Webサービスの管理

ONTAP 9

NetApp
February 12, 2026

目次

Webサービスの管理

Webサービスの管理 - 概要

クラスタまたはStorage Virtual Machine（SVM）のWebサービスを有効化または無効化したり、Webサービスの設定を表示したり、ロールのユーザーがWebサービスにアクセスできるかどうかを制御したりできます。

クラスタまたはSVMのWebサービスは次の方法で管理できます。

- 特定のWebサービスを有効化または無効化する
- Webサービスへのアクセスを暗号化されたHTTP（SSL）のみに限定するかどうかを指定する
- Webサービスの可用性を表示する
- あるロールのユーザのWebサービスへのアクセスを許可する、または禁止する
- Webサービスへのアクセスが許可されているロールを表示する

ユーザがあるWebサービスへアクセスするには、次の条件をすべて満たしている必要があります。

- 認証されたユーザであること。

  たとえば、Webサービスからユーザ名およびパスワードの入力を求められた場合、ユーザは有効なアカウントの情報を入力する必要があります。

- ユーザに正しいアクセス方法が設定されていること。

  認証は、指定されたWebサービスに対する正しいアクセス方法を持つユーザに対してのみ成功します。ONTAP API Webサービス `ontapi`の場合、ユーザは `ontapi`アクセス方法を持っている必要があります。その他のすべてのWebサービスの場合、ユーザは `http`アクセス方法を持っている必要があります。

  `security login`コマンドを使用して、ユーザーのアクセス方法と認証方法を管理します。

- Webサービスがユーザのアクセス制御ロールを許可するように設定されていること。

  `vserver services web access`コマンドを使用して、ロールのWebサービスへのアクセスを制御します。

ファイアウォールが有効になっている場合は、Webサービスに使用するLIFのファイアウォール ポリシーを設定して、HTTPまたはHTTPSを許可する必要があります。

WebサービスアクセスにHTTPSを使用する場合は、Webサービスを提供するクラスタまたはSVMのSSLも有効にする必要があり、クラスタまたはSVMのデジタル証明書を提供する必要があります。

ONTAP Webサービスへのアクセスを管理する

Webサービスは、HTTPまたはHTTPSを使用してユーザがアクセスできるアプリケーションです。クラスタ管理者はWebプロトコル エンジンをセットアップし、SSLを設定し、Webサービスを有効にし、ロールのユーザがWebサービスにアクセスできるようにします。

ONTAP 9.6以降では、次のWebサービスがサポートされます。

- サービスプロセッサインフラストラクチャ (`spi`)

  このサービスは、クラスタ管理LIFまたはノード管理LIFを介して、ノードのログ、コアダンプ、およびMIBファイルをHTTPまたはHTTPSでアクセスできるようにします。デフォルト設定は `enabled`です。

  ノードのログファイルまたはコアダンプファイルへのアクセス要求があると、 `spi`Webサービスは、あるノードから、ファイルが存在する別のノードのルートボリュームへのマウントポイントを自動的に作成します。マウントポイントを手動で作成する必要はありません。

- ONTAP API (`ontapi`)

  このサービスを使用すると、ONTAP APIを実行してリモートプログラムから管理機能を実行できます。デフォルト設定は `enabled`です。

  一部の外部管理ツールにはこのサービスが必要です。たとえば、System Managerを使用する場合は、このサービスを有効にしておく必要があります。

- Data ONTAP検出(`disco`)

  このサービスにより、オフボックス管理アプリケーションがネットワーク内のクラスタを検出できるようになります。デフォルト設定は `enabled`です。

- サポート診断(`supdiag`)

  このサービスは、問題の分析と解決を支援するために、システム上の特権環境へのアクセスを制御します。デフォルト設定は `disabled`です。このサービスは、テクニカルサポートから指示された場合にのみ有効にしてください。

- System Manager(`sysmgr`)

  このサービスは、ONTAPに含まれるSystem Managerの可用性を制御します。デフォルト設定は `enabled`です。このサービスはクラスタでのみサポートされます。

- ファームウェア ベースボード管理コントローラ（BMC）アップデート(`FW_BMC`

  このサービスを使用すると、BMCファームウェアファイルをダウンロードできます。デフォルト設定は `enabled`です。

- ONTAP ドキュメント(`docs`)

