RBAC の設定

ここでは、次の内容について説明します。

RBAC

ロールベース アクセス コントロール（RBAC）は、ユーザのロールとロケールに基づいてユーザのシステムアクセスを制限または許可する方法です。 ロールによってシステム内でのユーザの権限が定義され、ロケールによってユーザがアクセス可能な組織（ドメイン）が定義されます。 権限がユーザに直接割り当てられることはないため、個々のユーザ権限の管理では、適切なロールとロケールを割り当てることが主な作業になります。

必要なシステム リソースへの書き込みアクセス権限がユーザに与えられるのは、割り当てられたロールによりアクセス権限が与えられ、割り当てられたロケールによりアクセスが許可されている場合に限ります。 たとえば、エンジニアリング組織内のサーバ管理者ロールを持つユーザは、エンジニアリング組織内のサーバ設定を更新できますが、そのユーザに割り当てられたロケールに財務組織が含まれていなければ、財務組織内のサーバ設定を更新できません。

VNMC のユーザ アカウント

ユーザ アカウントは、システムにアクセスするために使用されます。 各 VNMC インスタンスで、最大 128 個のローカル ユーザ アカウントを設定できます。 各ユーザ アカウントには、一意のユーザ名が必要です。

ローカル ユーザは、パスワードまたは SSH 公開キーを使用して認証できます。 公開キーは、OpenSSH と SECSH のいずれかの形式で設定できます。

デフォルトのユーザ アカウント

各 VNMC インスタンスには、変更も削除もできないデフォルトのユーザ アカウント admin が存在します。 このアカウントは、システム管理者またはスーパーユーザ アカウントであり、すべての権限が与えられています。 admin アカウントには、デフォルトのパスワードは割り当てられません。初期システム セットアップ時にパスワードを選択する必要があります。

ユーザ アカウントの有効期限

ユーザ アカウントは、事前に定義した時間に有効期限が切れるように設定できます。 有効期限の時間になると、ユーザ アカウントはディセーブルになります。

デフォルトでは、ユーザ アカウントの有効期限はありません。

VNMC ユーザ名のガイドライン

ユーザ名は、VNMC のログイン ID としても使用されます。 VNMC ユーザ アカウントにユーザ名を割り当てるときは、次のガイドラインおよび制約事項を考慮してください。

- ログイン ID には、次を含む 1 ～ 32 の文字を含めることができます。
  - 任意の英数字文字
  - ピリオド（.）
  - アンダースコア（_）
  - ハイフン（-）
  - アットマーク（@）
- 一意のユーザ名もローカル ユーザのユーザ名も数字のみでは構成できません。
- 一意のユーザ名の先頭を数字にすることはできません。
- AAA サーバ（LDAP）にすべて数字のユーザ名が存在し、ログイン時にこのユーザ名が入力された場合、VNMC はユーザをログインさせることができません。

ユーザ アカウントの作成後は、ユーザ名を変更できません。 ユーザ アカウントを削除し、新しいユーザ アカウントを作成する必要があります。

（注） 1 つの VNMC インスタンスには、最大 128 個のユーザ アカウントを作成できます。

VNMC パスワードのガイドライン

認証上の理由により、各ユーザアカウントにはパスワードが必要です。ユーザが安全性の低いパスワードを選択しないように、強力なパスワードを要求する必要があります。 [Password Strength Check] オプションがイネーブルになっている場合、VNMC は次の要件を満たさないパスワードを拒否します。

- 最低 8 文字を含む。
- 次の少なくとも 3 種類を含む。
  - 小文字の英字
  - 大文字の英字
  - 数字
  - 特殊文字
- aaabbb など連続して 3 回を超えて繰り返す文字を含まない。
- ユーザ名と同一、またはユーザ名を逆にしたものではない。
- パスワード ディクショナリ チェックに合格する。 たとえば、パスワードには辞書に記載されている標準的な単語に基づいたものを指定することはできません。
- 次の記号を含まない。ドル記号（$）、疑問符（?）、等号（=）。
- ローカル ユーザ アカウントおよび admin アカウントのパスワードは空白にしない。

（注） [Password Strength Check] オプションはデフォルトでイネーブルになっています。 [Locally Authenticated Users] ペイン（[Administration] > [Access Control] > [Locally Authenticated Users]）からディセーブルにできます。

（注） VNMC が、LDAP でリモート認証を使用するように設定されている場合、これらのリモート アカウントのパスワードは空白にできます。 この設定では、リモート クレデンシャル ストアは認証だけに使用され、許可には使用されません。 ローカル ユーザ ロールの定義は、リモート認証されたユーザに適用されます。

