# Active IQ Unified Manager を設定しています

Active IQ Unified Manager 9.8

NetApp
January 31, 2025

# 目次

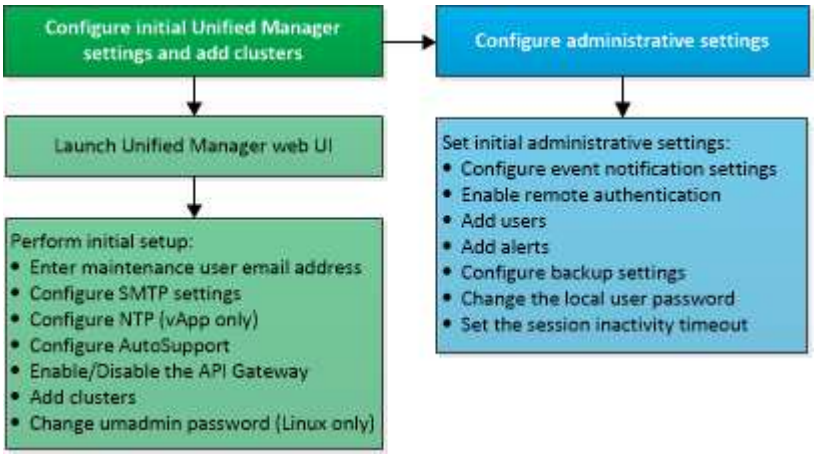
# Active IQ Unified Manager を設定しています

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。その後、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することができます。

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セットアップを完了するための必須の手順です。その他の手順は、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 システム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

以下は、 Unified Manager を使用する前に必要な設定作業のワークフローです。




## Unified Manager Web UI にアクセスします

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。

### 作業を開始する前に

- 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示す警告がブラウザ画面に表示されることがあります。リスクを承認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、https：//です/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。

