証明書を使用してリモートサーバの ID を確認します

ONTAP 9

NetApp
April 24, 2024

This PDF was generated from https://docs.netapp.com/ja-jp/ontap/system-admin/verify-identity-remote-servers-certificates-concept.html on April 24, 2024. Always check docs.netapp.com for the latest.

目次

証明書を使用してリモートサーバの ID を確認します 1
証明書の概要を使用してリモートサーバの ID を確認します 1
OCSP を使用してデジタル証明書が有効であることを確認します 1
TLS ベースのアプリケーションのデフォルト証明書を表示します 3

証明書を使用してリモートサーバの ID を確認します

証明書の概要を使用してリモートサーバの ID を確認します

ONTAP は、リモートサーバの ID を検証するセキュリティ証明書機能をサポートしています。

ONTAP ソフトウェアでは、次のデジタル証明書機能とプロトコルを使用して安全に接続できます。

- Online Certificate Status Protocol （ OCSP ）は、 SSL 接続と Transport Layer Security （ TLS ）接続を使用して、 ONTAP サービスからのデジタル証明書要求のステータスを検証します。この機能はデフォルトでは無効になっています。
- ONTAP ソフトウェアには、信頼されたルート証明書のデフォルトセットが付属しています。
- Key Management Interoperability Protocol （ KMIP ）の証明書を使用して、クラスタと KMIP サーバの相互認証を有効にできます。

OCSP を使用してデジタル証明書が有効であることを確認します

ONTAP 9.2 以降では、 Online Certificate Status Protocol （ OCSP ）を有効にすることで、 Transport Layer Security （ TLS ）通信を使用する ONTAP アプリケーションでデジタル証明書のステータスを受信できます。OCSP による証明書のステータスチェックは、特定のアプリケーションに対していつでも有効または無効にできます。デフォルトでは、 OCSP による証明書のステータスチェックは無効になっています。

必要なもの

このタスクを実行するには、advanced権限レベルのアクセス権が必要です。

このタスクについて

OCSP は、次のアプリケーションをサポートしています。

- AutoSupport
- イベント管理システム（ EMS ）
- LDAP over TLS
- Key Management Interoperability Protocol （ KMIP ）
- 監査ログ
- FabricPool
- SSH（ONTAP 9.13.1以降）

手順

1. 権限レベルを advanced に設定します。 `set -privilege advanced`。

2. 特定の ONTAP アプリケーションで OCSP による証明書のステータスチェックを有効または無効にするには、次の該当するコマンドを使用します。

一部のアプリケーションで **OCSP** による証明書のステータスチェックを有効または無効にする場合	使用するコマンド
有効	`security config ocsp enable -app app name`
無効	`security config ocsp disable -app app name`

次のコマンドは、 AutoSupport および EMS の OCSP サポートを有効にします。

```
cluster::*> security config ocsp enable -app asup,ems
```

OCSP を有効にすると、アプリケーションは次のいずれかの応答を受信します。

- Good - 証明書は有効で、通信可能な状態です。
- Revoked - 証明書は発行元の認証局によって永続的に信頼できないと判断されており、通信不可能な状態です。
- Unknown - サーバが証明書に関するステータス情報を持っていないため、通信不可能な状態です。
- OCSP server information is missing in the certificate - TLS 通信は続行していますが、サーバで OCSP が無効であると判断されているため、ステータスチェックは実行されません。
- No response from OCSP server - アプリケーションを実行できない状態です。

3. TLS を使用するすべてのアプリケーションで OCSP による証明書のステータスチェックを有効または無効にするには、次の該当するコマンドを使用します。

すべてのアプリケーションで **OCSP** による証明書のステータスチェックを有効または無効にする場合	使用するコマンド

有効	`security config ocsp enable`
	
	`-app all`

無効	`security config ocsp disable`
	
	`-app all`

有効にすると、指定した証明書が「有効」、「失効」、「不明」のいずれであるかを示す署名済みの応答が、すべてのアプリケーションに送信されます。証明書のステータスが revoked の場合は、アプリケーションは実行できません。アプリケーションが OCSP サーバから応答を受信できない場合、または OCSP サーバにアクセスできない場合、アプリケーションは続行できません。

4. を使用します `security config ocsp show` コマンドを使用して、OCSPをサポートするすべてのアプリケーションとそのサポートステータスを表示します。

```
cluster::*> security config ocsp show
         Application                        OCSP Enabled?
         --------------------               ---------------------
         autosupport                        false
         audit_log                          false
         fabricpool                         false
         ems                                false
         kmip                               false
         ldap_ad                            true
         ldap_nis_namemap                   true
         ssh                                true

         8 entries were displayed.
```

TLS ベースのアプリケーションのデフォルト証明書を表示します

ONTAP 9.2 以降では、 ONTAP に、 Transport Layer Security （ TLS ）を使用する ONTAP アプリケーション用の信頼されたルート証明書のデフォルトセットが付属しています。

必要なもの

デフォルトの証明書は、管理 SVM の作成時、または ONTAP 9.2 へのアップグレード時に、管理 SVM にのみインストールされます。

このタスクについて

現在クライアントとして機能し、証明書の検証が必要なアプリケーションは、 AutoSupport 、 EMS 、 LDAP 、監査ログ、 FabricPool 、 および KMIP を使用できます。

証明書の有効期限が切れると、ユーザに証明書を削除するよう要求する EMS メッセージが起動します。デフォルトの証明書は、 advanced 権限レベルでのみ削除できます。

> デフォルトの証明書を削除すると、一部の ONTAP アプリケーションが正常に機能しなくなる場合があります（ AutoSupport 、監査ログなど）。

ステップ

1. 管理 SVM にインストールされているデフォルトの証明書を表示するには、 security certificate show コマンドを使用します。

   `security certificate show -vserver -type server-ca`

```
fas2552-2n-abc-3::*> security certificate show -vserver fas2552-2n-abc-3
-type server-ca
Vserver    Serial Number   Common Name                             Type
---------- --------------- ---------------------------------------
------------
fas2552-2n-abc-3
           01              AAACertificateServices
server-ca
    Certificate Authority: AAA Certificate Services
          Expiration Date: Sun Dec 31 18:59:59 2028
```

著作権に関する情報

Copyright © 2024 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。