Session L75

The Success Story of the Québec Government in raising and training penguins within a crèche

Jocelyn Hamel, PMP

IBM Canada

IBM System z Expo
September 17-21, 2007
San Antonio, TX

LE CENTRE DE SERVICES PARTAGÉS

The Success Story of the Québec Government in raising and training penguins within a crèche

System z EXPO
Technical Conference
San Antonio , Texas
Session L75-User Experience
September, 2007

In collaboration with
IBM Canada LTD
VM Resources LTD

Centre de services partagés Québec

The Success Story of the Québec Government in raising and training penguins within a crèche[1]

Table Of Contents

- Client Context
- Business case
- Technical Challenges
- Architecture
- Cloning process
- Best Practices
- Project status
- Lessons Learned
- Conclusion

[1]: as young ones (penguins), they assemble in large groups called crèches

Centre de services partagés Québec

3

Client context

Centre de services partagés Québec

4

Client context
The DGTI

- CSPQ/DGTI IT service provider for many Québec government offices (125+)
  - Already a mainframe shop
  - 5 z890 + 2 z800 + 1 G5 on the floor on 3 sites
  - 1 z9 EC dedicated to Linux on z/VM
  - 450+ physical servers (750+ logical) (HP, SUN, pSeries, …)
- CSPQ/DGTI orientations :
  - Promote the mainframe environment
  - z/VM is the prime choice for future projects
  - Server consolidation is a priority
  - This project is in line with the new « online government » policy

Centre de services partagés Québec

5

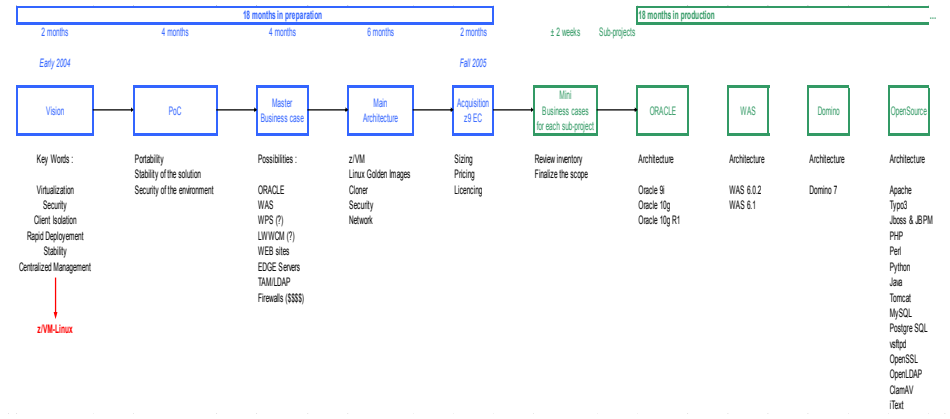
Client context
Project origin

- Initial needs :
  - Must solve many issues with the intermediate platform
    - Many operation systems
    - Many versions
    - Unsupported software
    - Unsatisfactory DR
    - Fast growing (unprecedented growth)
  - Understaffed
  - Need a flexible solution with rapid deployment
- Mainframe is a stable and mature environment
  - Staff is available and at early stages of their careers
  - Solid and well controlled DR process (MVS-like)
- The conclusion : GO with z/VM

Centre de services partagés Québec

6

Client context
Timeline of the project origin



Centre de services partagés Québec

7

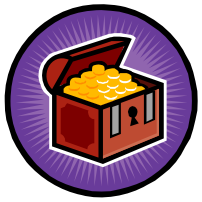
Client context
z/VM Linux Environment

- 1 z9 EC mainframe with 5 IFLs (~ 2750 mips)
- 8 LPARs
  - Oracle/DB
  - WAS (2)
  - OpenSource
  - Domino (2)
  - Service Zone
  - Lab Zone
- 40+ internal networks
- Software
  - Novell SLES (versions 8 & 9 & 10)
  - z/VM v.5.2 + & 5.3
  - Oracle/DB (versions 9i & 10g & 10gR1)
  - Velocity Software Performance Tools
  - CA products (Automation, Scheduler)

Centre de services partagés Québec

8

Business Case

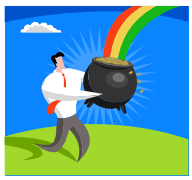


Centre de services partagés Québec

9

Master Business Case

- Identifying the potential for the client :
  - Databases
  - WebSphere Application Server (WAS)
  - WebSphere Portal + Lotus Workplace Web Content Management (LWWCM)
  - Firewalls
  - TAM & LDAP
  - EDGE servers
- Identifying the most cost efficient project – Oracle/DB
  - Reduction of the number of licenses
  - Success stories
  - Easy conversion (data transfer; unload/reload)



