Active IQ Unified Manager を設定しています

Active IQ Unified Manager 9.12

NetApp
December 18, 2023

目次

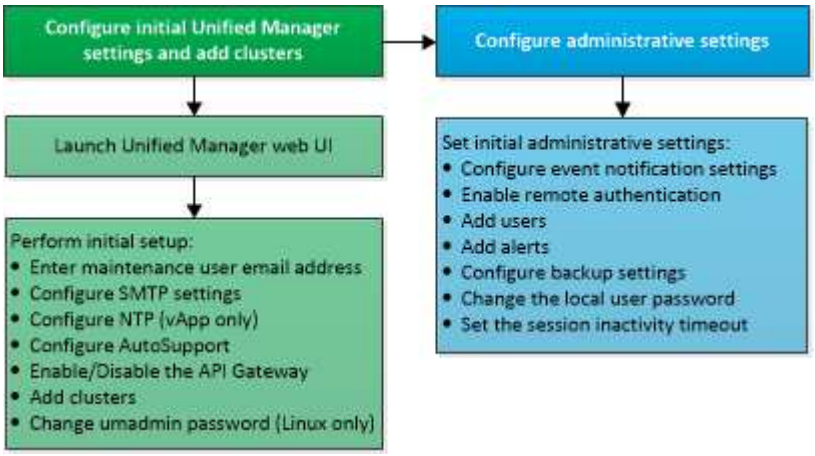
Active IQ Unified Manager を設定しています

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。

- 必要なもの *
- 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、システムがロックアウトされ、システム管理者に連絡する必要があります。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

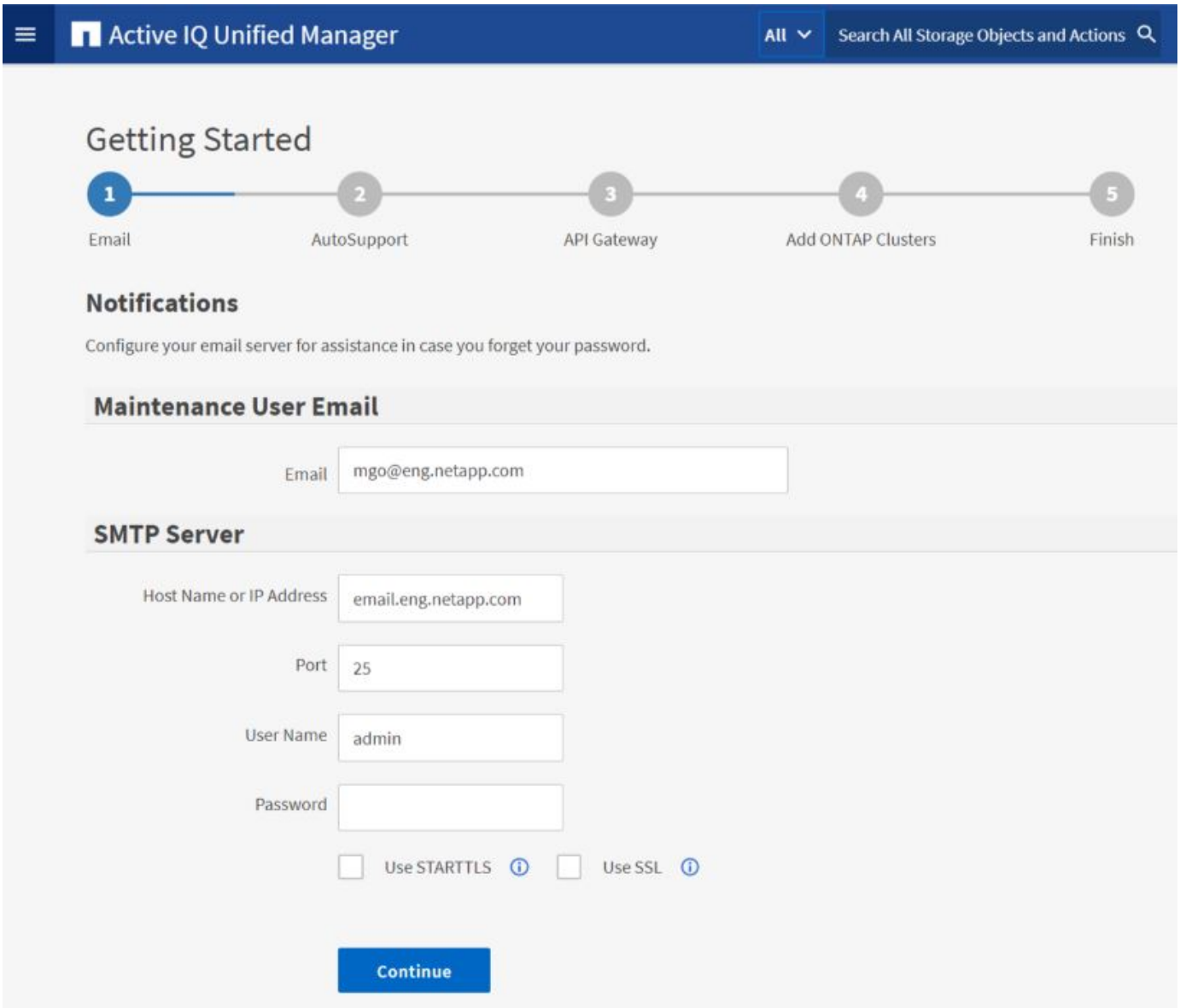
Unified Manager を使用するには、 NTP サーバ、メンテナンスユーザの E メールアドレス、 SMTP サーバのホストなどを最初に設定し、 ONTAP クラスタを追加する必要があります。

