

Avaya Call Management System

Security

Release 16.2
November 2010

© 2010 Avaya Inc. All Rights Reserved.

Notice

While reasonable efforts were made to ensure that the information in this document was complete and accurate at the time of printing, Avaya Inc. can assume no liability for any errors. Changes and corrections to the information in this document might be incorporated in future releases.

Documentation disclaimer

Avaya Inc. is not responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. Customer and/or End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation to the extent made by the Customer or End User.

Link disclaimer

Avaya Inc. is not responsible for the contents or reliability of any linked Web sites referenced elsewhere within this documentation, and Avaya does not necessarily endorse the products, services, or information described or offered within them. We cannot guarantee that these links will work all the time and we have no control over the availability of the linked pages.

Warranty

Avaya Inc. provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available through the Avaya Support Web site:

http://www.avaya.com/support

License

USE OR INSTALLATION OF THE PRODUCT INDICATES THE END USER'S ACCEPTANCE OF THE TERMS SET FORTH HEREIN AND THE GENERAL LICENSE TERMS AVAILABLE ON THE AVAYA WEB SITE http://www.avaya.com/support/LicenseInfo ("GENERAL LICENSE TERMS"). IF YOU DO NOT WISH TO BE BOUND BY THESE TERMS, YOU MUST RETURN THE PRODUCT(S) TO THE POINT OF PURCHASE WITHIN TEN (10) DAYS OF DELIVERY FOR A REFUND OR CREDIT.

Avaya grants End User a license within the scope of the license types described below. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the Documentation or other materials available to End User. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users. "Software" means the computer programs in object code, originally licensed by Avaya and ultimately utilized by End User, whether as stand-alone Products or pre-installed on Hardware. "Hardware" means the standard hardware Products, originally sold by Avaya and ultimately utilized by End User.

License type(s)

Designated System(s) License (DS). End User may install and use each copy of the Software on only one Designated Processor, unless a different number of Designated Processors is indicated in the Documentation or other materials available to End User. Avaya may require the Designated Processor(s) to be identified by type, serial number, feature key, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A "Unit" means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Product that permits one user to interface with the Software. Units may be linked to a specific, identified Server.

Copyright

Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights. Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

Third-party components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information identifying Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site:

http://www.avaya.com/support/ThirdPartyLicense

Preventing toll fraud

"Toll fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of toll fraud associated with your system and that, if toll fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya fraud intervention

If you suspect that you are being victimized by toll fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support Web site:

http://www.avaya.com/support

Trademarks

Avaya and the Avaya logo are either registered trademarks or trademarks of Avaya Inc. in the United States of America and/or other jurisdictions.

All other trademarks are the property of their respective owners.

Downloading documents

For the most current versions of documentation, see the Avaya Support Web site:

http://www.avaya.com/support

Avaya support

Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Support Web site:

http://www.avaya.com/support

Contents

Preface . . . 7
Purpose . . . 7
Intended users . . . 7
Overview . . . 8
Conventions and terminology . . . 9
Reasons for reissue . . . 9
Documentation Web sites . . . 9
Support . . . 10

Avaya CMS security . . . 11
Operating system hardening . . . 11
Third party security and management packages/tools . . . 12
Patching and patch qualification . . . 12
Operating System level security logs and audit trails . . . 12
Altering the ssh, telnet and ftp network service banners . . . 13
Banner modifications . . . 13
E-mail and SMTP . . . 14
DNS and NFS . . . 14
User file permissions and masks . . . 15
Support for KVM and headless CMS systems . . . 15
Authentication and session encryption . . . 15
User authentication and authorization . . . 16
Password complexity and expiration . . . 18
Enabling password aging . . . 18
Using passwd_age . . . 18
Lockouts and logging for failed logins . . . 19
Session timeouts and multiple-login prevention . . . 20
Encryption (including FIPS considerations) . . . 20
Use of telnet, ftp, tftp, rsh . . . 20
Using ssh within CMS . . . 21
SSH on R12 and R13/R13.1 . . . 22
CMS application security . . . 23
SPI link . . . 23
Application-level audit logging . . . 24
Backup and restore support . . . 24
Database security controls . . . 24
Physical Security . . . 25
Physical server protection . . . 25
EEPROM security . . . 25

Services security and CMS support 25
Remote connectivity and authentication 26
Services password management 26
Reviewing log files 26
Adding a firewall 26
Transmitting passwords 27

CMS version specific security 29
Limiting external access to UNIX services 29
Solaris services that can be disabled 30
Additional OS hardening 31
Firewall traversal considerations / Open ports (R12 and later) 32
Optional ports: 32
New security enhancements with R15 (r15ab.d and later) 33
Other (optional) scripts provided with r15ab.d and r15auxab.d 34
Changing the default password encryption algorithm on Solaris™ 35
Description 35
Steps to Follow 35
Implementation 36
Verify 37
Enabling long passwords in Solaris™ 10 38
Manual password complexity changes for R15 and Later (optional) 39
Changes to /etc/default/login 39
Security enhancements included with R16 and later 41
Basic Audit Reporting Tool 42
BART Components 42
BART Manifest 42
BART Report 43
BART Rules File 43
Basic Example of using BART 44
Permission and Ownership Changes 44
Make all cron entries use umask of 077 45
The /cms filesystem is mounted with nosuid option 45
Modify permissions of CMS user home directories as created by CMS application 46
Optional scripted security enhancements 46
Audit controls and logadm changes for rotation of audit logs 47
Controlling who can connect to the CMS system 48
Restricting access to the database 49

Appendix A: Enabling and Disabling Services in Solaris 9 and 10 53
Solaris 10 53
Service Management Facility (SMF) 53
svcs command 54
svcadm command 55
Solaris 9 60
The inetd configuration file 61
Limiting services to your machine to specific addresses 61
To disable a network service completely 61
CMS permissive use support policy 62
Links to Avaya security resource 64

Appendix B: CMS security/Hardening offer 67
CMS security / Hardening offer 67

Preface

Avaya Call Management System (CMS) is an application for businesses and organizations that use Avaya communication servers to process large volumes of telephone calls using the Automatic Call Distribution (ACD) feature. Avaya CMS supports solutions for routing and agent selection, multi-site contact centers, remote agents, reporting, interfaces to other systems, workforce management, desktop applications, system recovery, and quality monitoring.

Avaya CMS is part of the Operational Effectiveness solution of the Avaya Customer Interaction Suite.

This section includes the following topics:

- Purpose on page 7
- Intended users on page 7
- Overview on page 8
- Conventions and terminology on page 9
- Reasons for reissue on page 9
- Documentation Web sites on page 9
- Support on page 10

Purpose

The purpose of this document is to describe how to implement security features in Avaya CMS.

Intended users

This document is written for:

- Avaya support personnel.
- Avaya factory personnel.
- Contact center administrators.

Users of this document must be familiar with Avaya CMS and the Solaris operating system.

Overview

This document includes the following topics:

- Avaya CMS security on page 11

  This topic discusses the common security features available in CMS across all releases.

- CMS version specific security on page 29

  This topic discusses security features available in CMS in each version. It discusses in detail the progression in security aspects of CMS with new releases.

- Enabling and Disabling Services in Solaris 9 and 10 on page 53

  This topic discusses the facilities provided by Solaris 9 and Solaris 10 to enable and disable system services.

Conventions and terminology

If you see any of the following safety labels in this document, take careful note of the information presented.

CAUTION:
Caution statements call attention to situations that can result in harm to software, loss of data, or an interruption in service.

WARNING:
Warning statements call attention to situations that can result in harm to hardware or equipment.

DANGER:
Danger statements call attention to situations that can result in harm to personnel.

SECURITY ALERT:
Security alert statements call attention to situations that can increase the potential for unauthorized use of a telecommunications system.

Reasons for reissue

This document includes the following update:

- Information on security features in CMS.

Note:
Oracle Corporation now owns Sun Microsystems. Instead of rebranding references to Sun Microsystems with the Oracle name, all occurrences of Sun and Sun Microsystems will remain as is in this document.

Documentation Web sites

All CMS documentation can be found at http://www.avaya.com/support. New issues of CMS documentation will be placed on this Web site when available.

Use the following Web sites to view related support documentation:

- Information about Avaya products and service

  http://www.avaya.com
- Sun hardware documentation

  http://docs.sun.com

Support

Contacting Avaya technical support

Avaya provides support telephone numbers for you to report problems or ask questions about your product.

For United States support:

1- 800- 242-2121

For international support:

See the Support Directory listings on the Avaya Web site.

Escalating a technical support issue

Avaya Global Services Escalation Management provides the means to escalate urgent service issues.

Avaya CMS security

This document covers security-related information and configuration settings in the Solaris Operating System and Call Management System (CMS) applications that interest customers. This chapter covers the following topics:

- Operating system hardening on page 11
- Authentication and session encryption on page 15
- CMS application security on page 23
- Physical Security on page 24
- Services security and CMS support on page 25

Operating system hardening

The services discussed here can be disabled by customers, business partners, or professional services associates. Avaya provides support for disabling services only if the customer-documented procedures in the administration guide have been followed. Avaya Professional Services also provides a security hardening offer, discussed later, that can upgrade CMS systems to current hardening levels. This results in additional customizable security scripts and features, such as preventing more than one login by a user or an automatic session timeout. The hardening offer is available for CMS systems r3v9 and later. CMS R15 systems must be on load r15ab.d (r15auxab.d) or later. The only R15 load before r15ab.d was r15aa.m or r15auxaa.m. For more information on security features for different versions of CMS, see chapter CMS version specific security on page 29.

Operating system (OS) hardening can be achieved in the following ways:

- Third party security and management packages/tools on page 12
- Patching and patch qualification on page 12
- Operating System level security logs and audit trails on page 12
- Banner modifications on page 13
- E-mail and SMTP on page 14
- DNS and NFS on page 14
- User file permissions and masks on page 14
- Support for KVM and headless CMS systems on page 15

Third party security and management packages/tools

Traditionally, viruses do not target Solaris. However, several antivirus and other security software for Solaris are now available. Avaya does not support the use of such software on the CMS product as it can severely impact performance.

The Avaya Permissive Use Support Policy for customers who require third party software to be installed on their CMS system is reproduced in CMS permissive use support policy on page 62.This policy is subject to change in the future releases of CMS.

Patching and patch qualification

Avaya continuously monitors security alerts from a variety of sources, analyzes potential product impact, and posts appropriate product advisories at the Avaya Product Security Support web site, http://support.avaya.com/security. Customers can register at this web site to receive automatic notification of new and updated security advisories.

Avaya Labs conducts research and participates in international activities of security bodies, creating best practices for product development groups. Products are measured against such best practices, and improvements regularly made based on these assessments.

CMS includes all necessary components including security patches at the time of release. Avaya receives additional patch notifications from Sun Microsystems and certifies new Solaris OS patches. Then, Avaya assembles the Sun patch clusters and makes these available to customers. Avaya also updates security advisories with instructions on downloading and applying these certified patches when they are made available on the Avaya support Web site. Installation of patches is a customer responsibility unless specified otherwise in a premium services contract. Customers must contact services if they have questions regarding a specific patch.

Only the Avaya approved Solaris patches must be installed. All Sun Solaris patches are not required or fit for use on the CMS system as it does not incorporate all aspects of the Solaris OS. Installing non-Avaya-recommended Solaris patches can cause problems with the CMS server.

Note:

Avaya approves installation of Solaris kernel patches through the baseload or version upgrade process. The kernel patches are not released through any other method.

