CA-VTERM® for VM

Security Administrator Guide

3.3

Computer Associates®

R104MC33SAE

B01361-1E

Contents

Chapter 1. Resource Functions

The tables on the next two pages list the name, resource, and action of each CA-VTERM function which may be protected by the CA-ACF2 VM or CA-TOP SECRET security software packages. For additional information on the CA-VTERM functions, refer to the *CA-VTERM Operator Guide*. For additional information on the Task Manager functions, refer to the *CA-TASKMAN Systems Programmer Guide.*

To use these tables, select the CA-VTERM function (in the first column) you wish to protect. The second column indicates the resource function you must specify. For CA-ACF2 the resource function is the value you specify in the $KEY control statement. For CA-TOP SECRET, this is the value you insert as the CACMD value.

The Action column indicates the task which you are restricting or allowing.

1.1 CA-VTERM Operator Functions

CA-VTERM Command	CACMD Resource	Action
MSG	prodname.OPER.MSG	Send full-screen messages
OPERATOR	prodname.OPER.OPERATOR	Assign an operator to receive all CA-VTERM messages
PORTS	prodname.OPER.PORTS	Add virtual terminal addresses
QUERY	prodname.OPER.QUERY	Examine status of CA-VTERM tasks
RESET	prodname.OPER.RESET	Reset a CA-VTERM session
TERMINATE	prodname.OPER.TERMINATE	Deactivate CA-VTERM
VSNAP	prodname.OPER.VSNAP	Produce SNAP dumps

Where *prodname* is the value specified in the CA-VTERM PRODNAME system option.

1.2 CA-VTERM User Functions

CACMD Resource	Action
prodname.ADMIN	Perform CA-VTERM administrative functions, such as adding new profiles, and updating system options
prodname.USER.DUPLEX.userid	Initiate a duplex session
prodname.USER.TUTOR.userid	Become the master of a tutor session

Where *prodname* is the value specified in the CA-VTERM PRODNAME system option.

1.3 Messages

Two messages have been added to the CA-VTERM product to handle security violations. These are:

```
CAMC398W WARNING, SECURITY VIOLATION HAS OCCURRED ON xxxxxxxx
CAMC399E ACCESS DENIED BY EXTERNAL SECURITY
```

Consult the *CA-VTERM Message Guide* for the associated reasons and actions.

Chapter 2. Controlling CA-VTERM With CA-ACF2 VM

This chapter discusses protecting your VM system and your CA-VTERM software with CA-ACF2 VM. CA-ACF2 VM is one of the two access control software products from Computer Associates that are described in this guide. The other product, CA-TOP SECRET, is described in the chapter entitled "Controlling CA-VTERM with CA-TOP SECRET."

This chapter describes:

- requirements your system must meet before you can implement CA-ACF2 security with CA-VTERM.
- writing CA-ACF2 rules to protect the operator functions of CA-VTERM.

2.1 Prerequisites

Before you can implement CA-ACF2 security for CA-VTERM, the following conditions must be met:

- You must be running CA-ACF2 Release 3.2 or higher.
- The CA-VTERM service machine must be identified with the @SRF macro (in the ACFFDR) to use the System Request Facility (SRF). Refer to the *CA-ACF2 VM Field Definition Record Generation Manual* for additional information.
- You must turn the SRF Logonid privilege on to allow the CA-VTERM service machine to issue SRF requests to the CA-ACF2 service machine. Refer to the *CA-ACF2 VM User's Guide* for additional information.
- CAS9SEC MODULE, the CAS9M9rr (where *rr* represents the release of CA-ACF2 VM installed) translator module and the ACFSRF LOADLIB must be available to the CA-VTERM service machine. Note that in early CA-ACF2 3.2 GA genlevels, the translator may be called CAM9320. Refer to the ital CA-ACF2 VM Systems Programmer Guide-VM/SP-HPO or *CA-ACF2 VM Systems Programmer Guide-VM/XA* for additional information.
- The resource class (@RESCLAS) must be defined in the ACFFDR. The default is **CACMD,CAC.** You may alter this value in your FDR. For additional information, refer to the *CA-ACF2 VM Field Definition Record Generation Manual*

2.2 Writing CA-ACF2 Rules

CA-ACF2 VM protects all CA-VTERM and CA-TASKMAN functions by default. In other words, you must write a rule permitting a certain function to be performed. If no rule exists, the function cannot be performed.

The syntax for writing CA-ACF2 rules is:

```
$KEY(vtmfunc)
$TYPE(rsrc-code)
 UID(uidmask) permission
```

— or —

```
$KEY(vtmfunc) TYPE(CAC)
 UID(uidmask) permission
```

where

$KEY(vtmfunc) indicates the resource name being protected. *vtmfunc* is the specific CA-VTERM function to which this rule applies. Refer to the chapter entitled "Resource Functions" for a list of valid CA-VTERM functions.

TYPE(rsrc-code) is the resource type code. The default, as defined in the ACFFDR, is CAC.

UID(uidmask) is the mask that defines which users are permitted or denied the authority to issue the CA-VTERM command.

permission specifies the type of permission that applies to the users indicated in the rule. Valid permissions are shown below.

- **Allow** The user is allowed to perform the specified function.
- **Log** The user is allowed to perform the specified function, but the event is logged.
- **Prevent** The user is not allowed to perform the function.

Note: If external security is implemented, then the CA-ACF2 password, not the CA-VTERM password, must be specified on VTRM-1000 at logon.

