設定タスクと管理タスクの実行

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

設定タスクと管理タスクの実行 1
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 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 バックアップの設定 21
機能設定を管理します 21
Active IQ Unified Manager の機能設定について 21
Active IQ Unified Manager でポリシーベースのストレージ管理を有効にする 21
Active IQ Unified Manager の API Gateway 機能について 22
Active IQ Unified Manager で非アクティブタイムアウトを指定する 23
Active IQ Unified Manager で Active IQ ポータルイベントを有効にする 23
Active IQ Unified Manager でコンプライアンスのためのセキュリティ設定を有効化および無効化する 23
Active IQ Unified Manager でのスクリプトのアップロードの有効化および無効化 24
Active IQ Unified Manager にログインバナーを追加する 25
メンテナンスコンソールを使用する 25
Active IQ Unified Manager のメンテナンスコンソールについて 25
Active IQ Unified Manager のメンテナンスユーザーについて 25
Active IQ Unified Manager における診断ユーザー機能 26
Active IQ Unified Manager のメンテナンスコンソールにアクセスする 26
Active IQ Unified Manager の vSphere VM
コンソールを使用してメンテナンスコンソールにアクセスする 27
メンテナンス コンソールのメニュー 27
Active IQ Unified Manager で Windows のメンテナンスユーザーのパスワードを変更する 33
Linux システムでの Active IQ Unified Manager の umadmin パスワードの変更 33
Active IQ Unified Manager がHTTPおよびHTTPSプロトコルに使用するポートを変更する 34
Active IQ Unified Manager へのネットワークインターフェイスの追加 35
Active IQ Unified Manager でクライアント証明書を再生成する 35
ディスク容量を追加する 36
ユーザ アクセスの管理 39
ユーザの追加 39

Active IQ Unified Manager でユーザー設定を編集する 41
Active IQ Unified Manager でユーザーを表示する 41
Active IQ Unified Manager でユーザーまたはグループを削除する 41
Active IQ Unified Manager のロールベースアクセス制御について 42
Active IQ Unified Manager のユーザータイプについて 42
Active IQ Unified Manager のユーザーロールについて 43
Active IQ Unified Manager におけるユーザーロールと機能について 44
SAML認証設定の管理 45
Active IQ Unified Manager で SAML 認証を有効にする 45
Active IQ Unified Manager でIDプロバイダーを使用する 46
Active IQ Unified Manager で SAML 認証を有効にする 47
Active IQ Unified Manager でSAML認証IDプロバイダーを変更する 48
Active IQ Unified Manager のセキュリティ証明書変更後に SAML 認証設定を更新する 49
Active IQ Unified Manager で SAML 認証を無効にする 50
Active IQ Unified Manager メンテナンスコンソールから SAML 認証を無効にする 51
Active IQ Unified Manager の SAML 認証ページを使用する 51
認証を管理する 52
Active IQ Unified Manager で認証サーバーを編集する 52
Active IQ Unified Manager で認証サーバーを削除する 53
Active IQ Unified Manager で Active Directory または OpenLDAP を使用して認証する 53
監査ログ 53
Active IQ Unified Manager のリモート認証ページを使用する 56
セキュリティ証明書を管理する 59
Active IQ Unified Manager でHTTPSセキュリティ証明書を表示する 59
Active IQ Unified Manager で HTTPS 証明書署名要求をダウンロードする 60
CA署名付きHTTPS証明書をActive IQ Unified Managerにインストールする 60
Active IQ Unified Manager で外部ツールを使用して生成された HTTPS 証明書について 61
証明書管理のページの説明 63

設定タスクと管理タスクの実行

Active IQ Unified Managerの設定

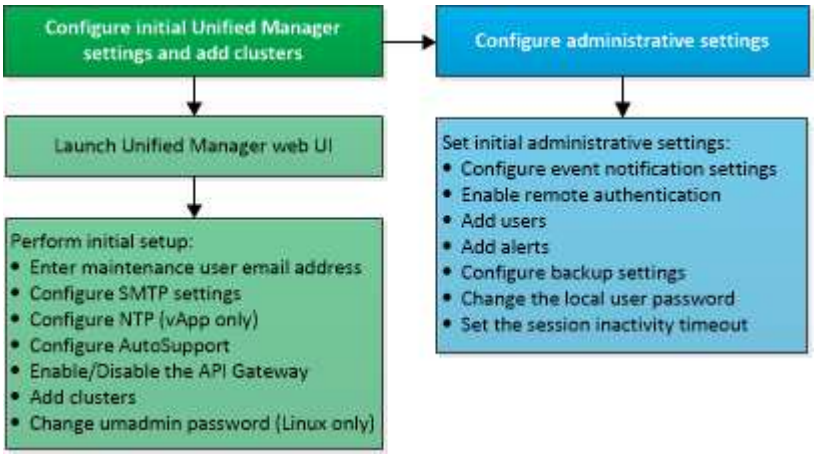
Active IQ Unified Manager の設定について

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

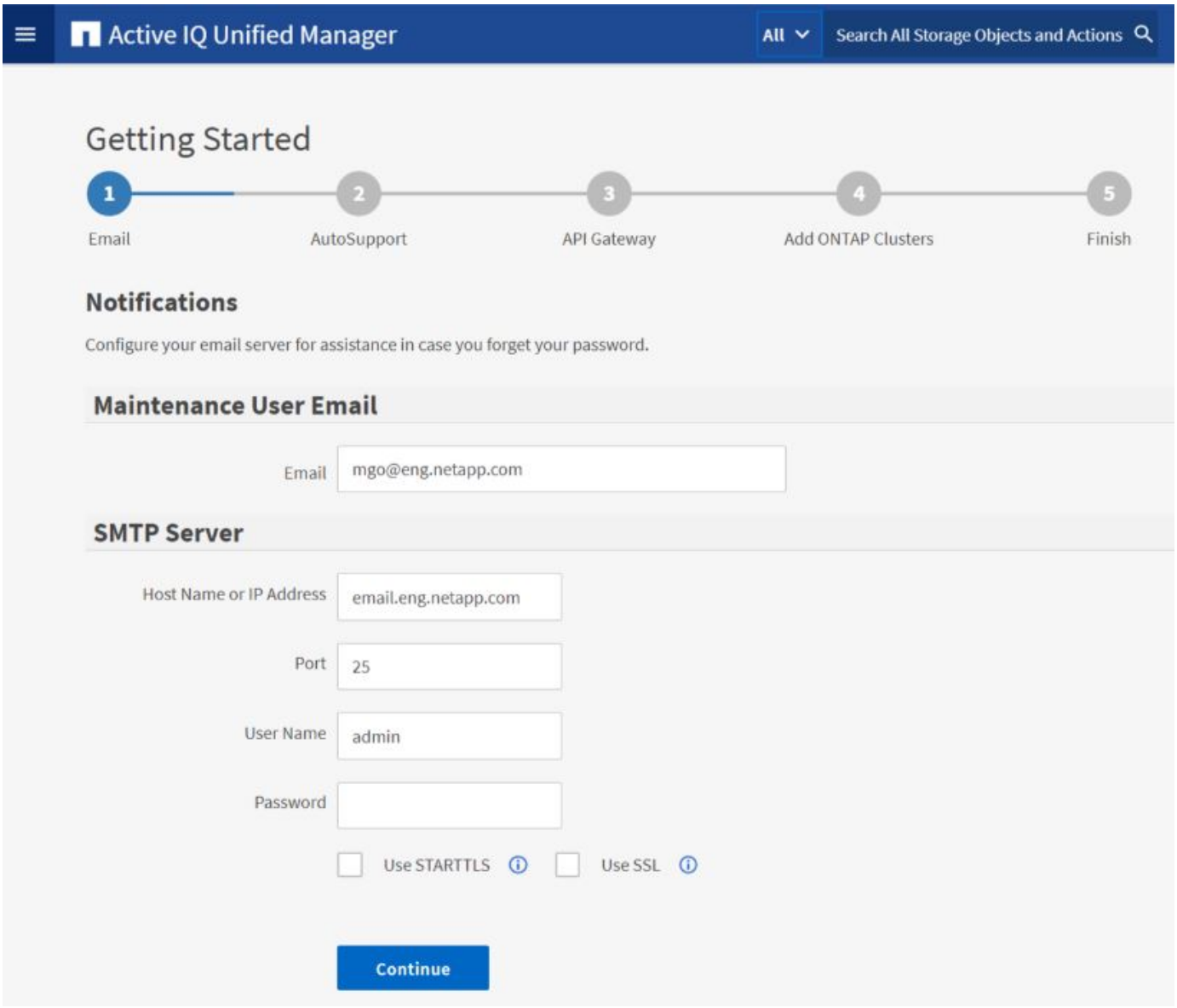
Unified Managerを使用するには、NTPサーバ、メンテナンス ユーザのEメール アドレス、SMTPサーバのホストなどを最初に設定し、ONTAPクラスタを追加する必要があります。

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） ◦ `domainname\username` ◦ `username@domainname` ◦ `Bind Distinguished Name`（適切なLDAP表記法を使用） • 管理者のパスワード • 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） • バインドパスワード • 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。 b. 認証サーバのベース識別名を指定します。 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。 b. 認証サーバのベース識別名を指定します。 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。 b. 認証サーバのベース識別名を指定します。 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。 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。 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。 b. 認証サーバーの領域で、*追加*をクリックします。 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。 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。 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。 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。 「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。 b. 認証サーバーの領域で、*追加*をクリックします。 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。 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。 「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。 • キーサイズの許容値は `2048`、`3072`、および `4096`です。 • 有効期間は1日～36500日です。 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。 • 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。

新コンテンツ	Location
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。

Active IQ Unified Manager バックアップの設定

Unified Managerのバックアップ機能は、ホストシステムで実行する一連の設定手順と、メンテナンスコンソールを通じて設定できます。

設定手順の詳細については、"バックアップとリストア処理の管理"を参照してください。

機能設定を管理します

Active IQ Unified Manager の機能設定について

[機能設定]ページで、Active IQ Unified Managerの特定の機能を有効または無効にできます。ポリシーに基づいたストレージ オブジェクトの作成と管理、APIゲートウェイとログイン バナーの有効化、アラート管理用スクリプトのアップロード、非アクティブ時間に基づくWeb UIセッションのタイムアウト、Active IQプラットフォーム イベントの受信停止などが含まれます。

[機能設定]ページは、アプリケーション管理者ロールが割り当てられたユーザだけが使用できます。

スクリプトのアップロードに関する情報については、"スクリプト アップロードの有効化と無効化"を参照してください。

Active IQ Unified Manager で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」オプションを使用すると、サービスレベル目標（SLO）に基づいてストレージを管理できます。このオプションはデフォルトで有効に

なっています。

この機能をアクティブ化すると、Active IQ Unified Managerインスタンスに追加されるONTAPクラスタのストレージ ワークロード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 レベルとストレージ効率化ポリシーに基づいてワークロードを管理できます。

この機能は、「一般」>「機能設定」>「ポリシーベースのストレージ管理」から有効または無効にすることができます。この機能を有効にすると、以下のページが操作および監視に利用可能になります。

- [プロビジョニング]ページ（ストレージ ワークロードのプロビジョニング）
- ポリシー > パフォーマンスサービスレベル
- ポリシー > ストレージ効率
- クラスター設定ページの「パフォーマンスサービスレベル別に管理されるワークロード」列
- ダッシュボードのワークロードパフォーマンスパネル

これらの画面を使用して、パフォーマンスサービスレベルとストレージ効率ポリシーを作成したり、ストレージワークロードをプロビジョニングしたりできます。割り当てられたパフォーマンスサービスレベルに準拠しているストレージワークロードだけでなく、準拠していないワークロードも監視できます。ワークロードパフォーマンスおよびワークロード IOPS パネルを使用すると、データセンター全体のクラスタにプロビジョニングされたストレージワークロードに基づいて、クラスタの総容量、利用可能容量、使用容量、およびパフォーマンス（IOPS）を評価できます。

