Veritabanı ve Dizin Yapılandırması

TheHive, verileri ve dizini yönetmek için Cassandra ve Elasticsearch veritabanlarını kullanır. Kuruluma göre, örnek kullanabilir:

Temel Yapılandırma

TheHive için tipik bir veritabanı yapılandırması şu şekildedir:

```
## Database configuration
db {
  provider = janusgraph
  janusgraph {
    ## Storage configuration
    storage {
      backend = cql
      hostname = ["IP_ADDRESS"]
      cql {
        cluster-name = thp
        keyspace = thehive
      }
    }
    ## Index configuration
    index.search {
      backend = elasticsearch
      hostname = ["127.0.0.1"]
      index-name = thehive
    }
  }
}
```

Mümkün parametrelerin listesi

Parametre Tipi Açıklama

Parametre	Tipi	Açıklama
`provider`	string	provider adı. Varsayılan `janusgraph`
`storage`	dict	storage configuration (deepolama yapılandırması)
`storage.backend`	string	storage type. Can be `cql` or `berkeleyje` (depolama türü.)
`storage.hostname`	list of string	list of IP addresses or hostnames when using `cql` backend (cql arka ucunu kullanırken IP adreslerinin veya ana bilgisayar adlarının listesi)
`storage.directory`	string	local path for data when using `berkeleyje` backend (BerkeleyJE arka uç kullanıldığında veri için yerel yol.)
`storage.username`	string	account username with `cql` backend if Cassandra auth is configured (Eğer Cassandra kimlik doğrulaması yapılandırılmışsa, cql arka uç ile hesap kullanıcı adı.)
`storage.password`	string	account password with `cql` backend if Cassandra auth is configured (Cassandra kimlik doğrulaması yapılandırıldıysa, cql arka uç için hesap şifresi.)
`storage.port`	integer	port number with `cql` backend (`9042` by default). Change this if using an alternate port or a dedicated port number when using SSL with Cassandra (Cql arka uç ile bağlantı noktası numarası (varsayılan olarak 9042). Cassandra ile SSL kullanıyorsanız alternatif bir bağlantı noktası veya özel bir bağlantı noktası numarası kullanmak için bunu değiştirin.)
`storage.cql`	dict	configuration for `cql` backend *if used* (Kullanıldığında cql backend için yapılandırma.)

Parametre	Tipi	Açıklama
`storage.cql.cluster-name`	string	name of the cluster name used in the configuration of Apache Cassandra
`storage.cql.keyspace`	string	Keyspace name used to store TheHive data in Apache Cassandra
`storage.cql.ssl.enabled`	boolean	`false` by default. set it to `true` if SSL is used with Cassandra (Apache Cassandra yapılandırmasında kullanılan küme adı.)
`storage.cql.ssl.truststore.location`	string	path the the truststore. Specify it when using SSL with Cassandra (TheHive verilerini depolamak için Apache Cassandra'da kullanılan keyspace adı.)
`storage.cql.ssl.password`	string	password to access the truststore (Güven deposuna erişmek için şifre)
`storage.cql.ssl.client-authentication-enabled`	boolean	Enables use of a client key to authenticate with Cassandra (Cassandra ile kimlik doğrulaması için bir istemci anahtarı kullanımını etkinleştirir.)
`storage.cql.ssl.keystore.location`	string	path the the keystore. Specify it when using SSL and client auth. with Cassandra (Keystore'un yolu. Cassandra ile SSL ve istemci kimlik doğrulaması kullanılırken belirtiniz.)
`storage.cql.ssl.keystore.keypassword`	string	password to access the key in the keystore (Anahtara erişmek için şifre)
`storage.cql.ssl.truststore.storepassword`	string	password the access the keystore (Keystore'a erişim için şifre)
`index.search`	dict	configuration for indexes (Dizinler için yapılandırma)

Parametre	Tipi	Açıklama
`index.search.backend`	string	index engine. Default: `lucene` provided with TheHive. Can also be `elasticsearch` (Dizin motoru. Varsayılan: TheHive ile sağlanan lucene. Ayrıca elasticsearch olabilir.)
`index.search.directory`	string	path to folder where indexes should be stored, when using `lucene` engine (Lucene motoru kullanıldığında dizinlerin depolanacağı klasörün yolu.)
`index.search.hostname`	list of string	list of IP addresses or hostnames when using `elasticsearch` engine (Elasticsearch motoru kullanıldığında IP adresleri veya ana bilgisayar adlarının listesi.)
`index.search.index-name`	string	name of index, when using `elasticseach` engine (Elasticsearch motorunu kullandığınızda dizin adı.)
`index.search.elasticsearch.http.auth.type: basic`	string	`basic` is the only possible value (basic tek mümkün değerdir.)
`index.search.elasticsearch.http.auth.basic .username`	string	Username account on Elasticsearch (Elasticsearch'teki kullanıcı adı hesabı)
`index.search.elasticsearch.http.auth.basic .password`	string	Password of the account on Elasticsearch (Elasticsearch üzerindeki hesabın şifresi)
`index.search.elasticsearch.ssl.enabled`	boolean	Enable SSL `true/false` (SSL'yi etkinleştir true/false)
`index.search.elasticsearch.ssl.truststore.l ocation`	string	Location of the truststore (Güven deposunun konumu)

