ロールベース アクセス コントロール

表 *1*: 機能の履歴

機能名	リリース情報	説明
リソースグループによるロールベースアクセス コントロール	Cisco IOS XE リリース 17.5.1a Cisco vManage リリース 20.5.1	この機能により、サイトまたはリソースグループに基づいたロールベース アクセス コントロール（RBAC）が導入されます。これは、ユーザーグループとリソースグループの組み合わせに基づいて、ユーザーのシステムアクセスを承認する方法です。 複数の地理的な場所にまたがる大規模なCisco SD-WAN展開の場合、この機能は、ネットワーク管理を異なる地域管理者間で分割するのに役立ちます。
ポリシーに対する RBAC	Cisco IOS XE リリース 17.6.1a Cisco vManage リリース 20.6.1	この機能を使用すると、Cisco vManage ポリシーに必要な読み取りおよび書き込み権限を持つユーザーおよびユーザーグループを作成できます。ポリシーに対する RBAC は、運用効率を最大化するのに役立つポリシーのすべての詳細へのアクセスをユーザーに提供します。これにより、構成要件を満たすことが容易になり、システム上の許可されたユーザーに必要なものへのアクセスのみが許可されることが保証されます。

機能名	リリース情報	説明
共同管理：機能テンプレートのきめ細かいロールベースアクセスコントロール	Cisco vManage リリース 20.7.1	この機能により、テンプレートの使用にあたって RBAC によるアクセス許可をより細分化して割り当てられるようになり、テナントに自己管理によるネットワーク構成タスクを与えることができます。ネットワーク管理者やマネージドサービスプロバイダーはこの機能を使ってエンドカスタマーにアクセス許可を割り当てることができます。
共同管理：きめ細かい構成タスクのアクセス許可の改善	Cisco vManage リリース 20.9.1	ユーザーが特定の構成タスクを自己管理できるようにするために、他のタスクを除外しながら、特定の構成タスクを実行する権限をユーザーに割り当てることができます。 この機能により、多数の新しいアクセス許可オプションが導入され、ユーザーに提供する構成タスクのアクセス許可をきめ細かく決定できます。
セキュリティ操作およびネットワーク操作のデフォルトのユーザーグループに対する RBAC	Cisco vManage リリース 20.9.1	この機能は、次のデフォルトのユーザーグループを提供します。 • 非セキュリティポリシー用の network_operations ユーザーグループ • セキュリティポリシー用の security_operations ユーザーグループ ポリシーに対する RBAC を使用すると、セキュリティポリシーと非セキュリティポリシーに必要な読み取りおよび書き込みアクセス許可を持つユーザーとユーザーグループを作成できます。ユーザーは、承認されたポリシータイプに対してのみ構成およびモニタリングアクションを実行できます。

- RBAC に関する情報 （3 ページ）
- RBAC の制約事項 （17 ページ）
- RBAC の設定 （18 ページ）
- CLI を使用した RBAC の設定 （47 ページ）
- RBAC の確認 （49 ページ）
- RBAC のモニタリング （49 ページ）

RBAC に関する情報

VPN によるロールベース アクセス コントロール

ロールベースアクセスコントロール（RBAC）は、ネットワーク設定およびリソースへのユーザーアクセスを制限するプロセスです。RBACでは、アクセスが必要なリソースに応じてユーザーにロールを割り当てます。VPN による RBAC 機能は、VPN に基づいてネットワークへのアクセスを管理および制御するのに役立ちます。これには、権限を持つユーザーがアクセスできるようにするアクセス許可と権限の設定が含まれます。

VPN による RBAC

VPNによるロールベースアクセスにより、ネットワーク管理者は1つ以上のネットワークセグメントを持つ VPN グループを定義できます。ネットワーク管理者は、ネットワーク内のデバイスおよびCisco vManageの機能へのユーザーアクセスを制限するVPNグループにユーザーを関連付けることができます。

VPN による RBAC は、VPN グループが設定されたユーザーに次の制限付きアクセスを提供します。

- VPN ダッシュボードへのアクセス
- VPNダッシュボードを介したデバイス、ネットワーク、およびアプリケーションのステータスのモニタリング
- VPN グループ内のセグメントを持つデバイスに制限された VPN ダッシュボード情報
- VPN グループ内のセグメントを持つデバイスに制限されたモニタリングオプション
- VPNグループ内のセグメントのインターフェイスに制限された各デバイスのインターフェイス モニタリング

VPN ダッシュボードの概要

VPN グループで設定されたユーザーは、VPN ダッシュボードにのみアクセスでき、読み取り専用アクセスになります。管理者アクセスのあるユーザーは、VPNグループを作成でき、管理ダッシュボードと VPN ダッシュボードの両方にアクセスできます。管理ユーザーは、Cisco vManage のメニューから [Dashboard] を選択して、これらのダッシュボードにアクセスできます。

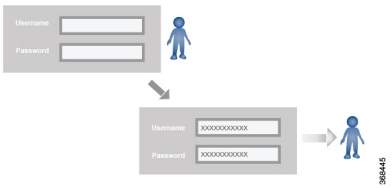
AAA を使用したロールベースアクセス

Cisco SD-WAN AAA ソフトウェアは、ロールベースのアクセスを実装して、Cisco IOS XE SD-WAN デバイス のユーザーの認可権限を制御します。ロールベースのアクセスは、次の 3 つのコンポーネントで構成されます。

- ユーザーは、Cisco IOS XE SD-WAN デバイス へのログインが許可されているユーザーです。
- ユーザーグループは、ユーザーのコレクションです。
- 権限は各グループに関連付けられています。これらは、グループのユーザーが発行を許可されているコマンドを定義します。

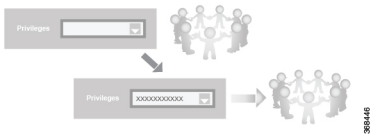
ユーザーとユーザーグループ

Cisco IOS XE SD-WAN デバイス での操作の実行が許可されているすべてのユーザーは、ログインアカウントを持っている必要があります。ログインアカウントについては、デバイス自体でユーザー名とパスワードを設定します。これらにより、ユーザーはそのデバイスにログインできます。ユーザーがアクセスを許可されている各デバイスで、ユーザー名とパスワードを設定する必要があります。



Cisco SD-WAN ソフトウェアは、UNIX スーパーユーザーと同様な、完全な管理者権限を持つユーザーである **admin** という 1 つの標準ユーザー名を提供します。デフォルトでは、**admin** ユーザー名のパスワードは **admin** です。このユーザー名を削除または変更することはできませんが、デフォルトのパスワードは変更できますし、変更する必要があります。

ユーザーグループは、Cisco IOS XE SD-WAN デバイス で共通のロールまたは権限を持つユーザーをプールします。ログインアカウント情報の構成の一環として、ユーザーがメンバーであるユーザーグループを指定します。**admin** ユーザーのグループを指定する必要はありません。このユーザーは自動的にユーザーグループ **netadmin** に属し、Cisco IOS XE SD-WAN デバイスでのすべての操作の実行が許可されるためです。



ユーザーグループ自体は、そのグループに関連付けられた権限を設定する場所です。これらの権限は、ユーザーが実行を許可されている特定のコマンドに対応し、Cisco SD-WAN ソフトウェア要素への役割ベースのアクセスを効果的に定義します。

Cisco SD-WAN ソフトウェアは、次の標準ユーザーグループを提供します。

- [basic]：[basic] グループは設定可能なグループであり、任意のユーザーおよび権限レベルに使用できます。このグループは、デバイス上の情報を表示および変更する権限を持つユーザーを含むように設計されています。
- [operator]：[operator] グループも設定可能なグループであり、任意のユーザーおよび権限レベルに使用できます。このグループは、情報を表示する権限のみを持つユーザーを含むように設計されています。
- [netadmin]：[netadmin] グループは設定不可能なグループです。デフォルトでは、このグループには**admin**ユーザーが含まれます。このグループに他のユーザーを追加できます。このグループのユーザーは、デバイスですべての操作を実行できます。
- サポート対象の最小リリース：Cisco vManage リリース 20.9.1

  [network_operations]：[network_operations] グループは設定不可能なグループです。このグループのユーザーは、デバイス上でセキュリティポリシー以外のすべての操作を実行でき、セキュリティポリシー情報は表示のみが可能です。たとえば、ユーザーはテンプレート設定を作成または変更し、災害復旧を管理し、アプリケーション対応ルーティングポリシーや CFlowD ポリシーなどの非セキュリティポリシーを作成できます。
- サポート対象の最小リリース：Cisco vManage リリース 20.9.1

  [security_operations]：[security_operations] グループは設定不可能なグループです。このグループのユーザーは、デバイス上ですべてのセキュリティ操作を実行でき、セキュリティポリシー以外の情報は表示のみが可能です。たとえば、ユーザーはUmbrellaキー、ライセンス、IPS 署名の自動更新、TLS/SSL プロキシ設定などを管理できます。

[network_operations] グループのユーザーは、デバイスへのポリシーの適用、適用されたポリシーの取り消し、およびデバイステンプレートの編集を許可されています。[security_operations] グループのユーザーは、デバイスにセキュリティポリシーを展開するために、[network_operations] ユーザーによる 0 日目の介入と、展開されたセキュリティポリシーを削除するために、N 日目の介入が必要です。ただし、セキュリティポリシーがデバイスに展開された後は、[security_operations] ユーザーは、[network_operations] ユーザーの介入を必要とせずにセキュリティポリシーを変更できます。

