Security Configuration Guide
for EC 9.0 and DTACS 5.2

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

About This Guide

Introduction

As networks become more complex, the requirements for data security become more important. It is no longer feasible to consider that your network exists in a *walled environment*; therefore, we have taken steps to enhance the security of the EC and the DTACs systems.

Notes:

- These changes were initiated due to the requests of our customers.
- 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 9.0 and DTACS 5.2*** or contact your system administrator for more information.

Purpose

This document contains instructions on changing your security defaults.

We recommend that you keep the operating system defaults to obtain the most benefit from these security features for your network. However, there may be times when you might need to change those defaults temporarily; for example, when you need to troubleshoot or when you need to unlock a user account.

This document contains instructions on many of the EC/DTACS security features. Any changes should be performed by a system administrator in collaboration with Cisco personnel so that your system remains fully functional. The EC/DTACS system administrator should be well versed in the administration of a CentOS Linux platform and must understand the ramifications of changing the security defaults.

You need to use your best judgment and abide by your company security policies and guidelines when changing or removing any EC/DTACS security features associated its NextX9 system release.

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

Audience

This document is written for our customers' EC/DTACS system administrators who are responsible for the security policies of their site. These system administrators should be well versed in Linux security procedures and policies. Our engineers may also find this document to be useful.

Acronyms Used in This Document

The following table lists the acronyms used in this document and their description.

Acronym	Stands For...	Description
API	Application Programming Interface	A language and message format used by an application to communicate with the operating system (OS) or another control program.
BOSS	Business Operations Support System	Software that supports the interface between the application and the back-office database.
CLI	Command Line Interface	A user interface to an application that accepts typed commands a single line at a time.
EAS	Emergency Alert System	A national public warning system that requires broadcasters, cable operators, and others to provide communications capability during national or regional emergencies.
EC	Explorer Controller	A server that operates as a network control element that provides command and control data for most Cisco network elements that reside within the Cisco video control plane.
FTP	File Transfer Protocol	A protocol used to transfer files over a TCP/IP network. FTP includes the ability to log in to the network, list directories, and copy files.
HTTP	HyperText Transfer Protocol	The communications protocol used to connect to Web servers on the Internet or on a local network.
HTTPS	HyperText Transport Protocol Secure	A common, widely used protocol which includes a combination of the HTTP and SSL/TLS protocols that provide encrypted communication and secure identification of a given network web server. HTTPS is used to create secure communication channels over insecure networks.
IP	Internet Protocol	A network that uses the TCP/IP communications protocol to transmit data.
LDAP	Lightweight Directory Access Protocol	A protocol used to access a directory listing. Usually implemented in web browsers and email programs.
OS	Operating System	A computer's or server's master control program.

Acronym	Stands For...	Description
RADIUS	Remote Authentication Dial-In User Service	A protocol for authentication servers. Uses a challenge and response method for authentication.
SCP	Secure Copy Protocol	A secure version of the Linux remote copy command.
SFTP	SSH File Transfer Protocol	A file transfer protocol using the SSH protocol.
SOA	Service-Oriented Architecture	The modulization of business functions for greater flexibility and reusability. Implemented using an API that allows the components to communicate with each other.
SSL/TLS	Secure Sockets Layer / Transport Layer Security	SSL is a protocol that provides communications security for applications transmitting information over a data network. SSL provides data encryption and ensures message integrity while supporting host authentication, typically using X.509 certificates. TLS is an IETF standards-tracked security protocol based on SSL.
SSH	Secure Shell	A security protocol for logging into a remote server. SSH provides an encrypted session for transferring files and executing server programs, and serves as a secure client/server connection for applications.
STB	Set-Top Box	A device that converts cable TV channels to TV input.
TFTP	Trivial File Transfer Protocol	Stripped down version of the FTP protocol that has no directory browsing or password capability. Uses UDP rather than TCP for transport.
VM	Virtual Machine	An instance of an OS and applications in a virtualized environment.
VMware	Virtual Machine Software	Allows multiple copies of the same OS (or several different OSs) to run in the same machine.
WS	Web Service	An interface for an SOA, where web-based applications dynamically interact with each other.