# Unified Manager Web UI の初期セットアップを実行する

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。

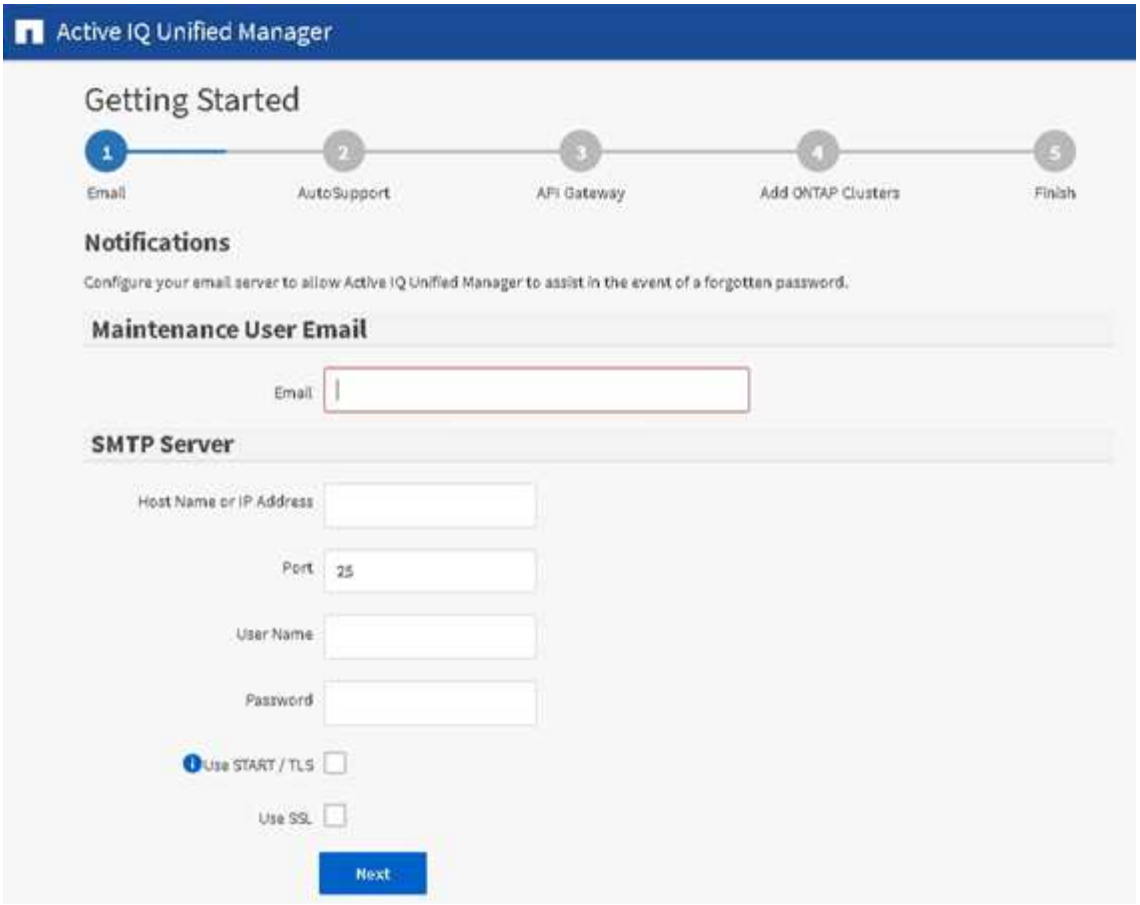
### 作業を開始する前に

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

### このタスクについて

Active IQ Unified Manager の Getting Started ページは、最初に Web UI にアクセスしたときにのみ表示されます。次のページは、 VMware 環境の場合のものです。




これらのオプションをあとから変更する場合は、 Unified Manager の左側のナビゲーションペインで一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。[* Continue （続行） ] をクリックします。
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。

   AutoSupport コンテンツの送信用に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する必要がある場合や、 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ます。

3. Red HatおよびCentOSのシステムの場合、umadminユーザのパスワードをデフォルトの「admin」から独自のパスワードに変更できます。
4. APIゲートウェイのセットアップ*ページで、ONTAP REST APIを使用して監視するONTAP クラスタをUnified Managerで管理できるようにするAPIゲートウェイ機能を使用するかどうかを選択します。[* Continue （続行） ] をクリックします。

   この設定は、 Web UI の * General * > * Feature Settings * > * API Gateway * で後から有効または無効にできます。APIの詳細については、を参照してください "Active IQ Unified Manager REST APIの使用を開始する"。

5. Unified Manager で管理するクラスタを追加し、 * Next * をクリックします。管理するクラスタごとに、ホスト名またはクラスタ管理 IP アドレス（ IPv4 または IPv6 ）、ユーザ名およびパスワードクレデンシャルが必要です。ユーザには「 admin 」ロールが必要です。

   この手順はオプションです。クラスタは、 Web UI の * Storage Management * > * Cluster Setup * からあとから追加できます。

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

### 結果

Getting Started（はじめに）ページが閉じ、Unified Manager Dashboard（Unified Managerダッシュボード）ページが表示されます。

# クラスタを追加する

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、クラスタの健常性、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できるようにすることができます。

### 作業を開始する前に

- 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。
  - 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 がクラスタへの接続に使用する 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 である必要があります。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* 、 *_ssh* 、および _http_に 設定された _admin_role 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 ）

    NAT / ファイアウォールの背後にあるクラスタは、 Unified Manager の NAT IP アドレスを使用して追加できます。接続された Workflow Automation または SnapProtect システムも NAT / ファイアウォールの背後に配置する必要があり、 SnapProtect API 呼び出しでは NAT IP アドレスを使用してクラスタを識別する必要があります。

- 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。

## このタスクについて

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、クラスタを正しく設定する必要があります。

クラスタに 2 つ目のクラスタ管理 LIF を設定し、 Unified Manager の各インスタンスを別々の LIF を介して接続すれば、 1 つのクラスタを Unified Manager の 2 つのインスタンスで監視できます。

## 手順

1. 左側のナビゲーションペインで、 * Storage Management * > * Cluster Setup * をクリックします。
2. [クラスタセットアップ]ページで、[*追加]をクリックします。
3. Add Cluster *（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. [Submit （送信） ] をクリックします。
5. [* Authorize Host *（ホストの認証 * ） ] ダイアログボックスで、 [* View Certificate *（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。

   Unified Manager では、クラスタが最初に追加されたときにのみ証明書がチェックされます。Unified Manager では、 ONTAP に対する API 呼び出しごとには証明書がチェックされません。

   証明書の期限が切れている新しいクラスタは追加できません。まずSSL証明書を更新してから、クラスタを追加する必要があります。

## 結果

新しいクラスタのオブジェクトがすべて検出されると（約15分後）、Unified Managerが過去15日間の履歴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の完了後、デフォルトではクラスタのリアルタイムのパフォーマンスデータが 5 分ごとに収集されます。

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チャートに表示されません。

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。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。

# Unified Manager でアラート通知を送信するための設定

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。

## 作業を開始する前に

アプリケーション管理者のロールが必要です。

## このタスクについて

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環境を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します"

   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. 認証サーバを追加します

   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. "ユーザを追加します"

   複数のタイプのローカルユーザまたは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割り当てます。

5. "アラートを追加します"

   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しています

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 サーバを設定したり、さまざまな通知メカニズムを設定したりできます。たとえば、ア

