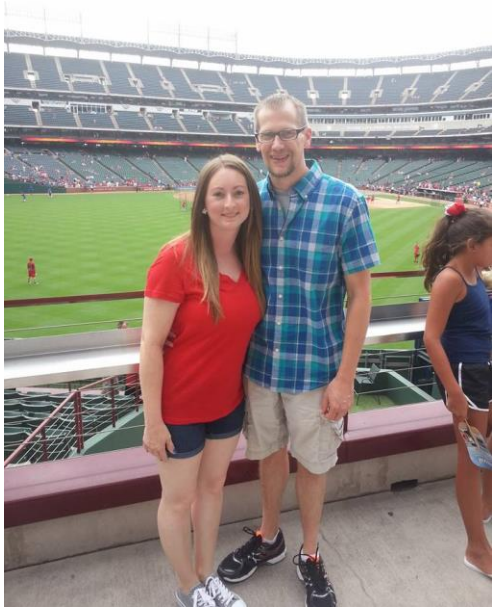
Active Directory & SQL Server

How AD can affect your SQL Servers

Ryan Adams

Ryan Adams

Microsoft Senior PFE



MCT

IT/Dev CONNECTIONS

Microsoft® Most Valuable Professional

PASS SUMMIT 2016
October 25-28
Seattle, WA
I'M SPEAKING
Where Data Professionals Connect, Share, and Learn

PASS SQL saturday

@ryanjadams

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

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

Objectives

- ❑ AD Topology
- ❑ DNS
- ❑ Group Policy
- ❑ Security Groups
- ❑ Password Policies
- ❑ Trusts
- ❑ SQLAgent
- ❑ Kerberos

Topology

- Sites – What are they?
- Sites – What you need to know
  - In what site is your SQL Server
  - How far away is the furthest DC in the site
  - Does the site have a Global Catalog
  - How far away is the furthest GC in the site
  - Does the site have a Read-only Domain Controller
    - If so, how far away is the closest writeable DC

Topology

- Forests – What are they
- Forests – What you need to know
  - In what forest is your SQL Server located
  - Are there any other forests in your network
  - If so, are those forests trusted
  - Are you contacting servers in another forest
    - Becomes important with Kerberos
    - You have to follow the trust path

Topology

- Domains – What are they?
- Domains – What you need to know
  - In what domain is your SQL Server
  - Where is located in the hierarchy
    - Becomes important with Kerberos
    - You have to follow the trust path
  - Do not get them confused with DNS Domain Names

DNS

- Always use Fully Qualified Domain Names
- What not NetBIOS?
  - NetBIOS is broadcast traffic and not normally routed
- Why not HOSTS?
  - HOSTS files are not dynamic

