Wazuh Aracısını Kaynaklardan Yükleme - Solaris

Bu bölümde, aşağıdaki Solaris sürümleri için Wazuh aracısının kaynaklardan nasıl indirileceği ve oluşturulacağı açıklanmaktadır:

- Solaris i386 için
- Solaris SPARC için

Solaris 10

> Not: Aşağıda açıklanan tüm komutların root kullanıcı ayrıcalıklarıyla yürütülmesi gerekir. Wazuh 3.5'ten beri, bu işlemi takip ederken bir İnternet bağlantısına sahip olmak gerekir.

1. Geliştirme araçlarını ve derleyicileri kurun.

    1. Bash kabuğunu çalıştırın ve pkgutil'i yükleyin.

        ```
        bash
        PATH="${PATH}:/usr/sbin:/usr/bin:/usr/sbin/:/opt/csw/gnu/:/usr/sfw/bin/:/opt/csw/bin/"
        export PATH
        pkgadd -d http://get.opencsw.org/now
        ```

    2. Aşağıdaki araçları yükleyin:

        ```
        /opt/csw/bin/pkgutil -y -i git cmake automake autoconf gmake libtool wget curl gcc5core
        gcc5g++ gtar
        ```

    3. gcc/g++ 5.5 derleyicisini indirin ve derleyin:

```
curl -L http://packages.wazuh.com/utils/gcc/gcc-5.5.0.tar.gz | gtar xz && cd gcc-5.5.0
curl -L http://packages.wazuh.com/utils/gcc/mpfr-2.4.2.tar.bz2 | gtar xj && mv mpfr-2.4.2 mpfr
curl -L http://packages.wazuh.com/utils/gcc/gmp-4.3.2.tar.bz2 | gtar xj && mv gmp-4.3.2 gmp
curl -L http://packages.wazuh.com/utils/gcc/mpc-0.8.1.tar.gz | gtar xz && mv mpc-0.8.1 mpc
curl -L http://packages.wazuh.com/utils/gcc/isl-0.14.tar.bz2 | gtar xj && mv isl-0.14 isl
unset CPLUS_INCLUDE_PATH && unset LD_LIBRARY_PATH
export PATH=/usr/sbin:/usr/bin:/usr/ccs/bin:/opt/csw/bin
mkdir -p /usr/local
./configure --prefix=/usr/local/gcc-5.5.0 --enable-languages=c,c++ --disable-multilib --disable-libsanitizer --disable-bootstrap --with-ld=/usr/ccs/bin/ld --without-gnu-ld --with-gnu-as --with-as=/opt/csw/bin/gas
gmake && gmake install
export CPLUS_INCLUDE_PATH=/usr/local/gcc-5.5.0/include/c++/5.5.0
export LD_LIBRARY_PATH=/usr/local/gcc-5.5.0/lib
echo "export PATH=/usr/sbin:/usr/bin:/usr/ccs/bin:/opt/csw/bin" >> /etc/profile
echo "export CPLUS_INCLUDE_PATH=/usr/local/gcc-5.5.0/include/c++/5.5.0" >> /etc/profile
echo "export LD_LIBRARY_PATH=/usr/local/gcc-5.5.0/lib" >> /etc/profile
rm -rf gcc-*
ln -sf /usr/local/gcc-5.5.0/bin/g++ /usr/bin/g++
cd ..
```

> Not: Adımın `gmake` tamamlanması birkaç dakika sürecektir. Bu normal bir davranıştır.

4. cmake kütüphanesini kurun:

```
curl -sL http://packages.wazuh.com/utils/cmake/cmake-3.18.3.tar.gz | gtar xz
cd cmake-3.18.3
./bootstrap
gmake && gmake install
cd .. && rm -rf cmake-3.18.3
ln -sf /usr/local/bin/cmake /usr/bin/cmake
```

5. Perl 5.10.1'i indirin ve kurun.

```
wget http://www.cpan.org/src/5.0/perl-5.10.1.tar.gz
gunzip ./perl-5.10.1.tar.gz && tar xvf perl-5.10.1.tar
cd perl-5.10.1
./Configure -Dcc=gcc -d -e -s
gmake clean && gmake -d -s
gmake install -d -s
cd ..
```

6. Perl'in eski sürümünü kaldırıp yerine perl 5.10.1 sürümünü yükleyin.

```
rm /usr/bin/perl
mv /opt/csw/bin/perl5.10.1 /usr/bin/
mv /usr/bin/perl5.10.1 /usr/bin/perl
rm -rf perl-5.10.1*
```

2. Wazuh'un son sürümünü indirin.

```
/opt/csw/bin/git clone -b v4.9.2 https://github.com/wazuh/wazuh.git
```

3. Kaynakları derleyin.

- Solaris 10 i386 için:

```
export PATH=/usr/local/gcc-5.5.0/bin:/usr/sbin:/usr/bin:/usr/ccs/bin:/opt/csw/bin:/opt/csw/gnu
export CPLUS_INCLUDE_PATH=/usr/local/gcc-5.5.0/include/c++/5.5.0
export LD_LIBRARY_PATH=/usr/local/gcc-5.5.0/lib
cd wazuh/src
gmake clean
gmake deps TARGET=agent
gmake -j 4 TARGET=agent PREFIX=/var/ossec USE_SELINUX=no
cd ..
```