Centre de services partagés Québec

10

Master Business Case Summary

- Oracle/DB
  - Hardware cost is about the same
  - Software cost has a big gain by a huge reduction of the number of licenses (result : z9 EC paid within 2-3 years)
- WebSphere Application server (WAS) including WMB, MQ
  - Hardware cost is little more expensive for the System z
  - Software cost has a big gain by reducing the number of licenses (we are saving money)
- TAM & LDAP
  - Hardware cost is more expensive on the System z
  - Redundancy, Backup/Restore and DR are easier
  - Installing secondary servers on the mainframe for redundancy purposes (reducing the cost and having the mainframe gains)

Centre de services partagés Québec

11

Master Business Case Summary

- Firewalls
  - Uncertain about the business case
  - Migration is a major impact on the organization
  - Investigation needed for the licensing (/CPU, /instance, /site)
- EDGE servers
  - Hardware cost is a little more expensive for the System z
  - Need to introduce the mainframe in the access zone (complexity and security concerns)
  - The benefits are at the intangibles level
- WebSphere Portal + LWWCM
  - Potential for a big financial gain
  - Performance on the mainframe must be confirmed
  - Need a proof of concept

Centre de services partagés Québec

12

Master Business Case Conclusion

- Overall, the cost of the software and hardware is reduced by 30%. Every extra instance will help to reduce the cost.
- The Oracle/DB migration project will break even within two years.
- Within the first two phases of the project (Oracle/DB and WAS), the mainframe will be repaid within three years. It was very important to build the business case around a worst case scenario. It can only be better, not worse.
- The business case doesn't consider the following :
  - Electricity
  - Floor space
  - Air conditioning
  - UPS

... All of which are favorable with System z ...

Centre de services partagés Québec

13

Business Case Revisited After 18 months in production...

- Oracle Project
  - License reduction from 49 to 4 (- 92%)
  - Version upgrades of 200 databases within 4 months
  - Saving in license acquisitions (27 - 1 time charge) and license maintenance (yearly)
- WAS Project (including WMB and MQ)
  - License reduction from 88 to 8 (- 91%)
  - Total migration within 4 months
  - Saving in license acquisitions (33 - 1 time charge) and license maintenance (yearly)
- Cloning engine
  - In-house development needed : 200-250 man/days
  - One major event : Had to generate (clone !) 53 Oracle Databases ASAP
    - Took 4 days with a team of 4 people
    - Old fashioned way : between 9 to 12 months (People needed unknown, dozens)
    - Result : Project proceeding on schedule (Government Portal)
    - Conclusion : Best decision made, cloner is free of charge after only one event !!!
  - No one is questioning the cloner anymore !!! That's the way to go, the only way !!!
- Overall Business Case
  - On day 1 : Break-even point = 36 months
  - Now : Break-even point = less than 24 months !!!
    - System z box is free
    - First two phases (Oracle and WAS)

Centre de services partagés Québec

14

Technical Challenges

Centre de services partagés Québec

15

Technical Challenges

- As a new and rather large implementation we encountered many technical challenges:
  - Improving the technical skills of the project personnel.
  - Ensuring the system and applications are safe and secure.
  - Guaranteeing that the clients are isolated from each other while still capitalizing on resource sharing.
  - Implementing networks that integrate seamlessly into the existing topology and practices.
  - Tiers of redundancy based on cost and defined need.
  - Need to satisfy the application needs of multiple clients and their data.

Centre de services partagés Québec

16

Technical Challenges
Training … training … training …

Winning hearts and minds through training …

- Over 200 person days of training to staff:
  - Mainframe Systems programmers
  - Unix administrators
  - Security officers
  - Network administrators
  - Architects
  - Analysts

- Training sessions with lectures and labs:
  - Architecture seminar
  - z/VM Systems Workshop
  - Linux on the Mainframe Workshop
  - z/VM Networking and Security Workshop
- Briefings for team leaders and management
- Summary presentations to executives

Centre de services partagés Québec

17

Technical Challenges
Security under z/VM

Challenge: securing the environment …

- Secured z/VM resources through RACF:
  - Minidisk linkage, VSWITCH membership, and other points of access controlled by RACF via rules database.
- Secured Linux on z/VM access points by combining:
  - PAM authentication for logins
  - Removal of unneeded packages
  - Usage of secured facilities instead of weaker facilities (SSH versus TELNET)
  - File system changes secured and monitored with TRIPWIRE
  - Ethical hacking attempts to ensure compliance and fortress galvanizing

