In this issue…

Security

OMEGAMON

Encryption Facility

Virtualization Engine

Problem determination

Academic Initiative

HMC, HCD, and HCM (oh my!)

and much more…
Letter from the editors

You knew it was bound to happen. At some point in time, we, the maniacal staff of the z/OS Hot Topics Newsletter, would find it appropriate to somehow associate ourselves with the twisted world of Oz. Luckily for us, in this case, “Oz” is merely a completely fabricated acronym for the IBM OMEGAMON z/OS Management Console—something with which we happily affiliate!

Now, Oz the land isn’t very secure—it was infiltrated by a perky teenager, for goodness’ sake. However, Oz the console, and z/OS in general, certainly is. Of all the topics covered in the Mainframe Charter (a strategic framework for IBM’s commitment to improving the mainframe), it’s this unending dedication to security that we currently admire most in z/OS. Therefore, we’ve decreed security the main topic of this, the 14th issue of the z/OS Hot Topics Newsletter!

To kick off the security focus with true Lollypop Guild fanfare, we’ve included Mission organization: Putting a lock on security by Jim Porell, Now, where did I put my keys… ? IBM Encryption Facility for z/OS by John Eells and Tan Lu, and Questions please… Unlocking the answers for Encryption Facility for z/OS by Ron Edick, Peggy Enichen, and Mike Kelly. They’re all not-to-be-missed articles about the various methods you can employ to improve the security of your system. Make sure you also catch all the other swell security-related articles we’ve included in the issue. You’ll be able to thwart those flying monkeys in no time.

Bernice Casey, Kevin Kelley and Joe Winterton cover the topic de jour for this whole bizarre tangent in The story of Oz. Skip on over for an overview of this groundbreaking advancement in the look and feel of z/OS! Also don’t miss the other articles throughout the issue that relate to z/OS usability. There’s even a call for ideas for improving the total user experience of z/OS in the centerfold alongside the ever-popular zFavorites CD.

Speaking of advancements in z/OS, how about the new munchkins coming in to manage it? Don’t miss the articles about the IBM Academic Initiative near the back of the issue, including feedback about the program and a list of the courses students can take. As you journey on, make sure you also stop to check out the selected Mainframe Challenge haikus we’ve sprinkled throughout the issue. They’re sure to grant you wisdom of wizardly proportions.

Just to keep you on your toes, whether they’re outfitted in striped stockings or not, we’ve introduced Level 2 with me department. Starting with this issue, our Level 2 with me department will feature articles that deal with various problem determination topics. The kickoff article is Got the PD blues? by Evan Haruta and Kathy Pfeiffer. Definitely check it out and watch for more PD articles in future issues!

We’re also trying out something new with the centerfold poster. No, it’s not a picture of Dorothy in her racy red shoes. It’s even better—a timeline of the life of z/OS, dating all the way back to the System/360! Go ahead and tack it on your wall as a proud shrine to your dedication to mainframes!

As always, we’re firm believers in the idea that variety is the spice of life, so we’ve included articles on topics as varied as the outfits worn by those fashionable munchkins. Find in this issue articles about the Hardware Configuration Manager, migration, the Hardware Management Console, z/OS communications server, benchmarks, availability, the IBM Virtualization Engine, and even much more.

All in all, we hope this issue bestows upon you the braininess in technology and courage in system security that you seek. (The heart part is unfortunately up to you, though hopefully yours is bigger knowing that you’re one of our beloved readers!) We hope that your journey through this issue takes you over the rainbow to better knowledge of z/OS, or at least to the end of our corny movie references. Either way, enjoy!

The Editors
newsletr@us.ibm.com
Contents

February 2006

Mission organization Putting a lock on security
BY JIM PORELL

Coming soon to a screen near you... The story of Oz
BY BERNICE CASEY, KEVIN KELLEY AND JOE WINTERTON

Winning the war on leisure time: HCM and I/O configuration management
BY DR. THOMAS KAMEI

Now, where did I put my keys...? IBM Encryption Facility for z/OS
BY JOHN EELLS AND TAN LU

Questions please... Unlocking the answers for Encryption Facility for z/OS
BY RON EDICK, PEGGY ENICHEN, AND MIKE KELLY

A security solution greater than the sum of its parts
BY TIM HAHN

RACF, you just keep getting better and better!
BY NANCY LEWALLEN AND DEBBIE MAPES

Smooth moves Seven habits of a highly effective migration
BY MARNA WALLE

Seeing the system for the trees The IBM System z9 109 Hardware Management Console
BY DON SPANGLER, KURT SCHROEDER, AND ERIC WEINMANN

A little-LDAP'll-do-ya
BY TOM SIRC AND ASHWIN VENKATRAMAN

Security alert: Do you want to proceed?
BY WAI CHOI AND RICH GUSKI

z/OS: The right ingredients for availability
BY DAVID RAFTEN

All in all we keep removing bricks from the wall Managing system constraints
BY ED MEKEEL AND MARK WISNIEWSKI

Some ping wrong? z/OS communications server can help you out
BY RICK ARMSTRONG AND MICHELE CARLO

Don't let IP data burst your bubble
BY LIN OVERBY AND MARK T. WRIGHT

No dynamic routing protocol? No problem!
BY ALFRED CHRISTENSEN AND GUS KASSIMS

It's SNA as hard as it looks Comm server: Consolidating SNA function
BY ERNIE GILMAN AND ERIKA LEWIS

HATS fantastic! Integrating host applications in an SOA environment
BY VIKRAM GULATI

Head to head with benchmarks
BY JIM PORELL

The more systems the merrier zSeries Electronic Service Agent
BY IVICA VARDIC AND MIKE EDWARDS

SystemPac is now on the menu
BY JUDY WASHO HARRIS

Revving up EWLM with IBM Virtualization Engine
BY BERNICE CASEY, ANUJA DEEDWANIYA, AND SUE SHUMWAY

And a one, and a two... All together now! Enhanced Preventive Service Planning Tool
BY KEVIN PETERS

Storage made easy Answers that won't drive you nuts
BY SEAN MCMILLEN AND EDWARD BAKER

Off to a great start! A+ for Academic Initiative
BY DON RESNIK AND MIKE TODD

Centerfold History of the mainframe poster

Back cover Coming to a college near you: z9 and zSeries operating systems curriculum

DEPARTMENTS

Letter from the editors

zFavorites CD

Level 2 with me: Got the PD blues?
BY EVAN HARUTA AND KATHY PFEIFFER

Our contributors
Mission organization
Putting a lock on security

BY JIM PORELL

This just in: Another tape with thousands of consumers’ personal data was lost off the back of a truck. In a related story, a new Trojan horse has been detected that has given hackers access to incredible amounts of business information. Fear and trepidation ensue for the online consumer. Brand images and value are lost based on perceived mismanagement of security and privacy. Each day, the complexity of securing a business seems more challenging than the day before.

Chaos reigns in the complexity of IT infrastructures
Fifty years ago, monolithic computers were introduced with punch cards and tape drives to address data processing needs. They took up a huge, physically secured raised floor with tremendous cooling and energy needs. The capabilities of those 1950’s era computers are less than the processing and storage capabilities of the iPod today. In fact, the evolution of laptops and PDAs has created a portable computing infrastructure that has eliminated most of the physical security value of the “glass house” environments of the past.

Today the Internet and the complexity of offerings within Windows® and Linux® desktops have created additional security exposures. Many of the tried and true mainframe security capabilities no longer appear relevant to this on demand world. What’s a business supposed to do to combat these losses? Well, panic is not one of the actions, though sometimes it seems that way.

Infrastructure simplification
Many times, a business will look at each server type, individually, for managing security. The mainframe team operates independently from the desktop team, which is independent of the networking team. Yet, when all these systems are interconnected, they’re really overseeing an enterprise view of security or just a collection of ill fitted piece parts? In a security conscious business, looking at the workflow, from end to end, can yield some simplifying assumptions that will reduce operational risk. It will be combinations of virtualization, open standards and collaboration across communities that can help the business simplify.

Avoiding tortured data flow
In many enterprises, managing the personally identifiable information associated with a consumer is paramount to maintaining a successful brand image. New government regulations provide penalties and/or costly actions for the inadvertent or unauthorized disclosure of such information.

So how can a business avoid that risk? Well, the first thing to do is look at how many copies of the data exist and examine the overall workflow. In the client/server era, with all the cheap computing out there, it seemed that copying the data or moving it to the applications was cost effective.

Now, in the on demand and privacy conscious world, bringing the applications to the data can be more economically feasible. There will certainly be copies of data that can’t be avoided. But don’t forget all the temporary data sets, used to stage extracts from production databases and then transferred to other temporary files and loaded into the database of another system. The business needs to protect the transient data stores as well as the master databases.

Are these resources protected? In many cases, a simple no is the answer. The above scenario is an example of a passive connection between systems and leveraging a file transfer program. By leveraging a file sharing or file serving structure, the transient data can be shared between the systems, thus eliminating a process step. An instance of the transient data is sometimes necessary to make the copy and the audit point of control. What does this mean to the business? Money savings and operational risk reductions and that’s music to most CIO’s ears.

Protecting data in flight
We’ve established that data needs to be copied or moved. Electronically, that can be achieved by database and file servers, as well as application to application transfers. These formats and protocols can be protected in a variety of ways:
1. Making sure the identification of the user is passed along with the data
2. The data being passed is encrypted.

There are a variety of mechanisms for cross platform authentication services. IBM® provides the Tivoli® Access Manager and Tivoli Directory Server to facilitate some cross platform authentication. In addition, RACF on z/OS® supports Digital Certificates with Public Key Infrastructure, Kerberos Domain Controllers and its aliasing functions to map user IDs of one domain to the z/OS domain.

Data confidentiality on a network can be achieved by exploitation of the Secure Sockets Library (SSL) or Transaction Layer Security (TLS) in a variety of middleware offerings. In addition, the use of a Virtual Private Network (VPN) and IP Security (IPSec) can encrypt all data being passed between two server systems.

For other removable media, IBM recently introduced the IBM Encryption Facility for z/OS, as well as a new encryption archive system within
DFSMSdss™. This enables tapes to be encrypted that might be shared with business partners or get stored within a vault for disaster recovery purposes. Should these tapes, inadvertently get in the wrong hands, it will be extremely difficult, if not impossible, to access the information on them. These utilities have Java™ counterparts for other systems to ensure a cross platform approach for securely sharing this removable media. Moreover, these offerings meet the requirements of several new privacy laws that state consumers would not have to be informed of the loss of encrypted media.

The network protections, authentication services and tape encryption utilities are all examples of stepping up to addressing security exposures that are beyond the walls of the glass house. Are they enough? No, there are still other areas to consider.

Putting security all together

So how can you put this into production in your business? There are a number of options:

1. Eliminate those tortured data flows. You won't eliminate them all, but any reduction should reduce the risk of inadvertent disclosure, as well as the cost of managing regulatory compliance.

2. Integration, either through virtualization or co-location of applications and database servers can further reduce operational risk.

3. Consider end-to-end costs, from a variety of perspectives, such as floor space, risk management, business continuity versus the same costs for individual piece parts. In many cases, the incremental addition of a new function to an existing server can be less expensive than the addition of a server dedicated to the new function.

4. And the last area to consider is collaboration across operations and application deployment teams. Working together, towards the elimination of stove pipes or islands of computing, may be the most difficult problem to solve, as it probably has a more organizational focus, than technological. However, opening up communications and operations across organizations might be the most effective way to improve on meeting business goals versus server centric goals.

Virtualization and integration

Open standards have allowed applications and data to be easily moved from one platform to another. While this has provided tremendous flexibility in choice of deployment and development effort, it also has increased security management domains and complexity. But have you considered that where you deploy a new application can dramatically change the operational characteristics?

In the distributed world, most applications and middleware reside in server images that are independent of the database servers that they access. These can be deployed in two basic ways: separate servers that are connected by a network or separate server images hosted as virtual images on the same hardware box. There are important distinctions between these two implementations. The virtual images may share a virtual LAN (VLAN) or HiperSocket network connection which is implemented within the hardware of the box. That means no external connection points, that reduces security intrusion points and points of failure, end to end. A virtual server Hypervisor, such as z/VM® or a PR/SM™ LPAR on zSeries®, can enable some operations and security set up changes to further simplify the complexity of the environment.

Additional integration is available on z/OS: hosting the application server and database server in the same operating system environment. This could be considered the Interstate Highway or Autobahn model of integration versus the local road or parkway styles identified above. In addition to the virtualization savings listed above, a single user authentication and access control flow can be utilized compared to one for each platform. This saves time, processing capacity and registration and audit control points.

Business continuity and recovery is easier through Parallel Sysplex® technology, zSeries architecture, such as storage protection keys and process isolation enable a greater level of business process integration with a level of integrity not available on alternative architectures. Besides inhibiting one application from inadvertently affecting the operations of another application, multiple middleware servers, such as CICS®, WebSphere® Application Server, IMS® and DB2® Stored Procedures can be run simultaneously, which again, simplifies business process integration, security, business resilience and workload management of an enterprise.

Regardless of how many servers are deployed, there will always be multiple administration points of control. The above examples help to demonstrate it’s not just security technology, such as RACF and network technologies, that influences the security of a business operation. It is also the levels of integration available through virtualization hypervisors, data sharing, middleware integration and hardware systems architecture, such as in the zSeries servers, that can dramatically influence the overall operational risk of an environment. You can move full speed ahead toward securing your business. Let’s hope your next headline focuses on positive business growth and not on data losses!
A security solution greater than the sum of its parts

BY TIM HAHN

Do you need to integrate multiple browser-based applications, running across multiple application servers including some running on z/OS systems in your environment? Do you need to support long rich user names, multi-factor authentication, and complex password policy settings across your applications? Do you need to employ access controls to protect your applications at multiple levels, covering multiple access paths by which those applications can be used? If the answer to any of these questions is “Yes”, then you probably want to take a closer look at using a solution from IBM to help manage user identity, and protect access to applications and information in your complex application serving environment.

Using z/OS, WebSphere Application Server for z/OS, RACF, Tivoli Access Manager, and Tivoli Identity Manager, you can build a computing infrastructure that allows you to provide all of the features above. This article describes such a solution, configured so that user and group administration as well as access control settings are managed and maintained easily and efficiently. Indeed, by using Tivoli Identity Manager for user and group management across multiple user/group registries, you can maintain a correspondence between user definitions in RACF and user definitions in an LDAP-accessible directory, the same directory that Tivoli Access Manager uses as its user/group registry.

The scenario
In this usage scenario, assume you have a set of browser-accessed applications running on two different systems in your environment. One of these applications runs in a WebSphere Application Server for z/OS environment and accesses various z/OS-based resources (IMS applications, DB2 UDB for z/OS tables, and MQ queues) as part of the application processing running within WebSphere Application Server for z/OS. On WebSphere Application Server for z/OS, the application runs using a SAF-based identity specific to the end user of the application. Another application runs on WebSphere Application Server for AIX®, using an LDAP directory-based identity corresponding to the end user of the application. This application base includes the following:

• An LDAP-accessible directory server.
• Two WebSphere Application Server deployments.
• A RACF user/group registry that supports the users running on the z/OS system.

See Figure 1.

The problem: complex password policy
Application users are accustomed to using two user IDs for the applications but are frustrated by differing password policies, password change intervals, and continually re-authenticating access to each application. Furthermore, password reset requests are quite common, requiring a significant amount of administrator time.

The solution: Tivoli Access Manager for e-Business
To ease this situation for users and at the same time provide additional layers of security for the organization, we introduce Tivoli Access Manager for e-Business into the computing environment. Deploying this product requires a number of configuration settings across the computing environment.

First, the WebSphere Application Server deployment configurations must be enabled to accept credentials passed to them from a Tivoli Access Manager reverse proxy server. In the case of WebSphere Application Server for z/OS, configured for “LocalOS” security, the security configuration must be modified to use a Trust Association Interceptor (TAI) module that is provided as part of the Access Manager for WebSphere Application Server integration package. That package is part of Tivoli Access Manager for e-Business and runs within the WebSphere Application Server for z/OS. There it transforms an incoming Tivoli Access Manager credential into a JAAS Subject that represents the SAF-based user that, in turn, corresponds to the Tivoli Access Manager user.

In a similar fashion, the WebSphere Application Server running on AIX, configured for LDAP security, must have its security configuration modified to use a Trust Association Interceptor (TAI) module provided by the Access Manager for WebSphere Application Server integration. This piece of processing, running within the WebSphere Application Server for AIX, transforms an incoming Tivoli Access Manager credential into a JAAS Subject that represents the LDAP-based user, which is identical to the Tivoli Access Manager user.

Next, Tivoli Access Manager must be deployed to support the various daemons that make up a Tivoli Access Manager deployment. A running Tivoli Access Manager deployment consists of a policy daemon (pdmgd), an LDAP-accessible directory server, and an authorization server (pdad). When you plan to use Tivoli Access Manager for e-Business, consider a set of reverse proxy servers (webseald), which act as the first point of contact for browser-based applications to contact when connecting to existing applications protected using Tivoli Access Manager.

You need to configure Tivoli Access Manager to use the LDAP-accessible directory server that the WebSphere Application Server for AIX is using. This uses user/group definitions in the LDAP-accessible directory server that you use for both Tivoli Access Manager and for the WebSphere Application Server that runs on AIX.

In configuring the Tivoli Access Manager reverse proxy servers, you need
to configure two “junctions” – one for each of the application servers to be contacted by the reverse proxy on behalf of the connecting user. When you configure these junctions, specify:

- Tivoli Access Manager credentials (iv-cred) to be passed to the downstream application
- The URL of the two applications
- Any other configuration settings.

In addition to handling user authentication, the reverse proxy servers handle two other important functions:

- **Session management**: The user’s authenticated state is maintained at the reverse proxy server allowing the user to move from application to application without re-authenticating.
- **Authorization**: Tivoli Access Manager access control settings can be employed to serve as one layer of access control checking at the URL level to protect applications that are accessible by certain users.

### Easing the burden with Tivoli Identity Manager

The use of Tivoli Access Manager for multiple applications simplifies their use while adding layers of protection in front of these applications. However, there remains the issue of managing corresponding user information across two separate user/group registries (RACF and an LDAP-accessible directory). To ease the administrative burden, you can use Tivoli Identity Manager, configured with two “services.”

A Tivoli Identity Manager deployment requires a DB2 database, LDAP directory, and WebSphere Application Server deployment in order to run the Tivoli Identity Manager application. When these are installed and configured, you can configure Tivoli Identity Manager with a service definition that communicates with RACF on z/OS and a service definition that communicates with the LDAP-accessible directory server. These two services, one using Tivoli Identity Manager’s RACF agent and one using Tivoli Identity Manager’s Tivoli Access Manager agent, allow Tivoli Identity Manager to maintain a correspondence between user definitions in the two separate registries. By setting up a policy in Tivoli Identity Manager to create users in both user registries when you add them to the environment as well as placing these users into pre-defined group definitions based on their job responsibilities, you can use a single set of processing that maintains a detailed log of operations and manage the two user registries in concert.

To cover end user password change and reset, users can utilize the Tivoli Identity Manager browser-based user interface to request password changes and resets. Tivoli Identity Manager supports a wide variety of password policy checks and can be configured with multiple challenge-response type questions that must be answered before a password reset is performed.

### Putting it all together

As Figure 1 shows, this environment provides ease of use for both end users and administrators, while providing for additional layers of access control checking and a more feature rich set of processing for password change and reset. Furthermore, because Tivoli Access Manager can be configured for a wide variety of single and multi-factor authentication mechanisms, access to the applications can be set up such that the right people can access the right applications from the right locations.

Indeed, the whole of this deployment is greater than the sum of its individual parts, simplifying usage and administration while increasing the set of security controls available for use.

---

Figure 1 - The Computing Environment using Tivoli Access Manager, Tivoli Identity Manager, WebSphere Application Server, and RACF.
No matter how good we make RACF, there’s always room for improvement. And you’re always letting us know about changes you’d like to see to make RACF more secure and more usable. In z/OS V1R7 we’ve made a number of changes to increase the security and usability of RACF.

