Kerberos and SharePoint

No ticket touting here, does SharePoint add another head?

Spencer Harbar (spence@harbar.net)

SharePoint User Group UK
February 27th 2008, London

MVP Microsoft Most Valuable Professional

Agenda

- What is Kerberos?
- What benefits does Kerberos offer?
- How does it work?
- I'm a SharePoint Guy, do I *really* need to know how it works?
- I'm a SharePoint Gal, why should I care?
- Do I care?
- Do I *really* need Kerberos for my SharePoint?
- What do I need to use Kerberos for my SharePoint?
- How do I configure my SharePoint to use Kerberos?
- Can I automate Kerberos configuration for SharePoint?

Before we dive in…

This session is geared to those implementing Active Directory based SharePoint solutions.

- Intranet, Extranet

This session is *all* about Authentication

- Authentication == who you are
- Authorisation == what you can access

What is Kerberos?

Open, Extensible ***Authentication*** Protocol developed at MIT

Implemented in Windows 2000 and above Domains

Implemented as a Security Support Provider (SSP) and accessed through the SSP Interface (SSPI)

Default Authentication Protocol in Windows 2000 and above Domains

Windows 2003 adds support for certificate based smart cards

Benefits of Kerberos

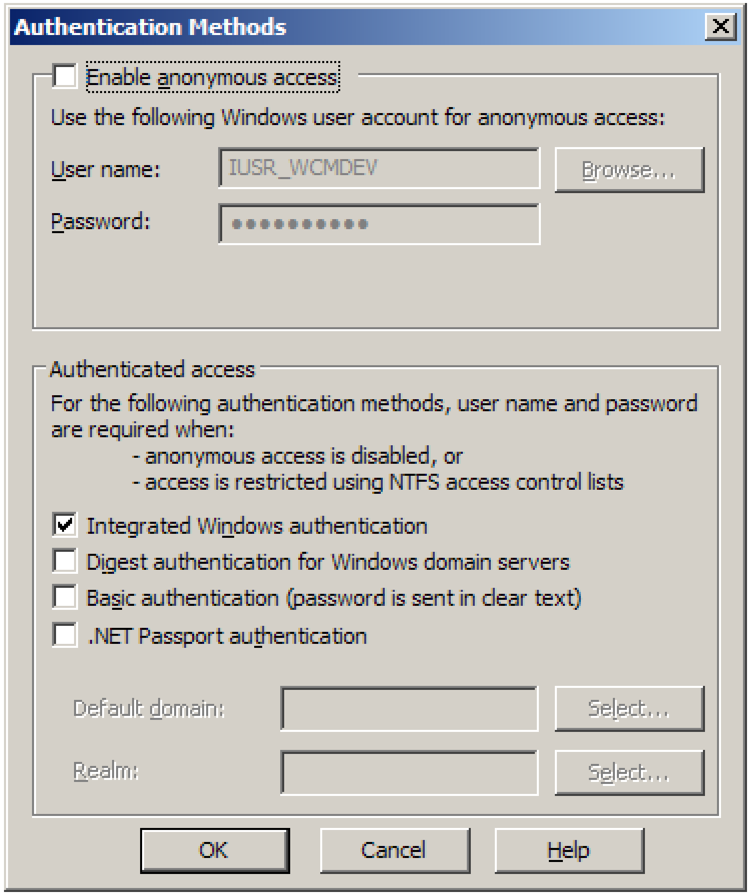
Delegated Authentication	• e.g. allows a web server to impersonate a client when accessing a database resource • a.k.a. “double-hop authentication”
Interoperability	• with other implementations, open (IETF based) • mature (10 years)
Efficient	• renewable session tickets • avoids unnecessary roundtrips to domain controllers
Mutual Authentication	• allows verification of server identity
Secure	• Assumes network is **un-trusted** • Real encryption!

