

CA VM:Secure

CA VM:SECURE GIVES YOU A COMPREHENSIVE SOLUTION TO SECURE YOUR USER, RESOURCE, DATA AND SYSTEM AUDIT ASSETS. IT ALSO PROVIDES z/VM DIRECTORY, DASD AND SHARED FILE SYSTEM (SFS) MANAGEMENT AND SUPPORT FOR THE IBM SYSTEMS MANAGEMENT APPLICATION PROGRAMMING INTERFACE ON THE z/VM OPERATING PLATFORM.

Overview

Most data centers undergo frequent changes that increase the potential for system security problems. Without a reliable and flexible security foundation, even routine data center changes can create unacceptable exposures.

CA VM:Secure provides a comprehensive solution to secure user, resource, data and system audit assets for the z/VM environment.

Benefits

As a comprehensive security solution, CA VM:Secure gives your IT group the ability to deliver flexible access and enforce rigid safeguards for the z/VM enterprise environment. By securing access to user, resource, data and system audit assets, CA VM:Secure brings together the management of disparate IT exposure points to help you simplify the management of your z/VM security policy.

The CA Advantage

CA VM:Secure enables you to enforce enterprise-wide security practices and password standards across your organization with reliability and flexibility. It is one of several products in the CA VM:Manager™ Management Suite, a group of z/VM solutions that help you govern, manage and secure the z/VM operating environment. As part of CA's vision for Enterprise IT Management (EITM), CA VM:Manager Management Suite helps you unify IT and simplify the management of complex computing operations across your enterprise.

CA VM:Secure Delivers a Comprehensive Security Solution for Your z/VM Users and Resources

Most data centers undergo frequent changes that increase the potential for system security problems. Consolidating data centers, increasing storage, installing connections to other systems, adding new users and upgrading to more powerful hardware all impact the environment that controls access to important information on your network. Without a reliable and flexible security foundation, even routine data center changes can create unacceptable exposures. Your z/VM security strategy must meet the needs of everyone in your organization. Users need simple system access to get their jobs done without unreasonable restrictions. Security auditors need up-to-date information that identifies who owns which resources and who can gain access to them. Management must be assured that sensitive data is protected from intentional and accidental destruction. And, system changes must be managed quickly without putting extra burden on your support staff.

CA VM:Secure provides a complete security and directory management system for z/VM. With it, you can control access to system resources, manage disk space and audit system activity. CA VM:Secure also prevents inadvertent security exposures by automatically maintaining synchronization between the z/VM user directory and your security rules.

Key Capabilities

Access Control

CA VM:Secure gives you complete control over access to all system resources. Using the Rules Facility in CA VM:Secure, you can customize security to meet your company, department, and user needs through rules. These rules permit or deny access to: systems, minidisks, system real storage, other virtual machines, printers, readers and punches, etc.

The Rules Facility also enables you to control CP commands (such as AUTOLOG, LOGON, TAG, SPOOL, TRANSFER, LINK, XAUTOLOG, STCP and STORE HOST) that go through the access control interface (ACI). Additionally, the Rules Facility allows you to control access to tape volumes in a CA VM:Tape catalog and to requests in CA VM:Schedule™.

SECURITY ADMINISTRATOR BENEFITS

- Enforce enterprise-wide security practices automatically
- Identify security offenders
- Produce complete security reports and audit listings

USER BENEFITS

- Improve user productivity with system security that does not interfere with daily work
- Allow users to maintain their own system password
- Permit users to limit access to their minidisks, tapes in CA VM:Tape, and requests in CA VM:Schedule
- Increase user productivity through menus and online help

LOCK OUT UNAUTHORIZED USERS CA VM:Secure monitors invalid logon attempts and records them by user ID and terminal address. When the site-defined threshold for rejected access attempts is reached, the user or terminal is denied system access. This locks out anyone who repeatedly attempts to guess passwords or run password-guessing algorithms to gain unauthorized system access.

ENFORCE PASSWORD STANDARDS CA VM:Secure helps you enforce password standards for your entire user base while still permitting users to maintain their own passwords. This offloads the tremendous burden of password maintenance from your systems' staff. You can set system-wide standards that require users to change their system password on a set frequency. And you can deny password reuse to ensure that old passwords do not become known to other users. When a user password expires, the user is required to supply a new password before being allowed system access. Users can also be permitted to change their passwords at any time, using the full screen menus in CA VM:Secure.

