Security Essentials for SQL Server 2012 & SharePoint 2010 BI

Who am I?

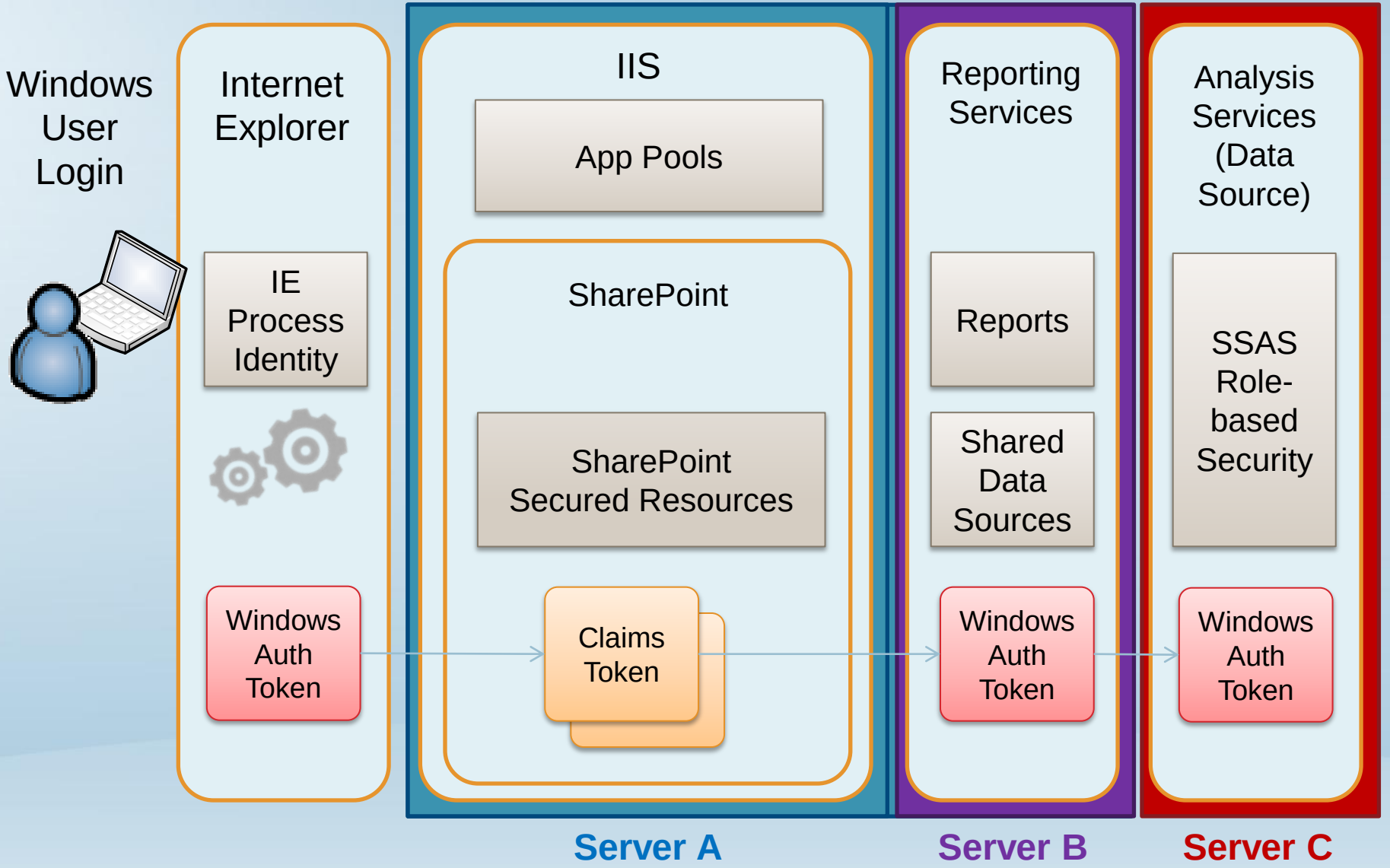
Paul Turley

Mentor, SQL Server MVP

pturley@SolidQ.com

SqlServerBiBlog.com

Authentication Boundaries



Configuration Steps

- Plan hardware & services architecture
- Plan service account assignments
- Create accounts
- Configure Claims to Windows Token Service
- Add service principal names
- Configure delegation
- Add data sources