Document Version

This is the first formal release of this document.

1

System Defaults and Access Control

Introduction

This chapter discusses the operating system defaults and any user 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.

- **Operating System:** CentOS 7.4-4
- **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 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:

- 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) script is delivered with the EC/DTACS.

Use the User Administration script, 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 Administrative 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 UI 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** user is used in examples for all Cisco DBDS documents pertaining to EC 9.0.
- The **dtacsuser** is used in all examples for all Cisco DBDS documents pertaining to DTACS 5.2
- Commands run as **root** user are shown with a **#** symbol.

  Example:

  ```
  [root@ec90/dtacs52 ~]#
  ```

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

  Example:

  ```
  [admin@ec90/dtacs52 ~]$
  [ecadmin@ec90/dtacs52 ~]$
  [dtacsadmin@ec90/dtacs52 ~]$
  [dncs@ec90/dtacs52 ~]$
  ```

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@ec90/dtacs52 ~]$ sudo vi
/etc/sysconfig/network-scripts/ifcfg-ens192
```

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@ec90/dtacs52 ~]$ 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@ec90/dtacs52 ~]$ sudo su – dncs
```

```
[dtacsadmin@ec90/dtacs52 ~]$ sudo su - dncs
```

Note: Throughout all Cisco DBDS documentation, the **ecadmin** or **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@ec90/dtacs52 ~]$ 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 work around 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 applies to remote web access to the Administrative Console
- Session timeout affects all users, including the root user
- Session timeout can be applied to SSH, the VM console, and shells launched during a session

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

- Administrative Console session timeout: 30 minutes (1800 seconds)
- Recovery: User logs in again
- Session timeout is not applied to OS level logins by default
- Session timeout is configurable for OS level logins
- Session timeout is not configurable for Administrative Console login

Changing the Session Timeout

You can apply a system wide OS login session timeout default and an individual user OS login session timeout.

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

Changing an Individual User's OS Login Session Timeout

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

   Note: Replace [username] with the desired username to apply the OS session timeout.

   ```
   [admin@ec90/dtacs52 ~]$ sudo vi /home/[username]/.bash_profile
   ```

2. Add the following two lines to the end of the file.

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

   ```
   TMOUT=300
   export TMOUT
   ```

3. Save and close the file.

Changing the System Wide OS Login Session Timeout

1. As **admin** user on the system, enter the following command to open **/etc/profile** in a text editor.

   ```
   [admin@ec90/dtacs52 ~]$ sudo vi /etc/profile
   ```

2. Add the following two lines to the end of the file.

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

   ```
   TMOUT=300
   export TMOUT
   ```

3. Save and close the file.

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 16) 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@ec90/dtacs52 ~]$ sudo vi /etc/pam.d/system-auth
   ```

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

   ```
   auth required pam_faillock.so preauth audit silent deny=5 unlock_time=900
   auth [default=die] pam_faillock.so authfail audit deny=5 unlock_time=900
   auth sufficient pam_faillock.so authsucc audit deny=5 unlock_time=900
   ```

3. Edit the deny variable (`deny=5`) in each line to match the desired number of failed login attempts before the account is locked for the time period specified (`unlock_time=900`).

   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. Repeat steps 1 through 4 for the **/etc/pam.d/password-auth** file.
6. 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@ec90/dtacs52 ~]$ 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@ec90/dtacs52 ~]$ 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@ec90/dtacs52 ~]$ sudo vi /etc/ssh/sshd_config
   ```

2. Locate the following line in the login file:

   ```
   LoginGraceTime 60
   ```

3. 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.

