IBM Tivoli Security and System z

While Tivoli® has been the champion of distributed systems management, including security management, for many years, its penetration into the mainframe space has been quietly occurring through internal development and acquisitions.

This IBM® Redpaper looks at two areas: the Tivoli Security products that can be installed on the different System z™ operating systems, and what security management capabilities our products provide for System z resources.

The paper assumes that the reader is familiar with the Tivoli Security products, but new to the mainframe. By way of introduction we discuss some of the fundamental System z terminology, including the different operating environments available for System z hardware.

What is all this “z”? 

The IBM mainframe has been around for over 40 years. What started as the System/360™ series of machines in 1964 has now grown into the current System z family of hardware. There have been a few name changes along the way, including the S/390® and zSeries®, coming now to System z. For a brief history see the article 40 Years of Mainframe Innovation and Value at the following location:

http://www.ibm.com/servers/eserver/zseries/timeline/

The current range of hardware includes:

- The System z9™ (or z9) Business Class
- The z9 Enterprise Class
- The eServer™ zSeries 990
- The eServer zSeries 890

Details on these machines can be found on the System z hardware page located at:

http://www.ibm.com/systems/z/hardware/

If you look at the specifications of these machines you will see a list of supported operating systems, such as z/OS®, z/VM®, z/VSE™, TPF, z/TPF, and Linux® on System z. When you
think of a mainframe, you tend to just think of one OS, much like you think of Windows® on Intel® and AIX® on System p™, but this is not the case with the mainframe.

**System z and virtualization**

Before looking at the different operating systems (OSs) we need to mention how they run on the System z hardware. There are two ways: running natively on the hardware, with one OS for one physical machine; or running in a virtualized environment such as a Logical Partition (or *LPAR*) or on z/VM.

A logical partition provides the set of resources necessary to load and execute an operating system and user applications. A single physical System z system can host several operating systems that operate concurrently under control of the PR/SM™ microcode and hardware mechanisms. Each logical partition appears as a complete system to its users and administrators.

Figure 1 shows these two virtualization technologies.

![Diagram showing System z and virtualization](image)

**Figure 1**  *System z and virtualization*

Figure 1 shows the System z machine split into three logical partitions (LPARs): LPAR A, running z/VM; LPAR B, running z/OS; and LPAR C, running VSE/ESA™.

At this level there are three logical machines running. However, the z/VM LPAR is hosting seven Linux images, so in total there are 10 virtual machines running, one by z/OS, one by VSE/ESA, one by z/VM (it is a machine in its own right), and seven by Linux on System z.

Figure 1 also shows two virtual networking mechanisms: *HiperSockets™* that are used to communicate between LPARs, and Guest LANs that can be used to mirror a networking topology identical to that of any distributed environment. As these are virtual (within memory) rather than physical (cabling and network devices), they can be much faster than traditional networking.
System z operating systems

Continuing on from the previous section, we can have a single OS running on a physical machine, or multiple OSs each running in its own logical partition, or on z/VM (itself an operating system). The following sections describe each of the operating systems supported on the System z hardware.

TPF* is a specialized high-speed transaction processing OS used by many of the airlines. z/OS.e is due for retirement. We do not discuss these operating systems in detail, as they are not relevant to Tivoli.

For further information see the Operating Systems for System z page at the following location:
http://www.ibm.com/systems/z/os/

z/OS

z/OS is the operating system normally associated with the mainframe. Most of the mission-critical business applications for the largest customers, often with large databases and CICS® transaction-based systems, run on z/OS. Its heritage can be traced to the OS/360 operating system back in the 1960s and has gone through many iterations, such as MVS™ and OS/390® to the current z/OS.

z/OS can run natively on the System z hardware, within an LPAR, or on top of the z/VM (Virtual Machine).

One of the components of z/OS is a POSIX-compliant UNIX® implementation called z/OS UNIX (also known as Open MVS (OMVS) and Unix Systems Services). z/OS UNIX runs within z/OS, not as an OS in its own right. This means that it can leverage other z/OS features, such as enhanced security through the External Security Manager feature (RACF® is a common external security manager). It provides UNIX services, such as TCP/IP, to other z/OS components. Some z/OS products cannot work without z/OS UNIX.

z/VSE

z/VSE can be thought of as the little sibling of z/OS. It runs many of the applications (such as DB2® and CICS) as z/OS, but is a smaller OS. It has its heritage in DOS/360 in the 1960s and has gone by the names of DOS/VS, DOS/VSE, VSE/SP, and VSE/ESA before becoming z/VSE.

z/VM

z/Virtual Machine (z/VM) has two basic components: a control program (CP) and a single-user operating system, CMS. As a control program, z/VM is a hypervisor because it runs other operating systems in the virtual machines it creates. Any of the IBM mainframe operating systems such as z/OS, Linux for zSeries, z/VSE, and z/TPF can be run as guest systems in their own virtual machines, and z/VM can run any combination of guest systems.

You can think of it as providing a similar function to VMWare in the distributed world.

Linux on System z

Linux has been available on mainframes since 1999. Unlike z/OS UNIX, which is similar to but often different from other flavors of Linux, the Linux on System z is the same as deployed to other platforms (such as x86).

Like the other operating systems, Linux on System z can run natively (one OS per physical machine), in a logical partition (one OS per LPAR), or on top of z/VM (many OSs per physical
machine or LPAR). Whereas you need a z/OS host for each z/OS UNIX, Linux on System z runs by itself. This means that you could potentially run hundreds or thousands of Linux virtual machines in one physical mainframe. There are many features of the mainframe, such as a high-speed virtual networking capability, that make this an attractive option for large server farms.

Several (non-IBM) Linux distributions can be used on a mainframe. There are two generic names for these distributions:

- Linux for S/390 (uses 31-bit addressing and 32-bit registers)
- Linux for zSeries (uses 64-bit addressing and registers).

Currently z/OS support includes SUSE Linux Enterprise Server 9.0 for Linux on System z 64-Bit kernel and Red Hat Enterprise Linux AS release 4 for Linux on System z 64-bit kernel.

**Putting it all together**

Figure 2 shows an example distributed application deployed on a single System z machine. It is the bookstore example taken from the IBM Redbooks® deliverable *Introduction to the New Mainframe: Security*, SG24-6776.

![Diagram](image)

**Figure 2   Example of multiple operating systems on System z**

This is similar to Figure 1 on page 2, but only has two LPARs: LPAR A is running a z/VM OS and LPAR B is running z/OS. The z/OS system is running an LDAP server (IBM Tivoli Directory Server), which is utilizing z/OS UNIX facilities. It is serving as a central authentication point for the various Linux virtual machines. Connecting the LPARs are HiperSocket connections (which carry TCP/IP traffic for the LDAP connections, amongst others).
In LPAR A, running on z/VM there are some z/VM components, such as DirMaint™ running on CMS and RACF for z/VM. There are also a number of Linux images (or virtual machines), some running applications, some running middleware, and some performing as firewalls. Connecting these virtual machines are three virtual LANs (Guest LAN1, Guest LAN2, and DMZ LAN). The only physical connections into these machines are via Firewall-1 (Internet), Firewall-2 (intranet) and some z/VM and z/OS consoles (appropriately secured). This is very similar to a standard e-business deployment with many machines and a physical network.

