Security infrastructure

from distributed UNIX to Linux on System z

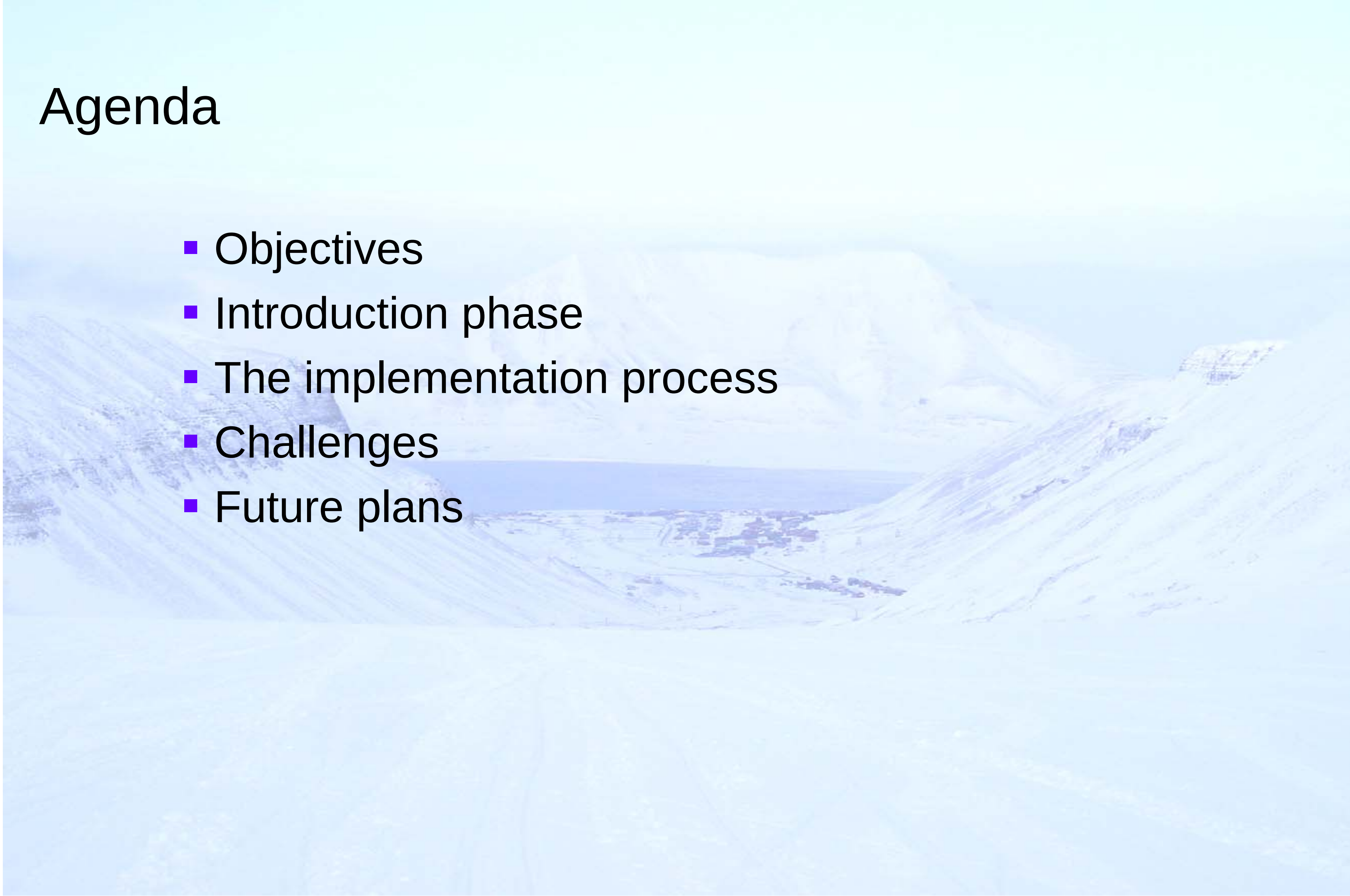
Per Fremstad

Senior I/T Specialist – IBM Certified

IBM Norway - STG

per_fremstad@no.ibm.com

Agenda



- Objectives
- Introduction phase
- The implementation process
- Challenges
- Future plans

Objectives

- The Customer
  - A reasonably large financial instituion in Norway
  - The security infrastructure for their J2EE applications
  - IT outsourced

- Objectives were to replace the original security infrastructure (distributed UNIX) with z/VM 5.2 virtual machines running SuSE Linux Enterprise Server 9 (SLES 9) with upgraded middleware

