SYSLOG AND WEBADM

Syslog and WebADM

SIEM Splunk syslog rsyslog WebADM

1. Overview

This HowTo describes how to configure WebADM to send logs to the local syslog and optionnaly after to a remote syslog (rsyslog) server. Procedure may changes according to the operating system, this configuration has been tested with CentOS Stream and RHEL OS. Please, refer to Rsyslog documentation for more information.

2. Configuration

2.1 WebADM configuration

On WebADM side, you need to edit the following configuration file :

```
/opt/webadm/conf/webadm.conf
```

Then you have to configure/enable the following settings:

```
log_syslog yes
syslog_facility LOG_LOCAL0
syslog_format CEF
```

Here, we are using le syslog facility local0 and the logs format is configured to the CEF which is a standard for every SIEM solutions.

Restart WebADM with the following command in order for changes takes effect:

```
/opt/webadm/bin/webadm restart
```

WebADM configuration is done.

2.2 Syslog configuration

WebADM is now configured to send logs to `/var/log/local0.log`. If the file does not already exist, you have to create it.

```
touch /var/log/local0
```

Set the proper permissions to `/var/log/local0.log` file:

```
chmod 600 /var/log/local0.log
chown root:root /var/log/local0.log
```

Now, configure the following in `/etc/rsyslog.conf`:

```
#### RULES ####

local0.*                        /var/log/local0.log
```

Restart syslog and rsyslog services.

```
systemctl restart rsyslog
systemctl restart syslog
```

WebADM logs should now be sent to `/var/log/local0.log`

```
cat /var/log/local0.log
```

```
Aug  9 12:09:40 webadm1 webadm[2170148]: CEF:0|RCDevs|WebADM|2.1.13|OpenOTP|New
openotpNormalLogin SOAP request|1|event=file rt=1660039780 sid=8QCFTXC6
src=192.168.4.20 spt=50652 dst=192.168.4.20 dpt=8080 request=/openotp/index.php?
token=5a5033bdbf34310a91267ae582e6fa680000434e3d796f616e6e2074726175742c4f553d5355504164

Aug  9 12:09:40 webadm1 webadm[2170148]: CEF:0|RCDevs|WebADM|2.1.13|OpenOTP|> Username:
yoann|1|event=file rt=1660039780 sid=8QCFTXC6 src=192.168.4.20 spt=50652
dst=192.168.4.20 dpt=8080 request=/openotp/index.php?
token=5a5033bdbf34310a91267ae582e6fa680000434e3d796f616e6e2074726175742c4f553d5355504164

Aug  9 12:09:40 webadm1 webadm[2170148]: CEF:0|RCDevs|WebADM|2.1.13|OpenOTP|> Domain:
SUPPORT|1|event=file rt=1660039780 sid=8QCFTXC6 src=192.168.4.20 spt=50652
dst=192.168.4.20 dpt=8080 request=/openotp/index.php?
token=5a5033bdbf34310a91267ae582e6fa680000434e3d796f616e6e2074726175742c4f553d5355504164

Aug  9 12:09:40 webadm1 webadm[2170148]: CEF:0|RCDevs|WebADM|2.1.13|OpenOTP|> LDAP
Password: xxxxxxxx|1|event=file rt=1660039780 sid=8QCFTXC6 src=192.168.4.20 spt=50652
dst=192.168.4.20 dpt=8080 request=/openotp/index.php?
token=5a5033bdbf34310a91267ae582e6fa680000434e3d796f616e6e2074726175742c4f553d5355504164

Aug  9 12:09:40 webadm1 webadm[2170148]: CEF:0|RCDevs|WebADM|2.1.13|OpenOTP|> Client
ID: LDAP|1|event=file rt=1660039780 sid=8QCFTXC6 src=192.168.4.20 spt=50652
```

dst=192.168.4.20 dpt=8080 request=/openotp/index.php?
token=5a5033bdbf34310a91267ae582e6fa680000434e3d796f616e6e2074726175742c4f553d5355504164(

