Wazuh Aracısını Kaynaklardan Yükleme - Linux

> Not: Aşağıda açıklanan tüm komutları çalıştırmak için kök kullanıcı ayrıcalıklarına ihtiyacınız var. Wazuh 3.5'ten beri, bu işlemi takip ederken bir İnternet bağlantısına sahip olmak gerekir.

> Not: CMake 3.12.4, Wazuh aracı çözümünü derlemek için gereken en düşük kütüphane sürümüdür.

> Not: GCC 9.4, Wazuh aracı çözümünü derlemek için gereken en düşük derleyici sürümüdür.

1. Geliştirme araçlarını ve derleyicileri kurun. Linux'ta bu, dağıtımınızın paket yöneticisini kullanarak kolayca yapılabilir:

   Yum

   CentOS 6/7

   ```
   yum update -y
   yum install make gcc gcc-c++ policycoreutils-python automake autoconf libtool centos-release-scl openssl-devel wget bzip2 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 /bin/g++ /usr/bin/c++ && ln -fs /bin/gcc /usr/bin/cc && cd .. && rm -rf gcc-*
   ```

   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 gcc gcc-c++ python3 python3-policycoreutils automake autoconf libtool openssl-devel cmake 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 /bin/g++ /usr/bin/c++ && ln -fs /bin/gcc /usr/bin/cc && cd .. && rm -rf gcc-*
yum-config-manager --enable powertools
yum install libstdc++-static -y
```

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 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-*
```

ZYpp

```
zypper install -y make gcc gcc-c++ policycoreutils-python automake autoconf libtool libopenssl-devel curl
```

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-*
```

> Not: Suse 11 için bazı araçların paket yöneticisinde bulunmaması mümkün olabilir, bu durumda aşağıdaki resmi depoları ekleyebilirsiniz:

```
zypper addrepo http://download.opensuse.org/distribution/11.4/repo/oss/ oss
```

Pacman

Wazuh'u derlemek için önerilen sürüm GCC/G++ 9.4'tür.

```
pacman --noconfirm -Syu curl gcc make sudo wget expect gnupg perl-base perl fakeroot python brotli automa
```

2. En son sürümü indirin ve çıkarın:

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

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

```
cd wazuh-4.9.2
./install.sh
```

Daha önce başka bir platform için derleme yaptıysanız, Makefile'ı kullanarak derlemeyi temizlemelisiniz `src`:

```
cd wazuh-4.9.2
make -C src clean
make -C src clean-deps
```

>

> Not: Kurulum sırasında kullanıcılar kurulum yolunu belirleyebilir. Çalıştırın `./install.sh` ve dili seçin, kurulum modunu olarak ayarlayın `agent`, ardından kurulum yolunu (. `Choose where to install Wazuh [/var/ossec]`) ayarlayın. Varsayılan kurulum yolu `/var/ossec` 'dir . Yaygın olarak kullanılan özel bir yol `/opt` olabilir . Varsayılandan farklı bir yol seçerken, dizin zaten mevcutsa, yükleyici dizini silmeyi veya içine Wazuh'u yüklemeyi isteyecektir. Ayrıca gözetimsiz bir kurulum da çalıştırabilirsiniz.

4. Komut dosyası ne tür bir kurulum istediğinizi soracaktır. Wazuh aracısını kurmak için aracı yazın:

   Output

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

Sonraki adımlar

Artık aracı yüklendiğine göre, bir sonraki adım aracı Wazuh sunucusuna kaydetmektir. Bu süreç hakkında daha fazla bilgi için lütfen Wazuh aracı kayıt bölümünü kontrol edin.

Kaldır

Wazuh aracısını kaldırmak için WAZUH_HOME'u geçerli yükleme yoluyla ayarlayın:

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

Hizmeti durdurun:

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

Daemon'u durdurun:

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

Kurulum klasörünü ve tüm içeriğini kaldırın:

```
rm -rf $WAZUH_HOME
```

Hizmeti silin:

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
```

Systemd

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

Wazuh kullanıcı ve grubunu kaldır:

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

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

Revision #14
Created 25 December 2024 23:56:03 by Ayşegül Sarıkaya
Updated 27 December 2024 22:33:01 by Ayşegül Sarıkaya