Spencer Harbar

Kerberos Part Two:

"Advanced" Scenarios and Additional Considerations

About the speaker…

- Spencer Harbar - www.harbar.net | spence@harbar.net
  - Microsoft Certified Master | SharePoint 2007
  - Microsoft Certified Master | SharePoint Instructor & Author
  - Most Valuable Professional | SharePoint Server
  - SharePoint Patterns & Practices Advisory Board Member
  - 15 years in Enterprise IT
  - ISPA Board Member
  - Enterprise Architect working with Microsoft's largest customers deploying Office SharePoint Server 2007.

Microsoft CERTIFIED Master

SDN SOFTWARE DEVELOPMENT NETWORK

MVP Microsoft Most Valuable Professional

Agenda

- Two-part session
- Part One (you missed it!)
  - Authentication Methodologies
  - Kerberos Overview
  - Why Kerberos with SharePoint?
  - Implementing Kerberos with SharePoint
  - Common Problems
  - Best Practices
- Part Two (this session!)
  - Troubleshooting
  - Shared Service Providers
  - Search
  - “Advanced” Scenarios
  - Kerberos Only?
  - More Tools
  - Q&A/Discussion

TROUBLESHOOTING

Windows Event Log

- System Event Log
  - First place to look
  - Sources
    - Kerberos
    - LSA
    - LsaSrv
  - Events include Kerberos Error Code
  - Document “Troubleshooting Kerberos Errors”
    - Includes Codes, Possible Causes, Resolutions
    - http://www.microsoft.com/downloads/details.aspx?FamilyID=7DFEB015-6043-47DB-8238-DC7AF89C93F1

Security Event Log

- Audit Logon Events

	WS 2008	WS 2003
An account was successfully logged on	4624	540, 528
An account failed to log on	4625	529, 530, 531, 532, 533, 534, 535, 536, 537, 539

- Account Logon Events (Windows Server 2008)

ID	Message
Subcategory: Kerberos Authentication Service	
4768	A Kerberos authentication ticket (TGT) was requested.
4771	Kerberos pre-authentication failed.
4772	A Kerberos authentication ticket request failed.
Subcategory: Kerberos Service Ticket Operations	
4769	A Kerberos service ticket was requested.
4770	A Kerberos service ticket was renewed.
4773	A Kerberos service ticket request failed.

Kerberos Auditing

- Enabled via Registry

  `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos\Parameters\LogLevel`

  - Value Type: REG_DWORD
  - Value Data: 1

- Don't leave on!
- Document "Troubleshooting Kerberos Errors"
  - Includes Codes, Possible Causes, Resolutions
  - http://www.microsoft.com/downloads/details.aspx?FamilyID=7DFEB015-6043-47DB-8238-DC7AF89C93F1

Kerberos DebugView

- Enabled via Registry

  `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos\Parameters\KerbDebugLevel`

  - Value Type: DWORD
  - Data: c0000043 (outputs the most standard set of debug messages)
    - Try it first, If you still want to see more output, set it to ffffffff

  `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos\Parameters\LogToFile`

  - Type: DWORD
  - Data: 1
  - Logs to %windir%\System32\lsass.log

- Don't leave on!

Network Monitor

- Or alternative network capture tools
  - Wireshark, NetSniffer, EtherDetect etc
- Captures packets for analysis
- Filter Capture for Authentication
- Will include detailed Kerberos related traffic
- Document "Troubleshooting Kerberos Errors"
  - Includes Codes, Possible Causes, Resolutions
  - http://www.microsoft.com/downloads/details.aspx?FamilyID=7DFEB015-6043-47DB-8238-DC7AF89C93F1

The Great Load Balancing Myth

- "Kerberos doesn't work with our Load Balancer"
  - Load Balancers don't know or care about Kerberos
  - It's not a Kerberos issue, it's a addressing issue

