

Indexer Single-Node Step-by-Step Installation

Initial Configuration

Create a working directory

```
1 mkdir /home/drilldowndefender/Documents/wazuh
```

Open the necessary ports

[Wazuh Architecture](#)

```
1 root@SentinelGuardTower-7REX:/home/drilldowndefender/Security/Wazuh# ufw status numbered
2 Status: active
3
4      To Action From
5      --
6 [ 1] 443/tcp ALLOW IN Anywhere
7 [ 2] 514/tcp ALLOW IN Anywhere
8 [ 3] 514/udp ALLOW IN Anywhere
9 [ 4] 1514/tcp ALLOW IN Anywhere
10 [ 5] 1514/udp ALLOW IN Anywhere
11 [ 6] 1515/tcp ALLOW IN Anywhere
12 [ 7] 1516/tcp ALLOW IN Anywhere
13 [ 8] 9200/tcp ALLOW IN Anywhere
14 [ 9] 9300:9400/tcp ALLOW IN Anywhere
15 [10] 55000/tcp ALLOW IN Anywhere
16 [11] 443/tcp (v6) ALLOW IN Anywhere (v6)
17 [12] 514/tcp (v6) ALLOW IN Anywhere (v6)
18 [13] 514/udp (v6) ALLOW IN Anywhere (v6)
19 [14] 1514/tcp (v6) ALLOW IN Anywhere (v6)
20 [15] 1514/udp (v6) ALLOW IN Anywhere (v6)
21 [16] 1515/tcp (v6) ALLOW IN Anywhere (v6)
22 [17] 1516/tcp (v6) ALLOW IN Anywhere (v6)
23 [18] 9200/tcp (v6) ALLOW IN Anywhere (v6)
24 [19] 9300:9400/tcp (v6) ALLOW IN Anywhere (v6)
25 [20] 55000/tcp (v6) ALLOW IN Anywhere (v6)
```

Download the wazuh installation assistant and the configuration file using admin privileges.

```
1 curl -sO https://packages.wazuh.com/4.7/wazuh-certs-tool.sh
2 curl -sO https://packages.wazuh.com/4.7/config.yml
```

Edit `./config.yml` and replace the node names and IP values with the corresponding information for the indexer, server, and dashboard nodes.

```
1 #retrieve IP address for node
2 ifconfig
3
4 #install text editor of choice
5 sudo apt-get install vim
6
7 #edit config.yml file
8 vim config.yml
```

Original `config.yml` file


```

27 - name: SentinelGuardTower-Dashboard
28     ip: "<host-ip>"
29

```

Create wazuh certificates.

```

1 sudo bash ./wazuh-certs-tool.sh -A
2
3     #output
4     root@SentinelGuardTower-7REX:/home/drilldowndefender/Security/Wazuh# bash wazuh-certs-tool.sh -A
5     26/03/2024 13:12:40 INFO: Admin certificates created.
6     26/03/2024 13:12:40 INFO: Wazuh indexer certificates created.
7     26/03/2024 13:12:40 INFO: Wazuh server certificates created.
8     26/03/2024 13:12:40 INFO: Wazuh dashboard certificates created.
9
10    root@SentinelGuardTower-7REX:/home/drilldowndefender/Security/Wazuh# ls
11    config.yml  wazuh-certificates  wazuh-certs-tool.sh
12    root@SentinelGuardTower-7REX:/home/drilldowndefender/Security/Wazuh# ls wazuh-certificates/
13    admin-key.pem  root-ca.key  SentinelGuardTower-Dashboard-key.pem  SentinelGuardTower-Indexer-key.p
14    admin.pem      root-ca.pem  SentinelGuardTower-Dashboard.pem      SentinelGuardTower-Indexer.pem


