Security Configuration Guide for EC 8.0 and DTACS 5.0

Please Read

Important

Read this entire guide. If this guide provides installation or operation instructions, give particular attention to all safety statements included in this guide.

Notices

Trademark Acknowledgments

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: **www.cisco.com/go/trademarks**.

Third party trademarks mentioned are the property of their respective owners.

The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Publication Disclaimer

Cisco Systems, Inc. assumes no responsibility for errors or omissions that may appear in this publication. We reserve the right to change this publication at any time without notice. This document is not to be construed as conferring by implication, estoppel, or otherwise any license or right under any copyright or patent, whether or not the use of any information in this document employs an invention claimed in any existing or later issued patent.

Copyright

Contents

1

System Defaults and Access Control

Introduction

This chapter discusses the operating system defaults and role-based access control.

In This Chapter

Operating System Defaults

Important: Upgrading the EC/DTACS System Release will invalidate any customized security settings you might have made. We recommend that you record any customized settings for future reference.

Note: The following defaults are applicable to the EC and the DTACS, except where noted.

- **Operating System:** CentOS 6.8 and later
- **Security Features:**
  - **Secure by Default** — OS is installed with minimal network services
  - **Networking**
    - SCP, SSH, FTP, and TFTP are the only network listening services installed for remote access; others are set to **off** or configured for local machine access only

      Note: FTP and TFTP are not enabled as part of the platform OS, but are enabled during the deployment process of the EC/DTACS.
  - **Restricted Network Resources** — - Authorized users have access to all network resources, but the system itself has minimal exposure to the network, making unauthorized access very difficult
  - **System Auditing** — Linux Audit system provides a way to monitor security-relevant information on the EC/DTACS

Operating system defaults are set up during system installation.

Important: We recommend that you do **not** change the system defaults so that you retain the highest level of system security. Cisco Systems, Inc. is not responsible for any damage that might occur to your EC/DTACS or the network if you choose to change the system defaults.

System Access Overview

To promote maximum security, the methods available for accessing the EC/DTACS are restricted to the following:

- The **admin** user, created by default
- Users created with the **/dvs/admin/useradmin** script
- Remote terminal access which is also limited to the admin user or operator-created users on the EC/DTACS

To administer user accounts, the User Administration (useradmin) menu is delivered with the EC/DTACS.

Use the User Administration menu delivered with the EC/DTACS to create users that can log into the system remotely (using SSH) and can access the Administrative Console. The users you create with the menu on the EC/DTACS can also access the EC/DTACS locally on the console.

Important: When you create users on the EC/DTACS, two separate users with the same username are created:

- One instance of the user name is for remote terminal access and local console access (OS User).
- The other instance of the user name is for access to the Administrative Console (Web UI User).

Although the user name is exactly the same, the two instances of the user name must be managed separately after the user is created.

For example, changing the password for the OS user will not apply to the Web interface user. The passwords must be changed separately.

Notes:

- The User Administration script contains an option to change both user account passwords at the same time. However, this menu option requires you to set each password individually.
- The two passwords can be the same.

Accessing the root and dncs User Accounts

Important:

- Role-Based Access Control (RBAC) is no longer supported. Please follow the steps below to switch between different user accounts.
- The **ecadmin/dtacsadmin** user is used in examples for all Cisco DBDS documents pertaining to EC 8.0 and DTACS 5.0.
- Commands run as **root** user are shown with a **#** symbol.

  Example:

  ```
  [root@vodwater ~]#
  ```

- Commands run as an **admin**, **dncs**, or any **Administrator** user are shown with a **$** symbol.

  Example:

  ```
  [admin@vodwater ~]$
  [ecadmin@vodwater ~]$
  [dtacsadmin@vodwater ~]$
  [dncs@vodwater ~]$
  ```

Once the EC/DTACS application installation is complete, you can only log in with the **admin** user account. The admin account is created by default during the installation, and is granted privileges to access the root user account, as root login is not permitted. These privileges allow the admin user to execute root commands by preceding the command with "sudo". For example, if you want to modify a network configuration file, the command will resemble the following:

Example: Executing a root command as admin user:

```
[admin@vodwater ~]$ sudo vi
/etc/sysconfig/network-scripts/ifcfg-eth0
```

As **admin** user, you can also change to the root user account by entering the following command.

Important: For any procedure in this guide that states "As root user", you must be logged into a terminal window as admin user and switch to the root user.

Command Syntax: Changing to root user:

```
[admin@vodwater ~]$ sudo –i
```

Any ***Administrator*** account that you create using the useradmin script (see the next section) has privileges to log into the EC/DTACS from a terminal window. Administrator accounts do not have privileges to access the root user account, but should be used to access the dncs user account.

Important: Do not access the dncs user account using the root user account.

To switch to the **dncs** user, type the following command from the terminal window where you are logged in as an Administrative user.

Important: For any procedure that states "As dncs user", you need to execute this command from the terminal window where you are logged in with your Administrator account.

Command Syntax: Changing to the dncs user:

```
[ecadmin@vodwater ~]$ sudo su – dncs
```

Note: Throughout all Cisco DBDS documentation, the **ecadmin/dtacsadmin** user is used as an example.

Overview:

Terminal Window Logged in as:	Use Account to change to:	Command to execute:
admin	root	sudo -i
[Administrator] **Example:** ecadmin/dtacsadmin	dncs	sudo su - dncs

Accounts and Access Control

Important:

- You cannot log in directly or remotely to the EC/DTACS as the **dncs** user.
- You cannot log in remotely to the EC/DTACS as the **root** user.
- You will need to set up individual user accounts for everyone who uses the EC/DTACS, including support personnel and third-party applications.
- See ***User Account Defaults*** (on page 20) for more information.

Accounts Available on the EC/DTACS Systems

The following accounts are available an EC/DTACS system:

- **root User** — The root user is the system administrator account and has all privileges and rights ***except*** for direct access to the system and for access to the EC/DTACS Web User Interface (Web UI)
- **admin User**
  - The admin account is created by default
  - Can directly log into the EC/DTACS
  - Can log into the system from the VMware console
  - By default, can change to the root user by executing the **sudo -i** command
  - Can also execute all root privileges by preceding a command with **sudo**
  - Does not have access to the EC/DTACS Web UI
- **Administrator**
  - Can log into the EC/DTACS system
  - Has permission to change to the dncs user
  - Has access to the EC/DTACS Web UI
  - Can log into the system from the VMware console
  - Can log into the system remotely
- **Operator**
  - Can view logs and other application files
  - Can log into the system from the VMware console
  - Can log into the system remotely

- **Regular Users**
  - Do ***not*** have permission to view application logs or other application files
  - Can log into the system from a VMware console
  - Can log into the system remotely

Account Privileges for the EC/DTACS Application

Account	Web UI Access (Admin Console)	Remote Login	VMware Console Login	Files*		Commands		
				Read	Write	Read	Write	Alter
Root	N	N	Y	Y	Y	Y	Y	Y
admin	N	Y	Y	Y	Y	Y	Y	Y
dncs	N	N	N	Y	Y	Y	Y	N
dbreader	N	N	N	N	N	Y	N	N
Administrator	Y	Y	Y	Y	N	N	N	N
Operator	N	Y	Y	Y	N	N	N	N
Regular	N	Y	Y	N	N	N	N	N
Command 2000	N	Y	Y	Y	Y	Y	Y	N

2

Sessions

Introduction

This chapter discusses sessions, including how to log in, how to deal with timeouts and session locks, and how to kill sessions.

In This Chapter

Logging into the EC/DTACS

In several procedures in this document, you will see a reference to *log into the EC/DTACS*. When you see this reference, you can use one of the following methods to log into the system:

Important: Direct root login is not permitted.

- From the vSphere/vCenter VM console:
  - Log in using the **admin** user account or using any account created by the useradmin script
- From a terminal window using SSH and a valid user account on the EC/DTACS:
  - Open a terminal window on a remote system
  - SSH to the EC/DTACS with a valid user account

With either of these methods, you will have Command Line Interface (CLI) access to the EC/DTACS. You can administer the system as appropriate from your workstation. From the same workstation, you may access the EC/DTACS Web UI using a supported Web browser using an Administrator user account.

Session Limitations

You can only have one active OS login session for any single username.

Notes:

- Session limits do NOT apply to remote Web UI access to the Administrative Console.
- Session limitations do NOT apply to the following users:
  - dncs
  - admin
  - root
  - dncsftp
  - dncsSSH
  - easftp
  - informix
  - Existing users:
    - Users that existed before the SR upgrade that included the security enhancements
    - Users that existed before the security enhancements were enforced

      Note: This restriction can be changed for a user by using the useradmin script. Refer to the next section for the procedure.

Overriding EC/DTACS Session Limitations

By default, users are restricted to having one active OS login session. This section describes how to override this default.

