Kurulum Rehberi

Wazuh, endpointler ve cloud ortamları için hem XDR hem de SIEM koruması sağlayan bir güvenlik platformudur. Bu çözüm agentlardan ve üç bileşenden oluşur: Wazuh server, indexer ve dashboard. Wazuh ücretsiz ve açık kaynaktır. Bileşenleri "GNU General Public License, version 2", ve "Apache License, Version 2.0 (ALv2)" ye uygundur. Bu bölümde Wazuh'u altyapınıza nasıl kuracağınızı öğreneceksiniz. Ayrıca Wazuh, agentlar dışında herhangi bir kurulum gerektirmeden SaaS olarak da hizmet vermektedir. Wazuh Cloud'u kullanarak herhangi bir kurulum yapmadan agentlarınızı ve log kaynaklarınızı bağlayabilirsiniz.

Wazuh Indexer

Wazuh Indexer, yüksek ölçeklenebilir, full-text search ve analiz motorudur. Bu bileşen, Wazuh server tarafından oluşturulan uyarıları indeksler ve saklar. Neredeyse gerçek zamanlı veri arama ve analiz yetenekleri sağlar.

Wazuh Kurulum Asistanı

Kurulum asistanı yöntemini kullanarak Wazuh Indexer'ı single-node veya multi-node şeklinde kurabilirsiniz. Bu yöntem manuel yapılacak bazı işlemlerin .sh dosyasına çevrilerek kolaylaştırılmasını sağlamaktadır.

Bu kurulum üç aşamaya ayrılmıştır:

1. İlk konfigürasyon
2. Wazuh indexer nodelarının kurulumu
3. Cluster başlatma

> Tüm komutları çalıştırırken root kullanıcı yetkisine ihtiyacınız olacak. "sudo su" ile root üzerinden kurulumu gerçekleştirmeniz önerilmektedir.

1.Initial configuration

Deployment konfigürasyonunuzu hazırlayın, Wazuh bileşenleri arasındaki iletişimi şifrelemek için SSL sertifikalarını oluşturun ve kurulum sırasında rastgele parolalar oluşturun. Tüm bunlar için aşağıdaki adımları izleyebilirsiniz.

1. Wazuh kurulum asistanı ve konfigürasyon dosyasını indirin.

```
curl -sO https://packages.wazuh.com/4.9/wazuh-install.sh
curl -sO https://packages.wazuh.com/4.9/config.yml
```

2. `./config.yml` dosyasını düzenleyin. Node isimleri ve IP değerlerini kurulumunuza göre düzenleyin. Eğer tek node kuracaksanız yorum satırlarınızı kaldırmanıza gerek yok. Ancak birden fazla indexer veya manager sunucusu kuracaksanız yorum satırı alanlarına name ve IP değerlerini girmeniz gerekiyor.

```
nodes:
  # Wazuh indexer nodes
  indexer:
    - name: node-1
      ip: "<indexer-node-ip>"
    #- name: node-2
```

```
    #  ip: "<indexer-node-ip>"
    #- name: node-3
    #  ip: "<indexer-node-ip>"

  # Wazuh server nodes
  # If there is more than one Wazuh server
  # node, each one must have a node_type
  server:
    - name: wazuh-1
      ip: "<wazuh-manager-ip>"
    #  node_type: master
    #- name: wazuh-2
    #  ip: "<wazuh-manager-ip>"
    #  node_type: worker
    #- name: wazuh-3
    #  ip: "<wazuh-manager-ip>"
    #  node_type: worker

  # Wazuh dashboard nodes
  dashboard:
    - name: dashboard
      ip: "<dashboard-node-ip>"
```

3. Kurulum için gerekli Wazuh cluster key, sertifikalar ve parolaları oluşturmak için Wazuh kurulum asistanını `--generate-config-files` parametresi ile birlikte çalıştırın. Bu komut size `./wazuh-install-files.tar` dosyalarını oluşturacak. Diğer sunucuların kurulumunda da bu dosyalara ihtiyacınız olacak. Kurulum boyunca bu dosyaları saklayın ve diğer sunuculara aktarın. Tüm Wazuh kurulumu tamamlandığında bu .tar dosyasını silmeniz faydalı olacaktır.

```
bash wazuh-install.sh --generate-config-files
```

4. `wazuh-install-files.tar` dosyasını diğer wazuh server, wazuh indexer ve wazuh dashboard nodelarına kopyalayın. Bu aşamada `scp` veya farklı yöntemler kullanabilirsiniz.

2. Wazuh Indexer Nodelarının Kurulumu

Daha önce indirdiğiniz `wazuh-install.sh` dosyasını `--wazuh-indexer` parametresi ve node adı ile çalıştırın. Node adı `config.yml` dosyasındaki ile aynı olmalıdır.

```
bash wazuh-install.sh --wazuh-indexer node-1
```

Eğer multi-node bir kurulum planladıysanız, yani birden fazla indexer node'u planlıyorsanız diğer nodelara da aynı işlemi uygulayın.

3. Cluster Başlatma

Kurulumun son aşamasında sertifika bilgilerini yüklemek ve clusterı başlatmak için herhangi bir indexer node'unda kurulum asistanı dosyanızı --start-cluster parametresi ile başlatın.

```
bash wazuh-install.sh --start-cluster
```

> Bu işlemi yalnızca bir indexer node'unda yapmanız yeterlidir. Birden fazla node üzerinde veya tüm node'larda bu işlemi yapmanıza gerek yok.

Kurulumun test edilmesi

Aşağıdaki komutu çalıştırın ve admin parolasını alın.

```
tar -axf wazuh-install-files.tar wazuh-install-files/wazuh-passwords.txt -O | grep -P "\'admin\'" -A 1
```

Ardından kurulumun sorunsuz tamamlandığını teyit etmek için aşağıdaki komutu çalıştırın. Önceki komut çıktısından elde ettiğiniz parolayı aşağıdaki <ADMIN_PASSWORD> alanıyla değiştirin. Aynı zamanda wazuh indexer IP adresini de <WAZUH_INDEXER_IP> alanıyla değiştirin.

```
curl -k -u admin:<ADMIN_PASSWORD> https://<WAZUH_INDEXER_IP>:9200
```

Örnek çıktı aşağıdaki gibiyse kurulumun gerçekleştiğini kabul edebiliriz.

```
{
  "name" : "node-1",
  "cluster_name" : "wazuh-cluster",
  "cluster_uuid" : "095jEW-oRJSFKLz5wmo5PA",
  "version" : {
    "number" : "7.10.2",
    "build_type" : "rpm",
    "build_hash" : "db90a415ff2fd428b4f7b3f800a51dc229287cb4",
    "build_date" : "2023-06-03T06:24:25.112415503Z",
    "build_snapshot" : false,
```

```
    "lucene_version" : "9.6.0",
    "minimum_wire_compatibility_version" : "7.10.0",
    "minimum_index_compatibility_version" : "7.0.0"
  },
  "tagline" : "The OpenSearch Project: https://opensearch.org/"
}
```

Parola ve IP değerini tekrar değiştirerek aşağıdaki komutla nodelarınızı test edebilirsiniz.

```
curl -k -u admin:<ADMIN_PASSWORD> https://<WAZUH_INDEXER_IP>:9200/_cat/nodes?v
```

Adım Adım Kurulum

Wazuh dizinleyicisini adım adım talimatları izleyerek tek düğümlü veya çok düğümlü küme olarak kurun ve yapılandırın. Wazuh dizinleyicisi son derece ölçeklenebilir bir tam metin arama motorudur ve gelişmiş güvenlik, uyarı, dizin yönetimi, derin performans analizi ve diğer birçok özelliği sunar.

Kurulum süreci üç aşamaya ayrılıyor.

1. Sertifika oluşturma
2. Düğüm kurulumu
3. Küme başlatma

> **Not:** Aşağıda açıklanan tüm komutları çalıştırabilmek için root kullanıcı ayrıcalıklarına sahip olmanız gerekir.
> 1. Sertifika Oluşturma

SSL Sertifikalarının Oluşturulması

1. `wazuh-certs-tool.sh`Komut dosyasını ve yapılandırma dosyasını indirin `config.yml`. Bu, Wazuh merkezi bileşenleri arasındaki iletişimleri şifreleyen sertifikaları oluşturur.

   ```
   curl -sO https://packages.wazuh.com/4.9/wazuh-certs-tool.sh
   curl -sO https://packages.wazuh.com/4.9/config.yml
   ```

2. Düğüm adlarını ve IP değerlerini düzenleyin `./config.yml`ve karşılık gelen adlar ve IP adresleriyle değiştirin. Bunu tüm Wazuh sunucusu, Wazuh dizinleyicisi ve Wazuh panosu düğümleri için yapmanız gerekir. Gerektiği kadar düğüm alanı ekleyin.

   ```
   nodes:
     # Wazuh indexer nodes
     indexer:
       - name: node-1
         ip: "<indexer-node-ip>"
       #- name: node-2
       #  ip: "<indexer-node-ip>"
       #- name: node-3
       #  ip: "<indexer-node-ip>"
   ```

```
# Wazuh server nodes
# If there is more than one Wazuh server
# node, each one must have a node_type
server:
  - name: wazuh-1
    ip: "<wazuh-manager-ip>"
  #  node_type: master
  #- name: wazuh-2
  #  ip: "<wazuh-manager-ip>"
  #  node_type: worker
  #- name: wazuh-3
  #  ip: "<wazuh-manager-ip>"
  #  node_type: worker

# Wazuh dashboard nodes
dashboard:
  - name: dashboard
    ip: "<dashboard-node-ip>"
```

3. Sertifikaları oluşturmak için çalıştırın `./wazuh-certs-tool.sh`. Çok düğümlü bir küme için, bu sertifikaların daha sonra kümenizdeki tüm Wazuh örneklerine dağıtılması gerekir.

```
bash ./wazuh-certs-tool.sh -A
```

4. Gerekli tüm dosyaları sıkıştırın.

```
tar -cvf ./wazuh-certificates.tar -C ./wazuh-certificates/ .
rm -rf ./wazuh-certificates
```

5. `wazuh-certificates.tar`Dosyayı Wazuh dizinleyicisi, Wazuh sunucusu ve Wazuh panosu düğümleri dahil tüm düğümlere kopyalayın . Bu `scp`, yardımcı programı kullanarak yapılabilir.

