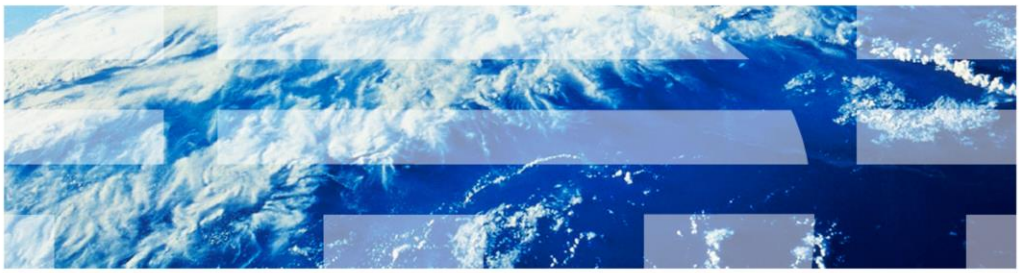
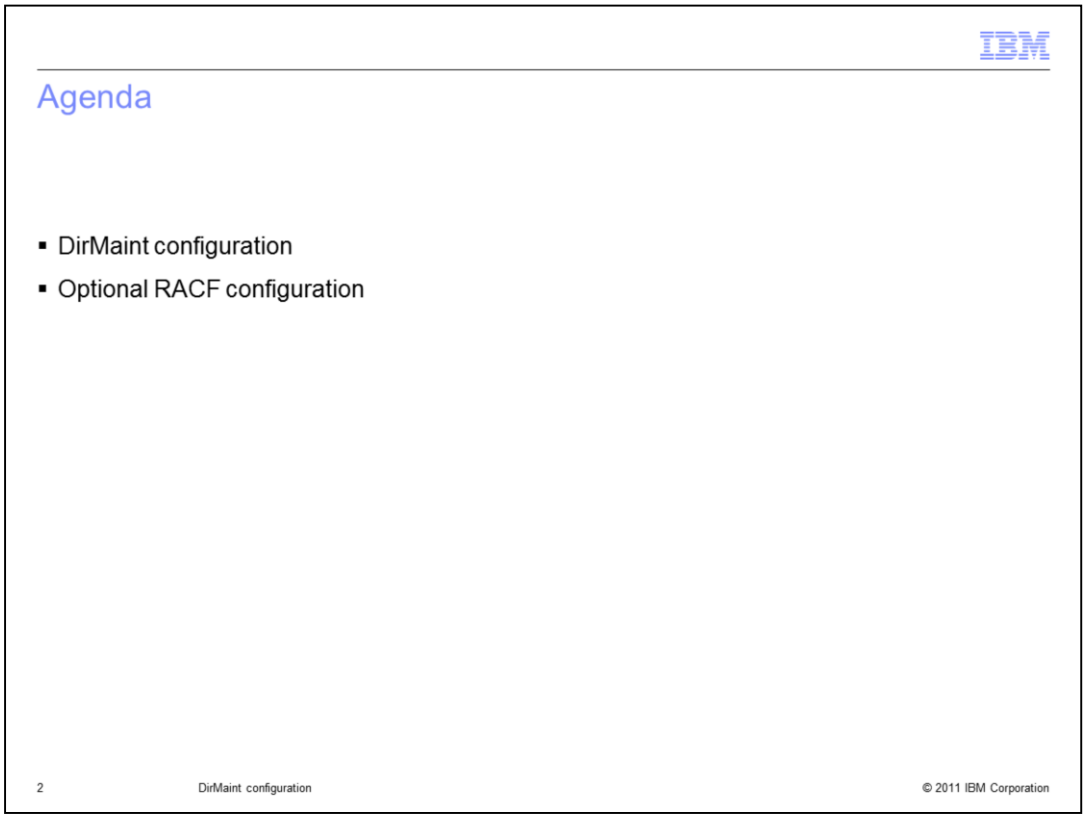
IBM Workload Deployer

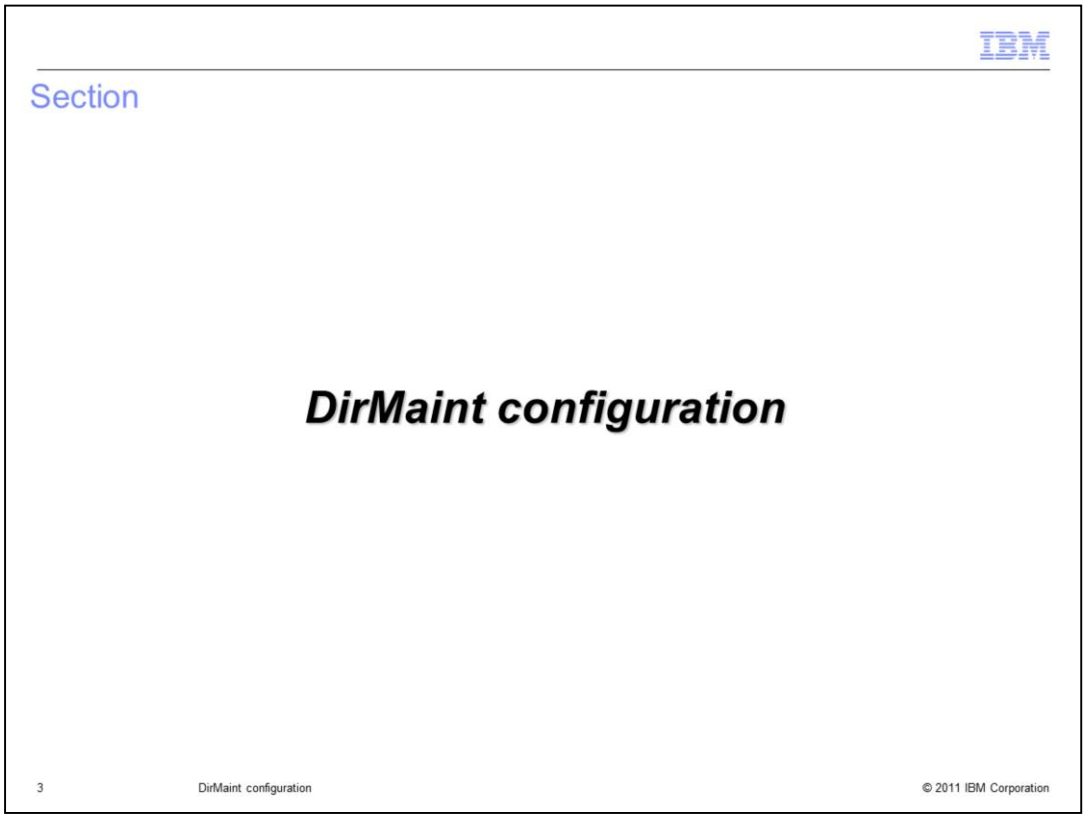
DirMaint as directory manager/RACF optional