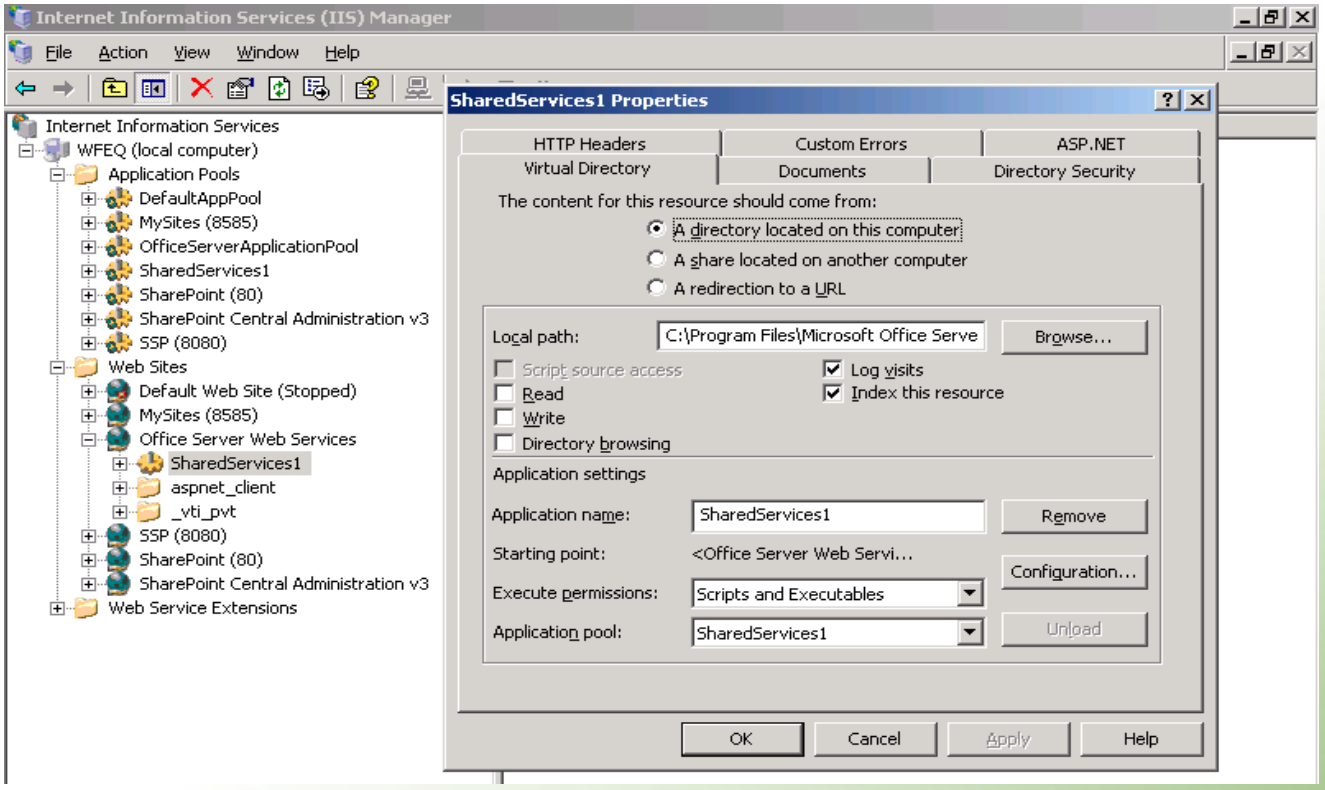
- SharePoint Web Application Configuration
  - Don't use CNames (again!)
  - Configure host name/host headers correctly
  - Certain Load Balancers need to address hosts directly