  このサービスはONTAPドキュメントへのアクセスを提供します。デフォルト設定は `enabled`です。

- ONTAP RESTful API (`docs_api`)

  このサービスは、ONTAP RESTful APIドキュメントへのアクセスを提供します。デフォルト設定は `enabled`です。

- ファイルのアップロードとダウンロード(`fud`)

  このサービスでは、ファイルのアップロードとダウンロードが可能です。デフォルト設定は `enabled`です。

- ONTAPメッセージング(`ontapmsg`)

  このサービスは、イベントをサブスクライブするためのパブリッシュ/サブスクライブインターフェースをサポートしています。デフォルト設定は `enabled`です。

- ONTAPポータル(`portal`)

  このサービスは、ゲートウェイを仮想サーバーに実装します。デフォルト設定は `enabled`です。

- ONTAP Restful Interface(`rest`)

  このサービスは、クラスタインフラストラクチャのすべての要素をリモートで管理するためのRESTfulインターフェースをサポートしています。デフォルト設定は `enabled`です。

- Security Assertion Markup Language（SAML）サービスプロバイダーサポート(`saml`)

  このサービスは、SAMLサービスプロバイダーをサポートするためのリソースを提供します。デフォルト設定は `enabled`です。

- SAML サービスプロバイダー(`saml-sp`)

  このサービスは、SPメタデータやアサーションコンシューマサービスなどのサービスをサービスプロバイダに提供します。デフォルト設定は `enabled`です。

ONTAP 9.7以降では、さらに次のサービスがサポートされます。

- 構成バックアップファイル(`backups`)

  このサービスを使用すると、設定のバックアップファイルをダウンロードできます。デフォルト設定は `enabled`です。

- ONTAP セキュリティ(`security`)

  このサービスは、認証を強化するためにCSRFトークン管理をサポートしています。デフォルト設定は `enabled`です。

ONTAPでWebプロトコルエンジンを管理する

クラスタ上でWebプロトコル エンジンを設定し、Webアクセスを許可するかどうか、およびどのSSLのバージョンが使用可能かを制御できます。また、Webプロトコル エンジ

ンの構成設定を表示することもできます。

Webプロトコル エンジンは、次の方法でクラスタ レベルで管理できます。

- `system services web modify`コマンドに `-external`パラメータを指定することで、リモートクライアントがWebサービスコンテンツにアクセスする際にHTTPまたはHTTPSのどちらを使用できるかを指定できます。
- `security config modify`コマンドを `-supported-protocol`パラメータとともに使用することで、安全なWebアクセスにSSLv3を使用するかどうかを指定できます。デフォルトでは、SSLv3は無効になっています。トランスポート層セキュリティ1.0（TLSv1.0）は有効になっており、必要に応じて無効にすることができます。

  `security config modify`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/security-config-modify.html["ONTAPコマンド リファレンス"^]を参照してください。

- クラスタ全体のコントロール プレーンWebサービス インターフェイス用に、Federal Information Processing Standard（FIPS）140-2準拠モードを有効にすることができます。

  FIPS 140-2準拠モードは、デフォルトでは無効になっています。

  - **FIPS 140-2** 準拠モードが無効の場合 `security config modify`コマンドの `is-fips-enabled`パラメータを `true`に設定し、 `security config show`コマンドを使用してオンライン状態を確認することで、FIPS 140-2 準拠モードを有効にできます。
  - **FIPS 140-2**準拠モードが有効になっている場合
    - ONTAP 9.11.1以降、TLSv1、TLSv1.1、SSLv3は無効になり、TSLv1.2とTSLv1.3のみが有効のままになります。これはONTAP 9の内部および外部の他のシステムと通信に影響します。FIPS 140-2準拠モードを有効にしてから無効にした場合、TLSv1、TLSv1.1、SSLv3は無効のままになります。以前の設定に応じて、TLSv1.2またはTLSv1.3のいずれかが有効のままになります。
    - ONTAP 9.11.1より前のバージョンでは、TLSv1とSSLv3の両方が無効になっており、TLSv1.1とTLSv1.2のみが有効のままです。ONTAPでは、FIPS 140-2準拠モードが有効になっている場合、TLSv1とSSLv3の両方を有効にすることはできません。FIPS 140-2準拠モードを有効にしてから無効にした場合、TLSv1とSSLv3は無効のままですが、以前の設定に応じて、TLSv1.2またはTLSv1.1とTLSv1.2の両方が有効になります。
- `system security config show`コマンドを使用して、クラスタ全体のセキュリティの設定を表示できます。

