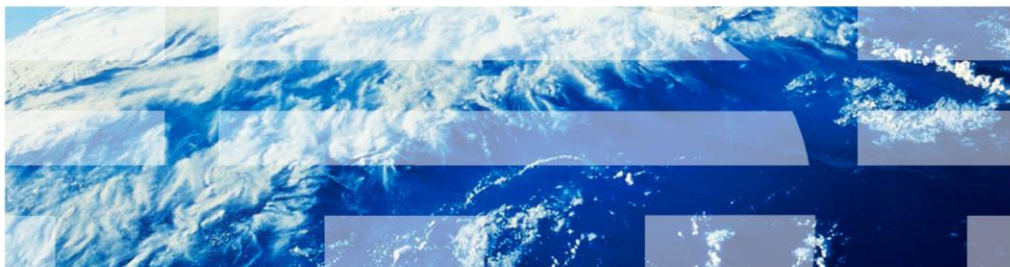


IBM Workload Deployer

DirMaint as directory manager/RACF optional



© 2011 IBM Corporation

This presentation will describe the necessary configurations if using DirMaint as your directory manager. It will also talk about additional RACF commands that are required if RACF Security Server for z/VM is active on your system.

Agenda

- DirMaint configuration
- Optional RACF configuration

This presentation will first discuss additional setup when using DirMaint as your directory manager in the z/VM environment. It will then talk about the optional RACF configuration.

DirMaint configuration

You will first look at the required DirMaint configuration.

MAPAUTH user ID

- Define a Class A user that will issue restricted system commands through the SMAPI interface (MAPAUTH)
 - Create MAPAUTH DIRECT:

```
USER MAPAUTH PASSWORD 32M 32M G  
INCLUDE IBMDFLT
```

- Add the guest to the z/VM directory

```
dirm add mapauth
```

You need to define a Class A user that is allowed to issue restricted system commands through the SMAPI. This slide shows the MAPAUTH user ID being created for this purpose.

VSMWORK1 user ID

- Issue `dirm needpass no` from the VSMWORK1 user ID
 - Verify the setting in VSMWORK1 DIRECT

```
*DVHOPT LNK0 LOG1 RCM1 SMS0 NPW0 LNGAMENG PWC20081106 CRCNi
```

To allow the VSMWORK1 user ID to not get prompted for its password when issuing DIRM commands, you need to issue the 'dirm needpass no' from the VSMWORK1 user ID. The setting can be verified in VSMWORK1 DIRECT. You should see the NPW0 value as an option at the bottom of the file. If it is set incorrectly, you will see NPW1 instead.

Update AUTHFOR CONTROL

- Need to update AUTHFOR CONTROL to authorize user IDs to issued needed commands

```
ALL MAPAUTH *      140A ADGHMOPS
ALL MAPAUTH *      150A ADGHMOPS
ALL VSMWORK1 *     140A ADGHMOPS
ALL VSMWORK1 *     150A ADGHMOPS
ALL VSMWORK2 *     140A ADGHMOPS
ALL VSMWORK2 *     150A ADGHMOPS
ALL VSMWORK3 *     140A ADGHMOPS
ALL VSMWORK3 *     150A ADGHMOPS
ALL MAPSRV *       140A ADGHOPS
ALL MAPSRV *       150A ADGHOPS
```

The DIRMAINT server uses the AUTHFOR CONTROL file as a repository of authorization information. This file contains a listing of user IDs who are authorized to act for other user IDs and the privilege classes that have been delegated to them. You need to update the file as shown on the slide to allow the various worker servers, the MAPAUTH user ID and the MAPSRV user ID to issue the needed commands to provision guests from the IBM Workload Deployer. Recall that the IBM Workload Deployer appliance interface to z/VM is through the MAPSRV guest.

