

## HOW TO

## ABILITAZIONE KERBEROS IN MOSS 2007

## Table of Contents

Introduzione.....	3
Kerberos behind the scene .....	4
Abilitazione Kerberos in ambiente Single Forest .....	6
Descrizione Ambiente.....	6
Creazione degli SPN in Active Directory .....	7
Abilitazione della Trust For Delegation .....	9
Abilitazione Kerberos per SQL Server .....	10
Abilitazione Kerberos per la Web Application in SharePoint.....	11
Abilitazione Kerberos in IIS .....	12
Abilitazione Kerberos per Shared Services Provider .....	13

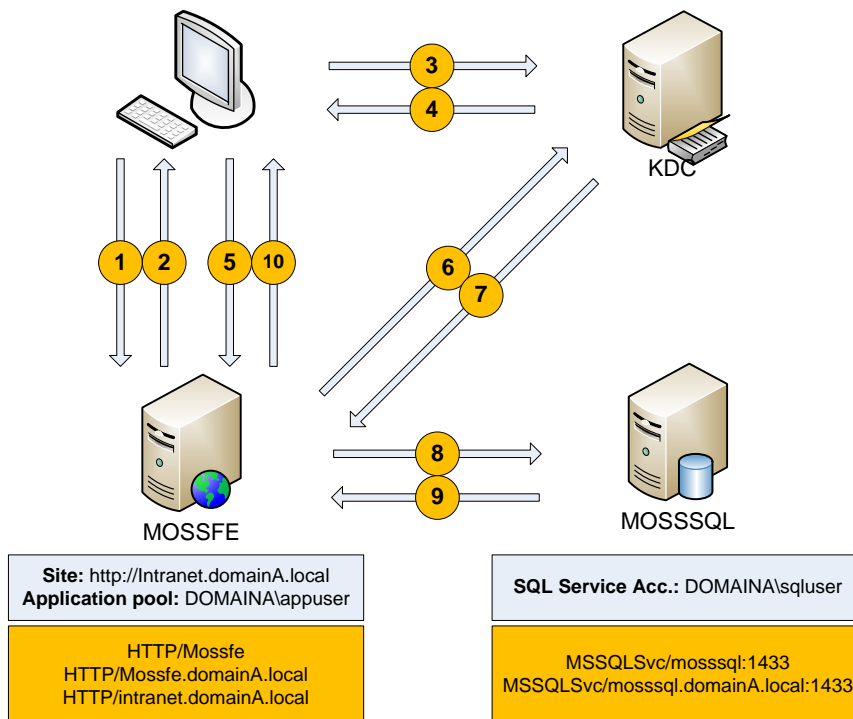
## Introduzione

Questa guida ha lo scopo di illustrare i passi fondamentali da seguire per abilitare l'autenticazione Kerberos su una Farm Microsoft Office SharePoint Server 2007.

L'abilitazione di Kerberos ha molti vantaggi rispetto alla tradizionale NTLM, primi fra tutti la maggiore velocità, scalabilità e sicurezza ma permette anche la cosiddetta "*user delegation*" molto utile (ad esempio per l'utilizzo di K2 BlackPearl, o anche per il semplice utilizzo dell' RSS Viewer)

## Kerberos behind the scene

Per capire al meglio ciò che si andrà a mostrare in questa guida, illustriamo brevemente il flusso che si innesca quando un client effettua una chiamata ad un website MOSS su cui è abilitato il protocollo Kerberos: questo ci chiarirà il perché sono necessari alcuni dei passi che verranno illustrati in questa guida.



1. Il client richiede l'apertura del sito `http://intranet.domainA.local`, il primo accesso è tentato in anonimo.
2. Il Front-end risponde con un errore di tipo 402.1 (Access Denied) ma fornisce anche i `WWWAuthenticate Headers` accettati dal sito: in pratica restituisce i protocolli di autenticazione accettati (Kerberos)
3. Il Client allora richiede al KDC di dominio un ticket Kerberos per SPN <http://intranet.domainA.local>

4. Se l'SPN viene trovato (ovvero è stato configurato su AD), il KDC risponde con il ticket richiesto.
5. Il ticket viene quindi passato alla Web Application che lo verifica.
6. Adesso che l'utente è abilitato al sito, il Front-end richiede di recuperare i dati dal Database SQL. Per far questo richiede al KDC un ticket per l'SPN *MSSQLSvc/mosssql:1433*
7. Se l'SPN viene trovato, il KDC risponde con il ticket richiesto
8. A questo punto il Front-end è in grado di passare il ticket al server SQL che lo valida
9. Una volta validato il ticket, il Server SQL invia i dati richiesti al Front-end
10. Il Front-end, con tutti i dati a disposizione, è in grado di mostrare il contenuto della pagina al Client che l'aveva richiesto.

