



# ユーザアクセスの管理

## OnCommand Unified Manager 9.5

NetApp  
October 23, 2024

# 目次

ユーザアクセスの管理	1
ユーザを追加する	1
ユーザ設定の編集	2
リモートユーザまたはリモートグループをテストする	2
ユーザの表示	3
ユーザまたはグループを削除する	3
ローカルユーザのパスワードを変更しています	3
メンテナンスユーザの役割	4
RBAC とは	4
ロールベースアクセス制御の機能	4
ユーザタイプの定義	5
ユーザロールの定義	6
Unified Manager のユーザロールと機能	7
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	8

# 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

管理/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

- OnCommand 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. ツールバーで、 をクリックし、左の[管理]メニューの[\*ユーザー]をクリックします。
2. [\* Management/Users\* (管理/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。

## 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

OnCommand 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. ツールバーで、 をクリックし、左の[管理]メニューの[\*ユーザー]をクリックします。
2. [管理/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。

## リモートユーザまたはリモートグループをテストする

認証サーバに指定された認証設定を使用してリモートユーザまたはリモートグループが Unified Manager サーバにアクセスできることを検証できます。

作業を開始する前に

- リモートユーザまたはリモートグループを Unified Manager サーバで検証できるように、リモート認証を有効にし、認証を設定しておく必要があります。
- OnCommand 管理者のロールが必要です。

手順

1. ツールバーで、 をクリックし、左の[管理]メニューの[\*ユーザー]をクリックします。
2. [\* Management/Users\* (管理/ユーザー\*) ] ページで、検証するリモートユーザまたはリモートグループを選択し、[\* Test\* (テスト\*) ] をクリックします。

## ユーザの表示

管理/ユーザページでは、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

OnCommand 管理者のロールが必要です。

### 手順

1. ツールバーで、をクリックします  \*をクリックし、左の[管理]メニューの[\*ユーザー]をクリックします。

ユーザのリストが[Management/Users]ページに表示されます。

## 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。

- OnCommand 管理者のロールが必要です。

### 手順

1. ツールバーで、をクリックします  \*をクリックし、左の[管理]メニューの[\*ユーザー]をクリックします。
2. [管理/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お問い合わせください。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 "[Maintenance Console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OnCommand 管理者のロールを割り当てられ、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、OnCommand Unified Managerサーバのさまざまな機能やリソースにアクセスす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、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、OnCommand 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 OnCommand 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する必要があります。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 OnCommand 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OnCommand 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。

- \* OnCommand 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すると、OnCommand 管理者ロールが割り当てられた最初のユーザには「umadmin」という名前が自動的に付けられます。

- \* 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	OnCommand 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	•	•	•		
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		•	•		

機能	演算子	ストレージ管理 者	OnCommand 管理者	統合スキーマ	レポートスキーマ
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				•	
レポートおよび その他のデータ ベースビューに 読み取り専用ア クセスを提供し ます					•
レポートのスケ ジュール設定と 保存	•	•	•		
インポートした レポートをイン ポートおよび削 除します			•		

## 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、管理/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。

## [管理／ユーザー] ページ

[Management/Users]ページには、ユーザとグループのリストが表示され、名前、ユーザのタイプ、Eメールアドレスなどの情報が示されます。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、OnCommand 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、OnCommand 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。

## 著作権に関する情報

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および/または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用権を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用権については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

## 商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。