Web サービスを管理します

ONTAP 9

NetApp
April 24, 2024

目次

Web サービスを管理します

Manage Web Services の概要

クラスタまたは Storage Virtual Machine （ SVM ）の Web サービスを有効または無効にしたり、 Web サービスの設定を表示したり、ロールのユーザが Web サービスにアクセスできるかどうかを管理したりできます。

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 サービスを有効または無効にします
- Web サービスへのアクセスを暗号化された HTTP （ SSL ）のみに制限するかどうかを指定する
- Web サービスの可用性を表示します
- あるロールのユーザに Web サービスへのアクセスを許可するかどうか
- 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 Web サービスにアクセスするには、次の条件をすべて満たしている必要があります。

- ユーザが認証されている必要があります。

  たとえば、 Web サービスからユーザ名とパスワードの入力を求められる場合があります。ユーザの応答は有効なアカウントと一致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。

  指定された Web サービスの正しいアクセス方法が設定されたユーザのみが正常に認証されます。ONTAP API Webサービス用 `ontapi`）を使用する場合は、を使用する必要があります `ontapi` アクセス方法。その他のすべてのWebサービスの場合は、が必要です `http` アクセス方法。

  > を使用します `security login` ユーザのアクセス方法と認証方法を管理するコマンド。

- 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必要があります。

  > を使用します `vserver services web access` ロールのWebサービスへのアクセスを制御するコマンド。

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 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。

Web サービスへのアクセスを管理します

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 (`spi`)

  このサービスによって、ノードのログファイル、コアダンプファイル、および MIB ファイルに、クラスタ管理 LIF またはノード管理 LIF から HTTP または HTTPS でアクセスできるようになります。デフォルト設定はです `enabled`。

  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発生すると、が表示されます `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`)

  このサービスでは、 ONTAP API を実行し、リモートプログラムで管理機能を実行できます。デフォルト設定はです `enabled`。

  一部の外部管理ツールではこのサービスが必要になる場合があります。たとえば、 System Manager を使用する場合、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`)

  このサービスは、外部の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します。デフォルト設定はです `enabled`。

- Support Diagnostics（診断）の略 (`supdiag`)

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

- System Manager の略 (`sysmgr`)

  このサービスは、 ONTAP に組み込まれている System Manager の可用性を管理します。デフォルト設定はです `enabled`。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）の更新 (`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。デフォルト設定はです `enabled`。

- ONTAP のドキュメント (`docs`)

  このサービスでは、 ONTAP のドキュメントにアクセスできます。デフォルト設定はです `enabled`。

- ONTAP RESTful API (`docs_api`)

  このサービスを使用すると、 ONTAP RESTful API のドキュメントにアクセスできます。デフォルト設定

はです enabled。

- ファイルのアップロードとダウンロード (fud)

  このサービスは、ファイルのアップロードとダウンロードを提供します。デフォルト設定はです enabled。

- ONTAP メッセージング (ontapmsg)

  このサービスでは、イベントをサブスクライブできるパブリッシュおよびサブスクライブインターフェイスがサポートされています。デフォルト設定はです enabled。

- 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に実装します。デフォルト設定はです enabled。

- ONTAP RESTfulインターフェイス (rest)

  このサービスは、クラスタインフラのすべての要素をリモートで管理するために使用する RESTful インターフェイスをサポートします。デフォルト設定はです enabled。

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

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

- SAMLサービスプロバイダ (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。デフォルト設定はです enabled。

ONTAP 9.7 以降では、次の追加サービスがサポートされます。

- 設定バックアップファイル (backups)

  このサービスでは、構成バックアップファイルをダウンロードできます。デフォルト設定はです enabled。

- ONTAPのセキュリティ (security)

  このサービスでは、 CSRF トークン管理をサポートして認証を強化しています。デフォルト設定はです enabled。

Web プロトコルエンジンを管理します

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。Web プロトコルエンジンの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。

