Active IQ Unified Managerを構成する

Active IQ Unified Manager

NetApp
October 15, 2025

目次

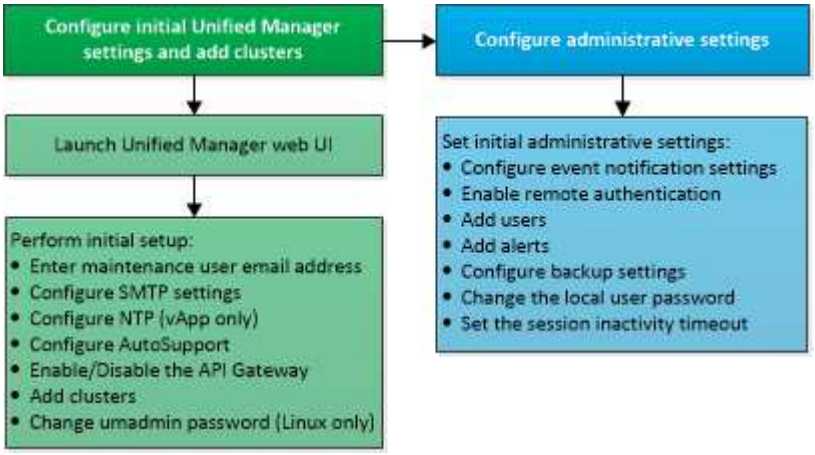
Active IQ Unified Managerを構成する

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。

このマニュアルで説明されている手順の一部は、Unified Manager インスタンスの初期セットアップを完了するために必要です。それ以外の手順は新しいインスタンスをセットアップする際に推奨される設定か、またはONTAPの定期的な監視を開始する前に把握しておくことが推奨される設定です。

設定手順の概要

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



Unified Manager 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。

Unified Manager Web UIの初期セットアップを実行します

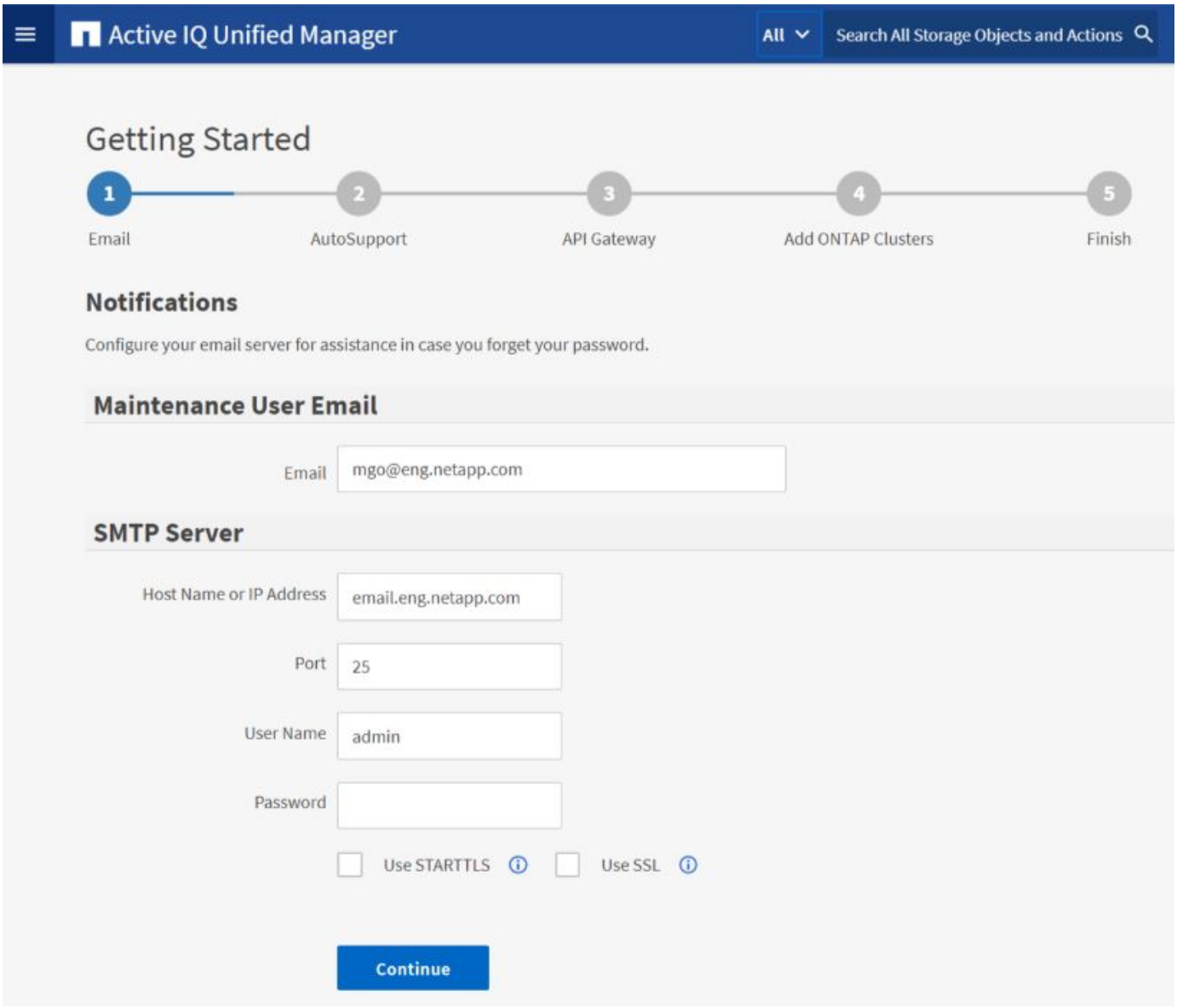
Unified Managerを使用するには、NTPサーバ、メンテナンス ユーザのEメール アドレス、SMTPサーバのホストなどを最初に設定し、ONTAPクラスタを追加する必要があります。

