z/VM Version 6 Release 1

Highlights

- ***Ability to virtualize each LPAR into hundreds or more virtual machines***
- ***Ability to virtualize processor, memory, I/O and networking resources***
- ***Dynamically configure processors, memory, I/O, and networking resources***
- ***Maximizing resources to achieve high system utilization and advanced dynamic resource allocation***
- ***Advanced systems management, administration and accounting tools***

Building successful virtual enterprises

The advanced virtualization technologies available with the z/VM® hypervisor combined with the highly attractive economics on the highly secure and reliable System z10™ servers can help clients extend the business value of mainframe technology across the enterprise by integrating applications and data with exceptional levels of availability, security and operational ease.

IBM System z® has a rich heritage of innovation in the area of virtualization and has refined the infrastructure with a coordinated investment in hardware, firmware, hypervisors and operating systems to enable exceptional qualities of service in the support of virtualization. z/VM Version 6 (V6) is optimized for consolidating workloads on the System z10 servers, helping clients build an even more cost effective dynamic infrastructure with exceptional levels of business resilience, speed to market, and the flexibility to expand and contract system resources to match business needs.

IBM System z

IBM System z10 servers are designed to be integrated into a robust, flexible infrastructure. The System z10 Enterprise Class (z10 EC) server and the System z10 Business Class (z10 BC) server respond to unprecedented demand by providing high levels of performance and scalability. System z10 servers are highly utilized, virtualized, scalable, and optimized for consolidating workloads to help lower overall operating costs and improve energy efficiency.

The z10 EC server, with its advanced combination of reliability, availability, serviceability, security, scalability, and virtualization, delivers the technology that can help define this framework for the future. The z10 EC server delivers improvements to performance, capacity, and memory that can help enterprises grow their existing businesses while providing a cost-effective infrastructure for large-scale consolidation.

With increased capacity, the z10 EC server virtualization capabilities can help to support more virtual servers than any other platform—hundreds or thousands of virtual servers in a single footprint. When consolidating on System z, you can create virtual servers on demand, achieve network savings through HiperSockets™ (internal LAN), provide security to enable and support new and existing applications, help improve systems management of virtual servers and, most importantly, consolidate software from distributed platforms onto fewer processors.

The z10 BC server delivers innovative technologies for small and medium enterprises that is designed to provide a whole new world of capabilities to run modern applications. Ideally suited as the cornerstone of your new enterprise data center, this competitively priced server delivers unparalleled qualities of service to help manage growth and reduce cost and risk in your business. The z10 BC server further extends the leadership of System z by delivering expanded granularity and optimized scalability for growth, enriched virtualization technology for consolidation of distributed workloads, improved availability and security to help increase business resiliency, and just-in-time management of resources.

The System z environment, with self-configuring and self-healing attributes, provides new functions and features to meet the challenges of businesses in a dynamic infrastructure. IBM mainframes provide reliability, security, scalability, virtualization and availability.

z/VM Version 6 (V6)

Version 6 Release 1 (V6.1) is the newest version of z/VM that helps increase the advantages of deploying Linux® solutions on the mainframe and is intended to be the base for all future z/VM enhancements. z/VM V6 implements a new Architecture Level Set (ALS) available only on the IBM System z10 servers and future generations of System z servers. Requiring z10 technology or later allows z/VM to take advantage of newer hardware technology for future exploitation.

Many IBM System z clients have found that the combination of Linux on System z and z/VM not only offers server consolidation savings, but also enables the flexible deployment of business-critical enterprise solutions on System z servers configured with Integrated Facility for Linux (IFL) specialty engines. z/VM virtualization technology is designed to provide the capability for clients to run hundreds or thousands of Linux servers as z/VM guests in a single mainframe while hosting other System z operating systems for non-Linux workloads such as z/OS®, z/VSE™, and z/TPF on the same System z server or as a large-scale Linux-only enterprise-server solution. Much of the success of Linux on

the mainframe can be attributed to the advanced virtualization technologies available in z/VM.

Scalability for growth

z/VM V6.1 has capabilities that enable enterprise growth and large-scale consolidation of applications on System z10 servers using technologies to allow scalability and provide storage (memory) constraint relief. Up to 32 real processors can be configured in a single z/VM system on an IBM System z10 server helping to reduce z/VM overhead. Multiple z/VM LPARs on a single System z10 server can share the same set of CPUs, memory, I/O adapters, devices and networking cards, allowing capacity to shift from one z/VM LPAR to another if a z/VM system needs to come down for service or release upgrades. z/VM can support up to 256 GB virtual images and more than 1 terabyte (TB) of total guest virtual memory, benefiting customers with large amounts of real memory by helping reduce or eliminate the need to spread large workloads across multiple z/VM images. The actual amount of usable real and virtual memory is dependent on the amount of real memory in the z/VM logical partition, the hardware server model, firmware level and configuration, and the number of guests and their workload characteristics.

The z/VM hypervisor concurrently supports many different virtual machines, each running its own operating environment ("guest" operating system) with security and isolation features. One of the greatest strengths of z/VM is the ability to share resources, such as memory, disks, and networks among virtual machines within a single hardware server. z/VM can significantly over-commit those real resources and allow users to create a set of virtual machines with assets that considerably exceed the amount of real hardware. z/VM offers several data-in-memory techniques that further enhance the scalability and performance of memory-intensive workloads. z/VM support for System z dynamic reconfiguration features allows the nondisruptive dynamic configuration of processors, channels, OSA adapters, and memory to both the z/VM system itself and to individual guests, helping to reduce the requirement to re-IPL z/VM. Real and virtual memory management is optimized for Linux and other guests, enabling additional workloads to run simultaneously supporting the need for sizeable applications and expanding file systems.