Centre de services partagés Québec

18

Technical Challenges
Intangibles

- Backup/restore : mainframe strategy (via z/OS)
- Disaster Recovery : mainframe stability with an external provider
- Virtualization
- Cloning
- High availability
- Performance (I/O) for Oracle
- Security
- Resource sharing
  - IPL pack
  - Linux Kernel
  - Oracle executables
  - Golden images
  - Partitioning (EAL 5 security level)
- On demand

Centre de services partagés Québec

19

Technical Challenges
Intangibles

- Flexibility of the solution
  - Fast track (no acquisition)
    - Creating/Installation a new server
      - Linux on z/VM : 30 min
      - SUN, AIX, Windows : between 1 week and 3 months (if RFP needed)
  - Cloning and deployment engine
  - Cloning/Installation an Oracle/DB instance
    - Under Linux on z/VM : 30-45 min
    - Under SUN : 10-14h
- Adjustments to the cloning engine for a new service (ex. WAS) :
  - Coding changes done within 2 weeks

Centre de services partagés Québec

20

Technical Challenges
Competing technologies

Category	Weight	z/VM Description	Level	Distributed platform Description	Level	Delta
Disciplin-ability (production mentality)	**50**		50		20	30
Change management	5	Formal & part of the culture	5	Formal	2	
Start-up disk	5	Unique IPL pack (like z/OS)	5	Starting a project for a cloning engine	2	
Performance hardware	**65**		56		26	30
Partitions	3	Partitions take only what they need (determine by the weight)	5	Partitions take everything available (determine by the weight)	3	
Processor(s) I/O	3	Dedicated processors	5	Same processors (CPU & I/O)	1	
Flexibility (ad-hoc demand)	3	A partition can use unused cycles from other partitions	4	Partition will always use all cycles available (determine by the weight)	2	
On demand	2	Annual cost for the service	3	Must purchase additional processors	2	
Experience (virtualization)	2	Close to 20 years	4	2 years +	2	
Performance software	**75**		61		26	35
Virtual machines	4	Virtual machines only use what they need	5	See Partition	3	
Control	4	Weight & priority	4	Weight only	2	
Flexibility (ad-hoc demand)	4	A virtual machine can use unused cycles from other virtual machines	4	N/A		
Utilisation reporting	3	Performance ToolKit	3	In-house tool	2	
Deployment (speed)	**50**		44		21	23
New environment creation	4	Define a new virtual machine & use the cloner	5	Define a partition & install the operating system	3	
Network	3	New definitions VLAN (VM) & firewalls	4	Network cards, cables, ports in router if new server and firewall	1	
I/O	3	Shared FICON/ESCON ports	4	HBA + ports in director, cables if new server	2	
Easiness to manage software keys	10		8		4	4
	2	Calculated with the number of IFLs per partition	4	Add all processors on which the software is running, must consider virtual vs physical	2	
Disaster recovery	**130**		117		35	82
Exercises	4	Remote installation	5	Staff on site (New Jersey)	2	
Operating system recovery	5	Disk recovery (from backup)	5	Installation of the operating system	1	
Testing results	4	Complete & successful (the process is identical as z/OS)	4	Not enough time to complete the tests	1	
Hardware isolation	4	z/VM is independent of the hardware	4	Must have compatible hardware (might need the same identical hardware)	1	
Backups	5	Well known & integrated process (from mainframe expertise)	4	Limited trust in the process	2	
Inventory	4	One unique inventory	5	Multiple inventories	1	
Security	**25**		23		16	7
Certification	3	LPAR EAL5A	5	Partition EAL 4+	4	
Cryptography	2	CPACF + Crypto cards	4	Software	2	
RAS	**55**		48		22	26
Redundancy	4	Backup processors always available	5	Backup processors only available if on demand package available ($)	2	
Operating system	4	100% of planned time	4	AIX, Windows, SAN	2	
Disks	3	Partitions 9980 & FICON	4	HDS 9585 & FCP and disk towers	2	
Total	460		407		170	237
			88,48%		36,96%	

