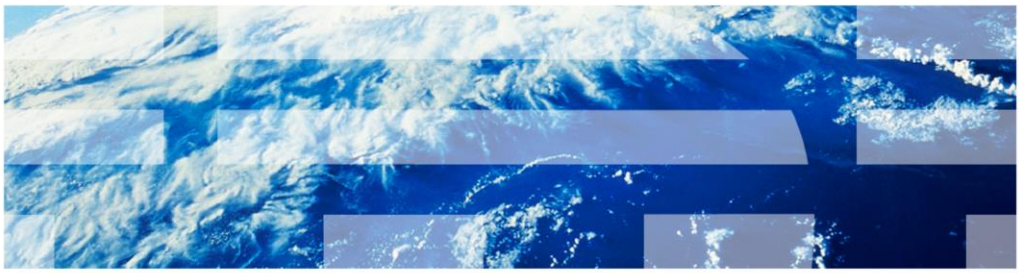
IBM Workload Deployer

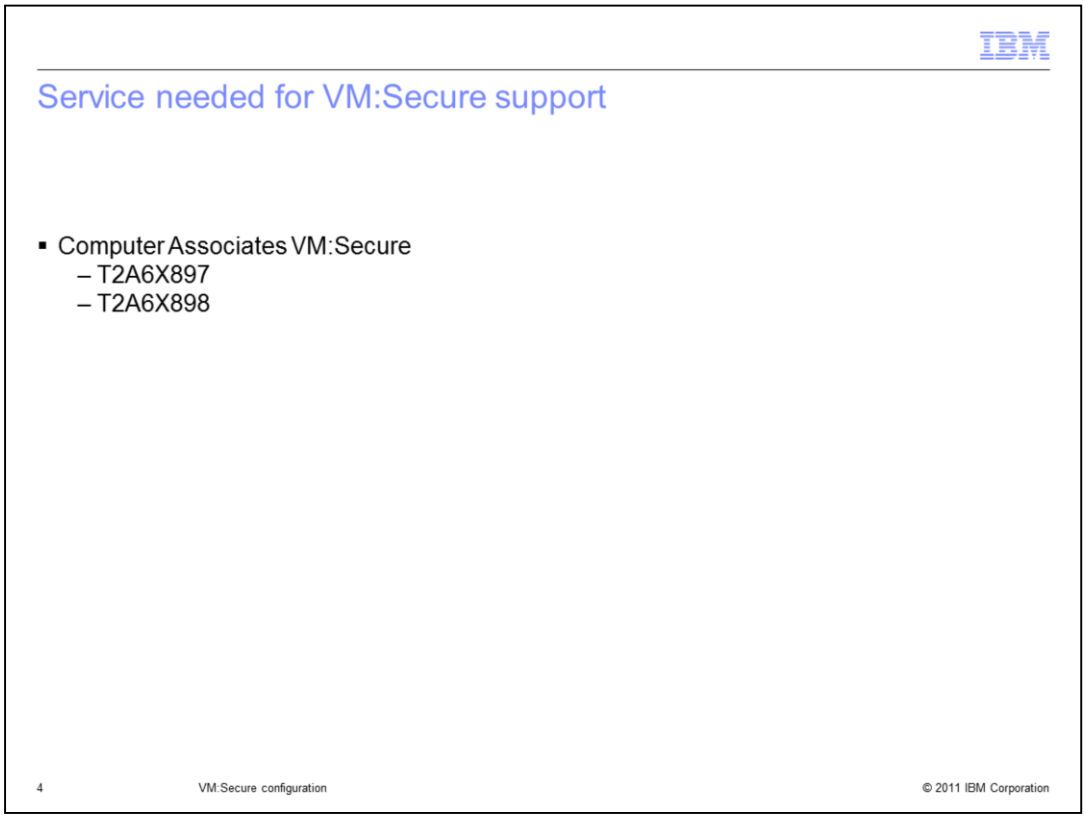
VM:Secure as directory manager



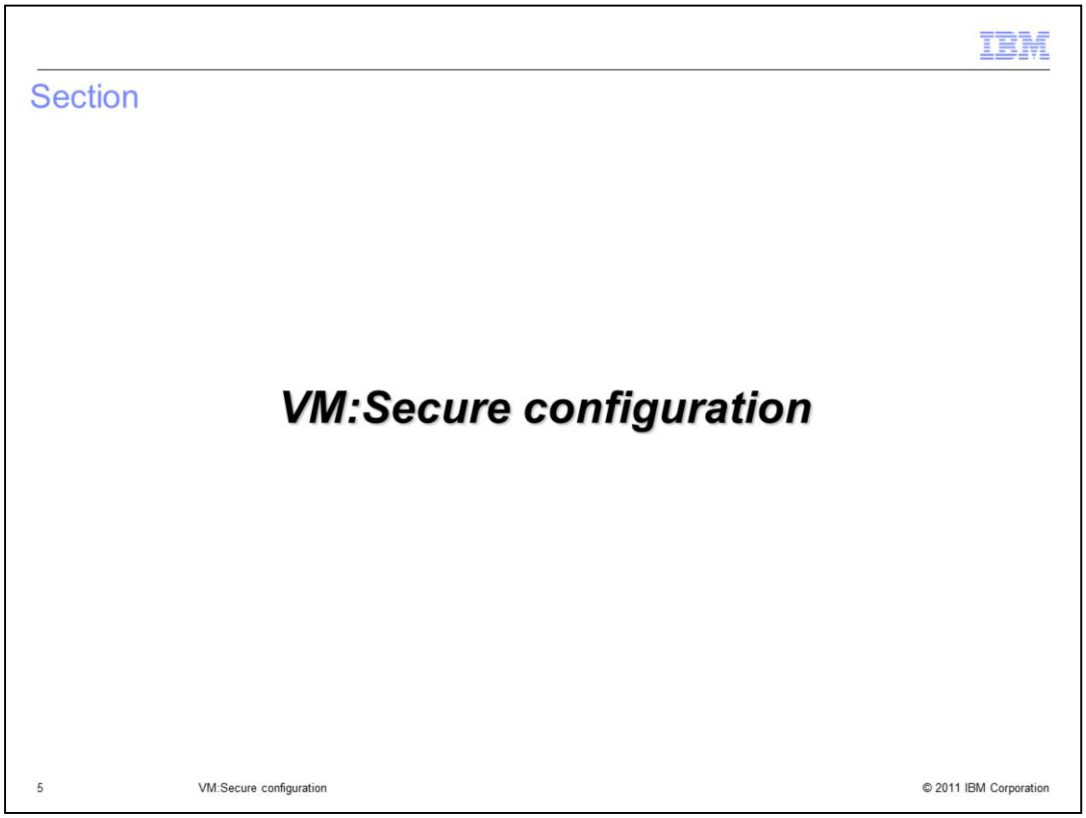
This presentation will describe the necessary additional configurations if using VM:Secure as your directory manager.

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.