Troubleshooting Kerberos

DEMONSTRATION

SHARED SERVICES

Shared Services




```
stsadm.exe –o setsharedwebserviceauthn
   -negotiate
```

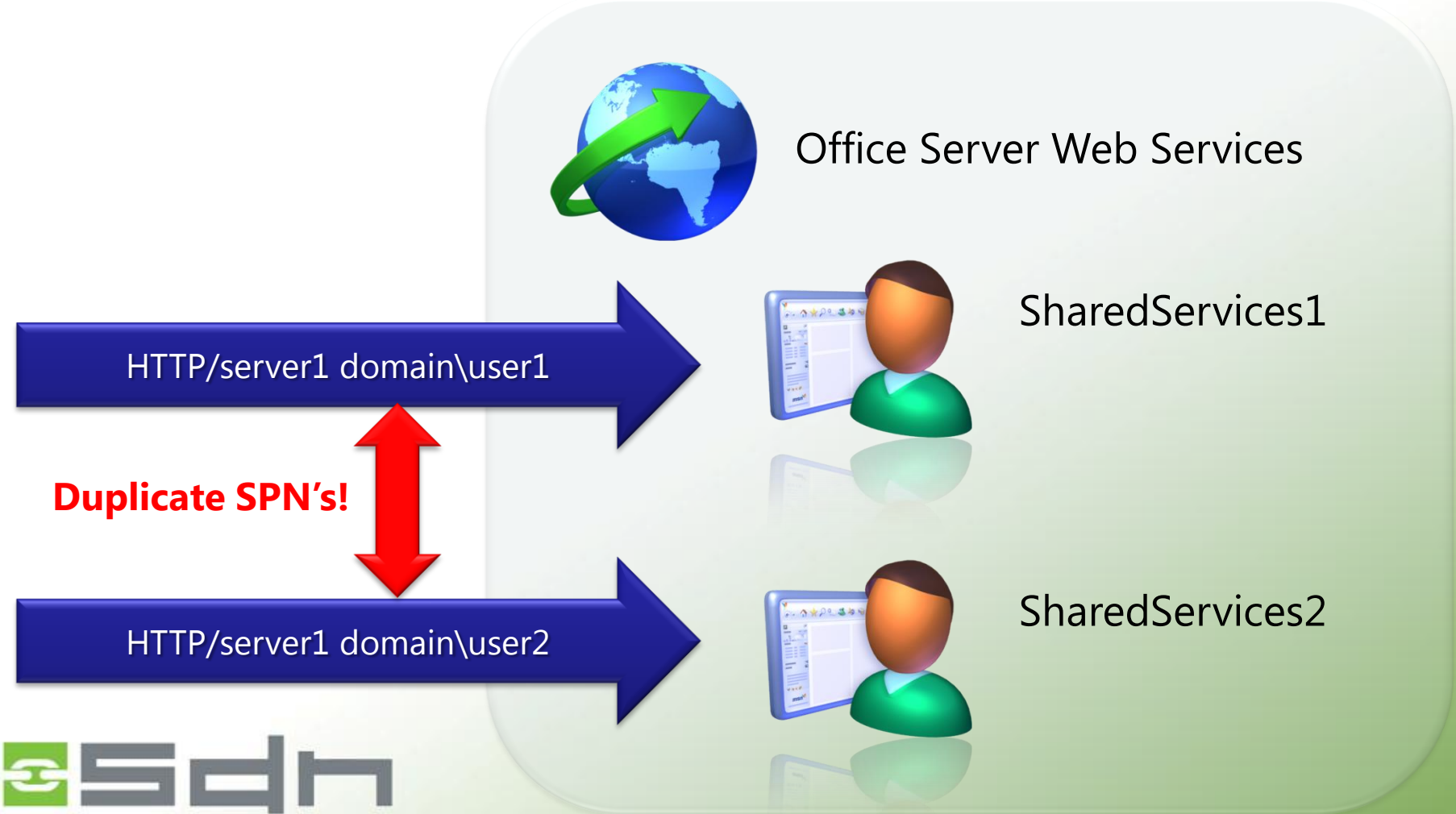
SOFTWARE DEVELOPMENT NETWORK

Issues with Shared Services

- .NET client can't bind to the server using non-default ports
  - Without host headers
  - SSP services use non default ports without host headers
    - http://server:56737 & https://server:56738
- Indexer can't crawl Kerberos Web Applications on non default ports