Windows Authentication

A framework for supporting protocols implemented as a Security Support Provider

Used to be called “Integrated Authentication”

Used to be called “Windows Integrated Authentication”



Authentication Methods

☐ Enable anonymous access

Use the following Windows user account for anonymous access:

User name: IUSR_WCMDEV

Password: ●●●●●●●●●●●

Authenticated access

For the following authentication methods, user name and password are required when:
- anonymous access is disabled, or
- access is restricted using NTFS access control lists

☑ Integrated Windows authentication

☐ Digest authentication for Windows domain servers

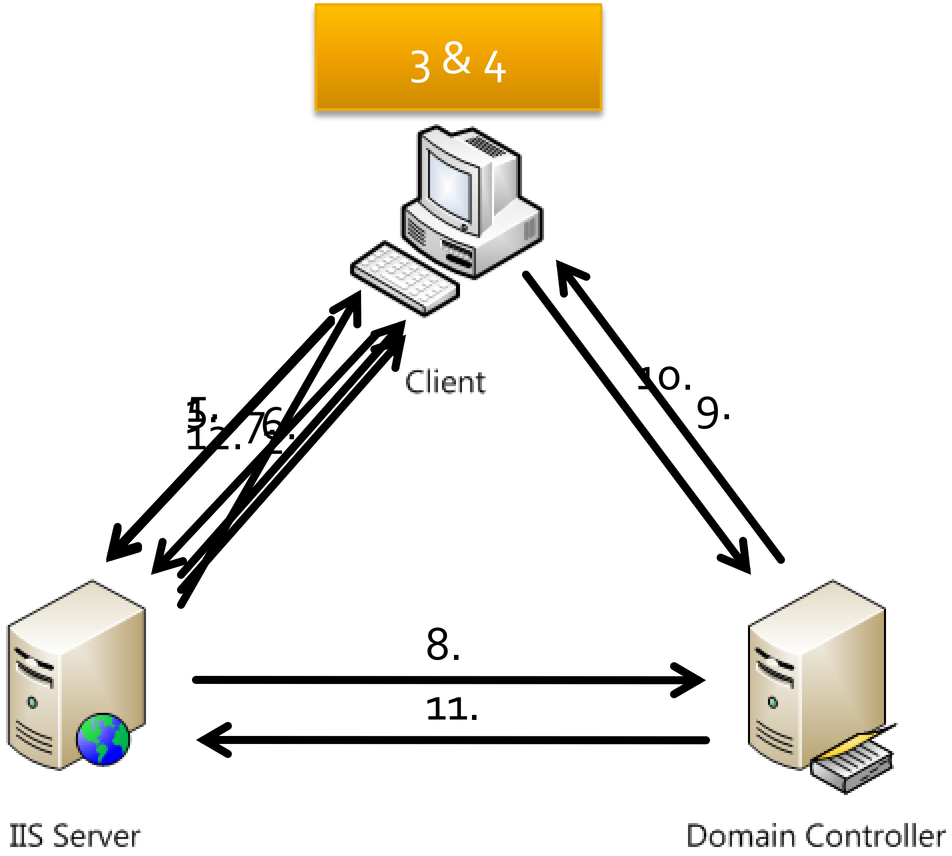
☐ Basic authentication (password is sent in clear text)

☐ .NET Passport authentication

Default domain:

Realm:

Windows Authentication (NTLM)



1. HTTP GET
2. HTTP: 401 WWW-Authenticate: NTLM Header
3. Acquire Credentials
4. Construct AuthN Token
5. HTTP GET with Username
6. HTTP 401: NTLM Challenge
7. NTLM Challenge Response
8. Username Token *
9. NTLM Challenge *
10. NTLM Challenge Response *
11. Authentication Success
12. HTTP 200: OK

Doesn't Scale

Doesn't Perform

Shared Secret over the wire

* Max NTLM Auths (2 by default) can be tweaked, but can tank your DCs

Key Kerberos Concepts

Key Distribution Centre (KDC)

- Provides Ticket-Granting Tickets to clients

Authorisation Server (AS)