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

- Can DNS Trick Us? **YES**

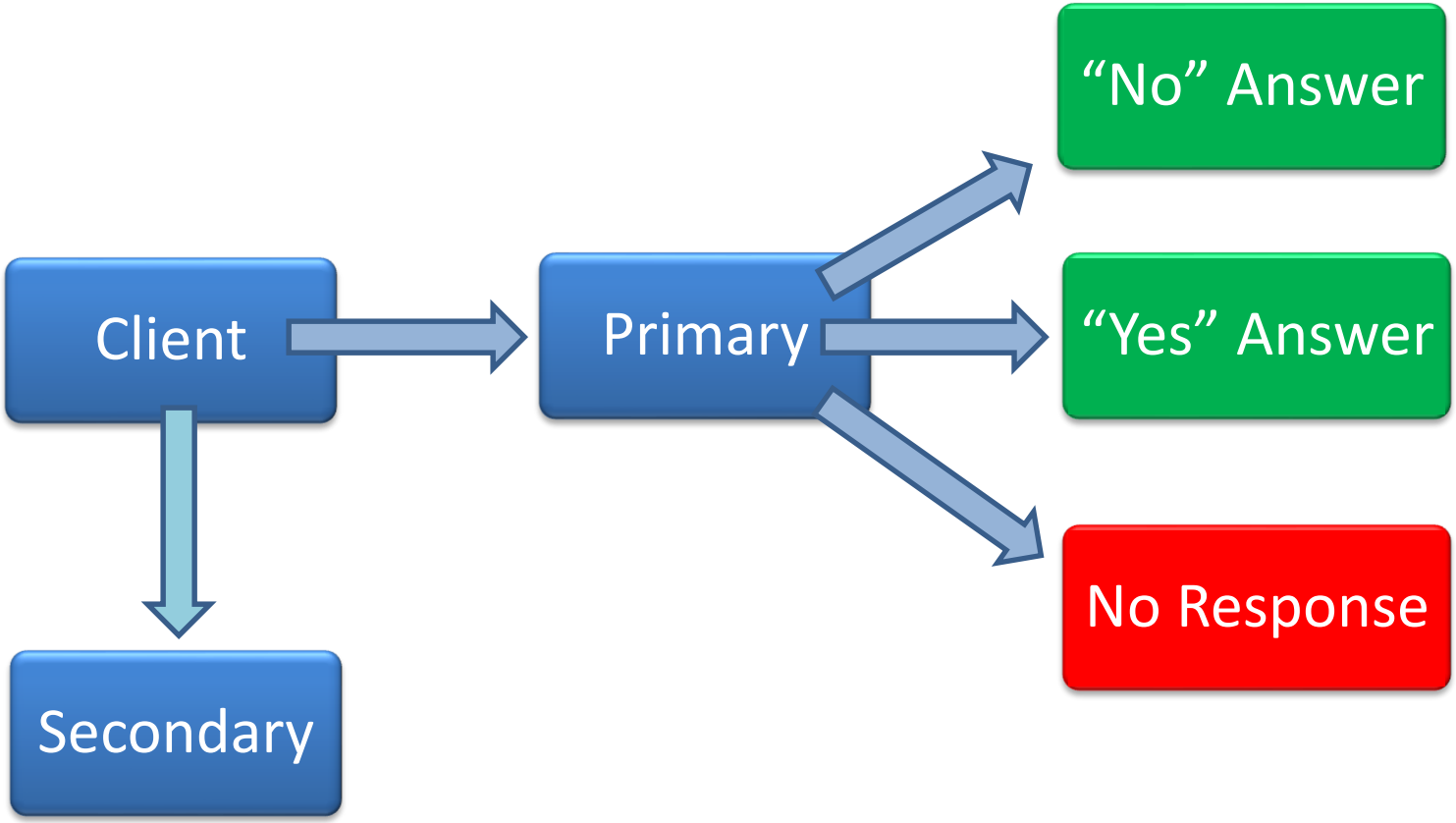
- Delegated DNS Namespace
  - Corporate DNS delegates a subdomain to AD DNS
  - Know your topology
  - Understand security boundaries
    - DNS domain name does not match AD domain name
    - Important with Kerberos

DNS

- Server Location
  - Which DCs are DNS servers
  - How far away is the closest DNS server
  - What zones does it host?
  - For what zones does it have forwarders

DNS

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



DNS

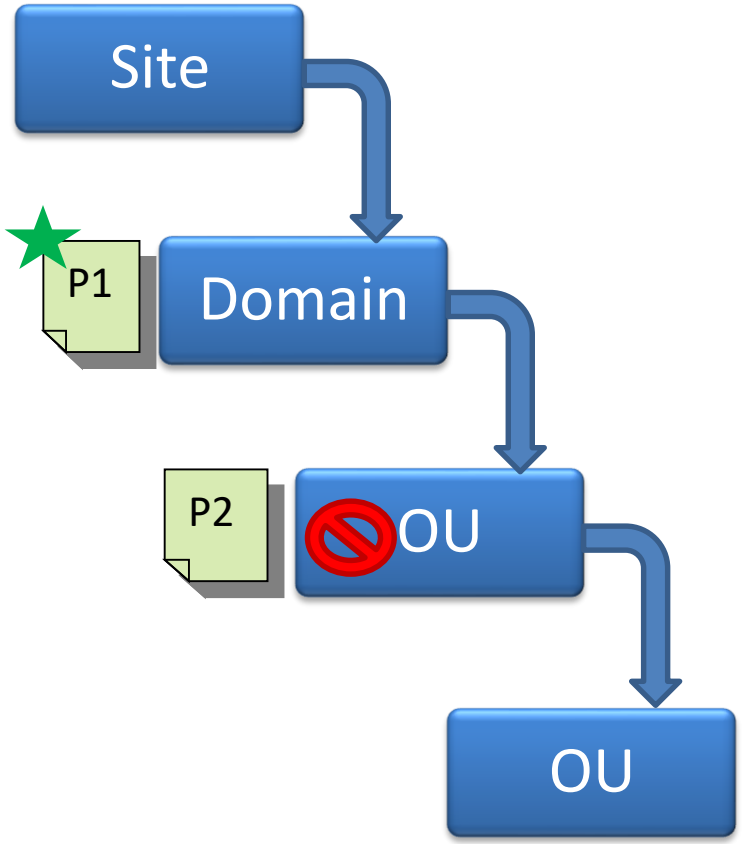
- DNS Suffix Search Order
  - Appended to NetBIOS if no broadcast response
  - Suffixes are appended in order
  - Not needed if FQDN is used