**Mixed case passwords**
Do you ever wish that you could include lower case alphanumeric characters in your password, to be consistent with the passwords you use on other operating systems? Or do you ever wish for a larger set of allowed characters for passwords to make them safer from random attacks? We hear you, and beginning in z/OS V1R7, you can use mixed-case passwords! The new MIXEDCASE and NOMIXEDCASE options on the SETROPTS PASSWORD command allow a security administrator to specify whether mixed case passwords are allowed on a system. New keywords for password rules specify where mixed case alphabetic characters can be specified in passwords. And with the additional 26 characters allowed in passwords, the probability that a random access attempt succeeds is lowered to less than 1 in 2.5 times $10^{14}$!

When z/OS V1R7 is installed, all users have upper case passwords but are used to entering them in lower case. So that users do not have to enter their existing passwords in upper case, RACF keeps track of whether a user has changed a password to mixed case. If the user has not, the password is checked both as entered and in upper case.

Before you turn on the MIXEDCASE option, evaluate applications that issue the RACROUTE REQUEST=VERIFY macro and update them so they no longer make passwords upper case. Applications can query a new bit in the RCVT to determine whether the MIXEDCASE option is active. You also need to update your password rules to allow mixed case.

Be aware that once activated the MIXEDCASE option is intended to be left active. If you activate it and then deactivate it, users who have changed their passwords to mixed case will not be able to log on until their passwords have been reset.

**Minimum password change interval**
RACF allows a security administrator to set a maximum password interval, requiring users to change their passwords periodically. However, some users want to use the same password all the time. Previously, to circumvent the password history, when a favorite password expires these users change that password multiple times, until the original password is no longer in the password history, and then change back to the original password. Security administrators have asked us to give them the ability to set a minimum password interval, to prevent this circumvention, and in z/OS V1R7 we have! The new MINCHANGE option on the SETROPTS PASSWORD command allows a security administrator the ability to specify the minimum number of days between password changes.

The minimum change interval is enforced when a user changes his or her own password with the PASSWORD command, ALTUSER command, or RACROUTE REQUEST=VERIFY macro. Authorized users can set another user’s password before the interval has passed, but they must have CONTROL authority if they are authorized based on the IRR. PASSWORD.RESET resource in the FACILITY class.

**SMF logging of password changes**
With SETROPTS AUDIT(USER) in effect, password changes made by RACROUTE REQUEST=VERIFY are now audited, in addition to password changes made using commands. Now auditors and security administrators can always find out when and how a user’s password was changed.

**Improvements to automatic revoking of user IDs**
Did you ever set the SETROPTS INACTIVE option, and then find that an old unused user ID was still active? That happened because RACF used to set the last access date to UNKNOWN when it created a new user ID. And, as long as the user ID was not used, it would never be revoked. Beginning in z/OS V1R7, RACF sets a new user ID’s last access date to its creation date. Now those old, unused user IDs will be automatically revoked if they aren’t used before their revoke dates.

**Retain the user ID revoke date after a RESUME command**
Before z/OS V1R7, RACF cleared revoke and resume dates when you specified the REVOKE or RESUME keyword on the ALTUSER and CONNECT commands, whether you wanted them cleared or not. Now, RACF will no longer do this. Instead, new keywords on the ALTUSER and CONNECT commands, NOREVOKE and NORESUME, allow the security administrator to clear the revoke and resume dates as needed.

In addition, we’ve updated the LISTUSER and LISTGRP commands to always display the revoke date if it is present, even if it is in the past, so that you...
can determine why a user or group ID was revoked. And LISTGRP now displays the group's creation date.

**Automatic switch to backup database when I/O error occurs**

There's an I/O error on your RACF database, and suddenly the console is flooded with error messages. The operator needs to do an RVARY SWITCH to activate the backup database, but it's difficult to enter the command with all the messages coming in, and where in the heck did we put the RVARY password? It can take valuable time to find the password and enter the command. Now you don't need to. Beginning with z/OS V1R7, RACF will automatically switch to the active backup database when an I/O error is detected on the primary RACF database and the UCB indicates that the device is varied offline! And nobody needs to enter a password.

**Auditing getpsent**

Tired of getting huge quantities of SMF type 80 records for getpsent when you've set the auditing option for the PROCACT class to FAILURES? Failures are normal for getpsent, so we've changed the way RACF audits it. Now it's audited only when you specify ALWAYS as the auditing option.

**PassTicket enhancements**

We've added a callable service interface that supports problem state callers for PassTicket generation and evaluation services. With the r_ticketserv interface, you can now use PassTicket functions for 31-bit callers. The r_gensec callable service now supports 64-bit callers. And we've added a new Java interface, using a Java Native Interface (JNI), which calls the updated r_ticketserv and r_gensec callable services, allowing Java code to easily access PassTicket services running on z/OS. These changes should make it easier to use PassTicket.

**Nested ACEEs and delegated resources**

A daemon is a highly privileged UNIX® program that processes requests on behalf of clients. The daemon creates a new address space in which the security environment is that of the client. Once the new address space has been created, there is no longer a relationship between the daemon and the client. That means that the client needs to have authorization to all resources that the daemon uses.

Enter the nested ACEE, new in z/OS V1R7. An access control environment element (ACEE) is a control block that describes the user's security environment. A nested ACEE associates a client identity with the daemon that spawned it by "nesting" the daemon identity within the security environment created for the client. When a nested ACEE is used in an authorization check, if the client check fails, RACF checks the daemon's authorization. Applications can create nested ACEEs using a new keyword NESTED on the RACROUTE REQUEST=VERIFY, ENVIR=CREATE macro. By using nested ACEEs, applications can remove the need to permit large numbers of users to highly sensitive RACF-protected resources.

Unconditionally honoring a nested ACEE might inappropriately grant client access to an unintended resource. Therefore, only certain resources honor nested ACEEs in authorization checks. These resources are referred to as delegated resources. The security administrator designates a resource as delegated by placing the string “RACF-DELEGATED” in the APPLDATA field of the RACF profile protecting the resource.

**Important note:** Security administrators should only create delegated resources if directed to do so by application documentation. An application must be specifically coded to exploit nested ACEE, and the application should document the names of the resources that must be delegated in order to ensure proper functioning of that application.

---

**Haikus in honor of the mainframe**

As part of the IBM Academic Initiative's recent Mainframe Challenge, college students were asked to submit haikus (short, three-line poems) on the topic of mainframe computers. Throughout this issue, we're pleased to feature a few of our favorites.

Enjoy – and let us know how you like them!

The Editors
newsletr@us.ibm.com
Smooth moves
Seven habits of a highly effective migration

BY MARNA WALL

So, you're migrating from z/OS V1R4 to z/OS V1R7 and you want to make it go as smoothly as possible? You're on the right page, because here's a list of seven things you can do now to help make your migration to z/OS V1R7 uneventful.

Even if you're migrating from z/OS V1R5 or z/OS V1R6 to z/OS V1R7, review this list because z/OS V1R7 introduces many of these items.

1. Get on z/Architecture. z/OS V1R6 introduced an Architecture Level Set, which means you must be running in z/Architecture (64-bit) mode. Hopefully, your V1R4 system is already in z/Architecture mode, and this is not an issue. If you're not running z/Architecture yet, migrate to a z/Architecture-capable server first. On z/OS V1R4, take advantage of the Bimodal Migration Accommodation to remain in 31-bit mode according to the terms and conditions agreement. Then move to 64-bit mode using the Washington Systems Center (WSC) Flash10185 at ibm.com/support/techdocs/atmsastra.nsf/Web/Flash10185 to help you. It is strongly recommended that you migrate to z/Architecture before migrating to z/OS V1R7, to avoid migrating architecture and software level at the same time.

2. Ensure that you are running JES2 Z2 mode. z/OS V1R7 JES2 requires that your system run in Z2 mode, also known as full-function mode (and not in R4 or compatibility mode). If you depend on the control blocks and field changes that have changed for Z2 mode, you might need to change your JES2 exits and modifications. If your system is already in Z2 mode, then cross this one off your list. If your system is still running in R4 mode, see z/OS V1R7 Migration, GA22-7499, that corresponds to your current z/OS JES2 level for details about the Z2 changes. Also, see z/OS JES2 Commands, SA22-7526, for information about using ACTIVATE to go to Z2 mode.

3. Do not use JOBCATs or STEPCATs. With z/OS V1R7, you cannot use JOBCAT or STEPCAT DD statements. If a job contains a JOBCAT or STEPCAT DD statement, the first step in the job that contains the statement is unsuccessful. The job ends with accompanying message IECF034I. If you use JOBCAT or STEPCAT extensively, your jobs will be impacted, and you'll need to remove the statements. If your system is at z/OS V1R5 or V1R6, you can detect these statements more easily than you can on z/OS V1R4, and allow JOBCAT and STEPCAT to be reenabled. Nevertheless, you can't use these statements for long, because z/OS V1R7 does not support the reenablement of JOBCAT or STEPCAT.

4. Move to the International Organization for Standardization (ISO) C/C++ compilers that z/OS has been shipping (and updating) since z/OS V1R2. The ISO C/C++ compilers have changes in semantics, and add keywords. To give you time to migrate from the older compilers to the newer ones, both have been shipped in z/OS since z/OS V1R2. In V1R7, however, the OS/390® R10 C/C++ compilers are gone. You can still reinstall them on your z/OS V1R7 system with limitations, but it's going to be additional work for you (see informational APAR PK05324). If you're not yet using ISO C/C++ compilers, which are now called XL C/C++ compilers, this item affects you.

5. Get ready for the one-byte console ID support removal in V1R7. As of z/OS V1R7, almost all of the one-byte console ID support is removed. (Programs compiled using older versions of the changed macros continue to work in z/OS V1R7.) If you are running a z/OS V1R4 system with the Consoles Enhancement feature or z/OS V1R5 or higher, you can use the Console ID Tracking Utility to help identify whether you use one-byte console IDs. If your z/OS V1R4 system does not have the Consoles Enhancement feature, that support is integrated into z/OS V1R7. Use the Console ID Tracking Utility in z/OS V1R7 to help with this activity. Before using the Console ID Tracking Utility, make sure you have retrieved the latest exclusion list for your appropriate z/OS level, at ibm.com/servers/eserver/zseries/zos/downloads. Remember, in the release after z/OS V1R7, the remainder of the one-byte console ID support is intended to be removed, so position yourself to have this work done before your migration to z/OS V1R7 or while on z/OS V1R7.

6. Plan your z/OS V1R7 JES2 user exit changes. In z/OS V1R7, there are many JES2 exit changes that might...
be required because some network job entry (NJE) and existing internal-reader processing was moved from the JES2 address space to user address spaces. If you have specialized JES2 exits, you might need to make many changes to accommodate this restructure. There might also be other updates to automation and procedures you need to make based on the new JES2 processing. If these changes will be too big for you to handle during your usual migration window to z/OS V1R7, remember you can plan to stage your JES2 level, and run your existing lower JES2 release on your z/OS V1R7 system which would also allow you to delay Z2 mode for a little while longer! For details on the changes required, see z/OS V1R7 Migration, GA22-7499.

7. Understand the IODF V5 coexistence requirement in z/OS V1R7. If you want to make changes to your input/output definition file (IODF) from z/OS V1R7, upgrade your IODF to the V5 level. And you must continue to use z/OS V1R7 hardware configuration definition (HCD) to update that IODF. If you want to use a JOBLIB or STEPLIB from the lower system, you need to use the higher HCD data sets for processing. This upgrade introduces coexistence considerations when sharing your V5 IODF with lower-level systems. These coexistence considerations are more complicated if your z/OS V1R4 system does not have the z990 Compatibility or z990 Exploitation feature installed (that is, you don’t have HCD FMID HCS7708). If you intend to share an IODF between z/OS V1R7 and a lower-level system, make sure you know the requirements for which are explained in z/OS V1R7 Migration, GA22-7499. These coexistence requirements might prompt you to delay making updates to your IODF from your z/OS V1R7 system (thus, not requiring an update to the V5 IODF level). You might also consider not sharing the IODF between z/OS V1R7 and lower systems.

By understanding these seven important migration actions, your smooth move to z/OS V1R7 can be well underway before you even place your order!
Coming to a screen near you... The story of Oz
IBM OMEGAMON z/OS Management Console

BY BERNICE CASEY, KEVIN KELLEY, AND JOE WINTERTON

Once upon a time, IBM’s z/OS system management team went searching for a new, modern face for z/OS. They were looking for a system management console that would be easy to learn and use, especially for all the college graduates who would soon be pounding the pavement looking for mainframe jobs. The z/OS team knew they had to act fast. But just when they were about to give up hope, a knight in shining armor—Sir Tivoli—rode up and offered them the Tivoli Enterprise Portal as the new face of z/OS. It was a marriage made in... well, maybe not heaven, but Los Angeles, Raleigh, Poughkeepsie, and White Plains.

This is the story of the IBM OMEGAMON z/OS Management Console Release 1.1.0. (Hmm... We'd better give it an unofficial nickname or we'll run out of ink. Let's call it Oz.)

A console is born
Oz is a baby brother of IBM Tivoli OMEGAMON XE for z/OS Version 3.1.0. Figure 1 is one of our first snapshots.

Although Oz does a subset of what the full OMEGAMON XE for z/OS product can do, it is still quite powerful and can perform the following tasks with ease:

- Oz displays information about the z/OS sysplexes and systems in a customer enterprise.
- Oz monitors the availability of sysplex and system resources.
- Oz raises alerts when problems occur and offers expert advice on how to handle those events.
- Oz displays the status of z/OS health checks.

Oz alerts you by raising an event, and giving you expert advice on how to respond.

Oz raises alerts when problems occur and offers expert advice on how to handle those events.

With Oz, you can define situations. Situations are conditions that Oz looks for on the z/OS systems that it is monitoring. For example, you might tell Oz to monitor page data set utilization, and tell it to let you know when a page data set becomes 60% full. When that threshold is reached, Oz alerts you by raising an event, and giving you expert advice on how to respond. This means an operator could respond by issuing a PAGEADD command from the console. Oz ships with pre-defined situations that you can modify or disable. You can also create your own situations.

Oz displays the status of z/OS health checks.

As Figure 2 shows, the IBM Health Checker for z/OS report displays a complete list of checks, including their state (active or not) and their status. Click on a blue link, and you’ll see a detailed report for that health check. You can also associate a situation with individual checks to alert you if a health check exception occurs. For more information on the IBM Health Checker for z/OS, see z/OS Hot Topics Newsletter Issue 13, August 2005, GA22-7501-09.

Behind the scenes
So how does Oz work? Exactly the same as other members of the Tivoli OMEGAMON family.

Installation agents on each z/OS system that you want to monitor. With Oz, you get one agent that has two subagents: one subagent monitors select sysplex and system resources, and the other agent communicates with the IBM Health Checker for z/OS.

Installation agents on each z/OS system that you want to monitor. With Oz, you get one agent that has two subagents: one subagent monitors select sysplex and system resources, and the other agent communicates with the IBM Health Checker for z/OS. Agents come with other Tivoli OMEGAMON products too, not only for z/OS but also for z/VM and Linux on System z9 109 and zSeries, and for distributed systems and middleware products as well. The Oz agent is well behaved and coexists peacefully with its sister and brother agents.

The Tivoli Enterprise Monitoring Server (TEMS) collects and correlates data that comes from the agents. The TEMS can run on z/OS. You can configure multiple servers, one serving as a hub to the other servers.

The Tivoli Enterprise Portal Server (TEPS) is responsible for presenting...
data to the console user. It builds the screens shown in Figures 1 and 2. It currently runs only on Windows and Linux platforms.

The console is the Tivoli Enterprise Portal (TEP). This console runs in a web browser as a Java applet. A logon ID and password secure it. The TEP is a highly customizable console; you have a fine degree of control over how to display system information and status.

Rolling…
Let’s roll some film and see the entire process in action…

Scene 1: Dorothy, the z/OS system programmer, decides that she wants to be notified whenever there’s an exception to health check OhNo. (She created the check herself using the IBM Health Checker for z/OS custom check support.) Dorothy opens up Oz’s Situation Editor user interface, finds check OhNo, and creates a situation for it. If it triggers, a critical event surfaces to Oz and an e-mail notification is sent to her.

Scene 2: The Oz HEALTHCHECK subagent goes to work, waiting eagerly for periodic updates from the IBM Health Checker for z/OS. One day, it happens… The OhNo check gets an exception.

Scene 3: Red alert! The TEP finds out (through the TEMS, from the agent) that the OhNo situation has triggered and turns the check red in the TEP console. A critical event is surfaced in other ways too: in the TEP event log and in the TEP navigation area.

Scene 4: All’s well again. Dorothy and her team, having been notified of the event, take action to correct the problem.

A happy ending
Wish you had Oz in your life? The fact is that the IBM OMEGAMON z/OS Management Console is available right now at no cost to customers running z/OS V1R4 and above. Get your copy today! Visit the z/OS downloads page: ibm.com/servers/eserver/zseries/zos/downloads/.

Figure 1- Baby Oz displays page data set status for the first time

Figure 2- Are you ready for your next checkup? Contact Oz.
Winning the war on leisure time
HCM and I/O configuration management

BY DR. THOMAS KAMEI

Do you ever wonder about the many coffee breaks you need when you are defining and connecting a complete IBM TotalStorage® DS Family subsystem or an IBM TotalStorage Enterprise Storage Server® in your IODF? Do you know all the steps you need to take when you want to update the PCHID information of your CHPIDs? If these tasks concern you, then this is the right place to explore some of the time-saving functions of the Hardware Configuration Manager (HCM).

HCM is the Windows-based GUI of Hardware Configuration Definition (HCD) and is an optionally priced feature. In addition to creating the logical I/O configuration definitions that are stored in an IODF, HCM also allows you to produce and store the physical documentation of the whole zSeries configuration. Imagine the time you can save having all your zSeries hardware definitions within one IODF and the associated HCM configuration file.

When you define a complete IBM TotalStorage DS Family subsystem or an IBM TotalStorage Enterprise Storage Server in the IODF, you often need to define and connect a significant number of control units and devices. The problem you face is that you have to define and connect many devices to the correct control units—a labor-intensive process.

Usually, the definition of a single device is the same as the definition of many other devices for a single subsystem. Without HCM the process can be time-consuming. You can see how adding all these definitions manually is an error prone process that can actually make you lose sight of what you have already been defining and connecting. Moreover, after you’re done, you’ll need to remember all of those changes to capture in the configuration report and that can take time.

HCM to the rescue
The latest HCM Subsystem Creation wizard can help you to make all of these definitions. With HCM and a few mouse clicks, you can create and connect multiple device groups with the same definitions to control units. At the time you logically define your new subsystem with the wizard, you are also physically documenting the changes for your new subsystem. In addition, the wizard captures all of the changes for you by providing a summary report at the end of the process that allows you to recall all your configuration changes.

The following steps provide an overview of the wizard dialogs:

1. On the Create Subsystem – Set Controller Attributes and Subsystem Type page, select some controller attributes for the subsystem that you want to create. For instance, these attributes characterize the graphical representation of the new subsystem in the diagram.

2. On the Create Subsystem – Add Control Units page define all the control units of your subsystem. If the control units are all of the same type and that the offset between the control units is a constant value, you can add all required control units by just one mouse click.

3. On the Create Subsystem – Connect Control Units to Segments page, assign the control units that you have just defined into the segments of the subsystem. If you are using the Subsystem Creation wizard to define one of the two mentioned types of DASD subsystems, HCM automatically assigns the subsystems on your behalf to the only existing segment for those subsystems.

4. On the Create Subsystems – Add Strings page, define all device ranges, which are defined inside the strings. You can define multiple strings containing the same number of devices of the same device type at the same time. You can also easily and quickly define multiple strings that have different device types, for instance strings with 3390 devices and strings with 3390A devices. See Figure 1.