For further reading on System z and the various operating systems, see the *Introduction to the new Mainframe* series of IBM Redbooks, specifically *Introduction to the New Mainframe: z/OS Basics*, SG24-6366 and *Introduction to the New Mainframe: Security*, SG24-6776.

**System z and security**

Many people equate mainframe security with RACF. While RACF is certainly the security heart of many mainframe systems in use, it is only one part.

The Resource Access Control Facility (RACF) is one of many External Security Managers (ESMs) that could be used for access control on a System z. Others include CA's ACF2 and TopSecret products. The System z comes with a basic authentication/authorization mechanism that can be used without an ESM. However, some components of z/OS require an ESM to be present (such as z/OS UNIX), and the native security mechanism does not provide the degree of control that current enterprise systems need.

There is a good introduction to RACF that can be found in the *OS/390 Security Server (RACF) Introduction*, GC28-1912-06. It provides a succinct overview of what RACF is, how it works with the OS, and how it ensures security for many of the z/OS products (such as CICS). Note that this document is a few years old (it relates to OS/390 2.10), but the concepts still apply.

There are many more System z security features available, such the hardware-based cryptography services, which are also discussed in the IBM Redbooks deliverable *Introduction to the New Mainframe: Security*, SG24-6776. Another good overview can be found in an IBM Systems Journal article (2001): *Security on z/OS: Comprehensive, current, and flexible* at:


There is another feature of z/OS that often has security implications — the System Management Facility (SMF). This is a central data store with a common data structure that is used by most mainframe applications (like RACF, CICS, and DB2) to write information. This may include usage activity records (audit trail) and performance-related records.

**Directory and data integration on System z**

You may be surprised to know that we have had an LDAP-compliant directory available on the mainframe since 1999. We now have four flavors of the Directory Server:

- One running on Linux on System z in the same way as Tivoli Directory Server does on the other Linux, UNIX, and Windows servers
- One running on z/VM
- Two running on z/OS that can be integrated with RACF.

The distributed product is called IBM Tivoli Directory Server (TDS) for Linux on System z. There are two different and distinct LDAP servers running on z/OS: IBM Tivoli Directory Server for z/OS and the z/OS Integrated Security Services LDAP server. The latest release of z/VM has also introduced an IBM Tivoli Directory Server. We look at each of these separately below.

The other product from the Tivoli Security stable is the IBM Tivoli Directory Integrator product that was written originally for data integration, but now encompasses many forms of data plumbing. It can run on both z/OS and Linux on System z. We look at the ramifications of this below.

**z/OS LDAP directories**

There has been an LDAP directory implementation on System z for many years, dating back to the last versions of OS/390. With z/OS V1R8.0 and z/OS V1R9.0 there are two z/OS LDAP servers shipped:

- The Integrated Security Services LDAP Server (or ISS LDAP) is the heritage z/OS LDAP server, and is no longer being enhanced. It supports multiple backend datastores, such as RACF (called the SDBM) and DB2 (TDBM). This version of the directory is often referred to as just z/OS LDAP.

- The IBM Tivoli Directory Server for z/OS (or Tivoli Directory Server for z/OS) is the newer z/OS LDAP server. It was introduced in March 2007, and new enhancements will go into this product going forward. It contains many of the features of ISS LDAP, but it provides an enhanced set of backend datastores and other functionality enhancements.

Both versions are shipped with z/OS V1R8.0 and V1R9.0 to help customers migrate to the newer Tivoli Directory Server for z/OS. Note that both of these products are different from the Tivoli Directory Server that runs on Linux on System z.

**Integrated Security Services LDAP on z/OS**

The ISS LDAP (or z/OS LDAP) is the z/OS v1R6.0 version. There is a co-existence PTF required to run it on z/OS V1R8.
Figure 3 shows the key components of the ISS LDAP.

Like a distributed directory, there is the central LDAP process: the slapd daemon. It is implemented as a z/OS started task but uses z/OS UNIX supplied functions, such as the TCP/IP stack. It supports any LDAP V2 or V3 client, and ships its own client that runs in z/OS UNIX (and can communicate with any V2 or V3 compliant LDAP server).

Unlike the distributed Tivoli Directory Server, ISS LDAP supports multiple backend datastores:

- **TDBM**: general purpose directory
  - Full LDAP V3 support, including modifiable schema
  - Data stored in DB2 database
  - Full scalability

- **SDBM**: RACF users, groups, and user-group connections
  - Provides remote RACF administration and authentication
  - Fixed schema
  - Data stored in RACF database
  - Limited search capability

- **GDBM**: Change log directory
  - Similar to TDBM (DB2 based) but restricted operations
  - Contains records of changes to other backends and RACF

**Note**: LDAP Version 2 is formally defined in Internet Engineering Task Force (IETF) Request for Comments (RFC) 1777. LDAP Version 3 is formally defined in IETF RFC 2251. You can view these RFCs at:

http://www.ietf.org

Like the distributed version, it supports SSL connections (through the use of certificates and keys) and has the usual configuration files (such as the slapd.conf file).
Note that there are different schemas for the different backend datastores, particularly the RACF (SDBM) backend, which is specific to the RACF users, groups, and user-group connections.

The TDBM datastore is similar to the RDBM (DB2) datastore in the distributed Tivoli Directory Server product (but with a different internal data structure).

**IBM Tivoli Directory Server on z/OS**

Tivoli Directory Server for z/OS was introduced in March 2007 and is supported on z/OS V1R8 and V1R9. It runs in either 31-bit or 64-bit mode (only 31-bit if using DB2-based backends).

One key change for this product over the older z/OS LDAP is that the disparate schemas used by the different backend datastores have been combined into a single server-wide schema.

Figure 4 shows the key components of the Tivoli Directory Server for z/OS product.

Figure 4  Tivoli Directory Server for z/OS components

Most of the components are the same. The following changes have been made:

- The configuration files have had name changes.
- The schema is now held in a single z/OS UNIX file, rather than with each of the backend datastores. It lives under cn=schema in the directory.
- The backend datastores supported have changed:
  - The GDBM (Changelog directory) can now be DB2 or z/OS UNIX files.
  - A new backend (LDBM) has been introduced that uses z/OS UNIX files (zFS or HFS) as the datastore.
- Native authentication can be done from both TDBM and the new LDBM.
- Changes to the API used to access the RACF (SDBM) datastore.
Other than these differences, the functionality provided by z/OS ISS LDAP and Tivoli Directory Server for z/OS are basically the same.

**Common features to z/OS ISS LDAP and Tivoli Directory Server for z/OS**

This section lists some of the common features of both the z/OS ISS LDAP and Tivoli Directory Server for z/OS. The term z/OS LDAP is used to refer to both z/OS ISS LDAP and Tivoli Directory Server for z/OS.

