

Erfahrungen aus dem WebSphere MQ 7.1.0 ESP & WebSphere MQ AMS PoC

Henning Kösters
IT-Bereitstellung/ Systeme
Middleware

- **Die GAD Unser Unternehmen**
- **WebSphere MQ in der GAD**
 - Übersicht
 - Early Support Program 7.1.0
 - Channel Security
 - z/OS Coupling Facility Resilience
 - Shared Message Dataset (SMDS)
- **WebSphere MQ Advanced Message Security (AMS) PoC**

Die GAD: Der genossenschaftliche IT-Dienstleister



Die GAD eG

- ist einer der führenden Spezialisten für Banken-IT.
- gehört den Volksbanken und Raiffeisenbanken.
Als Mitglieder haben sie direkten starken Einfluss auf ihren IT-Dienstleister.
- hat rund 50 Jahre IT-Erfahrung im Banking-Umfeld.
- beschäftigt rund 1700 Mitarbeiter und ist damit einer der größten Arbeitgeber in Münster.

Die GAD:

Der genossenschaftliche IT-Dienstleister

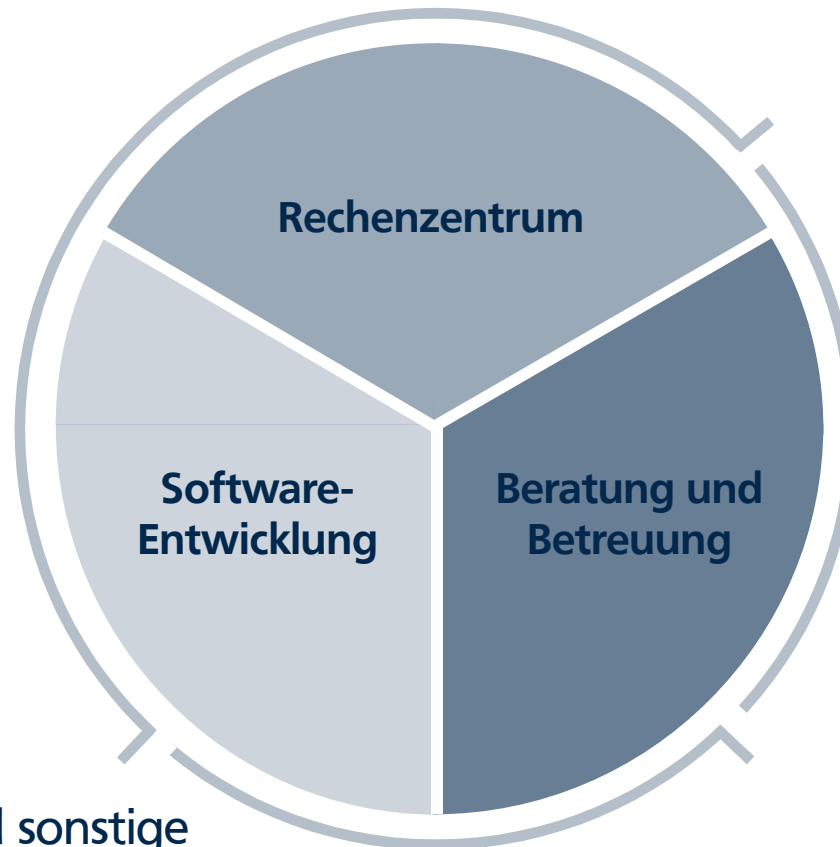


IT-Beratungs- und Kompetenzcenter, Softwarehaus und Rechenzentrum für

- 430 Volksbanken & Raiffeisenbanken sowie Retailbanken im deutschsprachigen Raum
- WGZ BANK, DZ BANK, genossenschaftliche Verbundunternehmen



Die GAD: Unsere Hauptgeschäftsfelder



- Banken und sonstige Finanzunternehmen

- sieben Tage die Woche
- 24-Stunden-Betrieb
- Internet-Service-Provider
- modernes multiprotokollfähiges Datennetz

