

InsightIDR – Orchestrator Migration

This is a documentation intended for an administrator for migrating InsightIDR Orchestrator to a new orchestrator.

1. Log into an old orchestrator (The Username and Password is locating in Bitwarden)
Follow the command below on an old orchestrator.

```
Last login: Fri May 10 21:34:20 2024 from 10.0.10.253
rapid7@rapid7-orchestrator:~$ orch-stop
rapid7@rapid7-orchestrator:~$ chmod 777 /opt/rapid7
chmod: changing permissions of '/opt/rapid7': Operation not permitted
rapid7@rapid7-orchestrator:~$ sudo chmod 777 /opt/rapid7
rapid7@rapid7-orchestrator:~$ cd /opt/rapid7
rapid7@rapid7-orchestrator:/opt/rapid7$ ll
total 68
drwxrwxrwx 3 root      root      4096 May 23 13:54 ./
drwxr-xr-x 4 root      root      4096 Mar 20 21:42 ../
drwxr-x--- 6 insightconnect insightconnect 4096 Mar 20 21:42 orchestrator/
-rw-r--r-- 1 rapid7    rapid7    55317 May 23 13:54 orchestrator.tar.gz
rapid7@rapid7-orchestrator:/opt/rapid7$ sudo tar -xvzf orchestrator.tar.gz
orchestrator/
orchestrator/etc/
orchestrator/etc/trigger-statistics
orchestrator/etc/executor.conf
orchestrator/etc/enrollment-text
orchestrator/etc/restartable-triggers
orchestrator/etc/plugins.conf
orchestrator/var/
orchestrator/var/bolt-log-20240408.gz
orchestrator/var/bolt-log-20240412.gz
orchestrator/var/cache/
orchestrator/var/cache/plugins/
orchestrator/var/cache/plugins/rapid7_active_directory_ldap_3.2.4/
orchestrator/var/cache/plugins/rapid7_cymru_malware_hash_2.0.0/
orchestrator/var/cache/plugins/rapid7_dig_1.0.1/
orchestrator/var/cache/plugins/rapid7_whois_1.0.3/
orchestrator/var/cache/plugins/rapid7_cymru_malware_hash_1.0.2/
orchestrator/var/tmp/
orchestrator/var/enrollment
orchestrator/var/bolt-log-20240411.gz
orchestrator/var/bolt-log-20240409.gz
orchestrator/var/bolt-log
orchestrator/var/bolt-log-20240410.gz
orchestrator/var/bolt-log-20240407.gz
orchestrator/var/keypair
orchestrator/var/bolt-log-20240413
orchestrator/var/executorddb
orchestrator/ca-cert-mirror/
rapid7@rapid7-orchestrator:/opt/rapid7$ sudo chmod 775 /opt/rapid7
rapid7@rapid7-orchestrator:/opt/rapid7$ orch-diagnostics
sudo: yum: command not found

Our online help guide is located at https://insightconnect.help.rapid7.com
For more specific Orchestrator troubleshooting guidelines, visit https://insightconnect.help.rapid7.com/docs/troubleshoot-an-orchestrator
Our Orchestrator build number is:
Our KOMAND_API_URL is: https://us.api.connect.insight.rapid7.com/
Our API Hostname is: us.api.connect.insight.rapid7.com
Our KOMAND_PLUGIN_REGISTRY_URL is: https://pulluser_7iymfaloyvf0j9bewmugpekzy:n5s80jr6sq848jkwvc8vy6yzm72ldg0yjmkkvjn20kgjk4v9dx@us.plugins.connect.insight.rapid7.com
Our KOMAND_PLUGIN_REGISTRY_URL Hostname is: us.plugins.connect.insight.rapid7.com
Our KOMAND_PLUGIN_REGISTRY_URL User is: pulluser_7iymfaloyvf0j9bewmugpekzy
Our KOMAND_PLUGIN_REGISTRY_URL Pass is: n5s80jr6sq848jkwvc8vy6yzm72ldg0yjmkkvjn20kgjk4v9dx
Our HTTP_PROXY setting is:
Our HTTPS_PROXY setting is:
Our NO_PROXY setting is:
Our KOMAND_CA_CERT_MIRROR_ENABLED setting is:
Our KOMAND_CA_CERT_MIRROR_DIR setting is:
Our Docker server version is: 25.0.5
Our Docker environment settings are: Environment=
Using DNS: 1.1.1.1
```