## ラート通知を E メールや SNMP トラップとして送信できます。

作業を開始する前に

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

  メール・アドレスは ' 送信されたアラート通知の送信元フィールドに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は、この E メールアドレスが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、およびサーバにアクセスするためのユーザ名とパスワード
- 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

  複数のトラップ送信先を指定するには、各ホストをカンマで区切ります。この場合、バージョンやアウトバウンドトラップポートなど、他の SNMP 設定はすべてリスト内のすべてのホストで同じでなければなりません。

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、 * 一般 * > * 通知 * をクリックします。
2. [*Notifications]ページで、適切な設定を構成し、[*Save]をクリックします。
   - 注：*
     - 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、実際の作業用 E メールアドレスに変更して、すべての E メール通知が正常に配信されるようにしてください。
     - 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。

## リモート認証の有効化

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。

作業を開始する前に

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。

このタスクについて

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と、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、 * 一般 * > * リモート認証 * をクリックします。
2. [Enable remote authentication…*] チェックボックスをオンにします。
3. [**Authentication Service**]フィールドで、サービスのタイプを選択し、認証サービスを設定します。

| 認証タイプ | 入力する情報 |
| --- | --- |
| Active Directory | • 認証サーバの管理者名。次のいずれかの形式で指定します。<br>◦ `domainname\username`<br>◦ `username@domainname`<br>◦ `Bind Distinguished Name` （適切なLDAP表記を使用）<br>• 管理者パスワード<br>• ベース識別名（適切な LDAP 表記を使用） |
| LDAP を開きます | • バインド識別名（適切な LDAP 表記を使用）<br>• バインドパスワード<br>• ベース識別名 |

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

認証サーバに Secure Connection オプションを使用する場合、 Unified Manager は Secure Sockets Layer （ SSL ）プロトコルを使用して認証サーバと通信します。

4. 認証サーバを追加し、認証をテストします。
5. [ 保存（ Save ） ] をクリックします。

## リモート認証でのネストされたグループの無効化

## 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。

作業を開始する前に

- 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

このタスクについて

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、 * 一般 * > * 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 *] チェックボックスをオンにします。
3. [ 保存（ Save ） ] をクリックします。

## 認証サーバを追加しています

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。

作業を開始する前に

- 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。

このタスクについて

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、いずれかの認証サーバにアクセスできない場合でも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、 * 一般 * > * リモート認証 * をクリックします。
2. [ セキュアな接続を使用する *] オプションを有効または無効にします。

| 状況 | 操作 |
| --- | --- |
| 有効にします | a. [ セキュアな接続を使用（ Use Secure Connection * ） ] オプションを選択します。<br>b. [Authentication Servers] 領域で、 [**Add**] をクリックします。<br>c. Add Authentication Server ダイアログボックスで、サーバの認証名または IP アドレス（ IPv4 または IPv6 ）を入力します。<br>d. [ ホストの認証 ] ダイアログボックスで、 [ 証明書の表示 ] をクリックします。<br>e. [ 証明書の表示 ] ダイアログボックスで、証明書の情報を確認し、 [ 閉じる *] をクリックします。<br>f. [ ホストの許可 ] ダイアログボックスで、 [ はい ] をクリックします。<br>ⓘ Secure Connection authentication * オプションを有効にすると、 Unified Manager は認証サーバと通信して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。 |
| 無効にします | a. [ セキュアな接続を使用する *] オプションをオフにします。<br>b. [Authentication Servers] 領域で、 [**Add**] をクリックします。<br>c. [Add Authentication Server] 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 ）、およびポートの詳細を指定します。<br>d. [ 追加（ Add ） ] をクリックします。 |

追加した認証サーバが Servers 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でユーザを認証できることを確認します。

## 認証サーバの設定をテストする

認証サーバの設定を検証して、管理サーバが認証サーバと通信できるかどうかを確認できます。設定を検証するには、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、設定済みの設定を使用して認証します。

作業を開始する前に

- 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。
- 認証サーバから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。

このタスクについて

認証サービスが Active Directory に設定されている場合に、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、 * 一般 * > * リモート認証 * をクリックします。
2. ［ * 認証のテスト * ］ 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。

## ユーザを追加する

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表示したりできます。

作業を開始する前に

- アプリケーション管理者のロールが必要です。
- リモートのユーザまたは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。
- SAML 認証を設定して、グラフィカルインターフェイスにアクセスするユーザをアイデンティティプロバイダ（ IdP ）で認証する場合は、これらのユーザが「「 morte 」ユーザとして定義されていることを確認します。

