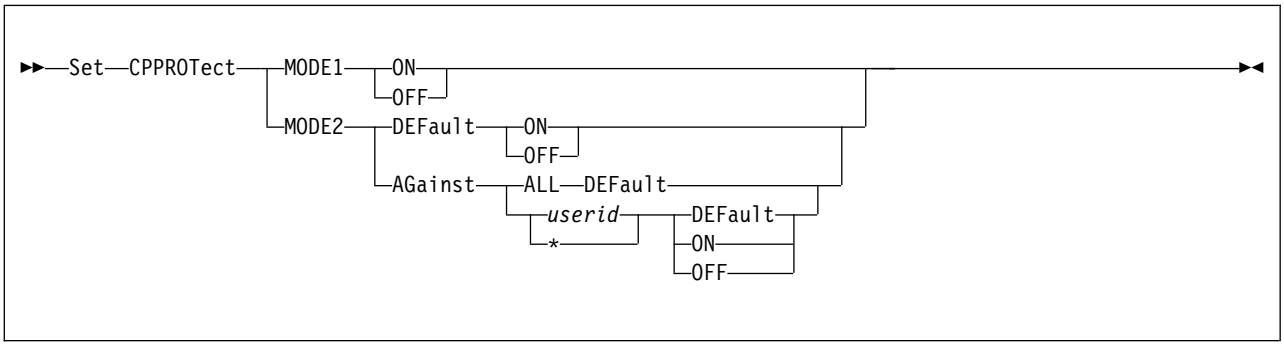
SET CPPROTECT



Authorization

Privilege Class: C

Purpose

Use SET CPPROTECT to control enablement of certain security modes in z/VM, such as limiting speculative execution in the machine. Speculative execution is an optimization mechanism designed into the processor to improve system performance.

The standard virtual machine isolation and protection mechanisms in z/VM are designed to prevent code being run in an unprivileged virtual machine from interfering with or gaining unauthorized access to resources or data owned by the z/VM Control Program or by other guests. Setting CPPROTECT modes ON offers additional protections against information leak attacks that might be attempted by malicious or compromised code running in an untrusted virtual machine. Running the system with MODE1 ON or MODE2 ON might increase system overhead, reduce capacity, or reduce throughput.

z/VM maintains a system-wide MODE1 setting and a MODE2 default setting. When z/VM is IPLed, MODE1 is ON and the default for MODE2 is OFF. In addition to changing the MODE1 setting and the default MODE2 setting, SET CPPROTECT can also establish per-user MODE2 override settings.

In choosing CPPROTECT settings, the system programmer might want to consider the degree to which the code running in virtual machines is known and controlled, the level of risk from unauthorized discovery of data in the memory of CP or other virtual machines, and the performance cost associated with the various protections. For example, an open multitenant cloud platform might call for greater protection than an isolated internal company system.

Details on the protection modes are not provided in this publication. Authorized personnel of IBM clients can consult the IBM Z Security Portal for further information and guidance. To request access to the portal, go to IBM System Integrity - IBM Z (www.ibm.com/it-infrastructure/z/capabilities/system-integrity). Scroll and review information on that page including the Terms and Conditions section. The IBM Z Security Portal section of the page includes links to request access and to obtain the required IBMid.

Operands

MODE1
refers to a system-wide mitigation mechanism that is either ON or OFF.

MODE2
refers to a mitigation mechanism that the z/VM Control Program (CP) can apply when it interacts with some users but not with others. MODE2 protection can be enabled or disabled against all users or against specific users.

DEFault
specifies that the system-wide default is to be set.

AGainst ALL DEFault
specifies that every logged-on user will be set to the default MODE2 setting. All user overrides will be removed.

AGainst *userid*
AGainst *
specifies that a user-specific override is to be set, taking precedence over the system default when the specified virtual machine is run. An asterisk refers to the virtual machine of the command issuer.

AGainst *userid* **DEFault**
cancels the user-specific override for the specified user. Subsequent handling of this virtual machine will be governed by the system-wide default MODE2 setting.

ON
OFF
indicates that a level of protection should be enabled (ON) or disabled (OFF) under the specified conditions.

Usage Notes

1. At z/VM IPL, the MODE1 setting is ON and the default MODE2 setting is OFF. These settings apply to all users on the system. To change these IPL settings, insert the following statement(s) into the directory of the primary system operator user ID (usually OPERATOR):

   ```
   COMMAND SET CPPROTECT MODE1 OFF
   COMMAND SET CPPROTECT MODE2 DEFAULT ON
   ```

   Because the operator is the first user automatically logged on at IPL, this will put the setting into effect before any virtual machine can run.
2. At logon, each user receives the system default MODE2 setting.
3. A user-specific MODE2 override remains in effect until the user logs off. To establish a persistent override for a user, insert the following statement into either the USER or IDENTITY directory entry, or the PROFILE entry included by this entry:

   ```
   COMMAND SET CPPROTECT MODE2 AGAINST * {ON|OFF}
   ```

   This will ensure that the setting is put into effect as soon as the user logs on.
4. If APAR VM65414 or its precursor, VM65396, is installed on the source and destination systems, VMRELOCATE will preserve a user-specific override set for the relocated virtual machine. If either APAR is installed on the source system but neither is installed on the destination system, a user override will be lost in relocation. If either APAR is installed on the destination system but neither is installed on the source system, the relocated guest will inherit the default MODE2 setting on the destination system.
5. Machine support is required to implement MODE1 ON and MODE2 ON. If the support is not available, the requested ON setting will be recorded and will be

preserved by VMRELOCATE as described above but will not be effective on this system. If the necessary machine service is applied dynamically, you can then issue QUERY CPPROTECT to cause CP to recognize the machine support and put the requested settings into effect.

Examples

Assuming a freshly IPLed system with the required machine support and no CP directory COMMAND statements, consider the following sequence of commands:

```
set cpprotect mode1 on
set cpprotect mode2 default off
set cpprotect mode2 against alice on
set cpprotect mode2 against bob off
```

MODE1 will be ON system-wide. MODE2 will be OFF with respect to all users except ALICE: with respect to BOB because of the user-specific override, and with respect to all others because of the system default.

If the following command is subsequently issued:

```
set cpprotect mode2 default on
```

MODE2 remains OFF with respect to user BOB, because of the user-specific override. MODE2 remains ON to protect against ALICE, because of the user-specific override. The rest of the users now run with MODE2 ON, because of the changed system default.

To remove all user overrides, in other words ALICE’s and BOB's overrides:

```
set cpprotect mode2 against all default
```

The user-specific overrides for ALICE and BOB are removed. All users now run with the system default, which in this example is MODE2 ON.

Messages

- HCP002E Invalid operand - *operand*
- HCP003E Invalid option - command contains extra option(s) starting with *option*
- HCP026E Operand missing or invalid
- HCP045E *userid* not logged on
- HCP1056I {MODE1|MODE2} ON request set, but required machine support not available.