VNMC のユーザ ロール

ユーザ ロールには、そのロールを割り当てられたユーザに対して許可される操作を定義した 1 つ以上の権限が含まれます。 ユーザには、ロールを 1 つ以上割り当てることができます。 複数のロールを割り当てられたユーザは、すべての割り当てロールを組み合わせた権限を持ちます。 たとえば、Role1 にポリシー関連の権限が含まれ、Role2 にテナント関連の権限が含まれている場合、Role1 と Role2 の両方を割り当てられたユーザは、ポリシー関連の権限とテナント関連の権限を持つことになります。

すべてのロールには、VNMC インスタンス内のすべての設定に対する読み取りアクセス権限が含まれています。 読み取り専用ロールと他のロールとの違いは、読み取り専用ロールのみを割り当てられたユーザは、システム状態を変更できないことです。 別のロールを割り当てられたユーザは、そのユーザの割り当て領域においてシステム状態を変更できます。

システムには、次のデフォルトのユーザ ロールが用意されています。

aaa

ユーザには、ユーザ、ロール、および AAA 設定への読み取りおよび書き込みアクセス権があり、残りのシステムに読み取りアクセス権があります。

admin

ユーザには、システム全体への読み取りおよび書き込みアクセス権があり、ほとんどの権限があります。 ただし、ユーザはファイルを作成または削除したり、システムをアップグレードしたりすることはできません。 これらの機能は、デフォルトの admin アカウントでのみ行うことができます。 デフォルトの admin アカウントには、デフォルトでこのロールが割り当てられ、変更できません。

ネットワーク

ユーザは、組織、セキュリティ ポリシー、およびデバイス プロファイルを作成します。

operations

ユーザは障害を確認し、ロギング設定などの基本的な操作を実行します。

read-only

ユーザにはシステム設定および動作ステータスへの読み取り専用アクセス権はありますが、操作を実行する権限はありません。

ロールは、作成、変更（新しい権限の追加や既存の権限の削除）、および削除できます。 ロールを変更すると、そのロールに割り当てられているすべてのユーザに新しい権限が適用されます。 権限の割り当ては、デフォルト ロールに定義されている権限に限定されません。 つまり、カスタムの権限の組み合わせを使用して、独自のロールを作成できます。 たとえば、デフォルトの Network および Operations ロールには異なる権限のセットがありますが、両方のロールの権限を組み合わせた新しい Network および Operations ロールを作成できます。

ロールがユーザへの割り当て後に削除されると、それらのユーザ アカウントからも削除されます。

ロケール ユーザへのロールとロケールの割り当ては、VNMC で変更できます。 リモート ユーザへのロールとロケールの割り当ては、LDAP で変更できます。 ユーザに割り当てられた次のいずれかの情報を変更する場合、管理者は、新しい権限が有効になるように、そのユーザの既存のセッションをすべて削除する必要があります。

- Role
- ロールの権限
- ロケール
- ロケール内の組織

Privileges

ユーザの権限

ユーザ ロールを割り当てられたユーザは、権限により、特定のシステム リソースへアクセスしたり、特定のタスクを実行したりできるようになります。 次の表に各権限とその説明を一覧表示します。

権限の名前	説明
AAA	システム セキュリティおよび AAA。
Admin	システム管理。
read-only	読み取り専用アクセス権。 読み取り専用は、権限として選択できません。この権限は、すべてのユーザ ロールに割り当てられます。
Resource Configuration	エッジ ファイアウォールおよびコンピュート ファイアウォールの設定。
Policy Management	エッジ ファイアウォールおよびコンピュート ファイアウォールのポリシー。
Fault Management	アラームおよびアラーム ポリシー。
Operations	ログ、コア ファイル管理、および **show tech-support** コマンド。

権限の名前	説明
Tenant Management	テナントおよび組織コンテナの作成、削除、変更。

権限とロールの割り当て

次の表に各権限のデフォルトのロール名（そのまま使用可）を一覧表示します。

デフォルトのロール名	権限の名前
aaa	aaa
admin	admin
network	policy, res-config, tenant
operations	fault, operations
read-only	read-only