（注） 実行中の設定およびローカル設定を表示できるのは管理ユーザーのみです。事前定義された [operator] ユーザーグループに関連付けられたユーザーは、実行中の設定およびローカル設定にアクセスできません。事前定義されたユーザーグループ [operator] には、テンプレート設定の読み取りアクセスのみがあります。管理者ユーザー権限のサブセットのみが必要な場合は、機能リストから選択した機能を使用して、読み取りと書き込みの両方のアクセス権を持つ新しいユーザーグループを作成し、そのグループをカスタムユーザーに関連付ける必要があります。

ロールベースのアクセス権限

ロールベースのアクセス権限は、タスクと呼ばれる 5 つのカテゴリに分類されます。

- インターフェイス：Cisco IOS XE SD-WAN デバイス 上のインターフェイスを制御するための権限。
- ポリシー：コントロール プレーン ポリシー、OMP、およびデータプレーンポリシーを制御するための権限。
- ルーティング：BFD、BGP、OMP、OSPF などのルーティングプロトコルを制御するための権限。
- セキュリティ：ソフトウェアや証明書のインストールなど、デバイスのセキュリティを制御するための権限。[netadmin] グループに属するユーザーのみがシステムにソフトウェアをインストールできます。
- システム：一般的なシステム全体の権限。

次のセクションの表は、ユーザーおよびユーザーグループの AAA 認証ルールの詳細を示しています。これらの認証ルールは、CLI から発行されたコマンドと Netconf から発行されたコマンドに適用されます。

操作コマンドのユーザー認証ルール

操作コマンドのユーザー認証ルールは、ユーザー名のみに基づいています。Cisco IOS XE SD-WAN デバイス にログインできるユーザーは、ほとんどの操作コマンドを実行できます。ただし、ソフトウェアのインストールとアップグレード、デバイスのシャットダウンなど、デバイスの基本的な操作に影響を与えるコマンドを発行できるのは **admin** ユーザーだけです。

どのユーザーも **config** コマンドを発行して設定モードに入ることができ、設定モードに入ると、一般的な設定コマンドを発行できることに注意してください。また、すべてのユーザーは、**system aaa user** *self* **password** *password* コマンドを発行して、その設定変更をコミットすることにより、自分のパスワードを設定することができます。デバイスの動作を設定する実際のコマンドでは、ユーザーグループのメンバーシップに従って承認が定義されます。「設定コマンドのユーザーグループの認証ルール」を参照してください。

次の表に、一般的な CLI コマンドの AAA 認証ルールを示します。注記があるものを除き、すべてのコマンドは操作コマンドです。また、「admin」ユーザーが使用できる一部のコマンドは、そのユーザーが「netadmin」ユーザーグループに属している場合にのみ使用できます。

CLI コマンド	すべてのユーザー	管理者ユーザ
clear history	X	X
commit confirm	X	X
complete-on-space	X	X
config	X	X
exit	X	X

CLI コマンド	すべてのユーザー	管理者ユーザ
file	X	X
help	X	X
[no] history	X	X
idle-timeout	X	X
job	X	X
logout	—	X（netadmin グループのユーザーのみ）
monitor	X	X
nslookup	X	X
paginate	X	X
ping	X	X
poweroff	—	X（netadmin グループのユーザーのみ）
prompt1	X	X
prompt2	X	X
quit	X	X
reboot	—	X（netadmin グループのユーザーのみ）
request aaa request admin-tech request firmware request interface-reset request nms request reset request software	—	X（netadmin グループのユーザーのみ）
request execute request download request upload	X	X
request（その他すべて）	—	×
rollback（設定モードコマンド）	—	X（netadmin グループのユーザーのみ）
screen-length	X	X
screen-width	X	X
show cli	X	X

CLI コマンド	すべてのユーザー	管理者ユーザ
show configuration commit list	X	X
show history	X	X
show jobs	X	X
show parser dump	X	X
show running-config	X	X
show users	X	X
system aaa user self password password（設定モードコマンド）（注：ユーザーは自分自身を削除できません）		
tcpdump	X	X
timestamp	X	X
tools ip-route	X	X
tools netstat	X	X
tools nping	X	X
traceroute	X	X
vshell	X	X（netadmin グループのユーザーのみ）

操作コマンドのユーザーグループの認証ルール

操作コマンドのユーザーグループの認証ロールを次の表に示します。

操作コマンド	インターフェイス	ポリシー	ルーティング	セキュリティ	システム
clear app		X			
clear app-route		X			
clear arp	X				
clear bfd			X		X
clear bgp			X		X
clear bridge	X				
clear cellular	X				

操作コマンド	インターフェイス	ポリシー	ルーティング	セキュリティ	システム
clear control				X	
clear crash					X
clear dhcp					X
clear dns					X
clear igmp			X		
clear installed-certificates				X	
clear interface	X				
clear ip			X		
clear notification					X
clear omp			X		
clear orchestrator				X	
clear ospf			X		
clear pim			X		
clear policy		X			
clear pppoe	X				
clear system					X
clear tunnel				X	
clear wlan	X				
clear ztp				X	X
clock					X
debug bgp			X		
debug cellular	X				
debug cflowd		X			
debug chmgr					X
debug config-mgr					X
debug dhcp-client					X

操作コマンド	インターフェイス	ポリシー	ルーティング	セキュリティ	システム
debug dhcp-helper					X
debug dhcp-server					X
debug fpm		X			
debug ftm					X
debug igmp			X		
debug netconf					X
debug omp			X		
debug ospf			X		
debug pim			X		
debug resolver			X		
debug snmp					X
debug sysmgr					X
debug transport					X
debug ttm					X
debug vdaemon				X	X
debug vrrp				X	
debug wlan	X				
request certificate				X	
request control-tunnel				X	
request controller				X	
request controller-upload				X	
request csr				X	
request device				X	
request device-upload				X	
request on-vbond-controller				X	
request port-hop				X	

操作コマンド	インターフェイス	ポリシー	ルーティング	セキュリティ	システム
request root-cert-chain				X	
request security				X	
request vedge				X	
request vedge-upload				X	
request vsmart-upload				X	
show aaa					X
show app		X			
show app-route		X			
show arp	X				
show bfd			X		X
show bgp			X		
show boot-partition					X
show bridge	X				
show cellular	X				
show certificate				X	
show clock					X
show control				X	X
show crash					X
show debugs：debug コマンドと同じ					
show dhcp					X
show external-nat				X	X
show hardware					X
show igmp			X		
show interface	X				
show ip			X		X

操作コマンド	インターフェイス	ポリシー	ルーティング	セキュリティ	システム
show ipsec				X	
show licenses					X
show logging					X
show multicast			X		
show nms-server					X
show notification					X
show ntp					X
show omp		X	X		X
show orchestrator				X	
show ospf			X		
show pim			X		
show policer		X			
show policy		X			
show ppp	X				
show pppoe	X				
show reboot					X
show security-info				X	
show software					X
show system					X
show transport					X
show tunnel				X	
show uptime					X
show users					X
show version					X
show vrrp	X				
show wlan	X				
show ztp				X	

設定コマンドのユーザーグループの認証ルール

次の表に、設定コマンドのユーザーグループの認証ルールを示します。

コンフィギュレーション コマンド	インターフェイス	ポリシー	ルーティング	セキュリティ	システム
apply-policy		X			
banner					X
bfd			X		X
bridge	X				
[omp]		X	X		X
ポリシー		X			
security				X	X
snmp					X
system					X
vpn interface	X				
vpn ip			X		
vpn router			X		
vpn service			X		
vpn（作成、削除、命名を含むその他すべて）					X
wlan	X				

リソースグループによる RBAC の概要

サポートされている最小リリース：Cisco IOS XE リリース 17.5.1a、Cisco vManage リリース 20.5.1

リソースグループによるRBACは、ユーザーグループとリソースグループに基づいてユーザーのシステムアクセスを制限または承認する方法です。ユーザーグループはシステム内のユーザーの権限を定義し、リソースグループはユーザーがアクセスできる組織（ドメイン）を定義します。権限がユーザーに直接割り当てられることはないため、個々のユーザー権限の管理では、適切なユーザーとリソースグループを割り当てることが主な作業になります。

複数の地理的な場所にまたがる大規模な Cisco SD-WAN 展開では、ネットワーク管理を異なる地域管理者間で分割できます。

ネットワーク管理者が割り当てられているユーザーグループとリソースグループに基づいて、それらをグローバル管理者と地域管理者として大まかに分類できます。グローバル管理者は、すべてのリソースグループのリソースにアクセスでき、すべての機能に対する完全な読み取り/書き込み特権を持っています。地域管理者グループには、すべての機能に対する完全な読み取り/書き込み権限がありますが、アクセスできるリソースは、割り当てられているリソースグループによって制御されます。

