# Active IQ Unified Managerの設定

Active IQ Unified Manager

NetApp
November 13, 2026

This PDF was generated from https://docs.netapp.com/ja-jp/active-iq-unified-manager-918/config/concept_configure_unified_manager.html on November 13, 2026. Always check docs.netapp.com for the latest.

# 目次


Active IQ Unified Managerの設定 1
- Active IQ Unified Manager の設定について 1
- Active IQ Unified Manager の設定手順について 1
- Active IQ Unified Manager の Web UI にアクセスする 1
- Active IQ Unified Manager ウェブ UI の初期設定を実行する 2
- Active IQ Unified Manager にクラスターを追加する 4
- 通知を設定する 6
  - Active IQ Unified Manager でアラート通知を送信するように設定する 6
  - Active IQ Unified Manager でイベント通知設定を構成する 7
  - Active IQ Unified Manager でリモート認証を有効にする 8
  - Active IQ Unified Manager でリモート認証のネストされたグループを無効にする 9
  - Active IQ Unified Manager で認証サービスを設定する 10
  - Active IQ Unified Manager に認証サーバーを追加する 11
  - Active IQ Unified Manager で認証サーバーの構成をテストする 12
  - Active IQ Unified Manager でアラートを追加する 13
- Active IQ Unified Manager でローカルユーザーのパスワードを変更する 15
- Active IQ Unified Manager でセッションの非アクティブタイムアウトを設定する 15
- Active IQ Unified Manager でCLIを使用してセッションタイムアウトを設定する 16
- Unified Managerのホスト名の変更 16
  - Active IQ Unified Manager 仮想アプライアンスのホスト名を変更する 16
  - Active IQ Unified Manager でHTTPSセキュリティ証明書を生成する 17
  - Active IQ Unified Manager 仮想マシンを再起動する 19
  - Linux システム上の Active IQ Unified Manager ホスト名の変更 19
- Active IQ Unified Manager でのポリシーベースのストレージ管理の有効化と無効化 20

# Active IQ Unified Managerの設定

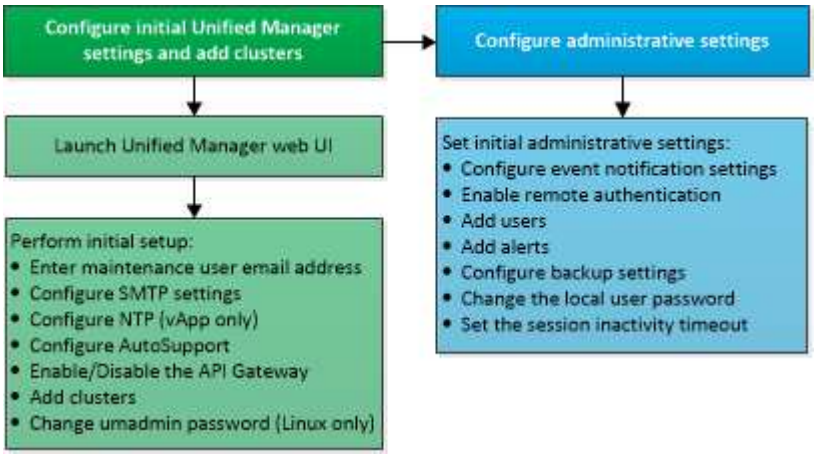
## Active IQ Unified Manager の設定について

Active IQ Unified Manager（旧OnCommand Unified Manager）をインストールしたら、Web UIにアクセスするために初期セットアップ（初期設定ウィザード）を完了する必要があります。初期セットアップを完了すると、クラスタの追加、リモート認証の設定、ユーザの追加、アラートの追加など、その他の設定作業を実行できるようになります。

このマニュアルに記載されている手順の一部は、Unified Managerインスタンスの初期設定を完了するために必要です。その他の手順は、新しいインスタンスで設定すると便利な推奨構成設定、またはONTAPシステムの定期的な監視を開始する前に知っておくと役立つ設定です。

## Active IQ Unified Manager の設定手順について

構成ワークフローでは、Unified Managerを使用する前に実行する必要のあるタスクについて説明します。




## Active IQ Unified Manager の Web UI にアクセスする

Unified Managerをインストールしたら、ONTAPシステムの監視を開始できるように、Web UIにアクセスしてUnified Managerをセットアップします。

開始する前に

- Web UIへのアクセスが初めての場合は、メンテナンス ユーザ（Linux環境の場合はumadminユーザ）としてログインする必要があります。
- 完全修飾ドメイン名（FQDN）またはIPアドレスの代わりに短縮名を使用したUnified Managerへのアクセスをユーザに許可する場合は、短縮名が有効なFQDNに解決されるようにネットワークを設定する必要があります。
- 自己署名のデジタル証明書がサーバで使用されている場合、信頼されていない証明書であることを伝える警告がブラウザ画面に表示されることがあります。その場合は、危険を承諾してアクセスを続行するか、認証局（CA）の署名のあるデジタル証明書をインストールしてサーバを認証します。

手順

1. インストールの完了時に表示されたURLを使用して、ブラウザからUnified Manager Web UIを起動します。URLは、Unified ManagerサーバのIPアドレスまたは完全修飾ドメイン名（FQDN）です。

   リンクの形式は次のとおりです： `https://URL`。

2. メンテナンス ユーザのクレデンシャルを使用して、Unified Manager Web UIにログインします。

> 1時間以内にWeb UIへのログインに3回連続して失敗すると、システムからロックアウトされ、システム管理者への連絡が必要になります。これはローカル ユーザにのみ該当します。

