Webサービスを管理します。

ONTAP 9

NetApp
December 20, 2024

目次

Webサービスを管理します。

Webサービスの管理の概要

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サービスの有効化と無効化
- 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の指定
- Webサービスの可用性の表示
- あるロールのユーザに対するWebサービスへのアクセスの許可と禁止
- 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、次の条件がすべて満たされ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。ユーザー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。

  認証が成功するのは、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だけです。ONTAP API Webサービス `ontapi`の場合）、ユーザにアクセス方法が必要です `ontapi`。それ以外のすべてのWebサービスでは、ユーザにアクセス方法が設定されている必要があります `http`。

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

- ユーザのアクセス制御ロールを許可するようにWebサービスが設定されている必要があります。

  ロールのWebサービスへのアクセスを制御するには、コマンドを使用し `vserver services web access`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 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、ユーザがHTTPまたはHTTPSを使用して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することができます。

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`)

  このサービスにより、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、Webサービスは `spi`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 (`ontapi`API)

  このサービスでは、ONTAP APIを実行して、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を使用する場合は、このサービスを有効なままにしておく必要があります。

- Data ONTAP検出(`disco`)

  このサービスを使用すると、外部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。デフォルト設定はです `enabled`。

- 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 (`sysmgr`Manager)

  このサービスは、ONTAPに含まれる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）のアップデート(`FW_BMC`

  このサービスでは、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のマニュアル(`docs`を参照)

  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`)

  このサービスでは、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をサポートしています。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、RESTfulインターフェイスをサポートしています。このインターフェイスを使用して、クラスタインフラのすべての要素をリモートで管理できます。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。

- 構成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セキュリティ(security)

  このサービスは、認証を強化するためのCSRFトークン管理をサポートします。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て、Webアクセスを許可するかどうか、およびどのSSLバージョンを使用できるかを制御できます。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。

- コマンドでパラメータを指定する `-external`と、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`。
- コマンドでパラメータを指定する `-supported-protocol`と、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`。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）が有効になっており、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。

  デフォルトでは、FIPS 140-2準拠モードは無効になっています。

  - * FIPS 140-2準拠モードが無効になっている場合*コマンドの `security config modify`パラメータを `true`に設定し、コマンドを使用して `security config show`オンラインステータスを確認することで、FIPS 140-2準拠モードを有効にできます `is-fips-enabled`。
  - * 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および通信に影響します。FIPS 140-2準拠モードを有効にしたあとに無効にした場合、TLSv1、TLSv1.1、およびSSLv3は無効なままになります。以前の設定に応じて、TLSv1.2またはTLSv1.3のいずれかが有効なままになります。
    - 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たあとに無効にした場合、TLSv1とSSLv3は無効なままですが、以前の設定に応じてTLSv1.2またはTLSv1.1とTLSv1.2の両方が有効になります。
- コマンドを使用すると、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`。

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変更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の管理用コマンド

Webプロトコルエンジンを管理するには、コマンドを使用し `system services web`ます。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には、コマンドと `network interface modify`コマンドを使用し `system services firewall policy create`ます。

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` パラメータをまたは `https`に `http`設定する `-service`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 と関連付ける	`network interface modify` パラメータを使用すると、LIFのファイアウォールポリシーを変更できます `-firewall-policy`。

Webサービスへのアクセスの設定

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を確認するには、コマンドを使用し `system services firewall show`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、コマンドを使用し `system services firewall policy show`ます。

ポリシーでWebアクセスをサポートするには、コマンドのパラメータを `system services firewall policy create`または `https`に `http`設定し `-service`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、パラメータを指定してコマンドを `-firewall-policy`使用し `network interface show`ます。

LIFに対してファイアウォールポリシーを有効にするには、コマンドで `-firewall-policy`パラメータを使用し `network interface modify`ます。

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、コマンドを使用し `system services web modify`ます。
3. セキュアなWebサービス（HTTPS）を使用する場合は、コマンドを使用してSSLを有効にし、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`。
4. クラスタまたはSVMでWebサービスを有効にするには、コマンドを使用し `vserver services web modify`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、コマンドを使用し `vserver services web access create`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。既存のロールを表示する `security login role show`にはコマンドを使用します。新しいロールを作成するにはコマンドを使用します `security login role create`。

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、コマンドの出力を確認して、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 `security login show`ください。

ONTAP API Webサービスにアクセスするには `ontapi`）、ユーザにアクセス方法が設定されている必要があります `ontapi`。他のすべてのWebサービスにアクセスするには、ユーザにアクセス方法が設定されている必要があり `http`ます。

ユーザのアクセス方法を追加するには、コマンドを使用し `security login create`ます。

Webサービスの管理用コマンド

クラスタまたはStorage Virtual Machine（SVM）でのWebサービスの使用を管理するには、コマンドを使用し `vserver services web`ます。ロールのWebサービスへのアクセスを制御するには、コマンドを使用し `vserver services web access`ます。

状況	使用するコマンド
クラスタまたはSVMのWebサービスを設定します。 • 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のみを使用できるかどうかを指定する	`vserver services web modify`

状況	使用するコマンド
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`
特定のロールがクラスタまたはSVMのWebサービスにアクセスできないようにする	`vserver services web access delete`

関連情報

"ONTAPコマンド リファレンス"

ノード上のマウントポイントの管理用コマンド

Webサービスは `spi`、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、コマンドを使用して管理できます `system node root-mount`。

状況	使用するコマンド
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手動で作成する	`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する	`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する	`system node root-mount delete`

関連情報

"ONTAPコマンド リファレンス"

SSLの管理

コマンドを使用して `security ssl`、クラスタまたはStorage Virtual Machine（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が有効になっているかどうかを確認し、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する
- 使用できるSSLのバージョンの定義
- 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

クラスタまたはStorage Virtual Machine（SVM）のSSLプロトコルを管理するには、コマンドを使用し`security ssl`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、デジタル証明書を関連付ける	`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

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サービスにアクセスしようとすると、Webブラウザからまたは `failure to establish a connection`エラーが返されます `unable to connect。	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。 LIFにpingを送信するには、コマンドを使用し `network ping`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。 ファイアウォールポリシーを管理するには、コマンドを使用し `system services firewall policy`ます。ポリシーとLIFを関連付けるには、コマンドと `-firewall-policy`パラメータを使用し `network interface modify`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 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。 クラスタのWebプロトコルエンジンを管理するには、コマンドを使用し `system services web`ます。	Webサービスにアクセスしようとすると、Webブラウザからエラーが返され `not found`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。 Webサービスへのアクセスを有効にするには、コマンドを使用し `vserver services web modify`ます。	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。 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には、コマンドを使用し `security login`ます。ONTAP API Webサービスにアクセスするには、アクセス方法が必要 `ontapi`です。他のすべてのWebサービスにアクセスするには、アクセス方法が必要 `http`です。Webサービスへのロールのアクセスを管理するには、コマンドを使用し `vserver services web access`ます。	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。 HTTPサーバのSSL設定を管理するにはコマンドを使用し、デジタル証明書情報を表示するにはコマンドを `security certificate show`使用し `security ssl`ます。	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。

著作権に関する情報

商標に関する情報