  SAML 認証が有効になっている場合、「ローカル」または「メンテナンス」タイプのユーザーに UI へのアクセスは許可されません。

このタスクについて

Windows Active Directory からグループを追加した場合は、ネストされたサブグループが無効になっていないかぎり、すべての直接メンバーとネストされたサブグループは Unified Manager で認証できます。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、 * 一般 * > * ユーザー * 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、追加するユーザーのタイプを選択し、必要な情報を入力します。

   必要なユーザ情報を入力するときは、そのユーザに固有の 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（ Add ） ] をクリックします。

## アラートの追加

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。

作業を開始する前に

- イベント生成時に 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、 Scripts 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。

このタスクについて

アラートは、ここで説明するように、 Alert Setup ページからアラートを作成するだけでなく、イベントを受信した後に Event Details ページから直接作成できます。

手順

1. 左側のナビゲーションペインで、 * Storage Management * > * Alert Setup * をクリックします。
2. [* Alert Setup* ] ページで、 [* Add] 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、アラートの名前と概要を入力します。
4. [* リソース ] をクリックし、アラートに含めるリソースまたはアラートから除外するリソースを選択します。

   [ * 次を含む名前（ * Name Contains ） ] フィールドでテキスト文字列を指定してフィルタを設定し、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使用可能なリソースのリストに表示されます。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の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. [*Actions] をクリックし、通知するユーザを選択し、通知頻度を選択し、 SNMP トラップをトラップレシーバに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。

   ユーザに対して指定されている E メールアドレスを変更し、アラートを再び開いて編集しようとすると、変更した E メールアドレスが以前に選択したユーザにマッピングされていないため、名前フィールドは空白になります。また、選択したユーザの E メールアドレスを Users 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（ Save ） ] をクリックします。

アラートの追加例

この例は、次の要件を満たすアラートを作成する方法を示しています。

- 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を対象に含め、名前に「 xyz 」が含まれるすべてのボリュームを対象から除外する
- イベント：健全性に関するすべての重大なイベントを含みます
- アクション:「sample@domain.com」、「Test」スクリプトを含み、15分ごとにユーザーに通知される必要があります

[Add Alert] ダイアログボックスで、次の手順を実行します。

1. [名前]をクリックし、と入力します `HealthTest` [アラート名]フィールドに入力します。
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. 入力するコマンド `abc` 「* Name contains *」フィールドには、名前に「abc」が含まれるボリュームが表示されます。
   b. 「 * + 」を選択します[All Volumes whose name contains 'abc']+* を使用可能なリソース領域から選択したリソース領域に移動します。
   c. [除外する]をクリックし、と入力します `xyz` [名前に*が含まれています]フィールドで、[*追加]をクリックします。
3. [* イベント ] をクリックし、 [ イベントの重要度 ] フィールドから [ クリティカル *] を選択します。

4. [Matching Events] 領域から [*All Critical Events] を選択し、 [Selected Events] 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. 15 分ごとにユーザに通知するには、「 * 15 分ごとに通知する」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（ Save ） ] をクリックします。

# Unified Manager に自動的に追加される EMS イベント

次の ONTAP EMS イベントが Unified Manager に自動的に追加されます。これらのイベントは、 Unified Manager が監視しているいずれかのクラスタでトリガーされると生成されます。

ONTAP 9.5 以降のソフトウェアを実行しているクラスタの監視では、次の EMS イベントを使用できます。

| **Unified Manager** のイベント名 | **EMS** のイベント名 | 影響を受けるリソース | **Unified Manager** の重大度 |
|---|---|---|---|
| アグリゲートの再配置でクラウド階層へのアクセスが拒否されまし | arl.netra.ca.check.failed | アグリゲート | エラー |
| ストレージフェイルオーバー時にアグリゲートの再配置でクラウド階層へのアクセスが拒否されました | gb.netra.ca.check.failed | アグリゲート | エラー |
| FabricPool ミラーレプリケーションの再同期が完了しました | wafl.ca.resync.complete | クラスタ | エラー |
| FabricPool スペースがほぼフルです | fabricpool.Nearly .full | クラスタ | エラー |
| NVMF の猶予期間 - 開始されました | nvmf.graceperiod.start | クラスタ | 警告 |
| NVMF の猶予期間 - アクティブ | nvmf.graceperiod.active | クラスタ | 警告 |
| NVMF の猶予期間 - 終了 | nvmf.graceperiod.expired | クラスタ | 警告 |