Virtualization technology enables guests, including Linux

z/VM guest virtual machines can create virtual specialty processors on processor models that support the same types of specialty processors. This allows users to assess the operational and CPU utilization implications of configuring a z/OS system with zIIP or zAAP processors without requiring the real specialty processor hardware to be purchased. z/VM can also create virtual specialty processors for virtual machines by dispatching the virtual processors on real specialty processors, allowing available zAAP and zIIP capacity not being used by z/OS LPARs to be allocated to a z/VM LPAR hosting z/OS guests running Java™, IBM DB2®, and other zIIP- and zAAP-eligible software.

In addition to virtualizing processors, z/VM can also virtualize I/O devices and channels reducing or eliminating the need for the real hardware. z/VM can be used to host z/OS, z/VSE, and z/TPF to run transaction processing applications as well as a wide-range of UNIX® applications on Linux on System z to run on z/VM.

With z/VM and Integrated Facility for Linux (IFL) processors, a low-cost, flexible environment can be created to test and develop on Linux while simultaneously running Linux production applications. z/VM V6 support for IFL processors is designed to run Linux on System z workloads without increasing the IBM software charges for z/OS, z/VM, z/VSE, or z/TPF operating

systems and applications running on System z standard processors. Only Linux workloads in an LPAR and Linux or OpenSolaris guests of z/VM V6 can operate on IFL processors.

Linux servers running as guests of z/VM can help improve their availability due to the reliability of the underlying System z hardware. z/VM and Linux on System z work cooperatively in the management of memory, helping Linux on z/VM to run more efficiently.

z/VM support of Fibre Channel Protocol (FCP)-attached Small Computer System Interface (SCSI) disks enables the deployment and operation of a Linux server farm on z/VM using only SCSI disks.

With Discontiguous Saved Segment (DCSS) support, users can store program executables in a single z/VM memory location and share the executables with any or all of the hosted Linux systems.

Virtual Disks in Storage, in-memory emulated disks, allow guest systems to achieve memory-speed data transfers for read and write disk I/O. This technology has proven beneficial when used to store Linux swap (paging) data.

With the PTF for APAR VM64656 for z/VM V5.3 and later, targeted to be available in November, 2009, support for Crypto Express3 is planned to provide:

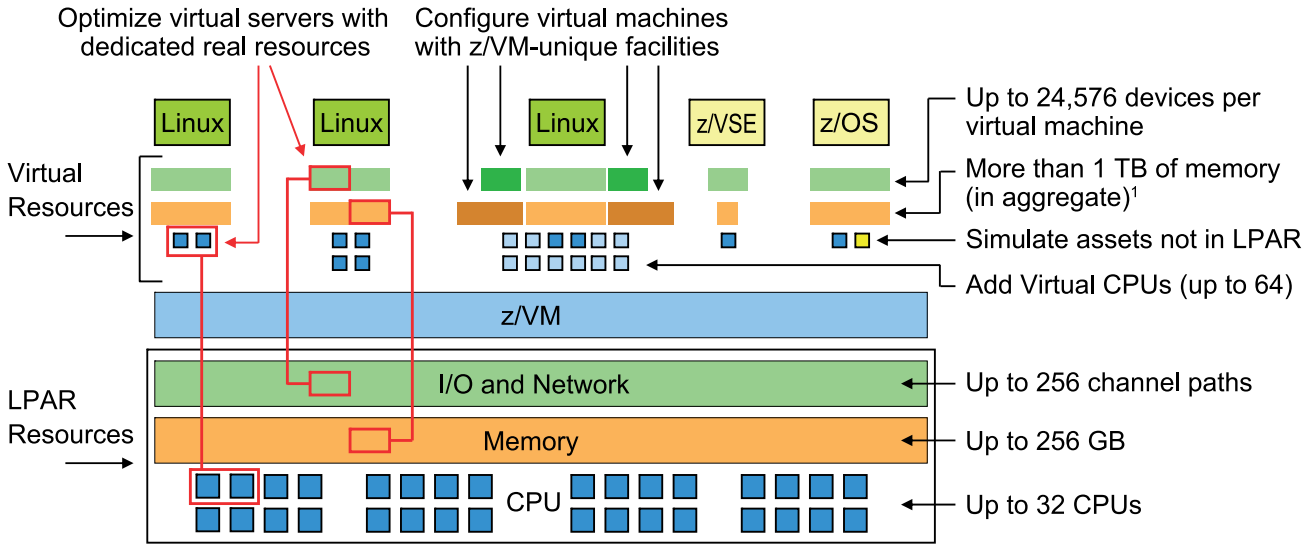
- *The ability to dedicate any available domain to a guest for clear-key and secure-key cryptographic functions*
- *The ability for guests to share available, nondedicated domains for clear-key cryptographic functions*
- *Enhancements to the* **CP QUERY CRYPTO APQS** *command to display user information about both shared and dedicated cryptographic domains. Prior to this enhancement, the command displayed user information for only dedicated domains.*

Note: All statements regarding IBM's plans, directions, and intent are subject to change or withdrawal without notice.

z/VM virtualization of the System z Coupling Facility provides a testing environment for z/OS Parallel Sysplex®.

