CA Performance Center

管理者ガイド

2.4

ca technologies

CA Technologies 製品リファレンス

このドキュメントでは、以下の CA Technologies 製品および機能に言及します。

- CA Performance Center
- CA Infrastructure Management Data Aggregator
- CA NetQoS® Performance Center
- CA Single Sign-On
- CA Network Flow Analysis
- CA Application Delivery Analysis
- CA Unified Communications Monitor
- CA eHealth
- CA Spectrum

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: CA Performance Center の概要

このセクションには、以下のトピックが含まれています。

CA Performance Center について

CA Performance Center は、物理および仮想ネットワーク、アプリケーション、およびデバイスの効率的な管理を支援する Web ベースのレポート インターフェースです。CA Performance Center のダッシュボードとレポートには、ネットワーク製品とシステム監視製品からのパフォーマンス データが表示されます。 1 つの Web ページ上で複数のソースからの大量の統計データを比較できます。

CA Performance Center は、アプリケーション サービス配信に対して「パフォーマンス重視」のアプローチを取っています。 このアプローチはエンド ユーザを中心的役割に据えます。 IT 組織がユーザへのアプリケーション配信を適切にサポートしているかどうかを判断するには、アプリケーション、デバイス、およびネットワークからデータを収集して分析する必要があります。

CA Performance Center は、アプリケーションの応答時間、トラフィック構成、インフラストラクチャ ヘルス、およびフローベースの診断に関する役割固有のビューを提供します。

データ収集

CA Performance Center は、パフォーマンス データ、デバイス識別、デバイス ステータス、サーバ ステータス、およびシステム ステータスをデータ ソースに依存しています。 サポートされているデータ ソースが、さまざまなタイプのデータ（デバイス MIB からのエンドツーエンド アプリケーションの応答時間、パケット、ネットワーク トラフィック フロー、およびインフラストラクチャに関する統計情報）を収集します。管理オーバーヘッドを最小化する CA Performance Center は、データ センター内で実行している組み込み型ネットワーク機器とパッシブ コレクション アプライアンスを使用します。 リモート プローブとエージェントは使用されません。 代わりに、SNMP や NetFlow などのデータ ソースが、多種多様なアーキテクチャからのデータを提供します。

CA Performance Center は、物理システムと仮想システムからパフォーマンス データの収集、保存、集計、および分析を行う複数のソースからのデータを表示します。 CA Performance Center は、再認証を必要とせずに、データを提供する製品への直接アクセスを可能にします。

大量のデータとアナリティクスを実用的な情報に変換するために、CA Performance Center は単一のレポート インターフェースを提供しています。ダッシュボードとアラートは、ネットワーク エンジニア、運用スタッフ、サーバ チームとアプリケーション チーム、および IT 担当重役のニーズに合わせて調整できます。 さまざまな形式でカスタマイズされたビューを構築できます。

CA Performance Center の起動

CA Performance Center セットアップ プログラムを実行して、インストールが完了したら、Web ブラウザからコンソール プログラムを起動できます。

以下の手順に従います。

1. Web ブラウザを開きます。
2. アドレス フィールドに、以下のアドレスを入力します。

   ```
   http://<server IP address>:8181/pc/desktop/page
   ```

   <server IP address>

   ソフトウェアがインストールされているコンピュータの IP アドレスです。

   8181

   ポート番号です。

   ブラウザにログイン ページが表示されます。
3. 表示されたフィールドに CA Performance Center のユーザ名とパスワードを入力します。詳細については、「事前定義のユーザ アカウント (P. 144)」を参照してください。
4. （オプション）管理者が設定したタイムアウト期間を超えてログイン状態を維持するには、［このコンピュータでログイン状態を保存する］を選択します。
5. ［ログイン］をクリックします。

   ホーム ダッシュボードで CA Performance Center コンソールが開きます。

第 2 章: CA Performance Center のセットアップ

このセクションには、以下のトピックが含まれています。

CA Performance Center のセットアップ方法

CA Performance Center を使用するための要件は、サポートされているデータ ソースの追加（データ ソースの登録）のみです。 ただし、レポートがより役立つように環境をカスタマイズできます。

CA Performance Center をセットアップするための以下のワークフローをお勧めします。

1. グループ構造と命名規則を計画します。 詳細については、「グループの作成と管理 (P. 75)」を参照してください。

   （オプション）テナント構造と命名規則を計画します。 MSP 環境で使用されるテナントは、CA Performance Center の単一のインスタンスで複数の個別の企業を監視できるようにします。 詳細については、「テナントの作成と管理 (P. 155)」を参照してください。

2. CA Performance Center のオペレータに必要なユーザ アカウントと役割を計画します。詳細については、「ユーザ アカウントの作成と管理 (P. 143)」と「役割の作成と管理 (P. 111)」を参照してください。

3. 役割ごとに適切なダッシュボードとメニューをリスト表示します。 詳細については、「メニュー内のダッシュボードの整理」を参照してください。

4. データ ソースを登録します。 詳細については、「データ ソースの登録 (P. 31)」を参照してください。

5. CA Performance Center ユーザがレポート ページを電子メール メッセージとして送信できるように、電子メール サーバを設定します。詳細については、「電子メール サーバの設定 (P. 15)」を参照してください。
6. デバイス MIB をポーリングするデータ ソースにセキュリティ情報を渡すための SNMP プロファイルを作成します。 詳細については、「SNMP プロファイルの追加 (P. 38)」を参照してください。
7. （オプション）営業時間の定義を作成して、レポートされたデータをビジネス アクティビティへの影響度に基づいて区別します。詳細については、「営業時間の概要 (P. 69)」を参照してください。
8. 管理対象アイテムのグループを作成します。 詳細については、「カスタム グループの作成 (P. 92)」を参照してください。
9. 役割を作成して、それらの役割にメニューを割り当てます。 詳細については、「役割の追加 (P. 129)」を参照してください。
10. ユーザ アカウントを作成して、それらのアカウントに役割と権限グループを割り当てます。詳細については、「ユーザ アカウントの追加 (P. 151)」を参照してください。
11. レポート用のダッシュボードを含むメニューを作成します。 詳細については、「メニューの追加」を参照してください。
12. （オプション）各ユーザ アカウントにログインして、各ユーザに付与されているアクセスのレベルをテストします。 詳細については、「ユーザ アカウントのプロキシ」を参照してください。
13. （オプション）すべての顧客企業を表すためのテナントを作成します。詳細については、「テナントの追加 (P. 161)」を参照してください。
14. （オプション）エクスポートされるレポートにヘッダ内のロゴが含まれるように、カスタム ロゴをテナント テーマに追加します。 詳細については、「テーマのカスタマイズ (P. 16)」を参照してください。
15. （オプション）ダッシュボードでアイテム名の代わりにエイリアスを表示するには［表示設定］を変更します。 詳細については、「表示設定 (P. 18)」を参照してください。
16. （オプション）イベント通知をセットアップします。詳細については、「通知 (P. 63)」を参照してください。

電子メール サーバの設定

ユーザが電子メールでレポートを送信できるように、電子メール サーバを設定します。 レポートは、スケジュールに基づいてまたは必要に応じて、電子メールで送信できます。 CA Performance Center サーバがネットワーク アクセス可能なサーバを選択します。

以下の手順に従います。

1. 管理の役割の権限 (P. 118)を持つユーザとしてログインします。
2. ［管理］-［システム設定］を選択して、［電子メール サーバ］をクリックします。

   ［電子メール サーバ設定］ページが表示されます。
3. ［電子メールの有効化］チェック ボックスをオンにします。

   ページが必須フィールドを強調表示するように更新されます。
4. 必要に応じて、以下のフィールドにデータを入力します。

   SMTP サーバ アドレス

   電子メールでレポートを送信するために使用されるサーバの IP アドレスまたはホスト名です。

   SMTP サーバ ポート

   メッセージの送信に使用される電子メール サーバ上のポートです。

   デフォルトは、ポート 25 です。

   電子メール返信アドレス

   CA Performance Center がレポートを送信する電子メール アドレスです。

   注: 管理者は、製品から送信された電子メール メッセージに応答するためにこのアドレスを監視する必要があります。

5. （オプション） SSL 暗号化を有効にします。 CA Performance Center からの電子メールの送信にセキュリティ保護接続を使用する場合は、このパラメータが必要です。
6. （オプション） SMTP 認証を有効にするために、以下の手順を実行します。
   a. ［認証の有効化］を選択します。
   b. ［ユーザ名］フィールドに、SMTP 認証用のユーザ名を入力します。
   c. ［パスワード］フィールドに、認証パスワードを入力します。
   d. ［パスワードの確認］フィールドに、再度認証パスワードを入力します。

   注: SMTP 認証はデフォルトで無効になっています。
7. ［保存］をクリックします。

   電子メール サーバが設定されます。

テーマのカスタマイズ

テーマは、エクスポートされるレポートの外観に影響を与えます。デフォルトで、すべてのテーマに CA Technologies のロゴが使用されます。 テーマをカスタマイズして、選択したロゴを使用することができます。

通常、テーマはテナントごとに適用されます。 テーマをカスタマイズして、テナントに割り当てます。 カスタム ロゴは、テナント ユーザが印刷したり電子メールで送信するレポート（PDF 形式）のヘッダに表示されます。 マルチテナンシーを展開しない場合、テーマはデフォルト テナントに適用されます。

グローバル管理者のみがテーマにカスタム ロゴを適用できます。 マルチテナンシーを展開していない場合は、事前定義済みの管理者の役割を持つユーザとしてログインします。

次の手順に従ってください:

1. ロゴ画像ファイルをコンピュータに保存します。 「画像ファイルのヒント (P. 17)」で指定されているガイドラインに従っていることを確認してください。
2. 管理者の役割を持つユーザとしてログインします。

3. ［管理］-［カスタム設定］を選択して、［テーマ］をクリックします。

   ［テーマ設定］ページが表示されます。

4. ［参照］ボタンをクリックして、カスタム テーマに使用する画像ファイルを探します。

5. カスタム ロゴを適用するテーマを選択します。

   注: マルチ テナンシーを展開していない場合は、［すべてのテーマ］を選択します。

6. ［保存］をクリックします。

   カスタム ロゴ画像はサーバ上で処理されます。それが画像基準を満たしている場合は、変更がテーマに保存されます。

   条件を満たさない画像があると、満たされていない要件を示すメッセージが表示されます。 その場合、画像を変更して、再度アップロードできます。

7. 変更したテーマを選択するには、テナントの編集 (P. 163)を実行します。

画像ファイルのヒント

カスタム テーマ用に選択する画像ファイルは、外観が鮮明で、使用可能なスペースに収まるという特定の要件を満たす必要があります。 CA Performance Center のカスタム テーマとして最適な画像は以下のガイドラインに従っています。

- 画像は正方形です。 1 対 1 の縦横比を使用します。 必要に応じて、正方形の背景でロゴを囲みます。
- 画像は以下のファイル形式のいずれかにする必要があります。
  - .bmp
  - .gif
  - .png
  - .jpg
- （オプション）画像は透明または白黒です。
- （オプション）画像は 300 ドット/インチ（DPI）以上の解像度に設定します。
- CMYK と RGB の両方の色モデルがサポートされています。 ただし、プリンタの互換性を考慮して、CMYK 色モードの選択をお勧めします。

表示設定

［表示設定］ページでは、CA Performance Center に表示されるダッシュボードの基本設定を選択できます。

ビューの非表示

デフォルトでは、いくつかのダッシュボードに、データがないデータ ビューが含まれています。 「表示するデータがありません」というメッセージが表示されます。

データ ビューは、設定または接続性の問題のために空になっている可能性があります。 CBQoS、MPLS、または IP SLA などの技術についてレポートするビューに関しては、そのビューまたはページ コンテキスト用に選択されているデバイスがこれらの技術をサポートするように設定されていないため、デフォルト ビューは空の場合があります。

しかし場合によっては、データ ソースがないために常にビューが空で表示されます。 ［ビューの非表示］を有効にすると、必要なデータ ソースが登録されていないか、または必要なテクノロジが設定されていないときにビューを非表示にします。

［表示設定］ページで「ビューの非表示」オプションが有効になっていると、登録データ ソースがないデータ ビューは、そのデータ ソースが登録されるまで非表示になります。 ビューに取り込まれるデータ ソースが登録されると、そのビューは表示されるようになります。 同様の動作は、コンテキスト タブおよびカスタム メニューに適用されます。 メニューまたはタブに非表示になっていないビューが 1 つでもある限り、カスタム メニューまたはタブは表示されたままになります。

［アイテム表示名］オプション

ユーザ アカウントに［アイテム表示名または名前エイリアスを表示］という役割の権限が与えられている場合、ダッシュボードやビューにアイテムを表示する方法を選択できます。 表示名はデフォルトで設定されます。このデフォルト設定を変更して、代わりにアイテム エイリアスを表示できます。

管理者はスクリプトを使用して、監視対象デバイスやインターフェースにエイリアスを設定 (P. 20)できます。 ［アイテム表示名］オプションが［アイテム名エイリアスを使用］に設定されている場合、デバイスまたはインターフェースの［インベントリ］リストにエイリアスが表示されます。