2. Düğümlerin Kurulumu

Paket Bağımlılıklarını Yükleme

1. Eksikse aşağıdaki paketleri yükleyin:

Yum:

```
yum install coreutils
```

APT:

```
apt-get install debconf adduser procps
```

Wazuh Deposunu Ekleme

Yum:

1. GPG anahtarını içe aktarın.

```
rpm --import https://packages.wazuh.com/key/GPG-KEY-WAZUH
```

2. Depoyu ekleyin.

```
echo -e '[wazuh]\ngpgcheck=1\ngpgkey=https://packages.wazuh.com/key/GPG-KEY-WAZUH\nenabled=1\nname=EL-$releasever - Wazuh\nbaseurl=https://packages.wazuh.com/4.x/yum/\nprotect=1' | tee /etc/yum.repos.d/wazuh.repo
```

APT:

1. Eğer eksikse aşağıdaki paketleri kurun.

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

2. GPG anahtarını yükleyin.

```
curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | gpg --no-default-keyring --keyring gnupg-ring:/usr/share/keyrings/wazuh.gpg --import && chmod 644 /usr/share/keyrings/wazuh.gpg
```

3. Depoyu ekleyin.

```
echo "deb [signed-by=/usr/share/keyrings/wazuh.gpg] https://packages.wazuh.com/4.x/apt/ stable main" | tee -a /etc/apt/sources.list.d/wazuh.list
```

4. Paket bilgilerini güncelleyin.

```
apt-get update
```

Wazuh dizinleyicisini yükleme

1. Wazuh indexer paketini yükleyin.

   Yum:

   ```
   # yum -y install wazuh-indexer
   ```

   APT:

   ```
   apt-get -y install wazuh-indexer
   ```

Wazuh dizinleyicisini yapılandırma

1. Edit the `/etc/wazuh-indexer/opensearch.yml` configuration file and replace the following values:

   a. `network.host`: Sets the address of this node for both HTTP and transport traffic. The node will bind to this address and use it as its publish address. Accepts an IP address or a hostname.

Use the same node address set in `config.yml` to create the SSL certificates.

   b. `node.name`: Name of the Wazuh indexer node as defined in the `config.yml` file. For example, `node-1`.

   c. `cluster.initial_master_nodes`: List of the names of the master-eligible nodes. These names are defined in the `config.yml` file. Uncomment the `node-2` and `node-3` lines, change the names, or add more lines, according to your `config.yml` definitions.

```
cluster.initial_master_nodes:
- "node-1"
- "node-2"
- "node-3"
```

d. `discovery.seed_hosts:`Ana uygun düğümlerin adreslerinin listesi. Her bir öğe bir IP adresi veya bir ana bilgisayar adı olabilir. Wazuh dizinleyicisini tek bir düğüm olarak yapılandırıyorsanız bu ayarı yorumlanmış olarak bırakabilirsiniz. Çoklu düğüm yapılandırmaları için bu ayarı yorumlanmamış olarak bırakın ve her ana uygun düğümün IP adreslerini ayarlayın.

```
discovery.seed_hosts:
- "10.0.0.1"
- "10.0.0.2"
- "10.0.0.3"
```

e. `plugins.security.nodes_dn`: List of the Distinguished Names of the certificates of all the Wazuh indexer cluster nodes. Uncomment the lines for `node-2` and `node-3` and change the common names (CN) and values according to your settings and your `config.yml` definitions.

```
plugins.security.nodes_dn:
- "CN=node-1, OU=Wazuh, L=California, C=US"
- "CN=node-2, OU=Wazuh, L=California, C=US"
- "CN=node-3, OU=Wazuh, L=California, C=US"
```

Sertifikaların dağıtımı

> **Not:** `wazuh-certificates.tar`İlk yapılandırma adımında oluşturulan dosyanın bir kopyasının çalışma dizininize yerleştirildiğinden emin olun.

1. Run the following commands replacing `<indexer-node-name>` with the name of the Wazuh indexer node you are configuring as defined in `config.yml`. For example, `node-1`. This deploys the SSL certificates to encrypt communications between the Wazuh central components.

   ```
   NODE_NAME=<indexer-node-name>
   ```

```
mkdir /etc/wazuh-indexer/certs
# tar -xf ./wazuh-certificates.tar -C /etc/wazuh-indexer/certs/ ./$NODE_NAME.pem ./$NODE_NAME-key.pem ./admin
```

```
# mv -n /etc/wazuh-indexer/certs/$NODE_NAME.pem /etc/wazuh-indexer/certs/indexer.pem
# mv -n /etc/wazuh-indexer/certs/$NODE_NAME-key.pem /etc/wazuh-indexer/certs/indexer-key.pem
# chmod 500 /etc/wazuh-indexer/certs
# chmod 400 /etc/wazuh-indexer/certs/*
# chown -R wazuh-indexer:wazuh-indexer /etc/wazuh-indexer/certs
```

2. **Önerilen eylem** : Bu düğüme başka Wazuh bileşeni yüklenmeyecekse, güvenliği artırmak için `wazuh-certificates.tar` dosyayı çalıştırarak kaldırın. `rm -f ./wazuh-certificates.tar`

Hizmet başlatılıyor

1. Wazuh dizinleyici hizmetini etkinleştirin ve başlatın.

Systemd:

```
systemctl daemon-reload
systemctl enable wazuh-indexer
systemctl start wazuh-indexer
```

SysV Init:

Kullanılan işletim sistemine göre bir seçenek seçin.

1. RPM tabanlı işletim sistemi:

```
chkconfig --add wazuh-indexer
service wazuh-indexer start
```

2. Debian tabanlı işletim sistemi:

```
update-rc.d wazuh-indexer defaults 95 10
service wazuh-indexer start
```

Kurulum sürecinin bu aşamasını kümenizdeki her Wazuh dizinleyici düğümü için tekrarlayın. Ardından bir sonraki aşamada tek düğümlü veya çok düğümlü kümenizi başlatmaya devam edin.

3. Küme başlatma

1. Yeni sertifika bilgilerini yüklemek ve tek düğümlü veya çok düğümlü kümeyi başlatmak için *herhangi bir* Wazuh dizinleyici düğümünde Wazuh dizinleyici `indexer-security-init.sh` betiğini çalıştırın.

   ```
   # /usr/share/wazuh-indexer/bin/indexer-security-init.sh
   ```

   Not: *Kümeyi yalnızca bir kez* başlatmanız yeterlidir , bu komutu her düğümde çalıştırmanıza gerek yoktur.

Küme Kurulumunu Test Etme

1. `<WAZUH_INDEXER_IP_ADDRESS>`Kurulumun başarılı olduğunu doğrulamak için aşağıdaki komutları değiştirin ve çalıştırın.

   ```
   curl -k -u admin:admin https://<WAZUH_INDEXER_IP_ADRESS>:9200
   ```

   Output

   ```
   {
     "name" : "node-1",
     "cluster_name" : "wazuh-cluster",
     "cluster_uuid" : "095jEW-oRJSFKLz5wmo5PA",
     "version" : {
       "number" : "7.10.2",
       "build_type" : "rpm",
       "build_hash" : "db90a415ff2fd428b4f7b3f800a51dc229287cb4",
       "build_date" : "2023-06-03T06:24:25.112415503Z",
       "build_snapshot" : false,
       "lucene_version" : "9.6.0",
       "minimum_wire_compatibility_version" : "7.10.0",
       "minimum_index_compatibility_version" : "7.0.0"
     },
     "tagline" : "The OpenSearch Project: https://opensearch.org/"
   }
   ```

2. `<WAZUH_INDEXER_IP_ADDRESS>`Tek düğümlü veya çok düğümlü kümenin doğru çalışıp çalışmadığını kontrol etmek için aşağıdaki komutu değiştirin ve çalıştırın.

   ```
   curl -k -u admin:admin https://<WAZUH_INDEXER_IP_ADDRESS>:9200/_cat/nodes?v
   ```

Sonraki adımlar

Wazuh dizinleyicisi artık tek düğümlü veya çok düğümlü kümenize başarıyla yüklendi ve Wazuh sunucusunu yüklemeye devam edebilirsiniz. Bu işlemi gerçekleştirmek için Wazuh sunucusunu adım adım yükleme bölümüne bakın.

Wazuh dizinleyicisini kaldırmak istiyorsanız Wazuh dizinleyicisini kaldırma bölümüne bakın .

Wazuh Indexer Sistem Gereksinimleri

Wazuh indexer için desteklenen ve önerilen sistem gereksinimleri ve işletim sistemleri aşağıda yer almaktadır. Kurulum sırasında root kullanıcı yetkisine ihtiyacınız olacak. Multi-node veya single-node olarak kurulum gerçekleştirebilirsiniz.

Önerilen işletim sistemleri

Wazuh 64-bit Linux işletim sistemlerine kurulabilir. Aşağıdaki işletim sistemlerini destekler:

Amazon Linux 2, Amazon Linux 2023	CentOS 7, 8
Red Hat Enterprise Linux 7, 8, 9	Ubuntu 16.04, 18.04, 20.04, 22.04, 24.04

Donanım Gereksinimleri

	Minimum		Önerilen	
Component	**RAM (GB)**	**CPU (cores)**	**RAM (GB)**	**CPU (cores)**
Wazuh Indexer	4	2	16	8

Veri miktarı, saniye başına oluşturulan uyarılara (APS) bağlıdır. Bu tablo, izlenen uç noktaların türüne bağlı olarak, bir Wazuh indeksleyici sunucusunda 90 günlük uyarıları depolamak için aracı başına ihtiyaç duyulan tahmini disk alanının ayrıntılarını verir.

Monitör edilen endpointler	**APS**	**Wazuh Indexer depolama (GB/90 gün)**
Sunucular	0.25	3.7
Workstationlar	0.1	1.5
Ağ cihazları	0.5	7.4

Örneğin, 80 workstation, 10 sunucu ve 10 ağ cihazının bulunduğu bir ortam için Wazuh indeksleyici sunucusunda 90 günlük uyarılar için gereken depolama alanı 230 GB'dir.

Wazuh Server

Wazuh Server, agentlardan alınan verileri analiz ederek tehditler veya anomalileri tespit ederek uyarılar oluşturur. Ayrıca agentların konfigürasyonlarını uzaktan yönetmek ve durumlarını takip etmek için kullanılır. Wazuh serverlarını single-node veya multi-node kurabilirsiniz. Multi-node mimariler yüksek kullabılabilirlik ve gelişmiş performans sağlar. Load balancer ile birlikte kullanıldığında kapasitesinini daha verimli şekilde kullanılması sağlanabilir.

Wazuh Kurulum Asistanı

Asistan aracılığıla single-node veya multi-node olarak kurulum yapabilirsiniz. Bu bileşen wazuh manager ve filebeat içerir.

1. Wazuh asistan kurulumunu indirin.

```
curl -sO https://packages.wazuh.com/4.9/wazuh-install.sh
```

2. Wazuh asistan kurulum dosyasını `--wazuh-server` parametresi ve server node adı ile birlikte kurun. Indexer sunucusunda hazırladığınız `config.yml` dosyasında yer alan isim ile parametre olarak verilen isim aynı olmalıdır.

> Indexer'da oluşturduğunuz wazuh-install-files.tar dosyasının bir kopyasının .sh dosyasını çalıştırdığınız dizinde olduğundan emin olun.

```
bash wazuh-install.sh --wazuh-server wazuh-1
```

Wazuh server kurulumu başarıyla tamamlandı. Eğer birden fazla server node'u kuracaksanız bu işlemi diğer node'lara da uygulamalısınız.