```

Compress the wazuh-certificates file and delete uncompressed version.

```

1 # Compress wazuh certificates
2 sudo tar -cvf ./wazuh-certificates.tar -C ./wazuh-certificates/ .
3     #the period at the end is part of the script#
4
5     #output
6     root@SentinelGuardTower-7REX:/home/drilldowndefender/Security/Wazuh# tar -cvf ./wazuh-certificates
7     ./
8     ./SentinelGuardTower-Indexer-key.pem
9     ./SentinelGuardTower-Server-key.pem
10    ./SentinelGuardTower-Dashboard.pem
11    ./SentinelGuardTower-Server.pem
12    ./admin-key.pem
13    ./root-ca.key
14    ./root-ca.pem
15    ./SentinelGuardTower-Dashboard-key.pem
16    ./SentinelGuardTower-Indexer.pem
17    ./admin.pem
18
19 #delete uncompressed directory
20 sudo rm -rf ./wazuh-certificates
21
22     #output
23     root@SentinelGuardTower-7REX:/home/drilldowndefender/Security/Wazuh# rm -rf wazuh-certificates
24     root@SentinelGuardTower-7REX:/home/drilldowndefender/Security/Wazuh# ls
25     config.yml  wazuh-certificates.tar  wazuh-certs-tool.sh
26

```

 Notice the certificates generated use the node names we added to the `config.yml` file

Nodes installation

Install the following packages

```

1 apt-get install debconf adduser procps

```

Debconf is a configuration system for Debian packages.

Adding the wazuh repository


Install the following packages

```
1 apt-get install gnupg apt-transport-https
```

GnuPG is a set of programs for public key encryption and digital signatures.

Install GPG Key

```
1 sudo su
2 curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | gpg --no-default-keyring --keyring gnupg-ring:/usr/share/
3
4         #output
5         gpg: keyring '/usr/share/keyrings/wazuh.gpg' created
6         gpg: directory '/root/.gnupg' created
7         gpg: /root/.gnupg/trustdb.gpg: trustdb created
8         gpg: key <REDACTED KEY VALUE>: public key "Wazuh.com (Wazuh Signing Key) <support@wazuh.com>" impo
9         gpg: Total number processed: 1
10        gpg:             imported: 1
```

 After transitioning to root via `sudo su`, I continue to use root privileges. Either use `sudo` for each command or remain in the root account for the remainder of the installation.

Add the repository and update the package information

```
1 #Add repository
2 echo "deb [signed-by=/usr/share/keyrings/wazuh.gpg] https://packages.wazuh.com/4.x/apt/ stable main" | tee -a /et
3
4         #output
5         deb [signed-by=/usr/share/keyrings/wazuh.gpg] https://packages.wazuh.com/4.x/apt/ stable main
6
7 #update packages
8 apt-get update
```

Installing the wazuh Indexer

Install the wazuh indexer package

```
1 apt-get install wazuh-indexer
2
3         #output
4         root@SentinelGuardTower-7REX:/home/drilldowndefender/Security/Wazuh# apt-get install wazuh-indexer
5         Reading package lists... Done
6         Building dependency tree... Done
7         Reading state information... Done
8         The following NEW packages will be installed:
9         wazuh-indexer
10        0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
11        Need to get 678 MB of archives.
12        After this operation, 969 MB of additional disk space will be used.
13        Get:1 https://packages.wazuh.com/4.x/apt stable/main amd64 wazuh-indexer amd64 4.7.3-1 [678 MB]
14        Fetched 678 MB in 38s (17.8 MB/s)
```


```
15 (Reading database ... 183154 files and directories currently installed.)
16 Preparing to unpack .../wazuh-indexer_4.7.3-1_amd64.deb ...
17 Unpacking wazuh-indexer (4.7.3-1) ...
18 Setting up wazuh-indexer (4.7.3-1) ...
19 Created opensearch keystore in /etc/wazuh-indexer/opensearch.keystore
20 Processing triggers for libc-bin (2.35-0ubuntu3.6) ...
21
```