**Administration and authentication methods**

RACF provides a highly secure and read-optimized database (RACF registry), somewhat like Tivoli Access Manager has with its policy database, which is great for storing passwords. Using RACF as the password store reduces the need to synchronize passwords between RACF (for z/OS user authentication) and LDAP (for distributed user authentication).

Use of different backend datastores means that different methods can be used to maintain and access user data:

- **With only RACF** (SDBM) deployed as a backend datastore, RACF data (users, groups, and user-group connections) can be maintained using LDAP commands and utilities. Authentication can be performed using an LDAP bind against the RACF user and password, meaning that distributed systems (such as Web servers and other LDAP clients) can authenticate against RACF without having to duplicate the RACF data to other repositories as long as the distributed account is the same as the RACF user ID.

- **With only DB2/File** (TDBM or LDBM) deployed as a backend datastore, z/OS LDAP operates like any other (distributed) LDAP with users, groups, and other objects managed through LDAP commands and utilities. Manual synchronization of RACF data with z/OS LDAP would be required if there was to be authentication against the RACF data. Otherwise, authentication would be against the LDAP person entries and their userPassword attributes.

- **With both RACF and DB2/File** backends, you get two sets of independent data, but both are accessible (for example, maintainable) via LDAP commands and utilities. You may do this if you want to maintain two discrete sets of user populations through the same tools and authenticate using the same mechanisms. For example, you may have an e-business application that is used by staff and external customers. Assuming that the staff members already have RACF accounts, there is no benefit in replicating their data across to the TDBM/LDBM, but you may also have hundreds of thousands, or even millions, of customers that have no need for a RACF account, so it makes sense to leave them in the TDBM/LDBM. Maintaining separate LDAP suffixes (a TDBM/LDBM suffix for the external customer accounts and a SDBM suffix for the internal RACF users) would be appropriate in this example.

- **With only DB2/File** (TDBM/LDBM) deployed as a backend store, but Native Authentication configured, all RACF users (who need LDAP authentication) have a TDBM entry that links them to their RACF account. When there is an LDAP bind against the TDBM distinguished name (dn) with their RACF password, z/OS LDAP uses a RACF API to authenticate the user against RACF.

- **With both RACF and DB2/File** backends and Native Authentication configured, you get the best of both previous models — a single password (RACF) when it is needed and the ability to maintain all entries through LDAP commands and utilities.

Note that there is a limitation to the number of RACF records returned via LDAP. Be wary of using the LDAP interface for searches that could return a large results set.
Figure 5 shows an example of the native authentication model.

Here the user is authenticating using jayb (data residing in the TDBM datastore) and their RACF password. The bind to LDAP uses the LDAP dn (for example, the reference to the entry in the TDBM, which is the only datastore mapped to LDAP). When the LDAP server performs a lookup of the entry in its datastore (TDBM), it finds that it is marked for native authentication. It retrieves the RACF ID (ibm-nativeId attribute on the person object) and uses this, and the passed password, to authenticate them as U12345 using native authentication to RACF.

**z/OS LDAP as central authentication repository**

A common use for the z/OS LDAP is to provide a single centralized repository for user authentication data. If you are running many Linux on System z images, it makes sense to centralize the user accounts to simplify administration and have consistent auditing. In this model, the Linux on System z systems use the Pluggable Authentication Modules (PAM), Name Service Switch (NSS), and LDAP communications protocol to authenticate users back to the central z/OS LDAP. As standard LDAP is being used over TCP/IP, this authentication framework could include machines outside of the System z (for example, other Linux and UNIX systems in the network). This centralized authentication repository model of z/OS LDAP is no different from a distributed LDAP directory doing the same thing.
Figure 6 shows this centralized authentication model with both the WebSphere® Application Server running on Linux on System z and login authentication on Linux on System z making use of a central z/OS LDAP for user authentication.

Figure 6   z/OS LDAP for centralized authentication

In this example there are three sets of client authentication:

- There are some Linux on System z images running on a z/VM and hosting WebSphere Application Server and some Java™ applications. When a user accesses one of these applications (via http/https from their browser), WebSphere Application Server uses the LDAP client to authenticate the user against the z/OS LDAP server.

- Some other Linux on System z images running on z/VM are configured to pass all login authentication attempts up to the central z/OS LDAP server. They have the Pluggable Authentication Modules and NSS configured to use the LDAP client on the Linux on System z image to do that.

- Some client applications on distributed machines are also configured to use the z/OS LDAP server as a central authentication server. These client applications use a local LDAP (V2 or V3) client to communicate with the z/OS LDAP server.

In all cases, the LDAP client-to-server communication can be via clear-text or SSL communication.

The LDAP authentication (bind) may be using native authentication (as described above) or normal authentication (where the password is held as an attribute in the person object).

Some additional information about this topic can be found in the developerWorks® article Authenticate SLES9 Linux clients using RACF and LDAP on z/OS²; the IBM Redpaper Linux on IBM zSeries and S/390: Securing Linux for zSeries with a Central z/OS LDAP Server (RACF), REDP-0221³; and the product manual z/OSIntegrated Security Services LDAP Server Administration and Use, SC24-5923-07⁴.

³ This publication is located at http://www.redbooks.ibm.com/abstracts/REDP0221.html?Open.
**RACF changelog mechanism**

With RACF defined as a backend datastore (SDBM) for LDAP, you can use the LDAP changelog mechanism to identify changes to RACF users and passwords. The changelog mechanism is implemented in DB2 (or z/OS UNIX files) and is referred to as the GDBM. Using SDBM, you can retrieve the RACF password envelope for a RACF user (this implies that the password envelope mechanism must be enabled in RACF). These functions (changelog and password envelope) were introduced with z/OS 1.3.

The LDAP changelog and RACF password envelope mechanisms could be combined with IBM Tivoli Directory Integrator to trigger password change cascading (synchronization). Tivoli Directory Integrator has a z/OS LDAP Password Change connector specifically for this purpose.

An interesting presentation from 2004 on the topic *RACF/LDAP Event Notification And Password Enveloping* is located at the following location:


Some of the minor details of this may have changed, but the overall mechanism is the same.

**IBM Tivoli Directory Server for z/VM**

The latest release of z/VM, V5R3, ships the ported version of the z/OS IBM Tivoli Directory Server (both client and server). It is a component of TCP/IP in z/VM and uses z/VM OpenExtensions and BFS files. It supports LDBM, GDBM, SDBM, and ICTX backends like its z/OS counterpart. It also supports native authentication and replication.

Details can be found in Chapter 3 of the IBM Redbook *Security on z/VM, SG24-7471-00*⁵. See also the z/VM V5R3.0 TCP/IP LDAP Administration Guide and the z/VM V5R3.0 TCP/IP Planning and Customization manuals⁶.

**IBM Tivoli Directory Server on Linux for System z**

The Tivoli Directory Server for Linux on System z is based on the same implementation as the other Linux/UNIX implementations. It uses DB2 UDB as the backend data store.

It can be used as an authentication source for the Linux on System z image (as with the Tivoli Directory Server on z/OS above). It can also be used as a traditional directory used by products such as Tivoli Identity Manager and Tivoli Access Manager for e-business or providing other directory services.