Operating System level security logs and audit trails

Log files can be used to detect suspicious system activity. The customer can review the following log files on a routine basis for signs of unusual activities:

- `/var/adm/messages`. This log includes system messages (syslog), including failed login attempts if `auth.debug` is enabled in `/etc/syslog.conf`.
- `/var/adm/sulog`. This log contains su records for access to root privileges.
- `/var/cron/log`. This log contains cron records for automated scripts run under the cron process.

New auditing options are discussed in the Security enhancements included with R16 and later on page 41.

Altering the ssh, telnet and ftp network service banners

Altering the telnet and ftp network service banners hides operating system information from individuals who want to take advantage of known operating system security holes.

To alter the telnet and ftp network service banners:

1. Create or edit the file /etc/default/telnetd.
2. Add the line:

   `BANNER="CMS OS"`

   Important:
   Add a blank line before and after the BANNER="CMS OS" line. If you do not, the Avaya CMS system will not display the CMS OS message correctly. When users either telnet or ftp to the CMS, the users will see a message similar to the following example:
3. Save the file.
4. Change the file permissions to 444.

Banner modifications

You can modify the banners displayed on login to any CMS system to obscure OS or application information or display legal access warnings.

Displaying a restricted warning for telnet users performs the following functions:

- Displays your corporate policy for illegal computer activity
- Scares off individuals who want to access a system illegally
- Allows you to prosecute an individual who has illegally accessed the system

To display a restricted warning for telnet users:

1. Create or edit the file /etc/issue

   ```
   # telnet cms_box
   Trying 192.168.1.22...
   Connected to cms_box.
   Escape character is '^]'.
   CMS OS
   ```

2. Add a message similar to the following:

   ```
   WARNING: This system is restricted to Company Name authorized users for
   business purposes. Unauthorized access is a violation of the law. This system
   may be monitored for administrative and security reasons. By proceeding, you
   consent to this monitoring.
   ```

   When users connect to the Avaya CMS system using network services, the system displays the warning message. A user would see the message if they telnet into the Avaya CMS system.

3. Save the file.
4. Change the file permissions to 644.

E-mail and SMTP

You must not configure CMS as a mail relay and not enable the Simple Mail Transfer Protocol (SMTP) daemon. You must reconfigure the SMTP daemon accordingly on older CMS systems (pre-R12).

DNS and NFS

In general, there is no support for sharing file systems to and from CMS system and you must disable associated daemons on older CMS systems. If `hosts.allow` and `hosts.deny` (or `.rhosts`) files are used for access control, any servers or files that control name resolution (Domain Name Servers or entries in the `/etc/hosts` file) are under appropriate administrative control within the customer network. This prevents an attacker from leveraging DNS services to enter a system.

User file permissions and masks

You can configure older CMS systems (pre-R12) with default file creation masks that customers consider excessively permissive. If this is a concern, the customer can implement the CSI Hardening Offer or upgrade to get the default umask set to 022. Due to limitations in the CMS system, a more stringent umask cannot be supported without impacting product functionality.

Support for KVM and *headless* CMS systems

It has come to the attention of Avaya that several customers have requested support for *headless* and/or KVM solutions for CMS systems. CMS does not support the use of *headless* or KVM solutions for CMS systems. Use of these solutions is only by *Permissive Use*. See the *Permissive Use* policy in CMS permissive use support policy on page 62.

Note:
If a customer insists on using a KVM for a CMS, it is suggested that they look at Network Technologies Incorporated (NTI) KVM switches. The NTI brand KVM switches seem to work better than other KVM switches for Sun SPARC systems.

Authentication and session encryption

This section covers the following topics:

- User authentication and authorization on page 15
- Password complexity and expiration on page 17
- Lockouts and logging for failed logins on page 19
- Session timeouts and multiple-login prevention on page 19
- Encryption (including FIPS considerations) on page 19
- Use of telnet, ftp, tftp, rsh on page 20
- Using ssh within CMS on page 20

User authentication and authorization

CMS uses login and password security measures within the Solaris OS and provides multiple levels of system access. To authenticate users, CMS uses Solaris capabilities, based on Pluggable Authentication Modules (PAM). At the system level, standard UNIX permissions are used. Within CMS, data permissions are administered per user.

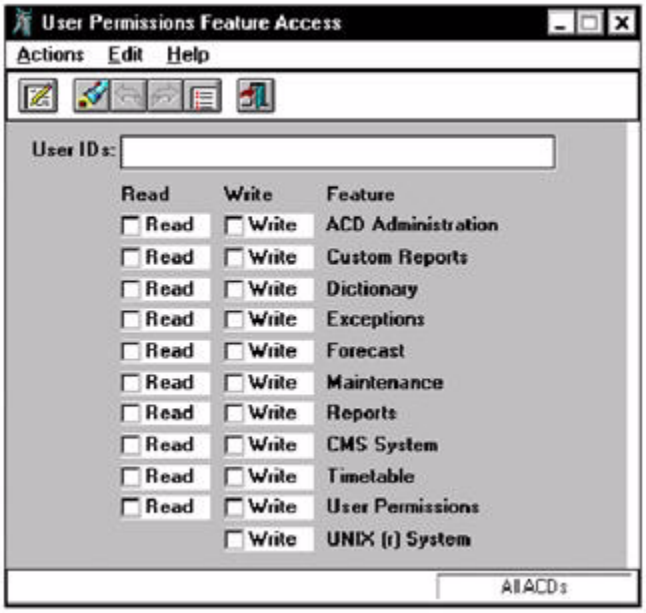
When you create a user in Call Management System, you provide the user either administrator or user access rights. As an administrator, your ability to modify the configuration of a CMS server is limited to the feature permissions provided to you. CMS user accounts are not permitted to make administrative changes unless they have been given the required feature permissions. Ordinary CMS users are not provided OS privileges and can be limited within the application, to particular skills, VDN, and trunk groups. Avaya also implements feature controls that must be unlocked in order to access the feature.

Using PAM configuration files, Solaris allows for integration with external authentication within a UNIX domain using a Network Integration Service (NIS or NIS+). CMS does not support add-on authentication packages for other external authentication services for Solaris. Use of external authentication can bypass local rules configured for password expiration and complexity, such as the settings within the two OS files /etc/passwd and /etc/shadow.

Avaya Access Security Gateway (ASG) software can authenticate Avaya Services and other remote users. This mechanism supports a one-time password. The system presents the user with a challenge string to which they respond with a string generated by a software tool, based on the challenge and product identification information.

You can define the following access permissions for each user login and password in CMS:

- ACD Access: User can assign, view, delete, and modify another user's ability to gain access to more than one real or pseudo ACDs. You can also turn on or off the exceptions notification for ACDs in this window.
- Feature Access: User can assign, view, or modify user access permissions for the CMS subsystems such as Reports, Dictionary and Exceptions and certain function key (SLK) menu items, such as UNIX system/Solaris system and Timetable. The access permissions given to a user affect what that user is able to do with CMS.



- Main Menu Addition Access - User can assign, view, or modify other users' access permissions for the additional menu items of your choosing. These items can provide access to your local electronic mail environment or daily news articles about your call center for agents or split/skill supervisors.

- Split/Skill Access - User can assign, view, modify, or delete another user's permissions to specific splits/skills. Split/Skill Access permissions determine your ability to access and administer agent/queue data for a particular split or skill. You must also turn on or off the exceptions notification for splits/skills in this window.
- Trunk Group Access - User can assign, view, modify, or delete another user's access permissions to specific trunk groups. Trunk Group Access permissions determine a user's ability to access and administer data for a particular trunk group. You must also turn on or off the exceptions notification for trunk groups in this window.
- User Data - User can assign CMS user IDs, specify a default printer,specify whether the user is an administrator, or a normal user such as a splits/skill supervisor, and administer the maximum number of open windows, the minimum refresh rate for real-time reports, and the default login ACD.
- VDN Access - User can assign, view, modify, or delete another CMS user's access permissions to specific VDNs. VDN access permissions determine a user's ability to administer VDNs with the various CMS subsystems and to access report/administration data for VDNs.
- Vector Access - User can define vector access permissions. These permissions specify the user's ability to administer vectors and to access report/administration data for vectors. Use to assign, view, modify, or delete a CMS user's access permissions to specific vectors.

Password complexity and expiration

In Call Management System R9 and later, you can enable and modify the password expiration attributes through the CMSADM menu. You can set the expiration intervals from 1 to 52 weeks, and the Solaris parameters in MINWEEKS, MAXWEEKS, and WARNWEEKS. For detailed instructions for configuring aging, see Enabling password aging on page 17.

Some custom integrations and configurations with scripted passwords can require careful application of password expiration settings. For this, you must always use the CMSADM script. Avaya does not recommend direct administration of password aging through Solaris.

Enabling password aging

Password aging forces users to change their passwords on a regular basis.

Using passwd_age

Use the `passwd_age` option to turn password aging on or off. If password aging is on, users will be prompted to enter a new password after a predetermined time interval has passed. Password aging is off by default.

CAUTION:
If you have any third party software or Avaya Professional Services (APS) offers, do not turn on password aging. Contact the National Customer Care Center (1-800-242-2121) or consult with your product distributor or representative to ensure that password aging will not disrupt any additional applications.

The `passwd_age` option will effect the passwords of all Avaya CMS users and regular UNIX users. When password aging is on, the Solaris policy file `/etc/default/passwd` is modified. The passwords of all Avaya CMS users that use the `/usr/bin/cms` shell and all UNIX users will age. If password aging is on when a new user is added, the user's password begins to age as soon as a password is entered for that account. You must exclude specific users before turning password aging on in order to prevent additional password administration. To prevent the aging of a specific user's password, see Adding and removing users from password aging and Troubleshooting password aging sections in *Avaya CMS Software Installation, Maintenance and Troubleshooting*.

Important:
Non-CMS users such as `root`, `root2`, or `informix` will not age. Password aging will not function on an Avaya CMS system that uses a NIS, NIS+, or LDAP directory service. If you are using NIS, NIS+, or LDAP, contact your network administrator. The passwords will need to be aged from the server running the directory service.

To use the `passwd_age` option:

1. Enter:

   `cmsadm`

   The system displays the CMSADM menu.

2. Select number for “passwd_age” menu item.

   The system displays the following message:

Note:
The system will also display a message that indicates that password aging is off or the current password aging schedule. You can enter q at any point to exit the password aging options.

3. Perform one of the following actions:

- To turn password aging on:

  a. Enter: 1

  The system displays the following message:

  b. Enter the number of weeks before passwords expire and users are prompted to enter a new password. The range is from 1 to 52 weeks.

- To turn password aging off:

a. Enter: 2

The system displays the following message:

b. Perform one of the following actions:

- To turn password aging off, enter: yes
- To leave password aging on, enter: no

- To change the password aging interval:

a. Enter: 3

The system displays the following message:

b. Enter the number of weeks before passwords expire and users are prompted to enter a new password. The range is from 1 to 52 weeks.

See the Manual password complexity changes for R15 and Later (optional) on page 39 for more options for R15 and later systems.

Lockouts and logging for failed logins

CMS does not currently support account lockouts, but if you enable `auth.debug` in `/etc/syslog.conf`, you can log the failed login attempts in the system message log (`syslog`).

R15 and later have added options that handle this to a certain extent. See Other (optional) scripts provided with r15ab.d and r15auxab.d on page 34.

Session timeouts and multiple-login prevention

By default, no timeouts exist for agent or administrator login sessions on the CMS system. However, you can configure a cron job for this purpose. Avaya also offers a custom hardening service that you can use to create an equivalent function. In addition, the CSI hardening offer prevents a login from being used more than once concurrently.