- を使用して、リモートクライアントがHTTPまたはHTTPSを使用してWebサービスコンテンツにアクセスできるかどうかを指定できます `system services web modify` コマンドにを指定します `-external` パラメータ
- を使用して、セキュアなWebアクセスにSSLv3を使用するかどうかを指定できます `security config modify` コマンドにを指定します `-supported-protocol` パラメータ
  デフォルトでは、 SSLv3 は無効になっています。Transport Layer Security 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。
- 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に対して、 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 準拠モードが無効な場合 *
    FIPS 140-2準拠モードを有効にするには、 `is-fips-enabled` パラメータの値 `true` をクリックします `security config modify` コマンドを実行し、を使用します `security config show` コマンドを使用してオンラインステータスを確認します。
  - * FIPS 140-2 準拠モードが有効な場合 *
    - ONTAP 9.11.1以降では、TLSv1、TLSv1.1、およびSSLv3は無効になり、TSLv1.2とTSLv1.3のみが有効なままになります。ONTAP 9の内部および外部にある他のシステムや通信に影響します。FIPS 140-2準拠モードを有効にし、その後無効にした場合、TLSv1、TLSv1.1、およびSSLv3は無効のままになります。TLSV.1またはTLSv1 1.3は、前の設定に応じて有効のままになります。
    - 9.11.1より前のバージョンのONTAP では、TLSv1とSSLv3は無効になり、TLSv1.1とTLSv1.2のみが引き続き有効になります。ONTAP では、 FIPS 140-2 準拠モードが有効な場合、 TLSv1 と SSLv3 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、その後無効にした場合、 TLSv1 と SSLv3 は無効なままですが、以前の設定によっては、 TLSv1.2 または TLSv1.1 と TLSv1.2 の両方が有効になります。
- 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 `system security config show` コマンドを実行します

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コマンド

を使用します `system services web` Webプロトコルエンジンを管理するコマンド。
を使用します `system services firewall policy create` および `network interface modify` 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するコマンド。

状況	使用するコマンド
クラスタレベルで Web プロトコルエンジンを設定します。 • クラスタの Web プロトコルエンジンを有効または無効にします • クラスタの SSLv3 を有効または無効にします • セキュアな Web サービス（ HTTPS ）に対する FIPS 140-2 準拠を有効または無効にする	`system services web modify`
クラスタレベルの Web プロトコルエンジンの設定を表示し、 Web プロトコルがクラスタ全体で機能しているかどうかを確認し、 FIPS 140-2 準拠が有効でオンラインになっているかどうかを表示します	`system services web show`
ノードレベルの Web プロトコルエンジンの設定と、クラスタ内のノードに対する 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` を設定します `-service` パラメータの値 `http` または `https` 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。
ファイアウォールポリシーを LIF と関連付ける	`network interface modify` を使用できます `-firewall-policy` LIFのファイアウォールポリシーを変更するためのパラメータ。

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ことで、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 ）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 サービスで使用される LIF のファイアウォールポリシーで HTTP または HTTPS のアクセスがセットアップされていることを確認してください。

   ファイアウォールが有効になっているかどうかは、を使用して確認できます `system services firewall show` コマンドを実行します

   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、を使用します `system services firewall policy show` コマンドを実行します

を設定します `-service` のパラメータ `system services firewall policy create` コマンドをに送信します `http` または `https` ポリシーで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をサポートしてい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、を使用します `network interface show` コマンドにを指定します `-firewall-policy` パラメータ

   を使用します `network interface modify` コマンドにを指定します `-firewall-policy` LIFに対してファイアウォールポリシーを有効にするためのパラメータ。

2. クラスタレベルのWebプロトコルエンジンを設定してWebサービスのコンテンツにアクセスできるようにするには、を使用します `system services web modify` コマンドを実行します
3. セキュアなWebサービス（HTTPS）を使用する場合は、SSLを有効にし、を使用してクラスタまたはSVMのデジタル証明書情報を入力します `security ssl modify` コマンドを実行します
4. クラスタまたはSVMでWebサービスを有効にするには、を使用します `vserver services web modify` コマンドを実行します

   この手順は、クラスタまたは SVM に対して有効にする各サービスについて繰り返す必要があります。

5. 特定のロールにクラスタまたはSVMのWebサービスへのアクセスを許可するには、を使用します `vserver services web access create` コマンドを実行します

   アクセスを許可するロールはすでに存在している必要があります。を使用して、既存のロールを表示できます `security login role show` コマンドを実行するか、を使用して新しいロールを作成します `security login role create` コマンドを実行します