Kerberos & Constrained Delegation

- Configuring Kerberos is uncomplicated as long as you get it right the first time
- Make checklist and validate each step
- Troubleshooting & fixing can be more complicated

Services & Principals

- SharePoint
- SQL Server
- Analysis Services
- Reporting Services
- Claims-to-Windows Token Service

Create Domain Service Accounts

- Each service will impersonate a user with another service
- One principal for each service or app pool (production)
- Consolidate (for dev/demo environments)

Service Principal Names

- Syntax:
  setspn –S <service name> <principal name>
- Set a SPN for both the principal fully-qualified & NetBIOS name

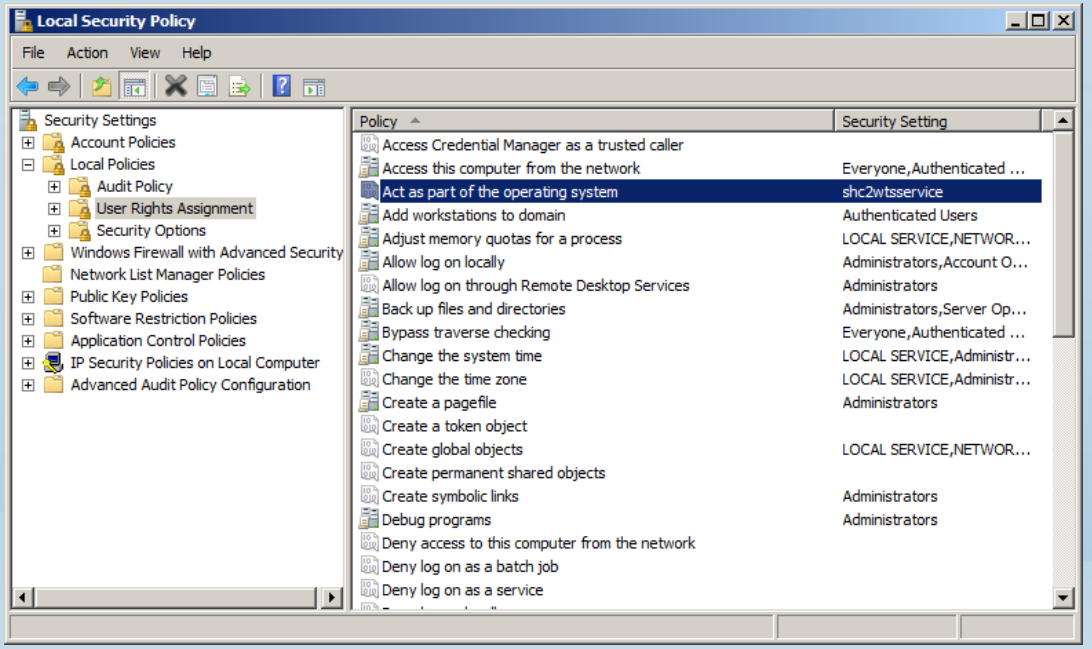
```
C:\>SetSPN -S http/Teams vmlab\svcTeamsApp

Checking domain DC=VMLab,DC=local
CN=svcTeams10App,OU=014,OU=Service Accounts,DC=VMLab,DC=local
        HTTP/Teams.vmlab.local
        HTTP/Teams
```

Service Names for SPNs

SharePoint	http/<hostname>
SQL Server (relational)	mssqlservice/<server>:1433
Analysis Services	msolapsvc.3/<server>
Reporting Services	sp/reportservice
PerformancePoint	sp/performancepointservice
Excel Services	sp/exelservices
PowerPivot	sp/powerpivotservice
Claims to Win Token Svc	sp/claimstowindowstokenservice