この機能を有効化すると、メニューバー > ヘルプボタン > **API**ドキュメント > *ストレージプロバイダー*カテゴリからUnified Manager REST APIを実行して、これらの機能の一部を実行できます。または、ホスト名またはIPアドレスを入力し、https://<hostname>/docs/api/ という形式のURLでREST APIページにアクセスすることもできます。

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。

Active IQ Unified Manager の API Gateway 機能について

API Gateway機能を使用すると、Active IQ Unified Manager は単一のコントロールプレーンとして機能し、複数の ONTAP クラスタに個別にログインすることなく管理できます。

この機能は、Unified Manager に初めてログインした際に表示される設定ページから有効にできます。または、**General** > **Feature Settings** > **API Gateway** からこの機能を有効または無効にすることもできます。

Unified Manager REST API は ONTAP REST API とは異なり、ONTAP REST API のすべての機能が Unified Manager REST API を使用して利用できるわけではありません。ただし、Unified Manager に公開されていない特定の機能を管理するために ONTAP API にアクセスする特定のビジネス要件がある場合は、API Gateway 機能を有効にして ONTAP API を実行できます。ゲートウェイはプロキシとして機能し、ONTAP API と同じ形式でヘッダーおよびボディのリクエストを維持しながら API リクエストをトンネリングします。Unified Manager の認証情報を使用して特定の API を実行し、個々のクラスタ認証情報を渡すことなく ONTAP クラスタにアクセスして管理できます。Unified Manager は、お客様の Unified Manager インスタンスで管理されている ONTAP クラスタ全体で API を実行するための単一の管理ポイントとして機能します。API から返されるレスポンスは、ONTAP から直接実行されたそれぞれの ONTAP REST API から返されるレスポンスと同じです。

この機能を有効にすると、メニューバー > ヘルプボタン > **API**ドキュメント > *ゲートウェイ*カテゴリか

らUnified Manager REST APIを実行できるようになります。または、ホスト名または IP アドレスと URL を入力して、次の形式で REST API ページにアクセスすることもできます `https://<hostname>/docs/api/`

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。

Active IQ Unified Manager で非アクティブタイムアウトを指定する

Active IQ Unified Manager の非アクティブタイムアウト値を指定できます。指定された時間操作がないと、アプリケーションは自動的にログアウトされます。このオプションはデフォルトで有効になっています。

この機能は、「一般」＞「機能設定」＞「非アクティブタイムアウト」から無効化したり、時間を変更したりできます。この機能を有効にしたら、「ログアウトまでの時間（分）」フィールドに、操作がない状態が続くとシステムが自動的にログアウトする時間制限を指定してください。デフォルト値は4320分（72時間）です。

> 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。

Active IQ Unified Manager で Active IQ ポータルイベントを有効にする

Active IQ ポータルイベントを有効にするか無効にするかを指定できます。この設定により、Active IQ ポータルがシステム構成、ケーブル配線などに関する追加イベントを検出して表示できるようになります。このオプションはデフォルトで有効になっています。

この機能を有効にすると、Active IQ Unified Manager は Active IQ ポータルで検出されたイベントを表示します。これらのイベントは、監視対象のすべてのストレージシステムから生成された AutoSupport メッセージに対して一連のルールを実行することによって作成されます。これらのイベントは、他の Unified Manager イベントとは異なり、システム構成、ケーブル配線、ベストプラクティス、および可用性の問題に関連するインシデントやリスクを特定します。

この機能は、**General** > **Feature Settings** > **Active IQ Portal Events** から有効化または無効化できます。外部のネットワーク アクセスがないサイトでは、**Storage Management** > **Event Setup** > **Upload Rules** からルールを手動でアップロードする必要があります。

この機能はデフォルトで有効になっています。この機能を無効にすると、Active IQ のイベントが Unified Manager 上で検出または表示されなくなります。無効になっている場合にこの機能を有効にすると、Unified Manager は、そのクラスターのタイムゾーンにおける事前定義された時刻（00:15）に、クラスター上の Active IQ イベントを受信できるようになります。

Active IQ Unified Manager でコンプライアンスのためのセキュリティ設定を有効化および無効化する

機能設定ページの*セキュリティダッシュボード*パネルにある*カスタマイズ*ボタンを使用すると、Unified Managerのコンプライアンス監視に関するセキュリティパラメータを有効または無効にすることができます。

このページから有効または無効にする設定は、Unified Manager上のクラスターおよびストレージVMの全体的

なコンプライアンス状態を制御します。選択内容に基づいて、対応する列がクラスターインベントリページの*セキュリティ：すべてのクラスター*ビューと、ストレージVMインベントリページの*セキュリティ：すべてのストレージVM*ビューに表示されます。

これらの設定を編集できるのは、管理者ロールのユーザだけです。

お客様のONTAPクラスター、ストレージVM、ボリュームのセキュリティ基準は、"NetApp ONTAP 9セキュリティ設定ガイド"で定義されている推奨事項に照らして評価されます。ダッシュボードのセキュリティパネルとセキュリティページには、クラスター、ストレージVM、およびボリュームのデフォルトのセキュリティ準拠ステータスが表示されます。セキュリティ違反が発生したクラスターおよびストレージVMに対しては、セキュリティイベントが生成され、管理アクションが有効になります。

セキュリティ設定のカスタマイズ

ONTAP環境に応じてコンプライアンス監視の設定をカスタマイズするには、次の手順を実行します。

手順

1. *一般 > 機能設定 > セキュリティダッシュボード > カスタマイズ*をクリックします。*セキュリティダッシュボード設定のカスタマイズ*ポップアップが表示されます。

   有効または無効にしたセキュリティ コンプライアンス パラメータは、[クラスタ]ページと[Storage VM]ページのデフォルトのセキュリティ ビュー、レポート、およびスケジュール済みレポートに直接影響します。これらのページからExcelレポートをアップロードしたあとにセキュリティ パラメータを変更した場合、ダウンロードしたExcelレポートに誤った情報が含まれることがあります。

2. ONTAPクラスタのカスタム設定を有効または無効にするには、*Cluster*の下にある必要な一般設定を選択します。クラスタコンプライアンスをカスタマイズするオプションの詳細については、"クラスタ コンプライアンスのカテゴリ"を参照してください。
3. ストレージVMのカスタム設定を有効または無効にするには、*ストレージVM*の下にある必要な一般設定を選択してください。ストレージVMのコンプライアンスをカスタマイズするためのオプションについては、"Storage VMのコンプライアンス カテゴリ"を参照してください。

AutoSupportと認証設定のカスタマイズ

*AutoSupport設定*セクションでは、ONTAPからAutoSupportメッセージを送信するためにHTTPSトランスポートを使用するかどうかを指定できます。

*認証設定*セクションから、デフォルトのONTAP管理者ユーザーに対してUnified Managerアラートが生成されるように有効にできます。

Active IQ Unified Manager でのスクリプトのアップロードの有効化および無効化

スクリプトをUnified Managerにアップロードして実行する機能は、デフォルトで有効になっています。セキュリティ上の理由からこの操作を禁止したい場合は、この機能を無効にすることができます。

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。

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、スクリプト機能を無効または有効にします。

状況	操作
スクリプトを無効にする	「スクリプトアップロード」パネルで、スライダーボタンを左に移動します。
スクリプトを有効にする	「スクリプトアップロード」パネルで、スライダーボタンを右に移動します。

Active IQ Unified Manager にログインバナーを追加する

ログイン バナーを追加して、システムへのアクセスを許可されているユーザや利用条件などの情報をログインとログアウトの際に表示することができます。

このログイン バナーのポップアップは、ストレージのオペレータや管理者などのすべてのユーザに対して、ログイン、ログアウト、セッション タイムアウトの際に表示されます。

メンテナンスコンソールを使用する

Active IQ Unified Manager のメンテナンスコンソールについて

Unified Managerメンテナンスコンソールを使用すると、Unified Managerシステムの設定を管理し、問題の発生を防ぐために必要な変更を行うことができます。

Unified Managerをインストールしたオペレーティングシステムに応じて、メンテナンスコンソールには次の機能があります。

- 仮想アプライアンスに関する問題、特にUnified Manager Webインターフェイスにアクセスできないときのトラブルシューティングを行います。
- Unified Managerの新しいバージョンへのアップグレード
- テクニカル サポートに送信するサポート バンドルの生成
- ネットワークの設定
- メンテナンス ユーザのパスワードの変更
- パフォーマンス統計の送信を目的とした外部データ プロバイダへの接続
- パフォーマンス データ収集の内部変更
- 以前にバックアップしたバージョンから、Unified Managerのデータベースと構成設定を復元します。

Active IQ Unified Manager のメンテナンスユーザーについて

Unified ManagerをRed Hat Enterprise Linuxシステムにインストールする場合、インスト

ール時にメンテナンス ユーザが作成されます。メンテナンス用ユーザー名は「umadmin」ユーザーです。メンテナンスユーザーはWeb UIでアプリケーション管理者ロールを持ち、そのユーザーは後続のユーザーを作成してロールを割り当てることができます。

メンテナンス ユーザまたはumadminユーザは、Unified Managerのメンテナンス コンソールにもアクセスできます。

Active IQ Unified Manager における診断ユーザー機能

診断アクセスの目的は、テクニカル サポートからトラブルシューティングのサポートを受けられるようにすることです。このため、テクニカル サポートから指示された場合にのみ診断アクセスを使用する必要があります。

診断ユーザは、テクニカル サポートからの指示を受けて、トラブルシューティングの目的でOSレベルのコマンドを実行できます。

Active IQ Unified Manager のメンテナンスコンソールにアクセスする

Unified Managerユーザ インターフェイスが動作状態でない場合、またはこのユーザ インターフェイスにない機能を実行する必要がある場合は、メンテナンス コンソールにアクセスしてUnified Managerシステムを管理できます。

開始する前に

Unified Managerをインストールして設定しておく必要があります。

15分間操作しないと、メンテナンス コンソールからログアウトされます。

VMwareにインストールした場合、VMwareコンソールからメンテナンス ユーザとしてすでにログインしているときは、Secure Shellを使用して同時にログインできません。

手順

1. 次の手順に従ってメンテナンス コンソールにアクセスします。

このオペレーティングシステムでは...	次の手順に従ってください。
VMware	a. Secure Shellを使用して、Unified Manager仮想アプライアンスのIPアドレスまたは完全修飾ドメイン名に接続します。 b. メンテナンス ユーザ名とパスワードを使用してメンテナンス コンソールにログインします。

このオペレーティングシステムでは...	次の手順に従ってください。
Linux	a. Secure Shellを使用して、Unified Managerシステムの IPアドレスまたは完全修飾ドメイン名に接続します。 b. メンテナンス ユーザ（umadmin）の名前とパスワードでシステムにログインします。 c. コマンド `maintenance_console`を入力し、Enterキーを押します。
Windows	a. 管理者のクレデンシャルでUnified Managerシステムにログインします。 b. Windows管理者としてPowerShellを起動します。 c. コマンド `maintenance_console`を入力し、Enterキーを押します。

Unified Managerメンテナンス コンソール メニューが表示されます。

Active IQ Unified Manager の vSphere VM コンソールを使用してメンテナンスコンソールにアクセスする

Unified Managerユーザ インターフェイスが動作状態でない場合、またはこのユーザ インターフェイスにない機能を実行する必要がある場合は、メンテナンス コンソールにアクセスして仮想アプライアンスを再設定できます。

開始する前に

- メンテナンス ユーザである必要があります。
- メンテナンス コンソールにアクセスするには、仮想アプライアンスの電源をオンにする必要があります。

手順

1. vSphere Clientで、Unified Manager仮想アプライアンスを見つけます。
2. 「コンソール」タブをクリックします。
3. コンソール ウィンドウ内をクリックしてログインします。
4. ユーザ名とパスワードを使用してメンテナンス コンソールにログインします。

