Kubernetes Installations

How to Use the Installer

This video covers the single node installer, but many of the concepts are also applicable to our multi-node installer.

https://www.youtube-nocookie.com/embed/1dXoajt6RCk

Overview

Our Element Enterprise Kubernetes Installer can handle the installation of Element Enterprise into your production kubernetes (k8s) environment.

To get started with a kubernetes installation, there are several things that need to be considered and this guide will work through them:

- k8s Environments
- Postgresql Database
- TURN Server
- SSL Certificates
- Extra configuation items

Once these areas have been covered, you'll be able to install a production environment!

Unpacking the Installer

Please make sure that you unpack `element-enterprise-installer` onto a system that has access to your k8s environment. The directory that it unpacks into will be referenced in this document as the installer directory.

You will also need to create a directory for holding the configurations for the installer. This will be referenced as the config directory going forward.

```
mkdir  ~/.element-onpremise-config
```

k8s Environments

Element Enterprise Installer allows you to either deploy directly into a kubernetes environment or to render a set of manifests for a future deployment in a kubernetes environment.

To configure your kubernetes environment for a direct deployment, you need to :

- Configure a kubectl context able to connect to your kubernetes instance
- Copy `k8s.yml.sample` to `k8s.yml` in your config directory. Edit `k8s.yml` with the following values :
- `provider_storage_class_name`: The storage class to use when creating PVCs.
- `ingress_annotations`: The annotations to add to the ingresses created by the operator.
- `tls_managed_externally`: Should be true if you don't expect the operator to manage the certificates of your kubernetes deployment. In this case, you will be able to skip the * *Certificates*- chapter of the `CONFIGURE.md` file.
- `operator_namespace`: The namespace to create to deploy the operator.
- `element_namespace`: The namespace to create to deploy the element resources.
- `k8s_auth_context`: The value of the context used in kubectl. If you want to use cert-manager for your tls certificates, it needs to be already installed in the targeted k8s cluster.

An example k8s.yml file would look like:

```
provider_storage_class_name: gp8-delete  # select an available storage class
ingress_annotations: ## below are expected annotations for an aws deployment
    kubernetes.io/ingress.class: alb
    alb.ingress.kubernetes.io/scheme: internet-facing
    alb.ingress.kubernetes.io/group.name: global
    alb.ingress.kubernetes.io/target-type: ip
    alb.ingress.kubernetes.io/ip-address-type: ipv4
    alb.ingress.kubernetes.io/listen-ports: '[{"HTTP": 80},{"HTTPS": 443}]'
synapse_ingress_annotations:  # below are required annotations if using the NGINX ingress
controller
    nginx.ingress.kubernetes.io/proxy-body-size: "50m"
tls_managed_externally: true  # true if the certificates are managed externaly to k8s
security_context_force_uid_gid: true  # true to enable pod runAsUser and fsGroup in security
context. false if it should not be used, in the case of openshift for example.
security_context_set_seccomp: true  # true to enable RuntimeDefault pod seccomp. false if it
```

```
should not be used, in the case of openshift for example.
operator_namespace: <namespace to create to deploy the operator>
element_namespace: <namespace to create to deploy the element resources>
k8s_auth_context: <the k8s auth context>
out_dir: # Absolute path to the directory where to render manifests, if render mode is used
# operator_manager_limits:  # Can be used to defined upper limits if the default one are not
large enough for your operator deployment
#   cpu: "2"
#   memory: 8Gi
```

If you do not want to deploy directly to kubernetes, but wish to render manifests instead, set all of the above mentioned variables except for `k8s_auth_context` and define a value for the parameter `out_dir`, which specifies where to write the kubernetes manifests. Further, when you go to run the installer, you need to invoke it as such:

```
bash install.sh  ~/.element-onpremise-config --target render
```

Using the above syntax, you will have a set of manifests written out to `out_dir` that you can then deploy into your kubernetes environment.

N.B. You will need to set your ingress controller's upload size to be at least 50 Mb to match synapse's default upload size if you wish to be able to have users upload files up to 50 Mb in size. Instructions for doing this with nginx are included in the `parameters.yml` section below.

Postgresql Database

The installation requires that you have a postgresql database with a locale of C and UTF8 encoding set up. See https://matrix-org.github.io/synapse/latest/postgres.html#set-up-database for further details.

Please make note of the database hostname, database name, user, and password as you will need these to begin the installation.

