# Auditing ESXi Shell logins and commands

Archived: 2026-04-05 17:54:15 UTC

### Auditing ESXi Shell logins and commands

calendar_today

**Updated On: 12-02-2025**

**Products**

VMware vSphere ESXi

**Issue/Introduction**

ESXi maintains a history of all commands entered in the ESXi Shell, whether accessed at the console or via SSH. This shell command history is maintained in the `shell.log` file. Within the transcription of commands, the command issuer is identified by the process or world ID. This article describes how to correlate authentication information from the `auth.log` file with the history of commands executed in the ESXi Shell.

**Environment**

**Resolution**

To determine the commands executed in the ESXi Shell, and which user and client issued the request:

1. Obtain access to the `auth.log` and `shell.log` log files.
    - Consume logs via syslog in vRealize Log Insight, and filter on `appname=login,sshd,shell`
    - Log in to the ESXi Shell and open each log using the `less` command.
    - Use a web browser to access `https://ESXiHostnameOrIP/host/auth.log` and `https://ESXiHostnameOrIP/host/shell.log`.
    - Use the `vifs` command line utility in the vCLI to copy the logs to a client and review the logs.
    - Read the files from within a `vm-support` log bundle.

2. Open the log file `/var/log/auth.log` in a text viewer.

3. Identify the authentication record, including the Username, Timestamp, and World ID for the session:

    - ESXi Shell login at the console appears similar to:

      ```
      YYYY-MM-DD HH:MM:SS login[64386]: root login on 'char/tty/1'
      ```

- ESXi Shell login via interactive SSH appears similar to:

```
YYYY-MM-DD HH:MM:SS sshd[12345]: Connection from 10.11.12.13 port 2605
YYYY-MM-DD HH:MM:SS sshd[12345]: Accepted keyboard-interactive/pam for root from 10.11.12.13 port 2605 ssh2
YYYY-MM-DD HH:MM:SS sshd[64386]: Session opened for 'root' on /dev/char/pty/t0
YYYY-MM-DD HH:MM:SS sshd[12345]: Session closed for 'root' on /dev/char/pty/t0
...
YYYY-MM-DD HH:MM:SS sshd[12345]: Session closed for 'root' 2
```

- ESXi Shell login via SSH with public key appears similar to:

```
YYYY-MM-DD HH:MM:SS sshd[12345]: Connection from 10.11.12.13 port 2605
YYYY-MM-DD HH:MM:SS sshd[12345]: Accepted publickey for root from 10.11.12.13 port 2605 ssh2
YYYY-MM-DD HH:MM:SS sshd[64386]: Session opened for 'root' on /dev/char/pty/t0
YYYY-MM-DD HH:MM:SS sshd[12345]: Session closed for 'root' on /dev/char/pty/t0
...
YYYY-MM-DD HH:MM:SS sshd[12345]: Session closed for 'root' 2
```

Each of these authentication records indicates a successful authentication for the user `root` on August 29th at 18:01 GMT. The SSH methods also include the IP address that the connection was initiated from. The shell session is being handled by World `64386`.

4. Close the `/var/log/auth.log` file.

5. Open the `/var/log/shell.log` file in a text viewer.

6. Identify commands entered that contain the same World ID as identified in Step 3, appearing similar to:

```
YYYY-MM-DD HH:MM:SS shell[64386]: Interactive shell session started
YYYY-MM-DD HH:MM:SS shell[64386]: cd /var/log
YYYY-MM-DD HH:MM:SS shell[64386]: ls
YYYY-MM-DD HH:MM:SS shell[64386]: vmware -v
YYYY-MM-DD HH:MM:SS shell[64386]: exit
```

Because the commands were entered in the console session handled by world ID `64386`, they correspond to the authentication session established by the user `root` as described in Step 3.

**Additional Information**

**Feedback**

Was this article helpful?

thumb_up Yes

thumb_down No

---