Active Directory & SQL Server

How AD can affect your SQL Servers

Ryan Adams
Blog - http://ryanjadams.com
Twitter - @ryanjadams

PASS SQL saturday

About Me

http://www.ryanjadams.com

@ryanjadams

Microsoft Most Valuable Professional

LINCHPIN PEOPLE

PASS SQL saturday

Learn... Network... Relax... Grow... Just Add Water

SQL CRUISE

Caribbean 2013 January 26, 2013 to February 12, 2013

Alaska 2013 May 25, 2013 to June 1, 2013

2013 TECHNICAL LEAD

Full Details available at SQLCruise.com

IT/Dev CONNECTIONS

24 HOURS OF PASS

PASS SUMMIT 2015

October 27 – 30

Seattle, WA

PASS SQLRally

redgate

Friend of Redgate 2015

I'M SPEAKING

Connect. Share. Learn.

Microsoft CERTIFIED Professional

Microsoft CERTIFIED Systems Administrator

Microsoft CERTIFIED Systems Engineer

Microsoft CERTIFIED Database Administrator

Microsoft CERTIFIED Technology Specialist

SQL Server 2005

Microsoft CERTIFIED IT Professional

Database Administrator

PASS SQL saturday

Objectives

- ❑ DNS
- ❑ Group Policy
- ❑ Security Groups
- ❑ Password Policies
- ❑ SQLAgent
- ❑ Kerberos

DNS

- When is Name Resolution important?

- Outgoing
  - Linked Server
  - OPENROWSET
  - SQLAgent – PowerShell
  - SQLAgent - CmdExec
- Incoming
  - Applications
  - Scripts
  - Kerberos
  - SPNs

