Contents

Overview .......................................................................................................................... 5
  Basic architecture ....................................................................................................... 5
  Related documentation ............................................................................................ 5

Creating a Skybox Virtual Appliance .......................................................................... 6
  Minimal requirements .............................................................................................. 6
  Downloading installation files for Skybox Appliance ............................................. 6
  Creating a virtual machine ....................................................................................... 7
  File system partitions ............................................................................................... 13

Setting up Skybox Appliance ...................................................................................... 14
  System configuration .............................................................................................. 14
    Initial network IP address configuration ............................................................. 14
    Setting up Skybox for configuration ................................................................... 15
    First-time configuration ....................................................................................... 15
  What’s next .............................................................................................................. 16

Configuring the Appliance ......................................................................................... 17
  Configuration and management options ................................................................. 17
  Setting up network interface bonding .................................................................... 19
    Supported bond modes .......................................................................................... 19
  Setting up SNMP configuration ............................................................................. 21
  RADIUS authentication ........................................................................................... 21
  LDAP authentication ............................................................................................... 22
  Changing the TLS version ....................................................................................... 23

Customizing the syslog server .................................................................................... 26
  Setting up TCP and UDP listeners .......................................................................... 26
  How to work with syslog files ................................................................................ 26

Skybox Manager Installation ....................................................................................... 28
  Skybox Manager system requirements ................................................................... 28
  Installing Skybox Manager ...................................................................................... 29
  Upgrading Skybox Manager .................................................................................... 29
Chapter 1

Overview

Skybox® Virtual Appliance enables you to deploy Skybox on VMware hypervisors, without the burden of setting up a server with its operating system on your own.

Skybox® is an Automated Risk and Compliance Management (ARCM) platform that helps enterprise IT departments to discover and resolve potential security and compliance risks before they impact your organization.

Skybox is a multi-tiered platform. Skybox Appliance runs the Skybox Server and users run Skybox Managers (clients) that connect to the Skybox Server over the network. Skybox also runs an additional Skybox component, the Skybox Collector, which connects to data sources and imports the data to the Skybox Server.

The Skybox Server and Collector are preinstalled on Skybox Appliance and run at startup.

In this chapter

Basic architecture ........................................................................................................... 5
Related documentation ................................................................................................. 5

Basic architecture

The Skybox platform consists of a 3-tiered architecture with a centralized server (Skybox Server), data collectors (Skybox Collectors), and a user interface (Skybox Manager). Skybox can be scaled to suit the complexity and size of any infrastructure.

See the Skybox architecture topic in the Skybox Installation and Administration Guide.

Related documentation

Related documentation includes:

- Skybox online help
- Skybox documentation

Note: If you are not using the latest version of Skybox, you can find the documentation for your version at http://downloads.skyboxsecurity.com/files/Installers/Skybox_View/<your major version>/<your minor version>/Docs. For example, http://downloads.skyboxsecurity.com/files/Installers/Skybox_View/10.0/10.0.400/Docs
Chapter 2

Creating a Skybox Virtual Appliance

This chapter describes how to implement the Skybox Virtual Appliance.

**Important**: Skybox Virtual Appliance must be installed on VMware hypervisors. Other hypervisors are not supported.

In this chapter

**Minimal requirements** ............................................................ 6
**Downloading installation files for Skybox Appliance** ............... 6
**Creating a virtual machine** ..................................................... 7
**File system partitions** ............................................................ 13

Minimal requirements

The minimal requirements for creating a Skybox Virtual Appliance on a VMware hypervisor are listed in the following table.

<table>
<thead>
<tr>
<th>Item</th>
<th>Standard deployment</th>
<th>Large deployment (over 250 firewalls)</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>8 cores</td>
<td>16 cores</td>
</tr>
<tr>
<td>RAM</td>
<td>32 GB</td>
<td>128 GB</td>
</tr>
<tr>
<td>Available disk space</td>
<td>500 GB</td>
<td>1 TB</td>
</tr>
</tbody>
</table>

Some organizations may require additional resources. For additional information, contact Skybox Support.

**Supported ESXi versions**

Skybox Virtual Appliance supports vSphere Hypervisor ESXi version 5.5 and higher. However, because general support for version 5.5 ended on September 19, 2018, we recommend using version 6.0 or higher.

**Downloading installation files for Skybox Appliance**

Access to the installation files is always available at
http://downloads.skyboxsecurity.com/files/iso/Skybox_<Appliance version>/ISO
For example,  

A text file containing the MD5 checksum is in the same folder; download both files to the same folder.

To verify that the installation file has not been corrupted or tampered with
1 Run the command `md5sum -c <md5 file name>` from the directory to which you downloaded the installation file.
2 Check that the value you receive is: `<ISO file name>`: OK.

Creating a virtual machine

This section explains how to create a virtual machine to use for the Skybox Virtual Appliance.

Note: Disk size, memory, and number of CPUs in the following instructions refer to standard and large deployments as listed in Minimal requirements (on page 6). If your resources differ, use the values agreed upon with Skybox Professional Services.

To create a virtual machine
1 Right-click the host and select New Virtual Machine.
2 On the Configuration page, select Typical.
3 On the Name and Location page, in the **Name** field, type a unique name for the virtual Appliance machine.

4 On the Storage page, select the storage destination (datastore) for the virtual machine files.

5 On the Guest Operating System page:
   a. In the **Guest Operating System** field, select **Linux**.
b. In the **Version** field, select **Other 2.6.x Linux (64-bit)**.

6 On the Network page:
   a. In the **How many NICs do you want to connect** field, select **1**.
   b. Select **Connect at Power On** for NIC1.

7 On the Create a Disk page:
   a. Confirm that the **Datastore** field contains the name of the storage unit specified on the Storage page.
   b. In the **Virtual Disk Size** field, select **500 GB** for a standard deployment, **1 TB** for a large deployment.
c. Select **Thick Provision Lazy Zeroed.**

8 On the Ready to Complete page, select **Edit the virtual machine settings before completion**; click **Continue.**
On the **Hardware** tab:

a. Set **Memory** to **32 GB** for standard deployments or **128 GB** for large deployments.

b. Set **CPUs** to **8** for standard deployments or **16** for large deployments.

c. Select CPUs in the list and then set:
   - **Number of virtual sockets** to **2**
   - **Number of cores per socket** to **1**
10 On the **Resources** tab, reserve a minimum of **32 GB** memory.

11 On the **Options** tab, select **Advanced > Boot Options** in the Settings list; then select **Force BIOS Setup**.

12 Click **OK**.

13 Turn on the machine.

The BIOS setup utility is displayed.
14 On the **Boot** tab of the BIOS setup utility, change the boot order so that **CD ROM Drive** is at the top.

15 Press **F10** to save the settings and exit the setup utility.

16 As appropriate, select **Connect to ISO image on local disk** or **Connect to ISO image on a datastore**, and then select the file.

