Gereksinimler

- TheHive'ın Gereksinimleri

TheHive'ın Gereksinimleri

TheHive platformunu başarılı bir şekilde kurmak ve kullanmak için belirli gereksinimler bulunmaktadır. Bu gereksinimler, platformun sorunsuz bir şekilde çalışması için gerekli olan donanım, yazılım ve yapılandırma gereksinimlerini içermektedir.

TheHive platformu aşağıdaki uygulamalara dayanır:

- Veri depolama Apache Cassandra (Desteklenen sürüm: 4.x)
- İndeksleme motoru olarak Elasticsearch (Desteklenen sürüm: 7.x)
- Dosya depolama çözümü de gereklidir; bağımsız sunucu senaryosunda uygulamayı barındıran sunucunun yerel dosya sistemi yeterlidir; aksi takdirde S3 MINIO

> Lucene Kullanımı 5.1 sürümünden bu yana, TheHive artık dizin motoru olarak Lucene arka ucunu desteklememektedir.

4.1.x ile veri dizinini işlemek için bir seçenekti; dizininizi Elasticsearch'e taşımak gerekir.

TheHive uygulaması, veritabanı & dizin motoru ve dosya depolama bağımsızdır. Tek başına bir düğüm veya küme olarak kurulabilir. Sonuç olarak sanal IP adresleri ve yük dengeleyicileri kullanılarak TheHive karmaşık bir küme mimarisinde kurulabilir.

Bağımsız Sunucu : Tüm uygulamalar aynı sunucuya yüklenir.

- Cassandra
- Elasticsearch
- Dosyalar dosya sisteminde saklanır (veya istenirse MinIO)
- TheHive
- NGINX (isteğe bağlı): HTTPS iletişimlerini yönetmek için

Küme veya Hibrit Mimari : TheHive ve yığının tüm uygulamaları, ihtiyaçlara göre doğru kurulumu seçebilecek kadar esnektir. Bir adanmış işletim sistemi üzerine , başka bir uygulama (örneğin : 1 Cassandra düğümü ile 1 Elasticsearch) ile kurulabilir.

Donanım gereksinimleri, entegrasyonları da içeren eşzamanlı kullanıcı ve sistemi nasıl kullandıklarına bağlıdır. Aşağıdaki tablo, tüm hizmetlerin aynı makinede barındırıldığında güvenli eşikleri göstermektedir:

Number of users	TheHive	Cassandra	ElasticSearch
< 10	2 / 2 GB	2 / 2 GB	2 / 2 GB
< 20	2-4 / 4 GB	2-4 / 4 GB	2-4 / 4 GB
< 50	4-6 / 8 GB	4-6 / 8 GB	4-6 / 8 GB

Öneri : Eğer her şeyi aynı sunucuya kuruyorsanız, en az 4 çekirdek ve 16 GB RAM öneriliyor . Elasticsearch için en azından jvm.options'ı ayarlamayı unutmamalıyız.

İşletim Sistemleri

TheHive a?a??daki i?letim sistemlerini desteklemektedir:

- Ubuntu 20.04 LTS & 22.04 LTS
- Debian 11
- RHEL 8
- Fedora 35 ve 37