詳細:

ビューの「データがありません」メッセージ (P. 190)
［ビューの非表示］の無効化 (P. 19)
ダッシュボードおよびビューに表示するアイテム エイリアスの設定 (P. 20)

［ビューの非表示］の無効化

［表示設定］ページで「ビューの非表示」オプションが有効になっていると、登録データ ソースがないデータ ビューは、そのデータ ソースが登録されるまで非表示になります。 ビューに取り込まれるデータ ソースが登録されると、そのビューは表示されるようになります。

［ビューの非表示］は、デフォルトでは、ダッシュボードに配置されるビューに適用されます。 管理者がビュー カテゴリを使用してダッシュボードを編集するときは、ビューは非表示になりません。

［ビューの非表示］オプションはデフォルトで有効になっています。 トラブルシューティング目的で、または別のデータ ソースの展開を考慮する際の意思決定に役立てるため、このオプションを無効にすることができます。 ［ビューの非表示］がオンにされた場合、［ビューの非表示］インジケータがページの右上に表示されます。

次の手順に従ってください:

1. 自身のユーザ アカウントへログインします。 ［ビューの非表示］は、任意の役割を持つユーザで使用できます。
2. ［マイ設定］ -［表示設定］を選択し、［表示設定］メニュー項目をクリックします。

   ［表示設定］ページが表示されます。
3. ［ビューの非表示］メニューから［すべてのビューの表示］を選択します。
4. ［保存］をクリックします。

   ［ビューの非表示］インジケータは［インフラストラクチャ概要］ページで非表示になります。

注: ［ビューの非表示］を有効にした場合、［表示設定］ページにアクセスするために［ビューの非表示］インジケータをクリックすることもできます。

ダッシュボードおよびビューに表示するアイテム エイリアスの設定

［アイテム表示名または名前エイリアスを表示］の役割権限を持つユーザは、ダッシュボードやビューに表示する名前を選択できます。 表示名はデフォルトで設定されます。 このデフォルト設定を変更して、代わりにアイテム エイリアスを表示できます。

管理者は役割の権限を設定できます。

次の手順に従ってください:

1. 自身のユーザ アカウントへログインします。
2. ［マイ設定］ -［表示設定］を選択し、［表示設定］メニュー項目をクリックします。このメニュー アイテムは、「アイテム表示名または名前エイリアスを表示」の役割の権限を与えられたユーザに利用可能です。
3. ［アイテム名表示オプション］メニューから［アイテム名エイリアスを使用］を選択します。

   これより、アイテム エイリアスはダッシュボードおよびビューに表示されます。

   列設定オプションがあるビューについては、この手順で指定した設定を上書きできます。 たとえば、インベントリ ビューでは、アイテムの表示名とエイリアスの両方を表示するように選択できます。 列の上にある白い矢印を使用して、テーブル列オプションのメニューにアクセスできます。 列を選択して、デフォルトでテーブルで有効になっているメトリックを有効または無効にします。

詳細:

複数の監視対象デバイスに対するエイリアス名の設定 (P. 200)
複数の監視対象デバイスにわたるインターフェースおよびコンポーネントへのエイリアス名の設定 (P. 203)

データ ソースの管理

*データ ソース*は、パフォーマンス データおよび設定データを CA Performance Center に提供するサポート対象製品です。 データを監視、収集、集計するデータ ソース製品は、多くの場合独立して機能します。 ただし、CA Performance Center のインスタンスに登録されると、データ ソースとして認識されます。

CA Performance Center で使用できるデータ ソースは、インストールして設定されている、互換性のある製品によって異なります。 CA Performance Center のインストール後にデータ ソースを登録します。

データ ソースが追加の管理を必要とする場合があります。 ユーザの環境で SSL 暗号化をセットアップした場合、データ ソース接続パラメータの編集が必要です。 データ ソース接続に伴う問題のトラブルシューティングを支援するためにデータ ソース ログ (P. 30)を利用できます。

設定データは、5 分ごとに、CA Performance Center と登録済みデータ ソース間で自動的に同期されます。 グローバル同期のステータスとすべての登録済みデータ ソースのリストが、［データ ソースの管理］ページに表示されます。

詳細:

データ ソースの登録 (P. 31)
データ ソースの編集 (P. 33)
データ ソースの同期 (P. 29)

データ ソースからの設定データの処理方法

各データ ソースの管理者は、一部の監視パラメータを設定したり、ユーザ アカウントおよびその他の定義を作成することができます。 これらのパラメータと定義は、登録後に、CA Performance Center とその他のすべての登録済みデータ ソース間で共有されます。

登録中に、CA Performance Center は、データ ソースから、ユーザ アカウント、SNMP プロファイル、およびその他の管理データをインポートします。CA Performance Center により、競合が解決され、重複が排除されます。次の同期で、更新された管理データがすべての登録済みデータ ソースに送信されます。

登録処理には「バインディング」手順が含まれます。その手順では個々のデータ ソース内の共有管理データに対する新たな変更は禁止されます。したがって、データ ソース管理者は、登録後に CA Performance Center 内の共有監視パラメータのみを変更できます。

データ ソース内の冗長定義

登録中に、CA Performance Center は、データ ソースから、ユーザ アカウントとその他の設定パラメータをインポートします。 競合や重複は、以降のセクションで説明するプロセスを使用して処理されます。

重複ユーザ アカウント

ユーザは、異なるデータ ソース製品で名前が同じ 2 つのアカウントを所有することがあります。 そのようなユーザ アカウントでは、最初に同期されるアカウントのパスワードが保持されます。 新たなデータ ソースが登録されるたびに、2 つ目または 3 つ目のアカウントから一意の役割の権限と許可がアカウントに追加されます。

異なるデータ ソースで、複数のユーザ アカウントが同じユーザ名を共有することがあります。いくつかのアカウント パラメータは異なります。この場合は、手動で編集する必要があります。 たとえば、CA Network Flow Analysis 内の Robert という名前のユーザと、CA Application Delivery Analysis 内の Robert という名前の別のユーザがいるとします。 この場合、CA Performance Center は、Robert という名前の 1 つのアカウントを作成します。 両データ ソースからの役割の権限と許可は新しいアカウントにマージされます。 アカウントごとに別々の役割の権限を割り当てる場合は、一意のユーザ名を持つアカウントを作成してください。

冗長 SNMP プロファイル

SNMP プロファイル定義が含まれるデータ ソースの登録は、自動的にプロファイルを CA Performance Center に追加します。 プロファイルは次の同期期間にその他の登録済みデータ ソースに配布されます。

データ ソースが追加されると、CA Performance Center は、以下の値と既存のプロファイルを比較することにより、SNMP プロファイルの重複を最小限に抑えます。

- ユーザ（SNMP v3 の場合）
- コミュニティ文字列（SNMP v1 と v2 の場合）

重複するパラメータを CA Performance Center が検出した場合、CA Performance Center はタイム スタンプに従って最新のプロファイルを保持します。

CA Performance Center は、［コミュニティ文字列］値が一致しない同期されたあらゆる重複プロファイル名に番号を追加して保存します。 CA Performance Center は新しいプロファイルを保存します。たとえば、Boston という名前の最初のプロファイルは Boston ですが、 2 つ目のプロファイルは Boston(1) になります。

データ ソースのリストの表示

［データ ソースの管理］ページには、登録済みデータ ソース（データをレポートに使用できるようにする監視製品）のインベントリが表示されます。

［データ ソースの管理］ページでは、データ ソースに関連付けられたタスクを実行できます。 また、このページにはグローバル同期ステータスも表示されます。CA Performance Center が設定のために各データ ソースに接続した最終日時、およびパフォーマンス データです。

次の手順に従ってください:

1. 管理者の役割を持つユーザとしてログインします。
2. ［管理］-［データ ソース設定］を選択し、［データ ソース］をクリックします。

   データ ソースの現在のリストが表示されます。 データ ソースが登録されていない場合は、リストには何も表示されません。

各データ ソースに関する以下の情報がリスト表示されます。

ソース名

データ ソースを識別します。

ステータス

CA Performance Center に関連しているデータ ソースのステータスを表示します。 ほとんどが同期フェーズを示しています。 詳細については、「同期 (P. 25)」を参照してください。

最終ポーリング

最後に成功した同期の時刻を示します。 通常の同期は 5 分ごとに自動的に発生します。

ソース タイプ

データ ソースのタイプです。

バージョン

データ ソース ソフトウェアの製品バージョンです。

3. このページ上でアクションを実行するには、データ ソースを選択してボタンをクリックします。

画面下のボタンを使用して以下のタスクを実行します。

すべてを再同期

すべてのデータ ソースを順番に使用して増分再同期を開始するようにデバイス マネージャ サービスに指示します。

再同期

選択されたデータ ソースの即時の同期を開始します。 同期には、最近変更されたすべてのユーザ、メニュー、およびグループ設定のデータ ソースへのプッシュが含まれます。 同期は 5 分ごとに自動的に行われますが、このボタンは同期をすぐに開始します。 詳細については、「同期 (P. 25)」を参照してください。

テスト

新しいデータ ソースが登録され、接続されていることを確認するためのテストを実行します。 メッセージにテスト結果が表示されます。

ログ

選択されたデータ ソースの［データ ソース ログ］ページを開きます。データ ソース ログには、データ ソースと同期に関連するイベントが記録されます。

追加

新しいデータ ソースを登録します。

編集

データ ソース パラメータを変更できます。

削除

選択されたデータ ソースを登録解除します。 このアクションは、データ ソースのリストから選択されたデータ ソースを削除します。 ほとんどのデータ ソースの場合、削除されると、登録中に読み取り専用になった製品管理機能が解除されます。 削除されたデータ ソースは、CA Performance Center の別のインスタンスに登録できます。

詳細:

データ ソースの登録 (P. 31)
データ ソースの編集 (P. 33)
データ ソースの管理 (P. 21)
データ ソースの同期 (P. 29)

同期

CA Performance Center は、定期的に、登録済みデータ ソースと同期して、設定情報の送信、およびデータの受信を行います。転送（プッシュ）フェーズは、増分的に、データ ソースに情報をレプリケートします。データ ソースは、グループ設定、認証設定、SNMP プロファイル、ユーザ、および役割を受信します。 データベースにレプリケートされる情報は、そのデータ ソースが CA Performance Center に報告したアイテムのみが含まれるようにフィルタされます。

CA Performance Center がデータを受信すると、メトリックと管理対象アイテムを関連付けるルールが適用されます。 これらの定義をさらに変更することは、個別のデータ ソース インターフェースでは許可されません。 データ ソース管理をロックダウンするプロセスは、「バインディング」として知られています。CA Performance Center に作成される定義のバインディングの後、それらはデータ ソースに送信されます。

*グローバル同期*は、データ ソースから情報を自動的に受理、処理および適用することを意味します。同期は 5 分ごとに発生し、登録済みのすべてのデータ ソースの設定データおよびパフォーマンス データが含まれます。新しい SNMP プロファイルが追加された場合も、自動的にバインディングが実行されます。

［データ ソースの管理］ページ上のテーブルに同期ステータスが表示されます。 失敗や詳細なステータスがデータ ソース ログに記録されます。

完全同期または増分同期

完全同期は、データ ソースが初めて CA Performance Center に登録されたときに発生します。 完全同期では、完全なデータベース レプリケーションも行われます。 CA Performance Center は、そのデータ ソース内のすべての管理対象アイテムに関する情報を受信します。 この種の同期は自動的に繰り返されませんが、必要に応じて、手動で実行できます。

製品設定を変更した場合は、手動同期を実行することをお勧めします。このアクションでは、次の同期間隔（5 分間）を待つのではなく、すぐにデータ ソースに新しい定義が送信されます。 手動同期を開始するときに、完全と増分のどちらのデータ ソースの同期を実行するか選択できます。

同期ステータス

*グローバル同期*に失敗した場合、コンソール ページの一番上にアイコンが点滅表示されます。 失敗に関する詳細情報を表示するには、このアイコンをクリックします。［データ ソースの管理］ページが表示されます。［グローバル同期ステータス］セクションの情報を確認します。

重要: ［グローバル同期ステータス］セクションの［最後の実行ステータス］に［失敗］と表示される場合は、CA サポートにお問い合わせください。

*データ ソースの同期*に失敗した場合、コンソール ページの一番上にアイコンが点滅表示されます。 失敗に関する詳細情報を表示するには、このアイコンをクリックします。 ［データ ソースの管理］ページが表示されます。 ［データ ソース］セクションの情報を確認します。

［データ ソース］セクションには、すべての登録済みデータ ソースのステータスが表示されます。 以下のメッセージに可能性のあるデータ ソース ステータス条件が示されます。

ポーリング待機

データ ソースが接続されておらず、デバイス マネージャのポーリングを待っていることを示します。デバイス マネージャが別のポーリングの実行中でなければ、データ ソースはすぐにポーリングされます。

