CA Performance Center

管理対象サービス プロバイダ ガイド

2.4

ca technologies

CA への連絡先

テクニカル サポートの詳細については、弊社テクニカル サポートの Web サイト（http://www.ca.com/jp/support/）をご覧ください。

目次

第 1 章: はじめに

このセクションには、以下のトピックが含まれています。

管理対象サービス プロバイダおよび CA Performance Center

CA Performance Center は管理対象サービスおよび他のホスト環境での監視をサポートします。 マルチテナンシー機能を使用することにより、複数の顧客を作成し、その環境を別々に監視できます。

*テナント*は、管理対象サービス プロバイダが管理するカスタマ環境を表します。 各テナント環境は独立しており、CA Performance Center の個別のインスタンスとして有効に機能します。 各インスタンスには、テナント間で共有されない複数のユーザおよび役割を含めることができます。

各レベルにおいて、2 つの顧客（テナント）は完全に区別されます。 あるテナントに割り当てられたユーザは、別のテナントからのデータを参照できません。 テナント内で管理者権限があるユーザは、その同じテナント内の設定の参照、変更のみが可能です。

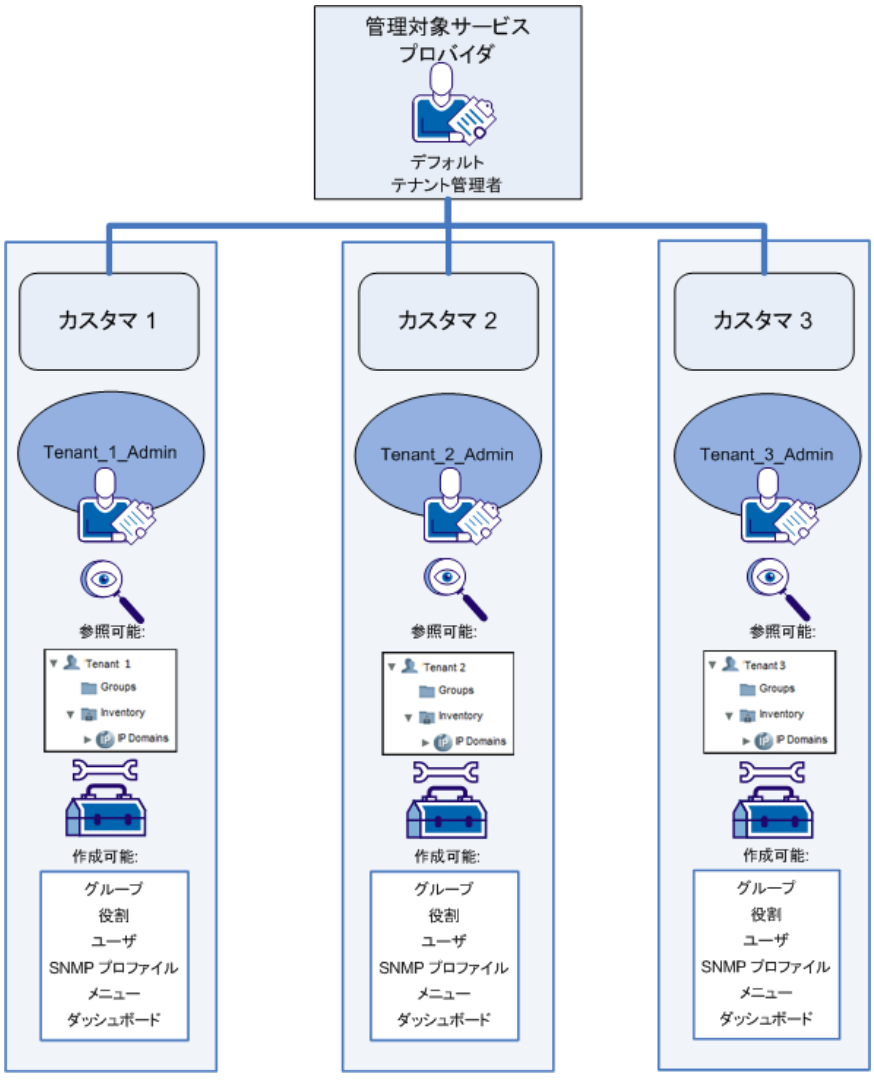
設定とデータはテナント間で共有されませんが、主製品管理者はそれらを参照できます。 *グローバル管理者*は、すべてのテナントの製品設定を管理します。 このユーザ アカウントはデフォルト テナントと関連しているため、「デフォルト テナント管理者」とも呼ばれ、テナントを作成してテナント設定を実行します。 デフォルト テナント管理者は通常 MSP 自体を表します。

マルチ テナンシーをサポートするための管理者役割

マルチ テナンシーを展開するために、次の 2 つの管理者役割がサポートされています。

- グローバル管理者（63以下のページで定義参照：）- デフォルト テナント管理者、通常は MSP を指します。製品設定とデータはテナント間で共有されませんが、デフォルト テナント管理者はそれらにアクセスして、すべての設定を変更できます。 このユーザには事前定義の「管理者」役割を付与する必要があります。
- テナント管理者（63以下のページで定義参照：）- 単一のテナントに関連付けられた制限付き管理者。 このオペレータは、ホスト（通常は MSP）に属している共有インフラストラクチャまたは設定にアクセスできません。 テナント ユーザ アカウントには、これらの管理者アカウントの 1 つ以上を含めることができます。

テナントを作成するときに、ユーザ インターフェースからテナント管理者とテナント ユーザ アカウントの作成が促されます。 これらのアカウントを使用するオペレータは、このテナント内でしか監視タスクや管理タスクを実行できません。 彼らは、他のテナントに関連付けられた管理対象アイテムやパラメータにはアクセスできません。 下の図を参照してください。



詳細情報:

テナントの追加 (P. 31)
テナントの管理 (P. 35)

展開オプションについて

展開計画は、いくつかの重要な要素を考慮して作成する必要があります。以下の要素について十分に理解してから、テナントまたは IP ドメイン定義を作成してください。

- 監視する環境のサイズ、範囲、および構成
- インストールおよび登録を計画している CA データ ソース
- CA Performance Center でのマルチテナンシー機能に対するデータ ソースのサポート

これらのすべての要素を考慮して、展開の方針を決定します。たとえば、一部のデータ ソースは、テナント内で作成される IP ドメインを検出しません。

マルチテナンシーの構成オプションを計画する際は、一度データ収集を開始すると、IP ドメインやテナント定義を後から変更するのは非常に困難になるということに注意してください。 CA データ ソースが収集および集計するデータには、元の IP ドメインまたはテナントとのデータベースによる関連付けが保持されます。

テナントまたは IP ドメインを作成する前に、「マルチテナンシーのデータ ソース サポート (P. 10)」および「ドメイン監視に関する考慮事項 (P. 13)」を参照して、記載されているガイドラインを把握しておくことを強く推奨します。

マルチテナンシーのデータ ソース サポート

CA Performance Center でのマルチテナント監視のサポートは、登録済みのデータ ソースによって制限を受けます。 Data Aggregator データ ソースでは、マルチテナンシーおよび IP ドメイン監視が完全に実装されていますが、以下のデータ ソースではサポートに制限があります。

- CA Network Flow Analysis
- CA Application Delivery Analysis
- CA Spectrum
- CA eHealth
- CA Application Performance Management

以下の表に、マルチテナント展開機能のデータ ソース サポートについて要約します。

データ ソース	サポートされている機能	注:
Data Aggregator	すべて： ■ IP ドメイン ■ デフォルトのテナント設定（テナント グループや SNMP プロファイルなど） ■ 管理対象アイテムのデフォルト テナント所有権 ■ 管理対象アイテムのカスタム テナント設定および所有権	すべてのマルチテナンシー機能のフルサポート
CA Network Flow Analysis	すべて	テナントと IP ドメインを各 Harvester およびルータを割り当てます。テナント割り当ては、使用可能な設定アイテムを確定します（テナント SNMP プロファイルなど）。 「展開に関するその他の考慮事項 (P. 15)」にいくつかの制限事項が記載されています。
CA Application Delivery Analysis	■ IP ドメイン ■ カスタム テナント設定	データ ソース インターフェース内のデータを分離しません。
CA Spectrum	すべて ただし、テナンシーは CA Performance Center インターフェースのみで表示され、OneClick には表示されません。	OneClick は CA Performance Center から IP ドメインを受信します。 IP ドメイン内のモデルは、CA Performance Center と同期されます（したがって、カスタム テナントに関連付けられます）。
CA Unified Communications Monitor	すべて	場所は、サブネットによって IP ドメインに自動的に関連付けられます。

データ ソース	サポートされている機能	注:
CA eHealth; CA Application Performance Management	なし。	これらのデータ ソースからのアイテムはすべてデフォルト テナントおよびデフォルト IP ドメインに関連付けられます。 これらのデータ ソースからのアイテムをサービス プロバイダ グループに追加して、それらへのテナント アクセス権を付与します。

注:

CA Application Delivery Analysis では、テナントの概念を使用せずに IP ドメインを監視します。 そのため、CA Performance Center は、デフォルト テナント内の CA Application Delivery Analysis からすべてのアイテムを受信します。 ただし、CA Application Delivery Analysis では IP ドメインをサポートしています。 CA Performance Center は、IP ドメインに基づいて、これらのアイテムをテナントに関連付けることができます。 一部の管理対象アイテムは、デフォルト テナントとカスタム テナントの間で重複していることに注意してください。

CA Spectrum r9.3 以降では、カスタム IP ドメインをサポートしています。 CA Spectrum デバイスは、カスタム IP ドメイン、またはデフォルト IP ドメインのいずれかに配置できます。 テナントは、CA Spectrum OneClick には表示されません。 ただし、CA Performance Center のテナントは、IP ドメインに基づいて CA Spectrum デバイスを関連付けています。 グローバル管理者は、これらのアイテムを［サービス プロバイダ アイテム］グループに配置することで、テナント ユーザの監視対象に含めることもできます。詳細については、「CA Spectrum-CA Performance Center Integration Guide」を参照してください。

ドメイン監視に関する考慮事項

IP ドメイン機能は、複数のエンタープライズ システムを別々に監視する必要がある環境をサポートします。 たとえば、管理対象サービス プロバイダ（MSP）が、さまざまな顧客のシステムおよびネットワークを個別に監視するような場合です。 MSP 管理者は、各顧客の企業に対して CA Performance Center でテナントを作成します。 各テナントのデータおよび設定は、他のすべてのテナント ユーザからは非表示になります。

ただし、他の状況では、マルチテナンシーを使用せずに CA Performance Center で複数の IP ドメインを展開できます。 すなわち、一部の展開モデルは、デフォルト テナント内にある複数の IP ドメインから構成されます。

IP ドメインを使用すると、データ収集のパラメータを制御できます。 カスタム IP ドメインを使用して、どの収集デバイスがユーザのインフラストラクチャ内の管理対象アイテムを監視するのかを決定します。 Data Collector や CA Unified Communications Monitor Collector などの収集デバイスは、それぞれ一つの IP ドメイン内で動作します。