Global Admin

グローバルリソースグループのユーザーアカウントは、すべてのリソースにアクセスできます。グローバル管理者は、ネットワーク全体を監視する責任がありますが、毎日の個々のデバイスの操作には関与しません。グローバル管理者は、デバイスを対応する地域に割り当て、地域管理者アカウントを割り当て、コントローラを管理し、共有可能で一元化された構成を維持し、必要に応じて個々のデバイスを操作できます。

netadmin 権限を持ち、グローバルリソースグループの一部でもあるシングル テナント セットアップのユーザーは、グローバル管理者と見なされます。Cisco vManage のデフォルトの管理者ユーザーもグローバル管理者であり、そのユーザーはさらにグローバル管理者を割り当てることができます。グローバルリソースグループには、すべての WAN エッジ、単一ビューのコントローラが含まれます。

グローバル管理者は、特定のリソースグループのみを表示するように切り替え、テンプレートを作成できます。地域管理者とも呼ばれるローカルリソースグループ管理者は、グローバルテンプレートを複製して、リソースグループ内で再利用できます。

地域管理者

地域管理者は、対応する地域のデバイスの日常的な操作（構成、監視、オンボーディング、など）を担当します。地域外のデバイスにアクセスしたり、表示したりしてはなりません。次のユーザーグループを作成できます。

- リソースグループ管理者：対応するリソースグループ内のデバイスへの完全な読み取り/書き込みアクセス権。グループ内の WAN エッジのテンプレートのトラブルシューティング、監視、アタッチ、またはデタッチを行うことができます
- リソースグループオペレータ：リソースグループ内の WAN エッジへの読み取り専用アクセス
- リソースグループ基本：基本アクセス

リソースグループの管理者は、新しいテンプレートを作成し、グループ内の WAN エッジにアタッチまたはデタッチできます。また、グローバルテンプレートをコピーして再利用することもできます。

リソースグループは、ユーザーがアクセスできるリソースを決定します。ただし、アクセスレベルは既存のユーザーグループによって制御されます。

- ユーザーが **resource_group_a** およびユーザーグループ **resource_group_admin** に属している場合、resource_group_a のすべてのリソースへの完全な読み取り/書き込みアクセス権があります。

- ユーザーが **resource_group_a** およびユーザーグループ **resource_group_operator** に属している場合、**resource_group_a** のすべてのリソースへの読み取り専用アクセス権があります。
- ユーザーが **resource_group_a** およびユーザーグループ **resource_group_basic** に属している場合、**resource_group_a** のインターフェイスおよびシステムリソースへの読み取り専用アクセス権があります。

グローバルリソースグループ

グローバルグループは、異なるアクセス制御ルールを持つ特別なシステム定義済みリソースグループです。

- このグループ内のユーザーはグローバル管理者と見なされ、システム内のすべてのリソース（デバイス、テンプレート、ポリシー）に完全にアクセスでき、リソースグループを管理し、リソースとユーザーをグループに割り当てることができます。
- 他のすべてのユーザーは、このグループ内のリソースへの読み取り専用アクセス権を持っています。
- システムのデフォルトの管理者アカウント（またはマルチテナント設定の tenantadmin アカウント）は、常にこのグループに属します。この権限は変更できません。ただし、管理者アカウントは、他のユーザーアカウントをこのグループに追加したり、このグループから削除したりできます。

IdP（SSO）管理グループ

ID プロバイダー（IdP）は、ユーザー ID を保存して検証するサービスです。IdP は通常、シングルサインオン（SSO）プロバイダーと連携してユーザーを認証します。ユーザーが IdP の SSO サービスで認証されている場合、グループ情報も IDP によって提供および管理されます。IdP は、ユーザー名やユーザーが属するすべてのグループ名など、ユーザーに関する情報を渡します。Cisco vManage は、グループ名をデータベースに保存されているグループ名と照合して、IdP から渡された特定のグループ名がユーザーグループ、リソースグループ、または VPN グループのものであるかどうかをさらに区別します。

マルチテナントサポート

Cisco SD-WAN マルチテナント機能を使用すると、サービスプロバイダーは、Cisco vManage からテナントと呼ばれる複数の顧客を管理できます。テナントは、Cisco vManage インスタンス、Cisco vBond Orchestrator、および Cisco vSmart Controller を共有します。サービスプロバイダーのドメイン名には、テナントごとにサブドメインがあります。Cisco vManage は、サービスプロバイダーによって展開および設定されます。プロバイダーは、マルチテナント機能を有効にし、テナントにサービスを提供する Cisco vManage クラスタを作成します。SSH 端末を介して Cisco vManage インスタンスにアクセスできるのはプロバイダーのみです。

プロバイダーには次の機能があります。

- プロバイダーはコントローラのみを管理するため、リソースグループは適用されません。

- プロバイダーが新しいテナントをプロビジョニングする場合、テナントのデフォルトのユーザーアカウントは tenantadmin です。
- プロバイダーによって作成された他のユーザーアカウントは、既定のグローバルリソースグループに含まれます。
- プロバイダーがテナント用のテンプレートを作成すると、そのテンプレートはグローバルリソースグループに含まれます。

ポリシーの RBAC の概要

サポートされている最小リリース：Cisco IOS XE リリース 17.6.1a、Cisco vManage リリース 20.6.1

ポリシーに対する RBAC により、ユーザーまたはユーザーグループは、Cisco vManage ポリシーへの選択的な読み取りおよび書き込み（RW）アクセスを行うことができます。次に例を示します。

- Cflowd ポリシーの RW アクセスを持つユーザーは、Cflowd ポリシーのみを構成でき、アプリケーション対応ルーティングポリシーを構成することはできません。
- アプリケーション対応ルーティングポリシーの RW アクセスを持つユーザーは、アプリケーション対応ルーティングポリシーのみを構成でき、他のポリシーを構成することはできません。

この機能は、集中化およびローカライズされたポリシーでのみサポートされており、セキュリティポリシーではサポートされていません。

機能テンプレートの詳細な RBAC に関する情報

サポート対象の最小リリース：Cisco vManage リリース 20.7.1

ユーザーグループのアクセス権を設定する場合、次のテンプレート権限を使用して、さまざまなタイプのテンプレートへの特定のレベルのアクセス権を RBAC ユーザーに付与できます。これにより、RBAC ユーザーが適用できるデバイス設定のタイプを管理できます。

権限	説明
CLI アドオンテンプレート	CLI アドオン機能テンプレートへのアクセス権を付与します。
デバイス CLI テンプレート	デバイス CLI テンプレートへのアクセス権を付与します。
SIG テンプレート	SIG 機能テンプレートおよび SIG ログイン情報テンプレートへのアクセス権を付与します。
その他の機能テンプレート	SIG 機能テンプレート、SIG ログイン情報テンプレート、および CLI アドオン機能テンプレートを除くすべての機能テンプレートへのアクセス権を付与します。

シングルテナントとマルチテナントのシナリオ

シングルテナントおよびマルチテナント Cisco vManage のシナリオでは、機能テンプレートに詳細な RBAC を使用できます。

ユーザーグループを作成して、テナントのさまざまなチームに特定の権限を割り当てることができます。これにより、チームは、デバイス CLI テンプレートを使用する権限がなくても、特定のネットワークサービスのみを管理できます。デバイス CLI テンプレートは他のテンプレートやデバイス設定を上書きする可能性があるため、テナントにデバイス CLI テンプレートを適用する権限を与えることは望ましくない場合があります。

たとえば、テナントのセキュリティ運用グループ用のユーザーグループを作成して、SIG テンプレートオプションへの読み取り/書き込みアクセスのみを許可することができます。これにより、セキュリティ運用グループはセキュリティ設定を使用できるようになります。

きめ細かい設定タスク権限に関する情報

Cisco vManage リリース 20.9.1 からは多数のユーザー権限オプションが利用可能であり、設定グループと機能プロファイルに関連する特定の設定タスクの管理権限をユーザーに割り当てる際にきめ細かい対応が可能です。

RBAC の利点

機能テンプレートのきめ細かい RBAC の利点

サポート対象の最小リリース：Cisco vManage リリース 20.7.1

共同管理のために追加する権限は、ネットワーク設定へのアクセスを詳細に制御するのに役立ちます。これらは、テナントで Cisco SD-WAN を使用する場合に便利で、特定のタイプのテンプレートへのテナントアクセスを提供できます。テナントの VPN 内でテナントに自己管理によるネットワーク構成タスクを与えることができます。

共同管理用に追加された権限については、機能テンプレートの詳細な RBAC に関する情報（16 ページ）を参照してください。

RBAC の制約事項

機能テンプレートの詳細な RBAC の制限

サポート対象の最小リリース：Cisco vManage リリース 20.7.1

- 共同管理用の RBAC に提供されているテンプレート制限オプションのいずれかを使用するには、[Template Configuration] オプションの権限を指定します。特定のユーザーロールに [Template Configuration] オプションで権限が割り当てられていない場合、そのユーザーに

対して [Templates] メニューは Cisco vManage に表示されません。「Manage Users」を参照してください。

- RBACユーザーがテンプレートをデバイスに適用できるようにするには、[Template Deploy] オプションに [Write] 権限を提供します。

RBAC の設定

ユーザの管理

Cisco vManage のメニューで、**[Administration]** > **[Manage Users]** を選択し、ユーザーおよびユーザーグループを追加、編集、表示、または削除します。

