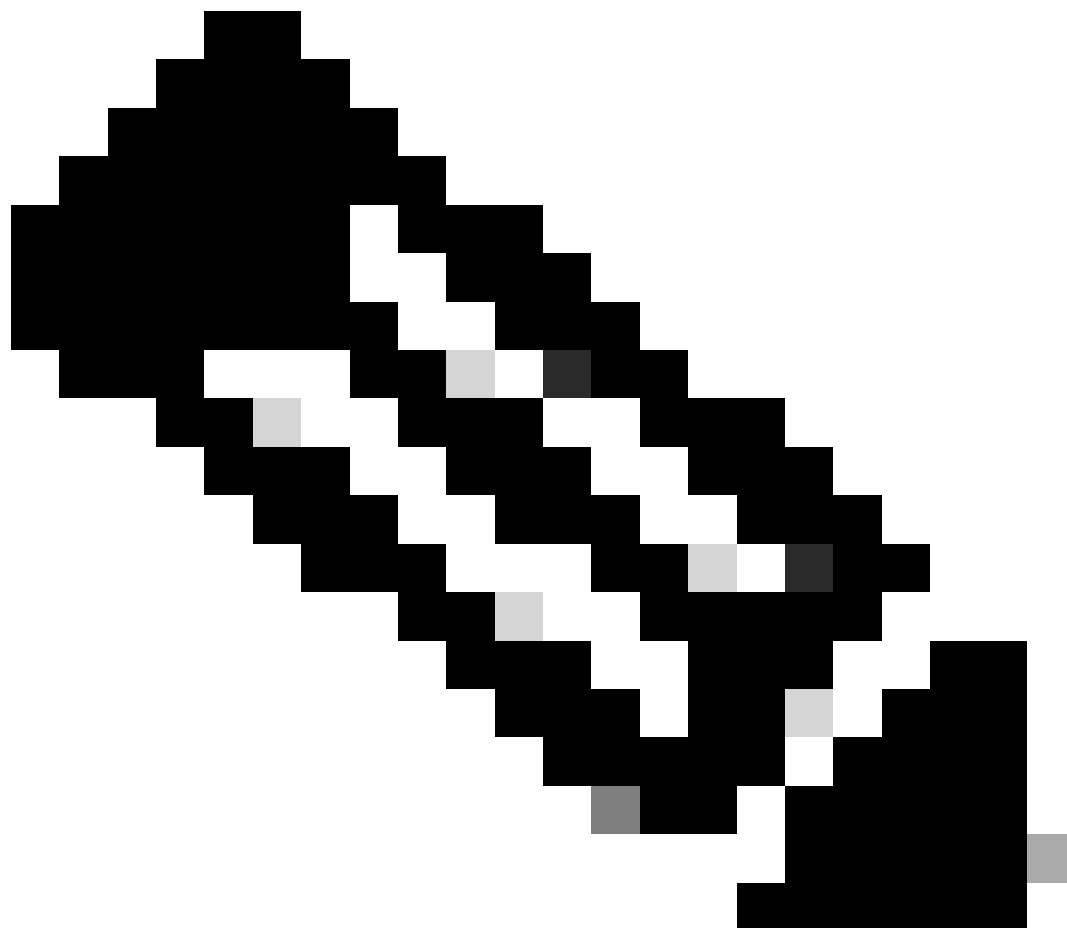


セキュアエンドポイントプライベートクラウド – 認証証明書の有効期限

内容

はじめに

このドキュメントでは、4年前（2020年）のオリジナルインストールを使用して、バージョン3.1.0から4.1.0を実行するCisco Secure Endpoint Private Cloud(VPN)の認証証明書の有効期限に関する必要な情報について説明します。



注：これらの証明書の有効期限は、アプライアンスのセットアップが行われた時刻によって異なります。

技術詳細

影響を受けるバージョン：バージョン3.1.0から4.1.0が稼働し、4年前のオリジナルインストールを使用しているCisco Secure Endpoint Private Cloud。