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の初期セットアップ ページで、メンテナンス ユーザのEメール アドレス、SMTPサーバのホスト名とその他のSMTPオプション、およびNTPサーバ（VMware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は、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、証明書を受け入れて、Web UIの初期セットアップを続行します。

2. AutoSupportページで「同意して続行」をクリックし、Unified Manager から NetAppActive IQ へのAutoSupportメッセージの送信を有効にします。

   AutoSupportコンテンツを送信するためにインターネット アクセスを提供するプロキシを指定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 全般 > * AutoSupport* オプションを使

用します。

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」文字列から個人用の文字列に変更します。
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することができます。 APIの詳細については、以下を参照してください。"Active IQ Unified Manager REST APIでの作業の開始" 。
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。管理する予定のクラスターごとに、ユーザー名とパスワードの資格情報とともに、ホスト名またはクラスター管理 IP アドレス (IPv4 または IPv6) が必要です。ユーザーには「admin」ロールが必要です。

   この手順はオプションです。後で Web UI の ストレージ管理 > クラスター設定 からクラスターを追加できます。
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。

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クラスター、 ONTAP Select、 Cloud Volumes ONTAP をサポートします。
  - 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*、*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 が所有します。Unified Managerの新規インストール時にデフォルトの自己署名SSL（HTTPS）証明書が生成されます。セキュリティを強化するために、この証明書をCA署名証明書にアップグレードすることを推奨します。サーバ証明書の有効期限が切れた場合は、証明書を再生成する必要があります。その後Unified Managerを再起動すると、新しい証明書がサービスに組み込まれます。 SSL証明書の再生成の詳細については、以下を参照してください。"HTTPSセキュリティ証明書の生成" 。

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

  相互 **TLS** 通信用の証明書: Unified Manager とONTAP間の相互 TLS 通信中に使用されます。証明書ベースの認証は、クラスタのONTAPバージョンに基づいて有効になります。ONTAP 9.5よりも前のバージョンを実行しているクラスタでは、証明書ベースの認証は有効ではありません。