- Authenticates users to services

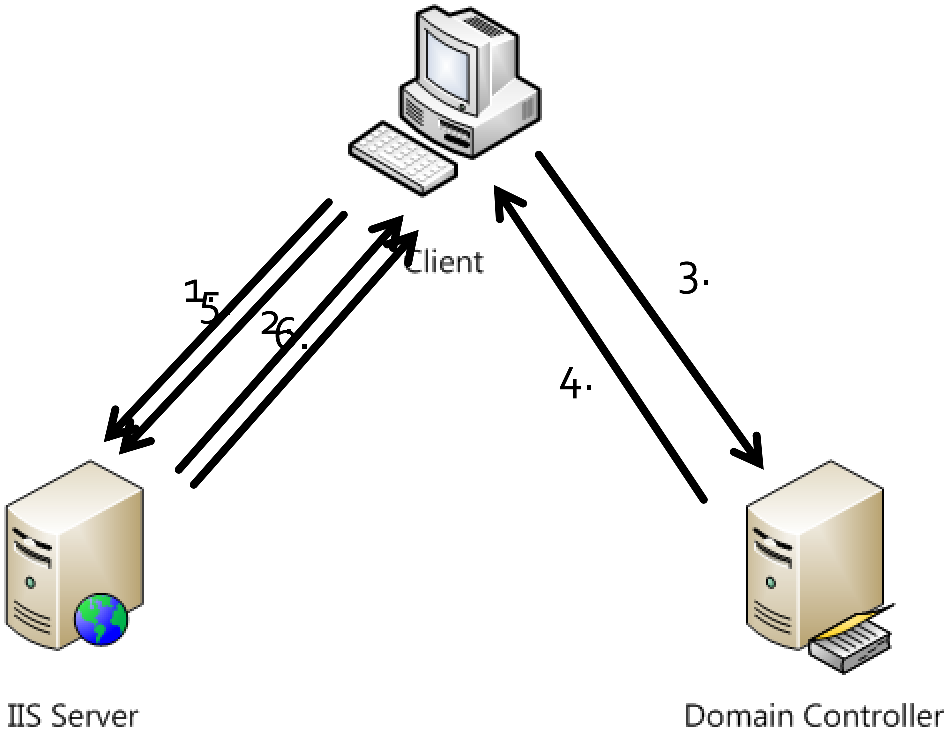
Service Ticket

- For authentication to a service (e.g. a web site)

Ticket Granting Ticket (TGT)

- Allows service tickets to be granted without re- authentication

Windows Authentication (Kerberos)



1. HTTP GET
2. HTTP: 401 WWW-Authenticate: Negotiate or Kerberos
3. Request Service Ticket from KDC
4. Service Ticket returned
5. HTTP GET with authenticator
6. HTTP 200 OK

Approx one authN every five minutes

It’s a knockout!

	NTLM	Kerberos
Cryptography	Symmetric	Symmetric and/or Asymmetric
Trusted 3rd Party	Domain Controller	Domain Controller with KDC Domain Controller and Enterprise CA
Supported Clients	Windows 9x, Me, NT4, 2000 and above	Windows 2000 and above
Features	Slow auth (pass thru)	Ticketing
	No mutual AuthN	Mutual AuthN
	No delegation	Delegation
	Proprietary	Open Standard
	Lamer data protection	Cryptographic data protection

That's all very nice…

- …but what about SharePoint?

- As a SharePoint person…
  - you don't really need to know the gory details
  - for the most part it's very simple
  - but of course the more you know, the more you know. You know?

- Learn more over at Ken Schaefer's IIS blog:

  http://www.adopenstatic.com/cs/blogs/ken/archive/tags/Security/default.aspx

Why Kerberos with SharePoint?

Significantly more secure than NTLM

- Based on ticketing system

Dramatically improves performance

- Avoids unnecessary authentication requests to your DCs

Yet another horrible SharePoint "rule of thumb"

- The 1 DC per 3 WFEs old wives tale

Do I *really* need Kerberos?

How many concurrent users do you have?

- Real concurrent, not total number

Are you suffering from performance problems?

- Despite dropping mucho cash on nice shiny boxes

Where are your Domain Controllers located?

Do you have a “medium” SharePoint Farm or larger?

Do you want to use the RSS Viewer Web Part or Excel Services?

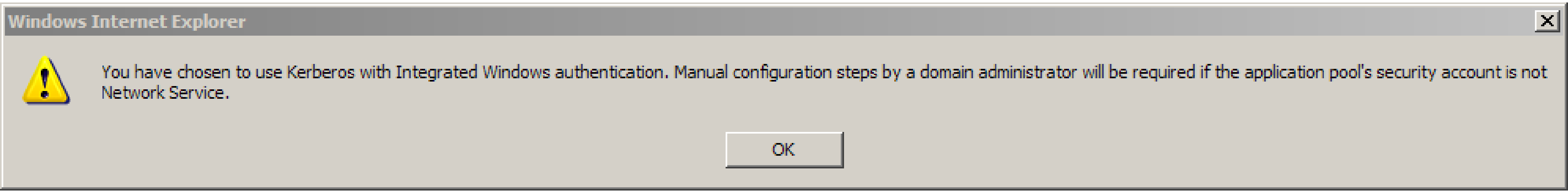
- Plenty of other examples

Kerberos Requirements

- Windows 2000 and above
- a TCP/IP Network
- DNS (hosts files still work)
- an Active Directory Domain
- Consistent Time Service
- Service Principal Names (SPNs)

SharePoint Comedy (sort of)

- You've all seen the lamer dialog:



Windows Internet Explorer

You have chosen to use Kerberos with Integrated Windows authentication. Manual configuration steps by a domain administrator will be required if the application pool's security account is not Network Service.

