Yardımcı Programlar

Cuckoo, bir dizi yaygın görevi otomatikleştirmek için önceden oluşturulmuş yardımcı programlarla birlikte gelir. Bu yardımcı programlar başlangıçta utils/ dizininde bulunuyordu, ancak artık Cuckoo Apps'a taşındı.

- Cuckoo Apps
- Submission Utility
- Web Utility
- Processing Utility
- Community Download Utility
- Stats Utility
- Machine Utility
- Distributed Scriptleri
- Mac OS X Bootstrap Scriptleri

Cuckoo Apps

Bir Cuckoo App aslında sadece bir Cuckoo alt komutudur. Çeşitli Cuckoo App'leri bulunmaktadır, her biri kendi işlevselliğine sahiptir. Her Cuckoo App'ini aynı şekilde çağırabilirsiniz. İşte bazı örnekler:

```
$ cuckoo submit --help
$ cuckoo api --help
$ cuckoo clean --help
```

Bu örneklerde, belirli bir Cuckoo App için işlevselliği ve tüm kullanılabilir parametreleri gösteren `--help` parametresini sağladık.

Submission Utility

Analiz için örnekleri gönderir. Bu araç, Analiz bölümünde açıklanmıştır.

Web Utility

Cuckoo’nun web arayüzü. Bu araç, Web Arayüzü bölümünde açıklanmıştır.

Processing Utility

2.0.0 sürümünde değişiklik: ./utils/process.py'nin rastgele donma sorunları vardı ve ./utils/process2.py'nin yalnızca PostgreSQL tabanlı veritabanlarıyla başa çıkabilme sorunları vardı. Bu iki komut şimdi tek bir Cuckoo App içinde birleştirildi ve artık söz konusu sorunları veya kısıtlamaları göstermiyor.

Daha büyük Cuckoo kurulumları için performans sorunları (çoklu iş parçacığı ve Python GIL ile) nedeniyle sonuç işleme işlemini Cuckoo analizlerinden ayırmak önerilir. cuckoo process kullanarak Cuckoo raporlarını yeniden oluşturmak da mümkündür, bu genellikle Cuckoo İşleme modülleri, Cuckoo İmzaları ve Cuckoo Raporlama modüllerini geliştirirken ve hata ayıklarken kullanılır.

Bir veya daha fazla ayrı işlemde sonuçları işlemek için, `$CWD/conf/cuckoo.conf` dosyasındaki `process_results` yapılandırma öğesini off olarak ayarlayarak devre dışı bırakmanız gerekir. Daha sonra bir Cuckoo İşleme örneği başlatılmalıdır, bu aşağıdaki gibi yapılabilir:

```
$ cuckoo process instance1
```

Eğer gelen tüm analizleri yönetmek için bir Cuckoo İşleme örneği yeterli değilse, sadece ikinci, üçüncü ve mümkünse daha fazla örnek oluşturun:

```
$ cuckoo process instance2
```

Bir analiz görevinin Cuckoo raporunu yeniden oluşturmak için -r anahtarını kullanın:

```
$ cuckoo process -r 1
```

Aynı anda birden çok veya bir aralıktaki Cuckoo raporlarını yeniden oluşturmak da mümkündür. Aşağıdaki örnek, görevleri 1, 2, 5, 6, 7, 8, 9, 10 yeniden işleyecektir:

```
$ cuckoo process -r 1,2,5-10
```

Daha fazla bilgi için bu Cuckoo App hakkındaki yardımı da inceleyin:

```
```

```
$ cuckoo process --help
Usage: cuckoo process [OPTIONS] [INSTANCE]

  Process raw task data into reports.

Options:
  -r, --report TEXT       Re-generate one or more reports
  -m, --maxcount INTEGER  Maximum number of analyses to process
  --help                  Show this message and exit.
```

Community Download Utility

Bu Cuckoo App, Cuckoo Topluluk Deposu'ndan Cuckoo İmzalarını, en son izleme ikililerini ve diğer öğeleri indirir ve bunları CWD'nize kurar.

Cuckoo Topluluğu'ndan en son ve en iyi öğeleri almak için sadece aşağıdaki gibi bir komutu yürütün ve bitene kadar bekleyin - şu anda herhangi bir ilerleme göstergesi yoktur:

```
$ cuckoo community
```

Daha fazla kullanım için aşağıdakine bakın:

```
$ cuckoo community --help
Usage: cuckoo community [OPTIONS]

  Utility to fetch supplies from the Cuckoo Community.

Options:
  -f, --force              Overwrite existing files
  -b, --branch TEXT        Specify a different community branch rather than
                           master
  --file, --filepath PATH  Specify a local copy of a community .tar.gz file
  --help                   Show this message and exit.
```

Stats Utility

2.0-rc2 sürümünden itibaren kullanım dışı: Bu yardımcı program, bu bilgiyi hem Cuckoo API hem de Cuckoo Web Arayüzü aracılığıyla almak mümkün olduğu için Cuckoo App'e taşınmayacak.

Machine Utility

2.0.0 sürümünde değişiklik: Bu eskiden bağımsız ve düzensiz bir betikti ve doğrudan Cuckoo konfigürasyonunu değiştiriyordu. Şimdi çok daha iyi entegre edilmiş ve Cuckoo ile oldukça uygun bir şekilde etkileşim kurabilecek.

Machine Cuckoo App, Cuckoo'daki sanal makinelerin yapılandırmasını otomatikleştirmenize yardımcı olmak için tasarlanmıştır. Argüman olarak bir makine ayrıntısı listesi alır ve bunları `cuckoo.conf`'de etkinleştirilmiş olan makina modülü için belirtilen yapılandırma dosyasına yazar. İşte kullanılabilir seçenekler:

```
$ cuckoo machine --help
Usage: cuckoo machine [OPTIONS] VMNAME [IP]

Options:
  --debug              Enable verbose logging
  --add                Add a Virtual Machine
  --delete             Delete a Virtual Machine
  --platform TEXT      Guest Operating System
  --options TEXT       Machine options
  --tags TEXT          Tags for this Virtual Machine
  --interface TEXT     Sniffer interface for this Virtual Machine
  --snapshot TEXT      Specific Virtual Machine Snapshot to use
  --resultserver TEXT  IP:Port of the Result Server
  --help               Show this message and exit.
```

Örnek olarak, Cuckoo'nun yapılandırmasına aşağıdaki gibi bir makine eklenebilir:

```
$ cuckoo machine --add cuckoo1 192.168.56.101 --platform windows --snapshot
vmcloak
```

Distributed Scriptleri

Bu araç Distributed Cuckoo'nda açıklanmıştır.

Mac OS X Bootstrap Scriptleri

2.0.0 sürümünden itibaren kullanım dışı.

Mac OS X analizi için kullanılan bazı başlangıç betikleri `utils/darwin` klasöründe bulunmaktadır; bunlar, Mac OS X kötü amaçlı yazılım analizi için konuk ve ana sistemleri başlatmak için kullanılır. Bazı ayarlar içeride sabit olarak tanımlanmıştır, bu nedenle bunlara göz atmanız ve ihtiyaçlarınıza göre yapılandırmanız önerilir.