Aug 9 12:09:40 webadm1 webadm[2170148]: CEF:0|RCDevs|WebADM|2.1.13|OpenOTP|> Source
IP: 192.168.3.132|1|event=file rt=1660039780 sid=8QCFTXC6 src=192.168.4.20 spt=50652
dst=192.168.4.20 dpt=8080 request=/openotp/index.php?
token=5a5033bdbf34310a91267ae582e6fa680000434e3d796f616e6e2074726175742c4f553d5355504164(

Aug 9 12:09:40 webadm1 webadm[2170148]: CEF:0|RCDevs|WebADM|2.1.13|OpenOTP|> Context
ID: f3b109f26a25b60a839984340c68ac56|1|event=file rt=1660039780 sid=8QCFTXC6
src=192.168.4.20 spt=50652 dst=192.168.4.20 dpt=8080 request=/openotp/index.php?
token=5a5033bdbf34310a91267ae582e6fa680000434e3d796f616e6e2074726175742c4f553d5355504164(

Aug 9 12:09:40 webadm1 webadm[2170148]: CEF:0|RCDevs|WebADM|2.1.13|OpenOTP|> Options:
WEBAUTH|1|event=file rt=1660039780 sid=8QCFTXC6 src=192.168.4.20 spt=50652
dst=192.168.4.20 dpt=8080 request=/openotp/index.php?
token=5a5033bdbf34310a91267ae582e6fa680000434e3d796f616e6e2074726175742c4f553d5355504164(

Aug 9 12:09:40 webadm1 webadm[2170148]: CEF:0|RCDevs|WebADM|2.1.13|OpenOTP|Enforcing
client policy: LDAP (matched client ID)|1|event=file rt=1660039780 sid=8QCFTXC6
src=192.168.4.20 spt=50652 suser=192.168.3.132 dst=192.168.4.20 dpt=8080
request=/openotp/index.php?
token=5a5033bdbf34310a91267ae582e6fa680000434e3d796f616e6e2074726175742c4f553d5355504164(

Aug 9 12:09:40 webadm1 webadm[2170148]: CEF:0|RCDevs|WebADM|2.1.13|OpenOTP|Registered
openotpNormalLogin request|1|event=file rt=1660039780 sid=8QCFTXC6 src=192.168.4.20
spt=50652 suser=192.168.3.132 dst=192.168.4.20 dpt=8080 request=/openotp/index.php?
token=5a5033bdbf34310a91267ae582e6fa680000434e3d796f616e6e2074726175742c4f553d5355504164(

Aug 9 12:09:40 webadm1 webadm[2170148]: CEF:0|RCDevs|WebADM|2.1.13|OpenOTP|Ignoring 3
groups for user 'CN=yoann ,OU=SUPAdmins,DC=support,DC=rcdevs,DC=com' (out of domain
group search base)|1|event=file rt=1660039780 sid=8QCFTXC6 src=192.168.4.20 spt=50652
suser=192.168.3.132 dst=192.168.4.20 dpt=8080 request=/openotp/index.php?
token=5a5033bdbf34310a91267ae582e6fa680000434e3d796f616e6e2074726175742c4f553d5355504164(

Aug 9 12:09:40 webadm1 webadm[2170148]: CEF:0|RCDevs|WebADM|2.1.13|OpenOTP|Resolved
LDAP user: CN=yoann ,OU=SUPAdmins,DC=support,DC=rcdevs,DC=com|1|event=file
rt=1660039780 sid=8QCFTXC6 src=192.168.4.20 spt=50652 suser=192.168.3.132
dst=192.168.4.20 dpt=8080 request=/openotp/index.php?
token=5a5033bdbf34310a91267ae582e6fa680000434e3d796f616e6e2074726175742c4f553d5355504164(

