設定タスクと管理タスクを実行

Active IQ Unified Manager 9.13

NetApp
December 18, 2023

目次

設定タスクと管理タスクを実行 . . . 1
Active IQ Unified Manager を設定しています . . . 1
Unified Manager のバックアップを設定しています . . . 21
機能設定の管理 . . . 21
メンテナンスコンソールを使用する . . . 25
ユーザアクセスの管理 . . . 39
SAML 認証の設定を管理する . . . 46
認証の管理 . . . 53
セキュリティ証明書の管理 . . . 60

設定タスクと管理タスクを実行

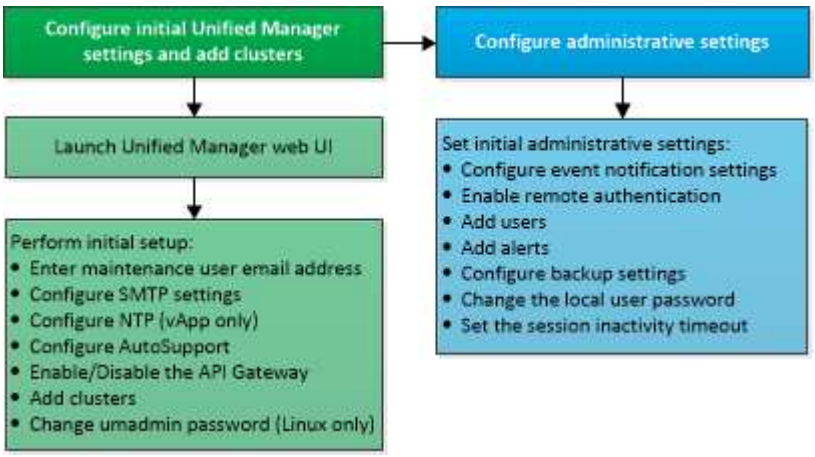
Active IQ Unified Manager を設定しています

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

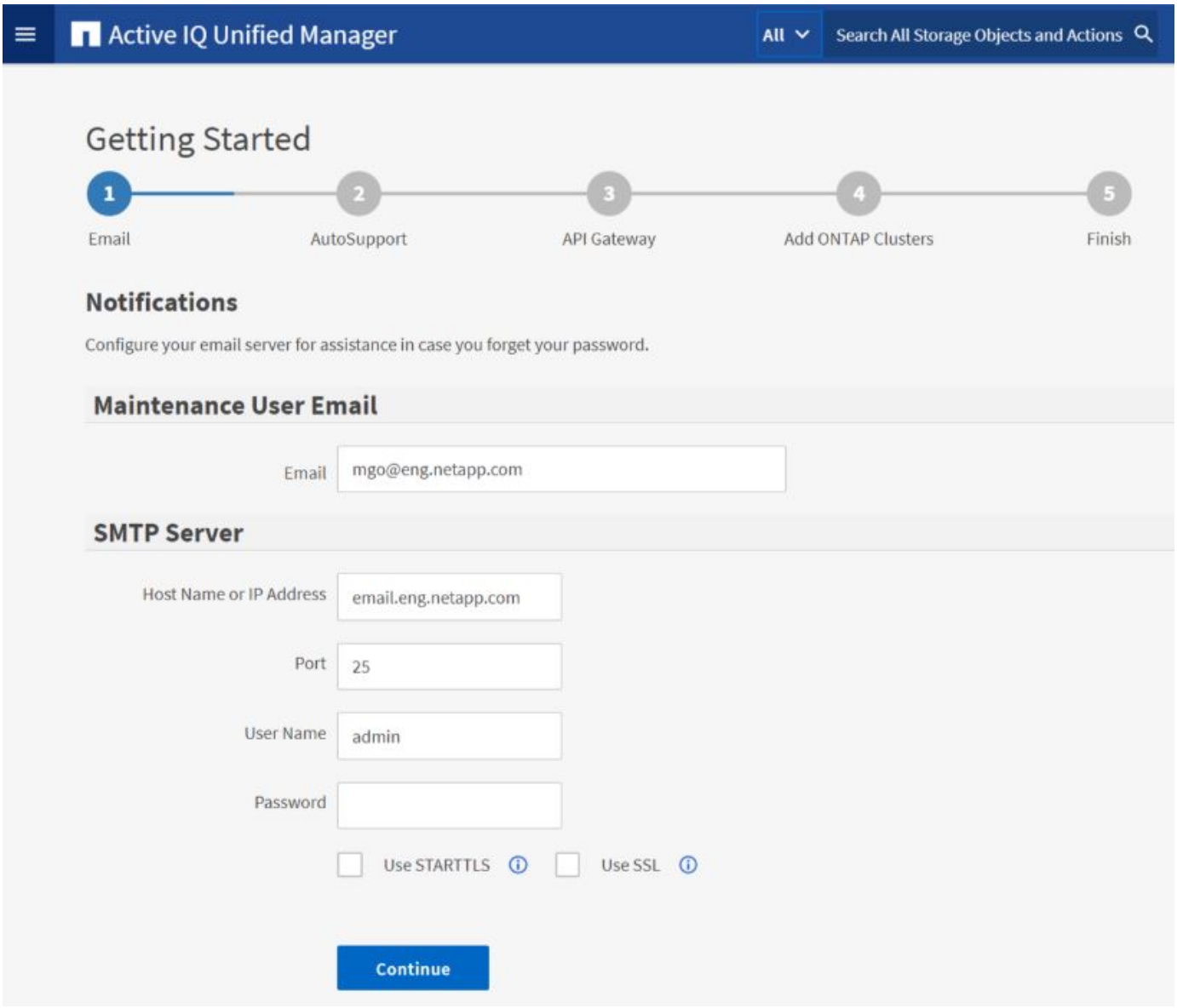
Unified Manager を使用するには、 NTP サーバ、メンテナンスユーザの E メールアドレス、 SMTP サーバのホストなどを最初に設定し、 ONTAP クラスタを追加する必要があります。

- 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。
  - 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。