DELEGATE MINIDISK ACCESS CONTROL Using the Rules Facility in CA VM:Secure, users may specify who can link to their minidisks. This capability gives users the control they need without taking up staff time. With a higher level rule, you can force users to supply a password to link to a minidisk owned by someone else, or you can selectively allow links to occur without passwords.

CONTROL TAPE VOLUME ACCESS Your tape data can be as safe as minidisk data. An interface to CA VM:Tape allows users to restrict who can access their tape volumes. You can add another level of tape security by configuring CA VM:Secure to require that each request for tape access be accompanied by a password.

ENCRYPT SENSITIVE DATA Enterprises of all sizes count on z/VM for ironclad security for their confidential data. Through a software implementation of the National Bureau of Standards Data Encryption Standard, CA VM:Secure enables you to encrypt CMS files. Even if everyone in a department has access to the encrypted file, the data is still secure because only certain users are authorized to read it. Users can also encrypt files on their own minidisks.

CA VM:Secure also provides the capability to encrypt logon and minidisk link passwords. This ensures that access passwords are never compromised by being available in plain text on your system. CA VM:Secure has been enhanced to include triple-DES encryption for passwords.

For additional security, you can also encrypt the source directory information. If the minidisk holding these files is ever accessed by an unauthorized person, the information in the source directory database would be unreadable and therefore, more secure. Triple-DES encryption can be used for this purpose.

SECURE THE DIAL COMMAND If you run guest operating systems under z/VM, it may be important to secure the DIAL command. With CA VM:Secure, you can establish rules that limit the use of the DIAL command to specific terminal addresses. You can also set up a DIAL password in the rules database for more flexible security.

Directory Management

SYNCHRONIZE DIRECTORY UPDATES No security system is safe unless it is always maintained to reflect your current user base and authorizations. In z/VM, an often overlooked security problem occurs when directory maintenance and security privileges are managed separately. This is exactly why CA VM:Secure integrates security rules with your z/VM directory. When you delete a user ID from the directory, CA VM:Secure automatically deletes all rules pertaining to that user ID. This prevents a new user from mistakenly inheriting privileges and authorizations that were granted to the previous owner of the user ID.

IMPROVE SERVICE TO USERS The full screen menus and automation of complex procedures provided by CA VM:Secure make directory management simple — so simple, in fact, that you can delegate directory management to others based on their role in your organization. CA VM:Secure allows you to define a directory manager for each group of users on your system. The directory manager can quickly perform routine functions such as defining minidisks, authorizing resource sharing and managing disk space. In addition to providing quick responses to user requests, directory managers can significantly reduce the workload of your system support staff.

SAVE TIME CA VM:Secure updates your z/VM directory faster than any traditional method. Multitasking capabilities allow multiple users to make directory changes simultaneously and directory managers to remain interactive while managing disk space. A WAIT/NOWAIT option saves time for directory managers by letting them regain access to their terminals without waiting for potentially long-running requests to complete.

SFS Support

CREATE SFS FILE POOLS To create a Shared File System file pool, you must define the file pool server and its storage groups, which are collections of minidisks. The CA VM:Secure directory management capabilities include:

- Full screens to walk you through the process
- Automatic location of DASD space for new minidisks
- Fast, reliable directory updates

All directory changes are audited and you can generate a report of those changes to assist you in completing the configuration of the file pool.

ENROLL USERS IN SFS Once a file pool is created, you can enroll users in that file pool. CA VM:Secure provides full screens and line mode commands that make it easy to enroll users and perform other SFS user administration tasks. In addition, CA VM:Secure provides a special MOVE2SFS command that automatically enrolls users, creates appropriate user file spaces and moves the files from the users' minidisks to file spaces.

MOVE MINIDISKS TO SFS Using the CA VM:Secure MOVE2SFS command greatly simplifies the process of moving user minidisks to SFS. When you issue the command, you specify the user ID, the minidisks to be moved, the file pool and other parameters. CA VM:Secure enrolls the user in the file pool, creates SFS file spaces and directories, copies files from minidisks to the directories and sets or adjusts the file space allocation limit. CA VM:Secure even calls a user exit that can perform special functions including notifying affected users and updating applications.

SIMPLIFY SFS ADMINISTRATION With native z/VM, SFS administration is performed by file pool administrators. These administrators have the ability to control all file pool resources and even read from or write to any file in the file pool. Full screens are not provided for file pool administrators and some of their activities are not audited. CA VM:Secure enables you to reduce the number of file pool administrators and improve security. The first step is to make CA VM:Secure a file pool administrator. The next step is to authorize a limited set of users to be CA VM:Secure SFS administrators. By using the full screens and line mode commands, these SFS administrators work through CA VM:Secure to administer the SFS environment to the level of authority that you define. All tasks are fully audited.