- Leading SharePoint books say:
  "we recommend Kerberos but we're not gonna tell you how to set it up, here's a link to a non SharePoint KB"

- Detailed badly on the web with a focus on single server scenarios.

- Improved slightly with KB832769

So how do I set it up?

- Trust SharePoint computers for delegation
- Add Service Principle Names for Application Pool Identities
- Trust Application Pool Identities for delegation
- Configure SharePoint Web Applications
- (Optional) Enable Kerberos for Shared Services

Spence’s Recommendation

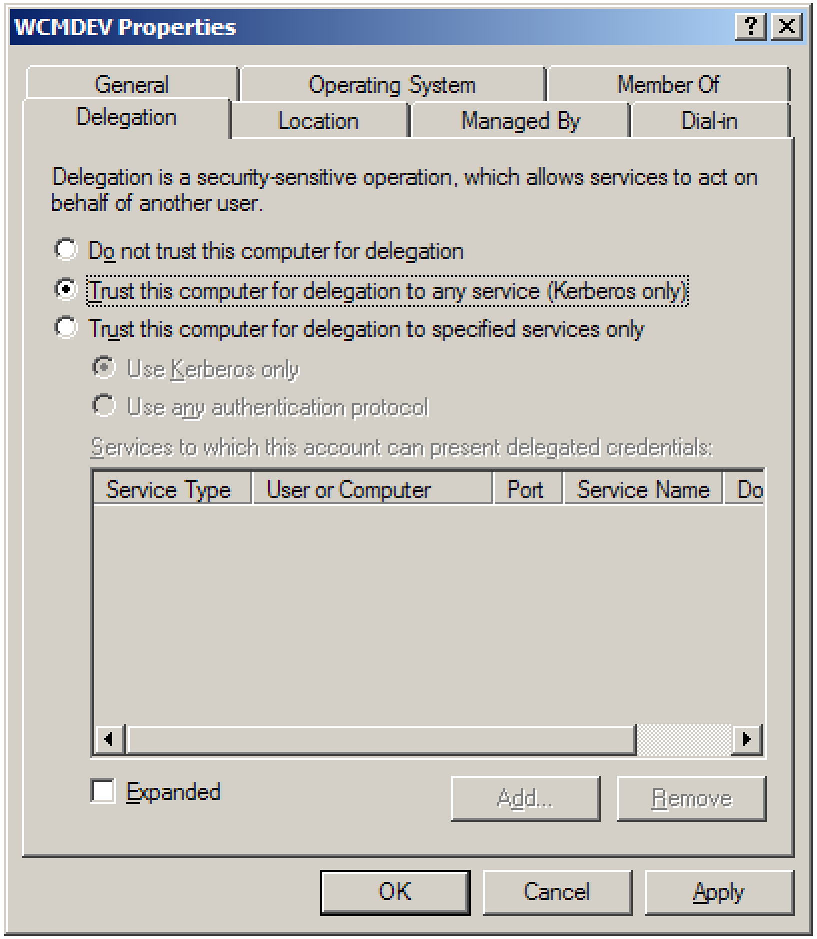
Start with NTLM and *then* configure Kerberos

- Especially for Central Administration
- Allows verification of functionality first

Automate once comfortable

Trust SharePoint computers for delegation

- Required for certain Web Parts
- Required for Excel Services
- Configure using AD Users & Computers



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:

□ Expanded

Service Principal Names (SPNs)

Ensures that only specified accounts have permission to delegate a specific service on a user's behalf.