1. As **admin** user, enter the following command to modify the session limit for an operator-created user (for example, ecadmin). The USER ADMINISTRATION MENU window opens.

   ```
   [admin@vodwater ~]$ sudo /dvs/admin/useradmin
   ```

2. Type **j** and press **Enter**. You are prompted to type the login name for the user.
3. Type the user name and press **Enter**. You are prompted to enter the number of sessions this user can have open.
4. Type the value (for example, 5) and press **Enter**. You are prompted to confirm this value.
5. Type **y** and press **Enter**. You are returned to the main menu.

6 Type **q** to exit the script.

Session Limit Exceeded

If the maximum number of sessions have been reached and a new connection to the session is attempted, the session will close. To workaround this issue, one of the following must occur:

- An existing connection to the session must be closed.
- The system administrator must increase the number of sessions for this user by executing the useradmin script.

Session Timeout

Session Timeout Defaults

Notes:

- Session timeout does NOT apply to remote web access to the Administrative Console
- Session timeout affects all users, including the root user
- Session timeout also affects SSH, the VM console, and shells launched during a session

The system will close an OS login session that has been idle for a configurable period of time. After a session is closed, users must log back into the system.

- Session timeout default time: 30 minutes (1800 seconds)
- Recovery: User logs in again

Changing the Session Timeout

You can change the OS login session timeout default for an individual user or for a session.

Important: We recommend that only the system administrator perform these procedures.

Changing the Session Timeout Default for a User

1. As **admin** user on the system, enter the following command to change to open the sshd_config file in a text editor.

   ```
   [admin@vodwater ~]$ sudo vi /etc/ssh/sshd_config
   ```

2. Modify the values for the following parameters:

   Note: This example sets the timeout to 300 seconds (5 minutes).

   - ClientAliveInteveral 300
   - ClientAliveCountMax 0
   - TCPKeepAlive yes

3. Save and close the file.
4. Enter the following command to restart the sshd service.

   ```
   [admin@vodwater ~]$ sudo service sshd restart
   ```

Session Lock

Session Lock Defaults

The system will lock an OS user account after a configurable number of unsuccessful OS login attempts. After the account is locked, the admin user can unlock the account with sudo root access.

Note: Session lock does NOT apply to web access to the Administrative Console.

- The default number of unsuccessful login attempts before the user account is locked is 5
- Recovery: the admin user with sudo root access must reset the user account

Refer to ***Unlocking a User Account*** (on page 15) for the procedure to unlock a user account.

Changing the Session Lock Number

1. As **admin** user, enter the following command to open the **system-auth** file in a text editor.

   ```
   [admin@vodwater ~]$ sudo vi /etc/pam.d/system-auth
   ```

2. Locate the following line in the **system-auth** file:

   ```
   auth        required      pam_tally2.so onerr=fail deny=5 unlock_time=300
   ```

3. Edit the deny variable (`deny=5`) to match the desired number of failed login attempts before the account is locked for the time period specified (`unlock_time=300`).

   Important:

   - We recommend that you not edit the PAM modules as incorrect settings can lock every account out of the system.
   - **DO NOT** set this number to 0 (zero). This provides 0 attempts to log into the system.

4. Save and close the **system-auth** file.
5. Log out of the system and log back in to make the changes effective.

Locking a User Account

Note: Account locking is not applicable to the Web UI users on the EC/DTACS.

1 As **admin** user, type the following command to launch the USER ADMINISTRATION MENU.

```
[admin@vodwater ~]$ sudo /dvs/admin/useradmin
```

2 Type **g** (option for Lock User Account) and press **Enter**.

3 When prompted to enter the user, type the **user login name** of the user whose account you want to lock and press **Enter**. A confirmation message displays.

4 Type **y** and press **Enter** to lock the user account. The user account is locked and you are returned to the USER ADMINISTRATION MENU.

Note: The user will not be able to log in until the account is unlocked.

5 Type **q** to exit the utility.

Unlocking a User Account

1 As **admin** user, type the following command to launch the USER ADMINISTRATION MENU.

```
[admin@vodwater ~]$ sudo /dvs/admin/useradmin
```

2 Type **h** (option for Unlock User Account) and press **Enter**.

3 When prompted to enter the user, type the **user login name** of the user whose account you want to unlock and press **Enter**. A confirmation message displays.

4 Type **y** and press **Enter** to unlock the user account. The user account is unlocked and you are returned to the USER ADMINISTRATION MENU.

Note: The user account retains the original password. To change the password, refer to Changing User Account Passwords.

5 Type **q** to exit the utility.

Login Time Limit

Time Limit to Login

The system will stop responding after a configurable number of seconds if the user does not log into the OS during that time.

Note: The session login time does NOT apply to remote web access to the Administrative Console.

- Default number of seconds before sessions stop: 2 minutes
- Recovery: User must restart and log into sessions again

  Note: Some software behaves differently from others as some freeze and must be restarted, while others do not freeze but must be logged into again.

Changing the Login Time Limit for SSH and SFTP

1. As **admin** user, enter the following command to open the **sshd_config file** in a text editor.

   ```
   [admin@vodwater ~]$ sudo vi /etc/ssh/sshd_config
   ```

2. Locate the following line in the login file:

   ```
   #LoginGraceTime 2m
   ```

3. Delete the comment symbol, #, and edit the value.
4. Change the login time limit to the time that you prefer.

   Notes:

   - To enter the value in seconds, simply type the value.
   - To enter the value in minutes, append an "m" to the value.

     Examples:

     – To enter a login time limit of **3 minutes**, change the field to `LoginGraceTime 180` or `LoginGraceTime 3m`

     – To disable the login time limit, change the field to `LoginGraceTime 0`
   - We recommend that you keep the time limit as short as possible. This helps prevent unauthorized use of your system.
5. Save and close the **sshd_config** file.
6. Type the following command to restart the sshd service.

   ```
   [admin@vodwater ~]$ sudo service sshd restart
   ```

Killing a Session

There might be times when a user closes an OS login session, but the session 'hangs' without closing; that is, the system still considers the session active even though the user terminated the session. If this happens, the user cannot start a new session until the session timer expires.

If the user needs to start a new session immediately, the admin user can kill a hung session using the following instructions.

1. Open a terminal window on the system.
2. As **admin** user, type the following command and press **Enter** to search for the ssh process.

   Command Syntax:

   ```
   ps -ef | grep [username]
   ```

   Example:

   ```
   [admin@vodwater ~]$ ps -ef | grep operator1
   ```

   Example Output:

   ```
   root      6364  6021  3 12:45 ?        00:00:00 sshd: operator1 [priv]
   907       6402  6364  0 12:45 ?        00:00:00 sshd: operator1@pts/1
   admin     6435  5661  0 12:45 pts/0    00:00:00 grep  operator1
   ```

3. Locate the PID for the ssh process. In the example above, it is **6402** (the second line).
4. Type the following command to kill the ssh process for this user.

   Command Syntax:

   ```
   sudo kill [PID]
   ```

   Example:

   ```
   [admin@vodwater ~]$ sudo kill 6402
   ```

5. Repeat Step 2 to verify that the session is no longer present.

   Example Output:

   ```
   admin     6531  5661  0 12:47 pts/0    00:00:00 grep operator1
   ```

3

User Accounts

Introduction

This chapter discusses user accounts, including how to add, edit, and delete user accounts.

Important: If your password management and/or user account management is administered by an external LDAP, RADIUS, or Sudo system, you must manage your passwords and user accounts on that system and not on the EC/DTACS.

In This Chapter

User Account Defaults

Regular User

- Can log into the operating system
- Cannot read or write EC/DTACS files
- Cannot execute EC/DTACS application files unless explicitly given sudo access
- Cannot switch to the dncs user

Operator

- Can log into the operating system
- Can read but cannot write EC/DTACS files
- Cannot execute EC/DTACS application files unless explicitly given sudo access
- Cannot switch to the dncs user

Administrator

- Can log into the operating system
- Can read but not write EC/DTACS files
- Cannot execute EC/DTACS application files unless explicitly given sudo access
- Can switch to the dncs user. Once switched to the dncs user:
  - Can read and write EC/DTACS application files
  - Can execute EC/DTACS application executable files

Creating a User Account

Important: If your password management and/or user account management is administered by an external LDAP, RADIUS, or Sudo system, you must manage your passwords and user accounts on that system and not on the EC/DTACS.

All applications (including third-party applications) and users who access the applications require an updated user account. You cannot log into the applications using the generic dncs user credentials.

Note: The user will be required to change their password during their first successful operating system login session.

Important: We recommend creating an individual username for each user that will access the system. We do **NOT** recommend creating a single, generic username for use by multiple users.

Follow these steps to create a user account on the EC/DTACS system.