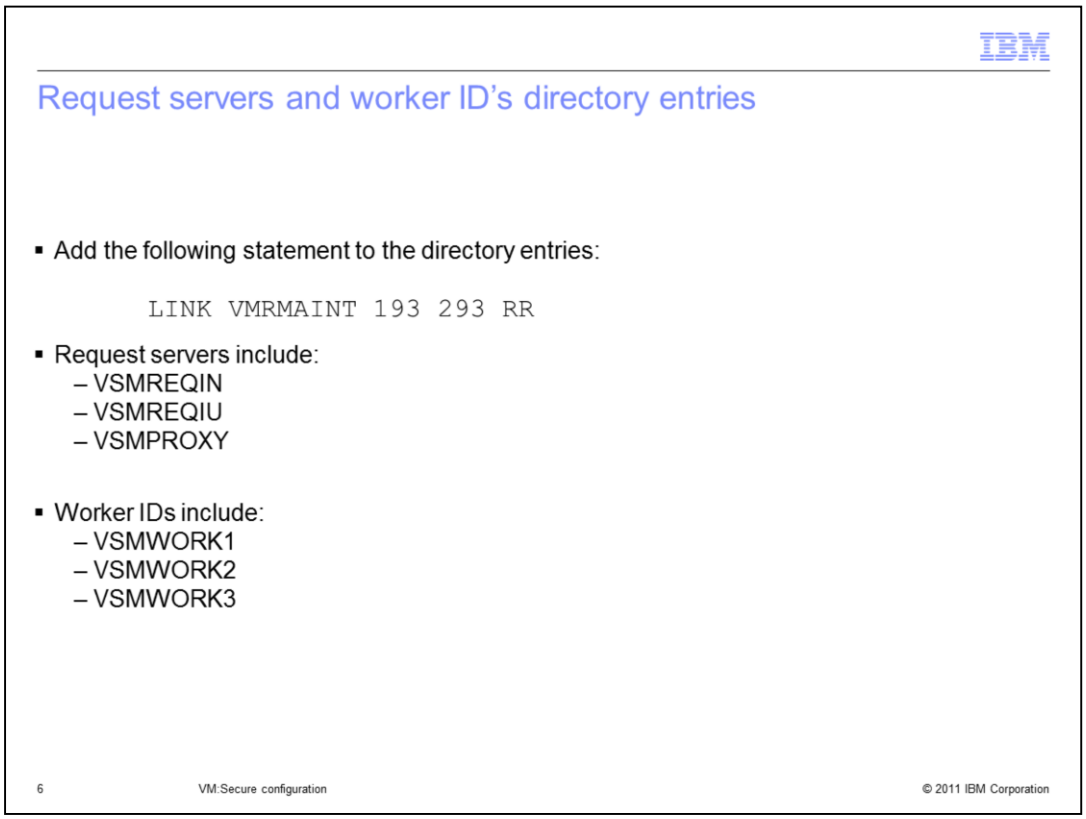
First you will look at the service needed in order to use VM:Secure on the z/VM® system where your IBM Workload Deployer hypervisor runs.



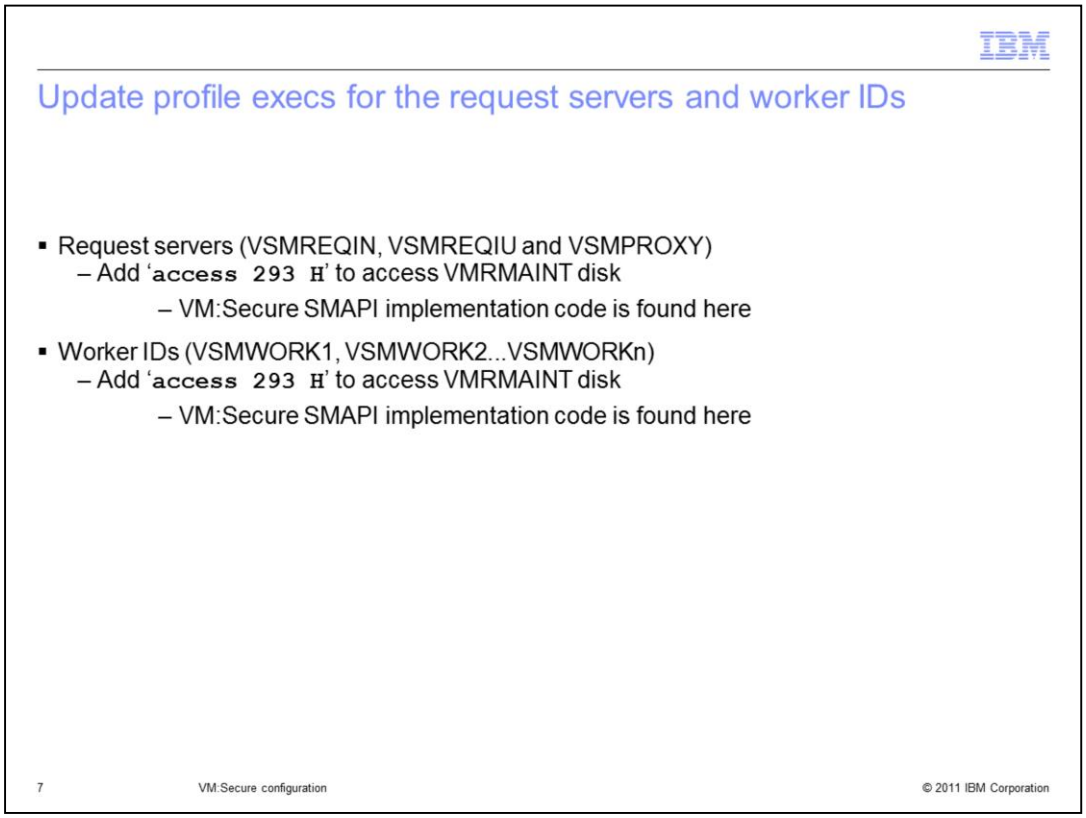
The first thing you need to do is put some important service on your z/VM system. This slide lists some necessary VM:Secure service that is required.



