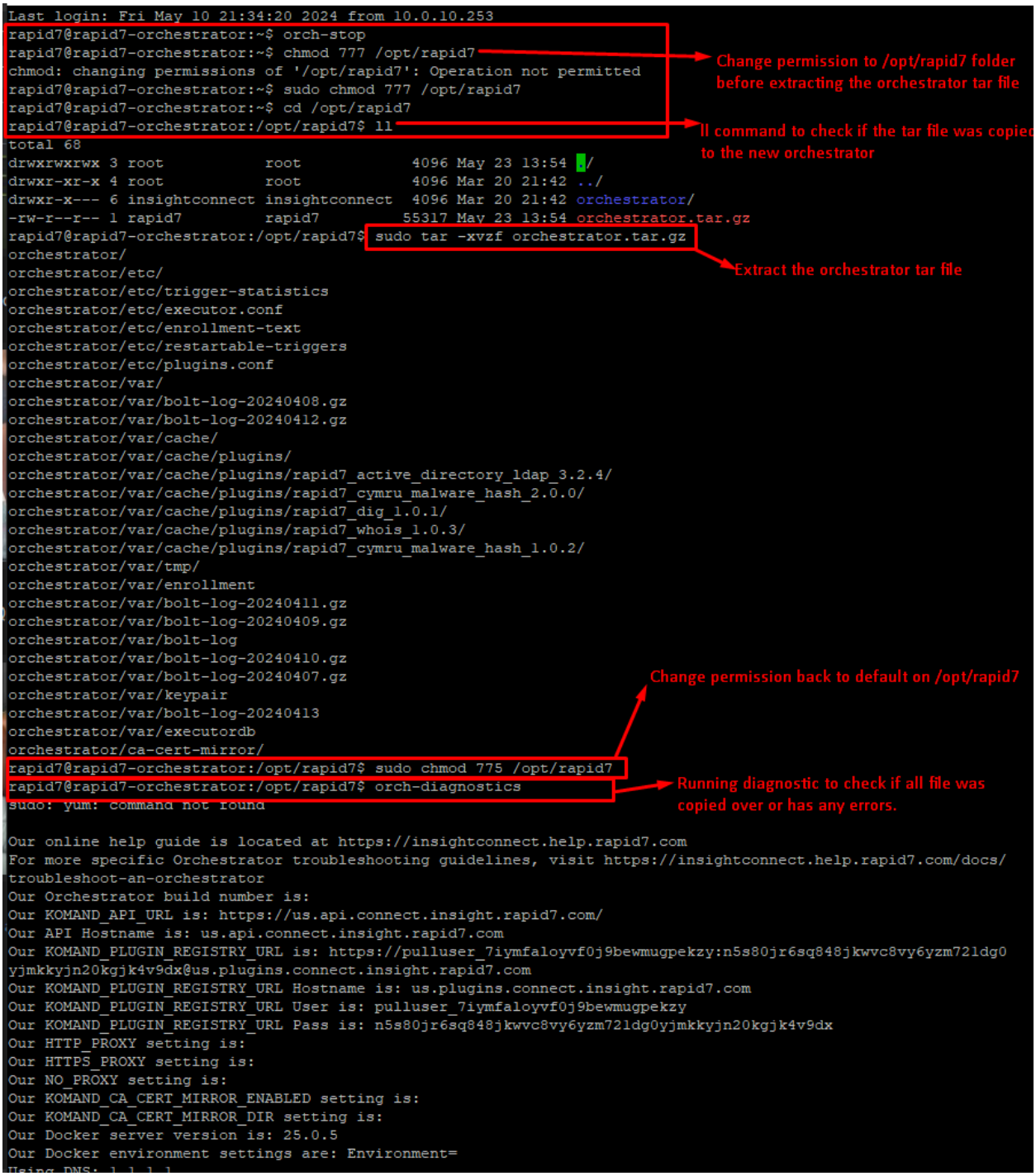
InsightIDR – Orchestrator Migration

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/executordb
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:n5s80jr6sq848jkwvc8vy6yzm72ldg0
yjmkkyjn20kgjk4v9dx@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: n5s80jr6sq848jkwvc8vy6yzm72ldg0yjmkkyjn20kgjk4v9dx
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
```

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**