| **Unified Manager** のイベント名 | **EMS** のイベント名 | 影響を受けるリソース | **Unified Manager** の重大度 |
| --- | --- | --- | --- |
| LUN が破棄されました | lun.destroy | LUN | 情報 |
| Cloud AWS メタデータ接続エラー | Cloud.AWS- メタデータの接続に失敗しました | ノード | エラー |
| Cloud AWS IAM クレデンシャルが期限切れです | Cloud.AWs.iamCredsExpired | ノード | エラー |
| Cloud AWS IAM クレデンシャルが無効です | Cloud.AWs.iamCredsInvalid | ノード | エラー |
| Cloud AWS IAM クレデンシャルが見つからない | Cloud.AWs.iamCredsNotFound | ノード | エラー |
| Cloud AWS IAM クレデンシャルが初期化されていない | Cloud.AWS.iamNotInitialized | ノード | 情報 |
| Cloud AWS IAM ロールが無効です | Cloud.AWs.iamRoleInvalid | ノード | エラー |
| Cloud AWS IAM ロールが見つからない | Cloud.AWs.iamRoleNotFound | ノード | エラー |
| クラウド階層のホスト解決不可 | objstor.host.unresolvable | ノード | エラー |
| クラウド階層のクラスタ間 LIF が停止しています | objstore.interclusterlifDown | ノード | エラー |
| 要求とクラウド階層シグネチャの不一致 | OSC.signignatureMismatch | ノード | エラー |
| NFSv4 プールの 1 つを使い果たしました | Nblade.nfsV4PoolExhaust | ノード | 重要 |
| QoS 監視メモリの最大化 | QoS 。monitor.memory.maxed | ノード | エラー |
| QoS 監視メモリの縮小 | QoS .monitor.memory.abated | ノード | 情報 |

| **Unified Manager** のイベント名 | **EMS** のイベント名 | 影響を受けるリソース | **Unified Manager** の重大度 |
| --- | --- | --- | --- |
| NVMe ネームスペースを破棄します | NVMeNS.destroy | ネームスペース | 情報 |
| NVMeNS Online | NVMe ネームスペースオフライン | ネームスペース | 情報 |
| NVMeNS はオフラインです | NVMe ネームスペースオンライン | ネームスペース | 情報 |
| NVMe ネームスペーススペーススペース不足です | NVMe ネームスペース不足です。スペース不足です | ネームスペース | 警告 |
| 同期レプリケーションが同期されていません | sms.status.out.out.out.sync | SnapMirror 関係 | 警告 |
| 同期レプリケーションがリストアされました | sms.status.in.sync | SnapMirror 関係 | 情報 |
| 同期レプリケーションの自動再同期に失敗しました | sms.resync.attempt 。失敗しました | SnapMirror 関係 | エラー |
| 多数の CIFS 接続 | Nblade.cifsManyAths | SVM | エラー |
| 最大 CIFS 接続数を超えました | Nblade.cifsMaxOpenSameFile | SVM | エラー |
| ユーザあたりの最大 CIFS 接続数を超えました | Nblade.cifsMaxSessPerUsrConn | SVM | エラー |
| CIFS NetBIOS 名が競合しています | Nblade.cifsNbNameConflict になっています | SVM | エラー |
| 存在しない CIFS 共有に対して試行します | Nblade.cifsNoPrivShare | SVM | 重要 |
| CIFS シャドウコピー処理に失敗しました | cifs.shadowcopy.failure | SVM | エラー |
| AV サーバがウィルスを検出しました | Nblad. vscanVirusDetected | SVM | エラー |

| **Unified Manager** のイベント名 | **EMS** のイベント名 | 影響を受けるリソース | **Unified Manager** の重大度 |
| --- | --- | --- | --- |
| ウィルススキャン用の AV サーバ接続がありません | Nbladen.vscanNoScannerConn | SVM | 重要 |
| AV サーバが登録されていません | Nbladet.vscanNoRegdScanner | SVM | エラー |
| 応答する AV サーバ接続がありません | Nbladet.vscanConnInactive | SVM | 情報 |
| AV サーバがビジーのため新しいスキャン要求の受け入れ不可 | Nbladet.vscanConnBackPressure です | SVM | エラー |
| 権限のないユーザが AV サーバへのアクセスを試みました | Nblad.vscanBadUserPrivAccess | SVM | エラー |
| FlexGroup コンスティチュエントのスペースに問題あり | flexgroup コンスティチュエント .have .spac確保 問題 | ボリューム | エラー |
| FlexGroup コンスティチュエントのスペースステータスはすべて正常です | flexgroup コンスティチュエント。 spac確保 。 status.all.ok | ボリューム | 情報 |
| FlexGroup 構成要素の inode に問題があります | flexgroup.constituents.have.inodes.issues | ボリューム | エラー |
| FlexGroup コンスティチュエントの inode ステータスはすべて正常です | flexgroup.constituents.inodes.status.all.ok | ボリューム | 情報 |
| ボリューム論理スペースはほぼフルです | monitor.vol.nearFull.inc.sav | ボリューム | 警告 |
| ボリューム論理スペースはフルです | monitor.vol.full.inc.sav | ボリューム | エラー |
| ボリューム論理スペースは正常な状態です | monitor.vol.one.ok.inc.sav | ボリューム | 情報 |
| WAFL ボリュームのオートサイズが失敗しました | wafl.vol.autoSize.fail | ボリューム | エラー |