2024年5月以降、バージョン3.1.0から4.1.0が稼働し、4年前のオリジナルインストールを使用しているSecure Endpoint Private Cloudの認証証明書は期限切れになります。これにより、サービスが中断されます。証明書の有効期限が切れる前に、管理コンソールに次の警告が表示されます。

System Warning 2024-02-12 00:05:07 +0000 Certificate audit.crt will expire in 3カ月。

System Warning 2024-02-12 00:05:07 +0000 Certificate refresh_token.crt will expire in 3カ月。

システム警告2024-02-12 00:05:07 +0000証明書jwt.crtは3カ月で期限切れになります。

System Warning 2024-02-12 00:05:06 +0000 Certificate saml.crt will expire in 3カ月。

次に示すように、SSH経由でコマンドラインコマンドを使用して、これらの証明書の有効期限を確認できます。

```
[root@fireamp certs]# /usr/bin/openssl x509 -text -noout -in /opt/fire/etc/ssl/certs/refresh_token.crt
```

証明書:

Data:

バージョン : 3 (0x2)

シリアル番号:

ee:ea:9f:f9:88:09:38:31:0b:90:bb:b5:1b:29:e3:6b

署名アルゴリズム : sha256WithRSAEncryption

発行者 : C=US、O=Sourcefire、O=Immunet、OU=PrivateCloud Appliance、CN=refresh-token

有効性

禁止期間 : 2022年9月28日00:52:02 GMT

Not After :9月27日00:52:02 2026 GMT

Subject: C=US, O=Sourcefire, O=Immunet, OU=PrivateCloud Appliance, CN=refresh-token

Secure Endpoint Private Cloud 4.2.0に更新すると、次の証明書が更新されます。

- audit.crt – 監査レコードの署名
- refresh_token.crt- ID管理サービスとの通信を処理する

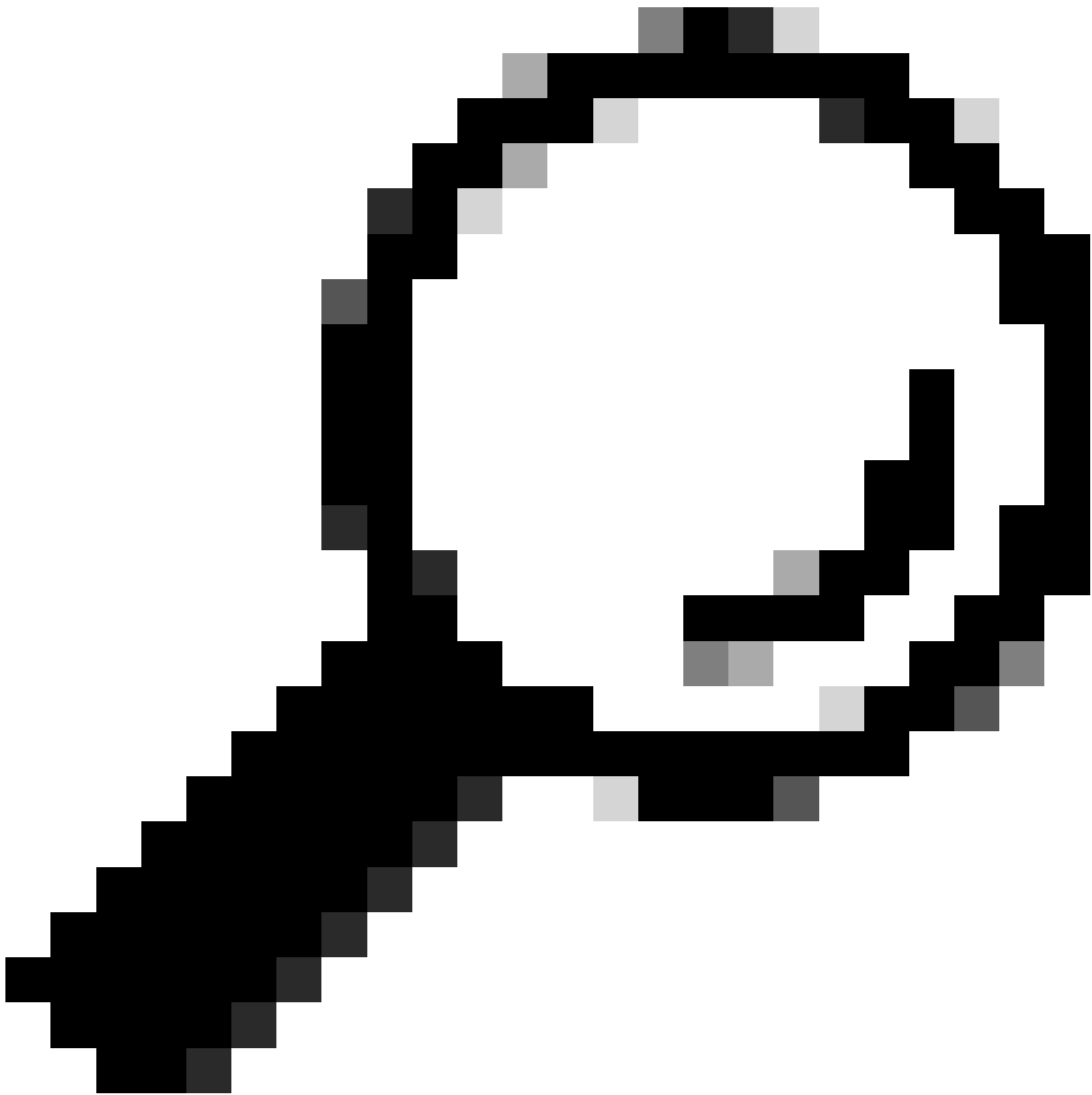
- jwt.crt : サービス間の相互通信を可能にします。
- saml.crt:SAML応答の署名