17 Restart the machine (press **Alt-Ctrl-Insert**).

18 When the Skybox Linux Installation menu appears, select **Skybox Appliance Installation**.

| Note: The restore process takes approximately 20 minutes. |

19 Restart the machine.

---

**File system partitions**

The Skybox Appliance file system is partitioned as follows:

- **SWAP**: 4 GB
- **/tmp**: 5% of the entire space
- **/**: 20% of the entire space
- **/var**: 45% of the entire space
- **/opt**: All remaining space on the disk

| Note: On machines with less than 200 GB of disk space, Skybox is installed on 1 partition. |
Chapter 3

Setting up Skybox Appliance

This chapter explains how to set up Skybox Appliance.

In this chapter

System configuration .......................................................... 14
What’s next ......................................................................... 16

System configuration

Before running the Skybox Server, configure Skybox Appliance to be part of your network and perform initial system configuration.

INITIAL NETWORK IP ADDRESS CONFIGURATION

To configure the network address

By default, the network interface is configured to receive the IP address from the DHCP server. If you configured the network card to support DHCP, it already has an IP address configured for the Appliance.

1 Connect the Skybox Appliance using console login with root credentials (root / skboxview).

2 On the console screen, check the IP address that the Appliance got from DHCP.

If this address is acceptable, continue to Setting up (on page 15).
3 If your network does not support DHCP or you need to change the IP address provided by DHCP, configure the network manually:
   a. Run the command `set_appliance_network`  
      (This command configures network interfaces with an IP address, netmask, and default gateway.)
      i. Select a network interface to configure.
      ii. Select the IP mode (static).
      iii. Provide the IP address, netmask, and default gateway.
4 Continue with Setting up (on page 15).

**SETTING UP SKYBOX FOR CONFIGURATION**

*To prepare for configuring the system remotely*

1 From a different machine on the network, open a browser to connect to the Skybox Appliance Administration using the following URL (<Appliance IP address> is the IP address of the Appliance (from DHCP or configured in Initial network IP address (on page 14))):
   - `https://<Appliance IP address>:444`
2 The default user name is `skyboxview`; the default password is `skyboxview`. The Skybox Appliance Administration main page appears.

**FIRST-TIME CONFIGURATION**

You must change the passwords and configure the date and time before using the Skybox Server. All other settings are optional; you can configure them later.

*To change the passwords*

1 On the Security tab, select **Appliance Passwords**.
2 To change the root password of the machine, click **Change Root Password**.
3 To change the Appliance Administration password, click **Change Skyboxview Password**.

*To configure the date and time*

1 On the System tab, select **Date and Time Configuration**.
2 To configure the date and time manually:
   a. Select **Manual Date and Time Configuration**.
   b. Click **Change Date and Time**; set the date and time for the Skybox time zone.
   c. Click **Change Time Zone**; set the time zone for the location of the Appliance, so that reports and other data are timestamped correctly.
3 To set the date and time from NTP servers:
   a. Select **Automatic Date and Time Configuration Using NTP Server**.
   b. Click **Change NTP Servers**; add the IP address or DNS of up to 3 NTP servers to use.
If you specify multiple NTP servers, the Appliance synchronizes to the average time between the servers.

c. Click **Change Time Zone**; set the time zone for the location of the Appliance, so that reports and other data are timestamped correctly.

**What’s next**

Skybox Manager is the client application that communicates with the Server. After installing and configuring the Appliance, you must install Skybox Manager on at least 1 remote machine (see **Skybox Manager Installation** (on page 28)).

**Using Skybox for change tracking**

You can use Skybox to track changes on firewalls. Although much change information can be collected directly from the firewalls, additional information (including a timestamp and the user who made the change) is taken from syslog change events that are sent to the syslog server in the Appliance. You collect the change events using **Change Tracking Events – Syslog Import** tasks.

**Syslog server**

The syslog server in the Appliance is preconfigured and is enabled by default.

Updates to the configuration files of the syslog server and syslog log file rotation are included (when necessary) as part of Skybox updates.

For information about customizing the syslog server, see **Customizing the syslog server** (on page 26).
Chapter 4

Configuring the Appliance

This chapter explains how to configure the Appliance.

In this chapter

Configuration and management options ........................................... 17  
Setting up network interface bonding ........................................... 19  
Setting up SNMP configuration .................................................. 21  
RADIUS authentication .................................................................. 21  
LDAP authentication ..................................................................... 22  
Changing the TLS version .............................................................. 23

Configuration and management options

Skybox Appliance configuration options are described in the following table.

<table>
<thead>
<tr>
<th>Pane</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>About tab</strong></td>
<td></td>
</tr>
<tr>
<td>System Information</td>
<td>Information about Skybox configuration</td>
</tr>
<tr>
<td><strong>Network tab</strong></td>
<td>Note that configuration changes made in this tab are only saved after you</td>
</tr>
<tr>
<td></td>
<td>click <strong>Save Network Configuration</strong>.</td>
</tr>
<tr>
<td>Network Configuration</td>
<td>Enables you to configure network settings (connection method, IP address,</td>
</tr>
<tr>
<td></td>
<td>netmask, and gateway) and bonding for each network interface connection, and</td>
</tr>
<tr>
<td></td>
<td>to configure the DNS servers.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: For non-virtual Appliances, this pane includes a link to a figure</td>
</tr>
<tr>
<td></td>
<td>of the back panel to help you to understand the connections.</td>
</tr>
<tr>
<td>Network Configuration</td>
<td>Displays a summary of the Appliance configuration.</td>
</tr>
<tr>
<td>Configuration Summary</td>
<td>Click <strong>Export</strong> to save this information to an HTML file.</td>
</tr>
<tr>
<td>Pane</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>System tab</strong></td>
<td></td>
</tr>
<tr>
<td>Date and Time Configuration</td>
<td>Enables you to view and change the date and time in the Appliance’s time zone.</td>
</tr>
<tr>
<td><strong>Notes:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• If you set this information manually, set the date and time and then the time zone for the location of the Appliance, so that reports and other data are timestamped correctly.</td>
</tr>
<tr>
<td></td>
<td>• Automatic configuration synchronizes Skybox with an NTP server. Provide the IP address or DNS of the NTP server to use. (You can use up to 3 NTP servers.)</td>
</tr>
<tr>
<td></td>
<td>Set the time zone after setting the NTP server.</td>
</tr>
<tr>
<td>Syslog Server</td>
<td>• Enables sending CentOS logs automatically from the Appliance to a remote syslog server (see Sending CentOS log to a remote syslog server).</td>
</tr>
<tr>
<td></td>
<td>• Starts or stops the Appliance syslog server service and enables you to configure TCP and UDP listeners (see Customizing the syslog server (on page 26)).</td>
</tr>
<tr>
<td>Host Name</td>
<td>Enables you to change the name of the Appliance.</td>
</tr>
<tr>
<td>Change System Mode</td>
<td>Toggles between Server mode (the Appliance functions as both the Skybox Server and a Skybox Collector) and Collector mode (the Appliance functions only as a Skybox Collector).</td>
</tr>
<tr>
<td>SNMP</td>
<td>Select Enable SNMP Service to set up SNMP configuration, host configuration, and sending traps (see Setting up SNMP configuration (on page 21)). You can also download the Appliance MIBs.</td>
</tr>
<tr>
<td><strong>Security tab</strong></td>
<td></td>
</tr>
<tr>
<td>Appliance Passwords</td>
<td>Enables you to change the root password for the Appliance, the password for the Appliance Administration, and the RMM password.</td>
</tr>
<tr>
<td>LDAP</td>
<td>Enables you to set up the Appliance to support authentication via LDAP (see LDAP authentication). (on page 22)</td>
</tr>
<tr>
<td>SSH</td>
<td>Toggles the SSH service on and off and enables the root user to log in via SSH.</td>
</tr>
<tr>
<td><strong>Control tab</strong></td>
<td></td>
</tr>
<tr>
<td>Skybox Services</td>
<td>Toggles the Skybox Server and Skybox Collector on and off.</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>Turning a Skybox service off stops the service and switches it to Manual mode. Turning the service on switches it back to Automatic mode.</td>
</tr>
<tr>
<td>Appliance Operations</td>
<td>Enables you to reboot or shut down the Appliance.</td>
</tr>
<tr>
<td><strong>Support tab</strong></td>
<td></td>
</tr>
<tr>
<td>Logs</td>
<td>Enables you to view Server, Collector, and other logs of the Appliance.</td>
</tr>
<tr>
<td><strong>Get Packlogs:</strong></td>
<td>Runs the packlogs utility and saves the</td>
</tr>
</tbody>
</table>
### Setting up network interface bonding

