

Veritabanı ve Dizin Yapılandırması

TheHive, verileri ve dizini yönetmek için Cassandra ve Elasticsearch veritabanlarını kullanır. Kurulumuna 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
<code>storage.cql.cluster-name</code>	string	name of the cluster name used in the configuration of Apache Cassandra
<code>storage.cql.keyspace</code>	string	Keyspace name used to store TheHive data in Apache Cassandra
<code>storage.cql.ssl.enabled</code>	boolean	<code>false</code> by default. set it to <code>true</code> if SSL is used with Cassandra (Apache Cassandra yapılandırmasında kullanılan küme adı.)
<code>storage.cql.ssl.truststore.location</code>	string	path the the truststore. Specify it when using SSL with Cassandra (TheHive verilerini depolamak için Apache Cassandra'da kullanılan keyspace adı.)
<code>storage.cql.ssl.password</code>	string	password to access the truststore (Güven deposuna erişmek için şifre)
<code>storage.cql.ssl.client-authentication-enabled</code>	boolean	Enables use of a client key to authenticate with Cassandra (Cassandra ile kimlik doğrulaması için bir istemci anahtarı kullanımını etkinleştirir.)
<code>storage.cql.ssl.keystore.location</code>	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.)
<code>storage.cql.ssl.keystore.keypassword</code>	string	password to access the key in the keystore (Anahtara erişmek için şifre)
<code>storage.cql.ssl.truststore.storepassword</code>	string	password the access the keystore (Keystore'a erişim için şifre)
<code>index.search</code>	dict	configuration for indexes (Dizinler için yapılandırma)

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

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

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

Kullanım durumları

Veritabanı ve izin motoru, kullanım durumuna ve hedef kurulumu 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