- 必要なもの *

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 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。

   [**Use STARTTLS ***]または[***Use SSL ***]オプションを選択した場合は、[***Continue**]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設定を続行します。

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します。
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. [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。

Getting Started ページが閉じ、 Unified Manager の Dashboard 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。

- 必要なもの *
- 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、*console*、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 ）
  - 必要な証明書を用意しておきます。Unified Managerでクラスタの追加時にセキュリティ証明書がイン

ストールされます。

サーバ証明書：この証明書はUnified Managerが所有しています。デフォルトの自己署名SSL（HTTPS）証明書が生成され、Unified Managerの新規インストールが実行されます。セキュリティを強化するために、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、再生成してUnified Managerを再起動し、サービスに新しい証明書を組み込む必要があります。SSL証明書の再生成の詳細については、を参照してください "HTTPS セキュリティ証明書の生成"。

相互**TLS**通信証明書：Unified ManagerとONTAP 間の相互TLS通信で使用されます。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で有効になります。ONTAP バージョン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が有効になっていません。

古いバージョンのUnified ManagerをUnified Manager 9.12に更新する場合、クラスタの証明書ベースの認証は自動的に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ることで有効にできます。証明書の有効期限が切れた場合は、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、を参照してください "クラスタを編集します"。

> ◦ 証明書ベースの認証は、Web UIからクラスタを追加した場合に自動的に有効になります。メンテナンスコンソールからクラスタを追加した場合、証明書ベースの認証は有効になりません。
>
> ◦ 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、Unified Managerのバックアップをサーバから作成し、ホスト名またはIPアドレスが変更された別のUnified Managerサーバにリストアすると、クラスタの監視が失敗することがあります。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。クラスタの詳細の編集の詳細については、を参照してください "クラスタを編集します"。

+ クライアント証明書：ONTAP から受信したEMSメッセージの認証時に使用されます。この証明書はONTAP が所有しており、ONTAP クラスタをUnified Managerに追加する場合に必要です。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。クライアント証明書の期限が切れている場合は、クラスタを追加する前に再生成する必要があります。ただし、追加済みのクラスタの証明書の有効期限が切れて Unified Manager で使用されている場合は、 EMS メッセージが期限切れの証明書を使用して引き続き機能します。証明書の生成については、ナレッジベース（KB）の記事を参照してください "System Managerユーザインターフェイスで ONTAP の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、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、 * 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. 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. [ホストの許可] 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。