次の点に注意してください。

- **admin** ユーザーとしてログインしているユーザー、または [Manage Users] 書き込み権限を持つユーザーだけが、Cisco vManage のユーザーおよびユーザーグループを追加、編集、または削除できます。
- 各ユーザーグループには、このセクションに示されている機能の読み取りまたは書き込み権限を付与できます。書き込み権限には読み取り権限が含まれます。
- すべてのユーザーグループが、選択された読み取りまたは書き込み権限に関係なく、Cisco vManage ダッシュボードに表示される情報を確認できます。

表 *2:* ユーザーグループ権限：*Cisco IOS XE SD-WAN* デバイス

機能	読み取り権限	書き込み権限
アラーム	**[Monitor]** > **[Logs]** > **[Alarms]** ページで、アラームフィルタを設定し、デバイスで生成されたアラームを表示します。 Cisco vManage リリース 20.6.x 以前のリリース：**[Monitor]** > **[Alarms]** ページで、アラームフィルタを設定し、デバイスで生成されたアラームを表示します。	追加の権限はありません。

機能	読み取り権限	書き込み権限
監査ログ	**[Monitor]** > **[Logs]** > **[Alarms]** ページと **[Monitor]** > **[Logs]** > **[Audit Log]** ページで、監査ログフィルタを設定し、デバイスのすべてのアクティビティに関するログを表示します。 Cisco vManage リリース 20.6.x 以前のリリース：**[Monitor]** > **[Alarms]** ページと **[Monitor]** > **[Audit Log]** ページで、監査ログフィルタを設定し、デバイスのすべてのアクティビティに関するログを表示します。	追加の権限はありません。
証明書	**[Configuration]** > **[Certificates]** > **[WAN Edge List]** で、オーバーレイネットワーク内のデバイスのリストを表示します。 **[Configuration]** > **[Certificates]** > **[Controllers]** ウィンドウで、証明書署名要求（CSR）と証明書を表示します。	**[Configuration]** > **[Certificates]** > **[WAN Edge List]** ウィンドウで、デバイスを検証および無効化し、デバイスをステージングし、有効なコントローラデバイスのシリアル番号を Cisco vBond オーケストレーション に送信します。 **[Configuration]** > **[Certificates]** > **[Controllers]** ウィンドウで、CSR を生成し、署名付き証明書をインストールし、RSA キーペアをリセットし、コントローラデバイスを無効化します。

機能	読み取り権限	書き込み権限
CLI アドオンテンプレート （サポート対象の最小リリース：Cisco vManage リリース 20.7.1）	**[Configuration]** > **[Templates]** ウィンドウで CLI アドオン機能テンプレートを表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** ウィンドウで、CLI アドオン機能テンプレートを作成、編集、削除、およびコピーします。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。 （注） このオプションの詳細については、機能テンプレートの詳細な RBAC に関する情報 （16 ページ）を参照してください。
Cloud OnRamp	**[Configuration]** > **[Cloud OnRamp for SaaS]** および **[Configuration]** > **[Cloud OnRamp for IaaS]** ウィンドウでクラウドアプリケーションを表示します。	追加の権限はありません。
[Cluster]	**[Administration]** > **[Cluster Management]** ウィンドウで、Cisco vManage で動作中のサービス、Cisco vManage サーバーに接続されているデバイスのリスト、およびクラスタ内のすべての Cisco vManage サーバーで使用可能なサービスと動作中のサービスに関する情報を表示します。	**[Administration]** > **[Cluster Management]** ウィンドウで、現在の Cisco vManage の IP アドレスを変更し、Cisco vManage サーバーをクラスタに追加し、統計データベースを設定し、クラスタの Cisco vManage サーバーを編集および削除します。
コロケーション	**[Configuration]** > **[Cloud OnRamp for Colocation]** ウィンドウでクラウドアプリケーションを表示します。	追加の権限はありません。

機能	読み取り権限	書き込み権限
[Config Group] > **[Device]** > **[Deploy]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	この権限では、機能は提供されません。	設定を Cisco IOS XE SD-WAN デバイス に展開します。 （注） 既存の機能設定を編集するには、[Template Configuration] の書き込み権限が必要です。
デバイス CLI テンプレート （サポート対象の最小リリース：Cisco vManage リリース 20.7.1）	**[Configuration]** > **[Templates]** ウィンドウでデバイス CLI テンプレートを表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** ウィンドウで、デバイス CLI テンプレートを作成、編集、削除、およびコピーします。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。 （注） このオプションの詳細については、機能テンプレートの詳細な RBAC に関する情報 （16 ページ）を参照してください。

機能	読み取り権限	書き込み権限
デバイス インベントリ	**[Configuration]** > **[Devices]** > **[WAN Edge List]** ウィンドウで、デバイスの実行中の設定とローカル設定、テンプレートアクティビティのログ、およびデバイスへの設定テンプレート適用のステータスを表示します。 **[Configuration]** > **[Devices]** > **[Controllers]** ウィンドウで、デバイスの実行中の設定とローカル設定や、コントローラデバイスへの設定テンプレート適用のステータスを表示します。	**[Configuration]** > **[Devices]** > **[WAN Edge List]** ウィンドウで、デバイスの許可済みシリアル番号ファイルを Cisco vManage にアップロードし、デバイスを Cisco vManage 設定モードから CLI モードに切り替え、デバイス設定をコピーし、ネットワークからデバイスを削除します。 **[Configuration]** > **[Devices]** > **[Controllers]** ウィンドウで、オーバーレイネットワークのコントローラデバイスを追加および削除し、コントローラデバイスの IP アドレスとログイン情報を編集します。

機能	読み取り権限	書き込み権限
デバイスのモニタリング	**[Monitor]** > **[Geography]** ウィンドウで、デバイスの地理的な位置を表示します。 **[Monitor]** > **[Logs]** > **[Events]** ページで、デバイスで発生したイベントを表示します。 Cisco vManage リリース 20.6.x 以前のリリース：**[Monitor]** > **[Events]** ページで、デバイスで発生したイベントを表示します。 **[Monitor]** > **[Devices]** ページで（デバイスが選択されている場合のみ）、ネットワーク内のデバイスのリストを、デバイスステータスの概要、SD-WAN Application Intelligence Engine（SAIE）および Cflowd フロー情報、トランスポートロケーション（TLOC）ロス、遅延、およびジッター情報、制御およびトンネル接続、システムステータス、ならびにイベントとともに表示します。 （注） Cisco vManage リリース 20.7.x 以前では、SAIE フローはディープパケットインスペクション（DPI）フローと呼ばれていました。 Cisco vManage リリース 20.6.x 以前のリリース：デバイス情報は **[Monitor]** > **[Network]** ページに表示されます。	**[Monitor]** > **[Devices]** ページで（デバイスが選択されている場合のみ）、デバイスを ping し、トレースルートを実行し、IP パケットのトラフィックパスを分析します。

機能	読み取り権限	書き込み権限
デバイス リブート	**[Maintenance]** > **[Device Reboot]** ウィンドウで、再起動操作を実行できるデバイスのリストを表示します。	**[Maintenance]** > **[Device Reboot]** ウィンドウで、1 つまたは複数のデバイスを再起動します。
ディザスタ リカバリ	**[Administration]** > **[Disaster Recovery]** ウィンドウで、Cisco vManage 上で実行されているアクティブクラスタとスタンバイクラスタに関する情報を表示します。	追加の権限はありません。
[Event]	**[Monitor]** > **[Logs]** > **[Events]** ページで、デバイスの地理的な位置を表示します。 **[Monitor]** > **[Events]** ページで、デバイスの地理的な位置を表示します。	**[Monitor]** > **[Logs]** > **[Events]** ページで（デバイスが選択されている場合のみ）、デバイスを ping し、トレースルートを実行し、IP パケットのトラフィックパスを分析します。
[Feature Profile] > **[Other]** > **[Thousandeyes]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > **（設定グループを表示する）** ページの [Other Profile] セクションで [ThousandEyes] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > **（設定グループを追加または編集する）** ページの [Other Profile] セクションで [ThousandEyes] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。
[Feature Profile] > **[Service]** > **[Dhcp]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > **（設定グループを表示する）** ページの [Service Profile] セクションで [DHCP] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > **（設定グループを追加または編集する）** ページの [Service Profile] セクションで [DHCP] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。

機能	読み取り権限	書き込み権限
[Feature Profile] > **[Service]** > **[Lan/Vpn]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > **（設定グループを表示する）** ページの [Service Profile] セクションで [LAN/VPN] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > **（設定グループを追加または編集する）** ページの [Service Profile] セクションで [LAN/VPN] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。
[Feature Profile] > **[Service]** > **[Lan/Vpn/Interface/Ethernet]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > **（設定グループを表示する）** ページの [Service Profile] セクションで [Ethernet Interface] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > **（設定グループを追加または編集する）** ページの [Service Profile] セクションで [Ethernet Interface] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。
[Feature Profile] > **[Service]** > **[Lan/Vpn/Interface/Svi]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > **（設定グループを表示する）** ページの [Service Profile] セクションで [SVI Interface] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > **（設定グループを追加または編集する）** ページの [Service Profile] セクションで [SVI Interface] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。