Update CONFIGxx DATADVH

- Need to update the CONFIGxx DATADVH to authorize worker servers

```
ALLOW_ASUSER_NOPASS_FROM=          VSMWORK1 *
ALLOW_ASUSER_NOPASS_FROM=          VSMWORK2 *
ALLOW_ASUSER_NOPASS_FROM=          VSMWORK3 *
ALLOW_ASUSER_NOPASS_FROM=          VSMPROXY *
```

- Add or verify these entries:

```
RUNMODE=OPERATIONAL
ONLINE=IMMED
DASD_ALLOCATE=EXACT_FF
DATAMOVE_MACHINE=DATAMOVE * *
DVHDXD_FLASHCOPY_BEHAVIOR=2
DVHDXD_FLASHCOPY_COMPLETION_WAIT=0 0
MAXIMUM_UNASSIGNED_WORKUNITS=100
```

- Issue these to update DIRM:

```
dirm file CONFIGxx DATADVH
dirm rldcode
dirm rlddata
dirm rldextn
```

The appropriate CONFIGxx DATADVH file needs to be updated with the ALLOW_ASUSER_NOPASS_FROM commands in order to allow the various sever machines to make requests without specifying a password on commands. Authentication for the API server requests are handled by the VSM API server. Additional DirMaint authentication of every API server request is not needed. In order for the API server to be able to request directory changes from DirMaint, however, DirMaint must be told to trust the user ID for requests made from any of the worker servers. You should also verify that the entries under the second bullet exist in the CONFIGxx DATADVH file.

The z/VM system can contain multiple CONFIGxx DATADVH files. The files are read by the system in reverse alphabetical order. You can name the file CONFIGZZ DATADVH to ensure IBM Workload Deployer required changes are picked up first. All DIRM commands issued must complete with RC=0. Follow the steps shown to create a customized CONFIGxx DATADVH file.

Update EXTENT CONTROL

- Update the EXTENT CONTROL file with IBM Workload Deployer minidisks

```

:Regions.:
  RegionId      VolSer      RegStart      RegEnd      Dev-Type      Comments
  000001        WD2001      00001         10016       3390-09
  000002        WD2002      00001         10016       3390-09
  000003        WD2003      00001         10016       3390-09
  000004        WD2004      00001         10016       3390-09
  000005        WD2005      00001         10016       3390-09

:Groups.:
*GroupName RegionList
POOL0 (ALLOCATE ROTATING)
POOL0 000001 000002 000003 000004 000005

```

Allocation groups are used to define DASDPOOLS to the z/VM system. The DASDPOOL is defined in two sections – regions and groups.

Regions consist of the pre-defined minidisks to be used by the various DASDPOOLS, or Groups. The regions are defined using a region ID value. All DASD must be formatted as a minidisk and defined in the SYSTEM CONFIG file as user volumes using the User_Volume_Include statement.

Groups are used to define the DASDPOOLS. Each Group will consist of several region IDs. In this example, WD2001-WD2005 are used as the minidisks for IBM Workload Deployer.

Create a default directory entry

- Create a default directory entry that is used to define common definitions for all provisioned guests (LINDFLT DIRECT)

```
PROFILE LINDFLT
CLASS G
STORAGE 512M
MAXSTORAGE 2047M
IPL 201
IUCV ALLOW
MACHINE ESA
OPTION QUICKDSP
CONSOLE 0009 3215 T
SPOOL 000C 2540 READER *
SPOOL 000D 2540 PUNCH A
SPOOL 000E 1403 A
LINK MAINT 0190 0190 RR
LINK MAINT 019D 019D RR
LINK MAINT 019E 019E RR
LINK TCPMAINT 0592 0592 RR
```

DIRM ADD LINDFLT

- Add the new profile using the DIRMADD command

```
dirm add lindflt
```

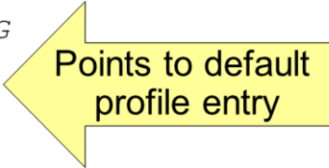
Default directory entries are used to define common definitions for all provisioned guests. This entry is referenced by the Linux prototype directory entry.

Create a file called LINDFLT DIRECT using Xedit. Shown here is an example of a default directory entry for Linux. Once created, add the new profile using the DIRM ADD command.

Create directory prototype

- Create a directory prototype that will allow provisioned guests to all share common statements (LINUX PROTODIR)

```
USER LINUX NOLOG 512M 2G G  
INCLUDE LINDFLT
```



Points to default
profile entry



DIRM FILE LINDFLT PROTODIR

A directory prototype allows provisioned guests to all share common statements. This slide shows the creation of a directory prototype using the LINDFLT directory entry you saw on the previous slide. Note that multiple directory prototypes can be created to support as many configurations as are needed.

RACF setup, optional

If you use RACF, the system RACF Administrator will need to configure RACF to allow for access to system resources. This section will describe the necessary configurations to use RACF.