Infrastructure role

- Tivoli Access Manager for e-business (TAMeB) is used for authentication, authorization and session management for J2EE applications running in WAS on distributed
- Tivoli Directory Server is used for user registry (LDAP/DB2)

Objectives for upgrading TAM

- The original infrastructure boxes were four years old
- Software upgrade needed (TAMeB v 3.9)
- Investment in new hardware necessary for new TAM functionality to be implemented
- (The customer was satisfied with the solution running on distributed UNIX)

The original solution

- Three environments: Prod, QA and Test
- Components
  - WebSphere EdgeServer
  - Active/passive with heartbeat monitoring
  - TAMeB WebSeal
    - Active/active, heartbeat monitored from active EdgeServer
  - TAMeB and Directory Server (LDAP)
- Redundancy at all levels
- Intranet and Internet access (isolated)

Simple cost estimates

- A colleague from STG did a simple cost analysis (TCO) which showed zLinux to be a favorable alternative to new distributed UNIX boxes
- This convinced the customer (the service provider) to invest in IFLs and z/VM-zLinux on their System z mainframes

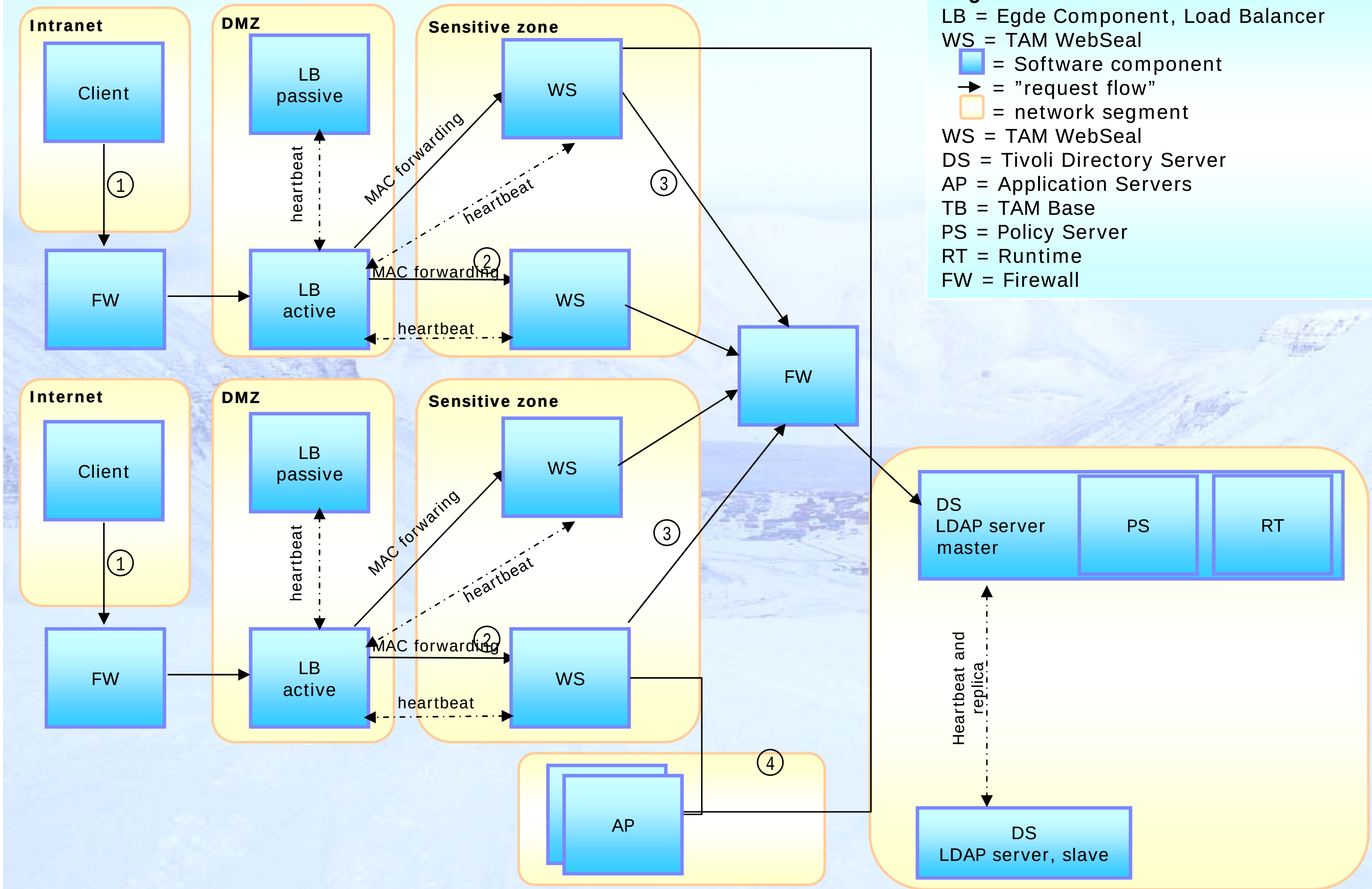
Introduction phase

- Customer attended a z/VM class and a Linux class
- z/VM 5.2 and zLinux was installed at the customer with good help from The Virtualization Cookbook for SLES9
- Thanks to Mike MacIsaac for great help!
- We also based our cloning of servers on this Redbook

Implementation experiences

- Cooperation between distributed departments and mainframe department – key for success!
- Software components must be compatible and supported !
  - OS and middleware / Software stack
  - 31- and 64-bit software components
- Available technical skills are important
  - TAM, LDAP, network and security skills needed
  - This infrastructure is not quite trivial !
- Ensure data integrity on install images with provided checksums!

Logical infrastructure, Prod



Legend

LB = Egde Component, Load Balancer

WS = TAM WebSeal

🟦 = Software component

→ = ”request flow”