For more information about writing rules for CA-ACF2 refer to the *CA-ACF2 VM User's Guide.*

Chapter 3. Controlling CA-VTERM With CA-TOP SECRET

This chapter discusses protecting your VM system and your CA-VTERM software with CA-TOP SECRET. CA-TOP SECRET is a Computer Associates security package. Computer Associates other security package, CA-ACF2 VM, is described in the chapter entitled "Controlling CA-VTERM With CA-ACF2 VM."

This chapter describes the prerequisites necessary to implement CA-TOP SECRET security on your system with CA-VTERM. It also explains how to use CA-TOP SECRET administration to protect the operator functions of CA-VTERM.

3.1 Prerequisites

Before you can implement CA-TOP SECRET security for CA-VTERM, be sure you have met the following conditions:

- CA-TOP SECRET VM Release 1.2 (any genlevel), Release 1.1 (any genlevel), or Release 1.0 (genlevel 8905 or higher), should be installed on your VM system.
- If you are running an earlier genlevel of CA-TOP SECRET VM Release 1.0, and do not wish to perform a full refresh to a new genlevel, you may install the following requisite Program Temporary Fixes (PTFs) to support the Standard Security Facility (SSF):

  CO15912 CO16892
  CO16003 CO17607
  CO16494 CO18110
  CO16891

  CO18110 is a new module (the translator) and is available on tape. To obtain these fixes, contact the CA technical support hotline.
- CAS9SEC MODULE, and the CAS9KVrr (where *rr* represents the release of CA-TOP SECRET VM installed) translator module must be available to the CA-VTERM service machine.
- Protect the CA-VTERM functions you choose to control by one of the following methods:
  - Individual CA-VTERM functions may be protected by defining each to the CA-TOP SECRET security database as follows:

    ```
    TSS ADDTO(acid) rescl(resname)
    ```

    where:

    acid Is usually the accessor ID (ACID) of a department (TYPE(DEPT)) or division (TYPE(DIV)).

rescl Is the CA-TOP SECRET resource class to be protected. For CA-VTERM functions the resource class is CACMD.

resname The name (or entity) of the resource within the specified class. This is the CA-VTERM function to be defined to the security data base. Other classes require a userid or schedule name as the resource name.

- You may protect *all* CA-VTERM functions generically by defining the function prefix, PRODNAME.OPER to the database with the following command:

  ```
  TSS ADDTO(acid) CACMD(PRODNAME.OPER)
  ```

- By assigning *default protection* to the CACMD resource class, product internal security may be overridden for all CACMD functions regardless of whether they are defined to the database. That is, all functions will be implicitly protected, although you must define either the individual function or the function prefix as shown above before their use can be authorized.

  Note, however, that this will protect not only CA-VTERM functions but also those used by other CA products. Assigning default protection provides maximum security for your installation.

  You may already have assigned default protection to this resource class. To find out, issue the command

  ```
  TSS LIST(RDT) RESCLASS(CACMD)
  ```

  Default protection may be assigned by the following command:

  ```
  TSS REPLACE(RDT) RESCLASS(CACMD) ATTR(DEFPROT)
  ```

Refer to the *CA-TOP SECRET TSS Command Functions Guide* for additional information on TSS commands.

3.2 CA-TOP SECRET Cross-Authorizations

Cross-authorizations grant users access to resources from logon until log off. Cross-authorizations are established via the TSS PERMIT command function.

The TSS PERMIT command syntax for cross-authorizing CACMD resources is:

```
TSS PERMIT(acid) CACMD(vtrmfunc) ACTION(actions)
```

where:

acid Is the accessor ID of the user that you want to let execute the command.

vtrmfunc Is the CA-VTERM function name to be cross-authorized.

actions Optionally specifies special actions to be taken.

Actions commonly used include:

AUDIT Permits access but records all usage in the Audit/Tracking File.

DENY Explicitly denies this user access to the resource.

FAIL Used with DENY, denies access to all modes.

You can use one command to let a user execute more than one CA-VTERM function (up to a maximum of five functions per entry). For example, the rule below permits user ACCRMZ to add virtual addresses (MCPORTS), reset a CA-VTERM session.

```
TSS PERMIT(ACCRMZ) CACMD(VTERM2.OPER.PORTS,VTERM2.OPER.RESET)
```

Refer to the chapter entitled "Resource Functions" for additional information about CA-VTERM resource types and actions.

You may also use generic prefixing to specify functions.

```
TSS PERMIT(ACCRMX CACMD(VTERM2.OPER)
```

The above rule lets ACCRMZ perform any CA-VTERM function.

Permission may also be grouped in profiles that can be shared by more than one user. The following example shows the creation of a profile, with the ACID VTRMADMN, which will be given to CA-VTERM administrators. All users possessing the VTRMADM profile will inherit the access permissions of the profile. In our example, ACCRMZ is the first user to be ADDed to the VTRMADM profile.

```
TSS CREATE(VTRMADMN) TYPE(PROFILE) DEPT(SYSPROG) NAME('CA-VTERM ADMINISTRATOR')
TSS PERMIT(MCADMIN) CACMD(VTERM2.OPER.PORTS)
TSS ADDTO(ACCRMZ) PROFILE(MCADMIN)
```

Note: If external security is implemented, then the CA-TOP SECRET password, not the CA-VTERM password, must be specified on VTRM-1000 at logon.

For additional information on writing rules, refer to the *CA-TOP SECRET TSS Command Functions Guide.*

Index

Special Characters

A

C

E

M

O

P

R

S