Exploiting new technology

z/VM provides a highly flexible test and production environment for enterprises deploying the latest business solutions. Enterprises that require multi-system server solutions will find that z/VM can help them address the demands of their businesses and IT infrastructures with a broad range of support for operating system environments such as z/OS, z/VSE, z/TPF, CMS and Linux on System z. The ability to support multiple machine images and architectures enables z/VM to run multiple production and test versions of System z operating systems, all on the same System z server. z/VM can help simplify migration from one release to another, facilitate the transition to newer applications,



[1] *The actual amount of usable real and virtual memory is dependent on the amount of real memory in the z/VM logical partition, the hardware server model, firmware level and configuration, and the number of guests and their workload characteristics.*

provide a test system whenever one is needed and consolidate several systems onto one physical server. z/VM can also be used to enable access to the latest storage and processor architectures for systems that lack such support.

- *Exploitation of selected functions of the System z10 servers including support for:*
  - *z/VM-mode logical partitions, allowing all System z processor-types (CPs, IFLs, zIIPs, zAAPs, and ICFs) to be defined in the same z/VM LPAR for use by various guest operating systems to help increase flexibility.*
  - *FICON® Express8, designed to provide faster access to data.*
  - *Prefetch Data instruction, exclusive to the IBM System z10, to help manage the CPU cache in order to help improve the performance of streaming guest-to-guest workloads within a guest LAN or Virtual Switch.*
  - *Crypto Express3 for significantly better and more highly secure guest transactions than Crypto Express2.*
  - *Dynamic addition and deletion of LPARs using the z/VM Control Program's dynamic I/O command interface and the z/VM HCD/HCM support.*
  - *Dynamic configuration of processors, memory, I/O, and networking devices.*
  - *Hardware assists QDIO Enhanced Buffer-State Management (QEBSM) and Host Page-Management Assist (HPMA) to allow a cooperating guest operating system to initiate QDIO operations directly to the applicable channel, without interception by z/VM, thereby helping to provide additional performance improvements.*
  - *HiperSockets to enable memory-to-memory network connectivity between LPARs.*
  - *HyperSwap® to allow virtual devices associated with one real disk to be swapped transparently to another.*

— *Recognition of all four ports on a OSA-Express3 Gigabit Ethernet (GbE) and 1000BASE-T Ethernet feature and two ports on the GbE and 1000BASE-T 2P features on the z10 BC server provides more physical to service the network and reduce the number of required resources (I/O slots, I/O cages, and fewer CHPIDs to define and manage).*
— *OSA-Express QDIO data connection isolation for port isolation security to provide the ability to restrict guest-to-guest communications within a Virtual Switch (VSWITCH).*
— *Hardware Configuration Definition (HCD) provides I/O device information from the input/output definition file (IODF) for the World-Wide Port Name (WWPN) prediction tool (available from Resource Link™).*
— *z/VM can be installed in an LPAR and both z/VM and Linux on System z can be installed in a virtual machine from media mounted in the Hardware Management Console (HMC) DVD drive without requiring an external network to be defined.*
— *Systems management provided by the HMC and Support Element (SE) exploit the z/VM System Management APIs to allow selected virtual resources and images to be defined and managed.*
— *OSA-Express Integrated Console Controller (OSA-ICC) helping to eliminate the requirement for external console controllers. Includes four-port exploitation of OSA-ICC on the 1000BASE-T Ethernet feature planned to be available in first quarter 2010. All statements regarding IBM's plans, directions, and intent are subject to change or withdrawal without notice.*
— *Virtual switch exploitation of Layer 2 and link aggregation support for OSA-Express2 and OSA-Express3 devices.*
— *OSA-Express3 Gigabit Ethernet (GbE), 10 GbE, and 1000Base-T Ethernet.*
— *On/Off Capacity on Demand (On/Off CoD) and the Capacity Backup Upgrade (CBU) functions, including functional enhancements that allow z/VM to recognize and report changed processor configuration and capacity.*
— *Dynamic I/O configuration to define, modify and delete a Coupling channel using InfiniBand link, CHPID type CIB, when z/VM is the controlling LPAR for dynamic I/O.*

In addition to processor exploitation, z/VM also exploits features of IBM storage devices including:

- *Support for features of the IBM System Storage™ DS6000™ and IBM System Storage DS8000®:*
  — *IBM Extended Address Volumes (EAV) function of the IBM DS8000 for guests to support volumes that can scale up to approximately 223 GB (262,668 cylinders) with the PTF for APAR VM64709 for z/VM V5.4 and later. With the PTF for APAR VM64711, CMS support has been doubled, up to 65,520 cylinders, for its own use. Both PTFs are planned to be available by year-end 2009. The z/VM Control Program (CP) continues to support 65,520 cylinders for its own use. All statements regarding IBM's plans, directions, and intent are subject to change or withdrawal without notice.*
  — *IBM FlashCopy® SE feature of the IBM DS8000, which provides a space-efficient snapshot capability that can greatly reduce the storage capacity needed for point-in-time copies with the PTFs for APARs VM64605 and VM64684.*