Configure wazuh indexer by editing the `/etc/wazuh-indexer/opensearch.yml` file

i Recommendation: before continuing, open a second terminal window and `cat` the `config.yml` file used to generate the certificates earlier in the installation, it'll come in handy as we proceed.

```
1 vim /etc/wazuh-indexer/opensearch.yml
2     #output
3     network.host: "10.0.0.49"                                <--- edit
4     node.name: "SentinelGuardTower-Indexer"                  <--- edit
5     cluster.initial_master_nodes:
6     - "SentinelGuardTower-Indexer"                           <--- edit
7     #- "node-2"
8     #- "node-3"
9     cluster.name: "wazuh-cluster"
10    #discovery.seed_hosts:
11    #  - "node-1-ip"
12    #  - "node-2-ip"
13    #  - "node-3-ip"
14    node.max_local_storage_nodes: "3"
15    path.data: /var/lib/wazuh-indexer
16    path.logs: /var/log/wazuh-indexer
17
18    plugins.security.ssl.http.pemcert_filepath: /etc/wazuh-indexer/certs/indexer.pem
19    plugins.security.ssl.http.pemkey_filepath: /etc/wazuh-indexer/certs/indexer-key.pem
20    plugins.security.ssl.http.pemtrustedcas_filepath: /etc/wazuh-indexer/certs/root-ca.pem
21    plugins.security.ssl.transport.pemcert_filepath: /etc/wazuh-indexer/certs/indexer.pem
22    plugins.security.ssl.transport.pemkey_filepath: /etc/wazuh-indexer/certs/indexer-key.pem
23    plugins.security.ssl.transport.pemtrustedcas_filepath: /etc/wazuh-indexer/certs/root-ca.pem
24    plugins.security.ssl.http.enabled: true
25    plugins.security.ssl.transport.enforce_hostname_verification: false
26    plugins.security.ssl.transport.resolve_hostname: false
27
28    plugins.security.authcz.admin_dn:
29    - "CN=admin,OU=Wazuh,O=Wazuh,L=California,C=US"
30    plugins.security.check_snapshot_restore_write_privileges: true
31    plugins.security.enable_snapshot_restore_privilege: true
32    plugins.security.nodes_dn:
33    - "CN=node-1,OU=Wazuh,O=Wazuh,L=California,C=US"
34    #- "CN=node-2,OU=Wazuh,O=Wazuh,L=California,C=US"
35    #- "CN=node-3,OU=Wazuh,O=Wazuh,L=California,C=US"
36    plugins.security.restapi.roles_enabled:
37    - "all_access"
38    - "security_rest_api_access"
39
40    plugins.security.system_indices.enabled: true
41    plugins.security.system_indices.indices: [".plugins-ml-model", ".plugins-ml-task", ".opendistro-al
42
43    ### Option to allow Filebeat-oss 7.10.2 to work ###
44    compatibility.override_main_response_version: true
```

```
45
46 # save file
47 :wq
```

 Confirm that the config file here reflects what you have. On previous installations, the config files were corrupted. Saving this copy here to reference during future installation troubleshooting.