# Active IQ Unified Manager ウェブ UI の初期設定を実行する

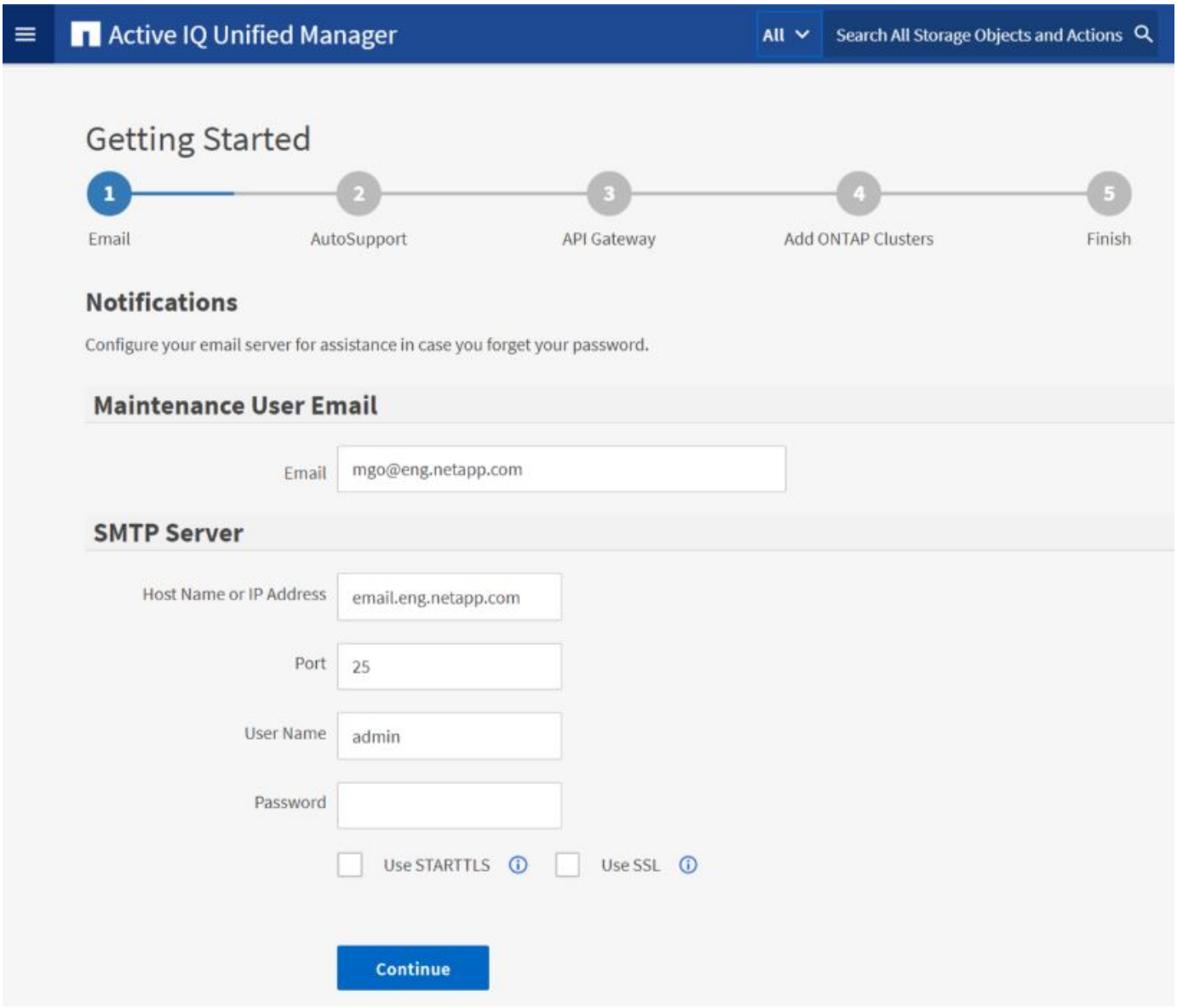
Unified Managerを使用するには、NTPサーバ、メンテナンス ユーザのEメール アドレス、SMTPサーバのホストなどを最初に設定し、ONTAPクラスタを追加する必要があります。

開始する前に

次の作業を完了しておきます。

- インストールの完了時に表示されたURLを使用してUnified Manager Web UIを起動します。
- インストール時に作成したメンテナンス ユーザ（Linux環境の場合はumadminユーザ）の名前とパスワードを使用してログインします。

Active IQ Unified Managerの[はじめに]ページは、Web UIへの初回アクセス時にのみ表示されます。次のページはVMware環境の場合の例を示したものです。




これらのオプションをあとで変更する場合は、Unified Managerの左側のナビゲーション ペインの[全般]オプションから選択できます。NTP設定はVMware専用です。この設定はあとからUnified Managerメンテナンスコンソールを使用して変更できます。

手順

1. Active IQ Unified Manager の初期設定ページで、メンテナンスユーザーのメールアドレス、SMTP サーバーのホスト名、その他の SMTP オプション、および NTP サーバー（VMware インストールの場合のみ）を入力します。次に「続行」をクリックします。

   *STARTTLSを使用する*または*SSLを使用する*オプションを選択した場合、*続行*ボタンをクリックすると証明書ページが表示されます。証明書の詳細を確認し、証明書を承認して、Web UIの初期設定を続行してください。

2. AutoSupport ページで **[Agree and Continue]** をクリックして、Unified Manager から NetAppActive IQ への AutoSupport メッセージの送信を有効にします。

   インターネットアクセスを提供するためにプロキシを指定して AutoSupport コンテンツを送信する必要がある場合、または AutoSupport を無効にする場合は、Web UI から **General** > **AutoSupport** オプションを

使用してください。

3. Red Hat システムでは、umadmin ユーザーのパスワードをデフォルトの「admin」文字列から、独自の文字列に変更してください。
4. [APIゲートウェイのセットアップ]ページで、監視対象のONTAPクラスタをUnified ManagerでONTAP REST APIを使用して管理できるようにAPIゲートウェイ機能を使用するかどうかを選択します。次に「続行」をクリックします。

   この設定は、Web UI の「一般」>「機能設定」>「API ゲートウェイ」から後で有効または無効にできます。API の詳細については、"Active IQ Unified Manager REST APIでの作業の開始"を参照してください。

5. Unified Managerで管理するクラスターを追加し、「次へ」をクリックします。管理する各クラスターについて、ホスト名またはクラスター管理IPアドレス（IPv4またはIPv6）と、ユーザー名およびパスワードの認証情報が必要です。ユーザーは「admin」ロールを持っている必要があります。