4. Save and close the **sshd_config** file.
5. Type the following command to restart the sshd service.

   ```
   [admin@ec90/dtacs52 ~]$ sudo systemctl restart sshd
   ```

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 As **admin** user, type the following command and press **Enter** to kill the SSH process associated with the user.

Command syntax:

```
sudo pkill -o -u [USERNAME] sshd
```

Example:

```
[admin@ec90/dtacs52 ~]$ sudo pkill -o -u testuser sshd
```

2 Type the following command and press **Enter** to verify processes associated with the user are no longer present.

Command syntax:

```
ps -U [USERNAME] -u [USERNAME]
```

Example:

```
[admin@ec90/dtacs52 ~]$ ps -U testuser -u testuser
```

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@ec90/dtacs52 ~]$ 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@ec90/dtacs52 ~]$ 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/sudoers.d/90-ec-privileges	dncsStart logLvl dncsControl
Application Server	/etc/sudoers.d/90-ec_appserv-privileges	appStart 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/sudoers.d/90-dtacs.privileges	dtacsStart 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@ec90/dtacs52 ~]$ 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@ec90/dtacs52 ~]$ 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@ec90/dtacs52 ~]$ 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@ec90/dtacs52 ~]$ 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@ec90/dtacs52 ~]$ sudo visudo -f
   /etc/sudoers.d/ncdsgroup-privileges
   ```

2. Add the following content to the file.

   - Replace "<group_name>" with the actual 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 the group (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 input: <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 Enter the following command to 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@ec90/dtacs52 ~]$ 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 input: Add a single command

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

Example input: Add multiple commands

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

Example input: All commands that match a wildcard

```
## Define NCDS Privileged Commands
Cmnd_Alias NCDSGEN      = /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 input: 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 input: 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.

   ```
   [admin@ec90/dtacs52 ~]$ sudo -l
   ```

   Example output:

   ```
   Matching Defaults entries for admin on ec90/dtacs52:
       !visiblepw, always_set_home, match_group_by_gid, env_reset,
   env_keep="COLORS DISPLAY
       HOSTNAME HISTSIZE 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 admin may run the following commands on ecnextx9:
       (dncs) NOPASSWD: NCDS
   ```

3. Enter the following command to execute a sudo command.

   Command syntax:

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

   Example:

   ```
   [admin@ec90/dtacs52 ~]$ sudo -u dncs
   /dvs/dncs/Utilities/ncdsGen/ncdsGen -V
   ```

   Example output:

   ```
   ncdsGen: 8.1.5
   ```

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@ec90/dtacs52 ~]$ 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@ec90/dtacs52 ~]$ 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 **dncs** user, type the following command and press **Enter** to change the password for Administrative user access to the Web UI.

   Command syntax:

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

   Example:

   ```
   [dncs@ec90/dtacs52 ~]$ /usr/bin/htdigest
   /etc/httpd/user-conf/CSCOec.digest "Cisco DNCS" ecadmin
   ```

2. At the **New password** prompt, type the new password for access to the Web UI interface for the user and press **Enter**.
3. At the **Re-type new 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, repeat steps 1 through 3.
   - 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/DTACS. For more information, see ***Enable RADIUS and LDAP Support Configuration Guide for EC 9.0 and DTACS 5.2*** or contact your system administrator for more information.

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.

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:

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

Example:

```
[admin@ec90/dtacs52 ~]$ sudo passwd -x 91 operator1
```

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

Command syntax:

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

Example:

```
[admin@ec90/dtacs52 ~]$ sudo chage -l operator1
```

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

Example output:

```
Last password change                                  : Apr 01, 2019
Password expires                                      : Jul 01, 2019
Password inactive                                     : Jul 31, 2019
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:

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

   Example:

   ```
   [admin@ec90/dtacs52 ~]$ sudo passwd -x 9999999 operator1
   ```

   Example output:

   ```
   Adjusting aging data for user operator1.
   passwd: Success
   ```

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

3. **Command syntax**:

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

   Example:

   ```
   [admin@ec90/dtacs52 ~]$ sudo chage -l operator1
   ```

   Example output:

   ```
   Last password change                                  : Apr 1, 2019
   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

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@ec90/dtacs52 ~]$ 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@ec90/dtacs52 ~]$ 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.