Servislerin doğru çalıştığından emin olmak için aşağıdaki iki komutu kullanabilirsiniz.

```
systemctl status wazuh-manager
systemctl status filebeat
```

Adım Adım Kurulum

Adım adım talimatları izleyerek Wazuh sunucusunu tek düğümlü veya çok düğümlü küme olarak kurun ve yapılandırın. Wazuh sunucusu, Wazuh yöneticisi ve Filebeat'i içeren merkezi bir bileşendir. Wazuh yöneticisi, dağıtılan Wazuh aracılarından veri toplar ve analiz eder. Tehditler veya anormallikler algılandığında uyarıları tetikler. Filebeat, uyarıları ve arşivlenmiş olayları güvenli bir şekilde Wazuh dizinleyicisine iletir.

Kurulum süreci iki aşamaya ayrılıyor.

1. Wazuh sunucu düğümü kurulumu
2. Çoklu düğüm dağıtımı için küme yapılandırması

> **Not:** Aşağıda açıklanan tüm komutları çalıştırabilmek için root kullanıcı ayrıcalıklarına sahip olmanız gerekir.

1. Wazuh Sunucu Düğümü Kurulumu

Wazuh Deposunu Ekleme

> **Not:** Wazuh sunucusunu Wazuh indeksleyicisinin bulunduğu ana bilgisayara kuruyorsanız, Wazuh deposunu daha önce eklemiş olabileceğiniz için bu adımları atlayabilirsiniz.

Yum:

1. GPG anahtarını içe aktarın.

```
rpm --import https://packages.wazuh.com/key/GPG-KEY-WAZUH
```

2. Depoyu ekleyin.

```
echo -e '[wazuh]\ngpgcheck=1\ngpgkey=https://packages.wazuh.com/key/GPG-KEY-
WAZUH\nenabled=1\nname=EL-$releasever -
```

```
Wazuh\nbaseurl=https://packages.wazuh.com/4.x/yum/\nprotect=1' | tee /etc/yum.repos.d/wazuh.repo
```

APT:

1. Eğer eksikse aşağıdaki paketleri kurun.

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

2. GPG anahtarını yükleyin.

```
curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | gpg --no-default-keyring --keyring gnupg-ring:/usr/share/keyrings/wazuh.gpg --import && chmod 644 /usr/share/keyrings/wazuh.gpg
```

3. Depoyu ekleyin.

```
echo "deb [signed-by=/usr/share/keyrings/wazuh.gpg] https://packages.wazuh.com/4.x/apt/ stable main" | tee -a /etc/apt/sources.list.d/wazuh.list
```

4. Paket bilgilerini güncelleyin.

```
apt-get update
```

Wazuh yöneticisinin kurulumu

1. Wazuh yönetici paketini yükleyin.

   Yum:

   ```
   yum -y install wazuh-manager
   ```

   APT:

   ```
   apt-get update
   ```

Filebeat'i yükleme

Yum:

```
yum -y install filebeat
```

APT:

```
apt-get -y install filebeat
```

Filebeat'i yapılandırma

1. Önceden yapılandırılmış Filebeat yapılandırma dosyasını indirin.

2. Yapılandırma dosyasını düzenleyin `/etc/filebeat/filebeat.yml`ve aşağıdaki değeri değiştirin:
   a. `hosts`: Bağlanılacak Wazuh dizinleyici düğümlerinin listesi. IP adreslerini veya ana bilgisayar adlarını kullanabilirsiniz. Varsayılan olarak, ana bilgisayar localhost olarak ayarlanmıştır . Bunu uygun şekilde Wazuh dizinleyici adresinizle d in.`hosts: ["127.0.0.1:9200"]`
   b. Birden fazla Wazuh dizinleyici düğümünüz varsa, adresleri virgül kullanarak ayırabilirsiniz. Örneğin,`hosts: ["10.0.0.1:9200", "10.0.0.2:9200", "10.0.0.3:9200"]`

   ```
   # Wazuh - Filebeat configuration file
   output.elasticsearch:
   hosts: ["10.0.0.1:9200"]
   protocol: https
   username: ${username}
   password: ${password}
   ```

3. Kimlik doğrulama bilgilerini güvenli bir şekilde depolamak için bir Filebeat anahtar deposu oluşturun.

   ```
   filebeat keystore create
   ```

4. Varsayılan kullanıcı adı ve parolayı `admin`: `admin`gizli anahtar deposuna ekleyin.

   ```
   echo admin | filebeat keystore add username --stdin --force
   echo admin | filebeat keystore add password --stdin --force
   ```

5. Wazuh indeksleyicisi için uyarı şablonunu indirin.

```
curl -so /etc/filebeat/wazuh-template.json
https://raw.githubusercontent.com/wazuh/wazuh/v4.9.2/extensions/elasticsearch/7.x/wazuh-template.json
chmod go+r /etc/filebeat/wazuh-template.json
```

6. Filebeat için Wazuh modülünü yükleyin.

```
curl -s https://packages.wazuh.com/4.x/filebeat/wazuh-filebeat-0.4.tar.gz | tar -xvz -C /usr/share/filebeat/module
```

Sertifikaların Dağıtımı

> **Not:** `wazuh-certificates.tar`İlk yapılandırma adımında oluşturulan dosyanın bir kopyasının çalışma dizininize yerleştirildiğinden emin olun .

1. `<SERVER_NODE_NAME>`Wazuh sunucu düğüm sertifika adınızla değiştirin , `config.yml` sertifikaları oluştururken kullanılanla aynı. Ardından, sertifikaları karşılık gelen konumlarına taşıyın.

```
NODE_NAME=<SERVER_NODE_NAME>
```

```
mkdir /etc/filebeat/certs
tar -xf ./wazuh-certificates.tar -C /etc/filebeat/certs/ ./$NODE_NAME.pem ./$NODE_NAME-key.pem ./root-ca.pem
mv -n /etc/filebeat/certs/$NODE_NAME.pem /etc/filebeat/certs/filebeat.pem
mv -n /etc/filebeat/certs/$NODE_NAME-key.pem /etc/filebeat/certs/filebeat-key.pem
chmod 500 /etc/filebeat/certs
chmod 400 /etc/filebeat/certs/*
chown -R root:root /etc/filebeat/certs
```

Wazuh Indexer Bağlantısını Yapılandırma

> Not: Eğer güvenlik açığı tespit özelliğini kullanmayacaksanız bu adımı atlayabilirsiniz.

> Not: Varsayılan adım adım kurulum kimlik bilgileri şunlardır `admin`:`admin`

1. Wazuh dizinleyici kullanıcı adını ve parolasını wazuh-keystore aracını kullanarak Wazuh yöneticisi anahtar deposuna kaydedin:

```
echo '<INDEXER_USERNAME>' | /var/ossec/bin/wazuh-keystore -f indexer -k username
echo '<INDEXER_PASSWORD>' | /var/ossec/bin/wazuh-keystore -f indexer -k password
```

2. `/var/ossec/etc/ossec.conf`Dizinleyici bağlantısını yapılandırmak için düzenleyin . Varsayılan olarak, dizinleyici ayarları bir ana bilgisayara yapılandırılmıştır. Aşağıda vurgulandığı gibi ayarlanmıştır `0.0.0.0`.

```
<indexer>
  <enabled>yes</enabled>
  <hosts>
    <host>https://0.0.0.0:9200</host>
  </hosts>
  <ssl>
    <certificate_authorities>
      <ca>/etc/filebeat/certs/root-ca.pem</ca>
    </certificate_authorities>
    <certificate>/etc/filebeat/certs/filebeat.pem</certificate>
    <key>/etc/filebeat/certs/filebeat-key.pem</key>
  </ssl>
</indexer>
```

   Wazuh dizinleyici düğüm IP adresiniz veya ana bilgisayar adınızla değiştirin `0.0.0.0`. Bu değeri Filebeat yapılandırma dosyasında bulabilirsiniz `/etc/filebeat/filebeat.yml`.

   Filebeat sertifikasının ve anahtar adının `/etc/filebeat/certs`.

   Bir Wazuh dizinleyici kümeniz varsa, `<host>`düğümlerinizin her biri için bir giriş ekleyin. Örneğin, iki düğümlü bir yapılandırmada:

```
<hosts>
  <host>https://10.0.0.1:9200</host>
  <host>https://10.0.0.2:9200</host>
</hosts>
```

   Güvenlik açığı tespiti, listedeki ilk düğüme raporlamayı önceliklendirir. Kullanılabilir olmadığında bir sonraki düğüme geçer.

Wazuh yöneticisinin başlatılması

1. Wazuh yönetici servisini etkinleştirin ve başlatın.

SysV Başlatma:

İşletim sisteminize göre bir seçenek seçin:

1. RPM tabanlı işletim sistemi:

```
chkconfig --add wazuh-manager
service wazuh-manager start
```

2. Debian tabanlı işletim sistemi:

```
# update-rc.d wazuh-manager defaults 95 10
# service wazuh-manager start
```

Systemd:

```
systemctl daemon-reload
systemctl enable wazuh-manager
systemctl start wazuh-manager
```

2. Wazuh yöneticisinin durumunu doğrulamak için aşağıdaki komutu çalıştırın.

SysV Başlatma:

```
service wazuh-manager status
```

Systemd:

```
systemctl status wazuh-manager
```

Filebeat hizmetini başlatma

1. Filebeat servisini etkinleştirin ve başlatın.

SysV Başlatma:

Kullanılan işletim sistemine göre bir seçenek seçin.
a. RPM tabanlı işletim sistemi:

```
chkconfig --add filebeat
service filebeat start
```

b. Debian tabanlı işletim sistemi:

```
update-rc.d filebeat defaults 95 10
service filebeat start
```

Systemd:

```
systemctl daemon-reload
systemctl enable filebeat
systemctl start filebeat
```

2. Filebeat'in başarıyla yüklendiğini doğrulamak için aşağıdaki komutu çalıştırın.

```
filebeat test output
```

Örnek yanıtı görmek için çıktıyı genişletin.

Output

```
elasticsearch: https://127.0.0.1:9200...
  parse url... OK
  connection...
    parse host... OK
    dns lookup... OK
    addresses: 127.0.0.1
    dial up... OK
  TLS...
    security: server's certificate chain verification is enabled
    handshake... OK
    TLS version: TLSv1.3
    dial up... OK
  talk to server... OK
  version: 7.10.2
```

Wazuh sunucu düğümünüz artık başarıyla kuruldu. Kurulum sürecinin bu aşamasını Wazuh kümenizdeki her Wazuh sunucu düğümü için tekrarlayın, ardından Wazuh kümesini yapılandırmaya devam edin. Wazuh sunucusu tek düğümlü bir küme istiyorsanız, her şey ayarlanmıştır ve doğrudan Wazuh panosunu adım adım yükleme ile devam edebilirsiniz .

