

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:

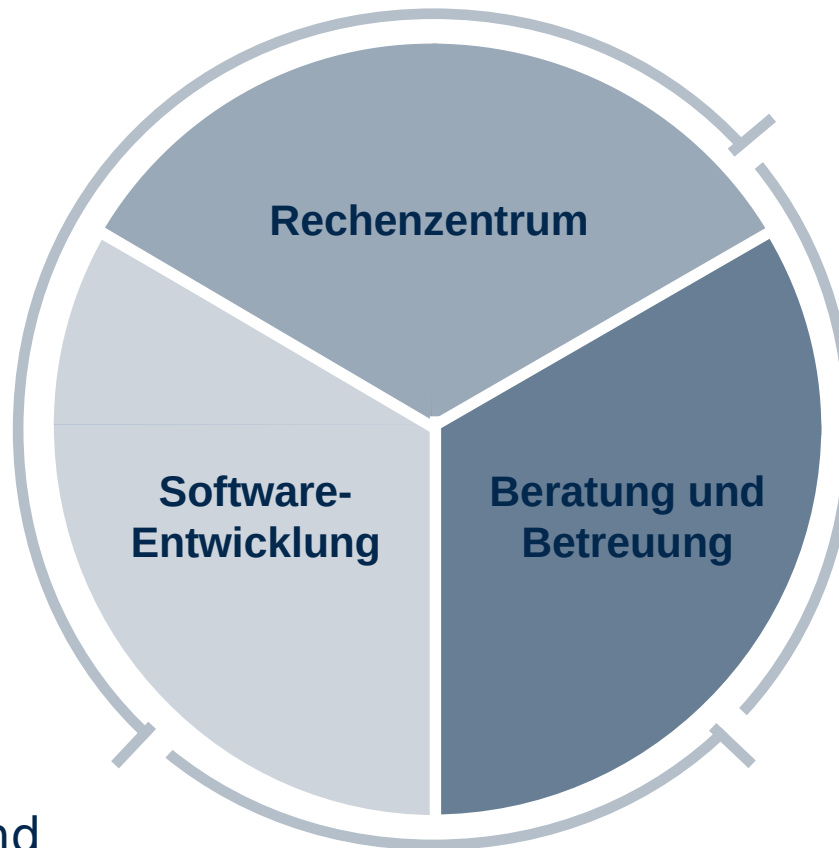
Der genossenschaftliche IT-Dienstleister

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

- **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

- **IT-Beratung und Schulung**
- **RZ-Dienstleistungen**
 - Rechenzentrumsbetrieb für Banken-Anwendungssysteme
 - Application-Hosting
 - Telekommunikation und Netzwerke
- **Unterstützung Business Prozesse**
 - Mailingservice
 - Output-Management
 - Dokumentenmanagement/Archivierung
 - Kundenservice-Prozesse
 - Produktion, Kryptografie

Die GAD: Zahlen und Fakten 2011

412

Mio. Euro Umsatz (GAD)

699

Mio. Euro Umsatz (GAD Unternehmensgruppe)