バインド待機

データ ソースからデータが取得（プル）されたことを示します。データ ソースは、CA Performance Center が設定情報を転送（プッシュ）して、対応する管理機能をロック（バインディング）するのを待っています。

利用可能

データ ソースがレポートに使用可能であることを示します。登録は成功しています。

ポーリング

デバイス マネージャがデータ ソースのポーリング中です。

登録

デバイス マネージャがデータ ソースの登録中であることを示します。

バインディング

デバイス マネージャがデータ ソース内で定義されたユーザ、役割、およびグループをロック中であることを示します。 バインディングは、データ ソース内の設定に対する新たな変更を禁止して、それらが CA Performance Center 内の定義と一致するようにします。 これらの定義に対する新たな変更は、データ ソースではなく、CA Performance Center 内で実行されます。

同期中

デバイス マネージャが設定情報の送受信を通してデータ ソースと同期中であることを示します。

ポーリング失敗

ポーリング中に予期せぬ障害が発生したことを示します。データ ソース ログを表示するには、［ログ］をクリックします。

同期失敗

同期中に障害が発生したことを示します。 データ ソース ログを表示するには、［ログ］をクリックします。

登録失敗

登録中に障害が発生しました。 データ ソース ログを表示するには、［ログ］をクリックします。

バインド失敗

ユーザ、グループ、および役割のバインディング中に障害が発生したことを示します。 データ ソース ログを表示するには、［ログ］をクリックします。

接続できません

通信問題が原因でデータ ソースに接続できません。

バージョン互換性なし

CA Performance Center のバージョンとデータ ソースに互換性がないことを示します。サポートされている製品を確認するには、CA テクニカル サポートに問い合わせるか、CA サポート オンラインをチェックしてください。

アップグレードが必要

データ ソースでソフトウェアのアップグレードが必要なことを示します。 CA テクニカル サポートにお問合わせください。

登録が必要

データ ソースで登録（待機）が必要なことを示します。

マイグレーションが必要

データ ソースでマイグレーション（デバイス マネージャの待機）が必要なことを示します。

保守中

データ ソースが現在保守中であることを示します。

無効

管理者がデータ ソースを無効にしたことを示します。

詳細:

データ ソース ログの表示 (P. 30)
データ ソースの同期の失敗 (P. 185)

データ ソースの同期

CA Performance Center は、5 分ごとに、すべての登録済みデータ ソースとの定期グローバル同期を実行します。 手動で同期を要求することもできます。 手動同期は、トラブルシューティングや迅速な設定変更の伝達手段として役立ちます。 たとえば、グループを追加する場合は、手動同期を実行することにより、変更をデータ ソースに迅速に伝達できます。

手動同期を開始するときに、完全と増分のどちらのデータ ソース同期を実行するかを選択できます。 単一のデータ ソースまたは複数のデータ ソースを同期できます。

以下の手順に従います。

1. 管理者の役割を持つユーザとしてログインします。
2. ［データ ソースの管理］ページに移動します (P. 23)。

   ［データ ソースの管理］ページには、登録済みデータ ソースのリストが表示されます。
3. 同期するデータ ソースを選択して、［再同期］をクリックします。

   ［データ ソースの再同期］ページが表示されます。

   注: デフォルトで、増分同期が実行されます。 最後の同期タイム スタンプ以降の新しいレコードのみが含まれます。
4. 完全再同期を実行する場合は、［完全な再同期を実行］チェック ボックスをオンにします。

   アクションの確定を促すメッセージが表示されます。
5. 同期を確定するために［再同期］をクリックします。

   CA Performance Center が同期を実行します。 問題が発生した場合にのみ、メッセージが表示されます。

詳細:

データ ソースの同期の失敗 (P. 185)

データ ソース ログの表示

エラーが発生するたびに、CA Performance Center が情報をログ記録します。サービスごとに別々のログ ファイルが使用されます。これらのログには、CA¥PerformanceCenter ディレクトリ下のサービス固有のサブディレクトリからアクセスできます。 詳細については、「ログ (P. 181)」を参照してください。

同期は 5 分ごとに発生します。ログがいっぱいにならないように、ログに記録されるのは、最初の同期のほかには、後続の完全同期または増分同期中に発生する障害のみです。 最後の同期がいつ行われたかを判断するには、［データ ソースの管理］ページで［最終ポーリング］の日付を確認します。

データ ソース ログを使用して、データ ソースの同期に伴う疑わしいエラーを調査します。 ［データ ソース ログ］ページからイベント詳細にドリル ダウンできます。 この情報は、データベース間の同期に伴って発生する可能性のある問題のトラブルシューティングに利用できます。

以下の手順に従います。

1. 管理者の役割を持つユーザとしてログインします。
2. ［データ ソースの管理］ページに移動します (P. 23)。

   このページには、現在の登録済みデータ ソースのリストが表示されます。
3. ログを表示するデータ ソースを選択して、［ログ］をクリックします。

   ［データ ソース ログ］ページが表示されます。 ログは、選択されたデータ ソースの同期に関連したイベントだけが表示されるようにフィルタされます。

詳細:

データ ソースの同期 (P. 29)
同期 (P. 25)
データ ソースの同期の失敗 (P. 185)

データ ソースの登録

データ ソースを登録するまで、CA Performance Center ダッシュボード内でデータを使用できません。 登録は CA Performance Center の［データ ソースの管理］ページで実行します。

注: データ ソース バージョンの互換性の詳細については、「リリース ノート」を参照してください。

以下の手順に従います。

1. 管理者の役割を持つユーザとしてログインします。
2. ［データ ソースの管理］ページに移動します (P. 23)。

   登録済みのデータ ソースの現在のリストが［データ ソースの管理］ページに表示されます。
3. ［追加］をクリックします。

   ［データ ソースの追加］ダイアログ ボックスが表示されます。
4. 追加するデータ ソースのタイプを［ソース タイプ］リストから選択します。

   注: CA Performance Center データ ソースとして登録可能なすべての CA 製品が［ソース タイプ］リストに表示されます。 このリストはインストール済みの製品を表示するようにはフィルタされていません。
5. データ ソースのステータスを選択します。 登録しているデータ ソースのポーリングを延期する場合は、［無効］を選択します。

   注: データ ソースを編集して［有効］ステータスを選択するまで、このデータ ソースからのデータはレポートされません。 このデータ ソースからのビューには、［表示するデータがありません］というメッセージが表示されます。
6. データ ソースのホスト名を入力します。

   ホスト名は通常、このデータ ソース用のデータベースがインストールされたサーバの IP アドレスまたは DNS ホスト名です。

   - Data Aggregator データ ソースでは、Data Aggregator コンポーネントがインストールされているホストの IP アドレスまたはホスト名を指定します。
   - 分散構成内の他のデータ ソースでは、管理コンソールのホスト名を指定します。

7. データ ソースとの接続に使用するポートを入力します。入力するポートは、選択するプロトコルによって異なります。

   詳細については、「CA Single Sign-On ユーザ ガイド」を参照してください。

8. データ ソースに接続するために使用するプロトコルを選択します。ネットワーク通信に SSL が使用されている場合は、**https** を選択します。**https** オプションを選択する前にシステムが正しく設定されていることを確認してください。

   注: CA Performance Center とデータ ソース製品間の通信に SSL を使用できます。 詳細については、「*CA Single Sign-On ユーザ ガイド*」を参照してください。

9. （オプション）データ ソース用の表示名を入力します。

   デフォルトで、データ ソース タイプとホスト名を組み合わせて表示名が作成されます。ここで別の名前を入力することができます。たとえば、NetworkFlowAnalysis@xxx.x.x.xx の代わりに、データ ソースを NetworkFlowAnalysis_NewYork と命名できます。

10. （オプション）Web コンソールの［データソースと同じ］チェック ボックスをオフにして、Web コンソール オプションを有効にします。データ ソース コンソールに別のホスト名およびポートを指定できます。

    注: データ ソース Web コンソール アドレスは、通常ホスト名と同じです。 ネットワークアドレス変換が展開される場合に、このパラメータを使用します。

11. （オプション）［他のデータ ソースからのデバイスを検出］チェック ボックスをオンにします。このオプションにより、他のデータ ソースによって CA Performance Center と同期しているデバイスを、Data Aggregator で自動的に検出するかどうかを設定できます。

    注: このオプションを使用できるのは、データ ソースとして Data Aggregator を選択している場合のみです。

12. ［保存］をクリックして、データ ソースを登録します。

    登録したデータ ソースが、［データ ソース］リストに表示されます。

詳細:

データ ソース接続のテスト (P. 33)
データ ソースの編集 (P. 33)

データ ソース接続のテスト

ほとんどの場合、ステータスは、データ ソース登録が正常に完了したことを示します。 ステータスがエラーを示している場合は、［データ ソースの管理］ページのテスト機能を使用します。

［テスト］ボタンはテストを開始して、新しいデータ ソースが正しく登録され、接続されていることを確認します。 このテストは、バージョンの互換性をチェックし、データ ソースが CA Performance Center ソフトウェアの別のインスタンスに登録されていないことを確認します。

テストに合格しなかった場合は、サーバ名または IP アドレスがソース タイプと合っていることを確認してください。 詳細については、「データ ソース テストの失敗 (P. 187)」を参照してください。

データ ソースの編集

登録済みデータ ソースを編集して、入力したパラメータを変更できます。たとえば、データ ソースに関連付けられた表示名を変更できます。

以下の手順に従います。

1. 管理者の役割を持つユーザとしてログインします。
2. ［データ ソースの管理］ページに移動します (P. 23)。

   ［データ ソースの管理］ページには、現在の登録済みデータ ソースのリストが表示されます。
3. 変更するデータ ソースを選択して、［編集］をクリックします。

   ［データ ソース管理］ダイアログ ボックスが表示されます。
4. 必要に応じて、設定を変更します (P. 31)。
5. （オプション）データ ソースが正しく接続されていることを確認するには、データ ソースを選択して［テスト］をクリックします。

   接続が失敗した場合は、「データ ソース テストの失敗 (P. 187)」で詳細を参照してください。
6. ［保存］をクリックします。

詳細:

データ ソースの登録 (P. 31)
データ ソース接続のテスト (P. 33)

データ ソースの削除

選択された管理者は、CA Performance Center に登録されているデータ ソースを削除できます。削除したデータ ソースは、別の CA Performance Center インスタンスに登録できます。 削除プロセスでは、データ ソース管理のロック解除も行われます。

データ ソースを削除すると、悪影響が生じる場合もあります。 ［データ ソースの削除］の役割権限 (P. 118)を持つ管理者のみがデータ ソースを削除できます。 この役割権限は、デフォルトでは付与されておらず、別の手順として役割に割り当てる必要があります。

［ビューの非表示］ (P. 18)が有効な場合、削除するデータ ソースと関連付けられるビューが非表示となります。 その結果、データ ソースを削除すると、メニューやダッシュボードが利用不可になる場合があります。ダッシュボード、コンテキスト タブ、またはカスタム メニューが表示されるには、データ ソースが登録済みのビューが少なくとも 1 つ含まれている必要があります。

次の手順に従ってください:

1. 管理者の役割を持つユーザとしてログインします。
2. ［役割の管理］ページに移動します (P. 128)。

   役割の現在のリストがページに表示されます。
3. ［管理者］の役割を選択して、［編集］をクリックします。データ ソースを削除する権限は、この事前定義済みの役割でのみ使用可能です。

   ［役割の権限の編集］ダイアログ ボックスが表示されます。
4. ［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。

   割り当てられた役割の権限は、この役割に対して読み取り専用になるので、使用できません。

5. ［データ ソースの削除］を選択します。

   右方向矢印をクリックして、［利用可能な権限］リストから［選択された権限］リストにアイテムを移動します。

6. ［OK］をクリックします。 次に［保存］をクリックし、変更を役割に保存します。

7. ［データ ソースの管理］ページに移動します (P. 23)。

   登録済みのデータ ソースの現在のリストが表示されます。

8. 削除（登録解除）するデータ ソースを選択します。

   ［削除］ボタンがアクティブになります。

9. ［削除］をクリックし、［はい］をクリックして削除を確定します。

   データ ソースがリストから削除されます。

SNMP プロファイル

多くの CA Performance Center データ ソースが、管理対象アイテムの MIB にパフォーマンス情報をクエリするときに SNMP を使用します。*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。これらの定義は、データ セキュリティの保証期間に、必要に応じて、データ ソースに SNMP パラメータを提供します。

データ ソースを登録すると、データ ソース内で作成されたすべてのプロファイルが CA Performance Center に追加されます。 逆の処理も行われます。CA Performance Center ですでに登録されているプロファイルが送り返され、すべての登録済みデータ ソース間で共有されます。 命名の競合が解消されます。また、プロファイルに対して加えられたすべての変更が、同期中に、すべての登録済みデータ ソースに伝達されます。

管理者役割を持つユーザは、SNMP プロファイルを作成、編集、および削除できます。 すべての SNMP プロファイルはデータ ソース間で共有されますが、それらはテナントに固有です。 デフォルト テナント管理者は、デフォルト テナントに関連付けられた SNMP プロファイルのリストを参照します（単一のテナント環境では認識されません）。 マルチテナント環境では、各テナント管理者は、そのテナントに対するプロファイルのみを参照できます。