- Solaris 10 SPARC için:

```
export PATH=/usr/local/gcc-5.5.0/bin:/usr/sbin:/usr/bin:/usr/ccs/bin:/opt/csw/bin:/opt/csw/gnu
export CPLUS_INCLUDE_PATH=/usr/local/gcc-5.5.0/include/c++/5.5.0
export LD_LIBRARY_PATH=/usr/local/gcc-5.5.0/lib
cd wazuh/src
gmake clean
gmake deps TARGET=agent
```

```
gmake -j 4 TARGET=agent PREFIX=/var/ossec USE_SELINUX=no
cd ..
```

4. Shebang'i değiştirmek için solaris 10 sh dosyalarını yamalayın.

```
for file in $(find . -name "*.sh");do
sed 's:#!/bin/sh:#!/usr/xpg4/bin/sh:g' $file > $file.new
mv $file.new $file && chmod +x $file
done
```

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

```
bash install.sh
```

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

```
gmake -C src clean
gmake -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 .

6. Komut dosyası ne tür bir kurulum istediğinizi soracaktır. `agent`Wazuh aracısını kurmak için şunu 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` geçerli kurulum yolunu 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:

```
find /etc/{init.d,rc*.d} -name "*wazuh*" | xargs rm -f
```

Wazuh kullanıcı ve grubunu kaldır:

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

Solaris 11

> Not: Aşağıda açıklanan tüm komutların root kullanıcı ayrıcalıklarıyla yürütülmesi gerekir. Wazuh 3.5'ten beri, bu işlemi takip ederken bir İnternet bağlantısına sahip olmak gerekir.

Geliştirme araçlarını ve derleyicileri kurun.

1. Pkgutil'i kurun ve güncelleyin.

```
pkgadd -d http://get.opencsw.org/now
export PATH="${PATH}:/usr/sfw/bin:/opt/csw/bin:/opt/ccs/bin"
pkgutil -y -U
```

2. Python 2.7'yi kurun.

```
/opt/csw/bin/pkgutil -y -i python27
ln -sf /opt/csw/bin/python2.7 /usr/bin/python
```

3. Aşağıdaki araçları yükleyin:

```
/opt/csw/bin/pkgutil -y -i git gmake cmake gcc5core gcc5g++
```

4. Bir sonraki adımda ihtiyaç duyulacak tüm dosyaları içerecek şekilde bir gcc sürümü yükleyin:

```
# pkg install gcc-45
```

5. gcc/g++ 5.5 derleyicisini indirin ve derleyin:

```
curl -O https://packages.wazuh.com/utils/gcc/gcc-5.5.0.tar.gz && gtar xzf gcc-5.5.0.tar.gz
ln -sf gcc-5.5.0 gcc
cd gcc && ./contrib/download_prerequisites
cd .. && mkdir -p gcc-build && cd gcc-build
../gcc/configure --prefix=/usr/local/gcc-5.5.0 --enable-languages=c,c++ --disable-multilib --
disable-libsanitizer --disable-bootstrap --with-ld=/usr/ccs/bin/ld --without-gnu-ld --with-gnu-as --
with-as=/opt/csw/bin/gas
gmake
gmake install
export PATH=/usr/local/gcc-5.5.0/bin/:/usr/local/bin/:/usr/bin/:/usr/sbin/:$PATH
export CPLUS_INCLUDE_PATH=/usr/local/gcc-5.5.0/include/c++/5.5.0/
export LD_LIBRARY_PATH=/usr/local/gcc-5.5.0/lib/
cd ..
```

> Not: Adımın `gmake` tamamlanması birkaç dakika sürecektir. Bu normal bir davranıştır.

6. cmake kütüphanesini kurun:

```
curl -sL http://packages.wazuh.com/utils/cmake/cmake-3.18.3.tar.gz | gtar xz
cd cmake-3.18.3
./bootstrap
gmake && gmake install
cd .. && rm -rf cmake-3.18.3
ln -sf /usr/local/bin/cmake /usr/bin/cmake
```

2. En son sürümü indirin.

```
git clone -b v4.9.2 https://github.com/wazuh/wazuh.git
```

> Not: Eğer Open SSL hatası nedeniyle dosyayı indiremiyorsanız, scp yardımcı programını kullanarak dizini kopyalamanız gerekir.

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

```
cd wazuh*
./install.sh
```

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

```
gmake -C src clean
gmake -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 .

1. Komut dosyası ne tür bir kurulum istediğinizi soracaktır. Wazuh aracısını kurmak için şunu `agent` 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` geçerli kurulum yolunu 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:

```
find /etc/{init.d,rc*.d} -name "*wazuh*" | xargs rm -f
```

Wazuh kullanıcı ve grubunu kaldır:

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

Revision #15
Created 25 December 2024 23:57:20 by Ayşegül Sarıkaya
Updated 27 December 2024 23:11:30 by Ayşegül Sarıkaya