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@ec90/dtacs52 ~]$ 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@ec90/dtacs52 ~]$ 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@ec90/dtacs52 ~]$ 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@ec90/dtacs52 ~]$ 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@ec90/dtacs52 ~]$ 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]
sudo chown root:root /dvs/[SFTP-home-directory]
```

Example:

```
[admin@ec90/dtacs52 ~]$ sudo mkdir /dvs/sftpuser1/uploads
[admin@ec90/dtacs52 ~]$ sudo chown sftpuser1:sftpuser1
/dvs/sftpuser1/uploads
[admin@ec90/dtacs52 ~]$ 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@ec90/dtacs52 ~]$ 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 input:

   ```
   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@ec90/dtacs52 ~]$ sudo systemctl restart sshd
   ```

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@ec90/dtacs52 ~]$ sudo ssh sftpuser1@localhost
   ```

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

   Important: You must be in the sftp-defined directory to successfully execute a file transfer to or from the directory.

   Command syntax:

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

   Example:

   ```
   [admin@ec90/dtacs52 ~]$ 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.

Changing the SSH and SFTP Connection MaxAuthTries Parameter

Complete the following steps to change the SSH and SFTP connection MaxAuthTries parameter on the EC/DTACS. The MaxAuthTries parameter defines the maximum number of authentication attempts allowed before the SSH connection is terminated.

1. Change the system session locking default to the number you prefer by following the procedure in Changing the Session Lock Number.
2. As **admin** user, enter the following command to change to the **/etc/ssh** directory.

   ```
   [admin@ec90/dtacs52 ~]$ cd /etc/ssh
   ```

3. Enter the following command to open the **sshd_config** file in a text editor.

   ```
   [admin@ec90/dtacs52 ~]$ 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@ec90/dtacs52 ~]$ sudo systemctl restart sshd
   ```

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 6.

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@ec90/dtacs52 ~]$ 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 You have completed this procedure. Go to the next section.

6 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@ec90/dtacs52 ~]$ 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:
```

7 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.

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.

Introduction to Audit Rules

The following three types of audit rules can be specified:

- **Control rules** — allows the audit system's behavior and some of its configuration to be modified
- **File system rules** — allows the auditing of access to a particular file or a directory (for example, creates a file watch)
- **System call rules** — allows logging of system calls

Managing Audit Rules

The following is an overview of audit rule management and syntax. All commands should be executed as **admin** user with the use of sudo or as **root**. The example commands below assume execution by the **admin** user.

Display the Audit Rules

Entering the following command to display the current audit rules.