| Unified Manager のイベント名 | EMS のイベント名 | 影響を受けるリソース | Unified Manager の重大度 |
|---|---|---|---|
| WAFL ボリュームのオートサイズ完了 | wafl.vol.autoSize.done | ボリューム | 情報 |
| WAFL READDIR ファイル処理タイムアウト | wafl.readdir.expired | ボリューム | エラー |

# ONTAP EMS イベントに登録する

ONTAP ソフトウェアがインストールされているシステムで生成された Event Management System （ EMS ；イベント管理システム）イベントを受け取るように登録することができます。一部の EMS イベントは Unified Manager に自動的に報告されますが、それ以外の EMS イベントは登録している場合にのみ報告されます。

## 作業を開始する前に

Unified Manager にすでに自動的に追加されている EMS イベントには登録しないでください。同じ問題のイベントを 2 つ受信すると原因で混乱する可能性があります。

## このタスクについて

EMS イベントはいくつでも登録できます。登録したすべてのイベントが検証され、検証済みのイベントだけが Unified Manager で監視しているクラスタに適用されます。ONTAP 9 EMS イベントカタログ _ は、指定したバージョンの ONTAP 9 ソフトウェアのすべての EMS メッセージに関する詳細情報を提供します。該当するイベントの一覧については、 ONTAP 9 製品ドキュメントページで該当するバージョンの _EMS イベントカタログを参照してください。

"ONTAP 9 製品ライブラリ"

登録した ONTAP EMS イベントにアラートを設定したり、それらのイベントに対して実行するカスタムスクリプトを作成したりできます。

登録した ONTAP EMS イベントが届かない場合は、クラスタの DNS 設定が含まれている問題で、クラスタから Unified Manager サーバに到達できなくなっていることが考えられます。クラスタ管理者はこの問題を解決するために、クラスタの DNS 設定を修正してから Unified Manager を再起動する必要があります。これにより、保留中の EMS イベントが Unified Manager サーバにフラッシュされます。

## 手順

1. 左側のナビゲーションペインで、 * Storage Management * > * Event Setup * をクリックします。
2. [* Event Setup*]ページで、[* Subscribe to EMS events]ボタンをクリックします。
3. [*Subscribe to EMS events]ダイアログボックスに、登録するONTAP EMSイベントの名前を入力します。

   登録可能なEMSイベントの名前を確認するには、ONTAP クラスタシェルでを使用します `event route`

`show` コマンド（ONTAP 9より前）または `event catalog show` コマンド（ONTAP 9以降）。

"OnCommand Unified Manager / Active IQ Unified Manager でONTAP EMSイベントサブスクリプションを設定する方法"

4. [ 追加（ Add ） ] をクリックします。

   EMS イベントはサブスクライブされた EMS イベントのリストに追加されますが、該当する [To Cluster] 列には、追加した EMS イベントのステータスが「 Unknown 」と表示されます。

5. Save and Close * をクリックして、 EMS イベントサブスクリプションをクラスタに登録します。
6. もう一度 [* EMS イベントをサブスクライブ * ] をクリックします。

   追加した EMS イベントの [Applicable to Cluster] 列には、ステータス「 Yes 」が表示されます。

   ステータスが「はい」でない場合は、 ONTAP EMS イベント名のスペルを確認します。入力した名前に間違いがある場合は、そのイベントを削除して追加し直す必要があります。

### 完了後

ONTAP の EMS イベントが発生すると、イベントが Events ページに表示されます。イベントを選択すると、EMS イベントに関する詳細をイベントの詳細ページで確認できます。イベントの処理を管理したり、イベントのアラートを作成したりすることもできます。

# SAML 認証の設定を管理する

リモート認証の設定が完了したら、 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にアクセスするユーザには影響しません。

### アイデンティティプロバイダの要件

すべてのリモートユーザについてアイデンティティプロバイダ（ IdP ）を使用して SAML 認証を実行するように Unified Manager で設定するときは、 Unified Manager に正しく接続できるように、いくつかの必要な設定を確認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 ）標準のサービスプロバイダ（ SP ）とみなされます。