Certificate Deployment

For organization and cleanly installing and managing certificates, we are going to set a variable for the indexer node name, make a copy of the certificates, and place them the appropriate place.

```
1 # Set variable for indexer node name set in the config.yml file
2 NODE_NAME=SentinelGuardTower-Indexer
3
4 # Create the directory for the indexer certificates:
5 mkdir /etc/wazuh-indexer/certs
6
7 # Ensure you're in the working directory with the compressed certificate file.
8     #output
9     root@SentinelGuardTower:/home/drilldowndefender/Documents/wazuh# ls
10     config.yml  wazuh-certificates.tar  wazuh-certs-tool.sh
11
12 # decompress, make a copy, and move certificates, using the variables set:
13 tar -xf ./wazuh-certificates.tar -C /etc/wazuh-indexer/certs/ ./${NODE_NAME}.pem ./${NODE_NAME}-key.pem ./admin.pem
14
15     #output
16     root@SentinelGuardTower-7REX:/home/drilldowndefender/Security/Wazuh# tar -xf ./wazuh-certificates.
17     root@SentinelGuardTower-7REX:/home/drilldowndefender/Security/Wazuh# ls /etc/wazuh-indexer/certs/
18     admin-key.pem  admin.pem  root-ca.pem  SentinelGuardTower-Indexer-key.pem  SentinelGuardTower-Inde
19
20
21 mv -n /etc/wazuh-indexer/certs/${NODE_NAME}.pem /etc/wazuh-indexer/certs/indexer.pem
22
23     #output
24     root@SentinelGuardTower-7REX:/home/drilldowndefender/Security/Wazuh# mv -n /etc/wazuh-indexer/cert
25     root@SentinelGuardTower-7REX:/home/drilldowndefender/Security/Wazuh# ls /etc/wazuh-indexer/certs/
26     admin-key.pem  admin.pem  indexer.pem  root-ca.pem  SentinelGuardTower-Indexer-key.pem
27
28
29 mv -n /etc/wazuh-indexer/certs/${NODE_NAME}-key.pem /etc/wazuh-indexer/certs/indexer-key.pem
30
31     #output
32     root@SentinelGuardTower-7REX:/home/drilldowndefender/Security/Wazuh# mv -n /etc/wazuh-indexer/cert
33     root@SentinelGuardTower-7REX:/home/drilldowndefender/Security/Wazuh# ls /etc/wazuh-indexer/certs/
34     admin-key.pem  admin.pem  indexer-key.pem  indexer.pem  root-ca.pem
35
36 # Make permissions and ownership changes
37     #output - before changes
38     drwxr-xr-x  2 root      root      4096 Mar 26 13:30 certs
39     -rwxr--r--  1 root      root      1704 Mar 26 13:15 admin-key.pem
40     -rwxr--r--  1 root      root      1119 Mar 26 13:15 admin.pem
41     -rwxr--r--  1 root      root      1704 Mar 26 13:15 indexer-key.pem
42     -rwxr--r--  1 root      root      1302 Mar 26 13:15 indexer.pem
43     -rwxr--r--  1 root      root      1204 Mar 26 13:15 root-ca.pem
44
45 chmod 500 /etc/wazuh-indexer/certs
```

```

46 chmod 400 /etc/wazuh-indexer/certs/*
47 chown -R wazuh-indexer:wazuh-indexer /etc/wazuh-indexer/certs
48
49 #output
50 dr-x----- 2 wazuh-indexer wazuh-indexer 4096 Mar 26 13:30 certs
51 -r----- 1 wazuh-indexer wazuh-indexer 1704 Mar 26 13:15 admin-key.pem
52 -r----- 1 wazuh-indexer wazuh-indexer 1119 Mar 26 13:15 admin.pem
53 -r----- 1 wazuh-indexer wazuh-indexer 1704 Mar 26 13:15 indexer-key.pem
54 -r----- 1 wazuh-indexer wazuh-indexer 1302 Mar 26 13:15 indexer.pem
55 -r----- 1 wazuh-indexer wazuh-indexer 1204 Mar 26 13:15 root-ca.pem
56

```

Fire up the service!

```

1 systemctl daemon-reload
2 systemctl enable wazuh-indexer
3 #output
4 <pre>Created symlink /etc/systemd/system/multi-user.target.wants/wazuh-indexer.service → /lib/syst
5
6 systemctl start wazuh-indexer
7 systemctl status wazuh-indexer
8 #output
9 • wazuh-indexer.service - Wazuh-indexer
10   Loaded: loaded (/lib/systemd/system/wazuh-indexer.service; enabled; vendor preset: enabled)
11   Active: active (running) since Tue 2024-03-26 13:36:07 EDT; 5s ago
12     Docs: https://documentation.wazuh.com
13   Main PID: 6776 (java)
14     Tasks: 81 (limit: 9331)
15    Memory: 1.3G
16      CPU: 38.369s
17   CGroup: /system.slice/wazuh-indexer.service
18           └─6776 /usr/share/wazuh-indexer/jdk/bin/java -Xshare:auto -Dopensearch.networkaddress.
19
20 Mar 26 13:35:27 SentinelGuardTower-7REX systemd[1]: Starting Wazuh-indexer...
21 Mar 26 13:35:28 SentinelGuardTower-7REX systemd-entrypoint[6776]: WARNING: A terminally deprecated
22 Mar 26 13:35:28 SentinelGuardTower-7REX systemd-entrypoint[6776]: WARNING: System::setSecurityMana
23 Mar 26 13:35:28 SentinelGuardTower-7REX systemd-entrypoint[6776]: WARNING: Please consider reporti
24 Mar 26 13:35:28 SentinelGuardTower-7REX systemd-entrypoint[6776]: WARNING: System::setSecurityMana
25 Mar 26 13:35:29 SentinelGuardTower-7REX systemd-entrypoint[6776]: WARNING: A terminally deprecated
26 Mar 26 13:35:29 SentinelGuardTower-7REX systemd-entrypoint[6776]: WARNING: System::setSecurityMana
27 Mar 26 13:35:29 SentinelGuardTower-7REX systemd-entrypoint[6776]: WARNING: Please consider reporti
28 Mar 26 13:35:29 SentinelGuardTower-7REX systemd-entrypoint[6776]: WARNING: System::setSecurityMana
29 Mar 26 13:36:07 SentinelGuardTower-7REX systemd[1]: Started Wazuh-indexer.

