Windows

Aracı, izlemek istediğiniz uç noktada çalışır ve Wazuh sunucusuyla iletişim kurarak şifrelenmiş ve kimliği doğrulanmış bir kanal aracılığıyla neredeyse gerçek zamanlı olarak veri gönderir. Windows XP'den Windows 11 ve Windows Server 2022 dahil olmak üzere en son mevcut sürümlere kadar Windows sistemlerinizi Wazuh ile izleyin.

> **Not:** Kurulumu gerçekleştirmek için yönetici ayrıcalıklarına sahip olmanız gerekmektedir.

1. Kurulum sürecini başlatmak için Windows yükleyicisini indirin .
2. İzlemek istediğiniz kurulum yöntemini seçin: komut satırı arayüzü (CLI) veya grafiksel kullanıcı arayüzü (GUI).

   CLI
   Wazuh aracısını uç noktanıza dağıtmak için komut kabuğu alternatiflerinden birini seçin ve `WAZUH_MANAGER`değişkeni Wazuh yöneticisi IP adresini veya ana bilgisayar adını içerecek şekilde düzenleyin.

   - CMD Kullanımı:

     ```
     wazuh-agent-4.9.2-1.msi /q WAZUH_MANAGER="10.0.0.2"
     ```

   - PowerShell Kullanımı:

     ```
     .\wazuh-agent-4.9.2-1.msi /q WAZUH_MANAGER="10.0.0.2"
     ```

   Aracı adı, aracı grubu ve kayıt parolası gibi ek dağıtım seçenekleri için Windows için Dağıtım değişkenleri bölümüne bakın.
   Kurulum süreci artık tamamlandı ve Wazuh aracısı başarıyla kuruldu ve yapılandırıldı. Wazuh aracısını GUI'den veya çalıştırarak başlatabilirsiniz:

   ```
   NET START Wazuh
   ```

   Başladıktan sonra Wazuh temsilcisi kayıt sürecini başlatacak ve yöneticiye kayıt yaptıracaktır.

   > 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.

Grafiksel Kullanıcı Arayüzü

Wazuh aracısını sisteminize yüklemek için Windows yükleyicisini çalıştırın ve yükleme sihirbazındaki adımları izleyin. Bazı istemleri nasıl yanıtlayacağınızdan emin değilseniz, varsayılan yanıtları kullanın. Yüklendikten sonra, aracı yapılandırma, günlük dosyasını açma ve hizmeti başlatma veya durdurma için bir GUI kullanır.

Windows aracı yöneticisi

Image not found or type unknown

Kurulum işlemi artık tamamlandı ve Wazuh aracısı Windows uç noktanıza başarıyla kuruldu. Bir sonraki adım, aracıyı Wazuh sunucusuyla iletişim kuracak şekilde kaydetmek ve yapılandırmaktır. Bu işlemi gerçekleştirmek için Wazuh aracısı kayıt bölümüne bakın.

Varsayılan olarak tüm aracı dosyaları kurulumdan sonra `C:\Program Files (x86)\ossec-agent` saklanır.

Revision #6
Created 6 December 2023 18:07:50 by LastGuard
Updated 23 December 2024 19:56:03 by Ayşegül Sarıkaya