   この手順は任意です。クラスターは、Web UI の「ストレージ管理」>「クラスター設定」から後から追加できます。

6. 概要ページで、すべての設定が正しいことを確認し、*完了*をクリックします。

[はじめに]ページが閉じ、Unified Managerの[ダッシュボード]ページが表示されます。

# Active IQ Unified Manager にクラスターを追加する

Active IQ Unified Managerにクラスタを追加して監視することができます。たとえば、クラスタの健全性、容量、パフォーマンス、構成などの情報を取得して、発生する可能性がある問題を特定して解決したりできます。

開始する前に

- アプリケーション管理者またはストレージ管理者のロールが必要です。
- 次の情報が必要です。
  - Unified Managerは、オンプレミスのONTAPクラスタ、ONTAP Select、Cloud Volumes ONTAPをサポートしています。
  - ホスト名またはクラスタ管理IPアドレス

    ホスト名は、Unified Managerがクラスタに接続するために使用する完全修飾ドメイン名（FQDN）または短縮名です。ホスト名は、クラスタ管理IPアドレスに解決できる必要があります。

    クラスタ管理IPアドレスは、管理用Storage Virtual Machine（SVM）のクラスタ管理LIFであることが必要です。ノード管理LIFを使用すると処理に失敗します。

  - クラスタでONTAPバージョン9.1以降が実行されている必要があります。
  - ONTAP管理者のユーザ名とパスワード

    このアカウントには、アプリケーションアクセスが *ontapi*、*amqp*、*console*、および *http* に設定された *admin* ロールが必要です。

  - HTTPSプロトコルを使用してクラスタに接続するポート番号（通常はポート443）

◦ 必要な証明書を用意しておきます。

**SSL（HTTPS）**証明書：この証明書はUnified Managerが所有しています。Unified Managerを新規インストールすると、デフォルトで自己署名SSL（HTTPS）証明書が生成されます。NetAppでは、セキュリティ向上のため、CA署名付き証明書へのアップグレードをお勧めします。サーバー証明書の有効期限が切れた場合は、証明書を再生成し、Unified Managerを再起動して、サービスに新しい証明書を反映させる必要があります。SSL証明書の再生成の詳細については、"HTTPSセキュリティ証明書の生成"を参照してください。

**EMS**証明書：この証明書はUnified Managerが所有しています。これは、ONTAPから受信したEMS通知の認証時に使用されます。

相互**TLS**通信用の証明書：Unified ManagerとONTAP間の相互TLS通信時に使用されます。証明書ベースの認証は、ONTAPのバージョンに基づいてクラスタに対して有効になります。クラスタで実行されているONTAPのバージョンが9.5より前の場合、証明書ベースの認証は有効になりません。

Unified Managerの旧バージョンを更新する場合、証明書ベースの認証はクラスタに対して自動的に有効になりません。ただし、クラスタの詳細を変更して保存することで有効にすることができます。証明書の有効期限が切れた場合は、新しい証明書を組み込むために証明書を再生成する必要があります。証明書の表示と再生成の詳細については、"クラスタの編集"を参照してください。

◦ クラスタはWeb UIから追加でき、証明書ベースの認証が自動的に有効になります。

◦ Unified Manager CLIを介してクラスターを追加できますが、証明書ベースの認証はデフォルトでは有効になっていません。Unified Manager CLIを使用してクラスターを追加した場合、Unified Manager UIを使用してクラスターを編集する必要があります。Unified Manager CLIを使用してクラスターを追加するには、"サポートされるUnified Manager のCLIコマンド"を参照してください。

◦ クラスターで証明書ベースの認証が有効になっている場合、サーバーからUnified Managerのバックアップを取得し、ホスト名またはIPアドレスが変更された別のUnified Managerサーバーに復元すると、クラスターの監視が失敗する可能性があります。このエラーを回避するには、クラスターの詳細を編集して保存してください。クラスターの詳細編集に関する詳細については、"クラスタの編集"を参照してください。

+ クラスタ証明書：この証明書はONTAPが所有しています。有効期限切れの証明書では、Unified Managerにクラスタを追加できません。証明書の有効期限がすでに切れている場合は、クラスタを追加する前に証明書を再生成する必要があります。証明書の生成に関する情報については、ナレッジベース（KB）の記事 "System Managerのユーザーインターフェイスでの自己署名証明書を更新する方法"を参照してください。

- Unified Managerサーバに十分なスペースが必要です。データベース ディレクトリのスペースの使用率が90%を超えている場合、サーバにクラスタを追加することはできません。

MetroCluster構成では、ローカル クラスタとリモート クラスタの両方を追加し、追加したクラスタを正しく設定する必要があります。

手順

1. 左側のナビゲーションペインで、ストレージ管理 > *クラスタ設定*をクリックします。
2. クラスター設定ページで、*追加*をクリックします。
3. [クラスタの追加]ダイアログ ボックスで、クラスタのホスト名またはIPアドレス、ユーザ名、パスワード、ポート番号など、必要な値を指定します。

クラスタ管理IPアドレスは、IPv6からIPv4またはIPv4からIPv6に変更できます。次の監視サイクルが完了すると、クラスタ グリッドとクラスタ設定ページに新しいIPアドレスが反映されます。

4. 「送信」をクリックしてください。
5. 「ホストの認証」ダイアログボックスで、*証明書の表示*をクリックして、クラスタに関する証明書情報を表示します。
6. *はい*をクリックします。

   クラスタの詳細を保存したあとに相互TLS通信用の証明書を表示できます。

   証明書ベースの認証が有効になっていない場合、Unified Managerではクラスタの初回追加時にのみ証明書がチェックされます。ONTAPへのAPI呼び出しのたびに証明書がチェックされることはありません。

新しいクラスタのオブジェクトがすべて検出されると、Unified Managerは過去15日間のパフォーマンス データの収集を開始します。これらの統計は、データの継続性収集機能を使用して収集されます。この機能では、クラスタが追加された直後から2週間分のクラスタのパフォーマンス情報を入手できます。データの継続性収集サイクルが完了すると、リアルタイムのクラスタ パフォーマンス データが収集されます（デフォルトでは5分間隔）。

15日分のパフォーマンス データを収集するとCPUに負荷がかかるため、新しいクラスタを複数追加する場合は、データの継続性収集のポーリングが同時に多数のクラスタで実行されないように、時間差をつけて追加するようにしてください。また、データの継続性収集期間にUnified Managerを再起動すると、収集が停止し、その間のデータがパフォーマンス グラフに表示されません。