Aug 9 12:09:40 webadm1 webadm[2170148]: CEF:0|RCDevs|WebADM|2.1.13|OpenOTP|New
openotpNormalLogin request (SUPPORT\\yoann)|1|event=sql rt=1660039780 sid=8QCFTXC6
src=192.168.4.20 spt=50652 suser=192.168.3.132 dst=192.168.4.20 dpt=8080
request=/openotp/index.php?
token=5a5033bdbf34310a91267ae582e6fa680000434e3d796f616e6e2074726175742c4f553d5355504164(

Aug 9 12:09:40 webadm1 webadm[2170148]: CEF:0|RCDevs|WebADM|2.1.13|OpenOTP|Started
transaction lock for user|1|event=file rt=1660039780 sid=8QCFTXC6 src=192.168.4.20
spt=50652 suser=192.168.3.132 dst=192.168.4.20 dpt=8080 request=/openotp/index.php?
token=5a5033bdbf34310a91267ae582e6fa680000434e3d796f616e6e2074726175742c4f553d5355504164(

```
Aug  9 12:09:40 webadm1 webadm[2170148]: CEF:0|RCDevs|WebADM|2.1.13|OpenOTP|Found user
language: FR|1|event=file rt=1660039780 sid=8QCFTXC6 src=192.168.4.20 spt=50652
suser=192.168.3.132 dst=192.168.4.20 dpt=8080 request=/openotp/index.php?
token=5a5033bdbf34310a91267ae582e6fa680000434e3d796f616e6e2074726175742c4f553d5355504164

Aug  9 12:09:40 webadm1 webadm[2170148]: CEF:0|RCDevs|WebADM|2.1.13|OpenOTP|Found 1
user mobiles: +33xxxxxxxx|1|event=file rt=1660039780 sid=8QCFTXC6 src=192.168.4.20
spt=50652 suser=192.168.3.132 dst=192.168.4.20 dpt=8080 request=/openotp/index.php?
token=5a5033bdbf34310a91267ae582e6fa680000434e3d796f616e6e2074726175742c4f553d5355504164

Aug  9 12:09:40 webadm1 webadm[2170148]: CEF:0|RCDevs|WebADM|2.1.13|OpenOTP|Found 1
user emails: yoann@suppot.rcdevs.com|1|event=file rt=1660039780 sid=8QCFTXC6
src=192.168.4.20 spt=50652 suser=192.168.3.132 dst=192.168.4.20 dpt=8080
request=/openotp/index.php?
token=5a5033bdbf34310a91267ae582e6fa680000434e3d796f616e6e2074726175742c4f553d5355504164

Aug  9 12:09:40 webadm1 webadm[2170148]: CEF:0|RCDevs|WebADM|2.1.13|OpenOTP|Found 48
user settings:
LoginMode=LDAP,OTPType=TOKEN,OTPFallback=SMS,PushLogin=No,PushVoice=No,LockTimer=5,MaxTri
1:HOTP-SHA1-6:QN06-
T1M,DeviceType=FIDO2,U2FPINMode=Discouraged,SMSType=Normal,SMSMode=Ondemand,ReplyData=
[1
Items],MailMode=Ondemand,PrefetchExpire=10,LastOTPTime=300,ListChallengeMode=ShowID|1|eve
rt=1660039780 sid=8QCFTXC6 src=192.168.4.20 spt=50652 suser=192.168.3.132
dst=192.168.4.20 dpt=8080 request=/openotp/index.php?
token=5a5033bdbf34310a91267ae582e6fa680000434e3d796f616e6e2074726175742c4f553d5355504164

Aug  9 12:09:40 webadm1 webadm[2170148]: CEF:0|RCDevs|WebADM|2.1.13|OpenOTP|Found 8
user data:
OTPPrefix,AppKeyInit,VoiceState,TokenType,TokenKey,TokenState,TokenID,TokenSerial|1|event
rt=1660039780 sid=8QCFTXC6 src=192.168.4.20 spt=50652 suser=192.168.3.132
dst=192.168.4.20 dpt=8080 request=/openotp/index.php?
token=5a5033bdbf34310a91267ae582e6fa680000434e3d796f616e6e2074726175742c4f553d5355504164