Skybox Appliances support network interface bonding for redundancy and for higher bandwidth.

**To create a network interface bonding**

1. On the **Network** tab, click **Network Configuration**.
2. Select **Network Interfaces**.
3. Select the interface to add to a network bond and click **Add to Network Bond**.
4. In the Network Bond Setup dialog box, add a bond interface.
5. Select the interfaces to bond to the new interface (as slaves).
6. Select the method for assigning the IP address for this interface.
   - If you select static mode, provide the IP address, netmask, and gateway.
7. Select the mode in which the bond is to work; we recommend active-backup.
   - For information about the supported bond modes, see **Supported bond modes** (on page 19).
8. Click **Save**.

**To view a list of the network interface bonding**

- On the **Network** tab, click **Network Configuration Summary**.

![Network Configuration Summary](image)

**SUPPORTED BOND MODES**

This section lists supported bond modes. We recommend active-backup for Skybox clusters.

**mode=0 (balance-rr)**

Round-robin policy: Transmits packets in sequential order from the 1st available slave to the last. This mode provides load balancing and fault tolerance.
**mode=1 (active-backup)**
Active-backup policy: Only 1 slave in the bond is active. A different slave becomes active if, and only if, the active slave fails. The bond’s MAC address is externally visible on a single port (network adapter) to avoid confusing the switch. This mode provides fault tolerance. The primary option affects the behavior of the mode.

**mode=2 (balance-xor)**
XOR policy: Transmits based on \[(source MAC address XORed with destination MAC address) modulo slave count\]. This selects the same slave for each destination MAC address. This mode provides balancing and fault tolerance.

**mode=3 (broadcast)**
Broadcast policy: Transmits everything on all slave interfaces. This mode provides fault tolerance.

**mode=4 (802.3ad)**
IEEE 802.3ad Dynamic link aggregation: Creates aggregation groups that share the same speed and duplex settings. Utilizes all slaves in the active aggregator according to the 802.3ad specification.

**mode=5 (balance-tlb)**
Adaptive transmit load balancing: Channel bonding that does not require any special switch support. The outgoing traffic is distributed according to the load (computed relative to the speed) on each slave. Incoming traffic is received by the current slave. If the receiving slave fails, another slave takes over the MAC address of the failed receiving slave.

**mode=6 (balance-alb)**
Adaptive load balancing: Includes transmit load balancing and receive load balancing for IPV4 traffic, and does not require any special switch support. The receive load balancing is achieved by ARP negotiation. The bonding driver intercepts the ARP replies sent by the local system on their way out and overwrites the source hardware address with the unique hardware address of a slave in the bond such that different peers use different hardware addresses for the server.
Setting up SNMP configuration

To use the Appliance as an SNMP Server
1. On the System tab, click SNMP.
2. Select Enable SNMP Service.
3. Set the following values:
   - On the General tab:
     - System Location: Physical location of the Appliance
     - Contact Details: Email address of the administrator
   - On the Security tab:
     - Read Only Community: SNMPv1 or SNMPv2 community string
     - Source: Name or IP address and subnet, represented as IP/netmask (10.10.10.0/255.255.255.0) or IP/bits (10.10.10.0/24). Comma-separate multiple sources
   - On the Notification (Traps) tab:
     - Destination: Name or IP address of the notification receiver traps server
     - Traps Community: SNMP community of the notification receiver traps server
4. When you are finished, click Save SNMP Configuration to save the configuration and update the service with the new configuration.

RADIUS authentication

This topic explains how to configure RADIUS authentication for Skybox Appliance.

Note: To use RADIUS authentication, the pam_radius package must be installed on the Skybox Server. To check whether the package is installed, run rpm -qa | grep pam_radius
If you need help installing the package, contact Skybox Support.

To configure RADIUS authentication
1. Open /etc/pam.d/system-auth in your editor.
2. Add the following line immediately after auth sufficient pam_unix.so nullok try_first_pass:
   auth sufficient pam_radius_auth.so
3. Save and close the file.
4. Open /etc/pam.d/password-auth in your editor.
5. Add the following line immediately after auth sufficient pam_unix.so nullok try_first_pass:
   auth sufficient pam_radius_auth.so
6 Save and close the file.

7 Open /etc/pam_radius.conf in your editor.

8 Replace 127.0.0.1 secret 1 with the relevant information for your RADIUS server.

There are 3 fields per line in this file, each line representing a RADIUS server. The fields are:

server[:port] secret [timeout]

Blank lines or lines beginning with # are ignored.

- The port number is optional. The default port is 1812.
- The timeout field is optional. The default timeout is 3 seconds. The timeout field controls how many seconds the module waits before deciding that the server has failed to respond.

If multiple RADIUS server lines exist, they are tried in order. If a server returns success or failure, the module returns the same result. If a server fails to respond it is skipped and the next server is tried.

9 Save and close the file.

10 Add the user on the operating system level by running:

   useradd <user1>

   There is no need to set the password; it comes from RADIUS.

   You can now log in to Skybox with the user credentials: <user1> /<password> (using the password stored on the RADIUS server for this user).

LDAP authentication

This topic explains how to configure LDAP authentication for Skybox Appliance.

Prerequisites

To use LDAP authentication, the LDAP server must support either TLS/SSL or secure LDAP (LDAPS).