5. On the Create Subsystem – Connect Device Interfaces and String Interfaces page, connect the physical string interfaces to the physical controller device interfaces. Again, if you define one of the above-mentioned subsystems, HCM will automatically provide the physical connection needed inside the HCM configuration on your behalf and you’re done with this panel.

6. On the Create Subsystem – Connect Control Units and Strings page, define the logical device control unit connections. You can now connect each string (each defined device range) to one or more control units. In case the number of strings is a whole-numbered multiple of the number of control units, HCM can symmetrically assign the strings to the control units. Of course, HCM allows you to modify the logical connections according to your needs, regardless of whether an automatic assignment has initially taken place. However, if the proposed connections are those you want to establish, you’re done with your definitions.
On the final Create Subsystem – Summary page, you can save the summary of all logical and physical definitions that the wizard establishes according to the data you have entered. You immediately can obtain a detailed report of all your configuration changes. That's it! With the time you save using this wizard during the subsystem definition process, you can relax and really enjoy that coffee break.

**Speed up your subsystem connection definitions**

Let's assume you have just created your new subsystem definition using HCM’s Subsystem Creation wizard. What's missing so far are the logical and physical connections from the subsystem to the CHPIDs. Assuming that you have already created new CHPIDs and all the CHPIDs to which you want to connect the subsystem through a switch are connected to switch ports, continue with the following steps:

1. Go to the Control Unit List dialog through the Controller dialog. See Figure 2.
2. Select two or more control units, and press **Connect alike**
3. On the following Processor and CHPID Connections dialog, select the CHPIDs to which you want to connect the control units.

4. When you press OK, all previously selected control units logically connect to the selected CHPIDs.

Besides speeding up the definitions of your brand new subsystem through the wizard, these steps make the task of connecting to CHPIDs faster.

**Speed up your PCHID definition**

Your definitions are almost finished. You have created a new subsystem, and you have already connected the subsystem to some CHPIDs. If you connected the subsystem to some new CHPIDs that were just added to the configuration, you probably haven’t assigned the correct PCHID values to them yet. Rely on IBM’s CHPID Mapping Tool (CMT) to perform that task.

The CMT is a separate standalone tool running on a PC under the Microsoft® Windows® operating system. It is a tool outside of the scope of HCD and HCM, and it takes as input, along with other data, an IOCP input data set.

Because the CHPID mapping tool is a Windows based tool, and the IOCP input data set is a host based data set, in the past you had to transfer the IOCP data set manually from the host to the PC. Afterward you would have to transfer it back from the PC to the host.

Starting with z/OS HCM 1.6 Service Level 7 and IBM zSeries CHPID Mapping Tool Version 04.02, the CHPID Mapping Tool (CMT), and HCM are integrated. Therefore, with the help of HCM, you can reduce the effort you need to spend defining PCHID values to your CHPIDs in the IODF.

The following steps provide an overview of the process:

1. Locate the processor for which you want to update PCHID values, and invoke the **Edit Processor** dialog for this processor.
2. Press **CMT** in order to invoke HCM’s CHPID Mapping Tool Support dialog. This is the central dialog from an HCM point of view and integrates the CMT and HCM.

---

Figure 1- The create subsystem panel allows you to define device ranges.

Figure 2- Control unit list dialog allows you to connect control units to CHPIDs
From the **CHPID Mapping Tool Support** dialog, perform the following tasks
to update the PCHID values on your CHPIDs:

1. Create an IOCP input data set on the host, and automatically transfer it to the PC. You only have to specify the corresponding filename on your PC.
2. Once you invoke the CMT, the IOCP input data set gets passed, and you already specified the name of the IOCP input data set that contains the updates from the CMT. The previously created and transferred IOCP file transfers immediately as input to the CMT.
3. Load the modified IOCP input data set, transfer it back to the host, and migrate the modified IOCP input data set into the configuration. Besides working with the CMT itself, from an HCM point of view you just need a couple of mouse clicks in order to update the PCHID information.

You're done. Now go get yourself a cup of coffee and enjoy.


---

**New world discovered**

Mainframes are a legacy
in old lies future.

Nathan Kruser, SUNY Binghamton University

**I love the Mainframe**

It is really, really cool

How much does this cost?

Ezra Fernandez, SUNY Binghamton University
Seeing the system for the trees
The IBM System z9 109 Hardware Management Console

BY DON SPANGLER, ERIC WEINMANN, AND KURT SCHROEDER

Hardware Management Console (HMC) Version 2.9.0, which is available with the IBM System z9 109 (z9-109) server, introduces a number of technological and user interface enhancements. The changes include a choice of user interface styles to allow you to manage your hardware configuration in the manner that you prefer.

The changes also create more consistency within the HMC user interface and allow the HMC to leverage common technologies across IBM products.

A choice of interfaces
One of the most visible changes to the HMC is the use of a browser-based user interface, which can support multiple user interface styles. The HMC comes shipped with two interface styles: A new ‘tree style’ user interface and the existing (or ‘classic’) user interface style.

The tree style interface implements a hierarchical “drill down” and “launch in context” model for navigating through system resources and tasks. The tree style offers usability enhancements supported by modern user interface paradigms.

By default, the HMC uses the ‘classic’ user interface style, which provides a look and feel similar to the one with which you are familiar, but rendered for a browser environment. The classic style interface lacks the hierarchical model of the tree style interface, but is retained in the HMC to preserve compatibility with your existing operations procedures.

Other new enhancements
Besides a browser-based user interface, HMC Version 2.9.0 also includes a number of other enhancements, as follows.

Full function remote access
One result of moving to a browser-based environment is that the HMC provides a single type of access for both local and remote users. Any number of users can use the HMC simultaneously, which requires network connectivity to the HMC and the use of a supported Web browser.

Although the local and remote interfaces are identical, there are some tasks, such as Format Media, that are available only through a local browser session. As always, you can enable and control remote access on a global and per-user basis.

SSL based encryption
Because access to the HMC is provided through an HTML-based user interface, current state-of-the-art browser-based encryption mechanisms can be used for enhanced security. In fact, all remote browser access is forced to use SSL encryption when accessing the HMC. The local user interface can use non-encrypted access because it has no external connections.

SSL encryption is required for all remote access to the HMC so, a certificate is required to provide the encryption. As shipped, the HMC provides a self-signed certificate that allows encryption to occur. For installations that choose to manage these certificates manually, the HMC provides a Certificate Management task.

Session disconnect
Using a Web-based paradigm for the HMC allowed us to move all of the state information for a logged on user-authorization level, currently running tasks, and so forth—onto the HMC itself.

Whenever you log off from a session with the HMC, you have the option to disconnect. Disconnecting will end your current session just as logoff does, but the state information for the session is not discarded as it is for logoff.

When you log on again, the HMC displays a list of any disconnected sessions for your user ID, and you can choose to reconnect to one of these existing sessions or start a new session. This session information is preserved as long as the HMC stays up. When you shut down the HMC, you are warned that disconnected sessions will be terminated.

Similarly, if a network failure occurs after the network problem is resolved, you can log on to the HMC and resume the previous session with its previous state because the tasks are kept running.
Because more and more applications are Web-based, the use of a completely HTML-based user interface provides a more consistent operating paradigm for you. Also, this shift in user interface technologies positions the HMC to provide common user interface technologies that can be used across IBM products.

The tree style interface provides a hierarchical view of system resources, categorized views of HMC tasks, and both ‘at-a-glance’ and detailed visualizations of overall system status. Because the tree view lets you launch tasks in context after drilling down to an area in which you are interested, it can help you work using a style you prefer rather than having to do things a particular way.

Advanced display features within table views include data selection, scrolling, filtering, simple and multi-column sorting, and column reordering and hiding.

**Making the switch**

To support your selection of user interface styles, a new **UI Style** tab has been added to the **User Settings** task. The tab provides options that allow individual users to select their preferred interface style (classic or tree style) and allow the user with Access Administrator authority (the default ACSADMIN user ID has this authority) to control whether users can change the interface style.

To allow users to change the interface style, you can log on with Access Administrator authority and launch the **User Settings** task under **Console Actions**. Selecting **Allow user to change UI style** will permit users to select the tree style user interface to begin taking advantage of the new presentation and visualization capabilities. Users will need to log off and log on again for the changes to take effect.

**User interface layout**

As shown in Figure 1, the tree style user interface is comprised of several major components:

- **Banner** (optional) appears across the top of the tree-style user interface.
- **Task Bar** displays the names of tasks that are running and the Help and Logoff tasks.
- **Navigation Area** contains the primary navigation links for managing system resources and the HMC.
- **Work Area** displays information for the current selection in the Navigation Area.
- **Tasks Pad** (optional) displays only those tasks that apply to the object or group of objects currently selected in the table in the Work Area or Navigation Area.
- **Status Bar** provides visual cues of current overall system status.

**Virtual demonstration**

The Navigation Area contains a list of all system resources including Servers, Directors/Timers, and Fiber Savers, if any. Besides the two pre-defined groups—**All Images** and **All Objects**—the HMC also allows you to create your own customized groups of objects.

In Figure 2, we have created several customized groups that represent the physical topology of our systems.

Suppose you would like to perform a task on an image for one of your servers. Selecting a particular server displays in the **Work Area** a table of the images associated with that server. For each image, the name of the image, and its current operating status and description are shown by default.

As with other IBM Web-based applications, the table display provides a number of advanced sorting and filtering capabilities. See Figure 3.

You can sort columns in ascending or descending order, reorder them, or...
even hide them. Further, you can define conditions to filter rows of objects, enabling you to view only the objects you want to see. You can then select from the table the image with which you want to work.

When you enable single object selection, the table displays radio buttons to allow you to select one item. When you enable multiple object selection, the table displays check boxes to allow you to make multiple selections. You can control this capability by toggling off or on the single object selection check box under User Settings on the Controls tab.

After you select the images, you can launch the task in several ways. You can use the Task Pad Area, the Tasks button at the top of the table, or the context menu icon, which is displayed next to the object name. Note that the task launched is the same task regardless of whether you select the classic style interface or the tree style interface.

The Status Bar presents an “at-a-glance” view of overall system status including all managed systems and the HMC. The Status Overview icon is always present; clicking it displays more granular status information in the Work Area.

More icons appear if Exceptions, Hardware Messages, or Operating System Messages exist. See Figure 4. Clicking any of these icons displays the list of objects with that condition in the Work Area. For example, if an LPAR and a server are in unacceptable state, the Exceptions icon appears. Clicking on it displays those objects in the Work Area.

Summary

HMC Version 2.9.0, which is available with the IBM System z9 server, takes advantage of new technologies to provide a number of enhancements. We integrated these enhancements while at the same time preserving the existing operations of the HMC with which you were familiar. The new tree style user interface implements many usability improvements for the presentation of system resources and task navigation.

You can find more information about the HMC through Resource Link™, which includes HMC documentation and education modules and courses.

For answers to your questions or a demonstration, contact your IBM representative. We welcome your feedback and would like to partner with customers interested in providing feedback on the HMC user interface.
“Now, where did I put my keys…”
IBM Encryption Facility for z/OS

BY JOHN EELLS AND TAN LU

Why encrypt?
The winds of change have reached gale force in the legal and regulatory environment where privacy is concerned. More laws and regulations seem to be passed almost daily, including the Sarbanes-Oxley Act (SOX), the Gramm-Leach-Bliley Financial Services Modernization Act (GLBA), and the European Union Data Protection Directive (EUPA). Consumers Union reports that more than twenty states have passed security breach laws, many requiring that consumers be notified if their personal information might have been compromised, and most specifically mentioning encryption. (See consumersunion.org.) Regulatory compliance is one of the industry’s leading drivers for data encryption.

Security breaches cost money, too. Determining the size of a breach, notifying customers, solving the underlying problem on short notice, and dealing with any liabilities that might result could be expensive.

Perhaps most important, though, are your company’s reputation and brand image. Consumers take a proprietary view of their personal information and want it safeguarded. Lost business can take years to regain. And Privacy Rights Clearinghouse reports over 80 security breach incidents from mid-February through September 2005 alone. See privacyrights.org.

It’s all about key management
OK, we’re preaching to the choir. You already know you want to encrypt some of your data. But how? Many politicians think it’s easy: computers support encryption, so simply passing laws and regulations will drive everyone to encrypt personal data, right? “Consumer privacy has been protected. Job done! Whew!”

Not so fast! If it were that easy, you would be doing it already. We all know that encrypting data is easy. Managing the encryption keys is much harder. Who can access the keys? Where and in how many places are they stored? How do you exchange them with business partners? Store and retrieve those used for backup and recovery? For disaster recovery? How do you find the keys for data you encrypted last year? Or ten years ago? Hold on to those thoughts.

Exchanging data with business partners
You can exchange data with business partners using well-established methods such as secure network connection or physical tape. This article will only address using tape.

To exchange encrypted data with business partners through tape, you have to do three things:
• Encrypt data using a technique that partners can decrypt
• Exchange keys to allow partners to decrypt data
• Use media and recording techniques that your partners’ equipment can read.

Sending backup data off-site
Most companies use off-site storage for backup data, usually a secure storage facility or backup data center. Either way, backup data written to tape is vulnerable while in storage or transit—to unauthorized access or even outright loss. Nonetheless, many corporate databases are so big that it is most practical to back them up to tape and send the tapes off-site.

Encrypting on-site data
Some data is sensitive enough to encrypt in place. RACF or other security system-based access controls can help protect data from unauthorized access, but stolen tapes removed from the security environment can be read elsewhere.

What about compression?
Today’s tape drives support hardware compression. Data sent to the drive is usually not compressed; compression hardware and microcode in the drive do that, with an eye toward increased tape capacity and higher I/O data rates. Compression, though, is based on finding repeated patterns, while one goal of data encryption is to eliminate them. As a result, encrypted data is usually not compressible. In fact, compressing encrypted data usually makes it grow slightly!

To improve tape capacity and I/O rates for encrypted data, then, we must compress the data before encrypting it and sending it to the tape drive.

Overview of the new IBM Encryption Facility for z/OS
IBM’s current solution for these challenges is the IBM Encryption Facility for z/OS. Using server-based encryption and compression hardware when available to avoid software overhead, and using Integrated Cryptographic Service Facility (ICSF) as its key manager, the Encryption Facility can allow you to compress and encrypt data to be written to either tape or disk.

The Encryption Facility is composed of two orderable features, but logically it has three parts:
• Encryption Services feature
• DFSMSdss Encryption feature
• Encryption Facility Client

For a complete list of hardware and software requirements, see “IBM Encryption Facility for z/OS, V1.1 helps to secure data stored to tape and other removable media,” IBM United States Software Announcement 205-243, dated September 27, 2005.

Encryption Services Feature
The Encryption Services feature runs on z/OS to support compression, encryption, and decryption of sequential files, members
of PDS and PDSE data sets, and data stored in z/OS UNIX System Services file systems. Entire PDS, PDSE, and VSAM data sets can be unloaded to sequential data sets using utilities (IEBCOPY and IDCAMS) to allow them to be encrypted.

Using the hardware compression features available on IBM System z9 and zSeries servers, the Encryption Facility will optionally compress data before using other hardware features to encrypt it. (The Encryption Facility potentially leverages both Crypto Express2 and CPACF.) Compression is optional because the hardware compression algorithm is not supported in all environments where a tape might need to be read later. The Encryption Feature can use ICSF as the key manager to centralize and help you control access to encryption key storage. There are recovery procedures you can use for ICSF’s key storage to prevent key loss; see “Questions please…” on page 23, for more information.

Data can be encrypted using TDES with triple-length keys or AES with 128-bit keys. Every file can be encrypted with a different key. The key used to encrypt the file is then itself encrypted and stored in a file header record. To decrypt the file, the key used to encrypt the original encryption key is needed first. More about this later.

**DFSMSdss Encryption feature**

The DFSMSdss Encryption feature lets you encrypt DFSMSdss dump data sets. DFSMSdss, of course, will dump an entire volume, a single data set, or a group of data sets. DFSMSdss encryption supports the same hardware compression and encryption features and encryption algorithms as the Encryption Services feature, supports using ICSF for key management, and, like the Encryption Services feature, encrypts the key used to encrypt the data and writes it to the output data set. Also, when DFSMSdss is used as the data mover, it can encrypt data migrated by DFSMSdss.

**Encryption Facility Client**

So—this sounds good so far, but how does the Encryption Facility let you exchange data with business partners running on other operating system platforms? By itself, it doesn’t. Enter the Encryption Facility Client, a separate, downloadable product. The Encryption Facility Client is an as-is, unwarranted product. For more information, see [ibm.com/servers/eserver/zseries/zos/downloads](http://ibm.com/servers/eserver/zseries/zos/downloads).

The Encryption Facility Client, written in Java to provide cross-platform portability, can decrypt data that has been encrypted by Encryption Services, and encrypt data to be decrypted by Encryption Services. It cannot, however, uncompress data that was compressed by Encryption Services. (Software decompression is very slow compared to hardware, and we chose not to put this capability in the client.) This is one reason compression is optional when using Encryption Services.

**Like we said…it’s all about the keys!**

So, how to manage the keys? You know Encryption Services and DFSMSdss Encryption will generate a new key for each data set or file. You know that key will be encrypted and written to the file header. What's used to encrypt the key?

Another key, of course! This sounds complicated, but it’s not. Most of us have seen the lock boxes that realtors use to hold the keys for houses they are selling hanging from a door knob. The realtor has a key—or perhaps a combination— to the box. The box holds the key to the house. To show the house to a prospective buyer, the realtor opens the box and uses the key within to open the door. Encryption key management works the same way.

What key to use for the lock box? You can use a business partner’s public key (using PKI), which would allow decryption using the partner’s corresponding private key. For intra-enterprise shipments and off-site storage, you can use your own public/private key pairs. You can also use passwords, which you might send to business partners through a separate, secure channel.

Public keys (theirs) and private keys (yours) can be stored in ICSF’s PKDS data set. Enhancements to the RACF RACDCERT command allow your partners’ public keys to be loaded into ICSF directly from digital certificates. The keys loaded into ICSF can be labeled, and you can use the labels to specify keys to be used for encryption. The keys themselves need never be exposed.

Don’t forget that centralized and certificate-based key management is not only useful for the Encryption Facility. You can use it for things such as TLS, SSL, client/server authentication, and even e-mail security. The ICSF one-stop shopping for z/OS key management can be used alongside the RACF Identrus-
certified digital certificate hosting services (z/OS V1R5 with RACF).
Centralized key management on z/OS, with its management, access controls, and
auditability, has been used in production for over a decade.

Watch this space
In the future, IBM intends to offer outboard encryption for devices in
the TotalStorage family, and continue leveraging the key management functions
provided by ICSF. Of course, we intend to keep extending our key management
facilities, too.

After all, why would we start over?

For more information
See the statement of direction in “IBM System z9 — the server built to protect and
grow with your on demand enterprise;” IBM United States Hardware Announcement

A little-LDAP’ll-do-ya
BY TOM SIRC AND ASHWIN VENKATRAMAN

Consider this scenario: A test environment
has three WebSphere Application Server
for z/OS cells (a logical grouping of servers
and nodes); let’s call them T1, T2, and
T3. All three cells use a Local operating
system (OS) user registry, and each has
its own user and group structure because
different application development teams are
testing their own Java 2 Enterprise Edition
(J2EE) application security. An issue
comes up — we need to figure out how to
share a cell between different application
development teams without sacrificing
security.

The security limitation we describe
above is that every application running in
a cell must share the user registry. Each
user that needs access to an application
running on the cell needs to be added
to the authorization list for the entire
WebSphere Application Server space. This
creates the burden of managing user
security and violates a security practice
because users who should not have access
to an application are still given the access
to connect to WebSphere Application Server
because of another application’s needs.
Having multiple WebSphere Application
Server cells to provide security isolation is
usually the way to deal with this problem.

We face other problems when
developing an application that exploits
form-based authentication on the T2
cell. At one point the T2 cell needs to be
down but our development deadline can’t
slip. And development and testing of our
application has to be completed on the T3
cell even though we have a different set of
users for that cell.