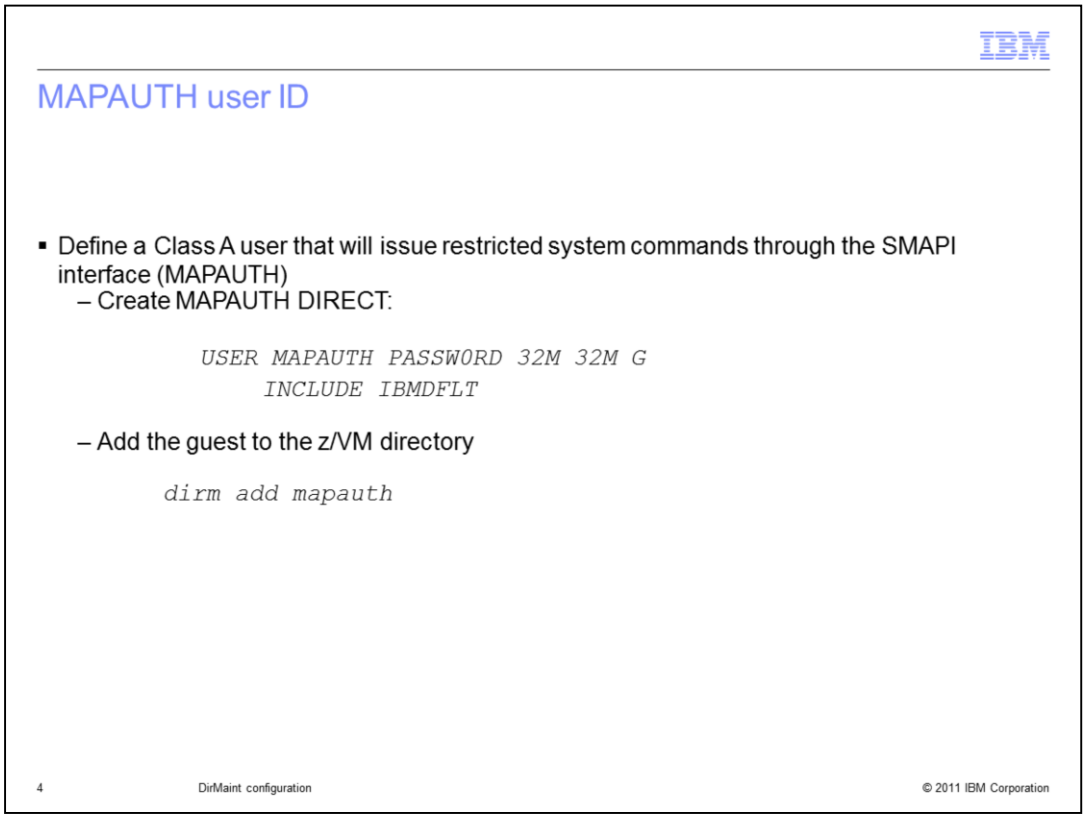
This presentation will describe the necessary configurations if using DirMaint as your directory manager. It will also talk about additional RACF commands that are required if RACF Security Server for z/VM is active on your system.



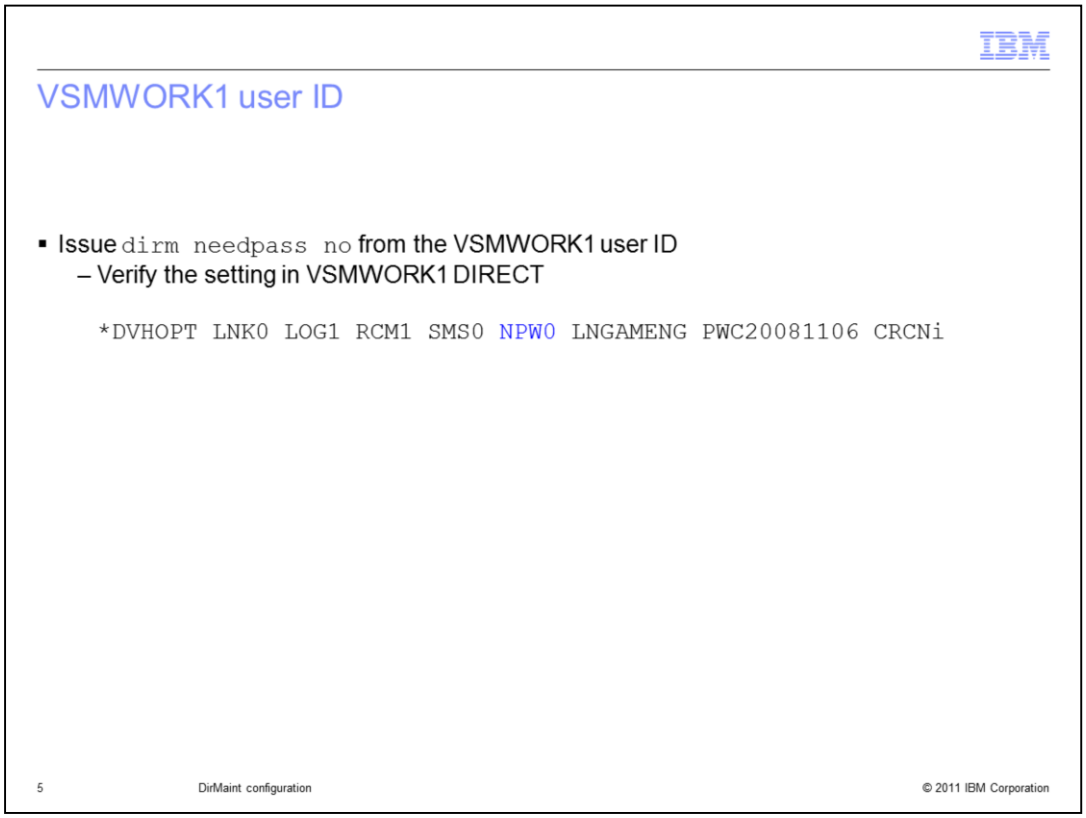
This presentation will first discuss additional setup when using DirMaint as your directory manager in the z/VM environment. It will then talk about the optional RACF configuration.