To set up LDAP authentication

1 On the Security tab, click LDAP.

2 Define the authentication according to the fields shown in the following table.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP Servers URI</td>
<td>A comma-separated list of LDAP servers against which to authenticate. The</td>
</tr>
<tr>
<td></td>
<td>format of the URI must match the format defined in RFC 2396: ldap[s]:&lt;server&gt;[:&lt;port&gt;] (where</td>
</tr>
<tr>
<td></td>
<td>&lt;server&gt; is the IP address or name of the LDAP server). The default ports:</td>
</tr>
<tr>
<td></td>
<td>- 389 for regular LDAP</td>
</tr>
<tr>
<td></td>
<td>- 636 for LDAPS</td>
</tr>
<tr>
<td>Force SSL Certification</td>
<td>Specifies whether to enable authentication for SSL certification (LDAPS).</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Certificate Authorities</td>
<td>If you are using SSL certification, a list of the CA chains needed to certify the LDAP servers. Start each certificate on a new line. Example:</td>
</tr>
</tbody>
</table>
| Certificates             | -----BEGIN CERTIFICATE-----
|                          | ...
|                          | ...
|                          | -----END CERTIFICATE-----
|                          | -----BEGIN CERTIFICATE-----
|                          | ...
|                          | ...
|                          | -----END CERTIFICATE-----
| **Note:**               | The certificates must be in PEM format.                                                                                                                                                                    |
| LDAP Search Base         | The default base DN to use for performing LDAP search operations. The syntax must be in DN format.                                                                                                       |
|                          | **Example:** CN=Users,DC=YOURDOMAIN,DC=LOCAL                                                                                                                                                    |
| LDAP Schema              | Select the schema type used on the target LDAP server. The default attribute names retrieved from LDAP servers may vary according to the schema type. The way that some attributes are handled may also differ. The main difference between the schema types is how group memberships are recorded in the server. |
|                          | • The Active Directory schema type sets the attributes to correspond with Active Directory 2008r2 values.                                                                                     |
|                          | • With rfc2307, group members are listed by name in the member uid attribute.                                                                                                                          |
|                          | • With rfc2307bis and IPA, group members are listed by DN and stored in the member attribute.                                                                                                       |
| LDAP Bind User DN        | The user bind DN to use for performing LDAP operations. This user needs to have read permissions to read the user groups.                                                                        |
|                          | **Example:** CN=LDAPUser,CN=Users,DC=YOURDOMAIN,DC=LOCAL                                                                                                                                           |
| LDAP Bind User Password  | The password for the bind user.                                                                                                                                                                        |
| Verify LDAP Bind User Password | Verify the user password.                                                                                                                      |
| Allowed Users            | A comma-separated list of permitted users. If empty, all users are permitted.                                                                  |
| Allowed Groups           | A comma-separated list of permitted groups. If empty, all groups are permitted.                                                                                                                         |

After LDAP authentication is set up, the permitted users can log in to the Skybox Appliance Administration interface using their LDAP user name and password.

**Changing the TLS version**

The Apache HTTP Server module `mod_ssl` provides an interface to the OpenSSL library, which provides Strong Encryption using the Secure Sockets Layer and Transport Layer Security (TLS) protocols.
There are 3 possible configurations for TLS:

- **Default (High) Security configuration for SSL:** TLS versions 1.2 and higher are enabled
  
  Supported browsers are: Firefox 27, Chrome 30, Internet Explorer 11 on Windows 7, Edge, Opera 17, Safari 9, Android 5.0, Java 8, and higher.

- **Medium Security configuration for SSL:** TLS versions 1.1 and higher are enabled
  
  Supported browsers are: Firefox 1, Chrome 1, Internet Explorer 7, Opera 5, Safari 1, Windows XP Internet Explorer 8, Android 2.3, Java 7, and higher.

- **Low Security configuration for SSL:** All TLS versions are enabled
  
  Supported browsers are: Windows XP Internet Explorer 6, Java 6, and higher.

The configuration settings are stored in

`etc/httpd/conf.d/skyboxwebadmin.conf`

**Important:** Use the highest TLS configuration that supports your browser.

**To change the TLS configuration settings**

1. Make a backup of `skyboxwebadmin.conf`
2. Open `skyboxwebadmin.conf` (using `vi`).
3. Comment out the default security configuration by adding “#” at the beginning of the `SSLProtocol` and `SSLCipherSuite` lines.

   ```
   # Default Security configuration for SSL. Oldest compatible clients:
   # Firefox 27, Chrome 30, IE 11 on Windows 7, Edge, Opera 17, Safari 9, 
   # Android 5.0, and Java 8.
   SSLProtocol all -SSLv3 -TLSv1 -TLSv1.1
   SSLCipherSuite ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-
   SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:ECDHE-
   ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-
   SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-
   SHA256
   ```

4. Uncomment either Medium or Low (not both) by deleting “#” from the appropriate `SSLProtocol` and `SSLCipherSuite` lines.

   **Note:** Do not uncomment the title line (Medium Security or Low Security).

   ```
   # Medium Security configuration for SSL. Oldest compatible clients: Firefox 
   # 1, Chrome 1, IE 7, Opera 5, Safari 1, Windows XP IE8, Android 2.3, Java 7
   #SSLProtocol all -SSLv3
   #SSLCipherSuite ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-
   POLY1305:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-
   ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-
   SHA256:DHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-
   SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256:
   ```
#SSLProtocol all
#SSLCipherSuite ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:
ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-
SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-DSS-
AES128-GCM-SHA256:kEDH+AESGCM:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-
SHA256:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES256-SHA384:
ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:DHE-
RSA-AES128-SHA256:DHE-RSA-AES128-SHA:DHE-DSS-AES128-SHA256:DHE-DSS-AES128-
SHA256:DHE-RSA-AES256-SHA256:DHE-DSS-AES256-SHA:DHE-RSA-AES256-SHA:ECDHE-
RSA-DES-CBC3-SHA:ECDHE-ECDSA-DES-CBC3-SHA:EDH-RSA-DES-CBC3-SHA:AES128-GCM-
SHA256:AES256-GCM-SHA384:AES128-SHA256:AES256-SHA256:AES128-SHA:AES256-SHA:
AES:DES-CBC3-SHA:HIGH:SEED:!aNULL:!eNULL:!EXPORT:!DES:!RC4:!MD5:!PSK:!RSAFSK:!aDH:!aECDH:
:!EDH-DSS-DES-CBC3-SHA:!KRB5-DES-CBC3-SHA:!SRP

5  Save the file.

6  Restart httpd by running:

    systemctl restart httpd
Chapter 5

Customizing the syslog server

The syslog server in Skybox Appliance is preconfigured and is enabled by default.

In this chapter

Setting up TCP and UDP listeners .......................................... 26
How to work with syslog files ..................................................... 26

Setting up TCP and UDP listeners

Skybox Appliance includes TCP and UDP listeners for the syslog server.

To set up TCP and UDP listeners

1. On the System tab, click Syslog Server.
2. Select the desired listeners and adjust their bind addresses and ports as necessary.
   The listeners are disabled by default; the default port for each is 514. You can enable either or both listeners, and you can change the bind address and port as necessary.
3. Click Apply Syslog Configuration.

How to work with syslog files

Updates to the configuration files of the syslog server and to the syslog log rotation file are included (when necessary) as part of Skybox updates.

Users can also modify the following files locally for local changes:

- syslog configuration file: /etc/syslog-ng/syslog-ng.conf
- cron file: /etc/cron.daily/syslog-ng-archive

How can I change where and for how long the logs are stored?