   15分間操作しないと、メンテナンス コンソールからログアウトされます。

メンテナンス コンソールのメニュー

Active IQ Unified Manager のメンテナンスコンソールメニューについて

メンテナンスコンソールは、Unified Manager サーバーの特殊機能や構成設定を維持・管理するための様々なメニューで構成されています。

Unified Managerをインストールしたオペレーティングシステムによって、メンテナンスコンソールは以下の

メニューで構成されます：

- Upgrade Unified Manager（VMwareのみ）
- Network Configuration（VMwareのみ）
- System Configuration（VMwareのみ）
  a. Support/Diagnostics
  b. Reset Server Certificate
  c. クライアント証明書を再生成する
  d. Backup Restore
  e. External Data Provider
  f. Performance Polling Interval Configuration
  g. SAML認証の無効化
  h. View/Change Application Ports
  i. Debug Log Configuration
  j. Control access to MySQL port 3306
  k. 終了

特定のメニューオプションにアクセスするには、リストから番号を選択します。たとえば、バックアップとリストアの場合は、_4_を選択します。

Active IQ Unified Manager のネットワーク設定メニュー

[Network Configuration]メニューでは、ネットワーク設定を管理することができます。このメニューは、Unified Managerユーザ インターフェイスを使用できない場合に使用してください。

Unified ManagerがRed Hat Enterprise LinuxまたはMicrosoft Windowsにインストールされている場合は、このメニューを使用できません。

表示されるメニュー項目は次のとおりです。

- **IP**アドレス設定の表示

  仮想アプライアンスの現在のネットワーク設定が表示されます（IPアドレス、ネットワーク、ブロードキャスト アドレス、ネットマスク、ゲートウェイ、DNSサーバなど）。

- **IP**アドレス設定の変更

  仮想アプライアンスのネットワーク設定（IPアドレス、ネットマスク、ゲートウェイ、DNSサーバーなど）を変更できます。メンテナンスコンソールを使用してネットワーク設定をDHCPから静的ネットワークに変更した場合、ホスト名を編集することはできません。変更を反映させるには、*変更を確定する*を選択する必要があります。

- ドメイン名検索設定を表示する

ホスト名の解決に使用されるドメイン名検索リストが表示されます。

- ドメイン名検索設定を変更する

  ホスト名の解決時に検索対象とするドメイン名を変更できます。変更を反映させるには、*変更を確定する*を選択する必要があります。

- 静的ルートの表示

  現在の静的ネットワーク ルートが表示されます。

- 静的ルートの変更

  静的ネットワークルートの追加または削除を可能にします。変更を反映させるには、*変更を確定する*を選択する必要があります。

  - ルートを追加

    静的ルートを追加することができます。

  - ルートを削除

    静的ルートを削除することができます。

  - 戻る

    メインメニューに戻ります。

  - 終了

    メンテナンス コンソールを終了します。

- ネットワークインターフェースを無効にする

  利用可能なネットワークインターフェースをすべて無効にします。利用可能なネットワークインターフェースが1つしかない場合、それを無効にすることはできません。変更を反映させるには、*変更を確定する*を選択する必要があります。

- ネットワークインターフェースを有効にする

  利用可能なネットワークインターフェースを有効にします。変更を反映させるには、*変更を確定する*を選択する必要があります。

- 変更をコミットする

  仮想アプライアンスのネットワーク設定に加えた変更を適用します。変更を有効にするには、必ずこのオプションを選択します。そうしないと、変更は適用されません。

- ホストにpingを送信

  IPアドレスの変更やDNS設定を確認するために、ターゲット ホストにpingを実行します。

- 初期設定に戻す

すべての設定を工場出荷時のデフォルト設定にリセットします。変更を反映させるには、*変更を確定する*を選択する必要があります。

- 戻る

  メインメニューに戻ります。

- 終了

  メンテナンス コンソールを終了します。

Active IQ Unified Manager のシステム構成メニューを使用する

[System Configuration]メニューには、仮想アプライアンスを管理するためのさまざまなオプションが用意されています（サーバ ステータスの表示、仮想マシンのリブートとシャットダウンなど）。

> Unified ManagerがLinuxまたはMicrosoft Windowsシステムにインストールされている場合、このメニューからは「`Restore from a Unified Manager Backup`」オプションのみが利用可能です。

表示されるメニュー項目は次のとおりです。

- サーバーの状態を表示する

  現在のサーバ ステータスを表示します。ステータスには「Running」と「Not Running」があります。

  サーバが実行されていない場合は、テクニカル サポートに連絡することを推奨します。

- 仮想マシンの再起動

  すべてのサービスを停止して仮想マシンをリブートします。リブート後、仮想マシンとサービスが再起動します。

- 仮想マシンのシャットダウン

  すべてのサービスを停止して仮想マシンをシャットダウンします。

  このオプションは、仮想マシン コンソールからのみ選択できます。

- **<logged in user>** ユーザーパスワードの変更

  現在ログインしているユーザ（メンテナンス ユーザ）のパスワードを変更します。

- データディスクサイズを増やす

  仮想マシンのデータ ディスク（ディスク3）のサイズを拡張します。

- スワップディスクサイズを増やす

  仮想マシンのスワップ ディスク（ディスク2）のサイズを拡張します。

- タイムゾーンを変更する

  タイムゾーンを現在の場所に変更します。

- **NTP**サーバーを変更する

  NTPサーバの設定を変更します（IPアドレスや完全修飾ドメイン名（FQDN）など）。

- **NTP**サービスの変更

  `ntp`と `systemd-timesyncd`のサービスを切り替えます。

- **Unified Manager**バックアップからの復元

  以前にバックアップしたバージョンから、Unified Managerのデータベースと構成設定を復元します。

- サーバー証明書のリセット

  サーバ セキュリティ証明書をリセットします。

- ホスト名の変更

  仮想アプライアンスがインストールされているホストの名前を変更します。

- 戻る

  [System Configuration]メニューを終了して[Main Menu]に戻ります。

- 終了

  メンテナンス コンソール メニューを終了します。

Active IQ Unified Manager のサポートと診断メニューを使用する

「サポートと診断」メニューを使用すると、トラブルシューティングの支援を受けるためにテクニカルサポートに送信できるサポートバンドルを作成できます。

表示されるメニュー オプションは次のとおりです。

- ライトサポートバンドルを生成

  30日分のログと構成データベース レコードのみを含む軽量なサポート バンドル（パフォーマンス データ、取得記録ファイル、サーバ ヒープ ダンプは含まれません）を作成できます。

- サポートバンドルを生成する

  診断ユーザーのホームディレクトリに、診断情報を含む完全なサポートバンドル（7-Zipファイル）を作成できます。システムがインターネットに接続されている場合は、サポートバンドルをNetAppにアップロードすることもできます。

  ファイルには、AutoSupportメッセージによって生成された情報、Unified Managerデータベースの内

容、Unified Managerサーバーの内部に関する詳細データ、および通常はAutoSupportメッセージや軽量サポートバンドルに含まれない詳細レベルのログが含まれています。

Active IQ Unified Manager のメンテナンスコンソールの追加メニューオプションについて

以下のメニューオプションを使用すると、Unified Managerサーバー上でさまざまな管理タスクを実行できます。

表示されるメニュー項目は次のとおりです。

- サーバー証明書のリセット

  HTTPSサーバ証明書を再生成します。

  Unified Manager GUIでサーバー証明書を再生成するには、**General** > **HTTPS Certificates** > *Regenerate HTTPS Certificate*をクリックします。

- **SAML**認証を無効にする

  SAML認証を無効にすることで、IDプロバイダー（IdP）がUnified Manager GUIにアクセスするユーザーに対してサインオン認証を提供しなくなります。このコンソールオプションは通常、IdPサーバーまたはSAML構成の問題により、ユーザーがUnified Manager GUIにアクセスできない場合に使用されます。

- 外部データプロバイダー

  Unified Managerを外部データプロバイダーに接続するためのオプションを提供します。接続が確立されると、パフォーマンスデータが外部サーバーに送信され、ストレージパフォーマンスの専門家がサードパーティ製ソフトウェアを使用してパフォーマンス指標をグラフ化できるようになります。以下のオプションが表示されます：

  - サーバー構成の表示--外部データプロバイダの現在の接続と構成設定を表示します。
  - サーバー接続の追加/変更--外部データプロバイダの新しい接続設定を入力したり、既存の設定を変更したりできます。
  - サーバー構成の変更--外部データプロバイダーの新しい構成設定を入力したり、既存の設定を変更したりできます。
  - サーバー接続の削除--外部データプロバイダへの接続を削除します。

    接続を削除すると、Unified Managerは外部サーバから切断されます。

- バックアップ復元

  詳細については、"バックアップとリストア処理の管理"のトピックを参照してください。

- パフォーマンスポーリング間隔設定

  Unified Managerがクラスターからパフォーマンス統計データを収集する頻度を設定するオプションを提供します。デフォルトの収集間隔は5分です。

  大規模なクラスタからの収集が時間内に完了しない場合は、この間隔を10分または15分に変更できます。

- アプリケーションポートの表示/変更

Unified ManagerがHTTPおよびHTTPSプロトコルに使用するデフォルトのポートを変更するためのオプションを提供します（セキュリティ上必要である場合）。デフォルトのポートは、HTTPの場合は80、HTTPSの場合は443です。

- **MySQL**ポート**3306**へのアクセスを制御します

  ホストからデフォルトのMySQLポート3306へのアクセスを制御します。セキュリティ上の理由から、Linux、Windows、およびVMware vSphereシステムへのUnified Managerの新規インストール中は、このポートを使用したアクセスはローカル ホストに限定されます。このオプションを使用すると、このポートの認識をローカル ホストとリモート ホストの間で切り替えることができます。つまり、このオプションをローカル ホストに対してのみ有効にすると、リモート ホストでポート3306を使用できるようにすることができます。逆に、すべてのホストに対して有効にすると、このポートのアクセスをローカル ホストに限定できます。アップグレード前にリモート ホストでアクセスが有効になっていれば、アップグレード後もその設定が維持されます。ポートの認識を切り替えたら、Windowsシステムのファイアウォール設定を確認し、MySQLポート3306へのアクセスが制限されている場合はファイアウォールの設定を無効にする必要があります。

- 終了

  メンテナンス コンソール メニューを終了します。

Active IQ Unified Manager で Windows のメンテナンスユーザーのパスワードを変更する

必要に応じて、Unified Managerのメンテナンスユーザーのパスワードを変更できます。

手順

1. Unified Manager の Web UI ログインページから、「パスワードを忘れた場合」をクリックします。

   パスワードをリセットするユーザの名前を入力するように求めるページが表示されます。

2. ユーザー名を入力して、送信 をクリックします。

   入力したユーザ名に定義されているEメール アドレスに、パスワードをリセットするためのリンクが記載されたEメールが送信されます。

3. メールに記載されている「パスワードをリセット」リンクをクリックして、新しいパスワードを設定してください。
4. ウェブUIに戻り、新しいパスワードを使用してUnified Managerにログインしてください。

Linux システムでの Active IQ Unified Manager の umadmin パスワードの変更

セキュリティ上の理由から、インストール プロセスの完了後すぐにUnified Managerのumadminユーザのデフォルト パスワードを変更する必要があります。このパスワードは、必要に応じてあとからいつでも再変更できます。

開始する前に

- Unified ManagerがRed Hat Enterprise Linuxシステムにインストールされている必要があります。
- Unified Managerがインストールされ ているLinuxシステムのrootユーザのクレデンシャルが必要です。

手順

1. Unified Managerが実行されているLinuxシステムにrootユーザとしてログインします。
2. umadminパスワードを変更します。

   ```
   passwd umadmin
   ```

   umadminユーザの新しいパスワードを入力するように求められます。

Active IQ Unified Manager がHTTPおよびHTTPSプロトコルに使用するポートを変更する

Unified ManagerがHTTPおよびHTTPSプロトコルに使用するデフォルトのポートは、インストール後に変更できます（セキュリティ上必要な場合）。デフォルトのポートは、HTTPの場合は80、HTTPSの場合は443です。

