file main.mk.
An example configuration file will be installed there if no main.mk is
present from a previous version.:
( default  --> /etc/check_mk):
```

```
check_mk_checks
check_mk's different checks are implemented as small Python scriptlets
that parse and interpret the various output sections of the agents. Where
shall those be installed:
( default  --> /usr/share/check_mk/checks):

check_mk_modules
Directory for main componentents of check_mk itself. The setup will
also create a file 'defaults' in that directory that reflects all settings
you are doing right now:
( default  --> /usr/share/check_mk/modules):

Check_MK_Multisite_GUI
Directory where Check_mk's Multisite GUI should be installed. Multisite is
an optional replacement for the Nagios GUI, but is also needed for the
logwatch extension.  That directory should not be
in your WWW document root. A separate apache configuration file will be
installed that maps the directory into your URL schema:
( default  --> /usr/share/check_mk/web):

Localization_dir
Base directory for gettext localization files. Multisite comes prepared for
 localzation
but does not ship any language per default.:
( default  --> /usr/share/check_mk/locale):

documentation
Some documentation about check_mk will be installed here. Please note,
however, that most of check_mk's documentation is available only online at
http://mathias-kettner.de/check_mk.html:
( default  --> /usr/share/doc/check_mk):

check_manuals
Directory for manuals for the various checks. The manuals can be viewed
with check_mk -M <CHECKNAME>:
( default  --> /usr/share/doc/check_mk/checks):

working_directory_of_check_mk
check_mk will create caches files, automatically created checks and
other files into this directory. The setup will create several subdirectori
es
and makes them writable by the Nagios process:
( default  --> /var/lib/check_mk):

agents_for_operating_systems
Agents for various operating systems will be installed here for your
conveniance. Take them and install them onto your target hosts:
( default  --> /usr/share/check_mk/agents):
```

Configuration of Linux/Unix Agents

```
  2) Configuration of Linux/UNIX Agents

extensions for agents
This directory will not be created on the server. It will be hardcoded
into the Linux and UNIX agents. The agent will look for extensions in the
subdirectories plugins/ and local/ of that directory:
( default  --> /usr/lib/check_mk_agent):

configuration dir for agents
This directory will not be created on the server. It will be hardcoded
into the Linux and UNIX agents. The agent will look for its configuration
files here (currently only the logwatch extension needs a configuration fil
e):
( default  --> /etc/check_mk):
```

Integration with Nagios

```
  3) Integration with Nagios

Name of Nagios user
The working directory for check_mk contains several subdirectories
that need to be writable by the Nagios user (which is running check_mk
in check mode). Please specify the user that should own those
directories:
( autodetected  --> nagios):

User of Apache process
Check_MK WATO (Web Administration Tool) needs a sudo configuration,
such that Apache can run certain commands as root. If you specify
the correct user of the apache process here, then we can create a valid
sudo configuration for you later::
( autodetected  --> apache):

Common group of Nagios+Apache
Check_mk creates files and directories while running as nagios.
Some of those need to be writable by the user that is running the webserver
.
Therefore a group is needed in which both Nagios and the webserver are
members (every valid Nagios installation uses such a group to allow
the web server access to Nagios' command pipe)::
( autodetected  --> nagios):
```

```
Nagios binary
The complete path to the Nagios executable. This is needed by the
option -R/--restart in order to do a configuration check.:
( autodetected --> /usr/bin/nagios):

Nagios main configuration file
Path to the main configuration file of Nagios. That file is always
named 'nagios.cfg'. The default path when compiling Nagios yourself
is /usr/local/nagios/etc/nagios.cfg. The path to this file is needed
for the check_mk option -R/--restart:
( autodetected --> /etc/nagios/nagios.cfg):

Nagios object directory
Nagios' object definitions for hosts, services and contacts are
usually stored in various files with the extension .cfg. These files
are located in a directory that is configured in nagios.cfg with the
directive 'cfg_dir'. Please specify the path to that directory
(If the autodetection can find your configuration
file but does not find at least one cfg_dir directive, then it will
add one to your configuration file for your conveniance):
( autodetected --> /etc/nagios/check_mk.d):

Nagios startskript
The complete path to the Nagios startskript is used by the option
-R/--restart to restart Nagios.:
( autodetected --> /etc/init.d/nagios):

Nagios command pipe
Complete path to the Nagios command pipe. check_mk needs write access
to this pipe in order to operate:
( autodetected --> /var/nagios/rw/nagios.cmd):

Check results directory
Complete path to the directory where Nagios stores its check results.
Using that directory instead of the command pipe is faster.:
( autodetected --> /var/nagios/spool/checkresults):

Nagios status file
The web pages of check_mk need to read the file 'status.dat', which is
regularily created by Nagios. The path to that status file is usually
configured in nagios.cfg with the parameter 'status_file'. If
that parameter is missing, a compiled-in default value is used. On
FHS-conforming installations, that file usually is in /var/lib/nagios
or /var/log/nagios. If you've compiled Nagios yourself, that file
might be found below /usr/local/nagios:
( autodetected --> /var/nagios/status.dat):

Path to check_icmp
check_mk ships a Nagios configuration file with several host and
service templates. Some host templates need check_icmp as host check.
That check plugin is contained in the standard Nagios plugins.
Please specify the complete path (dir + filename) of check_icmp:
( autodetected --> /usr/lib/nagios/plugins/check_icmp):
```

Integration with Apache

```
4) Integration with Apache

URL Prefix for Web addons
Usually the Multisite GUI is available at /check_mk/ and PNP4Nagios
is located at /pnp4nagios/. In some cases you might want to define some
prefix in order to be able to run more instances of Nagios on one host.
If you say /test/ here, for example, then Multisite will be located
at /test/check_mk/. Please do not forget the trailing slash.:
( default --> /):

Apache config dir
Check_mk ships several web pages implemented in Python with Apache
mod_python. That module needs an apache configuration section which
will be installed by this setup. Please specify the path to a directory
where Apache reads in configuration files.:
( autodetected --> /etc/httpd/conf.d):

HTTP authentication file
Check_mk's web pages should be secured from unauthorized access via
HTTP authenticaion - just as Nagios. The configuration file for Apache
that will be installed contains a valid configuration for HTTP basic
auth. The most conveniant way for you is to use the same user file as
for Nagios. Please enter your htpasswd file to use here:
( autodetected --> /etc/nagios/htpasswd.users):

HTTP AuthName
Check_mk's Apache configuration file will need an AuthName. That
string will be displayed to the user when asking for the password.
You should use the same AuthName as for Nagios. Otherwise the user will
have to log in twice:
( autodetected --> Nagios Access):
```

Integration with PNP4Nagios 0.6

```
  5) Integration with PNP4Nagios 0.6

PNP4Nagios templates
Check_MK ships templates for PNP4Nagios for most of its checks.
Those templates make the history graphs look nice. PNP4Nagios
expects such templates in the directory pnp/templates in your
document root for static web pages:
( default  --> /usr/share/check_mk/pnp-templates):

RRA config for PNP4Nagios
Check_MK ships RRA configuration files for its checks that
can be used by PNP when creating the RRDs. Per default, PNP
creates RRD such that for each variable the minimum, maximum
and average value is stored. Most checks need only one or two
of these aggregations. If you install the Check_MK's RRA config
files into the configuration directory of PNP, PNP will create
RRDs with the minimum of required aggregation and thus save
substantial amount of disk I/O (and space) for RRDs. The default
is to install the configuration into a separate directory but
does not enable them:
( default  --> /usr/share/check_mk/pnp-rraconf):
```

Check_MK Livestatus

Poichè è un modulo ancora sperimentale, abilitarlo solo nel caso si voglia integrare il modulo in Nagios.

```
  6) Check_MK Livestatus Module

compile livestatus module
This version of Check_mk ships a completely new and experimental
Nagios event broker module that provides direct access to Nagios
internal data structures. This module is called the Check_MK Livestatus
Module. It aims to supersede status.dat and also NDO. Currenty it
is completely experimental and might even crash your Nagios process.
Nevertheless - The Livestatus Module does not only allow extremely
fast access to the status of your services and hosts, it does also
provide live data (which status.dat does not). Also - unlike NDO -
Livestatus does not cost you even measurable CPU performance, does
not need any disk space and also needs no configuration.

Please answer 'yes', if you want to compile and integrate the
Livestatus module into your Nagios. You need 'make' and the GNU
C++ compiler installed in order to do this:
( default  --> yes): no
```

Terminate le schermate dei vari path, si presenta una videata riepilogativa delle impostazioni effettuate.

```
-----------------------------------------------------------------------

You have chosen the following directories:

 Executable programs              /usr/bin
 Check_MK configuration           /etc/check_mk
 check_mk checks                  /usr/share/check_mk/checks
 check_mk modules                 /usr/share/check_mk/modules
 Check_MK Multisite GUI           /usr/share/check_mk/web
 Localization dir                 /usr/share/check_mk/locale
 documentation                    /usr/share/doc/check_mk
 check manuals                    /usr/share/doc/check_mk/checks
 working directory of check_mk    /var/lib/check_mk
 agents for operating systems     /usr/share/check_mk/agents
 extensions for agents            /usr/lib/check_mk_agent
 configuration dir for agents     /etc/check_mk
 Name of Nagios user              nagios
 User of Apache process           apache
 Common group of Nagios+Apache    nagios
 Nagios binary                    /usr/bin/nagios
 Nagios main configuration file   /etc/nagios/nagios.cfg
 Nagios object directory          /etc/nagios/check_mk.d
 Nagios startskript               /etc/init.d/nagios
 Nagios command pipe              /var/nagios/rw/nagios.cmd
 Check results directory          /var/nagios/spool/checkresults
 Nagios status file               /var/nagios/status.dat
 Path to check_icmp               /usr/lib/nagios/plugins/check_icmp
 URL Prefix for Web addons        /
 Apache config dir                /etc/httpd/conf.d
 HTTP authentication file         /etc/nagios/htpasswd.users
 HTTP AuthName                    Nagios Access
 PNP4Nagios templates             /usr/share/check_mk/pnp-templates
 RRA config for PNP4Nagios        /usr/share/check_mk/pnp-rraconf
 compile livestatus module        no

Proceed with installation (y/n)?
```

Digitare y per procedere con l'installazione.

```
Proceed with installation (y/n)? y
Installation completed successfully.
Please restart Nagios and Apache in order to update/active check_mk's web p
ages.

You can access the new Multisite GUI at http://localhost/check_mk/
[root@nagios check_mk-1.1.12p6]#
```

Terminata l'operazione, riavviare i servizi Nagios e Apache.

```
# service nagios restart
# service httpd restart
```

```
[root@nagios check_mk-1.1.12p6]# service nagios restart
Stopping nagios:                                           [  OK  ]
Starting nagios:                                           [  OK  ]
[root@nagios check_mk-1.1.12p6]# service httpd restart
Stopping httpd:                                            [  OK  ]
Starting httpd:                                            [  OK  ]
[root@nagios check_mk-1.1.12p6]#
```

Per verificare la versione del plugin installato, utilizzare da console il comando:

```
# check_mk -version
```

```
[root@nagios check_mk]# check_mk --version
This is check_mk version 1.1.12p6
Copyright (C) 2009 Mathias Kettner

    This program is free software; you can redistribute it and/or modify
    it under the terms of the GNU General Public License as published by
    the Free Software Foundation; either version 2 of the License, or
    (at your option) any later version.

    This program is distributed in the hope that it will be useful,
    but WITHOUT ANY WARRANTY; without even the implied warranty of
    MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
    GNU General Public License for more details.

    You should have received a copy of the GNU General Public License
    along with this program; see the file COPYING.  If not, write to
    the Free Software Foundation, Inc., 59 Temple Place - Suite 330,
    Boston, MA 02111-1307, USA.

[root@nagios check_mk]#
```

Per effettuare il monitoraggio di un host, è necessario installare l'agent nell'host stesso.

Installazione agent in Linux

Tramite il comando *wget*, scaricare dal sito l'agent per Linux.

```
# wget http://mathias-kettner.de/download/check_mk-agent-1.1.12p6-1.noarch.rpm
```

```
[root@nagios install]# wget http://mathias-kettner.de/download/check_mk-age
nt-1.1.12p6-1.noarch.rpm
--2012-01-09 11:31:05--  http://mathias-kettner.de/download/check_mk-agent-
1.1.12p6-1.noarch.rpm
Resolving mathias-kettner.de... 87.106.4.132
Connecting to mathias-kettner.de|87.106.4.132|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 63900 (62K) [application/x-redhat-package-manager]
Saving to: `check_mk-agent-1.1.12p6-1.noarch.rpm'

100%[=================================>] 63,900       220K/s   in 0.3s

2012-01-09 11:31:05 (220 KB/s) - `check_mk-agent-1.1.12p6-1.noarch.rpm' sav
ed [63900/63900]

[root@nagios install]#
```

Tramite il comando *rpm* effettuare l'installazione.

```
# rpm -Uvh check_mk-agent-1.1.12p6-1.noarch.rpm
```

```
[root@nagios install]# rpm - Uvh check_mk-agent-1.1.12p6-1.noarch.rpm
Preparing...                ########################################### [10
0%]
   1:check_mk-agent         ########################################### [10
0%]
Activating startscript of xinetd
Starting xinetd...
Starting xinetd: [  OK  ]
[root@nagios install]#
```

I parametri di configurazione di *check_MK* sono salvati nel file /etc/check_mk/main.mk.

La configurazione basic prevede la presenza della variabile ***all_hosts*** che contiene gli host da monitorare. Per verificare la funzionalità del sistema, viene impostato localhost come primo host da monitorare.

```
# Put your host names here
all_hosts = [ 'localhost' ]
```

Effettuare l'inventory lanciando il comando:

```
# check_mk -I localhost
```

```
[root@nagios install]# check_mk -I localhost
cpu.loads          1 new checks
cpu.threads        1 new checks
df                 4 new checks
diskstat           1 new checks
kernel             3 new checks
kernel.util        1 new checks
lnx_if             1 new checks
mem.used           1 new checks
mem.vmalloc        1 new checks
mounts             4 new checks
ntp.time           1 new checks
tcp_conn_stats     1 new checks
uptime             1 new checks
[root@nagios install]#
```

Assegnare i permessi corretti ai file del sistema.

```
# cd /etc/nagios
# chown apache:apache check_mk.d/ -R
```

```
[root@nagios nagios]# chown apache:apache check_mk.d/ -R
[root@nagios nagios]# ll
total 256
-rwxrwxr-x 1 apache apache  1810 Jan  4 14:13 cgi.cfg
-rwxrwxr-x 1 apache apache 12145 Jan  4 14:13 checkcommands.cfg
drwxr-xr-x 2 apache apache  4096 Jan  9 13:36 check_mk.d
-rwxrwxr-x 1 apache apache 15700 Nov 26  2010 command-plugins.cfg
-rwxrwxr-x 1 apache apache  1277 Jan  4 14:13 contactgroups.cfg
-rwxrwxr-x 1 apache apache  1460 Jan  4 14:13 contacts.cfg
-rwxrwxr-x 1 apache apache  1089 Jan  4 14:13 contactTemplates.cfg
-rwxrwxr-x 1 apache apache  1089 Jan  4 14:13 dependencies.cfg
```

Per verificare la corretta configurazione e riavviare automaticamente *Nagios*, utilizzare il parametro -O.

```
# check_mk -O
```

```
[root@nagios nagios]# check_mk -O
Generating Nagios configuration...OK
Validating Nagios configuration...OK
Precompiling host checks...OK
Reloading Nagios...OK
[root@nagios nagios]#
```

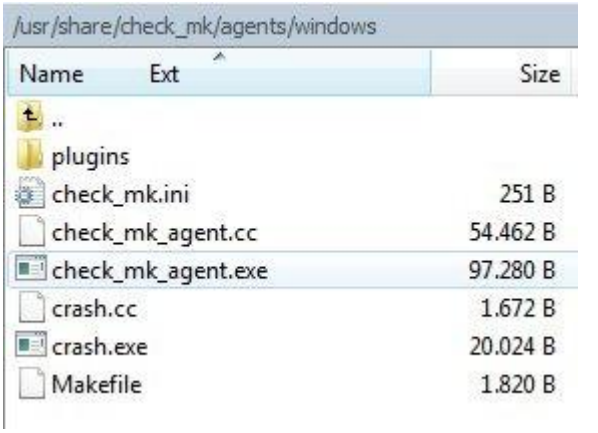
Accedendo tramite browser alla pagina di *Nagios*, l'host configurato compare con i parametri impostati per default.

localhost	CPU load	OK	OK - 15min Load 0.66 at 1 CPUs
	CPU utilization	OK	OK - user: 10.4%, system: 3.2%, wait: 0.7%
	Check_MK	OK	OK - Agent version 1.1.12p6, execution time 0.2 sec
	Disk IO SUMMARY	OK	OK - 24.27KB/sec read, 510.51KB/sec write
	Interface 2	OK	OK - [eth0] (up) speed unknown, in: 18.69KB/s, out: 11.36KB/s
	Kernel Context Switches	OK	OK - 278/s in last 59 secs
	Kernel Major Page Faults	OK	OK - 1/s in last 59 secs
	Kernel Process Creations	OK	OK - 5/s in last 59 secs
	Memory used	OK	OK - 0.12 GB used (0.12 GB RAM + 0.00 GB SWAP, this is 24.6% of 0.49 GB RAM)
	Mount options of /	OK	OK - mount options are data=ordered,rw
	Mount options of /boot	OK	OK - mount options are data=ordered,rw
	Mount options of /tmp	OK	OK - mount options are data=ordered,rw
	Mount options of /var	OK	OK - mount options are data=ordered,rw
	NTP Time	OK	OK - sys.peer - stratum 2, offset -0.24 ms, jitter 64.66 ms, last reached 145 secs ago (synchronized on flo.m4oc.it)
	Number of threads	OK	OK - 114 threads
	TCP Connections	OK	OK - ESTABLISHED: 6, TIME_WAIT: 65, FIN_WAIT2: 1
	Uptime	OK	OK - up since Mon Jan 9 12:25:12 2012 (0d 01:51:01)
	Vmalloc address space	OK	OK - total 496.0 MB, used 4.2 MB, largest chunk 491.7 MB
	fs_/	OK	OK - 45.0% used (1.92 of 4.3 GB), (levels at 80.0/90.0%), trend: 0.00B / 24 hours
	fs_/boot	OK	OK - 33.3% used (0.03 of 0.1 GB), (levels at 80.0/90.0%), trend: 0.00B / 24 hours
	fs_/tmp	OK	OK - 52.7% used (0.51 of 1.0 GB), (levels at 80.0/90.0%), trend: 0.00B / 24 hours
	fs_/var	OK	OK - 32.9% used (1.28 of 3.9 GB), (levels at 80.0/90.0%), trend: +13.86KB / 24 hours

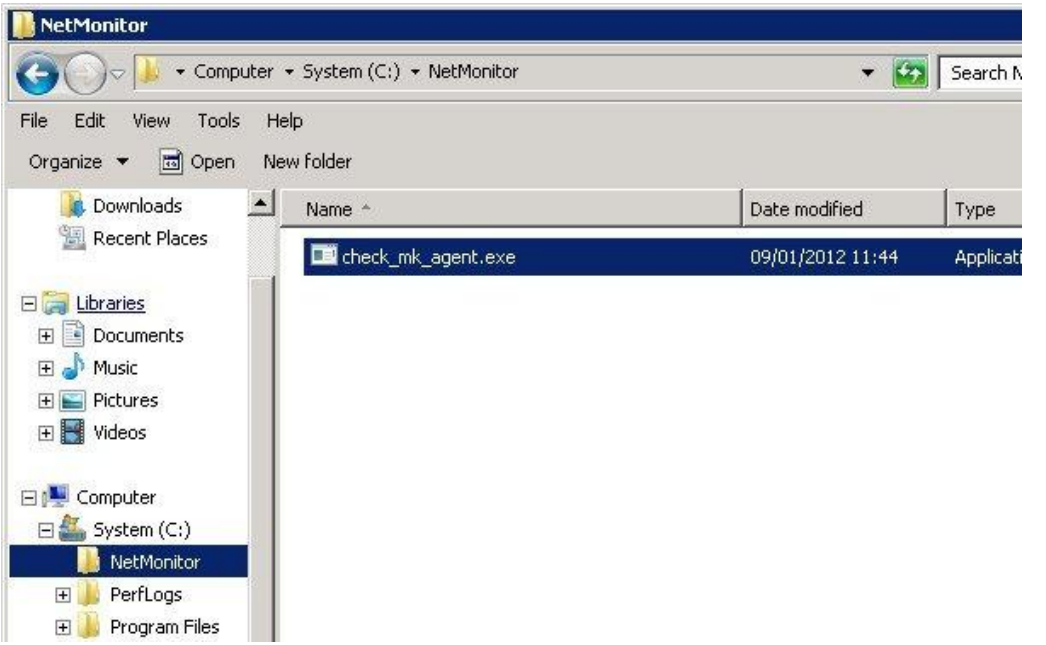
Installazione agent in Windows

Quando si effettua l'installazione del plugin in Nagios, l'agent di Windows viene salvato nel folder */usr/share/check_mk/agents/windows*.

Tramite *WinSCP* o simili copiare il file sul proprio PC in modo da poterlo installare sull'host designato.



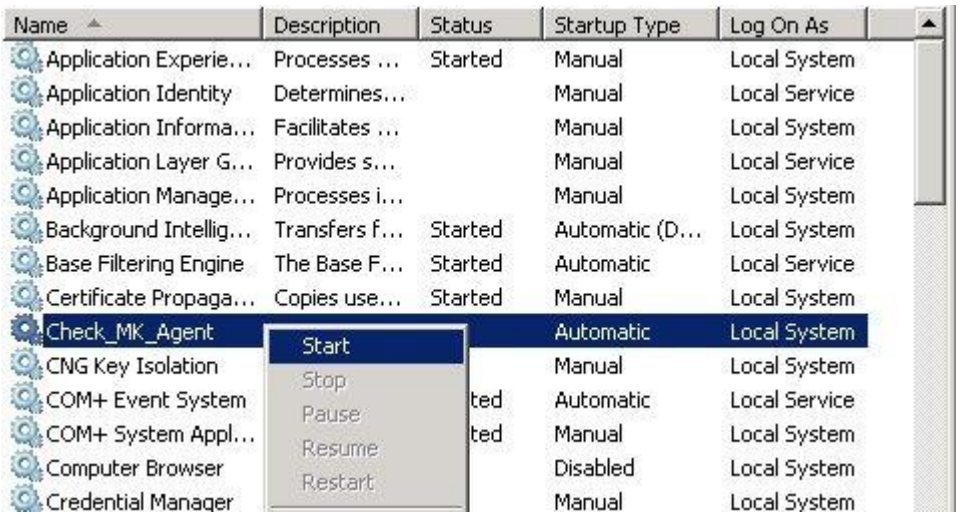
Creare una directory nell'host *Windows* (*NetMonitor* nell'esempio) e copiare il file eseguibile dell'agent.



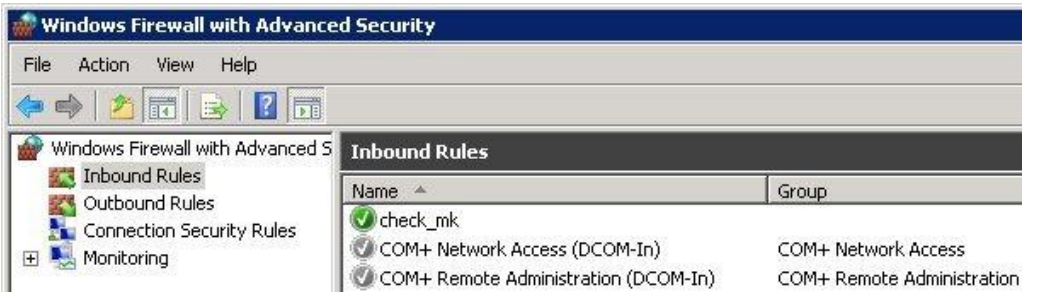
Dal *Command Prompt* di Windows, lanciare il comando di installazione:

```
:\> check_mk_agent.exe install
```

Tramite Start –> Administrative Tools –> Services selezionare il servizio Check_MK_Agent ed avviarlo.



Configurare il firewall di Windows aprendo la porta TCP 6556 per permettere il corretto funzionamento del plugin.



Da *Nagios*, editare il file *main.mk* ed aggiungere il nuovo host.

```
# vi /etc/check_mk/main.mk
```

```
# Put your host names here
all_hosts = [ 'localhost', 'labmail' ]
```

Eseguire ora l'inventory utilizzando il parametro -I con la sintassi:

check_mk -I *ip_address_host* or *hostname*

```
# check_mk -I labmail
```

```
[root@nagios /]# check_mk -I labmail
df                  2 new checks
logwatch            7 new checks
mem.win             1 new checks
systemtime          1 new checks
uptime              1 new checks
winperf_phydisk     1 new checks
winperf_processor.util 1 new checks
[root@nagios /]#
```

Aggiornare la configurazione di *Nagios* tramite il parametro -U.

```
# check_mk -U
```

```
[root@nagios /]# check_mk -U
Generating Nagios configuration...OK
Precompiling host checks...OK
Successfully created Nagios configuration file /etc/nagios/check_mk.d/check
_mk_objects.cfg.

Please make sure that file will be read by Nagios.
You need to restart Nagios in order to activate the changes.
[root@nagios /]#
```

Verificare ed eventualmente modificare i permessi assegnati al file */etc/nagios/check_mk.d/check_mk_objects.cfg*.

```
# chown apache:apache /etc/nagios/check_mk.d/ -R
```

Riavviare il servizio *Nagios* per attivare la nuova configurazione.