1 As **admin** user, enter the following command to create a user account. The USER ADMINISTRATION MENU opens.

```
[admin@vodwater ~]$ sudo /dvs/admin/useradmin
```

2 Type **a** and press **Enter**. You are prompted to confirm adding a new user.

3 Type **y** (for yes) and press **Enter**. You are prompted to select the type of user to add to the system.

4 Type the number of the type of user you want to create:

- 1: Add Regular User
- 2: Add Operator
- 3: Add Administrator

Example: To add a regular user, type **1**.

Note: See ***User Account Defaults*** (on page 20) for more information on the user types.

5 Type the name of the new user account and press **Enter**.

Notes:

- The username must be between 6 and 32 characters.
- The username can only contain alphanumeric characters and the underscore (_) special character.

Result: The **Do you wish to continue adding this user (Y/N)?** message appears.

6 Type **y** and press **Enter**.

7 At the **New password** prompt, enter a password for this user and press **Enter**.

Note: This is a temporary password and must be changed at the first login.

8 At the **Retype new password** prompt, enter the password again and press **Enter**.

9 Did you select the option to create an Administrator account (option 3 in step 4)?

- If **no**, the **Choose Type of User to Add** menu reappears. Go to Step 10.
- If **yes**, the system prompts for the Web UI password. Follow these steps and then go to Step 10:

  Note: This can be the same password as the system password you set for this user.

  a At the **New password** prompt for Web UI access, enter a password for this user and press **Enter**.

  b At the **Retype new password** prompt, enter the password again and press **Enter**.

10 Do you need to add another user?

- If **yes**, repeat this procedure starting from step 4.
- If **no**, type **q** (for quit) to close this menu and type **q** again to exit the script.

Deleting a User Account

Use this procedure to delete users that were added using the useradmin script.

Important: Do not delete any default users on the system.

1. As **admin** user, enter the following command to create a user account. The USER ADMINISTRATION MENU opens.

   ```
   [admin@vodwater ~]$ sudo /dvs/admin/useradmin
   ```

2. Type **b** and press **Enter**. You are prompted to enter the user name you want to delete.
3. Type the **user name** and press **Enter**. A confirmation message is displayed.
4. Type **y** and press **Enter**. The user is removed from the system.

sudo Access to EC and DTACS Commands

The EC/DTACS includes sudo functionality and configuration files that allow the system administrator to grant users, or groups of users, access to specific EC/DTACS and database commands.

This section includes procedures to grant users sudo access to these commands. With sudo access, the system administrator can grant specific "Operator" users the ability to execute designated commands but prevent the user direct access to the dncs user account or to other resources such as the database.

Groups That Can Execute sudo Commands

A specific group of users on the EC/DTACS can be granted access to the sudo command aliases in configuration files created by the system administrator. The system administrator then adds specific users to these groups. The group configuration files must be created and placed in the **/etc/sudoers.d/** directory on the EC/DTACS.

Commands Accessible Using sudo

The commands available for sudo access are defined using command aliases (Cmnd_Alias) in the privileges files located under **/etc/sudoers.d/**. The EC/DTACS includes several privileges files with various command aliases. These files should not be modified. Custom privilege files must be created by the system administrator if additional command aliases are required.

The following is a list of privileges files included with the **EC**.

	Absolute Path of Privilege File	Example Commands
EC	/etc/subdoers.d/90-ec.privileges	dncsStart logLvl dncsControl
Application Server	/etc/subdoers.d/90-appserv.privileges	appStop applogLvl
Backup/Restore	/etc/sudoers.d/90-backup_restore-privileges	backupDatabase restoreKeyFiles

The following is a list of privileges files included with the **DTACS**.

	Absolute Path of Privilege File	Example Commands
DTACS	/etc/subdoers.d/90-dtacs.privileges	dtacsStart logLvl dtacsControl
Backup/Restore	/etc/sudoers.d/90-backup_restore-privileges	backupDatabase restoreKeyFiles

Creating a Group for sudo Access to EC/DTACS Commands

Complete the following steps to create a group for sudo access to your system.

Note: This example is on an EC system but it also pertains to a DTACS system.

1 As the **admin** user, enter the following command to create a group.

Note: Replace <group_name> with a unique name. This group name will be assigned to users to grant access to specific sudo commands.

Command Syntax:

```
sudo groupadd <group_name>
```

Example:

```
[admin@vodwater ~]$ sudo groupadd ncdsgroup
```

2 Enter the following command to verify that the group was successfully created on the system.

Command Syntax:

```
less /etc/group | grep -i [group_name]
```

Example:

```
[admin@vodwater ~]$ less /etc/group | grep -i ncds
```

Example Output:

```
ncdsgroup:x:518:
```

Adding Users to the Group

"Operator" and "Administrator" user accounts can be granted access to sudo commands. These account types have read access to the EC/DTACS files, which is required to execute many of the EC/DTACS commands using sudo.

Note: "Regular User" accounts do not have read access to EC/DTACS files, thus they are not recommended for sudo execution.

Complete the following steps to add users to the group you created in the previous procedure to allow sudo access to EC/DTACS commands.

1 Enter the following command to assign the group created in the previous procedure to a user. The command prompt is returned without error.

Command Syntax:

```
sudo usermod -a -G [group_name] [username]
```

Example:

```
[admin@vodwater ~]$ sudo usermod -a -G ncdsgroup operator1
```

2 Enter the following command to verify that the user was added to the group.

Command Syntax:

```
sudo less /etc/group | grep [group_name]
```

Example:

```
[admin@vodwater ~]$ sudo less /etc/group | grep ncdsgroup
```

Example Output:

```
ncdsgroup:x:518:operator1
```

3 Repeat Step 1 to add more users to the group, if necessary.

Creating a sudo Privilege File for the Group

1 Enter the following command to create a custom privileges file with visudo for the new group.

Command Syntax:

```
sudo visudo -f /etc/sudoers.d/[group_name]-privileges
```

Example:

```
[admin@vodwater ~]$ sudo visudo -f
/etc/sudoers.d/ncdsgroup-privileges
```

2 Add the following content to the file.

- Replace <group_name> with the group name created in ***Creating a Group for sudo Access to EC/DTACS Commands*** (on page 25).
- Replace <group_alias> with a unique group alias name (for example, NCDSGRP).

```
## This sudoers file provides access to specific privileged commands
##
## This file must be edited with the 'visudo -f goqam' command.


## Everyone in the system group "<group_name>" are covered by the
<group_alias> alias
User_Alias <group_alias> = %<group_name>


## Maintain the user's env and define the path for sudo execution
Defaults:<group_alias> !env_reset
Defaults:<group_alias> secure_path =
/sbin:/bin:/usr/sbin:/usr/bin:/opt/cisco/informix/server/bin
```

Example: <group_name>=ncdsgroup and <group_alias>=NCDSGRP

```
## This sudoers file provides access to specific privileged commands
##
## This file must be edited with the 'visudo -f goqam' command.


## Everyone in the system group "ncdsgroup" are covered by the
## NCDSGRP alias
User_Alias NCDSGRP = %ncdsgroup


## Maintain the user's env and define the path for sudo execution
Defaults:NCDSGRP !env_reset
Defaults:NCDSGRP secure_path =
/sbin:/bin:/usr/sbin:/usr/bin:/opt/cisco/informix/server/bin
```

3 Save and close the file. The privileges file is created and the system returns the command prompt without error.

Adding sudo Accessible Commands

Prior to adding a command, verify that it does not already exist in one of the Cmnd_Alias entries in the privileges files located under /etc/sudoers.d/. Add command aliases to custom privilege files. Do not add them to the privilege files included with the EC/DTACS.

1 Open the appropriate custom privileges file with visudo.

Note: Do not modify the privilege files included with the EC/DTACS. For ease of use, open the privilege file associated with the group that will execute the sudo command.

Command Syntax:

```
sudo visudo -f /etc/sudoers.d/<group_name>-privileges
```

Example:

```
[admin@vodwater ~]$ sudo visudo -f
/etc/sudoers.d/ncdsgroup-privileges
```

2 Add the **Cmnd_Alias** entry, along with the appropriate amount of notes, for the desired command.

Syntax:

```
Cmnd_Alias <alias_cmd_name>      = <full_path_to_command(s)>
```

Notes:

- Replace <alias_cmd_name> with a unique name to identify the command alias.
- Replace <full_path_to_command(s)> with the full path of the command or list of commands separated with a "," or full path with a wildcard to capture multiple files.

Example: Add a single command

```
## Define NCDS Privileged Commands
Cmnd_Alias NCDSGEN      = /dvs/dncs/Utilities/ncdsGen/ncdsGen
```

Example: Add multiple commands

```
## Define NCDS Privileged Commands
Cmnd_Alias NCDS    = /dvs/dncs/Utilities/ncdsGen/ncdsGen, \
                     /dvs/dncs/Utilities/ncdsGen/ncdsPush
```

Example: All commands that match a wildcard

```
## Define NCDS Privileged Commands
Cmnd_Alias NCDS    = /dvs/dncs/Utilities/ncdsGen/*
```

3 Save and close the file. The privileges file is updated and the system returns the command prompt without error.

Note: Warnings can be ignored.