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?

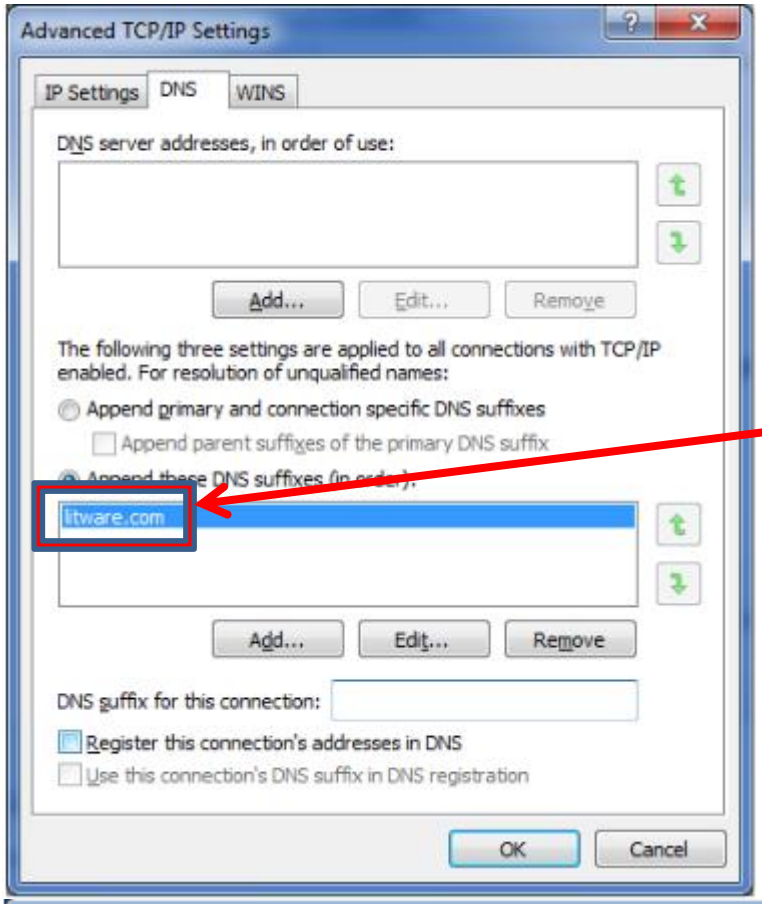
Software Install	Large Pages
Startup/Shutdown Script	Registry Settings
Login/Logoff Scripts	File System Permissions
System Services startup type	IPSec Policies
System Services Permissions	Windows Update Settings
Power Plans and CPU Usage	Instant File Initialization
Lock Pages in Memory	Firewall Settings

Group Policy

- Troubleshooting Tools
  - GPMC.msc – Group Policy Management Console
  - RSOP.msc – Resultant Set of Policies
  - GPResult.exe – Group Policy Result
  - GPUpdate.exe – Refresh/Reapply Policies