以下のリストに、デフォルト テナント内に複数の IP ドメインを展開できる環境の例を示します。

- CA Application Delivery Analysis または CA Spectrum データ ソースが含まれる展開。

  CA Application Delivery Analysis による IP ドメインの監視では、テナントの概念はありません。 カスタム テナント内に作成した IP ドメインは検出されません。 Data Aggregator または CA Network Flow Analysis がこれらのドメイン内のアイテムを監視する場合、それらのアイテムは CA Application Delivery Analysis で重複として表示されます。 重複したデータは集計されません。

  同様に、CA Spectrum では、デフォルト テナント領域の IP ドメインのみを認識します。 CA Application Delivery Analysis または CA Spectrum の展開を計画するときは、グローバル管理者としてログインしてから IP ドメインを作成してください。

- 負荷分散を必要とする大規模な展開。

  たとえば、ユーザの企業に、多数のインターフェースを持つ 10 個のルータ、IP SLA テスト、および QoS ポリシーが配置されているとします。そのような展開では、数百のサーバがある環境で CPU とメモリの統計情報のみが監視されるのと同じようなポーリング負荷が発生します。

  負荷の高いルータを監視するために、IP ドメインを作成して、そのドメイン内に Data Collector 用の強力なシステムを展開できます。さらに、そこまで強力ではない Data Collector 用のシステムを使用して、別の IP ドメインにあるサーバを監視できます。適切な IP ドメインでディスカバリを実行することで、それぞれの Data Collector がポーリングするデバイスを決定することができます。

- 大量の統計情報の収集によるネットワークへの影響を最小限に抑える方法

  たとえば、監視対象のデバイスの近くに Data Collector を展開できます。Data Collector は大量の統計情報を処理することができ、その情報を非常に小さな監視対象メトリック セットに削減して、Data Aggregator に送信できます。 その結果、2 つのコンポーネント間のネットワークを通過するデータは、より少なくて済みます。

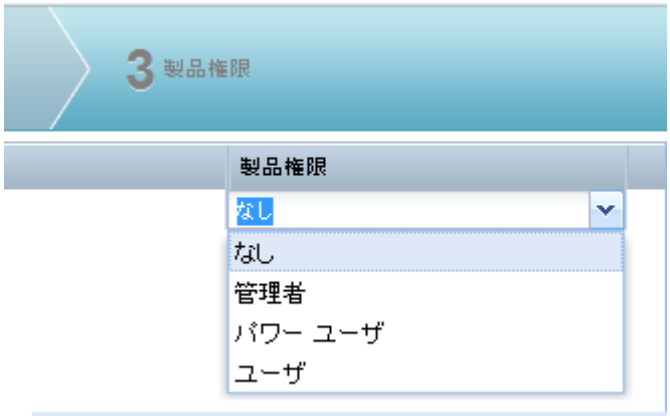
- 機密性の高い SNMP トラフィックを DMZ などの特定の領域から分離。

  たとえば、セキュリティ ポリシーにより、ネットワーク領域の境界となるルータを越えて SNMP トラフィックを転送できないとします。 1 つの選択肢は、ルータの背後に Data Collector を展開することです。処理済みのメトリックを Data Aggregator に返すための経路は開いている必要があります。

  コンポーネント間を移動するメトリック データは暗号化されません。ただし、メトリック データは、「スニッフィング」がより困難な方法でパッケージ化および圧縮されます。その結果、データは無変換の SNMP フローよりも安全になります。 このようなセットアップを行うには、DMZ 用の IP ドメインを作成し、その IP ドメイン内に Data Collector を展開します。

展開に関するその他の考慮事項

「マルチテナンシーのデータ ソース サポート (P. 10)」の図に示されるように、CA Network Flow Analysis は CA Performance Center のマルチテナンシー機能をサポートします。 ただし、ユーザ アカウントの製品権限を選択する際は注意してください。 データ ソースへの製品権限により、CA Performance Center のビューからデータのソースにドリルダウンできます。



異なるカスタマ環境から個別のテナントにデータを慎重に分離しているケースでは、ユーザが CA Network Flow Analysis インターフェースに戻らないようにする必要がある場合があります。 そのインターフェースでは、テナント分類は管理者およびパワー ユーザ レベルのユーザに適用されません。データはすべてレポートに表示できます。製品権限は、［ユーザ アカウントの追加］または［ユーザ アカウントの編集］ウィザードで設定されます。

重要: CA Network Flow Analysis データ ソースのすべてのデータへのアクセスを必要としないユーザには、「ユーザ」製品権限を割り当てます。

考慮すべきもう 1 つのポイントは、CA Network Flow Analysis の［レポートの管理］役割の権限です。 この役割の権限を有するユーザは、CA Network Flow Analysis コンソールですべてのデータを表示できます。

マルチテナンシーを展開する方法

CA Performance Center にマルチテナント環境を作成するには、事前定義済みの管理者の役割を持つユーザが最初の手順を実行する必要があります。この事前定義済み管理者アカウントは「グローバル」管理者と呼ばれ、デフォルト テナント領域に関連付けられています。

マルチテナント展開をセットアップするには、以下のプロセスを推奨します。

1. MSP カスタマの仮想システムおよび物理システムに関するデータを収集します。
2. IP ドメインおよび SNMP バージョン、コミュニティまたは各 MSP カスタマのパスワードのリストを作成します。
3. テナントを作成します。テナント定義は、関連するカスタマを識別するための少数の単純なパラメータから構成されます。

   またテナント定義には、テナント管理者およびユーザ アカウントも含まれます。
4. グローバル管理者としてログインし、テナント設定を管理するためのテナント範囲を設定します。
5. カスタマ ネットワークを表すために、少なくとも 1 つの IP ドメインを作成します。
6. カスタマ インフラストラクチャをサポートするデバイスの SNMP ポーリングを有効にするために、少なくとも 1 つの SNMP プロファイルを作成します。
7. テナント管理を終了します。テナントごとに上記の手順を繰り返します。

データ ソースがすでに登録されており、データを収集している場合は、数分待ちます。CA Performance Center は、監視中に検出されたアイテムに基づいてシステム グループを作成します。これらのグループは、カスタム グループを作成し、権限としてユーザに割り当てる際に役立ちます。詳細については、「グループ (P. 18)」を参照してください。

システム グループが利用可能な場合は、以下の手順を行います。

1. テナント設定を管理するため、またはテナント管理者としてログインするためにテナントの範囲を設定します。

2. カスタマ ネットワークおよびシステムを表すのに必要なカスタム グループを作成します。
3. 権限グループを追加するには、デフォルトのテナント ユーザ アカウントを編集します。

   このユーザに可能性の高い役割、およびこのユーザが管理する管理対象アイテムを考慮します。
4. このカスタマに必要な、その他のカスタム役割、ユーザ アカウント、SNMP プロファイル、ダッシュボードおよびメニューを作成します。

各カスタマの IT スタッフと協力して、テナント管理者としての役割を果たすユーザを指定します。必要に応じて、テナント管理者はカスタム グループおよび追加のユーザ アカウントを作成することで、テナント設定を行えます。

テナントについて

デフォルトでは、すべての管理対象アイテムおよびそのデータは、デフォルト テナントに関連付けられます。 CA Performance Center にカスタム テナントを追加すると、個別の CA Performance Center 監視環境を作成して単一のユーザ インターフェースから管理できます。 テナントは、管理対象サービス プロバイダが管理するカスタマ環境を表します。 各テナント環境は独立しており、CA Performance Center の個別のインスタンスとして有効に機能します。 各インスタンスには、テナント間で共有されない複数のユーザおよび役割を含めることができます。

基本的なテナント定義には MSP 顧客を識別するためのいくつかのパラメータが含まれており、管理対象アイテムおよび顧客用の設定を他のオペレータがアクセスできるようになります。 テナントごとに 1 つ以上の IP ドメイン (63以下のページで定義参照：)が必要です。 その後、ユーザまたはテナント管理者は、企業のインフラストラクチャおよびアプリケーションを管理するために、以下の定義を必要な数だけ設定できます。

- SNMP プロファイル
- その他のユーザ アカウント
- 役割
- カスタム グループ
- カスタム ダッシュボード
- カスタム メニュー

カスタム IP ドメイン (P. 24)は、管理対象アイテムをテナントと関連付ける方法を提供します。有効なテナント定義には、少なくとも 1 つのカスタム IP ドメインが含まれます。 有効なテナントを CA Performance Center に追加すると、IP アドレスがテナント ドメインに一致するすべてのアイテムが、そのテナントにすぐに関連付けられます。

グループ

管理者は、CA Performance Center 内の管理対象アイテムを構成するためにカスタム グループ構造を作成できます。 グループはフィルタのように動作し、関連するアイテムを構成し、レポート データをより活用できます。たとえば、グループは物理的な場所、デバイスおよびそのインターフェース、または類似デバイスのグループを表すことができます。 カスタム グループを使用すると、オペレータに対して選択したデータへのアクセスを限定しながら、オペレータが監視可能なアイテムを表示できます。

グループを適切に設定すると、セキュリティ上の理由により、選択したデータを CA Performance Center オペレータに表示しないようにできます。管理者は、ユーザに対し、ユーザの責任の範囲に入っているデータへのアクセスを選択的に許可できます。 またグループは、パフォーマンスの監視、レポートおよびトラブルシューティングも容易にします。

テナントには、カスタマ展開の分離を保守するための特別なタイプのシステム グループが含まれます。 またテナントには、カスタム グループ化構造全体を含むこともできます。

詳細:

カスタム グループの作成 (P. 52)
マルチテナント展開のグループ (P. 21)

システム グループ

データ ソースを登録すると、システム グループが自動的に作成され、データベースのアイテムが構成されます。 カスタム グループを構築し、インベントリのアイテムを管理するには、システム グループを使用します。

システム グループは編集できません。ただし、サブグループとしてカスタム グループに追加し、権限グループとしてユーザ アカウントに割り当てることができます。 ロック アイコンはそれらの読み取り専用ステータスである ▶  を示します。

以下のシステム グループは、グループ ツリーに自動的に含まれます。

インベントリ ▶ 

すべての登録済みデータ ソースによって検出されたすべての管理対象アイテムを含みます。 データ ソース、IP ドメイン、管理対象アイテムをサブグループ内で構成します。

CA Infrastructure Management Data Aggregator データ ソースを登録している場合、以下のシステム グループがグループ ツリー内に同じレベルで表示されます。

コレクション ▶ 

管理対象アイテムのコレクションを表します。 コレクションは、CA Infrastructure Management 監視プロファイルで指定されたルールを使用して監視されるアイテムのグループ化です。 「ファクトリ」コレクションはグループ ツリーに表示されません。

このグループでは、カスタムの CA Infrastructure Management コレクションを作成できます。コレクション グループに追加するサブグループは、コレクションとして CA Infrastructure Management Data Aggregator に同期されます。

少なくとも 1 つのカスタム テナントを作成すると、マルチテナント展開用の特別グループも表示されます。 詳細については、「マルチテナント展開用のグループ (P. 21)」を参照してください。