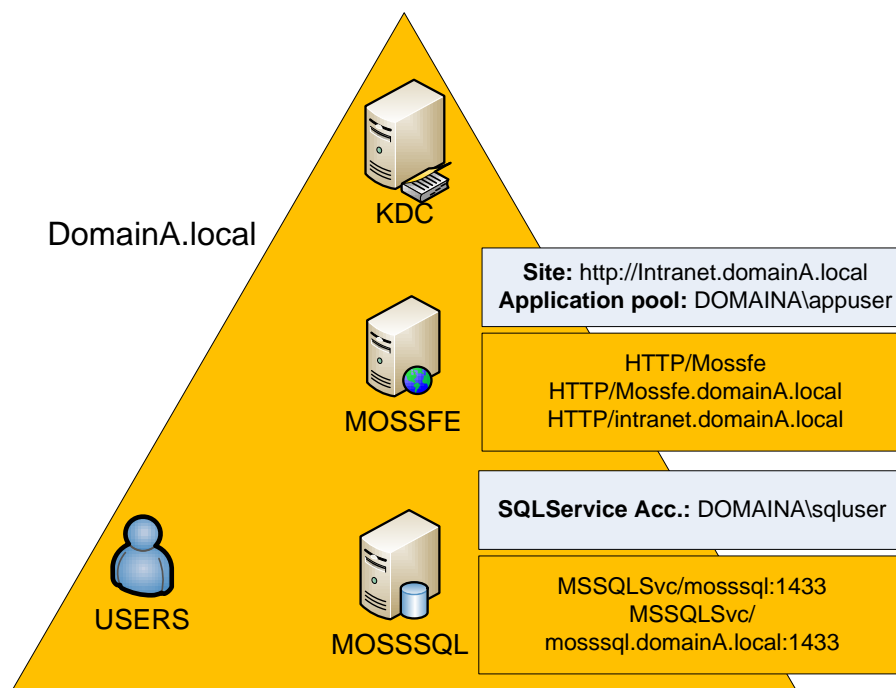
Il meccanismo di autenticazione appena descritto è eseguito solo alla prima richiesta, dopo di cui i ticket utilizzati rimangono i medesimi fino alla loro scadenza, questo significa un minor carico di lavoro per i Domain Controller.

**Nota:** è possibile limitare l'utilizzo di Kerberos al solo Front-End, autenticandosi quindi in NTLM sul Server SQL (l'account per l'autenticazione, in questo caso, è quello dell'application pool del sito: *DOMAINA\appuser*). In questo caso è comunque ancora possibile configurare il *double-hop* verso altri servizi (K2 BlackPearl per esempio).

## Abilitazione Kerberos in ambiente Single Forest

### Descrizione Ambiente

L'ambiente di riferimento per questa prima parte è mostrato in figura:



Questo è il caso più semplice: utenti e risorse coesistono nello stesso dominio della stessa foresta.

Ipotizziamo una configurazione composta da un Front-end e da un SQL server. Sul Front-End è pubblicato un sito che risponde all'indirizzo <http://intranet.domainA.local>. L'Application Pool legato a questo Web Site gira con le credenziali dell'utente *DOMAINA\appuser*.

Ipotizziamo inoltre che il server SQL sia installato con la sola l'istanza di Default attiva e che i servizi girino con l'account *DOMAINA\sqluser*.