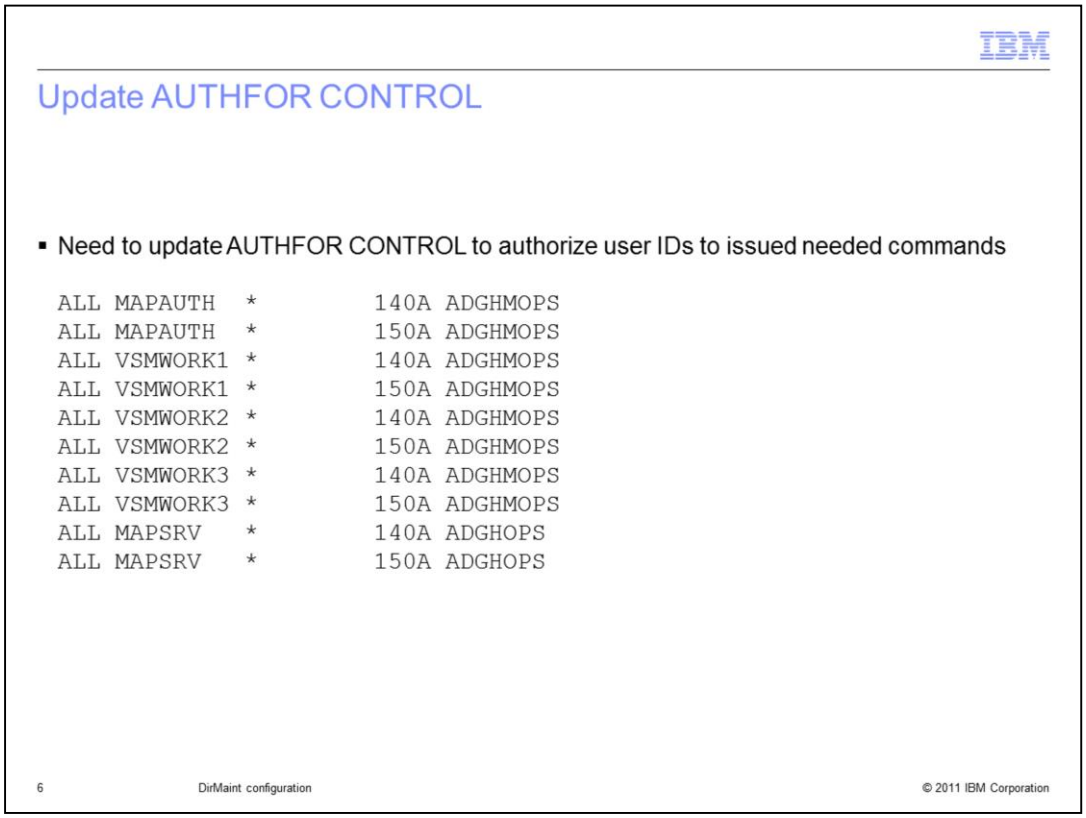
You will first look at the required DirMaint configuration.



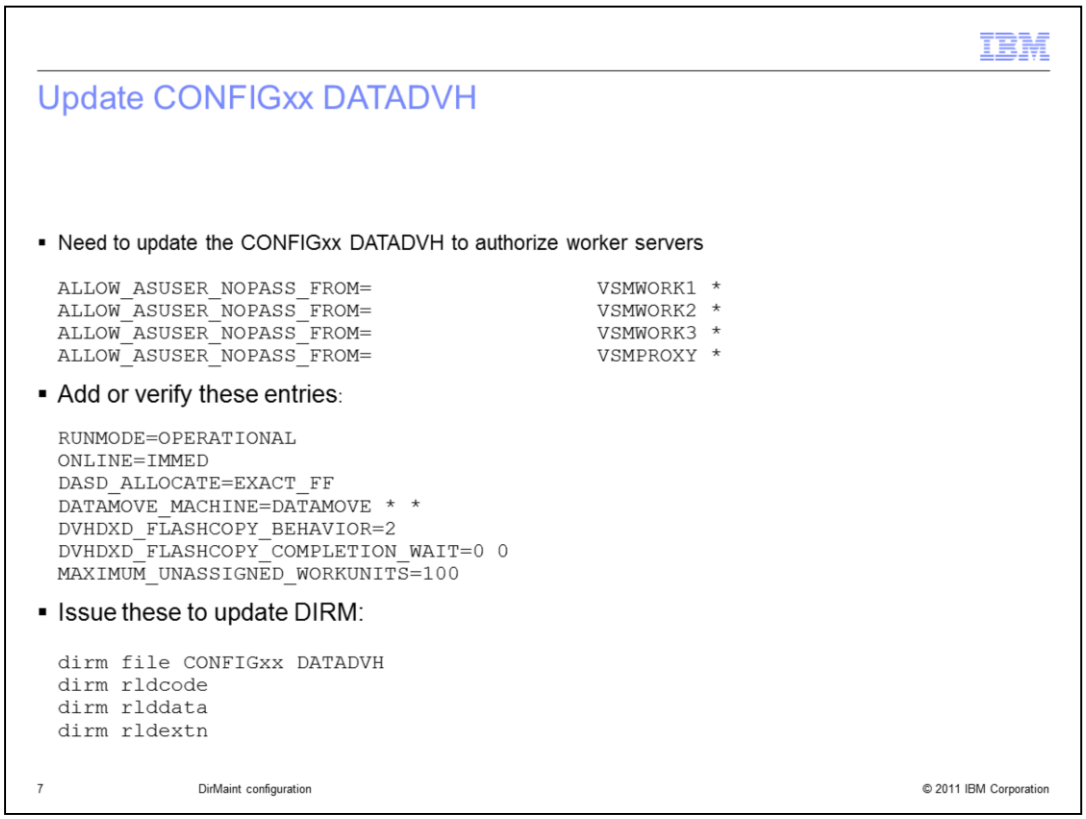
You need to define a Class A user that is allowed to issue restricted system commands through the SMAPI. This slide shows the MAPAUTH user ID being created for this purpose.