インベントリ グループには、自身のシステム サブグループが含まれており、管理対象アイテムをタイプによって構成します。システム サブグループは、ルータ グループなど複数のデータ ソースによって共有されます。他のサブグループは、単一のデータ ソースに固有です。

インベントリ ノードを展開すると、以下のシステム グループが表示されます。

すべてのアイテム ▶ 

タイプによって分類された管理対象アイテムのサブグループが含まれます。

データ ソース 

CA Performance Center に登録されているすべてのデータ ソースを含んでいます。このノードの下に、各データ ソースの専用グループがあります。

注: 通常データ ソースには、自身のシステム サブグループがあり、データ ソース グループを展開すると表示されます。

IP ドメイン 

管理者によって作成されたすべてのカスタム IP ドメインを含んでいます。 デフォルト ドメインも含んでおり、デフォルト ドメインにはカスタム ドメインに明示的に割り当てられないすべてのアイテムが含まれます。 詳細については、「IP ドメイン (P. 23)」を参照してください。

インベントリ グループの［すべてのアイテム］サブグループには、アイテムの以下のシステム サブグループが含まれます。 それらのグループの実際のメンバシップを表示するには、［アイテム］タブのいずれかのグループをクリックします。

すべての Ping 可能デバイス 

SNMP を使用した接続が不可能であると検出されたすべてのデバイスを含んでいます。

ESX ホスト 

仮想マシンをホストするすべての VMware サーバを含んでいます。

インターフェース 

すべてのデータ ソースのルータとスイッチのインターフェースを含んでいます。

ルータ 

すべてのデータ ソースのすべてのルータを含んでいます。

サーバ 

すべてのデータ ソースのすべてのサーバを含んでいます。

CA Application Delivery Analysis ネットワーク 

CA Application Delivery Analysis が監視したすべてのネットワークを含んでいます。 CA Application Delivery Analysis ネットワークは、IP アドレスとマスクから構成されます。

スイッチ

すべてのデータ ソースのスイッチが含まれます。

仮想マシン

すべての ESX サーバ上で実行されるすべての仮想マシンを含んでいます。

マルチテナント展開のグループ

グローバル管理者（デフォルト テナントの管理者）が少なくとも 1 つのテナントを作成すると、マルチテナントをサポートする機能が有効になります。 「マルチテナント展開」は、IP アドレスが重複する可能性のある個別の複数の企業から構成されます。 ［グループ］ツリーに追加のグループが表示されると、管理者はテナント インベントリを構成し、権限を割り当てることができます。

定義済みテナント

すべてのテナントを含みます。 テナントは、単一の CA Performance Center インスタンスで個別のカスタマ環境を監視するために、IP ドメインと共に使用されます。 各テナントには、テナント間で共有されないアイテムのサブグループを複数含めることができます。

テナント管理者は、テナント内にカスタム グループを作成できます。 グローバル管理者の場合、テナント グループは［グループ］ツリーの［テナント］ノードに表示されます。

サービス プロバイダ グローバル グループ

グローバル管理者がテナント環境を管理するのに役立つアイテムのグループが含まれています。 これらのグループは、管理者がテナントの IP ドメインに明示的に関連付けられていない共有アイテムを視覚化および構成するのに役立ちます。

共有アイテムからのデータにアクセスを割り当てるグループは、各テナントの下に表示されます。「サービス プロバイダ定義済みグループ」を参照してください。

トップレベルのインベントリ グループを展開すると、以下の追加グループがマルチテナント展開に表示されます。

ドメイン 

テナントと管理対象アイテムの関連付けに使用されるすべてのカスタム IP ドメインを含みます。デフォルト ドメインも含んでおり、デフォルト ドメインにはカスタム ドメインに明示的に割り当てられないすべてのアイテムが含まれます。詳細については、「IP ドメイン (P. 23)」を参照してください。

マルチテナント展開では、各テナントに自身のグループがあります。 グローバル管理者がサービス プロバイダ グループにテナント グループ外のアイテムへのアクセスを許可しない限り、テナント ユーザにはテナント グループ外のアイテムは表示されません。

グループ(テナント) 

グローバル管理者またはテナント管理者は、カスタム グループを作成できます。 [グループの追加] ボタンを有効にするには、このノードを選択します。

インベントリ(テナント) 

テナント IP ドメインに関連付けられているすべての管理対象アイテムを含んでいます。すべての登録済みデータ ソースからのアイテムを、このグループに表示できます。

また各テナントには、インベントリ グループに以下のシステム サブグループがあります。

IP ドメイン

このテナントと関連付けられた IP ドメインを表します。検出されたすべての管理対象アイテムが、その IP ドメインによってこのテナントに関連付けられます。 テナントの管理対象アイテムを参照するには、［グループ］ツリーのテナント IP ドメインをクリックします。

サービス プロバイダ定義済みグループ 

このテナントがアクセスできるデータを持つ共有アイテムをグローバル管理者が入力したグループが含まれます。 これらのグループを使用して、選択したテナント ユーザ アカウントに共有デバイスのデータへのアクセスを付与します。

たとえば、サービス プロバイダが所有するルータは、複数のテナント ドメインからのトラフィックを処理します。サービス プロバイダ定義済みグループを使用して、グローバル管理者は、そのルータのデータにテナント アクセスを割り当てることができます。この戦略によって、テナントはシステム パフォーマンスの独立した監視および検証を実行します。

サービス プロバイダ アイテム 

テナント IP ドメインに明示的に関連付けられないすべてのアイテムが含まれます。 このようなアイテムは、このグループに自動的に配置されます。 グローバル管理者はこれらのアイテムを「サービス プロバイダ定義済みグループ」に追加して、共有アイテムのデータにテナント アクセスを割り当てることができます。

IP ドメイン

*IP ドメイン*は、さまざまなデバイスおよびネットワークからのデータを識別する論理的なグループです。 ドメインによる監視は、IP アドレスと、それに関連する別のカスタマ ネットワークに属するインターフェースまたはアプリケーションを別々に監視することを意味します。 適切な権限と組み合わせることで、IP ドメインは単一のコンソールから監視されますが、ユーザには、自身が監視するドメインのデータのみ表示されます。

IP ドメインは、サービス プロバイダが個々の顧客ネットワークの監視に使用するために設計されました。 そのため、顧客アカウント（テナント）ごとに 1 つ以上の IP ドメインが含まれています。

管理者とデザイナは、カスタム ダッシュボードを作成して、特定のドメインまたはドメインのグループでのアクティビティを監視することができます。 サービス プロバイダ管理者（つまり、グローバル管理者 (63以下のページで定義参照：)）は、すべての IP ドメインからのデータを参照できます。 ただし、1 つの顧客ドメインからのデータだけを参照する権限を持つユーザ アカウントを作成できます。

多くの CA データ ソースがドメインに対応しています。その対応をデータ ソース内で有効にするには、CA Performance Center への登録が必要です。

IP ドメインについて

IP ドメインを使用すれば、潜在的な IP アドレス競合を解決できます。 ドメイン識別子は、重複 IP アドレスとして表示されかねない 2 つの管理対象アイテムが実際には 2 つの*異なる*管理対象アイテムであることを示します。 たとえば、1 つの IP アドレスを持つルータに、それぞれ別の企業に所属している複数のインターフェースが設定されているとします。 各インターフェースの DNS ID は、その IP ドメインを決定します。 ドメイン内のアイテムからのデータは、インターフェース所有者に対応する 1 人のテナントに報告されます。

ドメイン サイズによってサービス プロバイダ環境で CA データ ソースを機能させることができます。 同じソフトウェアで、複数のネットワークを個別のエンティティとして監視します。 ドメインを使用すると、Data Collector は、管理対象アイテムとデータを適切なサービス プロバイダ顧客、つまり、*テナント*に関連付けることができます。

データ ソースが登録されるとすぐに、それぞれのドメイン監視が有効になります。 ただし、1 つ以上のカスタム IP ドメイン定義が CA Performance Center 内で作成されるまで、ドメイン識別子がデータ ソース内に表示されません。 ドメイン監視が有効になると、以下の管理対象アイテム タイプがデフォルト ドメインに関連付けられます。

- デバイス
- インターフェースとインターフェース アドレス
- ネットワーク
- VoIP 場所

これらのアイテム タイプを監視するデータ ソースは、CA Performance Center との同期中に、ドメイン識別子とその他のプロパティを報告します。 データ ソースは、ドメイン ID プロパティを含めることにより、アイテムとドメインを関連付けることができます。 ドメイン ID が報告されないアイテムは、自動的に、デフォルト ドメインに配置されます。

管理者の役割を持つ CA Performance Center ユーザはカスタム IP ドメインを作成できます。 これらのドメインは、同期中に、データ ソースに送信され、そこで、データ収集設定中に使用可能になります。 ドメイン定義は、同一の CA Performance Center インスタンスに登録されたデータ ソース間で共有されます。

グループ ツリーでドメイン グループは、それ自体がテナントのサブグループであるインベントリ グループに含まれます。 ドメイン グループには、デフォルト ドメインと作成されたカスタム ドメインが含まれます。

データ ソース内でカスタム ドメインに割り当てられていないアイテムは、デフォルト ドメインに関連付けられます。 この割り当ては、監視対象トラフィックを識別するためにカスタム IP ドメインを使用していないユーザには認識されません。

詳細情報:

テナント IP ドメインの設定 (P. 34)
アイテムと IP ドメインの関連付け (P. 26)
IP ドメイン (P. 23)
IP ドメインの設定方法 (P. 26)

IP ドメインの設定方法

IP ドメインの機能は、管理対象アイテムを含めるためのグループと非常によく似ています。 グループと同様に、IP ドメインは CA Performance Center 内で作成されますが、アイテムをドメインに割り当てるタスクはデータ ソース内で実行されます。

IP ドメインは標準の CA Performance Center インストールでは必ずしも必要ありません。 ただし、マルチテナント環境に CA Performance Center を展開する場合は、IP ドメインが必須です。

IP ドメインを設定するためのワークフローは次のとおりです。

1. テナントを作成します。詳細については、「テナントの作成と管理 (P. 29)」を参照してください。
2. テナントごとのカスタム IP ドメインを作成します。 詳細については、「テナント IP ドメインの設定 (P. 34)」を参照してください。
3. すべてのデータ ソースを同期化します。

   手動でデータ ソースの同期を実行することも、次の自動同期が発生するのを待つこともできます。詳細については、「データ ソースの同期」を参照してください。
4. データ ソースごとの手順に従って、アイテムとカスタム ドメインを関連付けます。詳細については、「アイテムと IP ドメインの関連付け (P. 26)」を参照してください。

   注: データ ソースは、カスタム IP ドメインに明示的に割り当てられていないアイテムをデフォルト ドメインに関連付けます。
5. CA Performance Center 内のすべてのデータ ソースを同期させます。アイテムが検出されるとすぐに、グループ ツリー内のドメイン コンテナがそれらのアイテムで生成されます。