- SSL（HTTPS）証明書*：この証明書の所有者はUnified Managerです。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"。
- 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通知の認証時に使用されます。

  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。

  Unified Managerの古いバージョンを更新する場合、クラスタで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"。

  ◦ Web UIからクラスタを追加すると、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を追加する場合は、Unified Manager UIを使用してクラスタを編集する必要があります。を参照してください "Unified Manager の CLI コマンドがサポートされています" をクリックしてください。

  ◦ 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"。

  クラスタ証明書：この証明書の所有者はONTAP です。証明書の有効期限が切れているクラスタをUnified Managerに追加することはできません。証明書の有効期限が切れている場合は、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。

   クラスタの詳細を保存すると、クラスタの相互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。

Unified Manager のバックアップを設定しています

Unified Manager のバックアップ機能は、ホストシステムおよびメンテナンスコンソールから実行する一連の設定手順で設定できます。

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

機能設定の管理

[機能設定] ページでは、 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。

[機能の設定] ページは、アプリケーション管理者ロールを持つユーザーのみが使用できます。

スクリプトのアップロードについては、を参照してください "スクリプトアップロードの有効化 / 無効化"。

ポリシーベースのストレージ管理の有効化

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た 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。

この機能のアクティブ化または非アクティブ化は、 * General * > * Feature Settings * > * Policy-Based Storage Management * から選択できます。この機能をアクティブ化すると、次のページで操作と監視を行うことができます。

- プロビジョニング（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 * > * ストレージ効率化 *
- クラスタセットアップページのパフォーマンスサービスレベルで管理されるワークロードの列
- ダッシュボード上のワークロードのパフォーマンスパネル *

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化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たストレージワークロードと準拠しないストレージワークロードを監視することもできます。ワークロードのパフォーマンスとワークロードの IOPS パネルでは、データセンター内のクラスタの合計容量、使用可能容量、使用済み容量、およびパフォーマンス（ IOPS ）を、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評価することもできます。

この機能をアクティブ化したら、 Unified Manager REST API を実行して、 * 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 * カテゴリから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アドレスと<hostname> APIページにアクセスするためのURLを+https：// rest /docs/api/+の形式で入力することもできます。

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"。

API ゲートウェイを有効にしてい

API ゲートウェイ機能を使用すると、 ONTAP を個別にログインせずに、複数の Active IQ Unified Manager クラスタを一元的に管理できます。

この機能は、 Unified Manager に最初にログインしたときに表示される設定ページから有効にできます。または、 * 一般 * > * 機能設定 * > * API ゲートウェイ * 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 と ONTAP REST API は別のものであり、 Unified Manager REST API を使用して ONTAP REST API のすべての機能を利用できるわけではありません。ただし、 Unified Manager では提供されていない特定の機能を管理するために ONTAP API にアクセスする必要がある場合は、 API ゲートウェイ機

能を有効にして ONTAP API を実行できます。ゲートウェイは、ヘッダーと本文の形式を ONTAP API と同じにすることで、 API 要求をトンネリングするプロキシとして機能します。Unified Manager のクレデンシャルを使用して特定の API を実行することで、個々のクラスタのクレデンシャルを渡すことなく ONTAP クラスタにアクセスして管理することができます。Unified Manager は単一の管理ポイントとして機能し、 Unified Manager インスタンスで管理される ONTAP クラスタ全体で API を実行できます。API から返される応答は、対応する ONTAP REST API を ONTAP から直接実行した場合と同じです。

この機能を有効にしたあと、 * 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 を実行できます。また、ホスト名またはIPアドレスとURLをの形式で入力して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、を参照してください "Active IQ Unified Manager REST APIの使用を開始する"。

非アクティブ時のタイムアウトの指定

Active IQ Unified Manager に非アクティブ時のタイムアウト値を指定できます。非アクティブな状態が指定した時間を経過すると、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。

この機能を非アクティブにするか、 * 一般 * > * 機能設定 * > * 非アクティブタイムアウト * から時間を変更できます。この機能をアクティブにしたら、システムが自動的にログアウトするまでの時間制限（分単位）を * logout after * フィールドに指定する必要があります。デフォルト値は 4320 分（ 72 時間）です。

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。

Active IQ ポータルイベントの有効化

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。この設定を有効にすると、 Active IQ ポータルでシステム構成やケーブル配線などに関する追加のイベントが検出されて表示されます。このオプションはデフォルトで有効になっています。

Active IQ Unified Manager でこの機能を有効にすると、 Active IQ ポータルで検出されたイベントが表示されます。イベントは、すべての監視対象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 Unified Manager の他の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。

この機能をアクティブ化または非アクティブ化するには、 * 一般 * > * 機能設定 * > * Active IQ ポータルイベント * を選択します。外部ネットワークへの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 イベントが Unified Manager で検出または表示されなくなります。無効にすると、この機能を有効にすると、クラスタタイムゾーンの事前定義された時刻（ 00 ： 15 ）に Unified Manager がクラスタで Active IQ イベントを受信できるようになります。

準拠のためのセキュリティ設定の有効化と無効化

Features Settings ページの * Security Dashboard * パネルにある * Customize * ボタンを

使用して、 Unified Manager でセキュリティパラメータを有効または無効にして、コンプライアンス監視を実行できます。

このページで有効または無効になる設定によって、 Unified Manager でのクラスタと Storage VM の全体的な準拠ステータスが制御されます。選択内容に応じて、対応する列がクラスタインベントリページの「セキュリティ：すべてのクラスタ」の「 * セキュリティ：すべての Storage VM * 」ビューと「 Storage VM インベントリ」ページの「 * セキュリティ：すべての Storage 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。

ONTAP クラスタ、 Storage VM 、およびボリュームのセキュリティ条件は、で定義されている推奨事項に照らして評価されます "Security Hardening Guide for NetApp ONTAP 9"。ダッシュボードおよびセキュリティページのセキュリティパネルには、クラスタ、 Storage VM 、およびボリュームのデフォルトのセキュリティコンプライアンスステータスが表示されます。また、セキュリティイベントが生成され、セキュリティ違反があるクラスタと Storage VM に対して有効になる管理操作も実行されます。

