Deepwatch HF Manual Build - Rocky Linux 8 Minimal

Overview

In the event a customer is unable to utilize our .ova image for standing up a Heavy Forwarder, a customer can still stand up the Heavy Forwarder with our recommended specs and OS.

VM Requirements listed here: Deepwatch HF Deployment

Rocky Download Page: Download - Rocky Linux

Initial Validation

1. Validate OS partitions are per our recommendation found here Deepwatch HF 3.0 Base Configurations | Base Partitions
   a. `df -h` to view partitions and mount points
2. Validate CPU and Memory aligns with our requirements found here ServiceNow
   a. **Note:** If the customer has under-sized the HF when compared to our requirements, explain to them that as the amount of data routing through the HF increases, this could be problematic and may need to be up-sized.
      i. Check vCPU (we recommend 12 for HF/DS/Syslog servers - `lscpu | grep '^CPU(s):'`
      ii. Check memory (we recommend 16GB for HF/DS/Syslog servers) - `free -h`

Configure OS

Manual (Preferred)

It is recommended to run each command individually in order to ensure the desired outcome has been applied correctly, as opposed to leveraging a script. The commands must be run as root, or as a sudo-privileged user prefixing each command with 'sudo'.

Create User Accounts

1. Create the **deepwatch** user[a], remove password expiration requirements[b], and give the user sudo capabilities[c]
    a.
    ```
    sudo adduser deepwatch
    ```
    b.
    ```
    sudo chage -M -1 deepwatch
    ```
    c.
    ```
    sudo echo "deepwatch ALL=(ALL) NOPASSWD:ALL" | sudo tee --append /etc/sudoers.d/deepwatch
    ```
2. Create the **splunk user**
    a.
    ```
    sudo adduser splunk
    ```
3. Add **deepwatch** to the **splunk** group
    a.
    ```
    sudo usermod -a -G splunk deepwatch
    ```
4. Add splunk to the systemd-journal for scripted inputs
    a.
    ```
    sudo usermod -a -G systemd-journal splunk
    ```
5. Set the Message of the Day for the Deepwatch user
    a. **Build date and case # should be updated prior to running**
        i.
        ```
        sudo mkdir /etc/motd.d
        ```
        ii.
        ```
        sudo cat > /etc/motd.d/deepwatch << 'EOF'
        ################################
        #                              #
        # Deepwatch Manual HF3.0 Build #
        #    Build date: MM/DD/YYYY    #
        #    Build case: CSXXXXXXX     #
        #                              #
        ################################
        EOF
        ```

Initial OS Patching

Since the VM will either be a fresh Rocky Linux ISO or an image from the Azure Marketplace, the OS will need patching. Deepwatch is not responsible for the long-term patching of HF's that do not use our image, however this is required when initially setting up the HF.

1.
    ```
    sudo dnf update -y
    ```
    a. This will take roughly 5-10 minutes to complete

Package Installation

Add Repositories

1.
    ```
    sudo dnf config-manager --add-repo https://download.docker.com/linux/centos/docker-ce.repo
    ```

Install Packages

ⓘ **Note:** When running the command in step 2, please verify all packages are installed. Occasionally some packages are skipped with this command. Re-running the install of a specific package to check is fine.

1. Extended Packages for Enterprise Linux (EPEL):

   a.
      ```
      sudo dnf install -y https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
      ```

2. Common Packages for Administration

   a.
      ```
      sudo dnf install -y \
          epel-release \
          bc \
          wget \
          net-tools \
          nmap-ncat \
          socat \
          htop \
          vim \
          docker-ce \
          docker-ce-cli \
          containerd.io \
          dnf-automatic \
          sysstat \
          nano \
          rsync \
          bind-utils \
          yum-utils \
          tcpdump
      ```

ZTNA/Docker Requirements

1. Public certificate for ZTNA connections

   a.
      ```
      sudo curl -s https://public-prod-us.luminatesec.com/ssh-install-scripts/deepwatch/c590e3ab-7dc9-4e90-bcdd-cd70268fd7eb/install_ca_key.sh | sudo bash
      ```