See more details on this hardening offer in CMS security/Hardening offer on page 67.

Encryption (including FIPS considerations)

The CMS system has not been formally FIPS-approved but it can use FIPS-based algorithms and key lengths within the SSH family of protocols (ssh, sftp) as long as the SSH server and client configurations are set to use FIPS-approved cryptosuites (the specific algorithm is negotiated between client and server). Selection of an algorithm takes place at run time. SSH uses RSA or DSA. The default encryption used is RSA and key length of 1024 bits.

Standard UNIX one-way password encryption is used within the `/etc/shadow` file.

For R15 and later systems, the Standard UNIX one-way password encryption can be changed to the md5 method using the instructions in Changing the default password encryption algorithm on Solaris™ on page 35. If you have an Oracle/Sun account you can refer directly to the Oracle document at http://sunsolve.sun.com/search/document.do?assetkey=1-71-1001835.1-1.

Use of telnet, ftp, tftp, rsh

Traditionally, computer-based CMS clients, such as Supervisor, Terminal Emulator, and Network Reporting, use telnet to interface with the CMS server. Do not use telnet for communication over a network because it is an insecure protocol. For example, in telnet, passwords are exchanged in clear text.

Therefore, Avaya has created a secure alternative for several customers. This alternative is now available in CMS Supervisor R13, and later. Terminal Emulator, R15 and later, also has this capability. Network Reporting uses telnet as the only connection option. In the case of tftp and rsh, these protocols are unauthenticated (or easily spoofed). So use the secure equivalents, such as ssh and sftp.

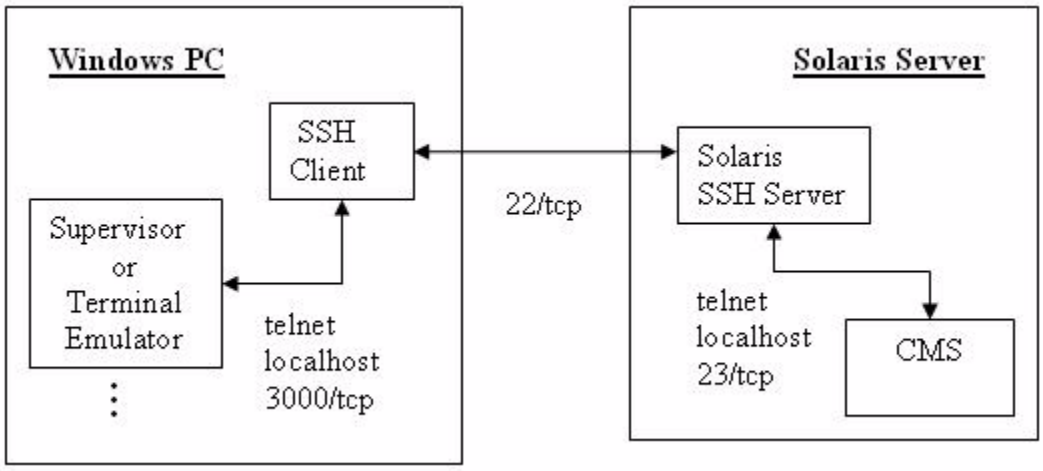
To limit interactive access, you must always provision ordinary users with the `/usr/bin/cms` shell.

Using ssh within CMS

CMS R13 and later deliver simplified installation of a secure Supervisor client login over a public or unsecured network. To do this, CMS uses Secure Shell (SSH), a protocol that encrypts the packets sent between a client workstation and a host server. This secures the transmission of login information and other sensitive data.

On the client, an SSH client package creates the SSH tunnel and does the encryption/decryption for the SSH connection. In addition, the Microsoft Crypto API provides the password encryption and decryption functionality. It protects the login/password information stored in the registry for automatic scripts.

On the CMS server, the solution utilizes the Solaris SSH packages SUNWsshcu, SUNWsshdr, SUNWsshdu, SUNWsshr, and SUNWsshu. The following figure illustrates the connectivity between the various components:



On the CMS server, you can restrict the telnet service to the local host using the following restrictions:

- `/etc/hosts.allow`

  `in.telnetd : localhost` # allow telnet only from within the server

- `/etc/hosts.deny`

  `in.telnetd`: ALL # deny all telnet except as specified in hosts.allow

Other points to be noted:

- Although the telnet service runs on the CMS server, it is configured so that any attempt to gain access to port 23 from outside the system results in a "connection refused" message. This is now true for R16.1 and later systems. Previous releases did not work properly to restrict the access to localhost only. See above to codify the in.telnetd line for localhost access only.
- Multiple applications can run concurrently on the computer. You can allocate the ports 3000, 3005, 3010, and so on as needed.
- In CMS, the Windows SSH clients and SSH server negotiate the encryption algorithm, typically 128-bit AES (recommended) or Blowfish. A variety of industry standard algorithms, such as 128-bit AES, Blowfish, SHA-1, MD5, RC4, and key lengths are provided as a result of including an SSH client. The specific algorithm is negotiated between the client and the server. The U.S. government accepts all for domestic and international use, with certain restrictions. Selection of an algorithm takes place at run time. SSH uses RSA or DSA. CMS servers use SSH Protocol 2. The default encryption is RSA and the key length is 1024 bits. SSH uses SHA-1 or MD5 message authentication.
- This SSH implementation is not available for Network Reporting or Visual Vectors.

Note:
A minor issue with ssh on R12 and R13/R13.1 systems exists. The details and a workaround are noted below. This is documented in document id KB00105609.

SSH on R12 and R13/R13.1

Description: Customer having a problem with Supervisor generating errors on SSH logins. Customer would like to have this error turned off, as it indicates there is a problem but they are not having any login problems.

Details: Software: Call Management System (CMS) - version r3 any 12 or 13

Avaya Supervisor (CVSUP) - SSH version

Cause: sshd is trying to use ipv6.

Workaround: change sshd from using both ipv4 and ipv6 to just use ipv4 on CMS.

SSH continues to log messages until this is updated.

The following steps are required to implement the solution:

```
1) vi /etc/ssh/sshd_config
```

Change:

```
# IPv4 only
#ListenAddress 0.0.0.0
# IPv4 & IPv6
ListenAddress ::
```

to this

```
# IPv4 only
ListenAddress 0.0.0.0
# IPv4 & IPv6
#ListenAddress ::

:wq!
vi /etc/init.d/sshd
```

change:

```
[ -x /usr/lib/ssh/sshd ]&& /usr/lib/ssh/sshd &
```

to this:

```
[ -x /usr/lib/ssh/sshd ]&& /usr/lib/ssh/sshd -4 &
```

2) Restart sshd

```
/etc/init.d/sshd stop
/etc/init.d/sshd start
```

This issue must be resolved in CMS R14.The workaround will be implemented as part of the base CMS package.

CMS application security

This section covers the following topics:

- SPI link on page 23
- Application-level audit logging on page 23
- Backup and restore support on page 24
- Database security controls on page 24

SPI link

The SPI link is a binary (not text-based), proprietary protocol used to communicate between the CMS system and the Communication Manager ACD switch. Access can be controlled by IP address. Communication Manager sends ACD configuration information and ACD-related events to the CMS using this communication channel. For instance, CMS systems can use the SPI link to modify CM vectors, agent and VDN assignments.

Application-level audit logging

There are several application logs with CMS. The most detailed application audit trails can be traced through the `/cms/install/logdir/admin.log` and the `/cms/pbx/acd?/spi.err` logs. The `admin.log` records administrative changes to the CMS application. The `spi.err` logs show the information for setting up and debugging ACD links. These logs are intended for support purposes, but can provide a partial audit trail for customers.

CMS also provides the log `/opt/cc/ahl/log`. This log tracks changes to specific system files that affect the administration of the Solaris system. Example: changes to `/etc/hosts` are logged in the `ahl` log.

Avaya COMPAS Document ID 90815 (R3V11 CMS Maintenance Logs Guide) provides detailed information regarding these log files, their formats and messages.

The customer error log is accessible from the main CMS menu ("Error log report" under the maintenance menu).This log was designed to be the primary customer-facing application log, but does not capture the debug and trace information included in other logs, such as admin.log and spi.err.

Backup and restore support

CMS supports direct backup to a tape system. CMS versions V11 and later support a LAN backup solution through the use of IBM Tivoli Backup software (see *Avaya Call Management System LAN Backup User Guide*). No other 3rd party backup software is supported on CMS, and backup media cannot be encrypted. It is a customer responsibility to ensure regular backups are successfully performed so that a restore can be successful in the event of a disaster.

Database security controls

CMS users do not log into the Informix database or have any privileges within the Informix subsystem. High-level users and administrators can use the dbaccess utility on CMS for accessing data. However, ordinary users can access the database only through the CMS application that has its own access controls. An ISQL interface is installed on new CMS systems. This is an internal password-protected interface that does not have an external (network-facing) listener. Access to the database is provided only through inter-process communication (IPC), so an external exposure to the CMS database is limited to the above interfaces unless Openlink ODBC (port 121/tcp) is enabled. ODBC is as an option for all versions of CMS but is not enabled by default. The ODBC interface requires a password for all client connections.

Update for R15 and later with Informix ODBC/JDBC enabled. See Restricting access to the database on page 49 for new dbaccess password options in R16.1 and later.

Physical Security

The Avaya CMS system must be installed in an area restricted to persons of trust, such as a locked server room or data center. This section covers the following topics:

- Physical server protection on page 24
- EEPROM security on page 25

Physical server protection

The keyboard, console, CD-ROM, and tape drive are all sensitive devices and can be used to compromise an unprotected CMS system. If the Avaya CMS system is a Sun Fire, E3x00, or Netra server, turn the key switch to the locked position.

Store all backup tapes and all original Avaya CMS software in a secure location on site. Store a copy of the backup tapes at an off site location to aid disaster recovery.

The modem connected to the Avaya CMS system can provide secure remote access and also allow Avaya CMS services personnel to perform remote support. Avaya CMS systems can be ordered with an Access Security Gateway (ASG) to provide secure remote access.

Note:
A lock and key modem will also provide secure remote access but it is no longer available for purchase from Avaya.

EEPROM security

Sun provides an EEPROM-level security mechanism for controlling access to the boot console. You need a password to access the boot console. For support purposes, customers must use other methods since a forgotten password can require hardware replacement.

Services security and CMS support

This section covers the following topics:

- Remote connectivity and authentication on page 25
- Services password management on page 25

Remote connectivity and authentication

CMS supports the Access Security Guard (ASG) software or ASG guard hardware to provide a one-time, challenge-response authentication for remote access. Contact your Avaya Services representative for options and details.

Services password management

Avaya Services can automatically change services passwords for the CMS system under an active maintenance contract. Contact your Avaya Services representative for details on how to enable this service.

Reviewing log files

Log files can be used to detect suspicious system activity. Review the following log files on a routine basis:

- `/var/adm/messages`

  This log contains system messages.

- `/var/adm/sulog`

  This log contains su records.

- `/var/cron/log`

  This log contains cron records.

Adding a firewall

Add a firewall on the edge of the network where the Avaya CMS system and Avaya CMS Supervisor clients reside. Both the Avaya CMS system and Avaya CMS Supervisor clients must remain behind a firewall to provide protection from the internet.

Firewalls are commonly used to prevent denial of service attacks on application servers similar to the Avaya CMS system. Firewalls will also prevent snooping of sensitive data, and hijacked sessions from appearing as an authenticated user.

Transmitting passwords

Do not use telnet or ftp to transmit passwords over the network in clear text. If you do so, the password can be snooped in transit.