開始する前に

Unified Managerサーバのメンテナンス コンソールへのログインが許可されているユーザIDとパスワードが必要です。

> Mozilla FirefoxまたはGoogle Chromeブラウザでは、安全でないとみなされるポートがいくつかあります。HTTPトラフィックとHTTPSトラフィックに新しいポート番号を割り当てる前にブラウザで確認してください。安全でないポートを選択すると、システムにアクセスできなくなる可能性があります。その場合、カスタマー サポートに連絡して解決を依頼する必要があります。

ポートを変更するとUnified Managerのインスタンスが自動的に再起動されるため、システムを短時間停止しても問題のないタイミングであることを確認してください。

1. SSHを使用して、Unified Managerホストにメンテナンス ユーザとしてログインします。

   Unified Managerメンテナンス コンソールのプロンプトが表示されます。

2. 「アプリケーションポートの表示/変更」というラベルの付いたメニューオプションの番号を入力し、Enter キーを押してください。
3. プロンプトが表示されたら、メンテナンス ユーザのパスワードをもう一度入力します。
4. HTTPポートとHTTPSポートの新しいポート番号を入力し、Enterキーを押します。

   ポート番号を空白のままにした場合は、プロトコルのデフォルトのポートが割り当てられます。

   ポートを変更してUnified Managerをすぐに再起動するかどうかを確認するメッセージが表示されます。

5. ポートを変更して Unified Manager を再起動するには、**y** と入力してください。
6. メンテナンス コンソールを終了します。

この変更後、ユーザーはUnified Manager Web UIにアクセスするために、URLに新しいポート番号を含める必要があります。例：https://host.company.com:1234、https://12.13.14.15:1122、または+https://[2001:db8:0:1]:2123+。

Active IQ Unified Manager へのネットワークインターフェイスの追加

ネットワーク トラフィックを分離する必要がある場合は、新しいネットワーク インターフェイスを追加できます。

開始する前に

vSphereを使用して仮想アプライアンスにネットワーク インターフェイスを追加しておく必要があります。

仮想アプライアンスの電源をオンにする必要があります。

Unified ManagerがRed Hat Enterprise LinuxまたはMicrosoft Windowsにインストールされている場合は、この処理を実行できません。

手順

1. vSphereコンソールのメインメニューで、システム構成 > *オペレーティングシステムの再起動*を選択します。

   再起動すると、新たに追加したネットワーク インターフェイスがメンテナンス コンソールで検出されます。

2. メンテナンス コンソールにアクセスします。
3. **Network Configuration** > **Enable Network Interface** を選択します。
4. 新しいネットワークインターフェースを選択し、**Enter** キーを押してください。

   eth1 を選択して **Enter** を押してください。

5. ネットワークインターフェースを有効にするには、**y** と入力してください。
6. ネットワークの設定を入力します。

   静的インターフェイスを使用している場合、またはDHCPが検出されない場合は、ネットワークの設定を入力するよう求められます。

   ネットワーク設定を入力すると、自動的に*ネットワーク設定*メニューに戻ります。

7. 「変更を確定」を選択します。

   ネットワーク インターフェイスを追加するには、変更をコミットする必要があります。

Active IQ Unified Manager でクライアント証明書を再生成する

メンテナンス コンソールを使用して、Unified Managerクライアント証明書を再生成できます。証明書の有効期間は5年間に延長されています。

手順

1. メンテナンス ユーザとしてログインします。
2. **Regenerate Client Certificate** を選択して、**Enter** キーを押します。
3. システムが認証を求めた場合は、必要な認証情報を入力してください。

4. *再生成の確認*を選択し、*Enter*を押します。
5. 証明書が再生成されたら、Unified Managerサービスを再起動して変更を適用してください。
6. 更新された証明書を確認するには、ONTAPにログインします。クライアント証明書のステータスと有効性ステータスを確認します。

関連情報 "System ManagerでONTAP証明書を管理する"

ディスク容量を追加する

Active IQ Unified Manager データベースディレクトリへのディスク容量の追加

ONTAPシステムから収集された健全性とパフォーマンスのデータは、すべてUnified Managerデータベース ディレクトリに格納されます。状況によっては、データベース ディレクトリのサイズの拡張が必要になることがあります。

たとえば、Unified Managerで多数のクラスタからデータを収集している場合、各クラスタに大量のノードがあると、データベース ディレクトリがいっぱいになることがあります。データベース ディレクトリの容量の95%に達すると警告イベントが生成され、95%に達すると重大イベントが生成されます。

ディレクトリの容量の95%に達すると、クラスタからデータが収集されなくなります。

データ ディレクトリの容量を追加する手順は、Unified ManagerをVMware ESXiサーバ、Red Hatサーバ、Microsoft Windowsサーバのいずれで実行しているかによって異なります。

Active IQ Unified Manager で **Linux** ホスト上のデータディレクトリにスペースを追加する

Linux ホストを最初にセットアップして Unified Manager をインストールした際に、Unified Manager をサポートするための `/opt/netapp/data`ディレクトリに割り当てたディスク容量が不足していた場合は、インストール後に `/opt/netapp/data`ディレクトリのディスク容量を増やすことでディスク容量を追加できます。

開始する前に

Unified ManagerがインストールされているRed Hat Enterprise Linuxマシンへのrootユーザ アクセスが必要です。

データ ディレクトリのサイズを拡張する前にUnified Managerデータベースをバックアップすることを推奨します。

手順

1. ディスク スペースを追加するLinuxマシンにrootユーザとしてログインします。
2. Unified Managerサービスと関連するMySQLソフトウェアを次の順序で停止します。

```
systemctl stop ocieau ocie mysqld
```

3. 一時的なバックアップフォルダ（例： `/backup-data`）を作成します。現在の `/opt/netapp/data`ディレクトリ内のデータを格納するのに十分なディスク容量を確保してください。
4. 既存の `/opt/netapp/data`ディレクトリのコンテンツと権限構成を、バックアップデータディレクトリにコ

ピーします：

```
cp -arp /opt/netapp/data/* /backup-data
```

5. SE Linuxが有効になっている場合は、次の手順を実行します。

   a. 既存の `/opt/netapp/data`フォルダのフォルダの SE Linux タイプを取得します：

   ```
   se_type= ls -Z /opt/netapp/data | awk '{print $4}' | awk -F: '{print $3}' |
   head -1
   ```

   次のような情報が返されます。

```
echo $se_type
mysqld_db_t
```

   a. chconコマンドを実行して、バックアップ ディレクトリに対してSE Linuxタイプを設定します。

   ```
   chcon -R --type=mysqld_db_t /backup-data
   ```

6. `/opt/netapp/data`ディレクトリの内容を削除します：

   a. `cd /opt/netapp/data`

   b. `rm -rf *`

7. `/opt/netapp/data`ディレクトリのサイズを、LVMコマンドを使用するか、ディスクを追加することで、最低150 GBまで拡張します。

   ディスクから `/opt/netapp/data`を作成した場合は、 `/opt/netapp/data`をNFSまたはCIFS共有としてマウントしないでください。この場合、ディスク領域を拡張しようとすると、 `resize`や `extend`などの一部のLVMコマンドが期待どおりに動作しない可能性があるためです。

8. `/opt/netapp/data`ディレクトリの所有者（mysql）とグループ（root）が変更されていないことを確認します：

   ```
   ls -ltr /opt/netapp/ | grep data
   ```

   次のような情報が返されます。

```
drwxr-xr-x.  17 mysql root  4096 Aug 28 13:08 data
```

9. SE Linux が有効になっている場合は、 `/opt/netapp/data`ディレクトリのコンテキストがまだ mysqld_db_t に設定されていることを確認してください。

   a. `touch /opt/netapp/data/abc`

   b. `ls -Z /opt/netapp/data/abc`

次のような情報が返されます。

```
-rw-r--r--. root root unconfined_u:object_r:mysqld_db_t:s0
/opt/netapp/data/abc
```

10. ファイルabcを削除して、この無駄なファイルがデータベース エラーの原因にならないようにします。
11. backup-data から拡張された `/opt/netapp/data`ディレクトリに内容をコピーして戻します：

    ```
    cp -arp /backup-data/* /opt/netapp/data/
    ```

12. SE Linuxが有効になっている場合は、次のコマンドを実行します。

    ```
    chcon -R --type=mysqld_db_t /opt/netapp/data
    ```

13. MySQLサービスを開始します。

    ```
    systemctl start mysqld
    ```

14. MySQLサービスが開始されたら、ocieサービスとocieauサービスを次の順序で開始します。

    ```
    systemctl start ocie ocieau
    ```

15. すべてのサービスが起動したら、バックアップフォルダを削除します `/backup-data`：

    ```
    rm -rf /backup-data
    ```

Active IQ Unified Manager を使用して **VMware** 仮想マシンのデータディスクに空き容量を追加する

Unified Managerデータベースのデータ ディスクのスペースを増やす必要がある場合は、インストール後にUnified Managerメンテナンス コンソールを使用して容量を追加できます。

開始する前に

- vSphere Clientへのアクセス権が必要です。
- 仮想マシンにスナップショットがローカルに格納されていない必要があります。
- メンテナンス ユーザのクレデンシャルが必要です。

仮想ディスクのサイズを拡張する前に仮想マシンをバックアップすることを推奨します。

手順

1. vSphereクライアントで、Unified Manager仮想マシンを選択し、データにディスク容量を追加します `disk 3`。詳細については、VMwareのドキュメントを参照してください。

   まれなケースでは、Unified Managerの展開において、データディスクとして「`Hard Disk 3`」ではなく「`Hard Disk 2`」が使用されることがあります。お使いの環境でこの問題が発生している場合は、容量の大きい方のディスクの容量を増やしてください。データディスクは、常に他のディスクよりも容量が大きくなります。

2. vSphere クライアントで、Unified Manager 仮想マシンを選択し、「コンソール」タブを選択します。
3. コンソール ウィンドウ内をクリックし、ユーザ名とパスワードを使用してメンテナンス コンソールにログインします。
4. メインメニューで、*システム設定*オプションの番号を入力します。
5. システム構成メニューで、*データディスクサイズの増加*オプションの番号を入力します。

Active IQ Unified Manager で **Windows** サーバーの論理ドライブに空き容量を追加する

Unified Managerデータベースのディスク スペースを増やす必要がある場合は、Unified Managerがインストールされている論理ドライブに容量を追加できます。

開始する前に

Windowsの管理者権限が必要です。

ディスク スペースを追加する前にUnified Managerデータベースをバックアップすることを推奨します。

手順

1. ディスク スペースを追加するWindowsサーバに管理者としてログインします。
2. スペースを追加する方法に応じて、該当する手順を実行します。

オプション	説明
物理サーバで、Unified Managerサーバがインストールされている論理ドライブに容量を追加する。	Microsoftの次のトピックの手順に従います。 "Extend a Basic Volume"
物理サーバで、ハード ディスク ドライブを追加する。	Microsoftの次のトピックの手順に従います。 "Adding Hard Disk Drives"
仮想マシンで、ディスク パーティションのサイズを拡張する。	VMwareの次のトピックの手順に従います。 "Increasing the size of a disk partition"

ユーザ アクセスの管理

ユーザの追加

Active IQ Unified Manager でユーザーを追加する

[ユーザ]ページを使用して、ローカル ユーザまたはデータベース ユーザを追加できます。また、認証サーバに属するリモート ユーザやリモート グループを追加することもできます。追加したユーザにロールを割り当てることで、ユーザはロールの権限に基づいてUnified Managerでストレージ オブジェクトやデータを管理したり、データベースのデータを参照したりすることができます。

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。

- リモート ユーザまたはリモート グループを追加する場合は、リモート認証を有効にし、認証サーバを設定しておく必要があります。
- IDプロバイダー（IdP）がグラフィカルインターフェイスにアクセスするユーザーを認証するようにSAML認証を設定する場合は、これらのユーザーが「`remote`」ユーザーとして定義されていることを確認してください。

  SAML認証が有効になっている場合、タイプが「`local`」または「`maintenance`」のユーザーはUIにアクセスできません。

Windows Active Directoryのグループを追加した場合、そのグループの直接のメンバーに加え、ネストされたサブグループも（無効になっていなければ）すべてUnified Managerで認証されます。OpenLDAPまたはその他の認証サービスからグループを追加した場合は、そのグループの直接のメンバーだけがUnified Managerで認証されます。