— *Parallel Access Volumes (PAVs) as minidisks for guest operating systems that exploit the PAV architecture and provide the potential benefit of PAVs for I/O issued to minidisks owned or shared by guests that do not exploit PAVs.*
— *Hyper Parallel Access Volume (HyperPAV) for the DS8000 for guests to potentially reduce the number of alias-device addresses needed for parallel I/O operations.*
— *Dynamic Volume Expansion simplifies disk management by allowing the dynamic increase of a DS8000 volume size to accommodate application data growth.*
— *IBM System Storage FlashCopy point-in-time copy solutions, designed to enable business continuance and to help improve business efficiency*
— *Guest use of Peer-to-Peer Remote Copy Extended Distance (PPRC-XD), designed to copy full volumes of data in non-synchronous mode.*

- *Support for features of the IBM System Storage TS1120 and IBM System Storage TS1130:*
  — *Drive-based data encryption designed to help protect data on tape in a cost-effective way*
- *Manage IBM TotalStorage® 3494 and 3500 tape libraries and IBM System Storage TS7700 Virtualization Engine containing 3590 and 3592 drives, including support for:*
  — *Write Once Read Many (WORM) data cartridges.*
  — *Disk-only tape configurations provided by the TS7720, well-suited for disaster recovery and data consolidation, protection, and sharing.*

Systems management

Systems management of z/VM consists of many functions and products or features working together to provide the tools for systems administrators to help keep z/VM and its guests running at the most optimal level and utilizing resources efficiently.

The z/VM Virtual Systems Management Application Programming Interface (SMAPI), a multitasking server, helps simplify the task of managing many virtual images running under a single z/VM image. A platform-independent client interface reduces the amount of z/VM-specific programming skill required to create and manage virtual images. SMAPI is a central hub for virtual image management that is utilized by numerous z/VM functions as well as the System z HMC. SMAPI provides integrated access to the IBM Directory Maintenance Facility (DirMaint™) or a vendor-supplied directory manager. IBM Systems Director for Linux on System z exploits SMAPI in order to provide advanced GUI-based systems management functions for both z/VM itself and virtual Linux images. The

System z HMC exploits the SMAPI to enable basic systems management functions without having to establish network connections, reducing complex system configuration.

Virtual Machine Resource Manager
The Virtual Machine Resource Manager (VMRM) provides functions to dynamically tune the z/VM system. Groups of virtual machines can be defined to be part of a workload. The workloads can then be managed to CPU and DASD I/O goals. VMRM automatically adjusts performance parameters when there is contention for a resource between virtual machines. VMRM also provides z/VM and Linux guests with the ability to manage memory constraints. VMRM detects when there is such constraint and notifies specific Linux virtual guests, which can then take action to adjust their memory utilization in order to relieve this constraint on the system.

Hardware Configuration Manager and Hardware Configuration Definition
The Hardware Configuration Manager (HCM) and Hardware Configuration Definition (HCD) components allow system administrators to create and manage the I/O configuration, providing a comprehensive, easy-to-use I/O configuration-management environment similar to that available with z/OS.

Programmable Operator Facility
The Programmable Operator Facility (PROP) is designed to increase the efficiency of system operation and to allow remote operation of systems in a distributed data processing environment. It does this by intercepting all messages and requests directed to its virtual machine and by handling them according to preprogrammed actions. It determines whether a message is to be simply recorded for future reference, whether the message is to be acted upon, or whether the message is to be sent on to an operator to handle.

HMC support for z/VM
The HMC can provide out-of-the-box, integrated GUI-based basic management of z/VM its guests. The HMC automatically detects z/VM images running on System z servers that it is enabled to manage. Management capabilities include the ability to:

- *Create new z/VM guests*
- *Activate and deactivate z/VM guests*
- *Display status and configuration information for all z/VM guests.*
- *Allocate additional disk space to the hypervisor*
- *Dynamically tune the z/VM system.*

These basic z/VM systems-management functions are performed from the HMC without having to establish network connections.

Installation using the HMC
The HMC with the Support Element (SE) on the System z10 servers can be used to install z/VM from DVD media into an LPAR or a z/VM virtual machine. It can also be used to install Linux on System z into a z/VM virtual machine. This support is intended for customers who have no alternative, such as a LAN-based server, for serving the DVD contents for installation.

Directory management

Directory Maintenance Facility (DirMaint)

IBM DirMaint is an optional, priced feature of z/VM that is designed to provide efficient and highly secure interactive facilities for maintaining the z/VM system directory. Directory management is simplified by the DirMaint command interface and automated facilities. DirMaint provides a command corresponding to every z/VM directory statement. DirMaint error checking validates directory changes and permits only authorized personnel to make them. The directory management functions of DirMaint are integrated with the security management functions of the RACF® Security Server, reducing the administrative effort and skills needed to deploy and manage users and their resources when DirMaint and RACF are used together. This eliminates the need to manually define and manage z/VM resources in RACF, reducing the possibility of incomplete or incorrect RACF configuration. DirMaint also provides support for the Systems Management APIs. DirMaint provides end-user authentication of password phrases, if one is defined in an external security manager (ESM).

Additional systems management products from IBM

IBM provides additional products to assist in the management of z/VM systems including:

- **IBM Operations Manager for z/VM**

IBM Operations Manager for z/VM is designed to help improve the monitoring and management of z/VM systems and virtual machines, including guests such as Linux on System z by providing the ability to automate routine maintenance tasks and automatically respond to predictable situations that require intervention. Operations Manager allows z/VM system programmers and administrators to devote their time to other critical tasks. It also assists with monitoring and problem determination by allowing authorized users to view and interact with live consoles of z/VM service machines or Linux guests.

