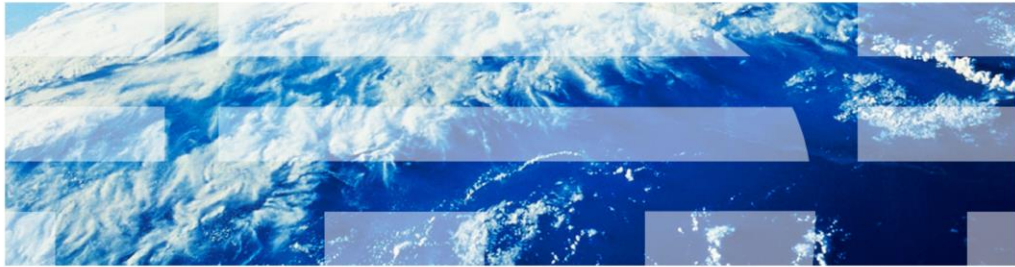


IBM Workload Deployer

VM:Secure as directory manager



© 2011 IBM Corporation

This presentation will describe the necessary additional configurations if using VM:Secure as your directory manager.

Agenda

- VM:Secure service required
- Additional configuration for VM:Secure

First you will see some VM:Secure service that is required. Then you will see the configuration required to use VM:Secure as your directory manager.

VM:Secure service

First you will look at the service needed in order to use VM:Secure on the z/VM[®] system where your IBM Workload Deployer hypervisor runs.

Service needed for VM:Secure support

- Computer Associates VM:Secure
 - T2A6X897
 - T2A6X898

The first thing you need to do is put some important service on your z/VM system. This slide lists some necessary VM:Secure service that is required.

VM:Secure configuration

Next you will look at the required VM:Secure configuration.

Request servers and worker ID's directory entries

- Add the following statement to the directory entries:

```
LINK VMRMANT 193 293 RR
```

- Request servers include:

- VSMREQIN
- VSMREQIU
- VSMPROXY

- Worker IDs include:

- VSMWORK1
- VSMWORK2
- VSMWORK3

In order for the request servers to access the VM:Secure code, you need to add the LINK VMRMANT statement shown on the slide to the directory entries. This includes all the request and worker IDs shown on the slide.

Update profile execs for the request servers and worker IDs

- Request servers (VSMREQIN, VSMREQUIU and VSMPROXY)
 - Add 'access 293 H' to access VMRMAINT disk
 - VM:Secure SMAPI implementation code is found here
- Worker IDs (VSMWORK1, VSMWORK2... VSMWORKn)
 - Add 'access 293 H' to access VMRMAINT disk
 - VM:Secure SMAPI implementation code is found here

The VM:Secure SMAPI implementation code is found on the VMRMAINT disk. In order to access the SMAPI implementation code, you need to add a statement to the profile execs for the request servers and worker IDs. The statement to access the VMRMAINT disk is shown on the slide and uses the link to the VMRMAINT disk that you created a link to in the directory entries.

VM:Secure skeleton file

- Provides a set of common definitions for z/VM guests
- Create a generic skeleton (for example, LINUX) based on the default skeleton named GENERAL

```
vmsecure admin skeleton linux general
```

- Customize it as needed

```
vmsecure admin linux
```

```
USER LINUX NOLOG  
MACHINE ESA  
CONSOLE 0009 3215  
SPOOL 00C 2540 READER *  
SPOOL 00D 2540 PUNCH A  
SPOOL 00E 1403 A
```

- Add the customized skeleton to VM:Secure directory

```
vmsecure addentry linux linux
```

VM:Secure has the concept of a skeleton file, which is equivalent to the prototype directory entries created for the DirMaint directory manager. Skeleton files are used to define common definitions for all provisioned guests. You are asked for its name when configuring the IBM Workload Deployer for deployments. The first statement shown on the slide creates a skeleton named LINUX based on the skeleton named SKELETON. Once you have the 'LINUX' skeleton customized for your environment, you can use the VM:Secure addentry command to add it to the VM:Secure directory.