Allowing Group Access to a sudo Command Alias

1 Open the group privileges file with visudo.

Command Syntax:

```
sudo visudo -f /etc/sudoers.d/<group_name>-privileges
```

Example:

```
sudo visudo -f /etc/sudoers.d/ncdsgroup-privileges
```

2 Add the following line with the appropriate amount of notes to assign a group alias access to a command alias.

Command Syntax:

```
<group_alias> ALL=(<username>) NOPASSWD: <alias_cmd_name>
```

Notes:

- Replace <group_alias> with the group alias name who will have access to the command(s) defined in the command alias.
- Replace <alias_cmd_name> with the command alias or list of command aliases separated by a comma (,).
- Replace <username> with the username that will be used to execute the command(s). *This will be either dncs or root.*
- The "NOPASSWD" option allows the users in the group alias to execute the command(s) in the command alias without providing its password.

Example: access to a single command alias

```
## Allow the NCDSGRP group alias access to the NCDS executables
## and execute as dncs
NCDSGRP ALL=(dncs) NOPASSWD: NCDS
```

Example: access to a list of command aliases

```
## Allow the DNCSOPGRP group alias access to various executables
DNCSOPGRP ALL=(dncs) NOPASSWD: DNCS_START, DNCS_STOP, DNCS_KILL,    \
                               DNCS_CTRL, SHOW_DB_SESS, KILL_DB_SESS,     \
                               START_WEB_SRV, STOP_WEB_SRV, DNCS_LOGLVL,  \
                               MODDHCT_CFG, MODDHCT_ADMIN, DELETE_SM, \
                               DELETE_HCT_CD, DELETE_DHCT, RELEASE_SESS,  \
                               DBACCESS, DOCTOR, APPSERV_START,           \
                               APPSERV_STOP, APPSERV_KILL, APPSERV_CTRL, \
                               APPSERV_LOGLVL
```

3 Save and close the file. The privileges file is updated and the system returns the command prompt without error.

Executing sudo Commands

1 From another terminal window, log into the EC/DTACS with the user you created in ***Adding Users to the Group*** (on page 26).

2 Enter the following command to display the sudo commands available for execution.

```
[operator1@vodwater ~]$ sudo -l
```

Example Output:

```
Matching Defaults entries for operator1 on this host:
    !visiblepw, always_set_home, env_reset, env_keep="COLORS DISPLAY HOSTNAME
HISTSIZE
    INPUTRC KDEDIR LS_COLORS", env_keep+="MAIL PS1 PS2 QTDIR USERNAME LANG
LC_ADDRESS
    LC_CTYPE", env_keep+="LC_COLLATE LC_IDENTIFICATION LC_MEASUREMENT
LC_MESSAGES",
    env_keep+="LC_MONETARY LC_NAME LC_NUMERIC LC_PAPER LC_TELEPHONE",
env_keep+="LC_TIME
    LC_ALL LANGUAGE LINGUAS _XKB_CHARSET XAUTHORITY",
    secure_path=/sbin\:/bin\:/usr/sbin\:/usr/bin, !env_reset,

secure_path=/sbin\:/bin\:/usr/sbin\:/usr/bin\:/opt/cisco/informix/server/bin


User operator1 may run the following commands on this host:
    (dncs) NOPASSWD: /dvs/dncs/Utilities/ncdsGen/ncdsGen
```

3 Enter the following command to execute a sudo command.

Command Syntax:

```
sudo -u <username> <full_path_to_command>
```

Example:

```
[admin@vodwater ~]$ sudo -u dncs
/dvs/dncs/Utilities/ncdsGen/ncdsGen -V
```

Example Output:

```
ncdsGen: 8.0.10
```

4

Password Management

Introduction

Regardless of password management rules enforced by a system, users must still be encouraged to choose difficult-to-guess (strong) passwords. Proper system management of passwords is important but the primary responsibility for strong passwords ultimately rests with the user.

Important: If your password management and/or user account management is administered by an external LDAP, RADIUS, or Sudo system, you must manage your passwords and user accounts on that system and not on the EC/DTACS.

In This Chapter

Password Guidelines

Note: These guidelines apply to all systems in your network.

Users must select a very strong, complex password. Strong passwords have the following general characteristics:

- Contain 8 or more characters
- Contain characters from at least three of the following:
  - Lower-case letters
  - Upper-case letters
  - Digits
  - Special characters
- Do **not** consist of only one character type (**aaaaaaa** or **11111111**)
- Do **not** contain any aspects of a date
- Are **not** proper names or words you would find in the dictionary
- Are **not** the same as previous passwords with an added capitalization
- Are **not** telephone numbers or similar numeric groups
- Are **not** user IDs, user names, group IDs, reversed user names, or other system identifiers
- Do **not** contain more than two (2) consecutive occurrences of the same character
- Are **not** consecutive keyboard patterns (for example, **qwerty**)
- Are **not** the product name, the manufacturer name, or variants thereof

System Password Retention

The system sets the following restrictions on re-using passwords:

- The system retains the last 5 passwords each user uses.
- The system does not allow you to re-use any of the last 5 passwords each user has used.

Changing User Account Passwords

Important: If your password management and/or user account management is administered by an external LDAP, RADIUS, or Sudo system, you must manage your passwords and user accounts on that system and not on the EC/DTACS.

Our recommendations for the following account passwords are as follows:

- **informix account:** Do not change the informix account password. Remote login for this user is disabled by default.
- **dncsSSH account:** Do not change the dncsSSH account password. Remote login for this user is disabled by default.
- **easftp and dncsftp accounts (EC only):** Modifying these account passwords should be done only in collaboration with the administrators of the EAS, EC, third-party systems, and billing systems.

A user account password can be changed by the root user or the admin user with sudo root access.

Changing User Passwords From the Command Line

Complete the following steps to change the password for a user.

1 As **admin** user, enter the following command and press **Enter**.

Command Syntax:

```
sudo passwd [username]
```

Example:

```
[admin@vodwater ~]$ sudo passwd operator1
```

2 At the **New password** prompt, enter a new password and press **Enter**.

3 At the **Retype new password** prompt, re-enter the new password and press **Enter**. The following message displays:

```
passwd: all authentication tokens updated successfully.
```

Changing User Passwords Using the useradmin Script

Follow these steps to change the password for a user account created with the useradmin script.

1. As **admin** user, enter the following command and press **Enter**. The USER ADMINISTRATION MENU opens.

   ```
   [admin@vodwater ~]$ sudo /dvs/admin/useradmin
   ```

2. Type **i** and press **Enter**. You are prompted to enter the user name whose password you want to change.
3. Type the user login name and press **Enter**. You are prompted to confirm this action.
4. Type **y** and press **Enter**.
5. At the **New password** prompt, enter a new password and press **Enter**.
6. At the **Retype new password** prompt, re-enter the new password and press **Enter**.
7. Is the user account an Administrative account?
   - If **no**, type `q` to exit the script.
   - If **yes**, you are prompted to change the password for Web UI access.
8. At the **New password** prompt, enter a new password for the Web UI and press **Enter**.
9. At the **Retype new password** prompt, re-enter the new password for the Web UI and press **Enter**.
10. Type **q** to exit the script.

Changing the Administrative User Web UI Password

Use this procedure to change an existing administrative user Web UI password.

1 As **admin** user, enter the following command to change the Web UI password of an administrative user on the EC/DTACS.

Command Syntax:

```
sudo /usr/bin/htdigest /etc/httpd/user-conf/CSCOec.digest
"Cisco DNCS" [username]
```

Example:

```
[admin@vodwater ~]$ sudo /usr/bin/htdigest
/etc/httpd/user-conf/CSCOec.digest "Cisco DNCS" ectestuser
```

2 When prompted for the new password, type the new password and press **Enter**.

3 When prompted to re-enter the password, type the new password again and press **Enter**. The system compares the two password entries.

4 Did the **They don't match, sorry** message appear?

- If **yes**, the two passwords do not match. Go back to Step 1 and re-type the command.
- If **no**, the system prompt is returned. You are finished with this procedure.

Password Expiration Period

Password Expiration Period Defaults

If your password management and/or user account management is administered by an external LDAP, RADIUS, or Sudo system, you must manage your passwords and user accounts on that system and not on the EC. For more information, see ***Enable RADIUS and LDAP Support Configuration Guide for EC 8.0 and DTACS 5.0*** or contact your system administrator for more information.

WARNING:

Do not enable password aging for any of the default users or roles (root, dncs, informix, dncsSSH, dncsftp, or easftp). The system (or components within the system) will become unstable if any of these default user or role passwords expire.