```
# service nagios restart
```

Nagios visualizza il nuovo host Windows con i parametri impostati per default.

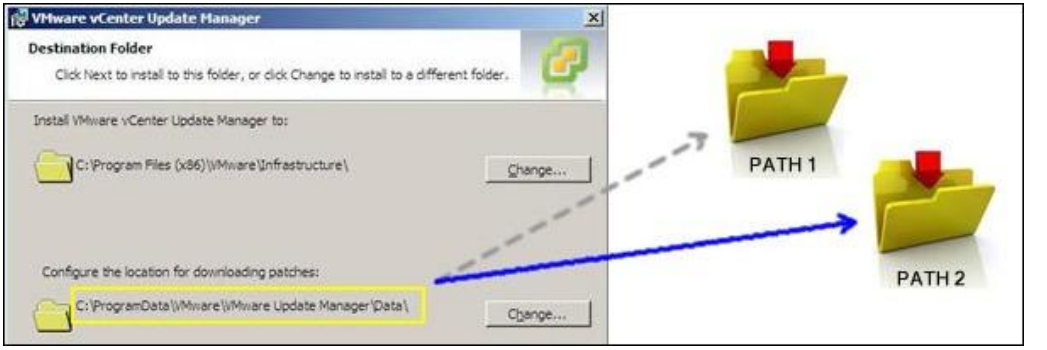
labmail	CPU utilization	OK	OK - 0% used (in last 61 secs)
	Check_MK	OK	OK - Agent version 1.1.12p6, execution time 0.1 sec
	Disk IO SUMMARY	OK	OK - 0.00B/sec read, 3.42KB/sec write
	LOG Application	OK	OK - no old or new error messages
	LOG HardwareEvents	OK	OK - no old or new error messages
	LOG Internet Explorer	OK	OK - no old or new error messages
	LOG Key Management Service	OK	OK - no old or new error messages
	LOG Security	OK	OK - no old or new error messages
	LOG System	OK	OK - no old or new error messages
	LOG Windows PowerShell	OK	OK - no old or new error messages
	Memory and pagefile	WARNING	WARN - Memory usage: 41.5% (1.7/4.0 GB), Page file usage: 58.3% (4.7/8.0 GB)(!)
	System Time	WARNING	WARN - Offset is +58.9 sec (levels at 30/60 sec)
	Uptime	OK	OK - up since Mon Jan 9 01:09:15 2012 (0d 14:27:26)
	fs_C:/	OK	OK - 59.5% used (17.80 of 29.9 GB), (levels at 80.0/90.0%), trend: -46.13MB / 24 hours
	fs_D:/	OK	OK - 36.7% used (3.67 of 10.0 GB), (levels at 80.0/90.0%), trend: 0.00B / 24 hours

I vari parametri delle configurazioni sono documentati e reperibili presso il sito del plugin.

E' decisamente un tool interessante che non richiede rischiose configurazioni nei server da monitorare e la sua installazione risulta semplice e veloce.

Procedure VMware

Modificare la directory di download di VMware Update Manager



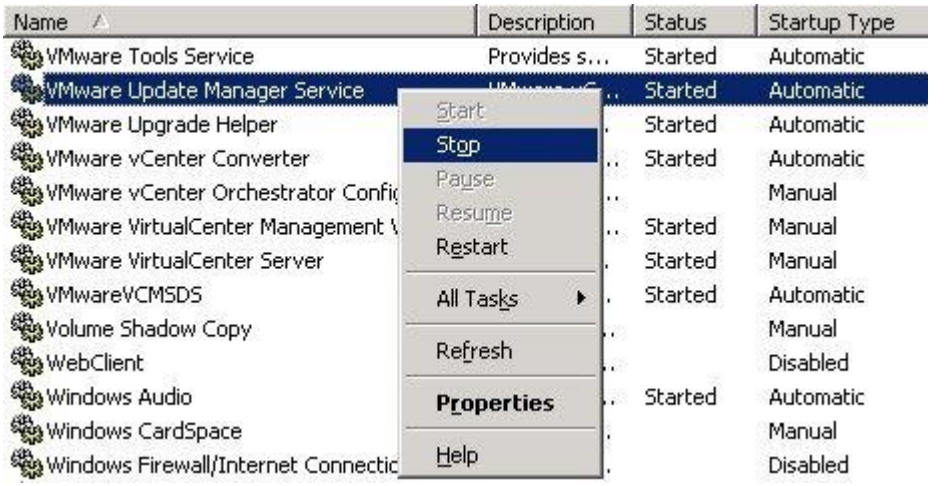
Quando vengono rilevati nuovi aggiornamenti delle categorie specificate nelle baseline in vCenter Server, il servizio *vSphere Update Manager* scarica gli update nella directory specificata durante la procedura di installazione.

Capita comunque che per esigenze di spazio disco o altro, è necessario modificare la directory di download. Reinstallare l'applicazione *Update Manager* permette di specificare la nuova directory di destinazione per gli aggiornamenti ma questo comporta ripetere l'intera operazione di installazione. Fortunatamente non è necessario rifare l'installazione poichè è possibile effettuare la modifica manualmente.

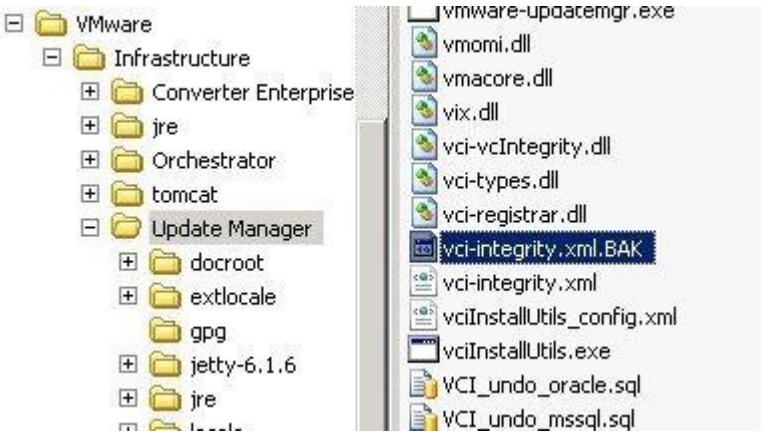
Procedura

Per modificare la directory di download, procedere nel modo seguente:

Il primo step è fermare da services.msc il servizio *VMware Update Manager Service*.

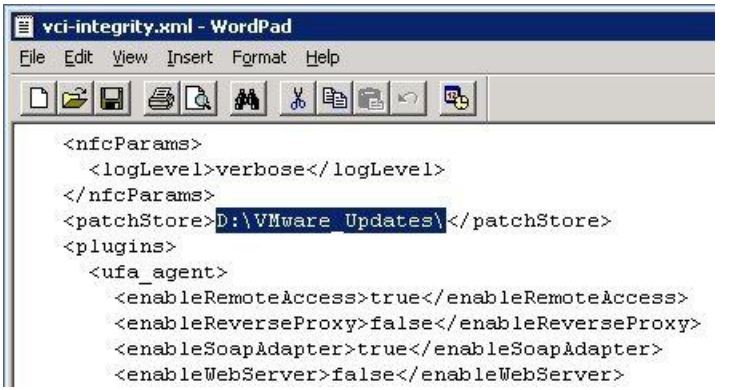


Nel vCenter Server, identificare la directory *C:\Program Files\VMware\Infrastructure\Update Manager* e selezionare il file di configurazione vci-integrity.xml. Effettuare una copia del file nel caso si avesse l'esigenza di ripristinare la configurazione precedente.

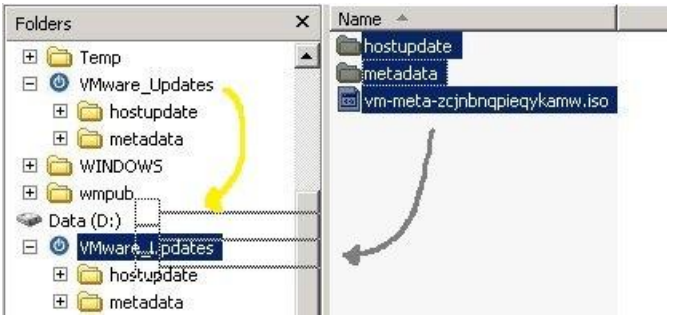


Editare il file vci-integrity.xml e modificare il path della directory di download indicata nei campi patchStore (D:\VMware_Updates\ nell'esempio) digitando il carattere \ alla fine della directory specificata.

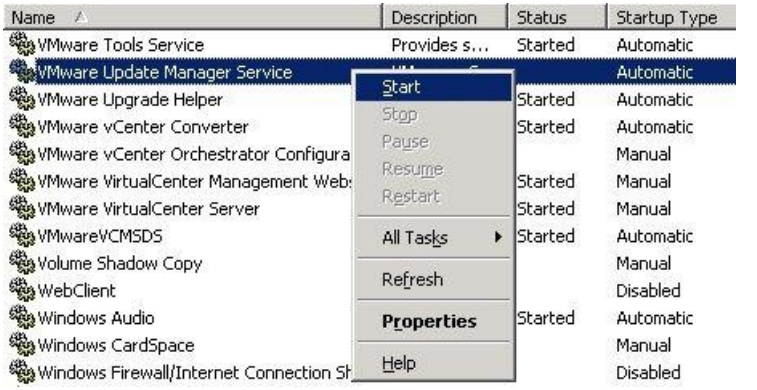
*<patchStore>*D:\VMware_Updates*</patchStore>*



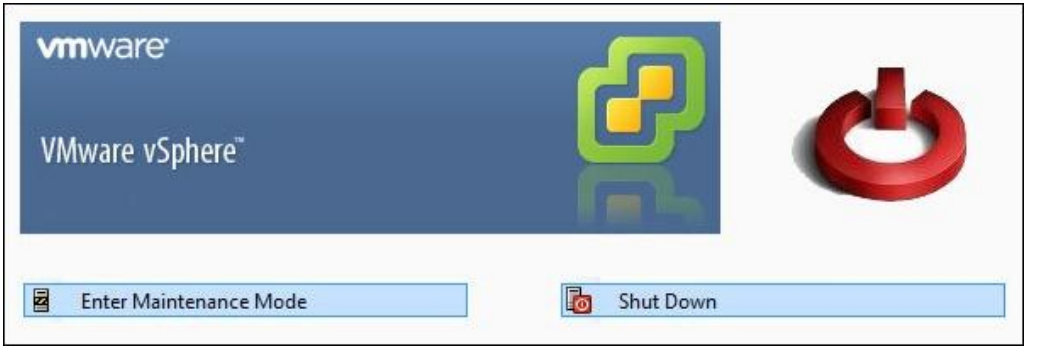
Copiare il contenuto dal vecchio patchstore alla nuova directory (*D:\VMware_Updates*).



Riavviare il servizio *VMware Update Manager Service*.



A questo punto il nuovo repository per le patch e gli aggiornamenti di *Update Manager* è operativo nel nuovo path.



Se, ad esempio, per una manutenzione della linea elettrica della stabile il tempo stimato per il completamento dei lavori va oltre la capacità dell'UPS o per un semplice trasloco, sorge la necessità di effettuare lo shutdown completo dell'intera infrastruttura virtuale.

La procedura, anche se non complicata, richiede degli step ben precisi per evitare che si presentino degli imprevisti dagli effetti potenzialmente minacciosi per la funzionalità della rete. Se fossero presenti 10 host nella struttura e venisse fatto uno shutdown scriteriato, oltre a rischiare di mandare in palla la funzionalità, come facciamo a sapere in quale host risiede vCenter? Li dobbiamo analizzare uno alla volta… non è decisamente un buon approccio.

Shutdown

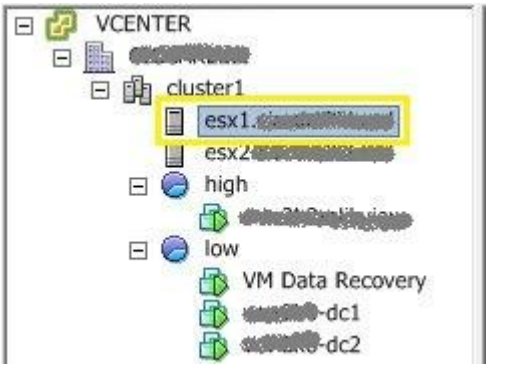
Effettuare lo shutdown di tutte le virtual machine eccetto vCenter Server (se virtualizzato) e l'eventuale server SQL se il database di vCenter è separato. Se sono presenti vari host nella struttura, annotare l'host che ospita vCenter\SQL.

Mettere tutti gli host, eccetto quello in cui risiede vCenter\SQL, in Maintenance Mode ed effettuare lo shutdown.

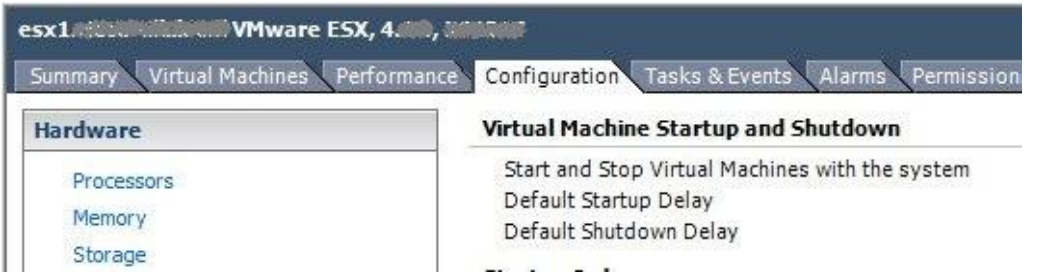
Connettersi tramite vSphere Client direttamente all'host ESX che ospita vCenter\SQL ed effettuare lo shutdown delle rimanenti virtual machine.

Ultimo step è lo shutdown dell'ultimo host. Questo è l'host che dovrà essere riavviato per primo. E' opportuno configurare questo server ESX in modo da permettere l'avvio automatico dei server core (vCenter, SQL, DC, …) per il corretto funzionamento della struttura.

Dal server VMware Virtual Center, selezionare l'host ESX che ospita vCenter.



Nel parte di destra cliccare su Configuration.



Configurare l'opzione Virtual Machine Startup/Shutdown per permettere l'avvio automatico del Virtual Center\SQL e di un eventuale domain controller (DC1) nel caso la struttura di rete presenta un ambiente di Active Directory.

Startup Order

Order	Virtual Machine	Startup	Startup Delay	Shutdown	Shutdown Delay
Automatic Startup					
1	[redacted]-dc1	Enabled	60 seconds	Shut do...	60 seconds
2	[redacted]-vcenter	Enabled	180 seconds	Shut do...	60 seconds
Manual Startup					
	[redacted]-ftp	Disabled	60 seconds	Shut do...	60 seconds
	[redacted]	Disabled	60 seconds	Shut do...	60 seconds
	[redacted]	Disabled	60 seconds	Shut do...	60 seconds
	[redacted]-ossec	Disabled	60 seconds	Shut do...	60 seconds
	[redacted]	Disabled	120 seconds	Shut do...	60 seconds

Power on

Avviare l'ultimo host ESX della sequenza precedentemente spento.

Se non è previsto un avvio automatico di vCenter\SQL, connettersi direttamente all'host tramite vSphere Client.

Avviare, se configurati in diverse VM, un eventuale domain controller, SQL e poi vCenter.

Da VI, disconnettersi dal singolo host e connettersi a vCenter.

Riavviare i rimanenti host e toglierli dallo stato di Maintenance Mode.

Riavviare le virtual machine verificando che il cluster sia ritornato allo stato ottimale per poter fornire tutte le risorse necessario a far girare correttamente tutte le VM.

Eseguendo correttamente le sequenze di shutdown e power on, l'infrastruttura virtuale può essere disattivata e riattivata senza problemi al presentarsi di situazioni particolari come manutenzioni (linea elettrica), traslochi o altro.

Integrare VMware ESXi 4.1 in Active Directory

Con la diffusione dei sistemi di virtualizzazione nelle aziende, il problema della gestione degli accessi e della sicurezza diventa prioritario. Avere una sistema per la gestione centralizzata delle autenticazioni per l'accesso all'infrastruttura informatica facilita notevolmente la parte amministrativa degli operatori IT oltre che fornire un fattore di sicurezza più affidabile.

Per accedere direttamente ad un server ESXi (quindi non con *vCenter*) è necessario utilizzare un account Linux definito nell'host. Questo vale per ogni server analogo presente nella rete. E' evidente che una gestione sicura e funzionale dei vari account all'interno di una rete risulti piuttosto laboriosa.

Dalla versione 4.1, *VMware* ha integrato in ESXi l'opzione per l'autenticazione in Active Directory che permette il login tramite utenti e gruppi definiti in AD. Questa funzione è operativa effettuando il join di ESXi al dominio AD in un modo molto più semplice.

Prerequisiti

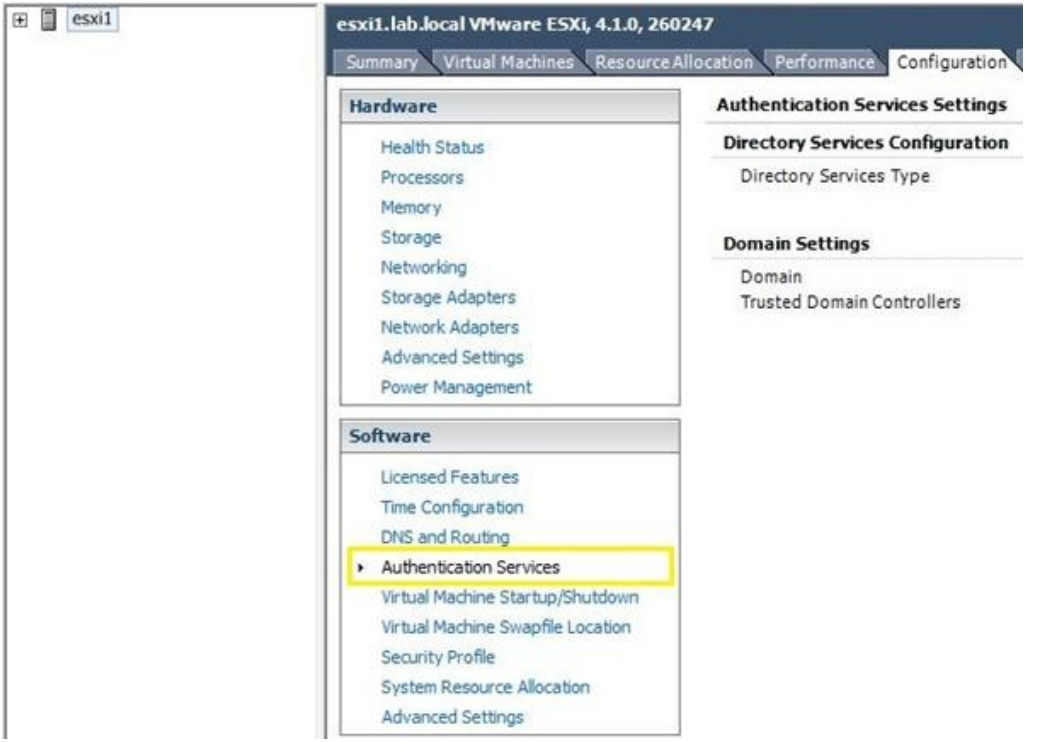
Per poter effettuare l'operazione correttamente, è necessario verificare alcuni aspetti:

- L'host ESXi e il Domain Controller hanno un corretto time synchronization per il funzionamento dell'autenticazione tramite il protocollo *Kerberos*.
- La DNS resolution funziona correttamente dall'host ESXi.
- L'host ESXi ha un corretto FQDN, ad esempio *esxi.domain.local*.

Procedura

Collegarsi al server ESXi tramite vSphere Client (non da vCenter!) e digitare username e password corretti dell'account con diritti amministrativi (default *root*) presenti in *ESXi*.

Selezionare il pannello Configuration e cliccare sulla voce Authentication Services.



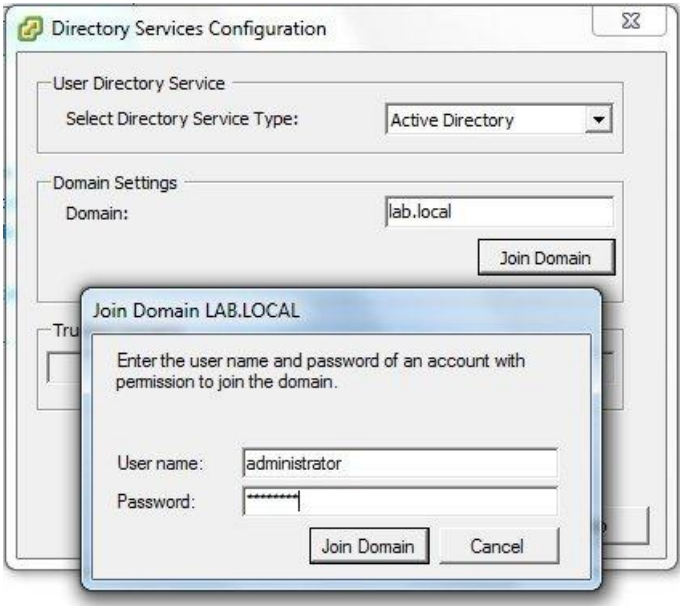
Si accede all'area per l'autenticazione. Nella parte destra dello schermo cliccare sulla voce Properties.

Si apre la finestra Directory Services Configuration. Impostare i parametri per l'autenticazione in Active Directory.

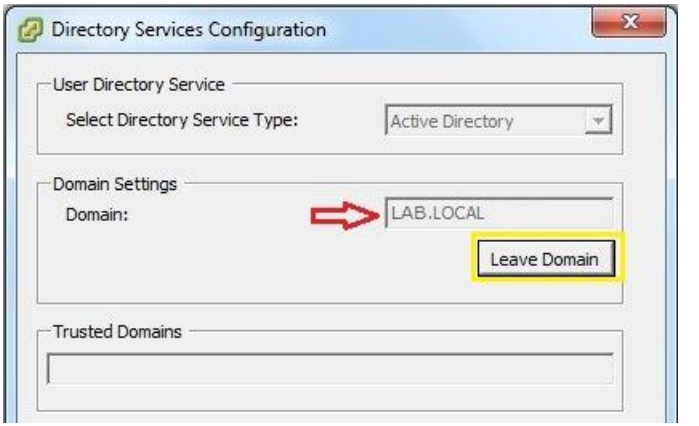
Select Directory Service Type: Active Directory
Domain: domain.local

Cliccare sul bottone Join Domain per effettuare l'operazione di *join al dominio*.

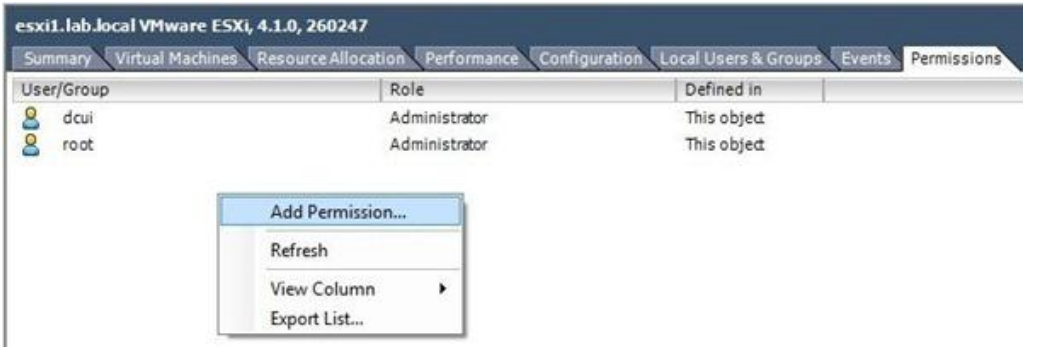
Viene visualizzata la finestra che richiede l'inserimento dell'account di *Active Directory* con i diritti sufficienti per effettuare il *join al dominio*. Cliccare sul bottone Join Domain.



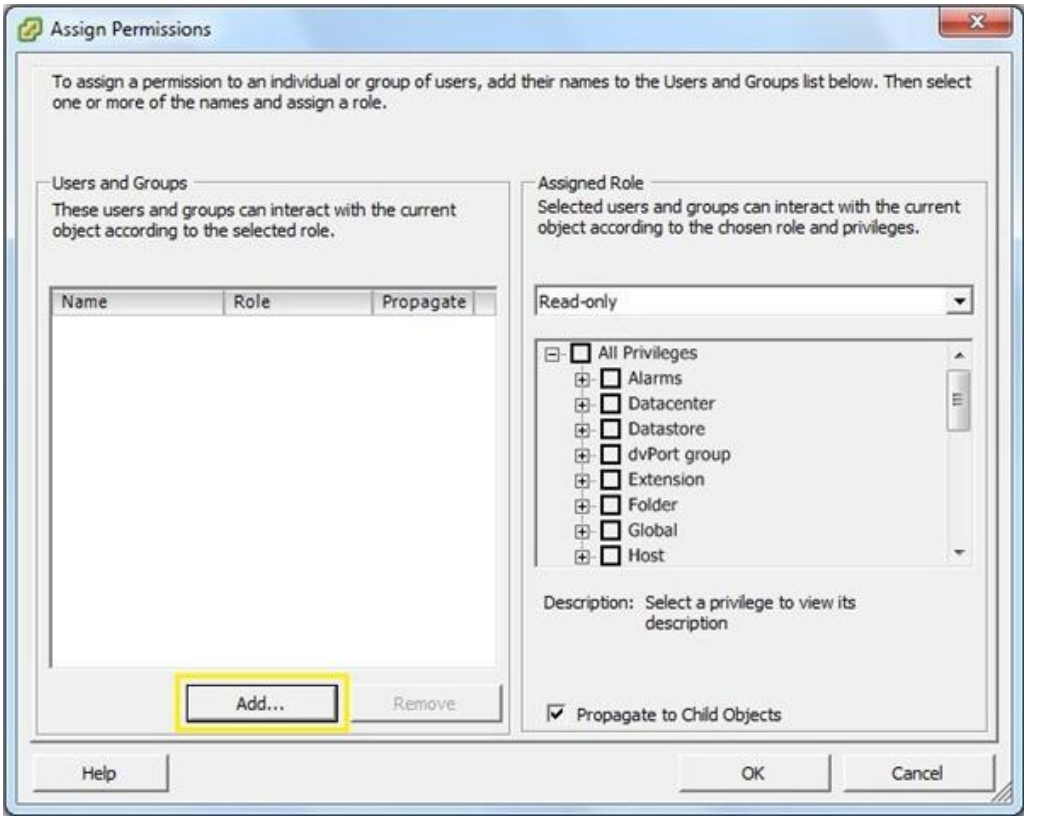
Conclusa l'operazione, il nome del dominio viene indicato nel campo *Domain*. Da notare la presenza del bottone Leave Domain che permette di rimuovere l'host da Active Directory.



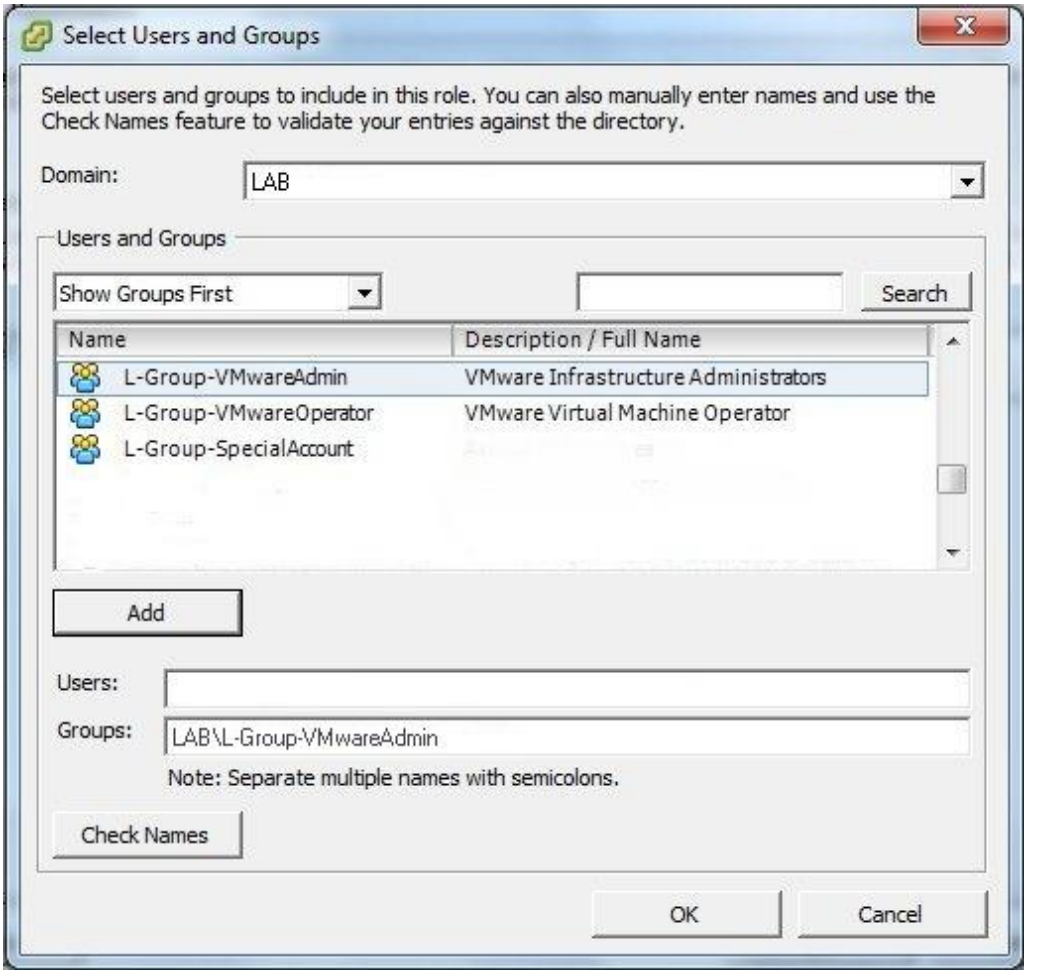
Per definire il gruppo AD dedicato all'amministrazione di ESXi, selezionare il pannello Permissions in *vSphere Client* e cliccare con il tasto destro in un punto della schermata. Selezionare la voce Add Permission.



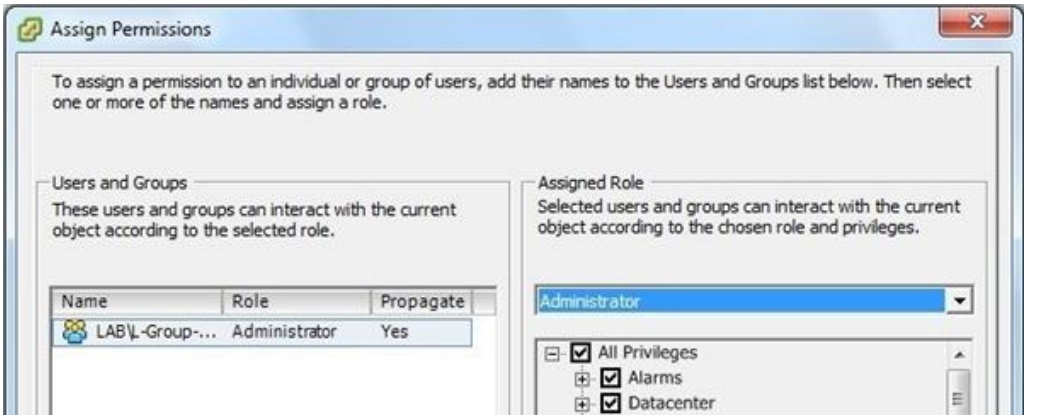
Compare la finestra Assign Permissions. Cliccare sul bottone Add per aggiungere il nuovo account AD.



Selezionando il dominio corretto (LAB nell'esempio), vengono visualizzati gli account presenti in AD. Selezionare il gruppo dedicato alla gestione della struttura *VMware* e cliccare poi su OK.

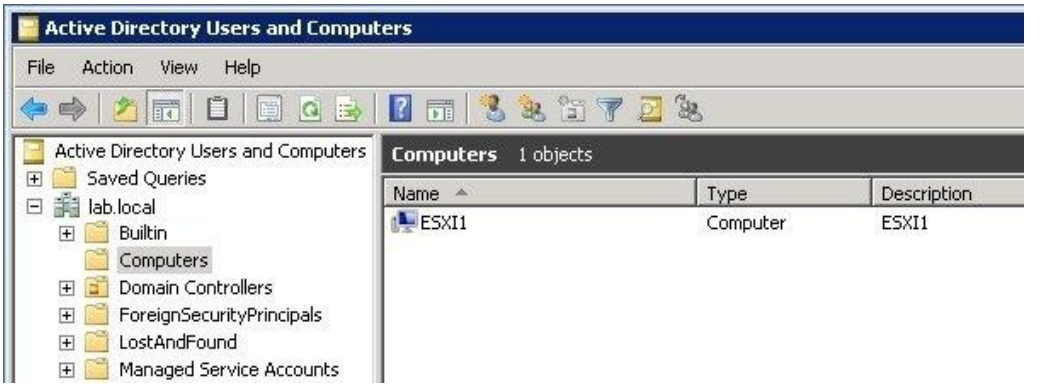


Assegnare il ruolo al gruppo selezionato (No Access, Read Only, Administrator) e cliccare su OK.



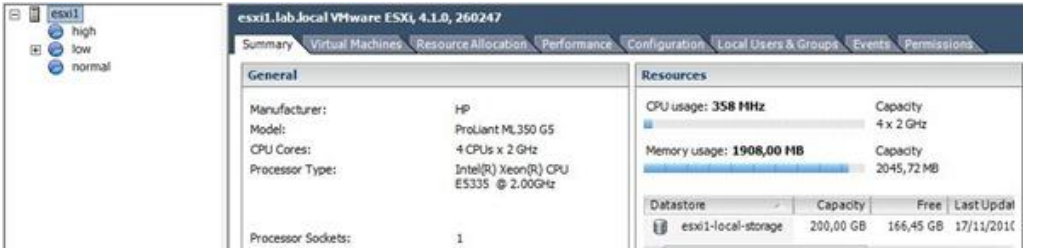
Osservando la lista degli account presenti su ESXi, compare anche il gruppo di Active Directory appena selezionato.

Dal *Domain Controller* aprendo Active Directory Users and Computers, è visibile il server ESXi.



Tramite *vSphere Client* effettuare ora il login all'host ESXi utilizzando l'account di Active Directory membro del gruppo impostato (LAB\L-Group-VMwareAdmin) spuntando l'opzione Use Windows session credentials.

L'accesso a ESXi viene così effettuato utilizzando l'account di Active Directory.



Con questa semplice procedura la gestione delle autenticazioni e sicurezza della rete viene notevolmente alleggerita permettendo l'utilizzo di un solo account per l'accesso a più sistemi.

Migrare una VM creata con VMware Workstation su ESXi 4.1

Mettere in produzione un nuovo servizio di rete, richiede una giusta configurazione e una fase di test per evitare imprevisti e/o malfunzionamenti.

Con la tecnologia di virtualizzazione, creare una *virtual machine* (ad esempio un server posta, un database, etc.) sul proprio computer di sviluppo ed implementare il servizio in base alle esigenze è ormai all'ordine del giorno.

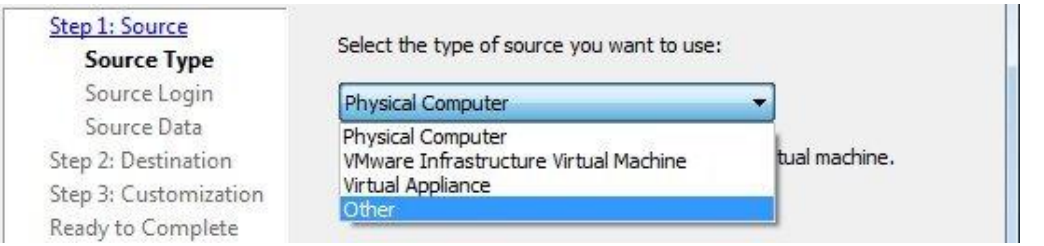
Quando la fase di lab risponde positivamente ai test, la *virtual machine* deve essere messa in produzione e quindi convertita in appliance per essere migrata sulla struttura vSphere (ESX/ESXi).

Procedura

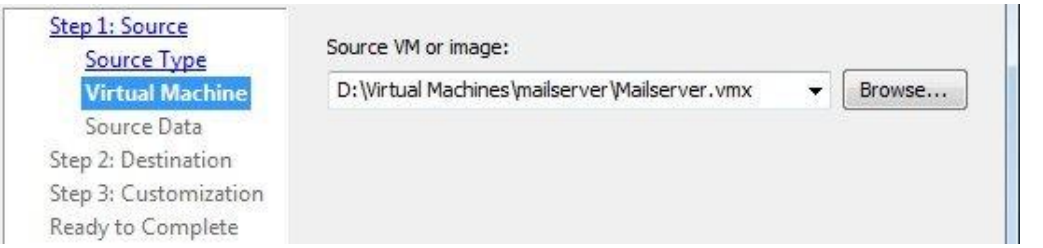
Da *VMware Workstation*, cliccare su File –> Import or Export.

Si apre la finestra Conversion Wizard che ci guida alla conversione della nostra virtual machine. cliccare Next per procedere.

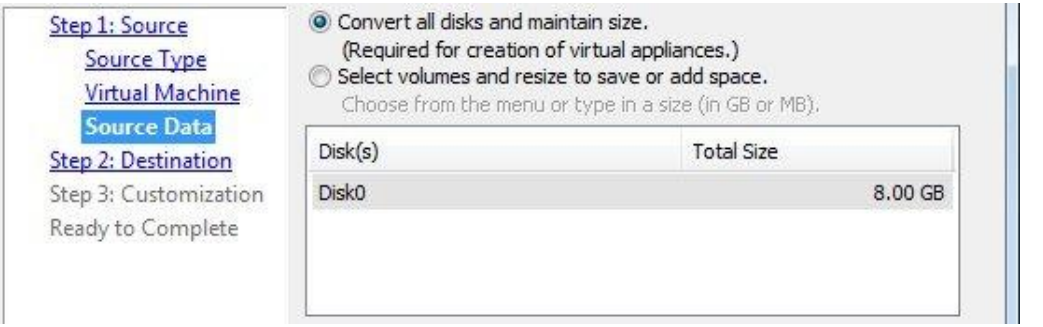
Poichè bisogna convertire una *virtual machine* creata con *VMware Workstation*, selezionare l'opzione Other e cliccare poi su Next.



Tramite il bottone Browse selezionare il file.vmx della VM da convertire. Click su Next.

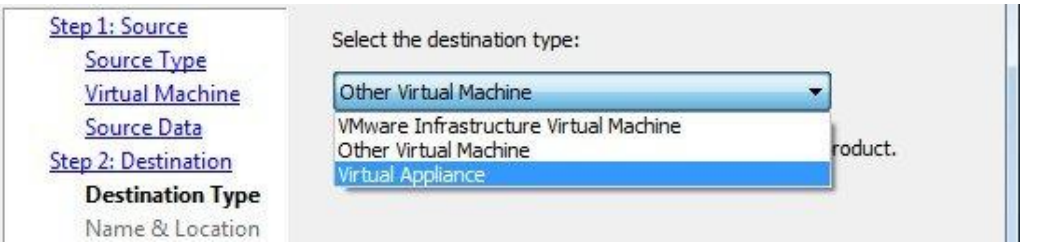


In questa finestra si può impostare un size del disco differente dall'originale. Selezionare l'impostazione che meglio risponde alle proprie esigenze. Click su Next.

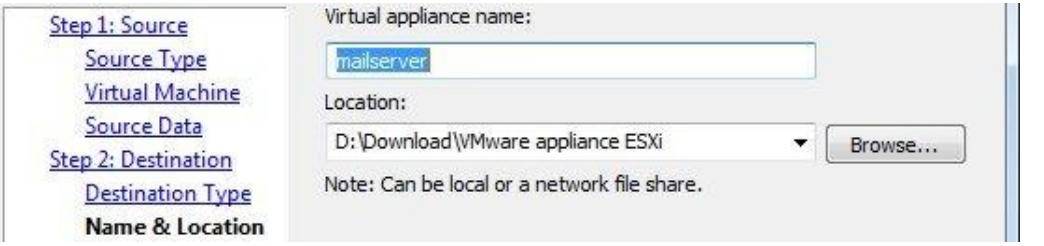


Impostati i parametri Source, il *Wizard* procede con la definizione dei valori di Destination. Non c'è nulla da configurare in questa finestra quindi click su Next per proseguire.

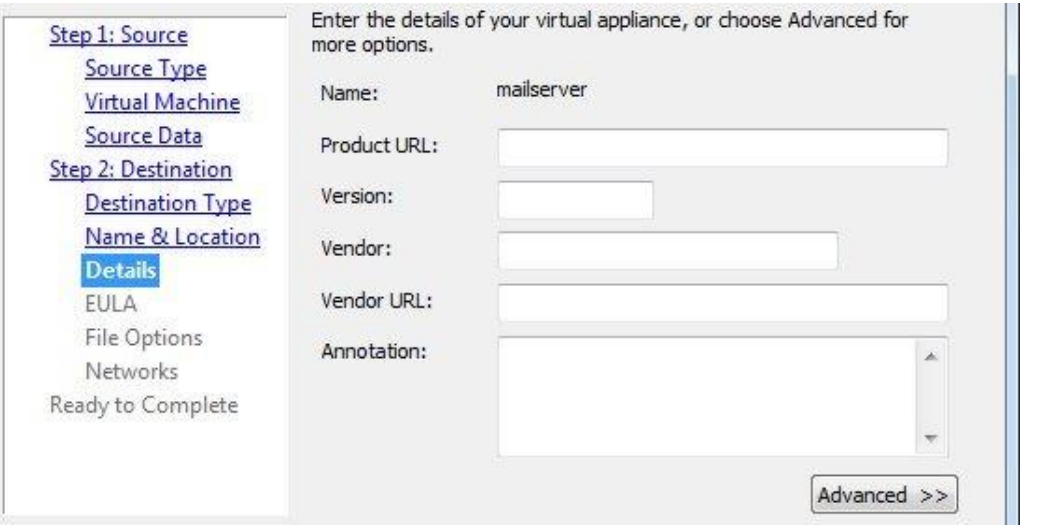
Poichè lo scopo è di convertire la VM in appliance, selezionare l'opzione Virtual Appliance e cliccare su Next.



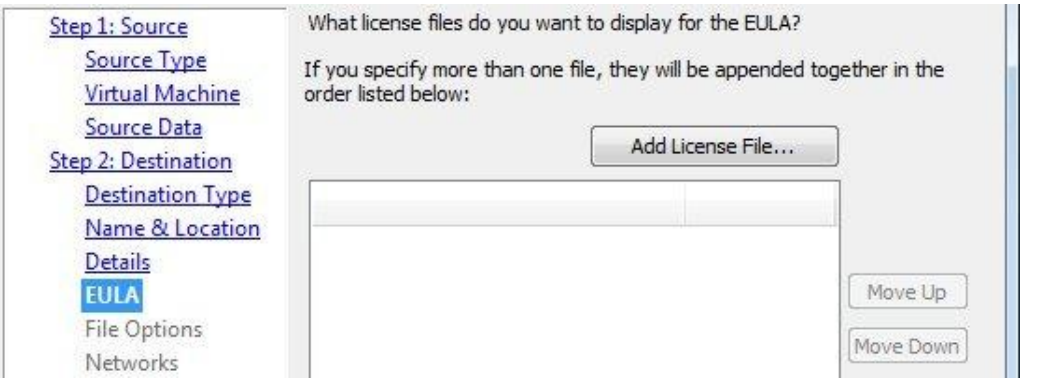
Dare un nome alla *Virtual Appliance* e specificare la Location su dove salvare i file. Click su Next.



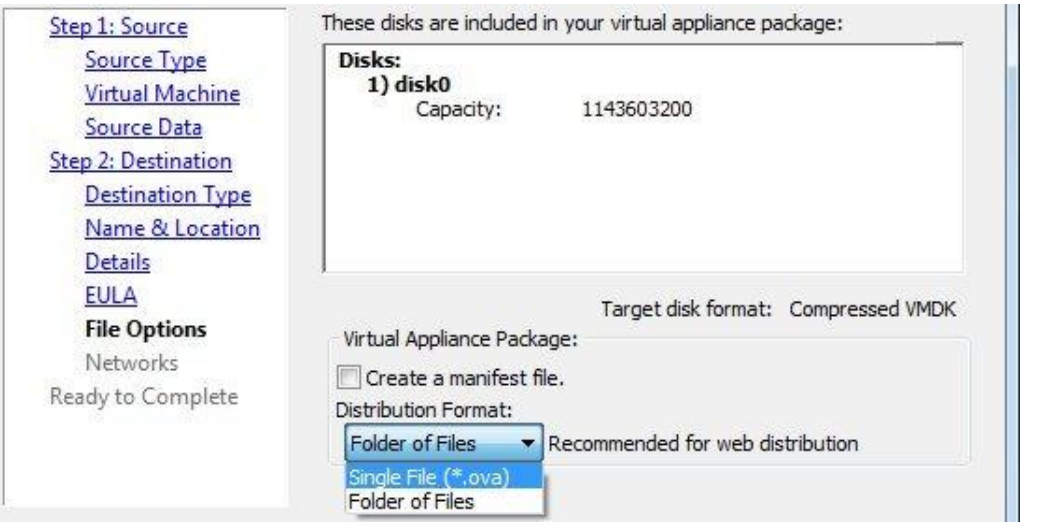
Specificare eventuali dettagli aggiuntivi se richiesto e cliccare su Next.



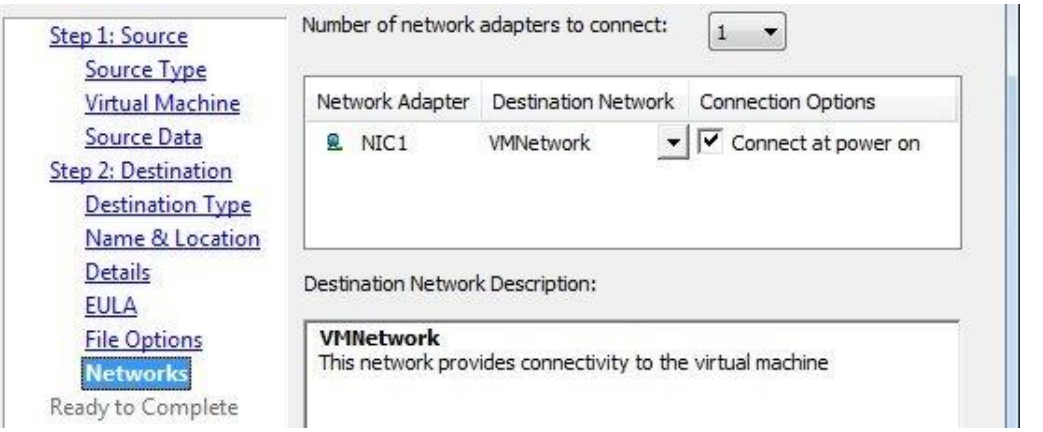
Se previsto, specificare un eventuale EULA. Click su Next.



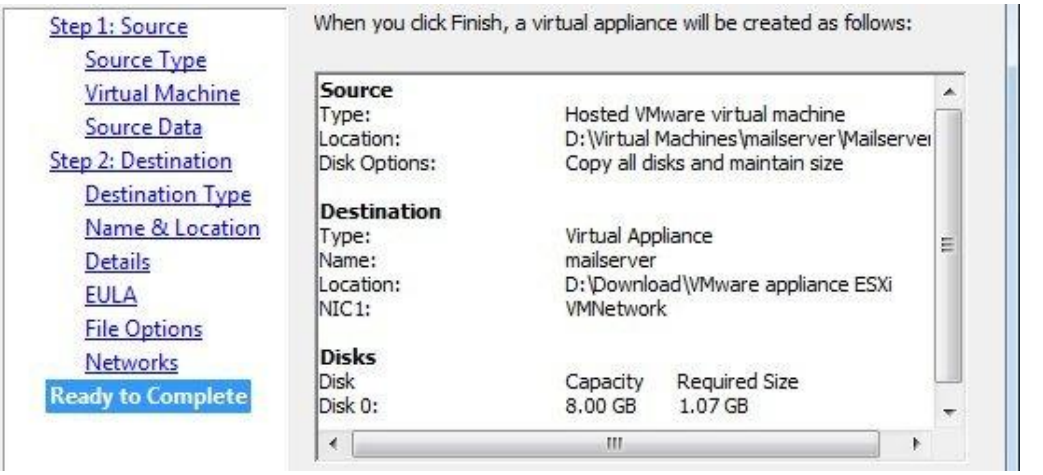
Qui specificare il tipo di Distribution Format. Nell'esempio l'opzione Single File permette di creare un unico file.ova. Click su Next.



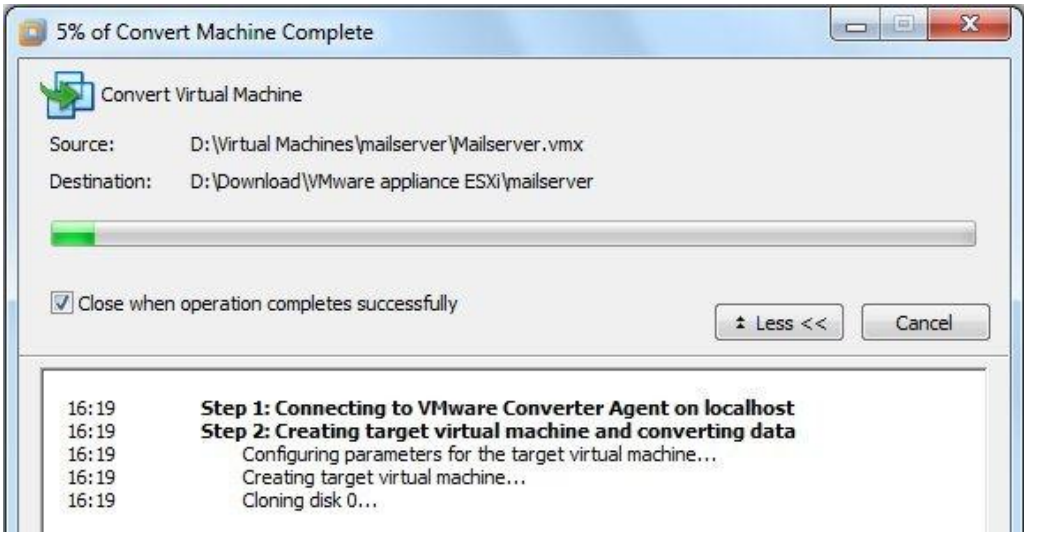
Associare il Network Adapter se è presente più di un NIC e abilitarlo o meno al power on. Click su Next.



Terminata la configurazione, viene presentato un riepilogo delle impostazioni effettuate. Click su Next per procedere con la conversione.

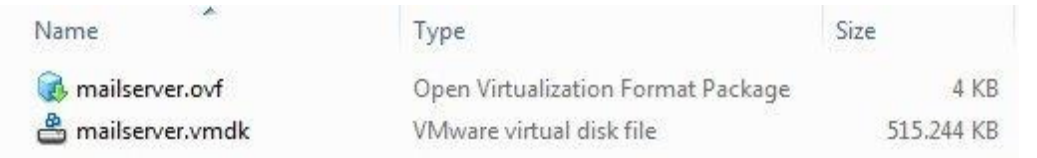


La fase di conversione ha inizio e la sua durata dipende dalla dimensione della *virtual machine* da convertire e dalla potenza del computer utilizzato.



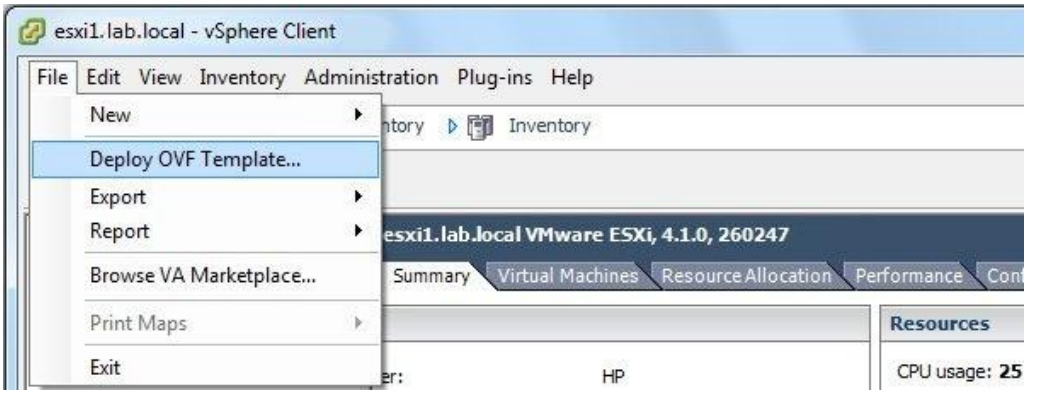
Terminata la conversione, i file creati dalla procedura sono due:

filename.ovf: contiene i parametri della virtual machine
filename.vmdk: contiene la virtual machine

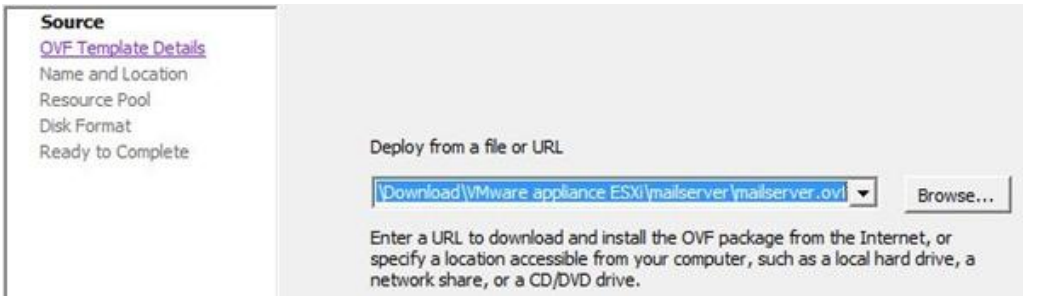


Importare l'appliance in ESXi

Da vSphere Client, cliccare su File –> Deploy OVF Template.

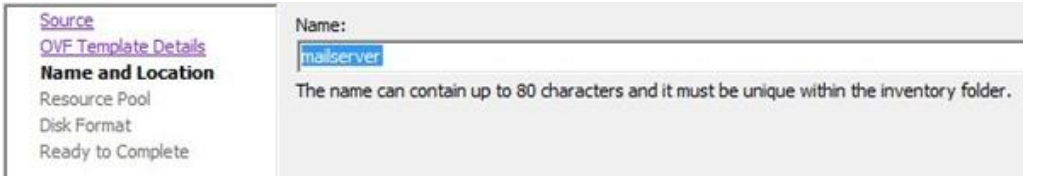


Specificare il file.ovf (appliance) da importare. Click su Next.

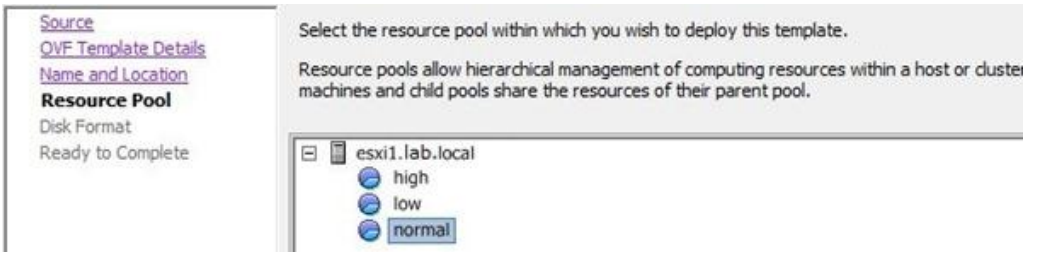


Vengono presentati i dettagli dall'appliance. Click su Next.

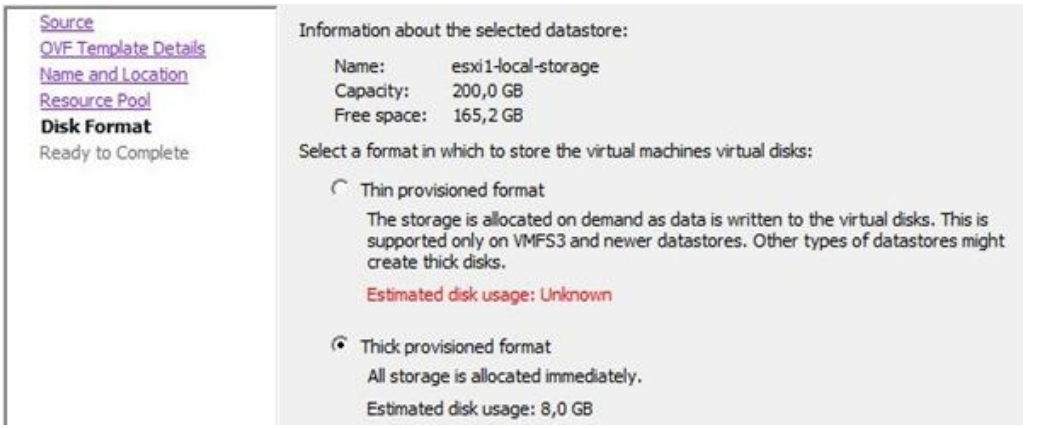
Specificare il nome della virtual machine in ESX. Per comodità e chiarezza converrebbe utilizzare lo stesso nome dato al file. Click su Next.



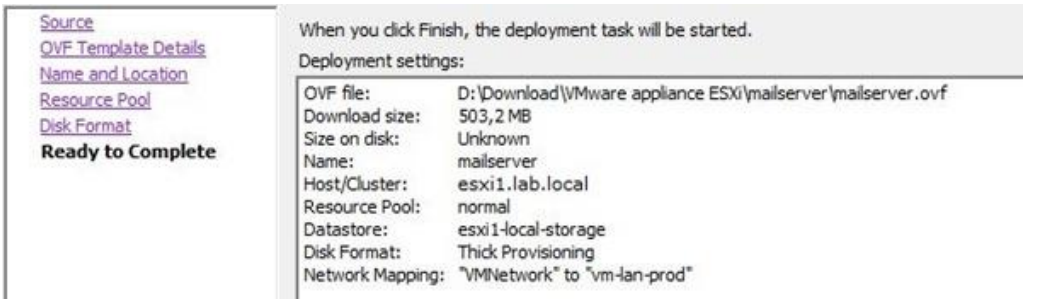
Se configurata in *ESXi, a*ssegnare l'appliance alla resource pool richiesta. Click su Next.



E' possibile selezionare l'opzione Thin provisioned format per risparmiare spazio sullo storage o Thick provisioned format (consigliato) per avere prestazioni migliori. Click su Next.

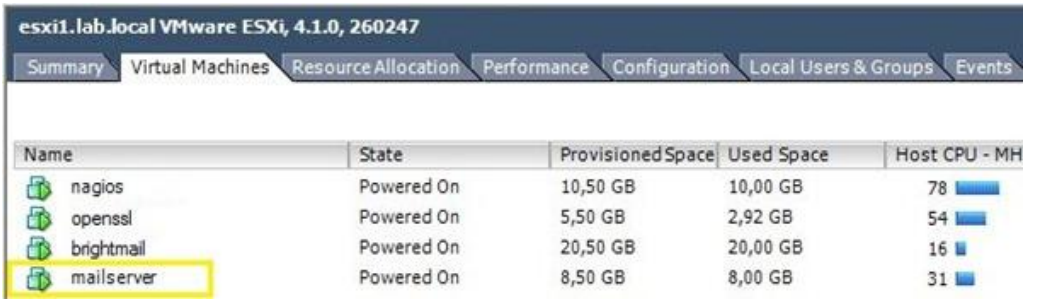


Vengono visualizzati i dettagli dei parametri impostati. Cliccare su Finish per importare l'appliance in ESXi.



La finestra successiva mostra il progress dell'operazione.

Terminata l'importazione, l'appliance compare nella lista delle *virtual machine* impostate sul server ESXi.



Una procedura molto semplice che permette di mettere in produzione delle *virtual machine* precedentemente create e testate con *VMware Workstation*.

Applicare le patch a VMware ESXi 4.1 tramite CLI

Con l'uscita delle patch e degli aggiornamenti rilasciati da VMware, si pone il problema di come applicare queste patch al sistema *ESXi*.

La versione gratuita di ESXi è largamente utilizzata nei vari lab e spesso anche in produzione ma non è possibile utilizzare vCenter Server senza la sua licenza e nemmeno l'host update utility, precedentemente disponibile fino alla release 4.0, ora rimossa nella nuova versione 4.1.

L'unico modo è utilizzare la *vSphere* Command Line Interface comunemente chiamata CLI per applicare gli aggiornamenti agli host *ESXi*.

Prerequisiti

Per poter eseguire la procedura di patching sono richiesti due componenti principali:

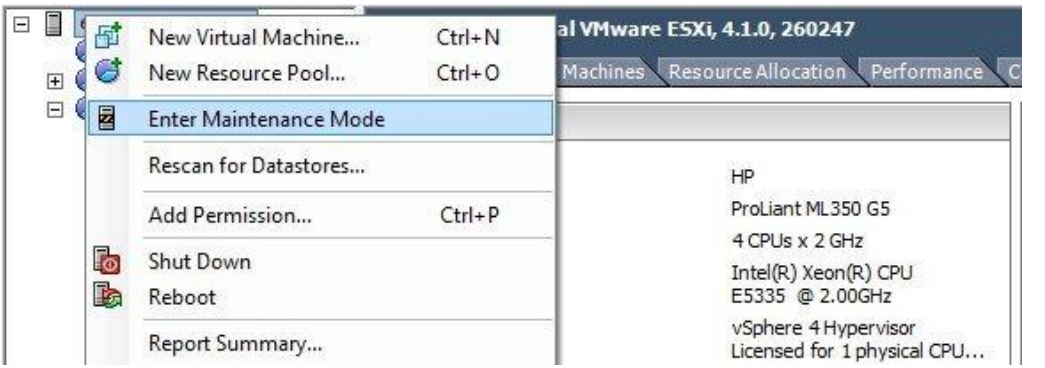
- VMware vSphere CLI 4.1
- Patch per ESXi

Installare *VMware vSphere CLI* sul proprio computer e scaricare dal sito *VMware* le patch per ESXi impostando i parametri di ricerca come in figura:

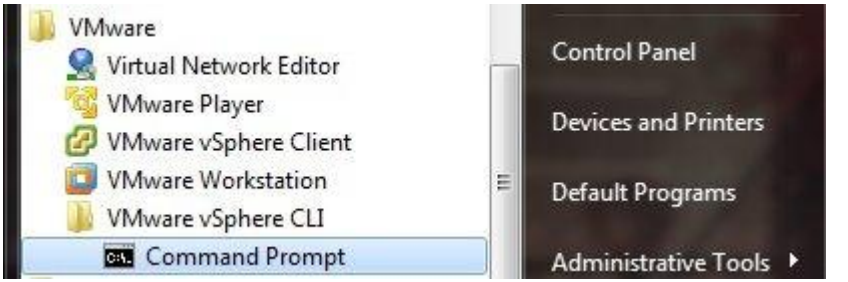
Selezionare la patch richiesta e cliccare sul bottone Download Now per scaricare il file .zip.

Procedura

Prima di procedere con l'applicazione delle patch, tramite *vSphere Client* spegnere le virtual machine presenti nell'host e mettere il server *ESXi* in Maintenance Mode.



Una volta che il sistema è in *Maintenance Mode*, lanciare da Windows il Command Prompt per digitare i vari comandi di *vSphere CLI*.



Poichè il package scaricato *filename.zip* potrebbe contenere diversi file di patch da applicare (come in questo caso), visualizzare il contenuto del package tramite il comando:

```
vihostupdate.pl --server IP_ESXi --username root --password
password -b namefilepatch.zip -l
```

```
D:\Network\ESXi patches>vihostupdate.pl --server 192.168.10.100 --username root
--password password -b ESXi410-201010001.zip -l

---------Bulletin ID---------   ----------------Summary-----------------
ESXi410-201010401-SG            Updates Firmware
ESXi410-201010402-BG            Updates VMware Tools
```

In questo package sono contenuti due file di patch o, per l'esattezza, Bulletin ID.

- ESXi410-201010401-SG
- ESXi410-201010402-BG

Applicare le patch effettuando l'operazione per tutti i *Bulletin ID* contenuti nel package utilizzando l'istruzione:

```
vihostupdate.pl --server IP_ESXi --username root --password
password -i -b namefilepatch.zip -B BulletinID
```

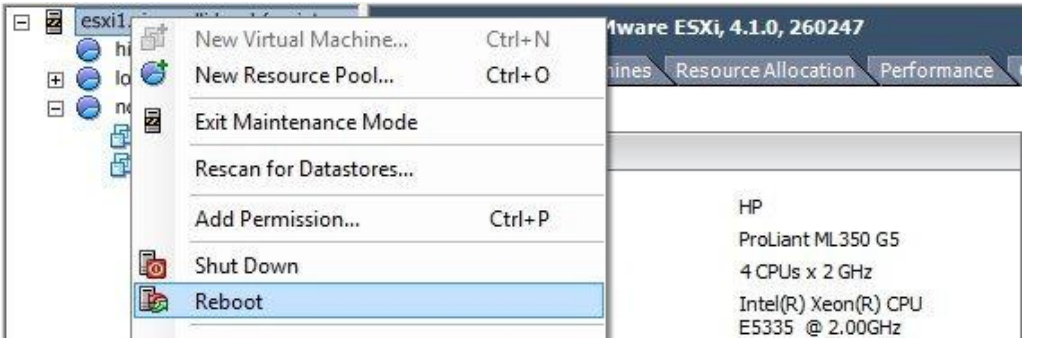
Applicare la prima patch *ESXi410-201010401-SG*.

```
D:\Network\ESXi patches>vihostupdate.pl --server 192.168.10.100 --username root
--password password -i -b ESXi410-201010001.zip -B ESXi410-201010401-SG
Please wait patch installation is in progress ...
The update completed successfully, but the system needs to be rebooted for the c
hanges to be effective.

D:\Network\ESXi patches>_
```

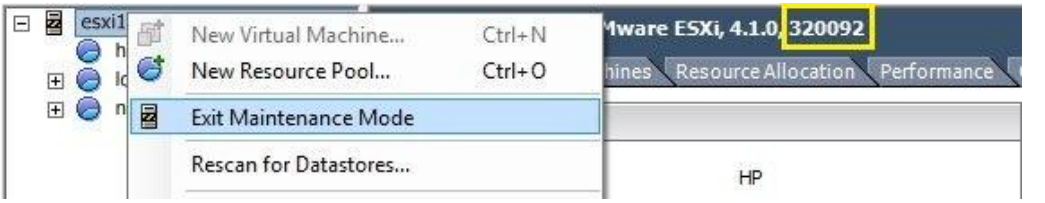
Applicare la seconda patch *ESXi410-201010402-BG*.

```
D:\Network\ESXi patches>vihostupdate.pl --server 192.168.10.100 --username root
--password password -i -b ESXi410-201010001.zip -B ESXi410-201010402-BG
Please wait patch installation is in progress ...
Host updated successfully.

D:\Network\ESXi patches>_
```

Da *vSphere Client* riavviare l'host *ESXi*.



Riavviato il sistema, uscire dalla *Maintenance Mode*. Ora è possibile riavviare nuovamente le *virtual machine*. Da notare il numero della versione riportata che adesso è variata dopo aver applicato le patch.



In questo modo siamo sicuri che il nostro sistema gode delle ultime patch e rimane allineato con gli aggiornamenti rilasciati periodicamente da *VMware*.

Aggiornare VMware ESXi 4.1 alla versione 5.0

Con l'uscita della nuova versione di VMware ESXi 5.0.0, è tempo di effettuare l'upgrade dei server alla nuova versione.

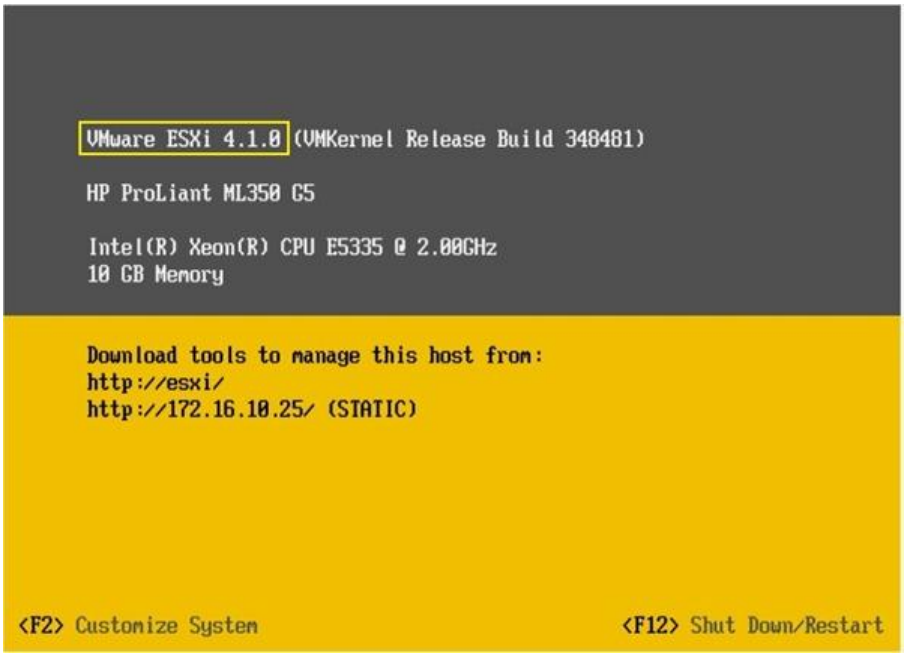
L'operazione di aggiornamento risulta semplice ed immediata senza implicare particolari configurazioni.

Naturalmente prima di effettuare la procedura e sempre buona cosa effettuare un backup delle virtual machine presenti sull'host in aggiornamento.

Procedura

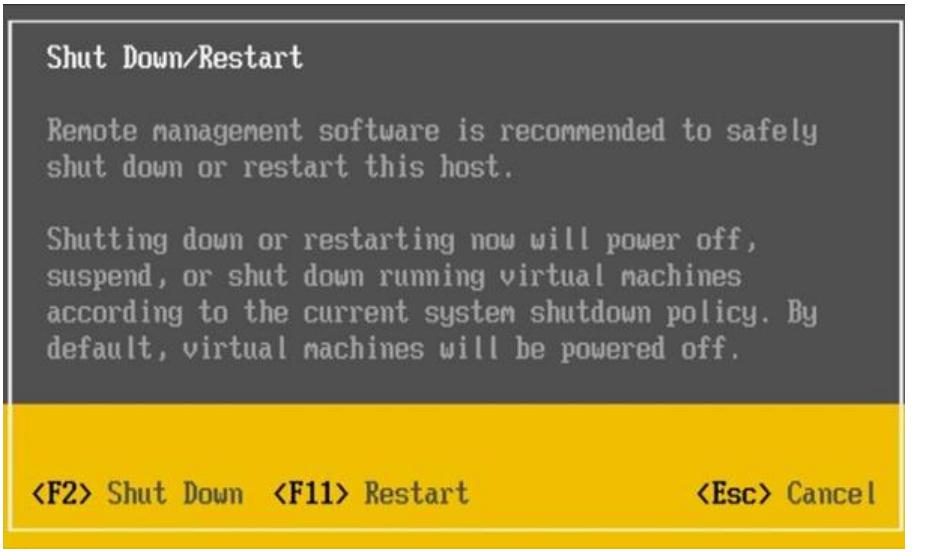
Scaricare il software dal sito VMware, ed inserire il CD di installazione nel drive del server fisico da aggiornare.

Premere il tasto F12 per effettuare il reboot dell'host ESXi da aggiornare.



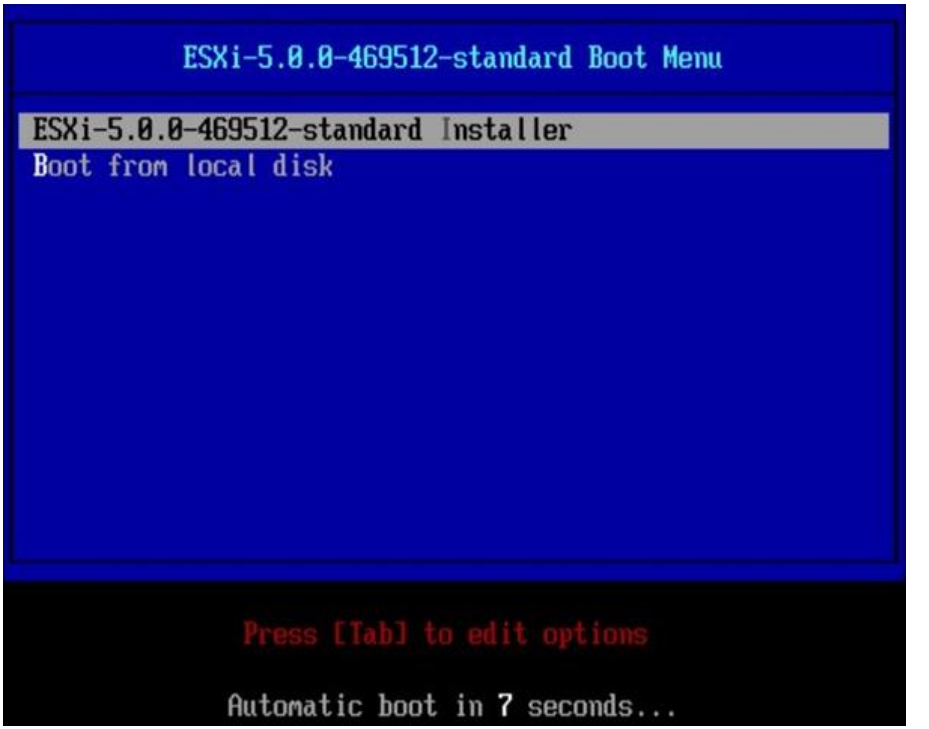
Inserire le credenziali dell'utente autorizzato per effettuare l'operazione di reboot.

Premere il tasto F11 per avviare la procedura di reboot del sistema.



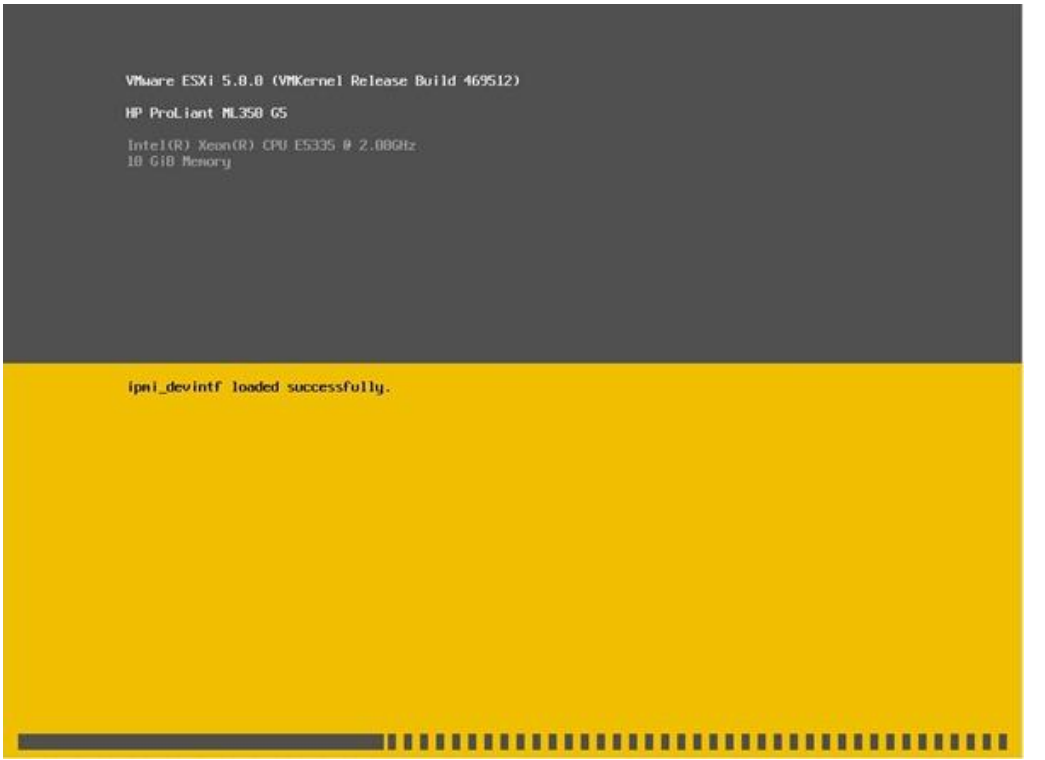
Il sistema inizia la fase di reboot.

Al riavvio del server, il sistema effettua il boot dal CD precedentemente inserito visualizzando il Boot Menu. Premere Invio per iniziare l'upgrade.

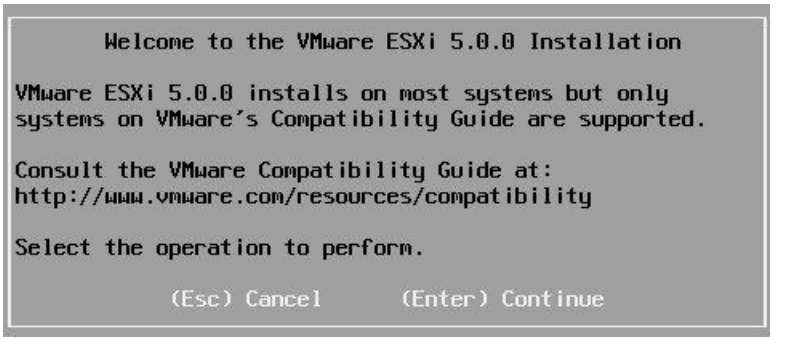


Vengono caricati i file di sistema necessari ad effettuare l'aggiornamento.

Compare la finestra in cui l'operazione di boot del sistema indica la nuova versione di ESXi in avvio.



Premere Invio per proseguire.



Premere F11 per accettare l'EULA.

```
End User License Agreement (EULA)

VMWARE END USER LICENSE AGREEMENT

IMPORTANT-READ CAREFULLY:  BY DOWNLOADING, INSTALLING, OR
USING THE SOFTWARE, YOU (THE INDIVIDUAL OR LEGAL ENTITY)
AGREE TO BE BOUND BY THE TERMS OF THIS END USER LICENSE
AGREEMENT ("EULA").  IF YOU DO NOT AGREE TO THE TERMS OF
THIS EULA, YOU MUST NOT DOWNLOAD, INSTALL, OR USE THE
SOFTWARE, AND YOU MUST DELETE OR RETURN THE UNUSED SOFTWARE
TO THE VENDOR FROM WHICH YOU ACQUIRED IT WITHIN THIRTY (30)
DAYS AND REQUEST A REFUND OF THE LICENSE FEE, IF ANY, THAT
YOU PAID FOR THE SOFTWARE.

EVALUATION LICENSE.  If You are licensing the Software for
evaluation purposes, your use of the Software is only
permitted in a non-production environment and for the period

Use the arrow keys to scroll the EULA text

(ESC) Do not Accept      (F11) Accept and Continue
```

Il sistema effettua lo scan per rilevare i device presenti nel server.

```
Scanning...

Scanning for available devices. This may take a few seconds.
```

Selezionare il disco da aggiornare e premere Invio.

```
Select a Disk to Install or Upgrade

* Contains a VMFS partition

Storage Device                                                  Capacity
-----------------------------------------------------------------------
Local:
 * VMware   Block device     (mpx.vmhba1:C0:T0:L0)          205.00 GiB
Remote:
   (none)

(Esc) Cancel    (F1) Details    (F5) Refresh    (Enter) Continue
```

Viene effettuata un'ulteriore scansione del drive selezionato.

```
Scanning...

Gathering additional information from the selected device.
This will take a few moments.
```

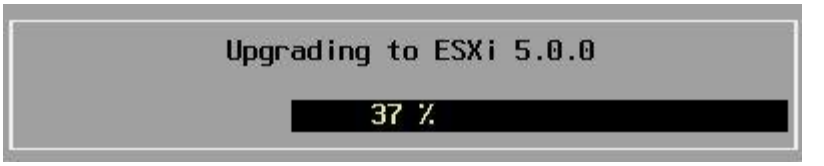
Se non si hanno particolari esigenze, lasciare l'opzione di default proposta selezionata e premere OK.

```
ESXi and VMFS Found

The selected storage device contains an installation of
ESXi and a VMFS datastore.  Choose whether to upgrade
or install and overwrite the existing ESXi
installation.  Also choose whether to preserve or
overwrite the existing VMFS datastore.

* Your system has custom VIBs (shown on next screen).
Proceeding with migration could cause it to not boot,
experience instability, or needed features may not be
present. You can use ImageBuilder to create an ISO with
VIBs that replace your custom VIBs.

(X) Force Migrate ESXi, preserve VMFS datastore *
( ) Install ESXi, preserve VMFS datastore
( ) Install ESXi, overwrite VMFS datastore

  Use the arrow keys and spacebar to select an option.

(Esc) Cancel      (Enter) OK
```

Raccolte le informazioni necessarie per l'aggiornamento, premere F11 per avviare il processo.

```
Confirm Upgrade

ESXi 5.0.0 is configured to be installed on:
mpx.vmhba1:C0:T0:L0.