SNMP プロファイル リストの表示

事前に定義された SNMP プロファイルのリストを表示できます。このリストには、各プロファイルの内容に関する概要情報が含まれます。

テナント定義が作成されていない場合は、SNMP プロファイル リスト内の定義がすべての登録済みデータ ソース間で共有されます。 グローバル管理者は、テナントに明示的に関連付けられない SNMP プロファイルのリストを参照します。

注: テナント管理者は自分のテナントに関連付けられたアイテムしか参照できません。

次の手順に従ってください:

1. 管理者の役割を持つユーザとしてログインします。
2. ［管理］-［システム設定］を選択し、［SNMP プロファイル］をクリックします。

   ［SNMP プロファイルの管理］ページが開き、現在の SNMP プロファイルのリストが表示されます。

   各プロファイルに関する以下の情報がリスト表示されます。

   順序

   SNMP プロファイルに含まれる保護された情報が、選択されたデバイスへのクエリに使用される順序を決定します。 クエリが失敗した場合は、優先順位に従って次のプロファイルが使用されます。

   プロファイル名

   SNMP プロファイルの名前を定義します。プロファイル名は、一意である必要があり、SNMP バージョン間での重複は許されず、大文字と小文字が区別されません。

   ポート

   このプロファイルに関連付けられたデバイスとの SNMP 接続に使用されるポートを指定します。

   デフォルト： UDP 161

SNMP バージョン

プロファイルで使用される SNMP のバージョンを指定します。 セキュリティの観点から SNMPv1 と SNMPv2C は似ているため、1 つのオプションが共有されます。SNMPv3 では別のオプションが使用されます。

認証プロトコル

（SNMPv3 のみ）このプロファイルに関連付けられたデバイスとの接続時に使用される認証プロトコルを指定します。SNMPv3 パケットを認証するために以下のアルゴリズムがサポートされています。

- なし（認証が試行されません）
- MD5 （メッセージ ダイジェスト 5）
- SHA （セキュア ハッシュ アルゴリズム）

プライバシー プロトコル

関連付けられたデバイスに接続するために使用される暗号化プロトコルを指定します。 どの許可プロトコルも使用されていない場合は、常に、「なし」です。

デフォルトで使用

デバイスに明示的に割り当てられなかったときにこのプロファイル内の情報が使用されるかどうかを示します。 無効の場合は、このプロファイルがプロファイルの除外をサポートするデータ ソース内の検出から除外されます。

詳細:

SNMP プロファイルの追加 (P. 38)

SNMP プロファイルの追加

管理者は、登録済みデータ ソースがデバイスにパフォーマンス データを問い合せるための SNMP プロファイルを作成できます。 SNMPv1/v2c 用または SNMPv3 用のこれらのプロファイルを作成できます。

テナント定義が作成されていない場合は、SNMP プロファイルがすべてのデータ ソース間で共有されます。ただし、SNMP プロファイルは各テナントに固有です。 グローバル管理者のみが、デフォルト テナントに関連付けられた SNMP プロファイルのリストを参照します。マルチテナント環境で、テナント管理者はそれぞれ、そのテナントのためのプロファイルのみを参照できます。

次の手順に従ってください:

1. 管理者の役割を持つユーザとしてログインします。
2. ［SNMP プロファイルの管理］ページに移動します (P. 36)。

   ［SNMP プロファイルの管理］ページには、現在の SNMP プロファイルのリストが表示されます。
3. ［New］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. すべてのフィールドにデータを入力し、必要に応じてデフォルト設定を変更します。 一部のフィールドは SNMPv3 にのみ適用されます。

   プロファイル名

   SNMP プロファイルの名前を定義します。プロファイル名は、一意である必要があり、SNMP バージョン間での重複は許されず、大文字と小文字が区別されません。

   SNMP バージョン

   プロファイルで使用される SNMP のバージョンを指定します。 セキュリティの観点から SNMPv1 と SNMPv2C は似ているため、1 つのオプションが共有されます。SNMPv3 では別のオプションが使用されます。

ポート

このプロファイルに関連付けられたデバイスとの SNMP 接続に使用されるポートを指定します。

注: SNMPv1/v2C のオプション パラメータ。

デフォルト： 161。

ユーザ名

（SNMPv3 のみ）プロファイルに対するユーザを特定します。その秘密鍵は SNMPv3 パケットの認証および暗号化に使用される可能性があります。 ユーザ名は文字列です。

コンテキスト名

（SNMPv3 のみ） SNMP エンティティによってアクセス可能な管理情報のコレクションを識別します。エンド ツー エンドの識別情報を提供し、SNMPv3 エージェントからデータを取得するために必要なオクテット文字列です。

コミュニティ名

（SNMPv1/v2C のみ）保護された文字列を定義し、関連するデバイスの MIB をデータ ソースにクエリするように指示します。 入力するコミュニティは、デバイス MIB への読み取り専用アクセスを提供している必要があります。

注: デフォルト SNMP プロファイルでは、コミュニティは「パブリック」です。

コミュニティ名の検証

保護されたコミュニティ文字列（名前）を確認します。

認証プロトコル

（SNMPv3 のみ）このプロファイルに関連付けられたデバイスとの接続時に使用される認証プロトコルを指定します。SNMPv3 パケットを認証するために以下のアルゴリズムがサポートされています。

- なし（認証が試行されません）
- MD5 （メッセージ ダイジェスト 5）
- SHA （セキュア ハッシュ アルゴリズム）

認証パスワード

（SNMPv3 のみ）SNMPv3 および選択した認証プロトコルを使用する認証のパスワードを指定します。

注: 長さが 8 文字以上の認証パスワードを指定します。一部のデータ ソースでは、この最小長より短い認証パスワードやプライバシー パスワードをサポートしません。 そのような場合、SNMP プロファイルは無効として処理され、一部のデータは収集されません。 空のパスワードは、認証プロトコルとして MD5 または SHA を使用する SNMP v3 プロファイルではサポートされていません。

認証パスワードの確認

認証パスワードを確認します。

プライバシー プロトコル

（オプション）データフローに使用する暗号化プロトコルを次のように指定します。データフローはこのプロファイルに関連付けられたデバイスまたはサーバに送信さます。

- なし（通信が暗号化されません）
- DES
- AES 128
- トリプル DES

注: このプロファイルに対する認証が有効になるまで、プライバシー プロトコル オプションは有効になりません。

プライバシー パスワード

暗号化キーの交換時に使用されるパスワードを定義します。 可能な長さの要件については、注を参照してください。

プライバシー パスワードの検証

暗号化キーの交換時に使用されるパスワードを定義します。

デフォルトで新しいデバイスに使用

このプロファイル内の情報をデフォルトで使用するかどうかを指定します。 CA Performance Center はこの情報を使用して、監視対象トラフィックから検出された新しいアイテムに接続します。 その接続が失敗した場合は、優先順位に従って次のプロファイルが使用されます。 検出からプロファイルを除外する場合は、このパラメータを無効にします。

注: このパラメータは CA Infrastructure Management Data Aggregator データ ソースに適用されません。

5. ［保存］をクリックします。
6. ［SNMP プロファイルの管理］ページが表示されます。新しいプロファイルがリストに表示されます。

   CA Performance Center が、自動的に、グローバル同期を実行して、すべての登録済みデータ ソースにプロファイル情報を送信します。

詳細:

SNMP プロファイルの編集 (P. 41)
クリア テキストでのデータの表示 (P. 43)

SNMP プロファイルの編集

必要な役割の権限を持つユーザは、セキュリティ設定に対する変更を反映するように SNMP プロファイルを変更できます。

注: いったん作成されたプロファイルの SNMP バージョンは変更できません。 プロファイルを削除してから、作り直す必要があります。

以下の手順に従います。

1. 管理者の役割を持つユーザとしてログインします。
2. ［SNMP プロファイルの管理］ページに移動します (P. 36)。

   このページには、現在の SNMP プロファイルのリストが表示されます。
3. リストでプロファイルを選択して、［編集］をクリックします。

   ［プロファイルの編集］ダイアログ ボックスが表示されます。
4. 必要に応じてプロファイル設定を変更します (P. 38)。

5. ［OK］をクリックします。

   変更内容が保存されます。

   ［SNMP プロファイルの管理］ページが表示されます。

   CA Performance Center が、自動的に、グローバル同期を実行して、すべての登録済みデータ ソースに更新された情報を送信します。

SNMP プロファイルの順序の変更

管理者は、SNMP プロファイルの優先順位を変更し、検出とレポート内の選択肢を変更することができます。［順序］パラメータは、SNMP プロファイル内に含まれる保護された情報を使用して選択済みデバイスにクエリを試行する順序を決定します。クエリが失敗した場合は、優先順位に従って次のプロファイルが使用されます。

テナント管理者は、関連付けられたテナント ドメインに使用可能な SNMP プロファイルのみを参照して管理できます。

以下の手順に従います。

1. 必要な管理の役割の権限（P. 118）を持つユーザとしてログインします。
2. ［SNMP プロファイルの管理］ページに移動します（P. 36）。

   このページには、現在の SNMP プロファイルのリストが表示されます。
3. リストでプロファイルを選択します。
4. ［上に移動］または［下に移動］をクリックしてリストの順序を変更するか、プロファイルを正しい位置にドラッグ アンド ドロップします。

   SNMP プロファイルがリスト内の上位または下位に移動します。 優先度の変更がデータベースに保存されます。

   注: ［上に移動］はリスト内の最初のアイテムには使用できません。［下に移動］はリスト内の最後のアイテムには使用できません。

クリア テキストでのデータの表示

デフォルトでは、保護されたデータは［SNMP プロファイルの追加］および［SNMP プロファイルの編集］ページで暗号化されます。そのため、SNMP ポーリングでの問題をトラブルシュートするのが難しくなる可能性があります。

プロファイルが使用しているコミュニティ、または SNMPv3 認証/プライバシー パスワードを、選択されたユーザが参照できるようにすることができます。

注: 保護された SNMP データをクリア テキストで表示する機能は、事前に定義された管理者の役割に制限されます。

次の手順に従ってください:

1. 管理者の役割を持つユーザとしてログインします。
2. ［役割の管理］ページに移動します (P. 128)。

   役割の現在のリストがページに表示されます。
3. ［管理者］の役割を選択して、［編集］をクリックします。 SNMP クリア テキストを表示する役割権限は、この事前定義済みの役割でのみ使用可能です。

   ［役割の編集］ダイアログ ボックスが表示されます。
4. ［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。

   割り当てられた役割の権限は、この役割に対して読み取り専用になるので、使用できません。
5. ［SNMP クリア テキスト］の役割権限を選択します。
6. 右方向矢印をクリックして、［利用可能な権限］リストから［選択された権限］リストにアイテムを移動します。
7. ［OK］をクリックします。

   ［役割の編集］ダイアログ ボックスが表示されます。
8. ［保存］をクリックします。

   役割への変更が保存されます。

デフォルトでは、保護された SNMP データをクリア テキストで表示する機能は、ユーザに提供されます。 事前定義済み管理者の役割は、デフォルトではグローバル管理者にのみ割り当てられます。 別のユーザが SNMP プロファイルのトラブルシューティングし、セキュリティ情報をクリア テキストで参照するには、別のユーザ アカウントに管理者の役割を割り当てます。

SNMP プロファイルの削除

ホスト管理者またはテナント管理者は、不要になった SNMP プロファイルを削除できます。

テナント管理者は、自分のテナントに関する SNMP プロファイルしか参照または削除できません。

以下の手順に従います。

1. 必要な管理の役割の権限 (P. 118) を持つユーザとしてログインします。
2. ［SNMP プロファイルの管理］ページに移動します (P. 36)。

   このページには、現在の SNMP プロファイルのリストが表示されます。
3. プロファイルを選択して、［削除］をクリックします。

   ［SNMP プロファイルの削除］ダイアログ ボックスで削除の確認が促されます。
4. ［はい］をクリックします。

   SNMP プロファイルが削除されます。

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）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. 167)
アイテムと IP ドメインの関連付け (P. 55)
IP ドメイン (P. 44)
IP ドメインの設定方法 (P. 47)
IP ドメインの追加 (P. 49)

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. 155)」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. 167)」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 (P. 29)」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. 55)」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。

IP ドメインのリストの表示

IP ドメインは、複数のテナントや、IP アドレスが重複している環境を監視するために必要です。 テナントごとに 1 つ以上の IP ドメインを関連付ける必要があります。

テナントの作成を開始するときに、IP ドメインのリストとそのパラメータにアクセスします。

以下の手順に従います。

1. 必要な管理の役割の権限 （P. 118）を持つユーザとしてログインします。
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。

   ［IP ドメインの管理］ページには、現在の IP ドメインのリストが表示されます。

   カスタム IP ドメインが作成されなかった場合は、デフォルト ドメインだけがリスト内に表示されます。 この事前定義のドメインのパラメータはすべて「NULL」に設定されます。