---

⁵ This publication is located at [http://www.redbooks.ibm.com/abstracts/sg247471.html](http://www.redbooks.ibm.com/abstracts/sg247471.html).
⁶ These publications are located at [http://publibz.boulder.ibm.com/cgi-bin/bookmgr_OS390/SHELVES/HCSHZ81](http://publibz.boulder.ibm.com/cgi-bin/bookmgr_OS390/SHELVES/HCSHZ81).
Platform support (as at Tivoli Directory Server 6.1 GA) is:

- **zSeries Linux (31-bit) operating system version - only 32-bit client supported:**
  - Red Hat Enterprise Linux 4 and 5
  - SuSE Linux Enterprise Server 9 and 10

- **zSeries Linux (64-bit) operating system version - 64-bit directory server components:**
  - Client, Server, and Web Administration Tool. 32-bit directory server components: Client only:
  - Red Hat Enterprise Linux 4 and 5
  - SuSE Linux Enterprise Server 9 and 10

**Note:** There is a limitation with the 31-bit Tivoli Directory 6.0 server components running on a 64-bit zSeries Linux system (such as SLES9 and RHEL4) — the TDS server must communicate with a 31-bit DB2 client, the DB2 client and server must (by design) run on the same server and be both 31-bit or 64-bit, but there is no 31-bit DB2 server. This means that it is not possible to run ITDS 6.0 (31-bit) and the required DB2 components on the same server. There is a technote that describes a workaround to use a remote 64-bit DB2 server running on another zSeries Linux system at:

http://www-1.ibm.com/support/docview.wss?uid=swg21230193

---

**IBM Tivoli Directory Integrator**

In the context of this paper, we can run Tivoli Directory Integrator on a number of operating systems on a System z machine, and we can manage various data types (including z/OS TSO commands) through Tivoli Directory Integrator.

**Tivoli Directory Integrator running on System z**

The Tivoli Directory Integrator server (ibmdisrv) can run in z/OS UNIX in a z/OS system. There are some specific requirements, such as JVM™ 1.5 (for more details see the product documentation). The System Store (using Cloudscape™, or configured to use DB2) is also supported on z/OS.

The Config Editor and AMC are not supported natively on z/OS. Instead, you should use remote management options, like:

- **The Remote Config Editor.** Run the Config Editor on a supported platform, and access Config files on z/OS using a configured Config Instance on z/OS.
- **The Administration and Monitor Console,** which is a Web-based application.
- **Applications** that use the remote Tivoli Directory Integrator Server API.

See below for connectors supported on z/OS.

Tivoli Directory Integrator running on Linux on System z acts the same as for other Linux on distributed platforms. There is no special System z functionality provided.
Table 1 shows the platform support for Tivoli Directory Integrator 6.1.

**Table 1 Platform support for Tivoli Directory Integrator 6.1**

<table>
<thead>
<tr>
<th>OS</th>
<th>Platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>z/OS</td>
<td>Tivoli Directory Integrator 6.1 runs on S/390 and zSeries, z/OS V1.6, z/OS V1.7</td>
</tr>
<tr>
<td></td>
<td>Note: The IBM Tivoli Directory Integrator Server runs in 31-bit tolerance mode. Tivoli Directory Integrator only supports the 31-bit IBM JRE™ 5.0.</td>
</tr>
<tr>
<td>Linux on System z</td>
<td>Tivoli Directory Integrator 6.1 runs on Linux S/390 and zSeries; RedHat Enterprise Linux ES/AS 3.0 (31bit supported), RedHat Enterprise Linux ES/AS 4.0 (64-bit supported), SLES 9 (64-bit supported), and SLES 10 (64-bit supported).</td>
</tr>
<tr>
<td></td>
<td>Note: The IBM Tivoli Directory Integrator Server and Config Editor run in 32-bit tolerance mode on all 64-bit operating systems. This is because Tivoli Directory Integrator ships and uses a 32-bit JRE. On native z/OS and zSeries Linux operating systems, the Tivoli Directory Integrator Server and Config Editor run in 31-bit tolerance.</td>
</tr>
</tbody>
</table>

**Tivoli Directory Integrator working with System z data**

The full list of connectors supported on z/OS can be found in “Chapter 15 z/OS environment support” in the IBM Tivoli Directory Integrator 6.1.1: Administrator Guide, SC32-2567-01. Of special note are the following facts:

- The **z/OS TSO Command Line Function Component** (z/OS TSO/E Command Line FC) is of particular relevance for the z/OS environment. It is able to execute privileged z/OS TSO commands. This component addresses the need to manage RACF, TopSecret, and ACF2 users. This can be achieved by executing TSO commands. Architecturally, this FC consists of a Java layer, a UNIX System Services shared library, and a REXX™ script component. The Java layer passes the command to the shared library, the shared library passes it to the REXX script through APPC, and the REXX script executes the TSO/E command and passes back the result.

- The **zOS Changelog Connector** that is used to access the z/OS LDAP changelog for password synchronization and event notification, as mentioned in the Tivoli Directory Server section above.

The connectors supported with the Linux on System z implementation of Tivoli Directory Integrator are the same as supported on the distributed Tivoli Directory Integrator implementations and do not have z/OS-specific functionality.

**Identity and access management products**

Identity and access management products, particularly the IBM Tivoli Identity Manager and IBM Tivoli Access Manager products, have been the core of Tivoli Security implementations for a number of years now. This year has seen the acquisition of Consul, bringing a new suite
of mainframe administration products to the fold, along with a number of risk and compliance products.

**IBM Tivoli Identity Manager**

Tivoli Identity Manager is our premier identity management product, providing centralized role-based account provisioning for over seventy platforms. For many years Tivoli Identity Manager has been able to manage accounts on mainframes, but we have just recently announced support for Tivoli Identity Manager running on Linux for System z and on z/OS.

**Tivoli Identity Manager running on System z (Linux)**

In August 2007 IBM Tivoli announced support for Tivoli Identity Manager 4.6 running on Linux for System z\(^7\). This includes the entire software stack: WebSphere Application Server, IBM Tivoli Directory Server, and DB2. This is similar to other products running on Linux on System z — they do not have any mainframe-specific features, it just allows customers to make use of the virtualization capabilities of the mainframe by hosting many Linux instances in one large server.

As of August 2007, Tivoli Identity Manager 4.6 System z support is as follows:

- SUSE Linux Enterprise Server 9.0 for Linux for System z 64-Bit Kernel (support as 31-bit implementation)
- Red Hat Enterprise Linux AS release 4 for Linux for System z 64-bit kernel (support as 31-bit implementation)

Tivoli Identity Manager can run on z/OS, but this is provided in a separate product — Tivoli Identity Manager for z/OS (see below).

**Tivoli Identity Manager managing System z security resources**

When talking about managing System z security resources, we are concerned with accounts, passwords, attributes, and group memberships. These normally reside in an External Security Manager (ESM) such as RACF, CA's ACF2, or CA's TopSecret.