- Mitglieder und Kunden

Die GAD: Unsere Produkte und Dienstleistungen



- **Starker Partner für Zentralbanken und Verbundpartner**
 - WGZ BANK
 - DZ BANK
 - WL BANK
 - R+V, BSH
 - Union Investment
 - DG VERLAG & Raiffeisendruckerei
 - CardProcess
- **Software-Lösungen**
 - für Privat- und Firmenkunden von Banken (z.B. Zahlungsverkehrsprogramme)
 - Internet- und eBusiness-Service

Die GAD: Zahlen und Fakten 2011



412	Mio. Euro Umsatz (GAD)
699	Mio. Euro Umsatz (GAD Unternehmensgruppe)
1.754	Mitarbeiter
430	Banken
62.848	Bankarbeitsplätze

Die GAD: Zahlen und Fakten 2011



2,34	Mrd. Buchungsposten
17,48	Mrd. Transaktionen
215,12	Mio. GAA-Abhebungen
235,85	Mio. SB-Kontoauszüge
29,95	Mio. aktive Konten
4,42	Mio. SB-Kontokorrentkonten mit Internet-Nutzung
15.379	SB-Geräte

Mehr als Nullen und Einsen: Unser Rechenzentrum in Zahlen (Stand 2011)

- Rechnerausstattung:
 - 4 x IBM z196 2817-M66 (2817-717)
 - 2 x IBM z10 2097-E64 (2097-722)
 - 4 x IBM z196 2817-M32 (Standalone CFs)
- Hauptspeicherkapazität Großrechner:
2.496 Gigabyte Hauptspeicher
- Leistungsfähigkeit der Großrechner:
112.806 MIPS (Mio. Instruktionen pro Sek.)
- Anzahl Server (Produktion):
 - **1014** Unix-Server
 - **2312** Virtuelle Unix-Server (LPARs & Zonen) ¹
 - **1525** Linux- und Windows-Server
 - **3308** Virtuelle Linux- u. Windows-Server
- Gesamtspeicherkapazität:
830 Terabyte

¹ LPARs = IBM-Systeme, Zonen = Sun-Systeme



- **Die GAD Unser Unternehmen**
- **WebSphere MQ in der GAD**
 - Übersicht
 - Early Support Program 7.1.0
 - Channel Security
 - z/OS Coupling Facility Resilience
 - Shared Message Dataset (SMDS)
- **WebSphere MQ Advanced Message Security (AMS) PoC**

Installation

- Primäre Plattform für WebSphere MQ ist z/OS
- nur wenige Queue Manager auf non-z/OS
- UNIX- und Windows-Server im RZ sind als MQ-Clients angebunden
- Gateway-Konzept zur Kommunikation mit externen Partner

Skalierung (Produktion)

- Produktions Sysplex 1: eine Queue-Sharing Group mit zwei Queue Manager pro IMS
- Produktions Sysplex 1: zwei eigene Queue Manager für den WBI-FN Message Broker
- Produktions Sysplex 2: eine Queue-Sharing Group mit zwei Queue Manager pro Mandantengruppe
- Produktions Sysplex 1 & 2: einige LPAR bezogene Queue Manager

Mengengerüst

- 104 Queue Manager auf z/OS (70 Produktion + 34 Entwicklung/Test)
- 4 dezentrale Queue Manager (Linux)
- ca. 40.000 Clients
- ca. 120.000 lokale Queues
- ca. 40.000.000 Messages pro Tag
- ca. 65 unterschiedliche Anwendungen mit MQ-Nutzung

Besonderheiten

- Umfangreicher Einsatz von Queue-Sharing Groups zur Realisierung höchster Verfügbarkeit
 - Shared-Queues, Shared-Channel
- Effizientes Nachrichten-Routing durch Nutzung eines Exits
- Komplexitätsreduktion durch das Konzept, alle MQ-Server auf einer Plattform zu betreiben