- **IBM Backup and Restore Manager for z/VM**

IBM Backup and Restore Manager for z/VM is designed to provide z/VM system administrators and operators the ability to efficiently and effectively back up and restore files and data on z/VM systems, including guest operating systems, such as Linux on System z. Source files and data can be both CMS and non-CMS format and the target media can be disk or tape. Backup and Restore Manager's full flexibility is apparent in its ability to do full physical and logical backup and restore operations with support for inclusion and exclusion of files, user IDs, and more.

- **IBM Tape Manager for z/VM**

IBM Tape Manager for z/VM is designed to provide z/VM system administrators and operators the ability to manage, monitor, and protect tape resources on z/VM systems. By helping to automate common daily tape operations and eliminate tedious, often error-prone, manual steps, Tape Manager can help increase data availability and improve administrator productivity.

- **IBM Archive Manager for z/VM**

IBM Archive Manager addresses storage and data management concerns by allowing users to archive historical or other infrequently used data to increase data availability and helps companies comply with data storage requirements mandated by fiscal or legal regulations and policies.

- **IBM Systems Director for Linux on System z**

Delivers a simplified platform management solution that streamlines the way physical and virtual systems are managed across a multisystem environment. Leveraging industry standards, IBM Systems Director supports multiple operating systems and virtualization technologies across IBM and non-IBM platforms. Through an easy-to-use, point-and-click, single user interface, IBM Systems Director provides consistent views for visualizing managed systems and determining how these systems relate to one another while identifying their individual status, thus helping to correlate technical resources with business needs. The z/VM Manageability Access Point (zMAP) agent is provided for IBM Systems Director to communicate with z/VM. This agent, now supplied with z/VM V6, allows IBM Systems Director server to obtain information about guest virtual machines as well as take action on behalf of these virtual machines such as create, manage, and delete. This agent runs in a Linux guest on z/VM.

- **IBM Systems Director VMControl Image Manager for Linux on System z**

IBM Systems Director VMControl Image Manager for Linux on System z, V2.1 is designed to simplify the management of virtual environments across multiple virtualization technologies and physical platforms to support the growing requirements of a dynamic infrastructure. IBM Systems Director VMControl Image Manager V2.1 is a plug-in to IBM Systems Director V6.1, providing support to manage and automate the deployment of virtual appliances (images) from a centralized location.

- **IBM Tivoli® virtualization management products for Linux on System z**

Tivoli provides a host of systems management products for managing Linux on System z. For specific products and releases, refer to the Tivoli platform support matrix at:
ibm.com/software/sysmgmt/products/support/Tivoli_Supported_Platforms.html

Performance management

Performance Toolkit for VM

The Performance Toolkit for VM, an optional, priced feature of z/VM, provides enhanced capabilities for a z/VM systems programmer, operator or performance analyst to monitor and report performance information. The Performance Toolkit for VM provides:

- *Full-screen system console operation and management of multiple z/VM systems (local or remote).*
- *Post-processing to produce VM history files and VM monitor data captured by the MONWRITE utility.*
- *Viewing of performance monitor data using either a Web browser or PC-based 3270 emulator graphics.*
- *Monitoring for TCP/IP for VM.*
- *Processing of Linux performance data obtained from the Resource Management Facility (RMF) Linux performance gatherer (rmfpms). Linux performance data obtained from RMF can be viewed and printed similar to the way that VM data is viewed and presented.*

Tivoli OMEGAMON XE on z/VM and Linux

OMEGAMON® XE on z/VM and Linux provides a wide range of information about the z/VM and Linux on System z operating systems, including information about your Linux instances running as z/VM guests and the Linux workloads, revealing how they are performing and affecting z/VM and each other. Capabilities include:

- *Comparing Linux operations side by side with detailed performance metrics from other important systems.*
- *Collecting data from the Performance Toolkit for VM (which is a prerequisite) complements data collected by the IBM Tivoli Monitoring for Linux for zSeries® agent.*
- *Navigation between Tivoli Enterprise Portal workspaces with Dynamic Workspace Linking.*
- *Viewing and monitoring workloads for virtual machines, groups, response times and LPAR reporting and viewing reports on z/VM and Linux usage of resources such as CPU utilization, storage, mini-disks and TCP/IP.*
- *Helping executives understand how systems performance influences business and the bottom line with high-level views.*
- *IT staff can more easily track complex problems that span multiple systems and platforms and share related information with granular views.*

Security

RACF Security Server

The RACF Security Server is an optional, priced feature of z/VM that works with the z/VM Control Program to provide improved z/VM system access and data security controls. RACF is designed to help meet today's need for industrial-strength information security by providing:

- *Encrypted extended-length mixed-case passwords and password life-cycle management*
- *Access Control Lists (ACLs) for z/VM system resources and networks*
- *Separation of system and security administration duties*
- *Authentication, authorization, and audit services to other products or servers*
- *Protection of customer-defined resources*
- *The ability to implement multiple security zones in a single z/VM instance*
- *A detailed record of administrator and virtual server activities*

All of these functions help you to provide a more secure, audit-ready foundation for users and virtual servers.

In addition to helping to secure the z/VM system itself, the RACF authentication, authorization and audit services are available to remote hosts through the z/VM LDAP server adapted from the IBM Tivoli Directory Server for z/OS. For example, authorization services are available to Linux by use of the Linux LDAP pluggable authentication module (PAM).

IBM recommends that all z/VM systems that have access to sensitive programs or data have an external security manager such as the IBM RACF Security Server installed to help ensure that access to those programs or data can be properly managed and audited in conformance with organizational and/or regulatory security policies.

