The Twelve Pillars of IBM z/VM System Management

Alan Altmark, IBM

Senior Managing z/VM Consultant

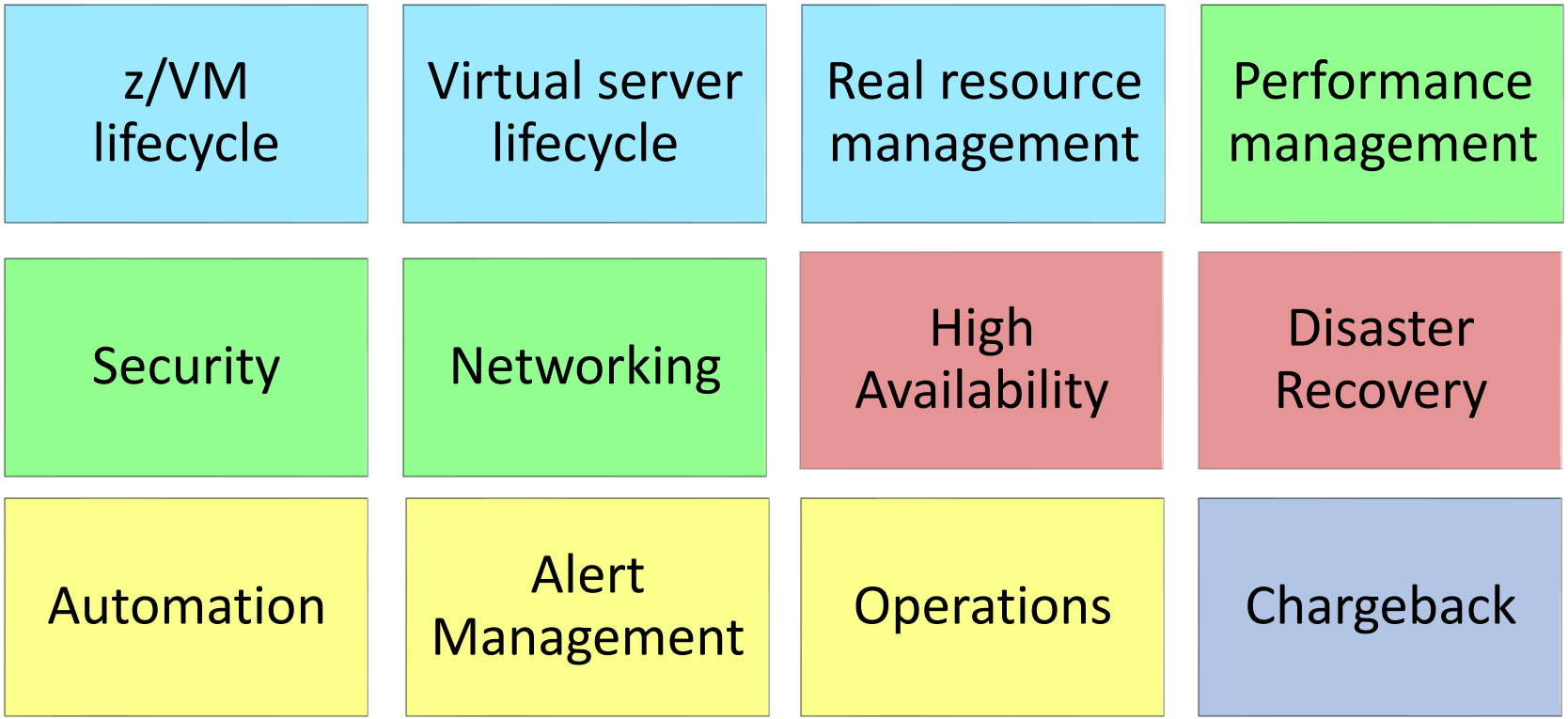
Alan_Altmark@us.ibm.com

May 8, 2019

Notes

References to IBM products, programs, or services do not imply that IBM intends to make these available in all countries in which IBM operates. Any reference to an IBM product, program, or service is not intended to state or imply that only IBM's product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe on any of the intellectual property rights of IBM may be used instead. The evaluation and verification of operation in conjunction with other products, except those expressly designed by IBM, are the responsibility of the user.