DECENTRALIZE SFS USER ADMINISTRATION By authorizing certain users as SFS managers, you reduce the workload for administrators. Each SFS manager is assigned a group of users and can perform tasks including enrolling users in file pools, setting and changing file space allocation limits, and deleting file spaces. Tasks can be performed using full screens or line mode commands that are designed for ease-of-use. SFS administrators always have control because they set limits under which SFS managers operate.

Manage Disk Space

DELEGATE DISK SPACE MANAGEMENT With CA VM:Secure, you can divide real disk volumes into subpools. The subpool resources can then be delegated to directory managers. For example, the system administrator might give 50 or 100 cylinders to an engineering group. The directory managers in that group can then allocate and deallocate minidisks from these cylinders without involving system personnel, again reducing demands on your central system support staff.

AUTOMATE DASD RELOCATION CA VM:Secure automates the tedious and error-prone process of CMS minidisk migration. From a single menu, you can reblock and move user data to a new DASD device and clear the old disk of residual data. You can also identify which DASD contains fragmented free space. Just a simple menu selection is used to move minidisks and maximize the amount of contiguous free space available.

Auditing

MANAGE WITH THE FACTS Management and system auditors can review computer security, space management and directory management with audit information provided by CA VM:Secure. You can obtain detailed audit listings of all access-controlled commands sorted chronologically by user, or even by command. Your security administrator can use these reports to identify violators.

IBM Systems Management Application Programming Interface (API) Support

CA VM:Secure provides back-end support for the IBM Systems Management API component of z/VM by replacing calls to IBM-supplied routines with CA VM:Secure directory management commands. This feature can be easily installed and integrated into an existing CA VM:Secure environment.

Implementation and Use

INSTALLATION CA VM:Secure is easily installed. It requires a few simple text deck replacements in your CP system for rules processing and no modifications to CMS. A simple utility copies and converts your existing source directory to the CA VM:Secure format so that you can automate directory management functions immediately. Advanced features, such as security control of minidisk access, can be implemented in phases. Use of CA VM:Secure to monitor resource access is transparent to users.

PHASE IN YOUR SECURITY SYSTEM You can implement the CA VM:Secure security system all at once or in stages. Phasing in security controls gives your users time to adjust to changes in their environment. Users need not even be aware that a security system has been installed. You can authorize users to have as many or as few privileges as necessary. This flexibility extends to the Rules Facility and gives you the option to define many, few, or no rules at all. The system is as open or closed as you need it to be. You have the choice of centralized directory and security management, or decentralized management by users, managers and administrators in a hierarchical structure. This allows you to retain control over all functions while delegating as many as needed.

EASE-OF-USE User and directory manager screens minimize training needs. With full-screen menus provided by CA VM:Secure, users can change the configuration of their own virtual machines. For example, from the user selection menu, users can change their logon passwords and their minidisk link modes and passwords, define directory links to other users' minidisks, and remove other users' directory links to their minidisks.

CHANGE DASD INFORMATION DYNAMICALLY Adding DASD and changing configuration information is a common system administrator task. You can modify the active configuration while CA VM:Secure remains operational, reducing the risk of a security violation. CA VM:Secure tracks all minidisks on your system and validates dynamic changes to the DASD and other configuration information.

CUSTOMIZE USER EXITS CA VM:Secure provides user exits that allow you to:

- Supply or validate new account numbers
- Control directory links
- Define restrictions or requirements for passwords set by users
- Evaluate and possibly reject rules set by users
- Keep specific terminals (such as the operator console) from being locked out of the system due to invalid passwords
- Keep specific user IDs from being locked out

INTERFACE WITH OTHER APPLICATIONS Applications running on different virtual machines can communicate with CA VM:Secure to change and verify the password of a user ID. This interface is possible through a DIAGNOSE subfunction in CA VM:Secure. It allows you to simplify system access for users by customizing your application. When your application can allow access to its capabilities, using a CA VM:Secure user ID and password verified by this CA VM:Secure interface frees users from having to maintain multiple passwords. Instead, with just a single password, users can get quick access to multiple applications by using just one ID and password.

INTEGRATE DATA CENTER MANAGEMENT TASKS CA VM:Secure interacts with other CA z/VM software products to enhance their functionality in your z/VM data center.