TURN Server

For installations in which you desire to use video conferencing functionality, you will need to have a TURN server installed and available for Element to use.

If you do not have an existing TURN server, our installer can configure one for you by following the extra steps in Setting Up Jitsi and TURN With the Installer.

If you have an existing TURN server, please create a file called `synapse/turn.yml` in your config directory and put the following in it:

```
turn_uris: [ "turn:turn.matrix.org?transport=udp", "turn:turn.matrix.org?transport=tcp" ]
turn_shared_secret: "n0t4ctuAllymatr1Xd0TorgSshar3d5ecret4obvIousreAsons"
turn_user_lifetime: 86400000
turn_allow_guests: True
```

based on your TURN server specifics. This will allow the installer to configure synapse to use your TURN server.

A few notes on TURN servers:

- The TURN server has to be directly accessible by end-users. Normally this means a public IP, however if all the end-users are going to be on a VPN/private network then they just need to be able to access the private IP of the TURN server.
- The only reason to have TURN on a private network is if the private network disallows user <-> user traffic and only allows user <-> TURN server traffic. If user <-> user is allowed within the private network then a TURN server isn't needed.

SSL Certificates

For SSL Certificates, you have three options:

- Signed PEM encoded certificates from an internet recognized authority.
- Signed PEM encoded certificates from an internal to your company authority.
- LetsEncrypt

In the case of LetsEncrypt, your hostnames must be accessible on the internet.

You will need to configure certificates for the following names:

- fqdn.tld
- element.fqdn.tld
- synapse.fqdn.tld
- dimension.fqdn.tld
- hookshot.fqdn.tld

Using our example hosts, this would mean that we need certificates for:

- local
- element.local
- synapse.local
- dimension.local
- hookshot.local

Certificates without LetsEncrypt

If you have certificates for all of the aforementioned host names, then you can simply place the `.crt` and `.key` files in the `certs` directory under the config directory. Certificates in the `certs` directory must take the form of `fqdn.cert` and `fqdn.key`.

Certificates with LetsEncrypt

Our installer also supports using LetsEncrypt to build certificates for your host names and automatically install them into your environment. If your hosts are internet accessible, this is the easiest method and only requires an admin email address to provide to LetsEncrypt.

parameters.yml

Now it is time to set `parameters.yml`. A sample has been provided and to get started, it is easiest to do:

```
cp config-sample/parameters.yml.sample ~/.element-onpremise-config/parameters.yml
```

Using the example hostnames of `element.local` and `synapse.local` (not resolvable on the internet), we would set the following parameters first in `parameters.yml`:

```
domain_name: local
element_fqdn: element.local
synapse_fqdn: synapse.local
```

Next, we need to set the variables related to Postgres. As you are installing into kubernetes, you will need to set the following for your Postgres database:

```
postgres_create_in_cluster: false
postgres_fqdn: `Postgres Server`
postgres_user: `Postgres User`
postgres_db: `Postgres Database for Element`
```

The next line states:

```
media_size: "50Gi"
```

You wll want to adjust that to match the size of storage you've allocated for your media. It must be at least 50Gb.

The next section pertains to certmanager. If you are using your own certificates, please leave these items both blank, as such:

```
certmanager_issuer:
certmanager_admin_email:
```

If you have chosen to use letsencrypt, please specify “letsencrypt” for the certmanager_issue and an actual email address for who should manage the certificates for certmanager_admin_email:

```
certmanager_issuer: 'letsencrypt'
certmanager_admin_email: 'admin@mydomain.com'
```

Starting with installer 2022-08.02, we have added two mandatory variables related to telemetry data. These are `max_mau_users` and `strict_mau_users_limit`. You should set `max_mau_users` to the value defined in your contract with Element. If you set this number above your contractual limit, then the software will allow you to exceed your contractual limit and Element will bill you appropriately for the overage.

Setting `strict_mau_users_limit` to `true` forces synapse to cap the number of monthly active users to the value defined in `max_mau_users`. Say for example, you've paid Element for 1,000 monthly active users and don't want to exceed that, you would set:

```
max_mau_users: 1000
strict_mau_users_limit: true
```

Let's say that you paid Element for 1,000 monthly active users, but didn't mind going over provided that you didn't exceed 2,000 monthly active users. In this scenario, you would set:

```
max_mau_users: 2000
strict_mau_users_limit: true
```

For more information on the data that Element collects, please see: What Telemetry Data is Collected by Element?

