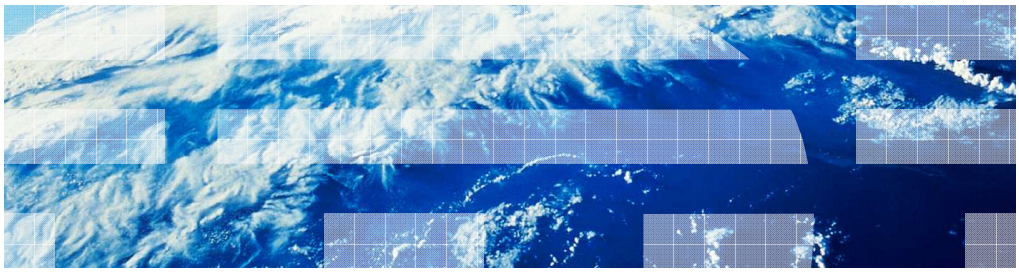
IBM WebSphere CloudBurst Appliance

RACF configuration



WebSphere. software

This presentation will describe the necessary configurations to use RACF®.

Agenda

- Optional RACF configuration

This presentation will discuss additional setup if the RACF Security Server for z/VM is installed on your system.

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

Permitting access to system resources

- Configure access to MAINT, OPERATOR and FTPSERVE readers

```
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)
```

- Allow VSMSERVE to access z/VM parm disk

```
rac setropts generic(vmmdisk)
rac permit maint.cf1 acc(alter) id(vsmserve)
rac permit maint.cf2 acc(alter) id(vsmserve)
```


First, it is necessary to grant some user IDs access to the VMRDR class as shown. The VSMSERVE ID will also need access to the parm disks.

Configuring z/VM networking (1 of 2)

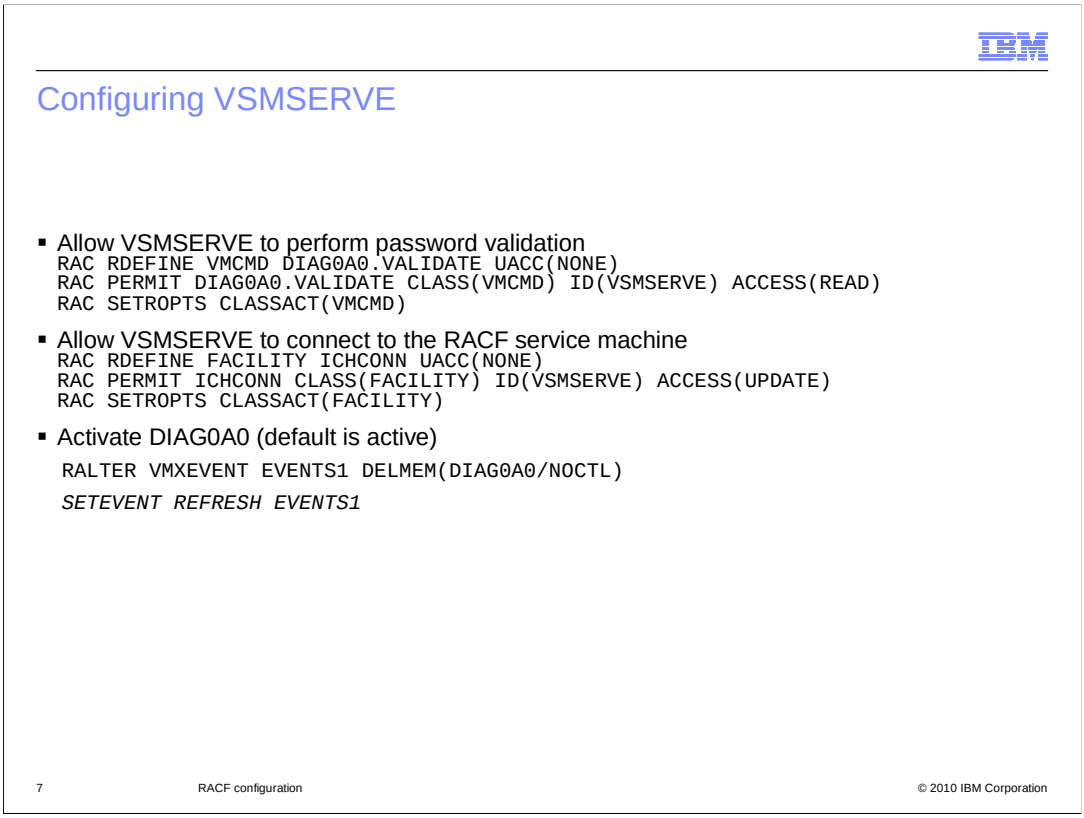
- Define RACF resources for Guest LANs (for example, MAPLAN), and VSWITCHes
```
RAC RDEFINE VMLAN SYSTEM.[zVM_LAN_Name] UACC(NONE)
RAC RDEFINE VMLAN SYSTEM.MAPLAN UACC(NONE)
```
- Define a RACF resource for the VLAN, if one exists
```
RAC RDEFINE VMLAN SYSTEM.[zVM_LAN_Name].[VLAN] UACC(NONE)
```
- Reset 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.

Configuring z/VM networking (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.



VSMSERVE will need to perform password validation of the MAPAUTH user ID and password. Allow this to occur with the DIAG0A0 profile in the VMCMD class. VMSERVE will also need to be able to issue the RACROUTE macro. Permit the VSMSERVE ID to the ICHCONN profile in the FACILITY class to allow this.

If protection for DIAG0A0 is not currently active, activate it by issuing the commands listed above.

Update VSMSERVE DTCPARMS

- Verify these statements exist in the VSMSERVE DTCPARMS file:

```
:Nick.VSMSERVE :Type.server   :Class.VSMAPI
               :ESM_ENABLE.YES
               :PARMS.-E
               :Owner.VSMSERVE
               :Exit.VSMEXIT

:Nick.VSMAPI :Type.class
               :Name.Virtual System Management API server
               :Command.DMSVSMAS
               :Runtime.C
               :Diskwarn.YES
               :ESM_Validate.RPIVAL
:ESM_Racroute.RPIUCMS
```


In order to use an ‘external’ security manager interface (for example, RACF), you will need to update the TCP/IP server definition file for VSMSERVE. Verify that your DTCPARMS file looks like the one shown on the slide.

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 WebSphere® CloudBurst®, 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 summary, this presentation looked at the configuration needed if RACF is being used.

Feedback

Your feedback is valuable

You can help improve the quality of IBM Education Assistant content to better meet your needs by providing feedback.

- Did you find this module useful?
- Did it help you solve a problem or answer a question?
- Do you have suggestions for improvements?

Click to send e-mail feedback:

mailto:iea@us.ibm.com?subject=Feedback_about_CB111_zVMHypervisorConfigurationRACF.ppt

This module is also available in PDF format at: ../CB111_zVMHypervisorConfigurationRACF.pdf

You can help improve the quality of IBM Education Assistant content by providing feedback.

Trademarks, disclaimer, and copyright information