Further customize DIRMAINT

- Update the **CONFIGxx DATADVH** member (add / verify) :

```

POSIX_CHANGE_NOTIFICATION_EXIT= DVHXPESM EXEC
LOGONBY_CHANGE_NOTIFICATION_EXIT= DVHXLB EXEC
USER_CHANGE_NOTIFICATION_EXIT= DVHXUN EXEC
DASD_OWNERSHIP_NOTIFICATION_EXIT= DVHXDN EXEC
PASSWORD_CHANGE_NOTIFICATION_EXIT= DVHXPN EXEC
RACF_ADDUSER_DEFAULTS= UACC(NONE) RACF_RDEFINE_VMMDISK_DEFAULTS= UACC(NONE)
AUDIT(FAILURES(READ))
RACF_RDEFINE_VMPOSIX_POSIXOPT.QUERYDB= UACC(READ)
RACF_RDEFINE_VMPOSIX_POSIXOPT.SETIDS= UACC(NONE)
RACF_RDEFINE_SURROGAT_DEFAULTS= UACC(NONE)
AUDIT(FAILURES(READ))
RACF_RDEFINE_VMBATCH_DEFAULTS= UACC(NONE) AUDIT(FAILURES(READ))
RACF_RDEFINE_VMRDR_DEFAULTS= UACC(NONE) AUDIT(FAILURES(READ))
RACF_RDEFINE_VMMDISK_DEFAULTS= UACC(NONE)
AUDIT(FAILURES(READ))
RACF_VMBATCH_DEFAULT_MACHINES= BATCH1 BATCH2
TREAT_RAC_RC.4= 0 | 4 | 30

```

If using RACF as a security manager on the hypervisor where you are utilizing IBM Workload Deployer, DIRMAINT needs to perform ADDUSER/DELUSER RDEFINE/RDELETE commands when the CP directory entries for provisioned servers are created and deleted. The DIRMAINT-RACF relationship present in the default DIRMAINT configuration files and the modifications shown here allow that to happen. You can extend these configuration files and the DVHXPN user exits as long as the ability to perform these operations is preserved.

Update VSMWORK1 and add sample RACF exit

- Sample RACF exit
 - Provided in the RPM installed on MAPSRV as `wcasepc.exec`
 - Copy `/opt/ibm/zensemble/zvm-scripts/wcasepc.exec` to MAINT's 193 disk
- On VSMWORK1, edit DMSSIUSR NAMES
 - Add the following statement to invoke the sample RACF exit

```
:nick.Security_Manager_Permit  
:program.wcasepc
```

- On VSMWORK1, edit DMSSICNF COPY and change ULONG to the following value:

```
ULONG = 'SECURITY_MANAGER_PERMIT'
```

In order to use RACF, a sample RACF exit is provided in the RPM that is installed on the MAPSRV user ID. It is found in the `/opt/ibm/zensemble/zvm-scripts` directory and needs to be copied to MAINT's 193 disk. To have the exit invoked, you need to update the DMSSIUSR NAME file on VSMWORK1 by adding the statement shown on the slide. You also need to update the DSMSICNF COPY file on VSMWORK1 so that the APIs can be dispatched to the other worker servers to improve multitasking capability. API names should be blank-separated.

Permitting access to system resources

- Configure access to the VMRDR class

```
rac PERMIT MAINT      CLASS (VMRDR) ID (DATAMOVE)  ACC (UPDATE)
rac PERMIT OPERATOR  CLASS (VMRDR) ID (TCPIP)    ACC (UPDATE)
rac PERMIT FTPSERVE  CLASS (VMRDR) ID (FTPSERVE)  ACC (CONTROL)
rac PERMIT DIRMAINT  CLASS (VMRDR) ID (VSMWORK2)  ACCESS (UPDATE)
rac PERMIT DIRMAINT  CLASS (VMRDR) ID (VSMWORK3)  ACCESS (UPDATE)
rac PERMIT DIRMAINT  CLASS (VMRDR) ID (VSMWORK1)  ACCESS (UPDATE)
```

First, it is necessary to grant some user IDs access to the VMRDR class as shown.