ユーザ ロケール

ユーザには、ロケールを 1 つ以上割り当てることができます。 各ロケールでは、ユーザにアクセスを許可する 1 つ以上の組織またはドメイン（総称してリソースと呼ばれる）を定義します。 さらに、ユーザには割り当てられたロケール外や組織ツリーの上部での読み取り専用のアクセス権限があります。 これにより、ユーザはポリシーの作成時にこれらのリソースを使用できます。 このルールの 1 つの例外として、組織が指定されていないロケールがあります。この場合、すべての組織内のシステム リソースに対して無制限のアクセスが可能になります。 組織の下にあるオブジェクトだけがロケールによって制御されます。 組織ツリーに存在しないユーザ、ロール、およびリソースなどの他のオブジェクトへのアクセスは、ロケールの影響を受けません。

AAA 管理者権限（AAA 管理者ロール）を持つユーザは、他のユーザのロケールに組織を割り当てることができます。 組織の割り当ては、それを行うユーザのロケール内の組織だけに制限されます。 たとえば、ロケールにエンジニアリング組織しか含まれていない場合、そのロケールを割り当てられたユーザは、他のユーザにエンジニアリング組織のみを割り当てることできます。

（注） AAA 権限を持つユーザは、他のユーザの権限とロールの割り当てを管理できるので、この権限は慎重に割り当てる必要があります。

組織は階層的に管理できます。 トップ レベルの組織に割り当てられたユーザは、自動的にその下にあるすべての組織にアクセスできます。 たとえば、エンジニアリング組織が、ソフトウェア エンジニアリング組織とハードウェア エンジニアリング組織で構成されているとします。 ソフト

ウェア エンジニアリング組織のみを含むロケールでは、その組織内のシステム リソースにしかアクセスできません。一方、エンジニアリング組織が含まれるロケールでは、ソフトウェア エンジニアリング組織とハードウェア エンジニアリング組織の両方のリソースにアクセスできます。

ロケール ユーザへのロールとロケールの割り当ては、VNMC で変更できます。 リモート ユーザへのロールとロケールの割り当ては、LDAP で変更できます。 ユーザに割り当てられた次のいずれかの情報を変更する場合、管理者は、新しい権限が有効になるように、そのユーザの既存のセッションをすべて削除する必要があります。

- Role
- ロールの権限
- ロケール
- ロケール内の組織

ユーザ ロールの設定

ユーザ ロールの作成

手順

ステップ 1 [Administration] > [Access Control] > [Roles] を選択します。

ステップ 2 [Create Role] をクリックします。

ステップ 3 [Create Role] ダイアログボックスで、次のフィールドに値を入力し、[OK] をクリックします。

フィールド	説明
Name	ユーザ ロール名です。

フィールド	説明
Privileges	使用可能な権限。選択したロールに権限を割り当てるには、次のチェックボックスのうち 1 つ以上をオンにします。 • Admin • AAA • Fault Management • Operations • Policy Management • Resource Configuration • Tenant Management （注） すべての権限を持つ admin 権限を割り当てるか、個別に権限を割り当てることができます。

ユーザ ロールの編集

手順

ステップ 1 [Administration] > [Access Control] > [Roles] を選択します。

ステップ 2 編集するロールを選択し、[Edit] をクリックします。

ステップ 3 [Edit] ダイアログボックスで、ロールを追加する権限の各チェックボックスをオンまたはオフにし、[OK] をクリックします。

ユーザ ロールの削除

admin および読み取り専用ロールを除き、環境に適切でないユーザ ロールを削除できます。

手順

ステップ 1 [Administration] > [Access Control] > [Roles] を選択します。

ステップ 2 削除するユーザ ロールを選択し、[Delete] をクリックします。

（注） admin または読み取り専用ロールは削除できません。

ステップ 3 [Confirm] ダイアログボックスで、[Yes] をクリックします。

ユーザ ロケールの設定

ロケールの作成

はじめる前に

ロケールを作成するには、1 つ以上の組織が存在する必要があります。

手順

ステップ 1 [Administration] > [Access Control] > [Locales] を選択します。

ステップ 2 [Create Locale] をクリックします。

ステップ 3 [Create Locale] ダイアログボックスで、次のフィールドに値を入力し、[OK] をクリックします。

フィールド	説明
Name	ロケール名。 この名前には、ID となる 1 ～ 256 文字を使用できます。ハイフン、アンダースコア、ドット、コロンを含む英数文字を使用できます。保存後は、この名前を変更できません。
Description	ロケールの簡単な説明。 このフィールドには、1 ～ 256 文字を使用できます。ハイフン、アンダースコア、ドット、コロンを含む英数文字を使用できます。
Assigned Organizations	
Assign Organization	クリックすると、組織をロケールに割り当てることができます。