手順

1. 左側のナビゲーションペインで、**General** > **Users** をクリックします。
2. ユーザーページで、*追加*をクリックします。
3. [ユーザの追加]ダイアログ ボックスで、追加するユーザのタイプを選択し、必要な情報を入力します。

   ユーザに固有なEメール アドレスを指定する必要があります。複数のユーザで共有しているEメール アドレスは指定しないでください。

4. *[追加]*をクリックします。

Active IQ Unified Manager でデータベースユーザーを作成する

Workflow AutomationとUnified Managerの間の接続をサポートする場合や、データベース ビューにアクセスする場合は、まずUnified Manager Web UIで、統合スキーマ ロールまたはレポート スキーマ ロールを割り当てたデータベース ユーザを作成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。

データベース ユーザは、Workflow Automationとの統合およびレポート固有のデータベース ビューへのアクセスを行えます。データベース ユーザは、Unified Manager Web UIやメンテナンス コンソールにはアクセスできず、API呼び出しも実行できません。

手順

1. 左側のナビゲーションペインで、**General** > **Users** をクリックします。
2. 「Users」ページで、**Add** をクリックします。
3. 「ユーザーの追加」ダイアログボックスで、*タイプ*ドロップダウンリストから*データベースユーザー*を選択します。
4. データベース ユーザの名前とパスワードを入力します。
5. *役割*ドロップダウンリストから、適切な役割を選択してください。

状況	この役割を選択してください
Unified ManagerをWorkflow Automationに接続する場合	統合スキーマ
レポートおよびその他のデータベース ビューにアクセスする場合	レポート スキーマ

6. *[追加]*をクリックします。

Active IQ Unified Manager でユーザー設定を編集する

ユーザごとに指定されたEメール アドレスやロールなどの設定を編集することができます。たとえば、ストレージ オペレータのユーザのロールを変更して、そのユーザにストレージ管理者の権限を割り当てることができます。

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。

ユーザに割り当てられているロールを変更した場合、次のいずれかの時点で変更内容が反映されます。

- ユーザがUnified Managerからログアウトして再度ログインしたとき
- セッションの開始から24時間が経過してタイムアウトしたとき

手順

1. 左側のナビゲーションペインで、**General** > **Users** をクリックします。
2. ユーザーページで、設定を編集するユーザーを選択し、*編集*をクリックします。
3. [ユーザの編集]ダイアログ ボックスで、ユーザに対して指定されている設定を編集します。
4. *保存*をクリックします。

Active IQ Unified Manager でユーザーを表示する

[ユーザ]ページでは、Unified Managerを使用してストレージ オブジェクトとデータを管理するユーザのリストを表示できます。ユーザに関する詳細（ユーザ名、ユーザのタイプ、Eメール アドレス、ユーザに割り当てられているロールなど）を参照できます。

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。

手順

1. 左側のナビゲーションペインで、**General** > **Users** をクリックします。

Active IQ Unified Manager でユーザーまたはグループを削除する

管理サーバ データベースから1人または複数のユーザを削除して、それらのユーザがUnified Managerにアクセスできないようにすることができます。また、グループを削除すると、そのグループのすべてのユーザによる管理サーバへのアクセスを禁止できま

す。

開始する前に

- リモート グループを削除するときは、リモート グループのユーザに割り当てられているイベントを再割り当てしておく必要があります。

  ローカル ユーザまたはリモート ユーザを削除する場合は、それらのユーザに割り当てられていたイベントの割り当てが自動的に解除されます。

- 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、**General** > **Users** をクリックします。
2. 「ユーザー」ページで、削除するユーザーまたはグループを選択し、*削除*をクリックします。
3. 削除を確定するには「はい」をクリックしてください。

Active IQ Unified Manager のロールベースアクセス制御について

RBAC （ロールベースアクセス制御）は、Active IQ Unified Manager サーバのさまざまな機能やリソースへのアクセスを制御する機能を提供します。RBAC を使用すると、管理者はロールを定義することでユーザーグループを管理できます。特定の機能へのアクセスを特定の管理者のみに制限する必要がある場合は、該当する管理者用に管理者アカウントを設定する必要があります。管理者が閲覧できる情報や実行できる操作を制限する場合は、作成する管理者アカウントにロールを適用する必要があります。

管理サーバでは、ユーザ ログインとロールの権限に対してRBACを使用します。管理サーバで管理ユーザ アクセスのデフォルト設定を変更していない場合は、ログインして設定を表示する必要はありません。

特定の権限を必要とする処理を開始すると、管理サーバによってログインが求められます。たとえば、管理者アカウントを作成するには、アプリケーション管理者アカウントのアクセス権でログインする必要があります。

Active IQ Unified Manager のユーザータイプについて

ユーザは、アカウントの種類に基づいて、リモート ユーザ、リモート グループ、ローカル ユーザ、データベース ユーザ、およびメンテナンス ユーザの各タイプに分類されます。それぞれのタイプには、管理者ロールを持つユーザによって独自のロールが割り当てられます。

Unified Managerには次のユーザ タイプがあります。

- メンテナンスユーザー

  Unified Managerの初期設定時に作成されます。その後、メンテナンスユーザーが追加のユーザーを作成し、ロールを割り当てます。メンテナンスユーザーは、メンテナンスコンソールにアクセスできる唯一のユーザーでもあります。Unified ManagerがRed Hat Enterprise Linuxシステムにインストールされている場合、メンテナンスユーザーには「`umadmin.`」というユーザー名が割り当てられます。

- ローカル ユーザ

  Unified Manager UIにアクセスし、メンテナンス ユーザまたはアプリケーション管理者ロールを持つユーザから割り当てられたロールに基づいて操作を実行します。

- リモートグループ

  認証サーバに保存されているクレデンシャルを使用してUnified Manager UIにアクセスするユーザのグループです。このグループの名前は、認証サーバに保存されているグループの名前と同じにする必要があります。リモート グループのユーザは、各自のユーザ クレデンシャルを使用してUnified Manager UIにアクセスできます。リモート グループに割り当てられたロールに基づいて操作を実行できます。

- リモートユーザー

  認証サーバに保存されているクレデンシャルを使用してUnified Manager UIにアクセスします。リモートユーザは、メンテナンス ユーザまたはアプリケーション管理者ロールを持つユーザから割り当てられたロールに基づいて操作を実行します。

- データベースユーザー

  Unified Managerデータベースのデータへの読み取り専用アクセスが許可されます。Unified ManagerのWebインターフェイスやメンテナンス コンソールにはアクセスできず、API呼び出しも実行できません。

Active IQ Unified Manager のユーザーロールについて

メンテナンス ユーザまたはアプリケーション管理者が、各ユーザにロールを割り当てます。各役割には、それぞれ特定の権限が付与されています。Unified Manager で実行できるアクティビティの範囲は、割り当てられた役割と、その役割に含まれる権限によって異なります。

Unified Managerには、以下の事前定義されたユーザーロールが含まれています。

- オペレーター

  Unified Managerによって収集されたストレージシステム情報やその他のデータ（履歴や容量傾向など）を表示します。この役割により、ストレージオペレーターはイベントの表示、割り当て、確認、解決、およびメモの追加を行うことができます。

- ストレージ管理者

  Unified Manager内でストレージ管理操作を設定します。この役割により、ストレージ管理者はしきい値の設定、アラートの作成、その他ストレージ管理固有のオプションやポリシーの作成を行うことができます。

- アプリケーション管理者

  ストレージ管理以外の設定を行います。ユーザ、セキュリティ証明書、データベース アクセスのほか、認証、SMTP、ネットワーク、AutoSupportなどの管理オプションの設定が可能です。

> Unified ManagerがLinuxシステムにインストールされると、アプリケーション管理者ロールを持つ最初のユーザーは自動的に「umadmin」という名前になります。

- 統合スキーマ

  UnifiedManagerとOnCommand Workflow Automation（WFA）の統合用にUnified Managerのデータベース ビューにアクセスするための読み取り専用アクセスが許可されます。

- レポートスキーマ

  この役割により、Unified Manager データベースからレポートやその他のデータベースビューへの読み取り専用アクセスが可能になります。閲覧可能なデータベースは以下のとおりです。

  - netapp_model_view
  - netapp_performance
  - ocum
  - ocum_report
  - ocum_report_birt
  - opm
  - scalemonitor

Active IQ Unified Manager におけるユーザーロールと機能について

Unified Managerで実行できる処理は、割り当てられているユーザ ロールに基づいて決まります。

次の表に、各ユーザ ロールで実行できる機能を示します。

機能	演算子	ストレージ管理者	アプリケーション管理者	統合スキーマ	レポート スキーマ
ストレージ システムの情報の表示	•	•	•	•	•
その他のデータ（履歴や容量の使用状況）の表示	•	•	•	•	•
イベントの表示、割り当て、解決	•	•	•		
SVM関連付けやリソースプールなどのストレージサービスオブジェクトを表示します	•	•	•		
しきい値ポリシーの表示	•	•	•		

機能	演算子	ストレージ管理者	アプリケーション管理者	統合スキーマ	レポートスキーマ
SVM関連付けやリソースプールなどのストレージサービスオブジェクトを管理する		•	•		
アラートの定義		•	•		
ストレージ管理オプションの管理		•	•		
ストレージ管理ポリシーの管理		•	•		
ユーザの管理			•		
管理オプションの管理			•		
しきい値ポリシーの定義			•		
データベース アクセスの管理			•		
WFAとの統合の管理とデータベース ビューへのアクセス				•	
レポートのスケジュール設定と保存		•	•		
管理アクションから「修正」操作を実行します		•	•		
データベース ビューへの読み取り専用アクセスの提供					•

SAML認証設定の管理

Active IQ Unified Manager で SAML 認証を有効にする

リモート認証を設定したあと、Security Assertion Markup Language（SAML）認証を有効にして、Unified ManagerのWeb UIにアクセスするリモート ユーザをセキュアなアイデンティティ プロバイダ（IdP）で認証するように設定できます。

SAML認証を有効にした場合、Unified Managerのグラフィカル ユーザ インターフェイスにアクセスできるの

はリモート ユーザのみです。ローカル ユーザとメンテナンス ユーザはUIにアクセスできません。この設定は、メンテナンス コンソールにアクセスするユーザには影響しません。

Active IQ Unified Manager でIDプロバイダーを使用する

Unified ManagerでIDプロバイダー（IdP）を使用してすべてのリモートユーザーのSAML認証を実行するように構成する場合、Unified Managerへの接続を成功させるために必要な構成設定について理解しておく必要があります。

Unified ManagerのURIとメタデータをIdPサーバーに入力する必要があります。この情報は、Unified ManagerのSAML認証ページからコピーできます。Unified Managerは、Security Assertion Markup Language （SAML）標準においてサービスプロバイダー（SP）と見なされます。

サポートされる暗号化標準

- Advanced Encryption Standard（AES）：AES-128およびAES-256
- Secure Hash Algorithm（SHA）：SHA-1およびSHA-256

検証済みのアイデンティティ プロバイダ

- Shibboleth
- Active Directoryフェデレーション サービス（ADFS）

ADFSの設定要件

- Unified Managerがこの証明書利用者信頼エントリのADFS SAML応答を解析するために必要な、3つのクレームルールを以下の順序で定義する必要があります。

要求規則	**Value**
SAM-account-name	Name ID
SAM-account-name	urn:oid:0.9.2342.19200300.100.1.1
Token groups – Unqualified Name	urn:oid:1.3.6.1.4.1.5923.1.5.1.1