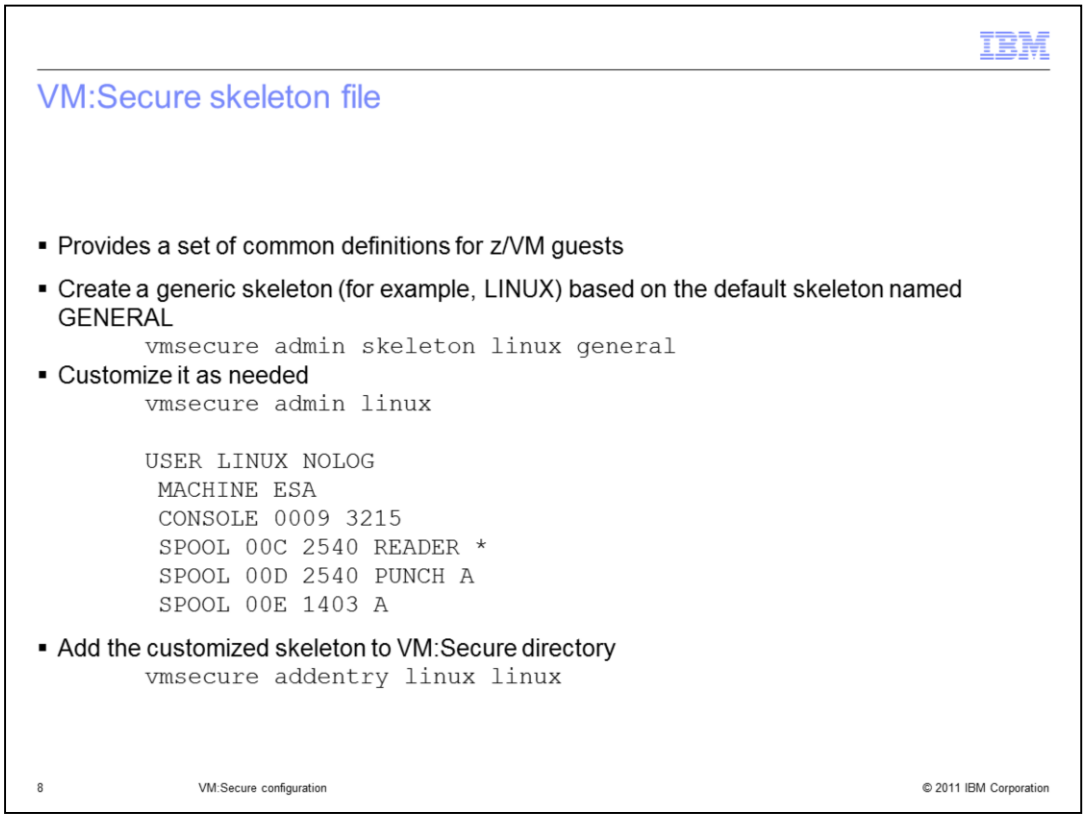
Next you will look at the required VM:Secure configuration.



