Wazuh Aracısını Kaynaklardan Yükleme - AIX

Aşağıdaki kurulum prosedürü için desteklenen sürüm AIX 6.1 TL9 veya üzeridir.

> 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. Aracı indirin `wget`.

      ```
      rpm -Uvh --nodeps http://packages-dev.wazuh.com/deps/aix/wget-1.19-1.aix6.1.ppc.rpm
      ```

   2. Aşağıdaki betiği indirin.

      ```
      wget https://raw.githubusercontent.com/wazuh/wazuh-packages/4.9/aix/generate_wazuh_packages.sh --no-check-certificate
      ```

      > Not: Eğer scripti bu şekilde indiremiyorsanız, o zaman başka bir makine kullanarak indirip scp yardımcı programını kullanarak AIX makinesine kopyalamalısınız.

   3. Bash ve libiconv'u indirin.

      ```
      rpm -Uvh --nodeps http://packages-dev.wazuh.com/deps/aix/bash-4.4-4.aix6.1.ppc.rpm
      rpm -Uvh --nodeps http://packages-dev.wazuh.com/deps/aix/libiconv-1.14-22.aix6.1.ppc.rpm
      ```

   4. Gerekli bağımlılıkları scripti kullanarak kurun.

      ```
      chmod +x generate_wazuh_packages.sh
      ./generate_wazuh_packages.sh -e
      ```

      >

> Not: Bu adım birkaç dakika sürebilir.

2. En son sürümü indirin.

```
wget -O wazuh.tar.gz --no-check-certificate https://api.github.com/repos/wazuh/wazuh/tarball/v4.9.2
gunzip -c wazuh.tar.gz | tar -xvf -
```

> Not: Eğer deponuzu bu şekilde indiremiyorsanız scp yardımcı programını kullanarak kopyalamalısınız.

3. Kaynakları derleyin.

```
cd wazuh-4.9.2
cd src
gmake clean-deps
gmake clean
gmake deps TARGET=agent RESOURCES_URL=http://packages.wazuh.com/deps/27
gmake TARGET=agent USE_SELINUX=no PREFIX=/var/ossec
```

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

```
cd ..
./install.sh
```

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

```
gmake -C src clean-deps
gmake -C src clean
```

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

5. Son olarak aşağıdaki yapılandırmayı uygulayın:

```
sed '/System inventory/,/^$/{/^$/!d;}' /var/ossec/etc/ossec.conf > /var/ossec/etc/ossec.conf.tmp
mv /var/ossec/etc/ossec.conf.tmp /var/ossec/etc/ossec.conf
```

> Not: Yukarıdaki komutların varsayılan kurulum yolu için yürütüldüğünü unutmayın `/var/ossec`. Aracı başka bir yola kurduysanız, bu komutların yolunu değiştirmeniz gerekecektir.

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/rc.d -name "*wazuh*" | xargs rm -f
```

Wazuh kullanıcı ve grubunu kaldır:

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

Revision #6
Created 25 December 2024 23:56:51 by Ayşegül Sarıkaya
Updated 26 December 2024 00:54:30 by Ayşegül Sarıkaya