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.

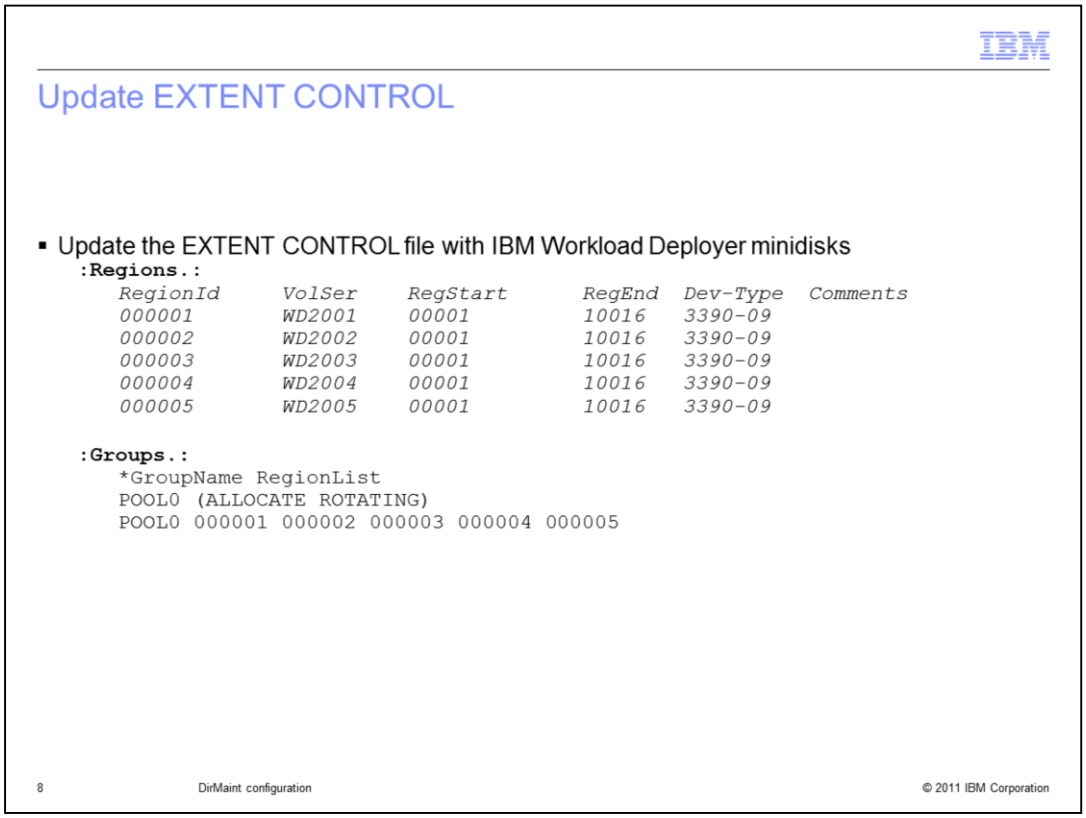


The DIRMAINT server uses the AUTHFOR CONTROL file as a repository of authorization information. This file contains a listing of user IDs who are authorized to act for other user IDs and the privilege classes that have been delegated to them. You need to update the file as shown on the slide to allow 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.



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.