Group Policy

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

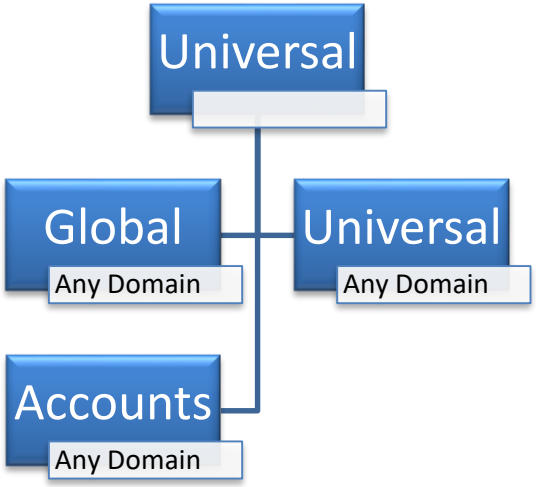


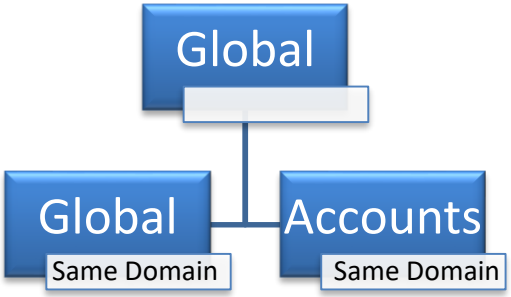
Security Groups

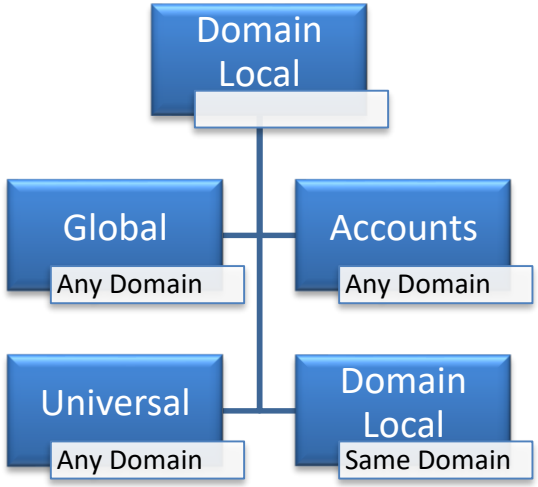
- Types
  - Global
  - Domain Local
  - Universal
    - Make sure you have a GC in the site
    - Or make the site has GC caching

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

Password Policy

- Managed Service Accounts
  - Introduced with Windows Server 2008 R2
  - Application Service Account Managed by AD
  - Can manage it'sCan manage it's own own password
  - SPNs
  - Disallowed Interactive Logon

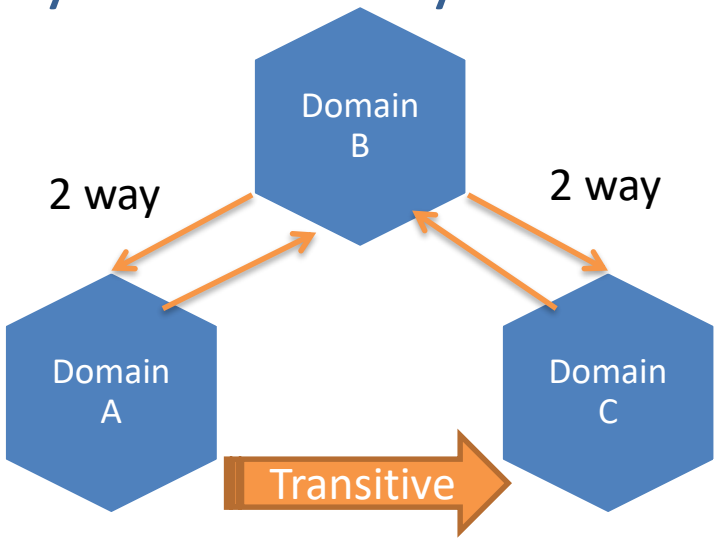
- The Problem
  - Did not support SQL Server
  - Cannot be used with Clusters