機能	読み取り権限	書き込み権限
[Feature Profile] > **[Service]** > **[Routing/Bgp]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > **（設定グループを表示する）** ページの [Service Profile] セクションで [Routing/BGP] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > **（設定グループを追加または編集する）** ページの [Service Profile] セクションで [Routing/BGP] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。
[Feature Profile] > **[Service]** > **[Routing/Ospf]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > **（設定グループを表示する）** ページの [Service Profile] セクションで [Routing/OSPF] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > **（設定グループを追加または編集する）** ページの [Service Profile] セクションで [Routing/OSPF] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。
[Feature Profile] > **[Service]** > **[Switchport]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > **（設定グループを表示する）** ページの [Service Profile] セクションで [Switchport] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > **（設定グループを追加または編集する）** ページの [Service Profile] セクションで [Switchport] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。

機能	読み取り権限	書き込み権限
[Feature Profile] > **[Service]** > **[Wirelesslan]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > **（設定グループを表示する）** ページの [Service Profile] セクションで [Wireless LAN] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > **（設定グループを追加または編集する）** ページの [Service Profile] セクションで [Wireless LAN] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。
[Feature Profile] > **[System]** > **[Interface/Ethernet]** > **[Aaa]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > **（設定グループを表示する）** ページの [System Profile] セクションで [AAA] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > **（設定グループを追加または編集する）** ページの [System Profile] セクションで [AAA] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。
[Feature Profile] > **[System]** > **[Interface/Ethernet]** > **[Banner]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > **（設定グループを表示する）** ページの [System Profile] セクションで [Banner] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > **（設定グループを追加または編集する）** ページの [System Profile] セクションで [Banner] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。

機能	読み取り権限	書き込み権限
[Feature Profile] > **[System]** > **[Basic]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > **（設定グループを表示する）** ページの [System Profile] セクションで [Basic] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > **（設定グループを追加または編集する）** ページの [System Profile] セクションで [Basic] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。
[Feature Profile] > **[System]** > **[Bfd]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > **（設定グループを表示する）** ページの [System Profile] セクションで [BFD] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > **（設定グループを追加または編集する）** ページの [System Profile] セクションで [BFD] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。
[Feature Profile] > **[System]** > **[Global]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > **（設定グループを表示する）** ページの [System Profile] セクションで [Global] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > **（設定グループを追加または編集する）** ページの [System Profile] セクションで [Global] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。

機能	読み取り権限	書き込み権限
[Feature Profile] > **[System]** > **[Logging]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > **（設定グループを表示する）** ページの [System Profile] セクションで [Logging] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > **（設定グループを追加または編集する）** ページの [System Profile] セクションで [Logging] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。
[Feature Profile] > **[System]** > **[Ntp]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > **（設定グループを表示する）** ページの [System Profile] セクションで [NTP] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > **（設定グループを追加または編集する）** ページの [System Profile] セクションで [NTP] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。
[Feature Profile] > **[System]** > **[Omp]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > **（設定グループを表示する）** ページの [System Profile] セクションで [OMP] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > **（設定グループを追加または編集する）** ページの [System Profile] セクションで [OMP] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。

機能	読み取り権限	書き込み権限
[Feature Profile] > **[System]** > **[Snmp]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > **（設定グループを表示する）** ページの [System Profile] セクションで [SNMP] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > **（設定グループを追加または編集する）** ページの [System Profile] セクションで [SNMP] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。
[Feature Profile] > **[Transport]** > **[Cellular Controller]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > **（設定グループを表示する）** ページの [Transport & Management Profile] セクションで [Cellular Controller] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > **（設定グループを追加または編集する）** ページの [Transport & Management Profile] セクションで [Cellular Controller] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。
[Feature Profile] > **[Transport]** > **[Cellular Profile]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > **（設定グループを表示する）** ページの [Transport & Management Profile] セクションで [Cellular Profile] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > **（設定グループを追加または編集する）** ページの [Transport & Management Profile] セクションで [Cellular Profile] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。

機能	読み取り権限	書き込み権限
[Feature Profile] > **[Transport]** > **[Management/Vpn]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > **（設定グループを表示する）** ページの [Transport & Management Profile] セクションで [Management VPN] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > **（設定グループを追加または編集する）** ページの [Transport & Management Profile] セクションで [Management VPN] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。
[Feature Profile] > **[Transport]** > **[Management/Vpn/Interface/Ethernet]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > **（設定グループを表示する）** ページの [Transport & Management Profile] セクションで [Management Ethernet Interface] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > **（設定グループを追加または編集する）** ページの [Transport & Management Profile] セクションで [Management VPN and Management Internet Interface] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。
[Feature Profile] > **[Transport]** > **[Routing/Bgp]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > **（設定グループを表示する）** ページの [Transport & Management Profile] セクションで [BGP Routing] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > **（設定グループを追加または編集する）** ページの [Transport & Management Profile] セクションで [BGP Routing] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。

機能	読み取り権限	書き込み権限
[Feature Profile] > **[Transport]** > **[Tracker]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > **（設定グループを表示する）** ページの [Transport & Management Profile] セクションで [Tracker] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > **（設定グループを追加または編集する）** ページの [Transport & Management Profile] セクションで [Tracker] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。
[Feature Profile] > **[Transport]** > **[Wan/Vpn]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > **（設定グループを表示する）** ページの [Transport & Management Profile] セクションで [Wan/Vpn] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > **（設定グループを追加または編集する）** ページの [Transport & Management Profile] セクションで [Wan/Vpn] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。
[Feature Profile] > **[Transport]** > **[Wan/Vpn/Interface/Cellular]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > **（設定グループを表示する）** ページの [Transport & Management Profile] セクションで [Wan/Vpn/Interface/Cellular] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > **（設定グループを追加または編集する）** ページの [Transport & Management Profile] セクションで [Wan/Vpn/Interface/Cellular] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。

機能	読み取り権限	書き込み権限
[Feature Profile] > **[Transport]** > **[Wan/Vpn/Interface/Ethernet]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** >（設定グループを表示する）ページの [Transport & Management Profile] セクションで [Wan/Vpn/Interface/Ethernet] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** >（設定グループを追加または編集する）ページの [Transport & Management Profile] セクションで [Wan/Vpn/Interface/Ethernet] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。
統合管理	**[Administration]** > **[Integration Management]** ウィンドウで、Cisco vManage で実行中のコントローラに関する情報を表示します。	追加の権限はありません。
ライセンス管理	**[Administration]** > **[License Management]** ウィンドウで、Cisco vManage で実行中のデバイスのライセンス情報を表示します。	**[Administration]** > **[License Management]** ページで、Cisco スマートアカウントの使用を設定し、管理するライセンスを選択して、Cisco vManage とライセンスサーバー間でライセンス情報を同期します。
インターフェイス（**Interface**）	**[Monitor]** > **[Network]** > **[Interface]** ページで、デバイスのインターフェイスに関する情報を表示します。 Cisco vManage リリース 20.6.x 以前のリリース：デバイスのインターフェイスに関する情報は **[Monitor]** > **[Network]** > **[Interface]** ページに表示されます。	**[Monitor]** > **[Devices]** > **[Interface]** ページで、[Chart Options] を編集して、表示するデータのタイプを選択し、データを表示する期間を編集します。

機能	読み取り権限	書き込み権限
ユーザーの管理	**[Administration]** > **[Manage Users]** ウィンドウで、ユーザーとユーザーグループを表示します。	**[Administration]** > **[Manage Users]** ウィンドウで、Cisco vManage のユーザーとユーザーグループを追加、編集、および削除し、ユーザーグループの権限を編集します。
その他の機能テンプレート （サポート対象の最小リリース：Cisco vManage リリース 20.7.1）	**[Configuration]** > **[Templates]** ウィンドウで、SIG 機能テンプレート、SIG ログイン情報テンプレート、および CLI アドオン機能テンプレートを除くすべての機能テンプレートを表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** ウィンドウで、SIG 機能テンプレート、SIG ログイン情報テンプレート、および CLI アドオン機能テンプレートを除くすべての機能テンプレートを作成、編集、削除、およびコピーします。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。 （注） このオプションの詳細については、機能テンプレートの詳細な RBAC に関する情報 （16 ページ）を参照してください。
ポリシー	**[Configuration]** > **[Policies]** ウィンドウで、ネットワーク内のすべての Cisco vSmart コントローラ またはデバイスの共通ポリシーを表示します。	**[Configuration]** > **[Policies]** ウィンドウで、ネットワーク内のすべての Cisco vSmart コントローラ またはデバイスの共通ポリシーを作成、編集、および削除します。
ポリシーの設定	**[Configuration]** > **[Policies]** ウィンドウで、作成されたポリシーのリストとその詳細を表示します。	**[Configuration]** > **[Policies]** ウィンドウで、ネットワーク内のすべての Cisco vSmart コントローラ およびデバイスの共通ポリシーを作成、編集、および削除します。