Centre de services partagés Québec

21

Architecture

Centre de services partagés Québec

22

Architecture
Networks within the box

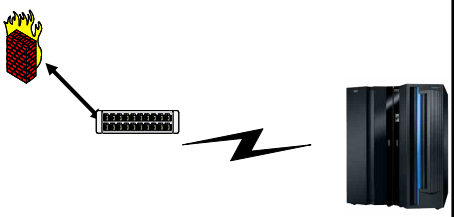
- A variety of choices for networks that keep the clients isolated
  - **OSA devices**
    - *Traditional connectivity from mainframe to physical switches*
  - **HiperSockets**
    - *Inter and Intra LPAR connectivity*
  - **Guest LANs**
    - *Connect virtual machines on virtual networks within an LPAR*
  - **VSWITCHes**
    - *Connect **guest LANs** to physical switches using **OSA devices***
    - *40+* VSWITCHes on 8 LPARs

Centre de services partagés Québec

23

Architecture
Networking with the real world

- We use a lot of VSWITCH networks.
  - Over 40 …
- VSWITCH connects to OSA port as conforms to the physical network topology.
- Redundancy provided only for production networks.
  - Handled within VSWITCH connecting to multiple unique OSA ports.
  - Does not require VIPA
- Some OSA ports shared across zones in multiple LPARs.
- Firewalling done downstream from the mainframe.



Centre de services partagés Québec

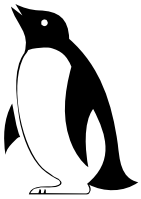
24

Architecture
We harden our Linux on the mainframe servers

- The Linux golden images are hardened, tested and certified by an independent team before allowing the image to be cloned.

Hardening tasks:

- Removing unneeded login accounts
- Removing many supplied services such as FTP, Telnet, and NFS.
- Sifting through the startup /etc/rc.d tasks and removing unneeded tasks.
- Using PAM authentication with strong password practices.
- Using Tripwire to inventory software and for file anomaly detection.
- Ethical hacking done on a regular basis for penetration testing and cracking.
  - Certified by an independent team.

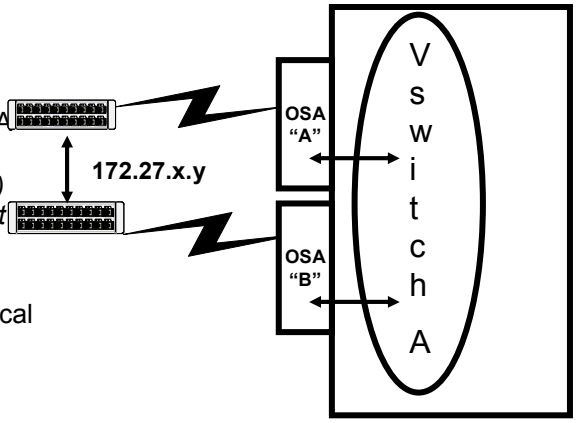


Centre de services partagés Québec

25

Architecture
Production Network Redondancy

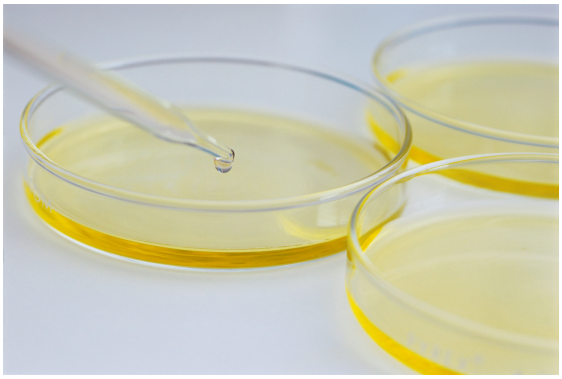
- 7of the networks (production) have redundancy with dual OSA ports.
  All others networks (30+) do not have redundant networking
- Managed by Vswitch.
- Connect to different physical switches.
- Switches are bridged.



Centre de services partagés Québec

26

Cloning Process



Centre de services partagés Québec

27

Cloning Process

- Capitalizing on z/VM virtual network technology
- Linux on z/VM replication mantra: « install once clone often »
- Creating the Linux golden images :
  - Linux Operating System = base golden image
  - Add administration tools = enhanced golden image
  - Add software = service golden image
  - Golden image certification before going to production
  - General deployment
- Responding to the Challenge: Guaranteeing Client Isolation
- Transcending Technical Cultures