エラー メッセージが表示されてクラスタを追加できない場合は、2つのシステムのクロックが同期されておらず、Unified ManagerのHTTPS証明書の開始日がクラスタの日付よりもあとの日付になっていないかを確認してください。この場合、NTPなどのサービスを使用してクロックを同期する必要があります。

関連情報

"CAの署名を受けて返されたHTTPS証明書のインストール"

# 通知を設定する

## **Active IQ Unified Manager** でアラート通知を送信するように設定する

Unified Managerでは、環境内のイベントについて警告する通知を送信するように設定することができます。通知を送信するには、Unified Managerのその他いくつかのオプションを設定する必要があります。

開始する前に

アプリケーション管理者のロールが必要です。

Unified Managerを導入して初期設定を完了したら、イベントの受信に対してアラートをトリガーし、通知EメールやSNMPトラップを生成するように設定することを検討する必要があります。

手順

1. "イベント通知を設定"。

   特定のイベントが発生したときにアラート通知を送信するには、SMTPサーバを設定し、アラート通知の送信元のEメール アドレスを指定する必要があります。SNMPトラップを使用する場合は、該当するオプションを選択し、必要な情報を指定します。

2. "リモート認証を有効化する"。

   リモートLDAPユーザまたはActive Directoryユーザが Unified Managerインスタンスにアクセスしてアラート通知を受信できるようにするには、リモート認証を有効にする必要があります。

3. "認証サーバを追加する"。

   認証サーバを追加することで、認証サーバ内のリモート ユーザが Unified Managerにアクセスできるようにすることができます。

4. "ユーザの追加"。

   さまざまなタイプのローカル ユーザやリモート ユーザを追加し、特定のロールを割り当てることができます。アラートを作成する際に、アラート通知を受信するユーザを指定します。

5. "アラートの追加"。

   通知を送信するEメール アドレスの追加、通知を受信するユーザの追加、ネットワークの設定、環境に必要なSMTPオプションとSNMPオプションの設定が完了したら、アラートを割り当てることができます。

## Active IQ Unified Manager でイベント通知設定を構成する

Unified Managerでは、イベントが生成されたときやユーザに割り当てられたときにアラート通知を送信するように設定することができます。アラートの送信に使用するSMTPサーバの設定や、さまざまな通知メカニズムの設定が可能です。たとえば、アラート通知はEメールやSNMPトラップとして送信できます。

開始する前に

次の情報が必要です。

- アラート通知の送信元Eメール アドレス

  送信されたアラート通知の「From」フィールドにメールアドレスが表示されます。何らかの理由でメールが配信できない場合、このメールアドレスは配信不能メールの受信者としても使用されます。

- SMTPサーバのホスト名とアクセスに使用するユーザ名およびパスワード
- SNMPトラップとSNMPバージョン、アウトバウンド トラップ ポート、コミュニティ、およびその他の必要なSNMP設定値を受信するトラップ送信先ホストのホスト名またはIPアドレス

  トラップの送信先を複数指定するには、各ホストをカンマで区切ります。この場合、他のすべてのSNMP設定（バージョンやアウトバウンド トラップ ポートなど）がリスト内のすべてのホストで同じである必要があります。

アプリケーション管理者またはストレージ管理者のロールが必要です。

手順

1. 左側のナビゲーションペインで、**[General]** > **[Notifications]** をクリックします。
2. [通知]ページで、該当する項目を設定します。

   注：

   - 送信元アドレスに「ActiveIQUnifiedManager@localhost.com」というアドレスがあらかじめ入力されている場合は、すべてのメール通知が正常に配信されるように、実際に使用可能なメールアドレスに変更してください。
   - SMTPサーバのホスト名を解決できない場合は、SMTPサーバのホスト名の代わりにIPアドレス（IPv4またはIPv6）を指定できます。
3. *保存*をクリックします。
4. 「STARTTLSを使用する」または「SSLを使用する」オプションを選択した場合、「保存」ボタンをクリックすると証明書ページが表示されます。証明書の詳細を確認し、証明書を承認して通知設定を保存してください。

   「証明書の詳細を表示」*ボタンをクリックすると、証明書の詳細が表示されます。既存の証明書の有効期限が切れている場合は、「STARTTLSを使用する」または「SSLを使用する」のチェックボックスをオフにして通知設定を保存し、再度「STARTTLSを使用する」または「SSLを使用する」*のチェックボックスをオンにして新しい証明書を表示してください。

## Active IQ Unified Manager でリモート認証を有効にする

Unified Managerサーバが認証サーバと通信できるように、リモート認証を有効にすることができます。認証サーバのユーザがUnified Managerのグラフィカル インターフェイスにアクセスしてストレージ オブジェクトとデータを管理できるようになります。

開始する前に

アプリケーション管理者のロールが必要です。

> Unified Managerサーバは認証サーバに直接接続する必要があります。SSSD（System Security Services Daemon）やNSLCD（Name Service LDAP Caching Daemon）などのローカルのLDAPクライアントは無効にする必要があります。

リモート認証は、Open LDAPまたはActive Directoryのいずれかを使用して有効にすることができます。リモート認証が無効になっている場合、リモート ユーザはUnified Managerにアクセスできません。

リモート認証は、LDAPとLDAPS（セキュアなLDAP）でサポートされます。Unified Managerでは、セキュアでない通信にはポート389、セキュアな通信にはポート636がデフォルトのポートとして使用されます。

> ユーザの認証に使用する証明書は、X.509形式に準拠している必要があります。

手順

1. 左側のナビゲーションペインで、**[全般]** > **[リモート認証]** をクリックします。
2. 「リモート認証を有効にする…」のチェックボックスをオンにしてください。
3. [認証サービス]フィールドで、サービスの種類を選択し、認証サービスを設定します。

| 認証タイプについて... | 以下の情報を入力してください... |
| --- | --- |
| Active Directory | • 認証サーバの管理者の名前（次のいずれかの形式を使用）<br>◦ `domainname\username`<br>◦ `username@domainname`<br>◦ `Bind Distinguished Name`（適切なLDAP表記法を使用）<br>• 管理者のパスワード<br>• ベース識別名（適切なLDAP表記を使用） |
| Open LDAP | • バインド識別名（適切なLDAP表記を使用）<br>• バインドパスワード<br>• ベース識別名 |