アイテムと IP ドメインの関連付け

ユーザが CA Performance Center で IP ドメインを作成しますが、アイテムとドメインを関連付けるのはデータ ソースです。 データ ソースが、監視対象のデータ トラフィックから検出したアイテムにドメイン ID を割り当てます。 そのため、データ ソース管理者が収集パラメータを設定するまで、管理対象アイテムにドメイン関連付けが送信されません。

テナントにはその IP ドメイン内のアイテムしか含まれていません。 そのため、以下の条件が揃うまで、テナント ダッシュボードは空のままです。

- IP ドメインがテナントに関連付けられる。
- CA Performance Center とデータ ソース間で同期が発生する。
- データ ソースが管理対象アイテムと IP ドメインを関連付けるように設定されている。

テナントを作成した直後に IP ドメインを作成することをお勧めします。「IP ドメインの設定方法 (P. 26)」に記載されている推奨ワークフローに従ってください。

ドメインが正しく生成されたことを確認するには、全監視対象エンタープライズ システム内の全ネットワークの IP アドレス構成を理解している必要があります。

第 2 章: テナントの作成と管理

このセクションには、以下のトピックが含まれています。

テナントのセットアップ方法

グローバル管理者は、CA Performance Center にマルチテナント展開をセットアップする最初の手順を実行する必要があります。 グローバル管理者はデフォルト テナントと関連付けられており、すべてのテナント設定パラメータへのアクセス権があります。 事前定義済みの管理者の役割によって、ユーザ アカウントでグローバル管理者アクセス権が有効になります。

CA Performance Center にテナントを作成する前に、顧客と密接に連携することをお勧めします。 顧客環境に関するいくつかの基本情報を収集します。 たとえば、この顧客に対して監視される IP ドメインを認識している必要があります。 物理および仮想システム トポロジに関する知識は、顧客環境を表すカスタム グループ化構造を作成するのに役立ちます。

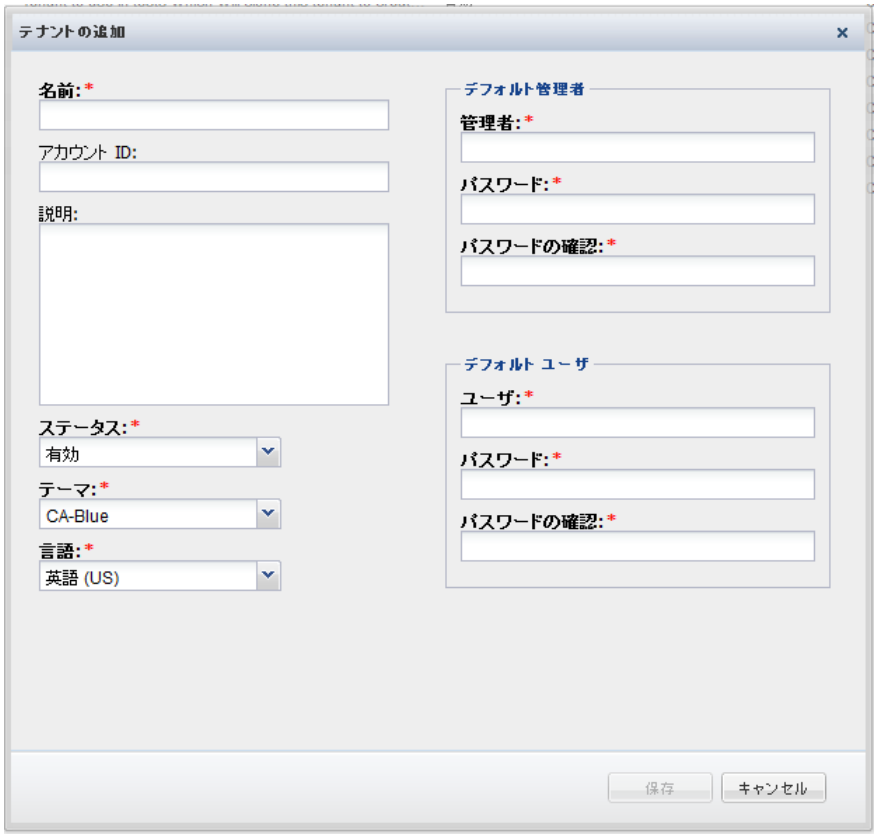
テナント管理者として機能するユーザを選択します。 このユーザは、顧客のシステムおよびネットワークについて幅広い知識を持っている必要があります。指定されたテナント管理者は、そのような知識に基づいて、カスタム グループ、役割、ユーザ、SNMP プロファイル、メニュー、およびダッシュボードを作成することで、テナント設定を行えます。

新しいテナントをセットアップするには、以下の手順に従います。

1. 顧客ネットワーク上の IP ドメインおよび SNMP コミュニティのリストを取得します。
2. テナント管理者として機能するユーザを指定します。 たとえば、監視される顧客サイトの担当者を選択します。

3. テナント定義を追加します。

   テナント作成の一環として、管理者権限を持つテナント ユーザ アカウントも作成します。



4. テナントを管理します（テナント範囲を設定することにより、テナント管理者として一時的にログインします）。
5. テナントに対して少なくとも 1 つの IP ドメインを作成します。
6. テナント環境内のデバイスに SNMP アクセスを行えるように、少なくとも 1 つの SNMP プロファイルを作成します。

   注: データ収集がすでに実行されている場合、テナント システム グループは自動的に作成され、このドメインからデータが入力されます。グループがすでに利用可能な場合、テナント ユーザにアクセス権限を割り当てることができます。

その後、指定されたテナント管理者はログインできます。 このユーザは他のすべてのテナント設定（テナントが必要とするすべてのカスタム グループ、役割、ユーザ、メニュー、およびダッシュボード）をセットアップできます。

テナントの追加

事前定義済みの管理者の役割を持つユーザ（「グローバル」管理者）のみが、カスタマのネットワークおよびシステムを識別するテナント定義を追加できます。 このユーザは、デフォルト テナントのテナント管理者に相当します。

またテナント作成中に、テナント管理者およびテナント ユーザも作成できます。 グローバル管理者と異なり、テナント管理者 (63以下のページで定義参照：)は単一のテナントのデータおよび設定のみを参照できます。テナント管理者は、他の MSP カスタマからのデータにはアクセスできません。

複数のテナントをすぐに追加するには、［テナントのクローン作成］機能を使用します。

次の手順に従ってください:

1. 事前定義済みの（グローバル）管理者の役割を持つユーザとしてログインします。

   注: テナント管理者はテナントを作成できません。

2. ［テナントの管理］ページに移動します。

   ページに、現在のテナントのリストが表示されます。

3. ［新規］をクリックします。

   ［新しいテナントの追加］ページが開きます。

4. 必要な情報を入力し、次に表示されたフィールドで選択します。

   名前

   テナントの名前です。

   アカウント ID

   このテナントを識別します。通常は、MSP アカウント番号と一致します。

説明

（オプション）テナントに関する説明です。

ステータス

このテナントのステータスです。 以下のオプションのいずれかを選択します。

- 有効： 使用するテナント ユーザ アカウントを有効にします。
- 無効： このテナントに関連付けられたユーザ アカウントによるすべてのアクションを禁止します。

テーマ

このテナントに使用する形式（ブラウザ ウィンドウ内のページの外観を制御するテーマ）を指定します。 このテナントに関連付けられているユーザ アカウントを持つすべてのオペレータにこのテーマが表示されます。

言語

このテナント用の言語（ロケール）を指定します。 リストから言語を選択します。

5. このテナントのテナント管理者アカウントを作成します。 次のアカウント パラメータの情報を入力します。

管理者

テナント管理者アカウントのログイン名です。

パスワード

ユーザ アカウント用のパスワードを定義します。パスワードは 32 文字までに制限されています。

パスワードの確認

パスワードを確認します。

6. テナントのユーザ アカウントを作成します。 関連するオペレータは、特定のテナントのダッシュボードにはアクセスできますが、管理機能にはアクセスできません。
7. ［保存］をクリックします。

新しいテナント定義が作成されますが、IP ドメインなど必要なパラメータが不足しています。詳細については、「テナント範囲の設定 (P. 33)」を参照してください。

詳細情報:

マルチ テナンシーをサポートするための管理者役割 (P. 8)

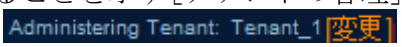
テナント範囲の設定

［テナントの管理］機能を使用して作成したテナントの環境を設定します。たとえば、テナントにカスタム IP ドメイン、ユーザ アカウントまたはグループを追加できます。 テナントの観点から CA Performance Center にアクセスするために、テナント範囲を設定します。

次の手順に従ってください:

1. 事前定義済みの管理者の役割（グローバル管理者）を持つユーザとしてログインします。
2. ［テナントの管理］ページに移動します。

   ページに、現在のテナントのリストが表示されます。
3. 管理するテナントを選択します。
4. ［管理］をクリックします。

   選択されたテナント環境を管理していることを示す［テナントの管理］インジケータが右上に表示されます。 

   選択されたテナントに関連付けられた設定のみ、表示できます。

   次に、このテナント環境を表し、監視するのに必要な IP ドメイン、SNMP プロファイル、役割、ユーザ、メニューおよびグループを作成します。 テナントを設定するには、［管理］タブの下にあるメニューを使用します。
5. （オプション）［テナントの管理］インジケータの隣の［変更］リンクをクリックして、テナント範囲を別のテナントに変更します。

   ［テナントの管理］ページに戻りますので、別のテナントを選択します。
6. テナント インジケータの隣りの［X］をクリックすると、テナント範囲を終了します。

テナント IP ドメインの設定

テナント定義を作成して設定するには、別の手順を行います。 テナント定義には、テナント環境内の管理対象アイテムの IP アドレスを識別する、少なくとも 1 つの IP ドメインが含まれる必要があります。

テナント定義を作成した後に、テナントの管理対象デバイスが含まれるすべての IP ドメインを追加します。

データ ソースは、別のメソッドを使用して管理対象アイテムを IP ドメインに分類します。 通常、CA Performance Center 内に少なくとも 1 つのカスタム ドメインを作成しない限り、データ ソースにドメイン識別子は表示されません。

次の手順に従ってください:

1. 選択されたテナントのテナント管理者としてログインします。

   または、グローバル管理者として、テナント範囲を設定 (P. 33)してテナント設定にアクセスします。

   選択されたテナント環境を管理していることを示す[テナントの管理]インジケータが表示されます。

2. ［管理］-［カスタム設定］を選択し、［IP ドメイン］をクリックします。

   ［テナント名］ページの［IP ドメインの管理］が開きます。

3. ［新規］をクリックします。

   ［IP ドメイン管理］ダイアログ ボックスが表示されます。

4. 必要なパラメータの情報を入力します。

5. ［保存］をクリックします。

   新しい IP ドメインがリストに表示され、現在のテナントに範囲指定されます。

   さらに多くのドメインをこのテナントに追加する場合は、必要に応じてこの手順を繰り返します。

テナント SNMP プロファイルの設定

テナント定義には、1 つまたは複数の SNMP プロファイルを含めることができます。それらのプロファイルは SNMP を使用するテナント企業システムのデバイスへのアクセスに使用されます。 テナント ユーザ アカウントの 1 つにログインしているオペレータには、そのテナントに対して作成された SNMP プロファイルのみを表示する権限があります。