Our first thought is to give the
developers of the application access to the
T3 cell. This requires multiple user IDs
and Enterprise Java Beans authorization
role (EJBROLE) access changes in
RACF. We also need to remember to
undo these changes after the T2 cell back
online. To solve this user management
issue, we realized that a little-LDAP’ll-do-
y! We pointed our T3 cell’s user registry
to a Lightweight Directory Access Protocol
(LDAP) server that already had the user
and group structure for the application. We
are able to change this setting in a short
amount of time because the environment
already exists, and the change won’t
leave negative side-effects after the cell
is switched back to the Local OS user
registry.

Using an LDAP authentication scheme
in a WebSphere Application Server
environment is a simpler, more secure
to allowing multiple development teams
to use the same WebSphere Application
Server cell without having to provide
unnecessary privileges in RACF. For this
to happen, J2EE application developers
need to add the user-to-role mappings to
the enterprise archive (EAR) deployment
descriptor because the RACF EJBROLE
class no longer handles that function.
To add the mappings, first understand
the user and group structure in the
LDAP directory. Only one application
development team can use the WebSphere
Application Server cell at any one time. If
security is a concern in your environment
and you can’t run multiple WebSphere
Application Server cells, an LDAP user
registry is the alternative to consider!
Questions, please…
Unlocking the answers to Encryption Facility for z/OS
BY PEGGY ENICHEN, RON EDICK, AND MIKE KELLY

You have some questions about Encryption Facility for z/OS? Here are some answers.

1. **What kinds of encryption keys can I use to encrypt and decrypt data?**

You can use the following kinds of keys with Encryption Facility for z/OS:
- Clear triple-length TDES key (CLRTDES)
- Clear 128-bit AES key (CLRAES128)
- Secure TDES triple-length key (ENCTDES).

The keywords in parentheses are options that you specify in the job control language (JCL) for Encryption Services encrypt/decrypt programs.

2. **What kind of performance can I expect with the Encryption Facility?**

It depends. A number of factors determine the performance of Encryption Facility, including the type of processor and cryptographic coprocessor you have, the types of keys you use to encrypt the data, and your installation security policy.

3. **Why should I use CLRTDES instead of ENCTDES—or vice versa?**

Generally, if your installation security policy requires that the data encryption key never appear in the clear in host storage, using the ENCTDES key provides the best security, but it does have a considerable impact on performance.

In contrast, if you use the CLRTDES or CLRAES128 keys, Encryption Services generates the keys dynamically. Unlike the ENCTDES key, the CLRTDES and CLRAES128 key values can appear in application storage. However, if Encryption Facility is running on a z890, z990, or IBM System z9 109 server, CSDFILEN encrypts the data using the clear TDES key or clear AES key on the CPACF. This method can give you better performance than using the ENCTDES key option.

4. **What hardware supports CLRTDES, CLRAES128, or ENCTDES keys for encryption?**

Figure 1 provides summary information

<table>
<thead>
<tr>
<th>Encryption key and key protection options</th>
<th>Processor type CCF</th>
<th>Cryptographic hardware</th>
</tr>
</thead>
<tbody>
<tr>
<td>CLRTDES key used with PASSWORD</td>
<td>z800 and z900</td>
<td>CCF</td>
</tr>
<tr>
<td></td>
<td>z890 and z990</td>
<td>CPACF</td>
</tr>
<tr>
<td></td>
<td>z9 109</td>
<td>CPACF</td>
</tr>
<tr>
<td>CLRTDES key used with RSA key pairs</td>
<td>z800 and z900</td>
<td>CCF¹</td>
</tr>
<tr>
<td></td>
<td>z890 and z990</td>
<td>PCICC²</td>
</tr>
<tr>
<td></td>
<td>z9 109</td>
<td>CCF and PCICC with LIC January 2005 or later and z990 and z890 Enhancements to Cryptographic Support web deliverable (ICSF HCR770B) or later³</td>
</tr>
<tr>
<td>CLRAES128 key used with PASSWORD</td>
<td>z800 and z900</td>
<td>CCF</td>
</tr>
<tr>
<td></td>
<td>z890 and z990</td>
<td>CPACF</td>
</tr>
<tr>
<td></td>
<td>z9 109</td>
<td>CPACF</td>
</tr>
<tr>
<td>CLRAES128 key used with RSA key pairs</td>
<td>z800 and z900</td>
<td>CCF¹</td>
</tr>
<tr>
<td></td>
<td>z890 and z990</td>
<td>PCICC²</td>
</tr>
<tr>
<td></td>
<td>z9 109</td>
<td>CCF and PCICC with LIC January 2005 or later and z990 and z890 Enhancements to Cryptographic Support web deliverable (ICSF HCR770B) or later³</td>
</tr>
<tr>
<td>ENCTDES key with RSA key pairs</td>
<td>z800 and z900</td>
<td>CCF¹</td>
</tr>
<tr>
<td></td>
<td>z890 and z990</td>
<td>PCICC²</td>
</tr>
<tr>
<td></td>
<td>z9 109</td>
<td>CCF and PCICC with LIC January 2005 or later and z990 and z890 Enhancements to Cryptographic Support web deliverable (ICSF HCR770B) or later³</td>
</tr>
</tbody>
</table>

1. For RSA modulus-exponent form keys with modulus length less than or equal to 1024 bits
2. For RSA Chinese Remainder Theorem keys with modulus length less than or equal to 1024 bits
3. For RSA keys with up to 2048 bit modulus

Figure 1 – Cryptographic keys and hardware requirements
about the use of the clear keys CLRTDES and CLRAES128, and the secure key ENCTDES for encryption for different processors and cryptographic hardware. For more information, see Encryption Facility for z/OS: User’s Guide, SA23-1349.

5 Does compressing the data before encryption affect the performance of the encryption and/or decryption job?

No, compressing the data before you encrypt it does not appreciably affect the performance.

6 I plan to use RSA keys to protect my encrypted data. How can I generate and store RSA key pairs?

You can generate and store RSA key pairs in the following ways:

- Use Integrated Cryptographic Services Facility (ICSF) callable services to generate RSA keys and place them in the PKDS. The required ICSF callable services are CSNDPKB PKA key token build, which builds a skeleton PKA token and CSNDPKG PKA key generate, which generates key values for the PKA token.
- Use the EFRSAKEY application, to generate an RSA key pair in the ICSF PKDS for Encryption Facility. EFRSAKEY runs under a TSO ISPF session and communicates to the Key Custodians through ISPF panels. Documentation for EFRSAKEY is available on the Techdocs Web site: ibm.com/support/techdocs/atmasr.nsf/WebIndex/PRS160?

7 How can ICSF help me manage my encryption keys?

You can store cryptographic keys in the ICSF public key data set (PKDS). Encryption Facility works with ICSF to perform encryption and decryption and to manage the cryptographic keys.

8 What should I know about storing and backing up encryption keys in the PKDS?

Understand that when you store the encryption keys in the ICSF PKDS, you can keep them stored indefinitely. For recovery purposes, treat the PKDS as a critical VSAM data set and back it up accordingly.

9 What else do I need to know about protecting keys?

You need to make sure that you can recover the PKA master key (ASYM-MK master key), which is resident in the cryptographic hardware in the event of a catastrophic system failure. The master key must be available at the recovery site. You can enter the PKA master key value on your backup server using key parts and the Trusted Key Entry (TKE) workstation.


10 What if I change the PKA master key (ASYM-MK master key)? Can I still recover encrypted files?

Most definitely. You can use ICSF to change the PKA master key (ASYM-MK master key), which is resident in the hardware multiple times and still recover the original data. If you do change the PKA master key, you will need to re-encipher the PKDS under the new value of the master key so that the keys in the PKDS are still usable.

11 Does the Java reference code for Encryption Facility for z/OS Client use the ICSF PKDS?

No. With the Encryption Facility for z/OS Client, you store your RSA keys in a Java keystore. The most common way to do this is through a utility called KEYTOOL. To transfer RSA key data between systems, the Encryption Facility for z/OS Client must use X.509 certificates.

12 How does that work?

For Encryption Facility for z/OS Client to send data that it has encrypted to a remote system, say for archiving, it requires...
How would you answer this question when you go to a Web site and a Security Alert window pops up telling you that there is a problem with the site's certificate – Yes, No or View Certificate? Or you might hope there's a fourth option – I don't know.

This article helps explain Digital Certificates in a simple way, starting from a daily experience—online shopping. When you click Check Out after you pick the product you want, do you know what happens before it displays a page for you to enter your personal information and your credit card number?

Actually, quite a bit happens. Your browser and the host site negotiate what is called a Secure Socket Layer (SSL) handshake, a process that goes like this: the Web site sends its certificate to your browser to prove its identity to ensure you that you are really dealing with the Web site that you think you are. Your browser then determines whether it can trust that certificate. If it can't decide, it will ask you to make a decision. That's why the Security Alert window pops up.

But how does the browser decide whether to trust the certificate? The first thing it checks is whether it knows the issuer of the certificate by checking whether a certificate for the issuer is in the browser's trusted certificate store. Certificates are issued by a Certificate Authority (CA). The CA must have its own certificate, either issued by another CA or issued by itself, before it can issue certificates for other parties. When you install your browser, there are a number of well-known CA certificates that are placed in your browser's trusted certificate store. Usually, a Web site applies for a certificate from a well-known CA, so when a user visits the site, the certificate it sends is known by the browser.

Let's dive a little deeper. How does the browser know which certificate in the trusted certificate store is the site's issuer certificate? If you look at the certificate, you find the following:

- Version
- Serial number
- Signature algorithm ID
- Issuer's name
- Validity period
- Subject's name
- Subject's public key
- Extension(s)
- Issuer's signature.

The browser finds the issuer's name from the host site's certificate. It then tries to find a certificate in the store, whose subject name is the same as that issuer's name. After it finds the issuer's certificate, it can verify the signature on that site's certificate by using the public key from the issuer's certificate.

Public Key cryptography involves a function in which encryption and decryption are using associated keys from a mathematically related key pair. The content encrypted with one key can only be decrypted by the other. One key of the pair, which is called the public key, is put in a digital certificate for public use, while the other key, which is called the private key, is kept securely by the owner. When a CA issues a certificate, it vouches for the binding between the owner's public key and the owner's name by cryptographically signing the certificate with its own private key. Public Key cryptography is the soul of a digital certificate when contrasted with Secret Key cryptography in which only one key is used to encrypt and decrypt.

Now you can understand why the verification on the certificate's signature is done using the issuer's public key – because that signature was generated using the issuer's private key. Let's review the verification steps involved so far. The browser identifies the issuer of the incoming certificate from the issuer's name in the certificate. The browser then verifies the certificate by checking the signature with the issuer's public key. The public key is located in the issuer's certificate, which is stored in the trusted certificate store.

But wait there's more! Validity period and revocation status also play a part in the validation process. If a certificate has expired or is revoked, it should not be trusted. While validity period can be checked directly from the information within the certificate itself, revocation status is checked from a Certificate Revocation List (CRL) which is located elsewhere, as indicated by the Certificate Revocation List Distribution Points extension.

After a certificate is issued, its owner can use it until it expires. However, if, during that period, the certificate needs to be revoked, the CA of that certificate puts that certificate on the Certificate Revocation List.
Revocation List. The list is updated according to a schedule determined by the CA. The CRL is posted to a public directory, for example a Light Weight Access Protocol (LDAP) server, for applications that use the certificate to check its status during the validation process. The CRL Distribution Point extension can indicate the URL of the list. If the application doesn’t find the target certificate on the list, it considers it not revoked.

You might now be thinking...what happens if the certificate is revoked, but the CRL hasn’t yet been updated by the time the application is checking? A newer scheme called Online Certificate Status Protocol (OCSP) was introduced to improve the revocation process. It works by having the CA place the URL of a designated responder into another validation related extension within the certificate, called the Authority Information Access Extension. As part of the validation process, a request goes to this URL, which may be the CA itself, or one or more designees, to ask for the certificate’s current status.

All the validations discussed so far are the basic checks – signature, validity period and revocation status. An application can check further for other information in the certificate. For example, an e-mail application might check whether the certificate has a Digital Signature key usage, or perhaps whether it includes an e-mail address in its subject name...in other words, different applications need different types of certificates.

Let’s continue with the browser scenario. After the browser has validated the site’s certificate, it can use that certificate to establish a secure environment for the customer to enter personal information. To simplify the underlying process, we can say that the browser uses the public key in the host site’s certificate to encrypt the information that it wants to send to the site. Even though a potential hacker might try to get the information within the traffic, he can’t decrypt the content because he doesn’t have the host’s private key. As you can see, digital certificates are used to verify the identity of users and to protect the information flowing within Web traffic. How the host site continues to protect your information is a topic for another day.

Now let’s take a look at the digital certificate from the host site’s point of view. The scenario we described previously, which is called Server Authentication, involves only two certificates: the site’s own certificate and its issuer’s certificate, which is in the browser’s trusted certificate store. Does the browser need to have a certificate to send to the site? It depends, and for online shopping, usually not. However, this might be different for a bank, a health organization and lots of other On Demand businesses of the future. If the site wants to authenticate the user, it requests that the browser send a certificate for the user. We refer to this process as Client Authentication. The client’s certificate is validated by the site in a manner similar to the way the browser authenticated the host, as we discussed earlier.

As you can imagine, the number of certificates involved in client authentication is far more than that in server authentication. As a z/OS customer, you have an economical opportunity to exploit digital certificates. You can use Public Key Infrastructure (PKI) Services to set up your own CA to issue and maintain certificates to your customers.

PKI Services is a component licensed with z/OS since V1R3, and it offers complete life-cycle management support for digital certificates – request, create, distribute, renew and revoke, and it offers a plug-in for a certificate validation service. In May 2005, it achieved the Certificate Authority software program certification from Identrus. Additional information on Identrus can be found at ibm.com/servers/eserver/zseries/security/identrus.

We hope this article has given you an overall picture of digital certificate technology and helped you to grasp the basic concepts needed for the tasks involved in exploiting this technology within your enterprise. When you need to set up a site or a CA, consider the low cost, good quality certificate service provided by PKI Services on z/OS. For further information, visit ibm.com/servers/eserver/zseries/zos/pki.

This article helps explain Digital Certificates in a simple way, starting from a daily experience — online shopping.
Wanted: Your feedback

The IBM z/OS User Technologies group is looking for your feedback to help those new to the z/OS user experience! This exciting design project aims to simplify the management of z/OS and make it easier for you to learn new tasks on z/OS. We’ve designed new and simplified books, education, user interfaces, and tools to meet this end.

Shape the future at SHARE...

If you or a colleague are new to z/OS and are at SHARE in Seattle, come to the IBM zSeries Make IT Easy booth (booth #421) in the Technology Exchange area to check out some solutions we’re designing. Not at SHARE but want to participate? Send an e-mail to Adrienne Becker at abecker@us.ibm.com. We’re especially interested in people from small and medium businesses. We hope to hear from you!

zFavorites!

It’s the zFavorites for zSeries CD!
You’re gonna love this! It has all sorts of helpful Web links, like those for:

- Hardcopy
- Operating systems
- Software
- Language and tools
- ISV development and applications
- Product documentation
- Marketing information
- Education
- Support
- Links to FREE downloads
- Redbooks™ sampler
- WebSphere® Application Server
- XML

To use the CD: Insert it in any standard CD-ROM and it should start automatically. If it does not, click on the Start button, choose Run… and then type x:\index.htm (where x is your CD-ROM drive letter) and press Enter.

Additional copies of zFavorites CD-ROM (GK3T-4331-08) are separately orderable.
z/OS: The right ingredients for availability

BY DAVID RAFTEN

A highly available operating system like z/OS doesn’t occur overnight. z/OS has built-in core recovery, availability, and serviceability (RAS) features that have been around for decades. Many of these features are not found in other operating systems.

Recovery and availability
z/OS is designed to have good first failure data capture (FFDC) techniques. FFDC is intended to make the operating system and major subsystems able to the capture data needed to identify problems that might occur during production while minimizing impacts to system availability. Moreover, these basic functions have been a core part of our mainframe operating system designs since 1974.

Because of the long history of recovery and availability functions and enhancements that come with z/OS, it can be easy to take the operating system for granted. In z/OS, if a task (comparable to a UNIX thread) fails, it can request that the system make a copy of its running programs, together with the data and system control blocks, to another location in memory and write it to a dump data set on disk or tape. Application and system programmers can then use diagnostic tools for later analysis.

Great serviceability
For many user applications and subsystems that run on z/OS, dumps don’t have a terribly disruptive impact on unrelated system work. Even for system-level problems, z/OS designs continue to focus on collecting the data needed to diagnose problems while minimizing the system-wide impact.

On z/OS, after a problem occurs, recovery routines can get control. Recovery routines include STAE, ESTAE, ESTAEX, and FRRs. They can capture diagnostic data, identify, and restore modified system structures, resources, and locks that a failed user might hold, and then return control to the program at a specified point. This means that after a dump is collected, the operating system and subsystems typically keep running without the need to re-IPL. Software products from IBM and others, and your own applications, can take advantage of these recovery features of z/OS. The ability to collect specific diagnostic data, based on situations the recovery routines can interpret, can also improve first-failure data capture, which speeds diagnosis and improves serviceability.

Better problem determination
In addition to other data captured with dumps, system trace records can help system programmers with problem determination (PD). (Think of system trace records as forming part of the z/OS flight data recorder!) Various z/OS component- and system-level traces are active by default. The z/OS operating system and many of its components write information about the flow of program control and execution to the system trace table in memory. This trace table, along with another area containing recent system messages, can be captured in dumps and its entries are used to help diagnose problems.

System programmers can turn on additional traces for many z/OS components to obtain more data and they can turn them off when they aren’t needed, all without restarting. This is key because data collection can be surgically targeted to minimize the impacts on overall performance. Other products can also write trace records.

Resource cleanup
Part of the fundamental z/OS recovery processing is the system’s attempt to clean up resources that ending programs have acquired. Cleaning up these resources can allow the system to free memory, release hardware and software locks, and close data sets and files. When programs encounter errors before cleaning up their own resources, or do not provide their recovery routines, the system’s recovery termination manager (RTM) invokes the end-of-task and end-of-memory processing to attempt to release their locks, latches, and other system resources.

z/OS has extensive logic that can allow you to restart canceled z/OS UNIX System Services processes and other (non-UNIX) address spaces without requiring re-IPL. Processes and address spaces can hang for any number of reasons. Deadlock situations can occur between applications holding enqueues or locks, or holding UNIX latches when one task or UNIX thread tries to acquire system-level locks for resources that another holds. z/OS can help you find and resolve these deadlocks.

Available and secure
Most systems require some form of security. Two aspects of system security that can affect availability are the need to protect a system from hackers who might accidentally make changes that can impact availability. z/OS includes a system component, the System Authorization Facility (SAF), which it calls to check a user’s authorization to do many tasks. With the optional Security Server (RACF) feature or an equivalent external security management product, z/OS can address the above security concerns in an efficient, manageable package.

Should a hacker gain access to a user’s identity (for example, by compromising the user’s password), the system is designed to grant the hacker access only to those resources for which that particular user can operate. Because most z/OS users are typically not authorized to use high-level system resources, this design can help you minimize the risk of damage to the system and contain how much data can be compromised. z/OS and RACF include auditing and notification capabilities that are designed to help you track resource usage and find unauthorized people who
are poking around trying to discover system weaknesses. In addition, security administrators and system programmers can specify that a user who exceeds a password attempt threshold be revoked to disallow further access. System messages can be generated when failed resource access attempts occur, and automation tools can be programmed to take immediate action.

Security features built into the system

Many functions are critical to providing security. Some of these include:

- Encrypting passwords when users sign on to the system
- Encrypting data transmitted across a network
- Protecting system and user files from unauthorized access
- Creating auditing records
- Protecting the security manager database itself.

z/OS’s SAF uses an external security manager like RACF, which is designed to provide a security-rich environment while providing good performance. RACF is designed to allow you to protect resources across the system, and to help you manage access control lists for both z/OS data sets and z/OS UNIX files. Using RACF Remote Sharing Facility (RRSF), you can shadow RACF definitions to other sysplexes, which can help you control administration cost and help assure a consistent security environment across your entire z/OS installation.