   作成されたカスタム ドメインには以下のパラメータの値が設定されます。

   名前

   ドメインを識別します。

   説明

   （オプション）所有企業の名前など、このドメイン ネームスペースに関する説明です。

DNS 設定

（オプション）［DNS 設定］チェック ボックスを選択し、ドメインのプライマリおよびセカンダリ IP アドレスを割り当てます。

プライマリ DNS アドレス

このドメインのプライマリ名前サーバの IP アドレスです。

プライマリ DNS ポート

プライマリ名前サーバが使用するポート番号です。

セカンダリ DNS アドレス

このドメインのセカンダリ名前サーバの IP アドレスです。 プライマリ アドレスと同じにできます。

セカンダリ DNS ポート

セカンダリ名前サーバが使用するポート番号です。

詳細情報:

IP ドメインについて (P. 45)
IP ドメインの設定方法 (P. 47)
IP ドメインの追加 (P. 49)
IP ドメインの編集 (P. 53)

IP ドメインの追加

IP ドメインは、複数のテナントや、IP アドレスが重複している環境を監視するために必要です。 アイテムがデータ ソースを通してドメインとテナントに関連付けられるように CA Performance Center でカスタム IP ドメインを作成します。

デフォルト ドメインは自動的に作成されます。 このドメインには、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すべてのアイテムが含まれます。

新しいドメインの作成が完了したら、手動同期を実行することにより、新しいドメインをデータ ソースにプッシュできます。 そうでない場合は、約 5 分ごとに、自動的に同期が発生します。

次の手順に従ってください:

1. 必要な管理の役割の権限 (P. 118) を持つユーザとしてログインします。
2. ［IP ドメインの管理］ページに移動します (P. 48)。

   このページには、現在の IP ドメインのリストが表示されます。
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. 以下のパラメータに関する情報を入力します。

   名前

   ドメインを識別します。

   説明

   （オプション）所有企業の名前など、このドメイン ネームスペースに関する説明です。

   デバイス名エイリアス

   重要: エイリアスの CSV ファイルのインポートについて、以下の方法は推奨されていません。 エイリアスの設定には付属のスクリプトを使用してください (P. 200)。

   管理対象デバイスに使用するエイリアスを表します。 デバイス エイリアスは、CA Performance Center 内の関連付けられた管理対象アイテムに適用されるユーザ設定名です。 ［参照］をクリックし、エイリアスの CSV ファイルを指定してインポートします。 CSV ファイルには、IP アドレスとデバイス エイリアスのマッピングのカンマ区切りリストが含まれます。

   デバイスのプライマリ IP アドレスに関連付けられたエイリアスは、任意のセカンダリ IP アドレスに関連付けられたエイリアスよりも優先されます。 ［インベントリ デバイス］リストの［アドレス］列で、プライマリ IP アドレスを探します。 CSV ファイルでは、常にデバイスのプライマリ IP アドレスを使用することを推奨します。

以下に例を示します。

```
172.24.36.107,Austin Router
```

ファイルを参照して選択し、［開く］をクリックします。

すでに管理しているデバイスにエイリアスを含める場合、これらのエイリアスの CA Performance Center との同期が開始するまで最大で 5 分かかる場合があります。

注: エイリアスを削除するには、デバイスの IP アドレスと空のエイリアスの列が含まれる CSV ファイルをインポートします。 エイリアスを変更するには、CSV ファイル内のエイリアス エントリを変更して、ファイルを再インポートします。

インターフェースの説明の上書き

重要: CSV ファイルの代替インターフェースの説明をインポートする際に、以下の方法の使用は推奨されていません。 代替の説明の設定には付属のスクリプトを使用してください (P. 203)。

インターフェースで使用する代替の説明を表します。 インターフェースの説明が CA Performance Center にすでに表示されている場合でも、代替の説明を指定できます。 ［参照］をクリックし、代替の説明が含まれる CSV または TXT ファイルを指定してインポートします。このファイルには、カンマ区切りリストの形式で、デバイスの IP アドレス、インターフェース名、インターフェースの説明、および代替となるインターフェースの説明（エイリアス）のマッピングを含めます。

以下に例を示します。

```
172.24.36.107,ethernet_7,vmxnet3 Ethernet Adapter,Connection to Dallas
```

注: CSV または TXT ファイルでは、関連するデバイスのプライマリ IP アドレスを使用します。 セカンダリ IP アドレスはサポートされていません。 ［インベントリ デバイス］リストの［アドレス］列で、プライマリ IP アドレスを探します。

ファイルを参照して選択し、［開く］をクリックします。

すでに管理しているインターフェースに代替の説明を含める場合、これらの説明の CA Performance Center との同期が開始するまで最大で 5 分かかる場合があります。

注: 2 つ以上のインターフェースに、同じ代替のインターフェースの説明を使用できます。

代替の説明を削除するには、インポートする CSV または TXT ファイルに、デバイスの IP アドレス、インターフェース名、インターフェースの説明、および空白のエイリアス列を含めます。 代替の説明を削除すると、元のインターフェースの説明が CA Performance Center ビューに再表示されます。

重要: 表計算プログラムを使用して、CSV ファイルから代替の説明をすべて削除する場合、インターフェース説明の上書き列の列ヘッダをインポートしたファイルに含めるようにします。 この列ヘッダを含めない場合、元のインターフェース説明は CA Performance Center ビューに再表示されません。

説明を変更するには、CSV または TXT ファイル内のエイリアス エントリを変更して、ファイルを再インポートします。

DNS 設定

（オプション）［DNS 設定］チェック ボックスを選択し、ドメインのプライマリおよびセカンダリ IP アドレスを割り当てます。

プライマリ DNS アドレス

このドメインのプライマリ名前サーバの IP アドレスです。

プライマリ DNS ポート

プライマリ名前サーバが使用するポート番号です。

セカンダリ DNS アドレス

このドメインのセカンダリ名前サーバの IP アドレスです。 プライマリ アドレスと同じにできます。

セカンダリ DNS ポート

セカンダリ名前サーバが使用するポート番号です。

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ます。

6. さらに IP ドメインを追加する必要がある場合は上記手順を繰り返します。

詳細情報:

デバイス名の表示 (P. 197)

詳細情報:

データ ソースの同期 (P. 29)
IP ドメインについて (P. 45)
IP ドメインの追加 (P. 49)

IP ドメインの編集

作成されたカスタム IP ドメインを編集できます。 変更は次の同期時にすべての登録済みデータ ソースに伝達されます。

デフォルト ドメインは編集できません。 このドメインには、データ ソースによってカスタム ドメインに割り当てられなかったすべての管理対象アイテムを含められるだけの十分な容量が必要です。

ドメイン定義の編集が完了したら、変更をデータ ソースにプッシュするために強制的に同期を実行できます。 そうでない場合は、約 5 分ごとに、自動的に同期が発生します。

以下の手順に従います。

1. 必要な管理の役割の権限 (P. 118) を持つユーザとしてログインします。
2. ［IP ドメインの管理］ページに移動します (P. 48)。

   このページには、現在の IP ドメインのリストが表示されます。
3. ［編集］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. 必要に応じて、パラメータを変更します (P. 49)。
5. ［保存］をクリックします。

   IP ドメインに対する変更が保存され、IP ドメイン リストに反映されます。

   IP ドメインに対する変更は、同期が発生するまで、管理対象アイテムに適用されません。 各テナント内部では、すでに報告された管理対象アイテムは履歴データ ビュー内で変化しません。

IP ドメインの削除

パフォーマンス統計と管理対象アイテム間の関連付けと同様に、IP ドメイン関連付けは各データ ソース コンソール上のデータベース内にアイテムと一緒に保存されます。 そのため、ドメインは、簡単に、CA Performance Center から削除できません。

ドメインを削除すると、そのドメインはデータ ソース内で非アクティブとしてマークできます。 非アクティブ ドメインは、新しいデータを表示するビューに公開されません。 ただし、データ ソースを登録解除（削除）し、後で再登録した場合は、最初の同期でデータ ソースから CA Performance Center にドメイン情報のバックアップが送信されます。 データ ソースのデータベース内の管理対象アイテムはドメイン関連付けを保持します。

データ ソースによっては、ドメインを削除すると、ポーリングされたデバイス情報および履歴などのデータの損失を引き起こします。 そのような場合、再インストールを行う必要があります。 IP ドメインを削除する場合は、注意して行ってください。

ほとんどの場合、以下の手順で示すワークフローが使用できます。

以下の手順に従います。

1. 必要な管理の役割の権限（P. 118）を持つユーザとしてログインします。
2. ［IP ドメインの管理］ページに移動します（P. 48）。

   このページには、現在の IP ドメインのリストが表示されます。
3. 削除する IP ドメインを選択します。
4. ［削除］をクリックし、［はい］をクリックして削除を確定します。

   ドメインが IP ドメインのリストから削除されます。
5. 影響を受けるデータ ソースの Data Collector を編集して、そこで使用されているドメイン割り当てを変更し、削除されたドメインを置き換えます。

   注: 影響を受ける Data Collector には別のカスタム ドメインを選択することをお勧めします。 そうしなかった場合は、アイテムとデフォルト ドメインが関連付けられます。

   過去に収集され、削除されたドメインに関連付けられていたデータは、その状態のまま履歴ビューと同様に表示されます。

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. 47)」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。

CA Infrastructure Management Data Aggregator を使用した IP ドメインの生成方法

それぞれの CA Infrastructure Management Data Collector ホストは、管理対象アイテムを 1 つの IP ドメインに関連付けます。 マルチテナント展開を有効にするには、ソフトウェアをインストールしたらすぐに、各 Data Collector へ IP ドメインを割り当てます。

Data Collector をインストールする前に、CA Performance Center 管理インターフェースを使用して、必要なテナントと IP ドメインを作成します。

注: 1 つの IP ドメインを複数の Data Collector コンポーネントに関連付けることができます。ただし、各 Data Collector コンポーネントには 1 つの IP ドメインのみを割り当てることができます。

次の手順に従ってください:

1. 管理者の役割 (グローバル管理者) を持つユーザとして CA Performance Center にログインします。

2. テナントを作成します。
3. テナントを管理するか、またはテナント管理者としてログインします。
4. CA Performance Center に IP ドメインを作成します。

   新しい IP ドメインが［IP ドメイン］リストに表示され、現在のテナントに範囲指定されます。 他のテナント ユーザは、この IP ドメインのアイテムを参照できません。
5. Data Aggregator コンポーネントをインストールします。
6. Data Aggregator コンポーネントを CA Performance Center と同期します。
7. Data Collector コンポーネントをインストールします。

   注: CA Infrastructure Management Data Aggregator コンポーネントのインストール方法の詳細については、「*CA Infrastructure Management Data Aggregator インストール ガイド*」を参照してください。

   Data Collector をデフォルト テナントと関連付けるかどうかを確認するメッセージが表示されます。マルチテナンシーを展開していない場合は、この関連付けを作成することを推奨します。
8. ［管理］-［データ ソース設定］を選択し、［Data Aggregator のデータ ソース］をクリックします。
9. ［システム ステータス］メニューから［Data Collector］をクリックします。

   Data Collector リスト ページが開き、利用可能な Data Collector インストールのリストが表示されます。
10. リスト内の各 Data Collector の IP ドメインおよびテナントを選択して、［割り当て］をクリックします。

    注: マルチテナンシーを展開していない場合は、デフォルト テナントの割り当てを保持します。
11. 設定した各 IP ドメインに関連付けられるディスカバリ プロファイルを作成します。

    注: ディスカバリの詳細については、「*CA Infrastructure Management Data Aggregator 管理者ガイド*」を参照してください。

インターフェースと CVI のドメインの変更

インターフェースおよび CVI は、最初のテナント/ドメイン設定を親ルータおよび Harvester から継承します。 親 Harvester が追加され、ルータおよびインターフェースが最初にアクティブになると、設定が継承されます。 Harvester がカスタム ドメインと関連付けられていない場合、ルータおよびインターフェースは、アクティブになるとデフォルト ドメインに割り当てられます。

インターフェースと CVI の設定を編集し、テナントおよびドメインにいつでも関連付けることができます。この設定は、親ルータまたは Harvester に一致させる必要はありません。

この設定を変更すると、インターフェースのデータにアクセス権があるオペレータに影響する可能性があります。ポーリングに使用される SNMP プロファイルには影響しません。 ルータ テナントによって、ポーリング用の SNMP プロファイルのセットが判断されます。

以下の手順に従います。

1. アクティブなインターフェース ページを開きます。
   a. NFA Console メニューから［環境管理］を選択します。

      ［環境管理］ページが表示されます。

   b. ［環境管理］メニューから［インターフェース: 物理および仮想］を選択します。

      ［アクティブなインターフェース］ページが開きます。
2. テナントおよびドメインと関連付けるインターフェースの横のチェック ボックスをオンにします（複数可）。
   - 親ルータ、インターフェース、または CVI を検索するには、ルータ IP アドレスのすべてまたは一部、ルータまたはインターフェースの名前、インターフェースの説明を［検索］フィールドに入力し、［検索］をクリックします。 ルータ詳細を展開します。
   - インターフェースまたは CVI に手動で移動するには、親ルータが含まれるページに移動し、ルータ名の横の矢印をクリックします。 ルータ詳細が展開され、インターフェースと CVI が標示されます。
3. ［編集］をクリックします。