MAPAUTH user ID

- User that is given access to issue restricted system commands through the SMAPI

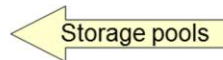
```
USER MAPAUTH PASSWORD 32M 32M G
INCLUDE IBMDFLT
```

- Directory manager-dependent commands are required to give MAPAUTH the needed authorization to issue commands on IBM Workload Deployer's behalf
 - From VMRMANT, enter the command "vmsecure config authoriz" and add this statement:

```
GRANT *ALL TO MAPAUTH
```

- From VMRMANT, enter the command "vmsecure admin managers" and add the following statement:

```
MANAGER MAPAUTH * WDPOOL1 WDPOOL2
SKELETON MAPAUTH GENERAL
DEVTYPE MAPAUTH 3390
```



Storage pools

In order to issue the SMAPI commands, a user ID and password is required. This is what the MAPAUTH user ID is used for. The directory entry is very basic for MAPAUTH however you need to give the MAPAUTH guest authorization to issue commands on IBM Workload Deployer's behalf. The first thing you need to do is give MAPAUTH authorizations to issue all commands. This is done by adding the GRANT statement shown to the 'AUTHORIZ CONFIG' file. This is done with the 'vmsecure config authoriz' command. The MAPAUTH user ID also needs to be defined to VM:Secure as a 'manager'. You also need to give MAPAUTH access to the storage pools that you will create. To do this add the statements shown on the bottom of the slide to the VMSECURE MANAGERS file. This is done with the 'vmsecure admin managers' command. In the example on the slide, the storage pools are defined as WDPOOL1 and WDPOOL2.

Set up APPC IUCV connection

- APPC IUCV is required to pass SMAPI commands between the client and the server on VM:Secure
 - Update 'config product' (enter the command "vmsecure config product")
 - Add this statement:
 - RESID SMAPIRES
 - Update 'vmsecure' (enter the command "vmsecure edit vmsecure")
 - Add the following statement:
 - IUCV *IDENT SMAPIRES LOCAL
 - Restart VMSECURE guest to pick up the changes to the directory entry.
 - Look for the following message on the console:

```
11:06:03 VM:SECURE 0007 VMXAIC1284I Initializing local APPCVM resource
SMAPIRES.
11:06:03 VM:SECURE 0007 VMXAIC1257I Completed SMAPIRES resource
definition for local.
```

For VM:Secure, APPC IUCV is required to pass SMAPI commands between the client and the server. This slide shows a few VM:Secure commands needed to accomplish this.

Update the PRODUCT CONFIG file with the RESID statement shown and the VMSECURE directory entry with the IUCV statement shown. The VMSECURE guest needs to be restarted to pick up these changes. Once these changes are made, you can check the VMSECURE console log for the messages shown at the bottom of the slide to be sure the configuration is correct.

Update DMSSICNF COPY

- Change the DM_EXIT statement to "VMXSIXDM". This is the exit supplied by VM:Secure:

```
DM_exit = "VMXSIXDM"
```

In order to use VM:Secure as your directory manager, you need to update the DMSSICNF COPY file. This is an important file for the VM:Secure configuration. This is where you need to point to the VM:Secure directory manager exit instead of the DirMaint directory manager exit. In order to use VM:Secure, the DM_exit parameter needs to be set to 'VMXSIXDM'.

VM:Secure storage pools

- DASD CONFIG (From VMMAINT, enter the command "vmsecure config dasd")
 - Two possible pools:
 1. Linux guests hosting the WebSphere® environment
 2. Cache images
 - Define pools ("DASD Subpools" section)


```
SUBPOOL WDPOOL1 ROTATING LOWEND *
SUBPOOL WDPOOL2 ROTATING LOWEND *
```
 - Define volumes to pools ("VM:SECURE Volume and Extent Definitions" section)


```
VOLUME WD2001 3390
* VOLUME 2001, CP SYSTEM
EXTENT 0 0 * Protects Allocation Record
EXTENT 1 60102 WDPOOL1

VOLUME WD2002 3390
* VOLUME 2002, CP SYSTEM
EXTENT 0 0 * Protects Allocation Record
EXTENT 1 60102 WDPOOL2
```

Mod54-3390

Recall that there are two possible storage pools that can be used by IBM Workload Deployer. The first one is required and is used to define the disks needed for the guests that IBM Workload Deployer deploys. The second one is optional and is used to cache images, if specified. The same pool can be used for both functions but separate pools are recommended. In order to define these pools to VM:Secure, you need to add the SUBPOOL statements to the "DASD Subpools" section. You also need to define the volumes that the pools will use in the 'VM:Secure Volume and Extent Definitions' section. In the example shown here the WD2001 volume is used for the WDPOOL1 storage pool and the WD2002 volume is used for the WDPOOL2 storage pool. Both volumes are of type MOD54-3390 as seen by the 60102 size.

Summary

- VM:Secure service
- VM:Secure configuration

In summary, this presentation looked at the VM:Secure specific service that is required and the additional configuration needed to use VM:Secure as your directory manager.

Trademarks, disclaimer, and copyright information

IBM, the IBM logo, ibm.com, DirMaint, WebSphere, 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.