Per i privilegi da dare alle utenze appena segnalate fare riferimento all'articolo: <http://technet.microsoft.com/en-us/library/cc263445.aspx>

L'Action Plan da implementare per l'abilitazione di Kerberos in questo ambiente è quindi il seguente:

- Creazione degli SPN in Active Directory
- Abilitazione della "Trust for Delegation"
- Abilitazione di Kerberos per SQL Server (facoltativo)
- Abilitazione di Kerberos per la Web Application in Sharepoint
- Abilitazione di Kerberos su IIS
- Abilitazione di Kerberos per SSP (facoltativo)

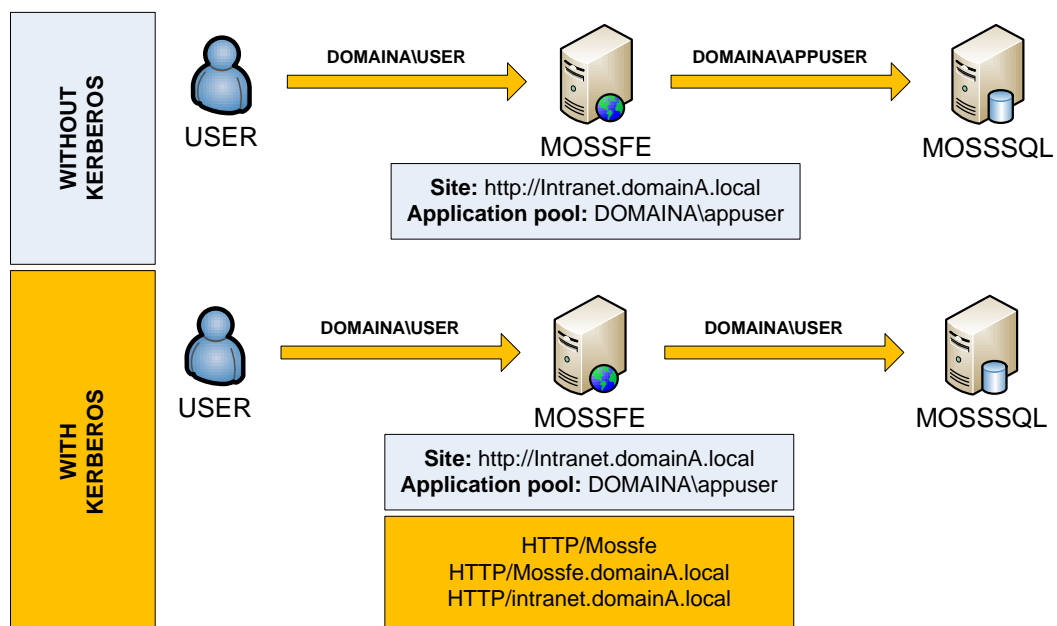
I punti segnalati come facoltativi sono necessari solo nel momento in cui si vuole abilitare Kerberos anche per l'autenticazione sul servizio SQL server.

Questi punti verranno analizzati singolarmente nei prossimi paragrafi.

### Creazione degli SPN in Active Directory

La prima cosa da fare per abilitare Kerberos è la configurazione in Active Directory degli SPN (Service Principle Name).

Gli SPN (insieme alla Trust for Delegation) sono usati da Active Directory per delegare agli account di specifici servizi la possibilità di impersonare l'utente nei confronti di un secondo servizio.



Nel primo caso in esempio (Without Kerberos) l'utente si presenta al front-end con le proprie credenziali. A questo punto, non essendo abilitati gli SPN (e la Trust for Delegation), il Front-End utilizza l'account dell'Application Pool per reperire i dati dal Server SQL.

Nel secondo caso (With Kerberos) invece, il Front-End è delegato per presentarsi al SQL Server con le credenziali utente, effettuando quello che in gergo viene chiamato *Double-Hop*.

Gli SPN sono configurabili mediante il tool a riga di comando SetSPN.exe contenuto nei Resource Kit di Windows Server 2003 o mediante l'utilizzo di ADSIEdit (noi utilizzeremo il primo metodo a mio avviso più comodo)

Gli SPN sono composti di tre parti: il servizio, l'hostname e la porta, quest'ultimo non sempre necessario.