Digital certificates can be a basic building block of a trusted computing infrastructure supporting secure transactions over the Internet. Public Key Infrastructure (PKI) services provide for the life-cycle management of digital certificates. With the PKI Services component of the Cryptographic Services element, which is built into z/OS, you can act as your own certificate authority (CA). Being your own CA means you have the capability to create and manage your own digital certificates. For more about digital certificates, see “Security alert: Do you want to proceed?” on page 25.

Hundreds of distributed systems can be consolidated on a single IBM System z9 or zSeries server. Within the server, data can be passed to other applications and other logical partitions within the box using virtual network technologies including HiperSockets™, TLS, SSL, IPSec, and Guest LANs. Between z/OS images on different servers within a Parallel Sysplex, data can also be exchanged using the coupling links. All these features can help you protect the data and applications running on z/OS and System z9 and zSeries servers from network-based attacks.

Part of the Communications Server base element of z/OS is Intrusion Detection Services (IDS). IDS is built within the TCP/IP stack and is designed to discover and defend against attacks such as scans, single packet attacks, and flooding. It can automatically log activity for later analysis.

Parallel Sysplex clustering for improved availability

The IBM Parallel Sysplex clustering is designed to allow you to remove single points of failures for data sharing applications. When you use dynamic workload balancing in a Parallel Sysplex, it can help you remove one or more systems from the configuration without affecting application availability, which can allow you to continue to process production work.

The z/OS operating system and middleware

Starting with MVS/ESA™ SP V4.3 in 1994, the operating system has also been a UNIX platform. z/OS supports zFS and many of the same programming interfaces and user interactions as other UNIX platforms. But consider the differences… While UNIX applications can run on z/OS as they can run on other platforms, they can also enjoy all the added benefits of z/OS availability, security, and serviceability described earlier, with better system management, and other great z/OS features like WLM. Moreover, z/OS is designed to prevent unauthorized applications from accidentally modifying code in the operating system code and even in other applications.

When a process stops running, the normal UNIX procedure is to kill the process. z/OS provides an additional recovery step, with the z/OS UNIX SUPERKILL command. SUPERKILL invokes z/OS services designed to cancel the address space running the UNIX process and use z/OS end-of-task and end-of-memory services to attempt to release the system resources it was using so it can be restarted. In addition, many UNIX servers running on z/OS are designed to use z/OS recovery routines to clean up after themselves to avoid having to restart them.

z/OS continues to deliver

Customers have long demanded a secure, reliable, serviceable, and available system – a robust 24x7x365 environment to run mission critical workloads where unscheduled IPLs are unacceptable. Application outages can cost thousands of dollars per minute in many business environments. These critical business necessities continue to help drive the evolution of the z/OS operating system and its objectives to provide robust recovery, availability, reliability, and serviceability.
Got the PD blues?

BY EVAN HARUTA AND KATHY PFEIFFER

Dear Level 2,

I’m running z/OS V1R7 with two reserved (offline) CPs and 22 online CPs. After defining 10 additional CPs to the image, which means there are 32 online general processors on a single image, I go into a WAIT07C state at IPL.

Signed,
Exceeded Limit

Dear Zapped and Exceeded Limit,

A WAIT07C state indicates that an error was detected during initialization in the system configuration that needs to be corrected before the system will properly initialize.

z/OS V1R4 and V1R5 each support 16 processors in a single image. z/OS V1R6 increased support to 32 processors. z/OS V1R7 scalability enabled support, first to 24, then to 32 processors in a single image.

Advice: Check the image profile to ensure that the sum of the online, offline (reserved), and zAAP processors do not exceed the z/OS software release limitation.

Note to our readers: A zAAP is an Integrated Facility for Applications (IFA).

You can issue the D M=CPU command to display the status of your processors while planning for migration to a new release. The processor status as illustrated in Figure 1 is as follows:

- ONLINE (+)
- OFFLINE (-)
- ASSIST PROCESSOR (A)

While more than 32 processors can be defined in the image profile (for example, to the hardware), and the activation of the image appears to be successful, z/OS V1R7 only recognizes up to 32 processors. In both of the described scenarios, you are exceeding the processors limit by two processors. When calculating the sum of your processors, include the following processors as a part of your total:

- Online
- Offline
- zAAPs

Therefore, z/OS counts all the processors in the dispatch pools: reserved, online, and zAAPs.

P.S. The D M=CPU command can also display WLM managed processors. However, WLM managed processors are not included in the sum of total processors.

Sincerely,
Level 2

Dear Level 2,

I have installed the 64-bit Java SDK 1.4.2 to use on our z/OS V1R6 system. When I get into the OMVS shell and enter “java -version”, I receive the following Language Environment initialization error:

BPXP018I THREAD 168C990000000000, IN PROCESS 67174483 ENDED WITHOUT BEING UNDUBBED WITH COMPLETION CODE 04000FFD AND REASON CODE 00000224.

Signed,
Exhausted Storage

Figure 1 - Example of six processors: four general purpose and two zAAPs
Dear Short Memory and Exhausted Storage,

This indicates that you are experiencing problems with your virtual storage. In the first scenario, virtual storage issues can lead to AUX storage shortages, which can be triggered by excessive use of above-the-bar storage. In the second scenario, Language Environment™ to obtain above-the-bar virtual storage is being limited and as a result isn’t able to obtain any storage.

**Advice:** Begin your review by looking at the MEMLIMIT parameter. The MEMLIMIT parameter specifies the limit on the total number of usable virtual pages above the bar in a single address space. The syntax for the MEMLIMIT parameter is as follows:

```plaintext
MEMLIMIT= {nnnnnM}
{nnnnnG}
{nnnnnT}
{nnnnnP}
{NOLIMIT}
```

You can manage the MEMLIMIT parameter using the following:

1. SMFPRMxx
2. JCL (on the JOB and EXEC statements)
3. IEFUSI installation exit.

### Specifying MEMLIMIT in the SMFPRMxx member

The SMFPRMxx member allows you to control how system management facilities (SMF) work at your installation. SMFPRMxx can specify the default MEMLIMIT for use by jobs that do not establish a MEMLIMIT in their JCL. If MEMLIMIT is not specified in SMFPRMxx, the default value for the system default is 0M. You can override the system-wide default MEMLIMIT by specifying REGION=0 (this is equivalent to MEMLIMIT=NOLIMIT) or MEMLIMIT on JOB or EXEC statements in JCL.

**A word of caution:** Specifying a REGION size that gives the job all the available storage (for example, specifying 0K or any value greater than 16 384K) can cause storage problems if you don’t use IEFUSI to establish a limiting value. You can use the D SMF,O command to display the current MEMLIMIT in SMFPRMxx.

### Specifying MEMLIMIT in JCL

You can express the MEMLIMIT value in megabytes (M), gigabytes (G), terabytes (T), or petabytes (P). The nnnnn variable can be a value from 0 to 99999, with a maximum value of 16384P. The default, if not specified anywhere, including SMFPRMxx, is MEMLIMIT=0M (or equivalent in G, T, or P) meaning that the step cannot obtain any virtual storage above the bar (2 gigabytes) for a single address space.

The MEMLIMIT parameter can be specifically on the JOB and EXEC statement. If the MEMLIMIT parameter is specified on both of these statements, the JOB statement MEMLIMIT parameter applies to all steps of the job and overrides the EXEC statement MEMLIMIT parameter.

The NOLIMIT option specifies that there is no limit on the use of virtual storage above the bar. Note that this is equivalent to REGION=0M.

Example 1 shows the use of MEMLIMIT set to 10 000 megabytes:

```plaintext
Example 1: //STEPA EXEC
FOM=JOB A,MEMLIMIT=10000M
```

In addition to the MEMLIMIT parameter, you can use the REGION parameter to specify the amount of central or virtual storage that a job requires. The system applies the values on the REGION parameter to each step of the job. A specification of REGION=0K/0M results in a MEMLIMIT value being set to NOLIMIT. Example 2 shows the use of REGION set to zero:

```plaintext
Example 2: //ACCT1 JOB A23,SMIT
H,REGION=0K,ADDRSPC=REAL
```

If no MEMLIMIT parameter is specified, the default is the value defined to SMFPRMxx, except when REGION=0K/0M is specified, in which case the default is NOLIMIT.

### Using IEFUSI (installation step-initiation exit)

The IEFUSI installation, a step-initiation exit, can override any JCL- or SMF-supplied values. In IEFUSI, register 1 points to the following parameter description for word 9. Word 9 identifies the address of an area that consists of three 64-bit fields. These fields communicate with MVS™ regarding the preferred MEMLIMIT; they include the following information.

The first 8 bits in the first 64-bit field indicate whether the source of the MEMLIMIT is from JCL or the SMF-supplied system default. The remaining 56 bits are not used. Possible values for the first 8 bits are as follows:

<table>
<thead>
<tr>
<th>Bit setting</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>0000 0001 (x’01’)</td>
<td>MEMLIMIT is from SMF</td>
</tr>
<tr>
<td>0000 0010 (x’02’)</td>
<td>MEMLIMIT is from JCL</td>
</tr>
<tr>
<td>0000 0011 (x’03’)</td>
<td>MEMLIMIT was set to NOLIMIT because the JCL specified REGION=0</td>
</tr>
<tr>
<td>0000 00FF (x’FF’)</td>
<td>MEMLIMIT is from SMF (indicating internal processing errors).</td>
</tr>
</tbody>
</table>

Other values are possible when initializing a child address space in the UNIX System Services environment. In the third 64-bit field a MEMLIMIT of NOLIMIT is equivalent to x’000000FFFFFFF0000’.

If you want to control the use of virtual storage above the 2 GB line, do the following:

1. Set a system wide default MEMLIMIT in SMFPRMxx.
2. Use the MEMLIMIT option on the JCL EXEC statement.
3. Use the IEFUSI exit (as a secondary limit) for the allocation of high virtual storage.

For more information, see the following:

- **z/OS MVS Installation Exits, SA22-7593**
- **z/OS MVS JCL Reference, SA22-7597**
- **z/OS MVS JCL User’s Guide, SA22-7598**
- **z/OS MVS Extended Addressability Guide, SA22-7614**

Sincerely,

Level 2
All in all we keep removing bricks from the wall
Managing system constraints

BY ED MEKEEL AND MARK WISNIEWSKI

Managing an IT shop today is difficult. It seems that overnight, walls show up making it difficult to achieve your business objectives. The dynamics associated with being successful in the marketplace can leave one comfortably numb. To help ease these barriers, we in z/OS Design and Development want to make sure that your large system throughput is not constrained in any way. We are continuously studying your workloads to understand growth trends to help get you outside the wall. Internal benchmarks, field surveys, and special studies allow us to focus on critical and pervasive constraints and develop solutions in a timely manner. This allows us to make sure our z/OS releases and subsystem software contains function that remove “constraint bricks” from the wall. By removing constraints, we simplify things, so that you don’t have to take extraordinary measures to bypass the limits. Here are some examples that you might recognize:

• Consoles enhancements work that began in z/OS V1R4 alleviates message production and consumption constraints.
• Real storage 64-bit that began in OS/390 V2R10 reduces paging overhead.

Let’s take a closer look at some of the constraint relief items that arrived in z/OS V1R6 and z/OS V1R7, their value to you, and what you might expect in the future. About the only issue we won’t cover is which one’s pink...

Speak to me

In z/OS V1R6, our design focus area became seamless vertical central processor (CP) growth. z/OS now supports 32 CPs in a single system image. Allowing for greater than 16 CPs provides vertical capacity growth that can complement the horizontal growth of a Parallel Sysplex. Larger single z/OS images don’t replace Parallel Sysplex, but rather work with it synergistically to maximize your growth options.

As images grow, so does the need for DASD space. To remove pressure on the limits of device addressability and allow for increased DASD capacity, z/OS provides 54 GB volume size. The number of members in a single XCF group grew from 1023 to 2047. In CICS workloads, this allows you to define more application owning regions (AORs) to a single group thereby facilitating cross-region communication.

Our development team has also redesigned global resource serialization latch manager and reduced the processor time involved with granting CMS locks. This helps to ensure that there won’t be a scaling issue with serialization mechanisms.

Another important factor in supporting application growth is the availability of storage below the 16 MB line. z/OS teams are progressively moving system control blocks above the 16 MB line to free up storage below the line for use by business applications. In z/OS V1R6, EXCP large blocks are above the line. Increasing the internal SMF buffer size to 1 GB helps to prevent important system management data from being lost due to buffer overflow. IPL time is another constraint brick we are working on removing. During IPL, IOS initializes dynamic pathing for all devices. Before V1R6, z/OS had to process each device path individually. Now, you can process up to 255 devices, which reduces the overall elapsed IPL time.

Keep talking

With z/OS V1R7, work on vertical CP growth continues. We’ve increased your ability to grow DASD capacity while staying within the limits of device addressability by making an additional 64K subchannels available to define PAV aliases.

Our teams continue to address the issue of storage constraints below the 16 MB line. This time around, by moving IOS large blocks and the program fetch work area above the line. With the delivery of larger DASD volumes, we’ve upgraded the sequential access method to support more than 64K tracks. This allows you to take advantage of the space available on larger volumes.

Enhancements to JES2 allow it to exploit the capability to use more than 64K tracks for spool data sets. Those of you with large DB2 workloads are probably aware that DB2 opens a large number of data sets when it initializes and that there is a limit to the number of data sets you can have open concurrently. With z/OS V1R7 and DB2 V8, that limit is 100K allowing for plenty of room before you get close to the thin ice.
Some ping wrong?
z/OS Communications Server can help you out

By RICK ARMSTRONG AND MICHELE CARLO

Imagine that you have just received a panicked phone call from one of your users complaining that he has “lost contact” with the system. After some preliminary investigation on your part, you determine that TCP/IP connectivity to the mainframe is down.

“Great,” you think, “What do I do next?”

We’re glad you asked! The z/OS Communications Server Troubleshooting Information Center is now available to help you with these kinds of problems. This Web-based resource is designed specifically to help you solve common networking problems. And it’s free of charge.

The z/OS Communications Server Troubleshooting Information Center includes diagnostic tips and information for researching common network problems. It also has links for more general information and offers you some ways in which to educate yourself about z/OS Communications Server.

The information center gives you access to:
- Tutorials
- Troubleshooting guides
- White papers
- Technotes
- Product publications.

For IP problems, the information center has troubleshooting guides on a variety of topics, including ping failures, device failures, secure Telnet problems, and what to do when you cannot establish a Telnet connection.

For SNA problems, the information center has tutorials on performing searches in mixed APPN and subarea networks. It also lists recommendations for APPN configurations, as well as their limitations.

You will find a link to a white paper that addresses how to adapt SNA applications in an IP world. And if you’ve ever wondered what to do when VTAM® cannot locate resources in border node configurations, you’ll find out in a troubleshooting guide about border nodes.

Regardless of whether it’s an IP problem or a SNA problem that’s bugging you, the z/OS Communications Server Troubleshooting Information Center has something useful to offer. Use the information center early and often.

Consider it to be an integral part of your diagnostic tools for solving networking problems.
Don’t let IP data burst your bubble
Get a head start on security configuration with the NSCA

BY LIN OVERBY AND MARK T. WRIGHT

Implementing network security is fast becoming a top priority in many IT organizations. Perhaps you, too, are being asked to protect the mainframe data in your network post-haste. If so, you need answers quickly.

In z/OS V1R7, Communications Server adds new security technologies designed for quick deployment through a new tool, the z/OS Network Security Configuration Assistant (NSCA). Let’s find out how you can hit the ground running with this tool.

Recap of new technologies
As discussed in z/OS Hot Topics Newsletter Issue 13, August 2005, GA22-7501-04, z/OS Communications Server has added two new security technologies:

- Application Transparent Transport Layer Security (AT-TLS)
- Communications Server IPSec (CS IPSec).

AT-TLS or IPSec?
IBM wants you to focus on your network security needs, not on the gory details of hundreds of configuration statements and parameters. Therefore, we have some good news for you.

First, if you happen to like the gory details and all the configuration statements and parameters, you’ll be like a pig in mud. We have close to 200 pages of excellent reference, guidance, and sample material for you.

Otherwise, IBM provides a tool, the NSCA that makes AT-TLS and CS IPSec configuration a snap. The NSCA provides a GUI interface using wizards, graphical tutorials, and contextual help panels to guide you through setup and installation of both AT-TLS and CS IPSec.

Regardless of which technology you are implementing, the configuration tasks are the same when using this tool. In fact, you can configure both AT-TLS and CS IPSec together as one configuration task.

Getting started
Did we hear you asking the question, “Where can I get the manual for this tool?” There is no manual. The tool itself tells you how to use it. It contains a series of how-tos, including “How to Get Started,” a ten-minute tutorial on the basics of the tool. Would you want really to stop and read it? Perhaps not if it were just a bunch of text. But it’s more than that. In fact, it’s loaded with easy-to-understand pictures. See Figure 1.

Still can’t get going? Go to the frequently asked questions (FAQ) section in the GUI. For example, to see the answer to “How do I configure IPSec in a Host to Gateway topology?” just click on the question. A complete pictorial guide showing each step of this process is available.

Now let’s look at the new z/OS Network Security Configuration Assistant, a tool designed to help you implement these new security technologies.
Is it hard to learn?

No, the NSCA provides a level of abstraction in which you work with no more than three GUI configuration objects, regardless of whether you are configuring AT-TLS or CS IPSec, as follows:

- Traffic Descriptor objects identify specific IP traffic or applications. The tool comes with a large number of preloaded Traffic Descriptors, such as "TN3270_Server" and "FTP_Server." With a few mouse clicks, you can extend the preloaded set and add more customized Traffic Descriptors.

- Security Level objects identify a specific security technology, AT-TLS or CS IPSec, and the level of cryptographic protection to apply. The tool comes with a number of preloaded Security Levels. With a few mouse clicks, you can extend the preloaded set to add more customized Security Levels.

- Requirement Map objects map specific Traffic Descriptors to specific Security Levels. For example, within a single Requirement Map, you can indicate an entire set of security requirements to govern the behavior from your z/OS system to a branch office.

After you build these objects for your environment, you can reuse them for many repeating network security scenarios. For example, that Requirement Map you built to cover traffic between your z/OS system to a branch office can be referenced multiple times in your configuration—one for each branch office to which you want to connect.

With the creation of the Requirement Maps, much of the heavy lifting is done. For each TCP/IP stack, you create a series of Connectivity Rules. See Figure 2.

Wizards...

The NSCA does its best to keep you on the right track. It provides wizards to guide you throughout the process and ensure that you enter all of the necessary information. Generally, each wizard asks you a basic question and then guides you through the remaining configuration.

Figure 3 shows an example of one such wizard at work.

...and a health checker, too

The wizards do their best to keep you out of trouble, but you can still get things wrong. So, before installing your configuration for a specific TCP/IP stack, click on the Health Check button. The NSCA comes with a built-in health checker function that examines your configuration for possible pitfalls and provides you with feedback on aspects of the configuration that look suspicious or incorrect.

Let the NSCA watch your back

The NSCA is designed to dramatically improve your time-to-value ratio. If you choose not to use the NSCA to configure AT-TLS or CS IPSec, that's fine. Without it, however, there are no wizards or health checker; you will be the expert.

Protect your IP data; never let it go out alone!

How do I get the NSCA?

You can download it from the z/OS Communications Server Web site: IBM.com/software/network/commserver/zos/support.
Okay, so you have heard about all the great benefits of Dynamic Virtual IP Addresses (DVIPAs) and you’re sold. That is, you want the availability, scalability and flexibility that DVIPAs provide. You want to shield your end users from failures in network interfaces, applications, and systems or changes in the network and computing infrastructure.