  `security config show`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/security-config-show.html["ONTAPコマンド リファレンス"^]を参照してください。

ファイアウォールが有効になっている場合は、Webサービスに使用する論理インターフェイス（LIF）のファイアウォール ポリシーを設定して、HTTPまたはHTTPSアクセスを許可する必要があります。

Webサービス アクセスにHTTPSを使用する場合は、Webサービスを提供するクラスタまたはStorage Virtual Machine（SVM）のSSLを有効にし、そのクラスタまたはSVMのデジタル証明書を提供する必要もあります。

MetroCluster構成では、クラスタ上のWebプロトコル エンジンの設定に対する変更内容は、パートナー クラスタにはレプリケートされません。

Webプロトコル エンジンを管理するためのONTAPコマンド

`system services web`コマンドを使用してWebプロトコルエンジンを管理します。 `system services firewall policy create`コマンドと `network interface modify`コマンドを使用して、Webアクセス要求がファイアウォールを通過できるようにします。

状況	使用するコマンド
クラスター レベルでWebプロトコル エンジンを構成します： • クラスターのWebプロトコル エンジンを有効または無効にする • クラスターの SSLv3 を有効または無効にする • セキュア Web サービス（HTTPS）の FIPS 140-2 準拠を有効または無効にする	`system services web modify`
クラスタ レベルでの Web プロトコル エンジンの構成を表示し、クラスタ全体で Web プロトコルが機能しているかどうかを確認し、FIPS 140-2 準拠が有効になっていてオンラインかどうかを表示します	`system services web show`
ノードレベルでのwebプロトコルエンジンの構成と、クラスター内のノードのwebサービス処理のアクティビティを表示します。	`system services web node show`
ファイアウォール ポリシーを作成するか、既存のファイアウォール ポリシーに HTTP または HTTPS プロトコル サービスを追加して、Webアクセス要求がファイアウォールを通過できるようにします。	`system services firewall policy create` `-service`パラメータを `http`または `https`に設定すると、Webアクセス要求がファイアウォールを通過できるようになります。
ファイアウォールポリシーをLIFに関連付ける	`network interface modify` `-firewall-policy`パラメータを使用して、LIFのファイアウォール ポリシーを変更できます。

関連情報

- "network interface modify"

ONTAP Webサービスへのアクセスを設定する

Webサービスへのアクセスを設定すると、許可されたユーザがHTTPまたはHTTPSを使用して、クラスタまたはStorage Virtual Machine（SVM）上のサービスコンテンツにアクセスできるようになります。

手順

1. ファイアウォールが有効になっている場合は、Webサービスに使用されるLIFのファイアウォールポリシーでHTTPまたはHTTPSアクセスが設定されていることを確認します：

   `system services firewall show`コマンドを使用してファイアウォールが有効になっているかどうかを確認できます。

   a. ファイアウォール ポリシーで HTTP または HTTPS が設定されていることを確認するには、 `system services firewall policy show` コマンドを使用します。

      `system services firewall policy create`コマンドの `-service`パラメータを `http`または `https`に設定して、ポリシーがWebアクセスをサポートできるようにします。

   b. HTTP または HTTPS をサポートするファイアウォール ポリシーが、Web サービスを提供する LIF に関連付けられていることを確認するには、 `-firewall-policy`パラメータを指定した `network interface show`コマンドを使用します。

      `network interface show`
      の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/network-interface-show.html["ONTAPコマンド リファレンス"^]を参照してください。

      `network interface modify`コマンドに `-firewall-policy`パラメータを指定して、LIFに対してファイアウォールポリシーを有効にします。

      `network interface modify`
      の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/network-interface-modify.html["ONTAPコマンド リファレンス"^]を参照してください。

2. クラスターレベルのWebプロトコルエンジンを構成し、Webサービスコンテンツにアクセスできるようにするには、 `system services web modify`コマンドを使用します。