We provide an out-of-the-box adapter for RACF in Tivoli Identity Manager 4.6. The current release of the adapter (4.6.4, Dec 2006) supports zOS 1.8. The adapter consists of two components: the DAML adapter that runs in z/OS UNIX, and a command processor started task that runs in z/OS. Figure 7 shows these components and where they reside.

Figure 7  Tivoli Identity Manager 4.6 RACF adapter components

The adapter comes with very detailed documentation, including a 140-page adapter Installation and Configuration guide. The adapter also ships with a reverse password synch module for RACF that relies on the z/OS LDAP RACF changelog discussed previously.

With Tivoli Identity Manager 4.5.1 there were agents to provision to CA ACF2 and TopSecret. These old ftp-based agents are no longer supported. Currently, there are no Tivoli Identity Manager 4.6 adapters available for CA ACF2 or TopSecret. If one is required, we recommend using Tivoli Director Integrator (either DSMLv2 or RMI) and using the z/OS TSO/E Command Line Function Component to perform the relevant administrative functions.

One of the key implementation concerns with Tivoli Identity Manager is the integration with an authoritative source for employee information, such as the HR system. If the HR system is running on a mainframe, Tivoli Director Integrator could be used to build the HR feed. This depends on how the HR system can be accessed, but Tivoli Director Integrator provides a lot of flexibility, such as running on a distributed system (and using TCP/IP-based access protocols), running on Linux on System z, or running on z/OS. If none of the standard connectors can be used, the z/OS TSO/E Command Line Function Component could be used for command-line access to the system.

IBM Tivoli Identity Manager for z/OS

Tivoli Identity Manager for z/OS was announced late in 2006. Unlike the distributed product that has been ported to Linux on System z (see above), this version runs completely on z/OS (with components in z/OS and z/OS UNIX). It uses z/OS LDAP, WebSphere Application Server for z/OS, and DB2 on z/OS. Functionally it is the same as the distributed product.

At general availability it supported z/OS 1.7 and certain levels of WebSphere Application Server, LDAP, and DB2. See the program directory document for more detailed information about the supported product versions. The product documentation can be located on the Tivoli Information Center Web site.

---

IBM Tivoli Access Manager for e-business

When discussing IBM Tivoli Access Manager for e-business, we are usually referring to two major components: the Tivoli Access Manager base (the central policy server, database, and user registry) and the Web policy enforcement engine (WebSEAL). Both of these components can run on Linux for System z, but not on z/OS.

WebSEAL also provides authentication and authorization services for Web applications running on mainframes, whether they be on Linux on System z, z/OS, or any other mainframe http server. One benefit of this is that it does not force the use of a logical partition (LPAR) to be in the demilitarized zone.

Tivoli Access Manager for e-business running on System z

The Tivoli Access Manager for e-business base component can run on Linux for System z. It cannot run on z/OS. It can use a Tivoli Directory Server user registry on a distributed machine, one running on a Linux on System z instance, or the z/OS LDAP.

Note: Tivoli Access Manager for e-business 6.0 base component, and thus Tivoli Access Manager for Operating Systems 6.0, only supports the z/OS Integrated Security Server (ISS) LDAP Releases 4, 5, and 6. It does not support the Tivoli Directory Server on z/OS. Support for Tivoli Directory Server on z/OS is expected in future releases of Tivoli Access Manager for e-business base.

As of fix pack 9 for Tivoli Access Manager for e-business 6.0 base, the following Linux on System z versions are supported (64-bit kernels in 32-bit compatibility mode):

- Red Hat Enterprise Linux Server 3.0 (zSeries) - Update 4
- Red Hat Enterprise Linux Server 4.0 (zSeries) - Update 1 with some compat rpms
- SUSE Linux Enterprise Server 8 (zSeries) - Service Pack 4
- SUSE Linux Enterprise Server 9 (zSeries) - Service Pack 1 or Service Pack 2
- SUSE Linux Enterprise Server 10 on zSeries - (PDRTE, PDMgr, PDAcld, and PDJRTE components, at Tivoli Access Manager fix pack 5 or later)

The Common Audit and Reporting Service (CARS) can also run on Linux for System z:

- Red Hat Enterprise Linux Advanced Server Version 4 with Update 3 or Update 4 (64-bit kernel support only)
- SUSE Linux Enterprise Server, Version 9 with SP3 (64-bit kernel support only)

The Tivoli Access Manager for e-business WebSEAL component can run on Linux for System z. It cannot run on z/OS. As of fix pack 9 for Tivoli Access Manager for e-business 6.0 WebSEAL, the following Linux on System z versions are supported (64-bit kernels in 32-bit compatibility mode):

- Red Hat Enterprise Linux Server 3.0 (zSeries) - Update 4
- Red Hat Enterprise Linux Server 4.0 (zSeries) - Update 1 with some compat rpms
- SUSE Linux Enterprise Server 8 (zSeries) - Service Pack 4
- SUSE Linux Enterprise Server 9 (zSeries) - Service Pack 1 or Service Pack 2

9 This information is located at http://publib.boulder.ibm.com/tividd/td/IBMTivoliIdentityManagerforzOS4.6.html
**Tivoli Access Manager for e-business securing System z access**

WebSEAL provides its usual Web application authentication and authorization services irrespective of where the http traffic is being served from (including Linux on System z and z/OS http and application servers).

z/OS platform support also includes administration and authorization APIs in Java and the Access Manager plug-in for WebSphere Application Server for z/OS allowing container-level security for z/OS servlets.

**Tivoli Access Manager and WebSphere Application Server on System z**

WebSphere Application Server (WAS) supports single sign-on from WebSEAL (and other perimeter authentication services) through trust associations. The Trust Association Interceptor (TAI) is a WAS pluggable module to handle the trust association. Tivoli Access Manager for e-business ships a TAI module called the **TAM Trust Association Interceptor Plus** (TAI++) to provide SSO between WebSEAL and WAS. This function works whether the components (TAMeb and WAS) are running on distributed systems, Linux for System z, or z/OS.

For more details on this implementation see the Tivoli Access Manager Trust Association Interceptor developerWorks article[^10].

---

**IBM Tivoli Access Manager for Operating Systems**

Tivoli Access Manager for Operating Systems performs the same functions in a Linux on System z environment as it does in the distributed world — enhanced OS-level security. Unlike z/OS UNIX where the underlying z/OS Enterprise System Manager (ESM) can enhance the native UNIX security, the Linux on System z requires additional security software to strengthen Linux. Tivoli Access Manager for Operating Systems provides that function.

Tivoli Access Manager for Operating Systems runs on Linux on System z only. It does not run on z/OS UNIX.

The supported Linux on System z systems for Tivoli Access Manager for Operating Systems 6.0 fix pack 7 are:

- Red Hat Enterprise Linux Server 3.0
- Red Hat Enterprise Linux Server 4.0
- United Linux 1.0
- SUSE LINUX Enterprise Server 9
- SUSE LINUX Enterprise Server 10

See the readme file that comes with the product documentation for details of 31-bit and 64-bit support.

Tivoli Access Manager for Operating Systems also uses the **Tivoli Access Manager Base**. See above for platform support.