CMS version specific security

This chapter covers the version-specific security aspects of CMS. There have been enhancements in CMS versions R12 and later, R15 and R16.1 in areas of operating system hardening that was introduced in the first chapter. The following topics explain the areas where these enhancements have occurred:

- Limiting external access to UNIX services on page 29
- Solaris services that can be disabled on page 30
- Additional OS hardening on page 31
- Firewall traversal considerations / Open ports (R12 and later) on page 32
- New security enhancements with R15 (r15ab.d and later) on page 33
- Other (optional) scripts provided with r15ab.d and r15auxab.d on page 34
- Changing the default password encryption algorithm on Solaris™ on page 35
- Manual password complexity changes for R15 and Later (optional) on page 39
- Security enhancements included with R16 and later on page 41

Limiting external access to UNIX services

In CMS R12 and later, the CMS security script creates the files `/etc/hosts.allow` and `/etc/hosts.deny`. Use these files to control which IP addresses are permitted to connect to the Avaya CMS system. Note that settings in `/etc/hosts.allow` cannot re-enable any services disabled through other means.

Note:
`/etc/hosts.allow` and `/etc/hosts.deny` are only honored when TCPWRAPPERS are enabled (which they are by default).

For example, your actions can be to:

- Deny telnet access to IP addresses outside the company firewall
- Permit SSH connections from IP addresses outside the company firewall
- Only permit SSH connections.

Detailed instructions for modifying services configuration files are found in Controlling who can connect to the CMS system on page 48.

Solaris services that can be disabled

On CMS systems prior to R12, the network services listed below are *not* required for standard CMS operations and can be disabled. For CMS systems R12 and later, these unnecessary services have been disabled by default. Note that custom scripts or other custom integration added after installation as part of an Avaya Professional Services Offer can require more than one of these services. The following network services are allowed to be disabled when not required for customized integration:

- Services can be enabled or disabled using information in Appendix A.
- Cache File System
- CDE Calendar (rpc.cmsd)
- CDE Desktop Subprocess Control Daemon (remote CDE support - 6112/tcp)
- Chargen (19/tcp, 19/udp)
- Daytime (13/tcp, 13/udp)
- Discard (9/tcp, 9/udp)
- Echo (network echo - 7/tcp, 7/udp)
- Finger (79/tcp)
- FTP (inbound - 21/tcp)
- Kerberos V5 Warning Message Daemon (88/tcp, 88/udp)
- Name (42/udp)
- NFS Server (2049/tcp, 2049/udp)
- NFS Client (lockd - 4045/tcp, 4045/udp)
- NIS Client
- OCF (Smart card) Daemon
- Printer (Network printing services, local printing is enabled - 515/tcp)
- Rexec (512/tcp)
- Syslog (514/udp)
- Rsh (514/tcp)
- Rlogin (513/tcp)
- Metastat Remote Services
- Sadmind (distributed sys admin agent)
- Sendmail (inbound - 25/tcp)
- Spray (100012/tcp, 100012/udp)

- Sun Font Server (7100/tcp)
- Sun ToolTalk Database Server
- Talk (517/tcp)
- UUCP Network services (540/tcp)
- Time Service (37/tcp, 37/udp)
- Wall

Disabling some of these services can interfere with network-related troubleshooting activities such as echo, and network monitoring tools.

Telnet (23/tcp) cannot be disabled even if ssh has been configured for clients, but it can be restricted to the local host so that it does not respond externally.

Additional OS hardening

On CMS R12 and later systems, root logins are only permitted on the console. In addition, `cron` is limited to users `root`, `sys`, `lp`, `adm`, and `cmssvc`, while `at` is limited to `root`, `sys`, and `cmssvc`. The `umask` for system daemons is set to 022. Customers running older versions of CMS must upgrade to the latest version to benefit from the more limited `umask` settings. Otherwise, a custom Avaya Professional Services offer must be pursued for older system `umask` changes.

In addition:

- The system stack is non executable.
- TCP sequence numbers are more difficult to determine (prevents packet snooping).
- TCP Wrappers are installed and enabled.
- Remote CDE sessions are disabled.
- Remote DT login is disabled.
- Ordinary users do not have interactive shell accounts unless the privilege is granted within CMS user permissions.

Firewall traversal considerations / Open ports (R12 and later)

The CMS system can be placed behind a packet filtering firewall, although no support for such configurations is provided (especially when Network Address Translation (NAT) takes place). See below for a list of port requirements for various aspects of CMS operations. Note that many CMS systems receive additional customization and configuration that can add to this list or make some optional items mandatory.

Also note that ports administered for the ACDs can be changed (default is 5001-5009)

- 22/tcp ssh (optional, can be used by Supervisor, clients)
- 23/tcp telnet (used by Supervisor; optional for Terminal Emulator)
- 111/tcp/udp sunrpc (required by CDE)
- 5001-5009/tcp (used by switch CLAN connection to the ACD)
- 32771-32777/tcp/udp (sometimes used by rps-X, sunrpc)

Optional ports:

- 21/tcp: ftp, used by a CSI (customized configuration) offer
- 25/smtp: sendmail, used by a CSI offer
- 37/tcp time: used by a CSI offer
- 121/tcp erpc: used by Openlink ODBC for the optional CMS data report capability (CMS R14.1 and earlier systems)
- 514/tcp: rsh, used by the High Availability option for the admin-sync utility (CSI offer) Also required for remote tape copy (provisioning)
- 540/tcp: uucp, used by the External Call History (ECH) interface
- 4008/tcp: required for Avaya Visual Vectors Server
- 9100/tcp, udp: hp-printers
- 515/tcp, udp: Printer server
- 6060: Geotel
- 9999: CVLan
- 9980: Link Admin
- 5678: Definity LAN Gateway
- 5011/5012: ASAI
- 5000 - 5020: OpenLink ODBC (CMS R14.1 and earlier systems)

Note:
Older systems use 4000-range ports. The ACD integration ports are different if the 5000-5009 range is used."

- 50000 - 50001/tcp: Informix ODBC Connections (CMS R15 and later, can be enabled for earlier releases, but uncommon)
- 60001/udp: OpenLink ODBC Connection Setup (CMS R14.1 and earlier systems)
- 4000-range: Visual Vectors

Note:
Each time a user logs in to visual vectors, the port increments for the next user; VV uses port 2890 for the Orbix Daemon and ports 4000-4200. Once the ports are incremented to 4200, VV reuses the released ports. The comments apply to vvsv12aa.x and higher, which means CMS R12 and higher. The port range is not administrable.

- 540/tcp: uucp for the External Call History (ECH) interface.

New security enhancements with R15 (r15ab.d and later)

CMS R15 maintenance release r15ab.d or r15auxab.d contains some additional operating system hardening based on results from a United States Air Force scan to qualify CMS for use in Department of Defense installations. The qualification is not yet complete, but some of the findings have been included with the latest R15 load.

The `/etc/shells` file has been populated with the following shells as the only shells allowable to be used on the system:

- `/bin/sh` (Bourne shell)
- `/usr/bin/ksh` (Korn shell)
- `/usr/bin/csh` (C-shell)
- `/usr/bin/pfksh` (profile Korn shell, used for Solaris 10 role-based access)
- `/usr/bin/cms` (CMS application shell)

In addition, the file has been created with root user and group ownership and permissions set to 640.

Additions have been made to the S98cms_ndd script that enables the system to prevent network Denial of Service (DoS) attacks. Specifically, the attempt is to prevent TCP SYN attacks by increasing the TCP queue for unestablished connections and the TCP queue for established connections. This does not deter a TCP SYN attack from a system that has more resources allocated than the larger queues can handle, but it prevents the known TCP SYN attacks.

```
ndd -set /dev/tcp tcp_conn_req_max_q0  2048
ndd -set /dev/tcp tcp_conn_req_max_q   1024
```

The cron.allow, at.allow, cron.deny, and at.deny files have been modified to restrict usage and make the files accessible only to root.

The /etc/ftpd/ftpusers file has been restricted to only be accessible by root.

When the cms_security script is run on the system, it modifies ownership and permissions on any and all *.mib files it finds.

Note:
This causes an issue if the customer system has remote mounts to other systems and has permission to change files on the remote mount. Any *.mib files on the remote system are also modified if the system has proper permissions on the remote mount. CMS R16.1 no longer has this issue. CMS R16.1 and later specifically search only the local filesystems for *.mib files.

Permissions on man pages and their directory structure are made to restrict user's ability to write or execute. This script restricts itself to known man page areas on the system.

Syslog is restricted from logging from any remote systems. The permissions on the syslog.conf file are restricted to root.

The /etc/mail/helpfile is truncated to zero length. Version information is removed from the sendmail greeting. Privacy options are restricted (noexpn, novrfy). The decode alias has been commented out in /etc/mail/aliases.

Other (optional) scripts provided with r15ab.d and r15auxab.d

There are some additional scripts that are provided on the CMS CD that are not automatically run on CMS systems.

- logperms - Restricts the permissions on several system log files. Intended to prevent tampering with log files.
- userperms - Restricts permissions on user home directories and files. See the script on the CD for specific limitations on running the script. Fixes only for existing users, it does not handle new users. The script must be run each time a user is added.

- `acctvrfy` - A Perl script that attempts to lock user accounts for inactivity. This script does *not* attempt to check on current sessions and verify an inactive session. See the script for instructions on how to use.

Changing the default password encryption algorithm on Solaris™

This section consists of the following topics:

- Description on page 35
- Steps to Follow on page 35
- Implementation on page 36
- Verify on page 37
- Enabling long passwords in Solaris™ 10 on page 38

Description

In the era of increased security awareness, many people are looking for better ways to encrypt data and passwords. This document explains the steps necessary to configure Solaris™ 9 12/02 and later to use Blowfish or MD5 encryption algorithm as the default method for encrypting user passwords.

Steps to Follow

Every user on a UNIX system has a password associated with their login account. These passwords are encrypted in a one-way hash using the traditional UNIX crypt algorithm called `crypt_unix`. This algorithm is no longer regarded sufficiently secure for current systems and is provided for backward compatibility. This remains the default algorithm used for password encryption on Solaris™.

One of the biggest limitations is that only the first 8 characters of the key passed to this algorithm are used. The rest are silently ignored.

Solaris 9 12/02 introduces the ability to change the default encryption algorithm for passwords to use the Blowfish (`crypt_bsdbf`) or MD5 (`crypt_sunmd5/crypt_bsdmd5`) algorithms.

There are two versions of the MD5 algorithm:

`crypt_sunmd5`: This is Sun's implementation of the MD5 algorithm

`crypt_bsdmd5`: This is the BSD implementation of the MD5 algorithm and provides compatibility with `md5crypt` on BSD and Linux systems.

Implementation

1. Establish that your release of Solaris 10 is 10/08 or later.

```
$ cat /etc/release
                     Solaris 10 10/08 s10s_u6wos_07b SPARC
           Copyright 2008 Sun Microsystems, Inc.  All Rights Reserved.
                        Use is subject to license terms.
                            Assembled 27 October 2008
```

   The first line of the output provides you with the release number. This example is using Solaris 10 10/08.

2. Change the default algorithm for user passwords.

   a. Login as root and open `/etc/security/policy.conf` using vi.