Aug  9 12:09:40 webadm1 webadm[2170148]: CEF:0|RCDevs|WebADM|2.1.13|OpenOTP|Requested
login factors: LDAP|1|event=file rt=1660039780 sid=8QCFTXC6 src=192.168.4.20 spt=50652
suser=192.168.3.132 dst=192.168.4.20 dpt=8080 request=/openotp/index.php?
token=5a5033bdbf34310a91267ae582e6fa680000434e3d796f616e6e2074726175742c4f553d5355504164

Aug  9 12:09:40 webadm1 webadm[2170148]: CEF:0|RCDevs|WebADM|2.1.13|OpenOTP|LDAP
password Ok|1|event=file rt=1660039780 sid=8QCFTXC6 src=192.168.4.20 spt=50652
suser=192.168.3.132 dst=192.168.4.20 dpt=8080 request=/openotp/index.php?
token=5a5033bdbf34310a91267ae582e6fa680000434e3d796f616e6e2074726175742c4f553d5355504164

Aug  9 12:09:40 webadm1 webadm[2170148]: CEF:0|RCDevs|WebADM|2.1.13|OpenOTP|Updated
user data|1|event=file rt=1660039780 sid=8QCFTXC6 src=192.168.4.20 spt=50652
suser=192.168.3.132 dst=192.168.4.20 dpt=8080 request=/openotp/index.php?
token=5a5033bdbf34310a91267ae582e6fa680000434e3d796f616e6e2074726175742c4f553d5355504164

Aug  9 12:09:40 webadm1 webadm[2170148]:
CEF:0|RCDevs|WebADM|2.1.13|OpenOTP|Authentication success (LDAP)|1|event=sql
rt=1660039780 sid=8QCFTXC6 src=192.168.4.20 spt=50652 suser=192.168.3.132
dst=192.168.4.20 dpt=8080 request=/openotp/index.php?
```

```
dst=192.168.4.20 dpt=8080 request=/openotp/index.php?
token=5a5033bdbf34310a91267ae582e6fa680000434e3d796f616e6e2074726175742c4f553d5355504164(

Aug  9 12:09:40 webadm1 webadm[2170148]: CEF:0|RCDevs|WebADM|2.1.13|OpenOTP|Sent login
success response|1|event=file rt=1660039780 sid=8QCFTXC6 src=192.168.4.20 spt=50652
suser=192.168.3.132 dst=192.168.4.20 dpt=8080 request=/openotp/index.php?
token=5a5033bdbf34310a91267ae582e6fa680000434e3d796f616e6e2074726175742c4f553d5355504164(
```

The structure of the generated logs in CEF format is the following:

```
DATE | SERVER NAME | Process Name & PID | LOG FORMAT | Product Provider | Product name
| Product version | Web Service/Application name | Request summary | severity | Log
details
```

3. Configure syslog to send logs to a remote syslog server

In order to send local syslog logs to a remote syslog, you have to edit the file `/etc/rsyslog.conf` and add the following:

```
local0.* action(type="omfwd"
queue.type="linkedlist"
queue.filename="rcdevs_fwd"
action.resumeRetryCount="-1"
queue.saveOnShutdown="on"
target="192.168.10.250" port="514" protocol="tcp"
)
```

Just replace the target and port by your Rsyslog IP address/hostname, port and protocol if needed according to your Rsylog server configuration. On my side it is 192.168.10.250, port 514/TCP.

Restart syslog and rsyslog services.

```
systemctl restart rsyslog
systemctl restart syslog
```

Logs should now be sent to your Rsyslog server.