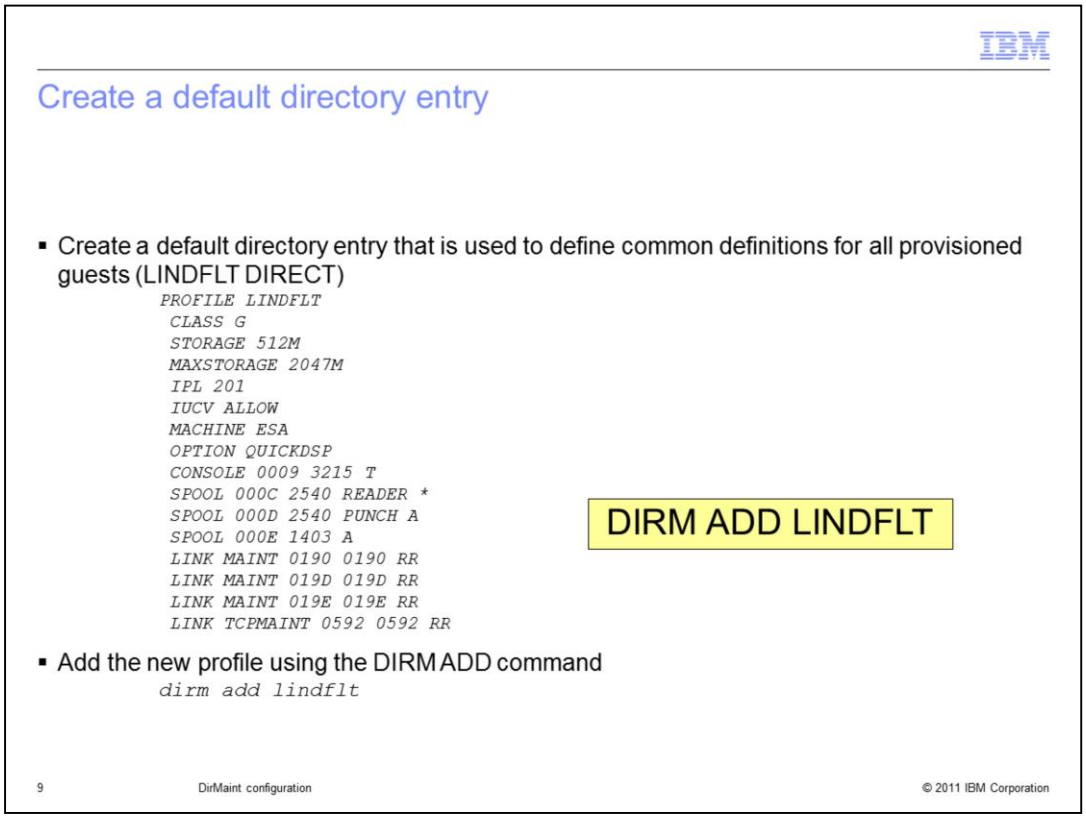
The z/VM system can contain multiple CONFIGxx DATADVH files. The files are read by the system in reverse alphabetical order. You can name the file CONFIGZZ DATADVH to ensure IBM Workload Deployer required changes are picked up first. All DIRM commands issued must complete with RC=0. Follow the steps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



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

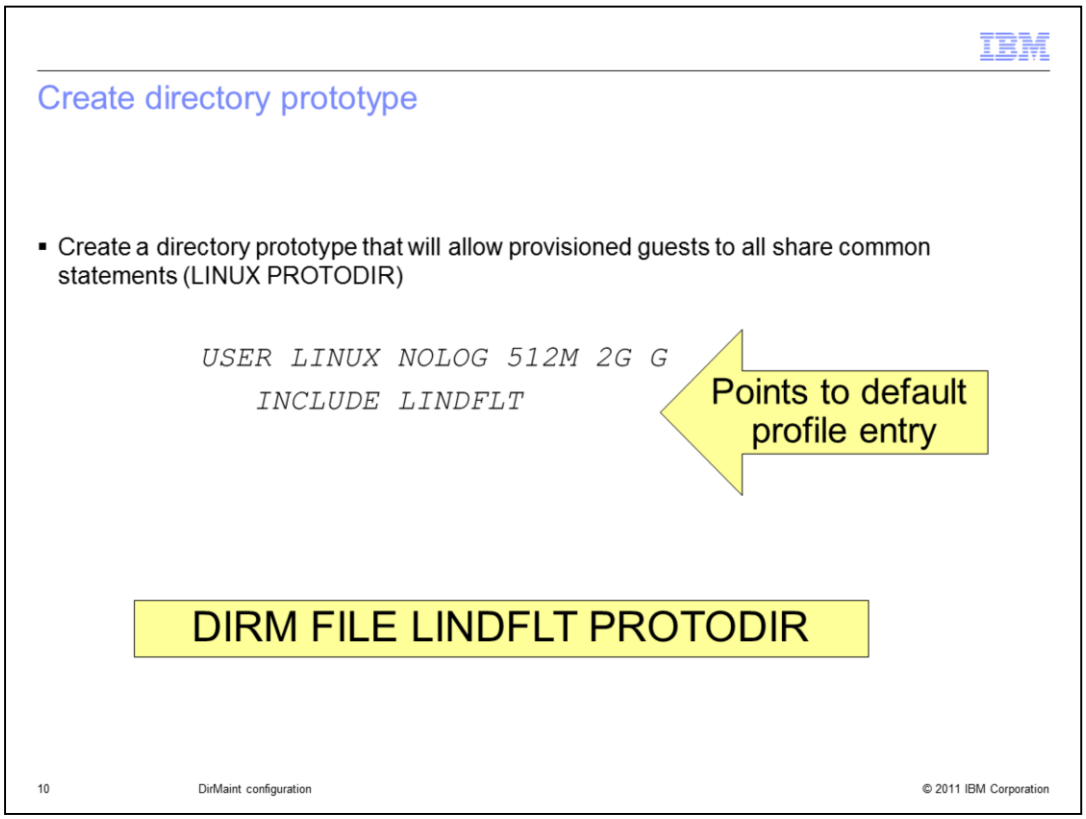
Regions consist of the pre-defined minidisks to be used by the various DASDPOOLs, or Groups. The regions are defined using a region ID value. All DASD must be formatted as a minidisk and defined in the SYSTEM CONFIG file as user volumes using the User_Volume_Include statement.

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.