```
[admin@ec90/dtacs52 ~]$ sudo auditctl -l
```

Note: The "-l" in the command is a lower case L.

Audit Rule Types

- **Filesystem Rules**
  - Rules to watch files and directories on the filesystem.

    Example:

    ```
    -w /etc/hosts -p wa -k system-locale
    ```

    Notes:

    - **-w** – path fully qualified path to the file or directory to watch
    - **-p** – [r | w | x | a] filesystem permission access type to watch (read | write | execute | attribute)
    - **-k** – key arbitrary string for use when performing audit searches

- **System Call Rules**
  - Rules to watch system calls. This includes EC/DTACS utility execution, DB utility execution, system time modification, file deletes, and more.

    Example:

    ```
    -a always,exit -S all -F path=/usr/bin/mount -F perm=x -F
    auid>=1000 -F auid!=-1 -F key=privileged
    ```

    Notes:

    - **-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 audit rule.
    - **-S [Syscall name or number|all]** – See the syscalls 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 string for use when performing audit searches.

EC Audit Rules

- **Default audit rules for EC executables and associated audit search keys:**

/dvs/admin/useradmin	useradmin_exec
/dvs/dncs/bin/dncsControl	dncsControl_exec
/dvs/dncs/bin/dncsStop	dncsStop_exec
/dvs/dncs/bin/dncsStart	dncsStart_exec
/dvs/dncs/bin/dncsKill	dncsKill_exec
/dvs/dncs/bin/appStop	appStop_exec
/dvs/dncs/bin/appControl	appControl_exec
/dvs/dncs/bin/appKill	appKill_exec
/dvs/dncs/bin/modDhctCfg	modDhctCfg_exec
/dvs/dncs/bin/modDhctAdmin	modDhctAdmin_exec
/dvs/dncs/bin/delete-sm	delete-sm_exec
/dvs/dncs/bin/deleteDhct	deleteDhct_exec
/dvs/dncs/bin/del-hct-cd	del-hct-cd_exec
/dvs/dncs/bin/releaseSession	releaseSession_exec
/dvs/dncs/Utilities/doctor/doctor	doctor_exec

- **Default audit rules for the EC database executables and associated audit search keys:**

/opt/cisco/informix/server/etc/onconfig	onconfig_write
/opt/cisco/informix/server/etc/sqlhosts	sqlhosts_write
/opt/cisco/informix/server/sai/bin/formatDbSpace	formatDbSpace_exec

- **Default audit rules for the EC files:**

/disk1/dvs/dvsFiles/BFS	BFS_attr_change

DTACS Audit Rules

- **Default audit rules for DTACS executables and associated audit search keys:**

/dvs/admin/useradmin	useradmin_exec

- **Default audit rules for the DTACS database executables and associated audit search keys:**

/opt/cisco/informix/server/etc/onconfig	onconfig_write
/opt/cisco/informix/server/etc/sqlhosts	sqlhosts_write
/opt/cisco/informix/server/sai/bin/formatDbSpace	formatDbSpace_exec

Adding Auditing Rules

Notes:

- An EC system is used in this example. To add an auditing rule to the DTACS, edit the **/etc/audit/rules.d/CSCOdtacs-audit.rules** file.
- For enhanced security, auditd is in immutable mode. This means that audit rules cannot be applied to the system dynamically using the auditctl command or by restarting the audit daemon. A restart of the system is required to apply audit rule changes.

1 As **admin** user, enter the following command to add an audit rule to the appropriate section of the **/etc/audit/rules.d/CSCOec-audit.rules** file. Do *not* modify other audit rules files.

Important: Do not add rules to the end of the file after the "-e 2" line.

```
[admin@ec90/dtacs52 ~]$ sudo vi /etc/audit/rules.d/CSCOec-
audit.rules
```

Example: audit rule for ncdsGen execution

```
# Watch for privileged execution
-w /dvs/admin/useradmin -p x -F success=1 -k useradmin_exec
…
-w /dvs/dncs/Utilities/doctor/doctor -p x -F success=1 -k doctor_exec
-w /dvs/dncs/Utilities/ncdsGen/ncdsGen -p x -F success=1 -k ncdsGen_exec
# Watch BFS files for attribute changes
-w /disk1/dvs/dvsFiles/BFS -p a -F success=1 -k BFS_attr_change
```

2 Save and close the file.

3 Enter the following command to reboot the system.

```
[admin@ec90/dtacs52 ~]$ sudo reboot now
```

4 Log back into the system as **admin** user.

5 Verify the audit rules file using the **augenrules** utility.

```
[admin@ec90/dtacs52 ~]$ sudo augenrules --load
```

Example output:

```
/usr/sbin/augenrules: No change
```

Note: If an error is detected, the utility will return the location of the error as shown below.