Change permission to /opt/rapid7 folder before extracting the orchestrator tar file

ll command to check if the tar file was copied to the new orchestrator

Extract the orchestrator tar file

Change permission back to default on /opt/rapid7

Running diagnostic to check if all file was copied over or has any errors.

2. Log into a new orchestrator and change directory to /ect

- Command: `cd /ect`
- Command: `Sudo nano resolv.conf` (This allows you to add your private DNS Ips)
- Command: `Sudo cat resolv.conf` (This allow you to check what DNS that you have entered from prevois step)

3. Last step is to start the orchestrator

- Command: `orch-start`

```
Testing ability to resolve KOMAND_PLUGIN_REGISTRY_URL hostname via 1.1.1.1 DNS resolution over UDP
PASS

Testing ability to reach KOMAND_API_URL via TCP
PASS

Testing ability to reach KOMAND_PLUGIN_REGISTRY_URL hostname via TCP
PASS

Testing ability to reach KOMAND_API_URL via HTTPS
PASS

Testing ability to reach KOMAND_PLUGIN_REGISTRY_URL via HTTPS
PASS

Testing ability to reach pypi.python.org via HTTP, used by the Python3 plugin package import feature
PASS

Testing ability to reach pypi.python.org via HTTPS, used by the Python3 plugin package import feature
PASS

Testing ability to login to KOMAND_PLUGIN_REGISTRY_URL over HTTPS (Docker proxy settings will be used if set)
PASS

Testing ability to pull a test image from KOMAND_PLUGIN_REGISTRY_URL over HTTPS (Docker proxy settings will be
used if set)
1.1.2: Pulling from rapid7/base64
f2b6b4884fc8: Pull complete
4fb899b4df21: Pull complete
74eaa8be7221: Pull complete
2d6e98fe4040: Pull complete
414666f7554d: Pull complete
0e48dd127edd: Pull complete
55029d0d78df: Pull complete
cdc35b6d4c7e: Pull complete
1289b9c7971a: Pull complete
1fec7ed2fe13: Pull complete
3b00e31d308b: Pull complete
51a9a6fd064d: Pull complete
aee2c25b7aba: Pull complete
8872df4f59ac: Pull complete
Digest: sha256:803cf538eba4e6adb37402cb63de8153a69e82ff145632a4f187e1120b503e32
Status: Downloaded newer image for us.plugins.connect.insight.rapid7.com/rapid7/base64:1.1.2
us.plugins.connect.insight.rapid7.com/rapid7/base64:1.1.2
PASS

Testing ability to logout from KOMAND_PLUGIN_REGISTRY_URL over HTTPS (Docker proxy settings will be used if s
et)
PASS

rapid7@rapid7-orchestrator:/opt/rapid7$ cd /etc
rapid7@rapid7-orchestrator:/etc$ nanl
Command 'nanl' not found, did you mean:
  command 'nano' from snap nano (7.2+pkg-4057)
  command 'nant' from deb nant (0.92~rc1+dfsg-7)
  command 'nano' from deb nano (6.2-1)
See 'snap info <snapname>' for additional versions.
rapid7@rapid7-orchestrator:/etc$ nano resolv.conf
rapid7@rapid7-orchestrator:/etc$ sudo nano resolv.conf
rapid7@rapid7-orchestrator:/etc$ sudo cat resolv.conf
nameserver 10.33.1.94
nameserver 10.43.1.99
nameserver 10.211.1.99
rapid7@rapid7-orchestrator:/etc$ orch-start
rapid7@rapid7-orchestrator:/etc$ |
```

Use Sudo command to add DNS addresses.
Ex. 10.43.0.95

Use CAT command to view the DNS addresses that have been added.

Start the orchestrator