Tivoli zSecure Manager for RACF z/VM

IBM Tivoli zSecure Manager for RACF z/VM is designed to provide administrators with tools to help unleash the potential of your mainframe system—enabling efficient and effective RACF administration, while helping use fewer resources. By automating many recurring system administration functions, Tivoli zSecure Manager for RACF z/VM can help you maximize IT resources, reduce errors, improve quality of services and demonstrate compliance. Capabilities include:

- *Automate complex, time consuming z/VM security management tasks with simple, one-step actions that can be performed without detailed knowledge of RACF commands*
- *Quickly identify and prevent problems in RACF before they become a threat to security and compliance*
- *Help ease the burden of database consolidation*
- *Create comprehensive audit trails without substantial manual effort*
- *Generate and view customized audit reports with flexible schedule and event sections*

Disk encryption

To help ensure your data-at-rest stays safe and secure, z/VM supports the use of the IBM Full Disk Encryption features of the IBM DS8000. No z/VM configuration change is required to use the encryption features. The encryption status of a volume is easily determined using a simple z/VM command.

Tape encryption

z/VM helps to protect data on tape in a cost-effective way by providing support for drive-based data encryption using the IBM System Storage TS1120 Tape Drive (machine type 3592, model E05) and the IBM System Storage TS1130 Tape Drive (machine type 3592, model E06). Encryption of tapes requires that the IBM Encryption Key Manager be running on another operating system, using an out-of-band (such as TCP/IP) connection to the tape control unit. z/VM support includes encryption for DDR and SPXTAPE, as well as for guests that do not provide their own encryption enablement (for example, CMS and Linux for System z). z/VM also enables encryption of tapes by guests (such as z/OS) that have the ability to control the tape-encryption facilities themselves and to optionally run the Encryption Key Manager. Previously encrypted tape cartridges can be re-encrypted with a new set of keys without reading and re-writing the data on the cartridge, allowing for continuous protection of tape cartridge data as the encryption certificates that were used to create them are changed or replaced.

z/VSE guests can use DFSMS/VM FL221 to locate encryption-capable 3592 tape drives in an Enterprise Automated Tape Library.

SSL server

The TCP/IP for z/VM SSL server is available to facilitate security-rich and private conversations between z/VM servers and external clients. With z/VM support for SSL and TLS, a VM server can communicate with a secure client without a change to the server itself. The SSL server supplied with z/VM supports 40-bit, 56-bit and 128-bit encryption/decryption services. The SSL server can provide transparent support for protocols that can be encapsulated in a secure SSL session, such as HTTPS, and it provides services to applications that need to transition from clear-text to secure-text such as TN3270, FTP, and SMTP.

Cryptographic Acceleration

The Cryptographic features of the IBM System z10 is designed to satisfy high-end server security requirements. It can be configured as coprocessors for secure key transactions or as an accelerator for Secure Sockets Layer (SSL) acceleration, providing significant improvements in the performance of cryptographic algorithms used for encryption and public-private keypair generation and verification. z/VM makes the Crypto Express2 and Crypto Express3 features available to guests with either dedicated access for use for both secure-key and clear-key operations or with shared access for clear-key operations.

The CP Assist for Cryptographic Function (CPACF) is a part of each processor in the IBM System z server. It provides a set of cryptographic functions that focuses on the encryption/decryption function of SSL, Virtual Private Network (VPN), and data-storing applications. The CPACF is used by SSL/TLS functions included in the z/VM Lightweight Directory Access Protocol (LDAP) client and server, and by the SSL functions provided by the z/VM SSL server. Any virtual machine can access the functions of the CPACF by using the Message-Security Assist (MSA) extensions of the IBM System z processor architecture. No explicit z/VM authorization or configuration is required.

Common Criteria certification

z/VM V5.3 with the RACF Security Server feature was certified by the German Federal Office of Information Security (Bundesamt für Sicherheit in der Informationstechnik [BSI]) for conformance to the Controlled Access Protection Profile (CAPP) and Labeled Security Protection Profile (LSPP) of the Common Criteria standard for IT security, ISO/IEC 15408, at Evaluation Assurance Level 4, augmented by flaw remediation procedures (EAL4+). z/VM V6.1 has not been evaluated for conformance, but is designed to meet the same standards.

Networking with z/VM

z/VM provides two types of virtual networking: Guest LAN and the Virtual Switch (VSWITCH). These technologies enable guests to communicate among themselves and with other hosts in the network without the need to dedicate hardware resources to each guest.

Guest LANs

Guest LANs are simulated LAN segments that have no built-in connection to any other LAN. They connect to another network only when a guest performs routing services. They can be defined to simulate HiperSockets or OSA-Express operating in QDIO mode. Guest LANs defined to function as OSA-Express can be configured to simulate OSA Layer 2 (Ethernet) or IP mode. In Ethernet mode, each guest on the Guest LAN is referenced by its

Media Access Control (MAC) address and data is transmitted and received as complete Ethernet frames. This mode supports IP, SNA, NetBios or any other Ethernet frame format. In IP mode each guest is addressed by its IP address. IPv4 or IPv6 can be used, helping application and TCP/IP stack developers to create and test new IPv6-enabled applications and device drivers.