Early Support Program MQ Version 7.1.0

- Projektbeginn (Kickoff und erster Beta Code): Mai 2010
- Projektende : Ende 2011

Teilnahme der GAD

- Einstieg im Frühjahr 2011
- Beschränkung auf z/OS
- Schwerpunkt Queue Sharing

Projektrahmen

- reine z/OS-Umgebung
- Test-Sysplex bestehend aus zwei LPARS z/OS 1.13.00
- Queue Sharing Group bestehend aus zwei Queue Managern
 - Ausgangsversion WMQ 7.0.1
 - eine Datenstruktur in Coupling Facility (CF)
 - DB2 Version 10
- Keine Anbindung von Anwendungen
 - Ausnahme: Service-Programme (COBOL)

Channel Security

- Stellt Zugriffsberechtigungen auf Channelebene zur Verfügung

- Neues Kommando

- SET CHLAUTH(channelname)

- ACTION: ADD, REPLACE, REMOVE, REMOVEALL

<u>TYPE</u>	<u>Parameter</u>	<u>Wirkung</u>
BLOCKADDR	ADDRLIST	blockt Adresse
BLOCKUSER	USERLIST	blockt User
ADDRESSMAP	ADDRESS	Adresse → MCAUSER
SSLPEERMAP	SSLPEER	DN → MCAUSER
USERMAP	CLNTUSER	UserID → MCAUSER
QMGRMAP	QMNAME	Remote Qmgr → MCAUSER

Test

- alle Funktionstests positiv

Fazit

- Allerdings keine Möglichkeit zu einem direkten Positiveintrag, d.h. es werden nur die Adressen zugelassen, die für den Channel eingetragen sind
- Die GAD setzt weiterhin einen selbstgeschriebenen Security Exit ein

WebSphere MQ in der GAD

Early Support Program: Channel Security



■ Beispiel GAD

- `DEFINE CHANNEL ('NZPIPE01.MQ1X') +`
`....`
`SCYEXIT (GMIH59S) +`
`SCYDATA ('XGESBADM 10.65.105.164 GAST -')`
- `dis chl(NZPIPE01.MQ1X)`
`...`
`SCYEXIT(GMIH59S)`
`SCYDATA(XGESBADM 10.65.105.164 GAST -)`

■ Vorschlag IBM

- `DEFINE CHANNEL (NZPIPE01.MQ1X')`
- `SET CHLAUTH (NZPIPE01.MQ1X') TYPE(ADDRESSMAP) ADDRESS(,10.65.105.164')`
`MCAUSER(XGESBADM)`
- `SET CHLAUTH (NZPIPE01.MQ1X') TYPE(ADDRESSMAP) ADDRESS(,*) USERSRC(NO ACCESS)`
- `DISPLAY CHLAUT(NZPIPE01.MQ1X)`
- `DISPLAY CHL(NZPIPE01.MQ1X)`

z/OS Coupling Facility Resilience

- Zwei Arten von CF Fehlern
 - Struktur-Failure
 - Struktur korrupt, Begrenzung auf einzelne Struktur
 - wird bereits von WMQ ab CFLEVEL(3) toleriert
 - Verlust der Konnektivität
 - z.B. CF-Links offline
 - bislang Abbruch des Queue Managers
 - mit 7.1.0 und CFLEVEL(5) wird Verlust toleriert

Tests

- Verlust der Konnektivität zur **Daten Struktur**
 - Fall 1: sekundäre Coupling Facility verfügbar
 - ein Qmgr hat noch Connect zur Struktur
 - Rebuild der Struktur auf der sekundären CF, sobald die Konnektivität zur primären Struktur verloren wurde
 - Test durch Deaktivieren der CF-Links zu einer LPAR
 - Fall 2: Konnektivitätsverlust aller Qmgr (Systeme) im Sysplex
 - wenn Konnektivität wieder gegeben ist, ist ggf. ein RECOVER CFSTRUCT notwendig
 - Test durch Deaktivieren der integrierten CF (ICF)