Configuring Claims to Windows Token Service

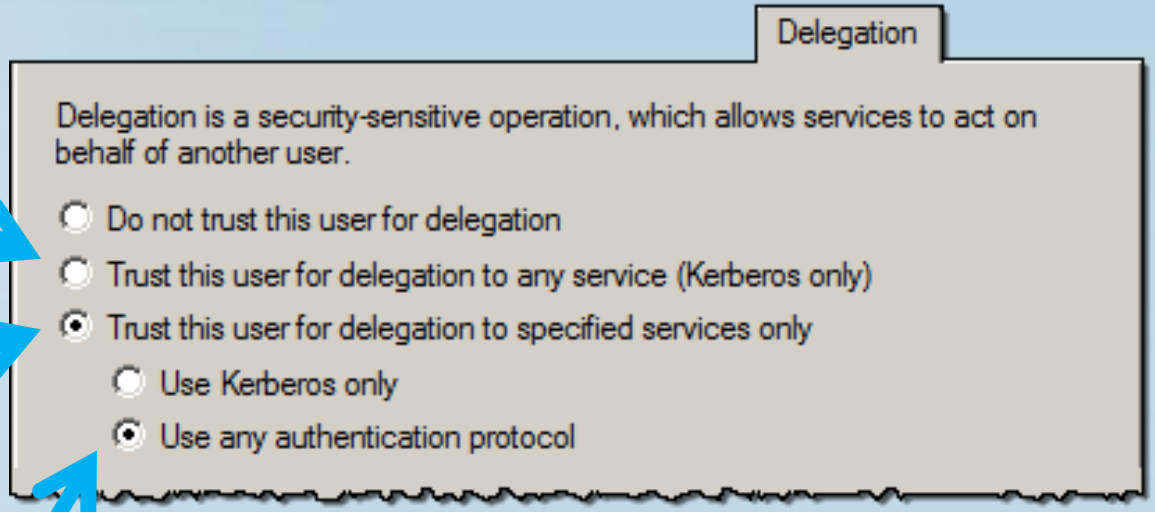
- Runs on every machine running a SharePoint managed service
- Uses local service account by default
- Change to run as a domain account in the local administrator group
- Set local policies:
  - Act as part of the operating system
  - Impersonate a client after authentication
  - Log on as a service



Delegation Options

Basic Delegation
Not supported in most SQL Server 2012 scenarios

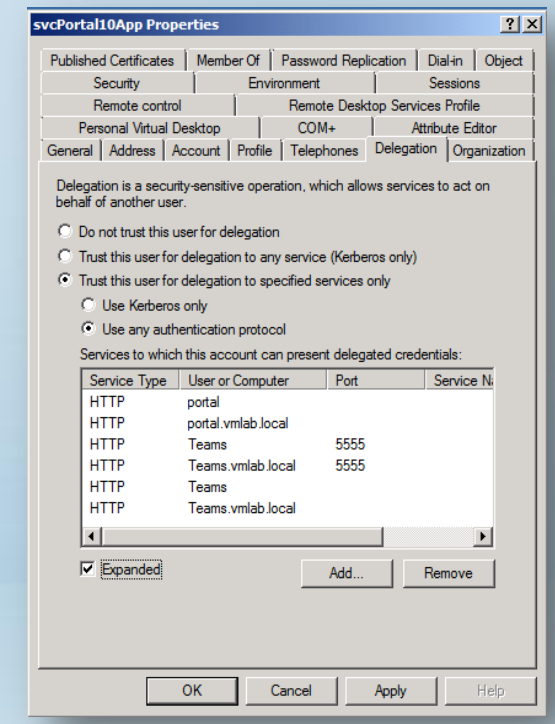
Constrained Delegation
Recommended

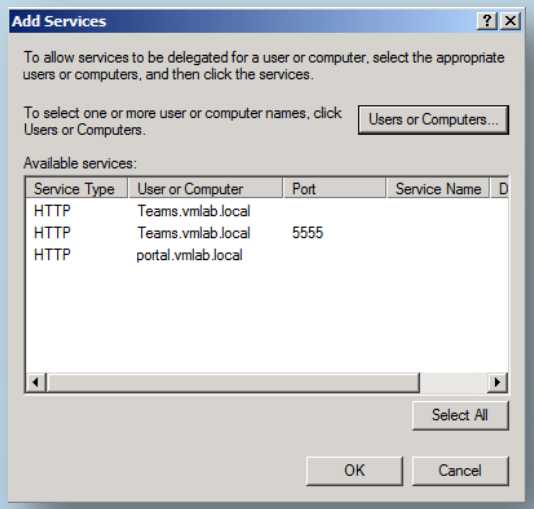


- Claims
- Kerberos
- NTLM

Constrained Delegation

- Tells OS to trust user for delegation to a list of specific services
- After SPN created, shows Delegation tab on AD User dialog





