Espy Server Troubleshooting

Sample Espy Server Installation

The following sections contain snippets of terminal logs from a sample installation. The sample installation was created using the installer included with AC-Hunter. The following logs detail how the installation was created.

```
# unpacked the installer and installed the Espy server on 192.168.3.20
tar xf AC-Hunter-v6.2.1.tar
cd achunter/
./install_acm.sh espy 192.168.3.20
…
```

We aren't transferring logs to AC-Hunter in this installation, so we select 127.0.0.1 when the installer asks where to send the resulting Zeek logs.

```
Please enter the hostname or IP address of your AC-Hunter system: 127.0.0.1
…
```

Checking the Docker Containers

After installing the Espy server, the espy.sh script will act as a wrapper for docker-compose. We can use this script to check the status of the two Docker containers which back the Espy service.

```
ssh 192.168.3.20
espy.sh ps
[sudo] password for ____:
      Name                     Command           State             Ports
-------------------------------------------------------------------------------
---
espy_espy_1             /espy                    Up
espy_redis-server_1   redis-server               Up    0.0.0.0:6379->6379/tcp,
                        /etc/espy/red ...                  :::6379->6379/tcp
```

In this example, we see that the Redis and the Espy log writing service are "Up" and running. If either container is consistently listed as restarting, that signals that the container is repeatedly crashing. If both are listed as Down, then the service needs to be restarted with the command `espy.sh up -d`.

Inspecting the Zeek Logs Written by Espy

Espy collects Sysmon logs from Windows endpoints and generates Zeek logs as a result. These Zeek logs are stored in `/opt/zeek/logs`.

As Espy runs, Zeek files are written out to the subdirectory `/opt/zeek/logs/ecs-spool`. There should be two files in this directory: `conn.log` and `dns.log`.

At the top of each hour, the files in the `ecs-spool` subdirectory are compressed and archived. The resulting files are archived by date and stored in the subdirectory `/opt/zeek/logs/YYYY-MM-DD`.

Espy will always write out a Zeek log even if there are no records to write. At a minimum, each Zeek log will contain a Zeek header with an `#open` timestamp and a footer with a `#close` timestamp.

Checking if Espy is Writing Zeek Records

To check if Espy is currently writing Zeek records, check the spool files for entries that do not begin with `#`. These files are located at `/opt/zeek/logs/ecs-spool/conn.log` and `/opt/zeek/logs/ecs-spool/dns.log`.

If Espy has not generated any Zeek records since the top of the hour, the following commands will return `0`. These commands count the number of uncommented lines in the spool files

```
grep -v "^#" /opt/zeek/logs/ecs-spool/conn.log | wc -l
0
grep -v "^#" /opt/zeek/logs/ecs-spool/dns.log | wc -l
0
```

Otherwise, if data is flowing correctly, these checks should show that there are uncommented entries in the spool files.

```
grep -v "^#" /opt/zeek/logs/ecs-spool/conn.log | wc -l
146
grep -v "^#" /opt/zeek/logs/ecs-spool/dns.log | wc -l
21
```

Monitoring the Espy Redis Server

Connect to the Espy Redis Server as an Administrator

In order to troubleshoot the Espy Redis server, we must connect to Redis over TLS with an authenticated account. The following terminal logs demonstrate how to use the redis-cli container to connect to the Espy Redis server.

```
ssh 192.168.3.20
sudo nano /etc/espy/docker-compose.yml
```

Remove the leading # marks from the following section of the file

```
#  redis-cli:
#    image: redis:6.0
#    volumes:
#      - ${ESPY_CONFIG_DIR:-/etc/espy}:/etc/espy
#    entrypoint: ""
#    command: ["redis-cli", "-h", "redis-server"]
```

Copy the Redis admin password. This password should only be used for troubleshooting.

```
sudo grep admin /etc/espy/redis.conf | cut -d'>' -f2
mlF_OBPU0kdN7HZahC9OYp6PYRfmFh6dCeri5o44Uyb5MPBQco
```

Connect to Redis with the redis-cli and authenticate as the admin

```
espy.sh run --rm redis-cli redis-cli -h redis-server --tls --cacert
/etc/espy/certificates/redis.crt

redis-server:6379> AUTH admin
mlF_OBPU0kdN7HZahC9OYp6PYRfmFh6dCeri5o44Uyb5MPBQco

OK
```

Logging Operations on the Espy Redis Server

At the redis-cli console, the command `MONITOR` will list all of the operations being performed on the Redis server.

```
redis-server:6379> MONITOR
OK
1668049060.260607 [0 172.18.0.2:34604] "blpop" "net-data:sysmon" "1"
1668049061.264316 [0 172.18.0.2:34604] "blpop" "net-data:sysmon" "1"
1668049062.267717 [0 172.18.0.2:34604] "blpop" "net-data:sysmon" "1"
1668125159.832850 [0 192.168.3.101:60014] "RPUSH" "net-data:sysmon"
"{\"@timestamp\":\"2022-11-10T04:55:20.983Z\" …
```

The `MONITOR` command does not like to exit cleanly. Use use `CTRL+P` followed by `CTRL+Q` in order to kill the process via the Docker daemon.

