Wazuh Yöneticisini Kaynaklardan Yükleme

Wazuh sunucusu, dağıtılan aracılardan alınan verileri toplar ve analiz eder. Wazuh yöneticisini, Wazuh API'sini ve Filebeat'i çalıştırır.

Wazuh yönetici paketi ve uyumlu ajan paketleri Paketler listesi bölümünden kontrol edilebilir veya indirilebilir .

Bağımlılıkları Yükleme

YUM

CentOS 7

```
yum update -y
yum install make gcc gcc-c++ policycoreutils-python automake autoconf libtool centos-release-scl openssl-devel wget bzip2 devtoolset-7 procps -y
curl -OL http://packages.wazuh.com/utils/gcc/gcc-9.4.0.tar.gz && tar xzf gcc-9.4.0.tar.gz  && cd gcc-9.4.0/ && ./contrib/download_prerequisites && ./configure --enable-languages=c,c++ --prefix=/usr --disable-multilib --disable-libsanitizer && make -j$(nproc) && make install && ln -fs /usr/bin/g++ /bin/c++ && ln -fs /usr/bin/gcc /bin/cc && cd .. && rm -rf gcc-* && scl enable devtoolset-7 bash
```

CMake 3.18 kurulumu.

```
curl -OL https://packages.wazuh.com/utils/cmake/cmake-3.18.3.tar.gz && tar -zxf cmake-3.18.3.tar.gz && cd cmake-3.18.3 && ./bootstrap --no-system-curl && make -j$(nproc) && make install
cd .. && rm -rf cmake-*
```

CentOS 8

```
yum install make cmake gcc gcc-c++ python3 python3-policycoreutils automake autoconf libtool openssl-devel yum-utils procps -y
curl -OL http://packages.wazuh.com/utils/gcc/gcc-9.4.0.tar.gz && tar xzf gcc-9.4.0.tar.gz  && cd gcc-9.4.0/ &&
```

```
./contrib/download_prerequisites && ./configure --enable-languages=c,c++ --prefix=/usr --disable-multilib --disable-libsanitizer && make -j$(nproc) && make install && ln -fs /usr/bin/g++ /bin/c++ && ln -fs /usr/bin/gcc /bin/cc && cd .. && rm -rf gcc-* && scl enable devtoolset-7 bash
yum-config-manager --enable powertools
yum install libstdc++-static -y
```

Kaynaklardan isteğe bağlı CMake 3.18 kurulumu

```
curl -OL https://packages.wazuh.com/utils/cmake/cmake-3.18.3.tar.gz && tar -zxf cmake-3.18.3.tar.gz && cd cmake-3.18.3 && ./bootstrap --no-system-curl && make -j$(nproc) && make install
cd .. && rm -rf cmake-*
export PATH=/usr/local/bin:$PATH
```

APT

```
apt-get update
apt-get install python gcc g++ make libc6-dev curl policycoreutils automake autoconf libtool libssl-dev procps
```

CMake 3.18 kurulumu.

```
curl -OL https://packages.wazuh.com/utils/cmake/cmake-3.18.3.tar.gz && tar -zxf cmake-3.18.3.tar.gz && cd cmake-3.18.3 && ./bootstrap --no-system-curl && make -j$(nproc) && make install
cd .. && rm -rf cmake-*
```

İsteğe bağlı: Aşağıdaki bağımlılıkları yalnızca CPython'u kaynaklardan derlerken yükleyin. v4.2.0'dan beri, yüklenmeye hazır taşınabilir bir CPython sürümü indirecektir. Yine de, 'yi çalıştırırken bayrağı ekleyerek CPython kaynaklarını indirebilirsiniz .`make deps TARGET=server PYTHON_SOURCE`make deps

Python yorumlayıcısını derlemek için gereken bağımlılıkları yüklemek için şu adımları izleyin:

Yum

```
yum install epel-release yum-utils -y
yum-builddep python34 -y
```

APT

```
echo "deb-src http://archive.ubuntu.com/ubuntu $(lsb_release -cs) main" >> /etc/apt/sources.list
apt-get update
apt-get build-dep python3 -y
```

> Not: Önceki komuttan alınan Python sürümü, ikili dosyaları derlemek için kullanılan işletim sistemine bağlı olarak değişebilir. Daha fazla bilgi için Bağımlılıkları yükleyin .