- 認証方法を「`Forms Authentication`」に設定する必要があります。そうしないと、Unified Managerからログアウトする際にユーザーがエラーを受け取る可能性があります。以下の手順に従ってください。
  a. ADFS管理コンソールを開きます。
  b. 左側のツリー ビューで[認証ポリシー]フォルダをクリックします。
  c. 右側の[操作]で、[グローバル プライマリ認証ポリシーの編集]をクリックします。
  d. イントラネット認証方法を、デフォルトの「`Windows Authentication`」ではなく「`Forms Authentication`」に設定してください。
- Unified Managerのセキュリティ証明書がCAによって署名されている場合、IdP経由のログインが拒否されることがあります。この問題を解決するには、2つの回避策があります。
  ◦ 次のリンクの手順に従って、CA証明書チェーンの関連する証明書利用者についてのADFSサーバでの失効確認を無効にします。

"信頼当事者トラストごとの失効チェックを無効にする"

- Unified Managerサーバーの証明書要求に署名するために、CAサーバーをADFSサーバー内に配置してください。

その他の設定要件

- Unified Managerのクロックスキューは5分に設定されているため、IdPサーバーとUnified Managerサーバー間の時間差は5分を超えてはならず、超えると認証が失敗します。

Active IQ Unified Manager で SAML 認証を有効にする

Security Assertion Markup Language（SAML）認証を有効にして、Unified ManagerのWeb UIにアクセスするリモート ユーザをセキュアなアイデンティティ プロバイダ（IdP）で認証するように設定できます。

開始する前に

- リモート認証を設定し、正常に動作することを確認しておく必要があります。
- アプリケーション管理者ロールが割り当てられたリモート ユーザまたはリモート グループを少なくとも1つ作成しておく必要があります。
- アイデンティティ プロバイダ（IdP）がUnified Managerでサポートされ、設定が完了している必要があります。
- IdPのURLとメタデータが必要です。
- IdPサーバへのアクセスが必要です。

Unified ManagerでSAML認証を有効にしたあと、Unified Managerサーバのホスト情報を使用してIdPを設定するまでは、ユーザはグラフィカル ユーザ インターフェイスにアクセスできません。そのため、設定プロセスを開始する前に、両方で接続の準備を完了しておく必要があります。IdPの設定は、Unified Managerの設定前にも設定後にも実行できます。

SAML認証を有効にしたあとでUnified Managerのグラフィカル ユーザ インターフェイスにアクセスできるのはリモート ユーザのみです。ローカル ユーザとメンテナンス ユーザはUIにアクセスできません。この設定は、メンテナンス コンソール、Unified Managerコマンド、ZAPIにアクセスするユーザには影響しません。

このページでSAMLの設定を完了すると、Unified Managerが自動的に再起動されます。

手順

1. 左側のナビゲーションペインで、**General** > **SAML Authentication** をクリックします。
2. 「SAML 認証を有効にする」チェックボックスを選択します。

   IdPの接続の設定に必要なフィールドが表示されます。

3. IdPのURIとUnified ManagerサーバをIdPに接続するために必要なIdPメタデータを入力します。

   IdP サーバーに Unified Manager サーバーから直接アクセスできる場合は、IdP URI を入力した後に **IdP** メタデータの取得 ボタンをクリックすると、IdP メタデータフィールドに自動的に入力されます。

4. Unified Managerのホスト メタデータURIをコピーするか、ホスト メタデータをXMLテキスト ファイルに

保存します。

この情報を使用してIdPサーバを設定できます。

5. *保存*をクリックします。

設定を完了してUnified Managerを再起動するかどうかの確認を求めるメッセージ ボックスが表示されます。

6. 「確認してログアウト」をクリックすると、Unified Manager が再起動されます。

許可されたリモート 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する際にクレデンシャルを入力するページが、次回からUnified Managerのログイン ページではなくIdPのログイン ページに変わります。

まだ完了していない場合は、IdPにアクセスし、Unified ManagerサーバのURIとメタデータを入力して設定を完了します。

IDプロバイダとしてADFSを使用している場合、Unified ManagerのGUIにはADFSのタイムアウトが適用されず、Unified Managerのセッションタイムアウトに達するまで動作し続けます。GUIセッションのタイムアウトを変更するには、一般 > 機能設定 > *非アクティブタイムアウト*をクリックします。

Active IQ Unified Manager でSAML認証IDプロバイダーを変更する

Unified Managerでリモート ユーザの認証に使用するアイデンティティ プロバイダ（IdP）を変更することができます。

開始する前に

- IdPのURLとメタデータが必要です。
- IdPへのアクセスが必要です。

新しいIdPの設定は、Unified Managerの設定前にも設定後にも実行できます。

手順

1. 左側のナビゲーションペインで、**General** > **SAML Authentication** をクリックします。
2. 新しいIdPのURIとUnified ManagerサーバをIdPに接続するために必要なIdPメタデータを入力します。

Unified Manager サーバーから IdP に直接アクセスできる場合は、IdP URL を入力した後、**IdP** メタデータの取得 ボタンをクリックすると、IdP メタデータフィールドに自動的に入力されます。

3. Unified ManagerのメタデータURIをコピーするか、メタデータをXMLテキスト ファイルに保存します。
4. 設定を保存 をクリックします。

設定を変更するかどうかの確認を求めるメッセージ ボックスが表示されます。

5. *OK*をクリックします。

新しいIdPにアクセスし、Unified ManagerサーバのURIとメタデータを入力して設定を完了します。

許可されたリモート 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する際にクレデンシャルを入力するページが、次回から古いIdPのログイン ページではなく新しいIdPのログイン ページに変わります。

Active IQ Unified Manager のセキュリティ証明書変更後に SAML 認証設定を更新する

Unified Managerサーバーにインストールされ ているHTTPSセキュリティ証明書に変更を加えた場合は、SAML認証構成設定を更新する必要があります。ホストシステムの名前を変更したり、ホストシステムに新しいIPアドレスを割り当てたり、システムのセキュリティ証明書を手動で変更したりすると、証明書が更新されます。

セキュリティ証明書が変更され、Unified Managerサーバーが再起動されると、SAML認証が機能しなくなり、ユーザーはUnified Managerのグラフィカルインターフェースにアクセスできなくなります。ユーザーインターフェースへのアクセスを再度有効にするには、IdPサーバーとUnified Managerサーバーの両方でSAML認証設定を更新する必要があります。

手順

1. メンテナンス コンソールにログインします。
2. *メインメニュー*で、*SAML認証を無効にする*オプションの番号を入力してください。

   SAML認証を無効にしてUnified Managerを再起動することの確認を求めるメッセージが表示されます。

3. 更新されたFQDNまたはIPアドレスを使用してUnified Managerのユーザーインターフェイスを起動し、更新されたサーバー証明書をブラウザで承認してから、メンテナンスユーザーの認証情報を使用してログインします。
4. *設定/認証*ページで、*SAML認証*タブを選択し、IdP接続を設定します。
5. Unified Managerのホスト メタデータURIをコピーするか、ホスト メタデータをXMLテキスト ファイルに保存します。
6. *保存*をクリックします。

   設定を完了してUnified Managerを再起動するかどうかの確認を求めるメッセージ ボックスが表示されます。

7. 「確認してログアウト」をクリックすると、Unified Manager が再起動されます。
8. IdPサーバーにアクセスし、Unified ManagerサーバーのURIとメタデータを入力して設定を完了してください。

IDプロバイダー	設定手順
ADFS	a. ADFS管理GUIで、既存の証明書利用者信頼エントリを削除します。 b. 更新されたUnified Managerサーバーの `saml_sp_metadata.xml`を使用して、新しい証明書利用者信頼エントリを追加します。 c. Unified Manager がこの証明書利用者信頼エントリの ADFS SAML 応答を解析するために必要な 3 つのクレームルールを定義します。 d. ADFS Windowsサービスを再開します。
Shibboleth	a. Unified Manager サーバーの新しい FQDN を `attribute-filter.xml`および `relying-party.xml`ファイルに更新します。 b. Apache Tomcat Webサーバを再起動し、ポート8005がオンラインになるまで待ちます。

9. Unified Managerにログインし、IdP経由のSAML認証が想定どおりに機能することを確認します。

Active IQ Unified Manager で SAML 認証を無効にする

Unified Manager の Web UI にログインする前に、セキュアな ID プロバイダー（IdP）を介したリモートユーザーの認証を停止する場合は、SAML 認証を無効にすることができます。SAML 認証が無効になっている場合、Active Directory や LDAP などの構成済みのディレクトリサービスプロバイダーがサインオン認証を実行します。

SAML認証を無効にすると、設定されているリモート ユーザに加え、ローカル ユーザとメンテナンス ユーザもグラフィカル ユーザ インターフェイスにアクセスできるようになります。

グラフィカル ユーザ インターフェイスにアクセスできない場合、SAML認証はUnified Managerメンテナンス コンソールからも無効にすることができます。

SAML認証を無効にしたあと、Unified Managerが自動的に再起動されます。

手順

1. 左側のナビゲーションペインで、**General** > **SAML Authentication** をクリックします。
2. 「SAML認証を有効にする」チェックボックスのチェックを外します。
3. *保存*をクリックします。

   設定を完了してUnified Managerを再起動するかどうかの確認を求めるメッセージ ボックスが表示されます。

4. 「確認してログアウト」をクリックすると、Unified Manager が再起動されます。

リモート 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する際にクレデンシャルを入力するページが、次回からIdPのログイン ページではなくUnified Managerのログイン ページに変わります。

IdPにアクセスし、Unified ManagerサーバーのURIとメタデータを削除してください。

Active IQ Unified Manager メンテナンスコンソールから SAML 認証を無効にする

Unified Manager GUIにアクセスできない場合は、必要に応じてメンテナンス コンソールからSAML認証を無効にすることができます。この状況は、設定に誤りがある場合やIdPにアクセスできない場合に発生します。

開始する前に

メンテナンス コンソールにメンテナンス ユーザとしてアクセスできる必要があります。

SAML認証が無効な場合は、Active DirectoryやLDAPなどの設定済みのディレクトリ サービス プロバイダによるサインオン認証が行われます。設定されているリモート ユーザに加え、ローカル ユーザとメンテナンス ユーザもグラフィカル ユーザ インターフェイスにアクセスできるようになります。

SAML認証は、UIの[セットアップ / 認証]ページからも無効にできます。

SAML認証を無効にしたあと、Unified Managerが自動的に再起動されます。

手順

1. メンテナンス コンソールにログインします。
2. *メインメニュー*で、*SAML認証を無効にする*オプションの番号を入力してください。

   SAML認証を無効にしてUnified Managerを再起動することの確認を求めるメッセージが表示されます。

3. 「y」と入力してEnterキーを押すと、Unified Managerが再起動されます。

リモート 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する際にクレデンシャルを入力するページが、次回からIdPのログイン ページではなくUnified Managerのログイン ページに変わります。

必要に応じて、IdPにアクセスしてUnified ManagerサーバのURIとメタデータを削除します。

Active IQ Unified Manager の SAML 認証ページを使用する

[SAML 認証]ページでは、Unified ManagerのWeb UIにログインするリモート ユーザを、セキュアなアイデンティティ プロバイダ（IdP）経由でSAMLを使用して認証するようにUnified Managerを設定することができます。

- SAML設定を作成または変更するには、アプリケーション管理者ロールが必要です。
- リモート認証を設定しておく必要があります。
- リモート ユーザまたはリモート グループを少なくとも1つ設定しておく必要があります。

リモート認証とリモート ユーザの設定後、[SAML認証を有効にする]チェックボックスを選択し、セキュアなアイデンティティ プロバイダを使用した認証を有効にすることができます。

- **IdP URI**

  Unified ManagerサーバーからIdPにアクセスするためのURI。以下にURIの例を示します。

ADFSのURIの例：

```
https://win2016-dc.ntap2016.local/federationmetadata/2007-
06/federationmetadata.xml
```