2. Start the Docker service[a] and Enable Docker as a Systemd process for boot-start[b]

   a.
      ```
      sudo systemctl start docker
      ```

   b.
      ```
      sudo systemctl enable docker
      ```

3. Enable and Start the Chrony Service Daemon for time synchronization

   a.
      ```
      sudo systemctl enable chronyd
      ```

   b.
      ```
      sudo systemctl start chronyd
      ```

4. Validate time synchronization

   a.
      ```
      sudo timedatectl
      ```

Splunk Requirements

1. Configure Ulimits

   a.
      ```
      sudo sed -i 's/#DefaultLimitNOFILE=/# deepwatch modified value below\nDefaultLimitNOFILE=64000/' /etc/systemd/system.conf
      ```

   b.
      ```
      sudo sed -i 's/#DefaultLimitNPROC=/# deepwatch modified value below\nDefaultLimitNPROC=16000/' /etc/systemd/system.conf
      ```

   c.
      ```
      sudo sed -i 's/#DefaultTasksMax=80%/# deepwatch modified value below\nDefaultTasksMax=8192/' /etc/systemd/system.conf
      ```

2. Disable Transparent Huge Pages (THP)

   a.
   ```
   sudo echo 'never' > /sys/kernel/mm/transparent_hugepage/enabled
   ```

   b.
   ```
   sudo echo 'never' > /sys/kernel/mm/transparent_hugepage/defrag
   ```

   c.
   ```
   sudo grub2-editenv - set "$(grub2-editenv - list | grep kernelopts) transparent_hugepage=never"
   ```

3. Configure Host Firewall (Firewalld) to allow Splunk Traffic *(May not be required for cloud based images ie. Azure/AWS)*

   a.
   ```
   sudo firewall-cmd --add-port=8000/tcp --add-port=8089/tcp --add-port=9997/tcp --permanent
   ```

   b.
   ```
   sudo firewall-cmd --add-service=syslog --permanent
   ```

   c.
   ```
   sudo firewall-cmd --permanent --zone=trusted --add-interface=lo --permanent
   ```

   d.
   ```
   sudo firewall-cmd --zone=drop --add-rich-rule='rule family=ipv4 source address="127.0.0.1" destination not address="127.0.0.1" drop'
   ```

   e.
   ```
   sudo firewall-cmd --zone=drop --add-rich-rule='rule family=ipv6 source address="::1" destination not address="::1" drop' --permanent
   ```

   f.
   ```
   sudo firewall-cmd --reload
   ```

4. Create Splunk Directory and change ownership

   a.
   ```
   sudo mkdir /opt/splunk
   ```

   b.
   ```
   sudo chown -R splunk:splunk /opt/splunk
   ```

5. Allow Splunk to read from `/var/log`

   a.
   ```
   sudo setfacl -Rdm u:splunk:rx /var/log/
   ```

   b.
   ```
   sudo setfacl -Rm "u:splunk:r-X" /var/log/
   ```

Splunk Installation

> **Note:** It is important for step 3 that we download the latest Deepwatch-supported version of Splunk. Refer here for the latest version - Deepwatch Approved Splunk Versions

1. Set temporary environment variable for `SPLUNK_HOME`

   a.
   ```
   SPLUNK_HOME="/opt/splunk"
   ```

2. Create temporary Splunk admin user file *(will be updated when HF automation is run)*

   a.
   ```
   sudo touch /tmp/user-seed.conf
   ```

   b.
   ```
   sudo cat > /tmp/user-seed.conf << 'EOF'
   [user_info]
   USERNAME = admin
   PASSWORD = dwwillchangeme
   EOF
   ```