3. セキュア Web サービス（HTTPS）を使用する予定の場合は、SSL を有効にし、 `security ssl modify`コマンドを使用してクラスタまたは SVM のデジタル証明書情報を提供します。

   `security ssl modify`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/security-ssl-modify.html["ONTAPコマンド リファレンス"^]をご覧ください。

4. クラスタまたは SVM の Web サービスを有効にするには、 `vserver services web modify`コマンドを使用します。

   クラスタまたは SVM に対して有効にするサービスごとに、この手順を繰り返す必要があります。

5. クラスタまたは SVM 上の Web サービスにアクセスするロールを承認するには、 `vserver services web access create` コマンドを使用します。

   アクセスを許可するロールは既に存在している必要があります。 `security login role show`コマンドを使用して既存のロールを表示するか、 `security login role create`コマンドを使用して新しいロールを作成できます。

   `security login role show`および `security login role create`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/search.html?q=security+login+role["ONTAPコマンド リファレンス"^]をご覧ください。

6. Webサービスへのアクセスが許可されているロールの場合は、 `security login show`コマンドの出力をチェックして、そのユーザも正しいアクセス方法で設定されていることを確認します。

   ONTAP API Webサービス `ontapi`にアクセスするには、ユーザに `ontapi`アクセス方法を設定する必要があります。その他のすべてのWebサービスにアクセスするには、ユーザに `http`アクセス方法を設定する必要があります。

   `security login show`の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/security-login-show.html["ONTAPコマンド リファレンス"^]を参照してください。

   ⓘ `security login create`コマンドを使用して、ユーザのアクセス方法を追加します。link:https://docs.netapp.com/us-en/ontap-cli/security-login-create.html["ONTAPコマンド リファレンス"^]の `security login create`の詳細を確認してください。

Webサービスを管理するためのONTAPコマンド

`vserver services web`コマンドを使用して、クラスタまたはStorage Virtual Machine（SVM）のWebサービスの可用性を管理します。 `vserver services web access`コマンドを使用して、ロールのWebサービスへのアクセスを制御します。

状況	使用するコマンド
クラスタまたはSVMのWebサービスを次のように設定する • Webサービスを有効または無効にする • WebサービスへのアクセスにHTTPSだけを許可するかどうかを指定する	`vserver services web modify`
クラスタまたはSVMのWebサービスの設定と可用性を表示する	`vserver services web show`
特定のロールに対して、クラスタまたはSVMのWebサービスへのアクセスを許可する	`vserver services web access create`
クラスタまたはSVMのWebサービスへのアクセスが許可されているロールを表示する	`vserver services web access show`
特定のロールに対して、クラスタまたはSVMのWebサービスへのアクセスを禁止する	`vserver services web access delete`

関連情報

"ONTAPコマンド リファレンス"

ONTAPノード上のマウントポイントを管理するためのコマンド

`spi`ウェブサービスは、ノードのログファイルまたはコアファイルへのアクセス要求に応じて、あるノードから別のノードのルートボリュームへのマウントポイントを自動的に作成します。マウントポイントを手動で管理する必要はありませんが、 `system node root-mount`コマンドを使用して管理できます。

状況	使用するコマンド
1つのノードから別のノードのルート ボリュームへのマウント ポイントを手動で作成する	`system node root-mount create`あるノードから別のノードへ存在できるマウント ポイントは 1 つだけです。

状況	使用するコマンド
クラスタ内のノードにある既存のマウント ポイントとその作成時刻、現在の状態を表示する	`system node root-mount show`
1つのノードから別のノードのルート ボリュームへのマウント ポイントを削除し、そのマウント ポイントへの接続を強制的に切断する	`system node root-mount delete`

関連情報

"ONTAPコマンド リファレンス"

ONTAPでのSSLの管理

`security ssl`コマンドを使用して、クラスタまたはストレージ仮想マシン（SVM）のSSLプロトコルを管理します。SSLプロトコルは、デジタル証明書を使用してWebサーバーとブラウザ間の暗号化された接続を確立することで、Webアクセスのセキュリティを強化します。