🟨 = network segment

WS = TAM WebSeal

DS = Tivoli Directory Server

AP = Application Servers

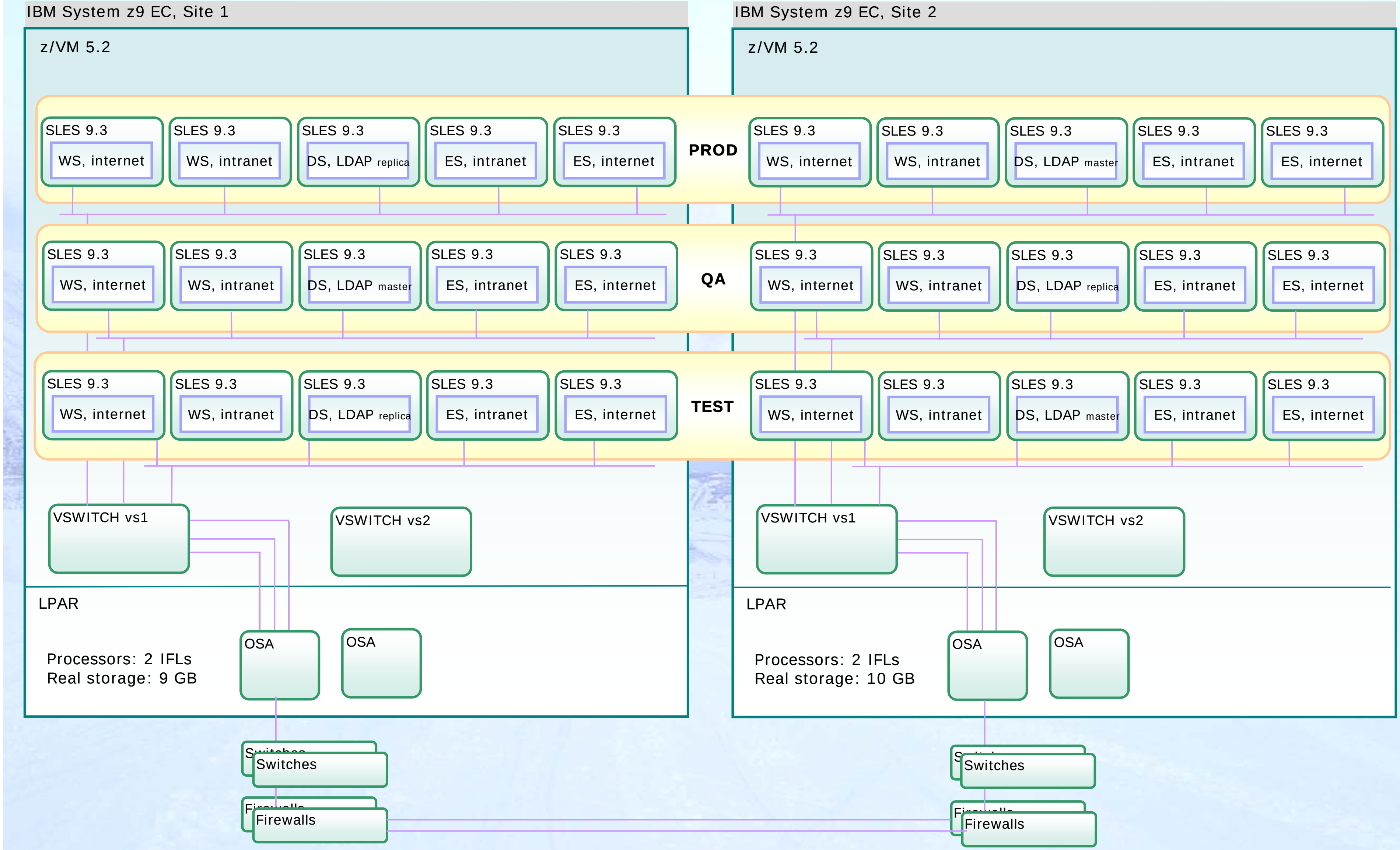
TB = TAM Base

PS = Policy Server

RT = Runtime

FW = Firewall

Logical infrastructure



IBM System z9 EC, Site 1

z/VM 5.2

PROD

SLES 9.3 WS, internet
SLES 9.3 WS, intranet
SLES 9.3 DS, LDAP replica
SLES 9.3 ES, intranet
SLES 9.3 ES, internet

QA

SLES 9.3 WS, internet
SLES 9.3 WS, intranet
SLES 9.3 DS, LDAP master
SLES 9.3 ES, intranet
SLES 9.3 ES, internet

TEST

SLES 9.3 WS, internet
SLES 9.3 WS, intranet
SLES 9.3 DS, LDAP replica
SLES 9.3 ES, intranet
SLES 9.3 ES, internet

VSWITCH vs1
VSWITCH vs2

LPAR

Processors: 2 IFLs
Real storage: 9 GB

OSA
OSA

Switches

Firewalls

IBM System z9 EC, Site 2

z/VM 5.2

PROD

SLES 9.3 WS, internet
SLES 9.3 WS, intranet
SLES 9.3 DS, LDAP master
SLES 9.3 ES, intranet
SLES 9.3 ES, internet

QA

SLES 9.3 WS, internet
SLES 9.3 WS, intranet
SLES 9.3 DS, LDAP replica
SLES 9.3 ES, intranet
SLES 9.3 ES, internet

TEST

SLES 9.3 WS, internet
SLES 9.3 WS, intranet
SLES 9.3 DS, LDAP master
SLES 9.3 ES, intranet
SLES 9.3 ES, internet

VSWITCH vs1
VSWITCH vs2

LPAR

Processors: 2 IFLs
Real storage: 10 GB

OSA
OSA

Switches

Firewalls

Challenges

- Major software upgrade
  - From TAMeB v 3.9 to TAMeB v 6.0
  - User migration was time consuming
- Entire new hardware platform
  - From distributed UNIX to System z
  - From dedicated boxes to virtual machines
    - Hence - some memory and CPU constraints
- Edge Server was not tested with network layer 2 switching
