Erstellen Sie ein vertrauenswürdiges SSL-Zertifikat über die REST-API

Veröffentlicht: 2023-10-24

Standardmäßig Sensoren und Konsolen fügen Sie ein selbstsigniertes SSL-Zertifikat hinzu. Sie können jedoch die Sicherheit und Leistung Ihres Systems verbessern, indem Sie ein vertrauenswürdiges Zertifikat hinzufügen, das von einer Zertifizierungsstelle (CA) signiert wurde. Sie können die Zertifikatsignieranforderung erstellen, um sie über die ExtraHop REST API an Ihre CA zu senden. Nachdem Sie das signierte Zertifikat erhalten haben, können Sie es auch zu Ihrem hinzufügen Sensor oder Konsole über die REST-API.

Bevor Sie beginnen

- Sie müssen sich anmelden bei Sensor oder Konsole mit einem Konto, das System- und Zugriffsadministrationsrechte um einen API-Schlüssel zu generieren.
- Sie benötigen einen gültigen API-Schlüssel, um Änderungen über die REST-API vornehmen und die folgenden Verfahren ausführen zu können. (siehe Generieren Sie einen API-Schlüssel.)
- Machen Sie sich vertraut mit dem ExtraHop REST API-Leitfaden um zu erfahren, wie Sie im ExtraHop REST API Explorer navigieren.

Hinweis: Sie können die Verfahren in diesem Thema auch über die Administrationseinstellungen ausführen. Weitere Informationen finden Sie in den folgenden Themen:

- Erstellen Sie eine Zertifikatsignieranforderung von Ihrem ExtraHop-System aus
- SSL Zertifikat

Erstellen Sie eine SSL-Zertifikatsignieranforderung

Um ein signiertes SSL-Zertifikat zu erstellen, müssen Sie eine Zertifikatsignieranforderung an eine vertrauenswürdige Zertifizierungsstelle senden.

Wichtig: Der REST-API-Explorer ist auf Reveal (x) 360 nicht verfügbar.

1. Navigieren Sie in einem Browser zum REST API Explorer.
   Die URL ist der Hostname oder die IP-Adresse Ihres Sensor oder Konsole, gefolgt von `/api/v1/explore/`. Wenn Ihr Hostname beispielsweise seattle-eda ist, lautet die URL `https://seattle-eda/api/v1/explore/`.
2. klicken **Geben Sie den API-Schlüssel ein** und fügen Sie dann Ihren API-Schlüssel ein oder geben Sie ihn in das **API-Schlüssel** Feld.
3. klicken **Autorisieren** und dann klicken **Schliessen**.
4. klicken **ExtraHop** und dann klicken **Post/ExtraHop/SSLCert/Signierungsanfrage**.
5. klicken **Probiere es aus**.
   Das JSON-Schema wird automatisch zum Anforderungsparameter für die SSL-Zertifikatsignierung Parameter-Textfeld.
6. In der Anforderungsparameter für die SSL-Zertifikatsignierung Parametertextfeld, geben Sie die Felder für die Anforderung zur Zertifikatsignierung an.
   a) In der `common_name` Feld, ersetzen `string` mit dem vollqualifizierten Domänenname Ihres Sensor oder Ihrer Konsole.
   b) In der `subject_alternative_names` Feld, fügen Sie einen oder mehrere alternative Domainnamen oder IP-Adressen für Ihren Sensor oder Ihre Konsole hinzu.

      Hinweis: Die `subject_alternative_names` Feld ist erforderlich. Wenn Ihr System nur einen Domänenname hat, duplizieren Sie den Wert aus `common_name` Feld. Sie müssen mindestens einen alternativen Betreffnamen angeben, dessen Typ auf

gesetzt ist `dns`, aber für zusätzliche alternative Namen kann der Typ auf gesetzt werden `ip` oder `dns`.

c) Optional: In der `email_address` Feld, ersetzen `string` mit der E-Mail-Adresse des Zertifikatsinhabers.

d) Optional: In der `organization_name` Feld, ersetzen `string` mit dem registrierten legalen Namen Ihrer Organisation.

e) Optional: In der `country_code` Feld, ersetzen `string` mit dem 2-stelligen ISO-Ländercode des Landes, in dem Ihre Organisation ansässig ist.

f) Optional: In der `state_or_province_name` Feld, ersetzen `string` mit dem Namen des Bundesstaates oder des Landes, in dem sich Ihre Organisation befindet.

g) Optional: In der `locality_name` Feld, ersetzen `string` mit dem Namen der Stadt, in der sich Ihre Organisation befindet.

h) Optional: In der `organizational_unit_name` Feld, ersetzen `string` mit dem Namen Ihrer Abteilung innerhalb Ihrer Organisation.

Die Wert Der Abschnitt sollte dem folgenden Beispiel ähneln:

```
{
  "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. klicken **Anfrage senden** um die Signaturanfrage zu erstellen.
   In der Antwort des Servers Abschnitt, der Antworttext zeigt die Signieranforderung in der `pem` Feld.

Nächste Schritte

Senden Sie die Signaturanfrage an Ihre CA, um Ihr signiertes SSL-Zertifikat zu erstellen.

Wichtig: Die Signieranforderung enthält Escape-Sequenzen, die Zeilenumbrüche (\n) darstellen. Ersetzen Sie jede Instanz von\ndurch einen Zeilenumbruch, bevor Sie die Anfrage an Ihre CA senden. Sie können die PEM-Anforderung manuell in einem Texteditor oder automatisch über ein JSON-Analyseprogramm ändern, wie im folgenden Beispielbefehl gezeigt:

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

Ersetze den `<json_output>` Variable mit der gesamten JSON-Zeichenfolge, die im Abschnitt Response Body zurückgegeben wurde.

Fügen Sie Ihrem Sensor oder Ihrer Konsole ein vertrauenswürdiges SSL-Zertifikat hinzu

Sie können ein von einer vertrauenswürdigen CA signiertes SSL-Zertifikat zu Ihrem hinzufügen Sensor oder Konsole über den REST API Explorer.

1. Navigieren Sie in einem Browser zum REST API Explorer.

Die URL ist der Hostname oder die IP-Adresse Ihres Sensor oder Konsole, gefolgt von `/api/v1/explore/`. Wenn Ihr Hostname beispielsweise seattle-eda ist, lautet die URL `https://seattle-eda/api/v1/explore/`.

2. klicken **API-Schlüssel eingeben** und fügen Sie dann Ihren API-Schlüssel ein oder geben Sie ihn in das **API-Schlüssel** Feld.
3. klicken **Autorisieren** und dann klicken **Schliessen**.
4. klicken **ExtraHop** und dann klicken **PUT/ExtraHop/SSLCert**.
5. klicken **Probiere es aus**.
6. In der **Zertifikat und Schlüssel** Feld, fügen Sie das SSL-Zertifikat ein.

   Das Zertifikat sollte dem folgenden Text ähneln:

```
-----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-----
```

   Hinweis: Wenn Sie möchten, dass das Zertifikat mit Ihrem eigenen privaten Schlüssel signiert wird, können Sie Ihren Schlüssel hinter dem SSL-Zertifikat angeben, getrennt durch einen Zeilenumbruch. Wir empfehlen jedoch, keinen eigenen Schlüssel anzugeben. Standardmäßig signiert der Sensor oder die Konsole das Zertifikat mit dem privaten Schlüssel auf dem System.

7. klicken **Anfrage senden** um das Zertifikat hinzuzufügen.