      The file looks as follows by default:

```
#
# Copyright 1999-2002 Sun Microsystems, Inc.  All rights reserved.
# Use is subject to license terms.
#
# /etc/security/policy.conf
#
# security policy configuration for user attributes. see policy.conf(4)
#
#ident  "@(#)policy.conf        1.6     02/06/19 SMI"
#
AUTHS_GRANTED=solaris.device.cdrw
PROFS_GRANTED=Basic Solaris User
# crypt(3c) Algorithms Configuration
#
# CRYPT_ALGORITHMS_ALLOW specifies the algorithms that are allowed to
# be used for new passwords.  This is enforced only in crypt_gensalt(3c).
#
CRYPT_ALGORITHMS_ALLOW=1,2a,md5
# To deprecate use of the traditional unix algorithm, uncomment below
# and change CRYPT_DEFAULT= to another algorithm.  For example,
# CRYPT_DEFAULT=1 for BSD/Linux MD5.
#
#CRYPT_ALGORITHMS_DEPRECATE=__unix__
# The Solaris default is the traditional UNIX algorithm.  This is not
# listed in crypt.conf(4) since it is internal to libc.  The reserved
# name __unix__ is used to refer to it.
#
CRYPT_DEFAULT=__unix__
```

   b. Decide which algorithm you wish to use for encrypting the passwords. The "`CRYPT_ALGORITHMS_ALLOW`" line lists the available algorithms.

```
1 = BSD/Linux compatible MD5 algorithm
2a = Blowfish algorithm
md5 = Sun's MD5 algorithm
```

Sun's MD5 is regarded stronger than the BSD/Linux compatible version, but it is not compatible with non-Solaris™ systems.

The Blowfish implementation is the most secure, and is compatible with other BSD/Linux/UNIX systems that utilize this algorithm.

c. Deprecate the less secure traditional UNIX algorithm by uncommenting the line containing "`CRYPT_ALGORITHMS_DEPRECATE=unix`"

d. Set the new default encryption algorithm by changing "`CRYPT_DEFAULT=unix`" to the appropriate algorithm that you wish to use.

For example:

```
CRYPT_DEFAULT=1
```

will implement the BSD/Linux compatible MD5 algorithm.

e. Save the file and exit your text editor.

The default encryption algorithm will take effect immediately. All subsequent password changes will be encrypted using the new selected algorithm. Passwords encrypted using the traditional UNIX crypt algorithm will continue to work too.

Verify

You can verify that the new passwords are being encrypted using the new algorithm by checking the password field in the `/etc/shadow` file. Each of the new algorithms have an identifier at the beginning of the password field.

Traditional UNIX crypt encrypted passwords are short with no distinguishing pattern at the beginning.

Example:

```
testuser:SkRrs95xihsQ.:12384::::::
```

BSD/Linux compatible MD5 encrypted passwords can be identified by "`$1$`" as the first 3 characters of the encrypted password:

Example:

```
testuser:$1$26sYv4pB$zo4xkXLRyBrolTF9IuT8d/:12384::::::
```

Blowfish encrypted passwords can be identified by "`$2a$`" as the first 4 characters of the encrypted password.

Example:

```
testuser:$2a$04$Ap60ohzOKIcRPJLazpcaBO4liyUzdYdbCpM.p6T6Q1W1ExOnkStiu:12384::::::
```

Sun MD5 encrypted passwords can be identified by "$md5$" as the first 4 characters of the encrypted password:

Example:

```
testuser:$md5$RPgLF6IJ$WTvAlUJ7MqH5xak2FMEwS/:12384::::::
```

Enabling long passwords in Solaris™ 10

The default encryption method for Solaris 10 is the traditional UNIX encryption. By changing the encryption method in Solaris 10, you can enable long (up to 256 characters) passwords.

In Solaris 10, the maximum number of characters for a password has been changed from 8 to 256. This change was made in the PASS_MAX variable in the `limits.h` (`/usr/include/limits.h`) file. The `getconf` and `getpass` commands have been updated to interact with this change.

To change the encryption scheme from the default UNIX algorithm, modify `/etc/security/policy.conf`.

Example edit of `/etc/security/policy.conf`:

```
--- BEGIN SNIP DEFAULT ENCRYPTION ---
# The Solaris default is the traditional UNIX algorithm.  This is not
# listed in crypt.conf(4) since it is internal to libc.  The reserved
# name __unix__ is used to refer to it.
#
CRYPT_DEFAULT=__unix__
  --- END SNIP DEFAULT ENCRYPTION ---
  --- BEGIN SNIP CHANGE TO MD5 ENCRYPTION ---
# The Solaris default is the traditional UNIX algorithm.  This is not
# listed in crypt.conf(4) since it is internal to libc.  The reserved
# name __unix__ is used to refer to it.
#
CRYPT_DEFAULT=md5
--- END SNIP CHANGE TO MD5 ENCRYPTION ---
```

After changing, no reboot is required. Validate by changing the password. Using md5, a sample encrypted password string in `/etc/shadow` will look like:

```
root:$md5$e8C9kZU9$$Ye6tfFUnKTF/K.jLoSuw8/:12858::::::
```

Note:

After changing the encryption type back to unix from md5 you will notice the system still accepts long passwords. Looking at the `/etc/shadow` file, you can see that the password string will remain as an md5 encryption string.

Manual password complexity changes for R15 and Later (optional)

Note:
These manual changes require the latest CMS Supervisor (R16.1 KB.17) be used to assure connection compatibility.

There are many options for improving security through restricting the login process and password policies. Many of these settings can also cause accessibility issues in some cases because of an overly strict set of rules. Customers are responsible for being cautious, and understanding the effect of these policy and login changes before implementing them.

Changes to /etc/default/login

There are several options in the `/etc/default/login` that can be changed to enhance the security of the system. One option that must not be used, but is required by some policies is changing the CONSOLE line to "`/dev/null`". This disallows direct root logins from the console. Use with extreme care.

Other options that can be set are in the following table:

Option	Initial Value	Description
MAXWEEKS	{Null}	Maximum time period that password is valid. (Best controlled through CMSADM `passwd_age` option)
MINWEEKS	{Null}	Minimum time period before the password can be changed. (Best controlled through CMSADM `passwd_age` option)
WARNWEEKS	{Null}	Time period until warning of date of password's ensuing expiration. (Best controlled through CMSADM `passwd_age` option)
PASSLENGTH	6	Minimum length of password, in characters. If the `policy.conf` is still using the default Solaris encryption, then only 8 characters are allowed. To use more than 8 characters, you must set a different encryption algorithm that supports more than 8 characters, see Changing the default password encryption algorithm on Solaris™ on page 35.

Option	Initial Value	Description
HISTORY	{Null}	Maximum number of prior password history to keep for a user. Setting the HISTORY value to zero (0), or removing the flag, causes the prior password history of all users to be discarded at the next password change by any user. The maximum value is 26. Currently, this functionality is enforced only for user accounts defined in the files name service.
MINUPPER	{Null}	Minimum number of upper case letters required. If MINUPPER is not set or is zero (0), the default is no checks.
MINLOWER	{Null}	Minimum number of lower case letters required. If not set or zero (0), the default is no checks.
MAXREPEATS	{Null}	Maximum number of allowable consecutive repeating characters.
MINSPECIAL	{Null}	Minimum number of special (non-alpha and non-digit) characters required. You cannot specify MINSPECIAL if you also specify MINNONALPHA.
MINDIGIT	{Null}	Minimum number of digits required. You cannot be specify MINDIGIT if MINNONALPHA is also specified.
DICTIONLIST	{Null}	DICTIONLIST can contain list of comma separated dictionary files such as DICTIONLIST=file1, file2, file3. Each dictionary file contains multiple lines and each line consists of a word and a NEWLINE character (similar to `/usr/share/lib/dict/words`.) You must specify full pathnames. The words from these files are merged into a database that is used to determine whether a password is based on a dictionary word.
DICTIONBDIR	{Null}	The directory where the generated dictionary databases reside. Defaults to `/var/passwd`.
MINNONALPHA	{Null}	Minimum number of non-alpha (including numeric and special) required. If MINNONALPHA is not set, the default is 1. You cannot specify MINNONALPHA if MINDIGIT or MINSPECIAL is also specified.

Option	Initial Value	Description
MINDIFF	{Null}	Minimum differences required between an old and a new password. If MINDIFF is not set, the default is 3.
WHITESPACE	{Null}	Determine if white space characters are allowed in passwords. Valid values are YES and NO. If WHITESPACE is not set or is set to YES, white space characters are allowed.
NAMECHECK	YES	Enable/disable checking or the login name. The default is to do login name checking. A case insensitive value of no disables this feature.

Note:
There are too many possible options for complete testing of these features to be done. Many combinations have been tested, but your specific implementation need not have been tested.

Security enhancements included with R16 and later

With the release of CMS R16.1, some new enhancements to system security have been implemented. Many of these enhancements were found to be needed by running JITC tests against the R15 CMS system. Three classes of enhancements have been introduced in CMS R16.1 and later systems. The first class of enhancements has been implemented in the CMS code and is part of the base product with R16.1 and later. The second class is provided through optional scripts that can be run to enforce the new security enhancement specified. A third class of enhancements is documented but not scripted or included on the CMS sytem. These three classes of enhancements make it easier for customers to choose the enhancements that are required by their industry without being forced to take enhancements that need not be required for their specific circumstances.

The security enhancements included in CMS R16.1 are as follows:

- Set up basic auditing on the system.
- Change the ownership and permissions on several files that defaulted to less restrictive permissions than recommended.
- Make all cron entries specify umask of 077.
- Mount the `/cms/filesystem` with the `nosuid` option.
- Modify permissions of CMS user home directories as created by CMS application.
- Optional scripted security enhancements

- Audit controls and logadm changes for rotation of audit logs
- Controlling who can connect to the CMS system.
- Restricting access to the database.

Basic Audit Reporting Tool

Basic Audit Reporting Tool (BART) is a file tracking tool that operates entirely at the file system level. Using BART gives you the ability to quickly, easily, and reliably gather information about the components of the software stack that is installed on deployed systems. Using BART can greatly reduce the costs of administering a network of systems by simplifying time-consuming administrative tasks.

WARNING:
As with any other auditing tool, BART can use a lot of space if you keep many copies of the manifest and comparisons. Take care not to overrun your filesystem space. This is not something Avaya has the ability or responsibility to manage.

BART enables you to determine what file-level changes have occurred on a system, relative to a known baseline. You use BART to create a baseline or control manifest from a fully installed and configured system. You can then compare this baseline with a snapshot of the system at a later time, generating a report that lists file-level changes that have occurred on the system since it was installed.

Note:
For a more information on BART see http://dlc.sun.com/pdf/816-4557/816-4557.pdf and "Integrating BART and the Solaris™ Fingerprint Database in the Solaris 10 Operating System" at http://www.sun.com/blueprints.

BART Components

BART has two main components and one optional component:

- BART Manifest
- BART Report
- BART Rules File

BART Manifest

You use the `bart create` command to take a file-level snapshot of a system at a particular time. The output is a catalog of files and file attributes called a manifest. The manifest lists information about all the files or specific files on a system. It contains information about attributes of files, which can include some uniquely identifying information, such as an MD5 checksum.

BART Report

The report tool has three inputs. The first two are manifests to be compared and the third one is the optional user-provided rules file that indicates which discrepancies are to be flagged.

You use the `bart compare` command to compare two manifests, a control manifest and a test manifest. These manifests must be prepared with the same file systems, options, and rules file that you use with the bart create command.

The output of the `bart compare` command is a report that lists per-file discrepancies between the two manifests. A discrepancy is a change to any attribute for a given file that is cataloged for both manifests. Additions or deletions of file entries between the two manifests are also regarded as discrepancies.