---

**IBM Tivoli Access Manager for Business Integration**

Like some of the other Tivoli Security products, there are two versions of IBM Tivoli Access Manager for Business Integration — one for distributed systems (often referred to as **TAMBI**)

[^10]: This publication is located at http://www.ibm.com/developerworks/tivoli/library/t-tamtai.
and one for zOS, or host-based, systems (often referred to as Tivoli Access Manager for Business Integration Host Edition).

IBM has announced end of support\(^{11}\) for the Tivoli Access Manager for Business Integration product set as of April 30, 2008. However, if customers are licensed for WebSphere MQ Extended Security Edition (which comes with Tivoli Access Manager for Business Integration 5.1.1) or WebSphere MQ Extended Security Edition for z/OS (which ships with Tivoli Access Manager for Business Integration Host Edition 4.1.1), then the Tivoli Access Manager for Business Integration components are supported until WebSphere MQ Extended Security Edition is withdrawn from support sometime in the future.

**Tivoli Access Manager for Business Integration (distributed)**
The current version of Tivoli Access Manager for Business Integration runs on Linux for System z in the same way in which it runs on other Windows/UNIX/Linux systems.

According to the Tivoli Access Manager for Business Integration 5.1 fix pack 5 readme file\(^{12}\), only WebSphere MQ 6.0 is supported on System z with:

- SuSE Linux Enterprise Server (SLES) 8 for zSeries (31-bit)
- SuSE Linux Enterprise Server (SLES) 9 for zSeries (31-bit)
- SuSE Linux Enterprise Server (SLES) 9 for zSeries (64-bit)
- Red Hat Enterprise Linux (RHEL) 3.0 for zSeries (31-bit)
- Red Hat Enterprise Linux (RHEL) 4.0 for zSeries (31-bit)
- Red Hat Enterprise Linux (RHEL) 4.0 for zSeries (64-bit)

**Tivoli Access Manager for Business Integration Host Edition**
The Tivoli Access Manager for Business Integration Host Edition is on back-level version 4.1.1. It was tested on z/OS V1R4 and V1R6 and is supported with the current release of z/OS (V1R9). The documentation for this product can be found in the z/OS V1R9.0 Library Center (the documentation is for 4.1.0, but applies to the current version). Tivoli Access Manager for Business Integration Host Edition 4.1.1 requires a distributed policy server (Tivoli Access Manager 5.1 or 6.0), which may be running on Linux on System z (but not z/OS). It is also dependant on:

- IBM Policy Director Authorization Services for z/OS and OS/390 (contains a z/OS version of pdacl)
- z/OS Security Server LDAP Server (now Tivoli Directory Server for z/OS)
- z/OS Security Server RACF (or an equivalent product)
- z/OS System Secure Sockets Layer (SSL)

**IBM Tivoli Federated Identity Manager, Tivoli Federated Identity Manager for z/OS, and Tivoli Federated Identity Manager Business Gateway**

IBM Tivoli Federated Identity Manager is the IBM implementation of the federated trust communications between various parties using industry standards such as SAML, Liberty, WS-Federation, and WS-Trust. It integrates with IBM Tivoli Access Manager for e-business for the HTTP-based federation protocols and WebSphere Application Server for the Web Services-based protocols.

---


\(^{12}\) This document can be found at [http://www3.software.ibm.com/ibmdl/pub/software/tivoli_support/patches/patches_5.1.0/5.1.0-TIV-TAMBI-FP0005/5.1.0-TIV-TAMBI-FP0005.README](http://www3.software.ibm.com/ibmdl/pub/software/tivoli_support/patches/patches_5.1.0/5.1.0-TIV-TAMBI-FP0005/5.1.0-TIV-TAMBI-FP0005.README).
The Tivoli Federated Identity Manager Business Gateway is a version of the Tivoli Federated Identity Manager for clients that are not running Tivoli Access Manager for e-business, and therefore only need a reduced set of functionalities.

Both Tivoli Federated Identity Manager and Tivoli Federated Identity Manager Business Gateway at their current releases (6.1.1) are supported on Linux for System z:

- Red Hat Enterprise Linux Advanced Server Version 4 with Update 3 or Update 4 (64-bit kernel support only)
- SUSE Linux Enterprise Server, Version 9 with SP3 (64-bit kernel support only)

As with the other products, this implementation is effectively the same as on distributed Linux systems.

Tivoli Federated Identity Manager is also supported on z/OS, but with limited functionality:

- The runtime and management service component, the Web services security management (WSSM) component, and the management console are supported on z/OS Version 1 Release 6, z/OS Version 1 Release 7, and z/OS Version 1 Release 8.
- The provisioning components, federated single sign-on, and the Common Auditing and Reporting Service are not supported on z/OS.

This version is titled *IBM Tivoli Federated Identity Manager for z/OS*.

**IBM Tivoli zSecure administration products**

With the acquisition of the company Consul, IBM has inherited the zSecure suite of products that perform both administration and auditing of mainframe external security managers, such as RACF.

The zSecure administrative products consist of zSecure Admin, zSecure Visual, and zSecure CICS Toolkit. These three products only apply to RACF.

Most of these products, and the rest of the zSecure suite, reside completely within z/OS.

Figure 8 shows the core components of the zSecure suite.

---

![Figure 8  zSecure suite components](image)
The products all share common components, including the CARLA programming language. The admin products are:

- IBM Tivoli zSecure Admin consists of an ISPF-based user interface for the administration of RACF attributes. It runs entirely within z/OS. There is no z/OS UNIX or Linux on System z component to the product.
- IBM Tivoli zSecure Visual consists of a Windows-based user interface running on a windows machine. It communicates with a started task that uses CKRCARLA to perform administration.
- IBM Tivoli zSecure CICS Toolkit has two facets. It is a pre-built administrative interface that runs as a CICS transaction in a CICS region. It also provides a CICS API to allow applications to perform their own security functions. For example, if an application needed a re-verification of user credentials when certain program constraints were met (such as funds transfer over a certain amount) the CICS Toolkit API could be used to drive this re-verification.

The zSecure Command Verifier product, previously known as zLock, is often listed as an audit or policy compliance tool. However, it can be a very effective delegated/distributed administration control mechanism. It allows profiles to be defined to limit the RACF command arguments that can be specified, including filters on values. For example, you could define a profile to restrict who could perform administration on users beginning with STC. This product runs completely within a z/OS system. As it is using an exit, it captures all administrative commands, whether they are done through a command line, a job, or an administrative tool.

IBM Tivoli Security Administrator for RACF

IBM Tivoli Security Administrator for RACF pre-dates the acquisition of Consul, and has been withdrawn from marketing. It should not be confused with zSecure Admin, zSecure Visual, or any of the other zSecure products, although there is a crossover of functionality of the two product sets.

Risk and compliance products

Risk and compliance products are not new to the Tivoli Security portfolio. One could argue that even the original Tivoli User Administration and Tivoli Security Management products were enforcing corporate security policy on to distributed systems. Tivoli Risk Manager was one of the first enterprise-wide exposure gathering and reporting tools. The recent acquisition of NetCool and Consul has significantly strengthened IBM capabilities in the risk, governance, compliance, and auditing arenas.