(Esc) Cancel      (F9) Back      (F11) Upgrade
```

Il sistema effettua l'aggiornamento alla nuova versione 5.0.0.



Quando l'operazione termina, viene visualizzata una schermata con lo status di aggiornamento (*successfully*). Rimuovere il CD di installazione dal drive e premere Invio per effettuare il reboot.

Quando termina la fase di boot di ESXi, la nuova schermata principale di ESXi 5.0.0 è visualizzata.

Con questa semplice procedura, il server è stato aggiornato alla nuova versione 5.0.0.

Installare le patch per VMware ESXi 5.0 tramite CLI

Dopo l'uscita ad Agosto della versione 5.0 di ESXi che di fatto introduce vSphere 5.0, *VMware* ha rilasciato la prima patch ESXi500-201109001 per la nuova release in cui vengono risolti alcuni bug ed introdotte delle migliorie.

Utilizzando il server ESXi non provvisto di command-line (con la versione 5 tutti gli ESX diventano ESXi) l'aggiornamento viene effettuato tramite vCenter Server, che richiede una costosa licenza, o tramite Command-Line Interface (CLI). E' importante installare le patch segnalate per tenere il sistema sempre efficiente e stabile.

Release Name	Description	Bulletin List	Category	Severity
ESXi500-201109001 Download **Product: :** ESXi (Embedded and Installable) 5.0.0 md5sum:9715997578351b01bef0eb4cc890cb75 sha1sum:44ec3c11019333a3fd4afc39794a4058e7399173 Download Size: 295.5 MB Build Number: 474610 KB 2001075 **Release Date: :** 09/13/2011 **System Impact :** VM Shutdown & Host Reboot	Updates tools-light Details	ESXi500-201109402-BG KB 2002778	Enhancement	Moderate
	Updates esx-base Details	ESXi500-201109401-BG KB 1027808	Bug Fix	Important

Informazioni più dettagliate si possono trovare nelle Patch Release Notes.

Bulletin ID	Category	Knowledge Base Article
ESXi500-201109401-BG	Bug Fix	KB 1027808
ESXi500-201109402-BG	Enhancement	KB 2002778

Prerequisiti

Per effettuare l'aggiornamento sono richiesti due componenti:

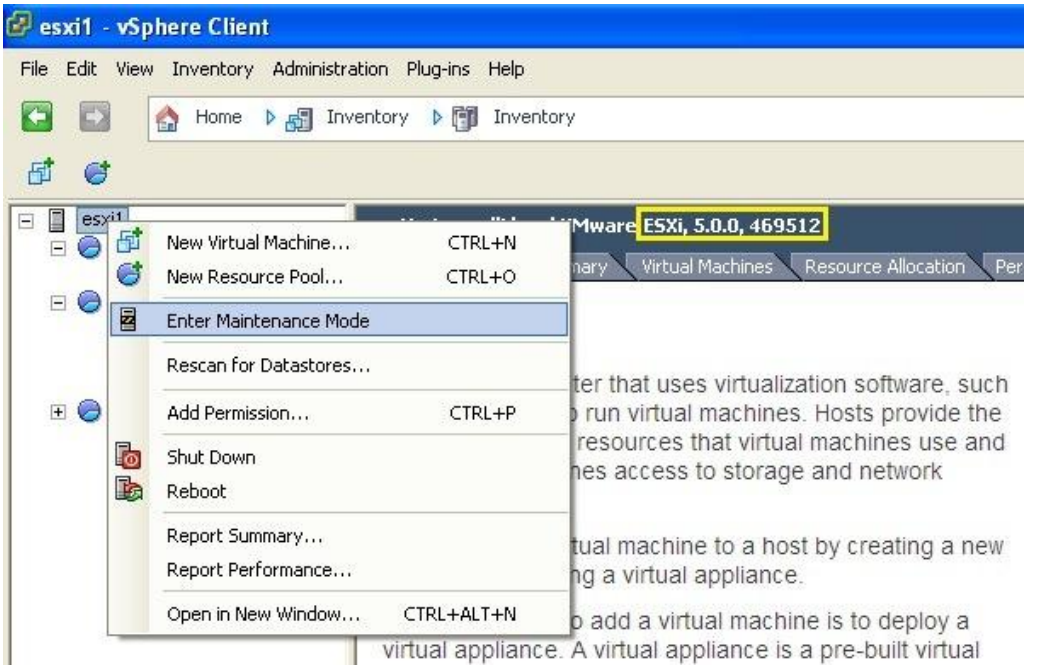
- Installazione di VMware vSphere CLI 5.0 che permette di effettuare il *patching* tramite command line.
- Download della patch ESXi500-201109001.

Procedura

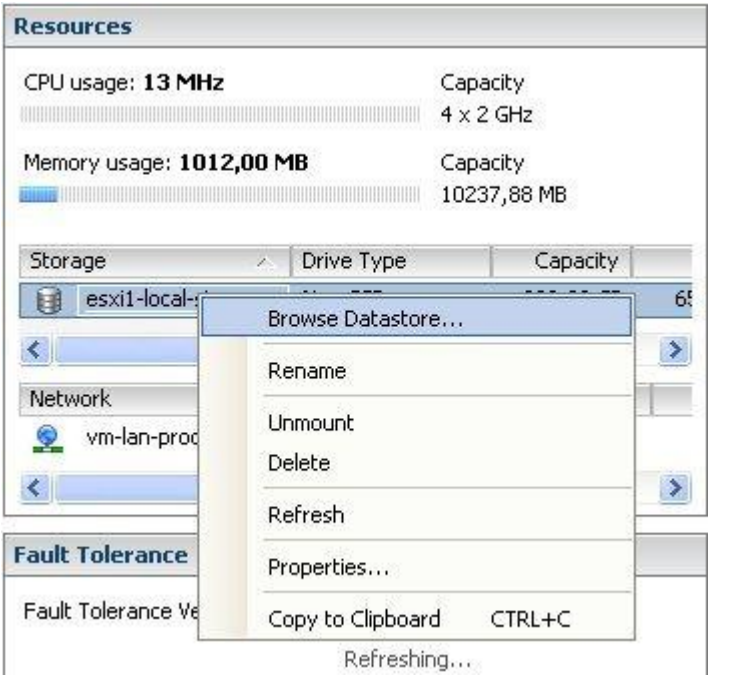
Installare sul proprio PC la versione 5.0 delle *vSphere CLI* per poter operare sulla versione nuova di *ESXi*.

Scaricata la patch dal sito *VMware*, avviare *vSphere Client 5* per la gestione dell'host *ESXi*.

Effettuare il vMotion o lo shutdown delle virtual machine attive e mettere l'*ESXi* da aggiornare in Maintenance Mode. Annotare la versione di *ESXi*: 5.0.0, 469512.



Copiare la patch di ESXi precedentemente scaricata nel datastore dell'ESXi da aggiornare. Accedere al datastore locale selezionando l'ESXi da aggiornare e cliccare con il tato destro del mouse sulla schermata di destra la voce Storage –> Browse Datastore nella sezione Resources.



Per comodità creare nel datastore un folder con nome patches ad esempio.

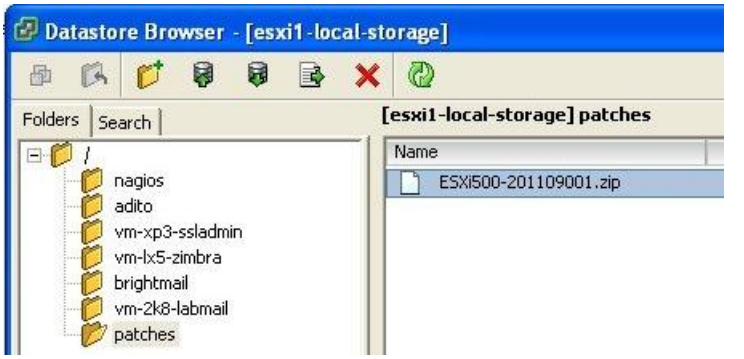
Cliccare sull'icona per effettuare l'upload del file.

Selezionare il file da caricare (in questo caso il file .zip della patch) e cliccare su Open.

Cliccare su Yes al messaggio di warning che compare.

Il file viene copiato nel datastore specificato.

Terminata l'operazione il file è visibile tramite il Datastore Browser.



Accedere alla command-line per eseguire i comandi di *vSphere CLI*. A differenza della versione *ESXi 4.1*, il comando vihostupdate.pl non è più utilizzato nella versione 5.0 e per effettuare la procedura di *patching* si utilizza il comando esxcli. Fare riferimento al manuale vSphere Upgrade Guide per maggiori dettagli.

Per visualizzare il contenuto dei VIB nel file .zip scaricato, lanciare il comando:

```
esxcli -server=hostname/IP_address software sources vib list -
depot=path_to_patch/patch_name.zip
```

```
esxcli -server=esxi1 software sources vib list -
depot=/vmfs/volumes/esxi1-local-storage/patches/ESXi500-
201109001.zip
```

```
C:\Programmi\VMware\VMware vSphere CLI>esxcli --server=esxi1 software sources vi
b list --depot=/vmfs/volumes/esxi1-local-storage/patches/ESXi500-201109001.zip
Enter username: root
Enter password:
Name                    Version                          Vendor  Release Date
Acceptance Level  Status
-------------------  ---------------------------------  ------  ------------
----------------  ---------
net-ixgbe               2.0.84.8.2-10vmw.500.0.0.469512  VMware  2011-08-19
VMwareCertified   Installed
ata-pata-hpt3x2n        0.3.4-3vmw.500.0.0.469512        VMware  2011-08-19
VMwareCertified   Installed
esx-base                5.0.0-0.3.474610                 VMware  2011-09-13
VMwareCertified   Update
ehci-ehci-hcd           1.0-3vmw.500.0.0.469512          VMware  2011-08-19
VMwareCertified   Installed
ata-pata-atiixp         0.4.6-3vmw.500.0.0.469512        VMware  2011-08-19
VMwareCertified   Installed
scsi-megaraid2          2.00.4-9vmw.500.0.0.469512       VMware  2011-08-19
VMwareCertified   Installed
sata-sata-sil           2.3-3vmw.500.0.0.469512          VMware  2011-08-19
VMwareCertified   Installed
net-r8168               8.013.00-3vmw.500.0.0.469512     VMware  2011-08-19
```

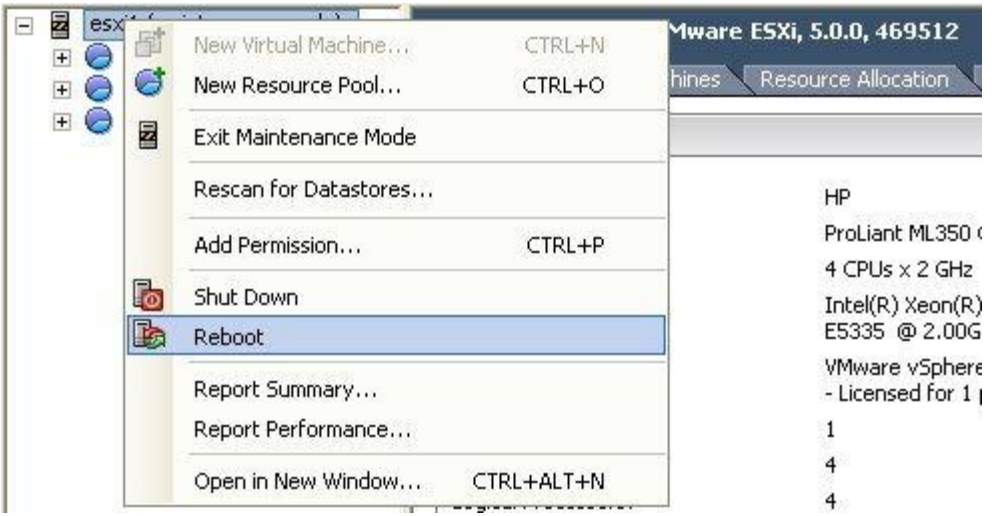
Per installare i nuovi VIB, utilizzare il comando:

```
esxcli -server=hostname/IP_address software vib update -
depot=path_to_patch/patch_name.zip
```

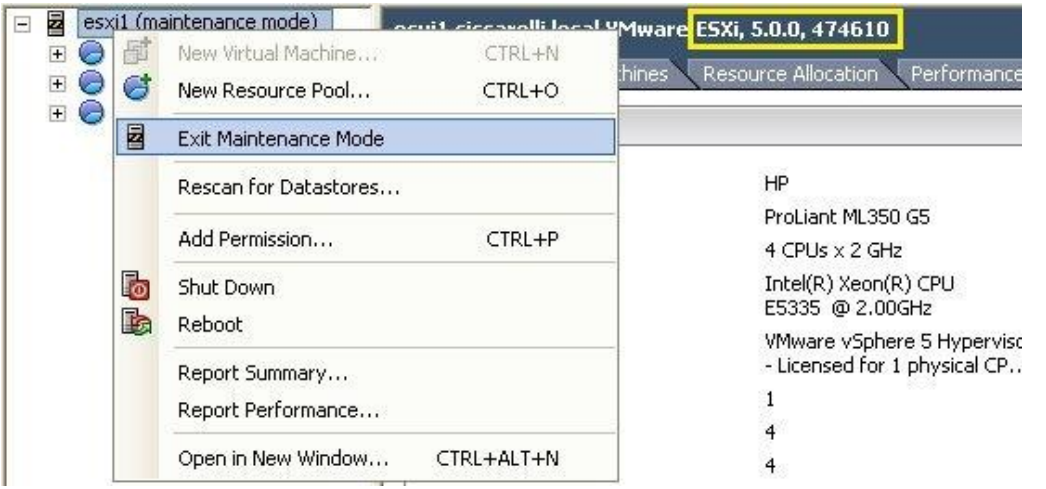
```
# esxcli -server=esxi1 software vib update -
depot=/vmfs/volumes/esxi1-local-storage/patches/ESXi500-
201109001.zip
```

```
C:\Programmi\VMware\VMware vSphere CLI>esxcli --server=esxi1 software vib update
 --depot=/vmfs/volumes/esxi1-local-storage/patches/ESXi500-201109001.zip
Enter username: root
Enter password:
Installation Result
   Message: The update completed successfully, but the system needs to be reboot
ed for the changes to be effective.
   Reboot Required: true
   VIBs Installed: VMware_bootbank_esx-base_5.0.0-0.3.474610, VMware_locker_tool
s-light_5.0.0-0.3.474610
   VIBs Removed: VMware_bootbank_esx-base_5.0.0-0.0.469512, VMware_locker_tools-
light_5.0.0-0.0.469512
   VIBs Skipped: VMware_bootbank_ata-pata-amd_0.3.10-3vmw.500.0.0.469512, VMware
_bootbank_ata-pata-atiixp_0.4.6-3vmw.500.0.0.469512, VMware_bootbank_ata-pata-cm
d64x_0.2.5-3vmw.500.0.0.469512, VMware_bootbank_ata-pata-hpt3x2n_0.3.4-3vmw.500.
0.0.469512, VMware_bootbank_ata-pata-pdc2027x_1.0-3vmw.500.0.0.469512, VMware_bo
otbank_ata-pata-serverworks_0.4.3-3vmw.500.0.0.469512, VMware_bootbank_ata-pata-
sil680_0.4.8-3vmw.500.0.0.469512, VMware_bootbank_ata-pata-via_0.3.3-2vmw.500.0.
0.469512, VMware_bootbank_block-cciss_3.6.14-10vmw.500.0.0.469512, VMware_bootba
nk_ehci-ehci-hcd_1.0-3vmw.500.0.0.469512, VMware_bootbank_esx-tboot_5.0.0-0.0.46
9512, VMware_bootbank_ima-qla4xxx_2.01.07-1vmw.500.0.0.469512, VMware_bootbank_i
pmi-ipmi-devintf_39.1-4vmw.500.0.0.469512, VMware_bootbank_ipmi-ipmi-msghandler_
39.1-4vmw.500.0.0.469512, VMware_bootbank_ipmi-ipmi-si-drv_39.1-4vmw.500.0.0.469
```

Poichè la patch applicata richiede il reboot dell'host, tramite *vSphere Client 5* procedere con il reboot dell'ESXi.

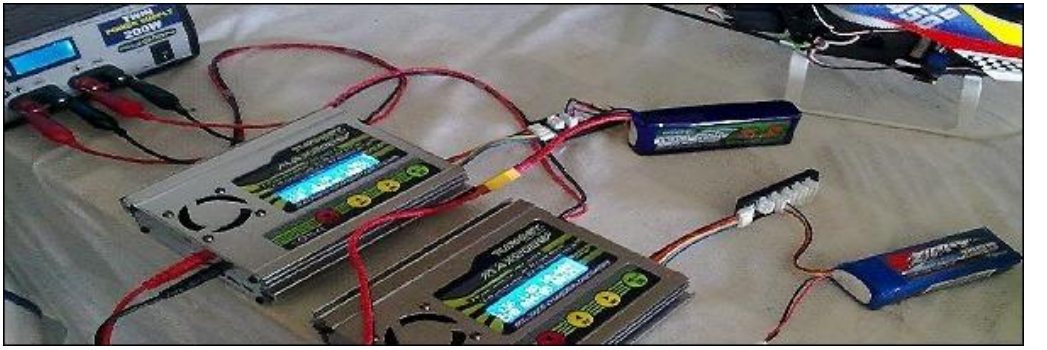


Effettuato il reboot, tramite *vSphere Client* verificare il numero della release che ora dovrebbe essere 5.0.0, 474610 e confrontarlo con il numero precedentemente annotato. Il numero di release è stato incrementato come previsto per l'applicazione della patch. Uscire dalla Maintenance Mode e avviare le virtual machine richieste.



Il server *ESXi 5.0* è aggiornato e pronto per ritornare in produzione. E' fortemente consigliato testare la procedura di patching su sistemi lab per non impattare sui servizi di rete operativi.

Backup della configurazione di ESX(i) 4.x, 5.x tramite vMA



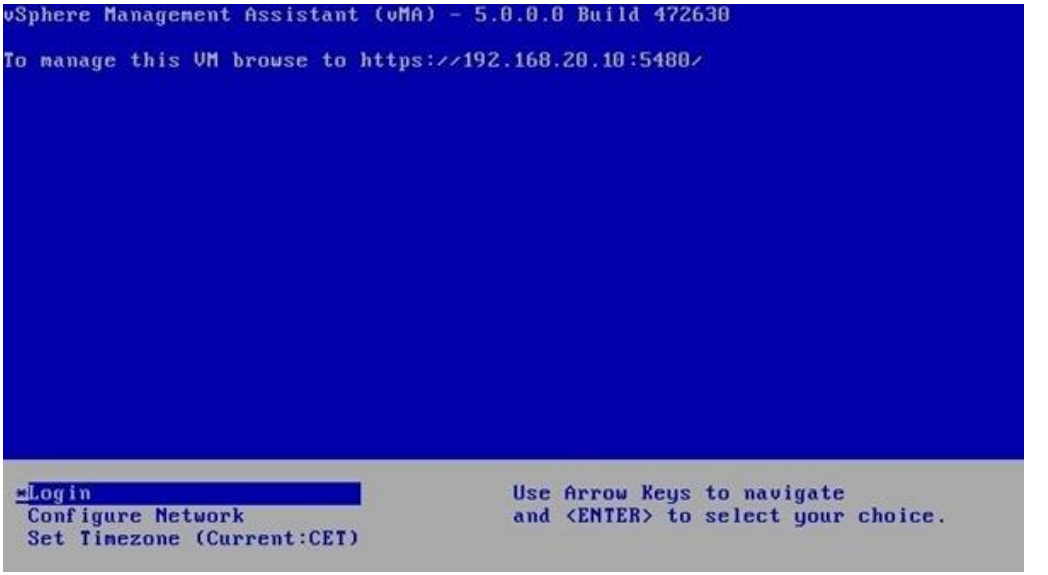
Ripristinare o reinstallare un server ESX in tempi rapidi permette di ristabilire la piena funzionalità della struttura virtuale limitando al minimo disservizi potenzialmente dannosi al business svolto.

L'operazione è possibile tramite l'appliance *VMware* vSphere Management Assistant che permette di eseguire script da console per interagire con i server ESX(i).

Prerequisiti

Dal sito *VMware* scaricare vSphere Management Assistant ed effettuare l'installazione della virtual machine.

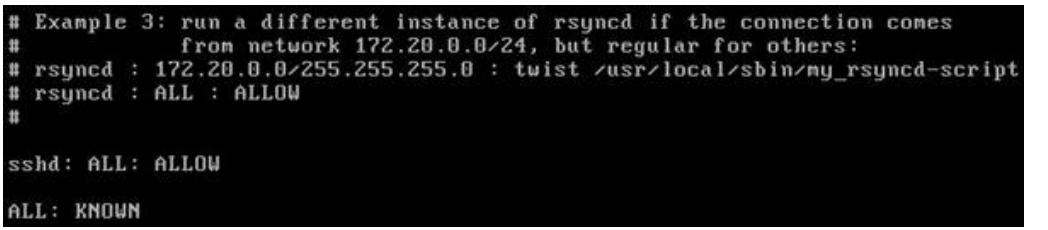
Avviare la virtual machine ed impostare, come richiesto, i parametri di rete e la password dell'utente vi-admin. Terminata l'operazione, viene visualizzata la schermata di default di vMA.



Connettersi in SSH a vMA tramite *PuTTY*, *KiTTY* o tool simili. Se la connessione in SSH dovesse fallire, editare il file */etc/hosts.allow* ed aggiungere la riga:

sshd: ALL: ALLOW

```
# sudo vi /etc/hosts.allow
```



Backup della configurazione

Da console, creare una directory backup in cui verrà salvato il backup e assegnare i corretti permessi di scrittura.

```
# sudo mkdir /backup
# sudo chmod 770 /backup
```

```
vi-admin@vm-lx-vma:/> sudo mkdir /backup
vi-admin@vm-lx-vma:/> sudo chmod 770 /backup/
vi-admin@vm-lx-vma:/> ll
total 89
drwxrwx---  2 root root  4096 2011-12-12 15:36 backup
drwxr-xr-x  2 root root  4096 2011-08-23 22:12 bin
drwxr-xr-x  4 root root  1024 2011-08-23 22:12 boot
drwxr-xr-x 11 root root  4300 2011-12-12 15:14 dev
drwxr-xr-x 77 root root  4096 2011-12-12 15:14 etc
```

Per effettuare il backup della configurazione, utilizzare da console il comando nella forma:

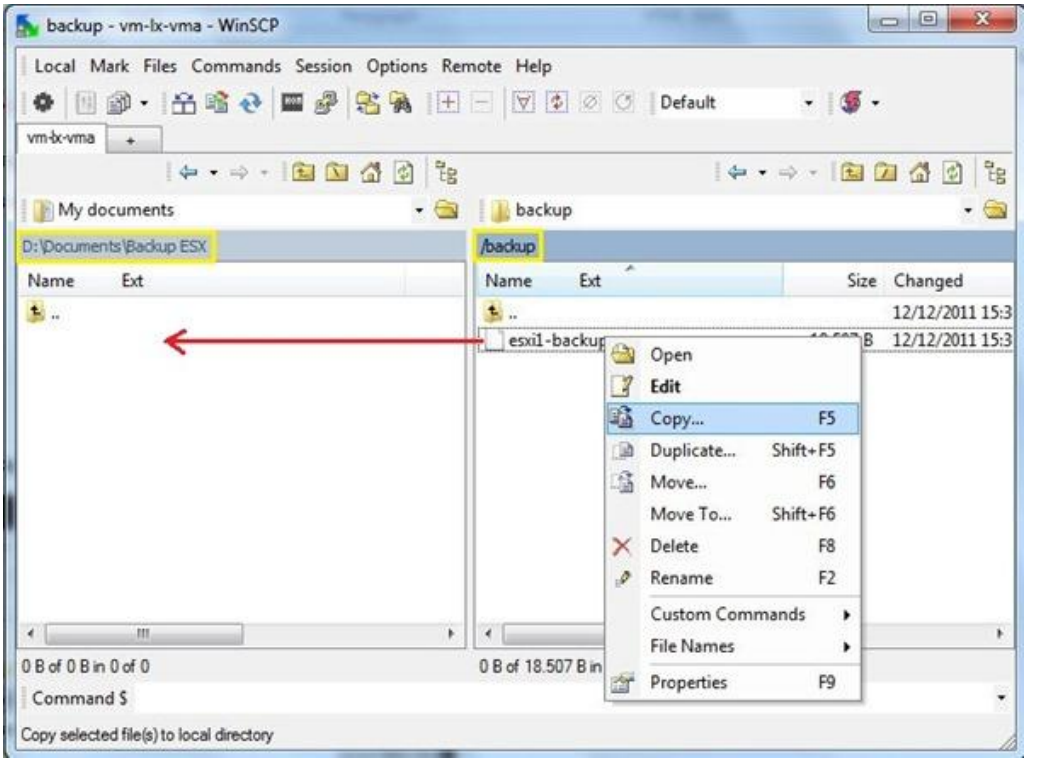
*vicfg-cfgbackup -s -server IP_address_ESX path_destination**

**path_destination* è la directory all'interno della virtual machine *vMA* precedentemente creata.

```
# vicfg-cfgbackup -s -server 192.168.20.10 /backup/esxi1-backup
```

```
vi-admin@vm-lx-vma:/> vicfg-cfgbackup -s -server 192.168.20.10 /backup/esxi
1-backup
Enter username: root
Enter password:
Saving firmware configuration to /backup/esxi1-backup ...
vi-admin@vm-lx-vma:/> ll /backup/
total 20
-rw------- 1 vi-admin root 18507 2011-12-12 15:36 esxi1-backup
vi-admin@vm-lx-vma:/> sudo mkdir /backup
```

Per salvare il file di configurazione nel proprio PC, tramite *WinSCP* o programmi simili collegarsi a *vMA e* copiare il file di backup precedentemente creato.



Restore della configurazione

Per ripristinare la configurazione salvata, effettuare innanzitutto lo shutdown delle virtual machine attive.

Da console digitare il comando nella forma:

vicfg-cfgbackup -l -server IP_address_ESX path_destination

```
# vicfg-cfgbackup -l -server 192.168.20.10 /backup/esxi1-backup
```

```
vi-admin@vm-lx-vma:~> vicfg-cfgbackup -l -server 192.168.20.10 /backup/esxi1-bac
kup
Enter username: root
Enter password:
The restore operation will reboot the host.
Type 'yes' to continue:
_
```

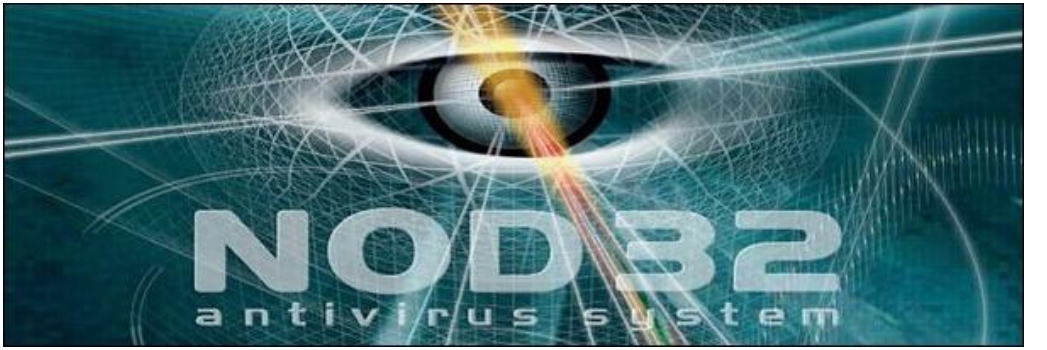
Per eseguire il restore, digitare YES e premere Invio. Completato il restore, il server ESX(i) viene riavviato per completare l'operazione.

```
vi-admin@vm-lx-vma:/> vicfg-cfgbackup -l -server 192.168.20.10 /backup/esxi1-bac
kup
Enter username: root
Enter password:
The restore operation will reboot the host.
Type 'yes' to continue:
yes
Uploading config bundle to configBundle.tgz ...
Performing restore ...
vi-admin@vm-lx-vma:/> _
```

Avere il backup della configurazione di un server facilita notevolmente il lavoro evitando di dover riconfigurare manualmente tutto il sistema.

Sicurezza

Installare NOD32 ERAS su Windows 2008 R2 con mySQL e IIS



Proteggere la rete è una degli aspetti fondamentali per la salvaguardia dei dati, specialmente in un ambiente aziendale dove il numero di PC e file "maneggiati" può assumere un aspetto importante. I sistemi antivirus non solo devono essere affidabili ma devono essere sempre aggiornati e notificare tempestivamente gli amministratori di sistema al presentarsi di un qualche problema.

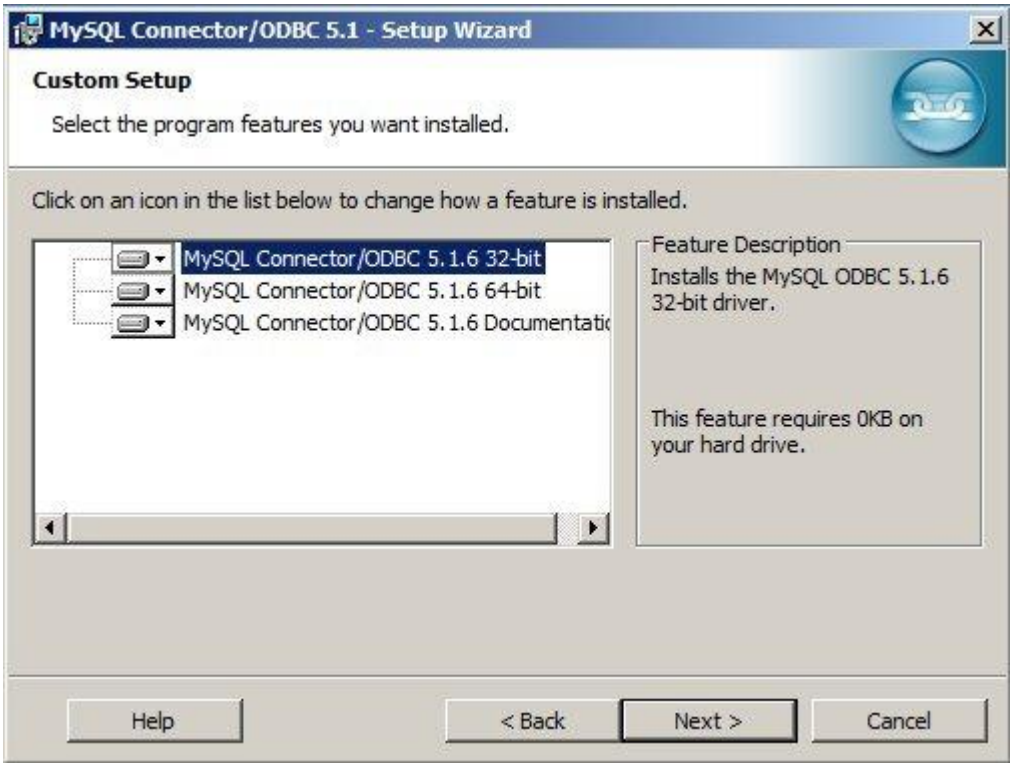
In una rete di una certa dimensione è impensabile gestire il tutto manualmente passando i computer ad uno ad uno per verificare che tutto sia a posto. Centralizzare la gestione diventa quindi una esigenza fondamentale. L'antivirus NOD32 della Eset è un ottimo prodotto che fornisce un elevata percentuale di protezione con una buona gestione in ambito aziendale.

Installazione dei driver ODBC mySQL

Poichè l'installazione del server ERA si deve appoggiare ad un database di mySQL, dobbiamo predisporre il nostro sistema Windows e mySQL per poter comunicare correttamente.

Innanzitutto scaricare i driver ODBC di mySQL (la versione attuale è la 5.1.x) dal sito http://dev.mysql.com/downloads/connector/odbc/ procedendo poi con la l'installazione.

Effettuiamo l'installazione *Typical* installando tutto il pacchetto (32 & 64 bit driver).



Nel database mySQL bisogna creare l'utente che sarà utilizzato dal sistema ERAS per accedere al db. Per motivi di sicurezza, non è una buona idea utilizzare l'account root.

Creare nel server mySQL l'utente *eset*:

```
# mysql -u root -p
mysql> CREATE USER eset@'%' IDENTIFIED BY 'password';
mysql> CREATE DATABASE ESETRADB;
mysql> GRANT ALL PRIVILEGES ON ESETRADB.* TO eset@'%';
mysql> FLUSH PRIVILEGES;
```

Se non si volesse concedere l'accesso al database da qualsiasi IP (definito da %), specificare dopo '@' l'IP o il nome DNS della macchina dalla quale si vuole accedere.

Installazione di ERAS

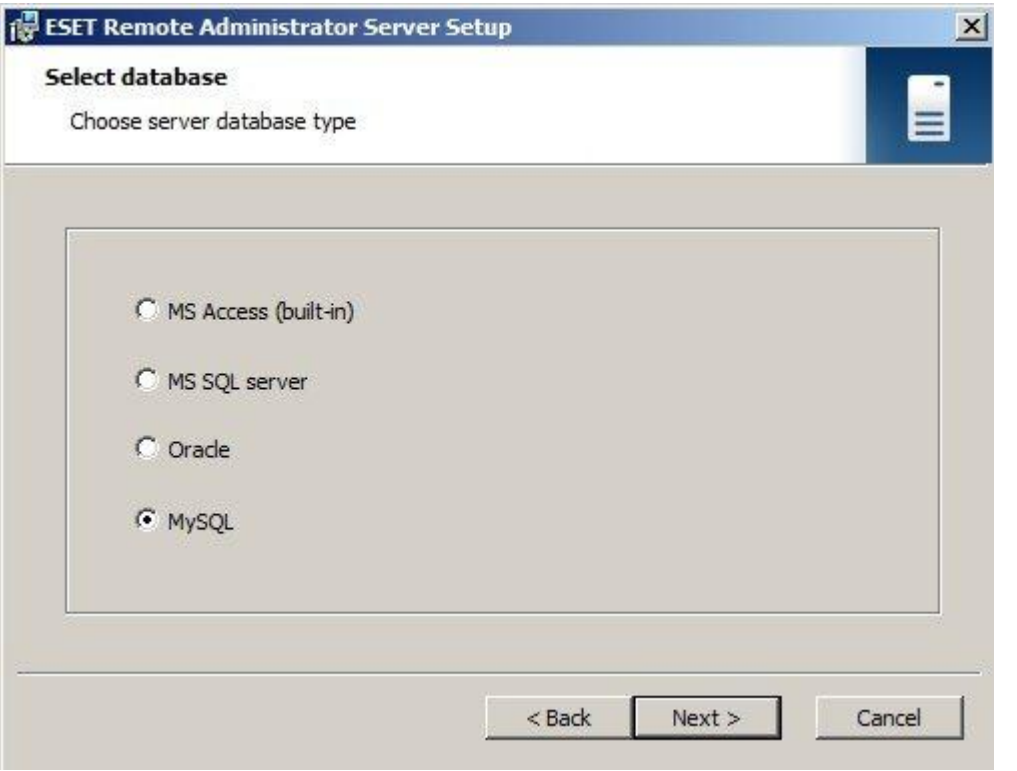
Lanciare il setup di ERAS dal file di installazione prelevato dal sito ESET.

Accettare l'EULA e procedere selezionando come Installation Type l'opzione *Advanced*.

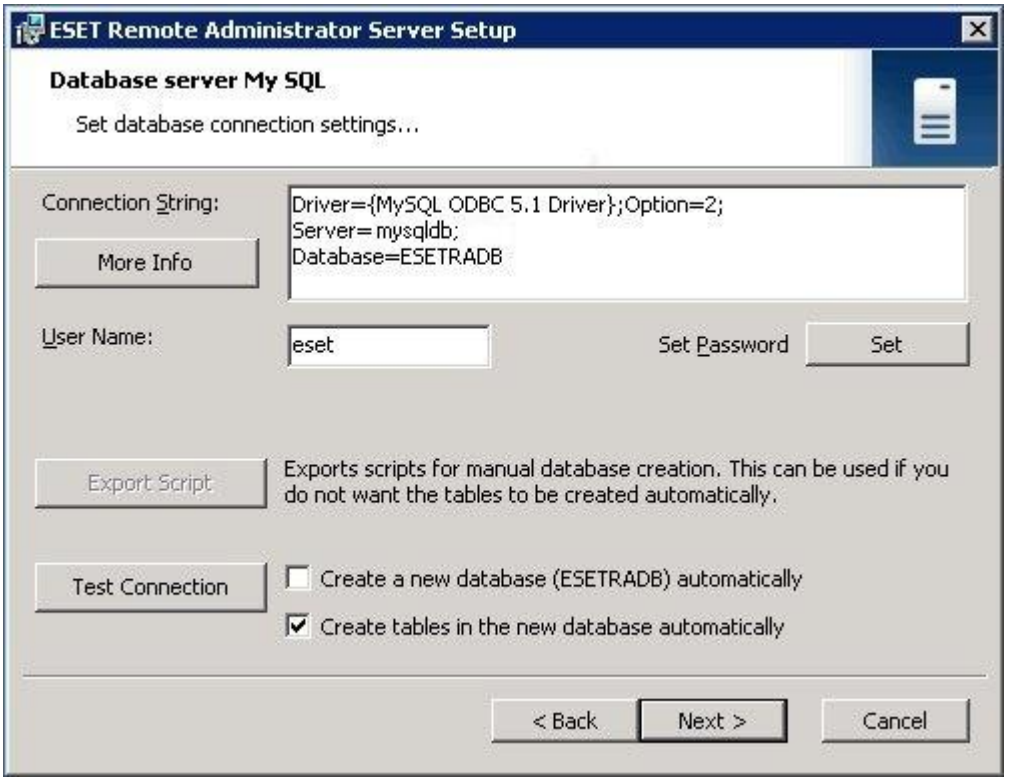
Tramite *Browse…* selezionare il file della licenza fornito da ESET *nod32.lic*. Next.

Lasciare come directory di installazione il *default* proposto e cliccare su OK.

Nella schermata Select database, selezionare il tipo di database che si intende utilizzare, mySQL nel nostro caso.



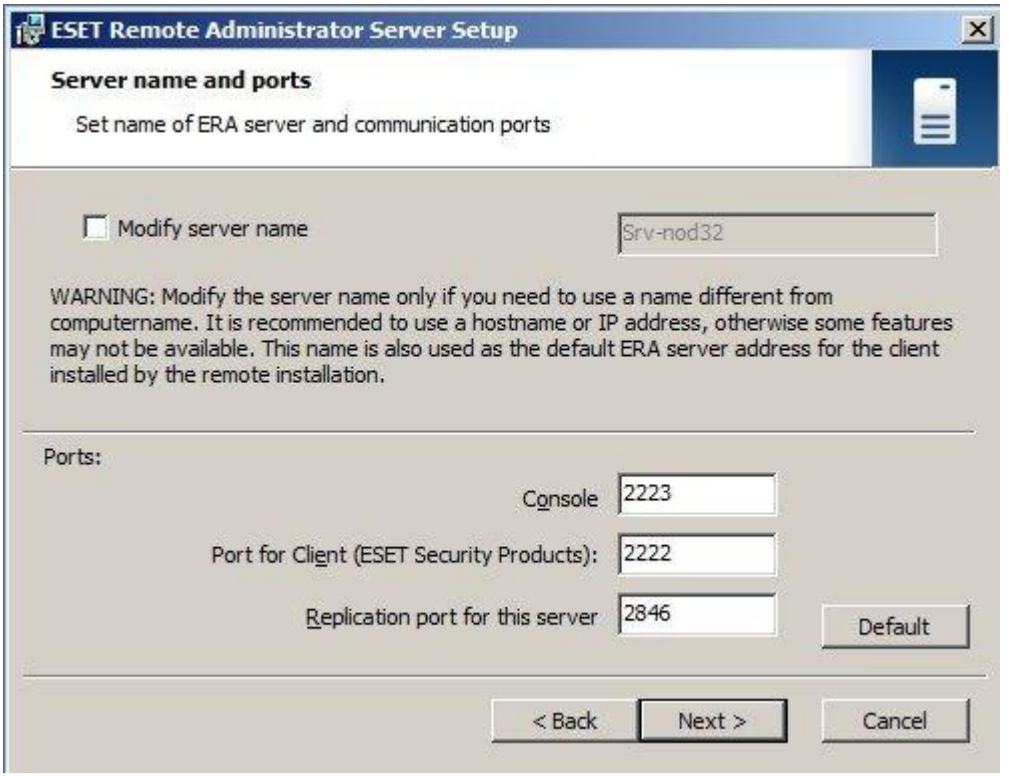
Nella finestra Database server My SQL, impostare i parametri del driver mySQL, del server e l'utente precedentemente.



Effettuare il Test Connection per verificare che il programma riesce a connettersi con il database correttamente. Cliccare su OK, poi Next per continuare.

Nella finestra successiva Data Directories accettare il default cliccando su Next.

In Server name and ports, lasciare le impostazioni di default se non si hanno particolari esigenze. Le porte indicate saranno successivamente impostate nel firewall di Windows.

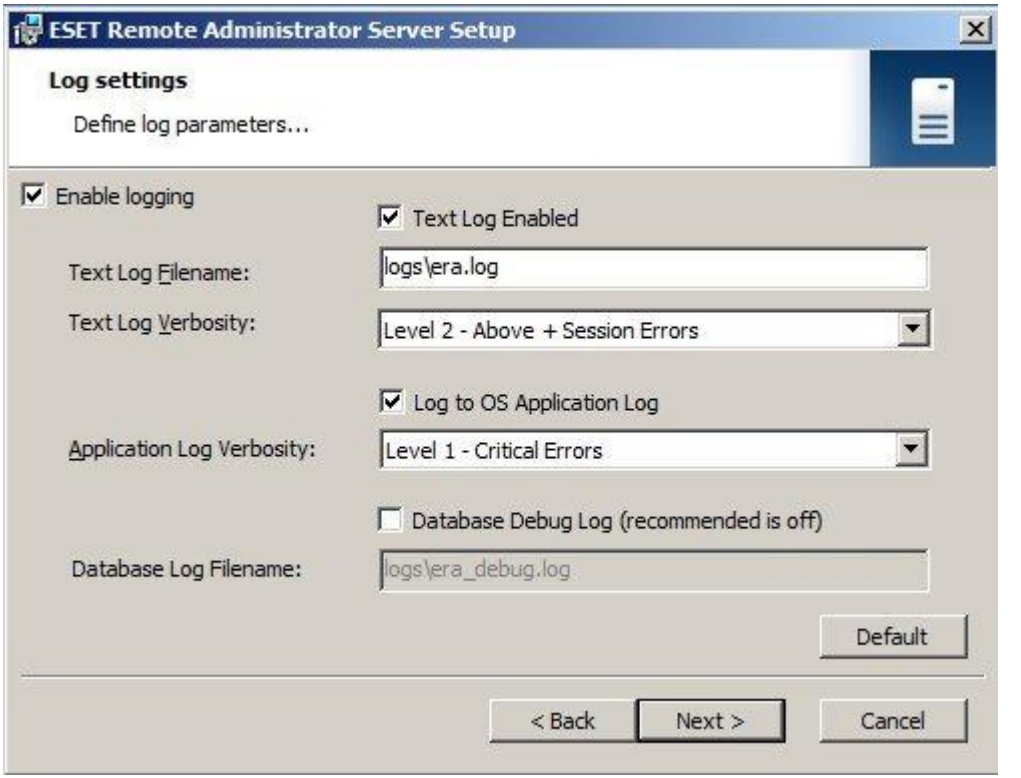


In Security settings impostare le password o lasciare il valore di default BLANK. E' comunque possibile impostarle anche successivamente tramite ERAC.

Nella schermata Updates digitare lo *username* e la *password* fornito da ESET per effettuare gli aggiornamenti.

Nella finestra SMTP Settings impostare i parametri che rispecchiano il vostro ambiente operativo.

Impostare il livello di log desiderato. Abilitando *Log to OS Application Log*, le informazioni vengono copiate nell'Event Viewer i Windows in System.

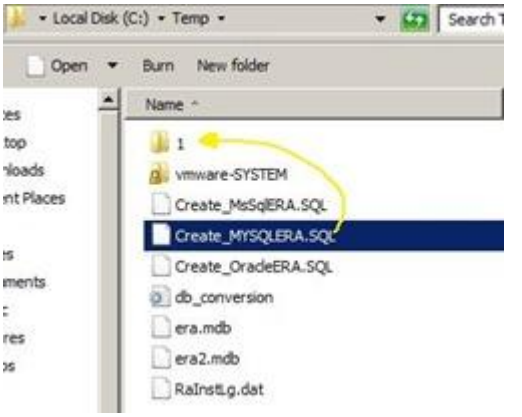


Se proseguendo con l'installazione, si dovesse presentare un errore simile a quello riportato in figura, la prima cosa da fare è visualizzare il log di installazione tramite il bottone View Log.

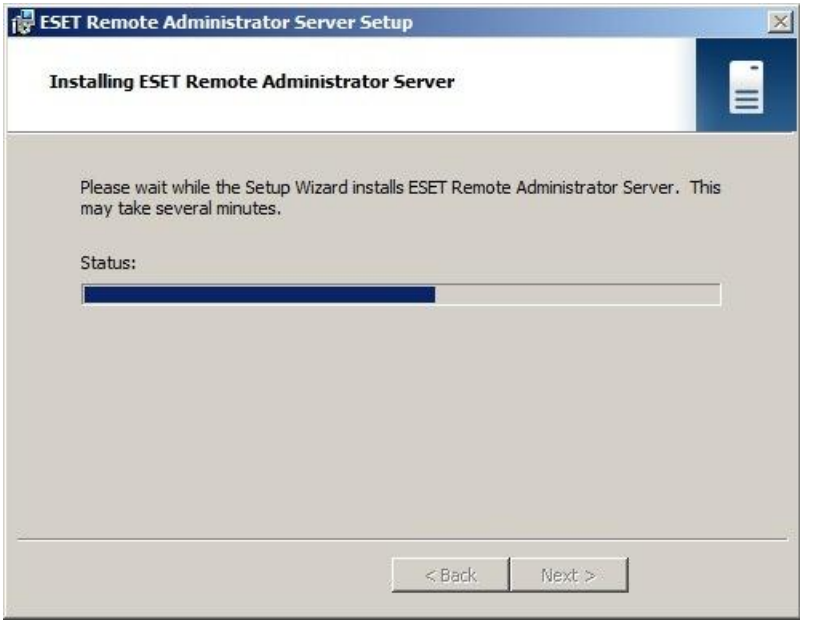
Analizzando il file di log, si nota che il sistema si aspetta di trovare il file *Create_MYSQLERA.SQL* nella directory \Temp\1\.

```
Accessing global data via SID
Account context: "SRV-NOD32\Administrator"
Current context has administrator privileges
Extracting temp files from MSI database...
Extracting item 'Create_MsSqlERA.SQL'
Extracting item 'Create_MYSQLERA.SQL'
Extracting item 'Create_OracleERA.SQL'
Extracting item 'db_conversion.ini'
Extracting item 'era.mdb'
Extracting item 'era2.mdb'
CreateSqlDatabase: Entered
Database platform: MySQL
Not found temp file: C:\Temp\1\Create_MYSQLERA.SQL
Cannot determine script file
Execute sequence terminated with error
```

Tramite una ricerca con Windows Explorer, il file risulta essere presente nel directory *Temp.* Copiando semplicemente il file nella directory richiesta *Temp\1* il problema si risolve.



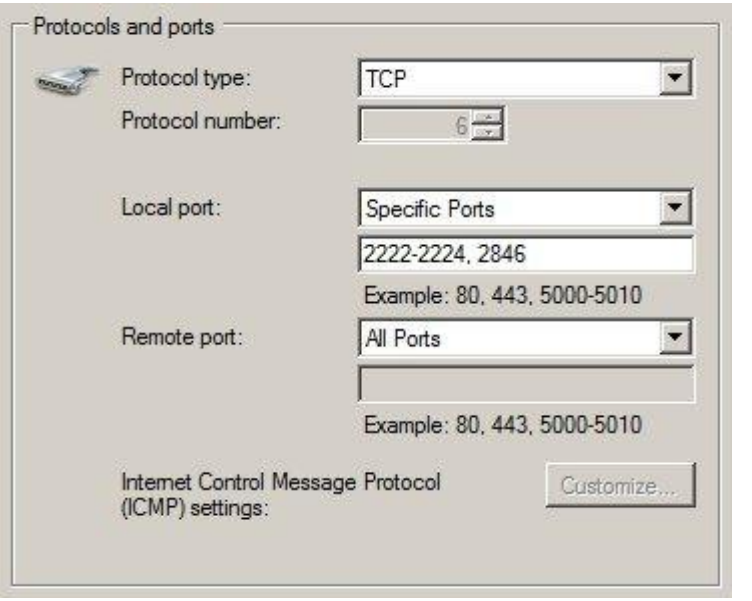
Dopo questo semplice intervento, riavviare la procedura di installazione nuovamente.



La fase di installazione termina correttamente.

Configurazione del firewall

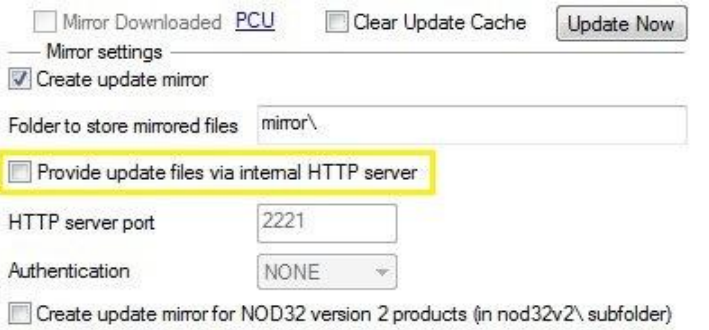
Per permettere la comunicazione tra ERAS, ERAC e client, bisogna aprire le porte richieste nel firewall di Windows, cioè TCP 2222, 2223, 2224 e 2846.



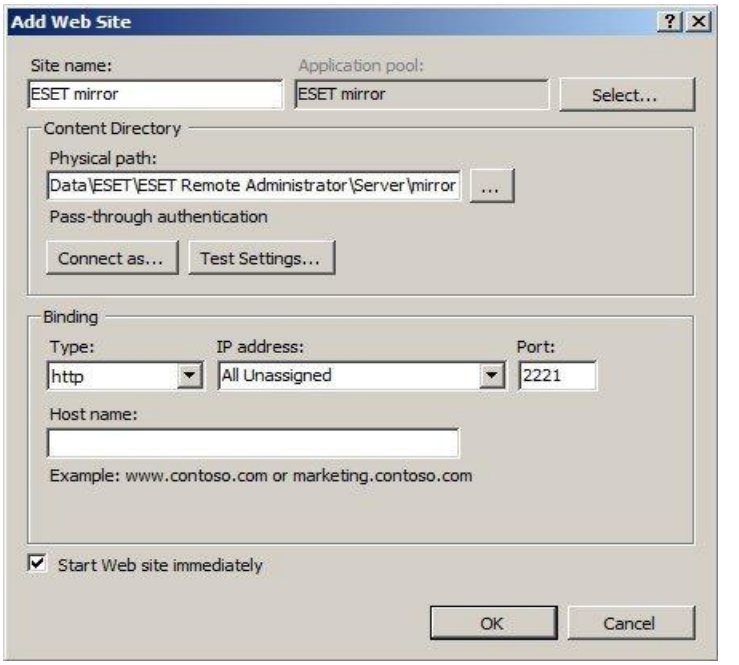
Impostare IIS come server HTTP per "l'Update Mirror Server"

Per poter utilizzare IIS come server http, bisogna verificare che il server http interno a ERAS sia disabilitato.

Se precedentemente abilitato, da ERAC cliccare Tools ? Server Options ? Updates e deselezionare l'opzione Provide update files via internal HTTP server. Click su OK.



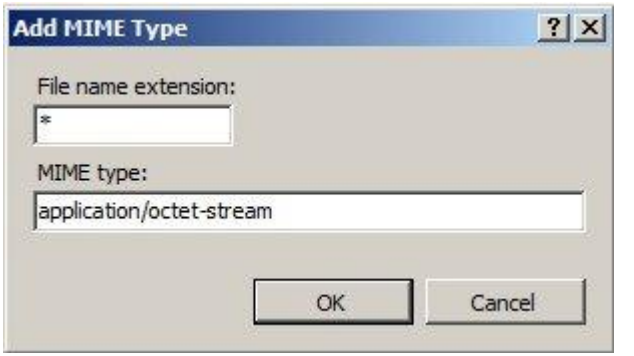
Creare un *nuovo Sito* e specificare come Physical path la directory in cui ERAS scarica gli aggiornamenti ***C:\ProgramData\ESET\ESET Remote Administrator\Server\mirror*** e come Port 2221 utilizzata per la comunicazione con i client.



Verificare in Authentication che la voce Allow anonymous access to this Web site sia *Enabled*.

Doppio click su MIME Types per accedere alla configurazione in modo da definire il parametro richiesto da ERAS.

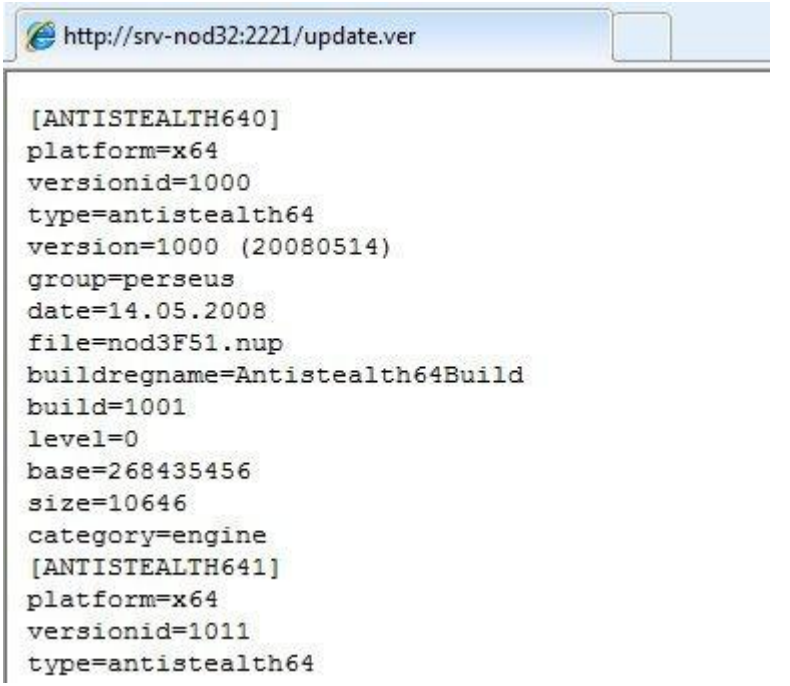
Cliccare su Add per aggiungere un nuovo tipo e digitare i parametri riportati nella figura:



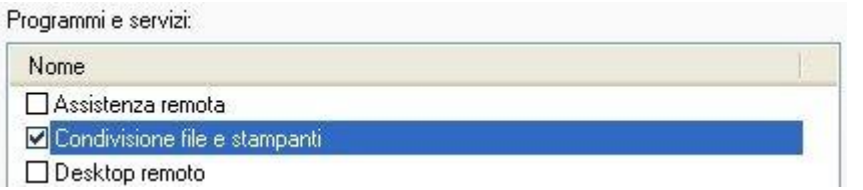
Aprire Default Document e cliccare su Disable. Click OK.

Aprire la porta TCP 2221 nel firewall del Server per permettere la connessione.

Per verificare che il server http funzioni correttamente, digitare nel browser l'indirizzo: *http://IP_Server:2221/Update.ver*. Se viene visualizzata la pagina simile a quella in figura, ERAS è operativo per distribuire gli aggiornamenti tramite IIS.

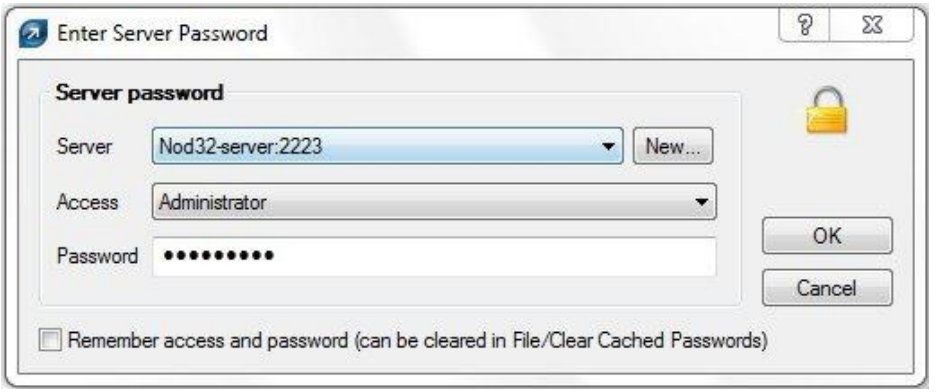


Per permettere il corretto funzionamento del sistema per la gestione dei client, verificare che nel firewall dei client stessi siano abilitate le porte 135-139 e 445 per la c*ondivisione dei file*. Nell'esempio l'opzione nel firewall di Windows XP.



Installazione di ERAC

L'installazione della console ERAC normalmente viene effettuata su una workstation diversa da ERAS (è possibile comunque installarla anche sulla stessa macchina) e non richiede particolari parametri per il suo funzionamento. Una volta terminata l'installazione è sufficiente specificare il server su cui è installato ERAS per poter gestire il sistema.



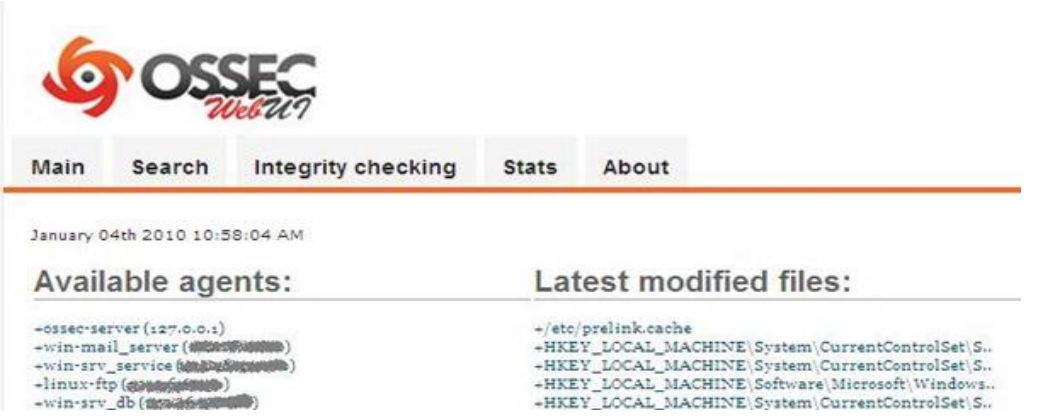
A questo punto siamo connessi con il server ed è possibile effettuare tutte le operazioni necessarie per configurare il sistema per la nostra rete.

Setup di OSSEC (log analyzer) su CentOS 5

Monitorare gli accessi ai sistemi informatici è un requisito fondamentale per assicurare il più alto elevato standard di sicurezza della rete. Inoltre dovuto alla recente variazione del garante sulla *legge della privacy* che, dopo qualche posticipo, è entrata ufficialmente in vigore il *15 Dicembre 2009*, agli amministratori di sistema è stata ulteriormente complicata la vita, come se questa non lo fosse già abbastanza…

Come prevede la normativa, bisogna registrare i log di accesso ai sistemi ed assicurare l'integrità dei file di sistema marcandoli temporalmente conservando il tutto per almeno sei mesi.

Tra le varie offerte disponibili sul mercato, la scelta è caduta su un software open source su piattaforma Linux chiamato OSSEC, un software IDS molto valido che risponde ai requisiti di legge ed è approvato dal Garante.



Prerequisiti

Partendo dalla configurazione minima di CentOS 5.x, sono richiesti alcuni package aggiuntivi da installare per il corretto funzionamento. Tramite il comando *yum* andiamo ad installare i package richiesti:

```
# yum install gcc glibc make which mysql-devel mysql-server httpd
mod_ssl php
# chkconfig httpd on
# chkconfig mysqld on
```

Installazione

Dal sito *www.ossec.net* si effettua il download dell'applicazione OSSEC-HIDS-2.3. OSSEC nel suo normale funzionamento salva i dati su file ma conviene appoggiarsi ad un database (sono supportati attualmente mySQL e postgreSQL) soprattutto se ci sono diversi server da monitorare e si vuole centralizzare il tutto.

L'abilitazione al supporto database (mySQL nel nostro caso) deve essere fatta durante l'installazione:

```
# tar -zxvf ossec-hids-2.3
# cd ossec-hids-2.3/src
# make setdb
```

```
[root@ossec ossec-hids-2.3]# cd src
[root@ossec src]# make setdb

Error: PostgreSQL client libraries not installed.