`RPUSH` commands are sent by each Espy agent to send data back to the Espy Redis server. The `MONITOR` log lists the IP address of each Espy agent alongside the full text of the Sysmon logs being monitored in an escaped JSON format.

After the agents push their logs to the Espy Redis server, the logs are collected by the Espy log writing service using the `blpop` command.

Uninstalling the Espy Server

The following commands remove the Espy server and configuration files.

```
espy.sh down -v                    # removes Docker containers and volumes:
sudo rm /usr/local/bin/espy.sh     # removes executable symlink
sudo rm -r /opt/Espy               # removes executable files
sudo rm -r /etc/espy               # removes configuration files
```

To remove the output from Espy, run the following command. Do not run this command if Zeek is also installed on the system.

```
sudo rm -r /opt/zeek               # removes Zeek folder created by Espy
```

Espy installs Docker and docker-compose as dependencies. Docker-compose may be installed in one of two ways. If the machine has an up to date version of `python3`, docker-compose is likely installed via `pip`. If the machine does not, docker-compose will be installed as a binary in `/usr/local/bin`.

First, remove the symlink used to add docker-compose to the `PATH`.

```
sudo rm /usr/bin/docker-compose          # remove symlinks
```

Then, run the following commands to uninstall docker-compose. The first command will uninstall docker-compose if it was installed via `pip`. The second command will uninstall docker-compose if it was installed as a binary.

```
python3 -m pip uninstall docker-compose   # uninstall docker-compose
sudo rm /usr/local/bin/docker-compose     # remove docker-compose binary
```

To remove Docker, use the system package manager such as `apt`, `yum`, or `dnf`.

```
sudo apt remove docker                    # Change apt to yum / dnf as needed
```

Espy Agent Troubleshooting

Finding the Agent Password on the Espy Server

We need the Redis agent password from the Espy server to connect Espy agents. This password is displayed during the Espy installation. Additionally, the password can be retrieved from the system using the following command.

```
sudo grep "user default" /etc/espy/redis.conf | cut -d'>' -f2
Aji2RCdxzk0X8SM1T_5E6xfAei_dPN4gJDrVTufyQ0YCUFduvN
```

Sample Agent Installation

On an up to date installation of Windows 10, the Espy agent installation script (`install-sysmon-beats.ps1`) was downloaded from https://github.com/activecm/espy/releases/tag/v0.0.8 (latest version at the time of writing).

Powershell was then used to install the agent:

```
cd .\Downloads
Set-ExecutionPolicy Bypass -Scope Process
… [A] Yes to All … : A

.\install-sysmon-beats.ps1
…
# Enter the domain name or IP address of the Espy server
RedisHost: 192.168.3.20
…
# Enter the password from the Espy installation.
Enter value for REDIS_PASSWORD:
Aji2RCdxzk0X8SM1T_5E6xfAei_dPN4gJDrVTufyQ0YCUFduvN
```

Ensure the Windows Services Are Running

Both Sysmon and Winlogbeat should run at startup. The services can be controlled with `start-service` and `stop-service` as well as the task manager.

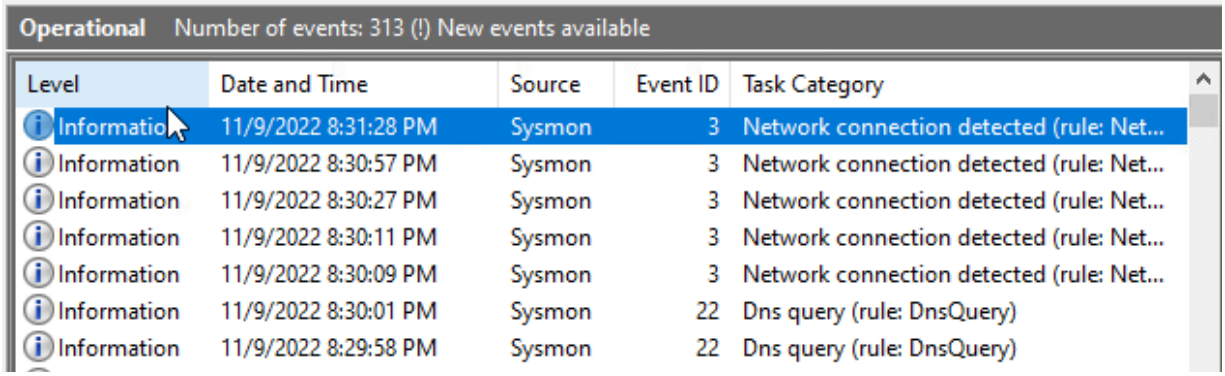
```
# Check if sysmon is running
get-service sysmon64

Status   Name               DisplayName
------   ----               -----------
Running  Sysmon64           sysmon64
```

```
# Check if winlogbeat is running
get-service winlogbeat
Status   Name               DisplayName
------   ----               -----------
Running  winlogbeat         winlogbeat
```