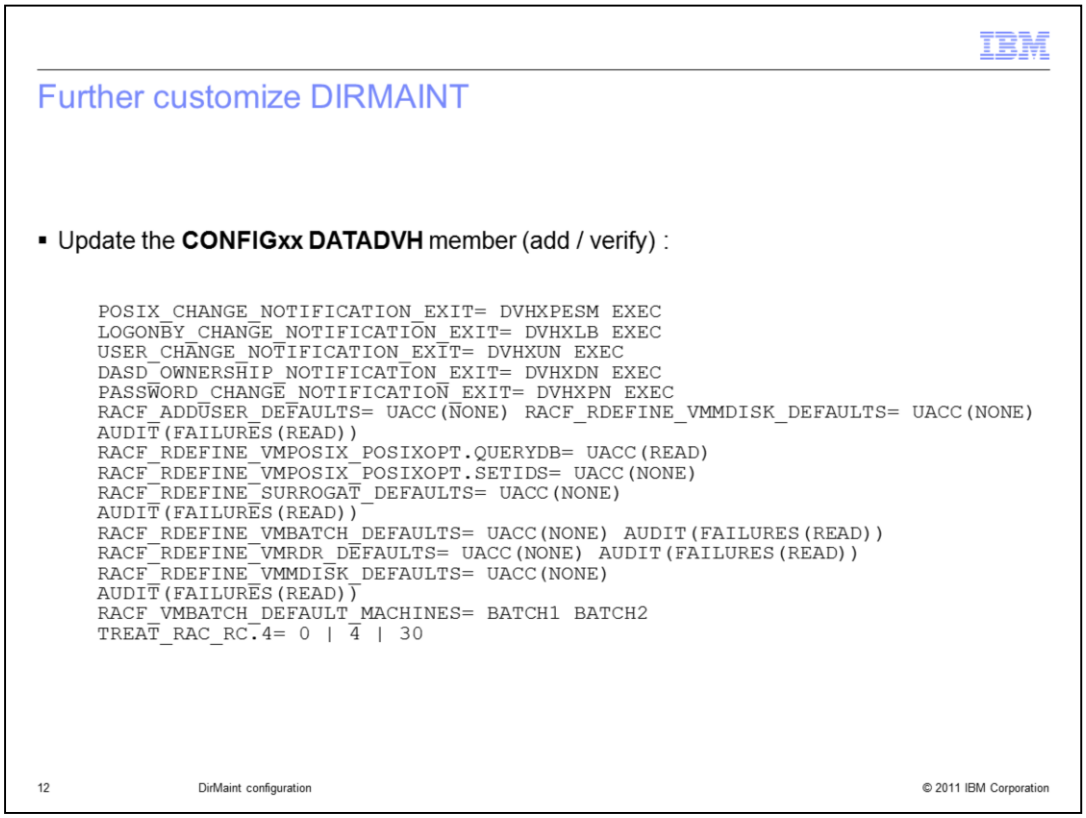
Default directory entries are used to define common definitions for all provisioned guests. This entry is referenced by the Linux prototype directory entry.

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.

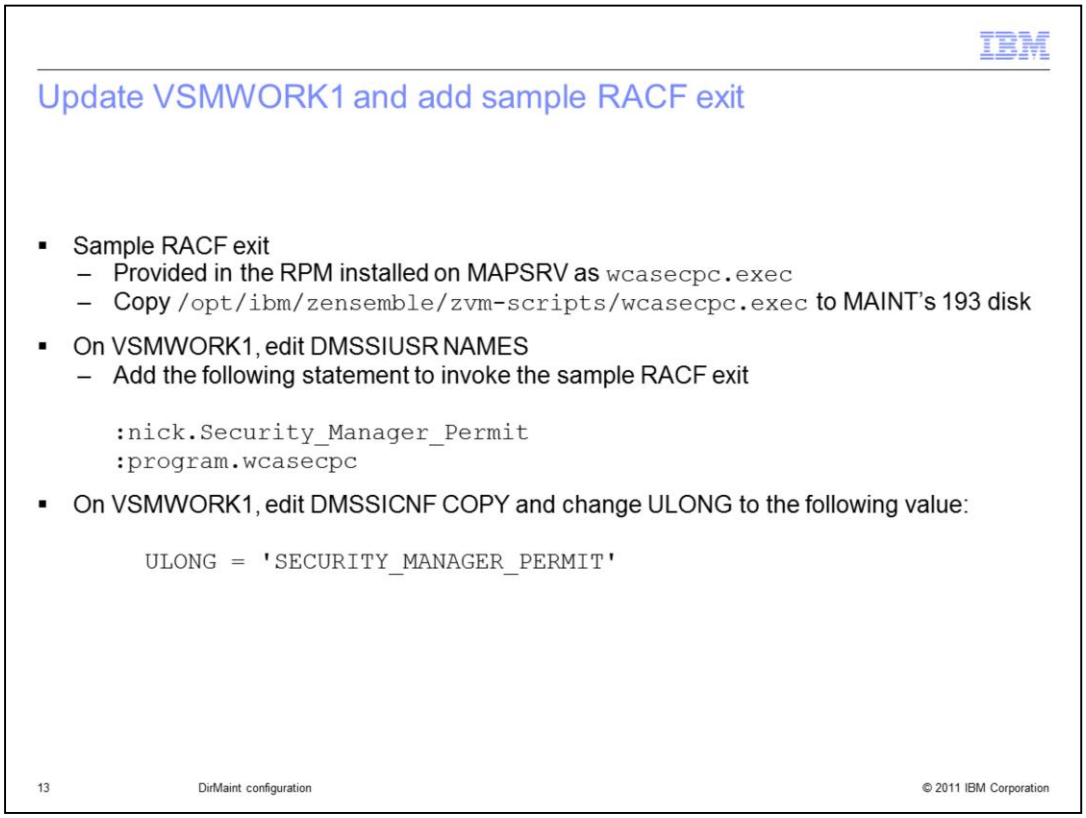


A directory prototype allows provisioned guests to all share common statements. This slide shows the creation of a directory prototype using the LINDFLT directory entry you saw on the previous slide. Note that multiple directory prototypes can be created to support as many configurations as are needed.