Centre de services partagés Québec

28

Cloning Process
Golden images : z/VM & Linux

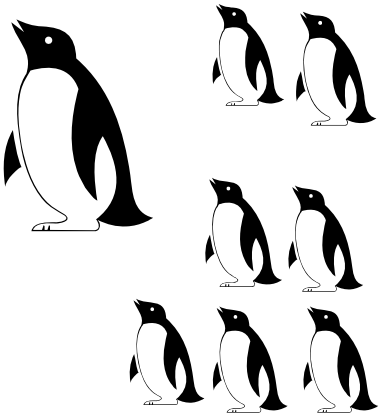
- Our z/VM golden image:
  - z/VM 5.3.0
  - All production mdisks on one volume per system
  - Goal is to service from one system
  - One flavor
- Our Linux on the mainframe golden images:
  - Novell SLES 8 or 9 or 10
  - Hardened
  - One application flavor per virtual server (Oracle or WAS)
  - Input to the cloner
- Both are rigorously tested and certified

Centre de services partagés Québec

29

Cloning Process
The Linux Golden Image
"*install once and clone often*"

- The golden image is really black and white and waddles on ice but not until:
  - Installed
  - Serviced
  - Hardened
  - Tested by various groups
  - Passes security penetration tests and certification
- There are a few masters and many many many clones!

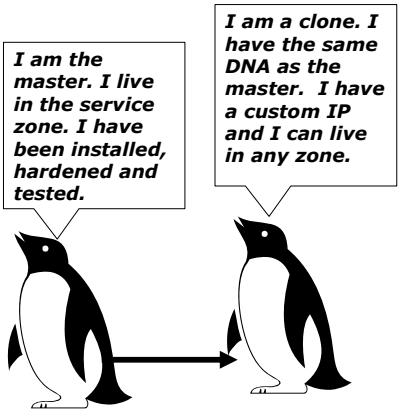


Centre de services partagés Québec

30

Cloning Process
Our cloner : Overview

- Hand crafted
- Pride of ownership
- Not a disk copier
- Intelligent decisions:
  - Choice of Linux
  - Choice of application
  - System and application position
  - VSWITCH membership
  - VLAN membership
  - IP address
  - Data replicated
  - Strong passwords

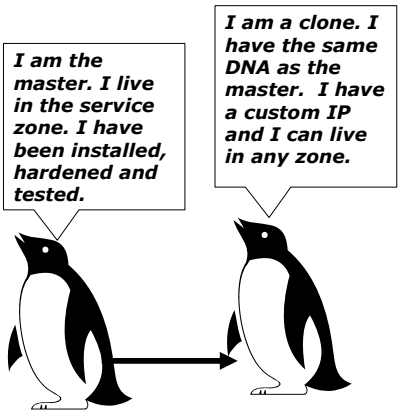


Centre de services partagés Québec

31

Cloning Process
Our cloner: Coding and interfaces

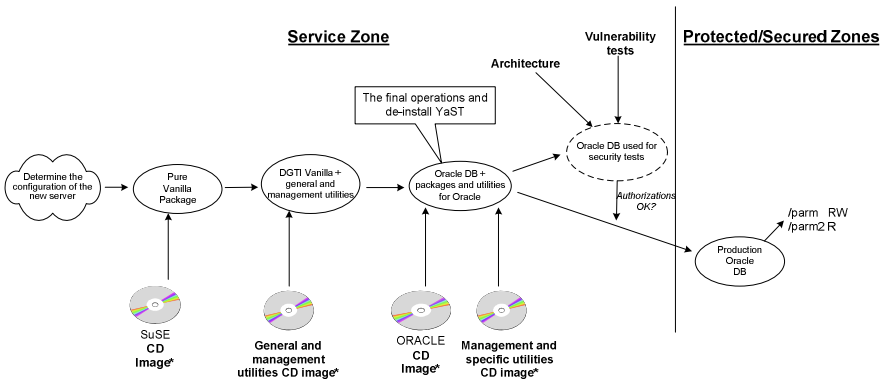
- Coded in REXX and PIPELINEs.
- Interfaces to DIRMAINT and RACF.
- Inputs include which system, application, storage size, etc.
- Interfaces with 3270.
- Can clone only from service zone to any other zone.



Centre de services partagés Québec

32

Cloning Process
The cloner at the DGTIC

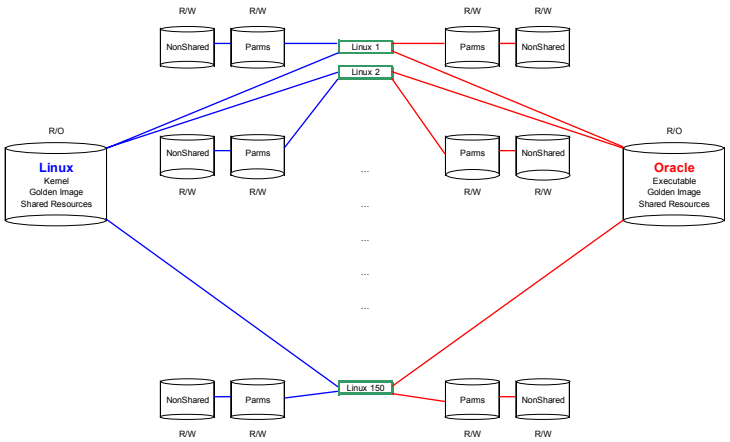


* : These images reside on a virtual Linux server in the service zone for access via FTP. This server contains software libraries.