Password Expiration for Critical (Default) Users

Password expiration is disabled for all critical users (also known as *default users*) on the system by default. Critical users are defined as the following users:

- root
- dncs
- informix
- dncsSSH
- easftp

If you turn on password aging for these users, and the passwords expire without updating, the system will become unstable in the following ways:

- The account is locked
- All services that use OS-level authentication fail
- Users cannot login as that user
- All cron jobs related to these users fail (specifically the root, dncs, and informix users)
- All FTP into the EC fail (for example, easftp user)
- All SSH communication between the EC and the DTACS fail

We strongly recommend **NOT** enabling password expiration for critical users on the EC/DTACS.

Password Expiration for All Other Users

For all other users on the system:

- The default number of weeks a password is valid: 13
- The default number of weeks prior to password expiration when the user receives a warning message to change passwords: 2
- The default values are applied to a user account at the time it is created
- Recovery: Administrator must reset the user account by changing the password

Notes:

- The default values are applied to an OS user account at the time the account is created.
- Password expiration does not apply to web access login accounts.

Changing a User Password Expiration Period

Use the following procedure to change the password expiration period for an individual user account.

WARNING:

Do not enable password aging for any of the default users (for example, admin, root, dncs, informix, dncsSSH, dncsftp or easftp). The system (or components within the system) will become unstable if any of these default user passwords expire.

1 As **admin** user, enter the following command to change the password expiration for a user password.

Command Syntax:

```
passwd -x [days] [username]
```

Example:

```
[admin@vodwater ~]$ sudo passwd -x 91 operator1
```

2 Enter the following command to verify the expiration period for the user.

Command Syntax:

```
passwd -x [days] [username]
```

Example:

```
[admin@vodwater ~]$ sudo chage -l operator1
```

Note: The `-l` in the above command is a lowercase L.

Example Output:

```
Last password change                                  : Dec 12, 2017
Password expires                                      : Mar 12, 2018
Password inactive                                     : never
Account expires                                       : never
Minimum number of days between password change        : 7
Maximum number of days between password change        : 91
Number of days of warning before password expires     : 14
```

Disabling a User Password Expiration Period

Use the following procedure to change the password expiration period for an individual user account.

1 As **admin** user, enter the following command to disable the password expiration period for a specific user.

Note: The -l in the below command is lowercase L.

Command Syntax:

```
passwd -x [No of days] [account name]
```

Example:

```
[admin@vodwater ~]$ sudo passwd -x 9999999 operator1
```

2 Enter the following command to verify the expiration period for the user.

3 **Command Syntax**:

```
chage -l [username]
```

Example:

```
[admin@vodwater ~]$ sudo chage -l operator1
```

Example Output:

```
Last password change                                  : Dec 12, 2017
Password expires                                      : never
Password inactive                                     : never
Account expires                                       : never
Minimum number of days between password change        : 7
Maximum number of days between password change        : 99999999
Number of days of warning before password expires     : 14
```

5

SSH, SFTP, and SCP Connections

Introduction

This chapter discusses SSH, SFTP, and SCP connections, including security file errors and changing the connection retries parameter.

In This Chapter

Overview

SSH, SFTP, and SCP connections use the RETRIES and the MaxAuthTries parameters to control the maximum number of login attempts. You typically want the MaxAuthTries parameter value to be one less than the RETRIES parameter value.

Notes:

- With SSH and SFTP, these attempts are password attempts only, not username/password combination attempts.
- If the RETRIES parameter value is lower than the MaxAuthTries parameter value, the RETRIES value takes precedence.
- If the MaxAuthTries parameter value is lower than the RETRIES parameter value by 2 or more, the MaxAuthTries value takes precedence.
- The maximum value for the RETRIES parameter is 15.
- Some clients have their own retries parameters. These usually override the system retries parameters.

Using SSH

SSH is an encrypted remote login protocol that is used to securely log onto remote systems in the network. Once you are remotely logged into another system, you can execute commands according to the permissions of the user you used to log in as.

Notes:

- When you use SCP to login to the system, use your individual username and password.
- You can only have one active session for each username. Consider setting up additional usernames if you require multiple sessions open at the same time.

Complete the following steps to remotely log in to another system.

1 Open an xterm window on your local system.

2 Type the following command and press **Enter**. You are prompted for the user password.

Command Syntax:

```
ssh [username]@[IP address of remote system]
```

Example:

```
[admin@vodwater ~]$ ssh admin@10.90.47.67
```

Example Output:

```
############################## WARNING!!! ###################################
################## READ THIS BEFORE ATTEMPTING TO LOGON ##################
#                                                                        #
#    This System is for the use of authorized users only.  Individuals   #
#    using this computer without authority, or in excess of their        #
#    authority, are subject to having all of their activities on this    #
#    system monitored and recorded by system personnel.  In the course   #
#    of monitoring individuals improperly using this system, or in the   #
#    course of system maintenance, the activities of authorized users    #
#    may also be monitored.  Anyone using this system expressly          #
#    consents to such monitoring and is advised that if such             #
#    monitoring reveals possible criminal activity, system personnel     #
#    may provide the evidence of such monitoring to law enforcement      #
#    officials.  You cannot copy, disclose, display or otherwise         #
#    communicate the contents of this server except to other Cisco       #
#    employees who have been authorized to access this server.           #
#                                                                        #
########################## Confidential Information ######################

admin@10.90.47.67's password:
```

3 Did an error occur while attempting to login to the system?

- If **no**, go to Step 9.
- If **yes** and the following error displayed, go to the next step.

  Notes:

  – Because the EC/DTACS is configured for strict RSA key checks, this error occurs if the remote host has been replaced or the OS has been reinstalled. Go to Step 5.

  – If neither scenario has happened, it is possible that something malicious is going on. In this case, contact Cisco Services.

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@

IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!

Someone could be eavesdropping on you right now (man-in-the-middle
attack)!
It is also possible that the RSA host key has just been changed.
The fingerprint for the RSA key sent by the remote host is
6c:e1:cf:83:41:1a:e4:06:bd:2b:7e:9c:0e:55:a1:88.
Please contact your system administrator.
Add correct host key in /.ssh/known_hosts to get rid of this message.
Offending key in /.ssh/known_hosts:13
RSA host key for 10.90.47.67 has changed and you have requested strict
checking.

Host key verification failed.
```

4 As **admin** user, enter the following command to open the **/.ssh/known_hosts** file in a text editor.

```
[admin@vodwater ~]$ sudo vi /.ssh/known_hosts
```

5 Search for the IP address of the system giving the error.

Note: From the above example, you would search for 10.90.47.67 in the file.

6 Delete the line containing the IP address.

7 Save and close the file.

8 Try to login again using the SSH protocol.

9 When prompted to enter the password of the user you are logging in as, type the password and press **Enter**. You are logged into the system.

Using SFTP

SFTP is used to securely transfer files between a local host and a remote host that allows you to use interactive commands (for example, list remote directories, create/delete directories, remove files). The ability to use interactive commands are all subject to system permissions.

Important: If your site requires SFTP support, go to the next section.

Notes:

- When you use SFTP to login to the system, use your individual username and password.
- You can only have one active session for each username. Consider setting up additional usernames if you require multiple sessions open at the same time.

Setting Up SFTP Support

Important:

- Only complete the procedures in this section if SFTP support is required at your site.
- For DTACS systems, the SFTP user can be used to communicate with an AGI Adapter provided you have configured an AGI Adapter.

This section describes how to add an SFTP user for SFTP support. It also includes procedures to restrict SFTP to a single home directory.

Creating a User for SFTP Support

Complete the following procedure to create an SFTP user.

1. As **admin** user, enter the following command to create an SFTP user. The USER ADMINISTRATION MENU displays.

   ```
   [admin@vodwater ~]$ sudo /dvs/admin/useradmin
   ```

2. Type **a** and press **Enter**.
3. When prompted to add a new user, type **y** and press **Enter**.
4. Type **1** and press **Enter** to add a regular user.
5. At the **New Username** prompt, type a name for this user (for example, sftpuser1).
6. When prompted to continue to add this user, type **y** and press **Enter**.
7. At the **New password** prompt, enter a new password (for example, sftpuser1) and press **Enter**.
8. At the **Retype a new password** prompt, re-enter the password and press **Enter**.

9 Type **q** to exit from adding any other users.

10 Type **q** to exit the USER ADMINISTRATION MENU. You are returned to an admin prompt.

11 Enter the following command to reset the password for the SFTP user.

Command Syntax:

```
sudo passwd [SFTP-username]
```

Example:

```
[admin@vodwater ~]$ sudo passwd sftpuser1
```

12 When prompted, enter the same or a new password for the SFTP user.

13 When prompted to re-enter the password, re-enter it.

Important: By default, the password for the SFTP user will expire in 91 days. Your system administrator must decide the password expiration policies for the SFTP user.

Creating a Directory for SFTP File Transfers

Complete the following steps to create a directory that restricts SFTP access to a single home directory. The directory you create and all directories above it *must* be owned by root and have write permissions only for root.

Note: This directory must be created under /dvs.

1 Enter the following command to create a directory in **/dvs**.

Command Syntax:

```
sudo mkdir /dvs/[SFTP-home-directory]
```

Example:

```
[admin@vodwater ~]$ sudo mkdir /dvs/sftpuser1
```

2 Enter the following command to set the ownership of the new SFTP home directory to **root:root**.

Command Syntax:

```
sudo chown root:root /dvs/[SFTP-home-directory]
```

Example:

```
[admin@vodwater ~]$ sudo chown root:root /dvs/sftpuser1
```

3 Enter the following command to update the permissions of the SFTP home directory to **0755**.

Command Syntax:

```
sudo chmod 0755 /dvs/[SFTP-home-directory]
```

Example:

```
[admin@vodwater ~]$ sudo chmod 0755 /dvs/sftpuser1
```

4 Enter the following command to create an upload directory under the new SFTP home directory and then change its ownership to the SFTP user with a directory permission of **0700**.

Command Syntax:

```
sudo mkdir /dvs/[SFTP-username]/[upload-directory]
sudo chown [SFTP-username]:[SFTP-username]
/dvs/[SFTP-username]/[upload-directory]
chown root:root /dvs/[SFTP-home-directory]
```

Example:

```
[admin@vodwater ~]$ sudo mkdir /dvs/sftpuser1/uploads
[admin@vodwater ~]$ sudo chown sftpuser1:sftpuser1
/dvs/sftpuser1/uploads
[admin@vodwater ~]$ sudo chmod 0700 /dvs/sftpuser1/uploads
```

Restricting SFTP Access to a Single Directory

Complete the following steps to restrict SFTP access to a single directory.

1 Open the **/etc/ssh/sshd_config** file in a text editor.

```
[admin@nextxVM ~]$ sudo vi /etc/ssh/sshd_config
```

2 Go to the end of the file and add the following content:

Command Syntax:

```
Match User [SFTP-username]
ForceCommand internal-sftp
PasswordAuthentication yes
ChrootDirectory /dvs/[SFTP-home-directory]
PermitTunnel no
AllowAgentForwarding no
AllowTcpForwarding no
X11Forwarding no
```

Example:

```
Match User sftpuser1
ForceCommand internal-sftp
PasswordAuthentication yes
ChrootDirectory /dvs/sftpuser1
PermitTunnel no
AllowAgentForwarding no
AllowTcpForwarding no
X11Forwarding no
```

3 Enter the following command to restart the **sshd** service.

```
[admin@nextxVM ~]$ sudo service sshd restart
```

Verifying the SFTP Configuration

Complete the following steps to verify the SFTP configuration.

1 Enter the following command to verify that you cannot complete an SSH request as SFTP user.

Command Syntax:

```
sudo ssh [SFTP-username]@localhost
```

Example:

```
[admin@vodwater ~]$ sudo ssh sftpuser1@localhost
```

2 Enter the following command to verify that you can successfully execute an SFTP file transfer.

Command Syntax:

```
sudo sftp[SFTP-username]@localhost
```

Example:

```
[admin@vodwater ~]$ sudo sftp sftpuser1@localhost
```

3 When prompted, enter the password for the SFTP user. You are connected to local host and a sftp prompt displays.

4 At the **sftp>** prompt, type **dir**. Your SFTP upload directory should display. You should be able to read and write into the directory.

Example:

```
sftp> dir
uploads
sftp>
```

5 Attempt a file transfer to the directory.

Opening an SFTP Session

Complete the following steps to open a session using SFTP.

1 Open an xterm window on the system.

2 Type the following command and press **Enter**. You are prompted for the user password.

Command Syntax:

```
sftp [username]@[IP address of the system]
```

Example:

```
[admin@vodwater ~]$ sftp admin@10.90.47.67
Connecting to 10.90.47.67...
The authenticity of host '10.90.47.67 (10.90.47.67)' can't be
established.
RSA key fingerprint is
d3:6f:52:47:cc:53:27:bf:d7:70:d5:f1:ae:f0:0e:e4.
Are you sure you want to continue connecting (yes/no)?
```

3 When prompted to continue to connect to the server, type **yes** and press **Enter**. The following displays.

Example Output:

```
Warning: Permanently added '10.90.47.67' (RSA) to the list of known hosts.
############################## WARNING!!! ###################################
################## READ THIS BEFORE ATTEMPTING TO LOGON ##################
#                                                                        #
#    This System is for the use of authorized users only.  Individuals   #
#    using this computer without authority, or in excess of their        #
#    authority, are subject to having all of their activities on this    #
#    system monitored and recorded by system personnel.  In the course   #
#    of monitoring individuals improperly using this system, or in the   #
#    course of system maintenance, the activities of authorized users    #
#    may also be monitored.  Anyone using this system expressly          #
#    consents to such monitoring and is advised that if such             #
#    monitoring reveals possible criminal activity, system personnel     #
#    may provide the evidence of such monitoring to law enforcement      #
#    officials.  You cannot copy, disclose, display or otherwise         #
#    communicate the contents of this server except to other Cisco       #
#    employees who have been authorized to access this server.           #
#                                                                        #
########################## Confidential Information ######################
admin@10.90.47.67's password:
```

4 When prompted to enter the password of the user you are connecting as, type the password and press **Enter**. A sftp prompt displays.

5 Type the directory path you want to navigate to and press **Enter**.

Command Syntax:

```
cd /[target directory]
```

Example:

```
sftp> cd /var/tmp
```

6 Use one of the following options to transfer a file between the systems.

- **Transfer a file from the system to your computer,** type **get [target file]** and press **Enter**.
- **Transfer a file from your computer to the system,** type **put [target file]** and press **Enter**.

Note: If the file transfer fails, make sure that both directories and files have the correct permissions. The following permissions are required for the Administrator and Operator accounts.

- If the directory is owned by the **root** user:

```
drwxr-xr-x 2     root  root  512   Aug 24 14:49     [target
directory]
```

- If the directory is owned by the **dncs** user:

```
drwxr-xr-- 2     dncs  dncs  512   Aug 24 14:49     [target
directory]
```

- If the file is owned by the **root** user:

```
-rw-r--r-- 1     root  root  2568  Aug 24 14:49     [target
directory]
```

- If the file is owned by the **dncs** user:

```
-rw-r----- 1     dncs  dncs  2568  Aug 24 14:49     [target
directory]
```

Changing the SSH and SFTP Connection Retries Parameter

SSH, SFTP, and SCP connections use the RETRIES and the MaxAuthTries parameters to control the maximum number of login attempts. You typically want the MaxAuthTries parameter value to be one less than the RETRIES parameter value.

Notes:

- With SSH and SFTP, these attempts are password attempts only, not username/password combination attempts.
- If the RETRIES parameter value is lower than the MaxAuthTries parameter value, the RETRIES value takes precedence.
- If the MaxAuthTries parameter value is lower than the RETRIES parameter value by 2 or more, the MaxAuthTries value takes precedence.
- The maximum value for the RETRIES parameter is 15.
- Some clients have their own retries parameters. These usually override the system retries parameters.

Complete the following steps to change the SSH, SFTP and SCP connection retries on the EC/DTACS.

1. Change the system session locking default to the number you prefer by following the procedure in ***Changing the Session Lock Number*** (on page 14).
2. As **admin** user, enter the following command to change to the **/etc/ssh** directory.
   ```
   [admin@vodwater ~]$ cd /etc/ssh
   ```
3. Enter the following command to open the **sshd_config** file in a text editor.
   ```
   [admin@vodwater ~]$ sudo vi sshd_config
   ```
4. Find the line that contains MaxAuthTries and enter the number of login attempts you prefer.

   Example: `MaxAuthTries 5`
5. Save and close the file.
6. Type the following command to restart the sshd service. The ssh process restarts and uses the new MaxAuthTries parameter.
   ```
   [admin@vodwater ~]$ sudo service sshd restart
   ```

Using SCP

SCP is a protocol that allows you to securely transfer files between a local host and a remote host.

Notes:

- When you use SCP to login to the system, use your individual username and password.
- You can only have one active session for each username. Consider setting up additional usernames if you require multiple sessions open at the same time.

Complete the following steps to transfer a file between a remote computer and a local computer.

1 Open an xterm window on your local system.

2 Do you want to transfer a file from a remote computer to your local computer?

- If **yes**, go to the next step.
- If **no** and you want to transfer a file from your local computer to a remote computer, go to Step 5.

3 Type the following command and press **Enter**. You are prompted for the user password.

Command Syntax:

```
scp [username]@[IP address of remote system]:absolute path of
file on remote system] [directory on local system]
```

Example:

```
[admin@vodwater ~]$ scp admin@10.90.47.67:/var/tmp/ec.envfile
/home/admin
```

Example Output:

```
############################## WARNING!!! ###################################
################## READ THIS BEFORE ATTEMPTING TO LOGON ##################
#                                                                        #
#    This System is for the use of authorized users only.  Individuals   #
#    using this computer without authority, or in excess of their        #
#    authority, are subject to having all of their activities on this    #
#    system monitored and recorded by system personnel.  In the course   #
#    of monitoring individuals improperly using this system, or in the   #
#    course of system maintenance, the activities of authorized users    #
#    may also be monitored.  Anyone using this system expressly          #
#    consents to such monitoring and is advised that if such             #
#    monitoring reveals possible criminal activity, system personnel     #
#    may provide the evidence of such monitoring to law enforcement      #
#    officials.  You cannot copy, disclose, display or otherwise         #
#    communicate the contents of this server except to other Cisco       #
#    employees who have been authorized to access this server.           #
#                                                                        #
########################## Confidential Information ######################

admin@10.90.47.67's password:
```

4 When prompted to enter the password of the user you are connecting as, type the password and press **Enter**. The progress of the file transfer displays and, when complete, you are returned to the command prompt.

5 Type the following command and press **Enter**. You are prompted for the user password.

Command Syntax:

```
scp
[absolute path of file on local system][username]@[IP address
of remote system]:[directory on remote system]
```

Example:

```
[admin@vodwater ~]$ scp /home/admin/ec.envfile
admin@10.90.47.67:/var/tmp
```

Example Output:

```
############################## WARNING!!! ################################
################## READ THIS BEFORE ATTEMPTING TO LOGON ##################
#                                                                        #
#    This System is for the use of authorized users only.  Individuals   #
#    using this computer without authority, or in excess of their        #
#    authority, are subject to having all of their activities on this    #
#    system monitored and recorded by system personnel.  In the course   #
#    of monitoring individuals improperly using this system, or in the   #
#    course of system maintenance, the activities of authorized users    #
#    may also be monitored.  Anyone using this system expressly          #
#    consents to such monitoring and is advised that if such             #
#    monitoring reveals possible criminal activity, system personnel     #
#    may provide the evidence of such monitoring to law enforcement      #
#    officials.  You cannot copy, disclose, display or otherwise         #
#    communicate the contents of this server except to other Cisco       #
#    employees who have been authorized to access this server.           #
#                                                                        #
########################## Confidential Information ######################
admin@10.90.47.67's password:
```

6 When prompted to enter the password of the user you are connecting as, type the password and press **Enter**. The progress of the file transfer displays and, when complete, you are returned to the command prompt.

6

Security Event Logs and Auditing

Introduction

This chapter discusses security logs, including what is logged and where the logs are located, and auditing the system.

In This Chapter

Security Event Logs

Security event logs are automatically generated by the system. Basic security event logs are located in the **/var/log/secure** file. This file logs the following types of events:

- SSH
- SFTP
- Successful and failed login attempts
- sudo execution
- User Administration

Note: You need to be logged in as root user or as a user that has sudo-root access (for example, the admin user) to open the /var/log/secure file.

Other log files you can monitor for security, along with their security restrictions:

- **/var/log/audit/audit.log** — Records all sudo commands
- **/var/log/messages** — Records messages from the kernel and daemons
- **/var/log/httpd-dncs/ and /var/log/httpd-dncsws** — Directories that contains the Apache web server log files which records Administrative Console and Web service access events
- **/var/log/audit** — Directory that contains all audit files including all security-related events (for example, logins, logouts, user actions)

Auditing

The auditd service is a monitoring tool for Linux that integrates with the kernel and watches system calls on the EC/DTACS system. This provides the ability to ensure that system operation is what is expected. It also allows logging any time a particular system call occurs, a file/directory is accessed, and more.

Understanding Audit Rules

Audit rules can be defined as one of the following three types:

- **Control Rules** — allows you to modify the behavior of the audit system
  - If creating a persistent audit rule, these are always in the first section of the audit.rules file
  - **Examples of common audit control rules**:
    - **-D** — removes all previous rules
    - **-b** — defines the buffer size (for example, -b 8192)
    - **-f** — panic on failure
    - **-r** — create the maximum allowable audit messages per second (for example, -r 120 creates at most 120 audit messages per second)
- **File System Rules** — also known as watch files, these rules allow you to audit access to particular files or directories
  - If creating a persistent file system rule, these are always in the first located after the control rules section
  - **Syntax:**
    ```
    -w [/path-to-file-or-directory] -p [permissions] -k [key-string]
    ```
  - **Options in Syntax:**
    - **-w** — path fully qualified path to the file or directory to watch
    - **-p** — [**r**ead | **w**rite | **e**xecute | **a**ttribute] file system permission access type to watch
    - **-k** — unique key string for use when performing audit searches
  - **Examples of common file system rules**:
    ```
    -w /etc/passwd -p wa -k passwd_changes
    -w /etc/group -p wa -k group_changes
    -w /etc/hosts -p wa -k host_changes
    ```

- **System Call Rules —** allows you to log system calls that any specified program makes
  - If creating a persistent file system rule, these are always in the first located after the control rules section
  - **Syntax**:

    ```
    -a [action],[list] -S [syscall] -F field=[value] -k [key-string]
    ```

  - **Options in Syntax**:
    - **-a [action,list|list,action] –** Add an audit rule to the end of the specified list with the specified action

      – action [never|always] – never: no audit records are generated; used to suppress event generation. always: collect at syscall entry time and write out an audit record at systecall exit time

      – list [task|exit|user|exclude] – Defines which list to apply to the audit rule
    - **-S [Syscall name or number|all] –** See the "syscall man" page for a list of syscall names
    - **-F [n=v | n!=v | n<v | n>v | n<=v | n>=v | n&v | n&=v] –** Defines the rule where n is the name and v is the value
    - **-k key** – arbitrary key string for use when performing audit searches
  - **Examples of file system rule to monitor a successful execution of dncsStart**:

    ```
    -a always,exit -S all -F path=/dvs/dncs/bin/dncsStart -F perm=x -F success=1 -F key=dncsStart_exec
    ```

Defining Audit Rules

Audit rules can be defined in the following manners:

- **auditctl Utility —** allows you to define rules on the command line; however, they ***are not*** persistent across reboots. Refer to ***Adding Temporary Audit Rules*** (on page 59) for guidelines.
- **/etc/audit/audit.rules File —** allows you to define rules in the audit.rules file which are persistent and remain after a system reboot. Refer to ***Adding Permanent Audit Rules*** (on page 60) for guidelines.

Adding Temporary Audit Rules

The **auditctl** command allows you to define rules at the command line by preceding the rule with "auditctl". Rules defined with auditctl are not maintained after restarting the EC/DTACS. To permanently add rules, go to ***Adding Permanent Audit Rules*** (on page 60).

Use the following procedure as a guideline to create temporary audit rules on your EC/DTACS system.

Note: There are many options you can use with the auditctl utility. Refer to ***Understanding Audit Rules*** (on page 57) or review the man page, **man auditctl,** for details.

1 As **root** user, use the following command syntax to add an audit rule on your EC/DTACS.

Note: For this procedure, we will add a rule to monitor the successful startup of EC processes.

Command Syntax:

```
auditctl -w [filesystem path] -p [permission access] -F
[success=[value]] -k [key-string]
```

Example:

```
[root@vodwater ~]# auditctl -w /dvs/dncs/bin/dncsStart -p x -F
success=1 -k dncsStart_exec
```

2 Enter the following command to view the new rule. The rule is appended to the end of the output.