Virtual Switch

z/VM provides the capability to deploy virtual Ethernet switches. The z/VM Virtual Switch (VSWITCH) eliminates the need for virtual machines acting as routers to connect a Guest LAN to a physical LAN through an OSA-Express adapter. Virtual routers consume valuable processor capacity due to the need to repeatedly copy the data being transported. The VSWITCH can help alleviate these problems as well as provide centralized virtual network configuration and control. These controls enable the z/VM administrator to more easily grant and revoke access to the network. The VSWITCH provides enhanced failover support for less disruptive recovery after some common network failures, helping to improve business continuity and infrastructure reliability and availability.

As with Guest LANs, the VSWITCH supports both Layer 2 (Ethernet) and IP data transport modes.

The VSWITCH also provides support for IEEE 802.3ad link aggregation. This support is designed to allow up to eight OSA-Express ports to be grouped together into a single logical port. This helps increase bandwidth beyond that provided by a single OSA-Express adapter and provides a faster and more seamless failover in the event of a link failure.

Guests are able to take advantage of these highly available and higher-bandwidth network connections with no additional guest configuration. There is no need to define and manage multiple virtual network adapters or implement dynamic routing protocols within the guest.

z/VM Network Virtualization

z/VM provides the ability to authorize a guest connected to a z/VM Guest LAN or Virtual Switch to cause a virtual network adapter (NIC) to enter "promiscuous mode." In this mode, the guest acts as a virtual "sniffer" to capture network traffic. This capability can help an administrator (or owner of the guest virtual machine) capture network data to help resolve virtual networking problems, or can be used to implement an intrusion detection system (IDS).

z/VM exploits IEEE VLAN technology to help reduce the number of OSA-Express2 or OSA-Express3 ports required to carry traffic for multiple LAN segments. To support VLANs, z/VM provides:

- *Virtual OSA-Express and HiperSockets network interface support of VLAN tagging of Ethernet frames by guests and by CP, as described in IEEE 802.1q.*
- *Virtual access ports that allow assignment of VLAN-unaware guests to specific VLANs without any change to the guest IP configuration.*
- *Virtual trunk ports that allow VLAN-aware guests to use any authorized VLAN.*
- *The ability to consolidate VLAN authorizations within an external security manager (ESM) such as RACF.*
- *Simplified networking administration and management of VLANs with support for Generic Attribute Registration Protocol (GARP) VLAN Registration Protocol (GVRP) using OSA-Express2 or OSA-Express3 on z/VM*

z/VM provides the ability to restrict guest-to-guest communications within a VSWITCH and between shared OSA-Express adapters used by the VSWITCH. Virtual Switch port isolation and QDIO data connection isolation can help you design virtual networks that adhere to strict traffic-separation policies. Traffic isolation on shared

OSA-Express adapters is available for OSA-Express2 and OSA-Express3 features on a System z10 EC server and z10 BC server with required minimum MCLs.

The z10 EC and z10 BC servers are designed to include:

- *Virtualized adapter interruptions: TCP/IP stack support allows adapter interruptions to be used for OSA-Express2 and OSA-Express3 channels and TCP/IP for z/VM can benefit from this performance assist for both HiperSockets and OSA-Express adapters. z/VM provides support for hardware performance assists to allow adapter interruptions to be passed directly to z/VM guests for OSA-Express, FCP and HiperSockets operating on a z10 EC and z10 BC server. These assists include:*
  - *QDIO Enhanced Buffer-State Management (QEBSM)—two new hardware instructions designed to help eliminate the overhead of VM-Hypervisor interception for cooperating guest operating systems that initiate QDIO operations.*
  - *Host Page-Management Assist (HPMA)—an interface to the z/VM paging-storage management function designed to allow page frames to be assigned, locked and unlocked without z/VM Hypervisor assistance, primarily benefiting the QEBSM environment.*

TCP/IP for z/VM

TCP/IP is used to build interconnections between networks (including the Internet) through open, industry-standard communication services. z/VM TCP/IP communicates with other hosts using a variety of technologies:

- *OSA-Express2 or OSA-Express3*
- *System z HiperSockets*
- *Channel-to-Channel*
- *z/VM IUCV*

In order to enable z/VM to connect to emerging IPv6 networks, the TCP/IP stack, the dynamic routing server, and the telnet server all provide support for IPv6.

The multi-protocol dynamic routing server (MPRoute) implements Open Shortest Path First (OSPF) and Routing Information Protocol (RIP), providing a powerful alternative to TCP/IP static routing. When properly configured, a z/VM host running the MPRoute server can become an active OSPF or RIP network router, providing network access to z/VM virtual networks. The MPRoute server allows the generation of up to 16 equal-cost routes to a destination, thus providing robust load-balancing support.

To simplify configuration, TCP/IP dynamically discovers the best Maximum Transmission Unit (MTU) size of a given path through the network. This helps to reduce fragmentation and packet congestion along the path, minimizing wasted network resources and helping to improve throughput by sending datagrams at the path MTU size. This function is automatically enabled for all IPv6 links and can be optionally enabled for IPv4 links.

Virtual IP Addressing (VIPA) can increase the reliability and availability of TCP/IP in the event of a network or interface failure. With VIPA, hardware link fault-tolerance is supplied for both inbound and outbound TCP/IP communications on z/VM, which can provide automatic recovery of hard link failures and network traffic splitting. VIPA support is designed to improve the ability of the TCP/IP stack to maintain connections in the event that a real network device fails.

