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.

Revision #1
Created 18 January 2024 21:25:54 by Ertan Sözer
Updated 18 January 2024 21:27:51 by Ertan Sözer