セキュリティ設定のカスタマイズ

ONTAP 環境に応じて準拠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 *] の順にクリックします。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、クラスタおよび Storage VM 画面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されたレポートに直接影響します。セキュリティパラメータを変更する前に、これらの画面から Excel レポートをアップロードした場合、ダウンロードした Excel レポートに問題がある可能性があります。

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 * 」で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ためのオプションについては、を参照してください "クラスタコンプライアンスのカテゴリ"。
3. Storage VMのカスタム設定を有効または無効にするには、* Storage VM *で必要な一般設定を選択します。Storage VM 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、を参照してください "Storage VM コンプライアンスのカテゴリ"。

AutoSupport および認証設定のカスタマイズ

AutoSupport 設定 * セクションでは、 AutoSupport からの ONTAP メッセージの送信に HTTPS 転送を使用するかどうかを指定できます。

認証設定 * セクションでは、デフォルトの ONTAP 管理者ユーザに対して Unified Manager のアラートを生成するように設定できます。

スクリプトアップロードの有効化 / 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アクティビティを許可しない場合は、この機能を無効にできます。

- 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。

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スクリプト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します	• スクリプトアップロード * パネルで、スライダボタンを左に動かします。
スクリプトを有効にします	• スクリプトアップロード * パネルで、スライダボタンを右に動かします。

ログインバナーを追加しています

ログインバナーを追加すると、システムへのアクセスを許可されているユーザ、ログインおよびログアウト時の使用条件などの情報を組織で表示できます。

このログインバナーのポップアップは、ストレージオペレータや管理者など、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

メンテナンスコンソールでは、ネットワークの設定、 Unified Manager がインストールされているシステムの設定と管理、潜在的な問題の防止とトラブルシューティングに役立つその他のメンテナンスタスクを実行することができます。

メンテナンスコンソールで提供される機能

Unified Manager のメンテナンスコンソールでは、 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。

メンテナンスコンソールでは、 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次の機能が提供されます。

- 仮想アプライアンスの問題、特に Unified Manager の Web インターフェイスを使用できない場合はトラブルシューティングを行ってください
- Unified Manager を新しいバージョンにアップグレードします
- テクニカルサポートに送信するサポートバンドルを生成する

- ネットワークの設定を行います
- メンテナンスユーザのパスワードを変更します
- パフォーマンス統計を送信するには、外部データプロバイダに接続してください
- パフォーマンスデータ収集の内部を変更します
- 以前にバックアップしたバージョンからの Unified Manager データベースと設定のリストア

メンテナンスユーザの役割

Unified Manager を Red Hat Enterprise Linux または CentOS 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。メンテナンスユーザの名前は「 umadmin 」です。メンテナンスユーザは、 Web UI でアプリケーション管理者のロールが割り当てられ、他のユーザ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。

診断ユーザの権限

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。

メンテナンスコンソールへのアクセス

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。

- 必要なもの *

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 分間操作を行わないと、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。

ステップ

1. メンテナンスコンソールにアクセスするには、次の手順を実行します。

オペレーティングシステム	実行する手順
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の名前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。
Linux の場合	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. 入力するコマンド `maintenance_console` を押します。
Windows の場合	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. 入力するコマンド `maintenance_console` 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。

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。

- 必要なもの *
- maintenance 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探します。
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 分間操作を行わないと、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

メンテナンスコンソールは各種のメニューで構成され、 Unified Manager サーバの特別な機能や設定の保守と管理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は次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. サポート/診断
  b. サーバ証明書をリセットします
  c. 外部データプロバイダ
  d. バックアップのリストア
  e. パフォーマンスポーリング間隔の設定
  f. SAML 認証を無効にする
  g. アプリケーションポートを表示/変更します
  h. デバッグログの構成
  i. MySQLポート3306へのアクセスを制御します
  j. 終了します

特定のメニューオプションにアクセスするための番号をリストから選択します。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。

Network Configuration （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 、 CentOS 、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。

次のメニュー項目を選択できます。

- * IP アドレス設定 * を表示します

  仮想アプライアンスの現在のネットワーク設定について、 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、 および DNS サーバです。

- * IP アドレス設定の変更 *

  IP アドレス、ネットマスク、ゲートウェイ、 DNS サーバなど、仮想アプライアンスのネットワーク設定を変更できます。メンテナンスコンソールでネットワーク設定を DHCP から静的ネットワークに切り替

えた場合は、ホスト名を編集できません。変更を実行するには、 [* 変更をコミットする *] を選択する必要があります。

- * ドメイン名検索設定を表示 *

  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の変更 *

  ホスト名を解決する際に検索するドメイン名を変更できます。変更を実行するには、 [* 変更をコミットする *] を選択する必要があります。

- * スタティックルートを表示 *

  現在の静的ネットワークルートが表示されます。

- * スタティックルートの変更 *

  静的ネットワークルートを追加または削除できます。変更を実行するには、 [* 変更をコミットする *] を選択する必要があります。

  - * ルートを追加 *

    静的ルートを追加できます。

  - * ルートの削除 *

    静的ルートを削除できます。

  - * 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イスを無効にします。 *

  使用可能なネットワークインターフェイスを無効にします。使用可能なネットワークインターフェイスが 1 つしかない場合は、それを無効にすることはできません。変更を実行するには、 [* 変更をコミットする *] を選択する必要があります。

- * ネットワーク・インターフェイスを有効にする *

  使用可能なネットワークインターフェイスを有効にします変更を実行するには、 [* 変更をコミットする *] を選択する必要があります。

- * 変更を確定 *

  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、このオプションを選択する必要があります。そうしないと、変更は行われません。

- * ホストに Ping を実行します *

  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。

- * デフォルト設定に復元 *

  すべての設定を工場出荷時のデフォルトにリセットします。変更を実行するには、 [* 変更をコミットする *] 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。

System Configuration （システム設定）メニュー

System Configuration メニューでは、サーバのステータスの表示、仮想マシンのリブートとシャットダウンなど、さまざまなオプションを指定して仮想アプライアンスを管理できます。