  - Caused some unpredictable problems and behavior

Our greatest challenge

- Original solution: MAC forwarding (Network layer 2 / Link layer)
- New solution: VSWITCH uses network layer 3 by default, but supports layer 2
- We decided to go for layer 3 switching between WebSphere EdgeServer and WebSeal
  - We tested it and it worked between Linux images under a single z/VM, but not across two z/VM partitions
- We decided therefore to enable layer 2 switching in the VSWITCH
  - Tested it and it worked
- But we experienced unpredictable networking behavior with layer 2
  - At that time we didn't know why and we could not isolate the problem
- Therefore, customer decided to use an external existing IP dispatching product instead of WebSphere EdgeServer
- Later we learned that EdgeServer v 6.0 (32-bit) was never tested with layer 2 switching !!
- Another challenge with the EdgeServer
  - It required a 31-bit Linux distribution !!

Future plans

- Upgrade to z/VM 5.3
- Upgrade from SLES 9.3 to SLES 10
- Three (3) LPARs (Prod, QA, Test) in each z9 EC
- Improve cloning process to include shared binaries, like TAM and WAS
- Should IBM System Director be a part of this……..?? (so far, we doubt it)
- Further consolidation of servers

Q&A

Credits

- Geir Hansen, Software specialist – Tivoli
- Per Fremstad, IT Specialist – System z
- Kristoffer Stav, IT Specialist – System z
- Mike MacIsaac, System z New Technology Center, Poughkeepsie
- Carlos Ordonez, System z New Technology Center, Poughkeepsie