Info: Compiled with MySQL support.
[root@ossec src]#
```

```
# cd ..
# ./install.sh
```

Lanciata la procedura di installazione, selezionare la tipologia di installazione e i parametri che si vogliono configurare. L'applicazione viene installata in */var/ossec*.

```
OSSEC HIDS v2.3 Installation Script - http://www.ossec.net

You are about to start the installation process of the OSSEC HIDS.
You must have a C compiler pre-installed in your system.
If you have any questions or comments, please send an e-mail
to dcid@ossec.net (or daniel.cid@gmail.com).

 - System: Linux ossec 2.6.18-92.el5
 - User: root
 - Host: ossec


 -- Press ENTER to continue or Ctrl-C to abort. --
```

Installazione della Web GUI

Per installare l'interfaccia web di OSSEC, procedere in questo modo:

```
# wget http://www.ossec.net/files/ui/ossec-wui-0.3.tar.gz
# tar -zxvf ossec-wui-0.3.tar.gz
# mv ossec-wui-0.3 /var/www/html/ossec-wui
```

```
[root@ossec install]# mv ossec-wui-0.3 /var/www/html/ossec-wui
[root@ossec install]#
```

Eseguire lo script di configurazione dell'interfaccia web:

```
# cd /var/www/html/ossec-wui
# ./setup.sh
```

Impostare lo username (apache nell'esempio) e la password.

```
[root@ossec ossec-wui]# ./setup.sh
Setting up ossec ui...

Username: apache
New password:
Re-type new password:
Adding password for user apache

Setup completed successfuly.
[root@ossec ossec-wui]#
```

Aggiungere l'utente impostato precedentemente (apache) al gruppo ossec:

```
# vi /etc/group
```

ossec:x:500:apache

```
vcsa:x:69:
utmp:x:22:
sshd:x:74:
haldaemon:x:68:
apache:x:48:
distcache:x:94:
mysql:x:27:
ossec:x:500:apache
-- INSERT --
```

Impostare i permessi per la directory */var/ossec/tmp*:

```
# cd /var/ossec
# chmod 770 tmp/ -R
# chown ossec:apache tmp/ -R
```

```
[root@ossec ossec]# chmod 770 tmp/ -R
[root@ossec ossec]# chown ossec:apache tmp/ -R
[root@ossec ossec]# ll
total 40
dr-xr-x---  3 root  ossec  4096 Dec 16 12:35 active-response
dr-xr-x---  2 root  ossec  4096 Dec 16 12:35 agentless
dr-xr-x---  2 root  ossec  4096 Dec 16 12:35 bin
dr-xr-x---  3 root  ossec  4096 Dec 16 12:35 etc
drwxr-x---  5 ossec ossec  4096 Dec 16 12:35 logs
dr-xr-x--- 11 root  ossec  4096 Dec 16 12:35 queue
dr-xr-x---  3 root  ossec  4096 Dec 16 12:35 rules
drwxr-x---  2 ossec ossec  4096 Dec 16 12:35 stats
drwxrwx---  2 ossec apache 4096 Dec 16 12:35 tmp
dr-xr-x---  3 root  ossec  4096 Dec 16 12:35 var
[root@ossec ossec]#
```

Riavviare Apache:

```
# service httpd restart
```

Configurazione

Importante da ricordare che se tra il server e l'agent è presente un firewall, la comunicazione di OSSEC avviene attraverso la porta UDP 1514.

Tramite il comando */var/ossec/bin/./manage_agent* si creano gli agent dei server che saranno monitorati. Per procedere con la definizione degli agent:

```
# cd /var/ossec/bin/
# ./manage_agents
```

Selezionare A per aggiungere un agent

Definire il nome dell'agent: srv-service-lab

Definire l'IP: 172.16.20.246

Definire l'ID: 006

Confermare digitando Y

```
****************************************
* OSSEC HIDS v2.3 Agent manager.     *
* The following options are available: *
****************************************
    (A)dd an agent (A).
    (E)xtract key for an agent (E).
    (L)ist already added agents (L).
    (R)emove an agent (R).
    (Q)uit.
Choose your action: A,E,L,R or Q: a

- Adding a new agent (use '\q' to return to the main menu).
  Please provide the following:
    * A name for the new agent: linux-ossec
    * The IP Address of the new agent: 172.16.20.246
    * An ID for the new agent[006]:
Agent information:
    ID:006
    Name:linux-ossec
    IP Address:172.16.20.246

Confirm adding it?(y/n): y
```

Successivamente è necessario estrarre la chiave per configurare l'agent nell'host desiderato (*srv-service-lab* nell'esempio).

Selezionare E per estrarre la chiave per l'agent

Specificare l'ID dell'agent da configurare

Questa chiave andrà copiata dove richiesto durante l'installazione dell'agent

```
Provide the ID of the agent to extract the key (or '\q' to quit): 004

Agent key information for '004' is:
MDAOIGxpbnV4LWZOcCAxNzIuMTYuMTAuMzAgZGQ5MGM3N2E5OTkONTFkMWUOZD1kZDg2ZTdmNWQwMDB1
OWEyOGJmNzh1NzViY2NhNWQyNzMwZTk5OTk2N2FkZg==

** Press ENTER to return to the main menu.
```

Abilitare il supporto database

Se si intende inviare i log al database, è necessario specificarlo prima di effettuare l'installazione quindi prima di lanciare lo script *install.sh*:

```
# cd ossec-hids-2.3/src
# make setdb
# cd ..
# ./install.sh
```

Dopo che l'installazione è terminata, abilitare il database:

```
# /var/ossec/bin/ossec-control enable database
```

<u>Configurare MySQL</u>

```
# mysql -u root -p

mysql> create database ossec;

mysql> grant INSERT,SELECT,UPDATE,CREATE,DELETE,EXECUTE on ossec.*
to ossecuser@localhost;

mysql> set password for ossecuser@localhost=PASSWORD('password!');

mysql> flush privileges;

mysql> quit
```

Effettuare il download dello schema e importarlo nel database creato:

```
# wget http://www.ossec.net/files/other/mysql.schema
# mysql -u root -p ossec < mysql.schema
```

<u>Configurare OSSEC per inviare gli alerts a MySQL</u>

Nell'esempio vengono inviati gli alert all'indirizzo IP *192.168.10.30*, utilizzando *ossecuser* come utente.

<ossec_config>
<database_output>
<hostname>192.168.10.30</hostname>
<username>ossecuser</username>

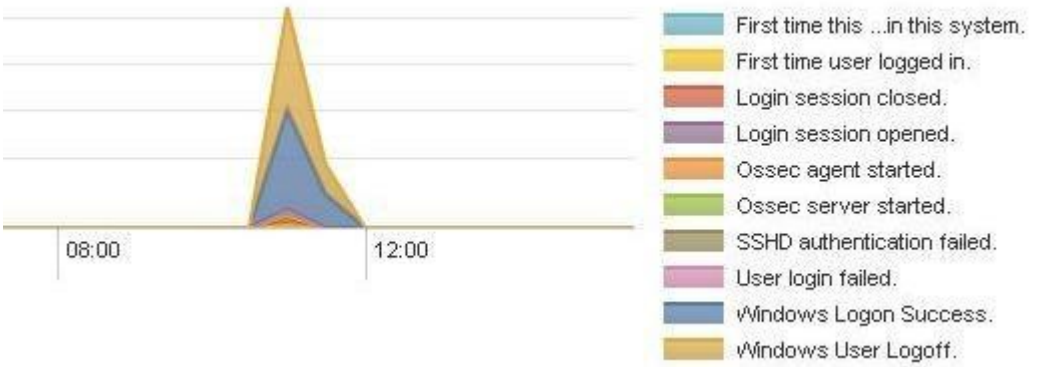
<password>password!</password>
<database>ossec</database>
<type>mysql</type>
</database_output>
</ossec_config>

Riavviare OSSEC e verificare che non ci siano errori nel log tramite il comando:

```
# cat /var/ossec/logs/ossec.log
```

Per migliorare la reportistica e le statistiche, molto scarne dell'interfaccia web di OSSEC, si può utilizzare il prodotto SPLUNK nella sua versione free che consente di avere vari report in un formato grafico più chiaro e leggibile.

E' qui riportato un esempio:



A questo punto non resta che mettere in sicurezza il server di OSSEC per evitare che venga compromesso.

Sincronizzazione data e ora

E' opportuno che l'ora e la data del server su cui è installato OSSEC siano corretti per salvare i log correttamente.

```
# yum install ntpd
# ntpdate ntp1.ien.it       # Effettare una prima sincronizzazione manuale
# chkconfig ntpd on
# service ntpd start
```

```
[root@ossec ~]# service ntpd start
Starting ntpd:                                             [  OK  ]
[root@ossec ~]#
```

Installazione del client Linux

L'installazione del client è molto semplice ma richiede l'installazione dei package richiesti per la compilazione di OSSEC.

```
# yum install gcc make which
# tar -xzvf ossec-hids-2.3.tar.gz
# cd ossec-hids-2.3
# ./install
```

Lanciata l'installazione, è sufficiente specificare agent come tipo di installazione.

```
1- What kind of installation do you want (server, agent, local or help)? agent
```

Completata l'installazione, eseguire la configurazione del client per attivare la connessione importando la chiave generata dal server:

```
# cd /var/ossec/bin/
# ./manage_agents
```

```
[root@[illegible] bin]# ./manage_agents


****************************************
* OSSEC HIDS v2.3 Agent manager.     *
* The following options are available: *
****************************************
    (I)mport key from the server (I).
    (Q)uit.
Choose your action: I or Q: I

* Provide the Key generated by the server.
* The best approach is to cut and paste it.
*** OBS: Do not include spaces or new lines.

Paste it here (or '\q' to quit): MDEwIHZtLWx4NS1teXNxbCAxNzIuMTYuMjAuMjA4IDdjNjczNmYy
YzA3M2RiMTA5MWM2NTB1NmY4NjV1ZDJhMWR1YzU4MWRhMGMyM2NjMjY1MGVhZTFiNjBkNWY0NjE=
```

Terminata la configurazione, riavviare il daemon OSSEC:

```
# service ossec restart
```

Troubleshooting

1. OSSEC riporta un agent come non connesso.

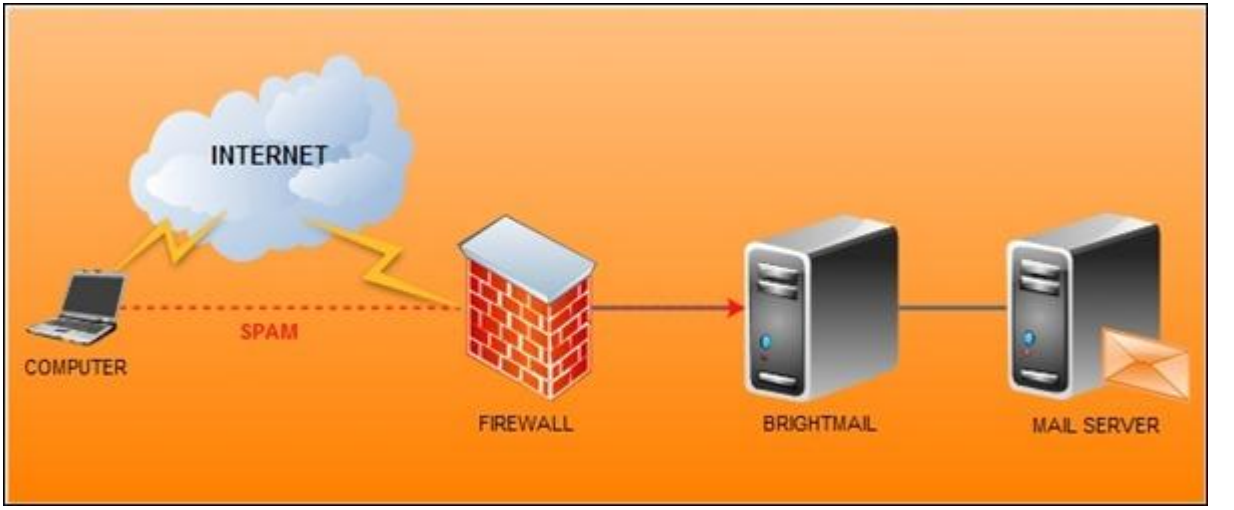
Dopo aver verificato che l'agent nel server da verificare è in modalità running (nel caso effettuare un restart del servizio), è necessario rimuovere l'ID del server dalla coda di OSSEC:

```
# cd /var/ossec/queue/rids
# rm 002 (nel caso l'ID del server da rimuovere corrisponda a 002)
# service ossec restart
```

```
[root@ossec rids]# ll
total 20
-rw-r--r-- 1 ossecr ossec 7 Dec 28 10:33 001
-rw-r--r-- 1 ossecr ossec 7 Dec 28 10:33 002
-rw-r--r-- 1 ossecr ossec 0 Dec 28 10:33 003
-rw-r--r-- 1 ossecr ossec 7 Dec 28 10:33 004
-rw-r--r-- 1 ossecr ossec 7 Dec 28 10:33 005
-rw-r--r-- 1 ossecr ossec 0 Dec 16 12:52 006
-rw-r--r-- 1 ossecr ossec 7 Dec 28 10:51 sender_counter
[root@ossec rids]#
```

Fatta questa semplice procedura, l'interfaccia web di ossec dovrebbe segnalare l'agent del server come connesso.

Proteggere il Mail Server da spam e virus con Brightmail



Il fenomeno spam e virus è di dimensioni così rilevanti che un qualsiasi mail server richiede la presenza di un valido sistema di difesa per garantire la sua funzionalità.

Fra i vari prodotti offerti dal mercato, un interessante prodotto per la protezione del mail server è Brightmail della *Symantec* che può essere implementato come appliance VMware.

In questa PRIMA PARTE dell'articolo viene analizzata la procedura di implementazione di un semplice server di posta necessario per effettuare l'installazione di *Brightmail* poichè il mail server richiesto non deve essere ovviamente in produzione.

1. REQUISITI MAIL SERVER

Poichè lo scopo è l'implementazione di *Brigthmail* nella rete, bisogna configurare un mail server per poter inviare e ricevere le email.

Come mail server semplice e veloce da installare da utilizzare per la parte di laboratorio, è stato utilizzato AllardSoft MailServer (http://www.allardsoft.com/mailserver), un prodotto anche in versione freeware ottimo per lo scopo che richiede pochi minuti per la configurazione ed è fornito come appliance VMware.

I requisiti per implementare il server sono principalmente tre:

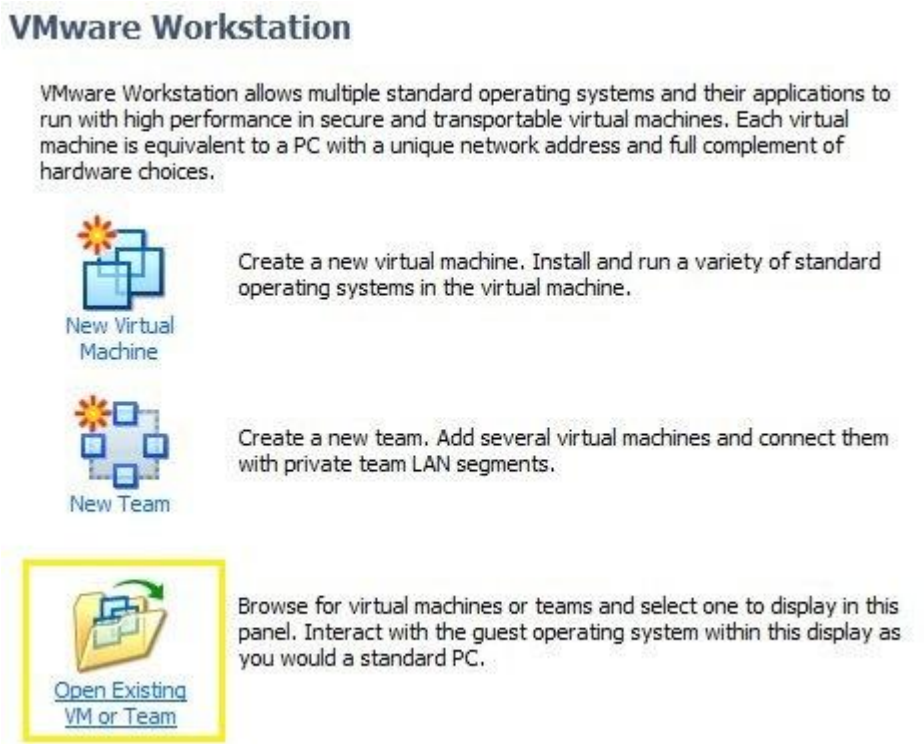
- Account presso http://www.dyndns.com per la creazione di un record MX pubblico

- VMware Workstation
- Allard MailServer

Installazione mail server

Effettuare il download dell'applicazione Mailserver_4612.zip dal sito Allardsoft, un *appliance VMware* che non richiede nessuna installazione.

Terminato lo scarico del software, scompattare il file *zip*. Lanciare il programma *VMware Workstation* e aprire la virtual machine *Mailserver* appena scaricata.



Avviare la virtual machine. Il sistema carica l'applicazione con i parametri di default che dovranno poi essere configurati al termine dell'operazione.

```
pckbc0: using irq 12 for aux slot
wsmouse0 at pmsi0 mux 0
pcppi0 at isa0 port 0x61
midi0 at pcppi0: <PC speaker>
spkr0 at pcppi0
lpt0 at isa0 port 0x378/4 irq 7
npx0 at isa0 port 0xf0/16: reported by CPUID; using exception 16
fdc0 at isa0 port 0x3f0/6 irq 6 drq 2
mtrr: Pentium Pro MTRR support
softraid0 at root
root on sd0a swap on sd0b dump on sd0b
Automatic boot in progress: starting file system checks.
/dev/rsd0a: file system is clean; not checking
/dev/rsd0d: file system is clean; not checking
setting tty flags
pf enabled
ddb.panic: 1 -> 0
starting network
```

Terminata la procedura di boot, il sistema necessita della configurazione dei parametri operativi. La configurazione dei parametri di rete conviene effettuarla tramite console poichè è più immediata. L'IP visualizzato è l'indirizzo che il sistema prende automaticamente nel caso della presenza del *DHCP*. Digitare setup e poi premere Invio.

```
=================================================================
AllardSoft Mailserver v4.6.12



- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Please browse to: https://192.168.1.105:4200 to get started

Alternatively, type 'setup' on the command prompt

setup, quit or help?  _
```

Impostare l'hostname e il domain. Digitare y e premere Invio.

Hostname: vm-mail
Domain: labtest.loc

```
Host Configuration details:

Hostname: [mail] vm-mail
Domain: [my.domain] labtest.loc

vm-mail.labtest.loc

Is this correct?  y
```

E' opportuno che il mail server abbia un IP statico. Digitare n ed impostare i parametri di rete. Digitare y e premere Invio per continuare.

```
IP Configuration details:

Do you want to use DHCP?  n
IP address: [192.168.1.105] 192.168.10.10
Netmask: [255.255.255.0]
Default Gateway: [192.168.1.254] 192.168.10.1
DNS Server: [192.168.1.254] 192.168.10.1
Is this correct?  y
```

Definire l'account Administrator e impostare la password. Digitare y e premere Invio per continuare.

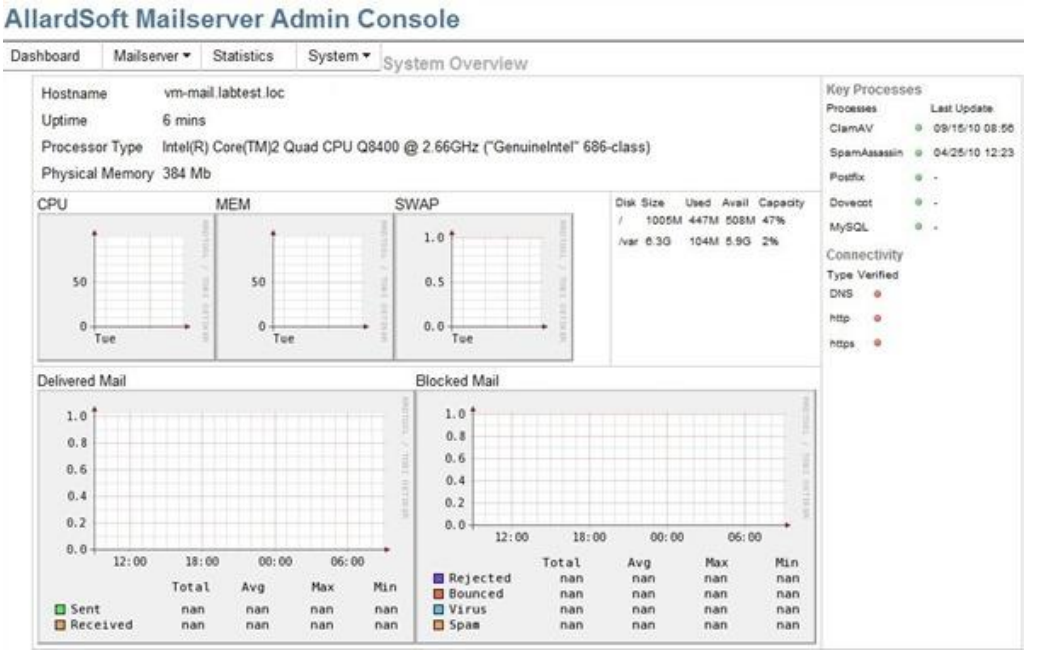
```
Add Administrator:

Username: admin
Email (optional, will be used for status emails): admin@labtest.dy
Password:  ********
Password Confirm:  ********
Is this correct?  y
```

La procedura di impostazione dei parametri di rete è terminata.

```
Please login to the Webadmin Interface to setup users and domains.

ping, hostconfig, ipconfig, shutdown, quit or help?  _
```

Aprire il browser di Internet e digitare https://IP_Address:4200 per accedere alla pagina di amministrazione. Inserire le credenziali dell'account Administrator definito precedentemente e cliccare su Login.

Effettuato il login, si accede alla schermata principale della console di amministrazione.



Configurazione mail server

Procedere con la configurazione dei parametri di sistema. Cliccare su System –> Hostname per modificare l'*Hostname* e il *Domain*.

Cliccare su System –> Network per modificare i *parametri di rete*.

Network Configuration: vic0

Property	Value
DHCP	Enabled Disabled
IP Address	192.168.10.10
Netmask	255.255.255.0
Default Gateway	192.168.10.1
Media, Speed & Duplex	default

Save & Enable

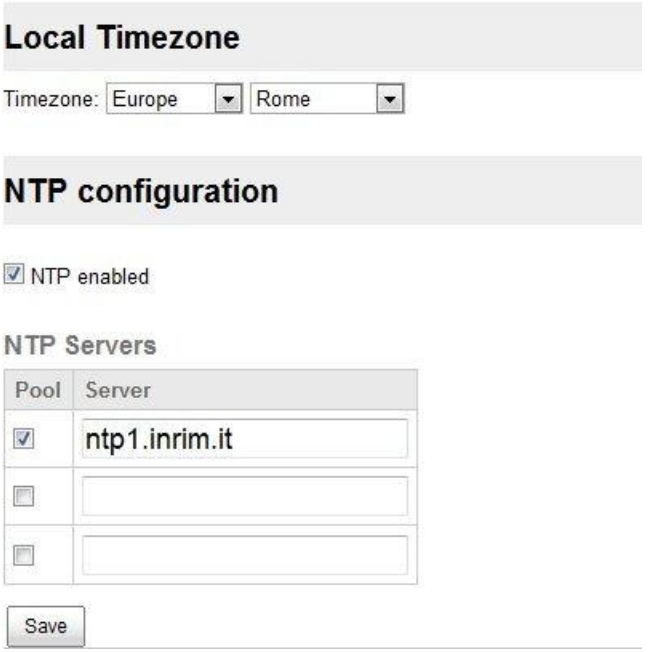
Cliccare su System –> DNS per impostare l'indirizzo del DNS.

DNS Configuration

Setting	Value	Description
Nameserver	192.168.10.1	
Nameserver		A total a 3 name (DNS) servers can b
Nameserver		
Search		Comma separated search list for host

Save

Cliccare su System –> Time per impostare la Timezone ed attivare il servizio NTP.



Cliccare su System –> System Update per effettuare gli aggiornamenti.

Per effettuare l'upgrade, cliccare sull'aggiornamento disponibile per scaricarlo ed effettuare successivamente l'installazione.

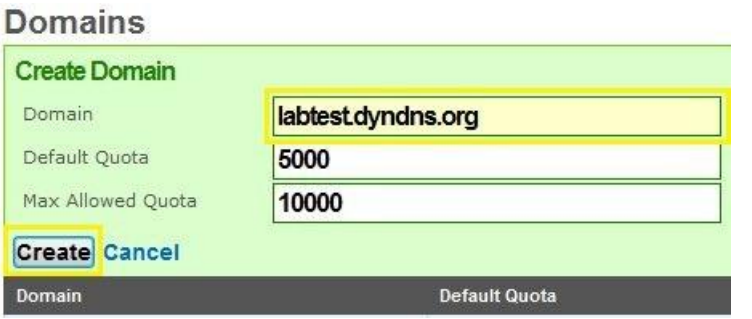
Creazione dominio e utenti

Per utilizzare il servizio email, bisogna definire il dominio di posta e configurare gli utenti tramite Mailserver –> Users & Domains.

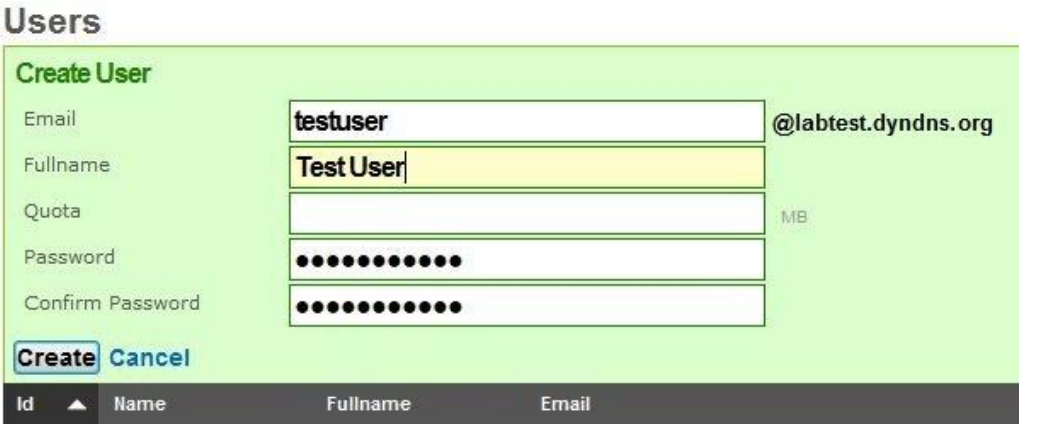
Cliccare su Create New per definire il dominio di posta. Nell'esempio viene utilizzato il dominio labtest.dyndns.org.

Questo è il dominio che deve essere configurato anche presso il servizio DNS www.dyndns.com per poter avere un record MX associato.

Digitare il nome del dominio scelto e cliccare su create.



Analogamente creare un utente di test cliccando, selezionando il dominio appena creato, la voce Manage. Cliccare su Create New per impostare l'utente.



Per poter raggiungere il server dall'esterno, nel sito DynDNS.com configurare i parametri hostname e dominio con i valori specificati nei passaggi precedenti. Indicare inoltre l'opzione mail server ed attivare il servizio.

Add New Hostname

Note: You currently don't have any active Dynamic DNS Pro in your account. You cannot use some of o
Paying for an Dynamic DNS Pro will make this form fully functional and will add several other features.

Hostname: labtest . dyndns.org

Wildcard Status: Disabled [Want Wildcard support?]

Service Type:
- Host with IP address [?]
- WebHop Redirect [?]
- Offline Hostname [?]

IP Address: xxx.xxx.xxx.xxx

Your current location's IP address is 94.90.112.34

TTL value is 60 seconds. Edit TTL.

Mail Routing: Yes, let me configure Email routing. [?]

What do you want to use this host for?

Select services and devices you would like to use with this hostname.

Work From Home Office or VPN:

vpn | remote file access | remote desktop | mail server | web server

chat server | ftp backup | ssh | database | voip

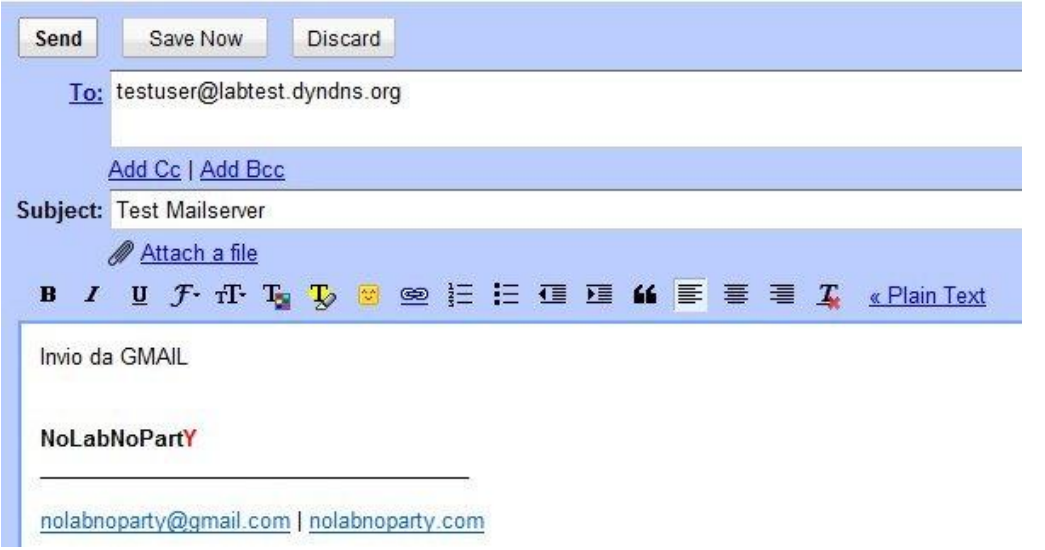
A questo punto il mail server è operativo. Se è presente un firewall nella rete, configurarlo opportunamente in modo da permettere le comunicazioni richieste dal mail server.

Test ricezione ed invio

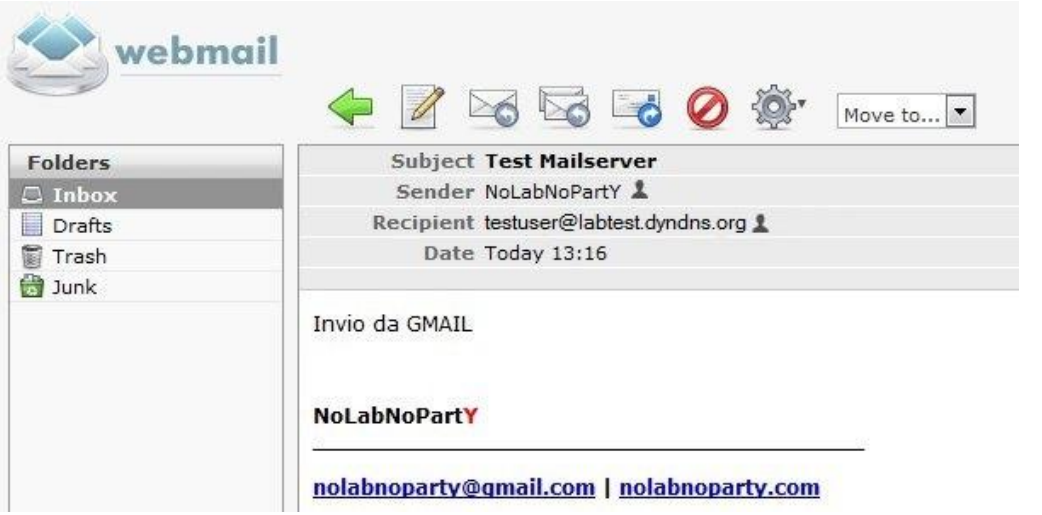
Effettuare un test di ricezione e invio per verificare che il sistema funzioni correttamente.

Test ricezione

Per il test di ricezione, da una casella di posta inviare una email all'utente appena creato.

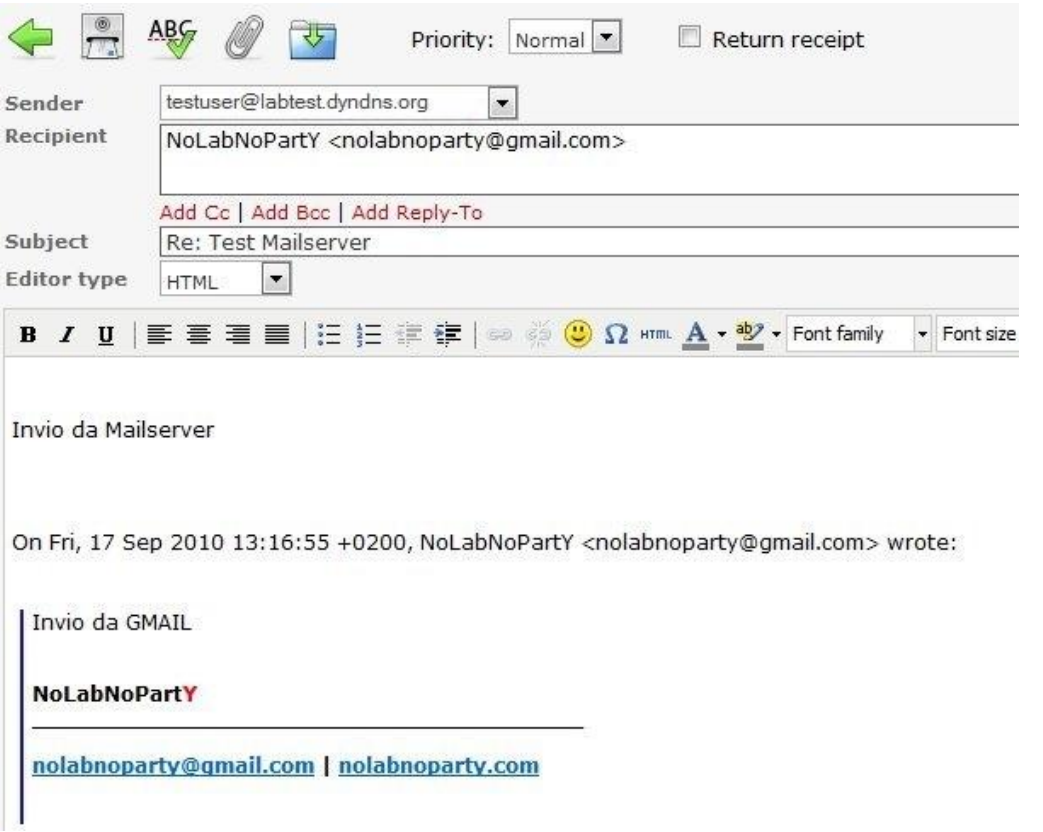


Tramite il browser di Internet, collegarsi alla webmail di *Mailserver* digitando l'indirizzo https://IP_Address. Se tutto è stato impostato correttamente, troviamo la mail inviata.



Test invio

Per il test di invio, effettuare un reply alla email appena ricevuta.



Verificando le nuove email arrivate nella casella di posta destinataria, troviamo il messaggio inviato da *Mailserver*.

Il mail server è operativo e funzionante. Se lasciassimo il server attivo per qualche giorno senza nessuna protezione, cominceranno ad arrivare le prime email spam che senza un adeguato controllo porteranno al crash del server dovuto alla saturazione del disco.

Installazione di Brightmail

Una volta configurato il mail server per effettuare i vari test, viene analizzata la procedura di installazione di Brightmail.

Data l'ampia diffusione di sistemi virtualizzati, viene utilizzata la Brightmail Gateway Virtual Edition su piattaforma *VMware* in formato ISO per il setup su *Workstation* e la versione appliance ovf per *vSphere*.

L'installazione è piuttosto semplice e rapida e richiede la configurazione di alcuni parametri per rendere l'applicazione accessibile tramite browser dove viene effettuata la maggior parte del setup.

Prerequisiti

I requisiti per l'installazione sono essenzialmente due:

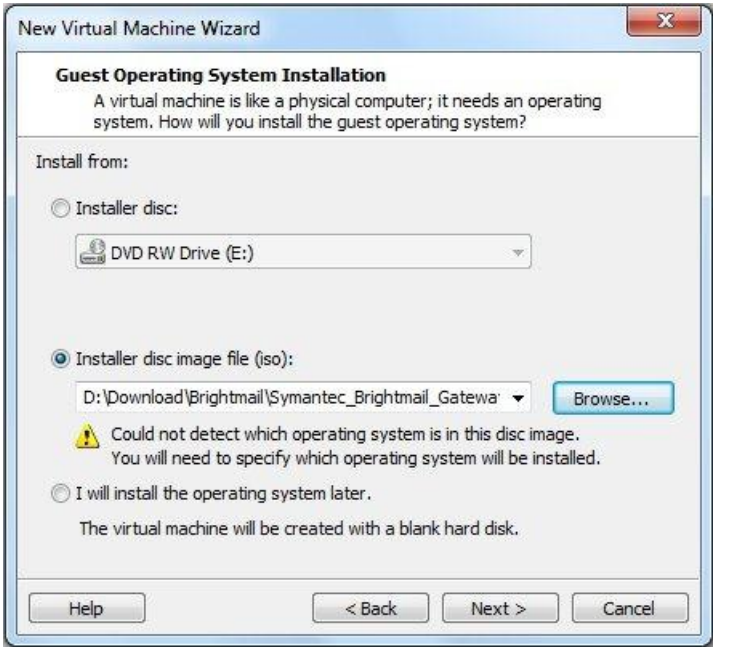
- VMware Workstation o vSphere
- L'applicazione Brightmail Gateway recuperabile dal sito della Symantec.

Installazione applicazione in VMware Workstation

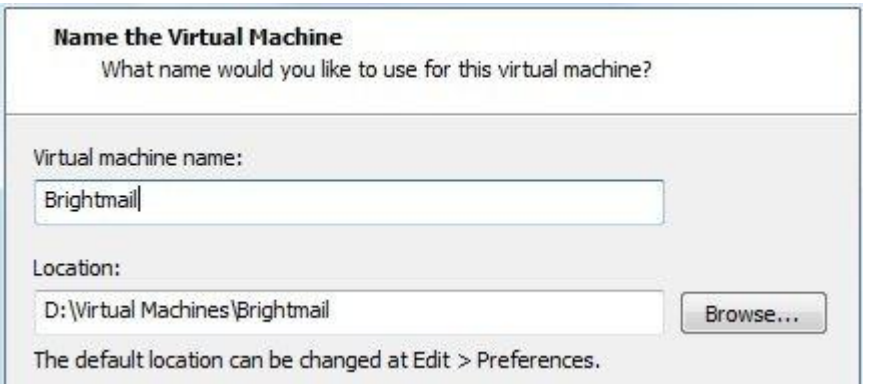
Avviare VMware Workstation per procedere alla creazione della virtual machine utilizzata da *Brightmail*.

Cliccare su ***File -> New -> Virtual Machine*** per lanciare il *Wizard*.

Avendo a disposizione l'immagine ISO dell'applicazione scaricata dal sito, selezionare nella finestra "*New Virtual Machine Wizard*" l'opzione Installer disc image file (ISO) e specificare il path in cui è stata salvata l'immagine ISO.



Assegnare il Virtual machine name specificando anche la Location, nell'esempio la virtual machine è chiamata *Brightmail*.

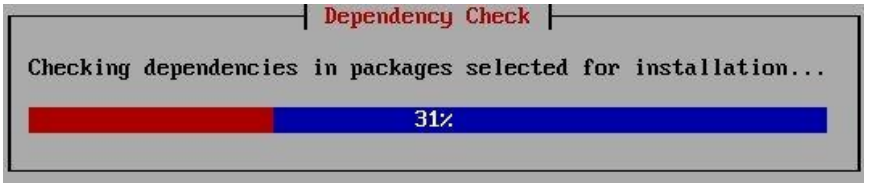


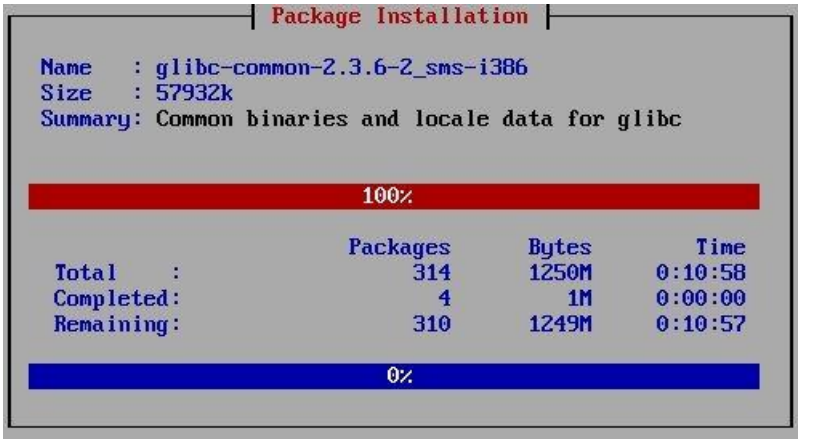
Abilitare nella VM solamente l'hardware richiesto per aumentare al massimo il fattore sicurezza. Per lo stesso motivo aggiungere anche un secondo NIC.

Avviare la virtual machine (Power on). Automaticamente viene eseguita la fase di installazione dell'applicazione.

Quando compare la finestra illustrata in figura, cliccare sul bottone YES per proseguire.

Durante il processo, il sistema effettua i vari controlli sulle dependencies procedendo poi con l'installazione dei packages richiesti.





Terminata la fase di installazione, il sistema effettua il reboot.

```
Mounting local filesystems:                                [  OK  ]
Enabling local filesystem quotas:                          [  OK  ]
Enabling swap space:                                       [  OK  ]
INIT: Entering runlevel: 3
Entering non-interactive startup
Starting issue:                                            [  OK  ]
Cleaning up lock files:                                    [  OK  ]
Starting sysstat:                                          [  OK  ]
```

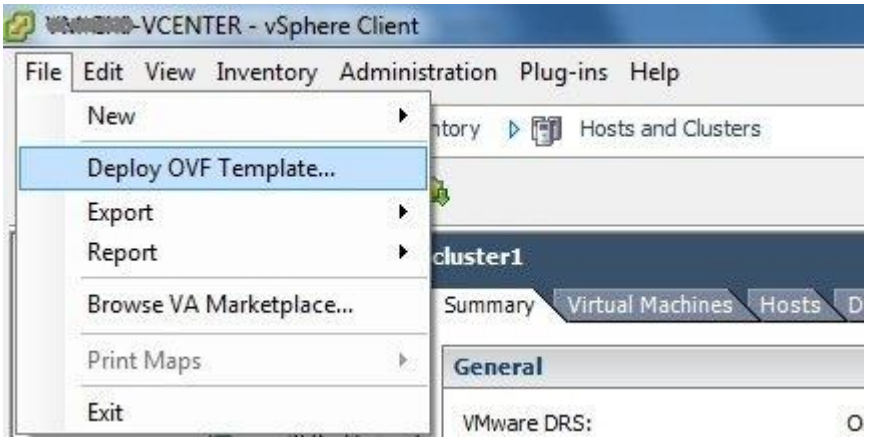
La fase di installazione termina con la richiesta di login.

```
Symantec Brightmail Gateway
Version 9.0.1-10
Copyright (c) 1998-2010 Symantec Corporation.  All rights reserved.

localhost login: admin
Password:
```

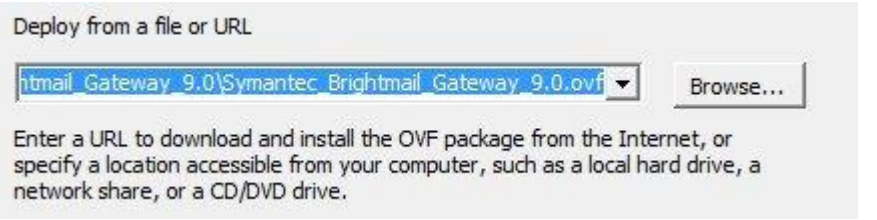
Installazione appliance in VMware vSphere

Se si ha a disposizione un'infrastruttura VMware *vSphere* o un server *ESX*, la versione appliance di *Brightmail* permette l'immediata funzionalità senza nessuna procedura di installazione.

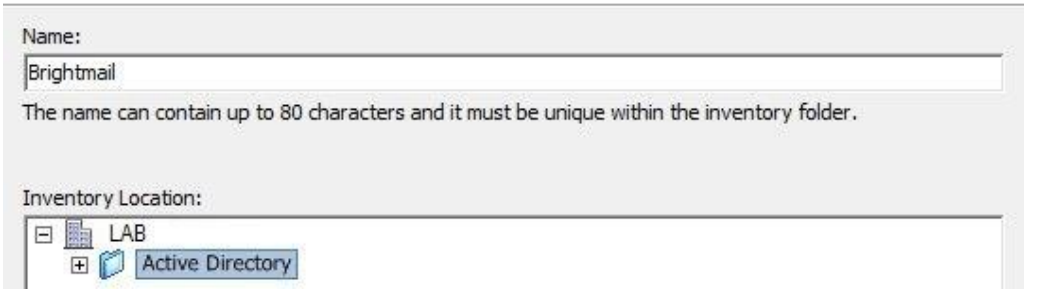
Da vSphere Client connettersi al *Server vCenter* ed installare l'appliance tramite: File –> Deploy OVF Template.



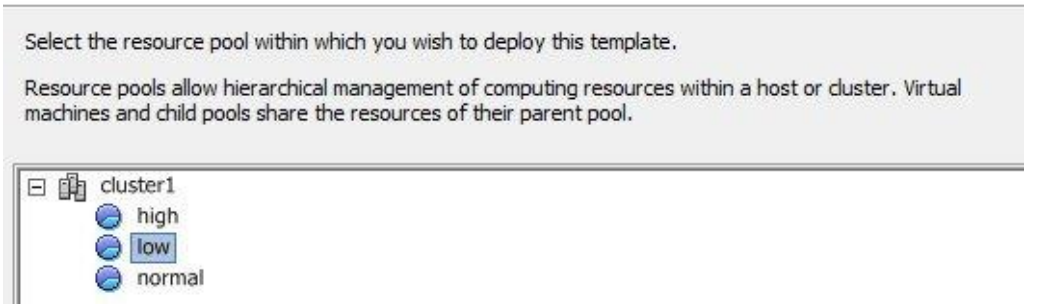
Specificare il path in cui è stato salvato il file ovf precedentemente scaricato.



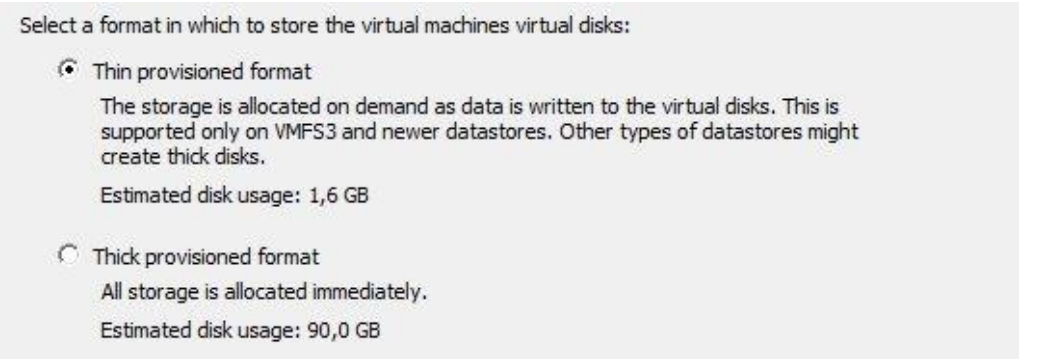
Assegnare un nome alla virtual machine. Nell'esempio viene chiamata semplicemente Brightmail. Assegnare inoltre un'eventuale riferimento nell'Inventory Location.



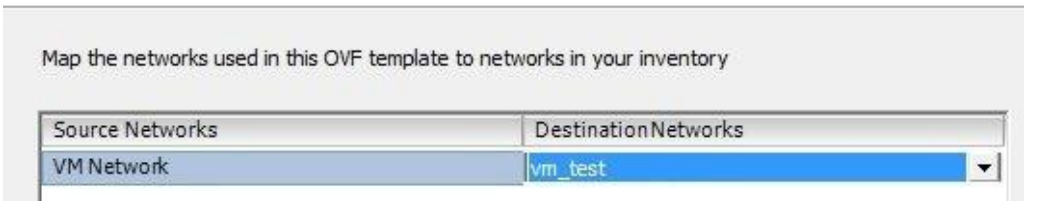
Se sono state create delle resource pool all'interno del cluster, selezionare la risorsa a cui si vuole assegnare l'applicazione. Essendo un test nell'esempio è stata selezionata la risorsa low.



In ambiente di produzione è consigliabile utilizzare il Thick provisioned format per migliorare le prestazioni. In questo caso essendo solo un test, è possibile selezionare l'opzione Thin provisioned format per risparmiare spazio prezioso sullo storage.

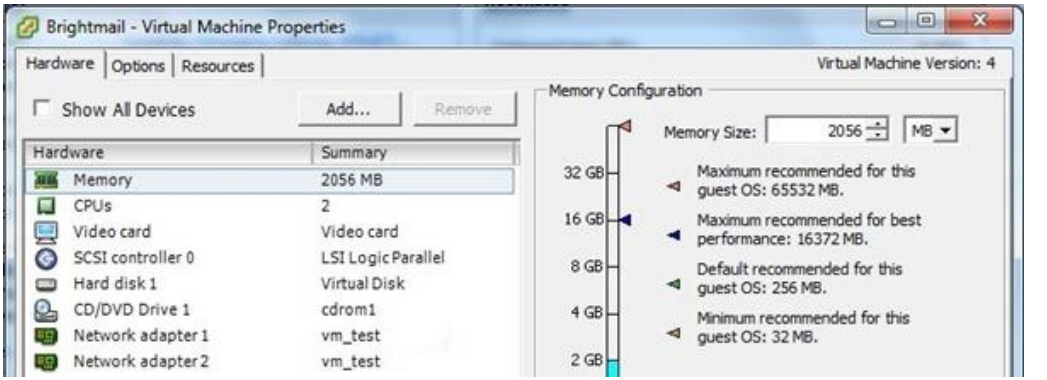


Assegnare la Destination Networks. Fare attenzione a cosa si seleziona in questa fase per non compromettere la funzionalità dell'applicazione.

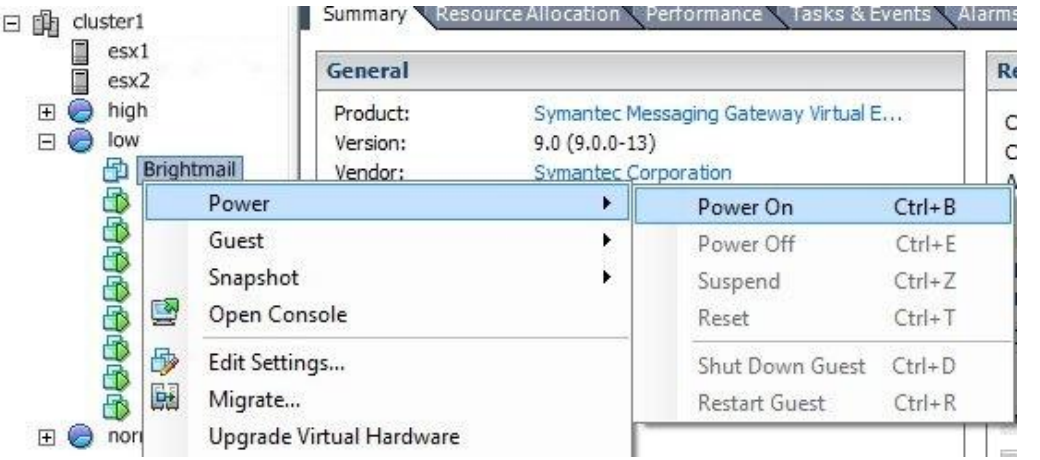


L'appliance viene caricata nello storage e resa disponibile in *vSphere/ESX*.

La configurazione hardware di default risulta come in figura. In base al carico di lavoro che *Brightmail* dovrà sostenere, bisognerà agire sui parametri RAM e CPUs.



A questo punto non rimane che effettuare il Power On della *virtual machine* per attivare l'applicazione.



Come già visto per l'installazione su *VMware Workstation*, il processo di boot si conclude con la richiesta del login.

Configurazione parametri di rete

Entrambi i metodi analizzati per l'installazione di *Brightmail* (immagine *ISO* o *appliance*) si concludono con la schermata di login.

Al primo login viene richiesto per motivi di sicurezza il cambio della password. I parametri di default per il primo accesso sono:

username: admin
password: symantec

```
Symantec Brightmail Gateway
Version 9.0.1-10
Copyright (c) 1998-2010 Symantec Corporation.  All rights reserved.

localhost login: admin
Password:
Welcome to Symantec Brightmail Gateway

Before you can begin using this appliance, it needs to be configured.
This wizard will guide you through the configuration process.