Unified Manager を Linux または Microsoft Windows システムにインストールしている場合、このメニューには「 Restore from a Unified Manager Backup 」オプションのみが表示されます。

次のメニュー項目を選択できます。

- * サーバーステータスを表示 *

  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必要があります。

- * 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。

- * < ログインユーザー > ユーザーパスワード * を変更します

  現在ログインしているユーザのパスワードを変更します。変更できるのはメンテナンスユーザだけです。

- * データディスクのサイズを増やします。 *

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・サイズの増加 *

  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。

- * タイムゾーンの変更 *

  タイムゾーンを自分の場所に変更します。

- * NTP サーバーを変更 *

  IP アドレスや Fully Qualified Domain Name （ FQDN ；完全修飾ドメイン名）などの NTP サーバ設定を変更します。

- * NTP サービスの変更 *

  を切り替えます `ntp` および `systemd-timesyncd` サービス：

- * Unified Manager バックアップからのリストア *

  以前にバックアップしたバージョンから Unified Manager データベースと設定をリストアします。

- * サーバー証明書をリセット *

  サーバセキュリティ証明書をリセットします。

- * ホスト名を変更 *

  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 （システム設定）メニューを終了し、 Main Menu （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メニューを終了します。

Support and Diagnostics （サポートと診断）メニュー

Support and Diagnostics メニューでは、トラブルシューティングのサポート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生成することができます。

次のメニューオプションを使用できます。

- * ライトサポートバンドル * を生成します

  30 日間のログと構成データベースのレコードを含む軽量なサポートバンドルを作成できます。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。

- * サポートバンドル * を生成します

診断ユーザ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、ネットアップにサポートバンドルをアップロードすることもできます。

このファイルには、 AutoSupport メッセージで生成された情報、 Unified Manager データベースの内容、 Unified Manager サーバの内部に関する詳細なデータ、および通常は AutoSupport メッセージや軽量なサポートバンドルには含まれない詳細なログが収められます。

その他のメニューオプション

次に示すメニューオプションでは、 Unified Manager サーバでさまざまな管理タスクを実行することができます。

次のメニュー項目を選択できます。

- * サーバー証明書をリセット *

  HTTPS サーバ証明書を再生成します。

  Unified Manager の GUI でサーバ証明書を再生成します。そのためには、 * General * > * HTTPS Certificates * > * Regenerate HTTPS Certificate * をクリックします。

- * SAML 認証を無効にします *

  SAML 認証を無効にし、 Unified Manager の GUI にアクセスするユーザのアイデンティティプロバイダ（ IdP ）によるサインオン認証を中止します。このコンソールオプションは、一般に、 IdP サーバまたは SAML の設定を使用する問題で Unified Manager の GUI へのアクセスがブロックされる場合に使用します。

- * 外部データプロバイダ *

  Unified Manager を外部データプロバイダ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に送信されて、ストレージパフォーマンスのエキスパート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。次のオプションが表示されます。

  - *Display Server Configuration *-- 外部データプロバイダの現在の接続設定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することができます。
  - * Modify Server Configuration * — 外部データプロバイダの新しい設定を入力したり、既存の設定を変更したりすることができます。
  - *Delete Server Connection *-- 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 は外部サーバとの接続を失います。

- バックアップの復元

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

- * パフォーマンスポーリング間隔の設定 *

Unified Manager がクラスタ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ための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 がセキュリティ上の理由から、 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オプションが用意されています。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、このポート経由のアクセスは、Linux、Windows、およびVMware vSphereシステムへのUnified Managerの新規インストール時にlocalhostにのみ制限されます。このオプションを使用すると、ローカルホストとリモートホストの間でこのポートの表示/非表示を切り替えることができます。つまり、環境内のlocalhostに対してのみポートが有効になっている場合は、このポートをリモートホストでも使用できるようにすることができます。または、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localhostのみに制限できます。アクセスがリモートホストで有効になっていた場合は、アップグレードシナリオで設定が保持されます。ポートの可視性を切り替えたあとにWindowsシステムのファイアウォールの設定を確認し、MySQLポート3306へのアクセスを制限するように設定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。

Windows でメンテナンスユーザのパスワードを変更する

Unified Manager のメンテナンスユーザのパスワードを必要に応じて変更することができます。

手順

1. Unified Manager Web UI のログインページで、 * 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求めるページが表示されます。

2. ユーザー名を入力し、 * Submit * をクリックします。

   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、そのユーザ名に定義された E メールアドレスに送信されます。

3. E メールの * パスワードのリセットリンク * をクリックし、新しいパスワードを定義します。
4. Web UI に戻り、新しいパスワードを使用して Unified Manager にログインします。

Linux システムでの 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。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。

- 必要なもの *
- Unified Manager が Red Hat Enterprise Linux システムまたは CentOS 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。

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、セキュリティ上の理由からインストール後に変更することができます。デフォルトのポートは、 HTTP の場合は 80 、 HTTPS の場合は 443 です。

- 必要なもの *

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 キーを押します。
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すると、プロトコルのデフォルト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. 「 * y * 」と入力してポートを変更し、 Unified Manager を再起動します。
6. メンテナンスコンソールを終了します。

変更後は、Unified Manager Web UIにアクセスするための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+,、+ https://[2001:db8:0:1]:2123+.）。

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。

- 必要なもの *

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、 * System Configuration * > * Reboot Operating System * を選択します。

   リブート後、新たに追加したネットワークインターフェイスはメンテナンスコンソールで検出できます。

2. メンテナンスコンソールにアクセスします
3. ネットワーク構成 **>*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イスを選択し、 * Enter * キーを押します。
   - eth1 * を選択し、 * Enter * を押します。
5. 「 * y * 」と入力してネットワーク・インターフェイスを有効にします。
6. ネットワーク設定を入力します。