フィールド	説明
Assigned Organization	既存の組織から成るリスト。

次の作業

ロケールを 1 つまたは複数のユーザ アカウントに追加します。詳細については、ローカル認証されたユーザ アカウントに割り当てられたロケールの変更, （16 ページ）を参照してください。

ロケールの編集

手順

ステップ 1 [Administration] > [Access Control] > [Locales] を選択します。

ステップ 2 ロケールのリストで、編集するロケールをクリックし、[Edit] をクリックします。

ステップ 3 [Description] フィールドで、必要に応じて説明を変更します。

ステップ 4 [Assign Organization] をクリックします。

ステップ 5 [Assign Organization] ダイアログボックスで、次の手順を実行します。

a) [root] ノードを展開して、利用可能な組織を表示します。

b) ロケールに割り当てる組織のチェックボックスをオンにします。

ステップ 6 開いているダイアログボックスの [OK] ボタンをクリックして、変更内容を保存します。

ロケールの削除

はじめる前に

注意 削除するロケールが任意のユーザに割り当てられている場合は、ロケールのユーザ リストからそのロケールを削除します。

手順

ステップ 1 [Navigation] ペインの [Administrationr] タブをクリックします。
ステップ 2 [Navigation] ペインの [Access Control] サブタブをクリックします。
ステップ 3 [Navigation] ペインで、[Locales] ノードをクリックします。
ステップ 4 [Work] ペインで、削除するロケールをクリックします。
ステップ 5 [Delete] をクリックします。
ステップ 6 [Confirm] ダイアログボックスで、[Yes] をクリックします。

ロケールへの組織の割り当て

手順

ステップ 1 [Administration] > [Access Control] > [Locales] を選択します。
ステップ 2 必要なロケールを選択し、[Assign Organization] をクリックします。
ステップ 3 [Assign Organization] ダイアログボックスで、次の手順を実行します。
a) [root] を展開して利用可能な組織を表示します。
b) ロケールを追加する組織のチェックボックスをオンにします。
ステップ 4 開いているダイアログボックスで [OK] をクリックし、[Save] をクリックしてロケールをクリックします。

ロケールからの組織の削除

手順

ステップ 1 [Navigation] ペインの [Administrationr] タブをクリックします。
ステップ 2 [Navigation] ペインの [Access Control] サブタブをクリックします。
ステップ 3 [Navigation] ペインで、[Locales] を展開します。
ステップ 4 [Work] ペインで、[General] タブをクリックします。
ステップ 5 [Assigned Organizations] 領域で、削除する組織をクリックします。
ステップ 6 [Delete Organization] リンクをクリックします。
ステップ 7 [Confirm] ダイアログボックスで、[Yes] をクリックします。

ローカル認証されたユーザ アカウントの設定

ユーザ アカウントの作成

手順

ステップ 1 [Administration] > [Access Control] > [Locally Authenticated Users] を選択します。

ステップ 2 [Create Locally Authenticated Users] をクリックします。

ステップ 3 [Properties] 領域で、次のフィールドに値を入力します。

フィールド	説明
Login ID	ログイン名 この名前は固有であるとともに、VNMCユーザ アカウントに関する次のガイドラインと制約事項を満たしている必要があります。 • ログイン ID には、次を含む 1 ～ 32 の文字を含めることができます。 ◦任意の英数字文字 ◦アンダースコア（_） ◦ハイフン（-） ◦アットマーク（@） • 各ユーザ アカウントのユーザ名をすべて数字にすることはできません。 • また、ユーザ名の先頭を数字にすることはできません。 ユーザ名を保存した後に変更することはできません。ユーザアカウントを削除し、新しいユーザ アカウントを作成する必要があります。
Description	ユーザの説明。
First Name	ユーザの名。 このフィールドには、32 文字までの値を入力できます。

フィールド	説明
Last Name	ユーザの姓。 このフィールドには、32 文字までの値を入力できます。
Email	ユーザの電子メール アドレス。
Phone	ユーザの電話番号。