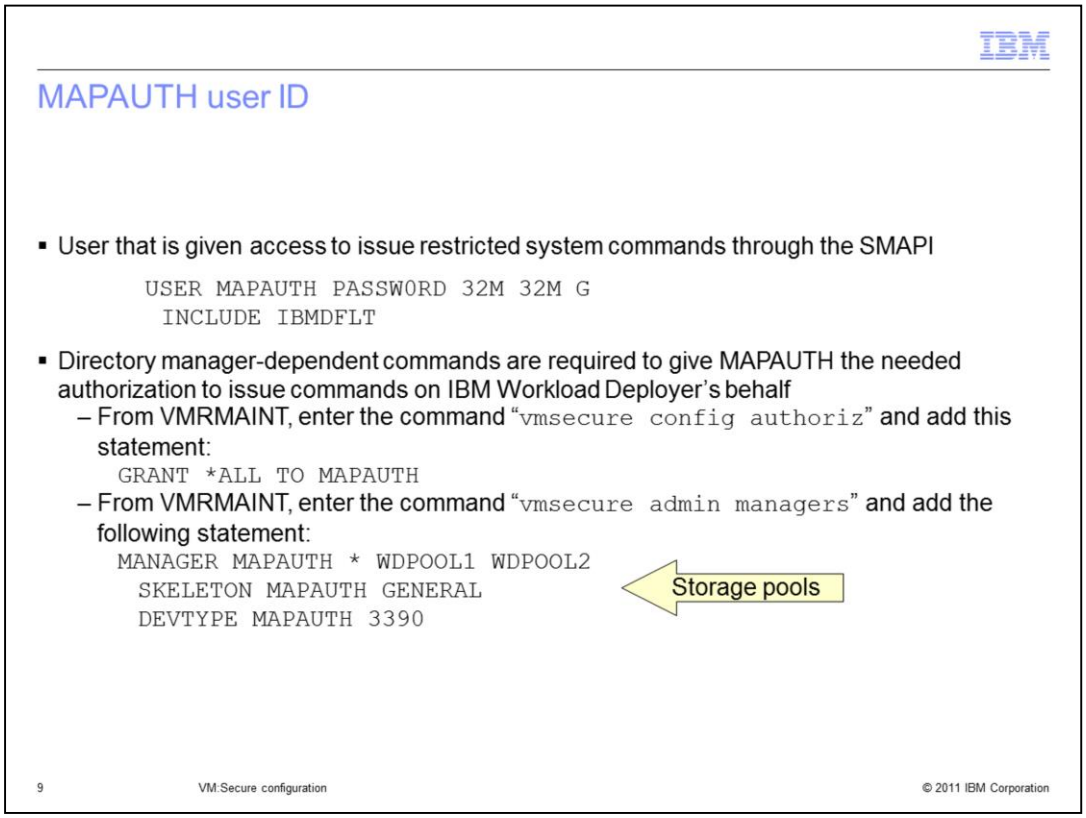
In order for the request servers to access the VM:Secure code, you need to add the LINK VMRMAINT statement shown on the slide to the directory entries. This includes all the request and worker IDs shown on the slide.