Active Directoryユーザの認証に時間がかかる場合やタイムアウトする場合は、認証サーバからの応答に時間がかかっている可能性があります。Unified Managerでネストされたグループのサポートを無効にすると、認証時間が短縮される可能性があります。

認証サーバの設定で[セキュアな接続を使用]オプションを選択すると、Unified Managerと認証サーバの間の通信にSecure Sockets Layer（SSL）プロトコルが使用されます。

4. オプション： 認証サーバを追加し、認証をテストします。
5. *保存*をクリックします。

## Active IQ Unified Manager でリモート認証のネストされたグループを無効にする

リモート認証を有効にしている場合、ネストされたグループの認証を無効にすることで、リモートからのUnified Managerへの認証を個々のユーザにのみ許可し、グループのメンバーは認証されないようにすることができます。ネストされたグループを無効にすると、Active Directory認証の応答時間を短縮できます。

開始する前に

- アプリケーション管理者のロールが必要です。
- ネストされたグループの無効化は、Active Directoryを使用している場合にのみ該当します。

Unified Managerでネストされたグループのサポートを無効にすると、認証時間が短縮される可能性があります。ネストされたグループが無効になっているUnified Managerにリモート グループを追加した場合、Unified Managerで認証されるためには個々のユーザがそのリモート グループのメンバーである必要があります。

手順

1. 左側のナビゲーションペインで、**[全般]** > **[リモート認証]** をクリックします。
2. 「ネストされたグループ検索を無効にする」のチェックボックスをオンにします。
3. *保存*をクリックします。

## Active IQ Unified Manager で認証サービスを設定する

認証サービスを使用すると、Unified Managerへのアクセスを許可する前に、リモート ユーザまたはリモート グループを認証サーバで認証できます。事前定義された認証サービス（Active DirectoryやOpenLDAPなど）を使用するか、または独自の認証メカニズムを設定してユーザを認証できます。

開始する前に

- リモート認証を有効にしておく必要があります。
- アプリケーション管理者のロールが必要です。

手順

1. 左側のナビゲーションペインで、**[全般]** > **[リモート認証]** をクリックします。
2. 次のいずれかの認証サービスを選択します。

| 選択すると... | 操作 |
| --- | --- |
| Active Directory | a. 管理者の名前とパスワードを入力します。<br>b. 認証サーバのベース識別名を指定します。<br><br>例えば、認証サーバのドメイン名が ou@domain.com の場合、ベース識別名は **cn=ou,dc=domain,dc=com** です。 |
| OpenLDAP | a. バインド識別名とバインド パスワードを入力します。<br>b. 認証サーバのベース識別名を指定します。<br><br>例えば、認証サーバのドメイン名が ou@domain.com の場合、ベース識別名は **cn=ou,dc=domain,dc=com** です。 |
| その他 | a. バインド識別名とバインド パスワードを入力します。<br>b. 認証サーバのベース識別名を指定します。<br><br>例えば、認証サーバのドメイン名が ou@domain.com の場合、ベース識別名は **cn=ou,dc=domain,dc=com** です。<br><br>c. 認証サーバでサポートされているLDAPプロトコルのバージョンを指定します。<br>d. ユーザ名、グループ メンバーシップ、ユーザ グループ、およびメンバーの属性を入力します。 |

認証サービスを変更する場合は、既存の認証サーバを削除してから新しい認証サーバを追加する必要があります。

3. *保存*をクリックします。

## Active IQ Unified Manager に認証サーバーを追加する

認証サーバを追加して管理サーバでリモート認証を有効にすると、その認証サーバのリモート ユーザがUnified Managerにアクセスできるようになります。

開始する前に

- 次の情報が必要です。
  - 認証サーバのホスト名またはIPアドレス
  - 認証サーバのポート番号
- 認証サーバのリモート ユーザまたはリモート グループを管理サーバで認証できるように、リモート認証を有効にし、認証サービスを設定しておく必要があります。
- アプリケーション管理者のロールが必要です。

追加する認証サーバがハイアベイラビリティ（HA）ペアを構成している（同じデータベースを使用している）場合は、パートナーの認証サーバも追加できます。これにより、どちらかの認証サーバが到達不能になったときに、管理サーバはパートナーと通信できます。

手順

1. 左側のナビゲーションペインで、**[全般] > [リモート認証]** をクリックします。
2. 「安全な接続を使用する」オプションを有効または無効にします。

| 状況 | 操作 |
| --- | --- |
| 有効にする | a. 「安全な接続を使用する」オプションを選択してください。<br>b. 認証サーバーの領域で、*追加*をクリックします。<br>c. [認証サーバの追加]ダイアログ ボックスで、サーバの認証名またはIPアドレス（IPv4またはIPv6）を入力します。<br>d. [ホストの承認]ダイアログ ボックスで、[証明書を表示]をクリックします。<br>e. 「証明書の表示」ダイアログボックスで証明書情報を確認し、*閉じる*をクリックします。<br>f. 「ホストの承認」ダイアログボックスで、*はい*をクリックします。<br>「セキュア接続認証を使用する」オプションを有効にすると、Unified Managerは認証サーバーと通信し、証明書を表示します。Unified Managerは、セキュアな通信にはデフォルトでポート番号636を使用し、セキュアでない通信にはポート番号389を使用します。 |
| 無効にする | a. 「安全な接続を使用する」オプションのチェックを外してください。<br>b. 認証サーバーの領域で、*追加*をクリックします。<br>c. [認証サーバの追加]ダイアログ ボックスで、サーバのホスト名またはIPアドレス（IPv4またはIPv6）を指定し、ポートの詳細を指定します。<br>d. *[追加]*をクリックします。 |

追加した認証サーバが[サーバ]領域に表示されます。

3. 認証テストを実行し、追加した認証サーバのユーザを認証できることを確認します。

## Active IQ Unified Manager で認証サーバーの構成をテストする

認証サーバの設定を検証し、管理サーバと通信できるかどうかを確認することができます。具体的には、認証サーバからリモート ユーザまたはリモート グループを検索し、設定されている情報を使用して認証を実行します。