There are two levels of control when reporting discrepancies:

- When generating a manifest
- When producing reports

These levels of control are intentional, since generating a manifest is more costly than reporting discrepancies between two manifests. Once you have created manifests, you have the ability to compare manifests from different perspectives by running the `bart compare` command with different rules files.

BART Rules File

The rules file is a text file that you can optionally use as input to the bart command. This file uses inclusion and exclusion rules. A rules file is used to create custom manifests and reports. A rules file enables you to express in a concise syntax which sets of files to catalog, as well as which attributes to monitor for any given set of files. When you compare manifests, the rules file aids in flagging discrepancies between the manifests. Using a rules file is an effective way to gather specific information about files on a system.

Using a rules file to monitor specific files and file attributes on a system requires planning. Before you create a rules file, decide which files and file attributes on the system to monitor. Depending on what you are trying to accomplish, you can use a rules file to create manifests, compare manifests, or for other purposes.

Note:

You can create several rules files for different purposes. However, if you create a manifest by using a rules file, you must use the same rules file when you compare the manifests. If you do not use the same rules file when comparing manifests that were created with a rules file, the output of the bart compare command will list many invalid discrepancies.

A rules file can also contain syntax errors and other ambiguous information as a result of user error. If a rules file contains misinformation, these errors will also be reported.

Basic Example of using BART

Create a manifest using the following commands:

```
cd /
bart create > /var/cms/security/bart_manifest
```

When needed, or in a cron job, run a bart compare periodically using the following commands:

```
cd /
bart create > /var/cms/security/bart_test
bart compare  /var/cms/security/bart_manifest /var/cms/security/
  bart_test
```

Note:
By default, BART tracks and reports on all attributes except directory timestamps. Even with minimal changes to the system like a user changing permissions on some home directory files resulting in system level logs being rotated, there can be significant differences. Use the bart rules file to limit the attributes collected if you need more change information than desired.

See the `bart` man page or the references at the beginning of this section for more information on using BART.

Permission and Ownership Changes

Permission and ownership changes are made to several files. The following is a list of the changes made to the files or file types.

- Change logfile permissions of any file named `btmp, messages, wtmp, nlog, cronlog, utmp, shutdownlog, syslog, sudo.log, loginlog, syslog.log, lastlog,` or `log` in the `/var` directory structure to 644. Intended targets include, but are not limited to :
  - `/var/adm/messages`
  - `/var/adm/sudo.log`
  - `/var/sadm/lastlog`
  - `/var/cron/log`
- `chmod 750 /var/audit`
- `chmod 640 /etc/security/audit_user`
- `chmod 640 /etc/ftpd/ftpusers`
- `chmod 700 /var/crash`
- Remove world write from the following files:

- /cms/cc/install.aot.cssrVVXX.X/data/log

  where VV is the version number and XX.X is the release
- /cms/db/journal/timetable/10
- /cms/db/journal/timetable/11
- /cms/perfbin/perf
- /cms/perfbin/perf/occ.thresh
- /cms/tmp
- /cms/tmp/errfile
- /cms/tmp/disklist
- /etc/lp/interfaces/tmp
- /opt/informix/etc/ilslsfl
- /opt/informix/etc/Lsils-cr
- /usr/lib/cms/pbxtrcflags
- /usr/dbtemp
- /var/adm/spellhist
- /var/dt/dtpower/_current_scheme
- /var/elog/elogLocal

- Change ownership fo directory /cms/perfbin to root:sys

Make all cron entries use umask of 077

The file /etc/cron/.proto has been modified to include the following line:

umask 077

This makes all future entries to cron use a umask of 077.

The /cms filesystem is mounted with nosuid option

The /cms/ filesystem is now mounted using the nosuid option.

Modify permissions of CMS user home directories as created by CMS application

When a new user is created, the system creates a new home directory for the user in `/export/home/[userid]`. The directory is created with permissions of `755`, and must be more restrictive. CMS now creates the user's home directory and modifies the permissions to `750`. Additional files created by users can be changed to this setting by running the `userperms.sh` script.

Optional scripted security enhancements

The optional security scripts can be found at `/cms/install/bin`. The scripts included with CMS R16.1 include the following:

- `tcp_trace`

  Enables TCP conection tracing. Use with caution. This type of tracing can make extremely large log files in the /var filesystem.

- `disable_core`

  Disables core files on the system. Also to be used with extreme caution. Core files can be very useful in determining the cause of application problems.

- `disable_crash`

  Disable crash files on the system. Another one to be cautious of using as crash files can be useful in determining system and OS problems that cause panics. Without crash files, your system panics might not be traceable.

- `move_root_home`

  Change the root user home directory from / to `/root`.

- `enable_audit`

  This script sets some auditing control parameters, enables auditing, and sets up `logadm.conf` to rotate log files in `/var/audit`. Details of what has been done are outlined below. Take care with auditing because once enabled, it can use large amounts of the `/var/filesystem`. With both auditing enabled and TCP connection tracing turned on, a system with many users can fill up the `/var` file system fairly quickly. Observe your filesystems when these items are in use.

Audit controls and logadm changes for rotation of audit logs

1. The `enable_audit` script above makes the following changes to the `/etc/security/audit_control` file:
   - dir:`/var/audit`

     Directory location where auditing logs are placed.
   - flags:`fr,fd,am,lo,fm`

     Set the `fr` (file read), `fd` (file delete), `am` (Administrative [meta-class]), `lo` (login [or] logout), and `fm` (file attribute modify) audit class flags.
   - minfree:20

     Set the minimum free space percentage. This setting causes `auditd` to invoke `audit_warn` if the free space falls below this percentage.
   - naflags:`lo`

     Set naflags to audit `lo` (login [or] logout) even if the user cannot be identified.
2. It then modifies the `/etc/logadm.conf` file to include the following:
   - **`audit -M '/usr/sbin/audit -n; sleep 1' -R '/bin/rm $file' -T '/var/audit/[0-9]*.[0-9]*.*' -t '$file' -z 0 -z"perl -ni -e 'print unless /^.var.audit.*not_terminated/' /etc/logadm.conf" /var/audit/*.not_terminated.*`**
3. Enable auditing using this command:

   `/etc/security/bsmconv`
4. The customer system must now be restarted to invoke auditing functionality. The script does not do so.

   `shutdown -y -i6 -g0`

Note:

Turning on auditing disables the `volfs` service. This service is used to automatically mount CDs and DVDs with other removable media devices. For CMS systems, the main focus would be on the CDs and DVDs. Typically, volfs is running on the system in which CMS is installed. If it is not, a CD or DVD needs to be manually mounted. Some customers can want the `volfs` service to be left turned off for security reasons. However, Avaya Provisioning and Services can turn the service back on. Therefore, customers must make prior arrangements to ensure the service is not enabled, or not left enabled.

5. To disable auditing, use the following commands:

   svcadm milestone svc:/milestone/single-user

   /etc/security/bsmunconv

   svcadm milestone svc:/milestone/multi-user

   shutdown -y -i6 -g0

Controlling who can connect to the CMS system

The CMS Security Script creates the files `/etc/hosts.allow` and `/etc/hosts.deny`. Use these files to control which IP addresses are permitted to connect to the Avaya CMS system.

Note:
The CMS security script will NOT write over existing /etc/hosts.allow and /etc/hosts.deny files. If you use an upgrade to get to CMS R16.1, the files will not contain the same information as below. To get the updated files, insert the CMS R16.1 Software DVD into the system DVD drive, then run the following commands:

cp /cdrom/cdrom0/security/sec_files/hosts.allow /etc/

cp /cdrom/cdrom0/security/sec_files/hosts.deny /etc/

To use the `/etc/hosts.allow` and `/etc/hosts.deny` files:

1. Edit `/etc/hosts.allow`

   This file contains the following settings:

   - `ALL: localhost`
   - `sshd : ALL`
   - `ALL : ALL : DENY`

   Note:
   Network services `rsh`, `rexec`, and `rlogin` are disabled on Avaya CMS systems. The lines in this file do not affect a service if the daemon for that service is not running.

This disables telnet from all remote hosts but still allows telnet via port forwarding from Supervisor users.

Note:
Avaya CMS Supervisor supports telnet and SSH connections.

2. Edit `/etc/hosts.deny`
3. It currently has the following entry:

   `ALL : ALL`

4. In order to allow certain IP addresses and subnets to connect to Avaya CMS system using a particular service, change file `/etc/hosts.allow` by replacing `ALL` with the permitted IP addresses.

The following table contains some examples of security setting use:

Example setting	Explanation of use
`in.telnetd : 10.8.10.0/255.255.255.0`	This setting allows telnet connections from all IP addresses from 10.8.10.1 to 10.8.10.255.
`sshd : 10.0.0.0/255.0.0.0`	This setting allows ssh connections from all IP addresses from 10.0.0.1 to 10.255.255.255.
`in.rshd :  10.8.31.100 10.8.31.55`	This setting allows connections from IP addresses 10.8.31.100 and 10.8.31.55.

Restricting access to the database

Use dbaccess to limit which CMS logins have ODBC/JDBC access to the CMS database. The CMS database has “open access” permissions as a standard feature which allows permission to any CMS login, connecting to the CMS server via ODBC/JDBC, to view any CMS table. No action is required if all CMS logins are allowed open access to the CMS database.

The dbaccess utility does not provide the ability to control which tables the CMS login has access to, or which ACD data the CMS login can view. The process of setting the secure database access is performed in two parts. First, all CMS login ids that are allowed CMS database access must be members of the UNIX group dbaccess. Second, you must execute the dbaccess option under the cmsadm menu.

Note:
Adding a single CMS login to the dbaccess group will disable “open access” permissions for all users that are not members of the dbaccess group.

1. Each CMS login allowed ODBC/JDBC access to the CMS database must be added to the UNIX group dbaccess. To add CMS logins to the dbaccess group, enter:

   `usermod -G dbaccess` *`cmslogin`*

   Where *cmslogin* is the user id of the specific CMS login to be placed in the group. You must execute the usermod command for each CMS login that you wish to provide CMS database access.

2. To determine which logins are in the dbaccess group, enter:

   `cat /etc/group | grep dbaccess`

3. Open the *Avaya Call Management System Administration* menu. Enter:

   cmsadm

   The system displays the *Avaya Call Management System Administration* menu.

4. Select the *dbaccess* option. The system displays the following message:

```
Begin CMS DB Access Permissions changes
grant resource to "public";

Your CMS database currently has public access permissions to all resources. Do you
wish to revoke this access and only grant access to specific CMS users? [y,n,?]
```

5. Enter: **y**

   The process continues. Messages similar to the following will be displayed:

```
Please wait while CMS Informix Database permissions are changed.
revoke resource from public;
revoke connect from public;
grant connect to cms;
grant connect to cmssvc;
Revoke resource from public on CMS database.
Please wait while connect permissions are granted for requested users
grant connect to <cmslogin>;
grant connect to <cmslogin>;
.
.
.
Changes to CMS DB Access Permissions finished.
```

Note:
The output will always display one “grant connect” message per CMS logid, including logids already in the dbaccess group with connect permissions.

After the changes are complete, you can use the CMS logids to run ODBC/JDBC clients and access the CMS database.

To remove ODBC/JDBC access permissions for CMS logids, first remove them from the UNIX dbaccess group then run dbaccess from the *Avaya Call Management System Administration* menu.

6. Remove ODBC/JDBC access permissions for CMS logids from the UNIX dbaccess group. Enter:

   usermod –G “” *cmslogin*

7. Open the *Avaya Call Management System Administration* menu. Enter:

   cmsadm

   The system displays the *Avaya Call Management System Administration* menu.