Tivoli Security Compliance Manager

The main functions of Tivoli Security Compliance Manager are to define a security baseline configuration of a system, to periodically check compliance with the baseline, and to report on discrepancies. Unlike most of the Tivoli security products, the server component of Tivoli Security Compliance Manager cannot run on Linux on System z. Only the client is supported, allowing it to monitor a Linux on System z system for policy compliance.
Tivoli Security Compliance Manager running on System z
The Tivoli Security Compliance Manager 5.1 client can run on a number of Linux for System z (5.1.1 fixpack 7):

- Red Hat Linux Advanced Server for zSeries 3.0
- SUSE Linux Enterprise Server for zSeries 8 and 9

The server and other components must run on distributed systems. There is no support for z/OS or z/OS UNIX.

Tivoli Security Compliance Manager monitoring System z policy compliance
For all intents and purposes, the Linux on System z system is the same as other Linux systems. The collectors that can be deployed to the Linux on System z systems are the same as for the other Linux systems.

Tivoli Security Operations Manager
The Tivoli Security Operations Manager is all about collecting real-time information, correlating the data with a view to finding policy violations or intrusion attempts, and reporting this. It is part of a security information and event management (SIEM) platform. Rather than having agents distributed to get the data, it acts as a central collection service and other components route data to it, such as from UNIX syslogs or intrusion detection software.

Tivoli Security Operations Manager running on System z
Tivoli Security Operations Manager does not run on Linux on System z or z/OS. The server and aggregation modules are only supported on RedHat (x86) and Solaris™ 9. The Universal Collection Module (UCM) will not run in a Linux on System z environment.

Tivoli Security Operations Manager gathering System z security-related data
While it does not have any component residing on System z, Tivoli Security Operations Manager could receive data from a Linux on System z system in the same way that it can from other Linux/UNIX systems. It uses conduits to receive SMTP messages, SNMP traps, and syslog data.

Tivoli Compliance Insight Manager
Tivoli Compliance Insight Manager reflects the recently acquired Consul Insight product. It is also part of the security information and event management (SIEM) system together with Tivoli Security Operations Manager, but it focuses on compliance functions related to people and system and data access.

It ships with a number of compliance modules for regulations such as HIPAA and SOX. Tivoli Security Operations Manager is focussed on real-time correlation and operations management, while Tivoli Compliance Insight Manager is more focussed on compliance and audit. In fact, Tivoli Security Operations Manager can be a data feed into Tivoli Compliance Insight Manager.
**Tivoli Compliance Insight Manager running on System z**

None of the Tivoli Compliance Insight Manager components run on Linux on System z or z/OS. However, syslog data from Linux on System z can be sent to an Actuator that receives syslog data.

The *Tivoli Compliance Insight Manager z/OS Actuator* (z/OS Agent for Insight) runs on z/OS, with some components (started tasks and data sets) residing in native z/OS and some components residing in z/OS UNIX.

**Tivoli Compliance Insight Manager gathering System z security-related data**

Tivoli Compliance Insight Manager has auditing capability for z/OS audit data.

It uses the event data that is created through normal SMF processing. It copies this data to a file that is stored in z/OS UNIX Services and then passes the data to the Tivoli Compliance Insight Manager. It can capture and process z/OS (including z/OS UNIX), RACF, ACF2, TopSecret, and DB2 SMF data. It can also process zSecure Alert events.

**Tivoli zSecure audit products**

The second half of the zSecure suite products is related to audit and compliance functions, *zSecure Audit, zSecure Alert* and *zSecure Command Verifier*. These three products all run on z/OS and operate on the z/OS security data and commands.

**IBM Tivoli zSecure Audit**

The zSecure Audit product supports RACF as well as ACF2.

zSecure Audit analyzes security data (such as historical SMF data) and security configuration (such as RACF objects and system libraries) to identify and report on any security exposures.

**IBM Tivoli zSecure Alert**

The zSecure Alert product supports both RACF and ACF2. As it gathers events from SMF and the system console it could theoretically gather TopSecret information also. It provides real-time monitoring of intruders, system activity (from a security perspective), and system configuration.

As with zSecure Audit, this product runs within z/OS.
Figure 9 shows the zSecure Alert, Audit, and z/OS Agent for Insight and data flow.

Both zSecure Alert and zSecure Audit can send data to Tivoli Compliance Insight Manager for analysis and reporting. There are also other destinations for report and alert data.

**IBM Tivoli zSecure Command Verifier**

The zSecure Command Verifier, or zLock as it was know previously, is concerned with controlling who can run ESM (such as RACF) administrative commands, and what arguments can be specified for different users. This allows specification of profiles based on command filters. For example, only administrative group XYZ members can create users with an ID starting with SYS* and connected to group ABC. It is a way of implementing policy (perhaps separation of duties).

This product uses a z/OS security exit and runs in z/OS.

**Conclusion**

In the preceding pages we have seen that there are a number of ways that the Tivoli Security products interact with the mainframe:

- Some utilize the Linux on System z platform as though it were just another distributed Linux platform.
- Some provide remote administrative capabilities on data specific to the mainframe.
- Some are written specifically for use on, and of, mainframe data.

Appendix, “Appendix A - summary of Tivoli Security products on System z” on page 25, contains a summary table showing all of the products covered in this article, with their System z platform support, clients (if any), and a summary of the functions provided.
Table 2 summarizes the products, where they can be installed, where the clients can run, and what functions they perform. The table relates to the product versions generally available at the time of writing this paper.