Parametre	Tipi	Açıklama
`index.search.elasticsearch.ssl.truststore.password`	string	Password of the truststore (Güven deposunun şifresi)
`index.search.elasticsearch.ssl.keystore.location`	string	Location of the keystore for client authentication (İstemci kimlik doğrulaması için keystore'un konumu)
`index.search.elasticsearch.ssl.keystore.storepassword`	string	Password of the keystore (Keystore'un şifresi)
`index.search.elasticsearch.ssl.keystore.keypassword`	string	Password of the client certificate (İstemci sertifikasının şifresi)
`index.search.elasticsearch.ssl.disable-hostname-verification`	boolean	Disable SSL verification `true/false` (SSL doğrulamasını devre dışı bırak true/false)
`index.search.elasticsearch.ssl.allow-self-signed-certificates`	boolean	Allow self signe certificates `true/false` (Kendinden imzalı sertifikalara izin ver true/false)

Not: İlk başlatma veya dizinleri yapılandırdıktan sonraki ilk başlatma, veritabanı büyük miktarda veri içeriyorsa biraz zaman alabilir. Bu süre, dizinlerin oluşturulmasından kaynaklanır.

Kullanım durumları

Veritabanı ve dizin motoru, kullanım durumuna ve hedef kuruluma bağlı olarak farklı olabilir:

Cassandra & Elasticsearch ile bağımsız sunucu :

1. Install a Cassandra server locally
2. Install Elasticsearch
3. Configure TheHive accordingly

```
## Database Configuration
db {
  provider = janusgraph
  janusgraph {
```

```
    ## Storage configuration
    storage {
      backend = cql
      hostname = ["127.0.0.1"]
      ## Cassandra authentication (if configured)
      username = "thehive_account"
      password = "cassandra_password"
      cql {
        cluster-name = thp
        keyspace = thehive
      }
    }
    ## Index configuration
    index.search {
      backend = elasticsearch
      hostname = ["127.0.0.1"]
      index-name = thehive
    }
  }
```

```
## Database Configuration
db {
  provider = janusgraph
  janusgraph {
    ## Storage configuration
    storage {
      backend = cql
      hostname = ["127.0.0.1"]
      ## Cassandra authentication (if configured)
      username = "thehive_account"
      password = "cassandra_password"
      cql {
        cluster-name = thp
        keyspace = thehive
      }
    }
    ## Index configuration
    index.search {
      backend = elasticsearch
      hostname = ["127.0.0.1"]
```

```
    index-name = thehive
  }
}
```

Cassandra ve Elasticsearch ile Küme:

1. Install a cluster of Cassandra servers
2. Get access to an Elasticsearch server
3. Configure TheHive accordingly

```
## Database Configuration
db {
 provider = janusgraph
 janusgraph {
  ## Storage configuration
  storage {
   backend = cql
   hostname = ["10.1.2.1", "10.1.2.2", "10.1.2.3"]
   ## Cassandra authentication (if configured)
   username = "thehive_account"
   password = "cassandra_password"
   cql {
    cluster-name = thp
    keyspace = thehive
   }
  }
  ## Index configuration
  index {
   search {
    backend  = elasticsearch
    hostname  = ["10.1.2.5"]
    index-name  = thehive
    elasticsearch {
     http {
      auth {
       type = basic
       basic {
        username = httpuser
        password = httppassword
       }
```

```
        }
      }
      ssl {
        enabled = true
        truststore {
          location = /path/to/your/truststore.jks
          password = truststorepwd
        }
      }
    }
  }
 }
}
```

> Bu yapılandırmada, tüm TheHive simgerleri aynı yapılandırmaya sahip olmalıdır. Elasticsearch yapılandırması script.allowed_types için varsayılan değeri kullanmalı veya aşağıdaki yapılandırma satırını içermelidir.

```
script.allowed_types: inline,stored
```

Revision #6
Created 12 April 2024 10:52:33 by Güldeniz Akca
Updated 13 April 2024 15:17:52 by Güldeniz Akca