```

⚠ you may need to `systemctl restart wazuh-indexer` if an error occurs during the initialization step up next

Initiate the cluster

```


1 /usr/share/wazuh-indexer/bin/indexer-security-init.sh
2
3 # output:
4 *****
5 ** This tool will be deprecated in the next major release of OpenSearch **
6 ** https://github.com/opensearch-project/security/issues/1755 **
7 *****
8 Security Admin v7

```

```

9      Will connect to 10.0.0.220:9200 ... done
10     Connected as "CN=admin,OU=Wazuh,O=Wazuh,L=California,C=US"
11     OpenSearch Version: 2.8.0
12     Contacting opensearch cluster 'opensearch' and wait for YELLOW clusterstate ...
13     Clustername: wazuh-cluster
14     Clusterstate: GREEN
15     Number of nodes: 1
16     Number of data nodes: 1
17     .opendistro_security index does not exists, attempt to create it ... done (0-all replicas)
18     Populate config from /etc/wazuh-indexer/opensearch-security/
19     Will update '/config' with /etc/wazuh-indexer/opensearch-security/config.yml
20         SUCC: Configuration for 'config' created or updated
21     Will update '/roles' with /etc/wazuh-indexer/opensearch-security/roles.yml
22         SUCC: Configuration for 'roles' created or updated
23     Will update '/rolesmapping' with /etc/wazuh-indexer/opensearch-security/roles_mapping.yml
24         SUCC: Configuration for 'rolesmapping' created or updated
25     Will update '/internalusers' with /etc/wazuh-indexer/opensearch-security/internal_users.yml
26         SUCC: Configuration for 'internalusers' created or updated
27     Will update '/actiongroups' with /etc/wazuh-indexer/opensearch-security/action_groups.yml
28         SUCC: Configuration for 'actiongroups' created or updated
29     Will update '/tenants' with /etc/wazuh-indexer/opensearch-security/tenants.yml
30         SUCC: Configuration for 'tenants' created or updated
31     Will update '/nodesdn' with /etc/wazuh-indexer/opensearch-security/nodes_dn.yml
32         SUCC: Configuration for 'nodesdn' created or updated
33     Will update '/whitelist' with /etc/wazuh-indexer/opensearch-security/whitelist.yml
34         SUCC: Configuration for 'whitelist' created or updated
35     Will update '/audit' with /etc/wazuh-indexer/opensearch-security/audit.yml
36         SUCC: Configuration for 'audit' created or updated
37     Will update '/allowlist' with /etc/wazuh-indexer/opensearch-security/allowlist.yml
38         SUCC: Configuration for 'allowlist' created or updated
39     SUCC: Expected 10 config types for node {"updated_config_types":["allowlist","tenants","rolesmappi
40     Done with success

```

 If this step fails, check that the ports are open, the `NODE_NAME` variable was set prior to moving the certificates, the certificates are in the correct place, and the configuration files are properly set

Test the connection

```

1  curl -k -u admin:admin https://10.0.0.220:9200
2  # switches
3  # -k, --insecure | (TLS SFTP SCP) By default, every secure connection curl makes is verified to be secure befo
4  # -u, --user <user:password> | Specify the user name and password to use for server authentication.
5      # output:
6      {
7          "name" : "SentinelGuardTower-Indexer",
8          "cluster_name" : "wazuh-cluster",
9          "cluster_uuid" : "xknyfwPhQkq0ZAHP1Ab1DA",
10         "version" : {
11             "number" : "7.10.2",
12             "build_type" : "rpm",
13             "build_hash" : "db90a415ff2fd428b4f7b3f800a51dc229287cb4",
14             "build_date" : "2023-06-03T06:24:25.112415503Z",
15             "build_snapshot" : false,
16             "lucene_version" : "9.6.0",
17             "minimum_wire_compatibility_version" : "7.10.0",
18             "minimum_index_compatibility_version" : "7.0.0"
19         },
20         "tagline" : "The OpenSearch Project: https://opensearch.org/"

```