



## Hot Spotlight Articles

*In the Spotlight*

### **TDS: The height of “z” curity!**

BY JONATHAN COTTRELL, SAHEEM GRANADOS, AND RAINER HIMMELSBACH

By choosing IBM System z, many customers have moved their core enterprise systems to the highest security levels. The IBM Tivoli Directory Server (TDS) for z/OS ships as part of the base operating system, and supports many z/OS security and high availability functions like the following:

- **Automatic Restart Management (ARM)**
- **Resource Access Control Facility (RACF)**
- **Workload Management (WLM)**
- **HiperSockets (wireless connection)**
- **File-based and DB2-based sysplex clustering**

This article discusses two new security-related features new to the IBM TDS for z/OS in V1R12. It also provides general information about how to configure the SAP NetWeaver application with the IBM TDS for z/OS.

#### **Tightening the screws**

In z/OS V1R12, the IBM TDS for z/OS introduces features for password policy and access control filter support to give LDAP administrators two powerful tools for even more data security control in the LDAP server.

#### **Password policy support**

What is password policy? Password policy is a set of rules to control how the LDAP server administers and uses passwords. Password policy ensures that users have strong passwords that cannot easily be compromised and are changed periodically. These rules:

- **Restrict the reuse of old passwords,**
- **Lock users out after a defined number of failed bind attempts**
- **Automatically expire passwords after a specified period of time**

#### **Configuring password policy**

Now doesn't having automatic password policy in your LDAP server sound like a great idea? We're certain it does. To configure password policy, we've summarized a few simple updates needed in the LDAP server configuration file:

1. Add the following configuration option to the CDBM backend:

database cdbm GLDBCD31/GLDBCD64

2. Ensure that the serverCompatLevel option is set to 6.

After these two steps are complete, restart the LDAP server. The *cn=pwdpolicy,cn=ibmpolicies* entry is automatically created in the CDBM backend. The *cn=pwdpolicy,cn=ibmpolicies* entry is known as the global password policy entry and applies to all LDBM and TDBM entries that have userPassword attribute values. The global password policy is not activated until you change the *ibm-pwdPolicy* attribute from false to true using an LDAP modify command. Use the *ldapmodify* utility to update the *ibm-pwdPolicy* attribute. For example:

```
ldapmodify -D adminDN -w adminPw -f modPolicy.ldif
```

where *modPolicy.ldif* has the following contents:

```
dn: cn=pwdpolicy,cn=ibmpolicies
changetype: modify
replace: ibm-pwdpolicy
ibm-pwdpolicy: true
```

Here is a summary of changes for password enhancements:

### **Global password policy entry**

The global password policy entry has many attributes that control various aspects of allowed userPassword attribute values in LDBM backend and TDBM backend entries. The password policy attributes give the LDAP administrator many knobs for fine-tuning password policy for the organization. These controls include automatic password expiration, requiring a minimum password length, and locking users after too many failed authentication attempts.

### **Additional password policy entries**

You can define additional password policy entries under the *cn=ibmpolicies* entry in the CDBM backend. These entries can apply to certain individual users or groups that must have a policy differing from the global policy for security reasons to provide even more control.

### **Password policy operational attributes**

For TDBM and LDBM user entries that are subject to password policy, the LDAP administrator can query several operational attributes in the user entries in order to obtain password policy state information such as when the password was last changed and a history of previous password values.

### **PasswordPolicy control**

You can also update LDAP client applications to send the PasswordPolicy control on requests to solicit additional warning and error information from the LDAP server related to password policy enforcement, for example, to find out if the length of the new password is not long enough.

## Access control filter support

Access control filter support is an extension to the standard access control list (ACL). These controls allow more granular permissions to be set for users in the LDAP server and allow permissions to be augmented, reduced, or replaced based on logical combinations of the following attributes:

- **Bind distinguished name (DN),**
- **Alternate DN**
- **Groups that the bind DN or an alternate DN belong to**
- **IP address of the client connection**
- **Time and day of week the entry was accessed**
- **Authentication mechanism**
- **SSL connection status**

You might ask, "Why would anyone want this granularity? Isn't this extra level of granularity too complicated to implement?"

Now consider a mobile workforce. Many times legal and regulatory requirements can require access control to be different depending on the location where a user attempts to access a resource. Alternatively, IT security officers might like to enhance security with additional attributes that the LDAP directory doesn't represent, for instance, time or day of access.