1.754

Mitarbeiter

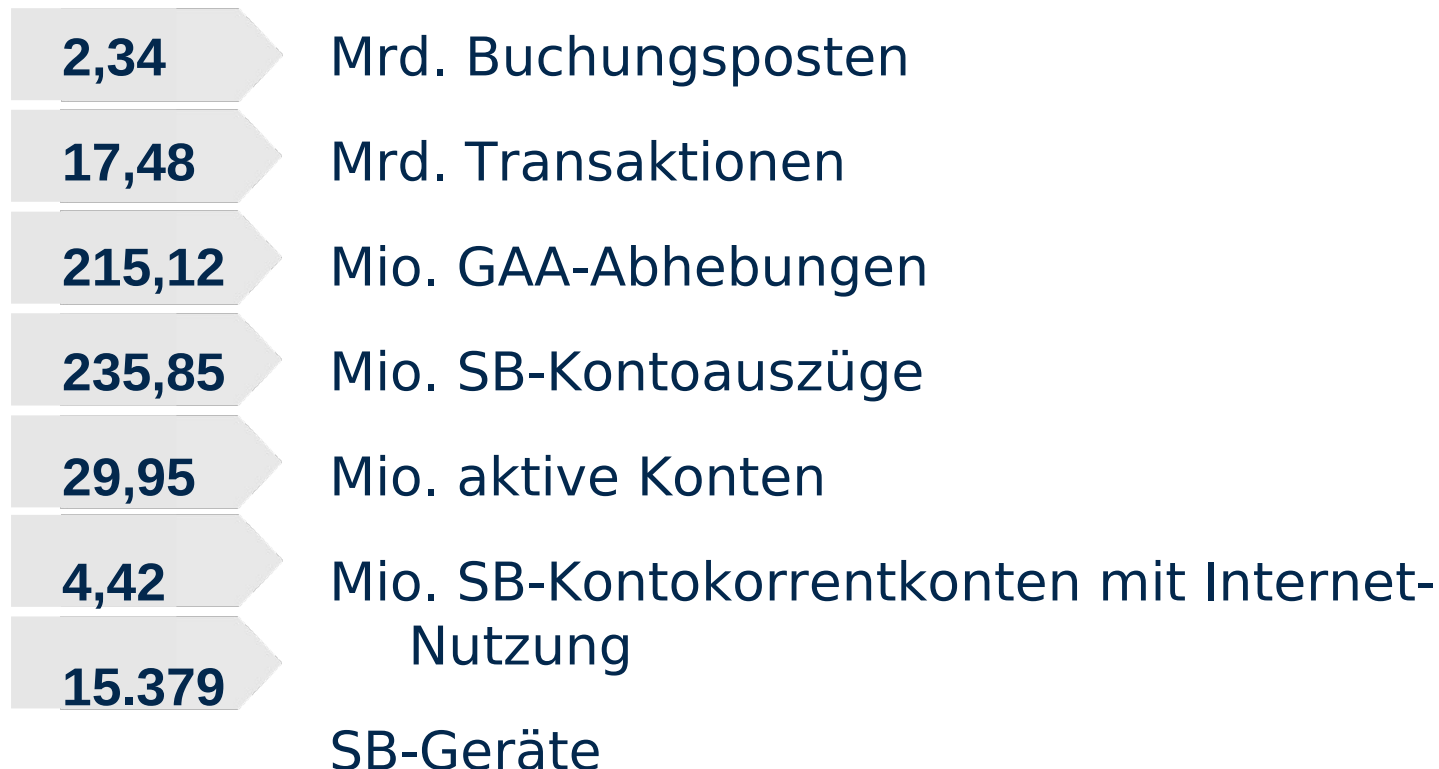
430

Banken

62.848

Bankarbeitsplätze

Die GAD: Zahlen und Fakten 2011

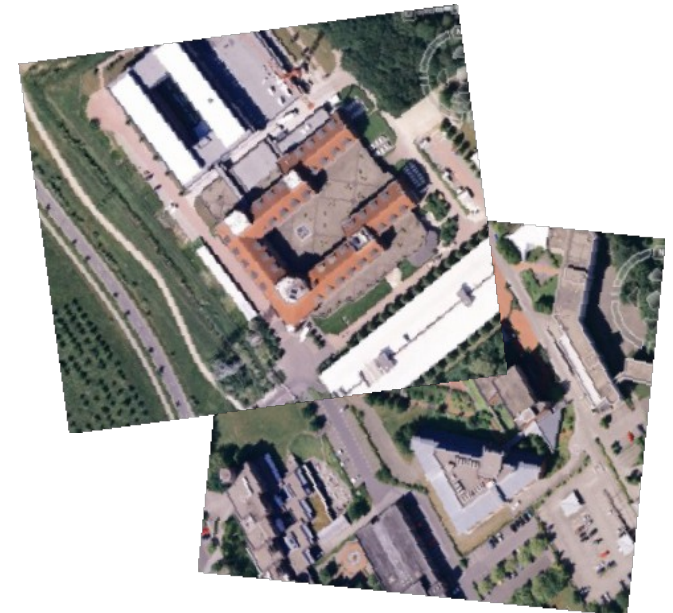


Mehr als Nullen und Einsen:

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



Mehr Leistung, mehr Sicherheit: Unser neues Rechenzentrum

Im April 2011 hat die GAD als erstes deutsches Banken-Rechenzentrum vom TÜViT das Level 4 Zertifikat erhalten.

Neues Rechenzentrum

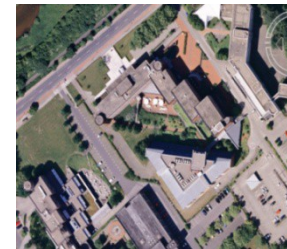


RZ-Fläche: 3.000m²

Bestehende Infrastruktur



GAD, 1.583m²



WGA, 1.327m²



Neubau

- Das neue RZ erfüllt die höchsten Sicherheits-Empfehlungen für Hochsicherheits-RZ: Die TÜViT-Level4-Zertifizierung
- GAD und WGA sind nun als zusammenhängendes Rechenzentrum konfiguriert
- Die Migration wurde im Herbst 2010 begonnen und ist seit Mai 2011 abgeschlossen.