OK, so they're more like rectangles….



z/VM Hypervisor Lifecycle

- Installation
- System cloning
- Customization
- Patching: RSU, COR, SPE, fix-test
- PSP bucket
- System upgrades
- Decommission

- Practice, practice, practice dumps and patches
  - Once a quarter
  - You never know when you'll need it in a hurry!

z/VM Hypervisor Lifecycle

- Recommended Service Upgrade (RSU)
  - Selected preventive service PTFs
  - Cumulative
  - Executables pre-built
  - Conservative content
- Corrective service
  - Individual PTFs
  - Fix-test for an open APAR
  - Needed to be current
- Small Programming Enhancements (SPEs)
  - Shipped as COR service
  - MAY eventually be placed on RSU

Virtual Server Lifecycle

- Virtual machines
  - Naming conventions
- Provisioning
  - Add / Change / Delete
  - Directory manager (e.g. DIRMAINT)
  - ICP, IBM wave
- Operations
  - Start / Stop / Pause / Move

Real Resource Management

- LPAR memory, CPU
- Dynamic I/O changes
  - IODF creation and activation
  - HCD v. HCM v. DPM
- Hardware upgrade (concurrent or off/on)
- Storage migration
- Threshold and status alerts (EREP, operator)

Performance Management

- Performance management
  - Real-time
  - Historical
  - Capacity planning
  - Advisories
  - Threshold and status alerts
- Performance Toolkit: Web, 3270
- OMEGAMON
- zVPS

Security - Policy

- Policy is a **roadmap** for implementation
  - Multi-factor authentication?
  - Password phrases?
- What you are supposed to accomplish, not how
  - Follow on with an **implementation guide** that is z/VM specific
- Policy should avoid implementation-specific naming
  - “Must use the Foo Facility” can lock out platforms that have same functionality, but don’t call it “Foo”
- Virtualization services are substantially different from traditional OS services

Security - Operational

- Provisioning
  - Person or workload?
  - Naming convention v. Groups
  - Authorizations & privileges
- Emergencies & Error recovery
  - Break glass
  - Database failure
  - ESM failure

Security - Operational

- What to audit?
- Detecting configuration changes
- Penetration testing

Security - Data

- Encryption
  - In flight: TLS servers (no self-signed certs, please)
  - At rest: pervasive encryption
  - Upgrade your TN3270E clients
- Resource access controls
  - External security manager
  - Access rights review
  - Based on group membership
- Residual data management
  - Clear, purge, destroy

Networking

- TCP/IP and VSWITCH
  - Bridge, HiperSockets, VLANs

- Planning
- Bandwidth (capacity)
- Hardware (cables, ports, switches, power)
- Alert generation (failure, thresholds, drops)
- Dropped packet diagnostics

Networking

- “Just because it’s valid doesn’t mean it’s wise”
  - Sir Alan, Lord of the Protocols

- Configuration review
  - Backup port on same chpid
  - All OSAs plugged into same physical switch
  - Link aggregation / portchannel / bonding