   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、ネットワーク設定を入力するように求められます。

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

7. [変更のコミット *] 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。

Unified Manager データベースディレクトリにディスクスペースを追加しています

Unified Manager データベースディレクトリには、 ONTAP システムから収集された健常性とパフォーマンスのデータがすべて含まれています。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、各クラスタに多数のノードがあると、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使用率が 90% の場合は警告イベントが生成され、ディレクトリの使用率が 95% の場合は重大イベントが生成されます。

ディレクトリの使用率が 95% に達すると、クラスタから追加の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 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。

Linux ホストのデータディレクトリにスペースを追加しています

に十分なディスクスペースを割り当てていない場合 `/opt/netapp/data` Unified Managerをサポートするディレクトリ：Linuxホストを最初にセットアップしたあとにUnified Managerをインストールしたときに、のディスクスペースを増やしてインストール後にディスクスペースを追加できます `/opt/netapp/data` ディレクトリ。

- 必要なもの *

Unified Manager がインストールされている Red Hat Enterprise Linux マシンまたは CentOS 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. 一時バックアップフォルダを作成する（例： `/backup-data`）には、現在のデータを格納できるだけの十分なディスクスペースがあります `/opt/netapp/data` ディレクトリ。
4. 既存ののの内容と権限の設定をコピーします `/opt/netapp/data` ディレクトリをバックアップデータディレクトリに移動します。

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

5. SE Linux が有効になっている場合：

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

      ```
      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の SE Linux タイプを設定します。

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

6. の内容を削除します `/opt/netapp/data` ディレクトリ：
   a. `cd /opt/netapp/data`
   b. `rm -rf *`
7. のサイズを展開します `/opt/netapp/data` LVMのコマンドを使用するかディスクを追加して、ディレクトリのサイズを150GB以上にします。

> を作成した場合は `/opt/netapp/data` ディスクからはマウントしないでください `/opt/netapp/data` NFS共有またはCIFS共有として設定する。このため、ディスクスペースを拡張しようとすると、などの一部のLVMコマンドが実行されます `resize` および `extend` 期待どおりに動作しない可能性があります。

8. を確認します `/opt/netapp/data` ディレクトリの所有者（mysql）とグループ（root）は変更されません。

```
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、のコンテキストを確認します `/opt/netapp/data` ディレクトリがmysqld_db_tに設定されたままである
   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. abc というファイルを削除して、この余分なファイルがデータベースエラーを原因しないようにします。
11. 拡張したにバックアップデータの内容をコピーします `/opt/netapp/data` ディレクトリ：

```
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開始されたら、バックアップフォルダを削除します `/backup-data`：

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

VMware 仮想マシンのデータディスクにスペースを追加しています

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 のメンテナンスコンソールを使用してディスクスペースを増やして容量を追加できます。

- 必要なもの *
- 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ことが必要です。
- 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お勧めします。

手順

1. vSphere Client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。

   Unified Manager の導入では、ごくまれに「 Hard Disk 3 」ではなく「 Hard Disk 2 」がデータディスクに使用されることがあります。これが導入環境で発生した場合は、ディスクのサイズを大きくします。データディスクには、常に他のディスクよりも多くの容量があります。

2. vSphere Client で、 Unified Manager 仮想マシンを選択し、 * Console * 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、 **System Configuration** オプションの番号を入力します。
5. System Configuration Menu （システム構成メニュー）で、 * データディスクサイズの増加 * オプションの数値を入力します。

Microsoft Windows サーバの論理ドライブにスペースを追加する

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。

- 必要なもの *

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 server 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。 "基本ボリュームを拡張します"
物理サーバで、ハードディスクドライブを追加します。	Microsoft の次のトピックの手順に従います。 "ハードディスクドライブの追加"
仮想マシンで、ディスクパーティションのサイズを拡張します。	VMware の次のトピックの手順に従います。 "ディスクパーティションのサイズを拡張する"

ユーザアクセスの管理

Active IQ Unified Manager へのユーザアクセスを制御するために、ロールを作成し、機能を割り当てることができます。Unified Managerで選択したオブジェクトにアクセスするために必要な権限を持つユーザを特定できます。これらのロールと機能を持つユーザのみがUnified Managerでオブジェクトを管理できます。

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。

- 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。
- 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。

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. [ユーザー] ページで、 [* 追加] 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。

データベースユーザを作成しています

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、 Integration Schema ロールまたは Report Schema ロールを持つデータベースユーザを作成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。

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うことができます。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、 * 一般 * > * ユーザー * 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. [ユーザーの追加] ダイアログボックスの [タイプ **]** ドロップダウンリストで **[** 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で、適切な役割を選択します。

実行する作業	このロールを選択します
Unified Manager を Workflow Automation に接続しています	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	レポートスキーマ

6. [追加（ Add ）] をクリックします。

ユーザ設定の編集

各ユーザを指定する E メールアドレスやロールなどのユーザ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。

- 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。

ユーザに割り当てられているロールを変更すると、次のいずれかのアクションが発生したときに変更が適用されます。

- 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
- セッションのタイムアウトが 24 時間に達しました。

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. 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. [ユーザーの編集] ダイアログボックスで、ユーザーに指定されている適切な設定を編集します。
4. [保存（ Save ）] をクリックします。

ユーザの表示

ユーザページを使用して、 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。ユーザの詳細を表示できます。これには、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の情報が含まれます。

- 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。

ステップ

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。

ユーザ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 人以上のユーザを削除して、特定のユーザが 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、グループを削除して、グループ内のすべてのユーザが管理サーバにアクセスできないようにすることもできます。

- 必要なもの *
- 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、 * 一般 * > * ユーザー * 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. [はい] をクリックして削除を確定します。

RBAC とは

RBAC （ロールベースアクセス制御）を使用すると、 Active IQ Unified Manager サーバのさまざまな機能やリソースにアクセスできるユーザを制御できます。

ロールベースアクセス制御の機能

管理者は、ロールベースアクセス制御（ RBAC ）を使用してロールを定義することで、ユーザのグループを管理できます。特定の機能のアクセスを選択した管理者に制限する必要がある場合は、その管理者の管理者アカウントを設定する必要があります。管理者が表示できる情報と、管理者が実行できる処理を制限する場合は、作成した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を求められます。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。