2. Çoklu düğüm dağıtımı için küme yapılandırması

Sonraki adımlar

Wazuh sunucu kurulumu artık tamamlandı ve adım adım Wazuh dashboard yüklemeye geçebilirsiniz .

Wazuh sunucusunu kaldırmak istiyorsanız Wazuh sunucusunu kaldırma bölümüne bakın .

Wazuh Server Sistem Gereksinimleri

Wazuh server için desteklenen ve önerilen sistem gereksinimleri ve işletim sistemleri aşağıda yer almaktadır. Kurulum sırasında root kullanıcı yetkisine ihtiyacınız olacak. Multi-node veya single-node olarak kurulum gerçekleştirebilirsiniz.

Önerilen işletim sistemleri

Wazuh 64-bit Linux işletim sistemlerine kurulabilir. Aşağıdaki işletim sistemlerini destekler:

Amazon Linux 2, Amazon Linux 2023	CentOS 7, 8
Red Hat Enterprise Linux 7, 8, 9	Ubuntu 16.04, 18.04, 20.04, 22.04, 24.04

Donanım Gereksinimleri

	Minimum		Önerilen	
Component	**RAM (GB)**	**CPU (cores)**	**RAM (GB)**	**CPU (cores)**
Wazuh Indexer	2	2	4	8

Veri miktarı, saniye başına oluşturulan uyarılara (APS) bağlıdır. Bu tablo, izlenen uç noktaların türüne bağlı olarak, bir Wazuh server node'unda 90 günlük uyarıları depolamak için aracı başına ihtiyaç duyulan tahmini disk alanının ayrıntılarını verir.

Monitör edilen endpointler	**APS**	**Wazuh Indexer depolama (GB/90 gün)**
Sunucular	0.25	0.1
Workstationlar	0.1	0.04
Ağ cihazları	0.5	0.2

Örneğin, 80 workstation, 10 sunucu ve 10 ağ cihazının bulunduğu bir ortam için Wazuh indeksleyici sunucusunda 90 günlük uyarılar için gereken depolama alanı 6 GB'dir.

Bir Wazuh Server'ın daha fazla kaynak gerektirip gerektirmediğini belirlemek için şu dosyaları izleyin.

- `/var/ossec/var/run/wazuh-analysisd.state` : `events_dropped` değişkeni, olayların kaynak eksikliği nedeniyle bırakılıp bırakılmadığını gösterir.
- `/var/ossec/var/run/wazuh-remoted.state` : `discarded_count` değişkeni, agentlardan gelen mesajların atılıp atılmadığını gösterir.

Ortam düzgün çalışıyorsa bu iki değişkenin sıfır olması gerekir. Aksi takdirde kümeye ek düğümler eklenebilir.

Wazuh Dashboard

Wazuh dashboard, güvenlik verilerinin madenciliği, analizi ve görselleştirilmesi için zengin bir web arayüzüdür. Güvenlik olaylarını, tespit edilen güvenlik açıklarını, dosya bütünlüğünü izleme verilerini, yapılandırma değerlendirme sonuçlarını, bulut altyapısı izleme olaylarını ve mevzuata uygunluk standartlarını görselleştirebilir.

Wazuh Kurulum Asistanı

Asistan aracılığıla Wazuh dashboard kurulumunu gerçekleştirin ve yapılandırın. Wazuh dashboard, güvenlik olaylarını incelemek ve görselleştirmek için esnek ve zenginleştirilmiş bir web arayüzü sunar.

1. Wazuh asistan kurulumunu indirin.

```
curl -sO https://packages.wazuh.com/4.9/wazuh-install.sh
```

2. Wazuh asistan kurulum dosyasını `--wazuh-dashboard` parametresi ve node adı ile birlikte kurun. Indexer sunucusunda hazırladığınız `config.yml` dosyasında yer alan isim ile parametre olarak verilen isim aynı olmalıdır.

> Indexer'da oluşturduğunuz wazuh-install-files.tar dosyasının bir kopyasının .sh dosyasını çalıştırdığınız dizinde olduğundan emin olun.

```
bash wazuh-install.sh --wazuh-dashboard dashboard
```

Varsayılan Wazuh web arayüzü bağlantısı 443 portudur. Bu portu isteğe bağlı olarak `-p` veya `--port` parametresini kullanarak değiştirebilirsiniz. Önerilen bağlantı noktalarından bazıları: 8443, 8444, 8080, 8888 ve 9000'dir.

Wazuh kurulumu tamamlandığında çıktıda erişim kimlik bilgileri ve kurulumun başarılı olduğunu onaylayan bir mesaj gösterilir.

```
INFO: --- Summary ---
INFO: You can access the web interface https://<wazuh-dashboard-ip>
  User: admin
  Password: <ADMIN_PASSWORD>

INFO: Installation finished.
```

Kurulum süreçleri tamamlandı. Bundan sonraki aşamada ihtiyacınız olan parolaları wazuh kurulum asistanının oluşturduğu `wazuh-install-files.tar` arşivinin içinde yer alan `wazuh-passwords.txt` dosyasında bulabilirsiniz. Aşağıdaki komutla bu dosyayı okuyabilirsiniz.

```
tar -O -xvf wazuh-install-files.tar wazuh-install-files/wazuh-passwords.txt
```

Wazuh web arayüzüne aşağıdaki formatta erişin:

- **URL:** https://<wazuh-dashboard-ip>
- **Username**: admin
- **Password**: <ADMIN_PASSWORD>

Wazuh kontrol paneline ilk kez eriştiğinizde tarayıcı, sertifikanın güvenilir bir yetkili tarafından verilmediğini belirten bir uyarı mesajı görüntüler. Web tarayıcısının gelişmiş seçeneklerine bir istisna eklenebilir. Daha fazla güvenlik için, önceden oluşturulan root-ca.pem dosyası bunun yerine tarayıcının sertifika yöneticisine aktarılabilir. Alternatif olarak güvenilir bir yetkiliden alınan bir sertifika da yapılandırılabilir.

Adım Adım Kurulum

Adım adım talimatları izleyerek Wazuh panosunu kurun ve yapılandırın. Wazuh panosu, Wazuh sunucu uyarılarını ve arşivlenmiş olayları çıkarmak ve görselleştirmek için bir web arayüzüdür.

> **Not**: Aşağıda açıklanan tüm komutları çalıştırabilmek için root kullanıcı ayrıcalıklarına sahip olmanız gerekir.

Wazuh Gösterge Paneli Kurulumu

Paket Bağımlılıklarını Yükleme

1. Eğer eksikse aşağıdaki paketleri kurun.
   Yum:

   ```
   yum install libcap
   ```

   APT:

   ```
   apt-get install debhelper tar curl libcap2-bin #debhelper version 9 or later
   ```

Wazuh Deposunu Ekleme

> **Not:** Wazuh panosunu Wazuh indeksleyicisi veya Wazuh sunucusuyla aynı ana bilgisayara yüklüyorsanız, Wazuh deposunu zaten eklemiş olabileceğiniz için bu adımları atlayabilirsiniz.

Yum:

1. GPG anahtarını içe aktarın.

```
rpm --import https://packages.wazuh.com/key/GPG-KEY-WAZUH
```

2. Depoyu ekleyin.

```
echo -e '[wazuh]\ngpgcheck=1\ngpgkey=https://packages.wazuh.com/key/GPG-KEY-WAZUH\nenabled=1\nname=EL-$releasever - Wazuh\nbaseurl=https://packages.wazuh.com/4.x/yum/\nprotect=1' | tee /etc/yum.repos.d/wazuh.repo
```

APT:

1. Eğer eksikse aşağıdaki paketleri kurun.

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

2. GPG anahtarını yükleyin.

```
curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | gpg --no-default-keyring --keyring gnupg-ring:/usr/share/keyrings/wazuh.gpg --import && chmod 644 /usr/share/keyrings/wazuh.gpg
```

3. Depoyu ekleyin.

```
echo "deb [signed-by=/usr/share/keyrings/wazuh.gpg] https://packages.wazuh.com/4.x/apt/ stable main" | tee -a /etc/apt/sources.list.d/wazuh.list
```

4. Paket bilgilerini güncelleyin.

```
apt-get update
```

Wazuh Panosunun Kurulumu

1. Wazuh gösterge paneli paketini yükleyin.

Yum:

```
yum -y install wazuh-dashboard
```

APT:

```
apt-get -y install wazuh-dashboard
```

Wazuh Panosunu Yapılandırma

1. Dosyayı düzenleyin `/etc/wazuh-dashboard/opensearch_dashboards.yml`ve aşağıdaki değerleri değiştirin:

   a. `server.host`: Bu ayar, Wazuh gösterge paneli sunucusunun ana bilgisayarını belirtir. Uzak kullanıcıların bağlanmasına izin vermek için, değeri Wazuh gösterge paneli sunucusunun IP adresine veya DNS adına ayarlayın. Değer, `0.0.0.0`ana bilgisayarın tüm kullanılabilir IP adreslerini kabul edecektir.

   b. `opensearch.hosts`: Tüm sorgularınız için kullanılacak Wazuh dizinleyici örneklerinin URL'leri. Wazuh panosu, aynı kümedeki birden fazla Wazuh dizinleyici düğümüne bağlanacak şekilde yapılandırılabilir. Düğümlerin adresleri virgülle ayrılabilir. Örneğin, `["https://10.0.0.2:9200", "https://10.0.0.3:9200","https://10.0.0.4:9200"]`

```
server.host: 0.0.0.0
server.port: 443
opensearch.hosts: https://localhost:9200
opensearch.ssl.verificationMode: certificate
```

Sertifikaların Dağıtımı

> **Not:** `wazuh-certificates.tar`İlk yapılandırma adımında oluşturulan dosyanın bir kopyasının çalışma dizininize yerleştirildiğinden emin olun .

1. `<DASHBOARD_NODE_NAME>`Sertifikaları oluşturmak için kullandığınız aynı adla Wazuh kontrol paneli düğümünüzün adını değiştirin `config.yml`ve sertifikaları ilgili konumlarına taşıyın.