8. Select the *dbaccess* option. The system displays the following message:

```
Begin CMS DB Access Permissions changes
Please wait while connect permissions are granted for requested users
grant connect to  <cmslogin>;
.
.
.
Changes to CMS DB Access Permissions finished.
```

   The UNIX dbaccess group information is re-set to only provide access permissions for members remaining in the UNIX dbaccess group.

   Perform the Steps 9 through 11 to remove all the CMS logins from the UNIX dbaccess group and restore “open access” permissions to all the CMS logins.

9. Run the usermod command for each CMS login in the dbaccess group. Enter:

   usermod –G “” *cmslogin1*

   usermod –G “” *cmslogin2*

   usermod –G “” *cmslogin3*

10. Open the Avaya Call Management System Administration Menu. Enter:

    cmsadm

    The system displays the *Avaya Call Management System Administration* menu.

11. Select the *dbaccess* option. The system displays the following message:

```
Begin CMS DB Access Permissions changes

No CMS user ids are in UNIX group dbaccess.
If you proceed, the CMS database will
be set to public permissions access for all resources.
Do you really want to do this? [y,n,?]
```

12. Enter: **y**

    The process restores public permissions to the CMS database. Messages similar to the following will be displayed:

```
Please wait while CMS Informix Database permissions are set to public.
grant resource to public;
revoke connect from cms;
revoke connect from cmssvc;
Grant resource to public on CMS database.
Changes to CMS DB Access Permissions finished.
```

Appendix A: Enabling and Disabling Services in Solaris 9 and 10

CMS R12 through R14.1 use Solaris 9 as the underlying OS. CMS R15 and later systems use Solaris 10. Follow the proper procedure for the OS for your CMS.

This section covers the following topics:

- Solaris 10 on page 53
- Service Management Facility (SMF) on page 53
- Solaris 9 on page 60
- CMS permissive use support policy on page 62
- Links to Avaya security resource on page 64

Solaris 10

Solaris 10 includes a new facility called the Service Management Facility (SMF) for managing most services on the system. A few services are still managed by inetd. See Table A-1 below.

Service Management Facility (SMF)

SMF provides an infrastructure that augments the traditional UNIX start-up scripts, init run levels, and configuration files. SMF provides the following functions:

Automatically restarts failed services in dependency order, whether they failed as a result of an administrator error, software bug, or were affected by an uncorrectable hardware error. The dependency order is defined by dependency statements.

Makes services objects that can be viewed, with the new `svcs` command, and managed, with `svcadm` and `svccfg` commands. You can also view the relationships between services and processes using `svcs -p`, for both SMF services and legacy `init.d` scripts.

Makes it easy to backup, restore, and undo changes to services by taking automatic snapshots of service configurations.

Makes it easy to debug and ask questions about services by providing an explanation of why a service isn't running by using `svcs -x`. Also, this process is eased by individual and persistent log files for each service.

Allows for services to be enabled and disabled using `svcadm`. These changes can persist through upgrades and reboots. If the `-t` option is used, the changes are temporary.

Enhances the ability of administrators to securely delegate tasks to non-root users, including the ability to modify properties and enable, disable, or restart services on the system.

Boots faster on large systems by starting services in parallel according to the dependencies of the services. The opposite process occurs during shutdown.

Allows you to customize the boot console output to either be as quiet as possible, which is the default, or to be verbose by using `boot -m verbose`.

Preserves compatibility with existing administrative practices wherever possible. For example, most customer and ISV-supplied rc scripts still work as usual.

Dependency statements define relationships between services. These relationships can be used to provide precise fault containment by restarting only those services that are directly affected by a fault, rather than restarting all of the services. Another advantage of dependency statements is that the statements allow scalable and reproducible initialization processes. By defining all of the dependencies, you can take advantage of modern, highly parallel machines, because all independent services can be started in parallel.

SMF defines a set of actions that can be invoked on a service by an administrator. These actions include enable, disable, refresh, restart, and maintain. Each service is managed by a service restarter which carries out the administrative actions. In general, the restarters carry out actions by executing methods for a service. Methods for each service are defined in the service configuration repository. These methods allow the restarter to move the service from one state to another.

The service configuration repository provides a per-service snapshot at the time that each service is successfully started so that fallback is possible. In addition, the repository provides a consistent and persistent way to enable or disable a service, as well as a consistent view of service state. This capability helps you debug service configuration problems.

SMF includes a couple of commands that allows you to display, troubleshoot, enable , disable, and restart SMF services. The commands are svcs and svcadm.

svcs command

The svcs command has several options, but only two of those options are discussed for now. More information on SMF and its commands can be found at http://docs.sun.com/app/docs/doc/817-1985.

The "`svcs -a`" command displays all services on the system. You can then pipe to grep to find information on specific services or to find the exact service name you need.

The "`svcs -xv`" command shows SMF services that are not running properly. This is useful in troubleshooting service issues.

svcadm command

The `svcadm` command is used to enable, disable or restart system services managed by SMF.

To enable a service, use the command:

```
svcadm enable {Service FMRI}
```

where the {Service FMRI} is the fully qualified service description item listed in Table 1 below. You can sometimes use the simple name (ssh), but it must be unique for the svcadm command to accept.

The following table lists some of the services that have been converted to use SMF. Each service includes the daemon or service name, the FMRIs for that service, the run script that is used to start the service, and whether the service is started by inetd.

.

Table 1: SMF Services

Service Name	FMRI	Run Script	inetd Service
automount	svc:/system/filesystem/autofs:default	autofs	Not applicable
consadmd	svc:/system/consadm:default	rootusr	Not applicable
coreadm	svc:/system/coreadm:default	coreadm	Not applicable
cron	svc:/system/cron:default	cron	Not applicable
cryptoadm	svc:/system/cryptosvc:default	N/A	Not applicable
cvcd	svc:/system/cvc:default	cvcd	Not applicable
dcs	svc:/platform/<arch>/dcs:default	None	Applicable
dtlogin	svc:/application/graphical-login/ cde-login:default	dtlogin	Not applicable
dtprintinfo	svc:/application/cde-printinfo:default	dtlogin	Not applicable
dtspcd	svc:/network/cde-spc:default	None	Applicable
dumpadm	svc:/system/dumpadm:default	savecore	Not applicable
efdaemon	svc:/platform/<arch>/ efdaemon:default	efcode	Not applicable
fmd	svc:/system/fmd:default	N/A	Not applicable
gssd	svc:/network/rpc/gss:default	None	Applicable
imapd	svc:/network/imap/tcp:default svc:/network/imapnew/tcp:default	None	Applicable

Table 1: SMF Services

Service Name	FMRI	Run Script	inetd Service
in.chargend	svc:/network/chargen:dgram svc:/network/chargen:stream	None	Applicable
in.comsat	svc:/network/comsat:default	None	Applicable
in.daytimed	svc:/network/daytime:dgram svc:/network/daytime:stream	None	Applicable
in.dhcpd	svc:/network/dhcp-server:default	dhcp	Not applicable
in.discardd	svc:/network/discard:dgram svc:/network/discard:stream	None	Applicable
in.echod	svc:/network/echo:dgram svc:/network/echo:stream	None	Applicable
in.fingerd	svc:/network/finger:default	None	Applicable
in.ftpd	svc:/network/ftp:default	None	Applicable
in.named	svc:/network/dns/server:default	inetsvc	Not applicable
in.rarpd	svc:/network/rarp:default	boot.server	Not applicable
in.rdisc	svc:/network/initial:default	inetinit	Not applicable
in.rexecd	svc:/network/rexec:default	None	Applicable
in.rlogind	svc:/network/login:rlogin svc:/network/login:eklogin svc:/network/login:klogin	None	Applicable
in.routed	svc:/network/initial:default	inetinit	Not applicable
in.rshd	svc:/network/shell:default svc:/network/kshell	None	Applicable
in.talkd	svc:/network/talk:default	None	Applicable
in.telnetd	svc:/network/telnet:default	None	Applicable
in.tftpd	svc:/network/tftp/udp6:default	None	Applicable
in.timed	svc:/network/time:dgram svc:/network/time:stream	None	Applicable
in.tnamed	svc:/network/tname:default	None	Applicable

Table 1: SMF Services

Service Name	FMRI	Run Script	inetd Service
in.uucpd	svc:/network/uucp:default	None	Applicable
inetd-upgrade	svc:/network/inetd-upgrade:default	N/A	Not applicable
inetd	svc:/network/inetd:default	inetsvc	Not applicable
intrd	svc:/system/intrd:default	None	Not applicable
ipop3d	svc:/network/pop3/tcp:default	None	Applicable
kadmind	svc:/network/security/kadmin:default	kdc.master	Not applicable
kbd	svc:/system/keymap:default	keymap	Not applicable
keyserv	svc:/network/rpc/keyserv:default	rpc	Not applicable
kpropd	svc:/network/security/krb5_prop:default	None	Applicable
krb5kdc	svc:/network/security/krb5kdc:default	kdc	Not applicable
ktkt_warnd	svc:/network/security/ktkt_warn:default	None	Applicable
ldap_cachemgr	svc:/network/ldap/client:default	ldap.client	Not applicable
loadkeys	svc:/system/keymap:default	keymap	Not applicable
lockd	svc:/network/nfs/client:default svc:/network/nfs/server:default	nfs.server	Not applicable
lpsched and lpshut	svc:/application/print/server:default	lp	Not applicable
mdmonitord	svc:/system/mdmonitor:default	svm.sync	Not applicable
metainit	svc:/system/metainit:default	svm.init	Not applicable
metadevadm	svc:/platform/<arch>/mpxio-upgrade:default	N/A	Not applicable
mount	svc:/system/filesystem/local:default svc:/system/filesystem/minimal:default svc:/system/filesystem/root:default svc:/system/filesystem/usr:default	nfs.client, rootusr, standardmounts	Not applicable
mountd	svc:/network/nfs/server:default	nfs.server	Not applicable

Table 1: SMF Services

Service Name	FMRI	Run Script	inetd Service
nfsd	svc:/network/nfs/server:default	nfs.server	Not applicable
nfsmapid	svc:/network/nfs/client:default svc:/network/nfs/server:default	nfs.server	Not applicable
nis_cachemgr	svc:/network/rpc/nisplus:default	rpc	Not applicable
nscd	svc:/system/ name-service-cache:default	nscd	Not applicable
ntpdate	svc:/network/ntp:default	xntpd	Not applicable
ocfserv	svc:/network/rpc/ocfserv:default	ocfserv	Not applicable
picld	svc:/system/picl:default	picld	Not applicable
pmconfig	svc:/system/power:default	power	Not applicable
printd	svc:/application/print/cleanup:default	spc	Not applicable
quotaon	svc:/system/filesystem/local:default	ufs_quota	Not applicable
rcapd	svc:/system/rcap:default	rcapd	Not applicable
rpcbind	svc:/network/rpc/bind:default	rpc	Not applicable
rpc.bootparamd	svc:/network/rpc/bootparams:default	boot.server	Not applicable
rpc.mdcomm	svc:/network/rpc/mdcomm:default	None	Applicable
rpc.metad	svc:/network/rpc/meta:default	None	Applicable
rpc.metamedd	svc:/network/rpc/metamed:default	None	Applicable
rpc.metamhd	svc:/network/rpc/metamh:default	None	Applicable
rpc.nisd	svc:/network/rpc/nisplus:default	rpc	Not applicable
rpc.nispasswdd	svc:/network/rpc/nisplus:default	rpc	Not applicable
rpc.rexd	svc:/network/rpc/rex:default	None	Applicable
rpc.rstatd	svc:/network/rpc/rstat:default	None	Applicable
rpc.rusersd	svc:/network/rpc/rusers:default	None	Applicable
rpc.smserverd	svc:/network/rpc/smserver:default	None	Applicable