The following parameters (shown here with their default values) can be changed in the cron file:

- LOGGER_TAG="skybox-syslog-ng-archive"
- TRAFFIC_LOGS_NEW="/var/log/syslog-ng/new" (directory for new files)
- TRAFFIC_LOGS_OLD="/var/log/syslog-ng/old" (archive directory)
- CHANGE_LOGS_NEW="/var/log/firewall_assurance/change_logs" (directory for new files)
What are the log files named?
A separate log is generated for each device. Log file names have the format:

- (New logs) <device name | IP address>_<time of creation>.log
- (Archived logs) <device name | IP address>_<time of creation>.zip

How can the logs be imported into Skybox?
Device logs can be imported using the following tasks, depending on the information that you are looking for:

- Change Tracking Events – Syslog Import
- Traffic Events – Syslog Import

To import the logs, you must include the following information:

- In the Basic tab:
  - The directory path of the files (/var/log/syslog-ng/new and /var/log/firewall_assurance/change_logs/new)
  - Modules: The scope of devices whose logs are imported

- In the Advanced tab:
  - The date format used by the device
  - (For Cisco and Juniper traffic events) The positions of the Device ID and date in the log
Skybox Manager Installation

You can install Skybox Manager from the DVD included with Skybox or you can download it from the Skybox Appliance over HTTP using the Appliance IP address (https://<Appliance IP address>:444/manager). For additional information, see Installing Skybox Manager (on page 29).

Skybox Manager runs on Windows.

In this chapter

Skybox Manager system requirements .................................. 28
Installing Skybox Manager ................................................. 29
Upgrading Skybox Manager.................................................. 29

Skybox Manager system requirements

Skybox Manager is a Java client application that connects to the Skybox Server (through port 8443).

You can install multiple Skybox Managers on 1 computer; this is useful when connecting to Skybox Servers of different versions.

**Operating system**

The following operating systems are supported for Skybox Manager:

- Windows 7 (64bit only)
- Windows 10 (64bit only)
- Windows Server 2012
- Windows Server 2016

**Screens**

The use of Skybox Manager (Java Client) on 4K screens is not supported. Some on-screen elements do not display as expected on these screens due to limitations of Java Runtime Environment at high resolutions.

**Browser**

The following browsers are supported for Skybox web-based user interfaces:

- Skybox Change Manager: Microsoft Internet Explorer 11, Google Chrome, Mozilla Firefox
  - Microsoft Edge is not supported for Change Manager.
Skybox Horizon: Microsoft Internet Explorer 11, Google Chrome, Mozilla Firefox, Safari
Microsoft Edge is not supported for Horizon.

Skybox Web Client: Google Chrome, Firefox, and Microsoft Edge (version 40 and higher)
Microsoft Internet Explorer is not supported for Web Client.

Hardware

The hardware requirements for Skybox Manager are listed in the following table.

<table>
<thead>
<tr>
<th>Item</th>
<th>Minimum</th>
<th>Recommended</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>Intel i3 or equivalent</td>
<td>Intel i5 or equivalent</td>
</tr>
<tr>
<td>RAM</td>
<td>2 GB</td>
<td>4 GB</td>
</tr>
<tr>
<td>Available disk space</td>
<td>1 GB</td>
<td>2 GB</td>
</tr>
</tbody>
</table>

Installing Skybox Manager

Note: Skybox Manager runs on most Microsoft Windows operating systems. For details, see Skybox Manager system requirements (on page 28).

Installing Skybox Manager requires administrator privileges.

To install Skybox Manager

1. Run the installation file (SkyboxManager-<version#>-<build>.exe).
2. Follow the directions in the wizard.

Note: Installation under <Drive>:\Program Files (or any other path containing a space) is not supported.

Post-installation notes

- Skybox Manager is configured to communicate with the server over 8443/TCP. If there is a firewall between Skybox Manager and Skybox Server, access on this port must be explicitly permitted.
- The user running Skybox Manager must have Modify permissions for the directory where Skybox Manager is installed.

Upgrading Skybox Manager

In some cases, the Skybox Manager installation file on the Appliance is outdated. In this case, you can download the new Skybox Manager installation file (or you might receive it from the Skybox product support team) to replace the old installation file. This way, when Skybox users install Skybox Manager from the Appliance, they are installing the latest version.
To replace the Skybox Manager installation file

1. Copy the installation file (SkyboxManager-<version#>-<build#>.exe) to the Appliance using PuTTY, WinSCP, or any other client program.
   
   Save the file at /usr/local/skyboxwebadmin/manager

2. Delete any other files in this directory, including any previous installation file; the directory must contain only the new installation file.

Updating the operating system on Skybox Appliance

In some cases (for example, after bug fixes or security patches are released for the operating system) it might be necessary to update the CentOS operating system on your Skybox Appliance.

Updates to the operating system do not affect Skybox.

Note: These updates are only possible for CentOS version 7 or higher. The OS update is cumulative: upgrading to the latest version is possible from any previously CentOS 7 based Appliance ISO release.

Before you start the update

Both the Skybox model and important operating system files can be saved as part of the update procedure or you can save them manually. Changes that you made in any Skybox settings files are not saved as part of the update; back them up manually before updating CentOS.

The backed-up files are at
/var/tmp/appliance_update_<installed_version>/backup/appliance_backup

To update the operating system

Note: The machine reboots as part of the update process.

1. Download the following files to your computer (not to the Appliance server), where <patch> is the patch number:
   
   • Skybox_<patch>.appliance_update
   • Skybox_<patch>.appliance_update.md5
2 Copy `Skybox_<patch>.appliance_update` to the Appliance server using SCP.
3 Copy `Skybox_<patch>.appliance_update.md5` to the same directory using SCP.
4 Connect to the Appliance server via SSH using skyboxview credentials.
5 Navigate to the directory where you saved the files.
6 Verify that the update file was copied without any mistakes by running the `md5sum` command:

```
md5sum -c Skybox_<patch>.appliance_update.md5
```

The output should be: `Skybox_<patch>.appliance_update: OK`

7 Install the update by running: `sudo /bin/sh Skybox_<patch>.appliance_update`

The update procedure begins.

8 We recommend that, when asked where to save the files, you select either a location on the file sharing system (as opposed to on the Appliance server) or an external drive.

The default location is `/var/tmp/appliance_update_<patch>/backup/`

Note: After the update finishes, a log of the process details is at `/opt/skyboxview/utility/log/appliance_update_<patch>.log`

9 (Optional) If something went wrong with the update process, you can either restore settings files manually or restore the files together (overwriting the original files but preserving the original ownership and permissions for the files) by running:

```
tar -xpjf /var/tmp/appliance_update_<patch>/backup/<Appliance_backup>.tar.bz2 --overwrite --same-owner -P
```
Chapter 7

SSH hardening

Starting in version 9.0.600, security hardening was added to prevent local users from logging in via SSH.

The following lines were added to `/etc/ssh/sshd_config`:

- `AllowUsers root skyboxview`
- `AllowGroups root skyboxview`
Chapter 8

Adding your own certificate

To connect to the Appliance Administration via your own certificate, add the certificate to the Apache server.

Note: If you generated your own certificate using the Generating and installing a certificate using the Java keytool procedure in the Skybox Installation and Administration Guide, follow the directions in Exporting the Server certificate and private key from the Java keystore (on page 34) before continuing below.

To add your own certificate

1. Log in to the Skybox Server or Collector via SSH as the root user.

2. Transfer the private key to /etc/pki/tls/private

   The private key must not have a passphrase. If a passphrase is used in the private key, the following errors will be seen in the log file /etc/httpd/logs/webadmin-error_log.