Tests

- Verlust der Konnektivität zur **Admin Struktur**
 - Fall 1: sekundäre Coupling Facility verfügbar
 - Rebuild der Struktur auf der sekundären CF, sobald die Konnektivität zur primären Struktur verloren wurde
 - Test durch Deaktivieren der CF-Links zu einer LPAR
 - Fall 2: keine sekundäre Coupling Facility verfügbar
 - eingeschränkte Operationalität
 - automatischer Reconnect und Rebuild der Struktur, sobald CF wieder verfügbar
 - Test durch Deaktivieren beider integrierten CF (ICF)

WebSphere MQ in der GAD

Early Support Program: z/OS Coupling Facility Resilience



Fazit

- die Funktionstests waren positiv
- Die Aktivierung muss genau bedacht werden
 - Anwendungen reagieren evtl. nicht richtig
 - Maßnahme muss evtl. durch die Automation erzwungen werden
- Die GAD wird dies Feature einsetzen

z/OS Shared Message DataSet (SMDs)

- Offload Dataset (VSAM) für shared Messages
- Voraussetzung: CFLEVEL(5)
- Parametrisierung anhand neuer Attribute
 - Füllgrad/Nachrichtengröße
- In der CF bleibt weiterhin ein Pointer zur Message erhalten

WebSphere MQ in der GAD

Early Support Program: Shared Message Dataset



Tests der SMDS Funktionalität sind positiv verlaufen

Fazit

- SMDS ist schneller als DB2
- kostengünstiger als CF Strukturen
- wird in der GAD schnellstmöglich eingesetzt

- **Die GAD Unser Unternehmen**
- **WebSphere MQ in der GAD**
 - Übersicht
 - Early Support Program 7.1.0
 - Channel Security
 - z/OS Coupling Facility Resilience
 - Shared Message Dataset (SMDS)
- **WebSphere MQ Advanced Message Security (AMS) PoC**

WebSphere MQ in der GAD

WebSphere MQ AMS



- Stellt Sicherheitsdienste zur Verfügung, die über diejenigen des MQ Basisproduktes hinausgehen
- End-zu-End-Schutz der Anwendungsdaten für Punkt-zu-Punkt Messaging
 - Asymmetrische Verschlüsselung zum Schutz einzelner Nachrichten
- Der AMS-Schutz wird mittels "Policies" auf der Ebene einzelner Queues administrativ spezifiziert
- "Non invasive"
 - MQ Anwendungen brauchen nicht verändert zu werden

Websphere MQ AMS PoC

- die Queue Manager Komponenten laufen auf unserem Entwicklungssysplex
- Es sind pro QMgr zwei Started Tasks einzurichten:
 - <QMGR>AMSD die AMS Data Services Task – für Zertifikatshandling zuständig
 - <QMGR>AMSM die AMS Main Server Task - “kümmert sich” um die Policies
- Auf Anwendungseite sind Interceptoren einzurichten
 - Programmcode der die MQ Calls abfängt

Tests von drei unterschiedlichen Zugriffstypen

- Batch Jobs: mit direktem Connect zu den Queue Managern

- Native MQ Client per MQ Channel
 - Installation C-Client Interceptor
 - Schlüssellänge von 4 KB wird nicht akzeptiert

- Websphere Application Server per MQ Channel
 - Installation Java Interceptor
 - Wegen eines Verzeichnis-Checks musste vorab der native MQ Client installiert werden

Fazit

- Funktionalitätstests positiv
- Hoher Aufwand für die Zertifikatskonfiguration
- Performance-Tests
 - CPU Verbrauch der Anwendung steigt stark an, dies gilt auch für nicht AMS geschützte Objekte, sobald die AMS Started Task gestartet ist

**Vielen Dank für Ihre
Aufmerksamkeit!**

Wir sind ein starkes Netzwerk: Die GAD-Unternehmensgruppe