1.
```
NODE_NAME=<DASHBOARD_NODE_NAME>
```

```
mkdir /etc/wazuh-dashboard/certs
tar -xf ./wazuh-certificates.tar -C /etc/wazuh-dashboard/certs/ ./$NODE_NAME.pem ./$NODE_NAME-key.pem ./root-ca.pem
mv -n /etc/wazuh-dashboard/certs/$NODE_NAME.pem /etc/wazuh-dashboard/certs/dashboard.pem
mv -n /etc/wazuh-dashboard/certs/$NODE_NAME-key.pem /etc/wazuh-dashboard/certs/dashboard-key.pem
chmod 500 /etc/wazuh-dashboard/certs
chmod 400 /etc/wazuh-dashboard/certs/*
chown -R wazuh-dashboard:wazuh-dashboard /etc/wazuh-dashboard/certs
```

Wazuh Panosu Hizmeti Başlatılıyor

1. Wazuh gösterge paneli hizmetini etkinleştirin ve başlatın.

   Systemd:

   ```
   systemctl daemon-reload
   systemctl enable wazuh-dashboard
   systemctl start wazuh-dashboard
   ```

   SysV Başlatma:

   İşletim sisteminize göre bir seçenek seçin:

   - RPM tabanlı işletim sistemi:

     ```
     chkconfig --add wazuh-dashboard
     service wazuh-dashboard start
     ```

   - Debian tabanlı işletim sistemi:

     ```
     update-rc.d wazuh-dashboard defaults 95 10
     service wazuh-dashboard start
     ```

2. Dosyayı düzenleyin `/usr/share/wazuh-dashboard/data/wazuh/config/wazuh.yml` ve `url` değeri Wazuh sunucusu ana düğümünün IP adresi veya ana bilgisayar adıyla değiştirin.

```
hosts:
  - default:
    url: https://<WAZUH_SERVER_IP_ADDRESS>
    port: 55000
    username: wazuh-wui
    password: wazuh-wui
    run_as: false
```

3. Kimlik bilgilerinizle Wazuh web arayüzüne erişin.
    - URL: *https://<WAZUH_DASHBOARD_IP_ADRESİ>*
    - **Kullanıcı adı** : *admin*
    - **Şifre** : *admin*

Wazuh panosuna ilk kez eriştiğinizde, tarayıcı sertifikanın güvenilir bir otorite tarafından verilmediğini belirten bir uyarı mesajı gösterir. Web tarayıcısının gelişmiş seçeneklerine bir istisna eklenebilir. Daha fazla güvenlik için, `root-ca.pem` daha önce oluşturulan dosya tarayıcının sertifika yöneticisine aktarılabilir. Alternatif olarak, güvenilir bir otoritenin sertifikası yapılandırılabilir.

Wazuh Kurulumunuzun Güvenliğini Sağlama

Artık tüm Wazuh merkezi bileşenlerini yüklediniz ve yapılandırdınız. Altyapınızı olası saldırılardan korumak için varsayılan kimlik bilgilerini değiştirmenizi öneririz.

Dağıtım türünüzü seçin ve hem Wazuh API'si hem de Wazuh dizinleyici kullanıcıları için varsayılan parolaları değiştirmek üzere talimatları izleyin.

Hepsi bir arada dağıtım:

1. Tüm dahili kullanıcıların şifrelerini değiştirmek için Wazuh şifre aracını kullanın.

```
/usr/share/wazuh-indexer/plugins/opensearch-security/tools/wazuh-passwords-tool.sh --api --change-all --admin-user wazuh --admin-password wazuh
```

Output

```
INFO: The password for user admin is yWOzmNA.?Aoc+rQfDBcF71KZp?1xd7IO
INFO: The password for user kibanaserver is nUa+66zY.eDF*2rRl5GKdgLxvgYQA+wo
INFO: The password for user kibanaro is 0jHq.4i*VAgclnqFiXvZ5gtQq1D5LCcL
INFO: The password for user logstash is hWW6U45rPoCT?oR.r.Baw2qaWz2iH8Ml
INFO: The password for user readall is PNt5K+FpKDMO2TlxJ6Opb2D0mYl*I7FQ
INFO: The password for user snapshotrestore is +GGz2noZZr2qVUK7xbtqjUup049tvLq.
WARNING: Wazuh indexer passwords changed. Remember to update the password in the Wazuh dashboard a
INFO: The password for Wazuh API user wazuh is JYWz5Zdb3Yq+uOzOPyUU4oat0n60VmWI
INFO: The password for Wazuh API user wazuh-wui is +fLddaCiZePxh24*?jC0nyNmgMGCKE+2
```

```
INFO: Updated wazuh-wui user password in wazuh dashboard. Remember to restart the service.
```

Dağıtılmış Dağıtım:

1. *Herhangi bir Wazuh dizinleyici* düğümünde , Wazuh dizinleyici kullanıcılarının parolalarını değiştirmek için Wazuh parolaları aracını kullanın.

   ```
   /usr/share/wazuh-indexer/plugins/opensearch-security/tools/wazuh-passwords-tool.sh --change-all
   ```

   Output

   ```
   INFO: Wazuh API admin credentials not provided, Wazuh API passwords not changed.
   INFO: The password for user admin is wcAny.XUwOVWHFy.+7tW9I8gUW1L8N3j
   INFO: The password for user kibanaserver is qy6fBrNOI4fD9yR9.Oj03?pihN6Ejfpp
   INFO: The password for user kibanaro is Nj*sSXSxwntrx3O7m8ehrgdHkxCc0dna
   INFO: The password for user logstash is nQg1Qw0nIQFZXUJc8r8+zHVrkelch33h
   INFO: The password for user readall is s0iWAei?RXObSDdibBfzSgXdhZCD9kH4
   INFO: The password for user snapshotrestore is Mb2EHw8SIc1d.oz.nM?dHiPBGk7s?UZB
   WARNING: Wazuh indexer passwords changed. Remember to update the password in the Wazuh dashboard a
   ```

2. Wazuh sunucunuzun *ana düğümünde* , Wazuh parolaları aracını indirin ve bunu kullanarak Wazuh API kullanıcılarının parolalarını değiştirin.

   ```
   curl -sO https://packages.wazuh.com/4.9/wazuh-passwords-tool.sh
   bash wazuh-passwords-tool.sh --api --change-all --admin-user wazuh --admin-password wazuh
   ```

   Output

   ```
   INFO: The password for Wazuh API user wazuh is ivLOfmj7.jL6*7Ev?UJoFjrkGy9t6Je.
   INFO: The password for Wazuh API user wazuh-wui is fL+f?sFRPEv5pYRE559rqy9b6G4Z5pVi
   ```

3. *Tüm Wazuh sunucu düğümlerinizde* , Filebeat anahtar deposundaki *yönetici* parolasını güncellemek için aşağıdaki komutu çalıştırın . `<ADMIN_PASSWORD>`İlk adımda oluşturulan rastgele parola ile değiştirin.

   ```
   echo <ADMIN_PASSWORD> | filebeat keystore add password --stdin --force
   ```

4. Değişikliği uygulamak için Filebeat'i yeniden başlatın.

   Systemd:

   ```
   systemctl restart filebeat
   ```

SysV Başlatma:

```
service filebeat restart
```

Not

3. ve 4. adımları *her Wazuh sunucu düğümünde* tekrarlayın .

5. *Wazuh kontrol paneli* düğümünüzde , Wazuh kontrol paneli anahtar deposundaki *kibanaserver* parolasını güncellemek için aşağıdaki komutu çalıştırın . `<KIBANASERVER_PASSWORD>`İlk adımda oluşturulan rastgele parola ile değiştirin.

```
echo <KIBANASERVER_PASSWORD> | /usr/share/wazuh-dashboard/bin/opensearch-dashboards-keystore --allow-root add -f --stdin opensearch.password
```

6. İkinci adımda oluşturulan `/usr/share/wazuh-dashboard/data/wazuh/config/wazuh.yml`yeni *wazuh-wui* şifresi ile yapılandırma dosyasını güncelleyin.

```
hosts:
  - default:
      url: https://127.0.0.1
      port: 55000
      username: wazuh-wui
      password: "<wazuh-wui-password>"
      run_as: false
```

7. Değişiklikleri uygulamak için Wazuh panosunu yeniden başlatın.

Systemd:

```
systemctl restart wazuh-dashboard
```

SysV Başlatma:

```
service wazuh-dashboard restart
```

Sonraki Adımlar

Wazuh merkezi bileşenlerinin tamamı başarıyla kuruldu ve sabitlendi.

Wazuh ortamı artık hazır ve izlenecek uç noktalara Wazuh aracısını yüklemeye devam edebilirsiniz. Bu eylemi gerçekleştirmek için Wazuh aracısı bölümüne bakın.

Wazuh panosunu kaldırmak istiyorsanız Wazuh panosunu kaldırma bölümüne bakın .

Wazuh Dashboard Sistem Gereksinimleri

Wazuh dashboard için desteklenen ve önerilen sistem gereksinimleri ve işletim sistemleri aşağıda yer almaktadır. Kurulum sırasında root kullanıcı yetkisine ihtiyacınız olacak.

Önerilen işletim sistemleri

Wazuh 64-bit Linux işletim sistemlerine kurulabilir. Aşağıdaki işletim sistemlerini destekler:

Amazon Linux 2, Amazon Linux 2023	CentOS 7, 8
Red Hat Enterprise Linux 7, 8, 9	Ubuntu 16.04, 18.04, 20.04, 22.04, 24.04

Donanım Gereksinimleri

	Minimum		Önerilen	
Component	**RAM (GB)**	**CPU (cores)**	**RAM (GB)**	**CPU (cores)**
Wazuh Indexer	4	2	8	4

Wazuh Agent

Windows

Aracı, izlemek istediğiniz uç noktada çalışır ve Wazuh sunucusuyla iletişim kurarak şifrelenmiş ve kimliği doğrulanmış bir kanal aracılığıyla neredeyse gerçek zamanlı olarak veri gönderir. Windows XP'den Windows 11 ve Windows Server 2022 dahil olmak üzere en son mevcut sürümlere kadar Windows sistemlerinizi Wazuh ile izleyin.

> **Not:** Kurulumu gerçekleştirmek için yönetici ayrıcalıklarına sahip olmanız gerekmektedir.

1. Kurulum sürecini başlatmak için Windows yükleyicisini indirin .
2. İzlemek istediğiniz kurulum yöntemini seçin: komut satırı arayüzü (CLI) veya grafiksel kullanıcı arayüzü (GUI).

   CLI
   Wazuh aracısını uç noktanıza dağıtmak için komut kabuğu alternatiflerinden birini seçin ve `WAZUH_MANAGER`değişkeni Wazuh yöneticisi IP adresini veya ana bilgisayar adını içerecek şekilde düzenleyin.

   - CMD Kullanımı:

     ```
     wazuh-agent-4.9.2-1.msi /q WAZUH_MANAGER="10.0.0.2"
     ```

   - PowerShell Kullanımı:

     ```
     .\wazuh-agent-4.9.2-1.msi /q WAZUH_MANAGER="10.0.0.2"
     ```

   Aracı adı, aracı grubu ve kayıt parolası gibi ek dağıtım seçenekleri için Windows için Dağıtım değişkenleri bölümüne bakın.
   Kurulum süreci artık tamamlandı ve Wazuh aracısı başarıyla kuruldu ve yapılandırıldı. Wazuh aracısını GUI'den veya çalıştırarak başlatabilirsiniz:

   ```
   NET START Wazuh
   ```

   Başladıktan sonra Wazuh temsilcisi kayıt sürecini başlatacak ve yöneticiye kayıt yaptıracaktır.

   > Not: Alternatif olarak, bir aracıyı kaydetmeden yüklemek istiyorsanız, dağıtım değişkenlerini atlayın. Farklı kayıt yöntemleri hakkında daha fazla bilgi edinmek için

> Wazuh aracı kayıt bölümüne bakın.