   編集用ダイアログ ボックスが開きます。複数のドメインが存在する場合のみ、ドメイン選択リストが編集ダイアログ ボックスに含まれます。

4. ［ドメイン］リストからテナント/ドメイン オプションを選択します。
5. ［保存］をクリックします。

   ダイアログ ボックスが閉じます。 変更が［アクティブなインターフェース］ページに表示されます。

注: Harvester およびルータに対してテナント/ドメインを設定を変更することもできます。

CA Application Delivery Analysis を使用した IP ドメインの生成

CA Application Delivery Analysis では重複した IP トラフィックを観測できます。 このようなトラフィックは管理対象サービス プロバイダ（MSP）環境で発生します。 プロバイダは、環境内でクライアント IP アドレスが重複している複数の顧客のために 1 台のサーバ上でアプリケーションをホストできます。

CA Application Delivery Analysis を有効にして、データ収集のセットアップ中に、個別の IP トラフィックを識別できるようにします。 データ収集パラメータを確認および変更するときに、以下の要素に同じ IP ドメインを割り当てます。

- 監視フィード
- クライアント ネットワーク
- サーバまたはサーバ サブネット

これらのフィードに同じ IP ドメインが割り当てられると、CA Application Delivery Analysis はドメインごとにクライアントとサーバ間のアプリケーション トラフィックをレポートします。

アプリケーションはドメイン独立です。 したがって、CA Application Delivery Analysis でドメイン全体のアプリケーション パフォーマンスを報告できるようにするために Exchange Company A と Exchange Company B のように、同じアプリケーションを 2 回定義する必要はありません。ただし、アプリケーション パフォーマンス、パフォーマンス OLA、および可用性 OLA に別々のしきい値を設定する場合は、IP ドメインごとにアプリケーションを作成します。

重複 IP トラフィックを分離する必要がない場合は、デフォルト ドメイン内の DNS 設定を使用して DNS をクエリし、CA Application Delivery Analysis サーバのホスト名を解決できます。 それ以外の場合は、CA Application Delivery Analysis でサーバに割り当てられた監視フィードを使用してホスト名が解決されます。

CA Application Delivery Analysis 内のドメイン リストの表示

CA Application Delivery Analysis 管理コンソールの管理セクションで、ドメイン定義と現在のドメイン関連付けのリストを表示できます。

注: データ ソース内の特定の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 グループに配属されます。 データ ソース内では、それらのアイテムがデフォルト ドメインに関連付けられているように見えます。

以下の手順に従います。

1. 管理コンソールで［管理］タブをクリックします。
2. ［表示項目］メニューの［データ監視］、［ドメイン］をクリックします。

   ［ドメイン］ページが表示されます。
3. （オプション）ドメインの DNS 設定を表示するには、［表示］列の虫眼鏡シンボルをクリックします。

   ［ドメイン プロパティ］ページが表示されます。
4. プロパティを確認します。
5. 完了したら、［OK］をクリックします。

   ［ドメイン］ページに戻ります。

監視フィードへのドメインの割り当て

CA Application Delivery Analysis 収集デバイス セットアップの一環として、各 Standard Monitor に監視するアイテムとカスタム ドメインを関連付けるように指示できます。

注: データ ソースによってカスタム IP ドメインに関連付けられていない管理対象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、カスタム IP ドメインを展開していないユーザに認識されません。

以下の手順に従います。

1. 管理コンソールで［管理］タブをクリックします。
2. ［表示項目］メニューの［データ監視］、［監視デバイス］をクリックします。

   CA Application Delivery Analysis 監視リスト ページが表示されます。
3. ［編集］をクリックして、Standard Monitor や Multi-Port Monitor などの多機能監視デバイスを編集します。

   ［監視のプロパティ］ページが表示されます。
4. ［監視フィード］リストまでスクロール ダウンします。
5. クリックして監視フィードを編集します。
6. カスタム IP ドメインを選択します。
7. ［更新］をクリックします。

   この監視フィードによって検出されたすべてのアイテムは、選択された IP ドメインに自動的に関連付けられます。

クライアント ネットワークへのドメインの割り当て

クライアント ネットワークを追加したら、その IP ドメイン関連付けを変更できなくなります。 割り当てられた IP ドメインを変更する必要がある場合は、ネットワークを削除して正しいドメインに追加し直す必要があります。

注: データ ソースによってカスタム IP ドメインに関連付けられていない管理対象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、カスタム IP ドメインを展開していないユーザに認識されません。

以下の手順に従います。

1. 管理コンソールで［管理］タブをクリックします。
2. ［表示項目］メニューの［データ監視］、［ネットワーク］をクリックします。

   ［ネットワーク リスト］ページが表示されます。
3. リストで IP ドメインを選択します。
4. ［ネットワークの追加］をクリックします。
5. ネットワークを追加するために必要な情報を入力します。
6. ［OK］をクリックします。

サーバまたはサーバ サブネットへのドメインの割り当て

サーバまたはサーバ サブネットを追加したら、その IP ドメインは変更できません。 間違った IP ドメインにサーバまたはサーバ サブネットを追加した場合は、そのサーバまたはサーバ サブネットを削除してから、正しいドメインに追加し直す必要があります。

注: データ ソースによってカスタム IP ドメインに関連付けられていない管理対象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、カスタム IP ドメインを展開していないユーザに認識されません。

以下の手順に従います。

1. 管理コンソールで［管理］タブをクリックします。
2. ［表示項目］メニューの［データ監視］、［サーバ］をクリックします。

   ［サーバ リスト］ページが表示されます。

3. リストで IP ドメインを選択します。
4. サーバまたはサーバ サブネットを追加するための情報を入力します。
5. ［OK］をクリックします。

CA Unified Communications Monitor を使用した IP ドメインの生成

CA Unified Communications Monitor 管理コンソールでは、検出されたアイテムを CA Performance Center 内のカスタム ドメインに関連付けるようコレクタに指示できます。CA Performance Center で 1 つのカスタム ドメインを作成することにより、すべての登録済みデータ ソース内の場所、ボイス ゲートウェイ、およびコール サーバのドメイン関連付けを有効にできます。

コール トラフィックから検出されたアイテムはすぐにドメイン指定付きで表示されます。 すでに検出済みのアイテムに対して関連付けが指定されることはありません。

場所は、含まれるサブネットによって IP ドメインと自動的に関連付けられます。 データ収集のフロー、およびデータと IP ドメインとの適切な関連を保持するには、新しい IP ドメインに場所を移動するときに注意してください。 CA Unified Communications Monitor オンライン ヘルプに説明されている手順に従い、IP ドメインの割り当てを変更します。

注: データ ソースによってカスタム IP ドメインに関連付けられていない管理対象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、カスタム IP ドメインを展開していないユーザに認識されません。

アイテムとカスタム IP ドメインを関連付けるようコレクタに指示します。

次の手順に従ってください:

1. ［管理］-［データ収集］-［コレクタ］をクリックします。
2. 各コレクタを編集して、［IP ドメイン］パラメータ用のドメインを選択します。
3. コレクタを再ロードして、コレクタにドメイン情報を送信します。

   次の製品同期後に、管理対象アイテムでドメインが生成されます。

通知

データ ソースからイベント マネージャに送信されたイベントに対して通知を設定できます。 受信イベントは、通知条件に設定した状態に対して評価されます。 条件を満たす場合のみ、イベント マネージャは通知アクションを実行します。 イベントが通知をトリガしない場合、このイベントはイベント リストに表示されたままになります。

注: 通知をサポートするデータ ソースの詳細については、「*CA Performance Center Readme*」を参照してください。

ユーザが設定および受信できるのは、アクセス権があるグループ内のアイテムに対するイベントの通知のみです。

重要: 通知を作成する前に、送信トラップ ポート (通常は 162) で SNMP プロファイルを作成します。

以下の情報を考慮します。

- 通知はユーザに固有です。他のユーザの通知を見ることはできません。
- イベント通知を削除するアクションは、実際のイベントまたは将来のイベントに影響しません。

通知の作成/編集ウィザードでは、以下の通知タイプが利用可能です。

トラップ

CA Spectrum など、環境内の障害管理システムまたはネットワーク管理システム (NMS) にトラップ通知を送信します。複数の送信先をサポートします。 最初の送信先は必須です。

既存のカスタマに互換性を提供するために、通知ウィザードでは 2 種類の MIB が利用可能です。

注: トラップ受信者はトラップを受信するように事前の設定が必要です。 各送信先では、SNMP コミュニティおよび IPV4 送信先に関する独自の設定を行うことができます。 トラップ形式の詳細については、トラップ受信者に対応する NMS ドキュメントを参照してください。

サポートされる役割: 管理者の役割を持つユーザ (グローバル管理者) がトラップ通知を設定できます。 管理者には、イベントを作成するデータ ソースに対する製品権限も必要です。

電子メール

イベントが発生するかクリアされたときに、1 人以上の受信者に電子メール通知を送信します。 電子メール内には、アラームをトリガしたデバイスまたはコンポーネントのコンテキスト ページへのリンクが提供されます。

サポートされる役割： ［通知の作成］の役割を持つユーザと、管理者の役割および製品権限を持つユーザが電子メール通知を設定できます。ただし、最初に管理者の役割で SMTP サーバを指定する必要があります。

管理者は、CA Performance Center ユーザ インターフェースの［管理］-［通知］メニューから、通知を表示、作成、または削除できます。 通知オプションが表示されるのは、イベント マネージャが有効であり、同期済みの［利用可能］状態にある場合のみです。

注: デフォルト テナント管理者は、実際のユーザ コンテキストで作業することで、テナント管理者またはテナント ユーザ用の通知を作成できます。テナント管理者またはテナント ユーザとしてログインします。 または、デフォルト テナント管理者はテナントを管理してユーザのプロキシを実行し、テナント範囲の通知を作成することができます。

代わりに、管理者はイベント マネージャ API を使用することもできます。次の URL を使用して、イベント マネージャ ホスト上のドキュメント インターフェースにアクセスします：
http://*hostname:*8281/EventManager/webservice/notifications/documentation

ユーザは、［マイ設定］-［通知］メニューから電子メール通知を作成できます。

詳細情報:

nhLiveAlarm 形式をトラップに使用 (P. 67)
EventManager 形式をトラップに使用 (P. 65)

EventManager 形式をトラップに使用

EventManager MIB は、トラップ通知をサポートしています。必要な場合、MIB ファイルは次の場所にあります。

InstallLocation/PerformanceCenter/PC/webapps/pc/mibs/netqos-em-mib

InstallLocation

CA Performance Center がインストールされたディレクトリです。

EventManager 形式が選択されると、送信されるトラップには以下の変数が含まれます。

netQosEventId

イベント マネージャがイベントに割り当てた識別子を指定します。

netQoSEventType

イベント タイプを指定します。

netQoSEventCategory

イベントを分類します。

値： 0 不明、1 障害、2 設定、3 アカウンティング、4 パフォーマンス、5 セキュリティ

netQoSEventSeverity

イベントの重大度を指定します。

値： 0 標準、1 不明、2 マイナー、3 メジャー、4 重大、5 使用不可

netQoSEventDescription

イベントの説明です。

netQoSEventState

イベントの現在の状態を指定します。 各状態にはそれぞれ通知があります。

値： 0 オープン、1 確認済み、2 クローズ、3 クリア

netQoSEventOpenTime

UTC タイムスタンプを指定します (eventState タイムスタンプから)。

netQoSEventMapURL

値は使用できません。 "" 文字列が送信されます。

netQoSEventDetailsURL

値は使用できません。 "" 文字列が送信されます。

netQoSEventAssociatedItemURL

アイテムの Web ページへの URL を指定します。

netQoSEventItemName

アイテム名を指定します。 アイテムごとに 1 つの通知があります。

最大長： 127 バイト

netQoSEventItemType

アイテムのタイプを指定します。

最大長： 32 バイト

netQoSEventItemSubtype

アイテムのサブタイプを指定します。

最大長： 32 バイト

netQoSEventItemIpAddress

アイテムの IP アドレスまたは空の文字列を指定します。

netQoSEventPropertyName

各プロパティに設定された 1 つの名前を指定します。 イベント内の各プロパティに PropertyName があります。 （プロパティはイベント タイプによって異なります。）