   ![Log entries](image)

3. Transfer the server certificate to /etc/pki/tls/certs

4. If you have an intermediate CA certificate:
   a. Concatenate the intermediate CA certificate with the root CA certificate using the following command: cat intermediate.pem root.pem > ca-chain.cert.pem
   b. Transfer the concatenated file to /etc/pki/tls/certs
5 Back up the file /etc/httpd/conf.d/skyboxwebadmin.conf

6 Edit /etc/httpd/conf.d/skyboxwebadmin.conf:
   a. Change **ServerName** from the default (skyboxapp) to the name used in the **Common Name** or **SAN** field of your certificate.
      
      For example: ServerName www.skyboxlab.com
   
   b. Change **SSLCertificateFile** from the default (/etc/pki/tls/certs/localhost.crt) to /etc/pki/tls/certs/<your certificate file>
      
      For example: SSLCertificateFile /etc/pki/tls/certs/skybox_lab.cer
   
   c. Change **SSLCertificateKeyFile** from the default (/etc/pki/tls/private/localhost.key) to /etc/pki/tls/private/<your private key file>
      
      For example: SSLCertificateKeyFile /etc/pki/tls/private/skybox_lab.key
   
   d. If you are using an intermediate CA certificate, add the following line under the line with **SSLCertificateKeyFile**:
      
      SSLCertificateChainFile /etc/pki/tls/certs/ca-chain.cert.pem

7 Restart the Apache server by running:
   
   systemctl restart httpd

8 Make sure that the root CA certificate is installed in your browser’s trusted CA certificate repository.

9 Access the Appliance Administration at https://<common_name>:444

In this chapter

Exporting the Server certificate and private key from the Java keystore

To export the server certificate and private key from the Java keystore

1 Log in to the Skybox Server or Collector as root.

2 Navigate to /opt/skyboxview/server/conf

3 Create a P12 keystore using the following command, replacing <alias> with the alias that you chose when you generated the private key in the Generating and installing a certificate using the Java keytool procedure.

   Replace <version#> with the JDK version (for example, 1.8.0_242).
   
   ../../thirdparty/jdk<version#>/bin/keytool -importkeystore -srckeystore server.keystore -srcstorepass skyboxview -destkeystore server.keystore.p12 -deststoretype PKCS12 -srcalias <alias> -deststorepass skyboxview -destkeypass skyboxview
If you do not remember your alias:

a. Execute the following command:

    ../../../thirdparty/jdk<version#/bin/keytool -list -v -keystore server.keystore -storepass skyboxview

b. Find your server certificate. Above it is the **Alias name** field; this is your alias.

4 Export the server certificate from the keystore using the following command. The certificate is exported directly to /etc/pki/tls/certs.

    openssl pkcs12 -in server.keystore.p12 -nokeys -out /etc/pki/tls/certs/skybox_cert.pem

5 When prompted **Enter Import Password**, enter **skyboxview**.

6 Export the private key from the keystore using the following command. The private key is exported directly to /etc/pki/tls/private.

    openssl pkcs12 -in server.keystore.p12 -nodes -nocerts -out /etc/pki/tls/private/skybox_key.pem

7 When prompted **Enter Import Password**, enter **skyboxview**.

8 Remove the P12 keystore by executing **rm server.keystore.p12**

    **Important**: Do not remove server.keystore.

9 Continue to **Adding your own certificate** (on page 33) and use the exported server certificate and private key when required.
Chapter 9

Monitoring SNMP

Skybox Appliance supports standard Linux OIDs. OIDs that you can monitor include:

**CPU load statistics**
- 1 minute load: .1.3.6.1.4.1.2021.10.1.3.1
- 5 minute load: .1.3.6.1.4.1.2021.10.1.3.2
- 15 minute load: .1.3.6.1.4.1.2021.10.1.3.3

**CPU statistics**
- Percentage of user CPU time: .1.3.6.1.4.1.2021.11.9.0
- Raw user CPU time: .1.3.6.1.4.1.2021.11.50.0
- Percentages of system CPU time: .1.3.6.1.4.1.2021.11.10.0
- Raw system CPU time: .1.3.6.1.4.1.2021.11.52.0
- Percentages of idle CPU time: .1.3.6.1.4.1.2021.11.11.0
- Raw idle CPU time: .1.3.6.1.4.1.2021.11.53.0
- Raw nice CPU time: .1.3.6.1.4.1.2021.11.51.0

**Memory statistics**
- Total swap size: .1.3.6.1.4.1.2021.4.3.0
- Available swap space: .1.3.6.1.4.1.2021.4.4.0
- Total RAM in machine: .1.3.6.1.4.1.2021.4.5.0
- Total RAM used: .1.3.6.1.4.1.2021.4.6.0
- Total RAM free: .1.3.6.1.4.1.2021.4.11.0
- Total RAM shared: .1.3.6.1.4.1.2021.4.13.0
- Total RAM buffered: .1.3.6.1.4.1.2021.4.14.0
- Total cached memory: .1.3.6.1.4.1.2021.4.15.0

**System uptime**
- System uptime: .1.3.6.1.2.1.1.3.0

**Skybox Server and Collector**
In addition to the standard OIDs, the following OIDs are supported for Skybox components.

- Skybox Server status: .1.3.6.1.4.1.8072.1.3.2.3.1.4.19.49.46.51.46.54.46.49.46.52.46.49.46.49.49.57.55.54.56.46.49
Skybox Collector status:
.1.3.6.1.4.1.8072.1.3.2.3.1.4.19.49.46.51.46.54.46.49.46.52.46.49.46.49.57
.55.54.56.46.50
Troubleshooting

Getting version information when the Appliance Administration is not available

If you need to know the version of the Appliance (the image version) and other information about the Appliance when the Appliance Administration is not available, run the `get_appliance_details` script from the CLI.

Sample output of `get_appliance_details`

```
APPLIANCE_VERSION: 8.5.103-7.1.11
CORES: 2
MODE: SERVER
MODEL:
RAM: 32014 MB
SERIAL_NUMBER:
SKYBOXVIEW: 8.0.513
```

Hardware issues

If there is a hardware issue on the Appliance (usually indicated by the system status LED turning amber or blinking):

1. Run `getlogs` as the root user.

   The diagnostic log file, `diagnostic_<timestamp>.log`, is in the `<Skybox_Home>/server/log` directory.

2. Open a support case and attach the (most recent) diagnostic file.
Chapter 11

CIS benchmarks for CentOS 7

All new Skybox Appliances meet the following CIS benchmark recommendations for CentOS 7. Appliances updated to the new ISO also meet the recommendations.