サポートされている暗号化標準

- 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

- 3 つの要求ルールを次の順序で定義する必要があります。これらは、この証明書利用者信頼エントリに対する ADFS SAML 応答を Unified Manager で解析するために必要です。

| 要求規則 | 価値 |
| --- | --- |
| Sam - アカウント名 | 名前 ID |
| Sam - アカウント名 | urn ： OID ： 0.9.2342.19200300.100.1.1 |
| トークングループ — 修飾されていない名前 | urn ： OID ： 1.3.6.1.4.1.5923.1.5.1.1 |

- 認証方法を「フォーム認証」に設定する必要があります。設定しないと、 Unified Manager からログアウトするときにユーザにエラーが表示されることがあります。次の手順を実行します。
  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 [Authentication Policies] フォルダをクリックします
  c. 右の [ アクション ] 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式をデフォルトの「 Windows 認証」ではなく「フォーム認証」に設定します。
- Unified Manager のセキュリティ証明書が CA 署名証明書の場合、 IdP 経由で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方法は 2 つあります。
  - 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 サーバでの失効チェックを無効にします。

    "証明書利用者信頼ごとの失効チェックを無効にします"

  - ADFS サーバ内にある CA サーバで Unified Manager サーバ証明書要求に署名します。

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 サーバと Unified Manager サーバの時間の差が 5 分を超えないようにします。時間の差が 5 分を超えると認証が失敗します。

## SAML 認証の有効化

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。

作業を開始する前に

- リモート認証を設定し、正常に実行され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。

このタスクについて

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、両方の接続を完了できるように準備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. Enable SAML authentication * チェックボックスをオンにします。

   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 サーバに Unified Manager サーバから直接アクセスできる場合は、 IdP の URI を入力したあとに「 * IdP メタデータの取得」ボタンをクリックすると、 IdP のメタデータフィールドに自動的に値が入力されます。

4. Unified Manager のホストメタデータ URI をコピーするか、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（ Save ） ] 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 が再起動します。

結果

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。

完了後

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。

アイデンティティプロバイダに ADFS を使用している場合は、 Unified Manager GUI で ADFS のタイムアウトが考慮されず、 Unified Manager のセッションタイムアウトに達するまでセッションが続行されます。GUI セッションのタイムアウトを変更するには、 * General * > * Feature Settings * > * Inactivity Timeout * をクリックします。

# データベースダンプバックアップのデスティネーションの設定とスケジュール設定

Unified Manager のデータベースダンプバックアップ設定で、データベースのバックアップパス、保持数、およびバックアップスケジュールを設定できます。日単位または週単位のスケジュールされたバックアップを有効にすることができますデフォルトでは、スケジュールされたバックアップは無効になっていますが、バックアップスケジュールを設定する必要があります。

## 作業を開始する前に

- 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。
- バックアップパスとして定義する場所に 150GB 以上の利用可能なスペースが必要です。

  Unified Manager ホストシステムとは別のリモートの場所を使用することを推奨します。

- Unified ManagerをLinuxシステムにインストールしている場合は、「jboss」ユーザにバックアップディレクトリへの書き込み権限が割り当てられていることを確認してください。
- 新しいクラスタの追加後にUnified Managerで15日分の履歴パフォーマンスデータを収集している間は、バックアップ処理を実行しないようにスケジュールしてください。

## このタスクについて

初回のバックアップではフルバックアップが実行されるため、 2 回目以降のバックアップよりも時間がかかります。フルバックアップは 1GB を超えることもあり、 3~4 時間かかる場合があります。2 回目以降のバックアップは増分バックアップとなり、所要時間は短くなります。

増分バックアップファイルがバックアップ用に割り当てたスペースに対して増えすぎている場合は、新しいフルバックアップを定期的に作成して、古いフルバックアップとそのすべての子増分ファイルを置き換えることができます。Unified Manager が Linux システムにインストールされている場合は、別の方法として NetApp Snapshot のバックアップを開始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、 * General * > * Database Backup * をクリックします。
2. [* データベース・バックアップ * ] ページで、 [ * バックアップ設定 * ] をクリックします。
3. バックアップパス、保持数、およびスケジュールの値を設定します。

   保持数のデフォルト値は 10 です。バックアップを無制限に作成する場合は 0 に設定します。

4. 「毎日スケジュール」または「毎週スケジュール」 * ボタンを選択し、スケジュールの詳細を指定します。
5. [ 適用（ Apply ） ] をクリックします。

### 結果

スケジュールに基づいてデータベースダンプバックアップファイルが作成されます。使用可能なバックアップファイルは、 [ データベースバックアップ ] ページに表示されます。

- 関連情報 *

"Active IQ Unified Manager 内で新しい増分バックアップ・チェーンを開始する方法"