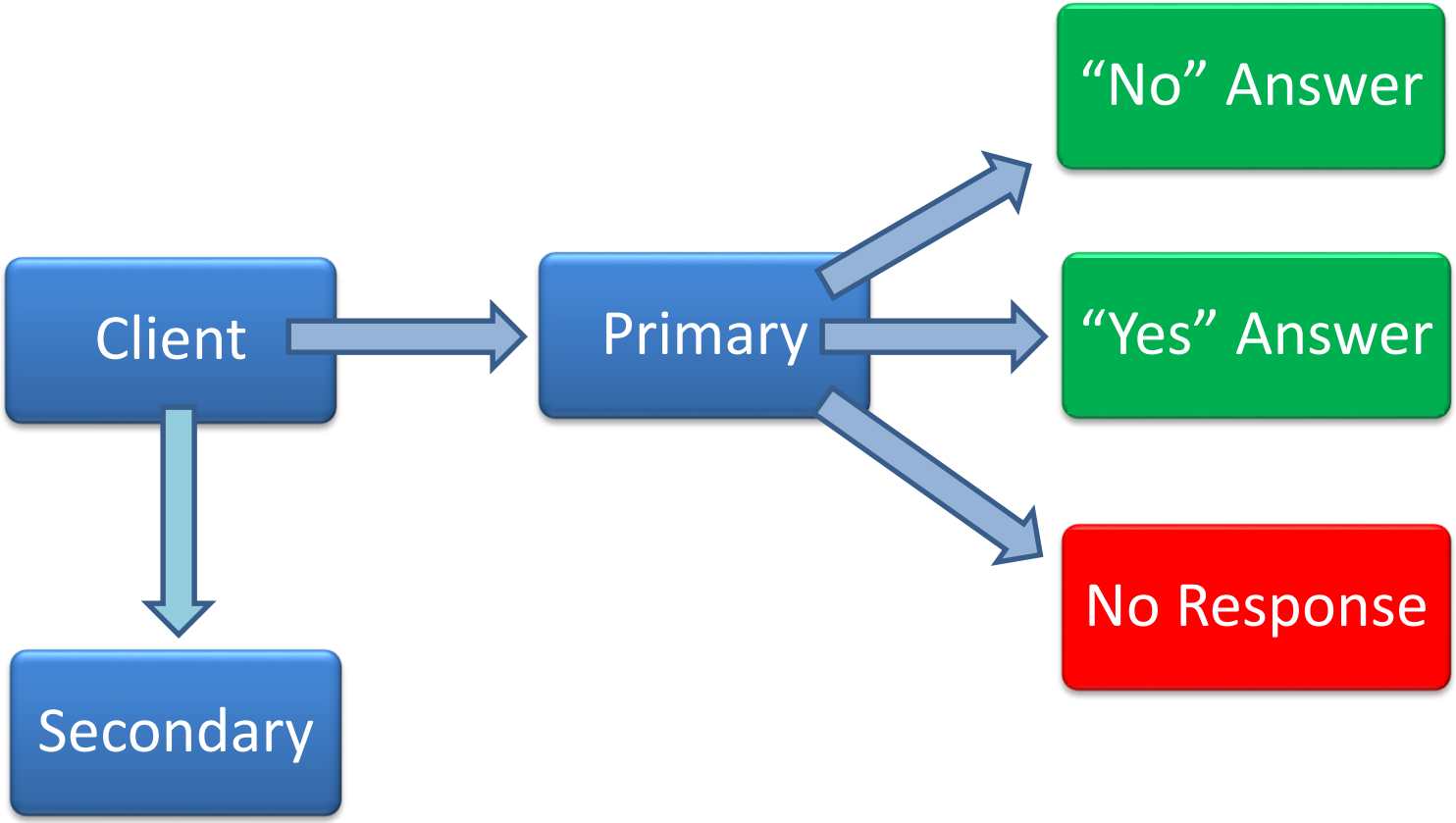
DNS

- Can DNS Trick Us? **YES**

- Slow Replication
- Multiple HOST (A) Records for a single IP → Auto PTR
- Multiple Alias (CNAME) Records for a single HOST (A)
- Split DNS
  - AD DNS Domain Name does match company's DNS domain name
  - Always use the AD DNS Name (Kerberos)

DNS

- Don’t rely on the secondary DNS server
- Primary & Secondary should resolve all names



DNS

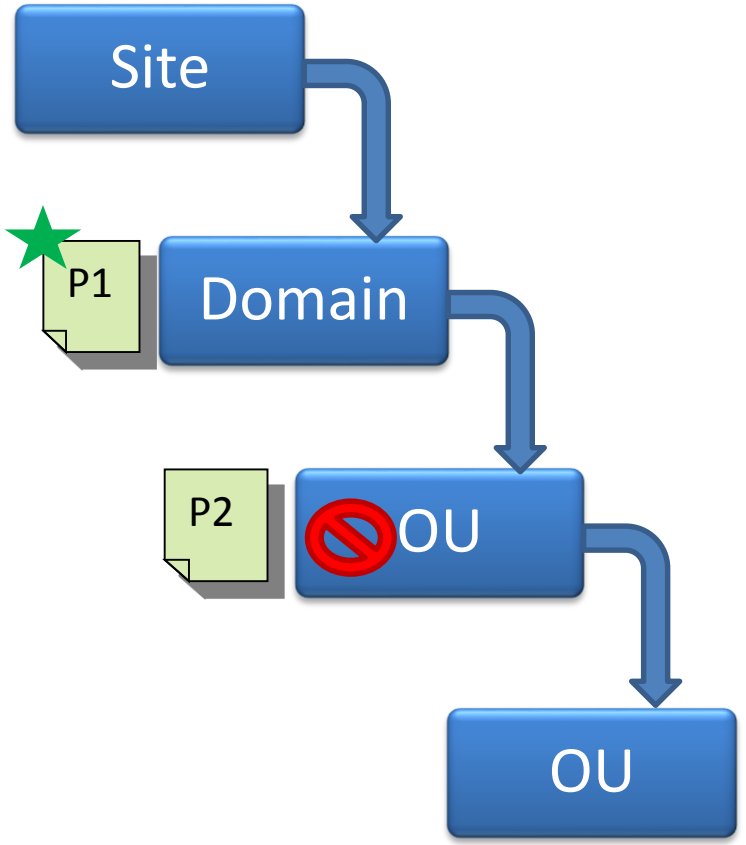
- DNS Suffix Search Order
  - Appended to NetBIOS if no broadcast response
  - Suffixes are appended in order
  - Not needed if FQDN is used