<table>
<thead>
<tr>
<th>Recommendation</th>
<th>Scored</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1.1.1.1 – 1.1.1.8 | ✔️ | Ensure that mounting of the following file systems is disabled:  
  • cramfs  
  • freevxfs  
  • JFFS2  
  • HFS  
  • HFS+  
  • SquashFS  
  • UDF  
  • FAT  
  Rationale: Removing support for unneeded file system types reduces the local attack surface of the system. If this file system type is not needed, disable it. |
| 1.3.1 | ✔️ | Ensure that AIDE is installed. AIDE takes a snapshot of the file system state including modification times, permissions, and file hashes, which can then be used to compare against the current state of the file system to detect modifications to the system.  
  Rationale: By monitoring the file system state, compromised files can be detected to prevent or limit the exposure of accidental or malicious misconfigurations or modified binaries. |
| 1.3.2 | ✔️ | Ensure that file system integrity is regularly checked. Periodic checking of the file system integrity is needed to detect changes to the file system.  
  Rationale: Periodic file checking enables the system administrator to determine on a regular basis if critical files have been changed in an unauthorized fashion. |
| 1.4.1 | ✔️ | Ensure that permissions on bootloader config are configured. The `grub` configuration file contains information about boot settings and passwords for unlocking boot options. The `grub` configuration is usually located at `/boot/grub2/grub.cfg` and linked as `/etc/grub2.conf`  
  Rationale: Setting the permissions to read and write for root only prevents non-root users from seeing the boot parameters or changing them. Non-root users who read the boot parameters may be able to identify weaknesses in boot security and be able to exploit them. |
<p>| 1.4.2 | ✔️ | Ensure that the bootloader password is set. Setting the boot loader password requires that anyone rebooting the system must enter a password before being able to set command line |</p>
<table>
<thead>
<tr>
<th>Recommendation</th>
<th>Scored</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>boot parameters</td>
<td></td>
<td>Rationale: Requiring a boot password on execution of the boot loader prevents an unauthorized user from entering boot parameters or changing the boot partition. This prevents users from weakening security (for example, turning off SELinux at boot time).</td>
</tr>
</tbody>
</table>
| 1.5.1 | ✓ | Ensure that core dumps are restricted. A core dump is the memory of an executable program. It is generally used to determine why a program aborted. It can also be used to glean confidential information from a core file. The system provides the ability to set a soft limit for core dumps, but this can be overridden by the user.  
Rationale: Setting a hard limit on core dumps prevents users from overriding the soft variable. If core dumps are required, consider setting limits for user groups. In addition, setting the `fs.suid_dumpable` variable to 0 prevents setuid programs from dumping core. |
| 1.6.1.5 | ✓ | Ensure that the MCS Translation Service (`mcstrans`) is not installed. The `mcstransd` daemon provides category label information to client processes requesting information. The label translations are defined in `/etc/selinux/targeted/setrans.conf`  
Rationale: Because this service is not used very often, remove it to reduce the amount of potentially vulnerable code running on the system. |
| 1.7.1.3 | ✓ | Ensure that the remote login warning banner is configured properly. The content of the `/etc/issue.net` file is displayed to users prior to login for remote connections from configured services.  
Unix-based systems have typically displayed information about the OS release and patch level when a user logs in to the system. This information can be useful to developers who are developing software for a particular OS platform. If `mingetty(8)` supports the following options, they display operating system information:  
- `\m`: Machine architecture (`uname -m`)  
- `\r`: Operating system release (`uname -r`)  
- `\s`: Operating system name  
- `\v`: Operating system version (`uname -v`)  
Rationale: Warning messages inform users who are attempting to log in to the system of their legal status regarding the system and must include the name of the organization that owns the system and any monitoring policies that are in place. Displaying OS and patch level information in login banners also has the side effect of providing detailed system information to attackers attempting to target specific exploits of a system. Authorized users can get this information by running `uname -a` after they log in. |
| 3.1.2 | ✓ | Ensure that packet redirect sending is disabled  
Rationale: An attacker could use a compromised host to send invalid ICMP redirects to other router devices in an attempt to
### Chapter 11  CIS benchmarks for CentOS 7

<table>
<thead>
<tr>
<th>Recommendation Scored Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>corrupt routing and have users access a system set up by the attacker as opposed to a valid system.</td>
</tr>
</tbody>
</table>

#### 3.2.1 – 3.2.3

**3.2.1:** Ensure that source routed packets are not accepted.  
**Rationale:** Setting `net.ipv4.conf.all.accept_source_route` and `net.ipv4.conf.default.accept_source_route` to 0 disables the system from accepting source routed packets.  
Assume that the system is capable of routing packets to Internet routable addresses on one interface and private addresses on another interface, and the private addresses are not routable to the Internet routable addresses and vice versa. Under normal routing circumstances, an attacker from the Internet routable addresses cannot use the system as a way to reach the private address systems. If, however, source routed packets are permitted, they can be used to gain access to the private address systems as the route can be specified, rather than relying on routing protocols that do not permit this routing.  

**3.2.2:** Ensure that ICMP redirects are not accepted.  
**Rationale:** Attackers could use bogus ICMP redirect messages to maliciously alter the system routing tables and get them to send packets to incorrect networks and permit your system packets to be captured.  

**3.2.3:** Ensure that secure ICMP redirects are not accepted.  
**Rationale:** Even known gateways can be compromised. Setting `net.ipv4.conf.all.secure_redirects` to 0 protects the system from routing table updates by possibly compromised known gateways.  

#### 3.2.4

**Ensure that suspicious packets are logged.** When enabled, this feature logs packets with un-routable source addresses to the kernel log.  
**Rationale:** Enabling this feature and logging these packets enables administrators to investigate the possibility that an attacker is sending spoofed packets to their system.  

#### 3.5.1 – 3.5.4

**Ensure that DCCP, SCTP, RDS, and TIPC are disabled.**  
**Rationale:** If these protocols are not being used, it is recommended that the kernel modules not be loaded, disabling the services to reduce the potential attack surface.  