Il comando per la registrazione di un SPN in Active Directory è il seguente e deve essere eseguito ovviamente con i privilegi di Domain Administrator:

***setspn.exe -A SERVICE/hostname:port DOMAIN\Account***

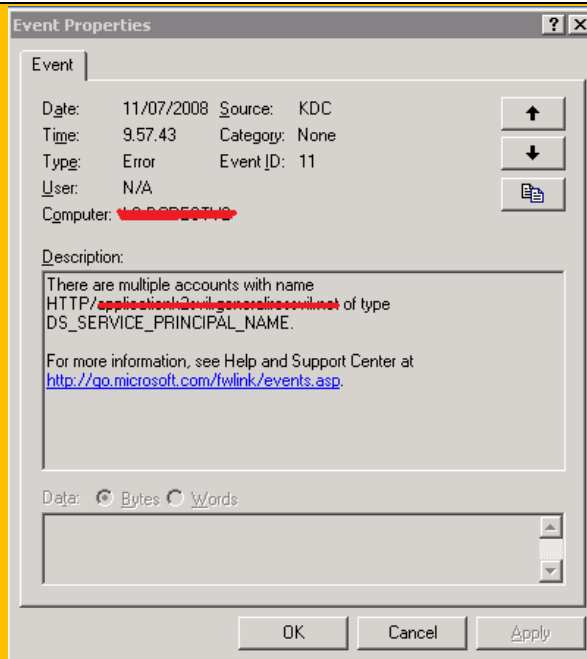
per maggiori informazioni riguardo il tool SetSPN.exe vi rimando a questo link:  
<http://technet2.microsoft.com/windowsserver/en/library/b3a029a1-7ff0-4f6f-87d2-f2e70294a5761033.msp?mfr=true>

Considerando la nostra configurazione, è necessario registrare i seguenti SPN:

User Account	SPN	Note
MOSS Farm Account	HTTP/mossfe HTTP/mossfe.domainA.local	
DOMAINA\appuser	HTTP/intranet HTTP/intranet.domainA.local	
MySite Account	HTTP/mysite HTTP/mysite.domainA.local	Sostituire con l'URL del vostro mysite

Per ogni altra web application per cui ritenete necessario abilitare Kerberos dovete registrare gli SPN come nella seconda riga della precedente tabella, assegnandoli all'account dell'Application Pool a cui questa fa riferimento.

**Nota:** Non è possibile avere due SPN identici per account distinti nella foresta. Quindi fate attenzione a non duplicarli, altrimenti Active Directory li ignorerà, segnalando l'errore sul solo domain controller.



Non saranno segnalati errori invece né dal SetSPN.exe né dall'ADSIEdit.

## Abilitazione della Trust For Delegation

Per completare la configurazione degli account per Kerberos è necessario abilitare i diritti di delega su Active Directory.

I passi da seguire sono i seguenti (ipotizzo la presenza di un Domain Controller con Windows Server 2003)

- Aprire la console *Active directory Users and Computers*
- Selezionare l'account (macchina o utente che sia) cui si vogliono fornire di diritti di Trust For Delegation
- Cliccare con il tasto destro e selezionare Properties
- Selezionare il tab *Delegation*
- Selezionare *Trust this user for delegation to any services (Kerberos only)* come mostrato in figura

Location	Managed By	Object	Security	Dial-in
General	Operating System	Member Of	Delegation	

Delegation is a security-sensitive operation, which allows services to act on behalf of another user.

Do not trust this computer for delegation  
 Trust this computer for delegation to any service (Kerberos only)  
 Trust this computer for delegation to specified services only

Use Kerberos only  
 Use any authentication protocol

Services to which this account can present delegated credentials:

Service Type	User or Computer	Port	Service Name	Dc

Expanded

Considerando la nostra configurazione, è necessario abilitare la delegation ai seguenti account:

Account	Tipo Account
MOSSFE	Account Macchina
DOMAINA\appuser	Account Utente
MySite Account	Account Utente

Per ogni altra web application per cui ritenete necessario abilitare Kerberos dovete abilitare al Trust For Delegation l'utente dell'Application Pool a cui questa fa riferimento.

### Abilitazione Kerberos per SQL Server

L'abilitazione di Kerberos su SQL server prevede la registrazione di alcuni SPN e dell'assegnazione dei diritti di Trust For Delegation ad alcuni account che si aggiungono a quelli segnalati nei paragrafi precedenti.

