Introduction to Element Enterprise

What is Element Enterprise?

Element Enterprise provides an enterprise-grade secure communications platform that can be run either on your own premise or in our Element Cloud. Element Enterprise includes all of the security and privacy features that you get with Element:

- Built on the Matrix open communications standard.
- Provides end to end encrypted messaging, voice, and video through a consumer style messenger with the power of a collaboration tool.
- Delivers data sovereignty.
- Affords a high degree of flexibility that can be tailored to many use cases.
- Allows secure federation within a single organisation or across a supply chain or ecosystem.

and combines them with the following unique Enterprise specific features:

- Group Sync: Synchronize group data from your identity provider and map these into Element spaces.
- Adminbot: Give your server administrator the ability to be admin in any rooms on your homeserver.
- Auditbot: Have an auditable record of conversations conducted on your homeserver.
- Chatterbox: Give your website a light-weight Matrix client for customers to chat with your company.
- Security and feature updates: Updates are easy to deploy and handled by our installer.
- Support: Access to the experts in federated, secure communications giving you confidence to deploy our platform for your most critical secure communications needs.

Given the flexibility afforded by this platform, ours has a number of moving parts to configure. This documentation will step you through architecting and deploying Element Enterprise On-Premise.

Deploying to a Single Node or Multiple Nodes?

Element Enterprise On-Premise can be deployed both to a single node or a set of multiple nodes. In the case of the multiple node deployment, this requires kubernetes, a container orchestration platform. In the case of our single node deployment, our installer deploys microk8s (a smaller distribution of kubernetes) and deploys our application to that microk8s instance.

In general, regardless of if you pick a single node deployment or a multiple node deployment, you will need a base level of hardware to support the application.

For scenarios that utilise closed federation, Element recommends a minimum of 4 vcpus/cpus and 16GB ram for the host(s) running synapse pods.

For scenarios that utilise open federation, Element recommends a minimum of 8 vcpus/cpus and 32GB ram for the host(s) running synapse pods.

Architecture

This document gives an overview of our secure communications platform architecture:

(Please click on the image to view it at 100%.)

Comprising our secure communications platform are the following components:

- synapse : The homeserver itself.
- element-web : The Element Web client.
- dimension: Our integration manager.
- synapse admin ui : Our Element Enterprise Administrator Dashboard.
- postgresql (Optional) : Our database. Only optional if you already have a separate PostgreSQL database.
- groupsync (Optional) : Our group sync software
- adminbot (Optional) : Our bot for admin tasks.
- auditbot (Optional) : Our bot that provides auditability.
- hookshot (Optional) : Our integrations with gitlab, github, jira, and custom webhooks.
- chatterbox (Optional) : Light weight client for your website.
- jitsi (Optional) : Our VoIP platform for group conferencing.
- coturn (Optional) : TURN server. Required if deploying VoIP.

- prometheus (Optional) : Provides metrics about the application and platform.
- grafana (Optional) : Graphs metrics to make them consumable.

For each of the components in this list (excluding postgresql, groupsync, adminbot, auditbot, and prometheus), you must provide a hostname on your network that meets this criteria:

- Fully resolvable to an IP address that is accessible from your clients.
- Signed PEM encoded certificates for the hostname in a crt/key pair. Certificates should be signed by an internet recognised authority, an internal to your company authority, or LetsEncrypt.

It is possible to deploy Element Enterprise On-Premise with self-signed certificates and without proper DNS in place, but this is not ideal as the mobile clients and federation do not work with self-signed certificates. Information on how to use self-signed certificates and hostname mappings instead of DNS can be found in How to Setup Local Host Resolution Without DNS

In addition to hostnames for the above, you will also need a hostname and PEM encoded certificate key/cert pair for your base domain. If we were deploying a domain called example.com and wanted to deploy all of the software, we would have the following hostnames in our environment that needed to meet the above criteria:

- example.com (base domain)
- synapse.example.com (homeserver)
- element.example.com (element web)
- dimension.example.com (integration manager)
- admin.example.com (admin dashboard)
- hookshot.example.com (Our integrations)
- chatterbox.example.com (Our light weight client)
- jitsi.example.com (Our VoIP platform)
- coturn.example.com (Our TURN server)
- grafana.example.com (Our Grafana server)

As mentioned above, this list excludes postgresql, groupsync, adminbot, auditbot, and prometheus.

Further, if you want to do voice or video, you will need a TURN server. If you already have one, you do not have to set up coturn. If you do not already have a TURN server, you will want to set up coturn and if your server is behind NAT, you will need to have an external IP in order for coturn to work.

Installation

Multiple Nodes

For a multiple node installation, make sure you have a kubernetes platform deployed that you have access to and head over to Kubernetes Installations

Single Node

For a single node installation, please note that we support these on the following platforms:

- Ubuntu Server 20.04
- Enterprise Linux 8 (RHEL, CentOS Stream, etc.)

Once you have a server with one of these installed, please head over to Single Node Installations

---

Revision #13
Created 25 July 2022 17:44:50 by Karl Abbott
Updated 29 August 2022 13:08:50 by Karl Abbott