Grafiksel Kullanıcı Arayüzü

Wazuh aracısını sisteminize yüklemek için Windows yükleyicisini çalıştırın ve yükleme sihirbazındaki adımları izleyin. Bazı istemleri nasıl yanıtlayacağınızdan emin değilseniz, varsayılan yanıtları kullanın. Yüklendikten sonra, aracı yapılandırma, günlük dosyasını açma ve hizmeti başlatma veya durdurma için bir GUI kullanır.

Windows aracı yöneticisi

Kurulum işlemi artık tamamlandı ve Wazuh aracısı Windows uç noktanıza başarıyla kuruldu. Bir sonraki adım, aracıyı Wazuh sunucusuyla iletişim kuracak şekilde kaydetmek ve yapılandırmaktır. Bu işlemi gerçekleştirmek için Wazuh aracısı kayıt bölümüne bakın.

Varsayılan olarak tüm aracı dosyaları kurulumdan sonra `C:\Program Files (x86)\ossec-agent` saklanır.

macOS

Aracı, izlemek istediğiniz uç noktada çalışır ve Wazuh sunucusuyla iletişim kurarak şifrelenmiş ve kimliği doğrulanmış bir şekilde neredeyse gerçek zamanlı olarak veri gönderir.

> Not: Aşağıda açıklanan tüm komutları çalıştırabilmek için root kullanıcı ayrıcalıklarına sahip olmanız gerekir.

1. Kurulum sürecini başlatmak için mimarinize uygun Wazuh aracısını indirin:
   - **Intel** : wazuh-agent-4.9.2-1.intel64.pkg . macOS Sierra ve sonrası için uygundur.
   - **Apple silikonu** : wazuh-agent-4.9.2-1.arm64.pkg . macOS Big Sur ve sonraki sürümler için uygundur.
   - İzlemek istediğiniz kurulum yöntemini seçin: Komut satırı arayüzü (CLI) veya grafiksel kullanıcı arayüzü (GUI).

     CLI
     Wazuh aracısını uç noktanıza dağıtmak için mimarinizi seçin, `WAZUH_MANAGER` değişkeni Wazuh yöneticinizin IP adresini veya ana bilgisayar adını içerecek şekilde düzenleyin ve aşağıdaki komutu çalıştırın.

     1. Wazuh aracısını uç noktanıza dağıtmak için mimarinizi seçin, `WAZUH_MANAGER`değişkeni Wazuh yöneticinizin IP adresini veya ana bilgisayar adını içerecek şekilde düzenleyin ve aşağıdaki komutu çalıştırın.

        Intel

        ```
        # echo "WAZUH_MANAGER='10.0.0.2'" > /tmp/wazuh_envs && installer -pkg wazuh-agent-4.9.2-1.intel64.pkg -target /
        ```

        Apple Silikonu

        ```
        echo "WAZUH_MANAGER='10.0.0.2'" > /tmp/wazuh_envs && installer -pkg wazuh-agent-4.9.2-1.arm64.pkg -target /
        ```

2. Kurulum sürecini tamamlamak için Wazuh aracısını başlatın.

```
# /Library/Ossec/bin/wazuh-control start
```

Kurulum işlemi artık tamamlandı ve Wazuh aracısı macOS uç noktanızda başarıyla dağıtıldı ve çalışıyor.

Grafiksel Kullanıcı Arayüzü

1. Wazuh aracısını sisteminize yüklemek için indirilen dosyayı çalıştırın ve yükleme sihirbazındaki adımları izleyin. Bazı istemleri nasıl yanıtlayacağınızdan emin değilseniz, varsayılan yanıtları kullanın.

2. Kurulum sürecini tamamlamak için Wazuh aracısını başlatın.

```
# sudo /Library/Ossec/bin/wazuh-control start
```

Kurulum süreci artık tamamlandı ve Wazuh aracısı macOS uç noktanıza başarıyla kuruldu. Bir sonraki adım, aracıyı Wazuh sunucusuyla iletişim kuracak şekilde kaydetmek ve yapılandırmaktır. Bu işlemi gerçekleştirmek için Wazuh aracısı kayıt bölümüne bakın.

`/Library/Ossec/`Varsayılan olarak tüm aracı dosyaları kurulumdan sonra saklanır .

Linux

Wazuh aracılarını Linux uç noktalarına dağıtma

Aracı, izlemek istediğiniz ana bilgisayarda çalışır ve Wazuh sunucusuyla iletişim kurarak şifrelenmiş ve kimliği doğrulanmış bir kanal üzerinden neredeyse gerçek zamanlı olarak veri gönderir.

Bir Wazuh aracısının Linux sistemine dağıtımı, aracı yükleme, kaydetme ve yapılandırma görevini kolaylaştıran dağıtım değişkenlerini kullanır. Alternatif olarak, Wazuh aracı paketini doğrudan indirmek istiyorsanız, paketler listesi bölümüne bakın.

> **Not:** Aşağıda açıklanan tüm komutları çalıştırabilmek için root kullanıcı ayrıcalıklarına sahip olmanız gerekir.

Wazuh deposunu ekleyin

Resmi paketleri indirmek için Wazuh deposunu ekleyin.

YUM:

1. GPG anahtarını içe aktarın:

```
rpm --import https://packages.wazuh.com/key/GPG-KEY-WAZUH
```

2. Depoyu ekleyin:

```
cat > /etc/yum.repos.d/wazuh.repo << EOF
[wazuh]
gpgcheck=1
gpgkey=https://packages.wazuh.com/key/GPG-KEY-WAZUH
enabled=1
name=EL-\$releasever - Wazuh
baseurl=https://packages.wazuh.com/4.x/yum/
```

```
protect=1
EOF
```

APT:

1. GPG anahtarını yükleyin:

```
curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | gpg --no-default-keyring --keyring gnupg-ring:/usr/share/keyrings/wazuh.gpg --import && chmod 644 /usr/share/keyrings/wazuh.gpg
```

2. Depoyu ekleyin:

```
echo "deb [signed-by=/usr/share/keyrings/wazuh.gpg] https://packages.wazuh.com/4.x/apt/ stable main" | tee -a /etc/apt/sources.list.d/wazuh.list
```

3. Paket bilgilerini güncelleyin:

```
apt-get update
```

Not: Debian 7, 8 ve Ubuntu 14 sistemleri için GCP anahtarını içe aktarın ve aşağıdaki komutları kullanarak Wazuh deposunu ekleyin (adım 1 ve 2).

```
apt-get install gnupg apt-transport-https
curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | apt-key add -
echo "deb https://packages.wazuh.com/4.x/apt/ stable main" | tee -a /etc/apt/sources.list.d/wazuh.list
```

Zypp:

1. GPG anahtarını içe aktarın:

```
rpm --import https://packages.wazuh.com/key/GPG-KEY-WAZUH
```

2. Depoyu ekleyin:

```
cat > /etc/zypp/repos.d/wazuh.repo <<\EOF
[wazuh]
gpgcheck=1
gpgkey=https://packages.wazuh.com/key/GPG-KEY-WAZUH
enabled=1
name=EL-$releasever - Wazuh
baseurl=https://packages.wazuh.com/4.x/yum/
protect=1
EOF
```

3. Depoyu yenileyin:

```
zypper refresh
```

Bir Wazuh aracısı dağıtın

1. Wazuh aracısını uç noktanıza dağıtmak için paket yöneticinizi seçin ve `WAZUH_MANAGER`değişkeni Wazuh yöneticinizin IP adresini veya ana bilgisayar adını içerecek şekilde düzenleyin.

YUM:

```
WAZUH_MANAGER="10.0.0.2" yum install wazuh-agent
```

Aracı adı, aracı grubu ve kayıt parolası gibi ek dağıtım seçenekleri için Linux için Dağıtım değişkenleri bölümüne bakın.

> **Not:** Alternatif olarak, bir aracıyı kaydetmeden yüklemek istiyorsanız, dağıtım değişkenlerini atlayın. Farklı kayıt yöntemleri hakkında daha fazla bilgi edinmek için Wazuh aracı kayıt bölümüne bakın.

APT:

```
WAZUH_MANAGER="10.0.0.2" apt-get install wazuh-agent
```

Aracı adı, aracı grubu ve kayıt parolası gibi ek dağıtım seçenekleri için Linux için Dağıtım değişkenleri bölümüne bakın.

> **Not:** Alternatif olarak, bir aracıyı kaydetmeden yüklemek istiyorsanız, dağıtım değişkenlerini atlayın. Farklı kayıt yöntemleri hakkında daha fazla bilgi edinmek için Wazuh aracı kayıt bölümüne bakın.

ZYpp:

```
WAZUH_MANAGER="10.0.0.2" zypper install wazuh-agent
```

Aracı adı, aracı grubu ve kayıt parolası gibi ek dağıtım seçenekleri için Linux için Dağıtım değişkenleri bölümüne bakın.

> **Not:** Alternatif olarak, bir aracıyı kaydetmeden yüklemek istiyorsanız, dağıtım değişkenlerini atlayın. Farklı kayıt yöntemleri hakkında daha fazla bilgi edinmek için Wazuh aracı kayıt bölümüne bakın.

2. Wazuh aracı hizmetini etkinleştirin ve başlatın.

Systemd:

```
systemctl daemon-reload
systemctl enable wazuh-agent
systemctl start wazuh-agent
```

SysV init:

İşletim sisteminize göre bir seçenek seçin.

1. RPM tabanlı işletim sistemleri:

```
# chkconfig --add wazuh-agent
# service wazuh-agent start
```

2. Debian tabanlı işletim sistemleri

```
update-rc.d wazuh-agent defaults 95 10
service wazuh-agent start
```

No Service Manager:

On some systems, you need to start the agent manually:

```
/var/ossec/bin/wazuh-control start
```

The deployment process is now complete, and the Wazuh agent is successfully running on your Linux system.

- **Recommended action** - Disable Wazuh updates
  Compatibility between the Wazuh agent and the Wazuh manager is guaranteed when the Wazuh manager version is later than or equal to that of the Wazuh agent. Therefore, we recommend disabling the Wazuh repository to prevent accidental upgrades. To do so, use the following command:

YUM:

```
sed -i "s/^enabled=1/enabled=0/" /etc/yum.repos.d/wazuh.repo
```

APT:

```
sed -i "s/^deb/#deb/" /etc/apt/sources.list.d/wazuh.list
apt-get update
```

Alternatively, you can set the package state to `hold`. This action stops updates but you can still upgrade it manually using `apt-get install`.

```
echo "wazuh-agent hold" | dpkg --set-selections
```

ZYpp:

```
sed -i "s/^enabled=1/enabled=0/" /etc/zypp/repos.d/wazuh.repo
```

Solaris

Aracı, izlemek istediğiniz ana bilgisayarda çalışır ve Wazuh yöneticisiyle iletişim kurarak şifrelenmiş ve kimliği doğrulanmış bir kanal üzerinden neredeyse gerçek zamanlı olarak veri gönderir.