Password Policy

- GROUP Managed Service Accounts
  - Introduced with Windows Server 2012
  - Same features as an MSA in Server 2008 R2
  - Supports SQL 2012
  - Supports Clustering
- Requirements
  - Windows Server 2012 Schema
    - Functional level not required but no auto SPNs
  - Client must be Windows Server 2012
  - .NET Framework 3.5
  - AD PowerShell Snap-in

Trusts

- Trusts – What are they?
- By default they are two way and transitive



- You need to know your locations and your users' location
  - Can help you identify slow authentication issues
  - Trust hierarchy must be followed (Kerberos)
  - Shortcut trusts

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
  - Has nothing to do with job security context
  - Use a SQL Account
  - 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

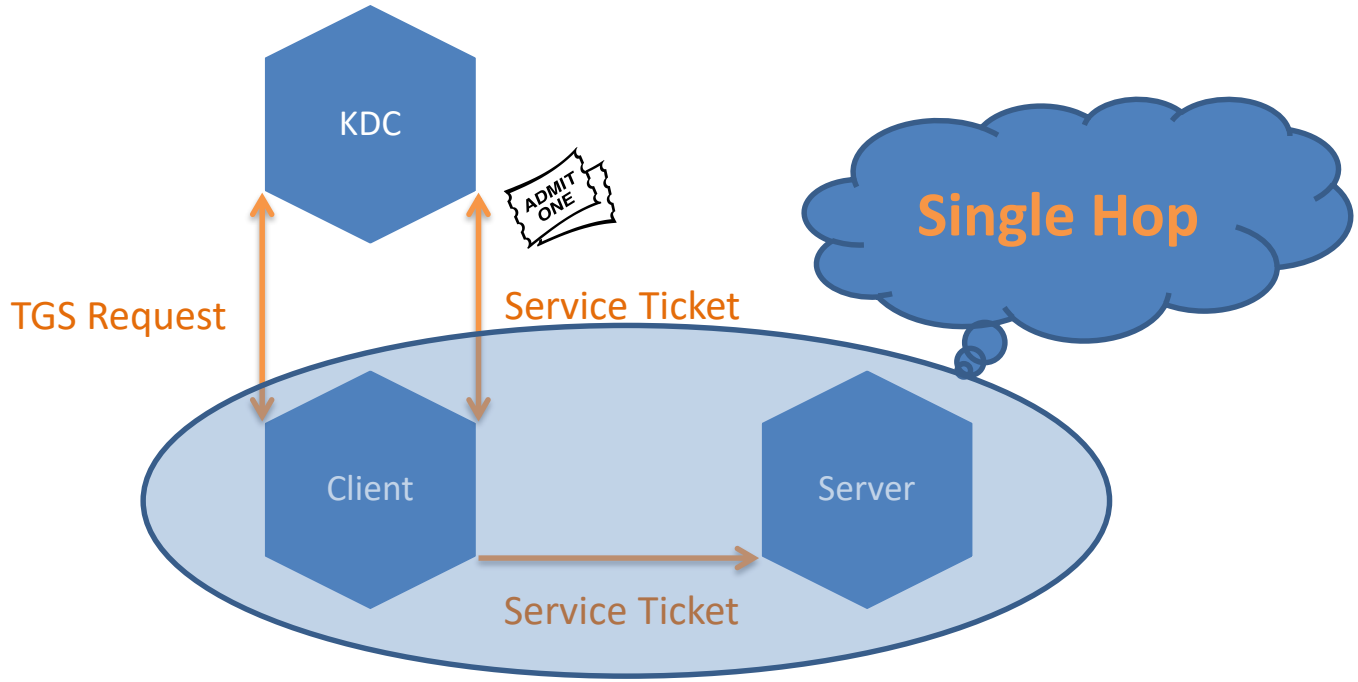
- Requirements
  - Server and client must be in same or trusted domain
  - SQL Server must use TCP/IP
    - Names Pipes allowed starting in SQL 2008
  - SQL Server's SPN must be registered in AD
  - SPNs must be unique
    - However, AD allows for duplicates

