Önerilen Kurulum

Aşağıdaki açıklama, iki Cuckoo makinesi, cuckoo0 ve cuckoo1 ile bir Dağıtılmış Cuckoo kurulumunu tasvir eder. Bu kurulumda ilk makine, cuckoo0, aynı zamanda Distributed Cuckoo REST API'yi barındırır.

- Konfigürasyon Ayarları
- Distributed Cuckoo Kurulumu
- Cuckoo Node Kaydetme

Konfigürasyon Ayarları

Kurulumumuz, yapılandırma dosyalarıyla ilgili birkaç güncelleme gerektirecektir.

conf/cuckoo.conf

`process_results`'ı kapatmak için güncelleme yapın, çünkü kendi sonuç işleme betiğimizi çalıştıracağız (performans nedenleriyle).

`tmppath`'i birkaç yüz ikili dosyayı depolamak için yeterli alan içeren bir şeye güncelleyin. Bazı sunucularda veya kurulumlarda /tmp kısıtlı bir alan içerebilir, bu yeterli olmayabilir.

Bağlantıyı sqlite3 kullanmak yerine başka bir şeyi kullanacak şekilde güncelleyin. Tercihen PostgreSQL veya MySQL. SQLite3 çoklu iş parçacıklı uygulamaları desteklemez ve bu nedenle Cuckoo gibi sistemler için iyi bir seçenek değildir (mevcut haliyle).

Dağıtılmış cuckoo kurulumu için özel bir veritabanı oluşturmalısınız. Veritabanı betikleriyle güncelleme sorunlarından kaçınmak için mevcut herhangi bir cuckoo veritabanını kullanmaktan kaçının. Yapılandırmada yeni veritabanı adını kullanın. Kullanıcı adları, sunucular vb. gibi kalan yapılandırmaları cuckoo kurulumunuz için aynı tutabilirsiniz. Her bir düğüm için bir DB ve Dağıtılmış Cuckoo'yu çalıştıran makine için bir tane kullanmayı unutmayın (bu "yönetim makinesi" veya "denetleyici" olarak adlandırılır).

conf/processing.conf

Virustotal gibi bazı process modüllerini devre dışı bırakmak isteyebilirsiniz.

conf/reporting.conf

Sisteminizle entegrasyon için hangi rapor(lar)ın gerekli olduğuna bağlı olarak, yalnızca kullanacağın rapor(lar)ı ayarlamak mantıklı olabilir. Böylece diğerlerini devre dışı bırakmak mantıklı olacaktır.

conf/virtualbox.conf

Varsayılan olarak Sanal Makine yöneticisi olarak VirtualBox'u seçmişseniz, modu başsız (headless) olarak değiştirmeniz gerekecek; aksi takdirde bazı sıkıntılarla karşılaşabilirsiniz.

Distributed Cuckoo Kurulumu

Distributed Cuckoo makinesinde Distributed Cuckoo REST API ve Distibuted Cuckoo Worker'ı kurmanız gerekecek.

Daha önce belirtildiği gibi, Distributed Cuckoo REST API, cuckoo distributed server komutunu çalıştırarak veya uWSGI ve nginx ile düzgün bir şekilde dağıtarak başlatılabilir.

Distributed Cuckoo Worker'ı, CWD'de (Cuckoo'yu arka planda çalıştırmak için Cuckoo'ya göre supervisord'ı önce başlatmayı unutmayın) supervisorctl start distributed komutuyla başlatılabilir. Bu, Worker'ı doğru yapılandırma ve argümanlarla otomatik olarak başlatacaktır.

Cuckoo Node Kaydetme

Hızlı kullanımda belirtildiği gibi, Cuckoo nodelarının Dağıtılmış Cuckoo REST API'sine kaydedilmesi gerekir:

```
$ curl http://localhost:9003/api/node -F name=cuckoo0 -F
url=http://localhost:8090/
$ curl http://localhost:9003/api/node -F name=cuckoo1 -F
url=http://1.2.3.4:8090/
```

Cuckoo nodelarını kaydettikten sonra yapmanız gereken tek şey, görevleri göndermek ve tamamlandığında raporları almak. Bu komutlar hakkındaki belgeleri Hızlı Kullanım bölümünde bulabilirsiniz. Cuckoo node `localhost`'ta değilse, `localhost`'u Cuckoo REST API'nin çalıştığı node'un IP adresiyle değiştirin.

Nodelar arasında yük dengelemesi yapmak istiyorsanız, `$CWD/distributed/settings.py` dosyasındaki `threshold` parametresi için daha düşük bir değeri denemek isteyebilirsiniz, çünkü varsayılan değer 500'dür (bu, görevlerin 500'lük gruplar halinde Cuckoo düğümlerine atanması anlamına gelir).