機能	読み取り権限	書き込み権限
ポリシーの展開	**[Configuration]** > **[Policies]** ウィンドウで、ポリシーが適用されている Cisco vSmart コントローラ の現在のステータスを表示します。	**[Configuration]** > **[Policies]** ウィンドウで、ネットワーク内のすべての Cisco vManage サーバーの共通ポリシーをアクティブ化および非アクティブ化します。
RBAC VPN	**[Monitor]** > **[VPN]** ページで、ロールに基づいて VPN グループとセグメントを表示します。 Cisco vManage リリース 20.6.x 以前のリリース：**[Dashboard]** > **[VPN Dashboard]** ページで、ロールに基づいて VPN グループとセグメントを表示します。	**[Administration]** > **[VPN Groups]** ウィンドウで、Cisco vManage の VPN と VPN グループを追加、編集、および削除し、VPN グループの権限を編集します。
ルーティング	**[Monitor]** > **[Devices]** > **[Real-Time]** ページで、デバイスのリアルタイムルーティング情報を表示します。 Cisco vManage リリース 20.6.x 以前のリリース：デバイスのリアルタイムルーティングに関する情報は **[Monitor]** > **[Network]** > **[Real-Time]** ページに表示されます。	**[Monitor]** > **[Devices]** > **[Real-Time]** ページで、コマンドフィルタを追加して情報表示を迅速化させます。
セキュリティ	**[Configuration]** > **[Security]** ウィンドウで、セキュリティポリシーが適用されている Cisco vSmart コントローラ の現在のステータスを表示します。	**[Configuration]** > **[Security]** ウィンドウで、ネットワーク内のすべての Cisco vManage サーバーのセキュリティポリシーをアクティブ化および非アクティブ化します。
セキュリティポリシー設定	**[Configuration]** > **[Security]** > **[Add Security Policy]** ウィンドウで、ネットワーク内のすべての Cisco vManage サーバーの共通ポリシーをアクティブ化および非アクティブ化します。	**[Configuration]** > **[Security]** > **[Add Security Policy]** ウィンドウで、ネットワーク内のすべての Cisco vManage サーバーのセキュリティポリシーをアクティブ化および非アクティブ化します。

機能	読み取り権限	書き込み権限
セッション管理	**[Administration]** > **[Manage Users]** > **[User Sessions]** ウィンドウで、ユーザーセッションを表示します。	**[Administration]** > **[Manage Users]** > **[User Sessions]** ウィンドウで、Cisco vManage のユーザーとユーザーグループを追加、編集、および削除し、ユーザーセッションを編集します。
Settings	**[Administration]** > **[Settings]** ウィンドウで、組織名、Cisco vBond オーケストレーションの DNS または IP アドレス、証明書認証設定、デバイスに適用されているソフトウェアのバージョン、Cisco vManage のログインページのカスタムバナー、および統計情報を収集するための現在の設定を表示します。	**[Administration]** > **[Settings]** ウィンドウで、組織名、Cisco vBond オーケストレーションの DNS または IP アドレス、証明書認証設定、デバイスに適用されているソフトウェアのバージョン、Cisco vManage のログインページのカスタムバナー、および統計情報を収集するための現在の設定を編集し、Web サーバー証明書の証明書署名要求（CSR）を生成し、証明書をインストールします。
SIG テンプレート （サポート対象の最小リリース：Cisco vManage リリース 20.7.1）	**[Configuration]** > **[Templates]** ウィンドウで、SIG 機能テンプレートおよび SIG ログイン情報テンプレートを表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** ウィンドウで、SIG 機能テンプレートおよび SIG ログイン情報テンプレートを作成、編集、削除、およびコピーします。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。 （注） このオプションの詳細については、機能テンプレートの詳細な RBAC に関する情報 （16 ページ）を参照してください。

機能	読み取り権限	書き込み権限
ソフトウェアアップグレード	**[Maintenance]** > **[Software Upgrade]** ウィンドウで、デバイスのリスト、ソフトウェアアップグレードを実行できる Cisco vManage のカスタムバナー、およびデバイスで実行されているソフトウェアの現在のバージョンを表示します。	**[Maintenance]** > **[Software Upgrade]** ウィンドウで、デバイスに新しいソフトウェアイメージをアップロードし、デバイスのソフトウェアイメージをアップグレード、アクティブ化、および削除し、ソフトウェアイメージをデバイスのデフォルトイメージに設定します。
システム	**[Configuration]** > **[Templates]** > **[Device Template]** ウィンドウで、Cisco vManage テンプレートを使用して設定されたシステム全体のパラメータを表示します。 （注） Cisco vManage リリース 20.7.x 以前のリリースでは、[Device Templates] は [Device] と呼ばれます。	**[Configuration]** > **[Templates]** > **[Device Template]** ウィンドウで、Cisco vManage テンプレートを使用して設定されたシステム全体のパラメータを設定します。 （注） Cisco vManage リリース 20.7.x 以前のリリースでは、[Device Templates] は [Device] と呼ばれます。
テンプレートの設定	**[Configuration]** > **[Templates]** ウィンドウで、機能テンプレートとデバイステンプレートを表示します。	**[Configuration]** > **[Templates]** ウィンドウで、機能テンプレートまたはデバイステンプレートを作成、編集、削除、およびコピーします。 （注） Cisco vManage リリース 20.7.1 以降、デバイスにすでにアタッチされているテンプレートを作成、編集、または削除するには、ユーザーに [Template Deploy] オプションに対する書き込み権限が必要です。

機能	読み取り権限	書き込み権限
テンプレートの展開	**[Configuration]** > **[Templates]** ウィンドウで、デバイステンプレートにアタッチされているデバイスを表示します。	**[Configuration]** > **[Templates]** ウィンドウで、デバイステンプレートにデバイスをアタッチします。
ツール	**[Tools]** > **[Operational Commands]** ウィンドウで、**admin tech** コマンドを使用してデバイスのシステムステータス情報を収集します。	**[Tools]** > **[Operational Commands]** ウィンドウで、**admin tech** コマンドを使用してデバイスのシステムステータス情報を収集し、**interface reset** コマンドを使用して 1 回の操作でデバイスのインターフェイスをシャットダウンして再起動します。 **[Tools]** > **[Operational Commands]** ウィンドウで、ネットワークを再検索して新しいデバイスを検出し、Cisco vManage と同期させます。 **[Tools]** > **[Operational Commands]** ウィンドウで、デバイスへの SSH セッションを確立し、CLI コマンドを発行します。
vAnalytics	**[Cisco vManage]** > **[vAnalytics]** ウィンドウで vAnalytics を起動します。	追加の権限はありません。
Workflows	**[Cisco vManage]** > **[Workflows]** ウィンドウからワークフローライブラリを起動します。	追加の権限はありません。

マルチテナント環境の RBAC ユーザーグループ

次の表に、マルチテナント環境でのロールベース アクセス コントロール（RBAC）のユーザーグループ権限のリストを示します。

- R は読み取り権限を表します。
- W は書き込み権限を表します。

表 *3:* マルチテナント環境の *RBAC* ユーザーグループ

機能	Provider Admin	Provider Operator	Tenant Admin	テナントのオペレータ
Cloud OnRamp	RW	R	RW	R
コロケーション	RW	R	RW	R
RBAC VPN	RW	R	RW	R
セキュリティ	RW	R	RW	R
セキュリティポリシー設定	RW	R	RW	R
vAnalytics	RW	R	RW	R

Add User

1. Cisco vManage メニューから **[Administration]** > **[Manage Users]** を選択します。
2. デフォルトでは、[Users] が選択されています。テーブルに、デバイスで設定されているユーザーのリストが表示されます。
3. 既存のユーザーのパスワードを編集、削除、または変更するには、[...] をクリックして、[Edit]、[Delete]、または [Change Password] をそれぞれクリックします。
4. 新規ユーザを追加するには、[Add User] をクリックします。
5. [Full Name]、[Username]、[Password]、および [Confirm Password] の各詳細情報を追加します
6. [User Groups] ドロップダウンリストで、ユーザーを追加するユーザーグループを選択します。
7. [Resource Group] ドロップダウンリストで、リソースグループを選択します。

（注） このフィールドは Cisco IOS XE リリース 17.5.1a 以降で利用できます。

8. [Add] をクリックします。

ユーザーの削除

ユーザーがデバイスにアクセスする必要がなくなった場合は、そのユーザーを削除できます。ユーザーがログインしている場合、そのユーザーを削除してもログアウトされません。

ユーザーを削除するには、次の手順を実行します。

1. Cisco vManage メニューから **[Administration]** > **[Manage Users]** を選択します。

2. 削除するユーザーの [...] をクリックし、[Delete] をクリックします。
3. ユーザーの削除を確認するには、[OK] をクリックします。

ユーザーの詳細の編集

ユーザーのログイン情報を更新したり、ユーザーグループのユーザーを追加または削除することができます。ログインしているユーザーの詳細情報を編集した場合、変更はそのユーザーがログアウトした後に有効になります。

ユーザーの詳細情報を編集するには、次のようにします。

1. Cisco vManage メニューから **[Administration]** > **[Manage Users]** を選択します。
2. 編集するユーザーの [...] をクリックし、[Edit] をクリックします。
3. ユーザーの詳細を編集します。

   ユーザーグループのユーザーを追加または削除することもできます。
4. [Update] をクリックします。

ユーザー パスワードの変更

必要に応じて、ユーザーのパスワードを更新できます。強力なパスワードの使用を推奨します。

はじめる前に

管理者ユーザーのパスワードを変更する場合は、この手順を実行する前に、クラスタ内のすべての Cisco vManage インスタンスからデバイステンプレートをアタッチ解除してください。この手順を完了した後、デバイステンプレートを再アタッチできます。

ユーザーのパスワードを変更するには、次の手順に従います。

1. Cisco vManage メニューから **[Administration]** > **[Manage Users]** を選択します。
2. パスワードを変更するユーザーの [...] をクリックし、[Change Password] をクリックします。
3. 新しいパスワードを入力し、それを確認します。