クラスタまたはStorage Virtual Machine（SVM）のSSLは次の方法で管理できます。

- SSLを有効にする
- デジタル証明書を生成してインストールし、クラスタまたはSVMと関連付ける
- SSL設定を表示してSSLが有効かどうかを確認し、可能な場合はSSL証明書名を確認する
- クラスタまたはSVMのファイアウォール ポリシーを設定して、Webアクセス要求が通過できるようにする
- 使用できるSSLのバージョンを定義する
- WebサービスのHTTPS要求のみにアクセスを制限する

SSLの管理用コマンド

`security ssl`コマンドを使用して、クラスタまたはStorage Virtual Machine（SVM）のSSLプロトコルを管理します。

状況	使用するコマンド
クラスタまたはSVMのSSLを有効にし、デジタル証明書と関連付ける	`security ssl modify`
クラスタまたはSVMのSSL設定と証明書名を表示する	`security ssl show`

`security ssl modify`および `security ssl show`
の詳細については、link:https://docs.netapp.com/us-en/ontap-cli/search.html?q=security+ssl["ONTAPコマンド リファレンス"^]をご覧ください。

ONTAP WebサービスにHSTSを使用する

HTTP Strict Transport Security（HSTS）は、プロトコルダウングレード攻撃やCookieハイジャックといった中間者攻撃からWebサイトを保護するためのWebセキュリティポリシーメカニズムです。HTTPSの使用を強制することで、HSTSはユーザーのブラウザとサーバ間のすべての通信が暗号化されることを保証します。ONTAP 9.17.1以降、ONTAPはONTAP WebサービスにHTTPS接続を強制できるようになりました。

HSTSは、ONTAPとの最初のセキュアなHTTPS接続が確立された後にのみ、Webブラウザによって適用されます。ブラウザが最初のセキュアな接続を確立しない場合、HSTSは適用されません。HSTSの管理については、ブラウザのドキュメントを参照してください。

タスク概要

- 9.17.1以降では、新規にインストールされたONTAPクラスタではHSTSがデフォルトで有効になっています。9.17.1にアップグレードすると、HSTSはデフォルトで有効になりません。アップグレード後にHSTSを有効にする必要があります。
- HSTS はすべての"ONTAP Webサービス"でサポートされています。

開始する前に

- 次のタスクには高度な権限が必要です。

HSTS設定を表示

現在の HSTS 構成を表示して、有効になっているかどうかを確認し、最大経過時間の設定を表示できます。

手順

1. `system services web show`コマンドを使用して、HSTS設定を含む現在のWebサービス構成を表示します：

```
cluster-1::system services web*> show

                    External Web Services: true
                                HTTP Port: 80
                               HTTPS Port: 443
                          Protocol Status: online
                       Per Address Limit: 80
                     Wait Queue Capacity: 192
                            HTTP Enabled: true
                  CSRF Protection Enabled: true
Maximum Number of Concurrent CSRF Tokens: 500
       CSRF Token Idle Timeout (Seconds): 900
   CSRF Token Absolute Timeout (Seconds): 0
          Allow Web Management via Cloud: true
Enforce Network Interface Service-Policy: -
                            HSTS Enabled: true
                  HSTS max age (Seconds): 63072000
```

HSTSを有効にして最大期間を設定する

ONTAP 9.17.1以降、新しいONTAPクラスタではHSTSがデフォルトで有効になっています。既存のクラスタを9.17.1以降にアップグレードする場合は、クラスタでHSTSを手動で有効にして、HTTPSの使用を強制する必要があります。HSTSを有効にして最大有効期間を設定できます。HSTSが有効になっている場合は、いつでも最大有効期間を変更できます。HSTSを有効にすると、ブラウザは最初のセキュア接続が確立された後にのみ、セキュア接続の強制を開始します。

手順

1. `system services web modify`コマンドを使用して、HSTS を有効にするか、最大経過時間を変更します：

```
system services web modify -hsts-enabled true -hsts-max-age <seconds>
```

`-hsts-max-age`ブラウザがHTTPSの適用を記憶する期間（秒数）を指定します。デフォルト値は63072000秒（2年）です。

HSTSを無効にする

ブラウザは接続ごとにHSTSの最大有効期間設定を保存し、ONTAPでHSTSが無効になっている場合でも、全期間にわたってHSTSを強制適用し続けます。HSTSが無効になった後、ブラウザがHSTSの強制適用を停止するまでには、設定された最大有効期間までかかります。この期間中に安全な接続が不可能になった場合、HSTSを強制適用しているブラウザは、問題が解決されるかブラウザの最大有効期間が切れるまで、ONTAP Webサービスへのアクセスを許可しません。

