セキュリティ証明書の管理

OnCommand Unified Manager 9.5

NetApp
December 20, 2023

This PDF was generated from https://docs.netapp.com/ja-jp/oncommand-unified-manager-95/online-help/task-viewing-the-https-security-certificate-ocf.html on December 20, 2023. Always check docs.netapp.com for the latest.

目次

セキュリティ証明書の管理

Unified Manager サーバで HTTPS を設定することで、セキュアな接続を介してクラスタを監視および管理できるようになります。

HTTPS セキュリティ証明書の表示

HTTPS 証明書の詳細をブラウザで取得した証明書と比較して、 Unified Manager に対するブラウザの暗号化された接続が妨害されていないことを確認できます。

作業を開始する前に

オペレータ、OnCommand 管理者、またはストレージ管理者のロールが必要です。

このタスクについて

証明書を表示すると、再生成された証明書の内容を検証したり、Unified Managerへのアクセスに使用できるURLの別名を確認したりできます。

手順

1. ツールバーで、をクリックします*をクリックし、*設定*メニューから HTTPS証明書*をクリックします。

   HTTPS 証明書がページの上部に表示されます

完了後

HTTPS 証明書ページに表示されるものよりも詳細なセキュリティ証明書情報を表示する必要がある場合は、ブラウザで接続証明書を表示できます。

HTTPS セキュリティ証明書の生成

別の認証局の署名を使用する場合や現在のセキュリティ証明書の期限が切れた場合など、さまざまな理由で新しいHTTPSセキュリティ証明書を生成することがあります。新しい証明書で既存の証明書が置き換えられます。

作業を開始する前に

OnCommand 管理者のロールが必要です。

このタスクについて

Unified Manager Web UI にアクセスできない場合は、メンテナンスコンソールを使用して同じ値で HTTPS 証明書を再生成できます。

手順

1. ツールバーで、をクリックします*をクリックし、*設定*メニューから HTTPS証明書*をクリックします。
2. [* HTTPS 証明書の再生成 *] をクリックします。

   HTTPS 証明書の再生成ダイアログボックスが表示されます。

3. 証明書を生成する方法に応じて、次のいずれかのオプションを選択します。

状況	手順
現在の値で証明書を再生成します	[現在の証明書属性を使用して再生成（ Regenerate using current Certificate Attributes ）] オプションをクリックし
別の値を使用して証明書を生成します	`Click the *Update the Current Certificate Attributes* option.` 新しい値を入力しない場合は、 [共通名] フィールドと [代替名] フィールドに既存の証明書の値が使用されます。その他のフィールドには値は必要ありませんが、証明書に値を入力する場合は、たとえば、市区町村、都道府県、国などの値を入力できます。 証明書の代替名フィールドからローカル識別情報を削除する場合は'ローカル識別情報を除外(localhostなど)チェックボックスをオンにしますこのチェックボックスをオンにすると、 [代替名] フィールドに入力したフィールドのみが使用されます。空白のままにすると、結果の証明書に代替名フィールドがまったく表示されなくなります。

4. [はい] をクリックして証明書を再生成します。
5. 新しい証明書を有効にするために Unified Manager サーバを再起動します。

完了後

HTTPS 証明書を表示して新しい証明書の情報を確認します。

Unified Manager 仮想マシンを再起動しています

仮想マシンは、 Unified Manager のメンテナンスコンソールから再起動できます。新し

いセキュリティ証明書を生成した場合や仮想マシンで問題が発生した場合、仮想マシンの再起動が必要になります。

作業を開始する前に

仮想アプライアンスの電源をオンにします。

メンテナンスコンソールにメンテナンスユーザとしてログインします。

このタスクについて

[ゲストの再起動]オプションを使用して、vSphereから仮想マシンを再起動することもできます。詳細については、 VMware のドキュメントを参照してください。

手順

1. メンテナンスコンソールにアクセスします
2. システム構成 **>** 仮想マシンの再起動 * を選択します。

HTTPS 証明書署名要求のダウンロード

認証局にファイルを送信して署名を求めるために、現在のHTTPSセキュリティ証明書の証明書要求をダウンロードできます。CA 署名証明書は、中間者攻撃を阻止するのに役立ち、自己署名証明書よりも強力なセキュリティ保護を実現します。

作業を開始する前に

OnCommand 管理者のロールが必要です。

手順

1. ツールバーで、をクリックします*をクリックし、*設定*メニューから HTTPS証明書*をクリックします。
2. [* HTTPS 証明書署名要求のダウンロード *] をクリックします。
3. を保存します `<hostname>.csr` ファイル。