次の手順に従ってください:

1. このテナントに関連付けられたテナント管理者としてログインします。

   または、グローバル管理者としてログインする場合は、テナント範囲を設定 (P. 33)して、テナント設定にアクセスします。

   選択されたテナント環境を管理していることを示す［テナントの管理］インジケータが表示されます。

2. ［管理］-［ユーザ設定］を選択し、［SNMP プロファイル］をクリックします。

   ［テナント名］ページの［SNMP プロファイルの管理］が開きます。

3. ［新規］をクリックします。

   ［SNMP プロファイルの追加］ダイアログ ボックスが表示されます。

4. 必須フィールドに入力し、必要に応じて任意のデフォルト設定を変更します。 いくつかのフィールドは、［SNMPv3］が選択されているときに限り表示されます。

5. ［保存］をクリックします。

   ［テナント名］ページの［SNMP プロファイルの管理］に戻ります。

   新しいプロファイルが［SNMP プロファイル リスト］に表示され、現在のテナントに範囲指定されます。

テナントの管理

グローバル管理者またはテナント管理者には、テナントに属する監視パラメータを変更するために必要な権限があります。 テナントを管理する際に作成するカスタム定義は、そのテナントに固有であり、他のテナントとは共有されません。

テナントの IP ドメイン、SNMP プロファイル、ユーザ、役割、およびグループ定義を変更するには、テナント管理者の場合は単にログインします。グローバル管理者（デフォルト テナントの管理者）の場合は、選択されたテナントにテナント範囲を設定し、これらの定義へアクセスできるようにする必要があります。

注: グローバル管理者は、各テナントのテナント管理者ユーザ アカウントを作成できます。

テナント範囲が設定されている場合、テナントを管理するための手順は、単一のテナントの環境で実行する手順と同一です。

以下の手順に従います。

1. このテナントに関連付けられたテナント管理者としてログインします。

   または、グローバル管理者としてログインする場合は、テナント範囲を設定 (P. 33)して、テナント設定にアクセスします。

   選択されたテナント環境を管理していることを示す[テナントの管理]インジケータが表示されます。

   現在このテナントに関連付けられた定義のみが表示され、変更できます。

2. ［管理］タブをクリックし、変更するアイテムを選択します。
   - IP ドメイン
   - SNMP プロファイル
   - グループ
   - メニュー
   - 役割
   - ユーザ
3. 選択されたアイテムに固有の手順に従います。
4. 変更を保存します。

   その変更は、管理者、およびユーザ アカウントがこのテナント環境内に作成されているオペレータにのみ表示されます。

詳細情報:

テナント IP ドメインの設定 (P. 34)
テナント役割の設定 (P. 40)
テナント ユーザの設定 (P. 44)
テナント グループの設定 (P. 37)
テナント SNMP プロファイルの設定 (P. 35)
テナント メニューの設定 (P. 39)

テナント グループの設定

テナントを管理するときに作成するグループは、そのテナントに固有です。カスタム グループはテナントの間で共有されません。 マルチテナント監視環境で各テナントの一意の仮想および物理システムを反映するグループを作成します。

次の手順に従ってください:

1. このテナントに関連付けられたテナント管理者としてログインします。

   または、グローバル管理者としてログインする場合は、テナント範囲を設定 (P. 33)して、テナント設定にアクセスします。

   選択されたテナント環境を管理していることを示す[テナントの管理]インジケータが表示されます。

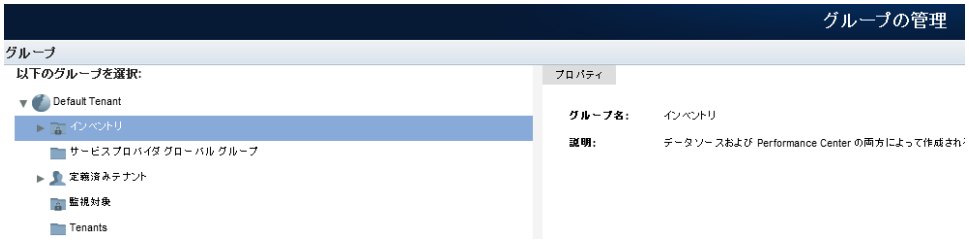
2. ［管理］-［ユーザ設定］を選択し、［グループ］をクリックします。

   ［テナント名］ページの［グループの管理］が開きます。

   テナントに範囲指定されている場合は、グループ ツリーのトップレベルのノードは、テナントに対して自動的に作成されたシステム グループ (P. 18)です。 このグループにサブグループを追加できますが、サブグループを追加しないと変更できません。

   グループ ツリーには、グローバル管理者の判断によってテナント間で共有される、テナント IP ドメイン用のノード、およびシステム グループ用のサービス プロバイダ ノードが含まれます。 サービス プロバイダ グループは、テナント管理者に対しては読み取り専用です。

3. グループ ツリーのテナント ノードを展開します。
4. グループという名前のテナント サブグループ内に新規グループを配置します。



5. ［グループの追加］をクリックします。

   ［グループの追加］ダイアログ ボックスが表示されます。デフォルトでは［新規］タブが選択されています。

6. 以下のパラメータの値を入力します。

   グループ名

   グループの名前を指定します。 グループ名には特殊文字（/&¥,%）を使用できません。

   説明

   （オプション）グループの識別を容易にします。

7. 以下のパラメータの設定を確認します。

   管理対象の子アイテムを含める

   管理対象アイテムがこのグループに追加されると、自動的にその子アイテムも追加されます。 このオプションを無効にして、ルータをグループに追加した場合は、そのルータ上のインターフェースは追加されません。 そのため、それらのデータはドリル ダウン ビュー内に表示されません。

   デフォルト： 選択済み。

8. ［グループ タイプ］リストから［カスタム］または［サイト］のどちらかを選択します。

9. ［保存］をクリックします。

   新規グループが、テナント¥グループ下のグループ ツリー内に表示されます。 このテナントに関連付けられたユーザには、このセクション内のグループおよびアイテムのみが表示されます。 その他のテナントドメインに関連付けられたグループまたはアイテムへのアクセス権はありません。

   ユーザがアイテムを追加するまで、グループにはアイテムが含まれていません。 カスタム グループにアイテムを追加するには、以下の 2 つのオプションがあります。

   - ［グループの管理］インターフェースでアイテムを追加することで、手動でグループを入力 (P. 58)します。
   - グループ メンバシップを管理するルールを作成 (P. 54)します。

テナント メニューの設定

メニューは、ユーザ単位でダッシュボードがどのように構成されるかを決定します。 各テナントの物理および仮想システムを監視するために CA Performance Center を使用する IT スタッフの役割に対応するメニューを作成します。

重要: テナント メニューおよびダッシュボードを管理するための手順は、他のテナント設定を実行するための手順と多少異なります。 メニューを作成するには、テナント範囲を設定した後に、テナント管理者のプロキシも必要です。

次の手順に従ってください:

1. このテナントに関連付けられたテナント管理者としてログインします。

   または、グローバル管理者としてテナント設定にアクセスするには、テナント範囲を設定 (P. 33)し、このテナントに関連付けられたテナント管理者のプロキシを行います。

2. ［管理］-［ユーザ設定］を選択し、［メニュー］をクリックします。

   ［テナント名］ページの［メニューの管理］が開きます。

   ページには、このテナントのメニューの現在のリストが表示されます。

3. ［新規］をクリックします。

   ［メニューの追加］ページが表示されます。

4. メニューの名前を入力します。 この名前は、［ダッシュボード］タブをクリックすると表示されるメニュー内に表示されます。
5. （オプション）他のオペレータが識別しやすくするために、メニューの［説明］を入力します。
6. ［利用可能なダッシュボード］リストのダッシュボードを選択します。
7. 右方向矢印をクリックします。

   ダッシュボードは、［選択されたダッシュボード］リストに移動します。

   複数のダッシュボードを選択するには、Shift キーを押しながらクリックするか、または Ctrl キーを押しながらクリックします。 メニューのダッシュボードの順序を変更するには、上方向および下方向矢印を使用します。

   注: 1 つのメニューに最大で 20 のダッシュボードを割り当てることができます。20 を超えるダッシュボードを追加しようとすると、エラーメッセージが表示されます。
8. ［保存］をクリックし、新しいメニューを保存します。 または、さらにメニューを作成する場合は、［保存してさらに追加］をクリックします。

   このテナントに関連付けられたユーザがログインすると、［ダッシュボード］タブに新しいメニューが表示されます。 その他のテナントに関連付けられたユーザには、それらは表示されません。

テナント役割の設定

テナントを作成し、設定するには、別の手順を行います。 テナント定義には、1 つまたは複数のユーザ アカウント役割を含めることができます。カスタム テナント役割は、インベントリを検索してデータ ソースにドリル ダウンできるが、単一のテナント内のダッシュボードのみを表示できるユーザなど、特定の要件に役立ちます。

各テナント役割でログインするオペレータには、そのテナントに属する管理対象アイテムのデータを表示する権限のみがあります。

事前定義済みの管理者の役割を持つユーザは、以下のような権限を持つテナント管理者の役割を作成することもできます。

- テナント ユーザ アカウントの追加
- カスタム テナント グループの作成
- カスタム テナント ダッシュボードの作成

グローバル管理者と異なり、テナント管理者には他のテナント環境内のデータや管理機能へのアクセス権はありません。 詳細については、「マルチ テナンシーをサポートするための管理者役割 (P. 8)」を参照してください。

次の手順に従ってください:

1. このテナントに関連付けられたテナント管理者としてログインします。

   または、グローバル管理者として、テナント範囲を設定 (P. 33)してテナント設定にアクセスします。

   選択されたテナント環境を管理していることを示すテナント インジケータが表示されます。

2. ［管理者］-［ユーザ設定］を選択し、［役割］をクリックします。

   ［テナント名］ページの［役割の管理］が開きます。

3. ［新規］をクリックします。

   ［テナント名］ページの［役割の追加］が表示されます。

4. 必要な情報を入力し、表示されたフィールドで選択します。

   名前

   新しい役割の名前です。 45 文字までに制限されてます。

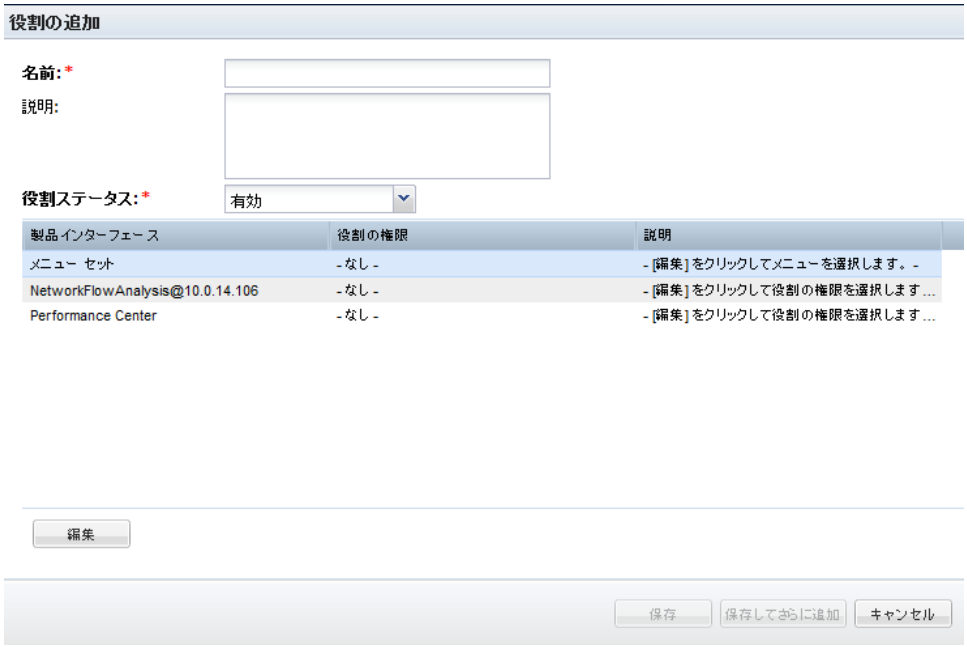
   説明

   （オプション）新しい役割に関する説明です。

役割ステータス

役割を有効にしてアクティブにできます。 ある役割を持つユーザに適切な権限を付与するには、その役割を有効にする必要があります。

テーブルは、役割の権限が役割に選択されていないことを示します。



5. ［メニュー セット］を選択し、［編集］をクリックします。

［編集メニュー セット］ダイアログ ボックスが表示されますので、この役割のメニューを選択します。 ［利用可能なメニュー］領域に表示されたメニューは、役割に追加できます。

6. 左側のアイテムから役割に追加するものをクリックし、次に右方向矢印をクリックします。

   選択したアイテムが［選択されたメニュー］リストに移動します。

   リスト内の複数のアイテムを選択するには、Shift キーを押しながらクリックするか、または Ctrl キーを押しながらクリックします。

7. （オプション）リスト内でアイテムを移動するには、上方向および下方向矢印を使用します。 リスト内のメニューの順序によって、［ダッシュボード］タブ内の順序が決定します。

8. ［保存］をクリックします。

   ［役割の追加］ページに戻ります。

9. CA Performance Center を選択し、［編集］をクリックします。

   ［役割の権限の編集］ダイアログ ボックスが表示されますので、この役割の各アクセス権限を選択します。

10. 役割に追加するアイテムをクリックし、次に右方向矢印をクリックして、そのアイテムを［選択された権限］リストに移動します。

    リスト内の複数のアイテムを選択するには、Shift キーを押しながらクリックするか、または Ctrl キーを押しながらクリックします。

11. （オプション）リスト内でアイテムを移動するには、上方向および下方向矢印を使用します。 役割の権限の順序によって、権限がオーバラップする場合の優先度が決定されます。

12. ［保存］をクリックします。

    ［役割の追加］ページに戻ります。

13. ［保存］をクリックします。

    新しい役割が［役割リスト］に表示され、現在のテナントに範囲指定されます。

テナント ユーザの設定

テナント定義には、1 つまたは複数のユーザ アカウントを含めることができます。 各ユーザ アカウントに関連付けられたオペレータには、そのテナントに属する管理対象アイテムのデータを表示する権限のみがあります。

次の手順に従ってください:

1. このテナントに関連付けられたテナント管理者としてログインします。

   または、グローバル管理者としてログインする場合は、テナント範囲を設定 (P. 33)して、テナント設定にアクセスします。

   選択されたテナント環境を管理していることを示す[テナントの管理]インジケータが表示されます。

2. ［管理］-［ユーザ設定］を選択し、［ユーザ］をクリックします。

   ［テナント名］ページの［ユーザの管理］が開きます。

   ページには、このテナントのユーザ アカウントの現在のリストが表示されます。

3. ［新規］をクリックします。

   ［新規ユーザの作成］ウィザードが開きます。

4. 必要なアカウント パラメータの情報を入力します。

名前

ユーザ アカウントのログイン名です。50 文字までに制限されてます。

説明

（オプション）理解を促すためのユーザ アカウントに関する説明です。

電子メール アドレス

（オプション）電子メール アドレスとユーザ アカウントを関連付けます。

優先言語

ユーザ アカウントに関連付けられたオペレータが使用する言語を指定します。

認証タイプ

このユーザ アカウントに適用される認証方式を指定します。 この方式は［Single Sign-On］設定と一致する必要があります。 以下のいずれかを選択します。

- Performance Center - CA Performance Center によって展開されたデフォルト認証スキーム。
- 外部 - LDAP、SAML などのサードパーティ認証スキーム。

パスワード

ユーザ アカウント用のパスワードを定義します。パスワードは 32 文字までに制限されています。

タイム ゾーン

ユーザがデータを表示するタイム ゾーンと一致します。

デフォルト： UTC （協定世界時）。

役割

ユーザ アカウントに割り当てられた役割です。

アカウント ステータス

アカウントが使用できる（アクティブなっている）かどうか決定します。

他のアカウント パラメータは、テナントに範囲指定されているユーザ アカウントには適用されません。

5. ［保存］をクリックします。

新規ユーザ アカウントは、テナント定義の一部として保存されます。このユーザ アカウントでログインするすべてのオペレータには、このテナントに関連付けられた IP ドメインの管理対象アイテムからのダッシュボードおよびデータをのみが表示されます。

第 3 章: グループ化戦略の展開

このセクションには、以下のトピックが含まれています。

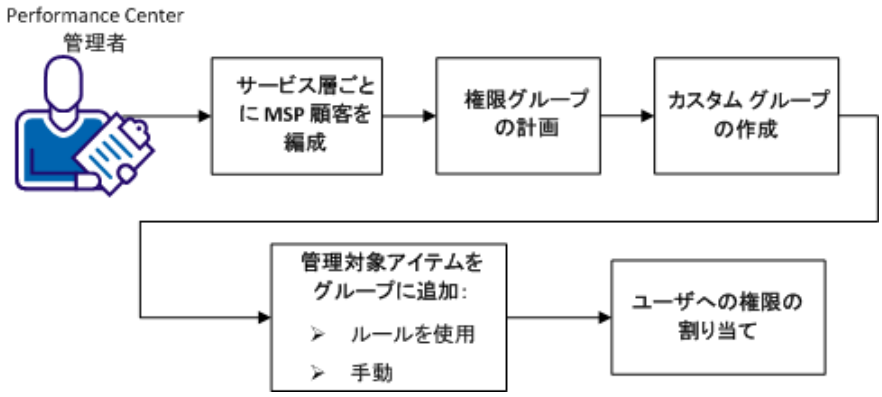
カスタム グループを作成して MSP 顧客を監視

ユーザは大規模な管理対象サービス プロバイダ（MSP）の管理者だとします。 CA Performance Center へのグローバル管理者 (63以下のページで定義参照：)アクセス権があります。 顧客サイトごとにインフラストラクチャの使用状況、ステータスおよびパフォーマンスを監視するため、データ ソースを登録しました。 これで、CA Performance Center 管理者としてカスタム グループを作成し、インフラストラクチャの監視とレポートを構成できるようになりました。

カスタムの CA Performance Center グループは、IT 組織の監視と管理のタスクをサポートします。 カスタム グループを使用することで、管理対象のアイテムを編成してトラブルシューティングをしやすくし、レポートを最適化できます。 グループを使用して、IT スタッフにデータ アクセス権を割り当てることもできます。 権限グループを使用すれば、選択したデバイスやシステムを監視しているチームが確実にパフォーマンス データを参照できるようになります。

MSP の展開には独自の要件がいくつかあります。 MSP レベルでは、幅広い顧客特性に対応するコンテナ グループを作成できます。 これらのグループを使用して IT スタッフや専用の IT リソースに権限を割り当て、個々の MSP 顧客に影響する問題に取り組めるようにします。

グループを作成するには、グループを計画して作成し、データを読み込んでから、ユーザ アカウントへの権限としてグループを割り当てます。



タスク
サービス層ごとに MSP 顧客を編成 (P. 48)
権限グループ割り当ての計画 (P. 50)
カスタム グループの作成 (P. 52)
ルールを使用して管理対象アイテムをグループに追加 (P. 54)
管理対象アイテムのグループへの手動追加 (P. 58)
ユーザへの権限の割り当て (P. 60)

サービス層ごとに MSP 顧客を編成

MSP 顧客システムを監視するためにカスタム グループを作成するには、まずサービス層ごとに顧客を編成してグループを計画します。 カテゴリごとに編成することにより、戦略を意識したグループ作成のアプローチが可能です。 詳細については、「MSP のグループ化戦略 (P. 50)」を参照してください。

通常、MSP 顧客は別のサービス層をサブスクライブします。 ユーザとそのチームが以下のカテゴリの顧客担当だとします。

- ティア 1 - このカテゴリは管理対象サービスの最も上の層を表します。MSP は、すべてのデータ センターおよびすべてのルータのサービス品質（QoS）を連続監視する必要があります。 このカテゴリには、迅速な問題解決など、他の厳しいサービス レベル アグリーメント（SLA）も含まれます。
- ティア 2 - このカテゴリは、上から 2 番目の管理対象サービス層を表します。 MSP は、重要なデータ センターを連続的に監視し、問題を迅速に解決し、特定のデータ センターの QoS を提供します。

次の手順に従ってください:

1. ユーザの IT スタッフのチームが担当する顧客システムのリストを作成します。
2. ユーザの MSP 組織が提供するサービス各層のサブスクライバ リストを取得します。
3. 別のリストを作成し、顧客のサブスクリプションに基づいて、チームが監視するシステムの顧客をカテゴリに分類します。

   たとえば、6 件の MSP 顧客を担当している場合は、以下のような 2 つのカテゴリに編成できます。

   ティア 1：

   - 顧客 A
   - 顧客 B
   - 顧客 C

   ティア 2：

   - 顧客 D
   - 顧客 E
   - 顧客 F

   このリストは、カスタム グループを計画して顧客データを編成し、IT スタッフに権限を割り当てるのに役立ちます。

MSP グループ化戦略

顧客サービスのレベル別に管理対象アイテムのグループを編成することが、管理対象サービス プロバイダ（MSP）に対するふさわしい戦略である理由は、いくつかあります。 たとえば、ティア 1 およびティア 2 レベルのサービスをサブスクライブする MSP 顧客をスタッフが監視する場合、各層を表すグループを作成します。 次に、各顧客を表すサブグループを作成し、これらサブグループに管理対象のアイテムを配置します。

サービス層それぞれに応じた個別グループについて専用スタッフを割り当て、層ごとに顧客を監視できます。 CA Performance Center データへのユーザ アクセスを持つアプリケーション、サーバ、およびネットワーク専門家を各層に割り当てることができます。