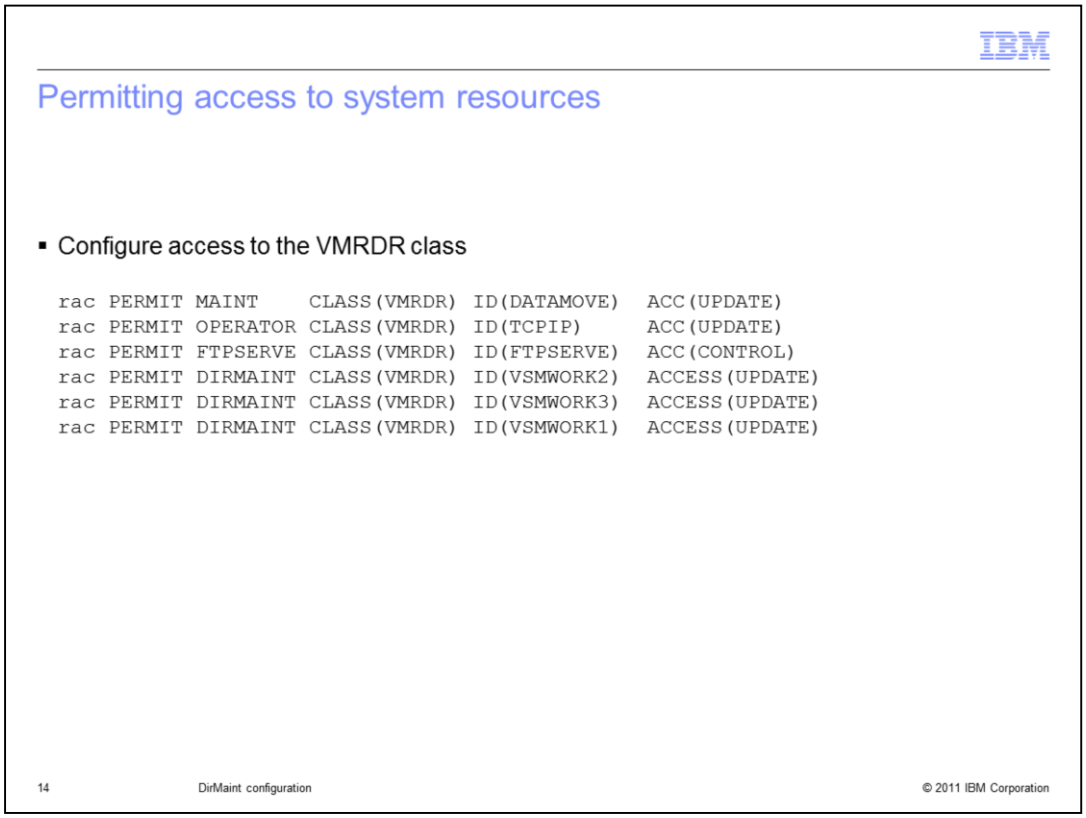
If you use RACF, the system RACF Administrator will need to configure RACF to allow for access to system resources. This section will describe the necessary configurations to use RACF.



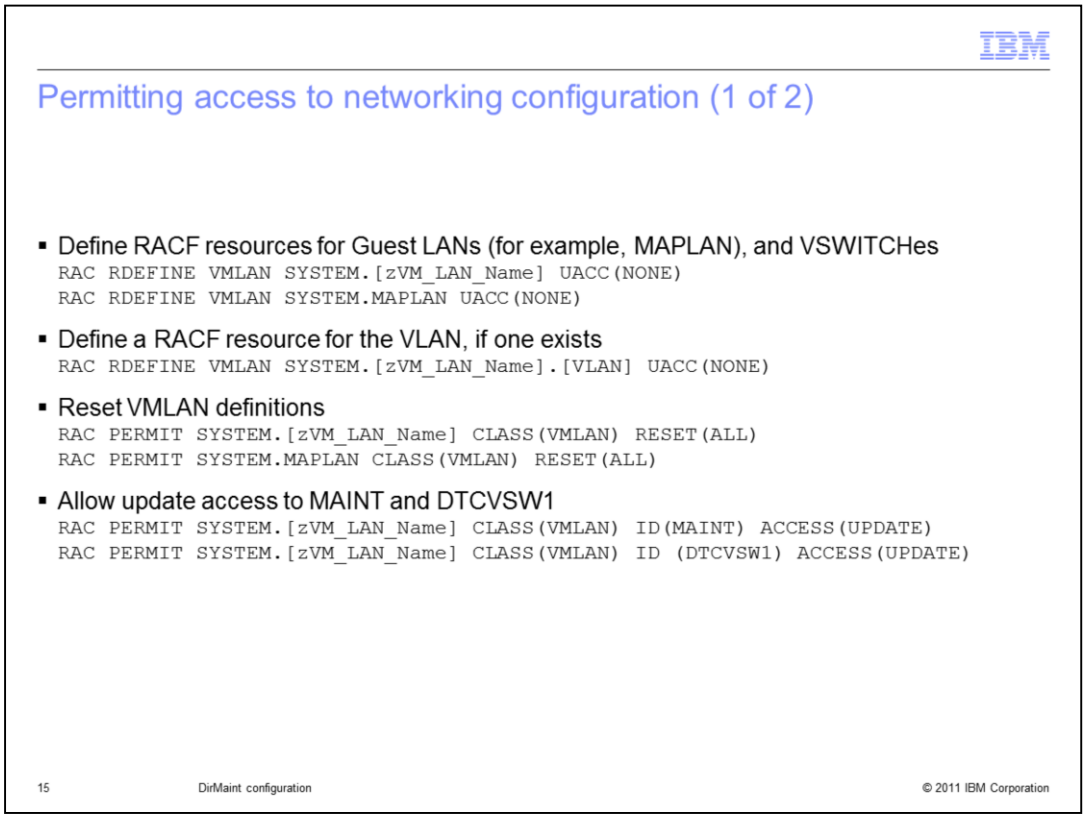
If using RACF as a security manager on the hypervisor where you are utilizing IBM Workload Deployer, DIRMAINT needs to perform ADDUSER/DELUSER RDEFINE/RDELETE commands when the CP directory entries for provisioned servers are created and deleted. The DIRMAINT-RACF relationship present in the default 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.