ShibbolethのURIの例：

```
https://centos7.ntap2016.local/idp/shibboleth
```

- **IdP**メタデータ

  XML形式のIdPメタデータ。

  Unified ManagerサーバーからIdP URLにアクセスできる場合は、*IdPメタデータの取得*ボタンをクリックしてこのフィールドに入力できます。

- ホストシステム（**FQDN**）

  インストール時に定義された、Unified ManagerホストシステムのFQDN。必要に応じてこの値を変更できます。

- ホスト**URI**

  IdPからUnified Managerホストシステムにアクセスするための URI。

- ホストメタデータ

  XML形式のホスト システム メタデータ。

認証を管理する

Active IQ Unified Manager で認証サーバーを編集する

Unified Managerサーバが認証サーバとの通信に使用するポートを変更することができます。

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。

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」チェックボックスをオンにします。
3. 「Authentication Servers」エリアで、編集する認証サーバーを選択し、「Edit」をクリックします。
4. 「認証サーバーの編集」ダイアログボックスで、ポートの詳細を編集します。
5. *保存*をクリックします。

Active IQ Unified Manager で認証サーバーを削除する

Unified Managerサーバと認証サーバの間の通信を中止する場合は、認証サーバを削除できます。たとえば、管理サーバが通信する認証サーバを変更する場合、認証サーバを削除して新しい認証サーバを追加できます。

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。

認証サーバを削除すると、認証サーバのリモート ユーザとリモート グループはUnified Managerにアクセスできなくなります。

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. 削除する認証サーバーを1つ以上選択し、*削除*をクリックします。
3. 削除リクエストを確定するには、「はい」をクリックしてください。

   「セキュア接続を使用する」オプションが有効になっている場合、認証サーバーに関連付けられた証明書は、認証サーバーとともに削除されます。

Active IQ Unified Manager で Active Directory または OpenLDAP を使用して認証する

管理サーバーでリモート認証を有効にし、管理サーバーが認証サーバーと通信するように構成することで、認証サーバー内のユーザーが Unified Manager にアクセスできるようになります。

事前定義された次の認証サービスのいずれかを使用するか、独自の認証サービスを指定できます。

- Microsoft Active Directory

  Microsoftのライトウェイト ディレクトリ サービスは使用できません。

- OpenLDAP

必要な認証サービスを選択し、適切な認証サーバーを追加することで、認証サーバー上のリモートユーザーが Unified Manager にアクセスできるようになります。リモートユーザーまたはグループの認証情報は、認証サーバーによって管理されます。管理サーバーは、構成済みの認証サーバー内でリモートユーザーを認証するために、Lightweight Directory Access Protocol （LDAP）を使用します。

Unified Managerで作成されたローカルユーザーの場合、管理サーバーはユーザー名とパスワードの独自のデータベースを保持します。管理サーバーが認証を実行し、認証にActive DirectoryやOpenLDAPは使用しません。

監査ログ

Active IQ Unified Manager の監査ログについて

監査ログを使用することで、監査ログが侵害されているかどうかを検出できます。ユー

ザーが実行したすべてのアクティビティは監視され、監査ログに記録されます。監査は、Active IQ Unified Managerのすべてのユーザーインターフェイスおよび公開されているAPIの機能に対して実行されます。

*監査ログ：ファイルビュー*を使用すると、Active IQ Unified Managerで使用可能なすべての監査ログファイルを表示およびアクセスできます。監査ログ：ファイルビューでは、ファイルは作成日順に一覧表示されます。このビューには、システムへのインストールまたはアップグレードから現在までに取得されたすべての監査ログの情報が表示されます。Unified Managerで何らかの操作を行うと、その情報が更新され、ログに記録されます。各ログファイルの状態は、「`File Integrity Status\`」属性を使用して取得され、ログファイルの改ざんや削除を検出するために積極的に監視されます。監査ログがシステム内で利用可能な場合、監査ログは次のいずれかの状態になります：

状態	説明
ACTIVE	ログを記録中のファイル。
NORMAL	圧縮されてシステムに格納されている、アクティブでないファイル。
TAMPERED	侵害されたファイル（権限のないユーザによって手動で編集された）。
MANUALL_DELETE	権限のあるユーザによって削除されたファイル。
ROLLOVER_DELETE	ローリング設定ポリシーに基づいてロールオフで削除されたファイル。
UNEXPECTED_DELETE	不明な理由で削除されたファイル。

[監査ログ]ページには、次のコマンド ボタンがあります。

- 設定
- 削除
- ダウンロード

*DELETE*ボタンを使用すると、Audit Logsビューに表示されている任意の監査ログを削除できます。監査ログを削除する際、必要に応じてファイルの削除理由を指定できます。これは、将来的に正当な削除であるかを判断するのに役立ちます。REASON列には、削除操作を実行したユーザー名とともに、その理由が表示されます。

ログ ファイルを削除すると、システムからファイルが削除されますが、DBテーブル内のエントリは削除されません。

Active IQ Unified Managerの監査ログセクションにある*DOWNLOAD*ボタンを使用して監査ログをダウンロードし、監査ログファイルをエクスポートできます。「NORMAL」または「TAMPERED」とマークされたファイルは、圧縮 `.gzip`形式でダウンロードされます。

監査ログ ファイルは定期的にアーカイブされ、参照できるようにデータベースに保存されます。セキュリティと整合性を維持するために、アーカイブ前に監査ログはデジタル署名されます。

完全なAutoSupportバンドルには、アーカイブされた監査ログ ファイルとアクティブな監査ログ ファイルの両方が含まれます。一方、軽量なサポート バンドルには、アクティブな監査ログのみが含まれます。アーカイブされた監査ログは含まれません。

Active IQ Unified Manager 監査ログの設定

監査ログセクションの*設定*ボタンを使用すると、監査ログファイルのローリングポリシーを設定したり、監査ログのリモートログ記録を有効にしたりできます。

システムに保管したいデータの量と頻度に応じて、最大ファイルサイズ*と*監査ログ保持日数*の値を設定できます。*監査ログ合計サイズ*フィールドの値は、システムに存在する監査ログデータの合計サイズを示します。ロールオーバーポリシーは、*監査ログ保持日数、最大ファイルサイズ、および*監査ログ合計サイズ*のフィールドの値によって決定されます。監査ログのバックアップサイズが*監査ログ合計サイズ*で設定された値に達すると、最初にアーカイブされたファイルが削除されます。これは、最も古いファイルが削除されることを意味します。しかし、そのファイルエントリはデータベース内に残っており、「`Rollover Delete`」とマークされます。*監査ログ保持日数*の値は、監査ログファイルが保持される日数を表します。このフィールドに設定された値よりも古いファイルはすべてロールオーバーされます。

手順

1. 監査ログ > > 設定 をクリックします。
2. 最大ファイルサイズ、監査ログの合計サイズ、および*監査ログの保持日数*に値を入力してください。

   リモートログを有効にするには、*リモートログを有効にする*を選択します。

Active IQ Unified Manager で監査ログのリモートロギングを有効にする

リモート監査ログを有効にするには、「監査ログの設定」ダイアログボックスで「リモートログを有効にする」チェックボックスを選択します。この機能を使用すると、監査ログをリモートSyslogサーバに転送できます。これにより、容量に制約がある場合でも監査ログを管理できるようになります。

監査ログのリモート ロギングは、Active IQ Unified Managerサーバ上の監査ログ ファイルが改ざんされた場合のバックアップとしても機能します。

手順

1. 「監査ログの設定」ダイアログボックスで、「リモートログを有効にする」チェックボックスを選択します。

   リモート ロギングを設定するためのフィールドが表示されます。

2. 接続するリモート サーバの*HOSTNAME*と*PORT*を入力します。
3. *サーバーCA証明書*フィールドで、*参照*をクリックして、対象サーバーの公開証明書を選択します。

   証明書は `.pem`形式でアップロードする必要があります。この証明書は対象の`Syslog`サーバから取得する必要があり、有効期限が切れていないものでなければなりません。証明書には、選択した「`hostname`」が `SubjectAltName`（SAN）属性の一部として含まれている必要があります。

4. 以下のフィールドに値を入力してください：**CHARSET**、**CONNECTION TIMEOUT**、**RECONNECTION DELAY**。

   ミリ秒単位の値を指定してください。

5. **FORMAT** および **PROTOCOL** フィールドで、必要なSyslogフォーマットとTLSプロトコル バージョンを選択します。

6. 対象のSyslogサーバが証明書ベースの認証を必要とする場合は、*クライアント認証を有効にする*チェックボックスを選択します。

   監査ログ設定を保存する前に、クライアント認証証明書をダウンロードしてsyslogサーバにアップロードする必要があります。そうしないと、接続が失敗します。syslogサーバのタイプによっては、クライアント認証証明書のハッシュを作成する必要があります。

   例：syslog-ng では、コマンド `openssl x509 -noout -hash -in cert.pem`を使用して証明書の<hash>を作成する必要があります。その後、クライアント認証証明書を<hash> .0 という名前のファイルにシンボリック リンクする必要があります。

7. *Save*をクリックしてサーバとの接続を設定し、リモートログ記録を有効にします。

   [監査ログ]ページにリダイレクトされます。

   *接続タイムアウト*の値は設定に影響を与える可能性があります。設定応答時間が規定値よりも長くなると、接続エラーにより設定が失敗する可能性があります。接続を正常に確立するには、*接続タイムアウト*の値を増やして、再度設定を試してください。

Active IQ Unified Manager のリモート認証ページを使用する

[リモート認証]ページでは、Unified Manager Web UIにログインするリモート ユーザを認証できるように、Unified Managerと認証サーバの通信を設定することができます。

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。

[リモート認証を有効化する]チェックボックスをオンにすると、認証サーバを使用したリモート認証を有効にすることができます。

- 認証サービス

  Active DirectoryやOpenLDAPなどのディレクトリ サービス プロバイダでユーザを認証するように管理サーバを設定するか、または独自の認証メカニズムを指定できます。認証サービスは、リモート認証を有効にした場合にのみ指定できます。

  - **Active Directory**
    - 管理者名

      認証サーバの管理者の名前を指定します。

    - パスワード

      認証サーバにアクセスするためのパスワードを指定します。

    - ベース識別名

      認証サーバーにおけるリモートユーザーの場所を指定します。例えば、認証サーバーのドメイン名が ou@domain.com の場合、ベース識別名は **cn=ou,dc=domain,dc=com** です。

    - ネストされたグループの検索を無効化

ネストされたグループの検索を有効にするか無効にするかを指定します。デフォルトでは、このオプションは無効になっています。Active Directoryを使用する場合は、ネストされたグループのサポートを無効にすることで認証を高速化できます。

- セキュアな接続を使用

  認証サーバとの通信に使用される認証サービスを指定します。

◦ **OpenLDAP**

- バインド識別名

  認証サーバでリモート ユーザを検出する際にベース識別名とともに使用されるバインド識別名を指定します。

- バインド パスワード

  認証サーバにアクセスするためのパスワードを指定します。

- ベース識別名

  認証サーバーにおけるリモートユーザーの場所を指定します。例えば、認証サーバーのドメイン名が ou@domain.com の場合、ベース識別名は **cn=ou,dc=domain,dc=com** です。

- セキュアな接続を使用

  LDAP認証サーバとの通信に使用されるセキュアなLDAPを指定します。

◦ その他

- バインド識別名

  設定した認証サーバでリモート ユーザを検出する際にベース識別名とともに使用されるバインド識別名を指定します。

- バインド パスワード

  認証サーバにアクセスするためのパスワードを指定します。

- ベース識別名

  認証サーバーにおけるリモートユーザーの場所を指定します。例えば、認証サーバーのドメイン名が ou@domain.com の場合、ベース識別名は **cn=ou,dc=domain,dc=com** です。

- プロトコル バージョン

  認証サーバでサポートされるLightweight Directory Access Protocol（LDAP）のバージョンを指定します。プロトコル バージョンを自動検出するか、またはバージョン2か3に設定するかを指定できます。

- ユーザ名属性

  管理サーバによって認証されるユーザ ログイン名を含む認証サーバ内の属性の名前を指定します。

- グループ メンバーシップ属性

  ユーザの認証サーバで指定されている属性と値に基づいて管理サーバのグループ メンバーシップをリモート ユーザに割り当てる値を指定します。

- UGID

  リモート ユーザがGroupOfUniqueNamesオブジェクトのメンバーとして認証サーバに含まれている場合は、このオプションを使用して、GroupOfUniqueNamesオブジェクトで指定されている属性を基に管理サーバのグループ メンバーシップをリモート ユーザに割り当てることができます。