Kurulum sürecini başlatmak için mimarinizi seçin: i386 veya SPARC.

> Not: Aşağıda açıklanan tüm komutları çalıştırmak için root kullanıcı ayrıcalıklarına ihtiyacınız var.

i386

Solaris Intel sürümünüzü seçin.

Solaris 10

1. Solaris 10 i386 paketi için Wazuh aracısını indirin .
2. Wazuh aracısını yükleyin.

```
pkgadd -d wazuh-agent_v4.9.2-sol10-i386.pkg wazuh-agent
```

Solaris 11

1. Solaris 11 i386 için Wazuh aracısını indirin .
2. Wazuh aracısını yükleyin.

```
pkg install -g wazuh-agent_v4.9.2-sol11-i386.p5p wazuh-agent
```

Paketi yüklemek istediğiniz Solaris 11 bölgesinin alt bölgeleri varsa, Wazuh aracısını yüklemek için bir depo oluşturun:

- ```
  pkg set-publisher -g wazuh-agent_v4.9.2-sol11-i386.p5p wazuh && pkg install --accept wazuh-agent && pkg unset-publisher wazuh
  ```
  ```

SPARC

Solaris SPARC sürümünüzü seçin.

Solaris 10

1. Solaris 10 SPARC paketi için Wazuh aracısını indirin .
2. Wazuh aracısını yükleyin.

```
pkgadd -d wazuh-agent_v4.9.2-sol10-sparc.pkg wazuh-agent
```

Solaris 11

1. Solaris 11 SPARC için Wazuh aracısını indirin .
2. Wazuh aracısını yükleyin.

```
pkg install -g wazuh-agent_v4.9.2-sol11-sparc.p5p wazuh-agent
```

Paketi yüklemek istediğiniz Solaris 11 bölgesinin alt bölgeleri varsa, Wazuh aracısını yüklemek için bir depo oluşturun:

- ```
  pkg set-publisher -g wazuh-agent_v4.9.2-sol11-sparc.p5p wazuh && pkg install --accept wazuh-agent && pkg unset-publisher wazuh
  ```

Kurulum süreci artık tamamlandı ve Wazuh aracısı Solaris uç noktanıza başarıyla kuruldu. Bir sonraki adım, aracıyı Wazuh sunucusuyla iletişim kuracak şekilde kaydetmek ve yapılandırmaktır.

Bu işlemi gerçekleştirmek için Wazuh aracısı kayıt bölümüne bakın.
  ```

AIX

Aracı, izlemek istediğiniz uç noktada çalışır ve Wazuh sunucusuyla iletişim kurarak şifrelenmiş ve kimliği doğrulanmış bir kanal üzerinden neredeyse gerçek zamanlı olarak veri gönderir.

Bir Wazuh aracısının AIX sistemine dağıtımı, aracı yükleme, kaydetme ve yapılandırma görevini kolaylaştıran dağıtım değişkenlerini kullanır.

> Not: Aşağıda açıklanan tüm komutları çalıştırabilmek için root kullanıcı ayrıcalıklarına sahip olmanız gerekir.
> **Gerekli Bağımlılıklar:**
> vuruş

1. Dağıtım sürecini başlatmak için AIX yükleyicisini indirin .
2. Wazuh aracısını uç noktanıza dağıtmak için `WAZUH_MANAGER`değişkeni Wazuh yöneticisi IP adresini veya ana bilgisayar adını içerecek şekilde düzenleyin.

   ```
   WAZUH_MANAGER="10.0.0.2" rpm -ivh wazuh-agent-4.9.2-1.aix.ppc.rpm
   ```

   Aracı adı, aracı grubu ve kayıt parolası gibi ek dağıtım seçenekleri için AIX için dağıtım değişkenleri bölümüne bakın.

   > Not: Alternatif olarak, bir aracıyı kaydetmeden yüklemek istiyorsanız, dağıtım değişkenlerini atlayın. Farklı kayıt yöntemleri hakkında daha fazla bilgi edinmek için Wazuh aracı kayıt bölümüne bakın.

3. Kurulum sürecini tamamlamak için Wazuh aracısını başlatın.

   ```
   /var/ossec/bin/wazuh-control start
   ```

Dağıtım işlemi artık tamamlandı ve Wazuh aracısı AIX uç noktanızda başarıyla çalışıyor.

HP-UX

Yüklenen aracı, izlemek istediğiniz uç noktada çalışır ve Wazuh sunucusuyla iletişim kurarak şifrelenmiş ve kimliği doğrulanmış bir kanal üzerinden neredeyse gerçek zamanlı olarak veri gönderir.

> Not: Aşağıda açıklanan tüm komutları çalıştırabilmek için root kullanıcı ayrıcalıklarına sahip olmanız gerekir.

1. Kurulum sürecini başlatmak için HP-UX yükleyicisini indirin .
2. Kullanıcıyı ve grubu oluşturun `wazuh`.

```
groupadd wazuh
useradd -G wazuh wazuh
```

3. Paketi içindeki sıkıştırmayı açın `/`.

```
gzip -d wazuh-agent-4.9.2-1-hpux-11v3-ia64.tar.gz
tar -xvf wazuh-agent-4.9.2-1-hpux-11v3-ia64.tar
```

Kurulum süreci artık tamamlandı ve Wazuh aracısı HP-UX uç noktanıza başarıyla kuruldu. Bir sonraki adım, aracıyı Wazuh sunucusuyla iletişim kuracak şekilde kaydetmek ve yapılandırmaktır. Bu işlemi gerçekleştirmek için, Linux/Unix aracı kaydı aracı yapılandırması bölümüne bakın. Aracı kaydı hakkında daha fazla bilgi edinmek için Wazuh aracı kaydı sayfasını ziyaret edin .

Paket Listesi

Bu indirme sayfası Wazuh kurulumu için gerekli paketleri içermektedir.

Wazuh indexer

Package type	Package
RPM	wazuh-indexer-4.9.2-1.x86_64.rpm (sha512)
DEB	wazuh-indexer_4.9.2-1_amd64.deb (sha512)

Wazuh server

Wazuh manager

Distribution	Version	Architecture	Package
Amazon Linux	1 and later	x86_64	wazuh-manager-4.9.2-1.x86_64.rpm (sha512)
		aarch64	wazuh-manager-4.9.2-1.aarch64.rpm (sha512)
CentOS	7 and later	x86_64	wazuh-manager-4.9.2-1.x86_64.rpm (sha512)
		aarch64	wazuh-manager-4.9.2-1.aarch64.rpm (sha512)
Debian	8 and later	x86_64	wazuh-manager_4.9.2-1_amd64.deb (sha512)
		aarch64	wazuh-manager_4.9.2-1_arm64.deb (sha512)
Fedora	22 and later	x86_64	wazuh-manager-4.9.2-1.x86_64.rpm (sha512)

Distribution	Version	Architecture	Package
aarch64	wazuh-manager-4.9.2-1.aarch64.rpm (sha512)		
OpenSUSE	42 and later	x86_64	wazuh-manager-4.9.2-1.x86_64.rpm (sha512)
		aarch64	wazuh-manager-4.9.2-1.aarch64.rpm (sha512)
Oracle Linux	7 and later	x86_64	wazuh-manager-4.9.2-1.x86_64.rpm (sha512)
		aarch64	wazuh-manager-4.9.2-1.aarch64.rpm (sha512)
Red Hat Enterprise Linux	7 and later	x86_64	wazuh-manager-4.9.2-1.x86_64.rpm (sha512)
		aarch64	wazuh-manager-4.9.2-1.aarch64.rpm (sha512)
SUSE	12	x86_64	wazuh-manager-4.9.2-1.x86_64.rpm (sha512)
		aarch64	wazuh-manager-4.9.2-1.aarch64.rpm (sha512)
Ubuntu	13 and later	x86_64	wazuh-manager_4.9.2-1_amd64.deb (sha512)
		aarch64	wazuh-manager_4.9.2-1_arm64.deb (sha512)
Raspbian OS	Buster and later	aarch64	wazuh-manager_4.9.2-1_arm64.deb (sha512)

Filebeat

Package type	Package
RPM	filebeat-oss-7.10.2-x86_64.rpm (sha512)
DEB	filebeat-oss-7.10.2-amd64.deb (sha512)

Wazuh dashboard

Package type	Package
RPM	wazuh-dashboard-4.9.2-1.x86_64.rpm (sha512)
DEB	wazuh-dashboard_4.9.2-1_amd64.deb (sha512)

Wazuh agent

Linux

Distribution	Version	Architecture	Package
Amazon Linux	1 and later	x86_64	wazuh-agent-4.9.2-1.x86_64.rpm (sha512)
		aarch64	wazuh-agent-4.9.2-1.aarch64.rpm (sha512)
CentOS	6 and later	i386	wazuh-agent-4.9.2-1.i386.rpm (sha512)
		x86_64	wazuh-agent-4.9.2-1.x86_64.rpm (sha512)
		aarch64	wazuh-agent-4.9.2-1.aarch64.rpm (sha512)
		armhf	wazuh-agent-4.9.2-1.armv7hl.rpm (sha512)
	5	i386	wazuh-agent-4.9.2-1.el5.i386.rpm (sha512)
		x86_64	wazuh-agent-4.9.2-1.el5.x86_64.rpm (sha512)
Debian	7 and later	i386	wazuh-agent_4.9.2-1_i386.deb (sha512)
		x86_64	wazuh-agent_4.9.2-1_amd64.deb (sha512)

Distribution	Version	Architecture	Package
aarch64	wazuh-agent_4.9.2-1_arm64.deb (sha512)		
armhf	wazuh-agent_4.9.2-1_armhf.deb (sha512)		
Fedora	22 and later	i386	wazuh-agent-4.9.2-1.i386.rpm (sha512)
		x86_64	wazuh-agent-4.9.2-1.x86_64.rpm (sha512)
		aarch64	wazuh-agent-4.9.2-1.aarch64.rpm (sha512)
		armhf	wazuh-agent-4.9.2-1.armv7hl.rpm (sha512)
OpenSUSE	42 and later	i386	wazuh-agent-4.9.2-1.i386.rpm (sha512)
		x86_64	wazuh-agent-4.9.2-1.x86_64.rpm (sha512)
		aarch64	wazuh-agent-4.9.2-1.aarch64.rpm (sha512)
		armhf	wazuh-agent-4.9.2-1.armv7hl.rpm (sha512)
Oracle Linux	6 and later	i386	wazuh-agent-4.9.2-1.i386.rpm (sha512)
		x86_64	wazuh-agent-4.9.2-1.x86_64.rpm (sha512)
		aarch64	wazuh-agent-4.9.2-1.aarch64.rpm (sha512)
	5	i386	wazuh-agent-4.9.2-1.el5.i386.rpm (sha512)
		x86_64	wazuh-agent-4.9.2-1.el5.x86_64.rpm (sha512)
Red Hat Enterprise Linux	6 and later	i386	wazuh-agent-4.9.2-1.i386.rpm (sha512)