6. Webサービスへのアクセスが許可されているロールについては、の出力を確認して、ユーザにも正しいアクセス方法が設定されていることを確認してください `security login show` コマンドを実行します

   をクリックしてONTAP API Webサービスにアクセスします `ontapi`）を使用してユーザを設定する必要があります `ontapi` アクセス方法。他のすべてのWebサービスにアクセスするには、ユーザがで設定されている必要があります `http` アクセス方法。

   > を使用します `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。

Web サービスを管理するためのコマンド

を使用します `vserver services web` クラスタまたはStorage Virtual Machine（SVM）のWebサービスの可用性を管理するためのコマンド。を使用します `vserver services web access` ロールのWebサービスへのアクセスを制御するコマンド。

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します • Web サービスへのアクセスに HTTPS だけを使用できるようにするかどうかを指定します	`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します	`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 9コマンド"

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` Web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、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、を使用して管理できます `system node root-mount` コマンド

状況	使用するコマンド
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します	`system node root-mount create` ノード間で作成できるマウントポイントは1つだけです。
クラスタ内のノード上の既存のマウントポイントを、マウントポイントが作成された時刻と現在の状態を含めて表示します	`system node root-mount show`
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終了します	`system node root-mount delete`

関連情報

"ONTAP 9コマンド"

SSLの管理

SSL プロトコルは、デジタル証明書を使用して Web サーバとブラウザの間に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向上させます。

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 の有効化
- 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 証明書名を表示します
- 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、 Web アクセス要求が通過できるようにします
- 使用できる SSL のバージョンを定義します
- 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

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

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、デジタル証明書を関連付けます	`security ssl modify`
クラスタまたは SVM の SSL 設定と証明書の名前を表示する	`security ssl show`

Web サービスへのアクセスに関する問題のトラブルシューティングを行う

設定エラー原因 Web サービスへのアクセスに関する問題が発生します。このエラーに対応するには、 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、 すべてのユーザアクセス許可が正しく設定されていることを確認します。

次の表は、 Web サービスの設定エラーを特定して対処する際に役立ちます。

アクセスに関する問題	原因となる設定エラー	エラーに対処する方法
Webブラウザからが返されます `unable to connect` または `failure to establish a connection` Webサービスにアクセスしようとするとエラーが発生します。	LIF が正しく設定されていない可能性があります。	Web サービスを配信する LIF に ping を送信できることを確認します。 を使用します `network ping` コマンドを使用してLIFにpingを送信します。ネットワーク設定の詳細については、『ネットワーク管理ガイド』を参照してください。
ファイアウォールが正しく設定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いて、ポリシーが Web サービスを配信する LIF に割り当てられていることを確認します。 を使用します `system services firewall policy` ファイアウォールポリシーを管理するためのコマンド。を使用します `network interface modify` コマンドにを指定します `-firewall -policy` ポリシーをLIFに関連付けるためのパラメータ。	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 プロトコルエンジンが有効になっていて、 Web サービスがアクセス可能であることを確認します。 を使用します `system services web` クラスタのWebプロトコルエンジンを管理するコマンド。	Webブラウザからが返されます `not found` Webサービスにアクセスしようとするとエラーが発生します。	Web サービスが無効になっている可能性があります。

アクセスに関する問題	原因となる設定エラー	エラーに対処する方法
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。 を使用します `vserver services web modify` Webサービスへのアクセスを有効にするコマンド。	Web ブラウザで、ユーザ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ない。	ユーザを認証できない、アクセス方法が正しくない、またはユーザに Web サービスへのアクセスが許可されていない
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が設定されていることを確認します。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ます。 を使用します `security login` ユーザアカウント、そのアクセス方法、および認証方法を管理するコマンド。ONTAP API Webサービスにアクセスするにはが必要です `ontapi` アクセス方法。他のすべてのWebサービスにアクセスするにはが必要です `http` アクセス方法。を使用します `vserver services web access` ロールのWebサービスへのアクセスを管理するコマンド。	HTTPS を使用して Web サービスに接続すると、接続が中断されたことが Web ブラウザに表示されます。	Web サービスを配信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る

アクセスに関する問題	原因となる設定エラー	エラーに対処する方法
クラスタまたは SVM で SSL が有効になっていて、デジタル証明書が有効であることを確認します。 を使用します `security ssl` HTTPサーバおよびのSSL設定を管理するコマンド `security certificate show` デジタル証明書情報を表示するコマンド。	HTTPS を使用して Web サービスに接続すると、信頼されていない接続であると Web ブラウザに表示されます。	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。