Group Policy

- What are they?
- Where can they be applied?
  - Site
  - Domain
  - OU
- How can they be filtered?
  - Object Type
  - Security Groups
  - WMI

Group Policy

- Precedence
  - Lower Level Wins
  - Block Policy Inheritance
  - No Override
    - Wins over lower levels
    - Wins over a block



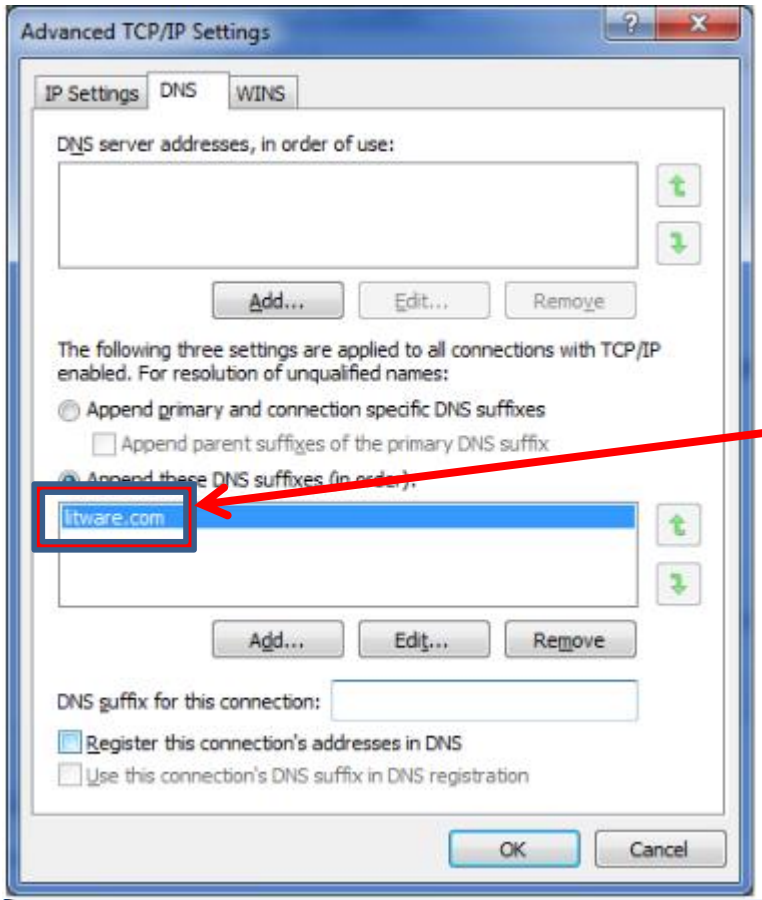
Group Policy

- What can they do?

Software Install	Large Pages
Startup/Shutdown Script	Registry Settings
Login/Logoff Scripts	File System Permissions
System Services startup type	IPSec Policies
System Services Permissions	Windows Update Settings
Power Plans and CPU Usage	Instant File Initialization
Lock Pages in Memory	Firewall Settings