First you need to change your password.
New password:
```

Specificare l'hostname della *virtual machine*.

```
Specify a fully qualified host name for this appliance.
(example: mail6.company.com):
> brightmail.labtest.loc_
```

Specificare il codice corrispondente alla Timezone che si vuole impostare. La lista dei codici si ottiene digitando il simbolo "?", per l'Italia il codice è 29.

```
Enter the number corresponding to the timezone for this appliance.
Press '?' for a list:
> 29
```

Vengono adesso richiesti i parametri di rete. Assegnare l'indirizzo IP al primo NIC.

```
Specify the first IP address that you want to assign to this appliance.
(example: 192.168.0.1):
> 192.168.10.80_
```

Specificare la subnet della rete.

```
Specify the subnet mask that is associated with this ethernet interface.
(example: 255.255.255.0):
[default: 255.255.255.0]> 255.255.255.0
```

Poichè vengono utilizzati due NIC per la scansione dei messaggi inbound e outbound, aggiungere una seconda interfaccia ethernet digitando YES.

```
Do you want to use a second ethernet interface?
For information on when to use a second ethernet interface,
refer to the Symantec Brightmail Gateway Appliance Installation Guide.
[default: NO]> YES_
```

Assegnare l'indirizzo IP al secondo NIC.

```
Specify the IP address that you want to assign to this ethernet interface.
(example: 192.168.0.1):
> 192.168.10.81
```

Specificare la subnet della seconda interfaccia ethernet.

```
Specify the subnet mask that is associated with this ethernet interface.
(example: 255.255.255.0):
[default: 255.255.255.0]> 255.255.255.0
```

Digitare NO nella schermata successiva. Chiaramente questo parametro dipende dalla struttura della rete.

```
Do you want to configure a static route to connect to the Internet,
your DNS server, your LDAP server, or another appliance?
You can configure up to 3 static routes. For more information on when
to use a static route, refer to the Symantec Brightmail Gateway Appliance
Installation Guide.
[default: NO]> NO
```

Specificare l'indirizzo IP del gateway della rete.

```
Specify the IP address of the default gateway
(also known as the default router) on your network.
(example: 192.168.0.20):
> 192.168.10.1_
```

Specificare l'indirizzo IP del DNS primario della rete.

```
Specify the IP address of your first DNS server.
(example: 192.168.0.45):
> 192.168.10.1
```

Digitare NO se non si intende aggiungere un DNS secondario.

```
Would you like to specify another DNS server?
[default: YES]> NO
```

Selezionare il ruolo che viene svolto dall'applicazione. In questo caso digitare l'opzione "3" per far operare il sistema come Scanner and Control Center.

```
Specify the role for this appliance.  Available roles are:

    1. Scanner only
    2. Control Center only
    3. Scanner and Control Center

See the Installation Guide for more information.  If you have only one
Symantec Brightmail Gateway appliance, choose 'Scanner and Control Center'
What is the role for this appliance? (Type 1, 2, or 3):
> 3
```

Assegnato il ruolo, vengono riepilogati i parametri di rete specificati. Digitare YES per confermare.

```
Please confirm your configuration:

        Host Name: brightmail.company.com
        Timezone: 29. (GMT+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vien
na
        Ethernet Interface 1:
                IP Address: 192.168.10.80
                Subnet Mask: 255.255.255.0
        Static IP Routes: N/A
        Default Gateway: 192.168.10.1
        DNS Server 1: 192.168.10.1
        Role: Scanner and Control Center

Is this correct?
[default: NO]> YES_
```

Terminata la configurazione, la *virtual machine* si riavvia.

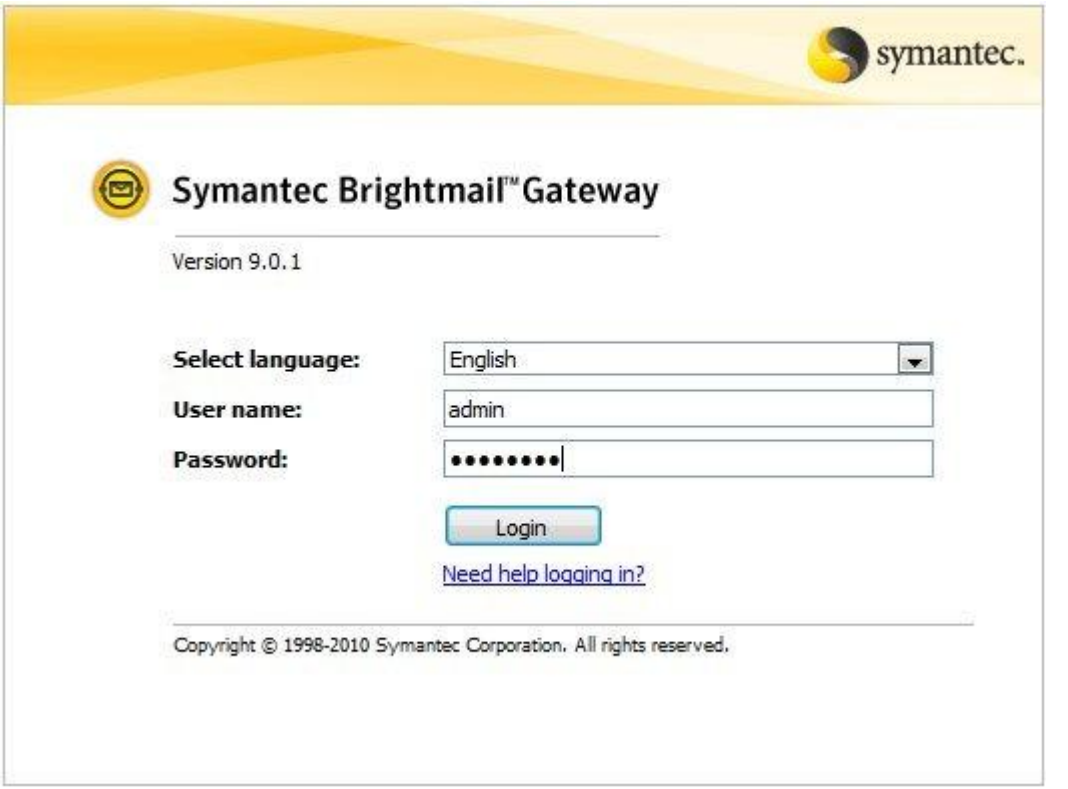
```
Initial configuration complete.

Broadcast message from root (tty1) (Mon Sep 20 15:48:20 2010):

INIT: Switching to runlevel: 6
INIT: Sending processes the TERM signal
Stopping sshd:                                             [  OK  ]
Stopping xinetd:                                           [  OK  ]
Stopping crond:                                            [  OK  ]
```

Login alla console di amministrazione

L'installazione di *Brightmail* è conclusa.

La fase di configurazione dei vari parametri si effettua tramite browser digitando l'URL https://IP_Address.

User name: admin
Password: quella impostata precedentemente durante il primo setup

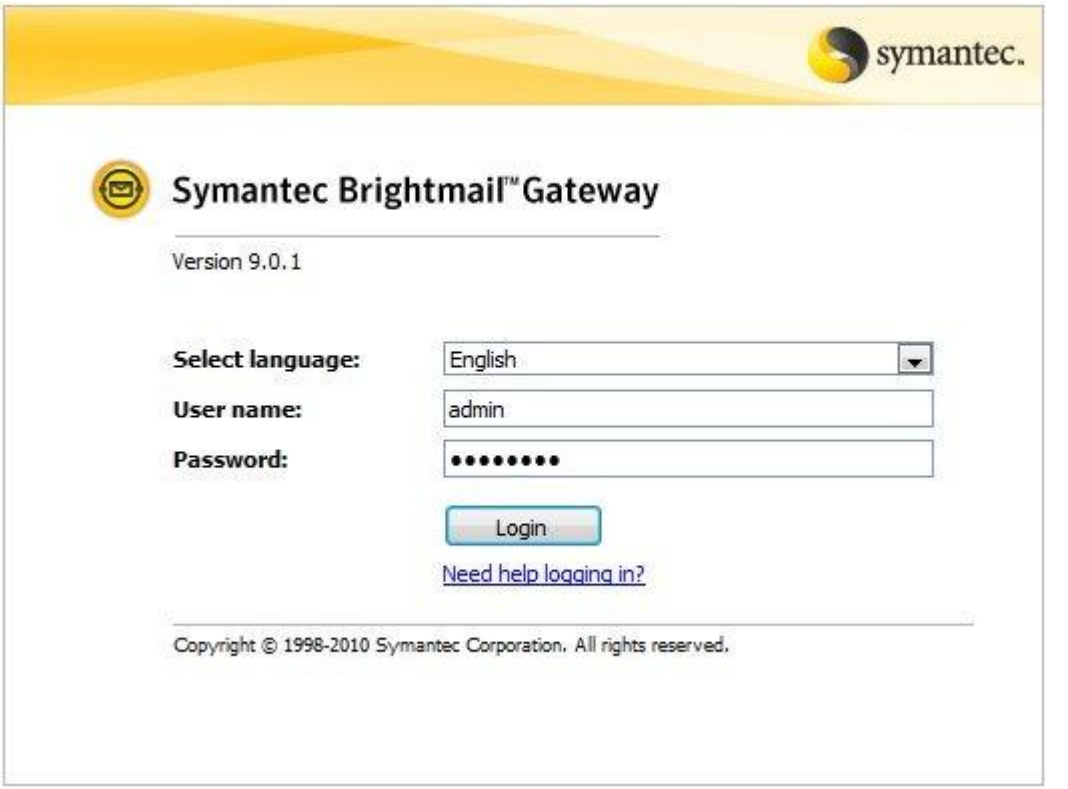


Installato il *mail server* e l'appliance *Brightmail*, viene analizzata la configurazione dell'applicazione per renderla finalmente operativa.

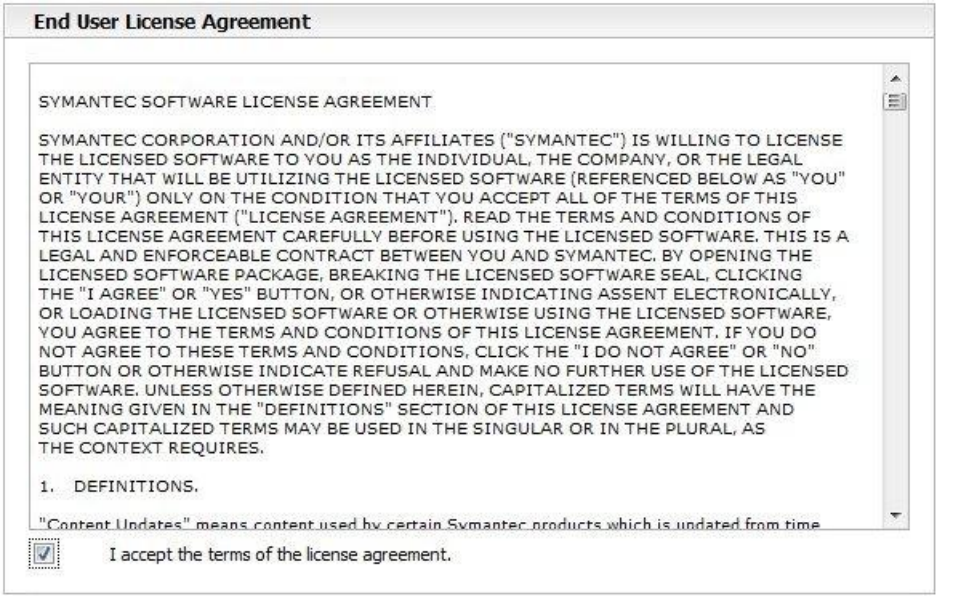
Naturalmente l'ottimizzazione della configurazione globale dell'applicazione dipende dalla tipologia e dimensione della rete. Fortunatamente il manuale fornito con *Brightmail* analizza in modo ampio le varie opzioni e parametri che si possono impostare.

Configurazione di Brightmail

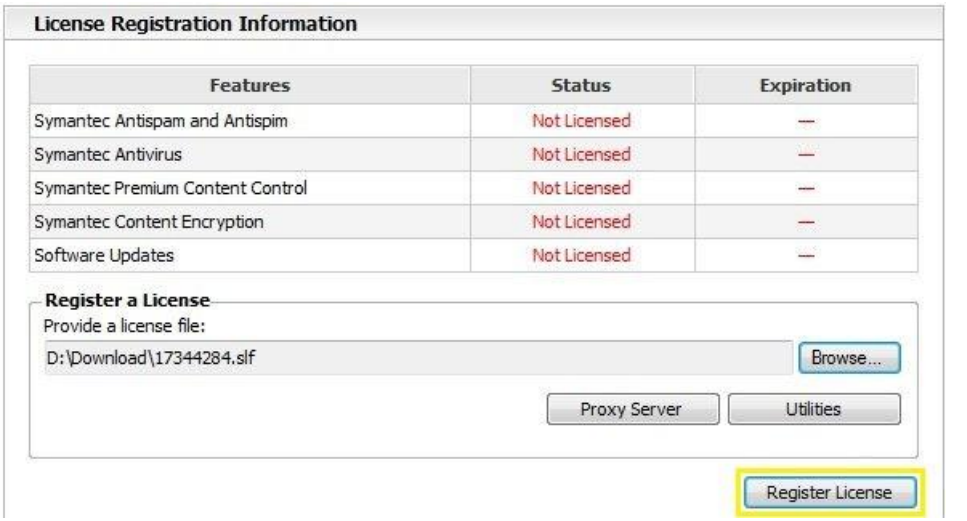
Per accedere al pannello di configurazione è necessario effettuare il login tramite browser. Digitare http://IP_Brightmail utilizzando come parametro uno dei due IP assegnati durante la fase di installazione. Digitare come username admin e come password quella assegnata in fase di installazione.



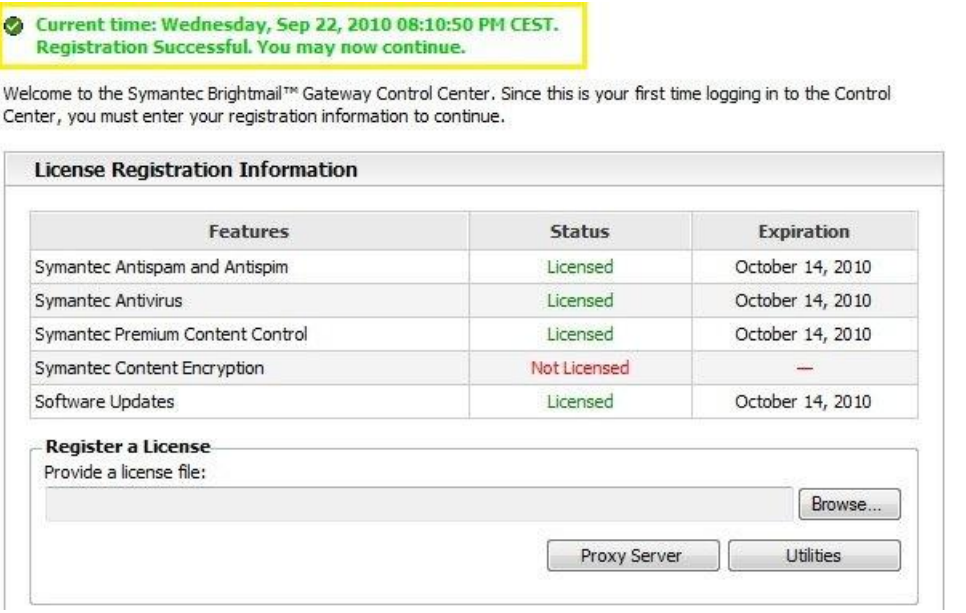
Al primo accesso viene presentata l'EULA. Mettere il flag su "*I accept the terms of the license agreement*." e proseguire cliccando su Next.



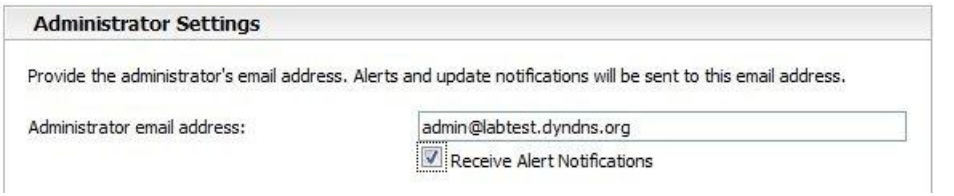
Quando è stato effettuato il download dell'applicazione dal sito della *Symantec*, nella casella email specificata durante la registrazione dovremmo trovare un file della licenza in formato *12345678.slf* che permette l'utilizzo di *Brightmail* per 30 giorni. Tramite il bottone Browse caricare il file di licenza e cliccare su Register License.



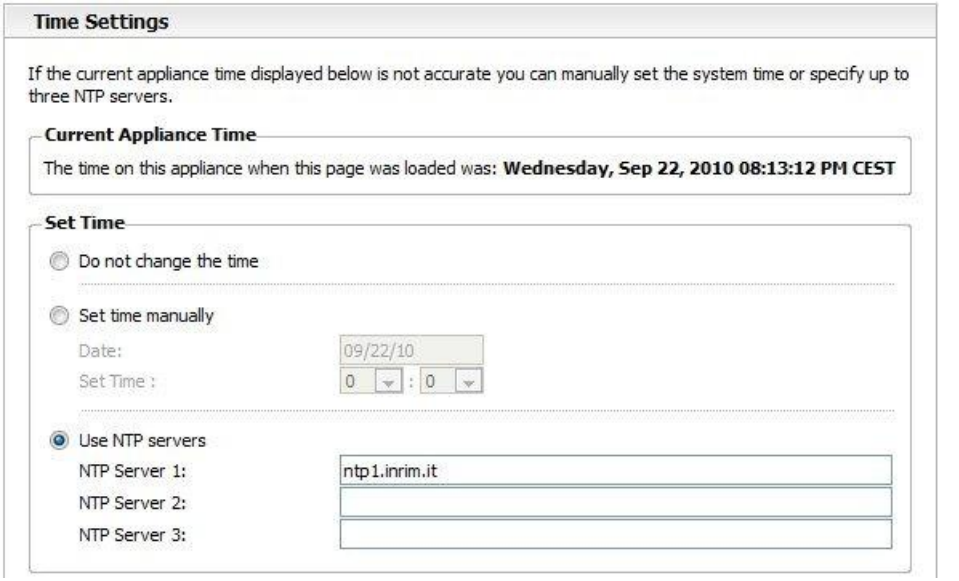
La corretta esecuzione del comando viene confermata dal messaggio di registrazione avvenuta.



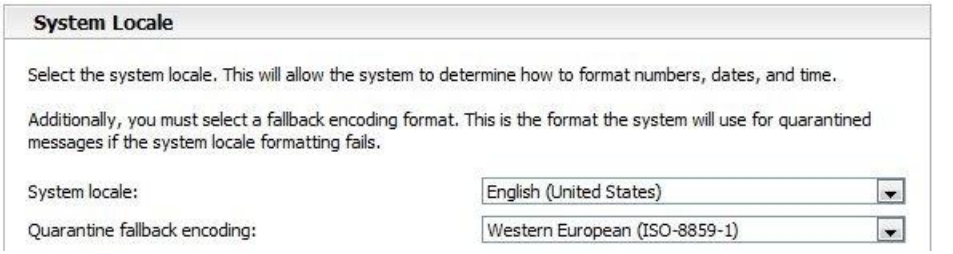
Attivato il prodotto, comincia la fase di configurazione. Specificare nella finestra che segue l'email dell'amministratore per ricevere le varie notifiche e messaggi del sistema.



Come visto più volte, tenere sincronizzati i sistemi presenti in una rete è un requisito fondamentale specialmente in presenza di strutture come Active Directory che richiedono la sincronizzazione del *Time* dei server per il protocollo di autenticazione Kerberos. E' opportuno quindi attivare l'opzione Use NTP servers specificando dei server NTP pubblici (ad esempio inrim.it) o che risiedono all'interno della rete.



Specificare il System Locale per determinare il formato dei numeri, della data e del tempo.



Nella finestra successiva bisogna specificare lo Scanner Role che si vuole attribuire al sistema. Volendo controllare sia i messaggi in entrata che in uscita, si attiva l'opzione Inbound and Outbound mail filtering.

Scanner Role

Specify the types of messages this scanner will filter. Any combination of SMTP can be combined with Instant Message filtering on your scanner.

If you have one Ethernet interface and you select instant message filtering along with any form of mail filtering, you must create a virtual IP address.

SMTP

- ○ Inbound mail filtering
- ○ Outbound mail filtering
- ◉ Inbound and Outbound mail filtering

Instant Messaging

- ☐ Instant message filtering

Assegnare quali interfacce Ethernet svolgeranno il compito di *inbound/outbound filter*. Come Inbound Mail Filtering specificare il primo IP configurato durante la fase di installazione.

Inbound Mail Filtering

Select an IP address and provide a port to be used for filtering inbound mail.

Inbound mail IP address:	Ethernet 1 (192.168.10.80)
Inbound mail SMTP port:	25

Essendo lo scanner delle email in arrivo (*Inbound Mail Filtering*), il filtro stesso dovrà accettare tutti gli indirizzi IP per permettere l'arrivo delle email da qualsiasi host.

Inbound Mail Filtering - Accepted Hosts

Does this machine receive mail directly from the internet or does it pass through upstream mail servers, either in your network or hosted? For the email firewall to work correctly with your upstream mail servers, ALL upstream mail servers must be listed.

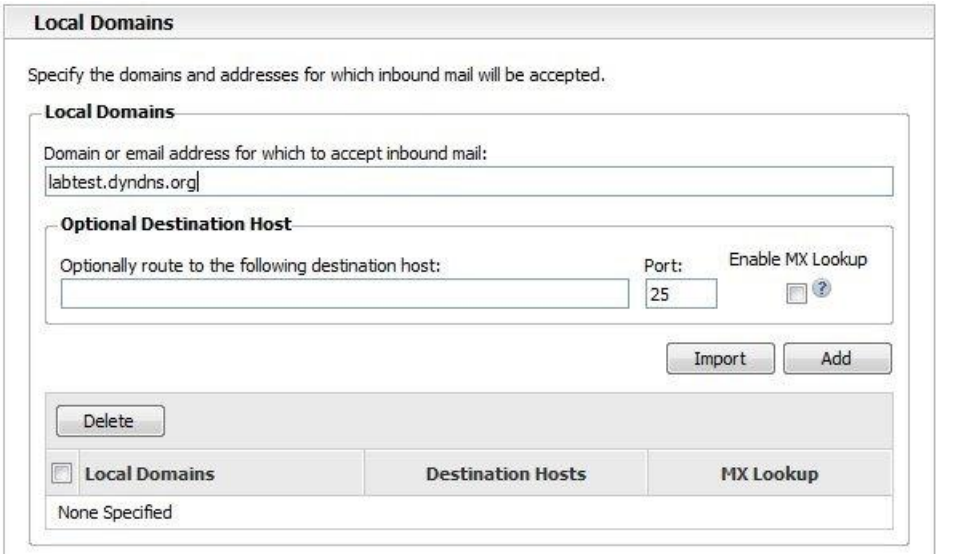
- ◉ All IP addresses
- ○ Specific IP addresses

Enter a list if IP addresses CIDR ranges or domains. You can also select existing IP addresses, CIDR ranges or domains.

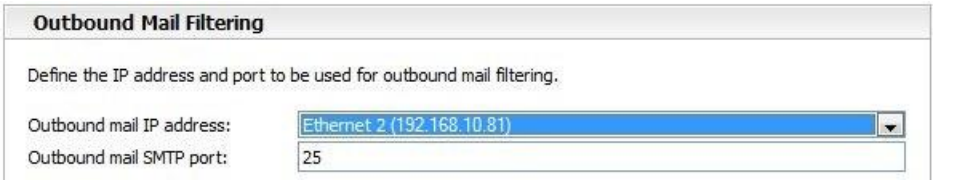
IP addresses/domains: [ ] Add

	Available IP Addresses/Domains
☐	192.168.10.80

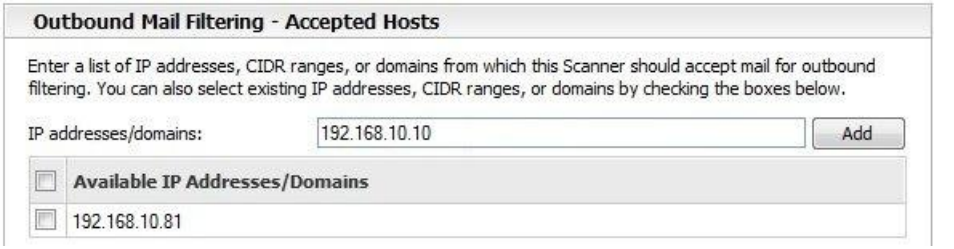
Specificare come Local Domains il dominio o domini di cui si vogliono ricevere le email. In pratica se il dominio aziendale è *companydomain.com*, questo è il dominio che deve essere indicato nel campo Domain or email address for which to accept inbound mail. Il domino utilizzato nel test è *labtest.dyndns.org*.



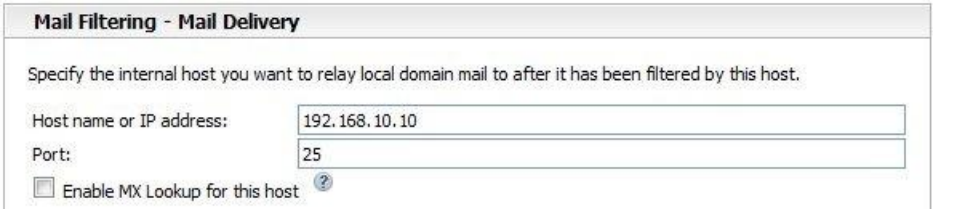
Come Outbound Mail Filtering specificare il secondo IP configurato durante la fase di installazione. Quindi delle due interfacce Ethernet configurate, una è assegnata per il controllo delle mail in entrata e la seconda per le mail in uscita.



Come Outbound Mail Filtering – Accepted Hosts specificare il dominio o gli indirizzi IP che lo scanner deve accettare per verificare le email in uscita. Aggiungere nel campo IP addresses/domains l'indirizzo IP del mail server aziendale.



Specificare come Mail Delivery l'hostname o l'indirizzo IP del mail server.

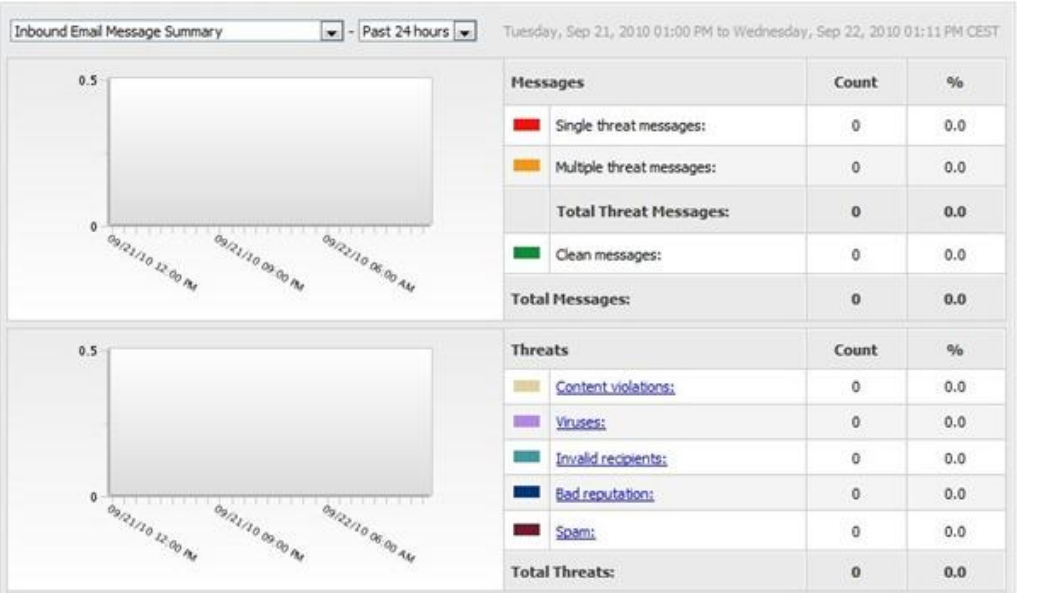


Come Mail Filtering – Non-local Mail Delivery, lasciare attiva l'opzione di default Use default MX Lookup.

Terminata la fase di configurazione, viene illustrato il riepilogo delle impostazioni effettuate.

Per attivare la configurazione appena terminata, salvare le impostazioni.

Quando il sistema viene attivato, si presenta la schermata inziale (Dashboard) dove vengono mostrate le varie statistiche. Inizialmente tutti i valori sono impostati a zero poichè non sono state processate ancora email.

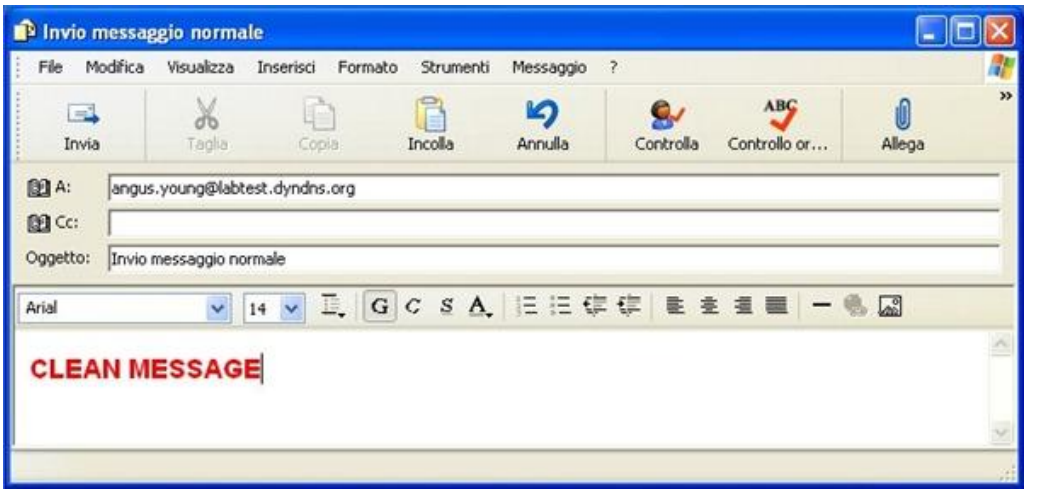


Testare Brightmail

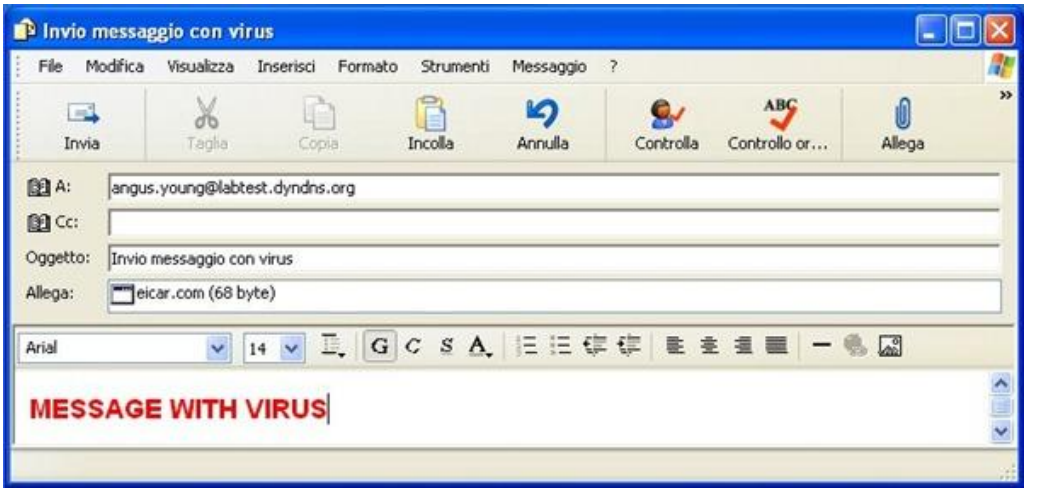
Impostato il sistema, la prossima fase prevede il test inviando alcune email contenenti messaggio normali, virus e spam.

Tramite un account di posta esterno al dominio aziendale, inviare una serie di email ad un account di posta del dominio interno protetto da *Brightmail*.

Il primo messaggio inviato è normale, clean.

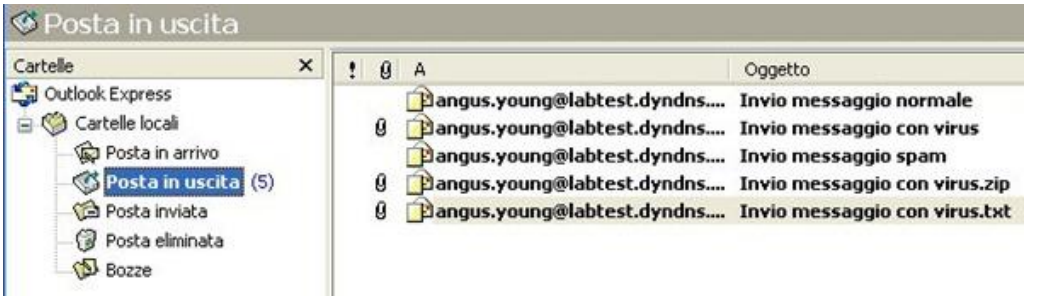


Viene inviato un secondo messaggio contenente un virus. Il virus per i test utilizzato è reperibile presso il sito http://eicar.org.



Il messaggio successivo contiene invece un codice di test che i sistemi riconoscono come spam.

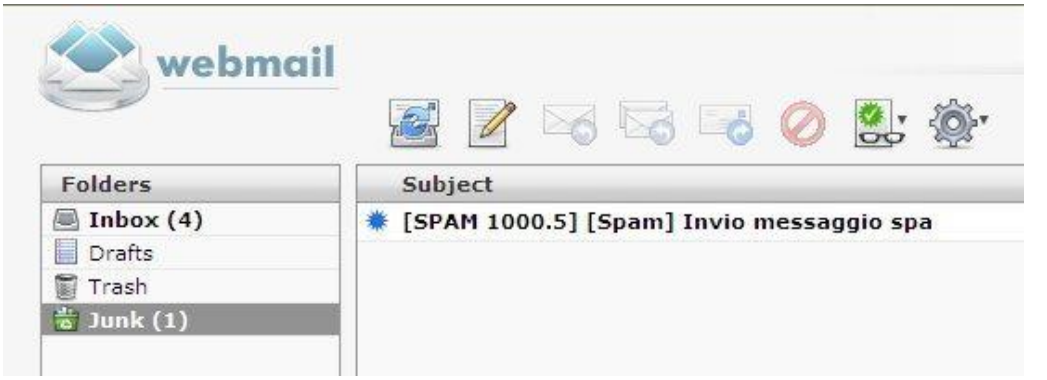
Nel test sono inviati inoltre messaggi con virus contenuti all'interno di file .zip e .txt. Nella posta di uscita sono visibili i vari messaggi che vengono inviati verso *Brightmail*.



Effettuare l'invio delle varie email.

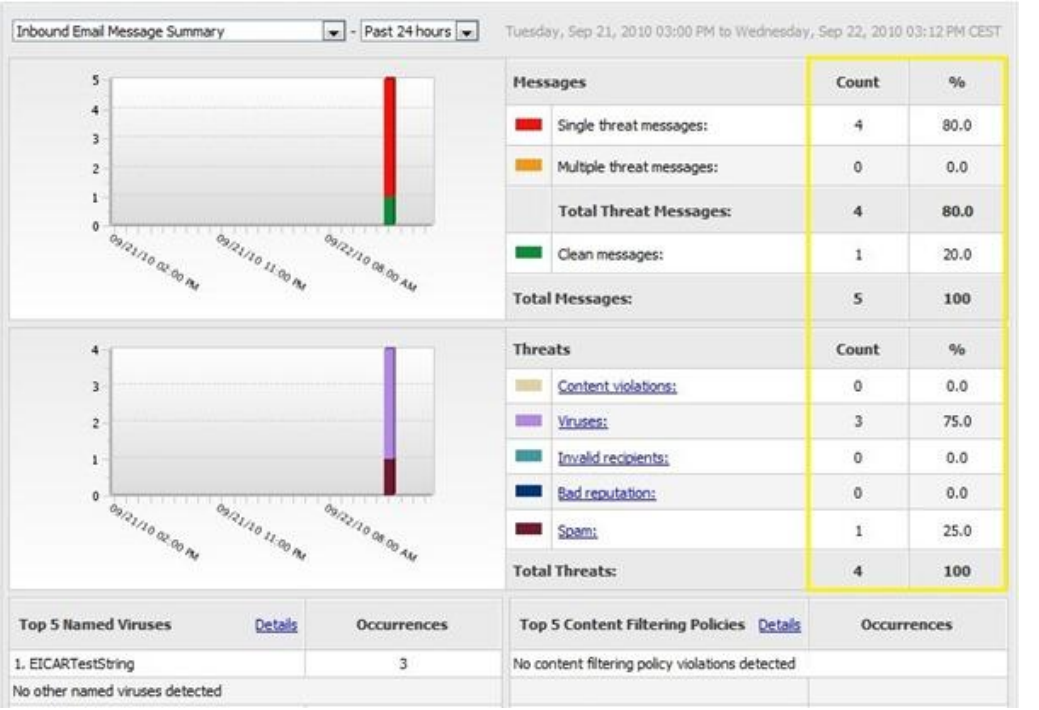
Se il tutto è stato configurato correttamente, al client di posta dell'account di dominio protetto da *Brightmail* dovrebbero arrivare le email inviate dall'account esterno.

Nel folder Junk compare anche la mail contenente la spam.



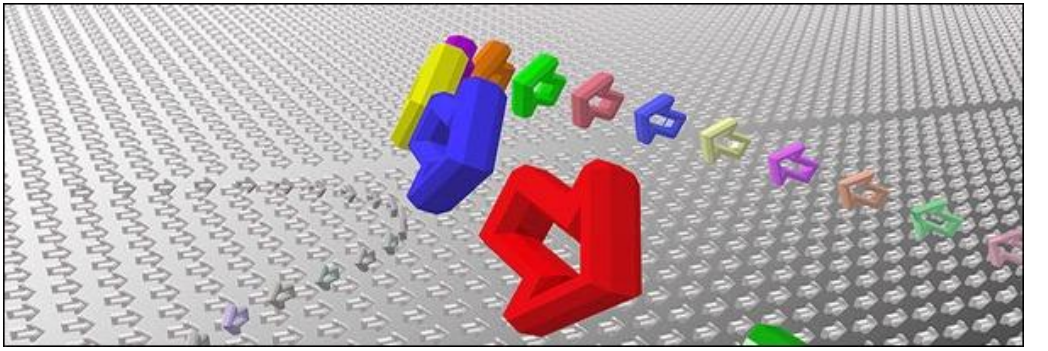
Aprendo il messaggio in cui era stato allegato un virus, si nota che il messaggio è stato scansionato da *Brightmail* che ha provveduto a cancellare il virus contenuto.

Dopo qualche minuto le statistiche dalla Dashboard vengono aggiornate dal sistema con le informazioni relative alle email appena ricevute.



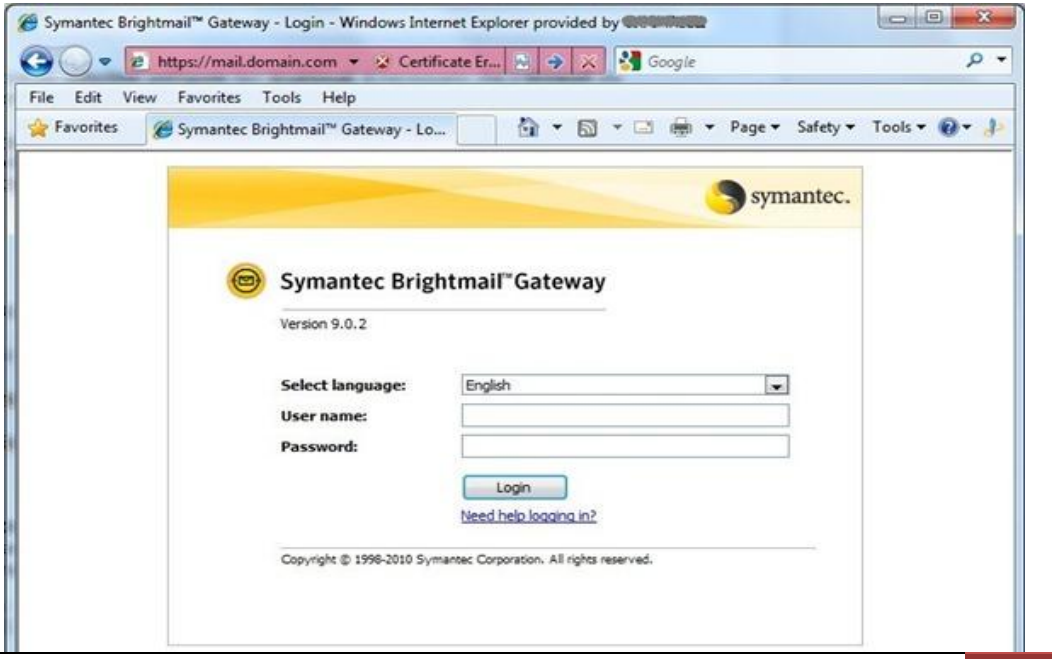
Brightmail è operativo proteggendo il dominio di posta aziendale in base ai parametri impostati. Tramite il manuale operativo è possibile ritoccare alcuni parametri adattando la funzionalità dell'applicazione allo specifico ambiente di rete.

Accedere alla WebMail (http) attraverso Brightmail



Utilizzando **soluzioni antispam** tipo *Brightmail*, il **firewall** deve essere configurato per permettere il corretto funzionamento del servizio email.

Poichè Brightmail viene **interposto tra l'accesso a Internet e il Mail Server**, quando si tenta di **accedere alla webmail** del sistema di posta tramite il **protocollo http**, viene visualizzata l'interfaccia di *Brightmail* anzichè della propria casella di posta.



Questo è il risultato che si ottiene quando il firewall non è configurato correttamente dopo l'installazione di *Brightmail*. Naturalmente per gli **utenti remoti o che utilizzano il browser** per accedere al servizio questo è un problema.

Proceedura

Supponiamo di avere il nostro sistema di posta formato da un Mail Server, Brightmail e un IP pubblico con i seguenti **parametri IP**:

Public IP: xx.xx.xx.78

Brightmail: 192.168.10.10

MailServer: 192.168.10.20

La configurazione viene effettuata sul firewall, quindi è necessario effettuare il login per **accedere alla configurazione**.

Configurazione firewall

Ovviamente data l'amplia gamma di firewall disponibili sul mercato, vengono **indicati solo i parametri** che devono essere impostati.

Bisogna intervenire su due parametri del firewall: **NAT e Rules**.

NAT

La logica è di instradare il **traffico smtp** da Internet su Brightmail che effettuerà l'analisi spam e virus, mentre il **traffico http/https** deve transitare direttamente sul Mail Server per accedere alla webmail.

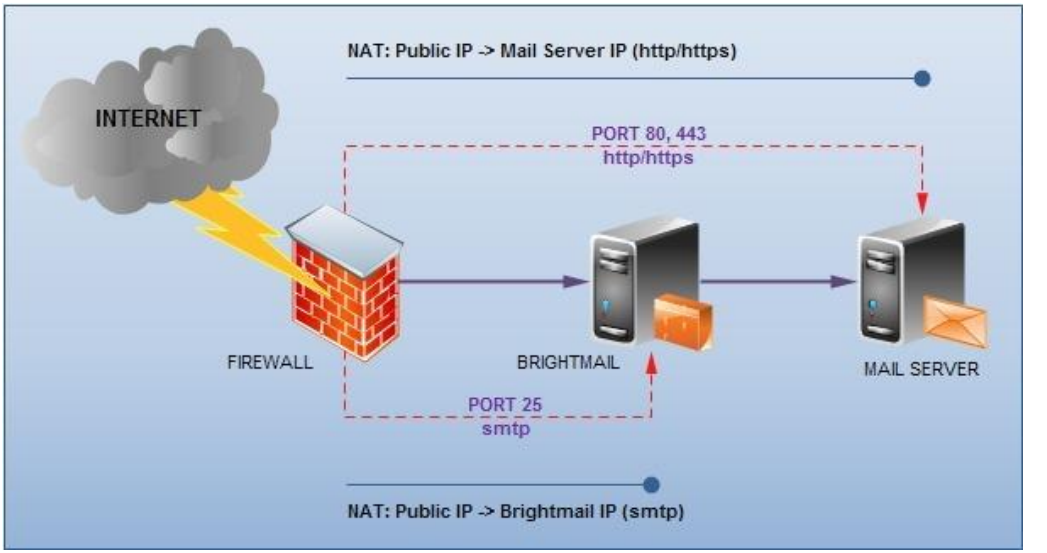
```
Public IP (xx.xx.xx.78) to Brightmail_IP (192.168.10.10) service
smtp
Public IP (xx.xx.xx.78) to MailServer_IP (192.168.10.20) service
http/https
```

RULES

Configurato il NAT, bisogna **aprire le porte del firewall** per permettere la comunicazione dei vari protocolli.

```
Allow from WAN to Brightmail_IP 192.168.10.10 port TCP 25 (smtp)
Allow from WAN to MailServer_IP 192.168.10.20 port TCP 80, 443
(http/https)
```

Lo **schema** è illustrato nella figura seguente:



Salvata la nuova configurazione del firewall, verificare che il tutto funziona come dovrebbe.

Digitando dal browser **l'URL della webmail** (es. mail.domain.com), compare correttamente la finestra di login al sistema di posta e non più a *Brightmail*.

Verificare inoltre che la **spedizione e ricezione delle email** funzioni correttamente.

La modifica al firewall richiede pochi passaggi e **non richiede nessuna interruzione** dei servizi di rete.

Testare il servizio AntiSpam

Il problema spam è così presente che le aziende sono costrette a dotarsi di un sistema di protezione per le proprie caselle email.

Il mercato offre varie soluzioni di sistemi antispam che possono soddisfare qualsiasi tipo di esigenza.

Ma come verificare la bontà e l'efficienza di un sistema antispam? Un sistema molto semplice è l'utilizzo di una stringa di testo (GTUBE test http://spamassassin.apache.org/gtube/) che permette di testare il servizio antispam.

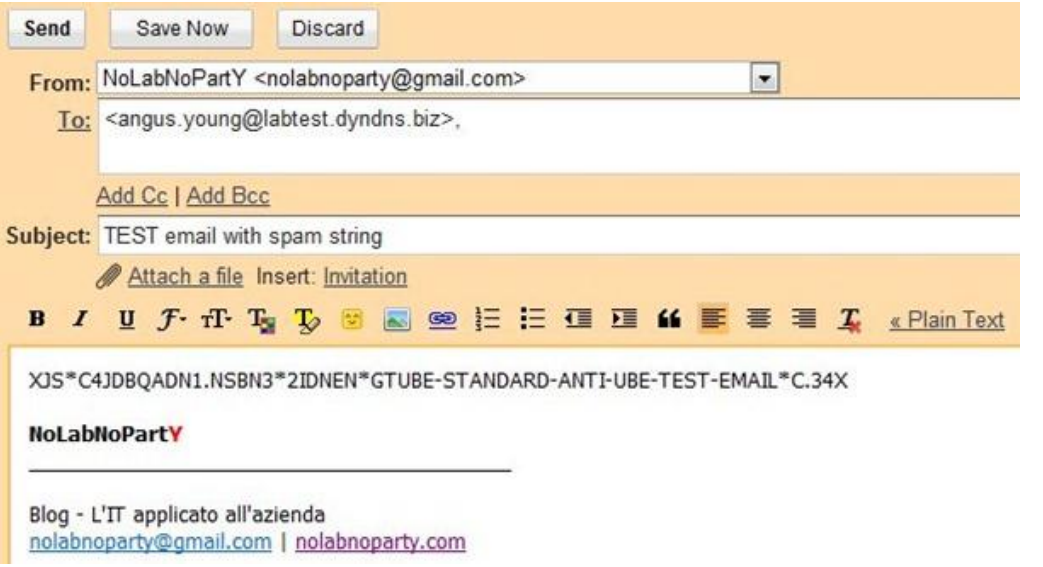
Procedura

Tramite un account di posta esterna, creare una nuova email.

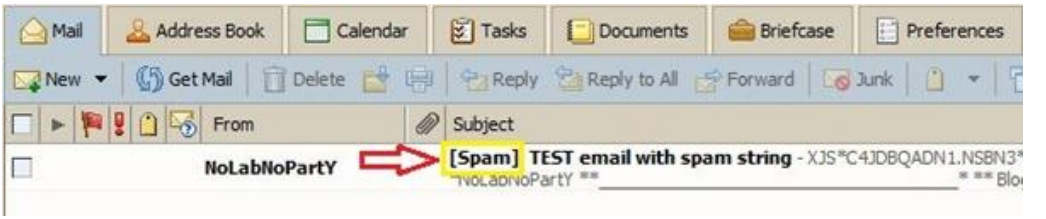
Copiare la stringa qui riportata nel corpo del messaggio verificando che non ci siano spazi extra.

*XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL*C.34X*

Inviare la mail all'indirizzo di una casella email nel server protetto dal sistema antispam che si vuole testare.



L'antispam riconosce la mail come un messaggio "junk" e agisce in base alla configurazione impostata nel sistema. In questo caso il messaggio viene marcato come [Spam] recapitato nella mailbox.



Analizzando il log del sistema antispam, viene riportato il transito di una email considerata spam.

Threats		Count	%
	Content violations:	0	0.0
	Viruses:	0	0.0
	Invalid recipients:	0	0.0
	Bad reputation:	0	0.0
	Spam:	1	100
Total Threats:		**1**	**100**

Con questo semplice test è possibile verificare nell'immediato se la soluzione antispam implementata risponde alle attese. E' meglio testare il sistema per qualche settimana prima di metterlo in produzione.

Messaggistica

Installare Zimbra come servizio di posta elettronica su CentOS 5.x

La posta elettronica è ormai un servizio indispensabile per il business di qualsiasi azienda. Testare nuove soluzioni per contenere i costi e migliorare la produttività è ormai un target per tutti gli addetti informatici.

Tra le varie proposte del mercato, Zimbra (acquisita nel 2010 da *VMware*) sembra essere una valida alternativa ai più blasonati sistemi di posta *Microsoft Exchange* o *Lotus Domino*. Nelle tre edizioni disponibili, i tagli utenti offerti sono molto vantaggiosi e soprattutto le PMI possono avere a disposizione un buon sistema alternativo con una spesa contenuta.

Naturalmente, come ogni prodotto, una fase di test deve essere effettuata per verificare che le esigenze del proprio business siano effettivamente soddisfatte.

Prerequisiti

Per eseguire l'installazione di *Zimbra*, sono richieste tre principali verifiche:

Spazio disco sufficiente

Presenza dei package prerequisiti

Impostazione corretta del file */etc/hosts*

Poichè Zimbra viene installato come default nella partizione ***/opt***, verificare che ci siano almeno 10GB di spazio disponibili su disco per evitare problemi durante l'installazione.

Partendo da un'installazione minima di *CentOS*, installare i package mancanti richiesti.

```
# yum install perl sudo libidn gmp sysstat
```

Editare il file */etc/hosts* ed impostare i seguenti parametri:

127.0.0.1 localhost.localdomain localhost
ip_host FQDN hostname

```
127.0.0.1       localhost.localdomain localhost
::1             localhost6.localdomain6 localhost6

192.168.10.20   vm-lx5-zimbra.lab.local
```

Procedura

Scompattare il file scaricato dal sito di *Zimbra* ed eseguire l'installazione lanciando il comando install.sh. Installando l'applicazione su Linux *CentOS*, è necessario specificare il parametro –platform-override.

```
# tar -xzvf zcs-NETWORK-6.0.9_GA_2686.RHEL5.20101115224226.tgz
# mv zcs-NETWORK-6.0.9_GA_2686.RHEL5.20101115224226 zcs
# cd zcs
# ./install -platform-override
```

```
[root@vm-lx5-zimbra zcs]# ./install.sh --platform-override

Operations logged to /tmp/install.log.4914
Checking for existing installation...
    zimbra-ldap...NOT FOUND
    zimbra-logger...NOT FOUND
    zimbra-mta...NOT FOUND
    zimbra-snmp...NOT FOUND
    zimbra-store...NOT FOUND
    zimbra-apache...NOT FOUND
    zimbra-spell...NOT FOUND
```

Durante la fase di installazione vengono verificati i prerequisiti di *Zimbra*. Nel caso manchi qualche package, il sistema blocca l'installazione visualizzando i prerequisiti mancanti.

```
Checking for prerequisites...
     FOUND: NPTL
     MISSING: sudo
     MISSING: libidn
     MISSING: gmp
     FOUND: /usr/lib/libstdc++.so.6
Checking for suggested prerequisites...
    FOUND: perl-5.8.8
    MISSING: sysstat does not appear to be installed.
```

Installare eventualmente i package mancanti e rilanciare lo script *install.sh*. Digitare Y per accettare l'EULA e premere Invio.