Centre de services partagés Québec

33

Cloning Process
The BIG Picture



de services partagés Québec

34

Cloning Process
DGTI Customizations of linux

- *No modifications to kernel source*
- Customized the initrd ramdisk file system at boot time:
  1. Premount file systems
  2. Preload dasd modules and device modules
  3. Create devices needed for device modules
  4. Mount bind real file systems onto virtual
  5. Switch to new file system
- Cleanup standard boot.local
- Custom initrd is created with modified mkinitrd (dgticinitrd) – executed whenever changes are required, or kernel is patched.

Centre de services partagés Québec

35

Cloning Process
To share or not to share

Mini-disk	Description	Mount Point	Access
0150	Start up	/boot	R/O
0152	Main shared disk /etc /bin /sbin /usr /lib /software	/SHARED	R/O
0154	Installation directory for optional software	/opt	R/O
0155	Scripts and binaries for DGTIC needs	/DGI	R/O
0151	Root	/	R/W
0153	Configuration parms for the Linux server (host name, IP address, routes, paasword files, config files for LVM & SSH)	/parm	R/W
0156	Data directory /users /var /deposit_axway /srv	/DATA	R/W
0157	Data for tripwire	/tripwire	R/W

90%

10%

Centre de services partagés Québec

36

Best Practices

Centre de services partagés Québec

37

Best practices At the DGTI

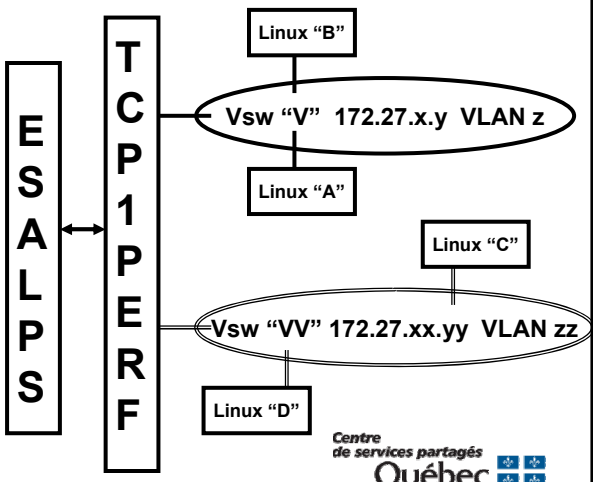
- In our project we planned to utilize best practices for systems and network management.
- Examples of in use best practices:
  - Networking:
    - Performance data collection using private VSWITCHes
    - Manage multiple networks from a single TCPMAINT
    - Production VLANs
  - Systems:
    - Golden images (z/VM & Linux)
    - Cloning engine
    - Sharing resources the DGTIC way
    - Sharing resources the IBM way

Centre de services partagés Québec

38

Best Practices
Performance data collection using private VSWITCHes

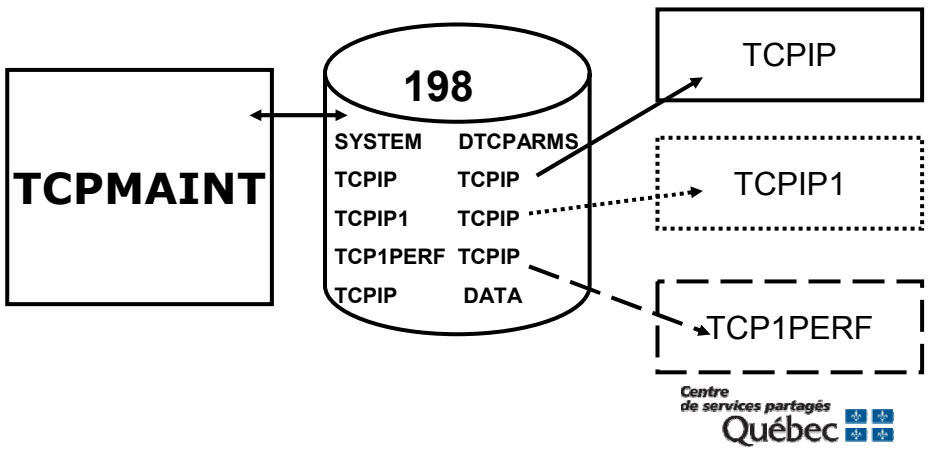
- A TCPIP stack with multiple guest LANs and VLANs collects data for the Velocity SNMP data collection.
- The VSWITCHes are defined without real devices.
- Membership in the VSWITCH and VLAN is RACF protected.