SOFTWARE DEVELOPMENT NETWORK

>1 SSP with different identities



SOFTWARE DEVELOPMENT NETWORK

Shared Services Solution

1. Install Infrastructure Updates (or later)
   - on all servers in farm
2. Add Registry Key

   ```
   HKLM\Software\Microsoft\Office Server\12.0\KerberosSpnFormat
   ```

   - Type: DWORD, Data: 1
3. Reboot!
4. Configure SPNs (for each server in farm)

   ```
   MSSP/server1:56737/SharedServices1
   MSSP/server1:56738/SharedServices1
   ```

5. Configure Shared Services

   ```
   stsadm.exe –o setsharedwebserviceauthn -negotiate
   ```

SOFTWARE DEVELOPMENT NETWORK

Shared Services

- Kernel Mode Authentication
  - Requires same configuration as end user applications
- You cannot mix and match NTLM and Kerberos
  - In the same Farm
  - Despite appearances
    - Central Admin setting is scoped to SSP
  - All SSPs must either be NTLM or Kerberos

Shared Services

DEMONSTRATION

SOFTWARE DEVELOPMENT NETWORK

“ADVANCED SCENARIOS”

Delegation to External Apps

- All depends upon the application
- Potential for additional configuration
- “Middle Tier” Host Delegation
- Example SQL Server Reporting Services
  - Host delegation if RS is on separate machines
  - Web.config & RSReportServer.config

Excel Services

- Do **NOT** follow KB953130!
  - Easily the worst security KB ever authored
  - Details a single MOSS server configuration!
  - Just plain wrong, many steps unnecessary
    - DCOM Configuration, Computer Account Delegation, etc
- OOTB Excel Services is a simple delegation scenario
  - Configure Web App Application Pool account for delegation to SSP SPN

```
stsadm.exe -o set-ecssecurity
   -ssp %SSPNAME% -accessmodel delegation
```

SOFTWARE DEVELOPMENT NETWORK

Excel Services & Analysis Services

- A more common scenario
  - Leveraging Data Connections
- When using with Analysis Services
  - Additional Configuration
  - Service Principal Names for Analysis Services
    - `MSOLAPSvc.3/HOST`
    - `MSOLAPSvc.3/HOST:instance`
  - Middle Tier Delegation
  - MSKB 917409

SOFTWARE DEVELOPMENT NETWORK

Excel Services

DEMONSTRATION

Kerberos Only?