開始する前に

- リモート ユーザまたはリモート グループをUnified Managerサーバで認証できるように、リモート認証を有効にし、認証サービスを設定しておく必要があります。
- 認証サーバのリモート ユーザまたはリモート グループを管理サーバで検索して認証できるように、認証サーバを追加しておく必要があります。
- アプリケーション管理者のロールが必要です。

認証サービスがActive Directoryに設定されている場合、認証サーバのプライマリ グループに属するリモートユーザの認証の検証では、認証結果にプライマリ グループに関する情報は表示されません。

手順

1. 左側のナビゲーションペインで、**[**全般**]** > **[**リモート認証**]** をクリックします。
2. 「認証テスト」をクリックします。
3. テストユーザーダイアログボックスで、リモートユーザーのユーザー名とパスワード、またはリモートグループのユーザー名を指定し、*テスト*をクリックします。

   リモート グループを認証する場合、パスワードは入力しないでください。

## Active IQ Unified Manager でアラートを追加する

特定のイベントが生成されたときに通知するようにアラートを設定できます。アラートは、単一のリソース、リソースのグループ、または特定の重大度タイプのイベントについて設定することができます。通知を受け取る頻度を指定したり、アラートにスクリプトを関連付けたりできます。

開始する前に

- イベントが生成されたときにActive IQ Unified Managerサーバからユーザに通知を送信できるように、通知に使用するユーザのEメール アドレス、SMTPサーバ、SNMPトラップ ホストなどを設定しておく必要があります。
- アラートをトリガーするリソースとイベント、および通知するユーザのユーザ名またはEメール アドレスを確認しておく必要があります。
- イベントに基づいてスクリプトを実行する場合は、[スクリプト]ページを使用してUnified Managerにスクリプトを追加しておく必要があります。
- アプリケーション管理者またはストレージ管理者のロールが必要です。

アラートは、ここで説明する手順に従って[アラート セットアップ]ページで作成できるほか、イベントを受け取ったあとに[イベントの詳細]ページで直接作成することもできます。

手順

1. 左側のナビゲーション ペインで、ストレージ管理 > アラート設定 をクリックします。
2. アラート設定ページで、「追加」をクリックします。
3. 「アラートの追加」ダイアログボックスで、「名前」をクリックし、アラートの名前と説明を入力します。
4. *Resources*をクリックし、アラートに含めるまたはアラートから除外するリソースを選択します。

   *名前に含む*フィールドにテキスト文字列を指定してフィルタを設定すると、リソースのグループを選択

できます。指定したテキスト文字列に基づいて、使用可能なリソースのリストには、フィルタルールに一致するリソースのみが表示されます。指定するテキスト文字列では大文字と小文字が区別されます。

あるリソースが対象に含めるルールと除外するルールの両方に該当する場合は、除外するルールが優先され、除外されたリソースに関連するイベントについてはアラートが生成されません。

5. * Events *をクリックし、アラートをトリガーするイベント名またはイベント重大度タイプに基づいてイベントを選択します。

   複数のイベントを選択するには、Ctrlキーを押しながら選択します。

6. * アクション * をクリックし、通知するユーザーを選択し、通知頻度を選択し、トラップ受信者に SNMP トラップを送信するかどうかを選択し、アラートが生成されたときに実行するスクリプトを割り当てます。

   該当するユーザのEメール アドレスを変更し、その後アラートを編集するために開くと、[名前]フィールドは空欄になります。これは、Eメールが変更されたことでユーザとのマッピングが無効になったためです。また、選択したユーザのEメール アドレスを[ユーザ]ページで変更した場合、変更後のEメール アドレスは反映されません。

   SNMPトラップを使用してユーザに通知することもできます。

7. *保存*をクリックします。

アラートの追加例

ここでは、次の要件を満たすアラートを作成する例を示します。

- アラート名：HealthTest
- リソース：名前に「`abc`」を含むすべてのボリュームを含め、名前に「`xyz`」を含むすべてのボリュームを除外します。
- イベント：健全性に関するすべての重大なイベントを対象に含める
- アクション：「sample@domain.com」、「`Test`」スクリプトが含まれ、ユーザーには15分ごとに通知する必要があります

[Add Alert]ダイアログ ボックスで、次の手順を実行します。

手順

1. *名前*をクリックし、*アラート名*フィールドに*HealthTest*を入力します。
2. *Resources*をクリックし、Includeタブでドロップダウンリストから*Volumes*を選択します。
   a. *Name contains*フィールドに*abc*と入力すると、名前に「`abc`」が含まれるボリュームが表示されます。
   b. [使用可能なリソース] 領域から **<<All Volumes whose name contains 'abc'>>** を選択し、[選択したリソース] 領域に移動します。
   c. *除外*をクリックし、*名前に含まれる文字列*フィールドに*xyz*と入力してから、*追加*をクリックします。
3. *イベント*をクリックし、イベントの重大度フィールドから*重大*を選択します。

4. [一致するイベント] 領域から すべての重要なイベント を選択し、[選択したイベント] 領域に移動します。
5. *アクション*をクリックし、「これらのユーザーに通知する」フィールドに*sample@domain.com*と入力します。
6. ユーザーに 15 分ごとに通知するには、*15 分ごとに通知*を選択します。

   指定した期間、受信者に繰り返し通知を送信するようにアラートを設定できます。アラートに対してイベント通知をアクティブにする時間を決める必要があります。

7. [実行するスクリプトの選択] メニューで、**Test** スクリプトを選択します。
8. *保存*をクリックします。

# Active IQ Unified Manager でローカルユーザーのパスワードを変更する

潜在的なセキュリティ リスクを回避するために、ローカル ユーザのログイン パスワードを変更することができます。

開始する前に

ローカル ユーザとしてログインする必要があります。

これらの手順では、メンテナンスユーザーおよびリモートユーザーのパスワードを変更することはできません。リモートユーザーのパスワードを変更するには、パスワード管理者にお問い合わせください。メンテナンスユーザーのパスワードを変更するには、"メンテナンス コンソールの使用"を参照してください。