ユーザタイプの定義

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。メンテナンスユーザは、別のユーザを作成してロールを割り当てます。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でもあります。Unified Manager を Red Hat Enterprise Linux または CentOS システムにインストールしている場合、メンテナンスユーザのユーザ名は「 umadmin 」です。

- * ローカルユーザー *

  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。このアカウントの名前は、認証サーバに保存されているグループの名前と一致している必要があります。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。

ユーザロールの定義

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。各ロールには特定の権限が含まれていますUnified Manager で実行できる操作の範囲は、割り当てられたロールとその権限で決まります。

Unified Manager には、事前定義された次のユーザロールが用意されて

- * 演算子 *

  履歴や容量の傾向など、 Unified Manager によって収集されたストレージシステムの情報やその他のデータを表示します。このロールを割り当てられたストレージオペレータは、イベントについて、表示、割り当て、応答、解決、メモの追加などの操作が可能です。

- * ストレージ管理者 *

  Unified Manager でのストレージ管理処理の設定を行います。このロールを割り当てられたストレージ管理者は、しきい値の設定、およびアラートなどのストレージ管理用のオプションやポリシーの作成が可能です。

- * 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、認証などの管理オプションを使用できます。 SMTP 、ネットワーク、および AutoSupport 。

  Unified Manager を Linux システムにインストールした場合は、アプリケーション管理者ロールが割り当てられた最初のユーザに自動的に「 umadmin 」という名前が付けられます。

- * 統合スキーマ *

  Unified Manager 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 *

  レポートおよびその他のデータベースビューに Unified Manager データベースから直接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。表示できるデータベースは次のとおりです。

  - NetApp_model_view
  - パフォーマンス
  - ocum
  - ocum_report
  - ocum_report_BIRT
  - OPM
  - 頭皮管理者

Unified Manager のユーザロールと機能

Unified Manager で実行できる操作は、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を表示する	•	•	•	•	•
履歴や容量のトレンドなど、その他のデータを確認できます	•	•	•	•	•

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
イベントを表示、割り当て、解決します	•	•	•		
SVM の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する	•	•	•		
しきい値ポリシーを表示します	•	•	•		
SVM の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		•	•		
アラートを定義		•	•		
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を管理する		•	•		
ユーザを管理します			•		
管理オプションの管理			•		
しきい値ポリシーを定義			•		
データベースアクセスの管理			•		

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
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「 Fix it 」オペレーションを実行します		•	•		
データベースビューへの読み取り専用アクセスを提供します					•

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。

- 必要なもの *
- 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。

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。

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。

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。

SAML 認証に使用するアイデンティティプロバイダを変更する

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。

- 必要なもの *
- 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 サーバから IdP に直接アクセスできる場合は、 IdP の URL 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。

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. [構成の保存 *] 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。

Unified Manager セキュリティ証明書変更後に SAML 認証設定を更新しています

Unified Manager サーバにインストールされている HTTPS セキュリティ証明書が変更されたときは、 SAML 認証の設定を更新する必要があります。証明書は、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更新されます。

セキュリティ証明書が変更されたあとに Unified Manager サーバが再起動されると、 SAML 認証は機能せず、ユーザは Unified Manager のグラフィカルインターフェイスにアクセスできなくなります。ユーザインターフェイスに再びアクセスできるようにするには、 IdP サーバと Unified Manager サーバの両方で SAML 認

証の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ます。

   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 のユーザインターフェイスを起動し、更新されたサーバ証明書をブラウザで受け入れ、メンテナンスユーザのクレデンシャルを使用してログインします。
4. [* Setup/Authentication] ページで [* SAML Authentication*] 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、メタデータを XML テキストファイルに保存します。
6. [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。

7. [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。
8. IdP サーバにアクセスし、 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	設定手順
ADFS （ 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. 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 `saml_sp_metadata.xml` 更新したUnified Managerサーバを使用します。 c. Unified Manager がこの証明書利用者信頼エントリに対する ADFS SAML 応答を解析するために必要な 3 つの要求規則を定義します。 d. ADFS Windows サービスを再開します。
Shibboleth	a. Unified Managerサーバの新しいFQDNをで更新します `attribute-filter.xml` および `relying-party.xml` ファイル。 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 経由で SAML 認証が想定どおりに機能することを確認します。

SAML 認証を無効にします

Unified Manager Web UI にログインするリモートユーザのセキュアなアイデンティティプロバイダ（ IdP ）による認証を中止する場合は、 SAML 認証を無効にします。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。

SAML 認証は、グラフィカルユーザインターフェイスにアクセスできない場合は Unified Manager メンテナンスコンソールを使用して無効にすることもできます。

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 *] チェックボックスをオフにします。
3. [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。

4. [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。

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 サーバの URI とメタデータを削除します。

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。

- 必要なもの *

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がサインオン認証を実行します。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 / 認証のページから無効にすることもできます。

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ます。

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 が再起動します。

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 URL とメタデータを削除します。

SAML Authentication ページ

SAML 認証ページを使用して、 Unified Manager の Web UI にログインするリモートユーザを SAML を使用して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 Unified Manager を設定できます。

- 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が完了したら、 SAML 認証を有効にするチェックボックスをオンにして、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 サーバから IdP にアクセスするための URI 。URI の例を次に示します。

  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 サーバから IdP の URL にアクセスできる場合は、「 * IdP メタデータの取得方法 * 」ボタンをクリックしてこのフィールドに値を入力できます。

- * 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 。この値は必要に応じて変更できます。

- *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

認証の管理

Unified Manager サーバで LDAP または Active Directory のいずれかを使用して認証を有効にし、サーバと連携してリモートユーザを認証するように設定することができます。

リモート認証の有効化、認証サービスのセットアップ、認証サーバの追加については、「 Unified Manager でアラート通知を送信するための設定」の前のセクションを参照してください。

認証サーバを編集しています

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。

- 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。

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 *] ボックスをオンにします。
3. [* 認証サーバ *] 領域で、編集する認証サーバを選択し、 [* 編集] をクリックします。
4. Edit Authentication Server* 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（ Save ）] をクリックします。