Centre de services partagés Québec

39

Best Practices
Administering multiple z/VM TCPIP machines from a single TCPMAINT



Centre de services partagés Québec

40

Resource sharing
HiperSockets network on the z9-EC

HiperSockets 192.168.150.x Chpid "BF"							
Service	Test	Domino 1	Domino 2	ORACLE	Open Source	WAS MBQ	WAS MBQ

- **Internal network only.**
- **Used for administrative purposes.**
- **Applications include the cloner, telnet, RSCS (file transfer and message queues).**
- **Secure memory-to-memory transfer.**

Centre de services partagés Québec

41

Project Status

- Oracle Databases
- WAS Migration
- Domino Pilot
- OpenSource initiatives

Centre de services partagés Québec

42

Project Status
Oracle Databases

- Original migration almost complete (95% completed)
  - Close to 200 Oracle instances
  - Running within 150 virtual machines (Linux)
- Current projects
  1) Oracle upgrade from v.9i to v.10gR1
  2) Oracle upgrade from v.10g to v.10gR1
  3) Linux upgrade (SuSE SLES 10 + maintenance)
  4) Second generation of the clones (Golden Image v.2)
  5) Data migration from Lightning to USP from HDS
- Because of the cloning engine and sharing strategy
  - Realization time = 4 months (Sept. To Dec.) vs 12+ months using the old fashioned way (mid-range hardware without cloning)

Centre de services partagés Québec

Project Status
WAS Migration

- Migration project WAS, WMB & MQ to System z
  - Close to 80 instances of WAS
  - 12 WMB & MQ servers
- Current projects
  1) WAS upgrade from v.5 to v.6.0.2
  2) WMB upgrade from v.5 to v.6
  3) MQ upgrade from v.6 to v.6
  4) Second generation of the clones (Golden Image v.2)
  5) Platform change
- Because of the cloning engine and sharing strategy
  - Realization time = 4 months (Sept. To Dec.) vs 12+ months using the old fashioned way (mid-range hardware without cloning)
- ***Note*** : We can do both projects (Oracle & WAS) in parallel !!!

Centre de services partagés Québec

Project Status
Domino Pilot

- Current project
  - Pilot for dozens of users
  - Domino Server v.7
  - Notes clients v.5, v.6.5 & v.7
  - Outlook clients (with DAMO)
- Go/No-Go decision in Sept. 2007
- Total migration of one Government department (CSPQ)
  - About 1800 users
- If migration successful (by the end of 2007)
  - Development of a Government Offering
    - Reduction of 900 mail servers

Centre de services partagés Québec

45

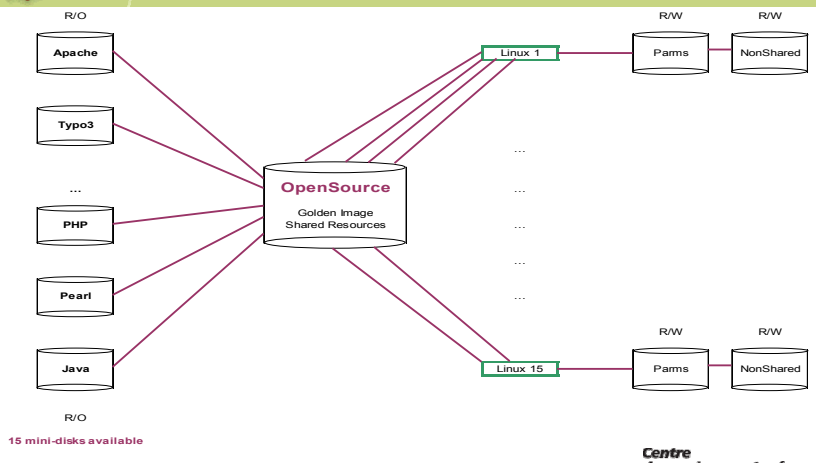
Project Status
OpenSource initiatives

- Current projects
  1) Government Intranet
  2) WEB sites (15)
  3) JBoss project with a Government department
- The current offering (16)
  - HTTP server : Apache
  - File Transfer : VsFTPD
  - Languages: JAVA & PHP & Pearl & Python
  - Databases : MySQL & PostGreSQL
  - Content manager : Typo3
  - WAS-like : JBoss & JBPM & TomCat
  - Security : OpenSSL & OpenLDAP
  - Anti-Virus : ClamAV
  - PDF generator : iText
- More packages can be added on-demand within the OpenSource Golden Image (between 2 days and 2 weeks of effort including adjustments of the cloner)
- Customers waiting avidly for this offering