There is one obstacle, however: does deploying DVIPAs mean that you have to deploy a dynamic routing protocol on your z/OS systems? And, if the answer is yes, does that become a deal breaker in your environment?

If this sounds familiar, read on, there might be some hope for you yet. While running a dynamic routing protocol on z/OS is the recommended approach to deploying DVIPAs, it is possible to reap many of the benefits of DVIPAs without doing so.

Before we go into the details of what that configuration looks like, let us quickly review the reasons for the dynamic routing protocol recommendation. That will help us better understand the alternative approach, including its benefits and any drawbacks.

Why a dynamic routing protocol is recommended

With a DVIPA, you can virtualize an IP address and the resources represented by the IP address. You can use a DVIPA to provide a virtual view of a system, an application or even an entire z/OS sysplex. This means that a VIPA is not tied to a specific network interface or even a specific system. This capability provides for a very flexible configuration, because a DVIPA can move dynamically from one system to another within a sysplex, during planned configuration changes or during unplanned outages.

Further, a DVIPA can tolerate failures in network components. Dynamic routing protocols, such as Open Shortest Path First (OSPF), and a dynamic routing daemon, such as the z/OS OMPROUTE daemon, facilitate this dynamic nature of VIPAs. OSPF and OMPROUTE help to keep the network infrastructure (such as routers) aware of the best current network paths to a DVIPA. As long as the system has some form of network connectivity, with at least one network path to the DVIPA, users can continue to use the DVIPA. This is true even if multiple failures occur within the network infrastructure.

Deploying DVIPAs without a dynamic routing protocol

Without dynamic routing protocols to keep routers and z/OS aware of the whereabouts of DVIPAs and the status of network adapters and LANs, we need to rely on a lower level protocol, the address resolution protocol (ARP), to help us achieve the availability characteristics we want. Using ARP for this purpose poses some restrictions on how we design and implement the IP network.

What is address resolution protocol?

Every network adapter that is connected to a local area network (LAN) has a hardware address associated with it. This address is known as the medium access control (MAC) address. A network adapter comes with a burnt-in MAC address—a universally unique MAC address.

When computers attached to a LAN need to send data to each other over the LAN, they build LAN frames. The frame header specifies the destination MAC address to which the frame will go. The frame body contains the data to be sent, such as an IP packet.

So, how does an IP node on a LAN discover the MAC addresses associated with other nodes on the same LAN? That’s where the ARP protocol comes into play. It allows any IP node on a LAN to ask for the MAC address associated with any IP address on the same LAN by sending a broadcast frame containing an ARP request for that IP address. The IP node that owns that IP address then responds with an Address Resolution Protocol (ARP) reply that contains the MAC address for one of its interfaces that is attached to this LAN. The IP node that receives the reply would then typically save the reply in an ARP cache. Caching the reply allows this information to be reused later if the IP node needs to send another IP packet to the same destination IP address.

OSA adapters and ARP processing

With OSA adapters operating in Queued Direct I/O (QDIO) mode, much of the ARP processing is done by the OSA microcode. Many TCP/IP stacks can share an OSA adapter and, as a result, share a single MAC address.

To help the OSA adapter determine which TCP/IP stack an incoming IP packet should be given, the OSA adapter maintains a table that includes the home IP addresses of all TCP/IP stacks that share the adapter. This table is known as the OSA address table (OAT) and its content is strictly controlled by the TCP/IP stacks, which register and deregister HOME IP addresses as they become active or inactive.

When an IP address is registered by a TCP/IP stack in the OAT, the TCP/IP stack indicates whether the OSA adapter will do ARP processing for this address. This allows the TCP/IP stacks to move ARP responsibility from one OSA adapter to another.

If an OSA adapter becomes unavailable, but a TCP/IP stack has another OSA adapter connected to the same subnet, the TCP/IP stack requests the other OSA adapter to take over ARP processing responsibility for the IP address of the failing OSA adapter in addition to its own IP address—or, in a sense, move the OSA IP address from one OSA adapter to another. This process is also known as ARP takeover.

VIPA and ARP processing

This ARP processing is the key to achieving high availability with DVIPAs.
in a sysplex without dynamic routing. The requirements for making this happen are the following:

- All OSA adapters from the LPARs in the sysplex attach to exactly one LAN subnet.
- All VIPA addresses are defined so they come out of that same LAN subnet.

Here, the routers attached to the same LAN use ARP processing to locate the network adapter to which they will send incoming IP packets for any of the VIPA addresses.

When a z/OS TCP/IP stack registers a VIPA address with multiple OSA adapters attached to the same subnet, the TCP/IP stack instructs one of them to do ARP processing for that VIPA address. If the OSA adapter becomes unavailable, the TCP/IP stack moves the ARP responsibility for that VIPA address to another OSA adapter, if one is available. See Figure 1.

If the VIPA address moves to another LPAR, the original owning TCP/IP stack deregisters the VIPA address and the new owner of the VIPA registers it with one of its OSA adapters to do ARP processing.

One element of ARP processing is that, during registration, the OSA adapter sends out a *gratuitous ARP reply* (an ARP reply no one asked for). If another IP node on the LAN (such as a router) has an entry in its ARP cache for that VIPA pointing to the originally owning OSA adapter MAC address, the entry is updated based on the gratuitous ARP reply. Afterward, it points to the new owner's OSA adapter.

In an environment without dynamic routing, it is not possible to re-route IP packets over alternative subnets, such as a dynamic XCF network, or MPC links between z/OS TCP/IP stacks. Availability for the LAN subnet, therefore, needs to be addressed through proper configuration of redundancy at the OSA adapter, LAN cabling, and LAN switch level.

The logical network in Figure 1 might look as shown in Figure 2 from a physical connectivity point of view.

Each z/OS LPAR has at least two physical OSA ports. Each of those ports is connected to two different switches that are connected to each other. To send outbound IP packets from z/OS systems that do not participate in dynamic routing updates, these systems must rely on the administrator defining static routing table entries. When using static routes, availability of the first-hop router might become an issue because there is no dynamic routing protocol to detect if such a first-hop router becomes unavailable.

One way to address this issue is to configure parallel first-hop routers to use technologies such as the Cisco Hot Standby Routing Protocol (HSRP) or the Virtual Router Redundancy Protocol (VRRP), which both allow the two first-hop routers to back each other up. If one of them becomes unavailable, the other detects it and takes over the router IP address of the failing router. Here, z/OS remains able to send IP packets to the first-hop router IP address.

**Summary**

The benefits of deploying a dynamic routing protocol in the network and on z/OS hosts go beyond the value provided in a DVIPA environment. A dynamic routing protocol can, for example, allow z/OS to have more optimal outbound route selection and can even provide for load balancing of outbound traffic over multiple adapters using the multipath routing feature, while retaining high availability and providing for a very flexible configuration.

At the same time, we realize that activating dynamic routing on z/OS might be an obstacle for some installations. If your site is one of these, we hope this article has provided a viable alternative to consider for exploiting DVIPAs without requiring dynamic routing.
It's SNA as hard as it looks
Consolidating SNA function

BY ERNIE GILMAN AND ERIKA LEWIS

Are you mulling over your SNA migration plans and SNA/IP integration strategies, and wondering what to do with your aging SNA networking equipment? If so, here’s a thought: Why not move some of that SNA function onto the mainframe itself, thus consolidating SNA traffic and skills, and providing a closer, more secure link to VTAM and the SNA applications running in z/OS?

To support this path, IBM has introduced Linux technology-based products for the mainframe. One example is IBM Communication Controller for Linux (CCL) on IBM System z9 and zSeries which allows you to move Network Control Program (NCP) functions such as SNI connectivity onto an IBM System z9 or zSeries mainframe.

Another product, IBM Communications Server for Linux (CSL) on zSeries, enables functions such as TN3270 server and Enterprise Extender in Linux. Moving these functions onto the mainframe allows you to consolidate them on a single machine, while preserving most of the existing VTAM and network definitions.

What to expect
When you consolidate SNA functions on the mainframe, much of your network management can continue to work as it does today. CCL comes with maintenance and operator subsystem (MOSS) console similar to the 3745 MOSS console, but with the added benefit of being accessible through a Web browser. Products like NTuneMon and Tivoli NetView® Performance Monitor (now part of IBM Tivoli OMEGAMON for Mainframe Networks) for monitoring and managing NCP work with only minor changes. CCL does not, for example, report CPU utilization, but will continue to report on things like control block pools, buffer pools, and token rings. You can also continue to use NetView for z/OS to manage the migrated SNA resources as you do today.

Making it easier to manage
Besides being able to retain the tools that you currently use, moving to the Linux on zSeries environment provides some advantageous new management opportunities. For example, IBM Tivoli OMEGAMON for Linux on zSeries provides real-time Linux monitoring. You can use it to collect and analyze information, such as CPU performance, network, system statistics, process and user information.

Because CCL and CSL use OSA Express adapters for network access, you can also take advantage of OMEGAMON XE for Mainframe Networks to monitor OSA utilization, transmission rates, and adapter capacity.

In addition, IBM Tivoli System Automation for Multiplatforms provides policy-based automation, which allows automated bring-up as well as fast detection and recovery of outages.

If you implement CCL and CSL on z/VM, you can use OMEGAMON for z/VM to manage multiple Linux images and obtain real-time analysis of key resource and workload performance indicators, as well as detect resource contention among virtual machines. You can also use various automation tools to monitor and recover Linux z/VM images from central site policy.

Find out more
To learn more about consolidating your NCP and Communication Server functions on the mainframe and managing these functions in the Linux environment, see the following Web links:


Thousands of options
Stable like the mountain peak
Can it play Starcraft?

Ian De Silva,
Michigan State University
HATS fantastic!
Integrating host applications in an SOA environment

BY VIKRAM GULATI

In today’s mainframe and core-systems environments, applications and processes built on traditional languages, such as COBOL and PL/I, and runtimes, such as CICS and IMS, continue to deliver a wealth of mission-critical benefits to enterprises of all sizes. Many of these existing applications run on the zSeries platform and are accessible through either 3270 terminals or terminal emulation programs.

These applications and processes might be the most valuable assets an enterprise owns. After all, they do run the business. However, much of this existing technology wasn’t designed to address today’s changing market and business conditions. More and more, enterprises are realizing that to respond effectively to these changing business conditions, the existing applications need to integrate with other IT environments across the entire enterprise and across the internet with business partners, suppliers, and customers.

This article explores the use of IBM WebSphere Application Server Host Access Transformation Services (HATS), which is designed to expose business logic from terminal based zSeries applications to perform a business activity. This business activity can then be integrated into a business process using WebSphere Process Server.

Service Oriented Architecture overview

Service Oriented Architecture (SOA) is a standards-based integration and development architecture that is independent of the differences in platforms, software architectures, languages, and network protocols. Even terminal access based applications can integrate into an SOA environment. Industry standard Web services provide a well-defined, scalable, and flexible implementation mechanism for SOA.

Web services allow applications to communicate with each other in a platform and programming language-independent manner. Applications work together by exchanging service messages back and forth. SOA communication relies on open standards that include:

• Simple Object Access Protocol (SOAP)
• Web Services Description Language (WSDL)
• Universal Description, Discovery and Integration (UDDI).

Web services are designed to cut the amount of time and money needed for systems integration—the single biggest IT expense of most companies. SOA, Web services, and HATS allow you to integrate current z/OS terminal application programs into your overall business processes.

HATS consists of two components:
• HATS toolkit with a set of wizards and editors that create J2EE applications using the IBM Rational® Software Development Platform
• A runtime program that provides connection management—the runtime program is packaged within the J2EE application built by the toolkit.

HATS macros and Integration Objects

You can build Web services using HATS macros and Integration Objects. Integration Objects are JavaBeans™ that run HATS macros. A HATS macro is a script that defines navigations through a set of host terminal screens. Each screen in a macro includes:

• A description of the screen
• The actions to perform for that screen
• The screen or screens that are presented after the actions are performed.

For optimal performance, you can configure connection pooling plus connect and disconnect macros. A connect macro “primes” a connection in a pool by navigating to the screen at which a ‘data’ macro can begin. A data macro prompts for input, navigates through the application to extract data based on the input, and then navigates back to where it can prompt for the next input.

Once macros are recorded to capture the actions on the terminal screen to complete a business activity, you need to construct HATS Integration Objects using the HATS toolkit. HATS Integration Objects have input properties for all macro prompts, and output properties for all macro extracts. You can use the feature of chaining to compose one or more interactive flows through the terminal application. Integration Object chaining is necessary when a single major task can take different screen navigation paths based on programmatic decisions.

HATS and Web services

Once Integration Objects are created in HATS, you can use the HATS toolkit to create Web services. These Web services provide the interface needed to invoke the business logic captured in the macros. Hence, with support for SOA in HATS, you can now extend existing terminal applications as Web services and make them “integration ready” to link to new applications. This enables “on-the-fly” integration among existing applications and across multiple business units across the enterprise. You can then link or integrate these applications into end-to-end, automated business processes — the essence of being an On Demand Business. This integration can be extended to partners, suppliers and customers to further automate business processes and drive higher productivity and efficiencies.

WebSphere Business Modeler and WebSphere Integration Developer

Within the context of business integration, there is a definite requirement for an integration framework that bridges the gap between the business people and the IT world. Business Process Execution Language for Web Services (BPEL4WS) fulfills this requirement by providing a standard XML language for expressing business processes consisting of functions defined through Web services interfaces.

A business analyst can use WebSphere Business Modeler (WBM) to choreograph business functions into a logical process model. WBM provides
comprehensive, user-friendly business process modeling and collaboration capabilities to graphically design processes across people, partners, and applications. You can translate and export the business process into BPEL4WS, which IT can apply into a service model using Web services through WebSphere Integration Developer (WID). WID can generate the code needed to deploy a BPEL4WS process to WebSphere Process Server (WPS).

HATS and WebSphere Process Server
WebSphere Process Server (WPS) helps to:

- Create and deploy new business processes
- Synchronize business information in multiple business applications on diverse platforms
- Transform message formats en-route between applications.

One of its components, WebSphere Interchange Server coordinates business process activities that span multiple applications.

While executing the various business activities in WPS that are part of a business process, there is a need to set up an interface with the host applications. Currently WPS can provide an interface with host applications, such as CICS through commarea invocations. However, many host applications do not allow for commarea invocation because the presentation logic is tightly mixed with the business logic, and the only way you can interface with the applications is by driving terminal screens.

The Web services feature in HATS allows customers to enable terminal based applications such as CICS and IMS. Consequently, a business activity can be completed by either a single Web service or a small collection of Web services, which drives the required number of terminal screens.

Example scenario using WPS and HATS
Figure 1 illustrates the scenario of obtaining a car insurance quote from an insurance company. The IT infrastructure consists of WPS, HATS, and other vendor specific applications. WPS is coordinating the entire business process and HATS interfaces with an Insurance Quote CICS application. When invoked, the HATS Web service will step through the required screens on the CICS host and send the output obtained back to WPS.

The entire process consists of the following steps:
1. Perform a credit check on the applicant.
2. Obtain a risk assessment of the applicant.
3. Send the data from the first two steps to a Web service running on WebSphere Application Server HATS through the Web services adapter in WPS. This Web service interfaces with a CICS application on the backend to obtain the quote based on the data sent. The results get sent back to WPS through HATS.
4. If the applicant likes the offer, the information from all the above steps is sent for underwriting.

This process can also be represented in Figure 2, which specifies the order in which it is meaningful to call a collection of services. Figure 2 shows how to model a simple business process in a Business Process Execution Language (BPEL) compliant mode. The steps of “Assign” and “Java Snippet” are simply the results of post processing the output from the earlier stage into an appropriate format for the next step. Figure 2 also shows that if a request is from a user whose credit information is already available, the process skips the steps of credit check and risk analysis. Similarly, upon credit check, there might not be any need for risk analysis and one could skip the risk analysis step and go to HATS directly for the quote.

With this infrastructure, an applicant can now get an insurance quote “on the fly.” Without HATS, a sales representative would have to manually collect the data from the first two steps, iterate through the green-screens on the host application to obtain the insurance quote, and finally send all that data for underwriting. Integration Objects and Web services can automate this process and help WPS communicate with the host application.

Conclusion
As we have seen in this article, HATS simplifies interactions with host applications and provides a way to invoke business logic on terminal applications through Web services. HATS is tops when you need a solution for your business to integrate z/OS terminal applications with other business activities in a SOA environment.
Head to head with benchmarks
Consider the mainframe

BY JIM PORELL

What is a benchmark? Typically, it is a comparison of two things in a “head to head” contest. In computer terms, it’s evolved down to the price performing solution. There is a problem with benchmarks, though. They can only compare one thing at a time. In a large enterprise, the cost of a single function may pale in comparison to a multi-function enterprise. And benchmarks sometimes compare mainframes to other systems in terms of cost and complexity often to the disadvantage of the mainframe.

Let’s look at an example of a benchmark. If you need to commute to work in Europe, the Smart brand car is a very attractive alternative to the cab of a tractor trailer truck. Both the car and truck hold two people with a couple cubic feet of storage. The car gets around 60 miles per gallon of gasoline and won’t cause sticker shock on the show room floor. The truck gets around 4 to 6 miles per gallon of diesel fuel and it will cause your checkbook to go up in flames if you were to acquire it. It is obviously cheaper to commute in the Smart car.

But, what if the problem was to move your house? You wouldn’t fit a piano in either vehicle, so you accessorize them with trailers. It’s still going to be tough to put a trailer behind a Smart car. And how many trips would you make in the car to get the move done? Now the tractor trailer combination can haul quite a bit of material in it. In fact, you might share trailer space with others to get a better price.

In these examples, we demonstrated the typical “either/or” mentality of most benchmarks. But we’re not done yet. Why can’t you use both? The family moves in the car and you hire the truck to move your furniture.

The same is true of computers today. Just like the tractor trailer that can’t zip through traffic, our mainframes just can’t drive the graphics in our PCs and PDAs. But they can do other great things. And they need a partnership with other systems to complete the tasks. This partnership can extend to application and database serving.

A recent customer test demonstrated that beginning a transaction on a non-z/OS web portal server to an existing mainframe transaction utilized 4 times more CPU on z/OS than when the same portal called Websphere on z/OS to launch the transaction. Those CPU savings translate directly to dollar savings in software license charges. But also in reduced operations complexity. Like all tests of this nature, the value to any particular business will vary.

So when you think of mainframes and you read about those benchmarking exercises that compare the mainframe to other kinds of systems, keep in mind what you’re comparing and understand how to leverage the power of the mainframe for your business. Remember to use the best of each of the servers that you may have to their advantages to get the best of all worlds. That’s something the benchmarks forget to tell you!

The wind blows softly through the leaves of autumn... Wait, that’s just the mainframe!

Frank Migacz,
Northern Illinois University

Nothing can compare; This mainframe beats all others flat into the ground.

Aaron McMahan,
West Virginia University at Parkersburg
The more systems the merrier
zSeries Electronic Service Agent

BY IVICA VARDIC AND MIKE EDWARDS

Back in z/OS Hot Topics Newsletter Issue 12, February 2005, GA22-7501-08, you learned that IBM Electronic Service Agent™ for zSeries helps you monitor your I/O environment. To enjoy the full benefits of Electronic Service Agent (program product 5655-F17), you should activate it across your entire system complex. This article offers some hints and tips to help you.

Installing on the first system and enabling connection to IBM

To set-up Electronic Service Agent on the first system in your system complex, follow these steps:

1. Learn the system requirements for installing Electronic Service Agent. Read Section 5 of Electronic Service Agent User’s Guide, SC38-7104.

2. Select a suitable z/OS system in your system complex for the initial install. The system should have catalog access to the SMP/E global CSI data sets, which have information on the installed products and services in your system complex.

   The system must satisfy the following software prerequisites:
   • z/OS or z/OS.e V1R5 or later
   • TCP/IP with FTP enabled
   • IBM Security Server or an equivalent product
   • z/OS UNIX System Services enabled and activated

3. Enable the Electronic Service Agent task, which is a Hardware Management Console (HMC) component on the initial system. This step allows Electronic Service Agent to send service data to IBM.