  古いバージョンのUnified Managerを更新しても、クラスタの証明書ベースの認証は自動では有効になりません。ただし、クラスタの詳細を変更して保存すれば、認証を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、証明書を再生成して新しい証明書を組み込む必要があります。証明書の表示と再生成の詳細については、以下を参照してください。"クラスタの編集" 。

  - 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のCLIを使用してクラスタを追加することもできますが、証明書ベースの認証はデフォルトでは有効になりません。Unified ManagerのCLIを使用してクラスタを追加した場合、クラスタを編集するにはUnified Manager UIを使用する必要があります。見ることができます"サポートされるUnified ManagerのCLIコマンド"Unified Manager CLI を使用してクラスターを追加します。
  - クラスタで証明書ベースの認証が有効になっている場合に、あるサーバからUnified Managerのバックアップを作成し、ホスト名またはIPアドレスが異なる別のUnified Managerサーバにリストアすると、クラスタの監視に失敗することがあります。このエラーを回避するには、クラスタの詳細を編集して保存します。クラスタの詳細編集の詳細については、以下を参照してください。"クラスタの編集" 。

  + クラスタ証明書: この証明書はONTAPが所有します。有効期限が切れた証明書でUnified Managerにクラスタを追加することはできません。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。証明書生成の詳細については、ナレッジベース（KB）の記事を参照してください。 "System Managerユーザーインターフェイスで ONTAP自己署名証明書を更新する方法" 。

- 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 > クラスター セットアップ 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*をクリックします。
5. [ホストの承認] ダイアログ ボックスで、[証明書の表示] をクリックして、クラスター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"

アラート通知を送信するようにUnified Managerを構成する

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にする"。

   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. "ユーザーを追加する"。

   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. "アラートを追加する"。

   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。

イベント通知を設定

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`」フィールドに電子メール アドレスが表示されます。何らかの理由でEメールを配信できない場合の不達メールの送信先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、[全般] > [通知] 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。

   注記:

   - 送信元アドレスに「ActiveIQUnifiedManager@localhost.com」というアドレスが事前に入力されている場合は、すべての電子メール通知が正常に配信されるように、実際に機能する電子メール アドレスに変更する必要があります。
   - 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は、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、証明書を受け入れて通知設定を保存します。

   証明書の詳細を表示するには、[証明書の詳細を表示] ボタンをクリックしてください。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] ボックスのチェックを外し、通知設定を保存し、[**STARTTLS** を使用する] または [**SSL** を使用する] ボックスを再度チェックして新しい証明書を表示します。

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…*のボックスをチェックします。
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。

認証タイプの場合...	次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）
オープンLDAP	• バインド識別名（適切なLDAP表記を使用） • パスワードをバインドする • 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: 認証サーバーを追加し、認証をテストします。
5. *保存*をクリックします。

リモート認証から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の検索を無効にする*のボックスをチェックします。

3. *保存*をクリックします。

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。

選択した場合...	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。 たとえば、認証サーバーのドメイン名が ou@domain.com の場合、基本識別名は **cn=ou,dc=domain,dc=com** になります。
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。 たとえば、認証サーバーのドメイン名が ou@domain.com の場合、基本識別名は **cn=ou,dc=domain,dc=com** になります。

選択した場合...	操作
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。 たとえば、認証サーバーのドメイン名が ou@domain.com の場合、基本識別名は **cn=ou,dc=domain,dc=com** になります。 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。

認証サーバを追加する

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ます。 b. 認証サーバー領域で、[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 は認証サーバと通信し、証明書を表示します。Unified Managerでは、セキュアな通信にはポート636、セキュアでない通信にはポート389がデフォルトのポートとして使用されます。
無効にする	a. *安全な接続を使用する*オプションをオフにします。 b. 認証サーバー領域で、[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。