Permitting access to networking configuration (1 of 2)

- Define RACF resources for Guest LANs (for example, MAPLAN), and VSWITCHes

```
RAC RDEFINE VMLAN SYSTEM.[zVM_LAN_Name] UACC(NONE)
RAC RDEFINE VMLAN SYSTEM.MAPLAN UACC(NONE)
```
- Define a RACF resource for the VLAN, if one exists

```
RAC RDEFINE VMLAN SYSTEM.[zVM_LAN_Name].[VLAN] UACC(NONE)
```
- Reset VMLAN definitions

```
RAC PERMIT SYSTEM.[zVM_LAN_Name] CLASS(VMLAN) RESET(ALL)
RAC PERMIT SYSTEM.MAPLAN CLASS(VMLAN) RESET(ALL)
```
- Allow update access to MAINT and DTCVSW1

```
RAC PERMIT SYSTEM.[zVM_LAN_Name] CLASS(VMLAN) ID(MAINT) ACCESS(UPDATE)
RAC PERMIT SYSTEM.[zVM_LAN_Name] CLASS(VMLAN) ID(DTCVSW1) ACCESS(UPDATE)
```

Define RACF resources for Guest LANs (for example, MAPLAN), VSWITCHes and the VLAN, if one exists. Before adding access to these resources then, use the RESET (ALL) parameter on the RACF PERMIT command to delete the current standard access list and the current conditional access list. Then allow the MAINT and the DTCVSW1 user IDs to have update access to the VSWITCH.

Permitting access to networking configuration (2 of 2)

- Allow MAPSRV and TCPIP to couple to MAPLAN

```
RAC PERMIT SYSTEM.MAPLAN CLASS (VMLAN) ID (TCPIP) ACCESS (UPDATE)
RAC PERMIT SYSTEM.MAPLAN CLASS (VMLAN) ID (MAPSRV) ACCESS (UPDATE)
```

- Allow MAPSRV and TCPIP to couple to the VSWITCH

```
RAC PERMIT SYSTEM.[zVM_LAN_Name] CLASS (VMLAN) ID (MAPSRV) ACCESS (UPDATE)
RAC PERMIT SYSTEM.[zVM_LAN_Name].[VLAN] CLASS (VMLAN) ID (MAPSRV) ACCESS (UPDATE)
```

- Activate VMLAN class

```
RAC SETROPTS CLASSACT (VMLAN)
```

The next thing you need to do in RACF for networking is allow the MAPSRV and TCPIP user IDs to couple to the guest LAN (for example MAPLAN) and VSWITCH that you have defined. Those commands are shown on the slide. You then can activate the VMLAN class.

Summary

- DirMaint configuration
- Optional RACF configuration

In summary, this presentation looked at the configuration needed if using DirMaint as the directory manager for a z/VM hypervisor in IBM Workload Deployer. It also looked at the optional RACF configurations needed if RACF is being used.

Trademarks, disclaimer, and copyright information

IBM, the IBM logo, ibm.com, DirMaint, RACF, and z/VM are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of other IBM trademarks is available on the web at "[Copyright and trademark information](http://www.ibm.com/legal/copytrade.shtml)" at <http://www.ibm.com/legal/copytrade.shtml>

Linux is a registered 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.

THE INFORMATION CONTAINED IN THIS PRESENTATION IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY. WHILE EFFORTS WERE MADE TO VERIFY THE COMPLETENESS AND ACCURACY OF THE INFORMATION CONTAINED IN THIS PRESENTATION, IT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. IN ADDITION, THIS INFORMATION IS BASED ON IBM'S CURRENT PRODUCT PLANS AND STRATEGY, WHICH ARE SUBJECT TO CHANGE BY IBM WITHOUT NOTICE. IBM SHALL NOT BE RESPONSIBLE FOR ANY DAMAGES ARISING OUT OF THE USE OF, OR OTHERWISE RELATED TO, THIS PRESENTATION OR ANY OTHER DOCUMENTATION. NOTHING CONTAINED IN THIS PRESENTATION IS INTENDED TO, NOR SHALL HAVE THE EFFECT OF, CREATING ANY WARRANTIES OR REPRESENTATIONS FROM IBM (OR ITS SUPPLIERS OR LICENSORS), OR ALTERING THE TERMS AND CONDITIONS OF ANY AGREEMENT OR LICENSE GOVERNING THE USE OF IBM PRODUCTS OR SOFTWARE.

© Copyright International Business Machines Corporation 2011. All rights reserved.