Group Policy

- Contoso.com set via GPO
- Litware.com set on client
- Contoso.com set via GPO

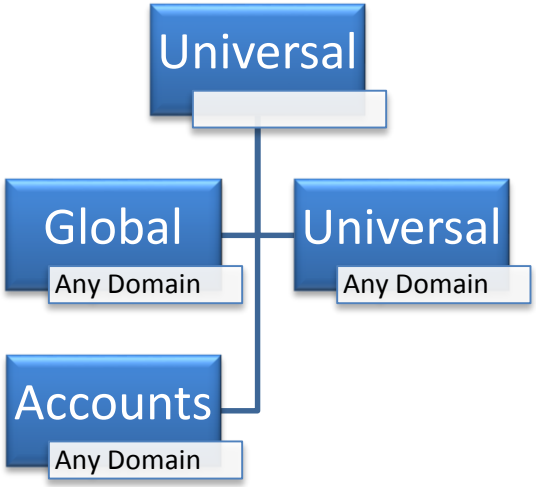


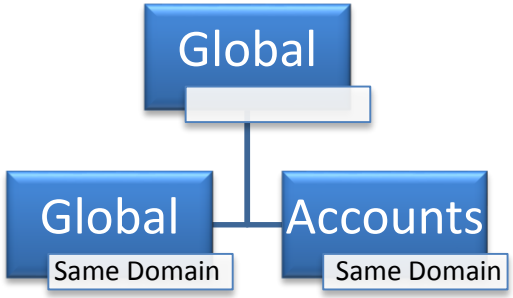
Security Groups

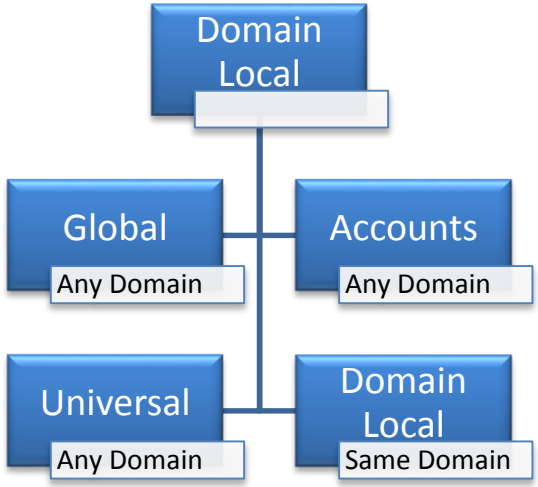
- Types
  - Global
  - Domain Local
  - Universal
    - Make sure you have a GC in the site
    - Or make the site has GC caching

Security Groups

- Nesting
  - Keep Recursive Membership in mind
  - Kerberos Token Access Size
    - Limited to 1024 SIDs
    - Default is 12k and max is 65k







Security Groups

- Who has access to your DB files?
  - Verify NTFS File Permissions
  - Don't use a Deny ACE
    - Best Practice is to simply omit the ACE
  - Check inheritance at the folder level
  - Check inheritance at the file level

TIP

You can have access to a file without having access to the folder it is in.

Password Policy

- Windows Authentication
  - Settings Determined by Default Domain Policy
- SQL Authentication
  - Settings Determined by Local Policy
  - Can be overridden by GPO
  - SQL Auth Accounts adhere to this policy
    - Enforce Password Policy (Complexity)
    - Enforce Password Expiration

SQLAgent

The job failed. Unable to determine if the owner (domain\username) of job MYJOB has server access (reason: Could not obtain information about Windows NT group/user 'domain\username'.

- Jobs will fail if the job owner cannot be found
  - Use a SQL Account
  - Has nothing to do with job security context
  - Account can be disabled

- Jobs run under the context of the SQLAgent Service Account
  - Unless credentials are defined in a job step

TIP

Credentials and proxy accounts don't work if SQLAgent Service is using a UPN.