```
[root@vodwater ~]# auditctl -l
```

```
-a always,exit -S all -F dir=/etc -F perm=rwxa -F success!=1 -F key=etc_dir_fail
-a always,exit -S all -F dir=/etc -F perm=w -F success=1 -F key=etc_dir_mon_writes
-w /sbin/ -p x -k sbin_exec
-w /usr/sbin/ -p x -k usr_sbin_exec
-a always,exit -S all -F path=/dvs/dncs/bin/dncsStart -F perm=x -F success=1 -F key=dncsSt
art_exec
-w /etc/hosts -p wa -k host changes
```

3 If desired, repeat Steps 1 through 2 to add additional rules.

4 Go to the ***The ausearch Utility*** (on page 62) for details on how to search the audit daemon log files based on the rule(s) you created.

Adding Permanent Audit Rules

The **/etc/audit/audit.rules** file allows you to define rules on the EC/DTACS that are persistent across reboots; you must add them in the **/etc/audit/audit.rules** file.

Note: There are many options you can use to define an audit rule. Refer to ***Understanding Audit Rules*** (on page 57) or review the man page, **man audit.rule**, for details.

Use the following procedure as a guideline to define a persistent audit rule.

1. As **root** user, enter the following command to open the **/etc/audit/audit.rules** file in a text editor.

   ```
   [root@vodwater ~]# vi /etc/audit/audit.rules
   ```

2. Go to the appropriate area of the file and open a line.

   Note: Because we will add a file system rule, we will go to the section after the Control Rules.

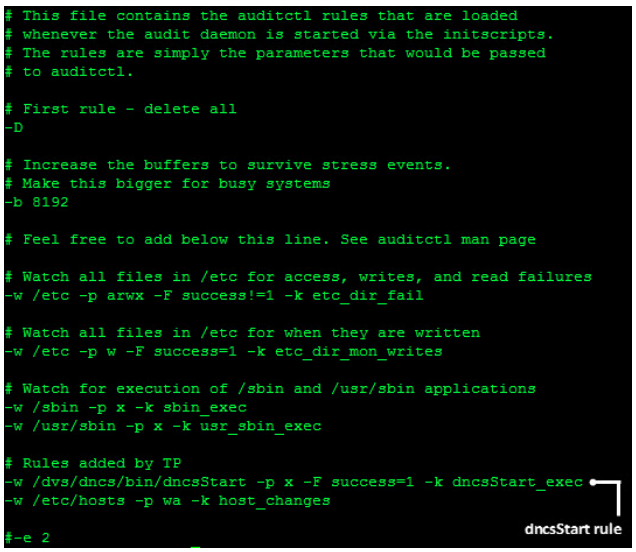
3. Add a rule(s) to the file.

   Note: For this procedure, we will add a rule to monitor the successful startup of EC processes.

4. After entering the rule(s), you can ***optionally*** add a line with **-e 2** to force a reboot after any update to the audit.rules file.

   Note: Adding this entry requires you to reboot the server after any changes to the audit.rules file and also inhibits you from adding any temporary audit rules.

   Example:


   ```
   # This file contains the auditctl rules that are loaded
   # whenever the audit daemon is started via the initscripts.
   # The rules are simply the parameters that would be passed
   # to auditctl.

   # First rule - delete all
   -D

   # Increase the buffers to survive stress events.
   # Make this bigger for busy systems
   -b 8192

   # Feel free to add below this line. See auditctl man page

   # Watch all files in /etc for access, writes, and read failures
   -w /etc -p arwx -F success!=1 -k etc_dir_fail

   # Watch all files in /etc for when they are written
   -w /etc -p w -F success=1 -k etc_dir_mon_writes

   # Watch for execution of /sbin and /usr/sbin applications
   -w /sbin -p x -k sbin_exec
   -w /usr/sbin -p x -k usr_sbin_exec

   # Rules added by TP
   -w /dvs/dncs/bin/dncsStart -p x -F success=1 -k dncsStart_exec
   -w /etc/hosts -p wa -k host_changes

   #-e 2
   ```

5. Save and close the file.

6. Enter the following command to restart the **auditd** service.

   ```
   [root@vodwater ~]# service auditd restart
   ```

7 Enter the following command to view the new rule. The rule is appended to the end of the output.

```
[root@vodwater ~]# auditctl -l
```

```
-a always,exit -S all -F dir=/etc -F perm=rwxa -F success!=1 -F key=etc_dir_fail
-a always,exit -S all -F dir=/etc -F perm=w -F success=1 -F key=etc_dir_mon_writes
-w /sbin/ -p x -k sbin_exec
-w /usr/sbin/ -p x -k usr_sbin_exec
-a always,exit -S all -F path=/dvs/dncs/bin/dncsStart -F perm=x -F success=1 -F key=dncsSt
art_exec
-w /etc/hosts -p wa -k host changes
```

8 Go to the ***The ausearch Utility*** (on page 62) for details on how to search the audit daemon log files based on the rule(s) you created.

The ausearch Utility

The ausearch utility is a simple command line tool used to search the audit daemon log files based on events and different search criteria (for example, event identifier, key identifier, hostname) related to audit rules.

By default, ausearch queries the **/var/log/audit/audit.log** file, which you can view just like any other text file.

ausearch Options

There are several options available when using the ausearch utility. To view a list of options along with a description of each option, refer to the man page, **man ausearch**.

Searchable Rules

Use the following procedure as a guideline to query the audit daemon logs using the ausearch utility.

1 As **root** user, enter the following command to search the audit logs for an event.

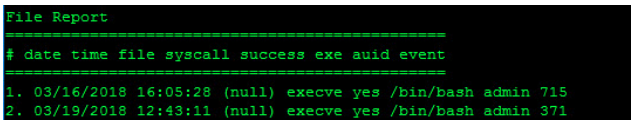
Note: In this example, we will search the log for the startup of EC services using the key-string that was defined for the rule (for example, dncsStart_exec).

Command Syntax:

```
ausearch -k [key-string] | aureport -f -i
```

Example:

```
[root@vodwater ~]$ ausearch -k dncsStart_exec | aureport -f -i
```



Result: The output indicates EC processes were successfully started on 03/16/2018 and on 03/18/2018.

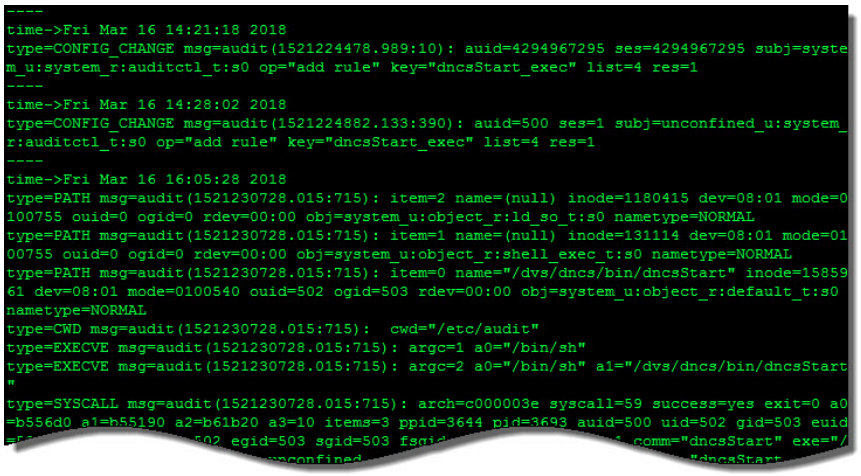
2 To see more detail about the monitoring of this event, search for the key-string within the audit.log file.

Command Syntax:

```
ausearch -k [key-string] | less
```

Example:

```
[root@vodwater ~]$ ausearch -k dncsStart_exec | less
```



Reviewing Audit Logs

The auditctl utility, installed on the system, logs a significant amount of event information based on audit rules, including OS login and logoff events, privileged command execution, and more. Data written to the audit logs are in plain text in the **/var/log/audit** directory.

Important: You must have sudo root access to view the audit log.

The system writes to the audit log until it reaches 6MB in size. It is then rotated. The system keeps a maximum of 5 audit logs.

Complete the following steps to view the **audit.log** file.

1 As **admin** user, type the following command to view a list of the audit logs.

```
[admin@vodwater8 ~]$ sudo ls -ltr /var/log/audit
```

Example Output:

```
total 19816
-r--------. 1 root root 6291582 Mar  6 17:39 audit.log.3
-r--------. 1 root root 6291508 Mar  7 12:24 audit.log.2
-r--------. 1 root root 6291477 Mar 19 10:08 audit.log.1
-rw-------. 1 root root 1387468 Mar 19 14:17 audit.log
```

2 Enter the following command to view the **audit.log** file.

```
[admin@vodwater ~]$ sudo less /var/log/audit/audit.log
```

Example Output:

A

Configure FTP Users and Start the vsftpd Service

Important: This appendix only applies if your site requires FTP support.

The vfstpd daemon (very secure FTP daemon) is the default FTP server used in CentOS.

For security reasons, the vsftpd service does not run at initial install/bootup. This appendix provides the procedure that must be performed to configure FTP users, provide FTP access to the users and to start the vfstp service.

In This Appendix

Configuring FTP Users and Starting the vsftp Service

1. As **admin** user, enter the following command to open the **/etc/vsftpd/user_list** file in a text editor.

   ```
   [admin@nextxVM ~] $ sudo vi /etc/vsftpd/user_list
   ```

2. Add an entry for the **easftp** and **dncsftp** users.
3. Save and close the file.
4. Enter the following command to start the **vsftpd** service.

   ```
   [admin@nextxVM ~]$ sudo service vsftpd start
   ```

5. Enter the following command to verify that the service has started.

   ```
   [admin@nextxVM ~]$ service vsftpd status
   ```

6. Enter the following command to set the vsftpd service to start automatically at bootup.

   ```
   [admin@nextxVM ~]$ sudo chkconfig vsftpd on
   ```

7

Customer Information

If You Have Questions

If you have technical questions, call Cisco Services for assistance. Follow the menu options to speak with a service engineer.

Access your company's extranet site to view or order additional technical publications. For accessing instructions, contact the representative who handles your account. Check your extranet site often as the information is updated frequently.

Index

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA

http://www.cisco.com
Tel: 408 526-4000
800 553-6387
Fax: 408 527-0883

March 2018

Part Number
TP_00145