Likewise, when the z/VM TCP/IP stack has two or more Ethernet devices on the same network and one device is stopped or fails, traffic destined for the failing device (or any devices the failing device had previously taken over) is automatically rerouted to an operating

device. This “IP takeover” support is provided for OSA-Express2 or OSA-Express3, Virtual IP Addresses (VIPAs) and addresses for which proxy ARP services are being provided through a takeover-eligible device.

A configuration wizard, **IPWIZARD**, automates the connection of a newly installed z/VM system to an IP network. This easy-to-use tool can help the z/VM installer provide IP configuration information such as host and domain names, IP addresses and subnet masks. This tool can generate an initial z/VM TCP/IP configuration and verifies that connectivity to the network has been established. Once the initial IP network configuration has been created, a dynamic TCP/IP configuration tool, **IFCONFIG**, is available that can eliminate the need to learn the statement syntax of the z/VM TCP/IP server configuration file. This tool can optionally generate configuration statements for incorporation into the configuration file so that the changes can be made permanent.

z/VM includes support for File Transfer Protocol (FTP). Files can be transferred to or from CMS minidisks, the Shared File System (SFS) or POSIX Byte File System (BFS). Remote FTP clients can also send files to CMS user’s virtual reader such that the CMS user can RECEIVE the file. File transfers can be secured using SSL/TLS in accordance with RFC 4217. Support for the Clear Command Channel (CCC) command is included to allow secure file transfer through a firewall without requiring any pre-configured port numbers.

The Network File System (NFS) V3 server allows applications and users from heterogeneous systems to access files stored in the VM Byte File System (BFS), Shared File System (SFS), and CMS minidisk file system. Through NFS, remote workstations or servers can access the CMS data stored on a z/VM system. Likewise, the z/VM NFS client gives CMS users and applications transparent access to data on remote systems that run NFS servers.

The Simple Mail Transfer Protocol (SMTP) server, which includes TCP/IP mail services, is integrated with CMS mail functions. This can deliver a consistent method of mail and file transfer for TCP/IP and CMS users. The SMTP server provides service extension support, including acceptance and forwarding of MIME-formatted messages and establishment of SSL/TLS-protected connections as defined by RFC 3207.

The Internet Message Access Protocol (IMAP) server allows you to use the strengths of z/VM (which include reliability, availability and security) for storing and serving electronic mail to clients that conform to the IMAP specification of RFC 3501. The IMAP server provides a user authentication exit to handle authentication by a user-written exit routine, providing greater flexibility for choosing authentication methods.

Access to virtual machine consoles is provided by the z/VM telnet server. Support for TN3270 and TN3270E is provided, including the ability to secure the connection using SSL/TLS-enabled telnet client such as IBM Personal Communications.

Users or applications can execute a command on a remote host and receive results based upon TCP/IP remote execution protocol (REXEC) and support from z/VM. Because the REXEC protocol transmits passwords in clear-text, REXEC should be used only to talk to hosts connected by internal networks.

TCP/IP for z/VM allows you to print data from your z/VM system on remote printers in your TCP/IP network. It also delivers enterprise-wide network printer support with line printer router (LPR), line printer daemon (LPD) and TN3270E printer attachment. VM LPR, LPD and TN3270E print support is incorporated into the RSCS print server. You can choose to have remote print data processed for delivery by either TCP/IP or RSCS.

z/VM provides network management support with Simple Network Management Protocol (SNMP):

- *The SNMPTRAP utility can be used to send messages or alerts to a central monitoring system. These messages are usually used to inform the monitor about special conditions that have occurred either in an agent system or in the network.*
- *The Virtual Switch SNMP Subagent provides the capability to monitor z/VM virtual switches from a Network Management System (NMS). This subagent provides the industry-standard bridge MIB variables defined in RFC 1493. In addition to being able in query the state of the virtual switch, the NMS is notified of virtual networking events such as changes in OSA-Express status.*

Message Queuing (MQ) is a popular method for applications to interface with one another across heterogeneous systems. MQ communication requires client API support on the communicating platforms and a message queue manager (MQ server) somewhere in the network. The MQ server facilitates communication between applications without requiring them to actually connect to one another. The IBM MQSeries® Client library is supplied with z/VM enabling CMS-based MQ applications to interact with other IBM WebSphere® MQ and MQSeries applications and servers.

Statements of Direction for z/VM V6.1

- **z/VM Single System Image**
  IBM intends to provide capabilities that permit multiple z/VM systems to collaborate in order to provide a single system image. This is planned to allow all z/VM member systems to be managed, serviced, and administered as one system across which workloads can be deployed. The single system image is intended to share resources among all member systems.
- **z/VM Live Guest Relocation**
  IBM intends to further strengthen single system image support by providing live guest relocation. This is planned to provide the capability to move a running Linux virtual machine from one single system image member system to another. This is intended to further enhance workload management across a set of z/VM systems and to help clients avoid planned outages for virtual servers.
- **Withdrawal of z/VM Domain Name System (DNS) Server Support**
  IBM intends to withdraw support in a future z/VM release for its native DNS server (NAMESRV). IBM does not plan to provide a replacement DNS server, but will continue to support the use of DNS servers on other platforms for TCP/IP host name resolution.

For more information

To learn more about z/VM V6.1, visit: **ibm.com**/vm

To learn more about the IBM System z environment, contact your IBM marketing representative, IBM Business Partner or visit: **ibm.com**/systems/z/

IBM Corporation
Systems and Technology Group
Route 100
Somers, New York 10589

Produced in the United States of America
October 2009

ZSD03013-USEN-02