Créez un certificat TLS fiable via l'API REST

Publié: 2024-11-04

Par défaut, capteurs et consoles inclure un certificat TLS auto-signé. Vous pouvez toutefois améliorer la sécurité et les performances de votre système en ajoutant un certificat sécurisé signé par une autorité de certification (CA). Vous pouvez créer la demande de signature de certificat à envoyer à votre autorité de certification via l'API REST ExtraHop . Après avoir reçu le certificat signé, vous pouvez également l'ajouter à votre sonde ou console via l'API REST.

Avant de commencer

- Vous devez vous connecter au sonde ou console avec un compte qui possède privilèges d'administration du système et des accès pour générer une clé API.
- Vous devez disposer d'une clé API valide pour apporter des modifications via l'API REST et suivre les procédures ci-dessous. (Voir Générer une clé API).
- Familiarisez-vous avec les Guide de l'API REST ExtraHop pour savoir comment naviguer dans l'explorateur d'API REST ExtraHop.

Note: Vous pouvez également exécuter les procédures décrites dans cette rubrique via les paramètres d'administration. Pour plus d'informations, consultez les rubriques suivantes :

- Créez une demande de signature de certificat depuis votre système ExtraHop
- Certificat TLS

Création d'une demande de signature de certificat TLS

Pour créer un certificat TLS signé, vous devez envoyer une demande de signature de certificat à une autorité de certification de confiance.

1. Dans un navigateur, accédez à l'explorateur d'API REST.

   L'URL est le nom d'hôte ou l'adresse IP de votre sonde ou console, suivi par `/api/v1/explore/`. Par exemple, si votre nom d'hôte est seattle-eda, l'URL est `https://seattle-eda/api/v1/explore/`.
2. Cliquez **Entrez la clé API** puis collez ou saisissez votre clé API dans le **Clé API** champ.
3. Cliquez **Autoriser** puis cliquez sur **Fermer**.
4. Cliquez **ExtraHop** puis cliquez sur **Post/ExtraHop/SSLCert/Demande de signature**.
5. Cliquez **Essayez-le**.
   Le schéma JSON est automatiquement ajouté au Paramètres de demande de signature de certificat SSL zone de texte des paramètres.
6. Dans le Paramètres de demande de signature de certificat SSL zone de texte du paramètre, spécifiez les champs de demande de signature de certificat.
   a) Dans le `common_name` champ, remplacez `string` avec le nom de domaine complet de votre sonde ou console.
   b) Dans le `subject_alternative_names` champ, ajoutez un ou plusieurs noms de domaine ou adresses IP alternatifs pour votre sonde ou votre console.

      Note: Le `subject_alternative_names` le champ est obligatoire. Si votre système ne possède qu'un seul nom de domaine, dupliquez la valeur du `common_name` champ. Vous devez inclure au moins un nom alternatif du sujet dont le type est défini sur `dns`, mais d'autres noms alternatifs peuvent avoir le type défini sur `ip` ou `dns`.
   c) Optionnel : Dans le `email_address` champ, remplacez `string` avec l'adresse e-mail du propriétaire du certificat.
   d) Optionnel : Dans le `organization_name` champ, remplacez `string` avec le nom légal enregistré de votre organisation.

e) Optionnel : Dans le `country_code` champ, remplacez `string` avec le code ISO à 2 caractères du pays dans lequel se trouve votre organisation.
f) Optionnel : Dans le `state_or_province_name` champ, remplacez `string` avec le nom de l'État ou du siège de votre organisation.
g) Optionnel : Dans le `locality_name` champ, remplacez `string` avec le nom de la ville dans laquelle se trouve votre organisation.
h) Optionnel : Dans le `organizational_unit_name` champ, remplacez `string` avec le nom de votre département au sein de votre organisation.

Le Valeur la section doit ressembler à l' exemple suivant :

```
{
  "subject": {
    "common_name": "example.com",
    "email_address": "admin@example.com",
    "organization_name": "Example",
    "country_code": "US"
  },
  "subject_alternative_names": [
    {
      "name": "www.example.com",
      "type": "dns"
    }
  ]
}
```

7. Cliquez **Envoyer la demande** pour créer la demande de signature.
Dans le Réponse du serveur section, la Organe de réponse affiche la demande de signature dans `pem` champ.

Prochaines étapes
Envoyez la demande de signature à votre autorité de certification pour créer votre certificat TLS signé.

Important: La demande de signature contient des séquences d'échappement qui représentent des sauts de ligne (\n). Remplacez chaque instance de\npar un saut de ligne avant d'envoyer la demande à votre autorité de certification. Vous pouvez modifier la demande PEM manuellement dans un éditeur de texte ou automatiquement via un utilitaire d'analyse JSON, comme illustré dans l'exemple de commande suivant :

```
echo '<json_output>' | python -c 'import sys, json; print
 json.load(sys.stdin)["pem"]'
```

Remplacez le `<json_output>` variable avec la chaîne JSON complète renvoyée dans la section Response Body.