Kerberos

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

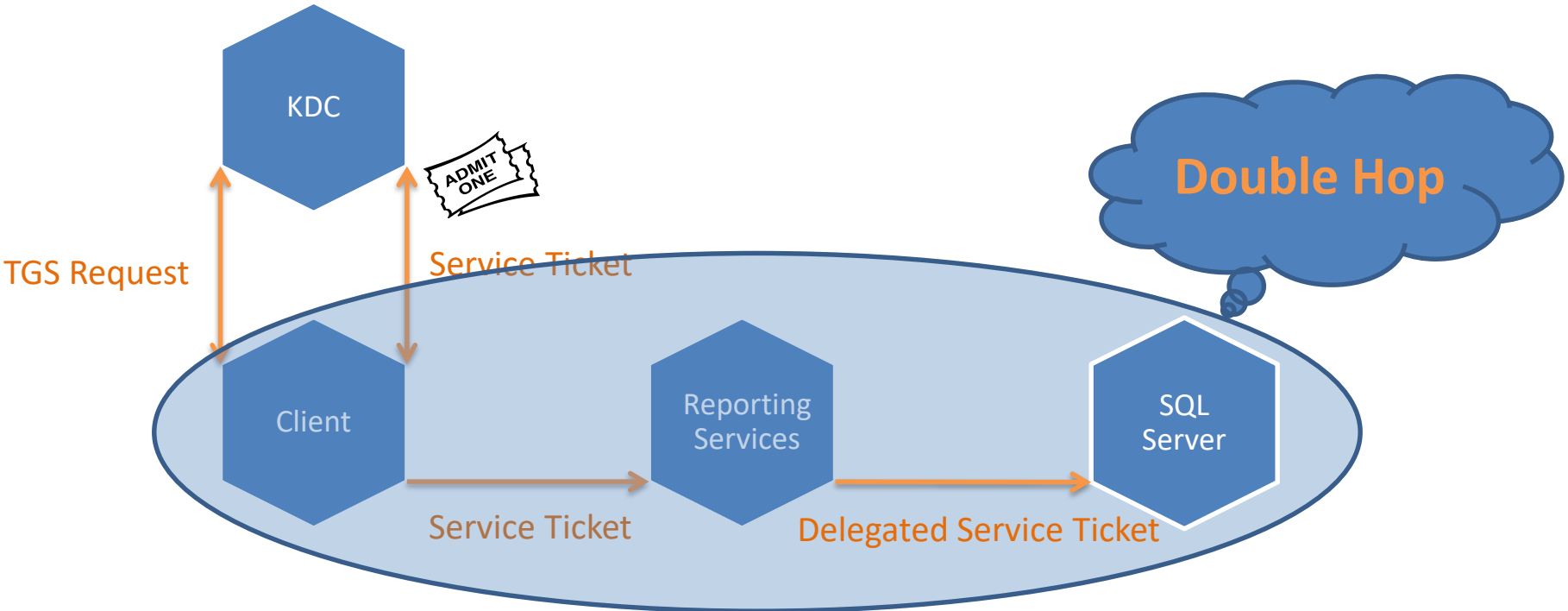
Kerberos

- 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

- Is my SQL Server using Kerberos or NTLM?

```
SELECT auth_scheme FROM sys.dm_exec_connections
WHERE session_id=@@SPID
```

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

- Case Study: Urgent Replication Impact

Partition	Before	After
EMEA	24:25	00:48
Asia Pacific	09:28	00:51
North America	25:35	00:58
Forest Wide	58:04	02:57

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

- GPOs Strike Again!

- 5 Kerberos settings governed by Domain Policy GPO
  - Enforce User Logon Restrictions
  - Maximum Lifetime for Service Ticket
  - Maximum Lifetime for User Ticket
  - Maximum Lifetime for User Ticket Renewal
  - Maximum Tolerance for Computer Clock Sync

Kerberos

- Troubleshooting Tools

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

Summary

- ❑ AD Topology
- ❑ DNS
- ❑ Group Policy
- ❑ Security Groups
- ❑ Password Policies
- ❑ Trusts
- ❑ SQLAgent
- ❑ Kerberos

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