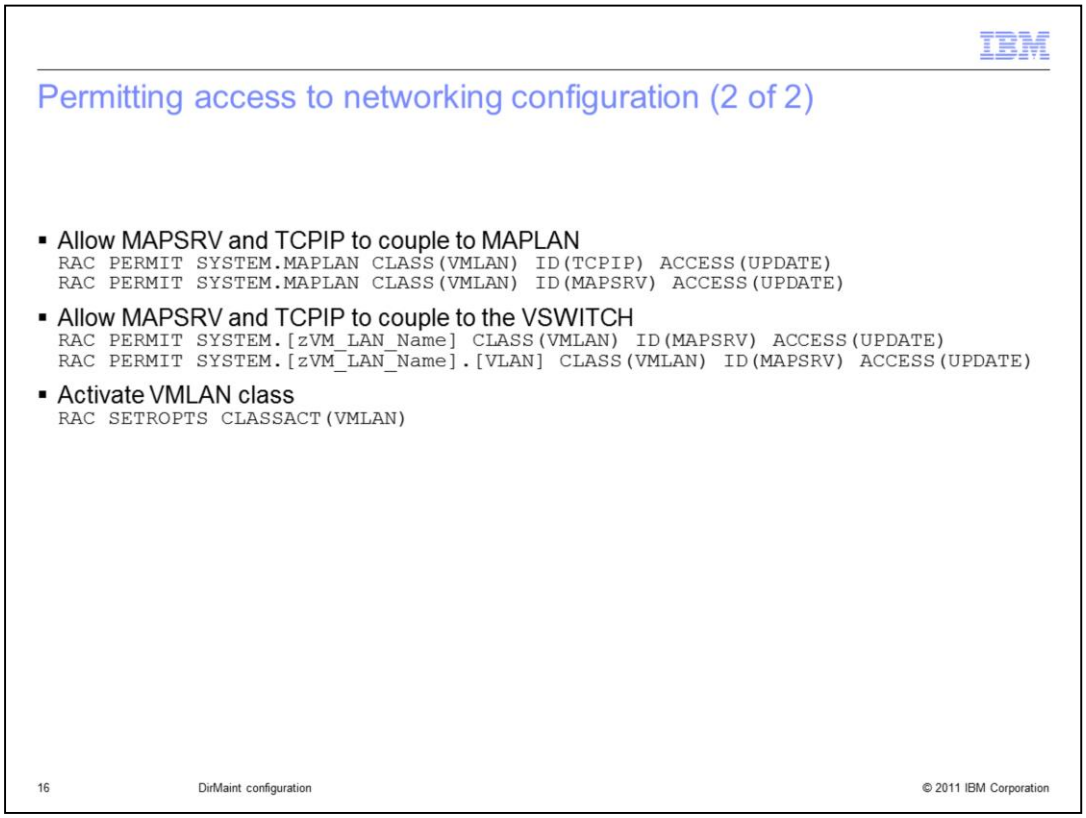
In order to use RACF, a sample RACF exit is provided in the RPM that is installed on the MAPSRV user ID. It is found in the /opt/ibm/zensemble/zvm-scripts directory and needs to be copied to MAINT's 193 disk. To have the exit invoked, you need to update the DMSSIUSR NAME file on VSMWORK1 by adding the 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.



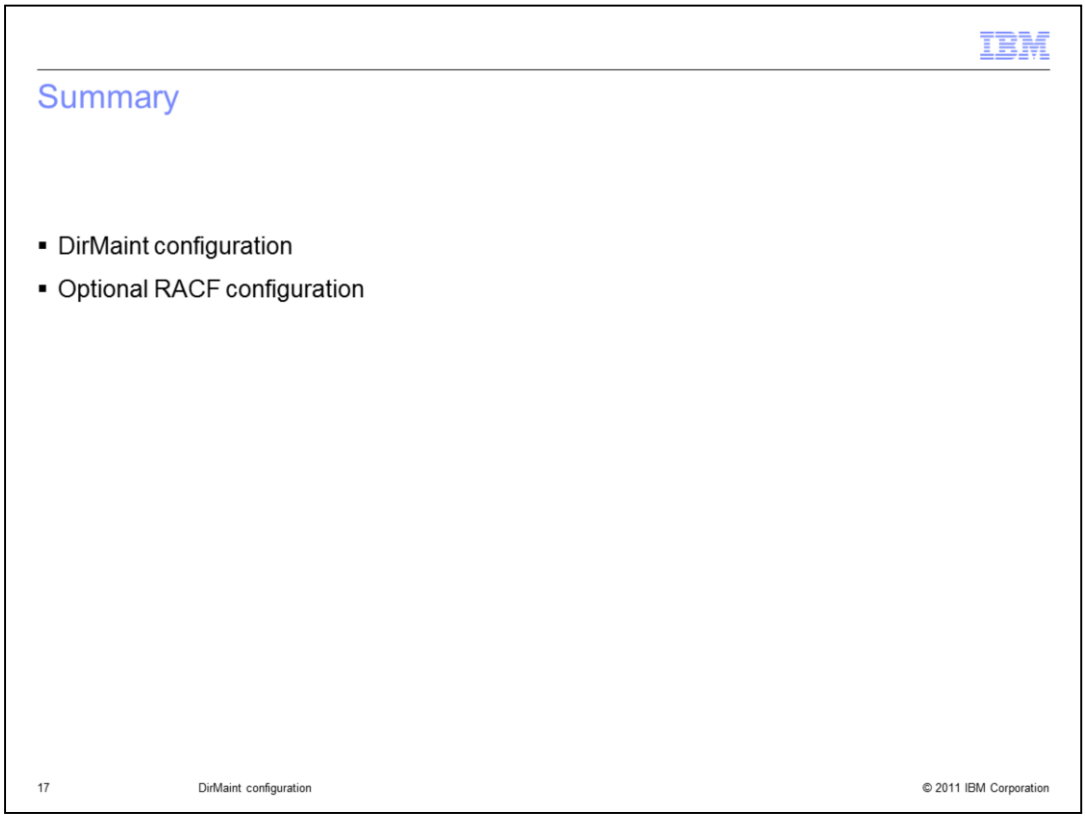
First, it is necessary to grant some user IDs access to the VMRDR class as shown.



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.



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.



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