Nella nostra configurazione è necessario registrare SPN dell'utenza di servizio di SQL come mostrato nella tabella successiva

User Account	SPN	Note
DOMAINA\squser	MSSQLSvc/mosssql:1433 MSSQLSvc/mosssql.domainA.local:1433	

Ed abilitare per la Trust For Delegation il seguente account

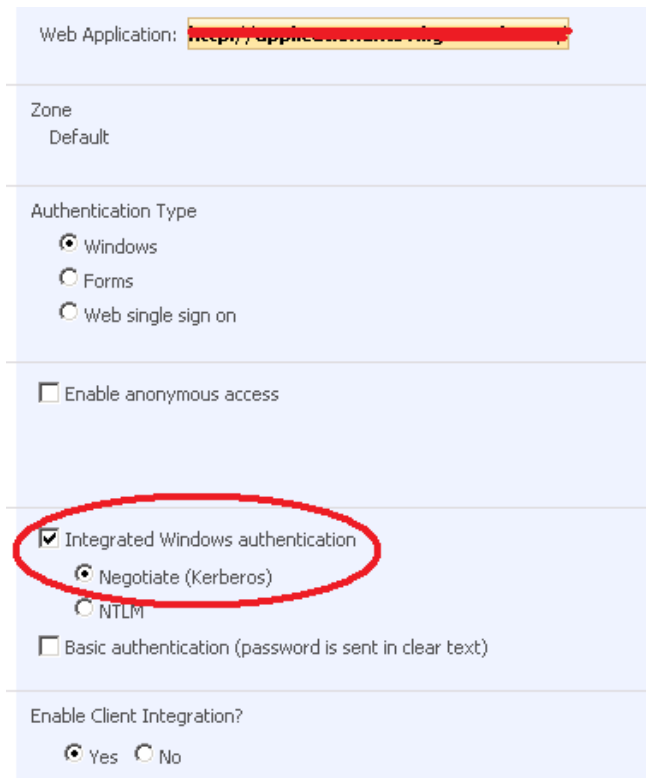
Account	Tipo Account
MOSSSQL	Account Macchina

Per maggiori informazioni fare riferimento a: <http://support.microsoft.com/kb/319723/en-us>

### Abilitazione Kerberos per la Web Application in SharePoint

L'abilitazione di Kerberos su MOSS 2007 è forse la parte più semplice di tutte:

- Aprire la Central Administration
- Navigare verso Application Management > Authentication Providers
- Selezionare la Web Application che si intende abilitare a Kerberos
- Selezionare Default come Zone
- In IIS Authentication Settings selezionare Integrated Windows Authentication e Negotiate (Kerberos) come mostrato nella figura seguente.
- Effettuare un IISReset



Web Application:

Zone  
Default

Authentication Type

Windows  
 Forms  
 Web single sign on

Enable anonymous access

Integrated Windows authentication  
 Negotiate (Kerberos)  
 NTLM  
 Basic authentication (password is sent in clear text)

Enable Client Integration?  
 Yes  No

## Abilitazione Kerberos in IIS

Questa operazione è utile per poter abilitare il site IIS che ospita la Web Application all'utilizzo di Kerberos e, in caso di errori, a scalare su l'autenticazione NTLM.

Non è un'operazione indispensabile, ma è utile perché permette di avere una sorta di salvagente in caso di problemi con Kerberos.

- Cliccare Start > Run e lanciare un prompt dei comandi (CMD)
- Localizzare il file adsutil.vbs (posizione di default C:\Inetpub\AdminScripts)
- Verificare i protocolli di autenticazioni attualmente accettati mediante il comando:  
**cscript adsutil.vbs get w3svc/Website/root/NTAuthenticationProviders**  
dove *Website* è l'ID del Website presente su IIS
- Nel caso la risposta fosse diversa da

**NTAuthenticationProviders : (STRING) "Negotiate,NTLM"**

Lanciare il seguente comando:

**cscript adsutil.vbs set w3svc/Website/root/NTAuthenticationProviders "Negotiate,NTLM"**

- Effettuare un IISReset

Per maggiori informazioni fare riferimento a: <http://support.microsoft.com/kb/215383/en-us>

### Abilitazione Kerberos per Shared Services Provider

Per abilitare anche SSP all'utilizzo di Kerberos sono necessari un altro SPN

User Account	SPN	Note
SSP Application Pool Account	HTTP/sspadmin HTTP/sspadmin.domainA.local	Sostituire con l'URL del vostro SSP

Ed abilitare un altro utente per la Trust For delegation

Account	Tipo Account
SSP Application Pool Account	Account Utente

È inoltre necessario eseguire il seguente comando:

**stsadm.exe -o SetSharedWebServiceAuthn -negotiate**