顧客に影響するすべての問題は、サービス層グループのレベルでレポートされます。 これらのグループに基づいて自動通知を設定し、適切なチームがアラートを受信するようにできます。 同じ IT 専門家が追加の層を監視する場合、より厳しい SLA を持つ顧客には、より厳しいパフォーマンス メトリックが適用されると予想されます。

階層化されたグループ化は拡張可能です。CA Performance Center ユーザは、一般的にサイトとデバイスの地理的位置に基づいてサブグループを作成します。 サービス層を表すグループ内に地理的なサブグループを配置できます。地理的なことが問題でない場合は、重要なインフラストラクチャ コンポーネントを編成するカスタム サブグループを作成できます。

優先度や、選択したルータ アップリンクに応じた重要なアプリケーション サーバなどへの依存関係に基づいてサブグループを構成することもできます。 作成するサブグループをより大きな「ティア 1」と「ティア 2」のコンテナ グループに追加し、関連付けられた層に対してアラートがレポートされるようにできます。

権限グループ割り当ての計画

CA Performance Center オペレータへの権限としてカスタム グループを割り当てるための戦略を計画します。

権限グループは、データ アクセスの目的で管理対象アイテムを編成するカスタム グループです。 権限セットとしてユーザ アカウントに割り当てられるまで、カスタム グループと呼ばれます。

権限としてカスタム グループを割り当てることには以下の利点があります。

- ユーザは、担当領域内のデータのみを参照できます
- 管理者は、セキュリティ上の理由でデータを参照できるユーザを制限できます

次の手順に従ってください:

1. 完全に展開されたら、CA Performance Center を使用する MSP 従業員のリストを作成します。

   注: CA Performance Center オペレータごとにユーザ アカウントが必要です。 ユーザ アカウントは共有できません。

2. MSP 顧客リストを使用して、スタッフを割り当てます。 詳細については、「サービス層ごとに MSP 顧客を編成 (P. 48)」を参照してください。

   テーブルを作成して割り当てを編成できます。 例 :

IT スタッフ	現在の顧客割り当て	顧客サービス層
スタッフ メンバ 1 スタッフ メンバ 2	顧客 A	ティア 1 :
スタッフ メンバ 3	顧客 B	ティア 1 :
スタッフ メンバ 4	顧客 C	ティア 1 :
スタッフ メンバ 5	顧客 D	ティア 2
スタッフ メンバ 6	顧客 E	ティア 2
スタッフ メンバ 7	顧客 F	ティア 2

複数のスタッフが同じ顧客に割り当てられる場合、同じ権限グループを割り当てられる必要があります。

3. 作成したテーブルを使用して、顧客すべてを監視するのに必要な権限グループを決定します。

   この例では、ティア 1 およびティア 2 の 2 つの権限グループを必要とします。すべての顧客システムからこれら 2 つのカスタム グループに管理対象アイテムを追加できます。

4. スタッフを権限グループにマップするリストを作成します。

   できあがったリストは、グループを作成してユーザ アカウントに権限として割り当てるときに利用します。 例：

IT スタッフ	権限グループ
スタッフ メンバ 1	ティア 1：
スタッフ メンバ 2	ティア 1：
スタッフ メンバ 3	ティア 1：
スタッフ メンバ 4	ティア 1：
スタッフ メンバ 5	ティア 2
スタッフ メンバ 6	ティア 2
スタッフ メンバ 7	ティア 2

カスタム グループの作成

グループの作成を開始する前に、戦略と構造を計画します。 CA Performance Center オペレータが監視処理を実行するために必要なアクセス権のタイプを考慮します。 必要に応じて、CA の技術担当者に組織的な目的および監視目的について相談してください。 営業時間の展開を計画する場合、詳細については「サイト グループの作成」を参照してください。

［グループ］ツリーの［すべてのグループ］ノードの下か、既存のカスタム グループまたはサイト グループ内にグループを作成します。 グループをシステム グループに追加することはできません。システム グループはグループ ツリー内で「ロック済み」として表示されます。

任意の親グループに最大 2000 の子グループを追加できます。

重要: CA Infrastructure Management Data Aggregator データ ソース用のグループを作成した場合、グループ メンバシップは 10,000 までのアイテムに制限することをお勧めします。 この数には、管理対象アイテムの子も含まれます。 この制限を守ることにより、レポート時間を 10 秒以内におさえることができます。

次の手順に従ってください:

1. 管理用に必要な役割の権限を持つユーザとしてログインします。
2. ［グループの管理］ページに移動します。

   ページに、ツリー構造内の現在のグループが表示されます。
3. 新規グループ用の場所を見つけるには、［グループ］ツリーのノードを展開します。
4. ノードを右クリックし、［グループの追加］を選択します。

   ［グループの追加］ウィンドウが開きます。

   デフォルトでは［新規］タブが選択されています。
5. 以下のパラメータの値を入力します。

   グループ名

   グループの名前を指定します。 グループ名には特殊文字（/&¥,%）を使用できません。

   説明

   （オプション）グループの識別を容易にします。
6. 以下のパラメータの設定を確認します。

   管理対象の子アイテムを含める

   管理対象アイテムがこのグループに追加されると、自動的にその子アイテムも追加されます。 このオプションを無効にして、ルータをグループに追加した場合は、そのルータ上のインターフェースは追加されません。 そのため、それらのデータはドリル ダウン ビュー内に表示されません。

   デフォルト： 選択済み。
7. ［グループ タイプ］リストから［カスタム］を選択します。

8. ［保存］をクリックします。

   新しいグループが、［グループ］ツリーに表示されます。

   ユーザがアイテムを追加するまで、グループにはアイテムが含まれていません。カスタム グループにアイテムを追加するには、以下の 2 つのオプションがあります。

   - ［グループの管理］インターフェースでアイテムを追加して、手動でグループを入力します。
   - グループ メンバシップを管理するルールを作成します。

詳細:

手動で管理対象アイテムをグループに追加 (P. 58)
ルールに従って管理対象アイテムをグループに追加 (P. 54)

ルールに従って管理対象アイテムをグループに追加

ネットワークとシステムは常に変化します。 管理対象アイテムが検出されると、CA Performance Center システム グループは、それらのアイテムを含めるために自動的に更新されます。 ただし、カスタム グループを最新にしておくことは難しい場合があります。そのため、ルールを使用して、カスタム グループを監視システムに入力することができます。 ルール仕様に適合するアイテムが新しく検出されると、グループに追加されます。同様に、ルール要件を満たさないアイテムまたは監視されなくなったアイテムは削除されます。

重要: CA Infrastructure Management Data Aggregator データ ソース用のグループを作成した場合、グループ メンバシップは 10,000 までのアイテムに制限することをお勧めします。 この数には、管理対象アイテムの子も含まれます。 この制限を守ることにより、レポート時間を 10 秒以内におさえることができます。

ルールを作成する前に、グループ化構造に追加するアイテムを定義するにはある程度の時間をかけましょう。 グループ ルールは、管理対象アイテムを構成し、オペレータに関連するデータへのアクセスを提供するために、全体のグループ化戦略の一部として実装するのが最適です。 引き続き、既存のルールでグループにアイテムを手動で追加できます。

注: グループ ルールはドメイン グループに適用されません。

以下の手順に従います。

1. ［グループの管理］ページに移動します。

   ページに、ツリー構造内の現在のグループが表示されます。

2. グループ ツリーに入力するグループを選択します。

   このグループにすでにアイテムが追加されている場合、それらのアイテムは右ペインに表示されます。

   注: 手作業として直接グループに追加されたアイテムは、［グループ プロパティ］ペイン内に直接アイテムとして表示されます。 管理対象アイテムの子であるという理由でグループに追加されたアイテムは、［グループ プロパティ］内に継承されたアイテムとして表示されます。

3. 右側のペインの［プロパティ］タブをクリックします。

   ［プロパティ］ページが表示されます。

4. 以下のオプションの設定を確認し、必要に応じて変更します。

   管理対象の子アイテムを含める

   管理対象アイテムがこのグループに追加されると、自動的にその子アイテムも追加されます。 このオプションを無効にして、ルータをグループに追加した場合は、そのルータ上のインターフェースは追加されません。 そのため、それらのデータはドリル ダウン ビュー内に表示されません。

   デフォルト： 選択済み。

5. ［保存］をクリックします。

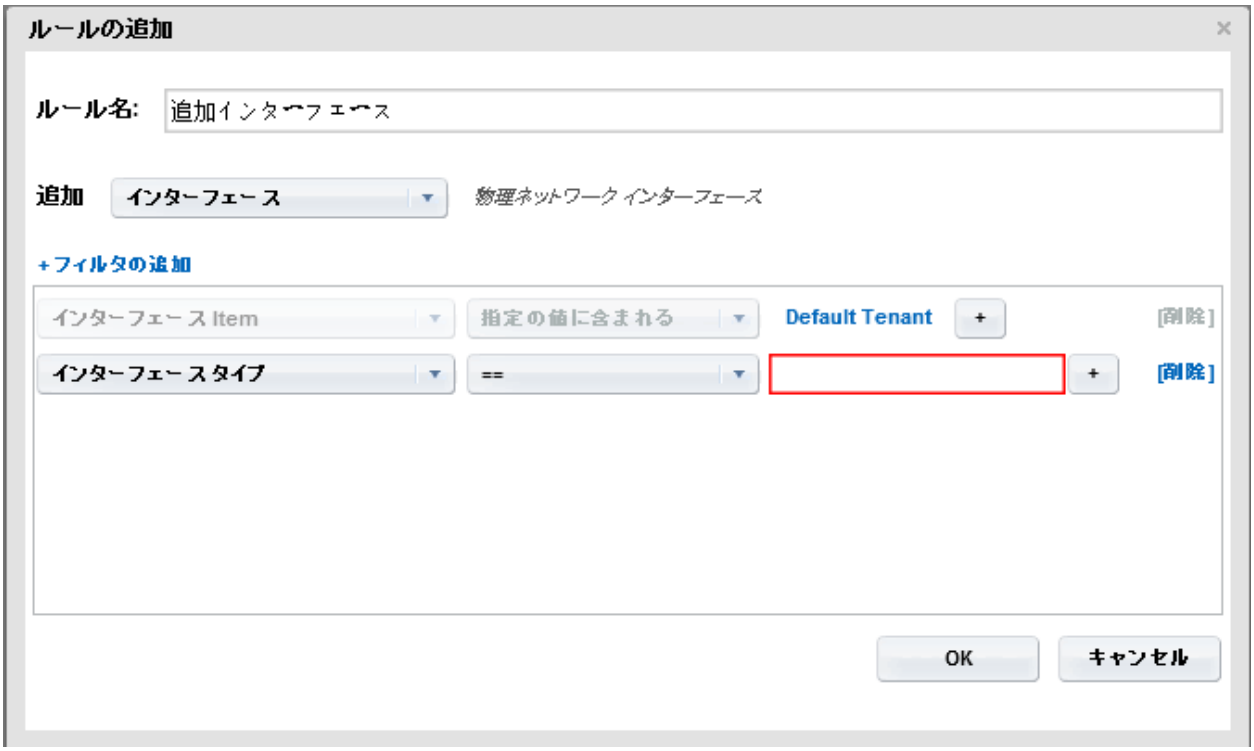
6. ［ルール］タブをクリックして、［ルールの追加］をクリックします。

   ［ルールの追加］ダイアログ ボックスが表示されます。

7. ［ルール名］フィールドにルール名を入力します。
8. ［追加］リストからグループに追加する管理対象アイテムのタイプを選択します。

   利用可能なオプションは、CA Performance Center に登録されたデータソースによって異なります。
9. ［条件の追加］をクリックします。

   ドロップダウン リストの行とフィールドが表示されます。



10. 最初のリストで、管理対象アイテムを識別するメソッドを選択します。たとえば、［デバイス タイプ］を選択します。 オプションには、アイテムの説明、名前、タイプ、場所、連絡窓口、モデル、ベンダー、オブジェクト ID、および IP アドレスなどが含まれます。「名前」および「名前エイリアス」アイテムは、管理者が設定する役割の権限に応じてユーザが利用できます。