認証サーバを削除しています

Unified Manager サーバが認証サーバと通信できないようにするには、認証サーバを削除します。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は、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。

- 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。

認証サーバを削除すると、認証サーバのリモートユーザまたは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、 * 一般 * > * 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. [はい] をクリックして、削除要求を確定します。

[セキュアな接続を使用する *] オプションが有効になっている場合、認証サーバに関連付けられている証明書は認証サーバとともに削除されます。

Active Directory または OpenLDAP による認証

管理サーバでリモート認証を有効にし、管理サーバが認証サーバと通信するように設定すると、認証サーバ内のユーザが 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 の略

  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、適切な認証サーバを追加して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します。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。管理サーバでは、設定された認証サーバ内のリモートユーザの認証に 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については、管理サーバのデータベースでユーザ名とパスワードが管理されます。管理サーバで認証が実行され、 Active Directory 認証または OpenLDAP 認証が使用されることはありません。

監査ログ

監査ログを使用すると、監査ログが侵害されたかどうかを検出できます。ユーザが実行するすべてのアクティビティが監視され、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と公開されている API の機能に対して実行されます。

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してアクセスするには、*監査ログ：ファイルビュー*を使用します。監査ログ：ファイルビュー内のファイルは、作成日に基づいて一覧表示されます。このビューには、インストール時またはシステム内のにアップグレードされたときにキャプチャされたすべての監査ログの情報が表示されます。Unified Manager で何らかの操作を実行すると、情報が更新され、ログに記録されます。各ログファイルのステータスは、ログファイルの改ざんや削除を検出するためにアクティブに監視される「 File Integrity Status 」属性を使用して取得されます。システムで監査ログが使用可能になると、監査ログの状態は次のいずれかになります。

状態	説明
アクティブ	ログが現在ログに記録されているファイル。
正常	非アクティブで圧縮され、システムに格納されているファイル。

状態	説明
改ざんされた	手動でファイルを編集したユーザーによって侵害されたファイル。
manual_delete_delete	許可されたユーザー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移動したために削除されたファイル。
予期しない削除です	不明な理由で削除されたファイル。

Audit Log 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監査ログを削除できます。監査ログを削除したり、ファイルを削除する理由を指定したりできます。これにより、あとで有効な削除を確認するのに役立ちます。理由列には、削除操作を実行したユーザの名前と理由が表示されます。

ログファイルを削除すると、原因によって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。

監査ログは、監査ログセクションの * download * ボタンを使用して Active IQ Unified Manager からダウンロードし、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、圧縮された形式でダウンロードされます `.gzip` の形式で入力し

監査ログファイルは定期的にアーカイブされ、参照用にデータベースに保存されます。アーカイブの前に、監査ログはセキュリティと整合性を維持するためにデジタル署名されます。

フルAutoSupport バンドルの生成時に、サポート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。ただし、簡易サポートバンドルが生成されると、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。

監査ログを設定しています

監査ログセクションの *Configure * ボタンを使用して、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ギングを有効にしたりできます。

システムに保存するデータの量と頻度に応じて、 * 最大ファイルサイズ * と * 監査ログの保持日数 * の値を設定できます。フィールド * total audit log size * は、システムに存在する監査ログデータの合計サイズです。ロールオーバーポリシーは、「 * 監査ログの保持日数 * 」、「 * 最大ファイルサイズ * 」、および「 * 監査ログの合計サイズ * 」フィールドの値によって決まります。監査ログのバックアップのサイズが、監査ログの合計サイズ * 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。つまり、最も古いファイルが削除されます。しかし、ファイルエントリはデータベースで引き続き使用でき、「ロールオーバー削除」とマークされます。監査ログの保持日数 * は、監査ログファイルを保持する日数です。このフィールドに設定された値より古いファイルは、ロールオーバーされます。

手順

1. [* 監査ログ **>] > [** 構成 *] 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 * 、監査ログの保持日数 * の値を入力します。

   リモート・ロギングを有効にする場合は、 * リモート・ロギングを有効にする * を選択する必要があります。

監査ログのリモートロギングを有効にする

監査ログの設定ダイアログ・ボックスのリモート・ログを有効にするチェックボックスをオンにすると ' リモート監査ログを有効にできますこの機能を使用すると、監査ログをリモートの syslog サーバに転送できます。これにより、スペースに制約がある場合でも監査ログを管理できます。

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に備えて、改ざんを防止するためのバックアップ機能を提供します。

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オンにします。

   リモートロギングを設定するための追加フィールドが表示されます。

2. 接続先のリモートサーバの * 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 * をクリックしてターゲットサーバーのパブリック証明書を選択します。

   証明書はにアップロードする必要があります `.pem` の形式で入力しこの証明書は、ターゲットの syslog サーバから取得し、有効期限が切れていないことを確認する必要があります。証明書には、の一部として選択した「ホスト名」が含まれている必要があります `SubjectAltName` （SAN）属性。

4. 次のフィールドの値を入力します。 * charset* 、 * connection timeout * 、 * reconnection delay * 。

   これらのフィールドの値はミリ秒単位で指定します。

5. [**format**] フィールドと [**protocol**] フィールドで、必要な syslog 形式と TLS プロトコルのバージョンを選択します。
6. ターゲット Syslog サーバーで証明書ベースの認証が必要な場合は、 * 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の作成が必要になる場合があります。

   例：syslog-ngには、コマンドを使用して証明書の<hash>が作成されている必要があります `openssl x509 -noout -hash -in cert.pem`をクリックし、クライアント認証証明書を<hash>.0のあと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. サーバとの接続を設定し、リモートロギングを有効にするには、 * Save * をクリックします。

[監査ログ] ページに移動します。

の値は、設定に影響する可能性があります。設定が定義された値よりも応答に時間がかかると、接続エラーが原因で設定に失敗する可能性があります。正常な接続を確立するには、[接続タイムアウト]*の値を増やして、設定をやり直してください。