- **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

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)

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

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**

- 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

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



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**

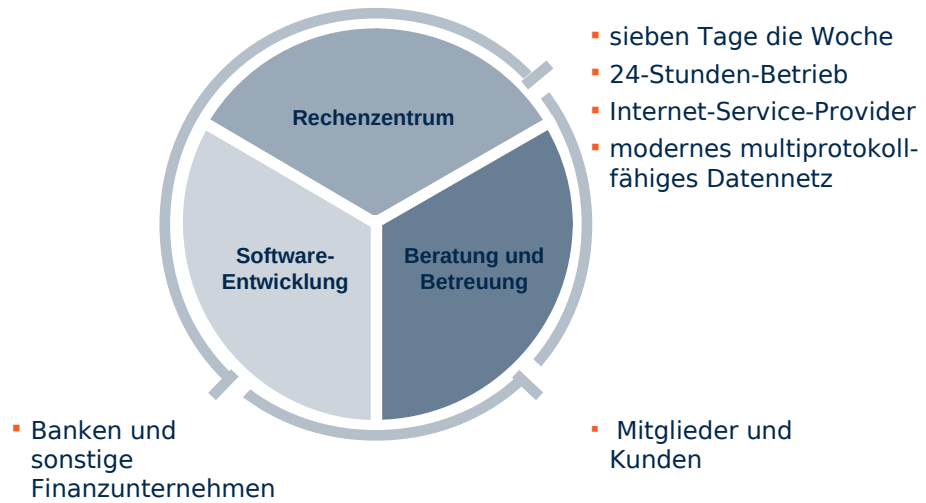
Die GAD eG

- 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.

IT-Beratungs- und Kompetenzzentrum, Softwarehaus und Rechenzentrum für


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



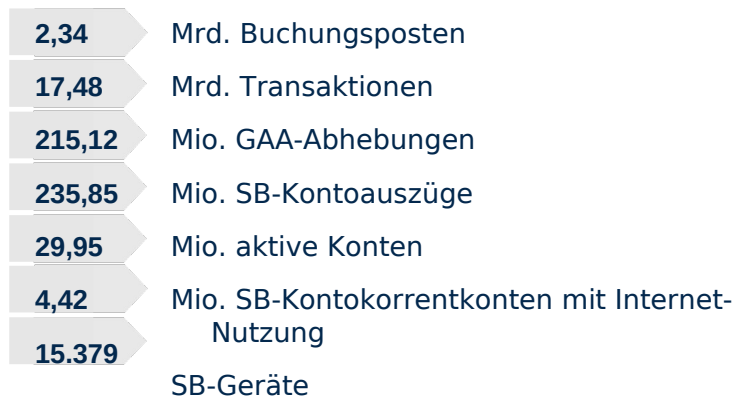


- **Starker Partner für Zentralbanken und Verbundpartner**
 - WGZ BANK
 - DZ BANK
 - WL BANK
 - R+V, BSH
 - Union Investment
 - DG VERLAG & Raiffeisendruckerei
 - CardProcess
- **Software-Lösungen**
 - für Privat- und Firmenkunden von Banken (z.B. Zahlungsverkehrsprogramme)
 - Internet- und eBusiness-Service

- **IT-Beratung und Schulung**
- **RZ-Dienstleistungen**
 - Rechenzentrumsbetrieb für Banken-Anwendungssysteme
 - Application-Hosting
 - Telekommunikation und Netzwerke
- **Unterstützung Business Prozesse**
 - Mailingservice
 - Output-Management
 - Dokumentenmanagement/Archivierung
 - Kundenservice-Prozesse
 - Produktion, Kryptografie



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



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



Im April 2011 hat die GAD als erstes deutsches Banken-Rechenzentrum vom TÜViT das Level 4 Zertifikat erhalten.

Neues Rechenzentrum



RZ-Fläche: 3.000m²

Bestehende Infrastruktur



GAD, 1.583m²



WGA, 1.327m²



Neubau

- Das neue RZ erfüllt die höchsten Sicherheits-Empfehlungen für Hochsicherheits-RZ: Die TÜViT-Level4-Zertifizierung
- GAD und WGA sind nun als zusammenhängendes Rechenzentrum konfiguriert
- Die Migration wurde im Herbst 2010 begonnen und ist seit Mai 2011 abgeschlossen.

- **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

- Mandantengruppe: Gruppierung von Banken die in einem IMS zusammengefasst sind

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

- Angaben für Produktion
- Open-Exit und Channel-Receive Exit

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 |

- ALTER QMGR CHLAUTH(ENABLED)
- Channelname kann generisch (allgemeingültig) sein / an allen Positionen „*“
- „Warnmode“ möglich -> protokolliert den Fehler, hat aber keine Auswirkungen
- DISPLAY CHLAUTH
- Blockuser nur für SRVCONN Channel (nicht in Dokumentation enthalten)

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

- Nach PMR und Requirement zum Positiveintrag: IBM Vorschlag durch zwei Setzungen
- SET CHLAUTH(CHANNEL)
TYPE(ADDRESSMAP) ADDRESS(IP'
MCAUSER())
- UND SET CHLAUTH(CHANNEL)
TYPE(ADDRESSMAP) ADDRESS(*'
USERSRC(NO ACCESS)
- GAD: Angabe direkt bei Channeldefinition im SecExit Feld.