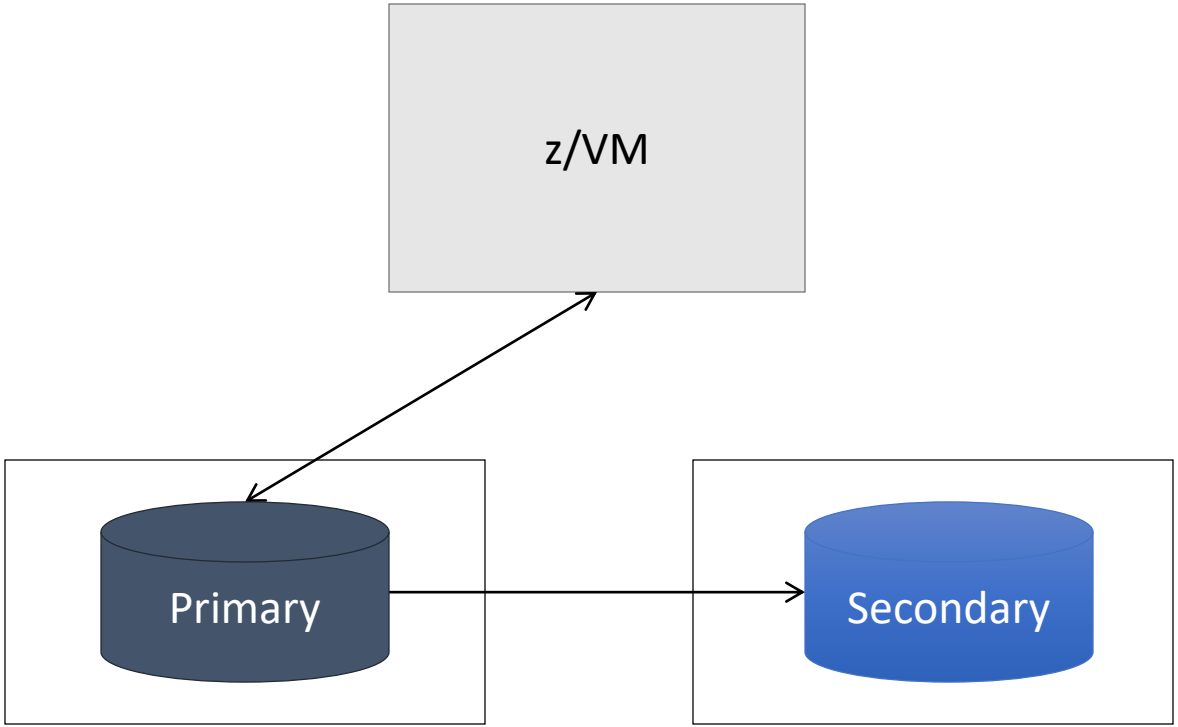
- Vulnerability assessments

- Don’t forget about RoCE!

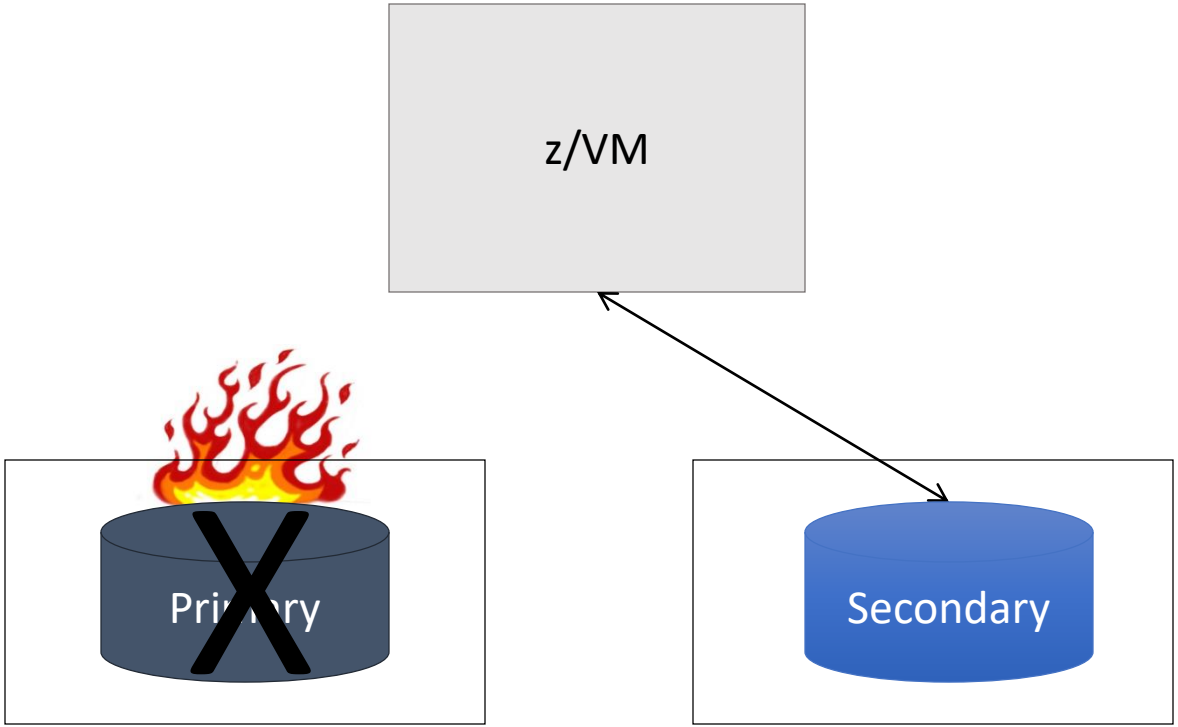
High Availability

- Single component outage
  - Planned or unplanned
  - Human or machine
- Clusters
  - Application, Database, Hypervisor, Server, Storage
  - All components eventually fail
- Storage mirrors: **GDPS®** and **hyperswap**
- Network link aggregation
- Alert generation (predictive, FYI, or unexpected)
- Archive / Retrieve (human failure)