Remote Authentication ページの略

Remote Authentication 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にする] チェックボックスをオンにすると、認証サーバーを使用してリモート認証を有効にできます。

- * 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 *
    - 管理者の名前

      認証サーバの管理者名を指定します。

    - 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

      認証サーバでのリモートユーザの場所を指定します。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。

    - 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します

      認証サーバとの通信に使用す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

  認証サーバでのリモートユーザの場所を指定します。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。

- セキュアな接続を使用します

  LDAP認証サーバとの通信にSecure LDAPを使用することを指定します。

◦ * 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

  認証サーバでのリモートユーザの場所を指定します。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。

- 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。プロトコルのバージョンを自動的に検出するか、バージョン 2 または 3 に設定するかを指定できます。

- ユーザー名属性

  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*,_GroupオブジェクトClass_attributesに入力する値は、Active Directory、OpenLDAP、およびLDAPの設定に追加する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します

  認証サーバとの通信に使用す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してください。

Authentication Servers 領域

Authentication Servers 領域には、管理サーバがリモートユーザの検索および認証の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 *

  認証サーバを追加、編集、または削除できます。

  - 追加（ Add ）

    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、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。

  - 編集

    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。

- * 認証のテスト *

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の管理

Unified Manager サーバで HTTPS を設定することで、セキュアな接続を介してクラスタを監視および管理できるようになります。

HTTPS セキュリティ証明書の表示

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。

- 必要なもの *

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 Alternative Name （ SAN ）を表示したりできます。

ステップ

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

HTTPS 証明書ページに表示されるものよりも詳細なセキュリティ証明書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できます。

HTTPS 証明書署名要求のダウンロード

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。

- 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。

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 証明書署名要求のダウンロード *] をクリックします。
3. を保存します `<hostname>.csr` ファイル。

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 署名済みで返された HTTPS 証明書をインストールする

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。

- 必要なもの *

次の作業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、認証局によって署名されています
- 証明書チェーンを PEM 形式で保存します
- チェーンに含まれるすべての証明書について、 Unified Manager サーバ証明書からルート署名証明書への中間証明書も含めます

アプリケーション管理者のロールが必要です。

CSR 作成の証明書の有効期間が 397 日を超える場合、証明書の署名と返却の前に CA によって有効期間が 397 日に短縮されます

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 証明書のインストール * ］ をクリックします。
3. 表示される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探します。
4. ファイルを選択し、 * Install * をクリックしてファイルをインストールします。

   詳細については、を参照してください "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

"。

証明書チェーンの例

証明書チェーンファイルの表示例を次に示します。

```
-----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-----
```

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

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

秘密鍵と証明書チェーンをロードするのは、外部で生成された公開鍵と秘密鍵のペアであるためです。許可される鍵ペアアルゴリズムは「 RSA 」と「 EC 」です。［一般］ セクションの ［HTTPS 証明書］ ページで、 ［* HTTPS 証明書のインストール *］ オプションを使用できます。アップロードするファイルは、次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. ルートまでの CA の証明書（上記の証明書への署名に使用）

EC キーペアを含む証明書をロードするための形式

許可される曲線は "prime256v1" と "`ecp384r1" です。外部で生成された EC ペアを含む証明書の例：

```
 -----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キーペアを使用して証明書をロードする形式

ホスト証明書に属する RSA キーペアで使用できるキーサイズは、 2048 、 3072 、および 4096 です。外部で生成された * RSA キーペア * の証明書：

```
-----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有効にする必要があります。

外部で生成された証明書をアップロードする際にチェック

システムは、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際にチェックを実行します。いずれかのチェックに失敗すると、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含まれます。

- 入力された秘密鍵が、入力されたホスト証明書に照らして検証されます。
- ホスト証明書の Common Name （ CN ；共通名）とホストの FQDN の照合が行われます。

- ホスト証明書の Common Name （ CN ；共通名）を空または空白にしたり、 localhost に設定したりすることはできません。
- 有効開始日は将来の日付にすることはできません。また、証明書の有効期限は過去の日付にすることはできません。
- 中間 CA または CA が存在する場合、証明書の有効開始日を将来の日付にすることはできません。また、有効期限は過去の日付にすることはできません。

入力内の秘密鍵を暗号化しないでください。暗号化された秘密鍵がある場合、それらの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-----
```

証明書管理のページの説明

HTTPS 証明書ページを使用して、現在のセキュリティ証明書を表示したり、新しい HTTPS 証明書を生成したりできます。

HTTPS 証明書ページ

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 * をダウンロードします

  現在インストールされている HTTPS 証明書の証明書要求をダウンロードします。認証局にファイルを送信して署名を求めるプロンプトがブラウザに表示され、 <hostname> .CSR ファイルを保存します。

- * HTTPS 証明書をインストール *

  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。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 証明書の再生成 *

  現在のセキュリティ証明書に代わる新しい自己署名HTTPS証明書を生成できます。新しい証明書は、Unified Manager を再起動すると有効になります。

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。

[現在の証明書属性を使用して再生成] および [現在の証明書属性を更新] を選択すると ' 現在の情報で証明書を再生成するか ' 新しい情報で証明書を生成できます

- * 共通名 *

  必須保護する対象の完全修飾ドメイン名（ FQDN ）。

  Unified Manager のハイアベイラビリティ構成では、仮想 IP アドレスを使用します。

- * 電子メール *

  任意。組織に問い合わせるための E メールアドレス。通常は、証明書管理者または IT 部門の E メールアドレスです。

- * 会社名 *

  任意。通常は会社の法人名です。

- * 部門 *

  任意。社内の部署の名前。

- * 都市 *

  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、このサーバへのアクセスに使用できるプライマリ以外のドメイン名が追加されました。代行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 (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。

- * キーサイズ（キーアルゴリズム： RSA ） *

  キーアルゴリズムは rsa に設定されています。キーサイズは 2048 、 3072 、または 4096 のいずれかを選択できます。デフォルトのキー・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性が変更されていない可能性があります。

詳細については、を参照してください "HTTPS証明書の生成"。

著作権に関する情報

商標に関する情報