影響

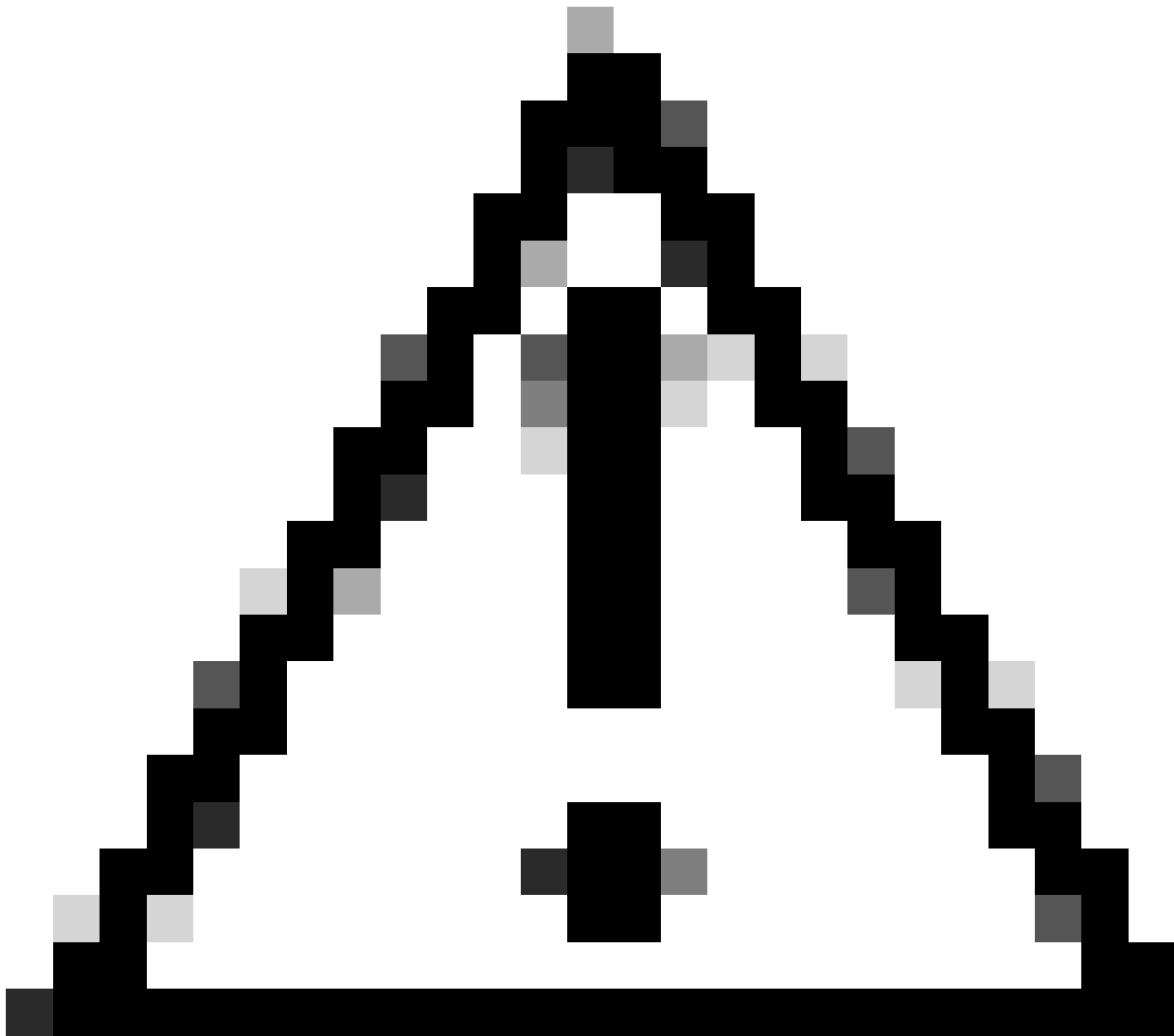
証明書の有効期限が切れる前に証明書が更新されないと、管理コンソールとSecure Endpoint Consoleへのアクセスが失われます。そのため、2024年5月に証明書の期限が切れる前にアプライアンスを更新することが重要です。

解決方法

証明書を更新するには、プライベートクラウドアプライアンスをバージョン4.2.0以降に更新する必要があります。更新は、SSHを介してコマンド・ラインから開始するか、管理コンソールのユーザー・インターフェースから開始できます。



ヒント：始める前に、このドキュメントの最後にリンクされている『Secure Endpoint Private Cloud Release Notes and Administration Portal User Guide』をお読みください。



注意：アプライアンスを4.2.0に更新する前に、コンテンツを2024年2月以降の最新バージョンに更新する必要があります。このドキュメントでリンクされているリリースノートを参照してください。

管理ポータルから：

1. Operations > Update Deviceの順に移動します。
2. Check/Download Updatesを選択します
3. アップデートをダウンロードしたら、Update Softwareを選択し、OKを選択して確定します。

SSHを使用したコマンドラインから：

1. コマンドamp-ctl update-checkを実行します。
2. アップデートをダウンロードしたら、コマンドamp-ctl updateを実行します。

このドキュメントの「技術詳細」セクションに記載されている手順に従うことで、証明書が正常に更新されたことを確認できます。



注：緊急の状況でアプライアンスを更新できない場合は、[こちら](#)からCisco TACにお問い合わせください。

セキュアエンドポイントプライベートクラウドリリースノート

[:https://docs.amp.cisco.com/Private%20Cloud%20Release%20Notes.pdf](https://docs.amp.cisco.com/Private%20Cloud%20Release%20Notes.pdf)

セキュアエンドポイントプライベートクラウド管理ポータルユーザガイド

[:https://docs.amp.cisco.com/AMPPrivateCloudAdminGuide-latest.pdf](https://docs.amp.cisco.com/AMPPrivateCloudAdminGuide-latest.pdf)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。