Table 1: SMF Services

Service Name	FMRI	Run Script	inetd Service
rpc.sprayd	svc:/network/rpc/spray:default	None	Applicable
rpc.ttdbserverd	svc:/network/rpc/ttdbserver:tcp	None	Applicable
rpc.walld	svc:/network/rpc/wall:default	None	Applicable
rpc.yppasswdd and rpc.ypupdated	svc:/network/nis/server:default	rpc	Not applicable
rquotad	svc:/network/nfs/rquota:default	None	Applicable
sadc	svc:/system/sar:default	perf	Not applicable
savecore	svc:/system/dumpadm:default	savecore	Not applicable
sendmail	svc:/network/smtp:sendmail	sendmail	Not applicable
sf880drd	svc:/platform/<arch>/sf880drd:default	sf880dr	Not applicable
slpd	svc:/network/slp:default	slpd	Not applicable
sshd	svc:/network/ssh:default	sshd	Not applicable
statd	svc:/network/nfs/client:default svc:/network/nfs/server:default	nfs.server	Not applicable
svc.startd	svc:/system/svc/restarter:default	N/A	Not applicable
syseventd	svc:/system/sysevent:default	devfsadm	Not applicable
sysidpm, sysidns, sysidroot, sysidsys	svc:/system/sysidtool:system	sysid.sys	Not applicable
sysidnet	svc:/system/sysidtool:net	sysid.net	Not applicable
syslogd	svc:/system/system-log:default	syslog	Not applicable
ttymon	svc:/system/console-login:default	inittab	Not applicable
utmpd	svc:/system/utmp:default	utmpd	Not applicable
vold	svc:/system/filesystem/volfs:default	volmgt	Not applicable
xntpd	svc:/network/ntp:default	xntpd	Not applicable
ypbind	svc:/network/nis/client:default	rpc	Not applicable

Table 1: SMF Services

Service Name	FMRI	Run Script	inetd Service
ypserv	svc:/network/nis/server:default	rpc	Not applicable
ypxfrd	svc:/network/nis/server:default	rpc	Not applicable
zoneadm	svc:/system/zones:default	N/A	Not applicable
None	svc:/network/loopback:default	network	Not applicable
None	svc:/network/physical:default	network	Not applicable

Solaris 9

Solaris 9 does not have the Service Management Facility. It uses traditional flat files to manage `/etc/inetd.conf` and the `inetd` daemon services on the system. Specifically, the `/etc/inetd.conf` file is used.

Services typically provided using `inetd` include:

- ftp: File transport protocol which allows users to transport files between remote sites.
- telnet: A protocol used to open user sessions from remote sites.
- exec, in.rexecd: Remote execution server that allows remote users to execute commands on the system provided they have proper authorization.
- rlogin: An older method of opening remote sessions, being replaced by telnet.
- rsh: Remote shell that you use to execute commands on a remote host.
- talk: A communication program that allows two users to talk by copying lines from one user's terminal to the other.
- finger: A service that allows users to get information about other users currently logged in on the local system or remote systems.
- comsat: A server that notifies users when they receive mail. The biff program is used to turn comsat service on and off for each user.
- uucp, uucico:The daemon that processes Unix to Unix copy (UUCP) file transfer requests that were queued by uucp or uux.
- netstat: A service that displays network connections, routing tables, and other networking information about a system. This works on the local system and over a network.

There are several others, but these are some of the more common services. Most of the list is disabled by default on CMS systems. These services can be controlled (added/removed) by adding or deleting (commenting out) lines in the file "/etc/inedt.conf". If you make a change to this file, you must restart the inetd daemon with the command:

```
kill -HUP inetd
```

The inetd configuration file

The file `/etc/inetd.conf` is used to configure these networking services. Its format is:

```
service    socket type    protocol    flags    user    server path    server arguments
```

This is explained in more detail in the "How Linux Works" document.

Limiting services to your machine to specific addresses

1. If your system is not set for services to use the tcpd daemon rather than the usual deamon by substituting the following in the "`/etc/inetd.conf`" file"
2. Change lines like this:

   ```
   finger stream tcp nowait nobody /usr/etc/in.fingerd in.fingerd
   ```

3. To this:

   ```
   finger stream tcp nowait nobody /usr/sbin/tcpd in.fingerd
   ```

4. Change the hosts deny file so the following lines are included with the comments:

   ```
   ALL: ALL
   ALL: PARANOID
   ```

5. Change the hosts.allow file to allow services to desired TCP/IP addresses. For example:

   ```
   ALL:  10.1.0.153, 10.1.2.252
   fingerd: 10.1.1.3
   ```

6. Reset the inetd deamon by issuing the command "`kill -HUP inetd`".

To disable a network service completely

To disable remote services like `finger`, `who`, and `w`, you must modify `/etc/inetd.conf` file. To disable finger services for example, change the `/etc/inetd.conf` file so the line that says "`in.fingerd`" at the end, is commented out. Do the same for any other services that you do not want to run. Then make the inetd daemon reload its configuration file and restart with the command "`kill -HUP inetd`".

CMS permissive use support policy

As of October 3, 2006, the following "Permissive Use" policy applies to CMS and must be taken into consideration when modifying the CMS system:

Call Management System (CMS) Standard Operating Environment

Under the terms of relevant hardware and software support contracts, Avaya will support the entire system, hardware and software, from end to end, managing the escalation and resolution of problems with any system component to the correct support organization. This includes hardware and software categorized as "standard" product. "Standard" product refers to configurations that have been initially designed, tested and certified by Avaya.

Some customers require the platform to perform other functions (for example: co-resident applications), or to connect with non-standard hardware configurations. Such configurations are specifically not recommended, but in the case where they are utilized, Avaya Global Services will continue to support the CMS application in a "permissive use" mode. For these non-standard configurations, the Avaya Global Services ITAC or Center

of Excellence will troubleshoot problems with the CMS application, but cannot and will not accept responsibility for end-to-end system integrity. When operating outside of a "standard" configuration, the customer has the added responsibility of managing the non-standard configuration and can incur additional charges when Avaya Global Services resources are required.

See Permissive Use statement below for a complete description of the permissive support policy and terms and conditions with respect to non-standard CMS configurations.

Permissive Use of Non-Standard CMS Configurations

Policy:

Avaya will allow and thereby support permissive use of non-standard networking, non-standard terminal equipment, and other application packages in conjunction with CMS. Avaya will not withdraw support of the CMS application if it is determined that other packages, applications, or hardware are running concurrently. The software packages and hardware connectivity that are running concurrently with the CMS can well be packages that are sold and toaab0111 Utilities, Token Ring LAN, or other physical interfaces including wallboards), as well as other vendor applications. Non-standard configurations are not to be installed by Avaya personnel.

Avaya reserves the right to implement enhancements or modifications of this policy at any time without providing prior written or verbal notice to Avaya maintenance contract customers.

Responsibilities under the Policy:

Avaya:

Avaya's responsibilities are limited to correcting faults with the standard CMS application. CMS customers operating in a non-standard environment who are seeking assistance from Avaya will be subject to standard maintenance response times. They are not eligible for priority queuing. When a trouble is reported to Avaya, and it is determined that other applications or non-standard terminals, link or hardware connectivity are being used, Avaya can require that this non-standard hardware and software be removed from the

system and the system be returned to a standard configuration in order to be able to diagnose the CMS trouble. Reasonable and timely effort will be made to troubleshoot the issue prior to requiring the CMS to be returned to a standard configuration; however, this can be the only way to separate CMS troubles from other non-standard issues. This reconfiguration decision is the sole responsibility of the Avaya Tier III engineer.

Upgrades: If it is determined that standard Avaya upgrade processes will be impacted by the existence of non-standard configurations, Avaya will not perform said upgrade until the CMS is returned to an Avaya "standard" configuration.

Customer:

If Avaya requires, it will be the responsibility of the customer to perform a reconfiguration of CMS to return it to a standard configuration. Customers must take notice that the CMS system can remain in a trouble state until this reconfiguration can be performed. Avaya will not be held responsible for any associated damages that can result from this period of delay.

Billing:

If trouble shooting can only be performed outside of the times of any applicable CMS software support contract (warranty or maintenance), the customer will be billed then-current premium Time and Material charges.

If it is determined that the trouble is no longer present after this re-configuration, the customer will be billed Time and Material charges for the trouble shooting effort, regardless of any pre-existing hardware or software contract agreements.

Note:

This policy is subject to change in the future and is reproduced here for reference purposes only.

Links to Avaya security resource

List of current versions of the security documents are shown below. Note that these documents typically change for each release. You can access these documents at www.avaya.com/support.

- Avaya CMS R15 documentation
- Avaya CMS R13 Software Installation, Maintenance and Troubleshooting Guide (07-300338), CID 106947
- Avaya Call Management System: Switch Connections, Administration & Troubleshooting (07-300739): CID 82509 - See CID 121524 FOR R14 (07-601582)
- Avaya Call Management System: LAN Backup Guide (07-601523) CID 106955 - See CID 121520 for R14 (07-601589)
- Avaya CMS capacities: CID 114395. See CID 121514 for R14.

- Avaya Call Management System Release 13 Administration (07-600956)
- Avaya Call Management System Release 13 External Call History Interface (07-300737), CID 106956. See CID 121516 for R14.
- R3V11 CMS Maintenance Logs Guide -Issue 1.1 (most current version): CID 90815
- Customer Procedures For Securing CMS Servers (for CMS R3V8, R3V9 and R3V11)

Appendix B: CMS security/Hardening offer

CMS security / Hardening offer

The Avaya Enterprise Security Practice offers CMS Security Hardening, an in-depth review of the CMS system that identifies vulnerabilities. It configures the hardening measures needed to bring older CMS systems into compliance with today's security requirements. For new CMS systems, this custom configuration can also deliver a method to prevent multiple sessions from a single agent and to close inactive agent sessions automatically after a timeout period.

The following security measures can be included in a hardening engagement. Note that items with an asterisk have already been delivered by default in newer CMS systems and generally apply to CMS systems prior to R12 ONLY:

- Install any critical Solaris security patches not yet installed.
- Disable all unnecessary network daemons (services) for older CMS systems*.
- Reconfigure the Solaris system stack to reduce the risk of buffer overflow attacks*.
- Modify Telnet and FTP login banners to obfuscate operating system information.
- Disable direct login access to "root" ID*.
- Disable privileged accounts from accessing the system using FTP*.
- Modify network device driver characteristics to prevent IP forwarding and redirects*.
- Reconfigure TCP stack to use smarter TCP sequence numbers*.
- Tighten file permissions in /etc and its subdirectories*.
- Modify file permissions and ownership of user shells*.
- Unless CMS utilizes HA Auto-Sync package, remove any "`rhosts`" files in CMS users' home directories.
- Prevent users from sharing authentication credentials.
- Implement Password Aging: All CMS user accounts are required to change their password once every 186 days. Users are notified one week before password expires.
- Display a customized warning message for restricted use, prior to login prompt.
- Display of customized warning message, after authentication, of corporate security policies must be adhered to and that unauthorized usage can result in disciplinary action.
- Install a script to disable user accounts that have not been utilized for the past 90 days.
- Lock "anonymous" and FTP user accounts*.

- Schedule automatic nightly logoff of users.
- Install various logging packages for advanced auditing.