フィールド	説明
Password	このアカウントに関連付けられているパスワード。 セキュリティを最大限にするため、強力なパスワードにする必要があります。 [Password Strength Check] チェックボックスがオンになっている場合、システムは次の要件を満たさないパスワードを拒否します。 • 最低 8 文字を含む。 • 次のうち、少なくとも 3 種類を含む。 ◦ 小文字の英字 ◦ 大文字の英字 ◦ 数字 ◦ 特殊文字 • aaabbb など連続して 3 回を超えて繰り返す文字を含まない。 • ユーザ名と同一、またはユーザ名を逆にしたものではない。 • パスワード ディクショナリ チェックに合格する。 たとえば、パスワードには辞書に記載されている標準的な単語に基づいたものを指定することはできません。 • 次の記号を含まない。ドル記号（$）、疑問符（?）、等号（=）。 • ローカル ユーザ アカウントおよび admin アカウントのパスワードは空白にしない。 （注） [Locally Authenticated Users] ペインの [password strength] チェックボックスをオフにすると、強力なパスワードを必要としなくなることを示します。 ただし、最低 8 文字を含んでいる必要があります。 パスワード フィールドは必須フィールドであるため、ユーザを作成するにはパスワードを指定する必要があります。

フィールド	説明
Confirm Password	確認のために新しいパスワードを再入力します。
Password Expires	パスワード有効期間をイネーブルにするかどうか。パスワード有効期間をイネーブルにするには、このチェックボックスをオンにします。
Expiration Date	パスワード有効期間をイネーブルにした場合に使用できます。 パスワードが期限切れになる日付です。

ステップ 4 [Roles/Locales] タブ領域で、次のフィールドに値を入力します。

フィールド	説明
Assigned Roles	ユーザに 1 つまたは複数のロールを割り当てるには、該当するチェックボックスをオンにします。 • aaa • admin • network • operations • read-only
Assigned Locale	ユーザに 1 つまたは複数のロケールを割り当てるには、該当するチェックボックスをオンにします。

ステップ 5 [SSH] タブ領域で、次のフィールドに値を入力します。

フィールド	説明
Key	SSH キー [Key] オプション ボタンを選択すると、[SSH Data] フィールドが表示されます。
Password	SSH パスワード。

フィールド	説明
SSH Data	[Key] を選択した場合に使用できます。 SSH 公開キーを入力します。

ステップ 6 [OK] をクリックします。

ローカル認証されたユーザアカウントに割り当てられたロケールの変更

手順

ステップ 1 [Navigation] ペインの [Administrationr] タブをクリックします。

ステップ 2 [Navigation] ペインの [Access Control] サブタブをクリックします。

ステップ 3 [Navigation] ペインで、[Locally Authenticated Users] ノードを展開します。

ステップ 4 *User_name*（ロケールを修正するユーザ アカウントのユーザ名を選択）をクリックします。

ステップ 5 [Work] ペインで、[General] タブをクリックします。

ステップ 6 [Work] ペインで、[Roles/Locales] タブをクリックします。

ステップ 7 [Assigned Locale(s)] 領域で、次の手順を実行します。

- ユーザアカウントに新しいロケールを割り当てるには、適切なチェックボックスをオンにします。
- ユーザアカウントからロケールを削除するには、適切なチェックボックスをオフにします。

ステップ 8 [Save] をクリックします。

ローカル認証されたユーザアカウントに割り当てられたロールの変更

手順

ステップ 1 [Navigation] ペインの [Administrationr] タブをクリックします。

ステップ 2 [Navigation] ペインの [Access Control] サブタブをクリックします。

ステップ 3 [Navigation] ペインで、[Locally Authenticated Users] ノードを展開します。

ステップ 4 *User_name*（ロケールを修正するユーザ アカウントのユーザ名を選択）をクリックします。

ステップ 5 [Work] ペインで、[General] タブをクリックします。

ステップ 6 [Roles/Locales] タブをクリックします。

ステップ 7 [Assigned Role(s)] 領域で、次の手順を実行します。

- ユーザ アカウントに新しいロールを割り当てるには、適切なチェックボックスをオンにします。
- ユーザ アカウントからロールを削除するには、適切なチェックボックスをオフにします。

ステップ 8 [Save] をクリックします。

ユーザ セッションのモニタリング

ローカル認証されたユーザとリモート認証されたユーザの両方について、セッションをモニタできます。

手順

ステップ 1 [Administration] > [Access Control] を選択し、次のいずれかを選択します。

- [Locally Authenticated Users] > [user]。
- [Remotely Authenticated Users] > [*user*]。

ステップ 2 [Sessions] タブをクリックしてユーザ セッションを表示します。

フィールド	説明
Host	ユーザのログイン元である IP アドレス。
Login Time	セッションが開始された日時。

フィールド	説明
UI	このセッションのユーザ インターフェイス： • [web]：GUI ログイン • [shell]：CLI ログイン • [ep]：エンド ポイント • なし
Terminal Type	ユーザがログインするときに使用する端末の種類。