- ネストされたグループの検索を無効化

  ネストされたグループの検索を有効にするか無効にするかを指定します。デフォルトでは、このオプションは無効になっています。Active Directoryを使用する場合は、ネストされたグループのサポートを無効にすることで認証を高速化できます。

- メンバー

  認証サーバがグループの個々のメンバーに関する情報を格納するために使用する属性の名前を指定します。

- ユーザ オブジェクト クラス

  リモート認証サーバ内のユーザのオブジェクト クラスを指定します。

- グループ オブジェクト クラス

  リモート認証サーバ内のすべてのグループのオブジェクト クラスを指定します。

  > *Member*、*User Object Class*、および_Group Object Class_属性に入力する値は、Active Directory、OpenLDAP、およびLDAP構成で追加した値と同じである必要があります。そうしないと、認証が失敗する可能性があります。

- セキュアな接続を使用

  認証サーバとの通信に使用される認証サービスを指定します。

  > 認証サービスを変更する場合は、既存の認証サーバをすべて削除してから新しい認証サーバを追加するようにしてください。

[認証サーバ]領域

[認証サーバ]領域には、管理サーバがリモート ユーザの検出と認証を行うために通信する認証サーバが表示されます。リモートのユーザまたはグループのクレデンシャルは、認証サーバで管理されます。

- コマンドボタン

  認証サーバの追加、編集、削除を行うことができます。

  - 追加

    認証サーバを追加できます。

追加する認証サーバがハイアベイラビリティ 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。

- Edit

  選択した認証サーバの設定を編集できます。

- 削除

  選択した認証サーバを削除します。

- 名前または**IP**アドレス

  管理サーバでユーザの認証に使用される認証サーバのホスト名またはIPアドレスが表示されます。

- ポート

  認証サーバのポート番号が表示されます。

- 認証テスト

  このボタンでは、リモートのユーザまたはグループを認証することで認証サーバの設定を検証します。

  テストの際にユーザ名のみを指定すると、管理サーバは認証サーバでリモート ユーザを検索しますが、ユーザの認証は行いません。ユーザ名とパスワードを指定すると、管理サーバはリモート ユーザの検索と認証を行います。

  リモート認証が無効になっている場合は、認証をテストできません。

セキュリティ証明書を管理する

Active IQ Unified Manager でHTTPSセキュリティ証明書を表示する

HTTPS証明書の詳細をブラウザで取得した証明書と比較して、Unified Managerに対するブラウザの暗号化された接続が妨害されていないことを確認できます。

開始する前に

オペレータ、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。

証明書を表示すると、再生成された証明書の内容を検証したり、Unified Managerへのアクセスに使用できるSubject Alt Name（SAN）を確認したりできます。

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。

   HTTPS証明書がページの上部に表示されます。

セキュリティ証明書について、[HTTPS 証明書]ページの情報よりも詳しい情報を表示する必要がある場合は、ブラウザで接続証明書を表示します。

Active IQ Unified Manager で HTTPS 証明書署名要求をダウンロードする

認証局にファイルを送信して署名を求めるために、現在のHTTPSセキュリティ証明書の証明書署名要求をダウンロードできます。CA署名証明書は、中間者攻撃を阻止するのに役立ち、自己署名証明書よりも強力なセキュリティ保護を実現します。

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。

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証明書署名要求をダウンロード」をクリックしてください。
3. `<hostname>.csr`ファイルを保存します。

認証局にファイルを送信して署名を求め、署名済み証明書をインストールできます。

CA署名付きHTTPS証明書をActive IQ Unified Managerにインストールする

認証局から署名を受けて返されたセキュリティ証明書を、アップロードしてインストールすることができます。アップロードしてインストールするファイルは、既存の自己署名証明書の署名済みバージョンである必要があります。CA署名証明書は、中間者攻撃の阻止に役立ち、自己署名証明書よりも強力なセキュリティ保護を実現します。

*What .始める前に

次の操作を完了しておきます。

- 証明書署名要求ファイルをダウンロードし、認証局の署名を受けます。
- 証明書チェーンをPEM形式で保存します。
- すべての証明書（Unified Managerサーバ証明書からルート署名証明書まで。存在する中間証明書もすべて含む）をチェーンに組み込みます。

アプリケーション管理者のロールが必要です。

CSRを作成した証明書の有効期間が397日より長い場合、CAは証明書に署名して返信する前に有効期間を397日に短縮します。

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証明書のインストール」をクリックします。
3. 表示されたダイアログボックスで、「ファイルを選択...」をクリックして、アップロードするファイルを選択します。
4. ファイルを選択し、*インストール*をクリックしてファイルをインストールしてください。

   詳細については、"外部ツールを使用して生成されたHTTPS証明書のインストール"を参照してください。

証明書チェーンの例

証明書チェーン ファイルの内容の例を次に示します。

```
-----BEGIN CERTIFICATE-----
<*Server certificate*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Intermediate certificate \#1 (if present)*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Intermediate certificate \#2 (if present)*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Root signing certificate*>
-----END CERTIFICATE-----
```

Active IQ Unified Manager で外部ツールを使用して生成された HTTPS 証明書について

自己署名またはCA署名の証明書に加え、OpenSSL、BoringSSL、LetsEncryptなどの外部ツールを使用して生成された証明書をインストールできます。

これらの証明書は外部で生成された公開鍵と秘密鍵のペアであるため、証明書チェーンとともに秘密鍵も読み込む必要があります。使用可能な鍵ペアアルゴリズムは「RSA」と「EC」です。「HTTPS証明書のインストール」オプションは、「HTTPS証明書」ページの「一般」セクションにあります。アップロードするファイルは、以下の入力形式である必要があります。

1. Active IQ Unified Managerホストに属するサーバの秘密鍵
2. 秘密鍵と一致するサーバの証明書
3. 上記の証明書への署名に使用された、ルートまでのCAの証明書

ECキー ペアを含む証明書のロード形式

許可されている曲線は「prime256v1」と「secp384r1」です。外部で生成されたECペアを含む証明書のサンプル：

```
 -----BEGIN EC PRIVATE KEY-----
<EC private key of Server>
-----END EC PRIVATE KEY-----
```

```
 -----BEGIN CERTIFICATE-----
 <Server certificate>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
```

```
 <Intermediate certificate #1 (if present)>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Intermediate certificate #2 (if present)>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Root signing certificate>
 -----END CERTIFICATE-----
```

RSAキー ペアを含む証明書のロード形式

ホスト証明書に属する RSA 鍵ペアに許可される鍵サイズは 2048、3072、および 4096 です。外部で生成された **RSA** 鍵ペア を持つ証明書：

```
-----BEGIN RSA PRIVATE KEY-----
 <RSA private key of Server>
 -----END RSA PRIVATE KEY-----
 -----BEGIN CERTIFICATE-----
 <Server certificate>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Intermediate certificate #1 (if present)>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Intermediate certificate #2 (if present)>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Root signing certificate>
 -----END CERTIFICATE-----
```

証明書をアップロードしたら、Active IQ Unified Managerインスタンスを再起動して変更を反映する必要があります。

外部で生成された証明書のアップロード チェック

外部ツールを使用して生成された証明書をアップロードすると、システムでいくつかのチェックが実行されます。チェックに1つでも失敗すると、証明書は拒否されます。また、製品内のCSRから生成された証明書、および外部ツールを使用して生成された証明書の検証も実施されます。

- 入力で指定された秘密鍵が入力で指定されたホスト証明書と照合して検証されます。
- ホスト証明書の共通名（CN）がホストのFQDNと照合してチェックされます。
- ホスト証明書の共通名（CN）を空または空白にしたり、ローカル ホストに設定したりすることはできません。
- 証明書の有効期間の開始日を将来の日付にしたり、有効期限を過去の日付にしたりすることはできません。

- 中間CAまたはCAが存在する場合、証明書有効期間の開始日を将来の日付にしたり、有効期限を過去の日付にしたりすることはできません。

入力で指定する秘密鍵は暗号化しないでください。暗号化された秘密鍵はシステムで拒否されます。

例1

```
----BEGIN ENCRYPTED PRIVATE KEY-----
<Encrypted private key>
-----END ENCRYPTED PRIVATE KEY-----
```

例2

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
<content here>
-----END RSA PRIVATE KEY-----
```

例3

```
-----BEGIN EC PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
<content here>
-----END EC PRIVATE KEY-----
```

証明書のインストールが失敗した場合は、ナレッジベース（KB）の記事を参照してください：https://kb.netapp.com/mgmt/AIQUM/AIQUM_fails_to_install_externally_generated_certificate["ActiveIQ Unified Manager が外部で生成された証明書のインストールに失敗する"^]

証明書管理のページの説明

Active IQ Unified Manager の HTTPS 証明書ページについて

[HTTPS 証明書]ページでは、現在のセキュリティ証明書の表示、証明書署名要求のダウンロード、新しい自己署名HTTPS証明書の生成、新しいHTTPS証明書のインストールを行うことができます。

新しい自己署名HTTPS証明書を生成していない場合は、インストール時に生成された証明書がこのページに表示されます。

コマンド ボタン

各コマンド ボタンを使用して次の処理を実行できます。

- **HTTPS**証明書署名要求をダウンロード

  現在インストールされているHTTPS証明書の認証要求をダウンロードします。署名のために認証局に提供できるように、ブラウザで<hostname>.csrファイルを保存するよう求められます。

- **HTTPS**証明書をインストールする

  認証局の署名を受けて返されたセキュリティ証明書を、アップロードしてインストールすることができます。新しい証明書は、管理サーバを再起動すると有効になります。

- **HTTPS**証明書を再生成する

  新しい自己署名HTTPS証明書を生成して現在のセキュリティ証明書と置き換えることができます。新しい証明書は、Unified Managerを再起動すると有効になります。

Active IQ Unified Manager の「**HTTPS**証明書の再生成」ダイアログボックス

[HTTPS 証明書の再生成]ダイアログ ボックスでは、セキュリティ情報をカスタマイズし、その情報を使用して新しいHTTPS証明書を生成することができます。

このページには現在の証明書の情報が表示されます。

「`Regenerate Using Current Certificate Attributes`」と「`Update the Current Certificate Attributes`」を選択すると、現在の情報を使用して証明書を再生成するか、新しい情報を使用して証明書を生成することができます。

- コモンネーム

  必須。保護する対象の完全修飾ドメイン名（FQDN）。

  Unified Managerの高可用性構成では、仮想IPアドレスを使用します。

- メール

  任意。組織の連絡先のEメール アドレス。証明書の管理者またはIT部門のEメール アドレスが一般的です。

- 会社

  任意。通常は会社の法人名。

- 部門

  任意。社内の部署の名前。

- 市区町村

  任意。会社の所在地の市区町村。

- 状態

  任意。会社の所在地の都道府県。

- 国

  任意。会社の所在地の国。通常はISOの2文字の国コードです。

- 別名

  必須。このサーバにアクセスするために既存のローカルホストやその他のネットワーク アドレスに加えて使用できる、プライマリ ドメイン以外の追加の名前。別名はそれぞれカンマで区切ります。

  証明書の「代替名」フィールドからローカル識別情報を削除する場合は、「ローカル識別情報を除外する（例：`localhost`）」チェックボックスを選択してください。このチェックボックスを選択すると、代替名フィールドにはフィールドに入力した内容のみが使用されます。空欄のままにした場合、作成される証明書には「代替名」フィールドは一切含まれません。

- 鍵サイズ（鍵アルゴリズム：**RSA**）

  鍵アルゴリズムはRSAに設定されています。鍵のサイズ：2048、3072、4096ビットのいずれかを選択できます。デフォルトの鍵サイズは2048ビットに設定されています。

- 有効期間

  デフォルトの有効期間は397日です。以前のバージョンからアップグレードした場合は、以前の証明書の有効期間がそのまま表示される可能性があります。

詳細については、"HTTPS証明書の生成"を参照してください。

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。