- IIS uses NTLM, Negotiate, or both

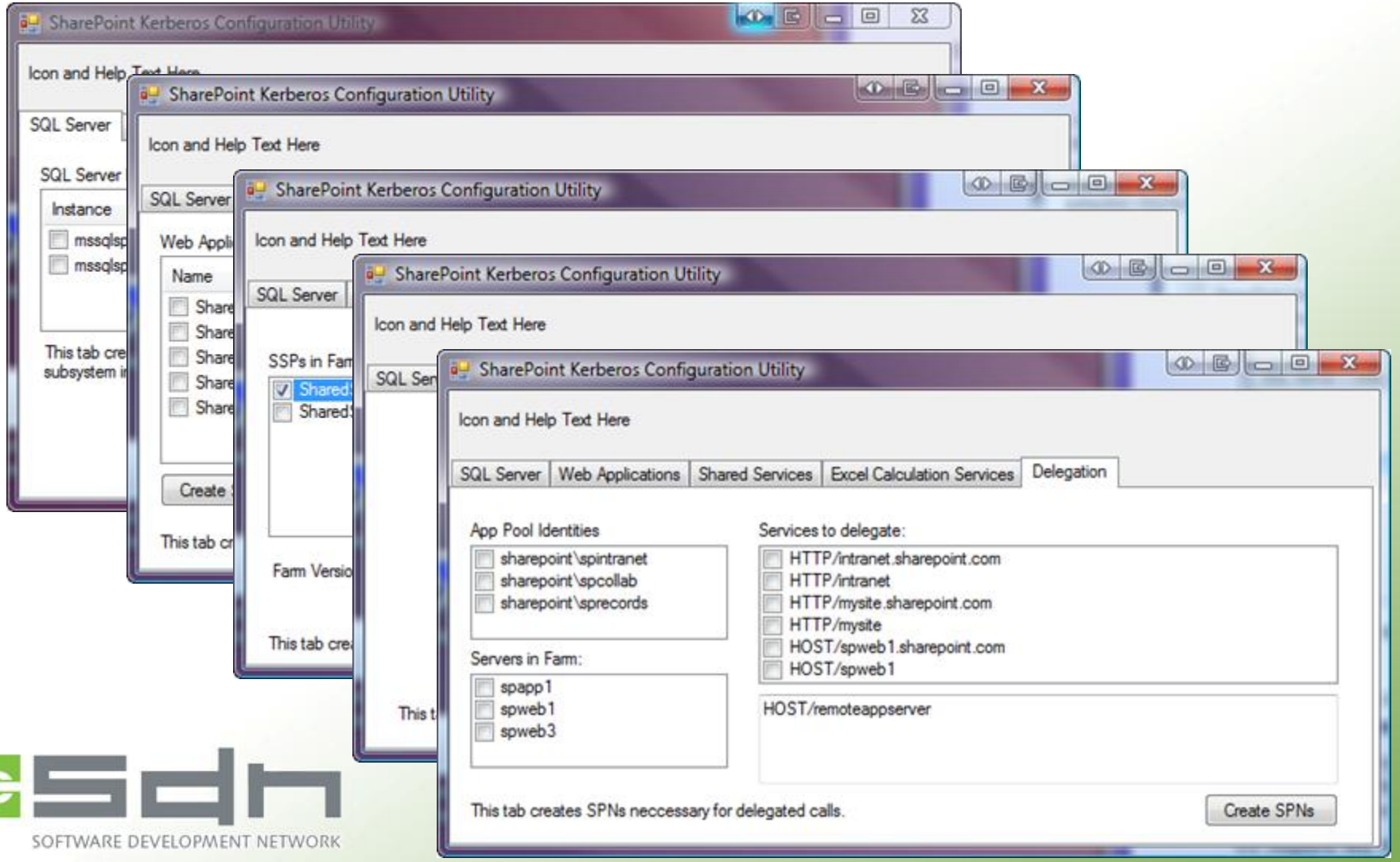
  `NTAuthenticationProviders = "Negotiate"`

  - Does not mean Kerberos only
- Negotiate will always "fall back" to NTLM
- HTTP_AUTHORIZATION server variable
  - Can be leveraged in HttpModule
  - Unsupported
- IIS7 in Windows Server 2008 R2 supports Nego2
  - allows granular Kerberos/NTLM enablement
  - Requires Windows 7 clients

Essential Tools

- CLI: Setspn.exe
  - Windows Server 2008: installed by default
  - Windows Server 2003: part of Resource Kit or separate download
    http://www.microsoft.com/downloads/details.aspx?familyid=9d467a69-57ff-4ae7-96ee-b18c4790cffd
- GUI: Adsiedit.msc
  - Windows Server 2008: installed by default
  - Windows Server 2003: part of support tools (on Windows CD)
- Kerbtray.exe http://www.microsoft.com/downloads/details.aspx?familyid=4E3A58BE-29F6-49F6-85BE-E866AF8E7A88
- Klist.exe http://www.microsoft.com/DownLoads/details.aspx?familyid=1581E6E7-7E64-4A2D-8ABA-73E909D2A7DC
  - Both part of the Windows 2003 Resource Kit Tools
    http://www.microsoft.com/downloads/details.aspx?familyid=9d467a69-57ff-4ae7-96ee-b18c4790cffd
- Network Monitor 3.3
  http://www.microsoft.com/downloads/details.aspx?FamilyID=983b941d-06cb-4658-b7f6-3088333d062f
- Fiddler http://www.fiddlertool.com/ DelegConfig http://www.iis.net/downloads/default.aspx?tabid=34&g=6&i=1434
  http://www.iis.net/downloads/default.aspx?tabid=34&g=6&i=1887

Announcing...



SOFTWARE DEVELOPMENT NETWORK

Q&A / Discussion

Thank You!

Please complete your evaluations

It makes us better next time!

SOFTWARE DEVELOPMENT NETWORK