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. [ユーザーのテスト] 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。

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. *リソース*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。

   *名前に含まれる*フィールドにテキスト文字列を指定してフィルターを設定し、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、フィルタ ルールに一致するリソースのみが利用可能なリソースのリストに表示されます。テキスト文字列の指定では、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. *イベント*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`」が含まれるすべてのボリュームが含まれ、名前に「`xyz`」が含まれるすべてのボリュームが除外されます
- 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」と「`Test`」スクリプトが含まれており、ユーザーに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*と入力します。
2. *リソース*をクリックし、含めるタブでドロップダウンリストから*ボリューム*を選択します。
   a. 名前に「`abc`」が含まれるボリュームを表示するには、「名前を含む」フィールドに **abc** と入力します。
   b. を選択**<<All Volumes whose name contains 'abc'>>** を [使用可能なリソース] 領域から選択し、[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*フィールドに*xyz*と入力して、*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警告] 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、[テスト スクリプト] を選択します。
8. *保存*をクリックします。

ローカル ユーザのパスワードを変更

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。

リモート ユーザとメンテナンス ユーザのパスワードについては、この手順では変更できません。リモート ユーザのパスワードを変更するには、パスワードの管理者に連絡してください。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" 。

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、*パスワードの変更*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。

アクティブでないセッションのタイムアウトを設定

Unified Manager の非アクティブ タイムアウト値を指定して、一定時間非アクティブになった後にセッションが自動的に終了されるようにすることができます。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、[全般] > [機能の設定*] をクリックします。
2. *機能設定*ページで、次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、「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。

CLI経由でセッションタイムアウトを設定する

CLI を使用して Unified Manager の最大セッション タイムアウト値を設定すると、一定時間後にセッションが自動的に終了されます。デフォルトでは、セッション タイムアウトは最大値の 4,320 分 (72 時間) に設定されています。つまり、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、セッションは 72 時間後に自動的に終了します。

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

Unified Managerのホスト名を変更する

必要に応じて、Unified Managerをインストールしたシステム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、Unified Managerサーバを識別しやすくなります。

ホスト名を変更する手順は、Unified ManagerをVMware ESXiサーバ、Red Hat Linux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。

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 が適切に構成されていない場合、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。

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、キーのサイズと有効期間を定義できます。を使用する場合`Reset Server Certificate`メンテナンス コンソールからオプションを選択すると、397 日間有効な新しいHTTPS 証明書が作成されます。また、RSAキーのサイズは2048ビットに設定されます。

手順

1. 左側のナビゲーション ペインで、全般 > **HTTPS** 証明書 をクリックします。
2. *HTTPS 証明書の再生成*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。

状況	操作
別の値で証明書を生成する	*現在の証明書属性を更新する*オプションをクリックします。 [共通名]フィールドと[別名]フィールドについては、新しい値を入力しなければ既存の証明書の値が使用されます。「Common Name」はホストの FQDN に設定する必要があります。それ以外のフィールドの値は必須ではありませんが、必要に応じて[Eメール]、[会社]、[部門]、[市町村]、[都道府県]、[国]などの値を入力し、証明書に表示することができます。利用可能なキー サイズ (キー 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次のとおりです。 2048 、 3072`そして `4096。 • 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。

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。

ゲストの再起動 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. システム構成 > *仮想マシンの再起動*を選択します。

Linux システムで Unified Manager のホスト名を変更する

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を使用してホスト名を変更する `hostnamectl`指示：

   ```
   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
```

ポリシーベースのストレージ管理を有効または無効にする

Unified Manager 9.7 以降では、 ONTAPクラスタ上でストレージ 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、QoS ポリシーをアタッチする機能に似ていますが、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。

新しいコンテンツ	**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
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 から利用できます

新しいコンテンツ	**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、[全般] > [機能の設定*] をクリックします。
2. *機能設定*ページで、次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

商標に関する情報