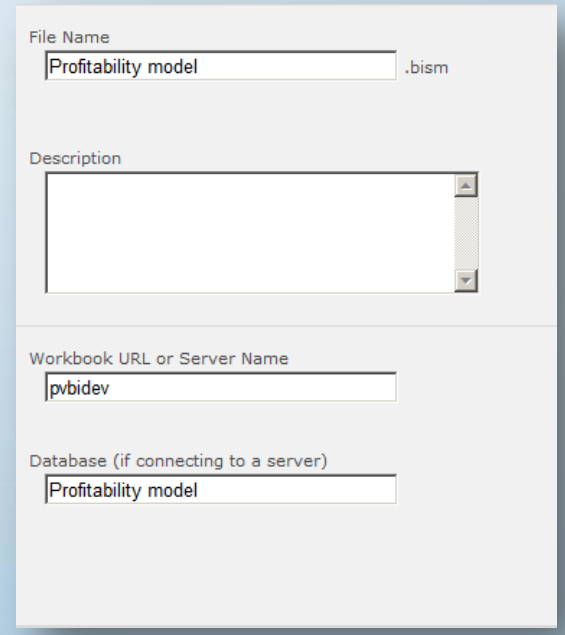
Troubleshooting

- Watch out of caching
  - Changes may not be applied right away
  - Error conditions may be persisted
  - No silver bullet method to clear cached settings
- Reboot after changes (if no effect)
- Use SQL Server Profiler trace to check for account names & connection events