手順

1. `system services web modify`コマンドを使用して HSTS を無効にします：

```
system services web modify -hsts-enabled false
```

関連情報

"RFC 6797 - HTTP Strict Transport Security（HSTS）"

ONTAP Webサービスアクセスの問題のトラブルシューティング

設定エラーによって、Webサービスへのアクセスに関する問題が発生します。LIF、ファイアウォール ポリシー、Webプロトコル エンジン、Webサービス、デジタル証明書、およびユーザ アクセス認証がすべて正しく設定されていることを確認することで、エラーに対処できます。

次の表は、Webサービスの構成エラーを識別して対処するのに役立ちます：

このアクセスの問題...	この設定エラーが原因で発生します...	エラーを解決するには...
Webサービスにアクセスしようとすると、Webブラウザから `unable to connect`または `failure to establish a connection`エラーが返されます。	LIF が正しく設定されていない可能性があります。	Webサービスを提供するLIFにpingできることを確認します。 LIF を ping するには、 `network ping` コマンドを使用します。

このアクセスの問題...	この設定エラーが原因で発生します...	エラーを解決するには...
ファイアウォールが正しく構成されていない可能性があります。	HTTP または HTTPS をサポートするようにファイアウォール ポリシーが設定されており、そのポリシーが Web サービスを提供する LIF に割り当てられていることを確認します。 `system services firewall policy`コマンドを使用してファイアウォール ポリシーを管理します。`network interface modify`コマンドを `-firewall-policy`パラメータとともに使用して、ポリシーをLIFに関連付けます。	Webプロトコル エンジンが無効になっている可能性があります。
Webサービスにアクセスできるように、Webプロトコル エンジンが有効になっていることを確認します。 `system services web`コマンドを使用して、クラスタのWebプロトコル エンジンを管理します。	Web サービスにアクセスしようとすると、Web ブラウザから `not found`エラーが返されます。	Webサービスが無効になっている可能性があります。

このアクセスの問題...	この設定エラーが原因で発生します...	エラーを解決するには...
アクセスを許可する各 Web サービスが個別に有効になっていることを確認します。 `vserver services web modify`コマンドを使用して、Webサービスへのアクセスを有効にします。	Webブラウザは、ユーザーのアカウント名とパスワードを使用してWebサービスにログインできません。	ユーザーを認証できないか、アクセス方法が正しくないか、またはユーザーにWebサービスへのアクセス権限がありません。

このアクセスの問題...	この設定エラーが原因で発生します...	エラーを解決するには...
ユーザ アカウントが存在し、正しいアクセス方法と認証方法で設定されていることを確認してください。また、ユーザのロールにWebサービスへのアクセスが許可されていることを確認してください。 `security login`コマンドを使用して、ユーザアカウントとそのアクセス方法および認証方法を管理します。ONTAP API Webサービスにアクセスするには、`ontapi`アクセス方法が必要です。その他のすべてのWebサービスにアクセスするには、`http`アクセス方法が必要です。`vserver services web access`コマンドを使用して、ロールのWebサービスへのアクセスを管理します。	HTTPS を使用して Web サービスに接続すると、Web ブラウザに接続が中断されたことが示されます。	Web サービスを提供するクラスタまたはStorage Virtual Machine（SVM）でSSLが有効になっていない可能性があります。

このアクセスの問題...	この設定エラーが原因で発生します...	エラーを解決するには...
クラスタまたは SVM で SSL が有効になっており、デジタル証明書が有効であることを確認します。 `security ssl`コマンドを使用してHTTPサーバのSSL設定を管理し、`security certificate show`コマンドを使用してデジタル証明書情報を表示します。	HTTPS を使用して Web サービスに接続すると、Web ブラウザには接続が信頼できないと表示されます。	自己署名デジタル証明書を使用している可能性があります。

関連情報

- "ONTAPのネットワーク設定のベストプラクティスとは？"
- "network ping"
- "network interface modify"
- "セキュリティ証明書 generate-csr"
- "security certificate install"
- "セキュリティ証明書の表示"
- "セキュリティ SSL"