#### 4.1.8 – 4.1.9

**Ensure that login and logout events are collected; Ensure that session initiation information is collected.** The file `/var/log/lastlog` maintain records of the last time a user successfully logged in. The `/var/run/faillock` directory maintains records of login failures via the `pam_faillock` module. The file `/var/run/utmp` file tracks all currently logged in users. The `/var/log/wtmp` file tracks logins, logouts, shutdown, and reboot events. All audit records are tagged with the identifier 'session'. The file `/var/log/btmp` keeps track of failed login attempts and can be read by entering the command `/usr/bin/last -f /var/log/btmp`. All audit records are tagged with the identifier 'logins'.  
**Rationale:** Monitoring login and logout events could provide a system administrator with information associated with brute
<table>
<thead>
<tr>
<th>Recommendation</th>
<th>Scored</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>force attacks against user logins. Monitoring session information files for changes could alert a system administrator to logins occurring at unusual hours, which could indicate intruder activity (for example, a user logging in at a time when they do not normally log in).</td>
</tr>
</tbody>
</table>
| 4.1.13         | ✓      | Ensure that successful file system mounts are collected. Monitor the use of the mount system call. The `mount` (and `umount`) system call controls the mounting and unmounting of file systems.  
Rationale: It is highly unusual for a non-privileged user to mount file systems to the system. Although tracking mount commands gives the system administrator evidence that external media may have been mounted (based on a review of the source of the mount and confirming that it is an external media type), it does not conclusively indicate that data was exported to the media. |
| 4.1.14         | ✓      | Ensure that file deletion events by users are collected. Monitor the use of system calls associated with the deletion or renaming of files and file attributes. This configuration statement sets up monitoring for `unlink` (remove a file), `unlinkat` (remove a file attribute), `rename` (rename a file) and `renameat` (rename a file attribute) system calls and tags them with the identifier ‘delete’.  
Rationale: Monitoring these calls from non-privileged users could provide a system administrator with evidence that inappropriate removal of files and file attributes associated with protected files is occurring. This audit option looks at all events; system administrators want to look for specific privileged files that are being deleted or altered. |
| 4.1.15         | ✓      | Ensure that changes to the system administration scope (`sudoers`) are collected. Monitor scope changes for system administrations. If the system has been properly configured to force system administrators to log in as themselves first and then use the `sudo` command to execute privileged commands, it is possible to monitor changes in scope. The file `/etc/sudoers` is written to when the file or its attributes have changed. The audit records are tagged with the identifier ‘scope’.  
Rationale: Changes in the `/etc/sudoers` file can indicate that an unauthorized change has been made to scope of system administrator activity. |
| 4.2.2.3        | ✓      | Ensure that `syslog-ng` default file permissions are configured. `syslog-ng` creates log files that do not already exist on the system. This setting controls the permissions that are applied to these newly created files.  
Rationale: It is important to ensure that log files exist and have the correct permissions to ensure that sensitive syslog-ng data is archived and protected. |
| 5.1.1 – 5.1.7  | ✓      | Configuration of `cron`:  
- Ensure that the `cron` daemon is enabled  
- Ensure that permissions on `/etc/crontab` are configured |
<table>
<thead>
<tr>
<th>Recommendation</th>
<th>Scored</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>- Ensure that permissions on <code>/etc/cron.hourly</code> are configured</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Ensure that permissions on <code>/etc/cron.daily</code> are configured</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Ensure that permissions on <code>/etc/cron.weekly</code> are configured</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Ensure that permissions on <code>/etc/cron.monthly</code> are configured</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Ensure that permissions on <code>/etc/cron.d</code> are configured</td>
</tr>
</tbody>
</table>

**Rationale:** Granting write access to these directories for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to these directories could give an unprivileged user insight into how to gain elevated privileges or circumvent auditing controls.

**5.2.5** ✓ Ensure that SSH `MaxAuthTries` is set to 4 or less. The `MaxAuthTries` parameter specifies the maximum number of authentication attempts permitted per connection. When the login failure count reaches half the number, error messages are written to the `syslog` file detailing the login failure.

**Rationale:** Setting the `MaxAuthTries` parameter to a low number minimizes the risk of successful brute force attacks to the SSH server.

**5.2.6** ✓ Ensure that SSH `IgnoreRhosts` is enabled. The `IgnoreRhosts` parameter specifies that `.rhosts` and `.shosts` files are not used in `RhostsRSAAuthentication` or `HostbasedAuthentication`.

**Rationale:** Setting this parameter forces users to enter a password when authenticating with SSH.

**5.2.7** ✓ Ensure that SSH `HostbasedAuthentication` is disabled. The `HostbasedAuthentication` parameter specifies whether authentication is permitted through trusted hosts via the user of `.rhosts`, or `/etc/hosts.equiv`, along with successful public key client host authentication. This option only applies to SSH Protocol Version 2.

**Rationale:** Even though the `.rhosts` files are ineffective if support is disabled in `/etc/pam.conf`, disabling the ability to use `.rhosts` files in SSH provides an additional layer of protection.

**5.2.15** ✓ Ensure that SSH access is limited. There are several options available to limit the users and groups that can access the system via SSH.

- **AllowUsers:** The `AllowUsers` variable gives the system administrator the option of permitting specific users to SSH into the system. The list consists of space-separated user names. Numeric user IDs are not recognized with this variable. If a system administrator wants to restrict user access further by only permitting these users to log in from a particular host, the entry can be specified in the form of `user@host`.

- **AllowGroups:** The `AllowGroups` variable gives the system
<table>
<thead>
<tr>
<th>Recommendation</th>
<th>Scored</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>administrator the option of permitting specific groups of users to SSH into the system. The list consists of space separated group names. Numeric group IDs are not recognized with this variable. Rationale: Restricting the users who can remotely access the system via SSH helps ensure that only authorized users access the system.</td>
</tr>
<tr>
<td>5.2.16</td>
<td>✓</td>
<td>Ensure that the SSH warning banner is configured. The Banner parameter specifies a file whose contents must be sent to the remote user before authentication is permitted. By default, no banner is displayed. Rationale: Banners are used to warn connecting users of the particular site’s policy regarding connection. Presenting a warning message prior to the normal user login may assist the prosecution of trespassers on the computer system.</td>
</tr>
</tbody>
</table>
| 5.3.1          | ✓      | Ensure that password creation requirements are configured. The pam_pwquality.so module checks the strength of passwords. It performs checks including making sure that a password:  
- Is not a dictionary word  
- Is a certain length  
- Contains a mix of characters (for example, alphabet, numeric, other)  
- And more  
The following options are set in the /etc/security/pwquality.conf file:  
- minlen=14: Password must be at least 14 characters  
- dcredit=-1: Provide at least one digit  
- ucredit=-1: Provide at least one uppercase character  
- ocredit=-1: Provide at least one special character  
- lcredit=-1: Provide at least one lowercase character  
**Note:** The values shown are sample values. Rationale: Strong passwords protect systems from being hacked through brute force methods. |
<p>| 5.4.4          | ✓      | Ensure that the default user umask is 027 or more restrictive. The default umask determines the permissions of files created by users. The user creating the file has the discretion of making their files and directories readable by others via the chmod command. Users who wish to permit their files and directories to be readable by others by default may choose a different default umask by inserting the umask command into the standard shell configuration files (.profile, .bashrc, and so on) in their home directories. Rationale: Setting a very secure default value for umask ensures that users make a conscious choice about their file permissions. A default umask setting of 077 causes files and directories created by users to not be readable by any other user on the system. A umask of 027 would make files and directories readable by users in the same Unix group; a umask of 022 would make files readable by every user on the system. |</p>
<table>
<thead>
<tr>
<th>Recommendation</th>
<th>Scored</th>
<th>Description</th>
</tr>
</thead>
</table>
| 6.1.5 – 6.1.9   | ✔      | Permission to user- and group-related files:  
  - /etc/gshadow  
  - /etc/passwd-  
  - /etc/shadow-  
  - /etc/group-  
  - /etc/gshadow-  
  Rationale: It is critical to ensure that these files are protected from unauthorized access. Although they are protected by default, the file permissions could be changed either inadvertently or through malicious actions. |
| 6.1.10         | ✔      | Ensure that no world writable files exist. Unix-based systems support variable settings to control access to files. World writable files are the least secure. See the `chmod(2)` man page for more information.  
  Rationale: Data in world-writable files can be modified and compromised by any user on the system. World writable files may also indicate an incorrectly written script or program that could potentially be the cause of a larger compromise to the system’s integrity. |
| 6.1.11         | ✔      | Ensure that no unowned files or directories exist. Sometimes when administrators delete users from the password file they neglect to remove all files owned by those users from the system.  
  Rationale: A new user who is assigned the deleted user’s user ID or group ID may then end up ‘owning’ these files, and thus have more access on the system than was intended. |

Note: For additional information, refer to CIS CentOS 7 Linux Benchmark, v2.1.1