Building hybrid applications using Windows Azure

Deepak Babu

Partner Technical Consultant – Microsoft

debabu@microsoft.com

Introduction

- Hybrid applications
  - Benefits
  - Challenges
- Windows Azure
  - SQL Data Sync
  - Service Bus
  - Connect
  - Access Control Service
- Demonstrations

Hybrid Applications

What is a hybrid application?

- Uses a range of components, resources, and services that are separated across:
  - Geographical boundaries (data centre or organisational)
  - Network boundaries (Internet and intranet)
  - Trust boundaries

- See http://msdn.microsoft.com/en-us/library/hh868043

Benefits

- Cost savings using in-the-cloud compute, storage, and network
- Federated identity
- Insurance against data loss using data replication
- Availability
- Scalability

Why a hybrid application?

- An on-premises application or service might be end-of-life or it cannot be migrated to the cloud
- Data might be shared with on-premises applications and services
- Proprietary data might be required to be stored on-premises
- Regulated data might be required to be stored on-shore
- Sensitive data might be required to be stored on-premises

Challenges

- Access control
- Cross-boundary communication
- Data synchronisation
- Availability, performance and scalability
- Operations
- Infrastructure
- It is difficult to build hybrid applications without “Services”!

Windows Azure

What is Windows Azure?

- Provides a range of services that enable you to extend, migrate, and off-load applications, services, and data from on-premises to the cloud
- Provides the “fabric” technologies for building, deploying, and managing hybrid applications
- Superglues “Software” to “Services”

- See http://msdn.microsoft.com/en-us/library/windowsazure/dd163896.aspx

SQL Data Sync

What is SQL Data Sync?

- A cloud service for synchronising data between multiple databases in multiple directions spanning multiple geographies
- Implements a hub-spoke topology
- Synchronises data to and from the hub database, to the hub database only, or from the hub database only
- Synchronises data between multiple SQL Azure databases or between SQL Azure and SQL Server databases
  - SQL Server databases must SQL Server 2005 SP2 and later
- Synchronises data spanning the same data centre or spanning multiple data centres

SQL Data Sync

About SQL Data Sync

- Synchronisations are created, managed, and scheduled using Windows Azure Management Portal
- Synchronisation groups define the collection of SQL Azure and SQL Server databases to be synchronised
  - Are composed of a SQL Azure "hub" database and one or more SQL Azure or SQL Server “member” databases
  - Define databases, tables, and columns to be synchronised
  - Define rows to be synchronised
- Access to a SQL Server database is enabled by a client agent that can be installed on any Internet-connected computer
  - The client agent connects out to SQL Data Sync rather than SQL Data Sync connects in to it

Supported SQL Azure data types

Data type category	Supported SQL Azure data type
Exact numbers	**bit**, **decimal**, **int**, **numeric**, **smallint**, **tinyint**
Approximate numbers	**float**, **real**
Date and time	**date**, **datetime**, **datetime2**, **datetimeoffset**, **time**
Character strings	**char**, **varchar**, **text**
Unicode character strings	**nchar**, **nvarchar**, **ntext**
Binary strings	**binary**, **varbinary**, **image**
Spatial data types	**geography**, **geometry**
Other data types	**sql_variant**, **table**, **uniqueidentifier**, **xml**

Data security

- All accesses managed by SQL Data Sync are authenticated
  - A SQL Server database authenticates the client agent using Windows Authentication or SQL Server Authentication
  - SQL Data Sync authenticates the client agent using a shared secret
  - SQL Data Sync authenticates itself using certificates
- All connections managed by SQL Data Sync are encrypted
- All data managed by SQL Data Sync are encrypted

Conflict resolution

- A data conflict occurs when the same data in two or more databases in the same synchronisation group is changed between synchronisations
- When a conflict situation occurs, one of the changed rows is kept and the other ones are lost
- SQL Data Sync supports two conflict resolution types:
  1. Hub Wins: The first changed row written to the hub is kept
  2. Client Wins: The last changed row written to the hub is kept

DEMO – SQL Data Sync

Service Bus

What is Service Bus?

- A cloud service for highly-available, large-scale, and secure communication
  - Eventing, naming, and publishing
- Provides “relayed” messaging for connected scenarios
  - One-way, request/response, and peer-to-peer messaging
- Provides “brokered” messaging for temporal scenarios
  - Asynchronous, durable, publish-subscribe

About Service Bus

- Connects cloud, rich desktop, and Web-enabled (REST-based) device applications with on-premises services
  - .NET applications can integrate with Windows Communication Foundation (WCF)
- Integrates with Access Control Service for securing service endpoints
- On-premises services connect out to Service Bus rather than Service Bus connects in to them
- Provides a registry (an Atom 1.0 feed) for discovering service endpoints
- Supports tunnelling between two endpoints for bi-directional streams

Relay

Cloud Application
Web Role
Worker Role
Partner Application
Client
Service Bus
Relay
Firewall
On-Premises Application
WCF Service

Relay: support

- Supports a range of protocols
  - REST
  - SOAP
  - WS-*
- Supports a range of messaging patterns
  - One-way
  - Request/response
  - Peer-to-peer
- Supports a range of connections
  - Relayed
  - Hybrid
  - Direct