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

- Bis jetzt war es so, dass der Queue manager terminierte, mit der Version 7.1.0 kann ein Konnektivitätsverlust toleriert. Dadurch ergibt sich eine höhere Verfügbarkeit da non-shared Queues weiter verfügbar sind.
 - Qmgr Attribut: QMGR CFCONLOS -> (Tolerate/Terminate/ASMGR) Tolerierung für Admin Struktur
 - CFSTRUCT Attribut: CFSTRUCT CFCONLOS -> Tolerierung für Daten Struktur
- GAD konnte CF Level 5 noch nicht einsetzen auf Grund von Softwarefehlern
- CF Links -> Connection zur CF Hardware
- CFSTRUCT RECAUTO -> automatische Log-Recovery

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)

- Voraussetzung: zweite CF verfügbar
- Fall 1: Wenn eine sekundäre CF verfügbar ist und ein Qmgr der QSG noch eine Connection zur Struktur hat, wird ein System Managed Rebuild auf die sekundären CF durchgeführt.
- Fall 2: Bei einem Konnektivitätsverlust aller Systeme im Sysplex ist nach dem Reconnect eine Recover Cf-Struct notwendig wenn nicht „CFSTRUCT RECAUTO =yes“ an der Struktur im MQ gesetzt ist.
- Qmgr beendet sich nicht, aber RECOVER CF ist notwendig, um persistente Messages wieder herzustellen
- RECOVER CFSTRUCT -> Admin Struktur muss vorhanden sein wegen
- ICF=integrated Coupling Facility
- System -Managed Rebuild = wird an der Struktur definiert (z/OS System Managed)

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)

- Test 2: Es können z. B. keine neuen MQ Objekte definiert werden
- Test 2: Da die Admin Struktur Informationen zu nicht vollständigen UoWs hält, muss sie beim RECOVER CFSTRUCT verfügbar sein

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

Zur Zeit sind noch 3 PMR bezüglich CF Level 5 offen (Truncated Messages auf XMIT Queues)

- Aber: Bei längerer Nichtverfügbarkeit der Cf müssen Anwendungen erkennen, dass Shared-Queues über den betreffenden Qmgr nicht genutzt werden können

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

- OFFLD1TH(percentage) OFFLD1SZ(size) -
OFFLD2TH(percentage) OFFLD2SZ(size) -
OFFLD3TH(percentage) OFFLD3SZ(size)
- „Mischbetrieb“ möglich: Struktur 1 SMDS / Struktur 2
DB2 anhand neuer Attribute z. b. ab Füllgrad xx%
geht alles in's SMDS
- Je kleiner die Zahlen desto mehr wird ausgelagert
- For OFFLOAD(SMDS) the defaults
are:OFFLD1TH(70) OFFLD1SZ(32K)
OFFLD2TH(80) OFFLD2SZ(4K)
OFFLD3TH(90) OFFLD3SZ(0K)
- For OFFLOAD(DB2) the defaults are:
OFFLD1TH(70) OFFLD1SZ(64K)
OFFLD2TH(80) OFFLD2SZ(64K)
OFFLD3TH(90) OFFLD3SZ(64K)

Tests der SMDS Funktionalität sind positiv verlaufen

Fazit

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

- Laut SupportPac MP1H „Performance Report“ for WMQ z/OS 7.1.0
- keine eigenen Messungen
- OFFLD1TH(percentage) OFFLD1SZ(size) -
OFFLD2TH(percentage) OFFLD2SZ(size) -
OFFLD3TH(percentage) OFFLD3SZ(size)
- Die GAD möchte möglichst alles auslagern
- Mögliche Szenarien: 1 Struktur für kleine Message mit hohem Durchsatz wo gar nichts ausgelagert wird
- 1 Struktur für große Messages die immer ausgelagert werden
- Muss jeder für sich testen

Batchdeleter

- Löschen von Nachrichten in CF-Struktur führt unter Umständen erst verzögert zur Freigabe von Space

- **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**

- 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

- Queue-Sharing Group

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

- Batch: Das Zertifikat für die AMS Zugriffe wird über den User mitgegeben unter dem der Job läuft
- Beim Einspielen eines Zertifikats in den Keystores des Clients mittels GSKit, haben wir festgestellt, dass dort eine 4 KB Schlüssellänge nicht akzeptiert wird. Neuversorgung mit 1 KB erfolgreich
- Beim Installieren des Java Interceptors gab es eine Verzeichnisprüfung auf das Verzeichnis des MQ Clients. Da im WAS die Verzeichnisstruktur anders ist, funktionierte dies nicht. Es musste vorab der 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