3. Download Splunk RPM file[a] and install Splunk[b]

a.
```
wget -O splunk-9.1.4-a414fc70250e.x86_64.rpm "https://download.splunk.com/products/splunk/releases/9.1.4/linux/splunk-9.1.4-a414fc70250e.x86_64.rpm"
```
b.
```
sudo rpm -i /tmp/splunk-9.1.4-a414fc70250e.x86_64.rpm
```

4. Move the file from step 2 to the Splunk directory

   a.
   ```
   sudo mv /tmp/user-seed.conf $SPLUNK_HOME/etc/system/local/user-seed.conf
   ```

5. Disable first time login message

   a.
   ```
   sudo touch $SPLUNK_HOME/etc/.ui_login
   ```

6. Enable SSL settings for Web UI

   a.
   ```
   echo -e "[settings]\nstartwebserver = True\nenableSplunkWebSSL = True\nsslVersions = tls1.2\n" >> $SPLUNK_HOME/etc/system/local/web.conf
   ```

7. Enable Splunk boot-start

   a.
   ```
   $SPLUNK_HOME/bin/splunk enable boot-start -systemd-managed 1 -user splunk --accept-license --answer-yes --no-prompt
   ```

8. Ensure Splunk ownership of `/opt/splunk`

   a.
   ```
   sudo chown -R splunk:splunk $SPLUNK_HOME
   ```

9. Reload Systemd Daemon[a], Enable Splunk[b] and Start Splunk[c]

   a.
   ```
   systemctl daemon-reload
   ```
   b.
   ```
   systemctl enable Splunkd
   ```
   c.
   ```
   systemctl start Splunkd
   ```

Security Best Practices

> **Note:** These configurations are recommended, but since this VM does not leverage Deepwatch’s image, it is up to the customer whether or not we should configure these settings as they will be primarily responsible for OS management.

1. Configure Bash History

   a.
   ```
   echo "# Add date / time information to bash history export HISTTIMEFORMAT=\"%F %T \" " | sudo tee -a /etc/profile.d/deepwatch.sh
   ```

2. Configure Timeout

   a.
   ```
   cat >> /etc/bashrc << 'EOF'

   # Added TMOUT as read-only for CIS compliance.
   TMOUT=300

   readonly TMOUT
   export TMOUT
   EOF
   ```

3. Configure Minimum Password Length

   a.
   ```
   echo "minlen = 14" | tee --append /etc/security/pwquality.conf
   ```

4. Configure DNF Automatic security patching

    a.
    ```
    cat > /etc/dnf/automatic.conf << 'EOF'
    [commands]
    upgrade_type = default
    random_sleep = 0
    network_online_timeout = 600
    download_updates = yes
    apply_updates = yes

    [emitters]
    emit_via = motd
    EOF
    ```

5. Cron job to restart the HF every Tuesday at 10:30 AM UTC if security patches are pending a reboot
    a. `sudo crontab -e` *(press 'i' to edit, like VIM)*
    b. `30 10 * * 2 /usr/bin/needs-restarting -r || /usr/sbin/shutdown -r 2 crontab triggered restart based on needs-restarting result.. Please save any important work you are doing now!`

Scripted

If you have decided to run the commands outlined above in a bash script, **please perform the following steps and validate that each step was completed successfully!!**:

- Verify the latest approved Splunk version and update the "**wget**" command in the code to reflect the appropriate RPM download link
- Save the script file to the /tmp directory on the target HF (i.e., hf_config.sh)
- Ensure it has executable permissions (chmod +x)
- Run as the root user
- Remove the script once finished
- **Validate expected outcomes**
- Reboot host to make sure changes for limits and services start on boot as they should.

hf_config.sh
07 Feb 2024, 06:00 PM

Troubleshooting

If you receive error messages when trying to install docker indicating containerd dependencies are missing after performing a dnf update and installing the listed packages in the code block above, installed containerd as needed by running:

```
dnf install -y https://download.docker.com/linux/centos/7/x86_64/stable/Packages/containerd.io-1.2.6-3.3.el7.x86_64.rpm
```

Then, install docker as normal.

Post Deployment

HF 3.0 Post Deployment Setup