```
No rules
enabled 1
failure 1
pid 728
rate_limit 0
backlog_limit 8192
lost 0
backlog 0
There was an error in line 26 of /etc/audit/audit.rules
```

6 Were any errors detected?

- If **no**, go to step 9.
- If **yes**, go to the next step.

7 Repeat step 1 to correct the **/etc/audit/rules.d/CSCOec-audit.rules** file.

8 Then repeat steps 2 through 5.

9 Enter the following command to verify that the rule was added to the file.

```
[admin@ec90/dtacs52 ~]$ sudo auditctl -l
```

Example output:

```
-a always,exit -S all -F path=/dvs/dncs/Utilities/ncdsGen/ncdsGen -F perm=x -
F success=1 -F key=ncdsGen_exec
```

Introduction to Audit Logs

The audit daemon logs a significant amount of event information, including OS login, logoff, file access, file permission modification, and kernel change events that the secure and messages logs do not capture.

The EC/DTACS includes default audit rules for capturing various system and EC/DTACS-specific events. These audit rules are located in the **/etc/audit/rules.d** rules files.

Notes:

- The audit log is rotated once it reaches 100 MB.
- The audit logs are not discarded. It is up to the system administrator to manage the removal of audit logs.
- The audit daemon will stop writing audit log files if the file system space is exhausted.
- The audit logs are located in the **/var/log/audit** directory.
- See the **/etc/audit/auditd.conf** file for audit daemon configuration parameters and associated values.

Reference: *https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html-single/security_guide/index#chap-system_auditing*

Audit Log Utilities

Audit logs are searched and viewed using the **ausearch** and **aureport** utilities.

Note: See the ausearch and aureport man pages for detailed usage.

Generating Data for an Example Search

1. Log into the system as one of the sudo users added to the group that you created in *Adding Users to the Group* (on page 26) (for example, operator1).
2. Enter the following command to execute the **ncdsGen** utility.

   ```
   [operator1@ec90/dtacs52 ~]$ sudo -u dncs
   /dvs/dncs/Utilities/ncdsGen/ncdsGen -V
   ```

   Example output:

   ```
   ncdsGen: version: 8
   release: CSCOecutils 8.1.5
   ```

Example Audit Log Search and Report Commands

- As **admin** user, enter the following command to search for events related to the **ncdsGen** utility that was executed **today**.

  Command:

  ```
  [admin@ec90/dtacs52 ~]$ sudo ausearch -i -ts today -k
  ncdsGen_exec
  ```

  Notes:

  - The **-i** converts numbers, such as the user ID and date/time, to the associated text value.
  - The **-ts today** start time displays output for "today" only.
  - The **-k ncdsGen_exec** search key is defined in the audit rule.

  Example output:

  ```
  type=PROCTITLE msg=audit(04/03/2019 11:51:50.232:347) :
  proctitle=/usr/bin/perl /dvs/dncs/Utilities/ncdsGen/ncdsGen -V
  type=PATH msg=audit(04/03/2019 11:51:50.232:347) : item=2 name=/lib64/ld-
  linux-x86-64.so.2 inode=3104262 dev=08:01 mode=file,755 ouid=root ogid=root
  rdev=00:00 obj=system_u:object_r:ld_so_t:s0 objtype=NORMAL
  type=PATH msg=audit(04/03/2019 11:51:50.232:347) : item=1 name=/usr/bin/perl
  inode=1212927 dev=08:01 mode=file,755 ouid=root ogid=root rdev=00:00
  obj=system_u:object_r:bin_t:s0 objtype=NORMAL
  type=PATH msg=audit(04/03/2019 11:51:50.232:347) : item=0
  name=/dvs/dncs/Utilities/ncdsGen/ncdsGen inode=117447721 dev=08:01
  mode=file,540 ouid=dncs ogid=dncs rdev=00:00
  obj=system_u:object_r:default_t:s0 objtype=NORMAL
  type=CWD msg=audit(04/03/201911:51:50.232:347) :  cwd=/home/ncdsuser1
  type=EXECVE msg=audit(04/03/2019 11:51:50.232:347) : argc=3 a0=/usr/bin/perl
  a1=/dvs/dncs/Utilities/ncdsGen/ncdsGen a2=-V
  type=SYSCALL msg=audit(04/03/2019 11:51:50.232:347) : arch=x86_64
  syscall=execve success=yes exit=0 a0=0x56112f1aa818 a1=0x56112f19c918
  a2=0x56112f1a19e0 a3=0x0 items=3 ppid=5263 pid=5264 auid=operator1 uid=dncs
  gid=dncs euid=dncs suid=dncs fsuid=dncs egid=dncs sgid=dncs fsgid=dncs
  tty=pts0 ses=10 comm=ncdsGen exe=/usr/bin/perl
  subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key=ncdsGen_exec
  ```

  Output notes:

  - The **Record Types** (type=<value>) are defined here: https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html-single/security_guide/#table-record_types (https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html-single/security_guide/#table-record_types)
  - **PROCTITLE** – In the example above, the proctitle value is the full command-line that triggered the Audit event

- **PATH –** Each path that is passed to the system call. In the example above, the following three paths are passed to the system call:
  - **/dvs/dncs/Utilities/ncdsGen/ncdsGen –** an executable perl script
  - **/usr/bin/perl the perl –** an executable
  - **/lib64/ld-linux-x86-64.so.2 –** the Linux dynamic link loader, which is called because the perl executable is a dynamically linked executable
- **CWD –** The user's working directory at the time of execution
- **EXECVE –** The arguments of the execve (execute program) system call. In the example above, three arguments are passed to the execve system call:
  - **/usr/bin/perl**
  - **/dvs/dncs/Utilities/ncdsGen/ncdsGen**
  - **-V**
- **SYSCALL –** The type of system call that was sent to the kernel. Notice that detailed information about the system call is included in the audit record. Some of the fields and values include:
  - **success=yes –** The system call succeeded
  - **exit=0 –** Exit code returned by the system call
  - **ppid=5263 –** Parent Process ID
  - **pid=5264 –** Process ID
  - **auid=operator1 –** Audit User ID: the ID of the login user which is inherited by every process even when the user's identity changes via su or sudo
  - **uid=dncs –** user ID of the user who executed the command that triggered the system call
  - **gid=dncs –** group ID of the user who executed the command that triggered the system call
  - **tty=pts0 –** terminal from which the executed command was invoked

- Enter the following command to search for commands executed by the **operator1** login user over the past **week**.

  Note: The audit events will include commands executed directly and indirectly by the specified login user.

  Command:

  ```
  [admin@ec90/dtacs52 ~]$ sudo ausearch -i -sc execve -ts
  this-week -ul operator1
  ```

  Commands notes:

  - **-i** converts numbers, such as user ID and date/time, to the associated text value.
  - **-sc execve** system call = execve (execute program)
  - **-ts this-week** start time = since the first day of the current week
  - **-ul operator1** login user = operator1

- Enter the following command to search all events on **04/03/2019** with **dncs** in the name of the audit rule key.

  Command:

  ```
  [admin@ec90/dtacs52 ~]$ sudo ausearch -i -ts "04/03/2019" -te
  "04/03/2019" -k dncs
  ```

  Commands notes:

  - **-i** converts numbers, such as user ID and date/time, to the associated text value.
  - **-ts "04/03/2019"** start time = 4/3/19
  - **-te "04/03/2019"** end time = 4/3/19
  - **-k dncs** search key = dncs

- Enter the following command to display a report of all events on **04/03/2019** with **dncs** in the name of the audit rule key.

  Command:

  ```
  [admin@ec90/dtacs52 ~]$ sudo ausearch -ts "04/03/2019" -te
  "04/03/2019" -k dncs | sudo aureport -i --comm
  ```

  Commands notes:

  - **-i** converts numbers, such as user ID and date/time, to the associated text value.
  - **--comm** report about executed commands

Example output:

```
Command Report
==================================
# date time comm term host auid event
==================================
1. 04/03/2019 10:47:31 dncsStop pts0 ? admin 24516
2. 04/03/2019 10:47:32 dncsKill pts0 ? admin 24527
3. 04/03/2019 11:42:49 dncsStart pts1 ? ecadmin 777
```

- Enter the following command to display the entire audit event for the **dncsStart** command executed by the user **dncsopuser1**.

  Command:

  ```
  [admin@ec90/dtacs52 ~]$ sudo ausearch -i -ts "04/03/2019" -te
  "04/03/2019" -a 24516
  ```

  Commands notes:

  - The start and end dates are provided to decrease the search time and limit the results to expected event ID. Event IDs may be reused over time.
  - **-i** converts numbers, such as user ID and date/time, to the associated text value.
  - **-ts "04/03/2019"** start time = 4/3/2019
  - **-te "04/03/2019" end time** = 4/3/2019
  - **-a 24516** = audit event ID

  Example output:

  ```
  type=PROCTITLE msg=audit(04/03/2019 10:47:31.095:24516) : proctitle=/bin/sh
  /dvs/dncs/bin/dncsStop
  type=PATH msg=audit(04/03/2019 10:47:31.095:24516) : item=2 name=/lib64/ld-
  linux-x86-64.so.2 inode=1340046 dev=08:01 mode=file,755 ouid=root ogid=root
  rdev=00:00 obj=system_u:object_r:ld_so_t:s0 objtype=NORMAL
  type=PATH msg=audit(04/03/2019 10:47:31.095:24516) : item=1 name=/bin/sh
  inode=99658 dev=08:01 mode=file,755 ouid=root ogid=root rdev=00:00
  obj=system_u:object_r:shell_exec_t:s0 objtype=NORMAL
  type=PATH msg=audit(04/03/2019 10:47:31.095:24516) : item=0
  name=/dvs/dncs/bin/dncsStop inode=104863104 dev=08:01 mode=file,540 ouid=dncs
  ogid=dncs rdev=00:00 obj=system_u:object_r:default_t:s0 objtype=NORMAL
  type=CWD msg=audit(04/03/2019 10:47:31.095:24516) :
  cwd=/opt/cisco/backup_restore
  type=EXECVE msg=audit(04/03/2019 10:47:31.095:24516) : argc=2 a0=/bin/sh
  a1=/dvs/dncs/bin/dncsStop
  type=SYSCALL msg=audit(04/03/2019 10:47:31.095:24516) : arch=x86_64
  syscall=execve success=yes exit=0 a0=0x558ea70a32f8 a1=0x558ea70a6648
  a2=0x558ea7095ff0 a3=0x0 items=3 ppid=13841 pid=13842 auid=admin uid=root
  gid=root euid=root suid=root fsuid=root egid=root sgid=root fsgid=root
  tty=pts0 ses=1 comm=dncsStop exe=/usr/bin/bash
  subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key=dncsStop_exec
  ```

- Enter the following command to display a report of **all authentication attempts since the last system boot**.

  Command:

  ```
  [admin@ec90/dtacs52 ~]$ sudo aureport -ts boot -te now -l
  ```

  Commands notes:

  - **-i** converts numbers, such as user ID and date/time, to the associated text value.
  - **-ts boot** start time = since last system boot
  - **-te now** end time = to current time

  Example output:

  ```
  Login Report
  ============================================
  # date time auid host term exe success event
  ============================================
  1. 04/03/2019 12:43:12 -1 10.82.168.61 /dev/pts/0 /usr/sbin/sshd yes 310
  2. 04/03/2019 12:44:45 -1 10.82.168.61 /dev/pts/1 /usr/sbin/sshd yes 374
  ```

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

S

U

W

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

April 2019