EXTENDING APPLICATIONS SECURELY USING SERVICE BROKER

Ed Leighton-Dick

Kingfisher TECHNOLOGIES

ABOUT ME

- Email: ed@leightondick.com
- Blog: edleightondick.com
- Twitter: @eleightondick

Kingfisher TECHNOLOGIES | I-380PASS | PASS | Microsoft CERTIFIED Solutions Expert Data Platform | MVP Microsoft® Most Valuable Professional

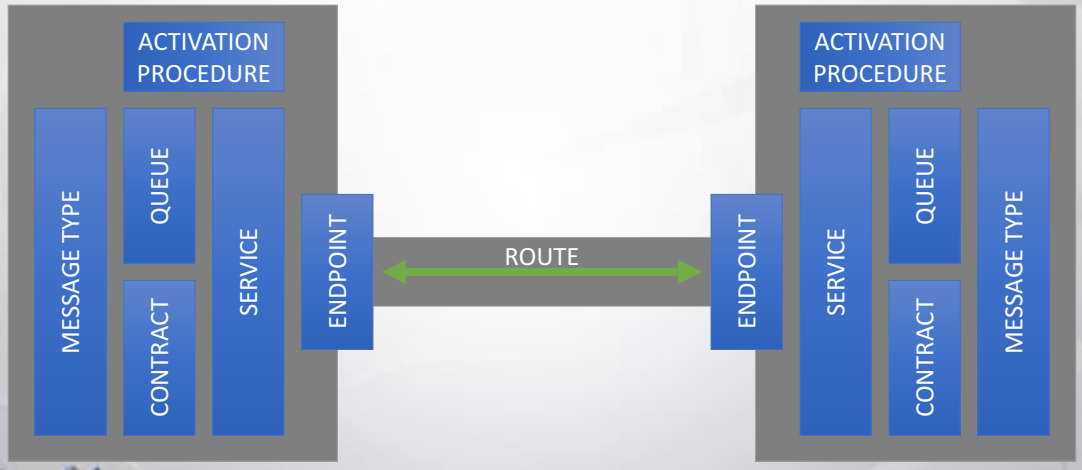
OUR GOALS

- Service Broker Architectures: Basic and Extended
- Extending: Routing
- Extending: External Activation
- Adding Security

Kingfisher

ARCHITECTURES

REVIEW: BASIC SERVICE BROKER ARCHITECTURE



Kingfisher

TRADITIONAL METHODS VS SERVICE BROKER

TRADITIONAL PROCEDURE	SERVICE BROKER
• Analogy: Communicating by phone	• Analogy: Communicating by letter
• Synchronous	• Asynchronous
• Real-time	• Not quite real-time
• One-to-one	• One-to-many
• More requests -> More processes	• Structured way of handling increases in demand
• Limit to number of requests that can be handled	• Scales out easily

Kingfisher

DEMO

Scenario

OUR SCENARIO: "SQLTALK"

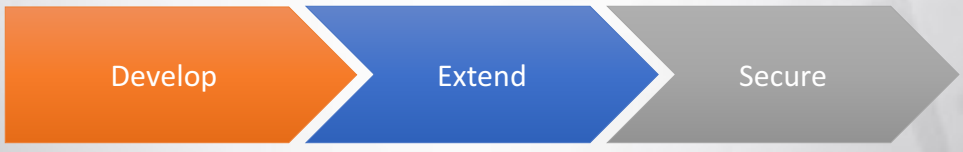
- New text messaging application
- Currently a prototype – Very limited

- Several improvements have been requested
  - Scale out
  - Allow messages to be sent to Twitter and SMS
  - Add encryption

Kingfisher

8

METHODOLOGY



Kingfisher

ROUTING

ENDPOINTS

- Allows connection to an instance of SQL Server
- One per instance of SQL Server
- CREATE ENDPOINT

Kingfisher

ROUTES: BASIC

- Specifies the address of the destination
- Always create in pairs
  - A -> B
  - B -> A
- CREATE ROUTE