Ensure Logs Are Being Written to the Windows Event Log

- Generate network traffic by opening a web browser or equivalent
- Check the Powershell output of
    - Get-WinEvent -LogName Microsoft-Windows-Sysmon/Operational
- Or, open Event Viewer
- Ensure the following log is available in the leftmost panel
    - `Applications and Services Logs`
        - `Microsoft`
            - `Windows`
                - `Sysmon`
                    - `Operational`
- Ensure that there are entries in the log with Event ID 3 and 22



Ensure Winlogbeat Is Sending Logs to the Espy Redis Server

The Winlogbeat log is stored at `C:\ProgramData\winlogbeat\logs\winlogbeat`.

When the system is running successfully, the log will contain lines that look like this.

```
2022-11-09T20:44:54.978-0700    INFO    pipeline/output.go:105    Connection
to redis(tcp://192.168.3.20:6379) established
2022-11-09T20:44:55.027-0700    INFO    beater/eventlogger.go:81
EventLog[Microsoft-Windows-Sysmon/Operational] successfully published 425
events
```

Ensure the Winlogbeat Is Set Correctly

The Winlogbeat log at `C:\ProgramData\winlogbeat\logs\winlogbeat` contains one of the following lines when the password does not match the password stored on the server.

```
2022-11-08T15:31:28.630-0800 ERROR pipeline/output.go:100 Failed to connect
to redis(tcp://192.168.3.20:6379): WRONGPASS invalid username-password

2022-11-09T20:34:19.218-0700 ERROR pipeline/output.go:100 Failed to connect
to redis(tcp://192.168.3.20:6379): NOAUTH Authentication required.
```

Resetting the Agent Redis Password

In order to reset the Winlogbeat password, we must remove the password from the Winlogbeat keystore, recreate it, and restart the service.

First, check if the password exists in the Winlogbeat keystore.

```
cd $Env:ProgramFiles\winlogbeat*
.\winlogbeat.exe --path.data "$Env:ProgramData\winlogbeat" keystore list
REDIS_PASSWORD
```

Be careful when pasting in the password using Powershell. It is difficult to tell whether the right-click to paste action worked correctly. (Tip: At the password prompt, hit the spacebar, backspace over it, and then right-click to paste the password. This ensures that the right-click performs the paste.)

```
cd $Env:ProgramFiles\winlogbeat*
.\winlogbeat.exe --path.data "$Env:ProgramData\winlogbeat" keystore remove
REDIS_PASSWORD
.\winlogbeat.exe --path.data "$Env:ProgramData\winlogbeat" keystore add
REDIS_PASSWORD
Enter value for REDIS_PASSWORD:
Aji2RCdxzk0X8SM1T_5E6xfAei_dPN4gJDrVTufyQ0YCUFduvN
Successfully updated the keystore

stop-service winlogbeat
rm C:\ProgramData\winlogbeat\logs\winlogbeat
start-service winlogbeat
```

From here, check the log at `C:\ProgramData\winlogbeat\logs\winlogbeat` for one of the two following messages.

The following message will be displayed if the password still does not match the Espy server.

```
2022-11-09T20:34:19.218-0700    ERROR    pipeline/output.go:100    Failed to
connect to redis(tcp://192.168.3.20:6379): NOAUTH Authentication required.
```

If the password was updated correctly and there are no other connection issues, messages like the following will be displayed.

```
2022-11-09T20:44:54.978-0700    INFO    pipeline/output.go:105    Connection
to redis(tcp://192.168.3.20:6379) established
2022-11-09T20:44:55.027-0700    INFO    beater/eventlogger.go:81
EventLog[Microsoft-Windows-Sysmon/Operational] successfully published 425
events
```

Uninstalling the Espy Agent

To uninstall the Espy agent, Winlogbeat and Sysmon must be removed from the system.

Uninstall Winlogbeat

```
Set-ExecutionPolicy Bypass -Scope Process
& ’C:\Program Files\winlogbeat*\uninstall-service-winlogbeat.ps1’
rm -Recurse ’C:\Program Files\winlogbeat*’
rm -Recurse ’C:\ProgramData\winlogbeat\’
```

Uninstall Sysmon

```
& ’C:\Program Files\Sysmon\Sysmon64.exe’ -u
rm -Recurse ’C:\Program Files\Sysmon’
```