手順

1. Unified Managerにログインします。
2. 上部のメニューバーからユーザーアイコンをクリックし、次に **Change Password** をクリックします。

   リモートユーザーの場合、「パスワードの変更」オプションは表示されません。

3. [パスワードの変更]ダイアログ ボックスで、現在のパスワードと新しいパスワードを入力します。
4. *保存*をクリックします。

Unified Managerがハイアベイラビリティ構成の場合は、セットアップのもう一方のノードでパスワードを変更する必要があります。パスワードは両方のインスタンスで同じにする必要があります。

# Active IQ Unified Manager でセッションの非アクティブタイムアウトを設定する

Unified Managerの非アクティブタイムアウト値を指定することで、一定期間操作がないとセッションが自動的に終了するように設定できます。デフォルトでは、タイムアウトは4,320分（72時間）に設定されています。

開始する前に

アプリケーション管理者のロールが必要です。

この設定は、ログインしているすべてのユーザ セッションに適用されます。

> このオプションは、Security Assertion Markup Language（SAML）認証を有効にしている場合は使用できません。

手順

1. 左側のナビゲーションペインで、**General** > **Feature Settings** をクリックします。
2. *機能設定*ページで、以下のいずれかのオプションを選択して、非アクティブタイムアウトを指定します。

| 状況 | 操作 |
| --- | --- |
| タイムアウトを設定しない（セッションを自動的に閉じない） | 「非アクティブタイムアウト」パネルで、スライダーボタンを左（オフ）に移動して、「適用」をクリックします。 |
| タイムアウト値（分）を設定する | 「非アクティブタイムアウト」パネルで、スライダーボタンを右（オン）に移動し、非アクティブタイムアウト値を分単位で指定して、「適用」をクリックします。 |

# Active IQ Unified Manager でCLIを使用してセッションタイムアウトを設定する

CLIを使用してUnified Managerのセッションタイムアウトの最大値を設定することで、一定時間経過後にセッションを自動的に終了させることができます。デフォルトでは、セッションタイムアウトは最大値である4,320分（72時間）に設定されています。これは、ログインしてUnified Managerをアクティブに使用している場合でも、72時間後にセッションが自動的に終了することを意味します。

タスク概要

アプリケーション管理者のロールが必要です。

セッションタイムアウト設定は、ログインしているすべてのユーザーセッションに影響します。

手順

1. Unified Manager CLIにログインするには、 `um cli login` コマンドを入力します。認証には有効なユーザ名とパスワードを使用してください。
2. セッションタイムアウト値を変更するには、 `um option set max.session.timeout.value=<in mins>` コマンドを入力します。

# Unified Managerのホスト名の変更

## Active IQ Unified Manager 仮想アプライアンスのホスト名を変更する

ネットワーク ホストの名前は、Unified Manager仮想アプライアンスの導入時に割り当てられます。このホスト名は導入後に変更することができます。ホスト名を変更する場合

は、HTTPS証明書も再生成する必要があります。

開始する前に

このタスクを実行するには、Unified Managerにメンテナンス ユーザとしてログインするか、アプリケーション管理者ロールが割り当てられている必要があります。

Unified Manager Web UIには、ホスト名（またはホストのIPアドレス）を使用してアクセスできます。導入時に静的IPアドレスを使用してネットワークを設定した場合は、指定したネットワーク ホストの名前を使用します。DHCPを使用してネットワークを設定した場合は、DNSからホスト名を取得します。DHCP または DNS が正しく設定されていない場合、ホスト名「`Unified Manager`」が自動的に割り当てられ、セキュリティ証明書に関連付けられます。

ホスト名を変更した場合、Unified Manager Web UIへのアクセスに新しいホスト名を使用するには、ホスト名の元の割り当て方法に関係なく、必ず新しいセキュリティ証明書を生成する必要があります。

ホスト名ではなくサーバのIPアドレスを使用してWeb UIにアクセスする場合は、ホスト名の変更時に新しい証明書を生成する必要はありません。ただし、証明書のホスト名が実際のホスト名と同じになるように証明書を更新することを推奨します。

Unified Managerでホスト名を変更したら、OnCommand Workflow Automation（WFA）で手動でホスト名を更新する必要があります。ホスト名はWFAでは自動的に更新されません。

新しい証明書は、Unified Manager仮想マシンを再起動するまで有効になりません。

手順

1. HTTPSセキュリティ証明書を生成する

   新しいホスト名を使用してUnified Manager Web UIにアクセスする場合は、HTTPS証明書を再生成して新しいホスト名に関連付ける必要があります。

2. Unified Manager仮想マシンを再起動する

   HTTPS証明書を再生成したら、Unified Manager仮想マシンを再起動する必要があります。

## Active IQ Unified Manager でHTTPSセキュリティ証明書を生成する

Active IQ Unified Managerを初めてインストールすると、デフォルトのHTTPS証明書がインストールされます。新しいHTTPSセキュリティ証明書を生成して、既存の証明書を置き換えることができます。

開始する前に

アプリケーション管理者のロールが必要です。

証明書を再生成する理由はいくつもあります。たとえば、識別名（DN）をより適切な値に変更する場合、キーのサイズを大きくする場合、有効期限を延長する場合、現在の証明書の有効期限が切れた場合などです。

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。証明書を再生成する際に、鍵のサイズと鍵の有効期間を指定できます。メンテナンス コンソールの `Reset Server Certificate`オプションを使用すると、397日間有効な新しいHTTPS証明書が作成されます。この証明書には、2048ビットのRSA鍵が含まれます。