Kingfisher

12

ROUTES: MULTIPLE STEPS (FORWARDING)

- Enable forwarding on endpoint
- Add appropriate routes on all servers
  - A -> F
  - F -> B
  - B -> F
  - F -> A
- Forwarder does not have copy of service

Kingfisher

13

MULTICAST

- Added in SQL 2012
- Allows a message to be sent to multiple destinations simultaneously
- Variation on SEND command
  - One OPEN DIALOG per destination
  - List all destinations in SEND

Kingfisher

14

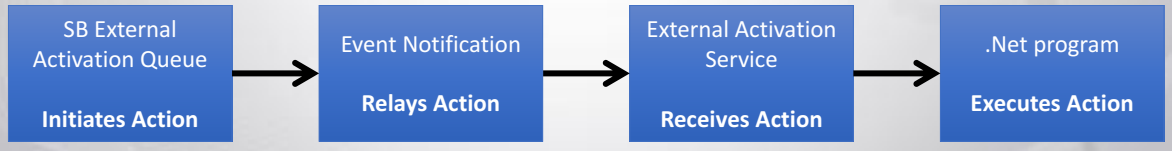
DEMO

Adding routing

EXTERNAL ACTIVATION

WHAT IS "EXTERNAL ACTIVATION"?

- Windows service
- Used to invoke lengthy processes or processes that wouldn't run safely or predictably within SQL Server



Kingfisher

INSTALLATION

- Download executable
  - Part of SQL Server Feature Pack (version-specific)
- Install service on separate machine for best performance
- Limited to one instance per machine
- Can write a custom external activator

Kingfisher

18

CONFIGURATION

- Service Broker
  - Initiator
  - Target
  - CREATE EVENT NOTIFICATION…FOR QUEUE_ACTIVATION
    - Consumes target queue
    - Directed to external activator

Kingfisher

19

CONFIGURATION

- Application
  - WHILE loop to repeatedly check queues
  - Parse messages
  - Commit transactions to ensure messages removed from queue

Kingfisher

20

CONFIGURATION

- External Activator
  - NotificationServiceList
  - ApplicationServiceList
  - LogSettings

Kingfisher

21

DEMO

Adding external activation

SECURITY

CERTIFICATES

- Types
  - Self-signed certificates
  - Third-party certificates
- Rotate regularly to maintain security
- Encryption Key Management
  - Hardware Security Modules (HSM)
  - Azure Key Vault

Kingfisher

TRANSPORT SECURITY

- Secures the connection between endpoints
- Enabled by default
- Transport security
  - Authentication between pairs of endpoints
- Transport encryption
  - Encryption between endpoints
  - Applies to all messages passing through connection

Kingfisher

25

DIALOG SECURITY

- Secures the messages themselves
- Dialog security
  - Authentication between initiator and target services
- Dialog encryption
  - Encrypts individual messages
  - End-to-end
  - Relies on dialog security for certificates

Kingfisher

26

SECURING THE CONNECTION

- Connection should be encrypted between any two SQL Servers
- Prevents ”man-in-the-middle” attacks
- SSL/TLS
  - Natively supported
  - Negotiated each time connection is opened
- VPN (IPSEC)
  - Persistent connection

Kingfisher

27

SECURING THE ENDPOINTS

- Change the port
  - Default: 4022
- Always use AES encryption
  - RC4 compromised; deprecated in SQL 2016
- Limit users via permissions

Kingfisher

28

ACCESS CONTROL

- Activation procedure execution
  - EXECUTE AS
- Permissions for principals
- Permissions for external activation

Kingfisher

29

DEMO

Adding Security

WRAP-UP

WHAT WE COVERED

- Service Broker Architectures: Basic and Extended
- Extending: Routing
- Extending: External Activation
- Adding Security

Kingfisher

QUESTIONS?

- Email: ed@leightondick.com
- Blog: edleightondick.com
- Twitter: @eleightondick

Kingfisher

THANK YOU FOR ATTENDING!

~ Please remember to fill out your comment cards ~

Kingfisher