<table>
<thead>
<tr>
<th>Product</th>
<th>Runs on Linux on System z?</th>
<th>Runs on z/OS?</th>
<th>Client (if any)</th>
<th>Client runs on</th>
<th>Notes/summary of function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tivoli Directory Server for z/OS</td>
<td>No</td>
<td>Yes</td>
<td></td>
<td></td>
<td>Can use DB2, RACF, and z/OS UNIX datastores. Has components in z/OS + z/OS UNIX.</td>
</tr>
<tr>
<td>Tivoli Directory Server</td>
<td>Yes</td>
<td>No</td>
<td></td>
<td></td>
<td>Just like any other distributed Tivoli Directory Server.</td>
</tr>
<tr>
<td>Tivoli Directory Integrator</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td></td>
<td>z/OS implementation has some z/OS-specific connectors/function commands.</td>
</tr>
<tr>
<td>Tivoli Identity Manager</td>
<td>Yes</td>
<td>No</td>
<td>Adapter for RACF</td>
<td>z/OS + z/OS UNIX</td>
<td>Provisioning of RACF users and attributes. Includes reverse password synch function.</td>
</tr>
<tr>
<td>Tivoli Identity Manager for z/OS</td>
<td>No</td>
<td>Yes</td>
<td>See Tivoli Identity Manager above</td>
<td></td>
<td>Uses z/OS WAS, DB2, LDAP. Has components in z/OS + z/OS UNIX.</td>
</tr>
<tr>
<td>Tivoli Access Manager for e-business</td>
<td>Yes</td>
<td>No</td>
<td>WebSEAL</td>
<td>Linux on System z</td>
<td>Base component (Policy Server) can run on Linux on System z and use Linux on System z or z/OS LDAP, WebSEAL can secure any http/https traffic; host or distributed.</td>
</tr>
<tr>
<td>Tivoli Access Manager for Operating Systems</td>
<td>Yes</td>
<td>No</td>
<td>Tivoli Access Manager for OS</td>
<td>Linux on System z</td>
<td>Base component (Policy Server) can run on Linux on System z and use Linux on System z or z/OS LDAP, Tivoli Access Manager for Operating Systems is securing Linux on System z resources in the same way as for other Linux/Unix systems.</td>
</tr>
<tr>
<td>Tivoli Access Manager for Business Integration</td>
<td>Yes</td>
<td>No</td>
<td></td>
<td></td>
<td>Currently still supported as part of WebSphere MQ ESE V6 (Tivoli Access Manager for Business Integration 5.1.1).</td>
</tr>
<tr>
<td>Tivoli Access Manager for Business Integration Host Edition</td>
<td>No</td>
<td>Yes</td>
<td></td>
<td></td>
<td>Currently still supported as part of WebSphere MQ ESE for z/OS V6 (Tivoli Access Manager for Business Integration Host Edition 4.1.1).</td>
</tr>
<tr>
<td>Tivoli Federated Identity Manager</td>
<td>Yes</td>
<td>No</td>
<td></td>
<td></td>
<td>All functionality available on Linux on System z.</td>
</tr>
<tr>
<td>Tivoli Federated Identity Manager for z/OS</td>
<td>No</td>
<td>Yes</td>
<td></td>
<td></td>
<td>Limited functionality (WSSM) on z/OS. Has components in z/OS + z/OS UNIX.</td>
</tr>
<tr>
<td>Product</td>
<td>Runs on Linux on System z?</td>
<td>Runs on z/OS?</td>
<td>Client (if any)</td>
<td>Client runs on</td>
<td>Notes/summary of function</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>----------------------------</td>
<td>---------------</td>
<td>-----------------</td>
<td>----------------</td>
<td>-------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Tivoli Federated Identity Manager Business Gateway</td>
<td>Yes</td>
<td>No</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>zSecure Admin</td>
<td>No</td>
<td>Yes</td>
<td></td>
<td></td>
<td>Product runs in z/OS to manage ESM (RACF and so on) objects.</td>
</tr>
<tr>
<td>zSecure Visual</td>
<td>No</td>
<td>Yes</td>
<td>Visual client</td>
<td>Windows</td>
<td>Product runs on Windows workstation but requires core zSecure functionality on z/OS.</td>
</tr>
<tr>
<td>zSecure CICS Toolkit</td>
<td>No</td>
<td>Yes</td>
<td></td>
<td></td>
<td>Product provides both a CICS transaction to perform RACF administration and an API.</td>
</tr>
<tr>
<td>zSecure Audit</td>
<td>No</td>
<td>Yes</td>
<td></td>
<td></td>
<td>Product runs in z/OS to audit ESM (RACF and so on) objects and system settings.</td>
</tr>
<tr>
<td>zSecure Alert</td>
<td>No</td>
<td>Yes</td>
<td></td>
<td></td>
<td>Product runs in z/OS to monitor ESM (RACF and so on) objects and system settings. It sends e-mail, SNMP traps, or issues WTOs to AOC for important security events.</td>
</tr>
<tr>
<td>zSecure Command Verifier</td>
<td>No</td>
<td>Yes</td>
<td></td>
<td></td>
<td>Product runs in z/OS to control ESM (RACF and so on) administration.</td>
</tr>
<tr>
<td>Tivoli Security Compliance Manager</td>
<td>No</td>
<td>No</td>
<td>Tivoli Security Compliance Manager CLI</td>
<td>Linux on System z</td>
<td>Same as for the client functions on other platforms.</td>
</tr>
<tr>
<td>Tivoli Security Operations Manager</td>
<td>No</td>
<td>No</td>
<td></td>
<td></td>
<td>Tivoli Security Operations Manager can receive data sent from z/OS forwarded syslogs, SMTP messages, and SNMP traps.</td>
</tr>
<tr>
<td>Tivoli Compliance Insight Manager</td>
<td>No</td>
<td>No</td>
<td>z/OS Agent for Insight</td>
<td>z/OS + z/OS UNIX</td>
<td>Collects mainframe data for z/OS audit capability.</td>
</tr>
</tbody>
</table>
The team that wrote this IBM Redpaper

This paper was produced by a team of specialists from around the world working at the International Technical Support Organization, Austin Center.

**Axel Buecker** is a Certified Consulting Software IT Specialist at the International Technical Support Organization, Austin Center. He writes extensively and teaches IBM classes worldwide on areas of Software Security Architecture and Network Computing Technologies. He holds a degree in computer science from the University of Bremen, Germany. He has more than 21 years of experience in a variety of areas related to Workstation and Systems Management, Network Computing, and e-business Solutions. Before joining the ITSO in March 2000, Axel worked for IBM in Germany as a Senior IT Specialist in Software Security Architecture.

**David Edwards** is a Consulting IT Specialist within the Tivoli Global Response Team, where his primary focus is the resolution of technical situations relating to the Tivoli Security products. He has twenty years of experience in the IT industry covering areas as diverse as mainframe applications programming, CICS systems programming, distributed systems management, and implementing and supporting the Tivoli Security portfolio. He holds a Bachelor of Science degree from Monash University and a Graduate Diploma of Applied Science (Computer Science) from Swinburne University. David has written numerous technical articles on Tivoli Security products, including contributing to a number of IBM Redbooks deliverables.

Thanks to the following people for their contributions to this project:

Joel Tilton, Joe Carusillo, Ted Ralston, Ram Sreerangam, Geoff Rousell, Michael Cairns, Glen Gooding, Weibo Yuan, Jon Cottrell, Bruce Wells

**IBM US & Australia**
Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user’s responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504-1785 U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.
This document REDP-4355-00 was created or updated on January 28, 2008.

Send us your comments in one of the following ways:

- Use the online Contact us review Redbooks form found at: ibm.com/redbooks
- Send your comments in an email to: redbooks@us.ibm.com
- Mail your comments to:
  IBM Corporation, International Technical Support Organization
  Dept. HYTD Mail Station P099
  2455 South Road
  Poughkeepsie, NY 12601-5400 U.S.A.

Trademarks

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

- Redbooks (logo) ®
- developerWorks®
- eServer™
- z/OS®
- z/VM®
- z/VSE™
- zSeries®
- AIX®
- Cloudscape™
- CICS®
- DirMaint™
- DB2®
- HiperSockets™
- IBM®
- MVS™
- OS/390®
- PR/SM™
- Redbooks®
- RACF®
- REXX™
- S/390®
- System p™
- System z™
- System z9™
- System/360™
- Tivoli®
- VSE/ESA™
- WebSphere®

The following terms are trademarks of other companies:

Java, JRE, JVM, Solaris, and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Windows, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Intel, Intel logo, Intel Inside logo, and Intel Centrino logo are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.