手順

1. 左側のナビゲーションペインで、**General** > **HTTPS Certificate** をクリックします。
2. *HTTPS証明書を再生成*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、次のいずれかを実行します。

| 状況 | 操作 |
| --- | --- |
| 現在の値で証明書を再生成する | 「現在の証明書属性を使用して再生成」オプションをクリックします。 |
| 別の値で証明書を生成する | *現在の証明書の属性を更新する*オプションをクリックします。<br><br>「共通名」と「代替名」のフィールドに新しい値を入力しない場合、既存の証明書の値が使用されます。「`Common Name`」には、ホストのFQDNを設定する必要があります。その他のフィールドには値を入力する必要はありませんが、証明書に値を反映させたい場合は、たとえばEMAIL、COMPANY、DEPARTMENT、City、State、Countryなどのフィールドに値を入力できます。利用可能な鍵サイズ（鍵アルゴリズムは「`RSA`」です）と有効期間を選択することもできます。<br><br>• キーサイズの許容値は `2048`、`3072`、および `4096`です。<br>• 有効期間は1日～36500日です。<br><br>ただし、推奨される有効期間は397日（13カ月）以内です。397日を超える有効期間を選択しても、CSRをエクスポートして既知のCAから署名を受ける場合にCAからは有効期間が397日に削減され署名済み証明書が返されます。<br><br>• 証明書の[別名]フィールドにローカルの識別情報を含めない場合は、[ローカルの識別情報を除外する（ローカルホストなど）]チェックボックスを選択します。このチェックボックスを選択すると、このフィールドで入力した情報だけが[別名]フィールドで使用されます。このフィールドを空白にした場合は、[別名]フィールドのない証明書が生成されます。 |

4. 証明書を再生成するには、「はい」をクリックします。
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。
6. HTTPS証明書を表示して新しい証明書の情報を確認します。

## Active IQ Unified Manager 仮想マシンを再起動する

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。

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。

*Restart Guest*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. **System Configuration** > **Reboot Virtual Machine** を選択します。

## Linux システム上の Active IQ Unified Manager ホスト名の変更

必要に応じて、Unified ManagerをインストールしたRed Hat Enterprise Linuxマシンのホスト名をあとから変更することができます。たとえば、タイプ、ワークグループ、監視対象のクラスタ グループなどがわかるような名前に変更すると、Linuxマシンのリストでの Unified Managerサーバを識別しやすくなります。

開始する前に

Unified ManagerがインストールされているLinuxシステムへのrootユーザ アクセスが必要です。

Unified Manager Web UIには、ホスト名（またはホストのIPアドレス）を使用してアクセスできます。導入時に静的IPアドレスを使用してネットワークを設定した場合は、指定したネットワーク ホストの名前を使用します。DHCPを使用してネットワークを設定した場合は、DNSサーバからホスト名を取得します。

ホスト名を変更した場合、Unified Manager Web UIへのアクセスに新しいホスト名を使用するには、ホスト名の元の割り当て方法に関係なく、必ず新しいセキュリティ証明書を生成する必要があります。

ホスト名ではなくサーバのIPアドレスを使用してWeb UIにアクセスする場合は、ホスト名の変更時に新しい証明書を生成する必要はありません。ただし、証明書のホスト名が実際のホスト名と同じになるように証明書を更新することを推奨します。新しい証明書は、Linuxマシンを再起動するまで有効になりません。

Unified Managerでホスト名を変更したら、OnCommand Workflow Automation（WFA）で手動でホスト名を更新する必要があります。ホスト名はWFAでは自動的に更新されません。

手順

1. 変更するUnified Managerシステムにrootユーザとしてログインします。

2. 次のコマンドを入力して、Unified Managerソフトウェアと関連するMySQLソフトウェアを停止します。

   ```
   systemctl stop ocieau ocie mysqld
   ```

3. Linux `hostnamectl`コマンドを使用してホスト名を変更します：

   ```
   hostnamectl set-hostname new_FQDN
   ```

   ```
   hostnamectl set-hostname nuhost.corp.widget.com
   ```

4. サーバのHTTPS証明書を再生成します。

   ```
   /opt/netapp/essentials/bin/cert.sh create
   ```

5. ネットワーク サービスを再起動します。

   ```
   systemctl restart NetworkManager.service
   ```

6. サービスが再起動されたら、新しいホスト名でpingを実行できるかどうかを確認します。

   ```
   ping new_hostname
   ```

   ```
   ping nuhost
   ```

   元のホスト名に対して設定していた同じIPアドレスが返されることを確認します。

7. ホスト名を変更して確認したら、次のコマンドを入力してUnified Managerを再起動します。

   ```
   systemctl start mysqld ocie ocieau
   ```

# Active IQ Unified Manager でのポリシーベースのストレージ管理の有効化と無効化

Unified Manager 9.7以降では、ONTAPクラスター上のストレージワークロード（ボリュームとLUN）をプロビジョニングし、割り当てられたパフォーマンスサービスレベルに基づいてそれらのワークロードを管理できます。この機能は、ONTAP System Managerでワークロードを作成してQoSポリシーを適用する操作に似ていますが、Unified Managerを使用して適用すると、Unified Managerインスタンスが監視しているすべてのクラスターにわたってワークロードをプロビジョニングおよび管理できます。

アプリケーション管理者のロールが必要です。

このオプションはデフォルトで有効になっていますが、Unified Manager を使用してワークロードをプロビジョニングおよび管理しない場合は、無効にすることができます。

このオプションを有効にすると、ユーザ インターフェイスに新しい項目がいくつか追加されます。

| 新コンテンツ | **Location** |
| --- | --- |
| 新しいワークロードのプロビジョニング ページ | 「共通タスク」＞「プロビジョニング」から利用可能です |
| パフォーマンス サービス レベル ポリシーの作成ページ | 「設定」＞「ポリシー」＞「パフォーマンスサービスレベル」から利用できます。 |
| パフォーマンス ストレージ効率ポリシーの作成ページ | 「設定」＞「ポリシー」＞「ストレージ効率」から使用できます。 |
| 現在のワークロードパフォーマンスとワークロードIOPSを説明するパネル | ダッシュボード |

これらのページおよびこの機能の詳細については、製品のオンライン ヘルプを参照してください。

手順

1. 左側のナビゲーションペインで、**General** > **Feature Settings** をクリックします。
2. 「機能設定」ページで、以下のいずれかのオプションを選択して、ポリシーベースのストレージ管理を無効または有効にします。

| 状況 | 操作 |
| --- | --- |
| ポリシーベースのストレージ管理を無効にする | 『ポリシーベースのストレージ管理』パネルで、スライダーボタンを左に移動します。 |
| ポリシー ベースのストレージ管理を有効にする | 「ポリシーベースのストレージ管理」パネルで、スライダーボタンを右に移動します。 |

## 著作権に関する情報

Copyright © 2026 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。