4. Install and configure Electronic Service Agent on the system, as described in the program directory and Electronic Service Agent User’s Guide, SC38-7104.

   Usually, your IBM customer representative performs the job of enabling the Electronic Service Agent task. This work requires selecting a suitable HMC, based on these requirements:
   • The HMC is at the most current level.
   • A local area network (LAN) connection exists between the HMC and all z/OS systems in the system complex for which Electronic Service Agent is to be used.

   To keep LAN access to the HMC separate from the CPU connections, configure a secondary LAN adapter on your HMC with a different IP submask for Electronic Service Agent use. As an alternative, you could assign one HMC exclusively for Electronic Service Agent use.

   As part of the enablement process, you must determine which data you want to collect and send to IBM:
   • IBM I/O device error data
   • IBM software inventory and PTF level.

   We recommend that you select both data collection options if you have zSeries or S/390 hardware that is under warranty or covered under an IBM maintenance agreement. If not, enable data collection for IBM software inventory and PTF level.

   With this option, you enable sending all Electronic Service Agent data, with the exception of I/O device errors.

   During the enablement process, you are prompted to define an FTP password to be used by Electronic Service Agents for transferring data through FTP to the HMC.

   For more information about enabling the HMC Electronic Service Agent task, see the “Console Actions” section in Hardware Management Console Operations Guide, SC28-6830.

Enabling and activating Electronic Service Agent reporting

You can activate Electronic Service Agent reporting in a phased approach; see the recommendations provided in Electronic Service Agent User's Guide, SC38-7104.

Which Electronic Service Agent reporting functions should you enable?
That depends on a number of factors, such as your current service contract agreement with IBM and your geography. For example:

- **Hardware problem reporting.**
  This reporting function requires your zSeries hardware to be under warranty or covered under an IBM maintenance agreement.

- **Software Inventory collection.** This reporting function is available at no additional charge.

- **HIPER/PE reporting.** This reporting function is available through selected service contracts with IBM and varies based on geography. HIPER stands for High-Impact, Pervasive.

Now let’s look at how to enable each of these reporting functions. If you are uncertain about whether you can enable a particular function, check with your IBM support representative.

### Activating hardware problem reporting

The hardware problem reporting function transmits selected LOGREC records to the HMC, which are then forwarded to IBM. By default, the function reports all I/O errors for the attached hardware devices. You can override this default by editing the HESPARMS data set. Clear any device addresses for which you do not want I/O errors to be reported.

### Activating software and HIPER/PE reporting

Use the Electronic Service Agent ISPF dialog to enable and activate the following reporting functions. See Figure 1.

### Deploying Electronic Service Agent in your system complex

By carefully planning the deployment of Electronic Service Agent product on your system complex, you ensure that your efforts will be efficient and effective. Use Table 1 as a guide in creating your deployment plan; it has recommendations for the number of reporting functions to deploy in your system complex.

Now you are ready to prepare for cloning the deployment data on other systems in the system complex. To do so, you will need to ensure that the other systems satisfy all of the prerequisites outlined for the initial installation system, according to the selected reporting functions.

Table 2 outlines the steps for deployment cloning.

### Exporting and importing configuration data

The import and export functions of Electronic Service Agent allow you to clone HESCONF customization data for all reporting functions, except for hardware problems reporting. With these functions,
you control which configuration data is imported or exported. You can invoke import and export through the Electronic Service Agent ISPF dialog or in batch mode. Figure 2 shows the dialog panel for the export function.

When deploying a new system, do not import or export enrollment information. The system to be deployed needs to be separately enrolled. Use import or export for enrollment information only when you want to backup your current system enrollment data.

**Activating reporting functions on deployed systems**
To activate Electronic Service Agent reporting functions on deployed systems, follow the steps in Electronic Service Agent User’s Guide, SC38-7104.

**Online resources**
You can find more information online; see the Electronic Services home page ([ibm.com/support/electronic](http://ibm.com/support/electronic)), and the following links:

---

**IBM’s mainframe: a stable lighthouse shining saves us from the darkness.**

Joshua Roys, Michigan State University
SystemPac is now on the menu

Are you ready to order?

BY JUDY WASHO HARRIS

Have you heard about the new house specialty at Chez ShopzSeries? It's a hit with the regulars, so we added it to the menu. You can order it now; just tell us how you want it—

“Garçon I’ll have a SystemPac® with z/OS V1R7 and some ISV products on the side. I’ll also like DB2, CICS, IMS and NCP on top. And, can I get that customized and served in a full-volume dump? And, may I have all that combined in a single order, please? Thank you.”

Wasn’t that easy? You can do it, too. z/OS migration is just a few mouse clicks away because SystemPac is now orderable on ShopzSeries. SystemPac, a customized system migration package for z/OS, is a recommended IBM delivery vehicle. With it, you save time, resources and effort to migrate, install, exploit, and maintain your z/OS system-related products, subsystems, and independent software vendor (ISV) products. With SystemPac, you can have a functional z/OS system—restored and IPLed—in less than a day. And with it comes the new technology, enabled and with subsequent service to upgrade your SystemPac’s maintenance.

You can now take advantage of the many key features of ShopzSeries when you order a SystemPac. You can browse the product catalog, including ISV products, select the appropriate products to configure your order, and reconcile technical requisites. You also have the option to upload your installed inventory report and the appropriate products are pre-selected to populate your SystemPac order. You can add or remove products as needed. You can view upgrade path information for both IBM and ISV products so that you can take advantage of the self-service ordering capability.

Want it to go?

Select your preferred delivery media. If your order contains products from multiple system releases (SRELs), you have the option to include all products in a single order, an exclusive feature of SystemPac. Alternatively, you can split your order into a separate order for each SREL. Another exclusive feature of SystemPac is the option to choose full volume dump as the delivery method. Dump by data set is also available. Then submit your order online.

Taking your order

Because SystemPac requires a service contract, your order is routed to Integrated Technology Services (ITS) for contract validation. ShopzSeries submits orders containing all licensed products automatically. ShopzSeries sends valid orders containing non-licensed products to the IBM Sales Center for order processing and fulfillment. If you do not currently have a service contract, you can request information about SystemPac. Someone in ITS will contact you, and you can establish the necessary contracts.

“Garçon, my check, please.”

On October 12, 2005, the price of a SystemPac in the U.S. was lowered to $9400.

In other geographies, SystemPac is included in other service offerings, such as Enhanced Technical Support in most of Europe, Comfort Line in Germany, and Express/Express+ in France. (Tipping is not allowed!)

For more information on SystemPac, visit: ibm.com/services/ca/en/custompac/deliverable/systempac.htm.

Ready for seconds?

You can now order several other CustomPac offerings in ShopzSeries:

- ProductPac®, available worldwide, is a software package that includes one product or a small number of products built according to your SMP/E consolidated software inventory (CSI).
- FunctionPac, available in Europe, is a group of z/OS related products in a new SMP/E zone as a snap-on.

For more information on these offerings, see the following Web sites:

Revving up EWLM with IBM Virtualization Engine

BY BERNICE CASEY, ANUJA DEEDWANIYA, AND SUE SHUMWAY

When you want to get your blood flowing and make the little hairs on the back of your neck stand on end, nothing compares to the thrill of a professional car race. It’s exhilarating to watch the masters of automotive manipulation as they race for the best lines, tune the suspension and refuel at the pit stops, and follow the advice of their crew chiefs as they jockey for position around the track. There is only one thing that motivates them — one final gleaming goal they all strive for… to cross the finish line first.

Finishing first, and finishing efficiently, is a goal that inspires us even when it comes to our IT environments. These days, a typical shop has multiple servers and storage devices running a variety of operating systems and middleware products. How can you most efficiently leverage all this to come out on top in the end? With EWLM, of course!

Learn to drive: An EWLM overview

Version 2, Release 1 of IBM Virtualization Engine™ Enterprise Workload Manager (EWLM) lets businesses monitor and/or manage workloads that span heterogeneous computing environments that include AIX, i5/OS, Linux, Microsoft Windows, HP-UX, Sun Solaris, and z/OS servers. EWLM allows you to define business-oriented performance objectives for workloads running across these different platforms, then monitor and manage actual performance against those objectives. You can monitor the performance of multi-tiered applications such as data mining, Web banking, e-mail, and B2B inventory management, as well as servers that run many different applications concurrently.

Wondering where Workload Manager (WLM) on z/OS fits in? EWLM and WLM can run simultaneously and actually complement each other very well. You can continue to manage z/OS workloads with WLM and then use EWLM to help intelligently monitor and manage application workloads, workflows, and the allocation of system resources across your heterogeneous enterprise.

Map the course: The EWLM landscape

A typical EWLM management environment consists of a domain manager, a combination of managed servers, and the EWLM Control Center, as illustrated in Figure 1.

Managed servers, domain managers, and other stars of the pit

The EWLM managed servers collect and aggregate transaction data for applications and operating system processes, then send the data to the domain manager. The domain manager collects all the data for the entire domain, aggregates it, and then displays it in the EWLM Control Center.

When choosing the platform on which to deploy your domain manager, consider the legendary availability, reliability, security, and intrinsic advantages of economy of scale inherent in z/OS. This makes z/OS an ideal choice to manage your expansive Virtualization Engine enabled infrastructure.

Sometimes your racing stars get really famous and need bodyguards. If a firewall exists between the domain manager and managed server, the EWLM environment will also need one or more firewall brokers. You might also opt for an external load balancer that distributes traffic based on goal-based recommendations from the domain manager. If you have POWER5 servers on your EWLM map, you can also configure partition workload groups that permit EWLM to dynamically adjust processing capacity among POWER5 partitions to ensure that performance goals are met.

EWLM Control Center

The EWLM Control Center acts as the crew chief passing tips and providing tactics to the driver navigating around the track. Installed with and hosted by the domain manager, it is a Web-based graphical user interface that manages and monitors the performance of servers in an EWLM management domain.

The EWLM Control Center supports three types of tasks:

- **Administrating:** Administration of an EWLM management domain involves creating, deploying, and maintaining the EWLM domain policy, which describes the set of classes that...
EWLM will apply to the EWLM domain.

- **Operating**: You can display the operational state of EWLM and of each server in a management domain, as well as trigger activities that alter operational states. You can query the identity of the service policy that is currently in effect for the management domain and initiate activation of a specific service policy by policy name.

- **Monitoring**: EWLM tracks and monitors work as it flows from one application or server to another, regardless of operating system. It monitors application-level transactions, operating system processes, or both. EWLM provides the most granular performance data when it monitors application-level transactions because the applications use the Open Group's Application Response Measurement (ARM) 4.0 standard APIs. These APIs are your mechanic’s true diagnostic tools—they allow EWLM to monitor a transaction as it hops from one application to another to continue processing. This allows you to determine at which hop a performance problem exists.

**Manage your fleet: Application instrumentation with ARM 4.0**

To ensure that work requests are performing as expected in a multi-tiered heterogeneous server environment, you must be able to identify work requests based on business importance, track the performance of those requests across server and subsystem boundaries, and manage the underlying physical and network resources used to achieve specified performance goals. You can collect this data by using versions of middleware that have been instrumented with the ARM 4.0 standard.

ARM 4.0 provides interfaces that are first called by an application and then used by EWLM to calculate the response time and status of work processed by the application. EWLM is responsible for aggregating and reporting the data collected from each managed server in a particular management domain. Using a standard, such as the ARM 4.0 interfaces, allows an operating environment, regardless of platform, to leverage the same set of base measurements.

**Brief your drivers: Domain policies**

A domain policy specifies performance goals for work processed in the EWLM domain. Each domain policy contains the following elements:

- Application definitions, which provide transactions for EWLM to monitor.
- Platform definitions (optional), which provide operating system processes for EWLM to monitor.
- Transaction classes, which identify application-level transactions for EWLM to monitor.
- Process classes (optional), which identify operating system processes for EWLM to monitor.
- Partition classes (optional), which identify partitions for EWLM to monitor.
- Performance goals defined in service classes that correspond to your business objectives or business partners' service level agreements.
- Multiple service policies, if you want to change a service class goal from one service policy to another.

Figure 2 shows the relationship between a domain policy’s components.

**Start your engines: Incorporate EWLM into your environment**

So, have we inspired you to satisfy your need for speed? If you’re interested in implementing EWLM in your own heterogeneous environment, race on over to the IBM Systems Software Information Center (publib.boulder.ibm.com/infocenter/eserver/v1r2/index.jsp) for more information. Enjoy the ride!

---

Figure 2 - Relationship between the components of a domain policy

---

I never knew that mainframes were so widely used throughout the whole world!

Van Landrum, University of South Alabama
And a one, and a two… All together now!
Enhanced Preventive Service Planning Tool

BY KEVIN PETERS

Have you ever been frustrated trying to determine not the recommended service, but the service needed to run a function within z/OS, particularly those which cross several components? Has the effort of determining whether you have service installed on your systems given you a headache? Well, the Enhanced Preventive Service Planning Tool (EPSPT) has been upgraded to help you with this problem!

Overview of the EPSPT
To make it easier for you to identify the maintenance that you need to order and install, IBM provides EPSPT, which was announced at SHARE 2004. The tool is located on the Web at: [techsupport.services.ibm.com/390/psp_main.htm](http://techsupport.services.ibm.com/390/psp_main.htm).

EPSPT provides you with an easy way to obtain service recommendations from a number of z/OS and z/OS related preventive service planning subsets — base z/OS components, CICS Transaction Server, DB2, IMS, MQSeries®, WebSpere Application Server and IBM System z™products. EPSPT also helps you quickly determine which of the service recommendations have already been applied or installed on a particular target zone in your system.

The new stuff!
In most subsets, the majority of service recommendations come from a single component with a few cross product dependencies. In some cases, however, IBM provides a function that spans multiple components. Some historic examples of cross component functions are “Sysplex DataSharing” and “YE2000”. The latest examples for which IBM has created functional service recommendation lists are the zSeries Application Assist Processor (zAAP) and IBM Health Checker for z/OS checks. We have also created an intra-component list for Global Resource Serialization Star.

Note that these service recommendation lists are not in RETAIN®. However, IBM is investigating whether to provide them through other service tools, such as ServiceLink.

You can obtain the service recommendations for function lists through the EPSPT graphical user interface, as follows:
1. Select Find Bucket Extract Files.
2. Select By Category.
3. Select Function under Step 1 — Select Type.
5. Press Add to cart.
6. Click the item in cart link.
7. Select the bucket and press Download now to extract the file from the cart.

As with previously supplied extract files, you can process the downloaded extract file with the EPSPT Host Tool to determine which service needs to be applied or installed.

Other enhancements
Previously, the extract files for RETAIN based PSP subsets only contained information from the service recommendation section. The new EPSPT information has been made more comprehensive. Now, all APARs and PTFs contained in each subset (and any extensions) are included in extract files. This is particularly beneficial for device related subsets that contain APARs and PTFs in the General Information section. Additionally, as of 12/07/2005, IBM TechSupport has merged the ability of researching PSP subsets and acquiring extract files; it is located on the Web at: [http://www14.software.ibm.com/webapp/set2/psp/srchBroke](http://www14.software.ibm.com/webapp/set2/psp/srchBroke). In the near future, the support of EPSPT will be transitioned from the earlier mentioned site to this one. Notice that the search capability from the earlier site is located on the bottom of the new page.

Feedback
Send us any comments, questions, or suggestions for future enhancements by using the Feedback link on the left navigation bar of the primary page.
Storage made easy
Answers that won’t drive you nuts

BY EDWARD BAKER AND SEAN MCMILLEN

z/OS system programmers, z/OS storage administrators and independent software vendors are asking IBM some typical questions about storage. Let’s take a look:

Dear IBM,
I use tape mount management (TMM) heavily in my shop. This is in order to minimize the number of tape mounts and maximize the usage of my tape resources during tape mounts. I have noticed that these tape mount management data sets are not eligible for the fast subsequent migration (FSM) function. Is there anything that one can do to allow these data sets to be candidates for fast subsequent migration?

Thanks,
Mr. Tapemount

Dear Mr. Tapemount,
You are in luck; beginning in z/OS R7 we have implemented changes to fast subsequent migration that can solve your common dilemma. As you’re aware, fast subsequent migration is a function that allows data sets that have been recalled from migration level 2 (ML2) tape to be reconnected to the initial place of origin on that ML2 tape. This is only possible if the data set was not modified since being recalled. In a tape mount management (TMM) environment, data sets are normally assigned to a management class or storage group that does not require backup. You were most likely encountering this problem because no valid backup copy typically exists for data sets in a TMM environment.

In z/OS V1R7, DFSMShsm, with assistance from other z/OS DFSMS components, developed a more rigorous FSM design that allows TMM-type data to be reconnected. In fact, even data sets without a valid backup copy are now eligible for fast subsequent migration as long as the data set remains unaltered since the recall. Let us know how this enhancement works for you!

Thanks,
IBMer

To DFSMShsm Development,
I utilize your HMIGRATE command daily. Typically, it’s when I am about to leave work and I want to migrate all my L0 volume data sets that I used that day.

I migrate most of my data sets to ML1 DASD, or even sometimes ML2 tape.

When I found out that I could use partially qualified data set names on the command with the use of filters (also known as wildcards) I was ecstatic. This allowed me to accomplish all migrations with a single command.

Because I don’t reuse every single data set created every day, I often find that I get an annoying error message.

The error message appears for every data set that meets the filter criteria that is already migrated. Is there a way to turn off notification of all these error messages? I really like using the HMIGRATE with wildcards (*).

Thank you,
Mrs. Migrate

Dear Mrs. Migrate,
We understand your request, and we have an answer for it beginning in DFSMShsm V1R7. We will no longer issue the ARC1224I message for data sets already migrated to ML1 when you use the HMIGRATE command with partially qualified data set names and filters.

Additionally, you will no longer see the ARC1282I error message when the data set already resides on an ML2 tape volume. This eliminates the multitude of error messages that you receive during your migration processing. By the way, we also implemented the bypassing of error messages whether or not you specify the ML2 parameter on your HMIGRATE command. Try it out and let us know what you think.

Thanks,
HSM Development

To IBM,
We have recently invested in your latest high capacity tape media, the IBM TotalStorage® 3592 Tape Cartridges. I find it just phenomenal that you can put 300 GB of uncompressed data on a single tape these days. I remember back when the 3480s came out in 1984 and the capacity was 200 MB of data. Back in those days that was a whole lot of data (ha-ha!). Anyway, we have found that DFSMShsm has not been filling our larger tapes to their full capacity. We see this primarily when we place hundreds of thousands

February 2006 z/OS HOT TOPICS Newsletter, Issue 14
Dear Mr. Quartercentury,

We have just the thing for your capacity concerns. We have a new enhancement in V1R7 of DFSMShsm that allows us to write significantly more data sets per tape. We used to be able to describe 330,000 data sets in a DFSMShsm tape volume tape table of contents (TTOC). Now in V1R7, DFSMShsm can describe up to 1,060,000 data sets in a tape volume TTOC (wow!). There is some preparation on your part if you want to use this new EXTENDED TTOC enhancement. Just follow the steps below and you will be on your way:

1. Ensure that all hosts in an HSMplex are at z/OS DFSMS V1R7.
2. Define your offline control data set (OCDS) with a maximum record size of 6144 bytes, as described in z/OS V1R7 DFSMShsm Implementation and Customization Guide.
3. Enter the SETSYS command with optional parameter EXTENDED TTOC(Y) to enable the support.

It is that easy. Remember, we might not write over 1 million data sets per tape if we do indeed fill the tape up with data. Oh, by the way, don’t feel bad about remembering the 3480s. I still have punch cards scattered around my office and a slide rule by my PC!