- If CA VM:Secure encounters an unknown account number, it communicates with CA VM:Account™ to check the number. CA VM:Secure then prevents users from charging resources consumed to invalid or unauthorized account numbers.
- When user IDs exceed the CA VM:Account budget limits, CA VM:Secure can change the logon password to NOLOG in the CP source and object directory to prevent further use of the user ID.
- CA VM:Secure provides CA VM:Backup with an abridged version of the CP source directory for producing backup jobs. This eliminates the need for the CA VM:Backup system administrator to have access to all the logon and minidisk passwords.
- The CA VM:Secure surrogate facility also works with CA VM:Batch™ to ensure that batch worker machines assume the privileges of the submitting user ID.
- The CA VM:Secure Rules Facility provides additional security for the SCHEDULE, QUERY, and CANCEL commands in the CA VM:Schedule product.
- You can define CA VM:Secure rules to protect the CA VM:Tape MOUNT, LIST and CATALOG commands.
- CA VM:Secure provides a set of Application Programming Interface (API) commands so that you can create EXECs to automate some of your more tedious directory management tasks.

What's New

CA VM:Director r2.8 SP1 provides support for z/VM 5.4.0 including:

- **z/VM 5.4.0 enhancements to the IBM Systems Management API** Support for new Systems Management API calls that ensures full compatibility with applications that use Systems Management API, such as mainframe Linux provisioning systems.

CA VM:Secure r2.8 provides support for z/VM 5.3.0 including:

- **COMMAND directory statement** The new COMMAND directory statement specifies commands to be issued by the user ID during the logon process. Support for new directory statements is part of CA's commitment to remain current with each new z/VM operating system from IBM.
- **Long password phrases** System security has been enhanced with the availability of long password phrases. Users can specify a long password phrase of a length greater than eight characters, which can consist of upper, and lower case characters, blanks and special characters.

CA VM:Secure supports a maximum long password phrase length of 200 characters. Implementation of long password phrase support into an existing CA VM:Secure system is simple and transparent to your users and there are no new commands to learn. With long password phrases, users can specify easy-to-remember and hard-to-guess phrases. The addition of this support is part of CA's commitment to satisfy modern security requirements introduced by legislation, such as Sarbanes-Oxley. Long Password Phrase support is available with the CA VM:Secure Rules Facility.

- **CHANGE operand on LOGON command** IBM has updated the CP LOGON command to support long password phrases by the addition of the new CHANGE operand. CA VM:Secure supports this new operand.

PRODUCT	FUNCTION	FEATURES	BENEFITS
CA VM:Secure	Access Control to z/VM System Resources	<ul style="list-style-type: none"> ▪ Rules Facility 	<ul style="list-style-type: none"> ▪ Enforce IT-wide security practices automatically ▪ Identify security offenders ▪ Produce complete security reports and audit listings ▪ Allow users control over their own logon and minidisk passwords and access to them ▪ Lock out unauthorized users ▪ Enforce password standards ▪ Encrypt sensitive data ▪ Control tape volume access
	Directory Management	<ul style="list-style-type: none"> ▪ Synchronized directory updates ▪ Control over multiple simultaneous directory updates 	<ul style="list-style-type: none"> ▪ Online directory always reflects the current user base ▪ Security rules always reflect the current user base and obsolete user IDs' rules are automatically deleted ▪ Saves time for users and directory managers
	Manage Disk Space	<ul style="list-style-type: none"> ▪ Delegate disk space management ▪ Automate DASD relocation through menu selections 	<ul style="list-style-type: none"> ▪ Directory managers can be given access to designated subpools of disk space, reducing demands on system support staff ▪ Tedious disk space relocation tasks are eliminated
	Auditing	<ul style="list-style-type: none"> ▪ Security Reports 	<ul style="list-style-type: none"> ▪ Violators of site defined security procedures are easily identified

The CA Advantage

CA VM:Secure is part of the group of z/VM security solutions that help you govern, manage and secure the z/VM operating environment. It supports CA's Enterprise IT Management (EITM) vision, which is to help you unify IT and simplify the management of complex computing environments across your enterprise, by giving you the ability to bring together the management of disparate IT exposure points to make the operation of your z/VM security policy easier and more straightforward.

This security solution is one of the products within a comprehensive portfolio of products that make up CA VM:Manager Management Suite. This product family offers solutions for automated operations, service level management, security, backup and recovery, performance management, and storage management.

To learn more, and see how CA software solutions enable organizations to unify IT and simplify the management of complex computing environments for better business results, visit ca.com/products.