Kerberos

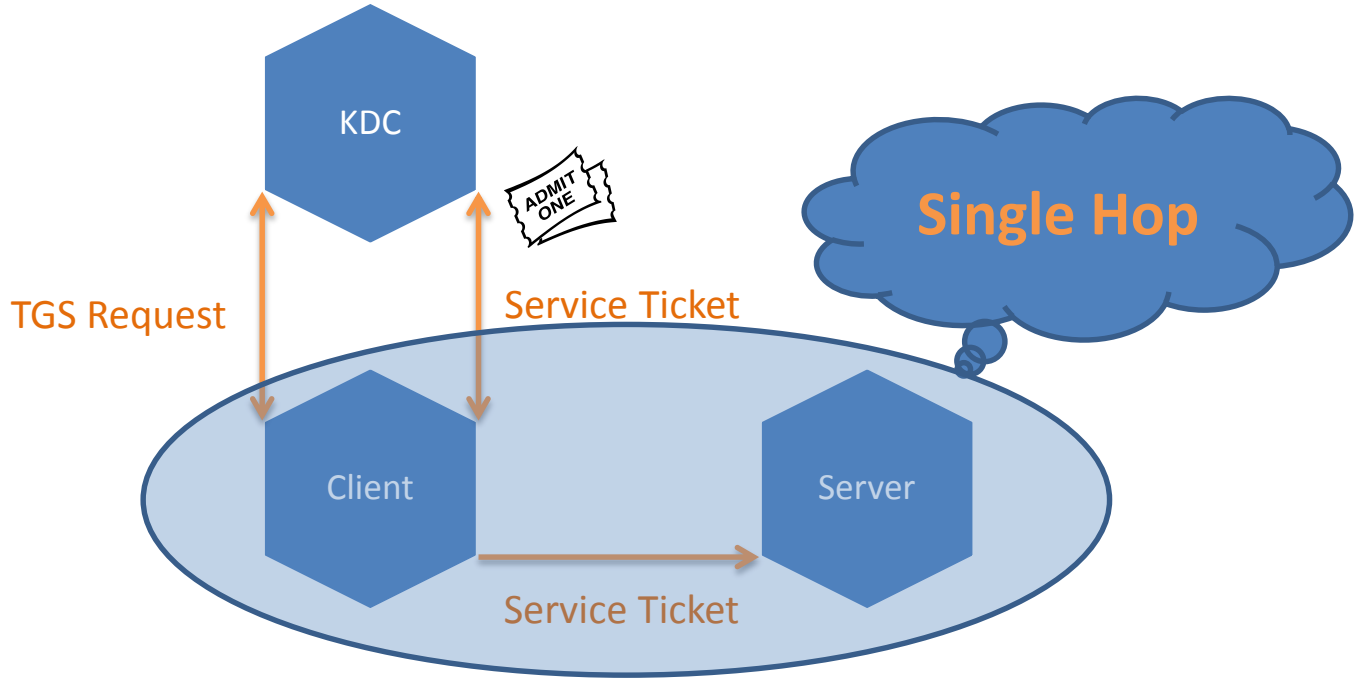
- Requirements
  - Server and client must be in same or trusted domain
  - SQL Server must use TCP/IP
    - Names Pipes allowed starting in SQL 2008
  - SQL Server's SPN must be registered in AD
  - SPNs must be unique
    - However, AD allows for duplicates

Kerberos

- Why should I use Kerberos over NTLM?
  - Mutual Authentication
  - Faster Authentication
  - Domain Trust Enhancement
  - Delegated Authority

