Настройка отправки событий по Syslog

1. Изменение конфигурационного файла JumpServer

Конфигурационные файлы JumpServer по умолчанию находятся в: `/opt/jumpserver/config/config.txt`

В конфигурацию JumpServer необходимо добавить следующие элементы:

```
# Настройка syslog
SYSLOG_ENABLE=true
SYSLOG_ADDR=10.1.12.116:514  # IP и порт сервера Syslog
SYSLOG_FACILITY=local2  # В соответствии с конфигурацией файла Syslog
```

2. Перезапуск JumpServer

После изменения конфигурационного файла JumpServer необходимо перезапустить для загрузки новых конфигураций.

Команда:

```
jmsctl restart
```

3. Проверка конфигурации

Войдите в службу JumpServer, чтобы создать журнал входа, и проверьте, есть ли вывод на сервере Syslog. Пример выходного журнала входа:

4. Анализ информации журнала Syslog

Тип события	Пример записи Syslog

Вход в систему	Apr 19 15:25:11 10.1.14.125 jumpserver: **login_log** - {"backend": "Password", "backend_display": "пароль", "city": "local", "datetime": "2023/04/19 15:18:36 +0800", "id": "cfc378e5-6337-4bf9-a8ac-15f33c2b0314", "ip": "10.1.10.35", "mfa": {"label": "отключено", "value": 0}, "reason": "", "reason_display": "", "status": {"label": "успешно", "value": true}, "type": {"label": "Web", "value": "W"}, "user_agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, как Gecko) Chrome/112.0.0.0 Safari/537.36 Edg/112.0.1722.48", **"user name": "admin"**}
Ззагрузка файла	Apr 19 15:27:26 10.1.14.125 jumpserver: **ftp_log** - {"account": "root(root)", "asset": "10.1.12.182-root(10.1.12.182)", "date_start": "2023/04/19 15:20:51 +0800", "filename": "**/tmp/vmware-root/файл.pdf**", "id": "6e7721c0-2091-49fb-8853-fc18e0a2e432", "is_success": true, "operate": {"label": "uploading", **"value": "upload"**}, "org_id": "00000000-0000-0000-0000-000000000002", "remote_addr": "10.1.10.35", "user": "Administrator(admin)"}
Скачивание файла	Apr 19 15:28:08 10.1.14.125 jumpserver: **ftp_log** - {"account": "root(root)", "asset": "10.1.12.182-root(10.1.12.182)", "date_start": "2023/04/19 15:21:33 +0800", "filename": "**/tmp/vmware-root/файл.pdf**", "id": "113c0601-80c1-47d1-a053-5038fd89698c", "is_success": true, "operate": {"label": "скачивание файла", **"value": "download"**}, "org_id": "00000000-0000-0000-0000-000000000002", "remote_addr": "10.1.10.35", "user": "Administrator(admin)"}
Выполнение операции	Apr 19 15:28:44 10.1.14.125 jumpserver: **operation_log** - {"action": {"label": "update", "value": "update"}, "datetime": "2023/04/19 15:22:09 +0800", "id": "f844f014-2ac5-459d-abd0-ec8f853fa09c", "org_id": "00000000-0000-0000-0000-000000000004", "org_name": "SYSTEM", "remote_addr": "10.1.10.35", "resource": "GLOBAL", "resource_type": "System settings", "user": "Administrator(admin)"}
Смена пароля	Apr 19 15:29:58 10.1.14.125 jumpserver: **password_change_log** - {"change_by": "Administrator(admin)", "datetime": "2023/04/19 15:23:23 +0800", "id": "0cd278ed-8335-49d5-a0c3-0211e9858441", "remote_addr": "10.1.10.35", "user": "Глобальный MFA(MFA)"}
Запуск сессии доступа	Apr 19 15:31:29 10.1.14.125 jumpserver: **host_session_log** - {"account": "root(root)", "account_id": "49536b5e-bf06-4d16-bacd-7d628de3a3f2", "asset": "10.1.12.182-root(10.1.12.182)", "asset_id": "dfba9962-7988-4d29-9b04-6f82dd8e02c3", "can_join": true, "can_replay": false, "can_terminate": true, "comment": null, "date_end": null, "date_start": "2023/04/19 15:24:54 +0800", "has_command": false, "has_replay": false, "id": "4896b882-299a-4759-804e-32250f5b05b7", "is_finished": false, "is_success": true, "login_from": {"label": "веб-терминал", "value": "WT"}, "org_id": "00000000-0000-0000-0000-000000000002", "org_name": "default", "protocol": "ssh", "**remote_addr": "10.1.10.35"**, "terminal": {"id": "7076d4aa-4050-4a2f-855b-2af7a7bd6674", "name": "[KoKo]-jumpserver-v3-86c4b2fc7167"}, "type": {"label": "normal", "value": "normal"}, "user": "Administrator(admin)", "user_id": "cdeb8352-9f45-46d9-8873-b3c7c53022fd"}
Выполнение команды	Apr 19 15:34:00 10.1.14.125 jumpserver: **session_command_log** - {"account": "root(root)", "asset": "10.1.12.182-root(10.1.12.182)", "id": "28400256-e9e2-4454-8127-4880fe5b9684", **"input": "free -h", "org_id": "00000000-0000-0000-0000-000000000002", "output": "free -h\r\n total used free shared buff/cache available\r\nMem: 7.6G 4.3G 136M 28M 3.2G 3.0G"**, "remote_addr": "10.1.10.35", "risk_level": {"label": "обычный", "value": 0}, "session": "4896b882-299a-4759-804e-32250f5b05b7", "timestamp": 1681889159, "timestamp_display": "2023/04/19 15:25:59 +0800", "user": "Administrator(admin)"}

Версия #1
Сергей Попцов создал 16 мая 2024 14:07:03
Сергей Попцов обновил 8 марта 2025 17:19:32