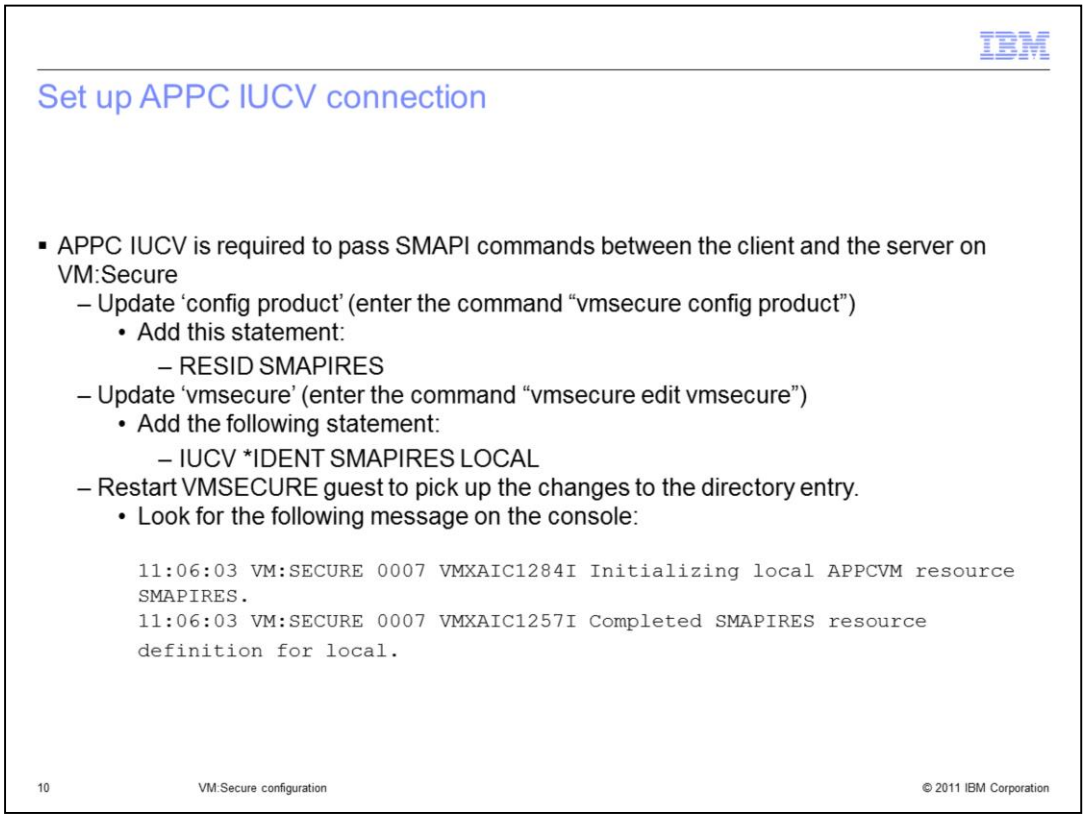
The VM:Secure SMAPI implementation code is found on the VMRMAINT disk. In order to access the SMAPI implementation code, you need to add a statement to the profile execs for the request servers and worker IDs. The statement to access the VMRMAINT disk is shown on the slide and uses the link to the VMRMAINT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



VM:Secure 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.