Wazuh yYöneticisinin Kurulumu

1. En son sürümü indirin ve çıkarın:

   ```
   curl -Ls https://github.com/wazuh/wazuh/archive/v4.9.2.tar.gz | tar zx
   cd wazuh-4.9.2
   ```

2. Daha önce başka bir platform için derleme yaptıysanız, Makefile'ı kullanarak derlemeyi temizleyin `src/`:

   ```
   make -C src clean
   make -C src clean-deps
   ```

3. Betiği çalıştırın `install.sh`. Bu, Wazuh kaynaklarını kullanarak kurulum sürecinde size rehberlik edecek bir sihirbaz görüntüler:

   > Uyarı: Veritabanı çıktısını etkinleştirmek istiyorsanız, kurulum betiğini çalıştırmadan önce bu bölümü inceleyin.

   ```
   ./install.sh
   ```

   İlk çalıştırma, güvenlik açığı algılama içeriğini indirip işlediği için biraz zaman alabilir . Bu süreci hızlandırmak için `DOWNLOAD_CONTENT`ortam değişkenini önceden olarak ayarlayabilirsiniz `y`. Ayarlanan komut, kurulum sırasında önceden hazırlanmış bir veritabanını indirir.

```
DOWNLOAD_CONTENT=y ./install.sh
```

4. Script size ne tür bir kurulum istediğinizi sorduğunda `manager`Wazuh yöneticisini kurmak için şunu yazın:

```
1- What kind of installation do you want (manager, agent, local, hybrid, or help)? manager
```

> Not: Kurulum sırasında kullanıcılar kurulum yolunu belirleyebilir. Çalıştırın `./install.sh` ve dili seçin, kurulum modunu olarak ayarlayın `manager`, ardından kurulum yolunu ( ) ayarlayın. Varsayılan kurulum yolu 'dir . Yaygın olarak kullanılan özel bir yol . olabilir .`Choose where to install Wazuh [/var/ossec]`/var/ossec/opt

> Uyarı: Varsayılandan farklı bir yol seçerseniz kritik bir kurulum dizini seçmemeye son derece dikkat edin. Dizin zaten mevcutsa, yükleyici dizini silmenizi veya Wazuh'u içine kurarak devam etmenizi isteyecektir.

5. Kurulum programı kurulumun sonunda Wazuh'u başlatmak isteyip istemediğinizi sorar. Eğer istemezseniz, daha sonra şu şekilde başlatabilirsiniz:

Systemd

```
systemctl start wazuh-manager
```

SysV Başlatma

```
service wazuh-manager start
```

Diğer Wazuh Bileşenlerinin Kurulumu

Wazuh yöneticisi kaynaklardan yüklendikten sonra Kurulum kılavuzunu izleyerek Wazuh indeksleyicisini, Filebeat'i ve Wazuh panosunu yükleyebilirsiniz .

Kaldır

1. Wazuh yöneticisini kaldırmak için `WAZUH_HOME`geçerli kurulum yolunu ayarlayın:

```
WAZUH_HOME="/WAZUH/INSTALLATION/PATH"
```

2. Hizmeti durdurun:

```
service wazuh-manager stop 2> /dev/null
```

3. Daemon'u durdurun:

```
$WAZUH_HOME/bin/wazuh-control stop 2> /dev/null
```

4. Kurulum klasörünü ve tüm içeriğini kaldırın:

```
rm -rf $WAZUH_HOME
```

5. Hizmeti silin:

Systemd

```
find /etc/systemd/system -name "wazuh*" | xargs rm -f
systemctl daemon-reload
```

SysV Başlatma

```
[ -f /etc/rc.local ] && sed -i'' '/wazuh-control start/d' /etc/rc.local
find /etc/{init.d,rc*.d} -name "*wazuh*" | xargs rm -f
```

6. Wazuh kullanıcı ve grubunu kaldır:

```
userdel wazuh 2> /dev/null
groupdel wazuh 2> /dev/null
```

Revision #11
Created 25 December 2024 23:55:35 by Ayşegül Sarıkaya
Updated 27 December 2024 22:33:36 by Ayşegül Sarıkaya