Connection Options

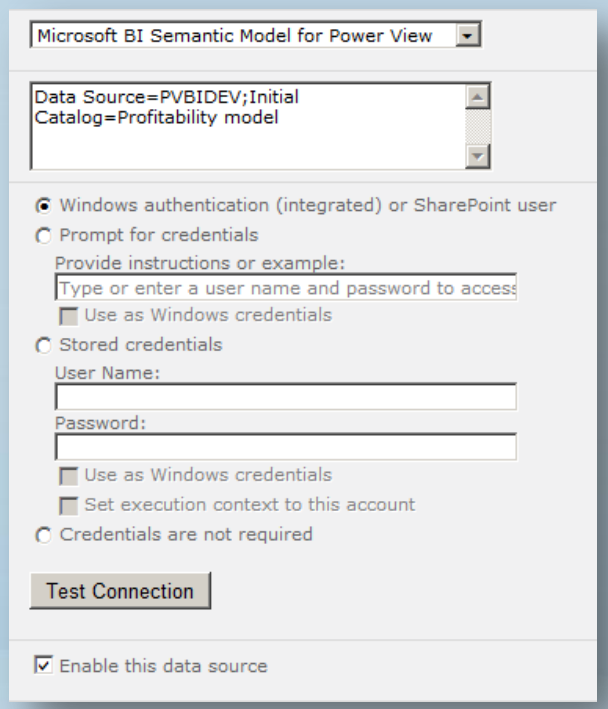
BISM Connection file

- Simple
- Specialized



RSDS report connection

- Flexible



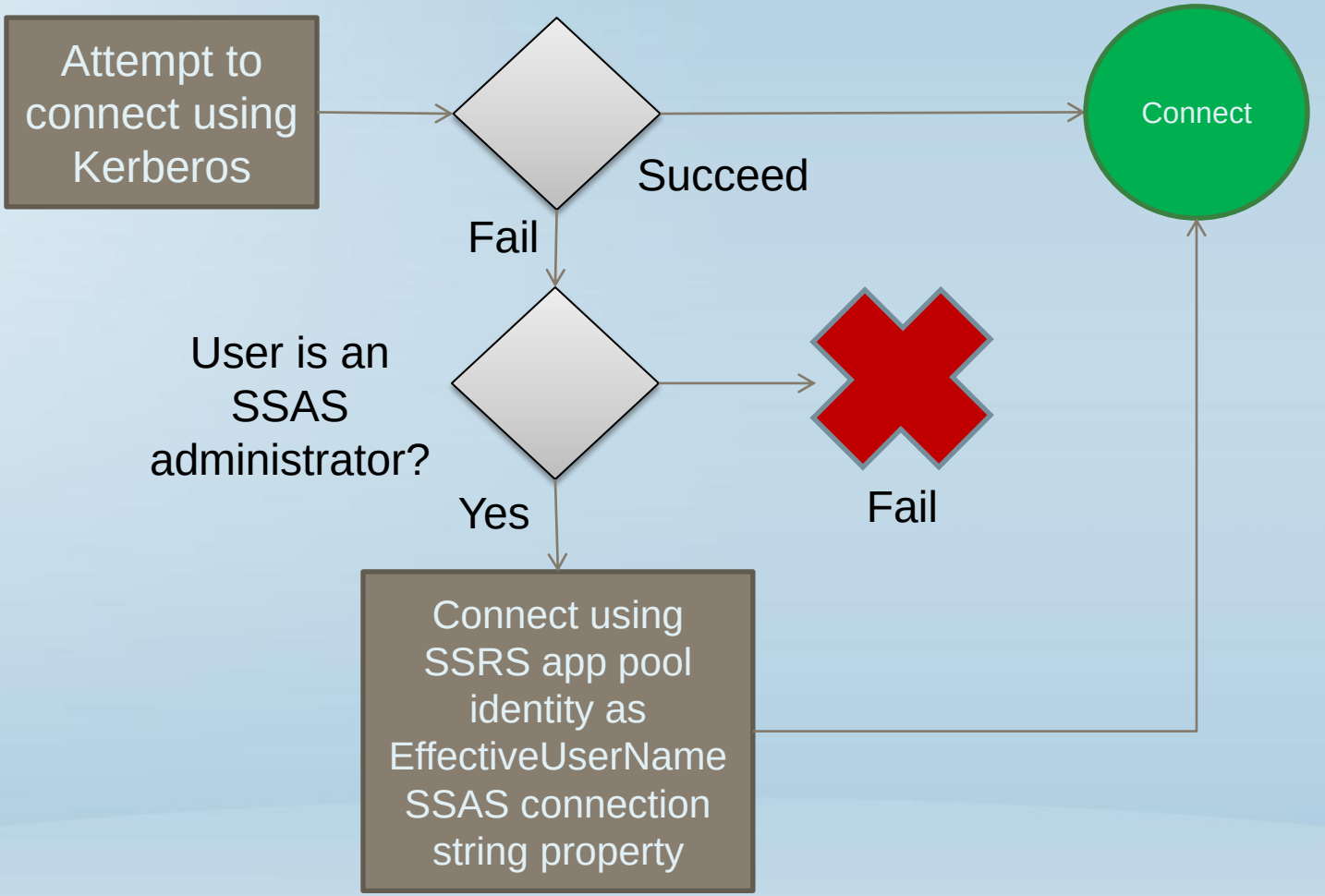
BISM Connection File

- Only connects to a tabular data source
- Use the URL for a .bism file in a connection string in place of the server name for any SSAS client
  - Uses EffectiveUserName

RSDS Connections

- Natively used by Reporting Services
- Can be used by Power View
- Credential options:
  - Windows authentication
  - Prompt for credentials
    - not supported by Power View
  - Stored Credentials
    - Always check Use Windows credentials for SSAS sources
    - Set execution context (passes user name in EffectiveUserName property)

Connection to SSAS with a BISM Connection File



The Comprehensive Reference

- SQLCAT.com
- 244 pages of pure bliss

Microsoft

Microsoft® SharePoint®

Configure Kerberos Authentication for SharePoint 2010 Products

Microsoft Corporation

Published: July 2010

Author: Tom Wisnowski. **Contributors:** Philippe-Joseph Arida, Luca Bandinelli, Kevin Donovan, Pej Javaheri , Denny Lee, Cephas Lin, Dave Manning, Carl Rabeler, Prash Shirolkar, Norm Warren, Josh Zimmerman. (itspdocs@microsoft.com)

Abstract

This document gives you information that will help you understand the concepts of identity in Microsoft SharePoint 2010 Products, how Kerberos authentication plays a very important role in authentication and delegation scenarios, and the situations where Kerberos authentication should be used or may be required in solution designs. Scenarios include business intelligence implementations which secure access to external data sources such as SQL Server. The document also shows how to configure Kerberos authentication end-to-end within your environment, including scenarios that use various service applications in Microsoft SharePoint Server. Additional tools and resources are described to help you test and validate Kerberos configuration.