# ローカルユーザのパスワードを変更しています

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。

### 作業を開始する前に

ローカルユーザとしてログインする必要があります。

### このタスクについて

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、パスワード管理者に問い合わせてください。メンテナンス・ユーザのパスワードを変更するには、『Active IQ Unified Manager システム構成ガイド』の「メンテナンス・コンソールの使用」の章を参照してください。

### 手順

1. Unified Manager にログインします。
2. トップ・メニュー・バーで、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（ Save ） ] をクリックします。

### 完了後

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である必要があります。

# セッションの非アクティブ時のタイムアウト設定

Unified Manager に非アクティブ時のタイムアウト値を指定して、一定の時間が経過したらセッションを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。

### 作業を開始する前に

アプリケーション管理者のロールが必要です。

### このタスクについて

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。

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

### 手順

1. 左側のナビゲーションペインで、 * 一般 * > * 機能設定 * 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時のタイムアウトを指定します。

| 状況 | 操作 |
| --- | --- |
| セッションが自動的に閉じないようにタイムアウトを設定しない | [* アクティビティなしタイムアウト * ] パネルで、スライダボタンを左（オフ）に移動し、 [ * 適用 * ] をクリックします。 |
| タイムアウト値として特定の時間（分）を設定します | [**Inactivity Timeout**] パネルで、スライダボタンを右（オン）に動かし、非アクティブ時のタイムアウト値を分単位で指定して、 [**Apply**] をクリックします。 |

# Unified Manager のホスト名を変更しています

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 サーバまたは CentOS 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。

### 作業を開始する前に

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。

### このタスクについて

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 が適切に設定されていないと、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、ホスト名を変更したとき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場合は、 OnCommand Workflow Automation （ WFA ）でホスト名を手動で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します

   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の生成

別の認証局の署名を使用する場合や現在のセキュリティ証明書の期限が切れた場合など、さまざまな理由で新しいHTTPSセキュリティ証明書を生成することがあります。新しい証明書で既存の証明書が置き換えられます。

作業を開始する前に

アプリケーション管理者のロールが必要です。

このタスクについて

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。

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、次のいずれかのオプションを選択します。

| 状況 | 手順 |
| --- | --- |
| 現在の値で証明書を再生成します | [ 現在の証明書属性を使用して再生成（ Regenerate using current Certificate Attributes ） ] オプションをクリックし |
| 別の値を使用して証明書を生成します | [ 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。<br><br>新しい値を入力しない場合は、 [ 共通名 ] フィールドと [ 代替名 ] フィールドに既存の証明書の値が使用されます。その他のフィールドには値は必要ありませんが、証明書に値を入力する場合は、たとえば、市区町村、都道府県、国などの値を入力できます。<br><br>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(localhostなど)チェックボックスをオンにしますこのチェックボックスをオンにすると、 [ 代替名 ] フィールドに入力したフィールドのみが使用されます。空白のままにすると、結果の証明書に代替名フィールドがまったく表示されなくなります。 |

4. [ はい ] をクリックして証明書を再生成します。
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。

完了後

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しています

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。

作業を開始する前に

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。

このタスクについて

[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 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 または CentOS 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 Unified Manager サーバを識別しやすくなります。

作業を開始する前に

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。

このタスクについて

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、ホスト名を変更したとき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場合は、 OnCommand Workflow Automation （ WFA ）でホスト名を手動で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します `hostnamectl` コマンドを実行します `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。 `service network restart`
6. サービスが再起動したら、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ものと同じ 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します

Unified Manager 9.7 以降では、 ONTAP クラスタに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処理に相当しますが、 Unified Manager を使用して適用した場合は、 Unified Manager インスタンスで監視しているすべてのクラスタのワークロードをプロビジョニングおよび管理できます。

## 作業を開始する前に

アプリケーション管理者のロールが必要です。

## このタスクについて

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 | 場所 |
| --- | --- |
| 新しいワークロードのプロビジョニングページ | 一般的なタスク * > * プロビジョニング * から使用できます |

| 新しいコンテンツ | 場所 |
| --- | --- |
| 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 * から選択できます |
| パフォーマンスストレージ効率化ポリシーの作成ページ | 設定 * > * ポリシー * > * ストレージ効率化 * で確認できます |
| 現在のワークロードパフォーマンスとワークロード IOPS を表示するパネル | ダッシュボードで確認できます |

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、 * 一般 * > * 機能設定 * をクリックします。
2. [ 機能の設定 * ] 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、スライダボタンを左に動かします。 |
| ポリシーベースのストレージ管理を有効化 | ポリシーベースのストレージ管理 * パネルで、スライダボタンを右に動かします。 |

## 著作権に関する情報



## 商標に関する情報