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
```

Revision #2
Created 11 December 2024 14:36:56 by Ayşegül Sarıkaya
Updated 11 December 2024 23:40:32 by Ayşegül Sarıkaya