   Unified Manager 9.12では、クラスタの詳細を保存したあと、クラスタの双方向TLS通信の証明書を確認できます。

   証明書ベースの認証が有効になっていない場合、Unified Managerはクラスタが最初に追加されたときにのみ証明書をチェックします。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。

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 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。

- 関連情報 *

"CA 署名済みで返された HTTPS 証明書をインストールする"

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。

- 必要なもの *

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。

- 必要なもの *

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. 通知ページで、適切な設定を行います。
   - 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。
3. [保存（ Save ）] をクリックします。
4. [*Use STARTTLS *]または[*Use SSL *]オプションを選択した場合は、[*Save]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ます。既存の証明書の有効期限が切れた場合は、「* STARTTLSを使用」または「* SSLを使用」チェックボックスをオフにし、通知設定を保存してから「* STARTTLSを使用*」または「SSLを使用*」チェックボックスを再度オンにして新しい証明書を表示します。

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。

- 必要なもの *

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。 ◦ `domainname\username` ◦ `username@domainname` ◦ `Bind Distinguished Name` （適切なLDAP表記を使用） • 管理者パスワード • 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） • 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. * 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（ 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。

- 必要なもの *
- 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、 * 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。

認証サービスをセットアップしています

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。

- 必要なもの *
- 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、 * 一般 * > * 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。

を選択した場合は	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、認証サーバのドメイン名が + ou@domain.com + である場合、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。 たとえば、認証サーバのドメイン名が + ou@domain.com + である場合、ベース識別名は * cn=ou 、 dc=domain 、 dc=com * です。

を選択した場合は	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、認証サーバのドメイン名が + ou@domain.com + である場合、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（ 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。

- 必要なもの *
- 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、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。 b. [Authentication Servers] 領域で、 [**Add**] をクリックします。 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。 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。 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。 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。 ⓘ 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。 b. [Authentication Servers] 領域で、 [**Add**] をクリックします。 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。 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。

- 必要なもの *
- 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。

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. Test User 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、 * Test * 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。

- 必要なもの *
- 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。

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 + 」、「テスト」スクリプトを含み、 15 分ごとにユーザー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. 「 * Name Contains * 」フィールドに「 * abc 」と入力して、「 abc 」という名前のボリュームを表示します。
   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、 [* 名前に * が含まれる *] 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。

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。

- 必要なもの *

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手順については、を参照してください "メンテナンスコンソールを使用する"。

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. Change Password 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。

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。

- 必要なもの *

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。

> 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。

- 必要なもの *

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

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

- 必要なもの *

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かあります。たとえば、識別名（ DN ）の値を大きくする場合や、キーのサイズを大きくする場合や、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ている場合などです。

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は、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。この証明書には、サイズが 2048 ビットの RSA キーがあります。

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。 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。「共通名」は、ホストの FQDN に設定する必要があります。その他のフィールドには値は必要ありませんが、電子メール、会社、部署、証明書に値を入力する場合は、 [市区町村] 、 [都道府県] 、および [国] を選択します。使用可能なキー・サイズ（キー・アルゴリズムは「 RSA 」）と有効期間から選択することもできます。 ⓘ • キーサイズに指定できる値は、です `2048`、 `3072` および `4096`。 • 有効期間は、 1 日 〜 最大 36500 日です。 有効期間は 36500 日ですが、有効期間は 397 日以内または 13 か月以内にすることをお勧めします。397 日以上の有効期間を選択し、この証明書の CSR をエクスポートして既知の CA によって署名された証明書を取得する予定であるため、 CA から返された署名済み証明書の有効性は 397 日に減少します。 • 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（ローカルホストなど）］ 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。
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。

- 必要なもの *

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。

また、「ゲストを再起動」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。

- 必要なもの *

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。

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
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。