完了後

認証局にファイルを送信して署名を求め、署名済み証明書をインストールできます。

HTTPSセキュリティ証明書をインストールする

認証局から署名を受けて返されたセキュリティ証明書を、アップロードしてインストールすることができます。アップロードしてインストールするファイルは、既存の自己署名証明書の署名済みバージョンである必要があります。CA 署名証明書は、中間者攻撃を阻止するのに役立ち、自己署名証明書よりも強力なセキュリティ保護を実現します。

作業を開始する前に

次の作業を完了しておきます。

- 証明書署名要求ファイルをダウンロードし、認証局によって署名されています
- 証明書チェーンを PEM 形式で保存します
- チェーンに含まれるすべての証明書について、 Unified Manager サーバ証明書からルート署名証明書への中間証明書も含めます

OnCommand 管理者のロールが必要です。

手順

1. ツールバーで、をクリックします*をクリックし、*設定*メニューから HTTPS証明書*をクリックします。
2. ［ * HTTPS 証明書のインストール * ］ をクリックします。
3. 表示されるダイアログボックスで、「 * ファイルを選択 … * 」をクリックして、アップロードするファイルを探します。
4. ファイルを選択し、 * Install * をクリックしてファイルをインストールします。

証明書チェーンの例

証明書チェーンファイルの表示例を次に示します。

```
-----BEGIN CERTIFICATE-----
<*Server certificate*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Intermediate certificate \#1 \(if present\)*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Intermediate certificate \#2 \(if present\)*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Root signing certificate*>
-----END CERTIFICATE-----
```

証明書管理のページの説明

HTTPS 証明書ページを使用して、現在のセキュリティ証明書を表示したり、新しい HTTPS 証明書を生成したりできます。

HTTPS 証明書ページ

HTTPS 証明書ページでは、現在のセキュリティ証明書の表示、証明書署名要求のダウンロード、新しい HTTPS 証明書の生成、新しい HTTPS 証明書のインストールを行うことができます。

新しい HTTPS 証明書を生成していない場合は、インストール時に生成された証明書がこのページに表示されます。

コマンドボタン

各コマンドボタンを使用して次の処理を実行できます。

- * HTTPS 証明書署名要求 * をダウンロードします

  現在インストールされている HTTPS 証明書の証明書要求をダウンロードします。を保存するように求めるメッセージがブラウザに表示されます `<hostname>.csr` ファイルを使用して、署名を行う認証局にファイルを提供します。

- * HTTPS 証明書をインストール *

  認証局から署名を受けて返されたセキュリティ証明書を、アップロードしてインストールすることができます。新しい証明書は、管理サーバを再起動すると有効になります。

- * HTTPS 証明書の再生成 *

  HTTPS 証明書を生成して現在のセキュリティ証明書と置き換えることができます。新しい証明書は、Unified Manager を再起動すると有効になります。

HTTPS 証明書の再生成ダイアログボックス

HTTPS 証明書の再生成ダイアログボックスでは、セキュリティ情報をカスタマイズし、その情報を使用して新しい HTTPS 証明書を生成できます。

このページには現在の証明書の情報が表示されます。

[現在の証明書属性を使用して再生成] および [現在の証明書属性を更新] を選択すると ' 現在の情報で証明書を再生成するか ' 新しい情報で証明書を生成できます

- * 共通名 *

  必須保護する対象の完全修飾ドメイン名（ FQDN ）。

  Unified Manager のハイアベイラビリティ構成では、仮想 IP アドレスを使用します。

- * 電子メール *

  任意。組織に問い合わせるための E メールアドレス。通常は、証明書管理者または IT 部門の E メールアドレスです。

- * 会社名 *

任意。通常は会社の法人名です。

- * 部門 *

  任意。社内の部署の名前。

- * 都市 *

  任意。会社の所在地の市区町村。

- * 状態 *

  任意。会社の所在地の都道府県。

- * 国 *

  任意。会社の所在地の国。通常は ISO の 2 文字の国コードです。

- * 別名 *

  必須既存のローカルホストやその他のネットワークアドレスに加えて、このサーバへのアクセスに使用できるプライマリ以外のドメイン名が追加されました。代行名はそれぞれカンマで区切ります。

  証明書の代替名フィールドからローカル識別情報を削除する場合は ' ローカル識別情報を除外 (localhost など) チェックボックスをオンにしますこのチェックボックスをオンにすると、 [代替名] フィールドに入力したフィールドのみが使用されます。空白のままにすると、結果の証明書に代替名フィールドがまったく表示されなくなります。

著作権に関する情報

Copyright © 2023 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータ ソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用権を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用権については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、http://www.netapp.com/TMに記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。