    残りのリストは、選択されたアイテムのタイプに一致するよう更新されます。

    注: 管理対象アイテムを識別する方法は、選択した管理対象アイテムよって異なります。

11. 2 番目のリストから一致するメソッドを選択します。たとえば、「==」を選択します。

    重要: ネットワーク サブネット条件を追加する場合： ［指定のサブネット内にある］および［指定のサブネット内にない］オプションで指定する IP アドレスには CIDR 表記を使用します。 ［指定の範囲内にある］および［指定の範囲内にない］オプションで指定する IP アドレスにはドット付き 10 進表記を使用します。

12. （オプション）残りの条件フィールドに一致するテキスト文字列を入力します。たとえば、「Southwest」地域のすべてのルータおよびサーバを追加するには、「sw*」など適切な命名規則の文字列を入力します。

    注: このフィールドでは、複数文字列と一致するアスタリスク（*）などのワイルドカード文字が使用できます。

13. （オプション）［OR］一致を追加するには、条件の最後の［+］をクリックします。

    ［OR］フィールドが表示されます。

14. （オプション）［AND］一致を追加するには、［条件の追加］をクリックします。デフォルトでは、追加されるすべての新しい条件は、他のすべての条件と AND ステートメントで結合されます。

    さらに 3 つのドロップダウン リストが表示されます。

    注: ［AND］条件インジケータは表示されません。 対照的に、［OR］オペレータを選択すると、［OR］インジケータが表示されます。

15. ［プレビュー結果］をクリックし、必要なアイテムが新規ルールに含まれていることを確認します。

    結果が［グループ ルール プレビュー］ウィンドウに表示されます。各アイテム タイプを展開して、追加された特定のアイテムを参照できます。

16. （オプション）グループにその他のアイテム タイプを追加するには、［+ ルールの追加］をクリックします。

    各アイテム タイプには、独自のルールが必要です。

17. ルールを作成し終わったら、［保存］または［ルールの保存と実行］をクリックします。
    - ［保存］- ルールを実行せずに保存します。グループは次のグローバル同期中に入力されます。グローバル同期は、約 5 分ごとに発生します。
    - ［ルールの保存と実行］- ルールを保存し、グループをすぐに入力します。

手動で管理対象アイテムをグループに追加

管理対象アイテムを追加することで、カスタム グループのデータを手動で入力できます。 グループ構造を詳細に調整する場合は、管理対象アイテムをグループに個別に追加する必要がある場合があります。 ただし、通常はグループ ルールをセットアップする方が、より効果的な戦略です。

重要: CA Infrastructure Management Data Aggregator データ ソース用のグループを作成した場合、グループ メンバシップは 10,000 までのアイテムに制限することをお勧めします。 この数には、管理対象アイテムの子も含まれます。 この制限を守ることにより、レポート時間を 10 秒以内におさえることができます。

次の手順に従ってください:

1. ［グループの管理］ページに移動します。

   ツリー構造内に現在のグループが表示されます。

   注: ［グループ］ツリー内に「錠前」のシンボル付きで表示されたシステム グループは読み取り専用であることを示します。 システム グループへのアイテムの追加、およびシステム グループからのアイテムの削除をすることができません。

2. ［グループ］ツリーのノードを展開し、管理対象アイテムを追加するグループを見つけて選択します。

   このグループにすでにアイテムが追加されている場合、それらのアイテムは右ペインに表示されます。

   注: 手作業として直接グループに追加されたアイテムは、［グループ プロパティ］ペイン内に直接アイテムとして表示されます。 管理対象アイテムの子であるという理由でグループに追加されたアイテムは、［グループ プロパティ］内に継承されたアイテムとして表示されます。

3. 右側のペインの［プロパティ］タブをクリックします。

   ［プロパティ］ページが表示されます。

4. 以下のオプションの設定を確認し、必要に応じて変更します。

   管理対象の子アイテムを含める

   管理対象アイテムがこのグループに追加されると、自動的にその子アイテムも追加されます。 このオプションを無効にして、ルータをグループに追加した場合は、そのルータ上のインターフェースは追加されません。 そのため、それらのデータはドリル ダウン ビュー内に表示されません。

   デフォルト： 選択済み。

5. ［保存］をクリックします。
6. ［アイテム］タブをクリックします。

   ［アイテムの表示］リストが表示されます。 ［アイテムの表示］リストは、メンバが含まれるグループにのみ適用されます。

7. ［アイテム タイプの追加］をクリックします。

   ［アイテムの追加］ダイアログ ボックスが表示されます。

8. 追加するアイテムのタイプを［利用可能なアイテム］リストから選択します。

   アイテムのリストが更新され、グループに追加可能な選択したタイプのアイテムが表示されます。

   利用可能なアイテムは、アイテム タイプ、登録されたデータ ソース、および検出されたアイテムによって異なります。

9. アイテムのその他のページを表示するには、リスト下のリンクをクリックします。

   ［検索］フィールドを使用して、リスト内のアイテムを検索することもできます。

10. 1 つ以上のアイテムを選択するには、アイテムの隣のチェック ボックスをオンにします。

    ページのアイテムをすべて選択するには、テーブル ヘッダ行内のチェック ボックスをオンにします。

11. ［アイテムの追加］をクリックします。

    ［アイテム］が更新され、新規グループ メンバを表示しますが、［アイテムの追加］ダイアログ ボックスは開いたままです。

12. アイテムの追加が完了したら、［閉じる］をクリックします。

    ［アイテムの追加］ダイアログ ボックスが閉じます。

    ［アイテム］タブに、追加したアイテムが表示されます。

ユーザへの権限の割り当て

それぞれの CA Performance Center オペレータには、MSP 顧客のデータを監視するためにデータ アクセス権が必要です。 CA Performance Center アクセス権はグループに基づいています。 カスタム グループ用の計画 (P. 50) に従ってアクセス権を割り当てることができます。

権限を割り当てるには、CA Performance Center ユーザ アカウントを編集します。 オペレータ全員が、各自の作業に必要なデータのみを参照するように設定することが必要です。

次の手順に従ってください:

1. 必要な管理の役割の権限を持つユーザとしてログインします。
2. ［管理］-［ユーザ設定］を選択し、［ユーザ］をクリックします。

   ［ユーザの管理］ページが開きます。

3. 変更するユーザ アカウントを選択し、［編集］をクリックします。

   ユーザの追加ウィザードが開きます。

4. ［権限グループ］ボタンをクリックします。

   ウィザードは権限グループ ページに進みます。

5. 以下の方法でユーザ アカウントに権限グループを追加します。
   - 左側の［利用可能なグループ］ツリーのグループを展開し、サブグループを表示します。
   - グループまたはサブグループを選択します。
   - 右方向矢印ボタンをクリックし、右側の［選択したグループ］に追加します。
   - 必要に応じて、手順を繰り返します。

   選択した権限グループが、［選択したグループ］ペインに表示されます。
6. ［デフォルト グループ］ドロップダウン リストからグループを選択します。

   ユーザがログインすると、デフォルト グループからのデータがデフォルトでダッシュボード内に表示されます。
7. ［保存］をクリックします。

   変更がユーザ アカウントに保存され、［ユーザの管理］ページに戻ります。

カスタム グループが作成され、IT スタッフへの権限として割り当てられました。 スタッフが CA Performance Center にログインすると、スタッフに割り当てられた MSP 顧客システムからのデータを参照できるようになります。

用語集

SNMP プロファイル

*SNMP プロファイル*は、SNMP を使用するデバイス MIB の安全なクエリを有効にするために必要な情報が含まれる定義です。

グループ

*グループ*は、管理対象アイテム用のコンテナとして機能するフィルタ定義です。 グループは、ツリー構造の管理対象アイテムを論理的に構成することができ、各グループにはサブグループまたは管理対象アイテムを含むことができます。 構造はデータ ソースに継承され、データ ソースでは、トップレベルのグループから、さらに狭い関連コンテキストにドリル ダウンできます。

グローバル管理者

*グローバル管理者*は、すべてのテナントの製品設定を管理します。 このユーザ アカウントはデフォルト テナントと関連しているため、「デフォルト テナント管理者」とも呼ばれ、テナントを作成してテナント設定を実行します。

テナント

*テナント*は、管理対象サービス プロバイダが管理するカスタマ環境を表します。 各テナント環境は独立しており、CA Performance Center の個別のインスタンスとして有効に機能します。 各インスタンスには、テナント間で共有されない複数のユーザおよび役割を含めることができます。

テナント管理者

*テナント管理者*は、単一のテナントからすべてのデータを表示する権限があります。 またテナント管理者は、このテナントに、グループ定義、プロファイルおよびユーザ アカウントなどの設定も追加できます。 この管理者役割には、その他のテナントに関連付けられたアイテムを表示する権限はありません。

ドメイン

*IP ドメイン*は、さまざまなデバイスおよびネットワークからのデータを識別する論理的なグループです。 ドメインによる監視は、IP アドレスと、それに関連する別のカスタマ ネットワークに属するインターフェースまたはアプリケーションを別々に監視することを意味します。 適切な権限と組み合わせることで、IP ドメインは単一のコンソールから監視されますが、ユーザには、自身が監視するドメインのデータのみ表示されます。

ホスト

*ホスト*は、メイン CA Performance Center 管理者に対応します。 多くの場合、ホストは管理されるサービスを表し、IT スタッフが複数のカスタマのネットワークおよびシステムを管理して監視します。各ホストには、IT スタッフ メンバ用の複数のユーザ アカウントと、共有インフラストラクチャの管理対象アイテムを構成するためのグループ化構造が含まれます。ホストは、複数のテナントのドメインおよびインフラストラクチャを管理できます。

役割

役割は、製品機能およびダッシュボード ページへのユーザ アクセスを制御するユーザ アカウントに割り当てられたパラメータです。 ユーザのジョブ機能に基づき、役割では、*役割の権限*を使用して製品設定への管理アクセス権を付与します。 役割によって、ユーザは役職を実行するのに必要なデータおよび製品機能にアクセスできるようになり、必要としない機能へのアクセスは制限されます。