Modeling Considerations

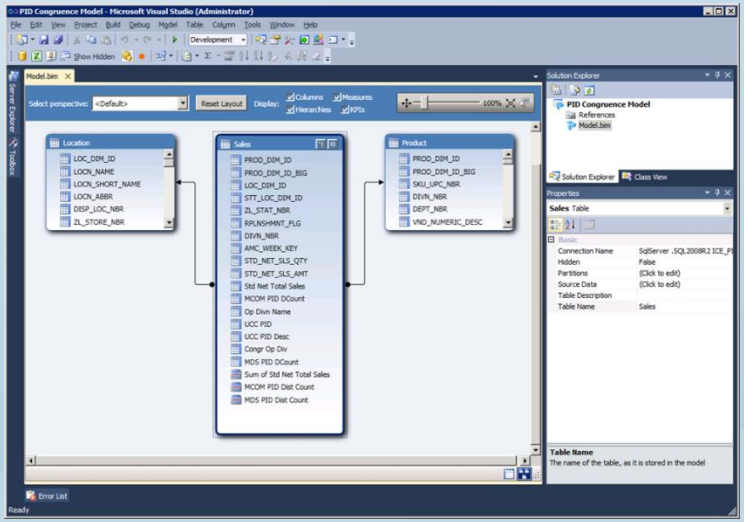
Finding the "Perfect" Modeling Platform

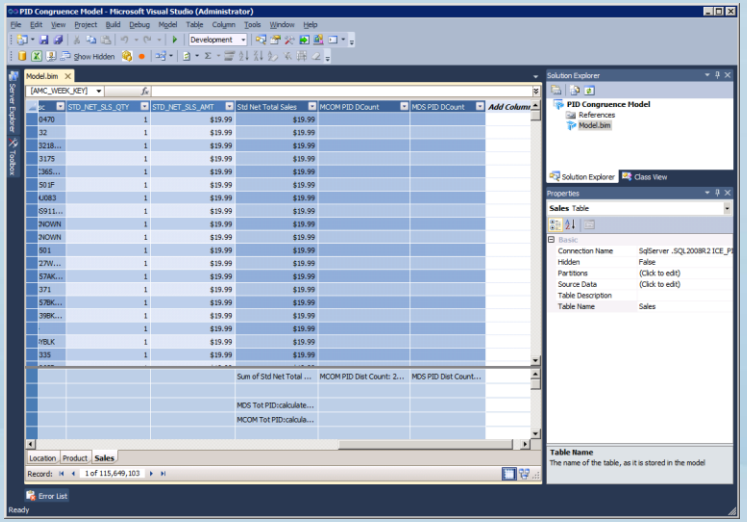
- Why Vertipaq?
- ~~Vertipaq vs UDM~~
- Tabular vs Multidimensional
- "BISM"
- Vertipaq is an impressive technology!
  - Can be less-complex than multidimensional
  - Can be faster than multidimensional (in the right scenarios)
  - Will eventually be as/more flexible than multidimensional
  - **We will break it**

Case Study

Solving Conditional Distinct Count performance

- UDM architectural limitations
- PowerPivot & tabular model
- Partitioning (CTP2 > CTP3)
- Hardware requirements





Tabular Model & Design Environment

- PowerPivot & Tabular models
- Analysis Services instance in Vertipaq storage mode
- Workspace & deployment target database
- Development environment
- Model project structure
- Migrate PowerPivot vs. create new model project

Modeling 101

- Import tables vs queries
- Use data sources views where possible
- Remove unwanted columns liberally
- Rename & use friendly names
- Date keys: datetime or int
- Role-playing dimensions:
  - One is active
  - Others activated through DAX
  - Make copy

Model Designer

- Graphical or Tabular
- Intuitive drag-and-drop relationships
- Excessive columns & relationships can slow graphical modeler

Demo

(time permitting)

Thank You