Thanks,
IBMer

Hello IBM,

I am head of architecture at ISV123. We specialize in developing data mining and reporting applications for the z/OS platform. Recently, we have had many customer requests for an application to data mine DFSMShsm’s migrated data and provide information back to the end-user. Currently, we are in the process of designing a new application. We have noticed that we cannot determine the logical record length (LRECL) of any migrated data sets without recalling the data set. This is very costly prohibitive for us and cumbersome. Is there something we are missing here?

Thanks,
Dr. Dataextract
ISV123 Lead Developer

Greetings, Dr. Dataextract!

DFSMShsm has a solution to your request beginning in z/OS V1R7. We have added a LRECL field in the MCD record for all VSAM and non-VSAM migrated data sets. In addition to the LRECL field, you might also be interested in another bit we added. It indicates whether the data set was empty at the time of migration. We have enhanced the DFSMShsm LIST MCDS command with the new option SELECT(EMPTY) to allow easier identification of all empty migrated data sets. You can use the IDCAMS DCOLLECT utility with MIGRATEDDATA option to retrieve this newly recorded information from the MCDS, along with many other data set characteristics. Keep in mind that this information is only available on those data sets that have been migrated using a z/OS DFSMShsm V1R7 system or higher.

Happy Mining!
IBMer

Hello Mr. Connected,

Currently, I create an aggregate backup and recovery support (ABARS) aggregate with an ALLOCATE statement in the selection data set for all my ICF user catalog and GDG base definitions. I call this aggregate my “baseline” aggregate because it defines the required ICF user catalogs (and the associated aliases), and the GDG base definitions. These need to be in place before I use the ARECOVER command to recover the remaining aggregates that contain critical application data. In this aggregate, I would prefer not to actually back up any data, but currently I’m required to include at least one data set in the aggregate or the ABACKUP command fails. Is there anything you can do to eliminate the need to have an INCLUDE statement in the selection data set for an aggregate group?

Thanks,
Ms. Noinclude

Hello, I have some connected sets that never get recycled even though the percentage of valid data on the connected set is below the PERCENTVALID specified on the generic RECYCLE command. In my shop we have a limited number of tape cartridges and we need to return tapes to scratch as quickly as possible. Can anyone tell me why DFSMShsm does not recycle these connected sets?

Thanks,
Mr. Connected

Hello Mr. Connected,

The algorithm used by the generic RECYCLE command calculates the PERCENTVALID criteria to decide if a connected set is eligible for recycle. In order for the connected set to get recycled, two criteria have to be met:

- The first volume in the connected set must meet the PERCENTVALID threshold.
- The connected set as a whole must meet the PERCENTVALID threshold.

Most likely, your connected set does not get recycled because too much valid data exists on the first volume in the connected set. This prevents recycle from even looking at the total amount of valid data in the entire connected set. DFSMShsm V1R7 provides you with a new option that allows you to decide if the first volume in the connected set must meet the PERCENTVALID threshold. A new CHECKFIRST(Y | N) keyword has been added to the RECYCLE command. The CHECKFIRST keyword indicates to RECYCLE processing whether or not to check whether the first
volume in the connected set meets the PERCENTVALID threshold. If you specify CHECKFIRST(N), then the first volume in the connected set no longer has to meet the PERCENTVALID criteria. The average percentage of valid data for the entire connected set must still be less than the PERCENTVALID. This allows you to RECYCLE those connected sets that have been giving you problems and return those needed tapes to your scratch pool.

Sincerely,
IBMer

Hello IBM,

We are a very large installation requiring DFSMSHsm to manage millions of data sets every month. We run primary space management, secondary space management, automatic backup and automatic dump daily. We also run interval migration hourly. We are encountering a problem because our DFSMSHsm journal fills up multiple times each day. This occurs even though we have it allocated as a full 3390-3 volume. When the journal fills up, we automatically schedule a control data set (CDS) backup to backup the CDSs and null the journal. Because of our heavy DFSMSHsm workload, we cannot afford to quiesce DFSMSHsm activity multiple times a day in order to backup the CDSs and null the journal. Is there something we can do to reduce the frequency of the need to backup the CDS to once a day or less?

Wondering…
Mrs. Journal

Hello Mrs. Journal,

Help has arrived in the new V1R7 release of DFSMSHsm. This release of DFSMSHsm allows the DFSMSHsm journal to be allocated as a large format sequential data set. A large format sequential data set eliminates the 64 K tracks per volume limitation that previously existed for sequential data sets. Installations can now take better advantage of the larger volume sizes by allocating their DFSMSHsm journal as a large format sequential data set on one of these volumes. By allocating larger journals, installations can reduce the frequency of CDS backups that are caused by journal-full conditions.

Important: Make sure that all instances of DFSMSHsm in an HSMplex are at DFSMS V1R7 or higher before defining their journal as a large format data set.

Thanks,
IBMer

Dear IBM,

Sometimes I encounter a situation where a DFSMSHsm task is endlessly waiting for a tape mount. The only way I can free up the tape drive is to stop DFSMSHsm and restart it. In our environment today, we cannot afford an outage to stop DFSMSHsm and restart it when such a problem occurs. It would sure be nice if we had a method to be able to cancel just the DFSMSHsm task that is having the problem.

Thank you,
Mr. Cancelactive

Hello Mr. Cancelactive,

Eureka! DFSMSHsm now provides the capability to cancel any active data movement task except for the DFSMSHsm Fast Replication functions of FRBACKUP and FRRECOV. The DFSMSHsm QUERY ACTIVE and CANCEL commands have been extended to allow installations to determine what data movement tasks are currently active on their system. They can then use this information to cancel an active task. Issuing the QUERY ACTIVE command with a new TCBADDRESS parameter causes DFSMSHsm to return a message for each active DFSMSHsm data movement task. It also returns either the address of the TCB for the task or an index to the secondary address space (for ABARS tasks). Installations can then use the CANCEL command with the TCBADDRESS or SASINDEX parameter to cancel the active task or address space. No more need to cancel the entire address space. This function is so new that we did not make the z/OS V1R7 publications deadline with our updates. Reference the APAR OA09344 for the documentation for this function.

Let us know how it goes,
IBMer

P.S. Here is some more good news: Because of the high demand for this function, APAR OA09344 is providing this support for lower level releases of DFSMSHsm including V1R4, V1R5 and V1R6.
Off to a great start!
A+ for Academic Initiative

BY DON RESNIK AND MIKE TODD

On October 3, 2005, hundreds of college and university students from across the United States and Canada logged into a mainframe system for the first time. They were racing to be among the first students to complete the challenges set forth in the Student Mainframe Contest, a grassroots effort devised by a team of IBM new hires, customer new hires, college students and co-ops, brought together under IBM’s Academic Initiative.

Increasing awareness
Many students are unaware that they use mainframes on a daily basis, or that the mainframe is still central to computing across just about every industry. The IBM Academic Initiative wants to make sure that students are aware of these things, but most importantly make sure they realize the significant career opportunities opening up as the current generation of mainframe professionals nears retirement age.

Through the Student Mainframe Contest, the Academic Initiative team hoped to reach out to 200 students. By the end of the contest, over 700 students from 77 colleges and universities had signed on to “master the mainframe.” The enthusiastic response from students—driven by their curiosity to find out more about the system while earning prizes as they completed mainframe challenges—clearly showed that students have quite an appetite for learning about the mainframe.

Pieces of the puzzle
There were three parts to the contest—each part more difficult than the previous one. In part one, students learned how to:

- Download a 3270 terminal emulator
- Navigate around the system
- Allocate their own data set member.

They were also encouraged, just for fun, to write a haiku poem about the mainframe in their data set. You’ll see some of the contestants’ poetic talent sprinkled throughout this issue of z/OS Hot Topics Newsletter.

In part two, contestants had to:

- Fix JCL errors
- Run REXX execs
- Use SDSF to check messages and output
- Debug problems with help from the LookAt tool
- Create their own ISPF panels
- Track down TCP/IP configuration settings.

You have to admit—that’s not too shabby for mainframe newbies!

By the time they got to part three, the contestants had to solve the most difficult challenges such as:

- Solving CICS/DB2 interactivity issues
- Fixing assembler and Java programs
- Resolving planted problems in their JES initiators.

Students showed such an aptitude for picking up mainframe concepts that they were encouraged to write their Student Mainframe Contest accomplishments on their resumes to discuss with recruiters. They had to show significant skills to complete these challenges, and that skillfulness will help differentiate them from other job seekers.

The Student Mainframe Contest increased students’ awareness of the opportunities and careers that mainframes offer, while giving them a taste of what the mainframe can do. The IBM Academic Initiative is already working to build on that momentum—with the excitement that students have shown recently, the future of mainframe skills is looking brighter all the time.

To find out more about the Academic Initiative, visit the Web site: [ibm.com/university/zseries].

Off to a great start!
A+ for Academic Initiative
Extra! Extra! Read all about it!
zSeries Platform Test Report for z/OS and Linux Virtual Servers

IBM zSeries Platform Test is the software testing team for all seasons—and for all releases of z/OS! We are a team of z/OS system programmers who run a Parallel Sysplex on which we perform the final verification of a z/OS release before it becomes generally available to you. As we do our testing, we gather our experiences, hints, tips, and recommendations and we publish them as zSeries Platform Test Report for z/OS and Linux Virtual Servers, SA22-7997.

We publish our test report with each new release of z/OS and provide a refreshed edition in between z/OS releases. You can find our experiences with z/OS V1R7 in the December 2005 edition. We also bring you late-breaking news in the form of our latest tips and experiences.

Our contributors

Rick Armstrong has been a VTAM and TCP/IP service expert for 16 years. He currently specializes in Web hints and tips.

Edward Baker is a Senior Software Engineer with IBM and currently is a developer on the DFSMShsm product. Ed has been with IBM for 26 years and has worked exclusively with MVS, OS/390, and z/OS software and hardware products during this period.

Julie Bergh is a Certified IT Specialist, currently with IBM's Software Migration Project Office (SMPO). She has over 25 years of IT experience in MVS and related areas. Her areas of expertise include MVS systems programming, RACF, and RACF migrations from competitive software.

Michele Carlo has been writing information to support IBM mainframe software products for over 20 years. In addition, she manages a variety of Communications Server projects.

Bernice Casey is an IBM Senior Technical Staff Member with almost 10 years experience on IBM mainframe systems. Her area of expertise is usability: understanding customer needs and translating those needs into product design.

Wai Choi has been working in RACF for nine years. In that time she has worked in development, test, and design. Her main projects include digital certificate support from RACF and PKI Services.

Alfred Christensen is a programming consultant in the Enterprise Networking and Transformation Solutions (ENTS) group at IBM Raleigh. He has worked with IBM mainframe operating systems and software for 30 years, with the last 10 years focused on z/OS networking software with special emphasis on the TCP/IP protocol suite on z/OS and, more recently, with general SNA over IP integration technologies. Alfred is a frequent speaker at various conferences, such as SHARE, NSTC, and the zSeries Expo.

Anuja Deedwaniya is an IBM Senior Technical Staff Member in the z/OS core design group. Her areas of expertise include Virtualization Engine on z/OS, z/OS Language Environment including the application stack on z/OS, and 64-bit Virtual.

Ronald Edick is an Advisory Engineer in Systems and Technology Group at IBM Poughkeepsie. He is a developer/tester in z/OS Cryptography and was test team lead for the Encryption Facility project. Ron has been with IBM for 25 years.

Mike Edwards is a software engineer on the development team for Electronic Service Agent for zSeries. He holds a Master's Degree in Engineering from the University of Toronto and has worked in the IT Industry for more than 20 years. Before joining IBM, Mike worked in a number of industries as an independent consultant.

John Eells is a former MVS and OS/390 system programmer, more recently a ServerPac designer, now a Senior Software Engineer in the IBM Systems & Technology Group. John's current assignments include z/OS Technical Marketing.

Peggy Enichen is a Senior Software Engineer in the z/OS Development organization in IBM Poughkeepsie, NY. She is a designer/developer for z/OS Integrated Cryptographic Service Facility (ICSF), and designer/developer for the IBM Encryption Facility for z/OS Encryption Services. Peggy has been with IBM for 36 years.

Ernie Gilman is a Senior Consulting IT Specialist with IBM, specializing in Tivoli zSeries end-to-end solutions. He is the creator of IBM NTuneMON, an expert system for managing z/40s. Ernie has been with IBM since 1974, and has worked on VTAM, NCP, NetView, and Tivoli solutions.

Vikram Gulati is an engineer in IBM Software Group at Raleigh. His main focus is on improving the scalability and performance of WebSphere HA TS to support many concurrent users efficiently. He holds a B.S. in Electrical Engineering from Purdue University.

Rich Guski is an IBM Senior Technical Staff Member focusing on zSeries Security Design and Architecture.

Tim Hahn is an IBM Senior Technical Staff Member with IBM and has been with the company for 15 years. He works on security product architecture, design, and development for IBM Tivoli. Tim has worked on a variety of products in the past including lead architecture, design, and development for the LDAP directory server for z/OS.

Judy Washo Harris is a project manager for IBM Global Services. Since joining IBM in 1981 as a systems programmer, she has worked in enabling ISVs for new technologies, and is now the SystemPac ISV business manager. Judy also does technical marketing for CustomPac and project manages ServiceLink/CustomPac development.

Evan Haruta is an Advisory Software Engineer in Systems and Technology Group at IBM Poughkeepsie. He works in z/OS Level2 for DV, auxiliary and real storage management.

Dr. Thomas Kamei joined IBM in 1999, and has since worked on HCD and HCM. As technical leader of HCM, he is responsible for the design, development, and testing of HCM. Thomas Kamei holds a diploma in mathematics from the Technical University of Munich (Germany) and a PhD in applied mathematics from the University of Bonn (Germany).

Gus Kassimis is a Senior Software Engineer in the Enterprise Networking and Transformation Solutions (ENTS) group at IBM Raleigh. He has worked on IBM mainframe technologies for over 18 years. Gus is currently focused on design for the z/OS Communications Server with a focus on high availability TCP/IP technologies. He is a frequent speaker at conferences, such as SHARE.

Kevin Kelley is a Senior Software Engineer with more than 30 years experience on IBM mainframe systems. His area of expertise is console operations and automation. Kevin is one of the designers of z/OS console support.

Mike Kelly is a Senior Software Engineer in Systems and Technology Group at IBM Poughkeepsie. He is a designer/developer for ICSF. Mike has been with IBM for 25 years.

Nancy Lewallen is an Advisory Software Engineer in zSeries Information Solutions at IBM Poughkeepsie, focusing on security.

Erika Lewis is a Senior Software Engineer in the Enterprise Networking and Transforming Solutions (ENTS) group at IBM Raleigh. She was the development release manager for the initial releases of IBM Communication Controller for Linux on System z9 and zSeries and IBM Communications Server for Linux on zSeries. She now works in the Business Development department within the same area, and serves as a development interface to sales representatives and customers for these new product offerings.

Tan Lu is the program manager for data encryption in Systems and Technology Group at IBM Poughkeepsie.

Debbie Mapes is a Senior Software Engineer at IBM Poughkeepsie. She has been a RACF designer for 15 years and previously provided support for RACF in the service organization.

Sean McMillen is a Software Engineer in z/OS DFSMShsm located in sunny Tucson, Arizona. He has been with IBM for 5 years and recently presented at SHARE Anaheim and the zSeries Expo. He enjoys spending time with his wife, Allison, and son, Jacob.
Ed Mekeel has been with IBM for 36 years. His background includes five years in computer operations and seven years with automated operations software development. Ed is currently the content manager for the BCP as part of the zSeries Software Portfolio Management department in Poughkeepsie, NY.

Lin Overby is an IBM Senior Technical Staff Member in the z/OS Communications Server strategy and design group. He is a designer for z/OS Communications Server with a focus on TCP/IP technologies and is the lead designer for network security on z/OS. Lin has been with IBM Raleigh for 27 years, holds 32 patents or patent applications, and was named an IBM Master Inventor.

Kevin Peters has been an IBM employee for 23 years and has spent most of his career in Remote Service and Support organizations.

Kathy Pfeiffer is an Advisory Software Engineer in Systems and Technology Group at IBM Poughkeepsie. She is the curriculum manager for the IBM Academic Initiative, System z9 Program.

Jim Porell is an IBM Distinguished Engineer and Chief Architect of zSeries software. He’s had 25 years in the mainframe arena, specializing in areas such as XRF, PR/SM LPAR, distributed computing, UNIX System Services and Security.

David Raften is an Advisory Software Engineer in IBM Poughkeepsie, with more than 22 years of experience at IBM. Currently on the GDPS® team, Dave has spent several years with a z/OS planning group, and has been helping customers with Parallel Sysplex technical support since 1994.

Don Resnik is the program manager for the IBM Academic Initiative for zSeries program.

Kurt Schroeder is a Senior Programmer in the eServer™ Hardware System Management organization at IBM Endicott. He is a lead designer for the eServer Hardware Management Console series of products. Kurt has been with IBM for 21 years.

Sue Shumway is an information developer for IBM Virtualization Engine who moonlights as executive editor of the z/OS Hot Topics Newsletter. She graduated from Rensselaer Polytechnic Institute with a B.S. in engineering and an M.S. in technical communication.

Tom Sirc has been testing IBM mainframes for over twenty years and leads the WebSphere test team in zSeries Integration Test at IBM Poughkeepsie.

Don Spangler is a Human Factors Engineer in the User Technologies organization of Systems and Technology Group at IBM Poughkeepsie. He is the User Experience Architect for the HMC. Don has been with IBM for 6 years.

Mike Todd is a Staff Software Engineer in the Information Development Department at IBM Poughkeepsie.

Joseph Turner is the zSeries Hardware Brand I/O program manager in Systems and Technology Group at IBM Poughkeepsie.

Ivica Vardic is the Technical Lead for the CustomPac Offerings group at IBM Canada, where he led the development of the Electronic Service Agent for zSeries product. Ivica holds a Bachelor of Science degree in Computer Science from the University of Belgrade, and has been a speaker at SHARE conferences.

Ashwin Venkatraman graduated from Clarkson University in 2003. He has been working at IBM for two years on WebSphere for z/OS security testing in the zSeries Integration Test group.

Marna Walle has been with the z/OS Build and Installation department for 16 years. Her current responsibilities include z/OS release migration and new installation technologies of the z/OS platform. She is a frequent speaker at customer conferences on z/OS installation topics.

Eric Weinmann is a Senior Software Engineer in Systems and Technology Group, Global Firmware Development team, at IBM Endicott. He is the Design/Development lead for HMC Tree Style Web User Interface. Eric has been with IBM for 18 years.

Joe Winterton is a release manager in Tivoli OMEGAMON development with over 30 years experience in IBM mainframe systems. He enjoys bringing to market system management solutions that met customer needs.

Mark Wisniewski has worked in Systems Performance for 24 years. He is responsible for assessing current and future systems growth constraints and improving performance across the zSeries platform. Mark also drives work efforts to improve high MIPS scalability for zSeries.

Mark T. Wright is a Senior Software Engineer in the z/OS Communications Server development group at IBM Raleigh. He is the lead developer for z/OS Communications Server new initiative, Make It Easy. Mark has been with IBM for 23 years.
Coming to a college near you
z9 and zSeries operating systems curriculum

Are you interested in finding out how the IBM Academic Initiative could influence the system programmers your company hires? Here is a sampling of the courses that participating colleges and universities are offering your potential new hires:

If you are an IBM Academic Initiative member, you can find course materials by looking for “Curriculum & courseware” in the navigation pane of the IBM Academic Initiative Web site: www.developer.ibm.com/university/scholars.

If you represent a college or university and are not yet a member, no problem! It’s easy to become one. Select “Apply Now” on the top right-hand corner of the same Web page to receive your free membership.

Currently, there are over 200 colleges and universities actively teaching or considering offering zSeries classes. You can find some of these schools by checking out the following Web site: www.developer.ibm.com/us/en/university/scholars/products/zseries.

Honorable Mention:

There was an old hacker from Lisbon
Who sighed as he logged on the system
“These mainframes,” said he
“are the best there can be,
it’s a damn shame those young kids have missed ‘em!”

Eric Entzel, North Dakota State University