```
Do you agree with the terms of the software license agreement? [N] y

Checking for prerequisites...
     FOUND: NPTL
     FOUND: sudo-1.7.2p1-9
     FOUND: libidn-0.6.5-1.1
     FOUND: gmp-4.1.4-10
     FOUND: /usr/lib/libstdc++.so.6
Checking for suggested prerequisites...
    FOUND: perl-5.8.8
    FOUND: sysstat
Prerequisite check complete.

Checking for installable packages

Found zimbra-core
Found zimbra-ldap
Found zimbra-logger
Found zimbra-mta
```

Successivamente specificare le opzioni che *Zimbra* deve installare.

- Install zimbra-ldap [Y] **y**
- Install zimbra-logger [Y] **y**
- Install zimbra-mta [Y] **y**
- Install zimbra-snmp [Y] **y**
- Install zimbra-store [Y] **y**
- Install zimbra-apache [Y] **y**
- Install zimbra-spell [Y] **y**
- Install zimbra-convertd [Y] **y**
- Install zimbra-memcached [N] **y**
- Install zimbra-proxy [N] **y**
- Install zimbra-archiving [N]

```
Select the packages to install

Install zimbra-ldap [Y] y

Install zimbra-logger [Y] y

Install zimbra-mta [Y] y

Install zimbra-snmp [Y] y
```

Poichè l'installazione viene effettuata sul sistema CentOS, la procedura di installazione visualizza un warning. Digitare Y e premere Invio per continuare.

```
You appear to be installing packages on a platform different
than the platform for which they were built.

This platform is CentOS5
Packages found: RHEL5
This may or may not work.

Using packages for a platform in which they were not designed for
may result in an installation that is NOT usable. Your support
options may be limited if you choose to continue.


Install anyway? [N] Y
```

Alla domanda successiva, digitare Y e premere Invio.

```
The system will be modified.  Continue? [N] Y

Removing /opt/zimbra
Removing zimbra crontab entry...done.
done.
Cleaning up zimbra init scripts...done.
Cleaning up /etc/ld.so.conf...done.
Cleaning up /etc/prelink.conf...done.
Cleaning up /etc/security/limits.conf...done.

Finished removing Zimbra Collaboration Suite.

Installing packages

    zimbra-core......zimbra-core-6.0.9 GA 2686.RHEL5-20101115224226.i386.rpm...
```

Terminata la procedura viene visualizzato il menu principale. Nelle voci dove compare il doppio asterisco (*Admin Password*), è necessario specificare i parametri mancanti.

Digitare 3 al *prompt* e premere Invio.

```
Main menu

   1) Common Configuration:
   2) zimbra-ldap:                                Enabled
   3) zimbra-store:                               Enabled
        +Create Admin User:                       yes
        +Admin user to create:                    admin@vm-lx5-zimbra.lab.local
******* +Admin Password                           UNSET
        +Enable automated spam training:          yes
        +Spam training user:                      spam.1ib5smjpap@vm-lx5-zimbra.lab.
        +Non-spam(Ham) training user:             ham.xbgmtcbrb@vm-lx5-zimbra.lab.lo
        +Global Documents Account:                wiki@vm-lx5-zimbra.lab.local
        +SMTP host:                               vm-lx5-zimbra.lab.local
        +Web server HTTP port:                    80
        +Web server HTTPS port:                   443
        +Web server mode:                         http
        +IMAP server port:                        143
        +IMAP server SSL port:                    993
        +POP server port:                         110
        +POP server SSL port:                     995
  ____________________________________________________________________________
  10) Enable default backup schedule:             yes
   c) Collapse menu
   r) Start servers after configuration           yes
   s) Save config to file
   q) Quit

Address unconfigured (**) items   (? - help) 3
```

Viene visualizzato un altro menu Store Configuration. Le voci indicate dagli asterischi devono essere configurate.

```
Store configuration

   1) Status:                                  Enabled
   2) Create Admin User:                       yes
   3) Admin user to create:                    admin@vm-lx5-zimbra.lab.local
** 4) Admin Password                           UNSET
   5) Enable automated spam training:          yes
   6) Spam training user:                      spam.1ib5smjpap@vm-lx5-zimbra.lab.local
   7) Non-spam(Ham) training user:             ham.xbgmtcbrb@vm-lx5-zimbra.lab.local
   8) Global Documents Account:                wiki@vm-lx5-zimbra.lab.local
   9) SMTP host:                               vm-lx5-zimbra.lab.local
  10) Web server HTTP port:                    80
  11) Web server HTTPS port:                   443
  12) Web server mode:                         http
  13) IMAP server port:                        143
  14) IMAP server SSL port:                    993
  15) POP server port:                         110
  16) POP server SSL port:                     995
  17) Use spell check server:                  yes
  18) Spell server URL:                        http://vm-lx5-zimbra.lab.local:7780/aspell.php
  19) Configure for use with mail proxy:       FALSE
  20) Configure for use with web proxy:        FALSE
  21) Enable version update checks:            TRUE
  22) Enable version update notifications:     TRUE
  23) Version update notification email:       admin@vm-lx5-zimbra.lab.local
  24) Version update source email:             admin@vm-lx5-zimbra.lab.local
** 25) License filename:                       UNSET

Select, or 'r' for previous menu [r]
```

Digitare 4 al *prompt* e inserire la password.

```
Select, or 'r' for previous menu [r] 4

Password for admin@vm-lx5-zimbra.lab.local (min 6 characters): [TM1Drqjd] password
```

Digitare 25 al *prompt* e specificare il path del file.xml della licenza.

```
Select, or 'r' for previous menu [r] 25

Enter the name of the file that contains the license: ZCSLicense.xml
ZCSLicense.xml must exist and be readable
Enter the name of the file that contains the license: /install/ZCSLicense.xml
```

I parametri appena specificati vengono marcati come SET.

```
Store configuration

   1) Status:                                  Enabled
   2) Create Admin User:                       yes
   3) Admin user to create:                    admin@vm-lx5-zimbra.ciccarelli.local
   4) Admin Password                           set
   5) Enable automated spam training:          yes
   6) Spam training user:                      spam.lib5smjpap@vm-lx5-zimbra.ciccarelli.local
   7) Non-spam(Ham) training user:             ham.xbgmtcbrb@vm-lx5-zimbra.ciccarelli.local
   8) Global Documents Account:                wiki@vm-lx5-zimbra.ciccarelli.local
   9) SMTP host:                               vm-lx5-zimbra.ciccarelli.local
  10) Web server HTTP port:                    80
  11) Web server HTTPS port:                   443
  12) Web server mode:                         http
  13) IMAP server port:                        143
  14) IMAP server SSL port:                    993
  15) POP server port:                         110
  16) POP server SSL port:                     995
  17) Use spell check server:                  yes
  18) Spell server URL:                        http://vm-lx5-zimbra.ciccarelli.local:7780/aspell.php
  19) Configure for use with mail proxy:       FALSE
  20) Configure for use with web proxy:        FALSE
  21) Enable version update checks:            TRUE
  22) Enable version update notifications:     TRUE
  23) Version update notification email:       admin@vm-lx5-zimbra.ciccarelli.local
  24) Version update source email:             admin@vm-lx5-zimbra.ciccarelli.local

Select, or 'r' for previous menu [r]
```

Digitare r per ritornare al Main menu. La configurazione è ora completa.

```
Select, or 'r' for previous menu [r] r

Main menu

   1) Common Configuration:
   2) zimbra-ldap:                              Enabled
   3) zimbra-store:                             Enabled
   4) zimbra-mta:                               Enabled
   5) zimbra-snmp:                              Enabled
   6) zimbra-logger:                            Enabled
   7) zimbra-spell:                             Enabled
   8) zimbra-convertd:                          Enabled
   9) Default Class of Service Configuration:
  10) Enable default backup schedule:           yes
   r) Start servers after configuration         yes
   s) Save config to file
   x) Expand menu
   q) Quit

*** CONFIGURATION COMPLETE - press 'a' to apply
Select from menu, or press 'a' to apply config (? - help)
```

Per salvare la configurazione, digitare a al *prompt* e premere Invio. In questa fase viene ultimata la configurazione del sistema.

```
*** CONFIGURATION COMPLETE - press 'a' to apply
Select from menu, or press 'a' to apply config (? - help) a
Save configuration data to a file? [Yes]
Save config in file: [/opt/zimbra/config.11754]
Saving config in /opt/zimbra/config.11754...done.
The system will be modified - continue? [No] yes
Operations logged to /tmp/zmsetup.11302010-153638.log
Setting local config values...done.
Setting up CA...done.
Deploying CA to /opt/zimbra/conf/ca ...done.
Creating SSL certificate...done.
```

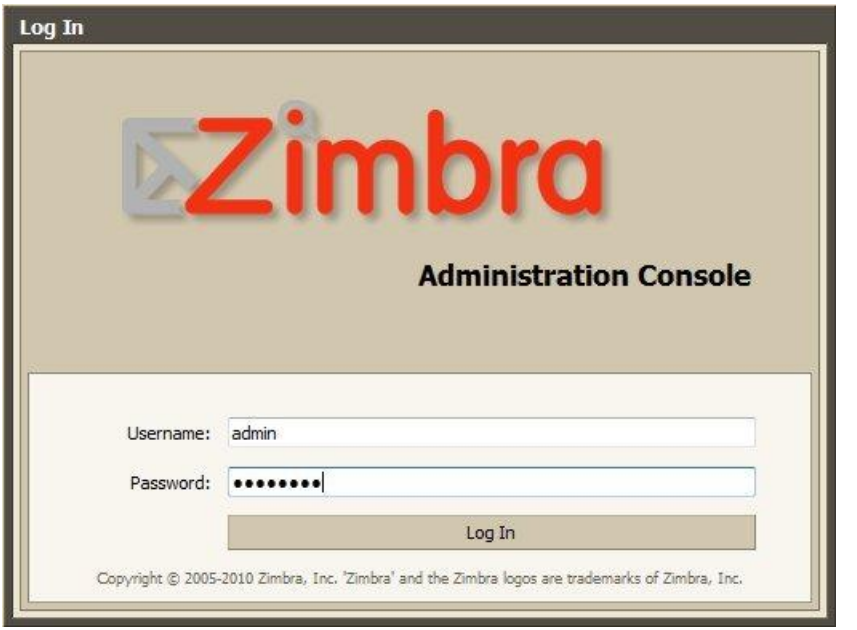
Dopo qualche minuto la procedura di installazione termina con la visualizzazione del messaggio Configuration complete. Premere Invio.

```
Finished installing network zimlets.
Initializing Documents...done.
Restarting mailboxd...done.
Setting up zimbra crontab...done.


Moving /tmp/zmsetup.11302010-153638.log to /opt/zimbra/log


Configuration complete - press return to exit
```

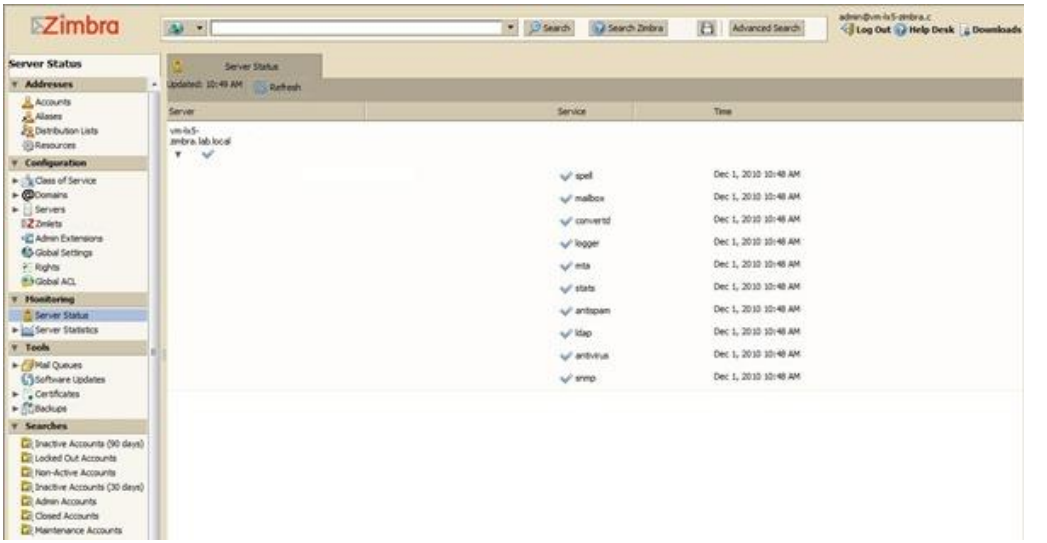
Dal browser di Internet, digitare l'indirizzo https://IP_zimbra:7071 per accedere alla pagina di login della Administration Console.

Per effettuare il login, digitare:

Username: admin
Password: la password specificata precedentemente



Cliccando sul bottone Log In si accede alla pagina di amministrazione di *Zimbra*.



Rimozione di Zimbra

Se per un qualsiasi motivo si ha l'esigenza di rimuovere l'applicazione, lanciare da console il comando:

```
# ./install -u
```

```
Completely remove existing installation? [N] y

Shutting down zimbra mail

Removing existing packages

   zimbra-ldap...done
   zimbra-logger...done
   zimbra-mta...done
   zimbra-snmp...done
```

L'installazione di *Zimbra* è conclusa.

Dopo aver visto l'installazione del sistema di posta *Zimbra*, non rimane che configurare e testare l'applicazione per verificare il suo funzionamento.

Naturalmente la configurazione ottimale dipende da molti fattori… numero di account, domini, tipo di autenticazione, etc. ma per le PMI senza necessità particolari la configurazione è abbastanza scorrevole.

Configurazione

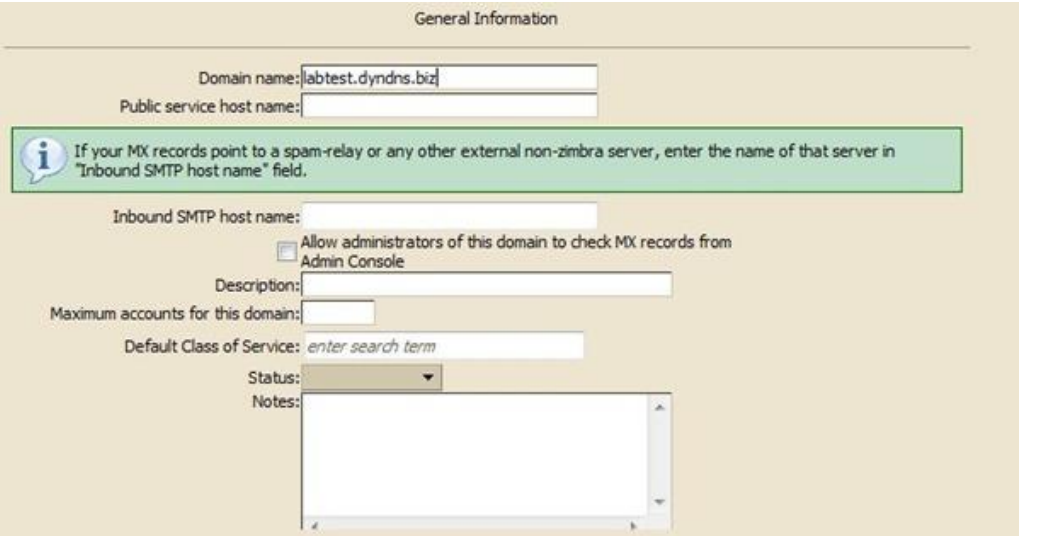
Prima cosa è necessario avere un indirizzo IP pubblico statico o dinamico perchè altrimenti la ricezione delle email dall'esterno sarebbe impossibile.

Con un IP statico bisogna far configurare nel DNS del maintainer il record MX. Nel caso invece di IP dinamico, quello rilasciato comunemente per utenze casalinghe, ci si affida ai servizi DNS dinamici tipo DynDNS dove occorre configurare opportunamente l'account.

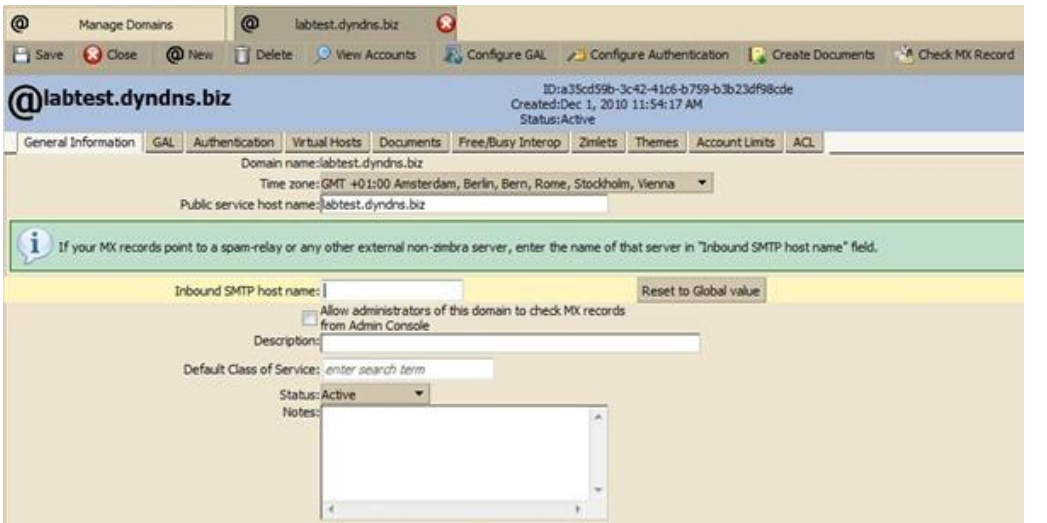
Creazione del dominio e degli account

Un'ampia documentazione è disponibile presso il sito e la pagina wiki di *Zimbra*.

Per creare/gestire i domini, dall'*Administration Console* selezionare nella parte sinistra Configuration –> Domains e cliccare sulla destra la voce New.



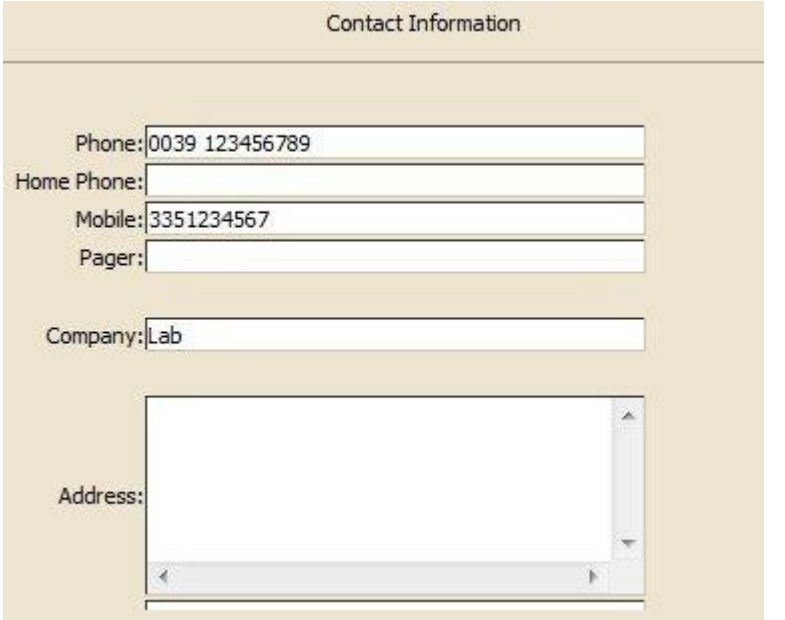
Creato il dominio è sempre possibile accedere alla sua configurazione selezionandolo e cliccando la voce Edit.



Per creare/gestire gli account, dall'*Administration Console* selezionare nella parte sinistra Addresses –> Account e cliccare sulla destra New-> Account.

Definire l'Account Name e completare i campi richiesti. Click Next per proseguire.

Da qui in poi sono visualizzate alcune finestre inerenti ad impostazioni supplementari non strettamente richieste per il funzionamento base dell'account.

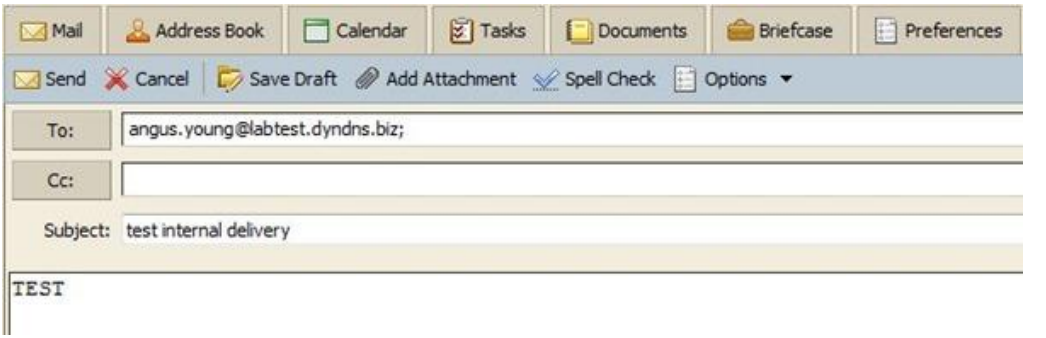


Cliccare sul bottone Finish per terminare e creare l'account.

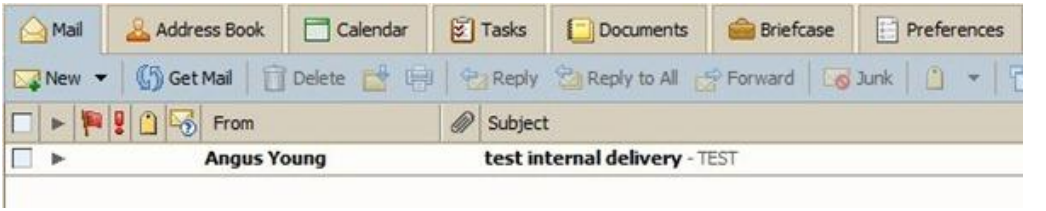
Testare Zimbra

Una volta configurato il sistema, non rimane che testarlo.

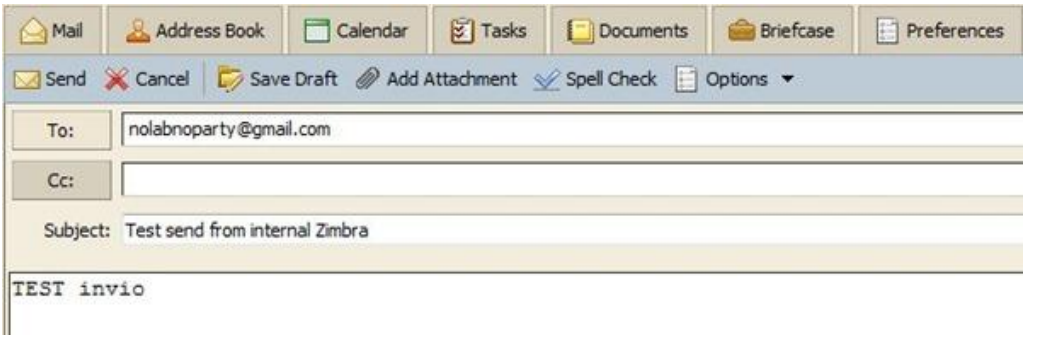
Spedire una email da *Zimbra* ad un account interno per vedere se il delivery della posta interna funziona.



Dopo qualche secondo, l'email viene recapitata.

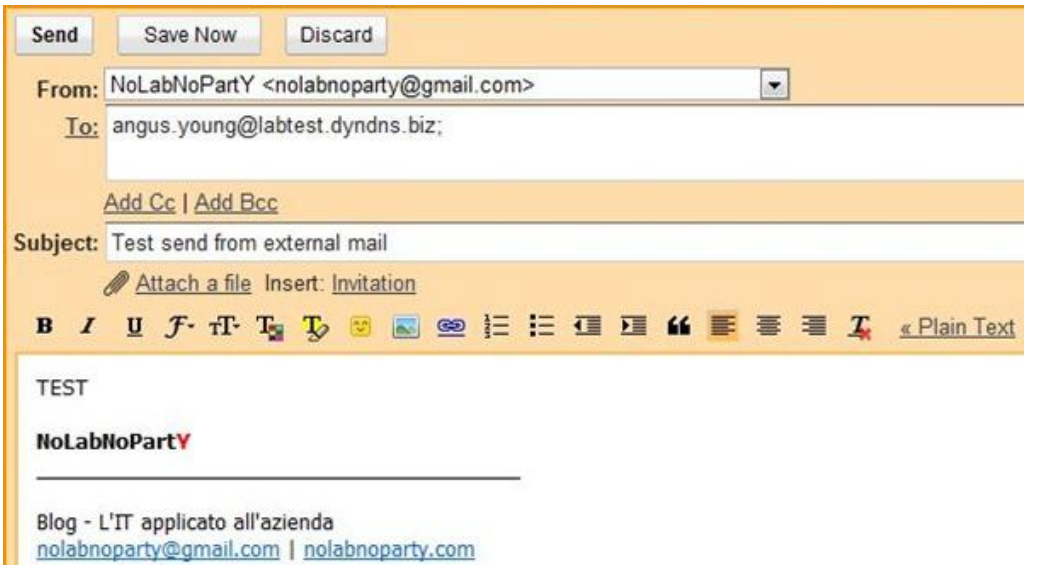


Spedire ora una email da *Zimbra* verso un account esterno (*Gmail* ad esempio) per verificare se la posta verso l'esterno funziona .



Accedendo all'account utilizzato per il test, se tutto è configurato correttamente, la posta viene recapitata.

Verificato che la spedizione verso l'esterno è operativa, spedire una email da un account esterno (*Gmail* ad esempio) verso *Zimbra* per verificare se la posta per l'interno funziona .



Se la configurazione è corretta, dopo qualche secondo l'email proveniente dall'esterno viene recapitata.

Il sistema di posta *Zimbra* è operativo e pronto all'utilizzo. Questa è una soluzione molto valida che può essere estesa anche per aziende di certe dimensioni, non solo per le PMI.

Configurare iNotes per l'accesso alla webmail di Lotus Domino tramite browser

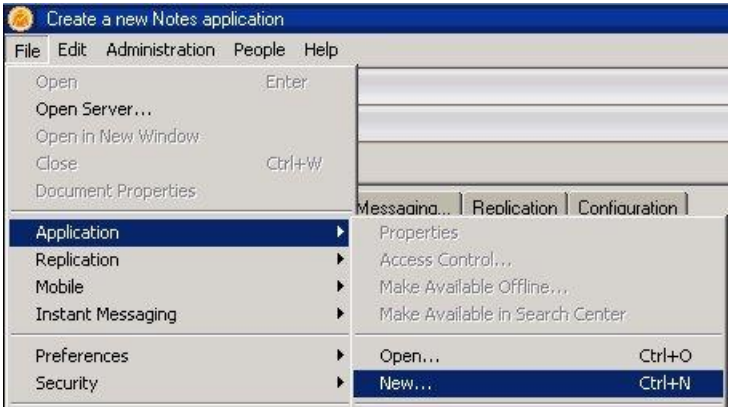
Accedere alla posta tramite browser è un requisito fondamentale per fornire agli utenti un **servizio funzionale e completo**.

Ovviamente tutti i maggiori software di posta offrono questa funzione che però **deve essere configurata**.

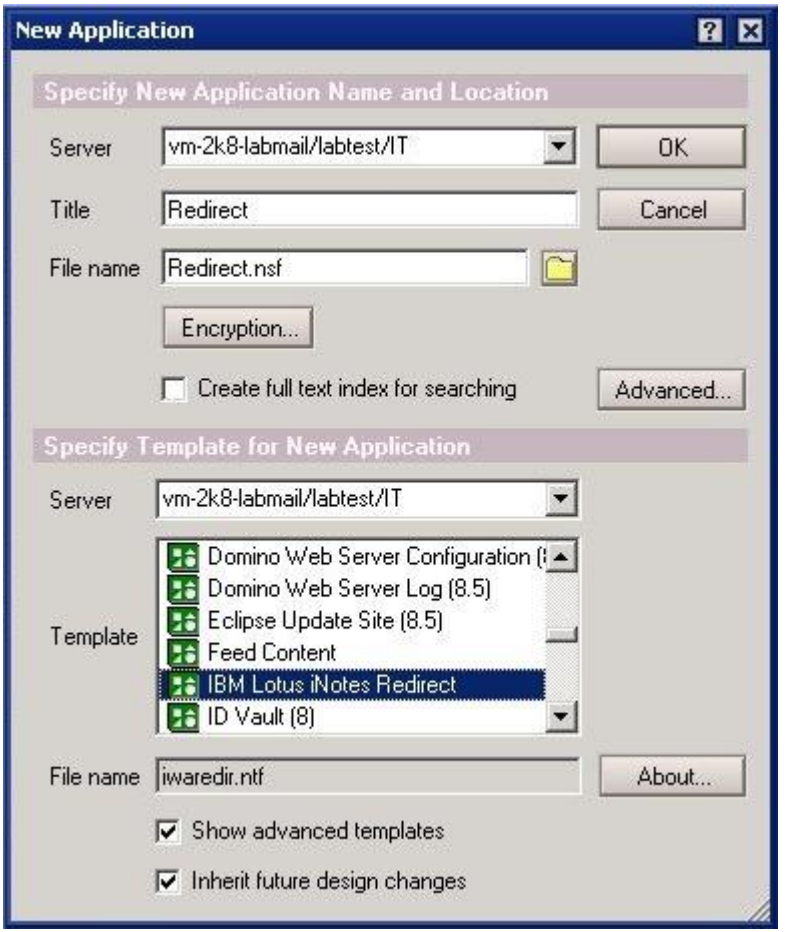
La procedura per attivare l'opzione in **Lotus Domino**, chiamata **iNotes**, comporta una serie di passaggi che permettono la configurazione ottimale del servizio a seconda delle esigenze.

Procedura

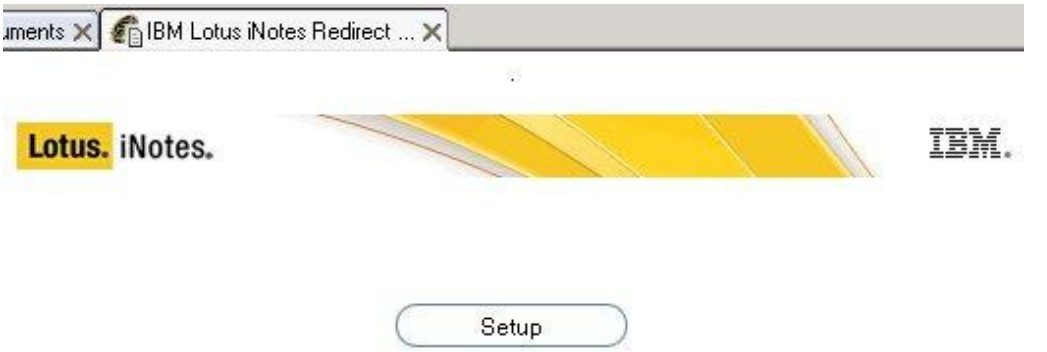
Da **Domino Administrator** cliccare su **File –> Application –> New**.



Selezionare il server su cui risiede l'applicazione ed impostare i campi **Title** e **File name**. Specificare il **Template** da utilizzare attivando l'opzione **Show advanced template** in modo da poter visualizzare e selezionare **IBM Lotus iNotes Redirect**.



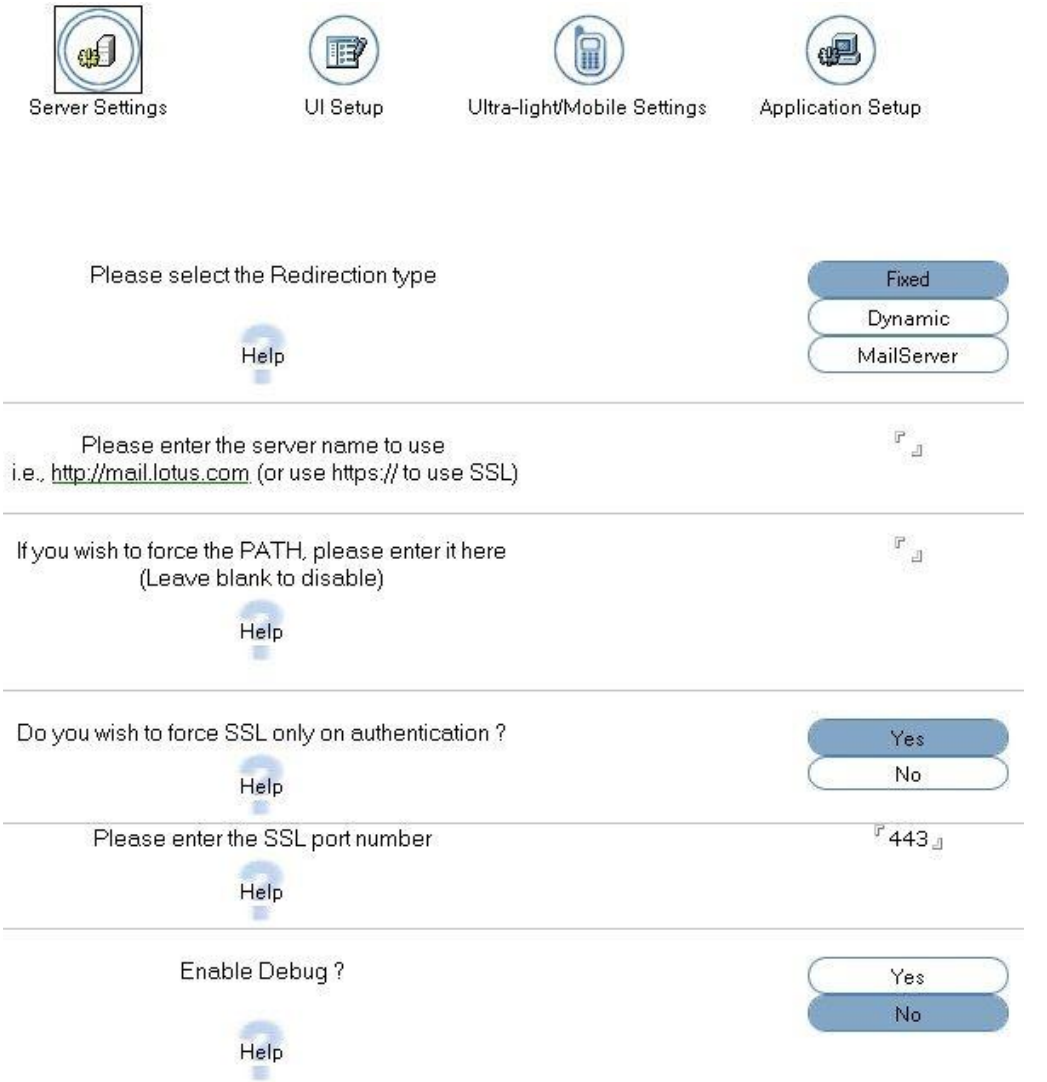
Cliccando su **OK** si apre la finestra per accedere alla **configurazione dell'applicazione** *IBM Lotus iNotes Redirect*. Cliccare su **Setup** per proseguire.



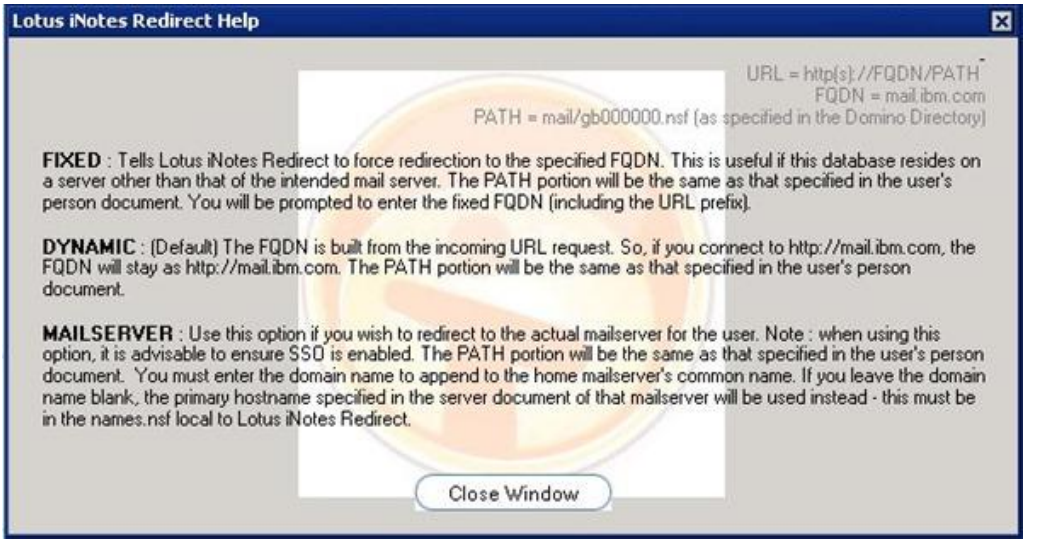
Vengono visualizzate i parametri di configurazione dell'applicazione. **Cliccare sulla varie voci** per accedere alla configurazione.

Server Settings. In questa schermata vengono impostati i parametri del server. I parametri dipendono dalla specifica esigenza e struttura della rete. **Impostare l'utilizzo SSL** al fine di aumentare la sicurezza del sistema.

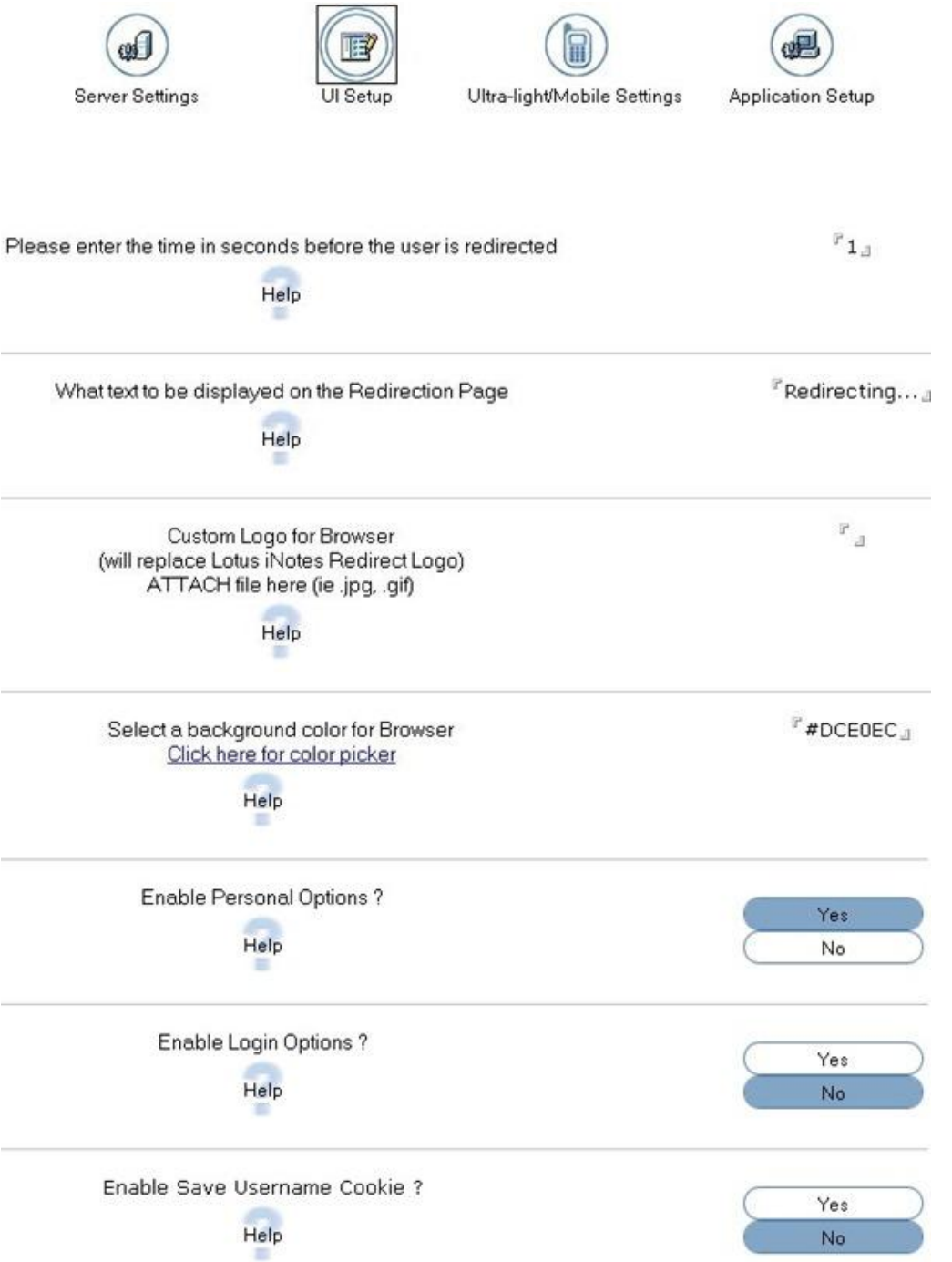
Cliccando su Help vengono spiegate le funzionalità delle varie opzioni.



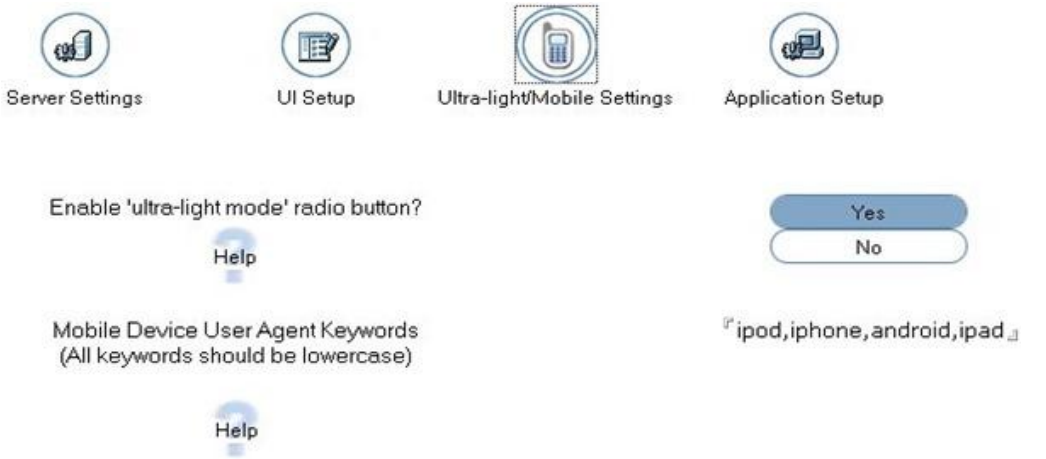
Per stabilire quale **Redirection Type** utilizzare ad esempio, l'**Help** illustra chiaramente le diverse funzionalità.



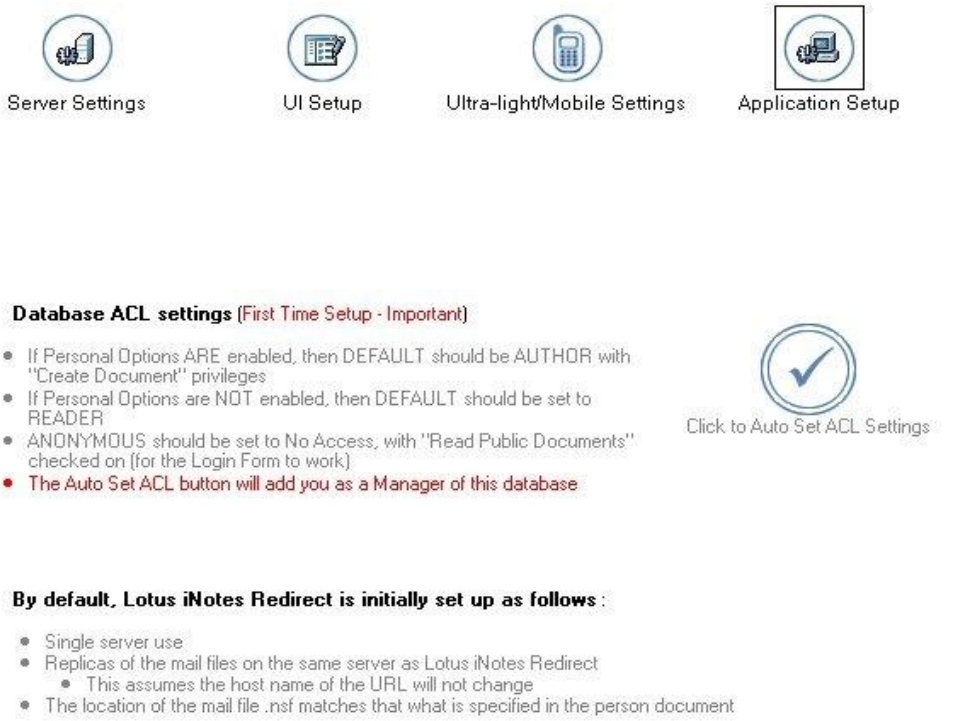
UI Setup. Le impostazioni sono piuttosto intuitive. Una configurazione tipica prevede l'impostazione dei campi come illustrato in figura. Anche qui bisogna tenere presente la struttura di rete si cui si lavora.


Server Settings
UI Setup
Ultra-light/Mobile Settings
Application Setup
Please enter the time in seconds before the user is redirected
1
Help
What text to be displayed on the Redirection Page
Redirecting...
Help
Custom Logo for Browser
(will replace Lotus iNotes Redirect Logo)
ATTACH file here (ie .jpg, .gif)
Help
Select a background color for Browser
Click here for color picker
#DCE0EC
Help
Enable Personal Options ?
Yes
No
Help
Enable Login Options ?
Yes
No
Help
Enable Save Username Cookie ?
Yes
No
Help

Ultra-light/Mobile Settings. Lasciare le impostazioni di **default**.



Application Setup. Qui bisogna semplicemente cliccare sul bottone **Click to Auto Set ACL Settings**.



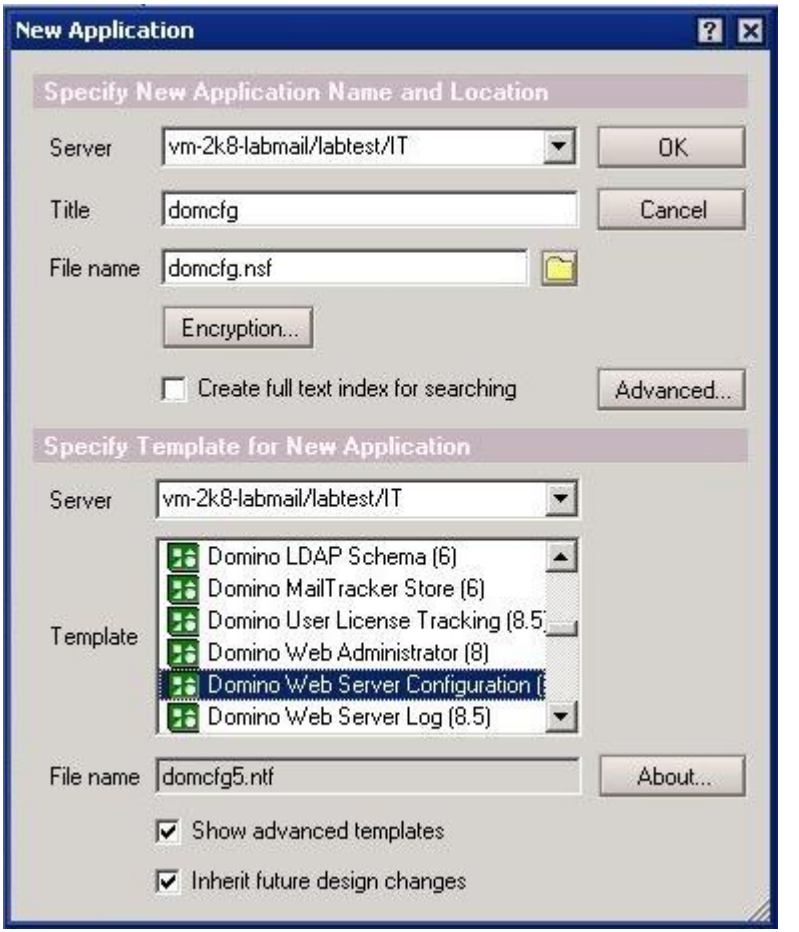
Viene visualizzata la seguente finestra. Click su **OK** per continuare.

Terminata la configurazione cliccare sul bottone **Save & Exit** per salvare le impostazioni appena effettuate.

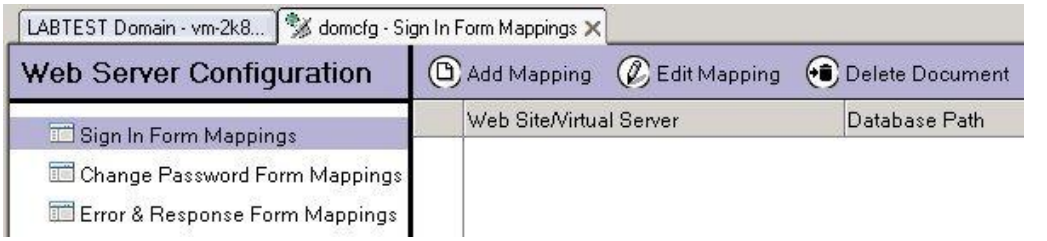
Sempre da **Domino Administrator** cliccare su **File –> Application –> New**. Impostare i seguenti parametri:

Title: ***domcfg***
File name: ***domcfg.nsf***

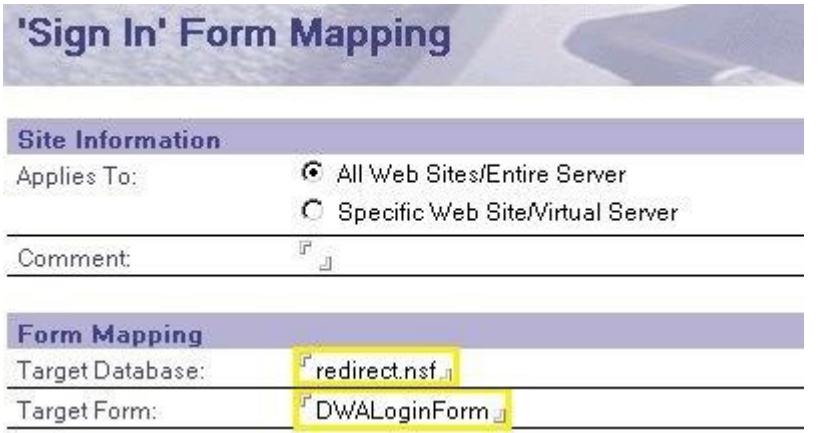
Selezionare come **Template** la voce **Domino Web Server Configuration** e cliccare su **OK**.



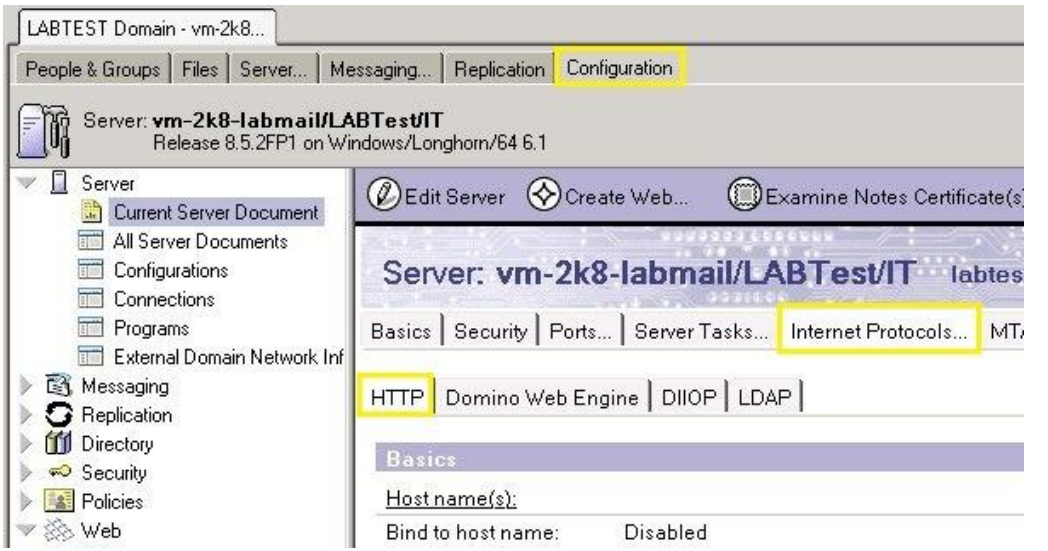
Si apre la **finestra di configurazione** dell'applicazione *Web Server Configuration*. Cliccare sulla voce **Add Mapping**.



Impostare dei campi **Target Database** e **Target Form** con i valori riportati in figura. Cliccare successivamente sulla voce **Save & Close** per salvare le impostazioni.

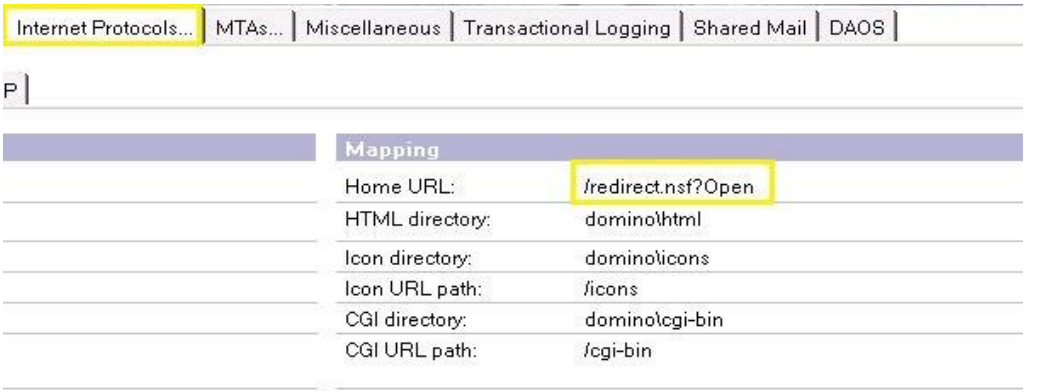


Da *Dominio Administrator* selezionare il pannello **Configuration**. Dalla schermata di sinistra cliccare su **Server –> Current Server Document** e selezionare a destra la voce **Internet Protocols-> HTTP**.



Nel campo **Home URL** impostare il parametro:

Home URL: ***/redirect.nsf?Open***

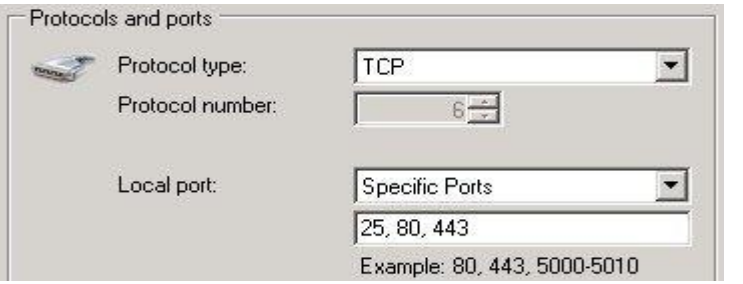


Cliccare sulla voce **Save & Close** per salvare le impostazioni. Per attivare le modifiche, dalla *server console* **riavviare il servizio http** tramite il comando:

```
# tell http restart
```

Impostazione del firewall in Windows

Per funzionare correttamente, il servizio richiede che le **porte TCP 25, 80, 443** siano aperte nel **firewall**.



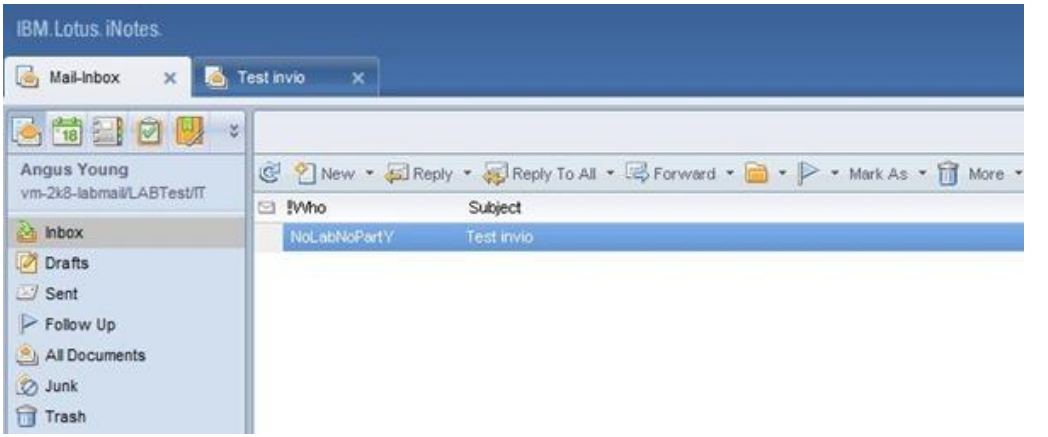
Testare la funzionalità

Configurato il server, non rimane che testare il funzionamento di quanto configurato.

Dal browser **digitare l'url** per accedere al server di posta. Il sistema richiede di inserire **username e password** per l'autenticazione.

Cliccato **OK**, il sistema effettua il **Redirecting** sul database dell'utente specificato.

Si accedete alla schermata della **webmail** di *Lotus Notes* che offre tutte le funzionalità per gestire al meglio le proprie email.



Abilitare la comunicazione in SSL

Per aumentare la sicurezza è consigliabile utilizzare il servizio **webmail in https** per tenere lontano possibili curiosi.

<u>Certificato SSL</u>

Da *Domino Administrator* creare un **certificato SSL** tramite l'applicazione **Server Certificate Admin**.

<u>Impostare il server</u>

Accedere al pannello **Configuration** e selezionare la voce **Server –> Current Server Document**. Cliccare sula voce **Ports –> Internet Ports**. Effettuare le seguenti impostazioni:

SSL Key file name: ***filename_certificate.kyr***
TCP/IP port status: ***Redirect to SSL***
SSL port status: ***Enabled***

Notes Network Ports | Internet Ports... | Proxies |

SSL settings

SSL key file name:	vm-2k8-labmail.kyr
SSL protocol version (for use with all protocols except HTTP):	Negotiated
Accept SSL site certificates:	Yes No
Accept expired SSL certificates:	Yes No
SSL ciphers: Modify	RC4 encryption with 128-bit key and MD5 MAC RC4 encryption with 128-bit key and SHA-1 MAC Triple DES encryption with 168-bit key and SHA-1 MAC DES encryption with 56-bit key and SHA-1 MAC RC4 encryption with 40-bit key and MD5 MAC
Enable SSL V2: (SSL V3 is always enabled)	Yes

Web | Directory | Mail | DIIOP | Remote Debug

Web
(HTTP/HTTPS)

TCP/IP port number:	80
TCP/IP port status:	Enabled
Enforce server access settings:	No
Authentication options:	
Name & password:	Yes
Anonymous:	Yes
SSL port number:	443
SSL port status:	Enabled

Select Keywords

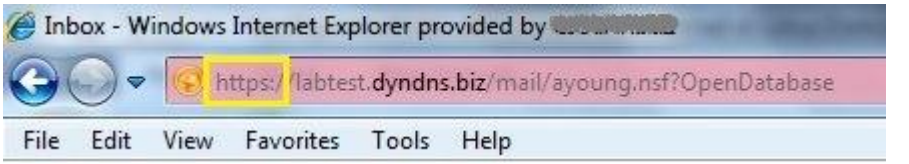
Keywords

Enabled
Disabled
Redirect to SSL

OK
Cancel

Cliccare su **Save & Close** e riavviare il servizio **http**.

Accedendo alla webmail, la comunicazione viene adesso **effettuata in SSL** come riporta il browser indicando il suffisso http**s**.



Il servizio webmail è ora configurato, operativo garantendo una certa sicurezza per le comunicazioni tramite il protocollo SSL.

Aggiungere automaticamente il disclaimer alle email in Lotus Domino

È ormai una consuetudine o forse più una moda **inserire in fondo alle e-mail** inviate un disclaimer con una frase in una o più lingue tipo:

"This e-mail and any attachments is a confidential correspondence intended only for use of the individual or entity named above. If you are not the intended recipient or the agent responsible for delivering the message …"

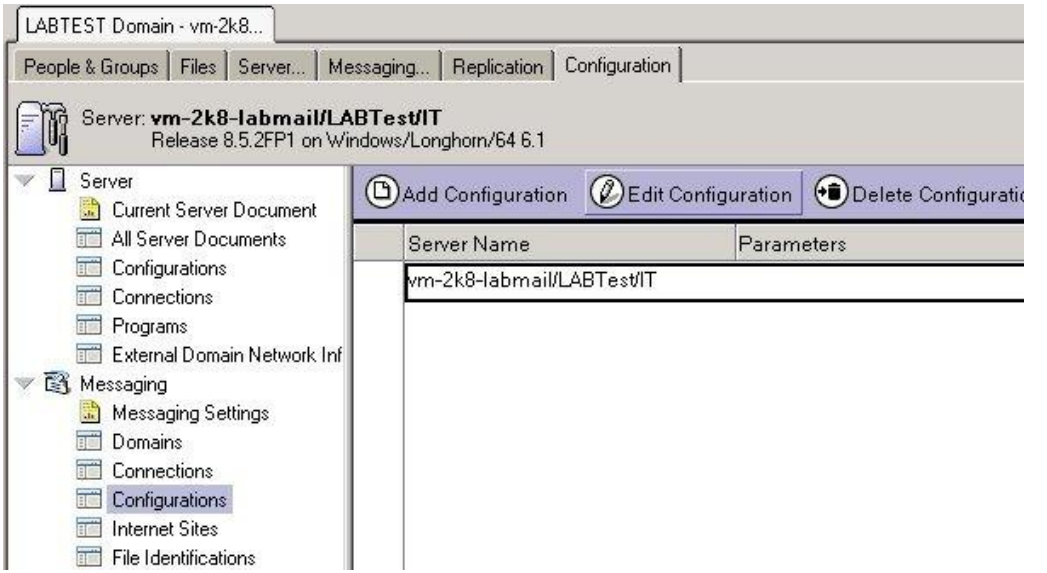
Quanto **valore giuridico** abbiano poi certi *disclaimer* è una domanda che spesso ci si pone.

Poichè il management spesso richiede che il *disclaimer* sia presente in calce alle email, è conveniente che sia il **sistema di posta utilizzato** ad inserire automaticamente nelle email in uscita (internamente non ha molto senso!) una frase che svolge la funzione di *disclaimer*.

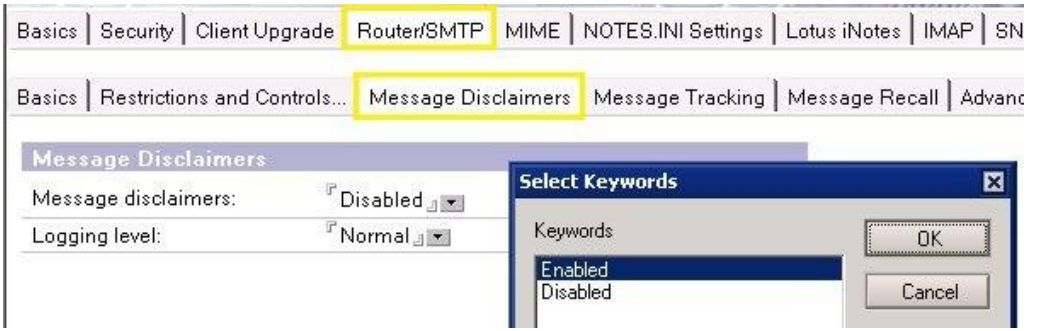
Procedura

L'inserimento automatico del *disclaimer* richiede alcuni passaggi completamente gestiti dal *Domino Administrator*. Accedere quindi al **Domino Administrator ed effettuare il login**.

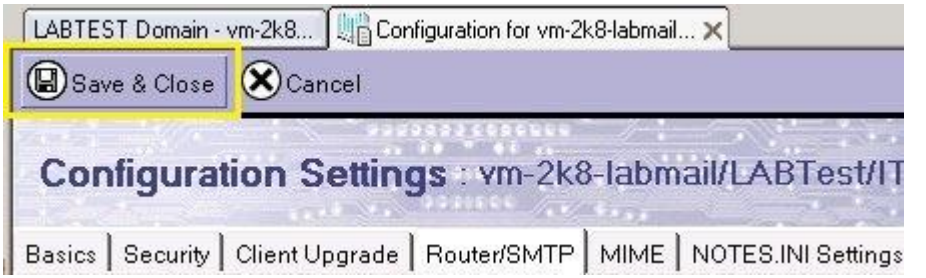
Selezionare la pagina **Configuration** per accedere alla sezione richiesta. Selezionare nella parte sinistra **Messaging –> Configurations** e cliccare sul bottone **Edit Configuration**.



Accedere alla sezione **Router/SMTP –> Message Disclaimer**. Impostare il campo **Message disclaimers** come **Enabled**.

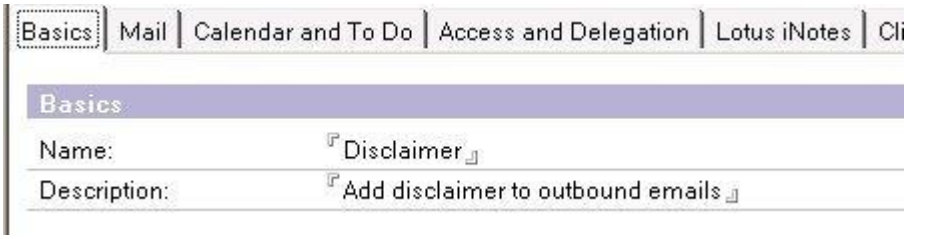


Cliccare su **Save & Close** per salvare la configurazione appena impostata.

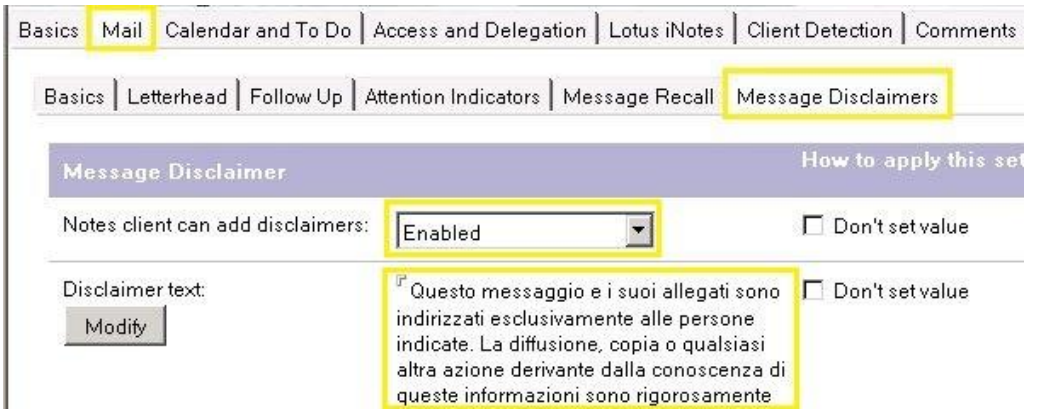


Accedere alla pagina **People & Groups** e selezionare **Settings** nella parte sinistra. Cliccare sul bottone **Add Settings** e selezionare l'opzione **Mail**.

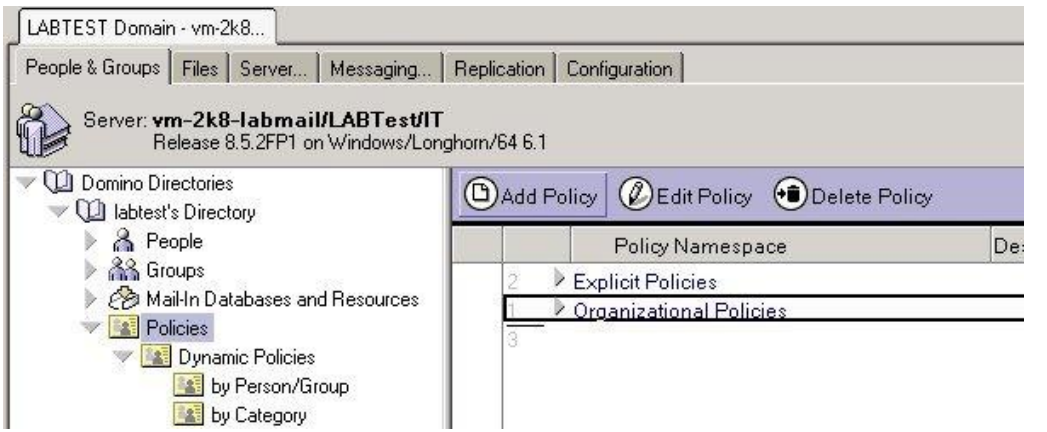
Assegnare nel campo **Name** un nome significativo (es. Disclaimer) per identificare il parametro e nel campo **Description** una descrizione operativa della configurazione.



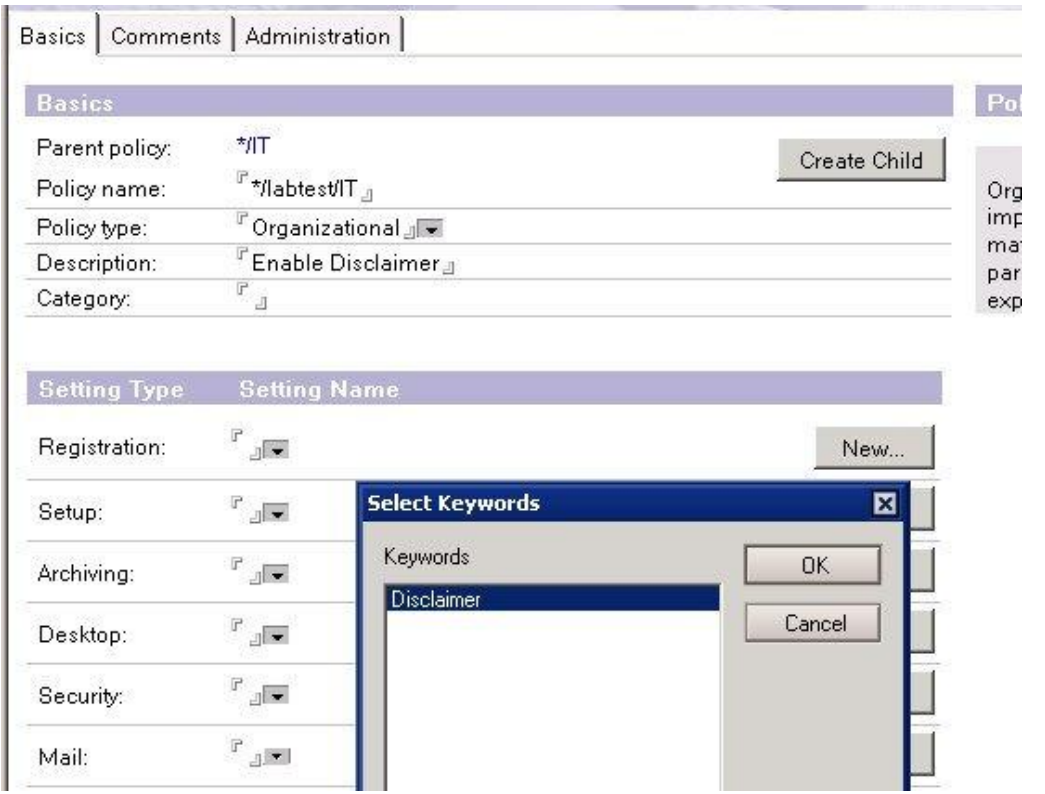
Selezionare successivamente **Mail –> Message Disclaimers** per impostare il tipo di messaggio che deve essere allegato alle email. **Abilitare** (**Enable**) il campo **Notes client can add disclaimers** ed inserire in **Disclaimer text** il testo che si vuole visualizzare. Cliccare infine su **Save & Close** per salvare la configurazione impostata.



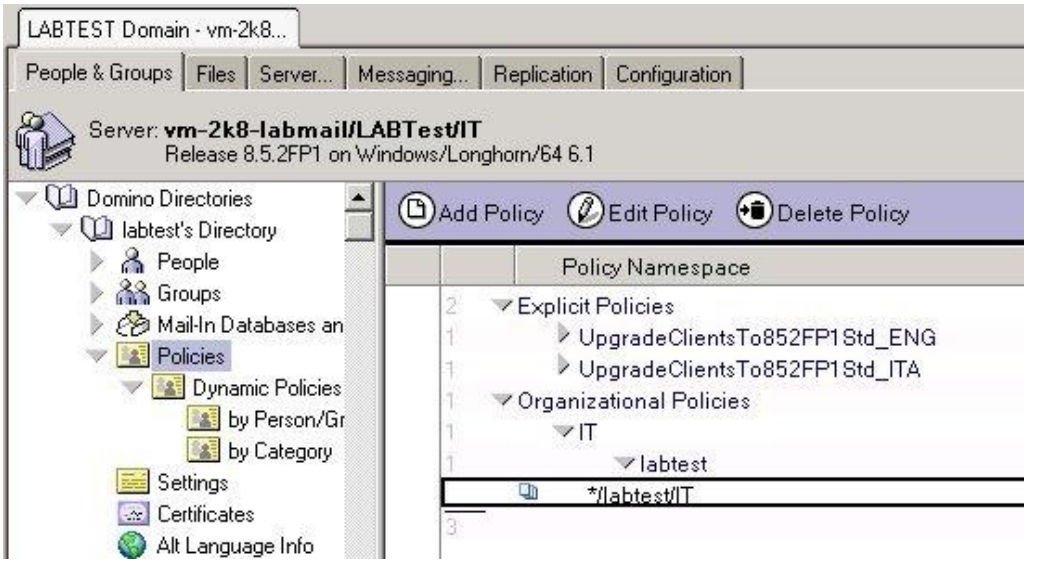
A questo punto non rimane che **creare una policy** per abilitare nel dominio la funzionalità del *disclaimer*. Dalla pagine **People & Group** selezionare **Policies** e cliccare sul bottone **Add Policy**.



Assegnare la **Policy name** specificando il dominio del sistema, una **Policy type** di tipo **Organizational** e una **Description**. Nei **Setting Type** cliccare sulla freccia in corrispondenza del campo **Mail** e selezionare dalla finestra che appare la configurazione **Disclaimer** precedentemente impostata. Cliccare su **Save & Close** per salvare la policy.



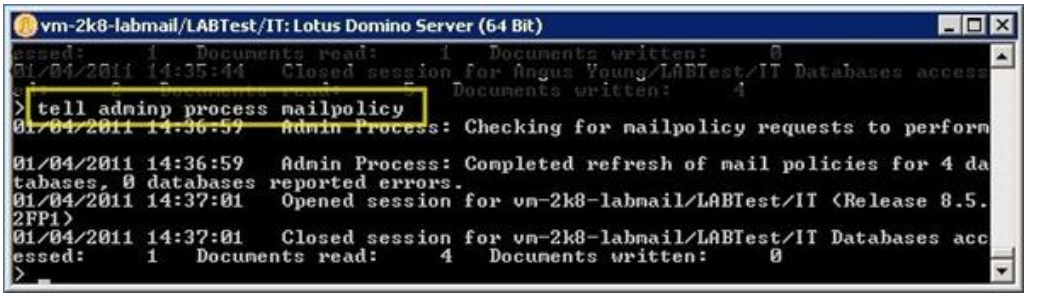
Nella parte destra della schermata sono **visualizzate le policy** applicate al dominio.



A questo punto la **configurazione è conclusa** e non rimane che **abilitarla**.

Per abilitare immediatamente la policy nel server utilizzare dalla console il comando:

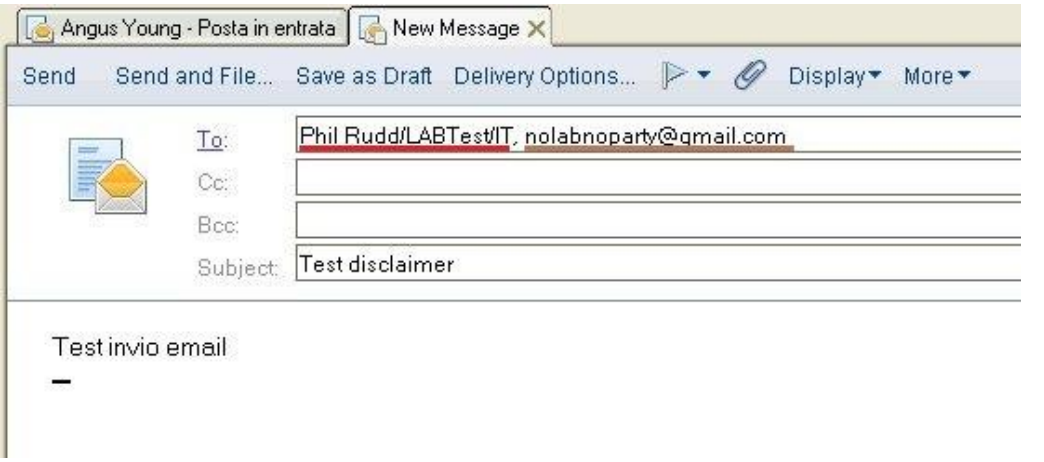
```
tell adminp process mailpolicy
```



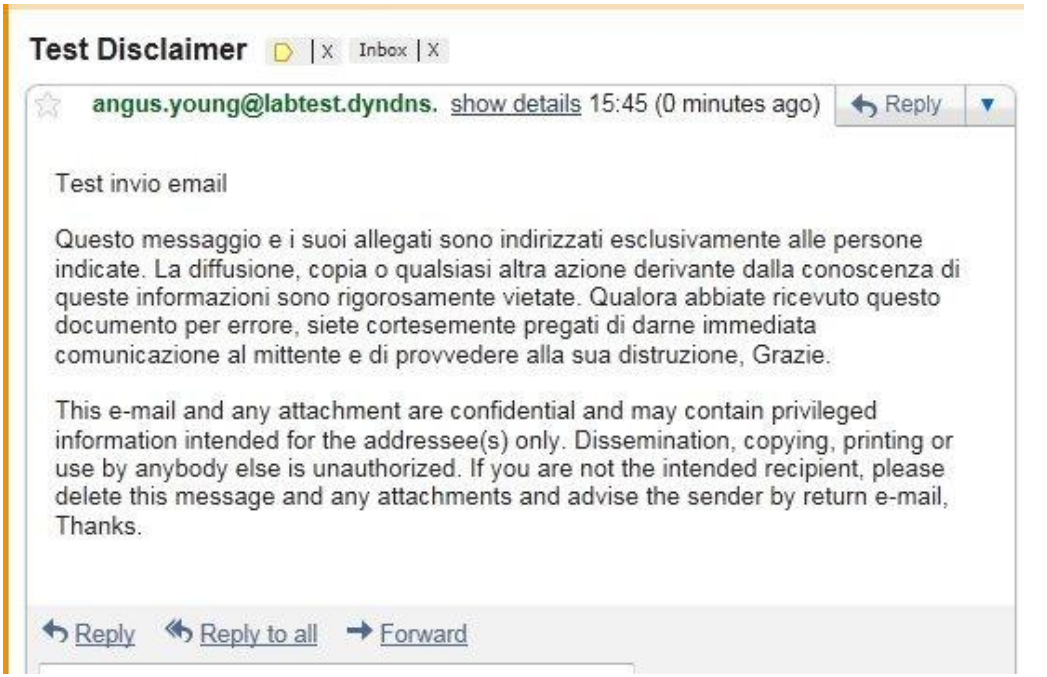
Nel caso la policy non risultasse operativa, riavviare il server. La procedura è conclusa e pronta per la **fase di test**.

Testare la configurazione

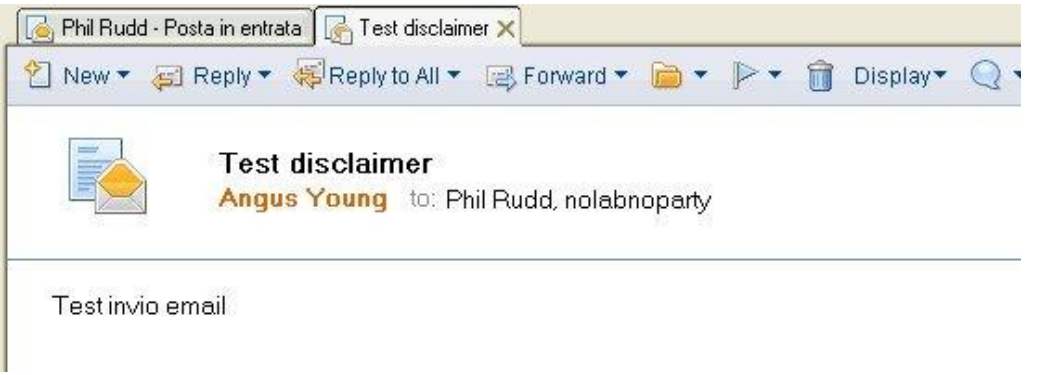
Dal **client di posta inviare una email** ad un **indirizzo interno** della rete (sottolineato in rosso nella figura) e una ad un **indirizzo esterno** (sottolineato in verde) per verificare il comportamento del sistema.



L'email ricevuta nella casella esterna riporta il **disclaimer correttamente**.



L'email ricevuta nella casella interna invece, **non presenta il disclaimer**. E' esattamente il comportamento voluto con questa configurazione.



Il sistema provvederà quindi ad **inserire automaticamente** il *disclaimer* in tutte le email **destinate all'esterno della rete**, quindi all'azienda, mentre per le comunicazioni interne le email non presenteranno nessuna dicitura.

Configurare ID Vault in Lotus Domino 8.5.3

L'ID Vault in *Lotus Domino* è un **repository degli "users ID Files"** presenti nel sistema che permette una **gestione più semplice ed efficiente** delle **password e degli ID** stessi.

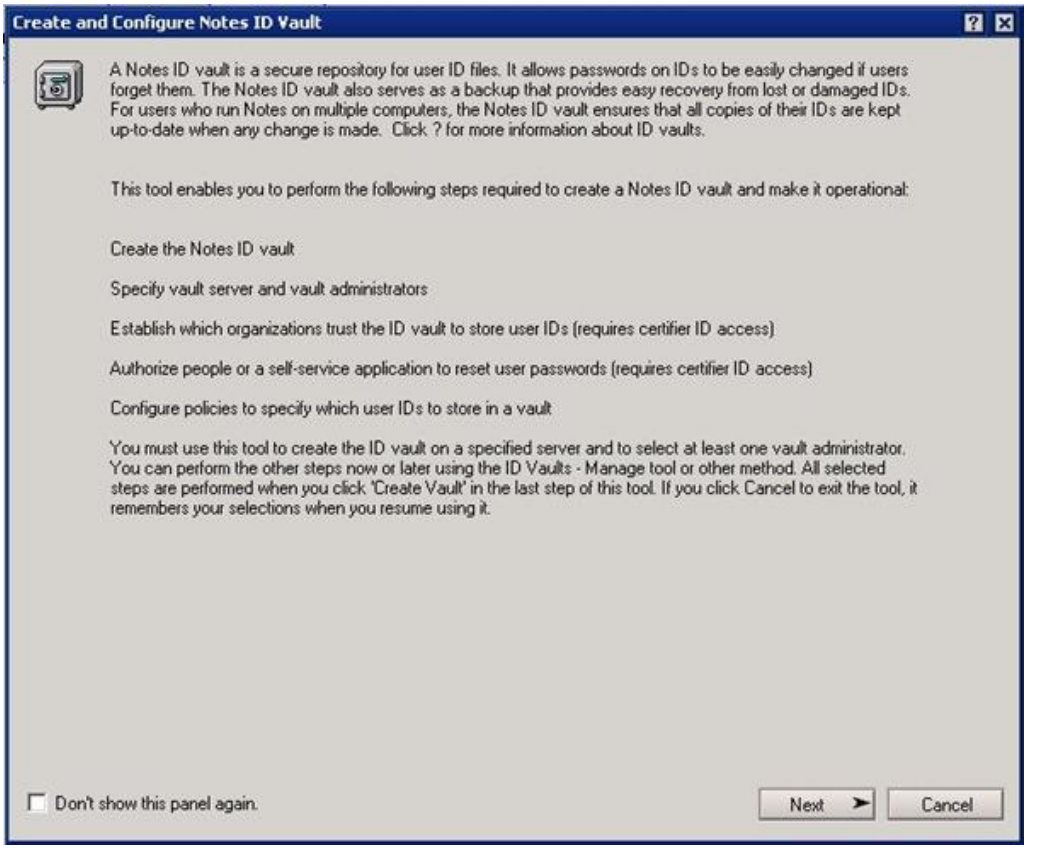
Ogni variazione effettuata è direttamente salvata nel repository permettendo di avere le copie degli ID sempre aggiornate.

La configurazione dell'ID Vault non è complicata ma richiede un'**attenta pianificazione** supportata da una buona fase di test.

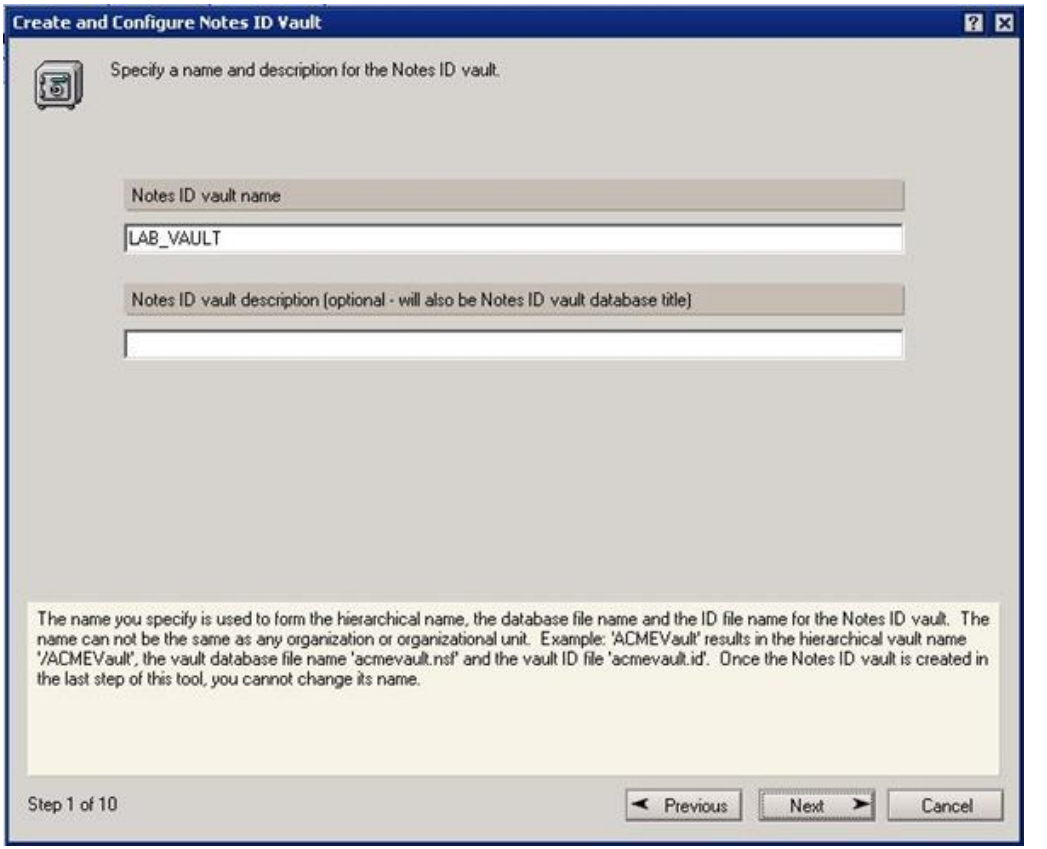
Procedura

Aprire **Domino Administrator**, selezionare **Configuration Tab –> Tools – > ID Vaults** e cliccare sula voce **Create**.

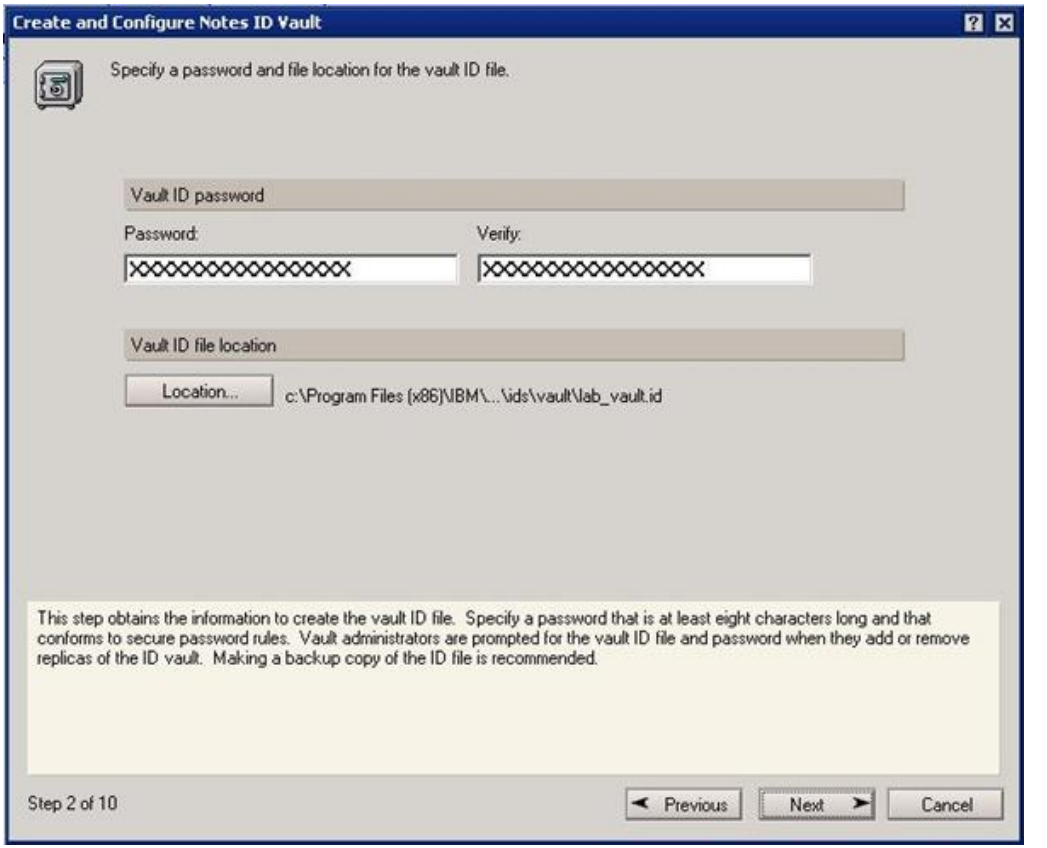
Si apre una pagina introduttiva. Cliccare su **Next** per proseguire.



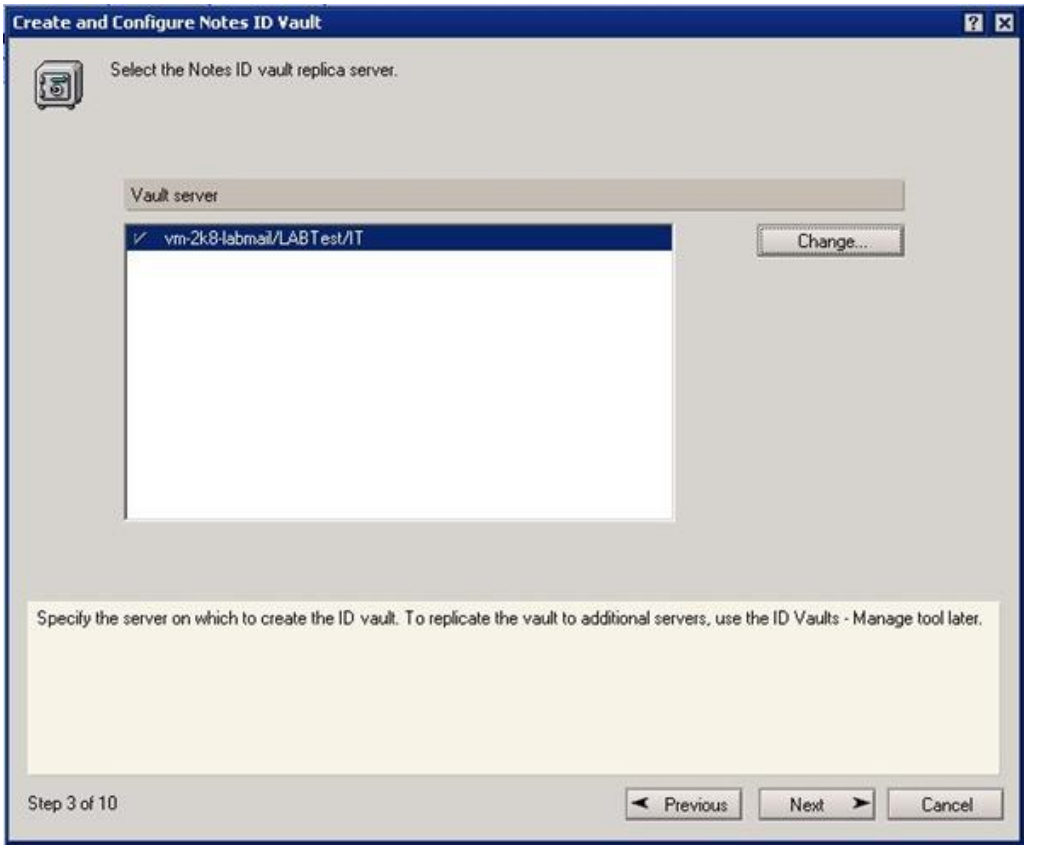
Assegnare un nome all'ID Vault che si sta creando compilando il campo **Notes ID vault name**. Cliccare su **Next**.



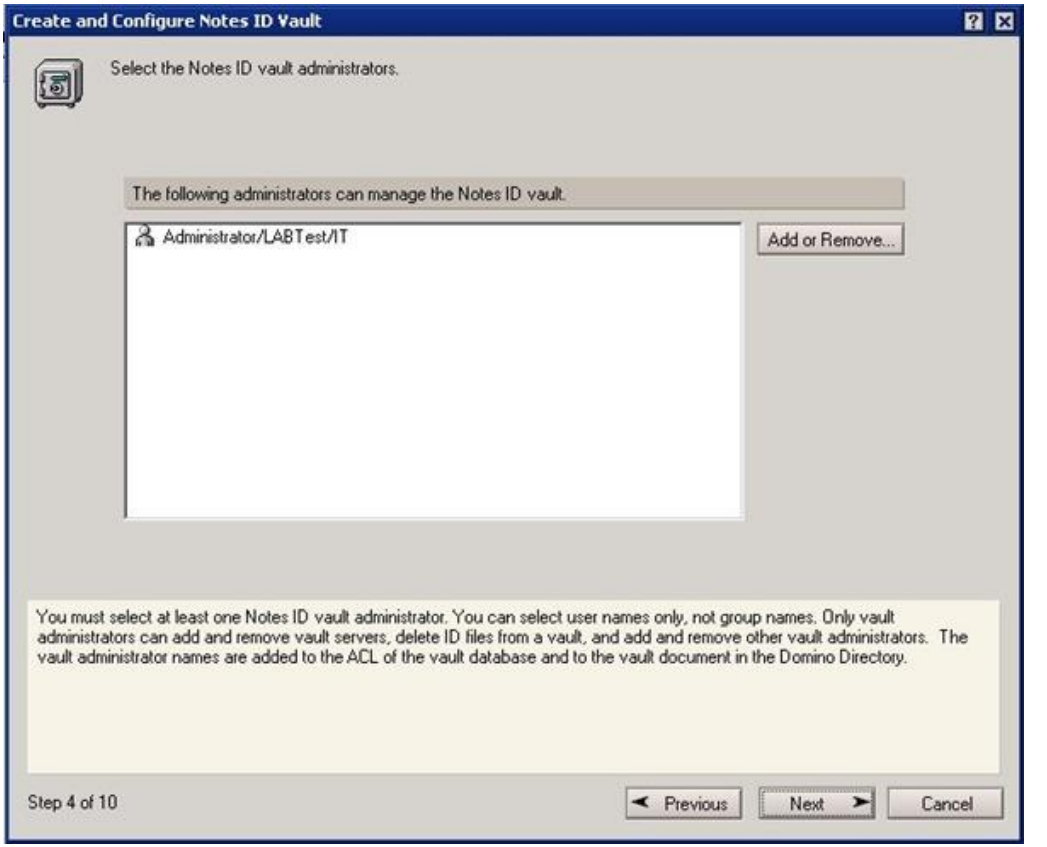
Specificare la **password e path** del *Vault ID file*. Come per l'ID del Certifier, del Server e dell'Administrator, copiare l'ID file del *Vault* e conservarlo in un posto sicuro nel caso venga accidentalmente cancellato dal server. Cliccare su **Next** per continuare.



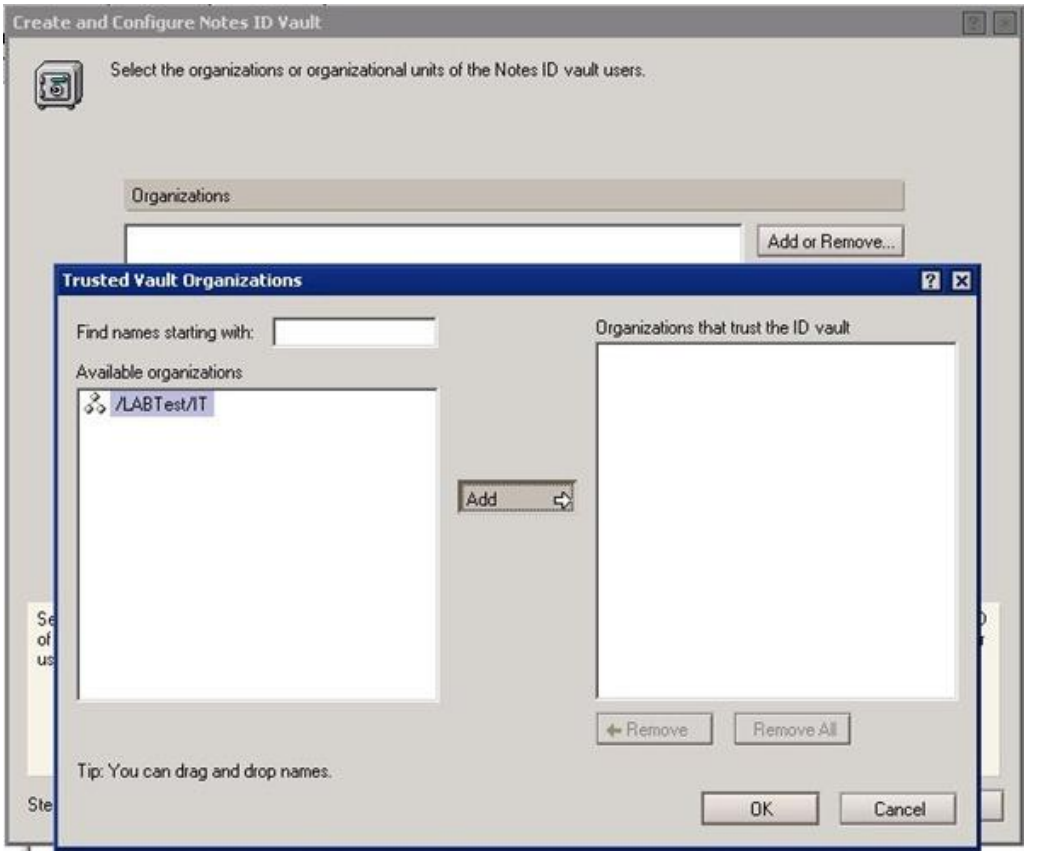
Specificare il server su cui creare l'ID Vault e cliccare su **Next**.



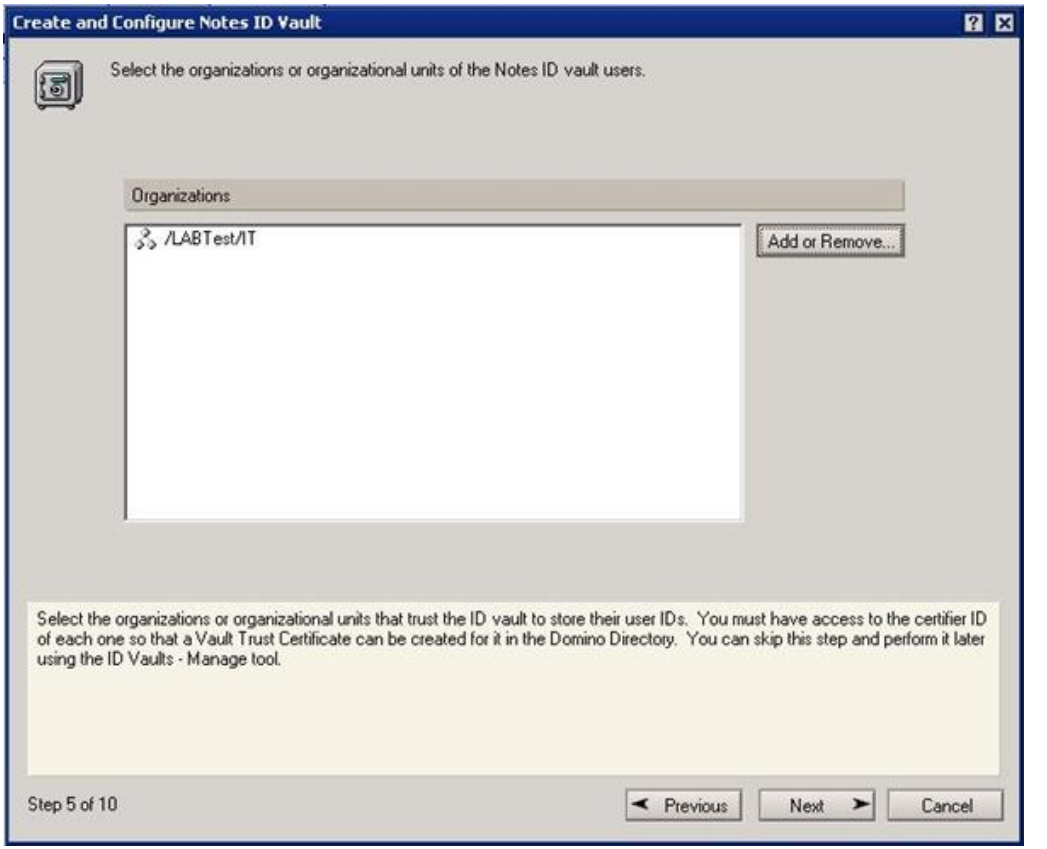
Assegnare gli amministratori del *Notes ID Vault* tramite il bottone **Add or Remove**. Cliccare su **Next** per proseguire.



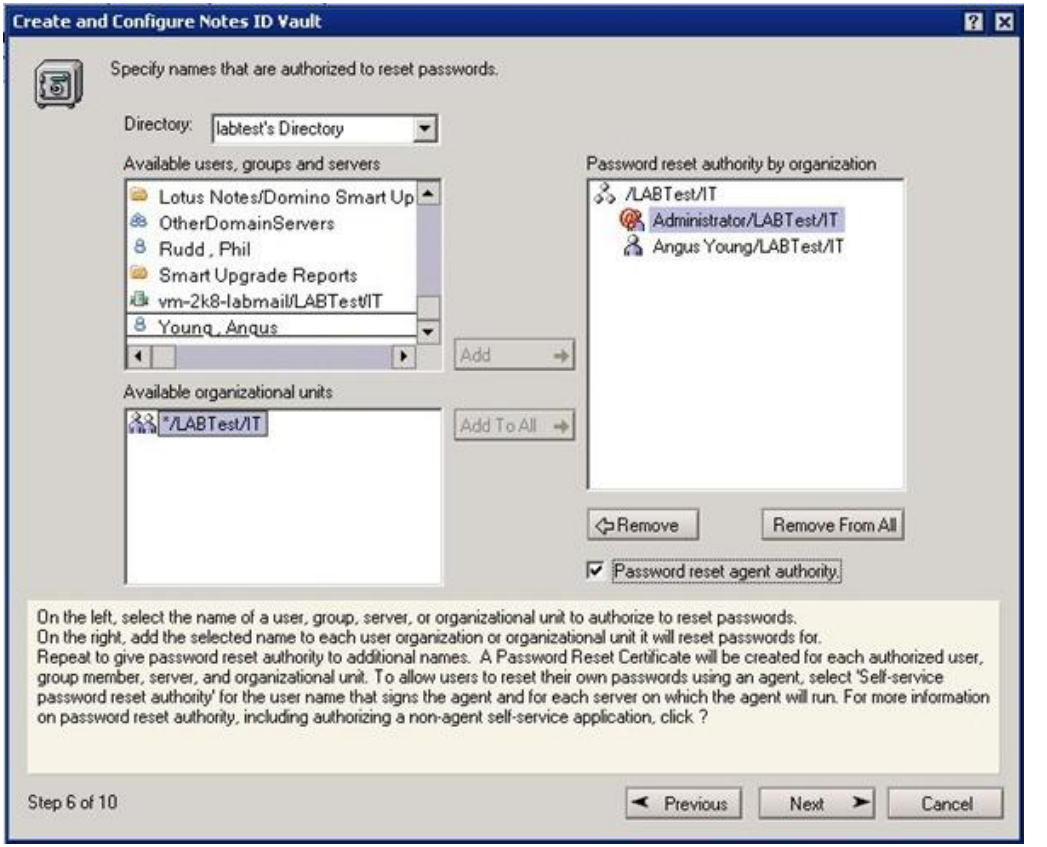
Cliccare sul bottone **Add or Remove**, selezionare le **Organizations** che saranno soggette al *Vault* e cliccare su **Add**.



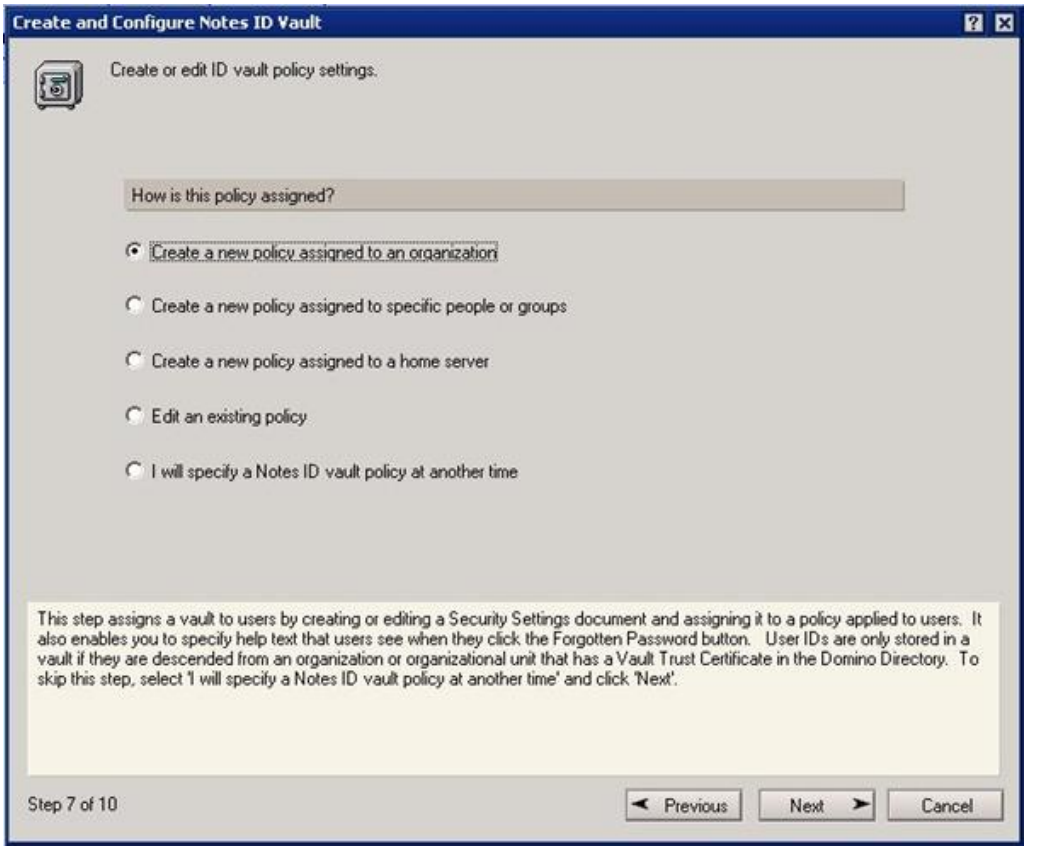
Indicare le ***Organizations*** **che si appoggeranno al Vault** (Trust) dove gli ID degli account saranno salvati.



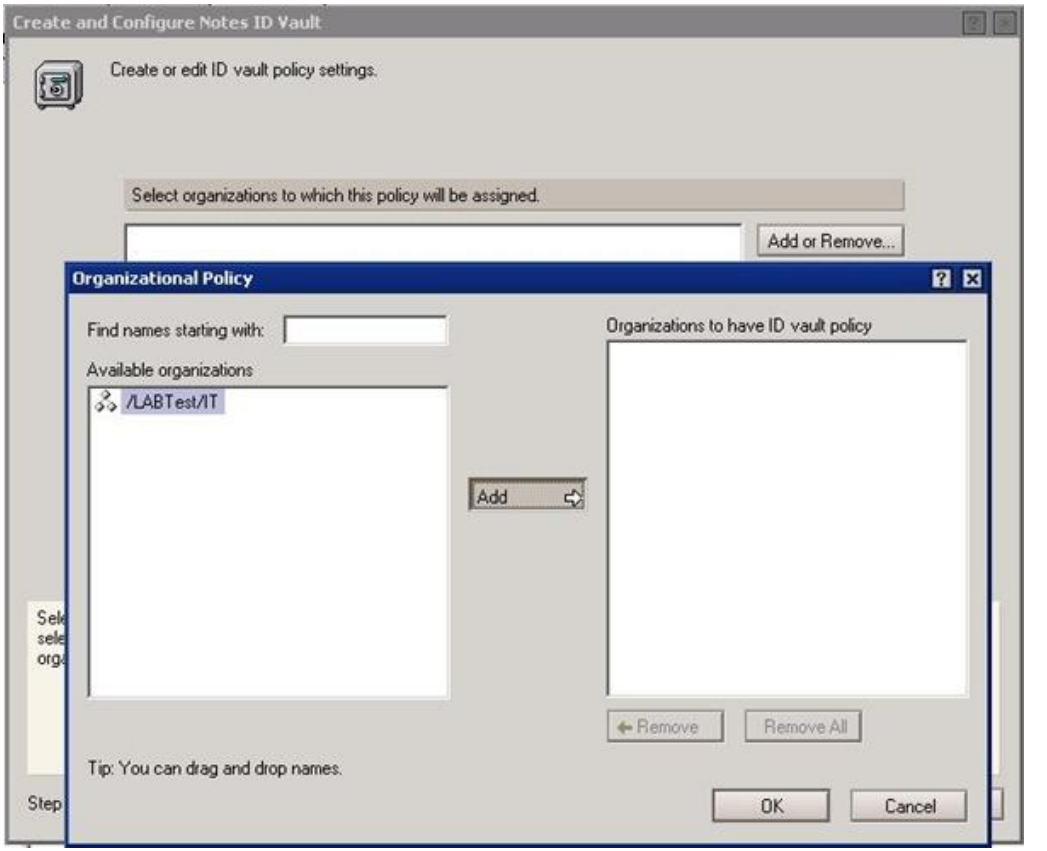