Relay: lifecycle

- Services are configured with WCF "relay" bindings
  - BasicHttpRelayBinding, WebHttpRelayBinding, WS2007HttpRelayBinding
  - NetTcpRelayBinding
- Services connect to the relay service using an outbound port
  - 80/HTTP, 443/HTTPS
  - 9350-4/TCP
- The relay service creates a bi-directional connection to a rendezvous URI
- Clients connect to the relay service
- The relay service "relays" messages from clients to services via the rendezvous URI

Relay: authentication

- Service Bus federates authentication with Access Control Service
  - Service Bus and ACS have a mutual trust
- Services are required to authenticate when connecting to Service Bus
  - Shared secret token
  - Simple Web Token (SWT)
  - SAML token
- Client can be required to authenticate when connecting to Service Bus
  - Services define this using the **RelayClientAuthenticationType** class

DEMO – Service Bus: Relay

Queues

Producer
Web Application
Mobile Application
Service
Service Bus
Queue
Consumer
Application or Service

Queues

- Queues provide first-in, first-out (FIFO) durable disconnected messaging
- Producers send messages to queues
- One or more "competing" consumers receive messages from queues
  - *Exactly Once*: ReceiveAndDelete
  - *At Least Once*: PeekLock, Complete or Abandon
  - *Time-to-live:* Expires messages, moving them to a special queue called *$DeadLetterQueue*
- Queues support "load leveling"
  - A fixed number of producers send messages at a faster rate
  - A variable number of consumers receive messages at a slower rate
  - The queue length expands/contracts over time
- Queues support sessions for grouping messages to be received by a single consumer
- Messages are sent with the **QueueClient** class
- Messages are received with the **QueueClient** class

Topics and subscriptions

Topics and subscriptions

- Topics and subscriptions provide once-in, many-times-out (publish/subscribe) durable disconnected messaging
- Producers send messages to topics
- Service Bus publishes messages from topics to subscriptions
- One or more "competing" consumers receive messages from subscriptions
- Subscriptions can contain Filters and Filter Actions
  - Filter is a SQL92 predicate for filtering messages
  - Filter Action is one or more SQL92 statements for modifying messages
- Messages are sent with the **TopicClient** class
- Messages are received with the **SubscriptionClient** class

Connect

What is Connect?

- A cloud service for connecting Windows Azure roles with on-premises servers
  - Connections are machine-to-machine, not site-to-site
- Roles can be joined to an on-premises domain
- Roles can be managed with on-premises tools

Connect

Cloud Application
Web Role
Worker Role
Connect
Local Endpoint Group
Local Endpoint Group
Firewall
On-Premises Servers
Web Server
File Server
Collaboration Server

About Connect

- Windows Azure roles can be Web, Worker, or VM roles
- On-premises servers might be Web, print, line-of-business, file, e-mail, database, or collaboration servers
- Connections are established using relays
- Connections are protected using IPsec
- Useful for extending legacy systems

Access Control Service

What is Access Control Service?

- A cloud service for authenticating users in relying party (RP) applications
- Externalises authentication logic for RP applications
- Federates authentication with a range of identity providers
- Transforms claims
- Issues claims for authorisation checks
  - E.g., Authorisation checks can be based on role, postcode, or age

About Access Control Service

- Compatible with .NET, Java, PHP, Python, and Ruby platforms
  - .NET RP applications can integrate with Windows Identity Foundation (WIF)
- Managed using Management Portal or an OData-based management service
- Supports a range of protocols and token formats

Supported identity providers

- Management Portal only

- Facebook
- Google
- Windows Live ID
- Yahoo!
- WS-Federation
  - E.g. Active Directory Federation Services (AD FS) 2.0

- Management Service only

- OpenID-based
  - E.g. PayPal
- WS-Trust

Authentication

Web applications

Web services

- See http://msdn.microsoft.com/en-us/library/hh868049

Authorisation

- WIF can express the role claim type as an **IPrincipal** role
- Role-based access control (RBAC)
  - Imperative:
    - `IPrincipal.IsInRole("Administrator")` returns Boolean
    - `PrincipalPermission.Demand()` throws Exception
  - Declarative: `[PrincipalPermission(SecurityAction.Demand, Role = "Administrator")]`
  - Administrative: `<authorization>`
- Claims-based access control (CBAC)

Summary

- In-the-cloud compute, storage, and network has many benefits
- Building hybrid applications has many challenges
- Windows Azure provides the "fabric" technologies for building, deploying, and managing hybrid applications in the cloud

Resources

- "Building Hybrid Solutions"
  - http://www.windowsazure.com/en-us/develop/net/fundamentals/hybrid-solutions/
- "Building Hybrid Applications in the Cloud on Windows Azure"
  - http://msdn.microsoft.com/en-us/library/hh871440.aspx
- "How To Guides"
  - http://www.windowsazure.com/en-us/develop/net/how-to-guides/

Microsoft

© 2012 Microsoft Corporation. All rights reserved. Microsoft, Windows, Windows Vista and other product names are or may be registered trademarks and/or trademarks in the U.S. and/or other countries.
The information herein is for informational purposes only and represents the current view of Microsoft Corporation as of the date of this presentation. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information provided after the date of this presentation. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS PRESENTATION.