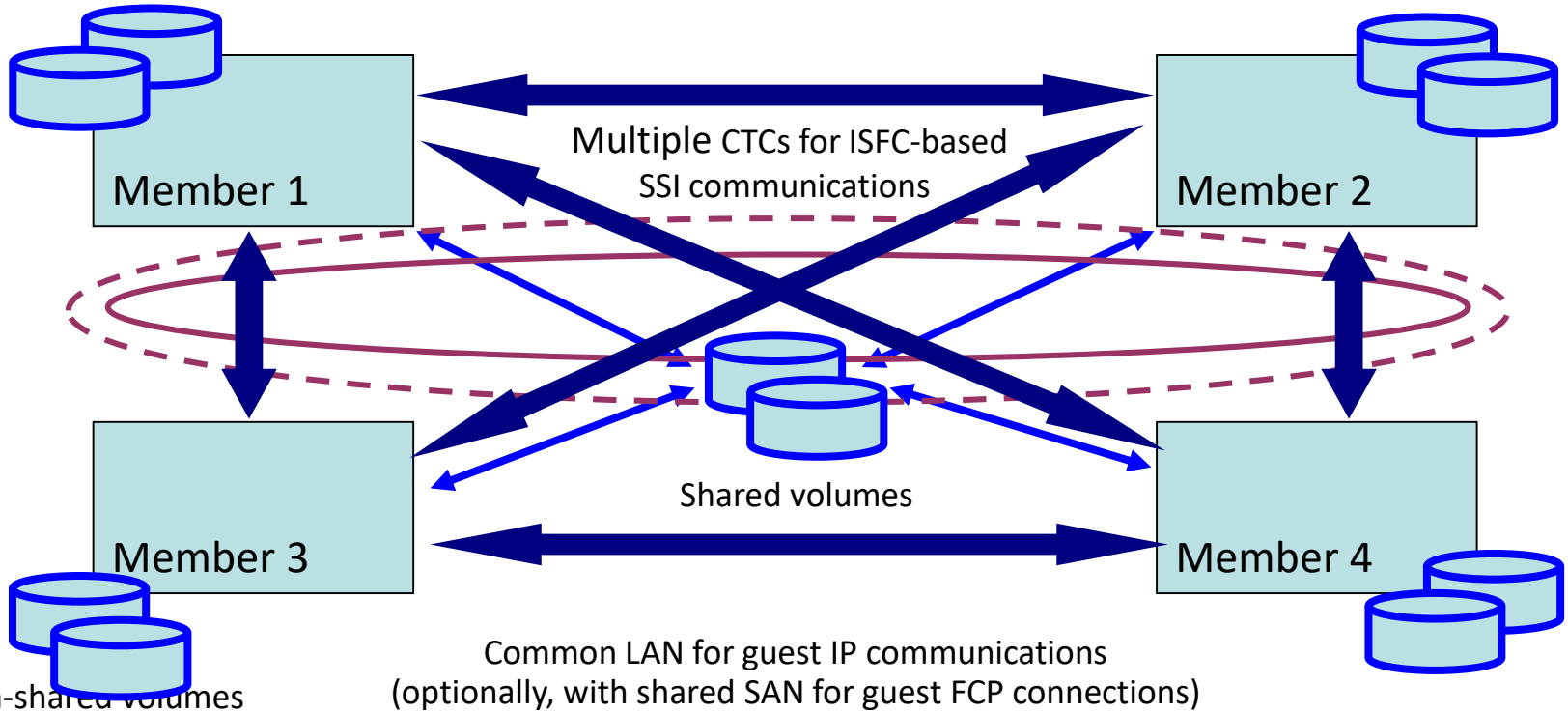
Hyperswap



Hyperswap



Single System Image



Disaster Recovery

- Multiple component failure
  - Includes complete site failure

- Asynchronous storage mirror
- Alternate machine, if you don’t have another one nearby
- GDPS-managed **region swap**

- Alternate configuration management
  - Return home
  - Planned test

- Backup / Restore

Automation

- System operator console
  - Tourist information or Important?
  - Response to prompts (e.g. from security server)
  - Use SECUSER - don’t run software IN the OPERATOR virtual machine
- Console log recording
  - All guests
  - Keep console data out of z/VM spool!
- Generate enterprise alerts
- File and command distribution
- Coordination of Flashcopy / Backup
- Startup / Shutdown staging and coordination with CP SIGNAL

Alert Management

- Performance
- User revocation (potential intrusion attempt)
- Predictive hardware failure
- FYI

- Enterprise event management integration
  - IBM, CA, HP, Microsoft, ….
  - Syslog forwarding
  - SNMP traps

- Locally generated e-mail

Operations

- IPL: Standalone program loader (SAPL)
  - LOADPARM
  - IPL parameters
  - SALIPL to set defaults

- SHUTDOWN / SHUTDOWN REIPL

- SNAPDUMP
- System restart full dump
- Stand-alone dump
- Practice, practice!