（注） 対象のユーザーがログインしている場合はログアウトされます。

4. [Done] をクリックします。

SSH セッションを使用してデバイスにログインしているユーザーの確認

1. Cisco vManage メニューから**[Monitor]** > **[Devices]**の順に選択します。

Cisco vManage リリース 20.6.x 以前：Cisco vManage メニューから**[Monitor]** > **[Network]**の順に選択します。

2. [Hostname] 列で、使用するデバイスを選択します。
3. [Real Time] をクリックします。
4. [Device Options] で、[AAA users]（Cisco IOS XE SD-WAN デバイス の場合）を選択します。

   このデバイスにログインしているユーザーのリストが表示されます。

HTTP セッションを使用してデバイスにログインしているユーザーの確認

1. Cisco vManage メニューから **[Administration]** > **[Manage Users]** を選択します。
2. [User Sessions] をクリックします。

   Cisco vManage 内のすべてのアクティブな HTTP セッションのリスト（ユーザー名、ドメイン、送信元 IP アドレスなどを含む）が表示されます。

ユーザーグループの管理

ユーザーはグループに配置されます。グループは、ユーザーが表示および変更を許可されている特定の構成および操作コマンドを定義します。1 人のユーザーが 1 つ以上のグループに属することができます。Cisco SD-WAN ソフトウェアには標準ユーザーグループが用意されており、必要に応じてカスタムユーザーグループを作成できます。

- [basic]：インターフェイスおよびシステム情報を表示する権限を持つユーザーが含まれます。
- [netadmin]：Cisco vManage ですべての操作を実行できる管理者ユーザーがデフォルトで含まれます。このグループに他のユーザーを追加できます。
- [operator]：情報を表示する権限のみを持つユーザーを含みます。
- サポート対象の最小リリース：Cisco vManage リリース 20.9.1

  [network_operations]：非セキュリティポリシーの表示と変更、デバイステンプレートのアタッチとデタッチ、非セキュリティデータの監視など、セキュリティ以外の操作を Cisco vManage で実行できるユーザーが含まれます。
- サポート対象の最小リリース：Cisco vManage リリース 20.9.1

  [security_operations]：セキュリティポリシーの表示と変更、セキュリティデータの監視など、セキュリティ操作を Cisco vManage で実行できるユーザーが含まれます。

注：すべてのユーザーグループが、選択された読み取りまたは書き込み権限に関係なく、Cisco vManage ダッシュボードに表示される情報を確認できます。

ユーザーグループの削除

不要になったユーザーグループは削除できます。たとえば、特定のプロジェクト用に作成したユーザーグループを、そのプロジェクトの終了時に削除する場合があります。

1. Cisco vManage メニューから **[Administration]** > **[Manage Users]** を選択します。
2. **[User Groups]**をクリックします。
3. 削除するユーザーグループの名前をクリックします。

（注） デフォルトのユーザーグループ（basic、netadmin、operator、network_operations、security_operations）は削除できません。

4. [Trash] アイコンをクリックします。
5. ユーザーグループの削除を確認するには、[OK] をクリックします。

ユーザーグループ権限の編集

既存のユーザーグループのグループ権限を編集できます。この手順では、必要なユーザーグループの構成済み機能の読み取りおよび書き込みアクセス許可を変更できます。

1. Cisco vManage メニューから **[Administration]** > **[Manage Users]** を選択します。
2. **[User Groups]**をクリックします。
3. 権限を編集するユーザーグループの名前を選択します。

（注） デフォルトのユーザーグループ（basic、netadmin、operator、network_operations、security_operations）の権限は編集できません。

4. [Edit] をクリックし、必要に応じて権限を編集します。
5. **[Save]** をクリックします。

adminユーザーがグループを変更することによってユーザーの権限を変更する場合、そのユーザーは、そのときにデバイスにログインしているとログアウトされ、再度ログインする必要があります。

ユーザーグループの作成

1. Cisco vManage メニューから **[Administration]** > **[Manage Users]** を選択します。
2. **[User Groups]**をクリックします。
3. [Add a User Group] をクリックします。

4. [User Group Name] を入力します。
5. ユーザーグループに割り当てる機能に対して、[Read] または [Write] チェックボックスをオンにします。
6. [Add] をクリックします。
7. 左側のナビゲーションパスで、新しいユーザーグループを表示できます。[Edit] をクリックして、既存の読み取りまたは書き込みルールを編集します。
8. [Save] をクリックします。

VPN セグメントの設定と管理

VPN セグメントを設定するには、次の手順を実行します。

1. Cisco vManage のメニューから、**[Administration]** > **[VPN Segments]** を選択します。Web ページに、構成されているセグメントのリストが表示されます。
2. 既存のセグメントを編集または削除するには、[…] をクリックし、[Edit] または [Delete] をクリックします。
3. 新しいセグメントを追加するには、[Add Segment] をクリックします。
4. [Segment Name] フィールドにセグメントの名前を入力します。
5. [VPN Number] フィールドに、設定する VPN の番号を入力します。
6. 新しいセグメントを追加するには、[Add] をクリックします。

VPN グループの設定と管理

VPN グループを設定するには、次の手順を実行します。

1. Cisco vManage のメニューで、**[Administration]** > **[VPN Groups]** を選択します。Web ページに、構成されているセグメントのリストが表示されます。
2. VPN グループを編集または削除するには、[…] をクリックし、[Edit] または [Delete] をクリックします。
3. ダッシュボードに既存の VPN を表示するには、[…] をクリックし、[View Dashboard] をクリックします。[VPN Dashboard] には、設定された VPN デバイスのデバイス詳細が表示されます。
4. 新規 VPN グループを追加するには、[Add Group] をクリックします。
5. [Create VPN Group] から、[VPN Group Name] フィールドに VPN グループ名を入力します。
6. [Description] フィールドに VPN の簡単な説明を入力します。

7. [Enable User Group access] チェックボックスをオンにして、ユーザーグループ名を入力します。
8. [Assign Segment] で、[Add Segment] ドロップダウンリストをクリックして、新規または既存のセグメントを VPN グループに追加します。
9. それぞれのフィールドに [Segment Name] と [VPN Number] を入力します。
10. 設定 VPN グループをデバイスに追加するには、[Add] をクリックします。

リソース グループの管理

サポートされている最小リリース：Cisco IOS XE リリース 17.5.1a、Cisco vManage リリース 20.5.1

リソースグループを設定するには、次の手順を実行します。

1. Cisco vManage のメニューで、**[Administration]** > **[Resource Groups]** を選択します。テーブルには、Cisco vManage に設定されているリソースグループのリストが表示されます。
2. リソースグループを編集または削除するには、[…] をクリックし、[Edit] または [Delete] をクリックします。
3. 新しいリソースグループを追加するには、[Add Resource Group] をクリックします。
4. [Resource Group Name] と [Description] を入力します。
5. [Site ID] で、ドロップダウンリストからリソースグループに含める [Range] または [Select ID(S)] を入力します。
6. リソースグループをデバイスに追加するには、[Add] をクリックします。

ユーザーを追加するには、次の手順を実行します。

1. Cisco vManage メニューから **[Administration]** > **[Manage Users]** を選択します。[Manage Users] 画面が表示されます。
2. デフォルトでは、[Users] が選択されています。テーブルに、デバイスで設定されているユーザーのリストが表示されます。
3. 既存のユーザーのパスワードを編集、削除、または変更するには、[...] をクリックして、[Edit]、[Delete]、または [Change Password] をそれぞれクリックします。
4. 新規ユーザーを追加するには、[Add User] をクリックします。
5. [Full Name]、[Username]、[Password]、および [Confirm Password] の各詳細情報を追加します
6. [User Groups] ドロップダウンリストで、ユーザーを追加するユーザーグループを選択します。
7. [Resource Group] ドロップダウンリストで、リソースグループを選択します。

（注） このフィールドは Cisco IOS XE リリース 17.5.1a 以降で利用できます。

8. [Add] をクリックします。

ポリシーに RBAC を設定するためのワークフロー

サポートされている最小リリース：Cisco IOS XE リリース 17.6.1a、Cisco vManage リリース 20.6.1

ポリシーに RBAC を設定するには、次のワークフローを使用します。

1. 選択した制御またはデータポリシーへの必要な読み取りまたは書き込み（R/W）アクセス権を持つユーザーグループを作成します。ユーザーグループの作成については、「ユーザーグループの作成」を参照してください。
2. ユーザーを作成して必要なユーザーグループに割り当てます。「ユーザーの作成」を参照してください。
3. 必要に応じて、ポリシー設定を作成、変更、または表示します。ポリシー設定については、「Configure Centralized Policies Using Cisco vManage」を参照してください。

ポリシー設定の変更

サポートされている最小リリース：Cisco IOS XE リリース 17.6.1a、Cisco vManage リリース 20.6.1

1. 新しいユーザー詳細情報を使用して Cisco vManage にログインします。
2. 要件に基づいて設定を変更または更新できます。

新しいユーザー詳細情報を使用して Cisco vManage にログインすると、自分に割り当てられているユーザー グループ コンポーネントのみを表示できます。ポリシーの設定の詳細については、『Cisco SD-WAN Policies Configuration Guide』を参照してください。