Syntax (is very important!):

- service/name:port domain\username

Configured with:

- SETSPN.EXE – Resource Kit or Windows 2008
- ADSIEdit – Support Tools or Windows 2008

SETSPN.EXE Examples

```
setspn -A http/intranet.company.com SHAREPOINT\apppool1
```

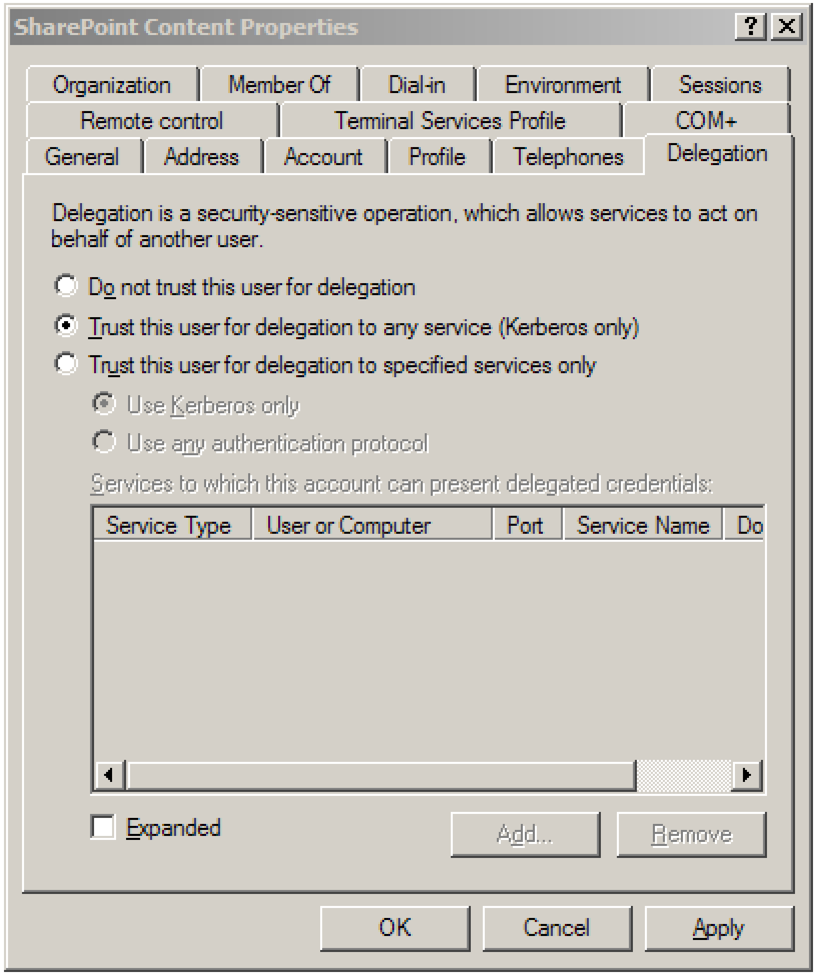
```
LIST SPNs for an account: setspn -l SHAREPOINT\apppool1
```

```
DELETE SPN: setspn -d http/moss SHAREPOINT\apppool1
```

- SPNs should not be in the form of URLs i.e. http//moss.harbar.com
- Best Practice: SPNs for both NetBIOS names and FQDNs
- If you are using a non default port (bad idea) the port should be included

Trust Accounts for delegation

- Required for AuthN to work!
- Configure using ADUC
- Available once an SPN has been created



SharePoint Content Properties

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

○ Do not trust this user for delegation

● Trust this user for delegation to any service (Kerberos only)

○ Trust this user 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	Do

□ Expanded

Configure Web Applications

Application Management > Authentication Providers

STSADM -o authentication -url http://whatever –type windows –usewindowsintegrated

Negotiate (Kerberos) means fallback

ADSUTIL.VBS

Configuring Kerberos for SharePoint

Demo

Common Issues

Mis-configured SPNs

Duplicate SPNs

PAC Validation (fixed in W2K3 sp2)

IE6 doesn't support Kerberos and CNames (hotfix available - 911149)

Troubleshooting

Know your W3SVC error codes:

- 401.1 means invalid credentials or auth type
- 401.2 means something is in the way (e.g. proxy server)

Don’t test from the local box, test remotely

Check out KerbTray.exe (reskit utility)

Coming Soon…

Detailed White Paper on Kerberos for SharePoint

- Medium and Large Farms
- Excel Services
- Troubleshooting and Tips and Tricks
- Improvements in Windows Server 2008

SharePoint Kerberos Configuration Utility

- Wizard based automation tool

QA & Disucssion

- Thanks for your attention!
- Feel free to post Kerberos related queries to the forums at http://suguk.org