Centre de services partagés Québec

46

Project Status
OpenSource initiatives



Centre de services partagés Québec

47

Lessons Learned

Centre de services partagés Québec

48

Lessons learned Volume 1

- Acceptance of virtual servers quicker than expected.
  - Grew to 200 Oracle servers ahead of plan.
- Fully tasked personnel (big shoulders):
  - Confirmed our expectation that 2 Linux administrators can support all virtual Linux servers.
    - *100:1 ratio of Linux virtual machines to administrator*
  - 2 z/VM systems programmers supporting 8 LPARs: (could support many more)
    - *New to z/VM*
    - *Mentored by consultant*
    - *z/VM support will be integrated into MVS group by year end 2007*
- Less than fully tasked personnel (arms and legs):
  - *Security administrator*
  - *Network programming*
  - *Storage*
  - *Automation*
  - *Performance*

Centre de services partagés Québec

49

Lessons learned Volume 2

- Big win early win with successful disaster recovery.
- Administration and reporting on centralized servers is excellent.
- Lots of new documentation and procedures integral part of project.
- Lots of training required.

Centre de services partagés Québec

50

Lessons learned Volume 3

- Critical mass of servers required – use more than 1 Linux virtual machine for benchmark, POCs, and business case!
- Initially, project was done for the $ savings, now the important gains:
  1) The flexibility of the solution
  2) Disaster recovery
  3) $ savings
- You must have a sponsor. Our sponsor was the operations directorate for the mainframe business interested in solving DR issues.

Centre de services partagés Québec

51

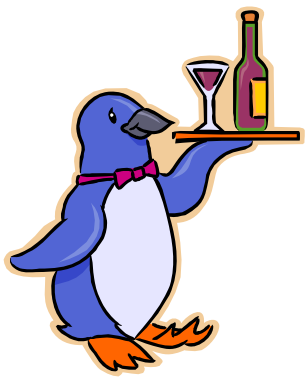
Lessons learned Oracle Project

- Mostly business as usual for the DBAs:
  - Use SSH client or “X” windows (no 3270 usage)
  - DBAs comment on rapid performance of I/O
  - DB loading faster than in other platforms.
- Benign ignorance of the virtual machine
  - Linux administration performed by Linux sysadmin.
  - z/VM administration performed by VM sysprogs.
- Rapid creation of new databases in virtual machines for testing, acceptance, and production.
- Initial install was difficult but once incorporated into cloning methods subsequent installs quick and easy.
- Almost all client needs satisfied with ORACLE cloned image (they don’t know).
  - ~ 2% require some sort of customizing.

Centre de services partagés Québec

52

Conclusion



Centre de services partagés Québec

53

Conclusion

- z/VM and Linux on the mainframe: a powerful combination for the CSPQ/DGTI
- Supported open source software on the mainframe provides the stability of z/VM with the ability to run modern applications.
- Service being offered to many government offices and agencies.
- The word is out that z/VM and Linux on the mainframe is a good place to host your applications:
  - Internal government emails and announcements from the project office promoting z/VM and Linux on the mainframe solution.
- Rapid growth is forecasted:
  - *and the CSPQ/DGTI is ready to keep up with the demand.*

Centre de services partagés Québec

54

Conclusion

- CSPQ/DGTI providing infrastructure to many offices and agencies.
- Building and nurturing business case critical to success of the project.
- The training was a vital part of the client acceptance of the concept.
- Architecture was developed and polished for over one year (on going activity).
- z/VM and Linux on the System z natural fit for the vertical and horizontal growth.
- Oracle project won the Share 2007 Award for Excellence in technology
- Project success will continue into the future!

Centre de services partagés Québec

55

Questions ?

For more information :

Charles Laflamme
charles.laflamme@cspq.gouv.qc.ca

Jocelyn Hamel
jhamel@ca.ibm.com

David Kreuter
dkreuter@vm-resources.com

Centre de services partagés Québec

56

www.gouv.qc.ca

Centre de services partagés Québec

57