ポリシーに RBAC を設定するためのユーザーの割り当て

サポートされている最小リリース：Cisco IOS XE リリース 17.6.1a、Cisco vManage リリース 20.6.1

CFlowd データポリシーを作成または変更するユーザーを割り当てるには

CFlowd ユーザーグループを作成するには、次の手順を実行します。

1. Cisco vManage から**[Administration]** > **[Manage Users]**の順に選択します。
2. [User Groups] と [Add User Group] をクリックします。
3. [User Group Name] を入力します。

たとえば、cflowd-policy-only などです。

4. ユーザーグループに割り当てる CFlowD ポリシー機能に対して、[Read] または [Write] チェックボックスをオンにします。
5. [Add] をクリックします。
6. 左側のナビゲーションパスで、新しいユーザーグループを表示できます。[Edit] をクリックして、既存の読み取りまたは書き込みルールを編集します。
7. **[Save]** をクリックします。

CFlowd ユーザーを作成するには、次の手順を実行します。

1. Cisco vManage で、**[Administration]** > **[Manage Users]** を選択します。
2. [ユーザー（Users）] をクリックします。
3. [ユーザの追加（Add User）] をクリックします。
4. [Add New User] ページで、[Full Name]、[Username]、[Password]、および [Confirm Password] に詳細情報を入力します。
5. [User Groups] ドロップダウンから [cflowd-policy-only] を選択します。

   [Resource Group] がデフォルトのリソースグループを選択できるようにします。
6. [Add] をクリックします。[Users] ウィンドウで新しいユーザーを表示できます。
7. ユーザーの既存の読み取りまたは書き込みルールを編集するには、[Edit] をクリックします。

Cflowd ポリシーを変更するには、次の手順を実行します。

1. 新しいユーザークレデンシャルを使用して Cisco vManage にログインします。

   ログインは [cflowd-policy-only] ユーザーグループに割り当てられるため、CFlowd ポリシーへのアクセスのみを表示できます。
2. 要件に基づいて構成を作成、変更、または更新できます。

機能テンプレートの詳細な RBAC の構成

サポート対象の最小リリース：Cisco vManage リリース 20.7.1

特定のテンプレートアクセスを設定するには、ユーザーグループを作成し、共同管理の RBAC に関する情報で説明されているアクセス許可タイプを使用して、読み取りおよび書き込みアクセス許可を割り当てます。テンプレートアクセスを制限するためのアクセス許可オプションは、ユーザーグループを追加するときに選択した他のアクセス許可オプションとともに表示されます。

機能テンプレートの詳細な RBAC については、機能テンプレートの詳細な RBAC に関する情報 （16 ページ）を参照してください。

ユーザーグループの追加については、「ユーザーグループの作成」を参照してください。

アクセス許可のタイプと説明のリストについては、「ユーザーの管理」を参照してください。

CLI を使用した RBAC の設定

CLI を使用したユーザーの設定

各デバイスでCLIを使用してユーザーログイン情報を設定できます。この方法により、追加のユーザーを作成し、それらのユーザーに特定のデバイスへのアクセス権を付与することが可能です。CLIを使用してユーザーのための作成するログイン情報は、そのユーザーのCisco vManageログイン情報とは異なるものにすることができます。また、デバイスごとに同じユーザーの異なるログイン情報を作成できます。**netadmin** 権限を持つすべての Cisco IOS XE SD-WAN デバイス ユーザーが、新しいユーザーを作成できます。

ユーザーアカウントを作成するには、ユーザー名とパスワードを設定し、ユーザーをグループに追加します。

次の例は、既存のグループへのユーザー Bob の追加を示しています。

```
デバイス(config)# system aaa user bob group basic
```

次の例は、新しいグループ `test-group` へのユーザー Alice の追加を示しています。

```
デバイス(config)# system aaa user test-group
デバイス(config)# system aaa user alice group test-group
```

ユーザー名の長さは 1 ー 128 文字で、先頭は英字にする必要があります。名前に使用できるのは、英小文字、0 ー 9 の数字、ハイフン（-）、下線（_）、ピリオド（.）のみです。英大文字は使用できません。一部のユーザー名は、予約されているために設定できません。予約済みユーザー名のリストについては、『Cisco SD-WAN Command Reference Guide』で **aaa** コンフィギュレーション コマンドを参照してください。

パスワードは、ユーザーのパスワードです。各ユーザー名にはパスワードが必要であり、ユーザーは自分のパスワードを変更できます。CLI では、文字列がすぐに暗号化され、パスワードは読み取り可能な形で表示されません。ユーザーには、 Cisco IOS XE SD-WAN デバイスにログインする際に、正しいパスワードの入力を 5 回試みることができます。5 回の試行で正しく入力できなかった場合、そのユーザーはデバイスからロックアウトされ、再度ログインを試みるまでに 15 分間待つ必要があります。

（注） 特殊文字 ! を含むユーザーパスワードは二重引用符（" "）で囲みます。パスワード全体を二重引用符で囲まない場合、構成データベース（?）はこの特殊文字をスペースとして扱い、パスワードの残りの部分を無視します。

たとえば、パスワードが C!sc0 の場合は、"C!sc0" を使用します。

グループ名は、Cisco SD-WAN の標準グループの名前（**basic**、**netadmin**、または **operator**）か、**usergroup** コマンド（後述）で設定されたグループの名前です。管理者ユーザーがグループを変更することによってユーザーの権限を変更する場合、そのユーザーは、そのときにデバイスにログインしているとログアウトされ、再度ログインする必要があります。

admin ユーザー名の工場出荷時のデフォルトパスワードは、admin です。 Cisco IOS XE SD-WAN デバイスを最初に設定するときに、このパスワードを変更することを強く推奨します。

```
デバイス(config)# username admin password
$9$3/IL3/UF2F2F3E$J9NKBeKlWrq9ExmHk6F5VAiDMOFQfD.QPAmMxDdxz.c
```

パスワードは、ASCII 文字列で設定します。次の例のように、CLI では、文字列がすぐに暗号化され、パスワードは読み取り可能な形で表示されません。

```
デバイス(config)# show run
...
aaa authentication login default local
aaa authentication login user1 group basic
aaa authentication login user2 group operator
aaa authentication login user3 group netadmin
aaa authorization exec default local
```

RADIUS を使用して AAA 認証を実行している場合は、パスワードを確認するように特定の RADIUS サーバーを設定できます。

```
デバイス(config)#  radius server tag
```

タグは、**radius server tag** コマンドで定義した文字列です（『Cisco SD-WAN Command Reference Guide』を参照）。

CLI を使用したグループの作成

Cisco SD-WAN ソフトウェアには、デフォルトのユーザーグループ（**basic**、**netadmin**、**operator**、**network_operations**、**security_operations**）が用意されています。ユーザー名 **admin** は自動的に **netadmin** ユーザーグループに配置されます。

必要に応じて、追加のカスタムグループを作成し、グループメンバーが持つ権限ロールを設定できます。特定の権限を持つカスタムグループを作成するには、グループ名と権限を設定します。

```
デバイス(config)# aaa authentication login user1 group radius enable
デバイス(config)# aaa authentication login user2 group radius enable
デバイス(config)# aaa authentication login user3 group radius enable
デバイス(config)#
```

group-name の長さは 1 ー 128 文字で、先頭は英字にする必要があります。名前に使用できるのは、英小文字、0 ー 9 の数字、ハイフン（-）、下線（_）、ピリオド（.）のみです。名前に大文字は使用できません。一部のグループ名は予約されているため、設定できません。それらのリストについては、aaa 設定コマンドを参照してください。

リモート RADIUS または TACACS+ サーバーが認証を検証しても、ユーザーグループを指定しない場合、ユーザーはユーザーグループ **basic** に配置されます。リモートサーバーが認証を検証し、VSA Cisco SD-WAN-Group-Name を使用してユーザーグループ（X とします）を指定する場合、ユーザーはそのユーザーグループのみに配置されます。ただし、そのユーザーがロー

カルにも設定され、ユーザーグループ（Y とします）に属している場合、ユーザーは両方のグループ（X と Y）に配置されます。

task オプションでは、グループメンバーが持つ権限ロールを一覧表示します。ロールは、**インターフェイス**、**ポリシー**、**ルーティング**、**セキュリティ**、および**システム**の 1 つ以上にすることができます。

RBAC の確認

詳細な RBAC アクセス許可を確認する

サポート対象の最小リリース：Cisco vManage リリース 20.7.1

この手順を使用して、ユーザーグループに設定したアクセス許可を確認します。

1. Cisco vManage メニューから **[Administration]** > **[Manage Users]** を選択します。
2. **[User Groups]**をクリックします。
3. ユーザーグループを表示するペインで、ユーザーグループを選択して、ユーザーグループに割り当てられている読み取りおよび書き込み権限を表示します。
4. テンプレートアクセスを制御する権限までスクロールして、ユーザーグループの設定を確認します。

RBAC のモニタリング

VPN グループのデバイスのモニタリング

デバイスをモニタリングするには、次の手順を実行します。

1. Cisco vManage のメニューから**[Monitor]** > **[Network]**の順に選択します。
2. [WAN - Edge] をクリックします。
3. ネットワークをモニタリングする [VPN Group] と [VPN Segment] を選択します。

   Web ページに、デバイスに設定されている VPN グループとセグメントのリストが表示されます。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。