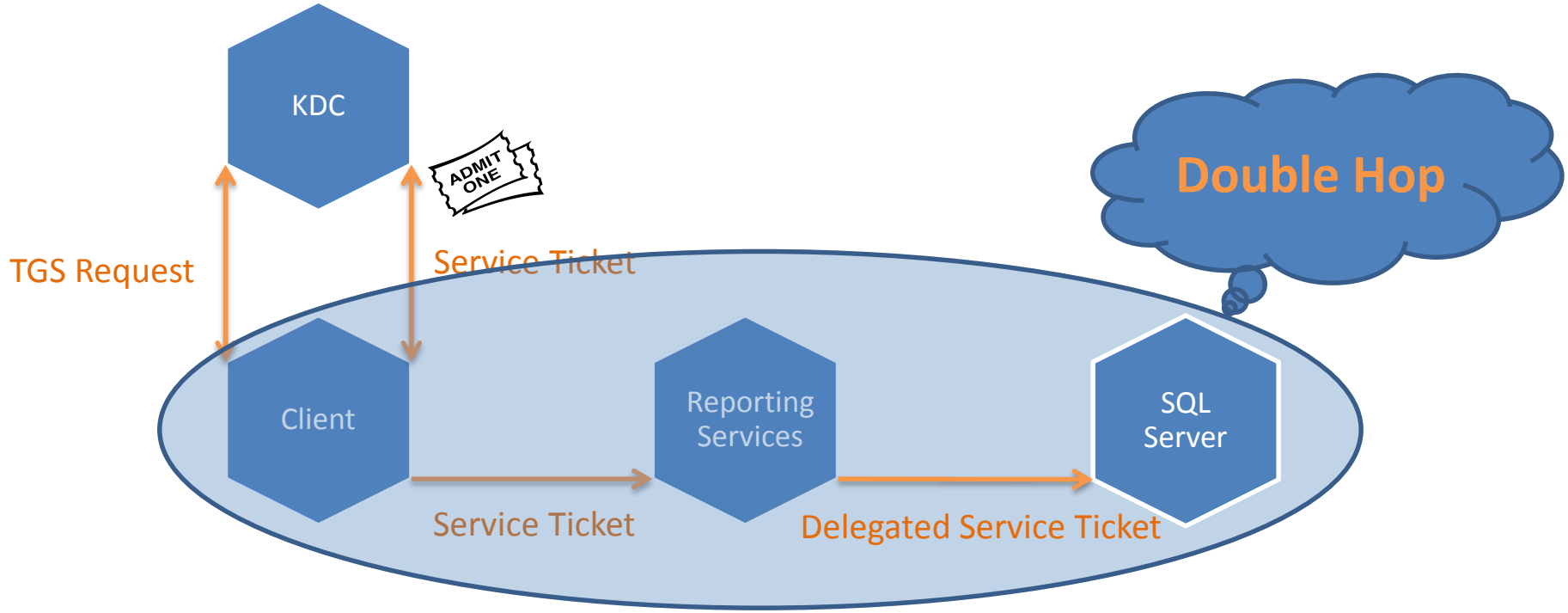
Kerberos

- How does it work?
  - Client authenticates to KDC
  - Client Requests a Service Ticket from KDC
  - Client presents Service Ticket to resource server



Kerberos

- How does delegation work?
  - Same as single hop, but one or more steps further
  - Distributed Reporting Services Solution



Kerberos

- Service Principal Names
- Register Manually
  - You have to figure out the SPN yourself
  - You need permissions on the account in AD
- Register Dynamically
  - Permissions not granted by default for SELF on account
    - Write Public Information
    - Write servicePrincipalName
    - Validated write to servicePrincipalName

Kerberos

- SPN Method Comparison
  - Dynamic registers/unregisters with SQL Service start/stop
    - AD replication can come into play
  - Due to replication dynamic is not recommended for clusters
    - Site topology and Urgent Replication can mitigate this

Versus

- Manual means intervention required if server name changes
- Manual means you can add an SPN for NetBIOS

Kerberos

- What should my SPN look like?
  - Default instance registered by SQL Service
    - TCP Connections
      - MSSQLSvc/FQDN:Port
    - Named Pipes Connections
      - MSSQLSvc/FQDN
  - Is this how I should do it for my manual registrations?
    - Yes, but also add SPNs for the NetBIOS name
      - MSSQLSvc/NetBIOS:Port
      - MSSQLSvc/NetBIOS

Kerberos

- Service Principal Names

- Where should they go?
  - SQL Server Service running under domain account

    Domain Account

  - SQL Server Service running under the following:
    - Local System
    - Local Service
    - Network Service

    AD Computer Account

Kerberos

- Troubleshooting Tools

- Klist.exe
- Kerbtray.exe
- SETSPN.exe
- Kerberos Configuration Manager

Summary

- ❑ DNS
- ❑ Group Policy
- ❑ Security Groups
- ❑ Password Policies
- ❑ SQLAgent
- ❑ Kerberos

Ryan Adams
Blog - http://ryanjadams.com
Twitter - @ryanjadams
Email – ryan@ryanjadams.com