ユーザアクセスの管理

Active IQ Unified Manager 9.9

NetApp
December 15, 2023

目次

ユーザアクセスの管理

選択したクラスタオブジェクト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。クラスタ内の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。これらのユーザにのみ、クラスタオブジェクトを管理するためのアクセス権が付与されます。

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。

作業を開始する前に

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

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

このタスクについて

Windows Active Directory からグループを追加した場合は、ネストされたサブグループが無効になっていないかぎり、すべての直接メンバーとネストされたサブグループは Unified Manager で認証できます。OpenLDAP またはその他の認証サービスからグループを追加した場合は、そのグループの直接のメンバーだけが Unified Manager で認証されます。

手順

1. 左側のナビゲーションペインで、 * 一般 * > * ユーザー * をクリックします。
2. [**Users**]ページで、[**Add**]をクリックします。
3. [ユーザーの追加*]ダイアログボックスで、追加するユーザーのタイプを選択し、必要な情報を入力します。

   必要なユーザ情報を入力するときは、そのユーザに固有の E メールアドレスを指定する必要があります。複数のユーザで共有している E メールアドレスは指定しないでください。

4. [追加（ Add ）] をクリックします。

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。

作業を開始する前に

アプリケーション管理者のロールが必要です。

このタスクについて

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。

作業を開始する前に

アプリケーション管理者のロールが必要です。

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。

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。

作業を開始する前に

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

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

- アプリケーション管理者のロールが必要です。

手順

1. 左側のナビゲーションペインで、 * 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。

ローカルユーザのパスワードを変更しています

潜在的なセキュリティリスクを回避するために、ローカルユーザのログインパスワードを変更することができます。

作業を開始する前に

ローカルユーザとしてログインする必要があります。

このタスクについて

リモートユーザとメンテナンスユーザのパスワードについては、この手順では変更できません。リモートユーザのパスワードを変更するには、パスワード管理者に問い合わせてください。メンテナンスユーザのパスワードを変更する手順については、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. [パスワードの変更*]ダイアログボックスで、現在のパスワードと新しいパスワードを入力します。
4. [保存（ Save ）] をクリックします。

完了後

Unified Manager がハイアベイラビリティ構成の場合は、セットアップのもう一方のノードでパスワードを変更する必要があります。パスワードは両方のインスタンスで同じである必要があります。

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。

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	•	•	•	•	•
イベントを表示、割り当て、解決します	•	•	•		

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
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			•		
WFA との統合の管理とデータベースビューへのアクセス				•	

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
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					•

ユーザアクセスのウィンドウとダイアログボックスの概要

RBACの設定に基づいて、のユーザページでユーザを追加し、それらのユーザにクラスタへのアクセスや監視を許可する適切なロールを割り当てることができます。

ユーザーページ

[ユーザー]ページには、ユーザーとグループのリストが表示され、名前、ユーザーのタイプ、電子メールアドレスなどの情報が提供されます。このページでは、ユーザの追加、編集、削除、テストなどのタスクを実行することもできます。

コマンドボタン

選択したユーザについて、各コマンドボタンを使用して次のタスクを実行できます。

- * 追加 * 。

  Add Userダイアログボックスが表示されます。このダイアログボックスでは、ローカルユーザ、リモートユーザ、リモートグループ、またはデータベースユーザを追加できます。

  リモートのユーザまたはグループは、認証サーバが有効かつ設定済みである場合にのみ追加できます。

- * 編集 * 。

  ユーザの編集ダイアログボックスが表示され、選択したユーザの設定を編集できます。

- * 削除 *

  選択したユーザを管理サーバデータベースから削除します。

- * テスト *

リモートのユーザまたはグループが認証サーバに存在するかどうかを検証できます。

このタスクを実行できるのは、認証サーバが有効かつ設定済みである場合だけです。

リストビュー

リストビューには、作成されたユーザに関する情報が表形式で表示されます。列のフィルタを使用して、表示するデータをカスタマイズできます。

- * 名前 *

  ユーザまたはグループの名前が表示されます。

- * タイプ *

  ユーザのタイプ（ローカルユーザ、リモートユーザ、リモートグループ、データベースユーザ、またはメンテナンスユーザ）が表示されます。

- * 電子メール *

  ユーザのEメールアドレスが表示されます。

- * 役割 *

  ユーザに割り当てられているロールのタイプが表示されます。オペレータ、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、またはレポートスキーマです。

Add Userダイアログボックス

ローカルユーザまたはデータベースユーザを作成するか、リモートユーザまたはリモートグループを追加し、それらのユーザがストレージオブジェクトやデータをUnified Managerで管理できるようにロールを割り当てることができます。

ユーザを追加するには、次のフィールドを設定します。

- * タイプ *

  作成するユーザのタイプを指定できます。

- * 名前 *

  ユーザがUnified Managerへのログインに使用するユーザ名を指定できます。

- * パスワード *

  指定したユーザ名のパスワードを指定できます。このフィールドは、ローカルユーザまたはデータベースユーザを追加する場合にのみ表示されます。

- パスワードの確認

  パスワードフィールドに入力した内容が正確になるように、パスワードを再入力できます。このフィール

ドは、ローカルユーザまたはデータベースユーザを追加する場合にのみ表示されます。

- * 電子メール *

  ユーザのEメールアドレスを指定できます。ユーザ名ごとに一意のEメールアドレスを指定する必要があります。このフィールドは、リモートユーザまたはローカルユーザを追加する場合にのみ表示されます。

- * 役割 *

  ユーザにロールを割り当て、ユーザが実行できるアクティビティの範囲を定義できます。ロールは、アプリケーション管理者、ストレージ管理者、オペレータ、統合スキーマ、レポートスキーマのいずれかになります。

コマンドボタン

各コマンドボタンを使用して次のタスクを実行できます。

- * 追加 * 。

  ユーザを追加して、[Add User]ダイアログボックスを閉じます。

- * キャンセル *

  変更内容をキャンセルして、[Add User]ダイアログボックスを閉じます。

Edit User ダイアログボックス

Edit Userダイアログボックスでは、選択したユーザに応じて、特定の設定だけを編集できます。

詳細

詳細領域では、選択したユーザに関する次の情報を編集できます。

- * タイプ *

  このフィールドは編集できません。

- * 名前 *

  このフィールドは編集できません。

- * パスワード *

  データベースユーザを選択した場合、パスワードを編集できます。

- パスワードの確認

  データベースユーザを選択した場合、確認済みのパスワードを編集できます。

- * 電子メール *

選択したユーザのEメールアドレスを編集できます。このフィールドは、ローカルユーザ、LDAPユーザ、またはメンテナンスユーザを選択した場合のみ編集可能です。

- * 役割 *

  ユーザに割り当てられているロールを編集できます。このフィールドは、ローカルユーザ、リモートユーザ、またはリモートグループを選択した場合のみ編集可能です。

コマンドボタン

各コマンドボタンを使用して次のタスクを実行できます。

- * 保存 *

  変更内容を保存して[Edit User]ダイアログボックスを閉じます。

- * キャンセル *

  変更内容をキャンセルして[Edit User]ダイアログボックスを閉じます。