Operations

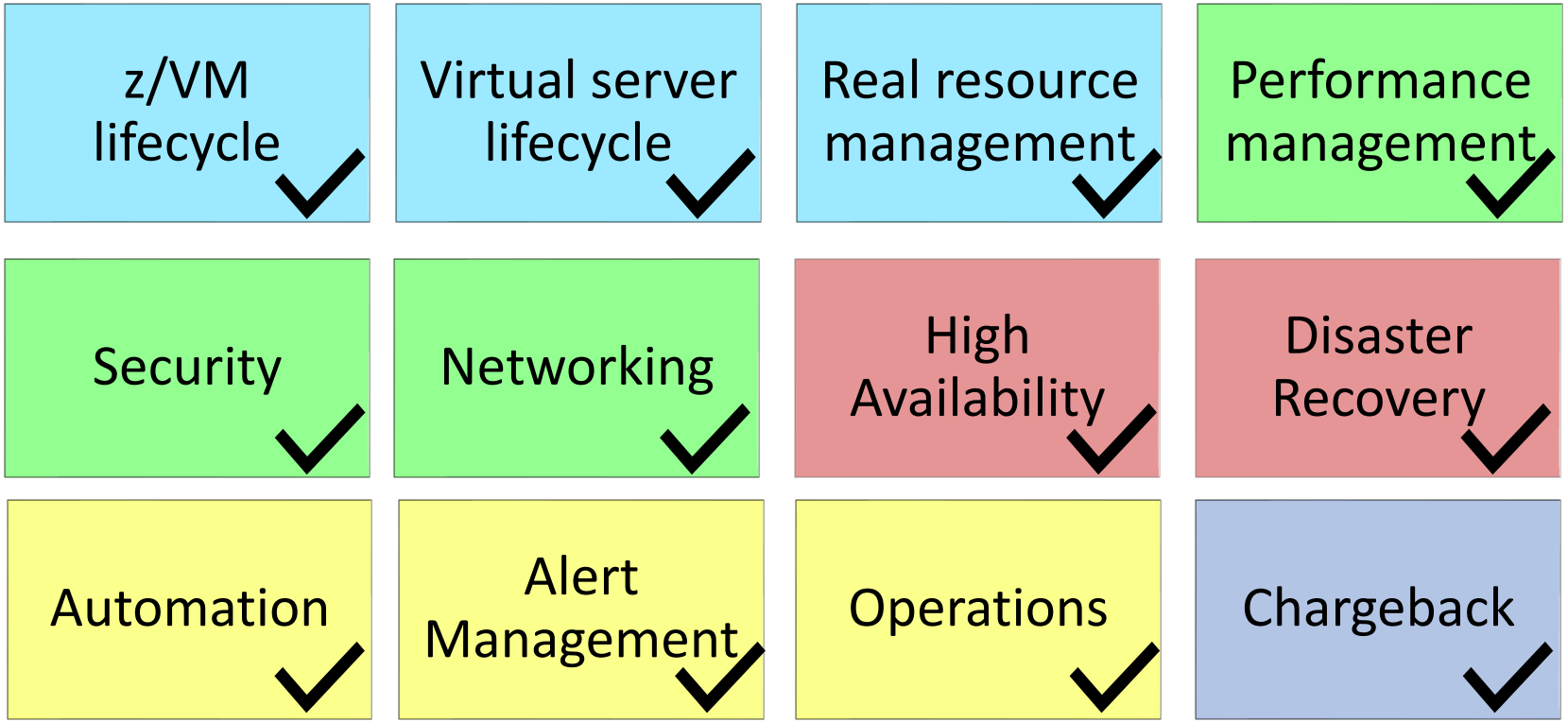
- HMC
  - Get your own ID
- OSA-ICC
  - “Gotta have it”
- Auto-IPL
- Recording: EREP (OFF), Symptom (OFF), ACCOUNT (if needed)
- Backup / Restore
- Service virtual machine (SVM) data collection and archive (sweep)

Chargeback

- Unit price per virtual server
- Unit price per CPU, disk, network
- Consumption (CPU) [hint: Don’t do this!]
- Premium charge for premium service
- See OPERACCT for accounting records

- No requirement to bill
  - May be used to calculate TCO for comparisons
  - Not using? Then turn off ACCOUNT record recording.

The goal is in sight!



Contact information

Alan Altmark
Senior Managing z/VM Consultant

IBM Systems Lab Services
z Systems Delivery Practice

IBM Systems Hardware Client Technical Team
IBM Systems Lab Services

IBM

1701 North Street
Endicott, NY 13760

Mobile 607 321 7556
Fax 607 429 3323
Email: Alan_Altmark@us.ibm.com