Specificare le **Password Reset Authority** indicando gli *User* delle *Organizational Units* presenti, cliccare successivamente sul bottone **Add**. E' inoltre possibile assegnare agli utenti indicati il diritto di **resettare la propria password** selezionando un determinato user e attivando l'opzione **Password reset agent authority**. Cliccare su **Next** per continuare.



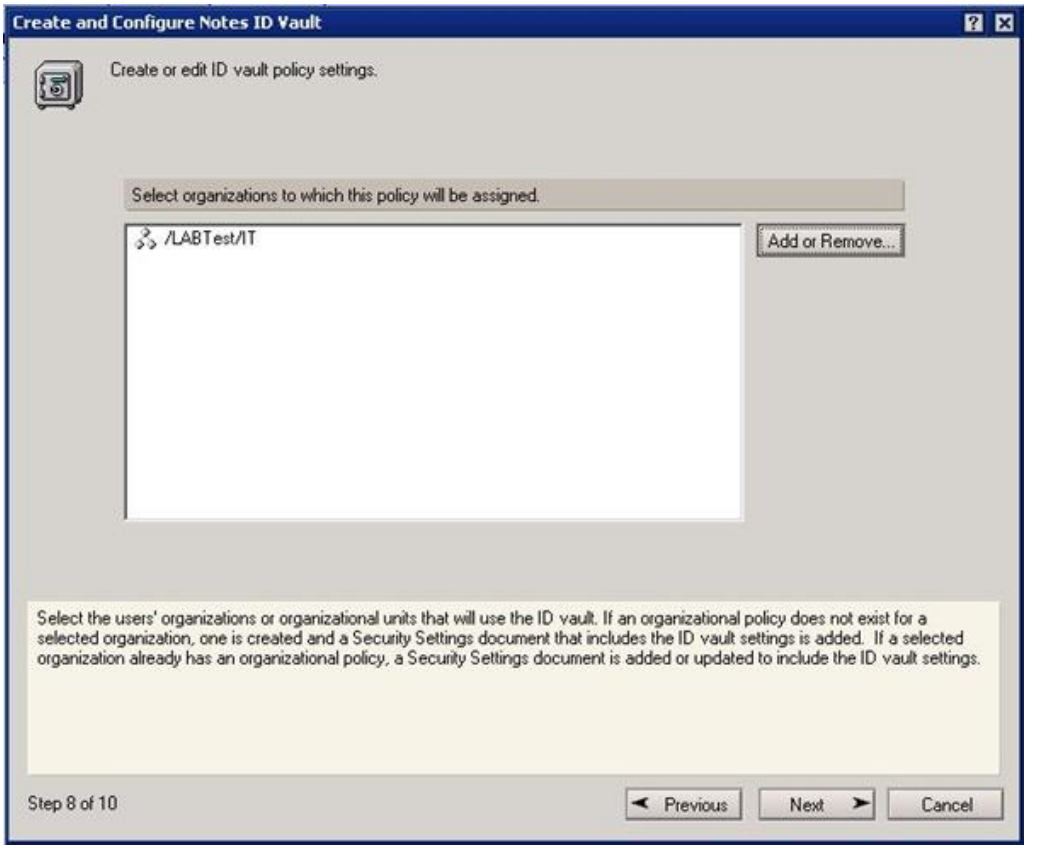
Selezionare l'opzione **Create a new policy assigned to an organization** per creare automaticamente la **policy che attiverà il Vault** alle *Trusted Organizations*. Cliccare su **Next**.



Selezionare le *Organizations* a cui si vuole **assegnare la policy**.

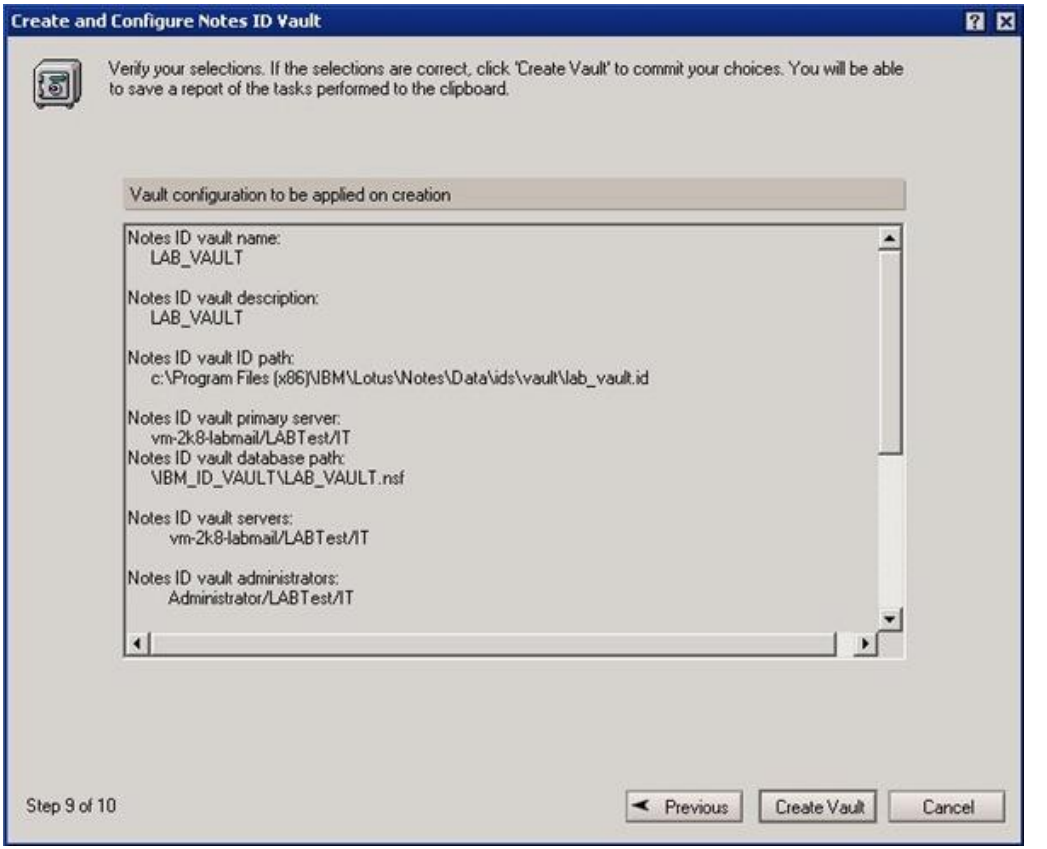


Tramite **Add or Remove**, selezionare le *Organizations* a cui **assegnare la policy**.

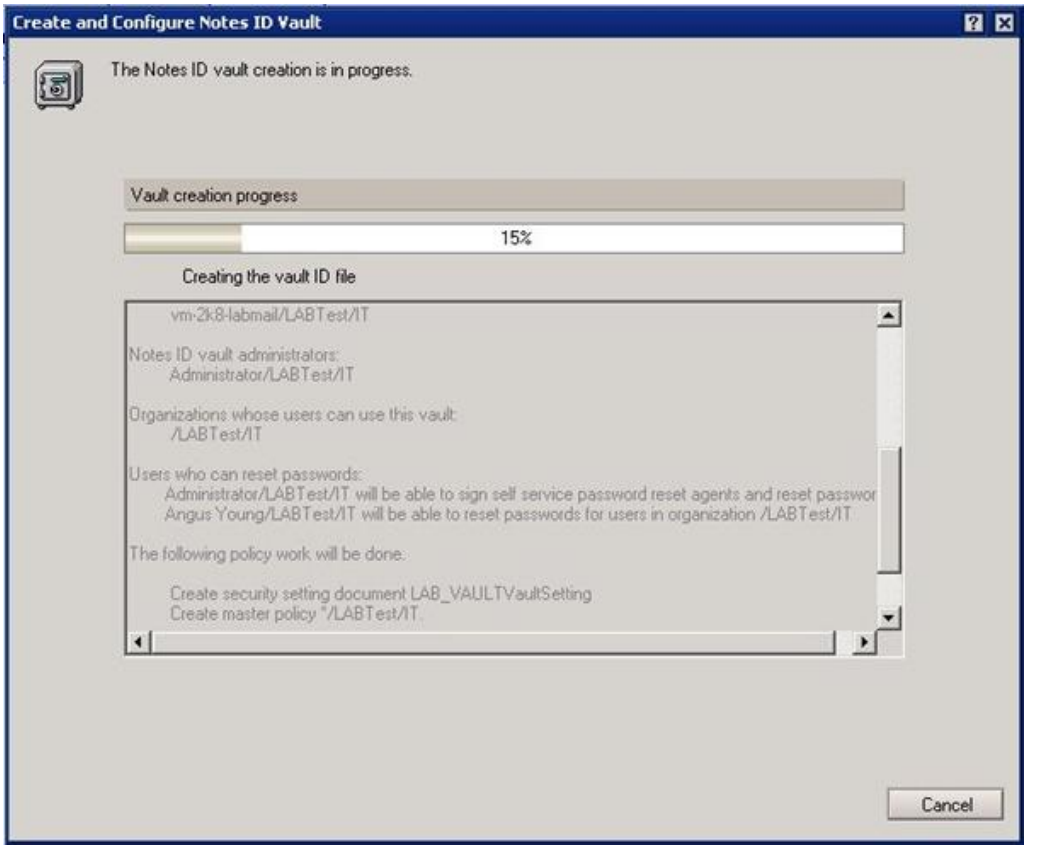


Specificare un testo in caso di dimenticanza della password.

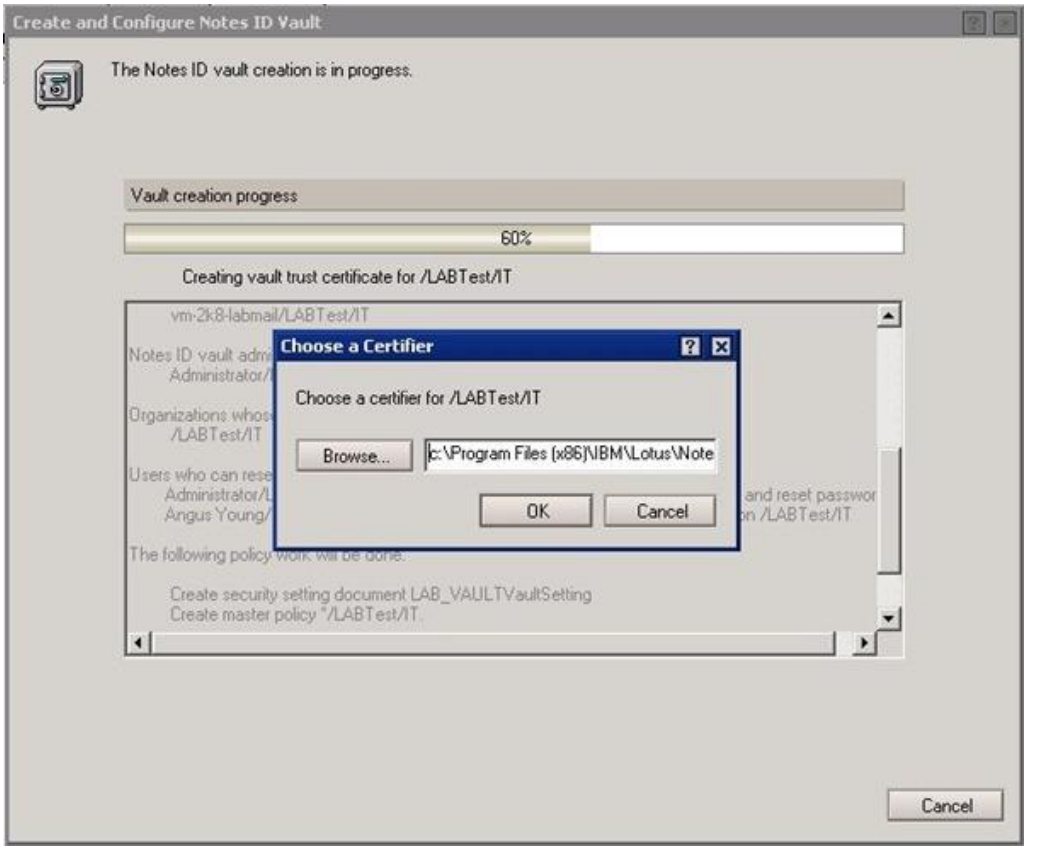
Viene presentata una **schermata riepilogativa** con le impostazioni specificate. Cliccare su **Create Vault** per procedere con l'installazione effettiva.



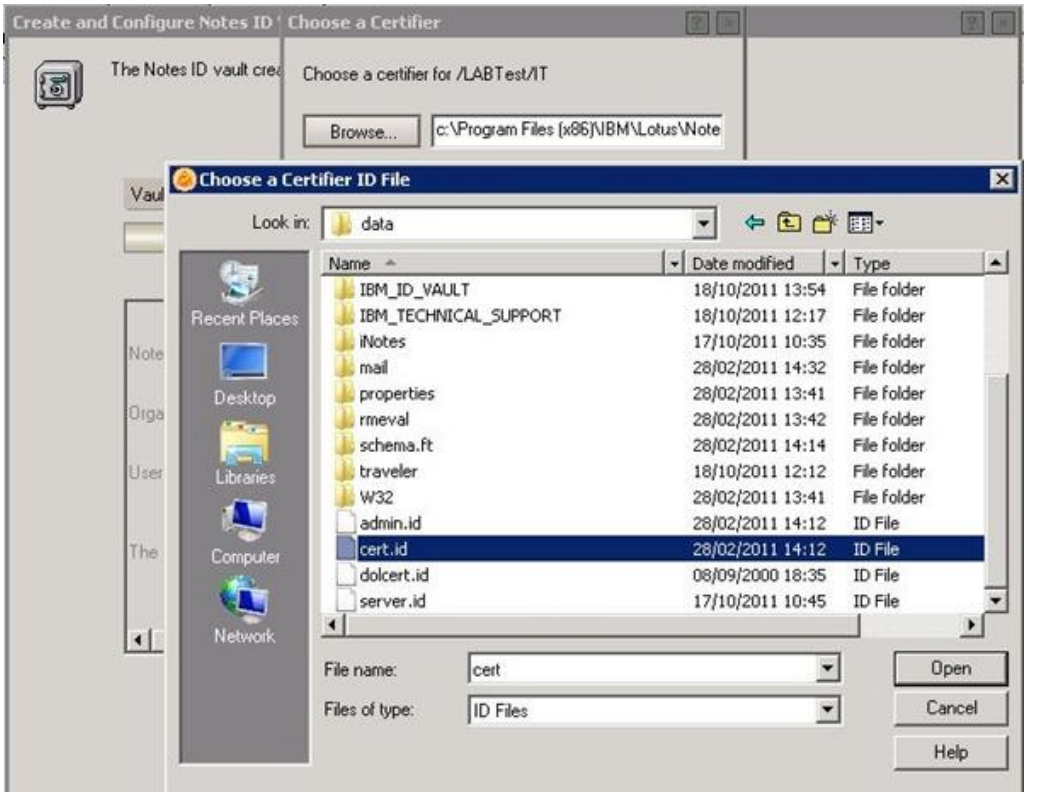
Viene mostrato lo **stato dell'installazione** tramite una schermata dedicata.



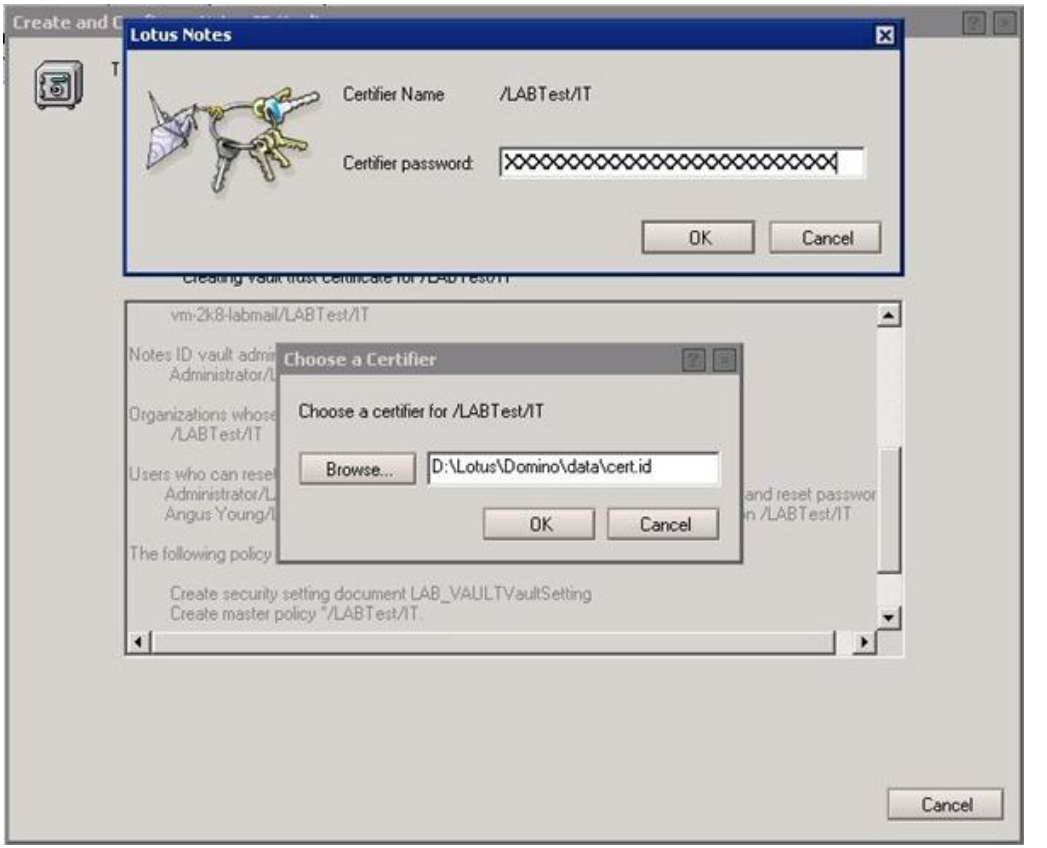
Durante l'installazione sono richieste le **credenziali del Certifier** per l'Organization soggetta al *Vault*. Cliccare sul bottone **Browse** per impostare la location del *cert.id*.



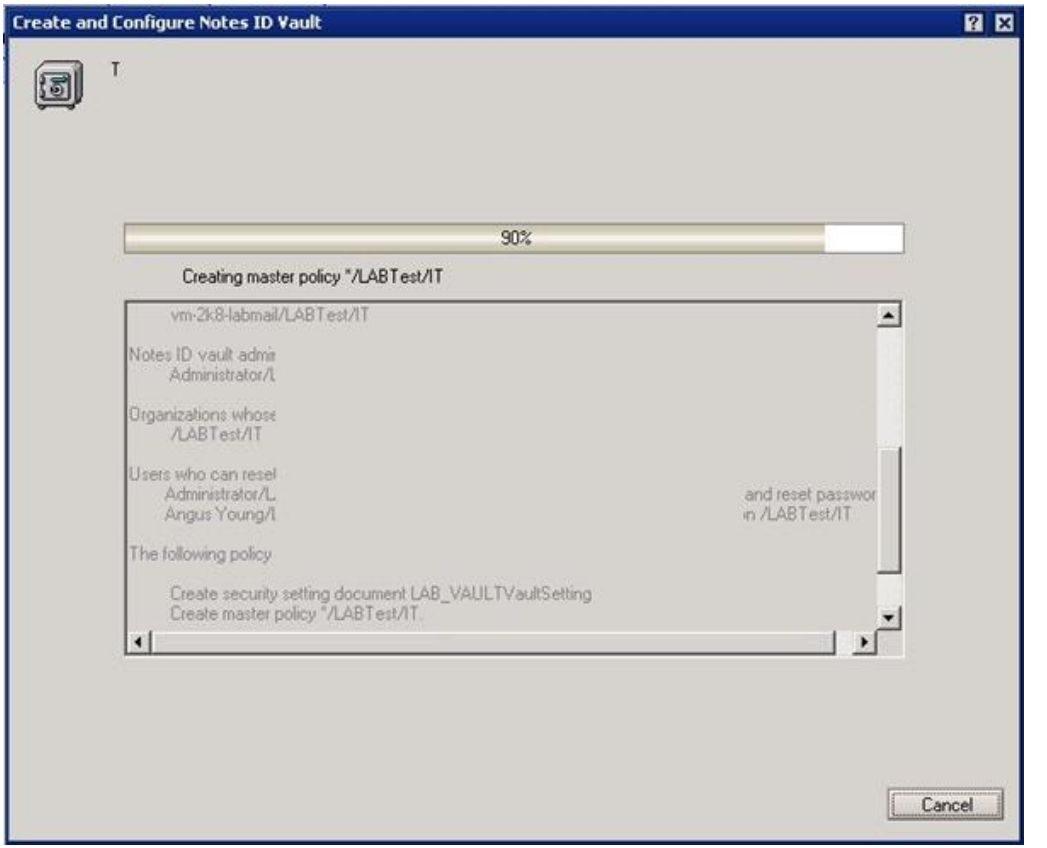
Selezionare il file **cert.id** e cliccare su **Open**.



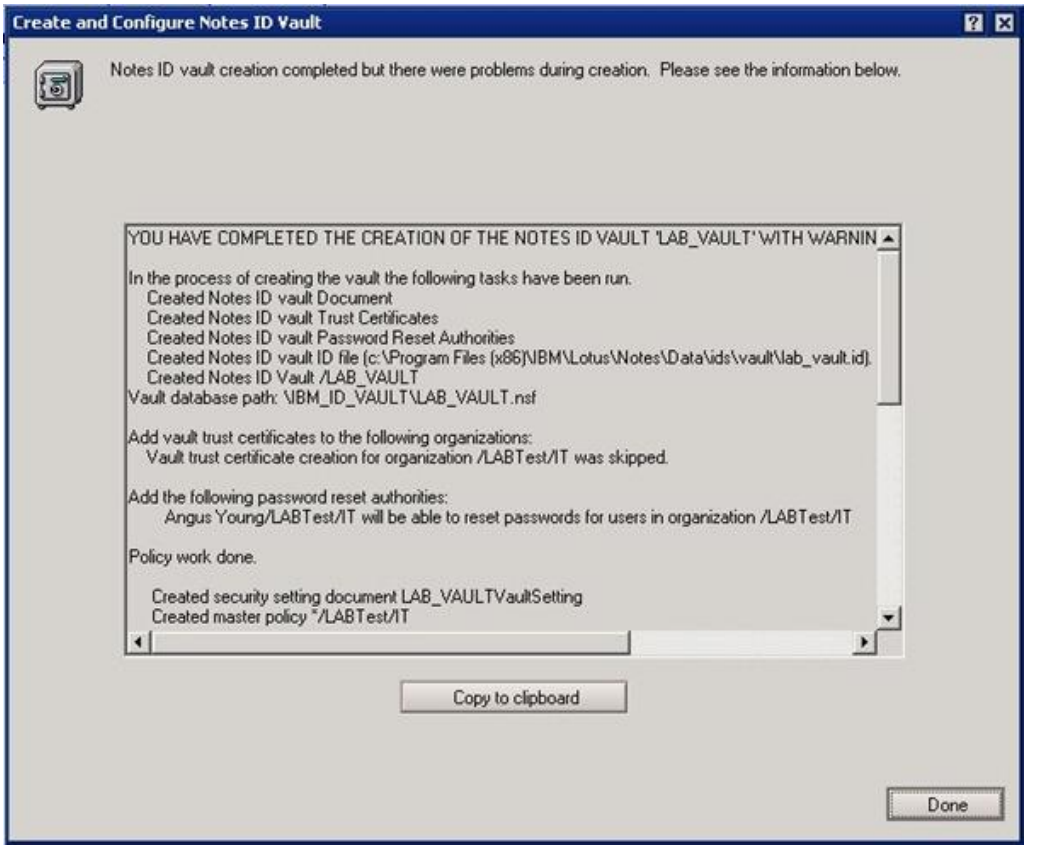
Digitare la **password del Certifier** e cliccare su **OK**.



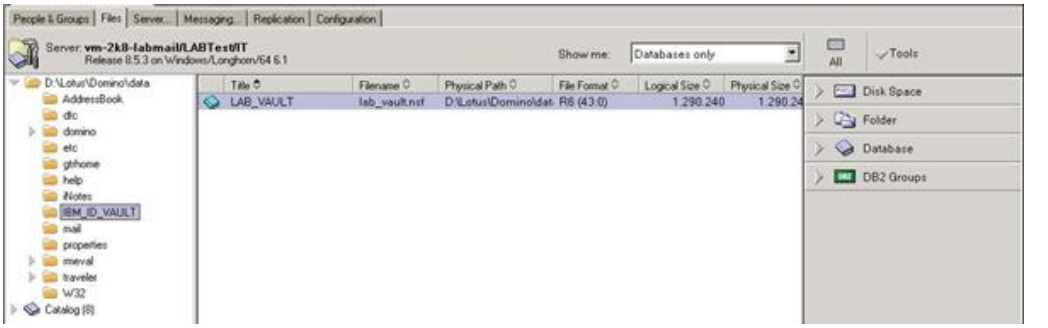
L’**installazione prosegue** creando le componenti rimanenti.



Terminata l'installazione, viene **presentato il log riepilogativo** delle configurazioni effettuate. E' consigliato **copiare queste informazioni** in un file come documentazione. Cliccare su **Done** per terminare.



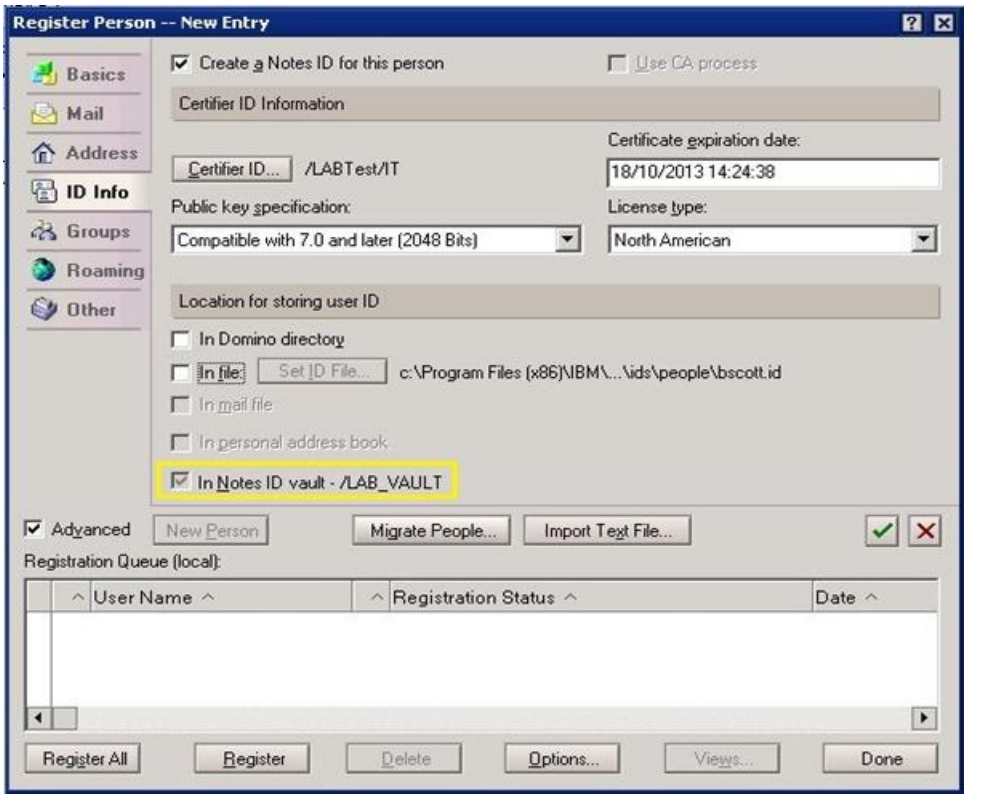
Il database è accessibile da *Domino Administrator* selezionando **Files Tab –> IBM_ID_VAULT –> Vault_name**. All'interno del database è possibile verificare **quali client sono già inseriti** nel *Vault*.



La **gestione del *Vault*** viene effettuata tramite *Domino Administrator* selezionando **Configuration Tab –> Tools –> ID Vaults –> Manage**.

Registrazione degli utenti nel Vault

Durante la **creazione di un nuovo account**, nella sezione **ID Info** è selezionata automaticamente come location dell'ID utente l'opzione **In Notes ID Vault -/***nome_vault*.

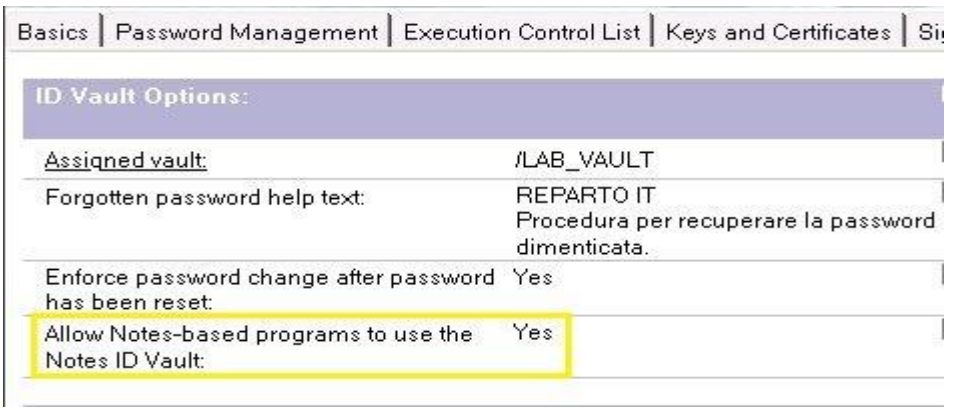


Per gli **account esistenti**, accedere a *Lotus Notes* e il sistema si farà carico, **tramite la policy** precedentemente creata, di **copiare l'ID user nel Vault**.

Configurazione Vault per iNotes

Per poter **sincronizzare la password di Lotus Notes anche con iNotes** (WebMail), bisogna innanzitutto attivare nella policy ID Vault il parametro:

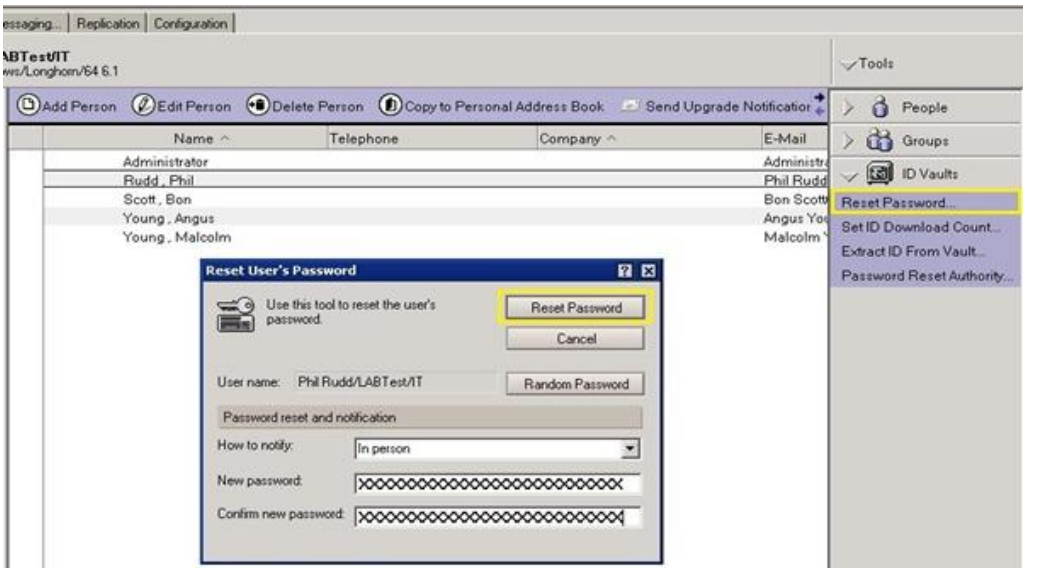
Allow Notes-based programs to use the Notes ID Vault: ***YES***



Accedere tramite browser a iNotes e cliccare da **Preferences -> Security** il bottone **Sync with Vault**.

Resettare la password di un client

L'operazione avviene **selezionando l'utente** a cui si vuole resettare la password e tramite **Tools –> ID Vaults** cliccare su **Reset Password**. Impostare la nuova password e cliccare su **Reset Password**.



Il **reset della password viene confermata** dalla schermata informativa.

A questo punto il sistema è operativo e la funzionalità della **gestione dei file ID degli utenti è attiva**. Testata la configurazione, la messa in produzione non richiede interruzioni del servizio di posta.

Gestire le prenotazioni di meeting room e risorse con Lotus Domino

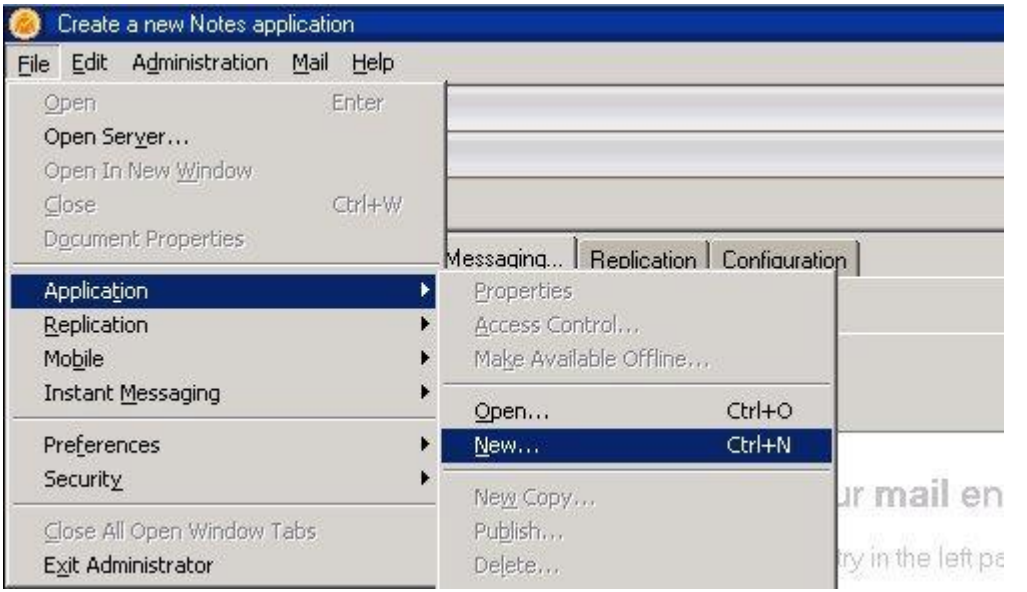
Spesso in alcune aziende la gestione e prenotazione delle risorse (meeting room, proiettori, etc.) si basano sul classico foglio *Excel* conservato sul pc di qualche segretaria o sul foglio di carta appeso sulla porta delle varie sale riunioni.

E' evidente che **questo tipo di gestione non è efficiente**. Per sapere la disponibilità di una certa risorsa bisogna chiamare una terza persona o recarsi fisicamente nel locale dove è custodito il foglio con le varie prenotazioni.

Avere accesso a questo tipo di servizio in tempo reale e senza doversi alzare dalla propria scrivania porta molti vantaggi. Non solo si **risparmia tempo** ma permette di avere un'**informazione precisa** (la disponibilità ad esempio) e una **gestione efficiente** delle varie risorse.

Procedura

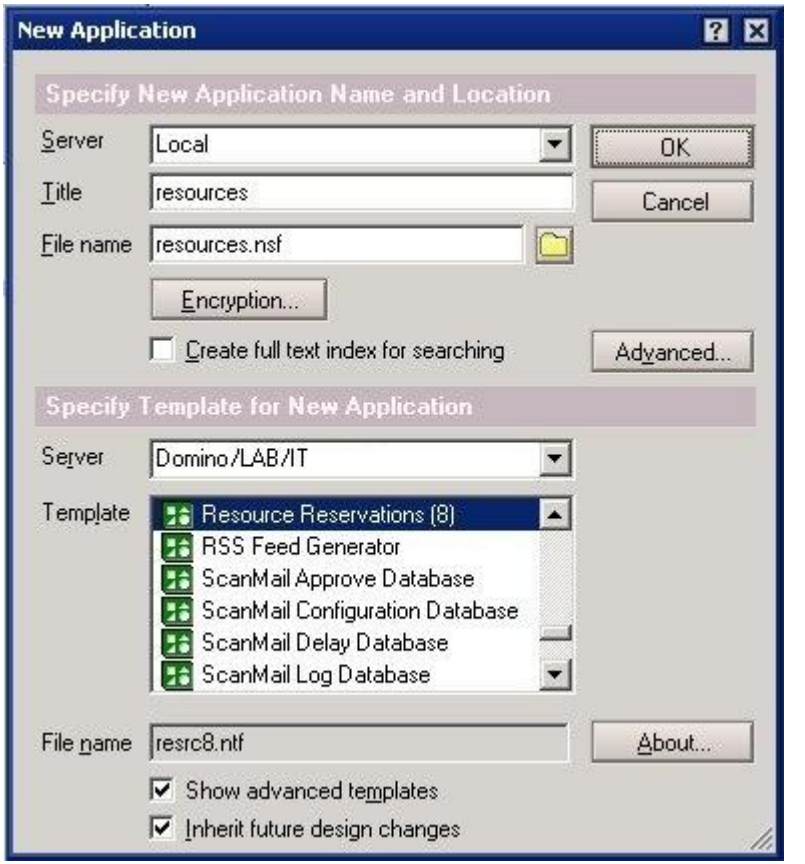
Da *Domino Administrator* fare click su **File –> Application –> New**.



Selezionare il server su cui si vuole installare il servizio, attribuire nel campo **Title** il nome del database e nel campo **File name** il nome del file del database. Impostare il **check** sulle due opzioni:

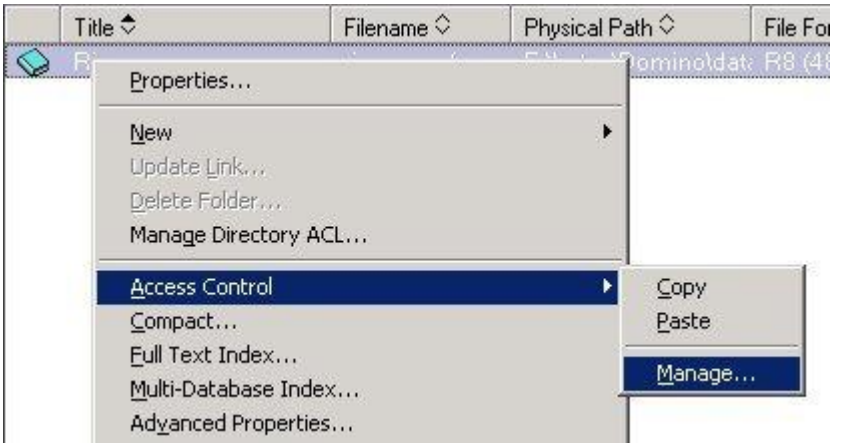
Show advanced templates
Inherit future design changes

Selezionare come **Template** la voce **Resource Reservation** e cliccare su **OK**.

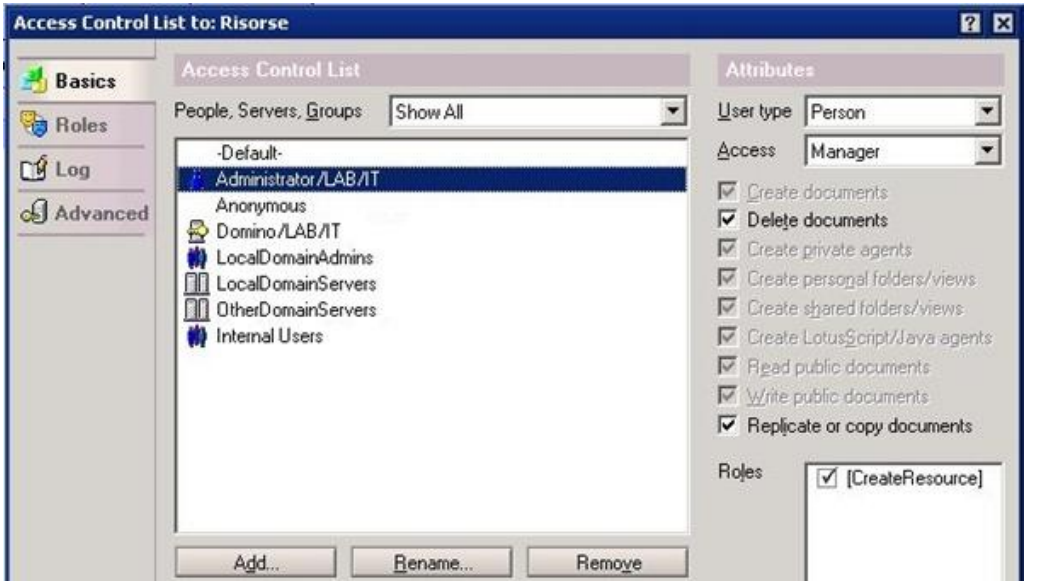


Per poter accedere e gestire il servizio, è necessario **configurare correttamente le ACL**, cioè i permessi di operatività per gli utenti e gruppi specificati.

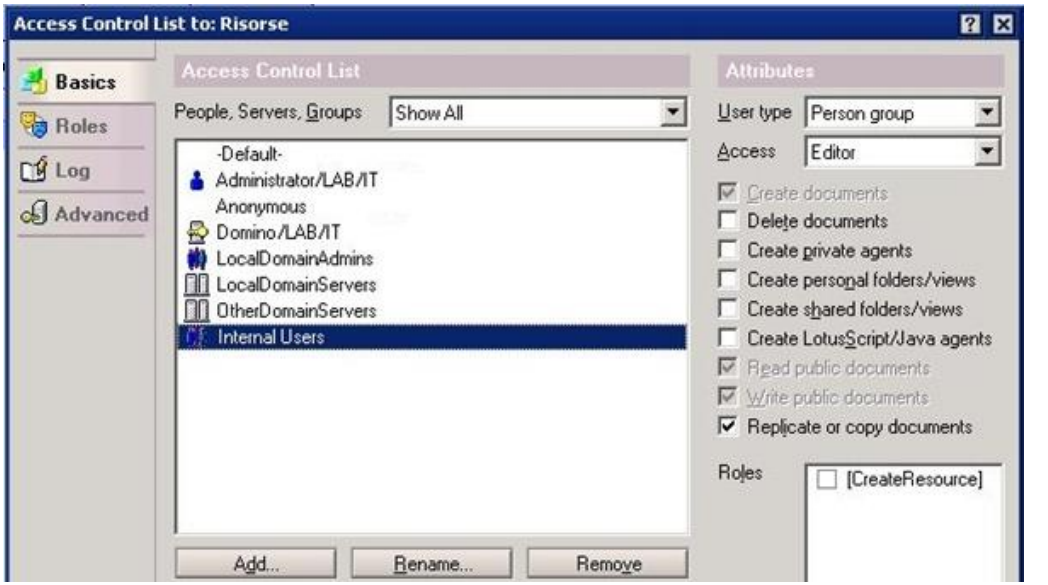
Da **Domino Administrator –> Files**, fare click con il tasto destro del mouse sul file del database appena creato (*resources.nfs*) e selezionare **Access Control –> Manage**.



Per poter **creare e gestire le risorse**, è necessario attribuire all'utente o gruppo il ruolo di **Create Resource** mettendo il **check** sull'opzione.



Per **creare e gestire le prenotazioni** è sufficiente impostare per l'utente o gruppo desiderato il valore **Editor** al campo **Access** .

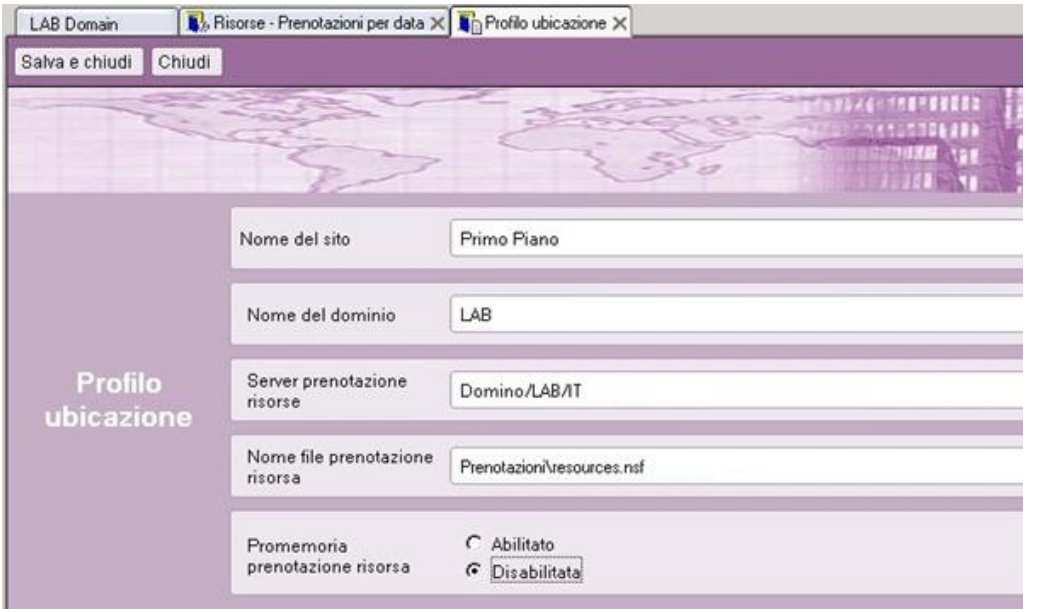


Creazione delle risorse

L'utente o gruppo con i diritti di *Create Resource* possono creare l'ubicazione e le risorse che saranno poi gestite dagli utenti.

Effettuare un doppio click sul file del database da **Domino Administrator –> Files** per accedere alla gestione delle risorse.

Come primo step è necessario **creare le Location o Ubicazioni** in cui si trovano le risorse. Cliccare sul bottone **Nuova ubicazione**, completare i campi richiesti e cliccare su **Salva e chiudi** per completare l'operazione.



Successivamente **creare le risorse** cliccando sul bottone **Nuova risorsa** completando i campi richiesti. Cliccare su **Salva e chiudi** per completare l'operazione.

Cliccando sulla voce **Risorse**, vengono visualizzate le **risorse appena create**.

Impostazione servizi sul server

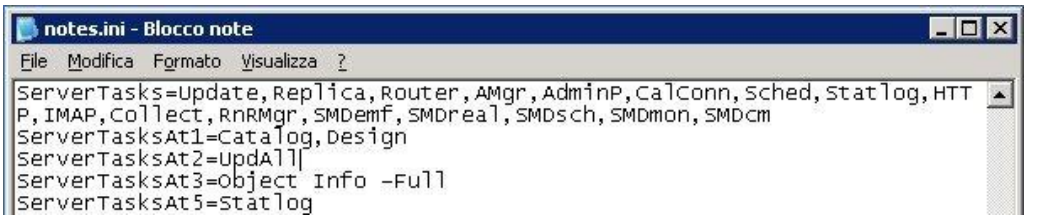
Per poter funzionare, la gestione delle risorse richiede che sul server *Domino* i seguenti **servizi siano attivi**:

- Schedule Manager (**Sched** task)
- Calendar Connector (**Calconn** task)
- Free Time system (**nnotes** task)

Se il servizio di prenotazione risorse non dovesse funzionare, **verificare** che questi servizi siano **caricati sul server**. Ad esempio per caricare il servizio *Calendar Connector* di *Domino*, eseguire da console il comando:

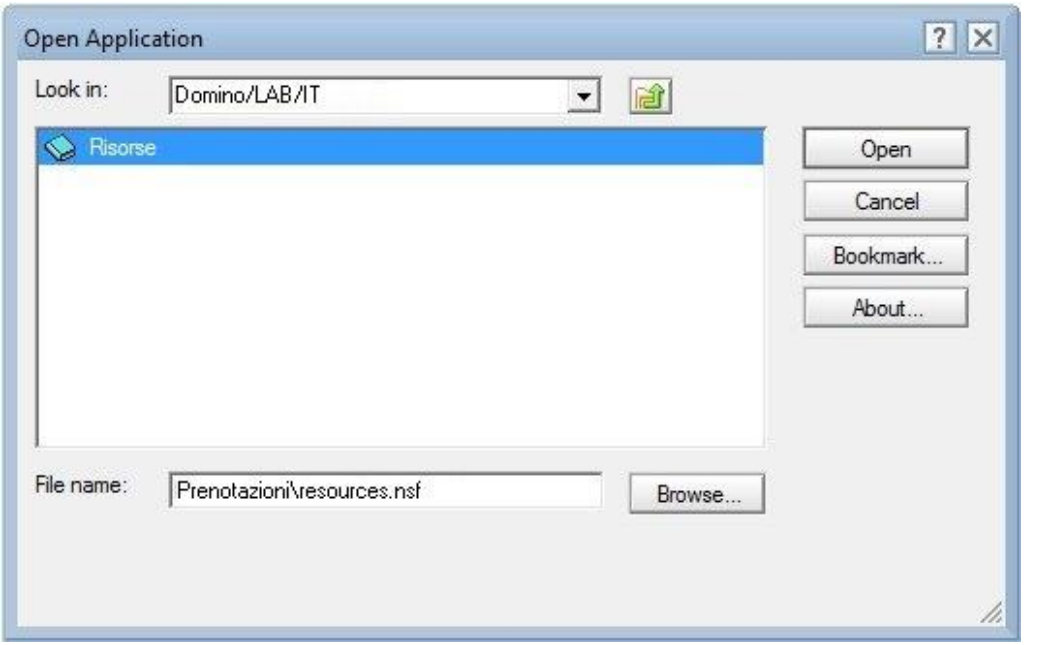
```
load calconn
```

Per **caricare automaticamente** i servizi mancanti durante il ravvio del server, aggiungere le opzioni nel file di configurazione **notes.ini** alla voce **ServerTasks**.

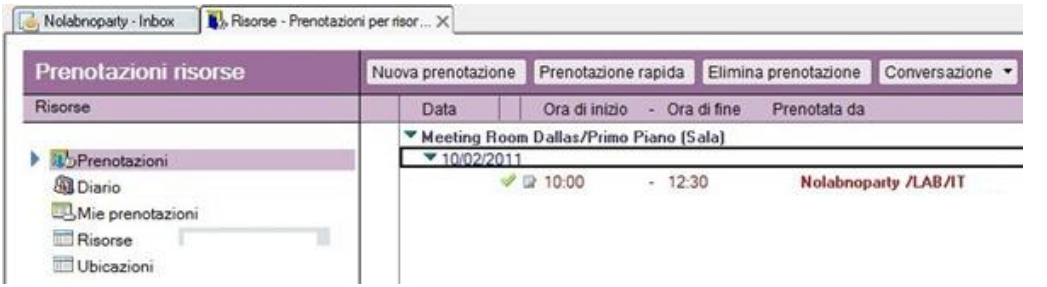


Test del servizio

Nel client *Lotus Notes*, cliccare su **File –> Application –> Open**, selezionare nel campo **Look in** il server in cui è stato configurato il servizio e fare doppio click sul **database creato sul server**.



A questo punto **effettuare una prenotazione**. Se il tutto funziona correttamente, vedremo nella lista delle Prenotazioni la risorsa appena riservata.



Questo è un ottimo sistema per **facilitare la gestione** di meeting room, proiettori e le risorse utilizzate in azienda per i vari eventi, riunioni ed appuntamenti.


NOLABNOPARTY

» Perchè questo blog?

Ho ideato questo blog perchè avevo la necessità di uno spazio da utilizzare come knowledge base personale raggiungibile ovunque su cui annotare i miei appunti di informatica relativi a soluzioni, procedure e fix.

» Chi sono

Lavoro nel campo dell'Information Technology da qualche anno e sono impiegato presso aziende come sistemista. Mi occupo principalmente dell'implementazione e della gestione di servizi informatici basati su piattaforma virtuale VMware vSphere con sistemi Microsoft Windows/Active Directory e Linux (Red Hat, CentOS).

Informatica applicata per l'azienda

procedure e guide step-by-step

- **Servizi Windows**
- **Servizi Linux**
- **Monitoraggio rete**
- **Procedure VMware**
- **Sicurezza**
- **Messaggistica**

PAOLO VALSECCHI
sistemista informatico

my LinkedIn profile

http://it.linkedin.com/in/paolovalsecchi

NOLABNOPARTY
COMPUTERS COUNT FROM 0 TO 1, THE REST IS JUST AN ILLUSION

Informatica applicata per l'azienda
http://nolabnoparty.com