Ajoutez un certificat TLS fiable à votre sonde ou à votre console

Vous pouvez ajouter un certificat TLS signé par une autorité de certification de confiance à votre sonde ou sur console via l'explorateur d'API REST.

1. Dans un navigateur, accédez à l'explorateur d'API REST.
L'URL est le nom d'hôte ou l'adresse IP de votre sonde ou console, suivi par `/api/v1/explore/`. Par exemple, si votre nom d'hôte est seattle-eda, l'URL est `https://seattle-eda/api/v1/explore/`.
2. Cliquez **Entrez la clé API** puis collez ou saisissez votre clé API dans **Clé API** champ.
3. Cliquez **Autoriser** puis cliquez sur **Fermer**.
4. Cliquez **ExtraHop** puis cliquez sur **PUT/ExtraHop/SSLCert**.
5. Cliquez **Essayez-le**.
6. Dans le **Certificat et clé** dans le champ, collez le certificat TLS.

Le certificat doit ressembler au texte suivant :

```
-----BEGIN CERTIFICATE-----
a0O8zvV4MlDhWX4e0VyvGAJx+9d4AqQB4Czy/P7z36CmHe2Y7PPdVSeWHNCQoJ0g
CnO42u2V9YKNFYRQejIJv8CxGVJKsdfV0iP0WnCvpZXkaBOYIrDvE5xn010WPUls
6qe3mCXsUK87i++mYuVDA1U0A5YVXRO2OOWIWy7P+MCU/cR/op3Jpekng2cxN4qD
FqGbtRpLdCuJ/xGWL1FFRHBg76+TbO+pxgZhiCtHYXfMKIaoPmDwsAqEtLbizz1W
mbMig9hs4QNcJ+aMNSnTZpkbeBR4a2nkGnQoYvnFOXV/nWzvfHmI4ydSH9g4I8qt
4ArqFepInvm70n07FYAKL6Mdd1i+7ieo9AqckltVzzKFzkakHm04214wtsYmle94
4HqIJ7p7NH5maXxttXMzHFlArbnjHWCl0gIv8lAu+IvLJ8aiGAb3zqveNz6ZAZ5j
PGAUsP+dVYV/8VjvqhkiP/1jWzUHwzpdlHbcD8qOkAF41fnbv+2EXqFJ096JSSiU
rqeJpgNuH3LbkT0KORAiLoGLMZKEKxF+3OpLVD7ox7NQh9pMdZlB8tcTbTmsvD8T
3L2tMVZssqYOANcidtd17t72VW4hzQURT1me5tGWxpN6od/q6B+FIvRq/7Vq0UE1
c2AG/om5UN/Vj3pUjXzq/B1IWUS9TicRcKdl5wrKEkPUGjK4w1R/87bj5HSn8nyd
lMCcOpLTokHj0B5+8O1ylNhVXNPlj3eY0n6OQOdClBqTDM0/4sB3XgeC/pjpleU3
3uot+wM/GoN/Dqb1LPt3BNpUQuCzSfmGSSOXiWELsEhz3ix/36a9eUWjfhmtPsW5
dne5Lf+G7cf+ebsRTb7R89GmgKzTpUl1KAzKINAebkT6WrWWljugpA0BcfANjS6o
mik4ZbY8d54UtA17evprr2+8UotIgVIrCbfLgA2DY8QOTCBYIFKJ3GZAedqRK9Sm
I2qdaB6QBczYNaVYSeCsBdHHw1+h7dBeqdUUwYKtmPW96/djj/6vJSXh9/UX/3c0
eqXG36w/lqJAYu8QtAydJsVC85IzqzikkX0f0KE315Doginpg59yix9dHD2sxLb1
X39BRpLkZ9nvW6ke2YHU/VKBVIxqSslukGoTUIcUtPJrtMQOwCi/EQQXbPK9a2pW
K51938h6OuLjNbDTFuxfhE4zITWHTgyAs2MNVR9+uDUiVJclX+CIPjhZzjyPqmD6
6uh8Sr3zndOMabqDquo69rMQyvclF0xOUMVgUw1Rb8Y=
-----END CERTIFICATE-----
```

Note: Si vous souhaitez que le certificat soit signé avec votre propre clé privée, vous pouvez inclure votre clé après le certificat TLS, en la séparant par un saut de ligne. Cependant, nous vous recommandons de ne pas spécifier votre propre clé ; par défaut, la sonde ou la console signera le certificat avec la clé privée du système.

7. Cliquez **Envoyer la demande** pour ajouter le certificat.