You will also see two paths:

```
# media_host_data_path: "/mnt/data/synapse-media"
# postgres_data_path: "/mnt/data/synapse-postgres"
```

For kubernetes installations, please make sure these are commented out.

You will also notice two lines towards the end regarding `synapse_registration` and `tls_managed_externally`. In most cases, you can leave these alone, but if you wish to close synapse registration or have your TLS managed externally, you may set them at this time.

If you are using nginx as your ingress controller and wish to send files up to 50 Mb in size, please add these two lines to parameters.yml:

```
synapse_ingress_annotations:
  nginx.ingress.kubernetes.io/proxy-body-size: "50m"
```

secrets.yml

Now we move on to configuring `secrets.yml`. You will need the following items here:

- A Macaroon key
- Your postgres password for the user specified in parameters.yml
- A Registration Shared Secret
- A signing Key
- An EMS Image Store username and token, which will have been provided to you by Element.

To build a `secrets.yml` with the macaroon key, the registration shared secret, the generic shared secret, and the signing key already filled in, please run:

```
sh build_secrets.sh
mv secrets.yml  ~/.element-onpremise-config/
```

You will need to uncomment and set your `postgres_password` field to the proper password for your database.

Do not forget to also set the values for `ems_image_store_username` and `ems_image_store_token`, which will both be provided by Element.

If you have a paid docker hub account, you can specify your username and password to avoid being throttled in the `dockerhub_username` and `dockerhub_token` fields. This is optional.

Extra Configuration Items

It is possible to configure anything in Synapse's homeserver.yaml or Element’s config.json.

To do so, you need to create json or yaml files in the appropriate directory under the config directory. These files will be merged to the target configuration file.

Samples are available in `config-sample` under the installer directory.

To configure synapse:

- Create a directory `synapse` at the root of the config directory : `mkdir ~/.element-onpremise-config/synapse`
- Copy the configurations extensions you want to setup from `config-sample/synapse` to `~/.element-onpremise-config/synapse`.
- Edit the values in the file accordingly to your configuration

To configure element:

- Create a directory `element` at the root of the config directory : `mkdir ~/.element-onpremise-config/element`
- Copy the configurations extensions you want to setup from `config-sample/element` to `~/.element-onpremise-config/element`.
- Edit the values in the file accordingly to your configuration

For specifics on configuring permalinks for Element, please see Setting up Permalinks.

For specifics on setting up Delegated Authentication, please see Setting up Delegated Authentication With the Installer

For specifics on setting up Group Sync, please see Setting up Group Sync

For specifics on setting up the Integration Manager, please see Setting Up the Integration Manager With the Installer

For specifics on setting up GitLab, GitHub, and JIRA integrations, please see Setting up GitLab, GitHub, and JIRA Integrations With the Installer

For specifics on setting up Chatterbox, please see: Setting Up Chatterbox

For specifics on setting up Adminbot and Auditbot, please see: Setting up Adminbot and Auditbot

For specifics on setting up the Enterprise Admin Dashboard, please see: Configuring the Enterprise Admin Dashboard

For specifics on pointing your installation at an existing Jitsi instance, please see Setting Up Jitsi and TURN With the Installer

For specifics on configuring the Teams Bridge, please see Setting Up the Teams Bridge

For specifics on configuring the Telegram Bridge, please see Setting Up the Telegram Bridge

For specifics on configuring the IRC Bridge, please see Setting Up the IRC Bridge

For specifics on configuring the XMPP Bridge, please see Setting Up the XMPP Bridge

Installation

Let’s review! Have you considered:

- k8s Environments
- Postgresql Database
- TURN Server
- SSL Certificates
- Extra configuration items

Once you have the above sections taken care of and your `parameters.yml` and `secrets.yml` files are in order, you are ready to begin the actual installation.

From the installer directory, run:

```
bash install.sh  ~/.element-onpremise-config
```

The first run should go for a little while and then exit, instructing you to log out and back in.

Please log out and back in and re-run the installer from the installer directory again:

```
bash install.sh  ~/.element-onpremise-config
```

Upgrading between installer versions

Installer 2022-08.02

Added two **mandatory** variables related to telemetry data:
`max_mau_users` and `strict_mau_users_limit`

They need to be set (ie: `max_mau_users = 1000` and `strict_mau_users_limit = true`).

Revision #14
Created 1 August 2022 18:32:51 by Karl Abbott
Updated 28 November 2022 20:28:32 by Karl Abbott