

# Syslog configuration

## 1. Modifying the JumpServer Configuration File

The configuration files for JumpServer are located at: `/opt/jumpserver/config/config.txt`

The following elements need to be added to the JumpServer configuration:

```
# Syslog Configuration
SYSLOG_ENABLE=true
SYSLOG_ADDR=10.1.12.116:514 # Syslog server IP and port
SYSLOG_FACILITY=local2 # Corresponds to the Syslog configuration file
```

## 2. Restarting JumpServer

After modifying the JumpServer configuration file, you need to restart the service to apply the changes.

Command:

```
jmsctl restart
```

## 3. Verifying the Configuration

Log into the JumpServer service to generate a login event log and check for output on the Syslog server. Example login event log:

```
[root@jumpserver ~]# cat /tmp/messages
Apr 18 16:27:23 10.1.14.125 root: message:rsyslog logging From JumpServer
Apr 18 16:27:42 10.1.14.125 root: message:rsyslog logging From JumpServer(UDP)
Apr 18 16:40:42 10.1.14.125 jumpserver: login_log - {"backend": "Password", "backend_display": "密码", "city": "局域网", "datetime": "2023/04/18 16:34:08 +0800", "id": "adf0e434-e306-4693-9a51-23f256cb025d", "ip": "10.1.10.35", "mfa": {"label": "禁用", "value": 0}, "reason": "", "reason_display": "", "status": {"label": "successful", "value": true}, "type": {"label": "Web", "value": "W"}, "user_agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/111.0", "username": "admin"}
```

## 4. Analyzing Syslog Information

Event Type	Syslog Record Example
Login	Apr 19 15:25:11 10.1.14.125 jumpserver: <b>login_log</b> - {"backend": "Password", "backend_display": "password", "city": "local", "datetime": "2023/04/19 15:18:36 +0800", "id": "cfc378e5-6337-4bf9-a8ac-15f33c2b0314", "ip": "10.1.10.35", "mfa": {"label": "disabled", "value": 0}, "reason": "", "reason_display": "", "status": {"label": "successful", "value": true}, "type": {"label": "Web", "value": "W"}, "user_agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, Gecko) Chrome/112.0.0.0 Safari/537.36 Edg/112.0.1722.48", " <b>username</b> ": "admin"}

<b>File Upload</b>	Apr 19 15:27:26 10.1.14.125 jumpserver: <b>ftp_log</b> - {"account": "root(root)", "asset": "10.1.12.182-root(10.1.12.182)", "date_start": "2023/04/19 15:20:51+0800", "filename": <b>"/tmp/vmware-root/file.pdf"</b> , "id": "6e7721c0-2091-49fb-8853-fc18e0a2e432", "is_success": true, "operate": {"label": "uploading", <b>"value": "upload"</b> }, "org_id": "00000000-0000-0000-0000-000000000002", "remote_addr": "10.1.10.35", "user": "Administrator(admin)"}
<b>File Download</b>	Apr 19 15:28:08 10.1.14.125 jumpserver: <b>ftp_log</b> - {"account": "root(root)", "asset": "10.1.12.182-root(10.1.12.182)", "date_start": "2023/04/19 15:21:33+0800", "filename": <b>"/tmp/vmware-root/file.pdf"</b> , "id": "113c0601-80c1-47d1-a053-5038fd89698c", "is_success": true, "operate": {"label": "downloading", <b>"value": "download"</b> }, "org_id": "00000000-0000-0000-0000-000000000002", "remote_addr": "10.1.10.35", "user": "Administrator(admin)"}

Версия #1  
Сергей Попцов создал 21 января 2025 11:52:07  
Сергей Попцов обновил 21 января 2025 11:55:49