This new extension to the LDAP access control model provides the means and flexibility to security officers so that they have dynamic access control using common LDAP constructs. Enterprises that require different access control given a user's location, time, or even connection type would simply add new `aclEntry` or `entryOwner` attribute values to protected LDAP objects.

### An `aclEntry` example

For example, the supported `aclEntry` and `entryOwner` attribute values have been extended in V1R12 to include new syntaxes. The following is an example of an `aclEntry` value that uses the new filtered `aclEntry` syntax:

```
aclentry: aclFilter: (&(ibm-filterDayOfWeek>=1) (ibm-
filterDayOfWeek<=5)) :union:critical:rwsc:restricted:rwsc
```

You can use this `aclEntry` to augment any matching `aclEntry` values for a user who attempts access on Monday through Friday. The `aclFilter` keyword (ownerFilter for `entryOwner` values) is required for these new filtered values. The string after the keyword `aclFilter: (ibm-filterDayOfWeek>=1) (ibm-`

`filterDayOfWeek<=5)`, is a standard LDAP filter that uses a predefined set of attributes to represent the user's new dynamic attributes (in this case, allow, access Monday through Friday). The keyword `:union:` indicates that TDS is to augment the `aclEntry` values. Finally, the string `critical:rwsc:restricted:rwsc` represents the permissions to augment. Entryowner attribute values have a similar syntax that allows entry ownership to be granted or denied dynamically.

### **Password policy management and access control filter support =more flexible security**

For z/OS V1R12, these new powerful security features of TDS give IT security officials the flexibility to really strengthen the security of an IT enterprise. To help address the many legal and regulatory requirements needed these days to secure your organization, TDS for z/OS 1.12 provides both password policy management and access control filter support with extended operations to allow an administrator to test deployed `aclEntry` and `entryOwner` values.

### **Enable your applications for TDS: The SAP application case**

TDS for z/OS ships as part of the base operating system so it is security virtually for free for SAP customers on IBM System z. You can secure---pardon, secure--- your SAP applications with IBM System z, deploying tools that the acclaimed, highly secure System z platform can offer. Of course, the TDS and the SAP application require some set up and configuration steps.

In our IBM SAP test environment, we successfully completed steps to achieve these application configurations with TDS:

- **Setting up and configuring SAP NetWeaver Application Server Java and SAP NetWeaver Enterprise Portal with the User Management Engine (UME) together with TDS for z/OS.**
- **Setting up and configuring SAP NetWeaver application server ABAP user repository to synchronize with TDS for z/OS.**

Our IBM SAP test environment includes the following hardware and software:  
**IBM System z9 Enterprise Class and two Linux on System z guests that were hosted by z/VM.**

**Two LPARS defined in a sysplex with one that operated as LDAP server and the other as data base server.**

**DB2 9 for z/OS as the data base backend.**

**Network connection that was over a public LAN and included fast HiperSockets for the connection from Linux on System z to z/OS**

See Figure 1.

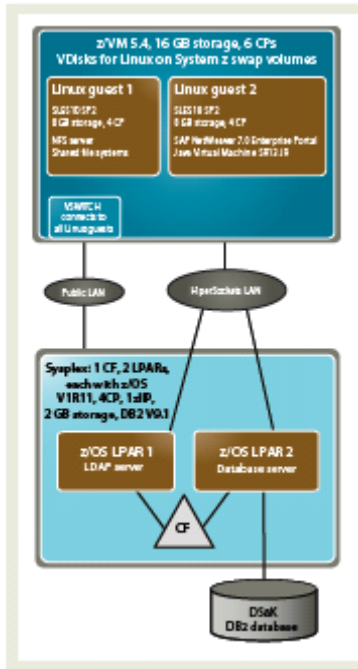


Figure 1. Set up and configuration of SAP NetWeaver Application Server Java application test environment with TDS

### Additional information

For a detailed description of the implementation of these configurations, see “SAP and IBM Tivoli Directory Server for z /OS” available on the following SAP Website:

[www.sdn.sap.com/irj/scn/index?rid=/library/uuid/b0822a13-1a25-2d10-4394-b9fc12b41733](http://www.sdn.sap.com/irj/scn/index?rid=/library/uuid/b0822a13-1a25-2d10-4394-b9fc12b41733)

For information about password policy and filtered ACL support, see *IBM Tivoli Directory Server Administration and Use for z/OS V1R12.0*, SC23-5191-05.