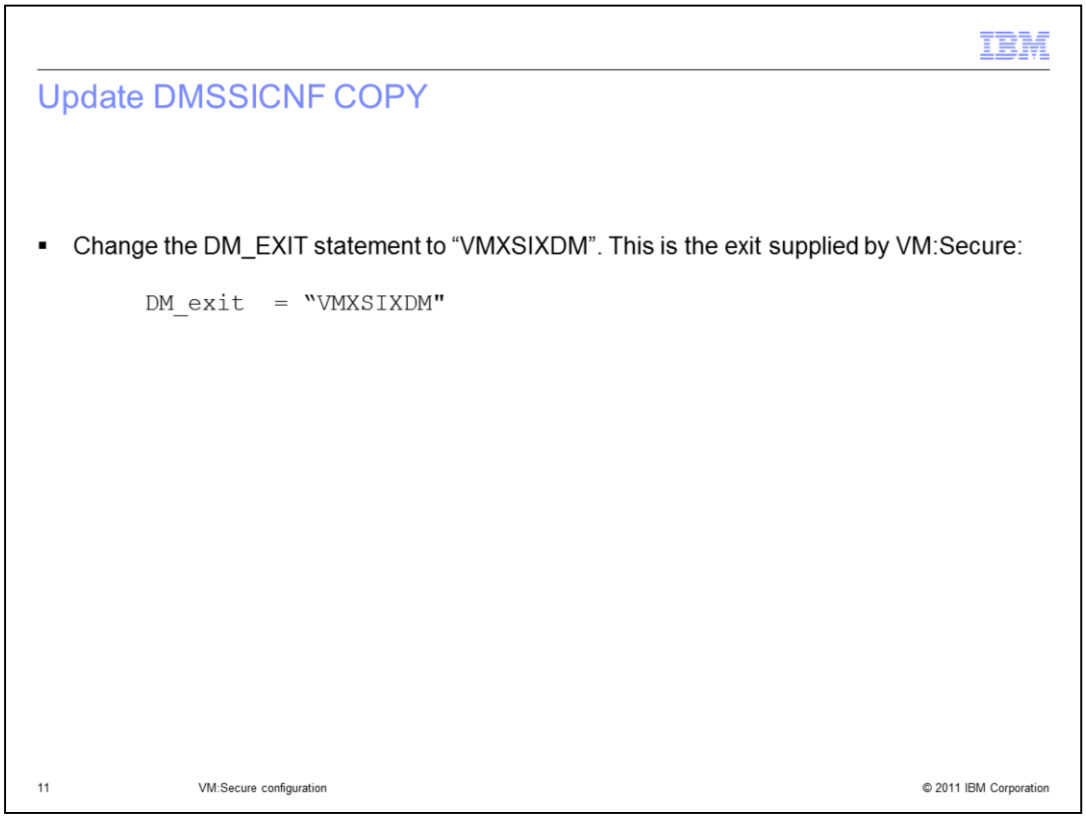


In order to issue the SMAPI commands, a user ID and password is required. This is what the MAPAUTH user ID is used for. The directory entry is very basic for MAPAUTH however you need to give the MAPAUTH guest authorization to issue commands on IBM Workload Deployer's behalf. The first thing you need 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.

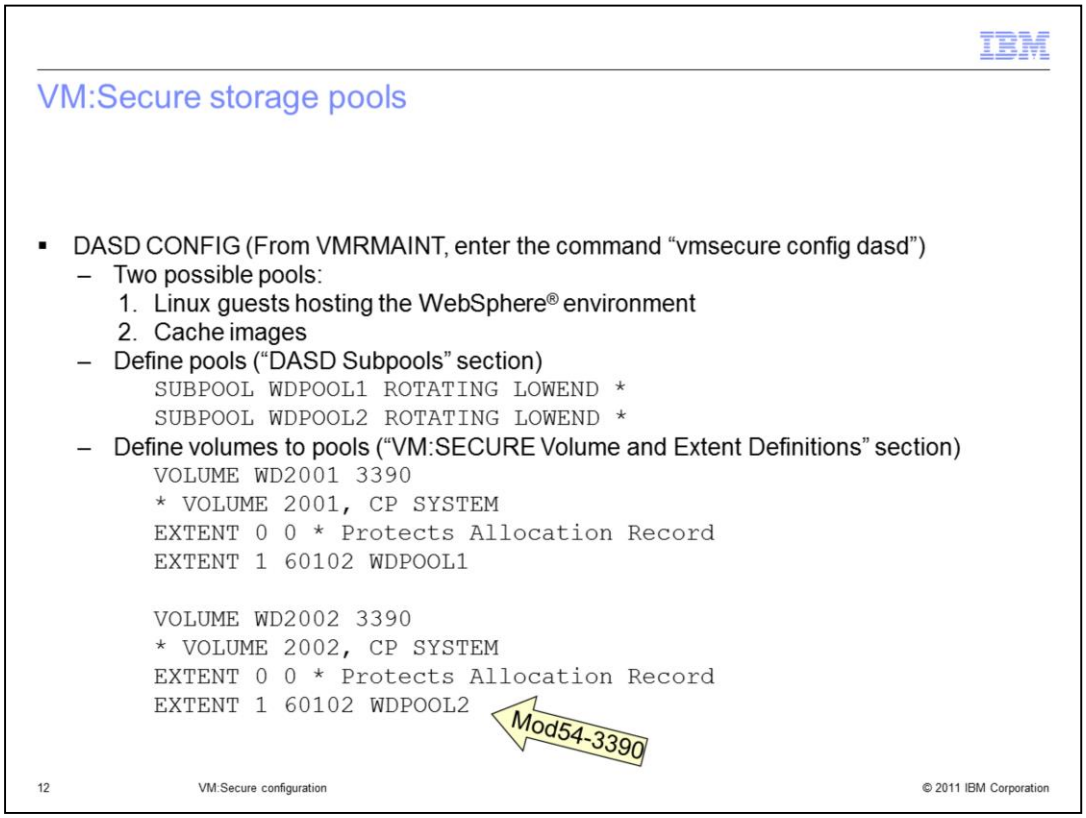


For VM:Secure, APPC IUCV is required to pass SMAPI commands between the client and the server. This slide shows a few VM:Secure commands needed to accomplish this.

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.



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’.



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.

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