Distribution	Version	Architecture	Package
x86_64	wazuh-agent-4.9.2-1.x86_64.rpm (sha512)		
aarch64	wazuh-agent-4.9.2-1.aarch64.rpm (sha512)		
5	i386	wazuh-agent-4.9.2-1.el5.i386.rpm (sha512)	
	x86_64	wazuh-agent-4.9.2-1.el5.x86_64.rpm (sha512)	
SUSE	12	i386	wazuh-agent-4.9.2-1.i386.rpm (sha512)
		x86_64	wazuh-agent-4.9.2-1.x86_64.rpm (sha512)
		aarch64	wazuh-agent-4.9.2-1.aarch64.rpm (sha512)
		armhf	wazuh-agent-4.9.2-1.armv7hl.rpm (sha512)
	11	i386	wazuh-agent-4.9.2-1.el5.i386.rpm (sha512)
		x86_64	wazuh-agent-4.9.2-1.el5.x86_64.rpm (sha512)
Ubuntu	12 and later	i386	wazuh-agent_4.9.2-1_i386.deb (sha512)
		x86_64	wazuh-agent_4.9.2-1_amd64.deb (sha512)
		aarch64	wazuh-agent_4.9.2-1_arm64.deb (sha512)
		armhf	wazuh-agent_4.9.2-1_armhf.deb (sha512)
Raspbian OS	Buster and later	aarch64	wazuh-agent_4.9.2-1_arm64.deb (sha512)
		armhf	wazuh-agent_4.9.2-1_armhf.deb (sha512)

Windows

Version	Architecture	Package
XP or later	32/64bits	wazuh-agent-4.9.2-1.msi (sha512)

macOS

Architecture	Package
Intel	wazuh-agent-4.9.2-1.intel64.pkg (sha512)
Apple silicon	wazuh-agent-4.9.2-1.arm64.pkg (sha512)

Solaris

Version	Architecture	Package
10	i386	wazuh-agent_v4.9.2-sol10-i386.pkg (sha512)
	SPARC	wazuh-agent_v4.9.2-sol10-sparc.pkg (sha512)
11	i386	wazuh-agent_v4.9.2-sol11-i386.p5p (sha512)
	SPARC	wazuh-agent_v4.9.2-sol11-sparc.p5p (sha512)

AIX

Version	Architecture	Package
6.1 or greater	PowerPC	wazuh-agent-4.9.2-1.aix.ppc.rpm (sha512)

HP-UX

Version	Architecture	Package
11.31	Itanium	wazuh-agent-4.9.2-1-hpux-11v3-ia64.tar.gz (sha512)

Wazuh'u Kaldırma

Wazuh Merkezi Bileşenlerinin Kaldırılması

Wazuh merkezi bileşenlerinin kaldırılması

Wazuh kurulum yardımcısını kullanarak tüm Wazuh merkezi bileşenlerini kaldırabilirsiniz .

Asistanı aşağıdaki gibi `-u`veya seçeneğiyle çalıştırın :`--uninstall`

```
sudo bash wazuh-install.sh --uninstall
```

Bu işlem Wazuh indeksleyicisini, Wazuh sunucusunu ve Wazuh panosunu kaldıracaktır.

Belirli bir merkezi bileşeni kaldırmak istiyorsanız aşağıdaki talimatları izleyin.

> **Not**: Aşağıda açıklanan tüm komutları çalıştırmak için root kullanıcı ayrıcalıklarına ihtiyacınız var.

Wazuh panosunu kaldırın

1. Wazuh gösterge paneli kurulumunu kaldırın.
   YUM:

   ```
   yum remove wazuh-dashboard -y
   rm -rf /var/lib/wazuh-dashboard/
   rm -rf /usr/share/wazuh-dashboard/
   rm -rf /etc/wazuh-dashboard/
   ```

   APT:

```
apt-get remove --purge wazuh-dashboard -y
```

Wazuh sunucusunu kaldırın

1. Wazuh yöneticisi kurulumunu kaldırın.
   YUM:

   ```
   yum remove wazuh-manager -y
   rm -rf /var/ossec/
   ```

   APT:

   ```
   apt-get remove --purge wazuh-manager -y
   ```

2. Wazuh yönetici hizmetini devre dışı bırakın.
   Sistemd:

   ```
   systemctl disable wazuh-manager
   systemctl daemon-reload
   ```

   SyssV init:

   1. Choose one option according to your operating system.
      1. RPM-based operating systems:

         ```
         chkconfig wazuh-manager off
         chkconfig --del wazuh-manager
         ```

      2. Debian-based operating systems:

         ```
         update-rc.d -f wazuh-manager remove
         ```

3. Filebeat kurulumunu kaldırın.

YUM:

```
yum remove filebeat -y
rm -rf /var/lib/filebeat/
rm -rf /usr/share/filebeat/
rm -rf /etc/filebeat/
```

APT:

```
apt-get remove --purge filebeat -y
```

Wazuh dizinleyicisini kaldırın

1. Wazuh indeksleyici kurulumunu kaldırın.

YUM:

```
yum remove wazuh-indexer -y
rm -rf /var/lib/wazuh-indexer/
rm -rf /usr/share/wazuh-indexer/
rm -rf /etc/wazuh-indexer/
```

APT:

```
apt-get remove --purge wazuh-indexer -y
```

Wazuh Agent Kaldırma

Wazuh aracısını kaldırma

Bu bölümde, aşağıdaki farklı işletim sistemlerine yüklenen Wazuh aracılarının nasıl kaldırılacağı açıklanmaktadır:

- Linux
- Windows
- macOS
- Solaris
- AIX
- HPUX

Bir Linux Wazuh aracısını kaldırma

Bir Linux aracısını kaldırmak için aşağıdaki komutları çalıştırın.

1. Wazuh aracı kurulumunu kaldırın.

YUM:

```
yum remove wazuh-agent
```

Bazı dosyalar yapılandırma dosyaları olarak işaretlenmiştir. Bu tanımlamadan dolayı, paket yöneticisi bu dosyaları dosya sisteminden kaldırmaz. `/var/ossec/`Tüm dosyaları tamamen kaldırmak istiyorsanız klasörü silin.

APT:

```
apt-get remove wazuh-agent
```

Bazı dosyalar yapılandırma dosyaları olarak işaretlenmiştir. Bu tanımlama nedeniyle, paket yöneticisi bu dosyaları dosya sisteminden kaldırmaz. Tüm dosyaları tamamen kaldırmak istiyorsanız aşağıdaki komutu çalıştırın

```
# apt-get remove --purge wazuh-agent
```

Zypp:

```
zypper remove wazuh-agent
```

Bazı dosyalar yapılandırma dosyaları olarak işaretlenmiştir. Bu tanımlamadan dolayı, paket yöneticisi bu dosyaları dosya sisteminden kaldırmaz. `/var/ossec/`Tüm dosyaları tamamen kaldırmak istiyorsanız klasörü silin.

2. Wazuh aracı hizmetini devre dışı bırakın.

Systemd:

```
systemctl disable wazuh-agent
systemctl daemon-reload
```

SysV init:

İşletim sisteminize göre bir seçenek seçin.

1. RPM tabanlı işletim sistemleri:

```
chkconfig wazuh-agent off
chkconfig --del wazuh-agent
```

2. Debian tabanlı işletim sistemleri:

```
update-rc.d -f wazuh-agent remove
```

No Service Manager:

> Herhangi bir işlem yapmanıza gerek yok

Wazuh aracısı artık Linux uç noktanızdan tamamen kaldırıldı

Windows Wazuh aracısını kaldırma

Aracı kaldırmak için, gözetimsiz işlemi gerçekleştirmek üzere orijinal Windows yükleyici dosyası gereklidir:

```
msiexec.exe /x wazuh-agent-4.9.2-1.msi /qn
```

Wazuh aracısı artık Windows uç noktanızdan tamamen kaldırıldı.

macOS Wazuh aracısını kaldırma

Wazuh aracısını macOS uç noktanızdan kaldırmak için şu adımları izleyin

1. Wazuh acente hizmetini durdurun.

```
# /Library/Ossec/bin/wazuh-control stop
```

2. Klasörü kaldırın `/Library/Ossec/`

```
/bin/rm -r /Library/Ossec
```

3. Kaldır `launchdaemons`ve `StartupItems`

```
/bin/rm -f /Library/LaunchDaemons/com.wazuh.agent.plist
/bin/rm -rf /Library/StartupItems/WAZUH
```

4. Wazuh kullanıcısını ve grubunu kaldırın

```
/usr/bin/dscl . -delete "/Users/wazuh"
/usr/bin/dscl . -delete "/Groups/wazuh"
```

5. Şuradan kaldır `pkgutil`:

```
/usr/sbin/pkgutil --forget com.wazuh.pkg.wazuh-agent
```

Wazuh aracısı artık macOS uç noktanızdan tamamen kaldırıldı.

Solaris Wazuh aracısını kaldırma

Kaldırmak istediğiniz Solaris sürümünü seçin.

Solaris 10:

Solaris 10'da Wazuh aracısını kaldırmak için aşağıdaki komutu çalıştırın.

```
# pkgrm wazuh-agent
```

Solaris 11:

Solaris 11'de Wazuh aracısını kaldırmak için aşağıdaki komutu çalıştırın

```
/var/ossec/bin/wazuh-control stop
pkg uninstall wazuh-agent
```

> **Not:** `wazuh`Solaris 11.4 veya sonraki sürümlerde Wazuh aracısını kaldırırsanız, Solaris 11 paket yöneticisi grubu sistemden kaldırmaz . Manuel olarak kaldırmak için komutu çalıştırın.`groupdel wazuh`

Wazuh aracısı artık Solaris uç noktanızdan tamamen kaldırıldı.

Bir AIX Wazuh aracısını kaldırma

Wazuh aracısını AIX uç noktasından kaldırmak için aşağıdaki adımları izleyin.

```
rpm -e wazuh-agent
```

Bazı dosyalar paket yöneticisi tarafından dosya sisteminden kaldırılmaz. `/var/ossec/`Tüm dosyaları tamamen kaldırmak istiyorsanız klasörü silin.

Wazuh aracısı artık AIX sisteminizden tamamen kaldırıldı

HP-UX Wazuh aracısını kaldırma

Wazuh aracısını HP-UX uç noktasından kaldırmak için aşağıdaki adımları izleyin.

1. Wazuh acente hizmetini durdurun.

```
/var/ossec/bin/wazuh-control stop
```

2. `wazuh`Kullanıcı ve grubu sil

```
groupdel wazuh
userdel wazuh
```

3. Wazuh dosyalarını kaldırın.

```
rm -rf /var/ossec
```

Wazuh aracısı artık HP-UX uç noktanızdan tamamen kaldırıldı.