Wazuh Agent

- Windows
- macOS
- Linux
- Solaris
- AIX
- HP-UX

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 .