最大長： 128 バイト

netQoSEventPropertyValue

イベントのプロパティ値を指定します。イベント内の各プロパティに PropertyValue があります。（プロパティはイベント タイプによって異なります。）

nhLiveAlarm 形式をトラップに使用

nhLiveAlarm MIB は、トラップ通知をサポートしています。 必要な場合、MIB ファイルは次の場所にあります。

InstallLocation/PerformanceCenter/PC/webapps/pc/mibs/concord-diagmon.mib

InstallLocation

CA Performance Center がインストールされたディレクトリです。

トラップ通知に nhLiveAlarm 形式を使用するときは、以下の制限に注意してください。CA eHealth トラップ MIB によって記述された変数値の多くは、旧バージョンの NetQoS Performance Center との統合から変更されました。

nhServerIp

値は使用できません。 "" 文字列が送信されます。

nhServerName

値は使用できません。 "" 文字列が送信されます。

nhServerPort

値は使用できません。 "" 文字列が送信されます。

nhElementIp

アイテムの IP アドレス、または IP アドレスが存在しない場合は "" を指定します。

nhElementName

アイテム名を指定します。

nhElementId

アイテムの CA Performance Center ID （グローバル ID）を指定します。

nhStartTime

イベントからのタイムスタンプを指定します。

nhDisplayStr

イベントからの MaxThresholdValue 変数の値を指定します。

nhGroup

値は使用できません。 "" 文字列が送信されます。

nhGroupList

値は使用できません。 "" 文字列が送信されます。

nhExceptionType

値は使用できません。 "" 文字列が送信されます。

nhVariable

イベント プロファイル ルールの変数を指定します。

nhSeverity

イベントの重大度を指定します。

nhOpenViewSeverity

値は使用できません。 "" 文字列が送信されます。

nhProfile

イベント プロファイル名を指定します。

nhExceptionId

イベント ID を指定します。

nhTechType

値は使用できません。 "" 文字列が送信されます。

nhEventCarrier

値は使用できません。 "" 文字列が送信されます。

nhElementAlias

値は使用できません。 "" 文字列が送信されます。

nhComponent

値は使用できません。 "" 文字列が送信されます。

nhDescription

イベントの説明が含まれます。

nhAlarmOccurId

アラーム ID を指定します。

profileId

イベント プロファイル ID を指定します。

nhElementBaseType

アイテムのタイプを指定します。

営業時間の概要

ビジネス アクティビティの量は、特定の時刻や特定の曜日に増減します。そのため、インフラストラクチャ使用パターンは、規則的で予測可能なものになります。 ビジネス アクティビティが増加する期間は、ネットワークおよびサーバで最適なパフォーマンスを実現することが非常に重要です。 デフォルトでは、CA Performance Center ダッシュボードは、レポートされたデータをビジネス アクティビティへの影響度に基づいて区別しません。

CA Infrastructure Management オペレータがビジネスへの影響度がもっとも高いデータに注意を向けることができるように、管理者はサイト グループに営業時間の定義を関連付けることができます。 サイト グループを使用すると、管理対象のネットワークやデバイスを地理的な場所に基づいて整理することができます。各サイト グループには、1 セットの営業時間と 1 つのタイム ゾーンを関連付けることができます。 IT オペレータおよびエンジニアがユーザの企業内の複数のタイム ゾーンを管理し、かつトラブルシューティング アクティビティに優先順位を付けやすくするために、関連する営業時間でサイト グループを展開します。

戦略計画を作成するには、以下の設定で営業時間を展開します。

- 地理的に近い管理対象アイテムをサイト グループに含める
- 関連するオペレータとロケールの正確なタイム ゾーンをユーザ アカウントに設定する
- 営業時間の定義に、企業全体のビジネス アクティビティが増加する時間を正しく反映する

営業時間の各定義には、時刻と曜日の両方が含まれます。 時刻と曜日を選択する際には、ビジネス アクティビティが増加する期間を正しく反映するようにしてください。 企業のすべての所在地に対して、これらの定義を作成することをお勧めします。

営業時間の定義の管理

［営業時間の定義の管理］ページには、サイト グループと関連付けることができる営業時間の定義が一覧表示されます。 このページのオプションを使用して、営業時間の定義に関連付けられたタスクを実行できます。

サイト グループを作成する前に、営業時間の定義を追加することをお勧めします。 そうすれば、サイト グループの作成中に営業時間を割り当てることができます。

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 (P. 118) を持つユーザとしてログインします。
2. ［管理］-［カスタム設定］を選択し、［営業時間］をクリックします。

   ［営業時間の管理］ページに、現在の定義のリストが表示されます。営業時間の定義を作成していない場合、リストは空になっています。

   注: テナント管理者は自分のテナントに関連付けられたアイテムしか参照できません。

   各定義には、以下の情報がリスト表示されます。

   名前

   営業時間の定義の名前です。 営業時間をサイト グループに関連付けるときに、この定義の識別名としてリストに表示されます。

   説明

   定義を識別するための説明です。
3. リスト内の定義を選択してボタンをクリックし、このページ上でアクションを実行します。

   サイトの表示

   この営業時間が割り当てられたサイト グループを表示します。必要に応じて割り当てを変更できます。

詳細情報:

サイト グループの作成 (P. 94)
営業時間の概要 (P. 69)
営業時間の定義の作成 (P. 71)
営業時間の編集と関連付け (P. 72)

営業時間の定義の作成

サイト グループと関連付けることができる営業時間の定義を作成します。それぞれの定義には、時刻と曜日の両方が含まれます。 時刻と曜日を選択する際には、ビジネス アクティビティが増加する期間を正しく反映するようにしてください。 企業のすべての所在地に対して、これらの定義を作成することをお勧めします。

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 (P. 118)を持つユーザとしてログインします。
2. ［管理］-［カスタム設定］を選択し、［営業時間］をクリックします。

   ［営業時間の定義の管理］ページが表示されます。
3. ［新規］をクリックします。

   ［営業時間の追加］ダイアログ ボックスが表示されます。
4. 営業時間の定義の名前を指定します。
5. （オプション）この定義の説明を指定します。

   注: この名前は、営業時間をサイト グループに関連付けるときに、この定義の識別名としてリストに表示されます。 説明は、［営業時間の定義の管理］ページの定義のリストにのみ表示されます。
6. この定義に含める曜日の隣にあるチェック ボックスをオンにします。

   たとえば、［月］、［火］、［水］、［木］、［金］を選択して、一般的な週の営業日を表す定義を作成します。

   注: 1 つのサイトに複数の営業時間の定義を割り当てることはできません。 また、開始時刻と終了時刻を選択して指定された期間は 24 時間を超えることはできません。
7. 左側にある最初のドロップダウンを使用して、これらの営業時間の開始時刻を選択します。

   2 番目のドロップダウンを使用して、終了時刻を選択します。 30 分単位の時間はサポートされていません。

   営業時間は、サイト グループと関連付けられるまで有効になりません。
8. （オプション）すでにサイト グループを作成している場合は、同じダイアログ ボックスで営業時間とサイト グループを関連付けます。

a. ［関連付けるサイト グループの選択］をクリックします。

［関連付けるサイト グループの選択］ダイアログ ボックスが表示されます。

b. ［利用可能なサイト］リストからサイト グループを選択します。

c. 右方向矢印ボタンをクリックし、［選択されたサイト］リストにグループを移動します。

注: 営業時間とタイム ゾーンのサイト グループへの関連付けは、サイト グループの作成 (P. 94)時に行うこともできます。

9. ［OK］をクリックします。

［営業時間の追加］ダイアログ ボックスに戻ります。

10. ［保存］をクリックします。

営業時間の定義がリストに表示されます。

詳細:

営業時間の概要 (P. 69)
営業時間の編集と関連付け (P. 72)

営業時間の編集と関連付け

［営業時間の定義の管理］ページでは、営業時間の定義を作成および変更することができます。 また、このページで営業時間をサイト グループに関連付けることができます。

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 (P. 118)を持つユーザとしてログインします。
2. ［管理］-［カスタム設定］を選択し、［営業時間］をクリックします。

［営業時間の定義の管理］ページに、現在の定義が一覧表示されます。

3. （オプション）変更する営業時間の定義の現在の使用状況を確認し、必要に応じて変更します。 以下の手順を実行します。

   a. 定義を選択します。

   b. ［サイトの表示］をクリックし、［選択された営業時間のサイトを表示］ダイアログ ボックスを表示します。

      ［選択されたサイト］のリストに、この営業時間に関連付けられたすべてのサイトが表示されます。

   c. （オプション）［利用可能なサイト］リストで新しいサイト グループを選択します。

      注: カスタム グループは選択できません。 マウス カーソルをツリー内のサイト グループの上に置くと、項目を選択できます。

   d. 右方向矢印ボタンをクリックし、［選択されたサイト］リストに移動します。

   e. （オプション）同じ方法で、営業時間の関連付けを削除します。 サイト グループを選択し、左矢印を使用して［選択されたサイト］リストから削除します。

4. 編集する定義を選択します。

5. ［編集］をクリックします。

   ［営業時間の定義の編集］ダイアログ ボックスが表示されます。

6. 必要に応じて、営業時間の設定を変更 (P. 71)します。

7. ［保存］をクリックします。

   定義の変更が保存されます。

営業時間の定義の削除

使用しなくなった営業時間の定義は削除できます。 サイト グループと関連付けられている営業時間の定義を削除すると、その関連付けは削除されます。

営業時間とサイト グループの関連付けは、別の手順で削除することもできます。 関連付けのみを削除すると、営業時間の定義は別のサイトに割り当て可能な状態になります。 関連付けを削除するには、［営業時間の定義の管理］ページで［サイトの表示］をクリックします。

営業時間の定義を削除するか、または営業時間の定義とサイト グループの関連付けを削除すると、そのサイト グループから、データ ビューでの営業時間によるフィルタリングが失われます。 このサイト グループに属するアイテムのコンテキスト ページでは、［詳細］タブに「このアイテムは時間設定を含むサイト グループのメンバではありません」と表示されます。

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 (P. 118) を持つユーザとしてログインします。
2. ［営業時間の定義の管理］ページに移動します (P. 70)。

   このページには、現在の営業時間の定義がリスト表示されます。
3. 削除する定義を選択して、［削除］をクリックします。

   ［営業時間の定義の削除］ダイアログ ボックスが表示されます。
4. ［はい］をクリックし、削除を確定します。

   定義は削除され、リストに表示されなくなります。 この営業時間が割り当てられていたすべてのサイト グループから、営業時間によるフィルタリングが失われます。これらのサイト グループに含まれる管理対象アイテムからも、このフィルタリング オプションが失われますが、それ以外の影響はありません。

第 3 章: グループの作成と管理

このセクションには、以下のトピックが含まれています。

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:

グループのタイプ

グループは、階層ツリー構造で構成されます。 グループ ツリーを使用すると、ユーザが組織内のサービス、デバイス、アプリケーション、場所およびユーザの関係、ポリシーおよび依存性を定義できます。 以下のリストでは、グループ ツリー内のグループのタイプの概要について説明します。

システム グループ 

読み取り専用グループで、データ ソースからの情報に基づいて CA Performance Center によって自動的に作成されます。 これらのグループは編集できません（「ロック」記号で示されます）。 ただし表示、ユーザ アカウントへの権限グループとしての適用、カスタム グループまたはサイト グループへのコピーは可能です。

カスタム グループ 

階層レベルを作成し、アイテムをグループ ツリー内の論理関係に構成します。グループ ツリーのトップ レベルのカスタム グループは通常、ユーザの組織内の地理的、位相的、または機能的な部署を表します。より低いレベルのカスタム グループ（またはサブグループ）は通常、デバイス、サービスまたはアプリケーションなど管理対象アイテムのタイプを表します。または、これらのサブグループは、IT スタッフのジョブ機能を表すことができます。

管理者のみが、カスタム グループを作成し編集できます。 管理者は、CA Performance Center ダッシュボードおよびビューのデータをフィルタします。 ダッシュボードまたはビューのグループ コンテキストによって、表示されるデータが決定します。

サイト グループ 

支社などサイトに基づく特別なカスタム グループか、または地域や都市など物理的な場所です。 サイト グループを使用すると、CA Performance Center ダッシュボードにナビゲーション機能を作成し、サイト全体のビューを表示できます。サイト グループには［タイム ゾーン］および［営業時間］パラメータが含まれており、1 日のうちビジネス上重要な時間のデータを優先して表示することができます。

また、ダッシュボードに適用する詳細なコンテキストも用意されています。たとえば、各サイトのサイト グループを作成すると、単一のダッシュボードで各サイトについて個別にレポートできます。 企業の各データ センターやその他の主要なインフラストラクチャの場所に対して、サイト グループを作成することを強く推奨します。

グループ参照

システム グループまたはカスタム グループの読み取り専用コピーです。グループ ツリー内で別の場所にグループをコピーすると、グループ参照が表示されます。 ユーザ権限は、グループ参照を使用して割り当てることができます。 参照を使用すると、グループ構造を作成した後に、その構造をグループ ツリー内の別の部分にコピーできます。グループ参照を変更した場合は、元のカスタム グループのみが変更されます。しかし、それらの変更はすべての参照場所に継承されます。

元のグループへのリンクにアクセスするには、グループ参照を選択します。リンクをクリックすると、グループ ツリーのノードが展開され、元のグループの［プロパティ］タブが開きます。

詳細情報:

カスタム グループ (P. 80)
システム グループ (P. 77)
IP ドメイン (P. 44)
ダッシュボードをカスタマイズするためのグループの使用 (P. 88)

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. 84)」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. 44)」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。

カスタム グループ

カスタム グループは、システムの監視および管理戦略において重要なコンポーネントです。 カスタム グループを作成すると、データを構成し、データにアクセスするために各 CA Performance Center に権限を割り当てることができます。

*権限グループ*とは、高レベルな権限として動作するよう選択されたグループを意味します。 権限グループは、ユーザ アカウントに割り当てられ、各オペレータに表示されるアイテムおよびデータを正確に決定します。 権限グループまたは管理対象グループとして割り当てが可能なカスタム グループを作成します。

構成ブロックとしてシステム グループを使用することで、グループを作成できます。 グループ ルールを使用することで、監視中にアイテムが検出されたら自動的にグループに追加できます。 ルールをセットアップすると、グループの入力と保持がより簡単になります。 また、論理上または地理的に関連するルータまたはインターフェースなど、特定のアイテムを手動で追加することで、カスタム グループを入力できます。

アクセス可能なデータのより絞り込んだセットを作成するには、サブグループを権限グループに追加します。 サブグループを使用して権限を割り当てることで、問題の領域を調査し監視するための対象を絞り込むことができます。 対象を絞り込む必要のあるユーザ アカウントにサブグループを割り当て、対象をより広範囲にする必要のあるユーザ アカウントにはより高いレベルのグループ コンテナを割り当てることができます。

カスタム グループを作成する際に主に考慮することは、ユーザに表示する必要のあるデータへのアクセス権を与えるためにカスタム グループをどのように使用するのかということです。カスタム グループを作成して、個々のジョブ機能をアドレス指定するか、または類似アイテムをひとまとめにすることができます。

*サイト グループ*は、都市、地域、支社またはキャンパスなど物理的な場所に基づくカスタム グループです。 通常、サイト グループには、アイテム、および場所によってグループ化されるアイテムのサブグループが含まれます。 サイト グループをツリー構造内の他のカスタム グループに追加することにより、地理的および論理的に整理されたレポートを構築できるようになります。 サイト グループを使用して、ダッシュボード ビューを営業時間でフィルタリングできます。

他のカスタム グループと同様、サイト グループにはサブグループを含めることができます。 たとえばサイト グループを構築する場合は、最初に地域を作成し、都市が含まれるサブグループを追加できます。 次により多くのサブグループを追加し、各都市の建物を含めることができます。

詳細:

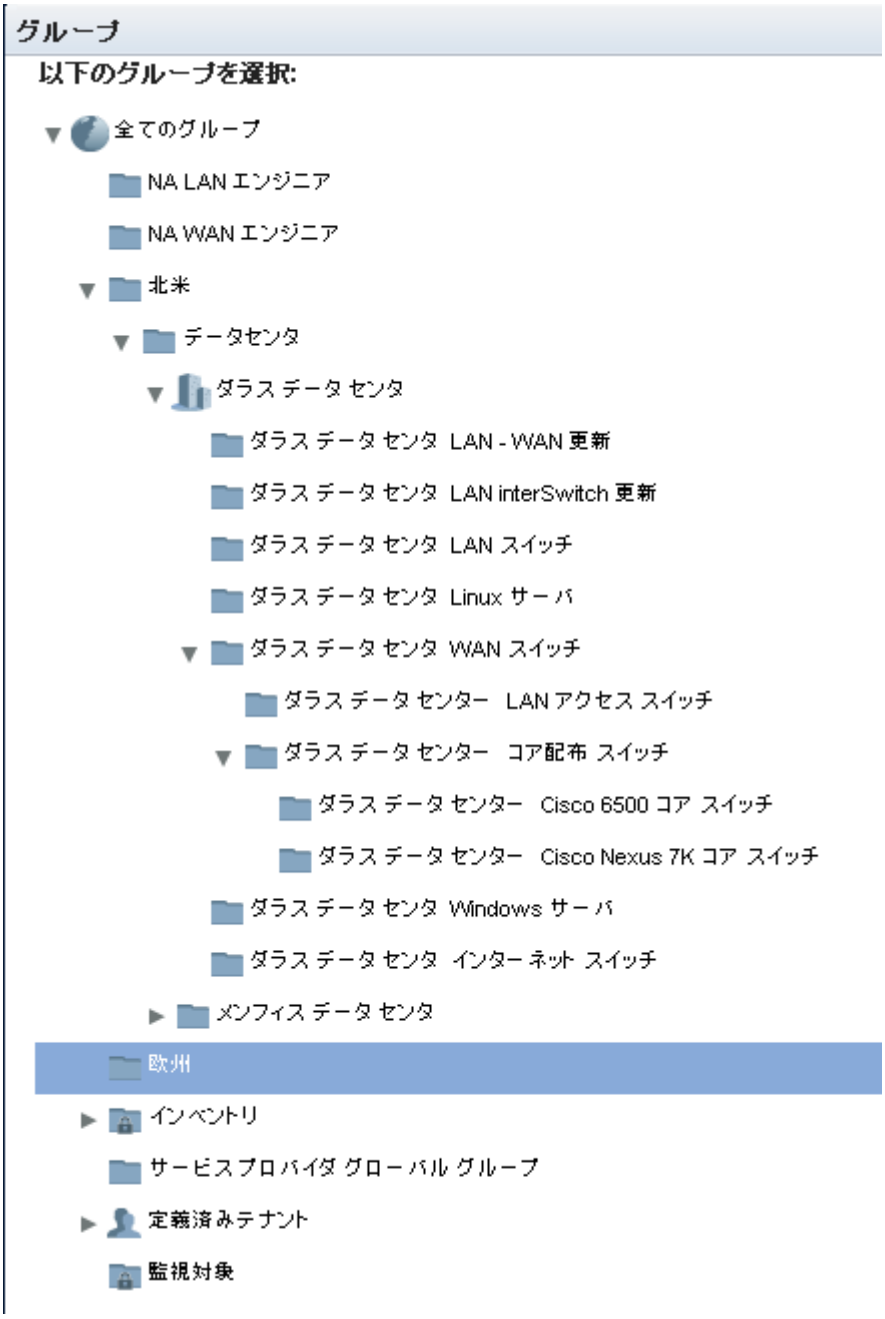
カスタム グループの作成 (P. 92)
グループのタイプ (P. 76)
サイト グループの作成 (P. 94)

ベスト プラクティスのグループ化

ユーザまたはカスタマのネットワークおよびデバイスを管理するカスタム グループを作成することは、ベスト プラクティスとして推奨されます。カスタム グループは、ジョブ機能、企業内のサイト、または関連するデバイスやデバイス インターフェースなど、より詳細なカテゴリに基づいて作成することができます。 グループ機能には、複数の構造を作成するための機能が含まれます。 グループ ツリーのさまざまな場所に、個別のグループを複数回使用できます。

有用なグループを作成するために推奨されるベスト プラクティスは、企業のインフラストラクチャ トポロジに基づいた「マスタ」グループ構造を作成することです。 その後、他のカスタム グループ構造で、これらのグループを参照として使用できます。

以下の例では、企業ネットワークの階層的なグループ構造を示します。


グループ
以下のグループを選択:
全てのグループ
NA LAN エンジニア
NA WAN エンジニア
北米
データセンタ
ダラス データ センタ
ダラス データ センタ LAN - WAN 更新
ダラス データ センタ LAN interSwitch 更新
ダラス データ センタ LAN スイッチ
ダラス データ センタ Linux サーバ
ダラス データ センタ WAN スイッチ
ダラス データ センター LAN アクセス スイッチ
ダラス データ センター コア配布 スイッチ
ダラス データ センター Cisco 6500 コア スイッチ
ダラス データ センター Cisco Nexus 7K コア スイッチ
ダラス データ センタ Windows サーバ
ダラス データ センタ インターネット スイッチ
メンフィス データ センタ
欧州
インベントリ
サービス プロバイダ グローバル グループ
定義済みテナント
監視対象

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. 44)」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。

権限グループとコンテキスト グループ

「権限グループ」および「コンテキスト グループ」は同じエンティティであるカスタム グループに適用される用語です。 権限グループは、データ アクセスを割り当てる目的で、管理対象アイテムを構成するために作成されます。 それらは権限セットとしてユーザ アカウントに割り当てられます。 ビューおよびダッシュボード ページのデータ コンテキストを決定するため、権限グループがフィルタとして適用されると、それらはコンテキスト グループと呼ばれます。

カスタム グループを権限として適用すると、次のものが有効になります。

- 特に物理的な場所など、ユーザの担当地域のデータを表示するユーザ
- セキュリティ上の理由で、データを表示できるユーザを制限する管理者

また権限グループより下のグループ ツリーのセクションを使用しても、サマリまたはグループのダッシュボードのデータ コンテキストを変更できます。

ユーザ アカウントに割り当てられたグループによって、ダッシュボードでユーザに表示されるデータが決定します。 現在のダッシュボードのフィルタとして機能するグループは、そのダッシュボードの *グループ コンテキスト*です。 CA Performance Center に初めてログインすると、表示されるページにデフォルトの権限グループのコンテキストが反映されます。

別のコンテキスト グループを選択すると、ダッシュボード ページのすべてのビューのコンテキストを変更できます。詳細については、「ダッシュボードのグループ コンテキストの変更」を参照してください。

グループとデータ ソース

読み取り専用システム グループは、データ ソースに固有です。 ほとんどのシステム グループは、データ ソースが登録されるまで作成されません。一致するシステム グループのみが、データ ソースと CA Performance Center の間で同期されます。

一方カスタム グループは、同期中にすべてのデータ ソースに送信されます。 ドリル ダウンをサポートするデータ ソースでは、グループ構造はレポートするインターフェースでレプリケートされます。 サポートされている場合は、グループ名から個別のグループ メンバのデータにドリル ダウンできます。

選択したデータ ソースについては、グループ化のいくつかの制限が適用されます。 たとえば CA eHealth グループは、カスタム グループまたはサイト グループにはコピーできません。それらは、CA eHealth で設定されたとおり、スタンドアロン グループとしてのみ使用できます。

ダッシュボードをカスタマイズするためのグループの使用

ユーザが CA Performance Center にログインすると、表示されるダッシュボードには、各ユーザに表示権限があるデフォルト グループのデータが含まれます。 ユーザ アカウント設定で各ユーザのデフォルト グループを設定できます。 たとえば、サイト A に対して主要な責任があり、サイト B ではバックアップとして機能するオペレータは、両方のグループのデータを表示できます。 ただしデフォルト グループの設定によって、このオペレータにデフォルトでサイト A 情報のみ表示することができます。

デフォルト グループ機能を使用すると、ユーザの企業内のすべてのサイトを表すカスタム ダッシュボードを作成できます。

次の手順に従ってください:

1. ユーザの企業の各サイトまたは支社を表すカスタム グループを作成します。 これらの場所を表すわかりやすい名前を使用します。
2. カスタム ダッシュボードを作成します。
3. ユーザの場所を監視するには、すべてのオペレータが毎日使用するビューを追加します。

   注: このダッシュボードは、すべてのユーザが表示できるメニューに追加します。ユーザ アカウント役割によって、メニューへのアクセスが決定します。
4. 新しいデフォルト グループを選択するには、これらの手順に従って、各ユーザ アカウントを編集します。
   a. 管理者権限を持つユーザとしてログオンします。
   b. ［ユーザの管理］ページに移動します (P. 149)。
   c. 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。
   d. ウィザードに従い［権限グループ］ダイアログ ボックスに進みます。
   e. ［デフォルト グループ］ドロップダウン リストを使用し、このユーザにデフォルトで表示されるグループを選択します。
   f. ［保存］をクリックします。

5. 各ユーザに対して別のデフォルト グループを設定するには、前の手順を繰り返します。

   別のユーザが同じカスタム ダッシュボードを表示する場合、彼らは別のデータを参照します。データはそれらのデフォルト グループに基づきます。

グループ管理

グループ機能は、管理者がデータを構成し、そのデータを誰に表示するのかを制御できる、強力なツールです。 パフォーマンス問題がレポートされた場合、ユーザ アカウントに割り当てられた権限グループを使用することで、オペレータはデータを論理的なフローで効率的に分析できます。すべての管理対象アイテムを平均化した管理対象アイテム データから、同じタイムフレーム内の単一のアイテムに関する情報にドリルダウンできます。

作成したグループ、およびそれらのグループが含まれる構造は、CA Performance Center を最適化するための重要な要件です。 ユーザの要件を満たす権限グループを割り当てる戦略を開発するには、CA の技術担当者に相談することを推奨します。

始めに、［グループの管理］ページのグループを表示します。 このページでは、左ペインにグループ ツリー (P. 76)が表示されます。 右ペインのタブ オプションから、グループの［アイテム］、［プロパティ］、［ルール (P. 96)］にアクセスできます。グループのデータ入力および編集 (P. 105)を行うには、これらのタブ オプションを使用します。

詳細:

カスタム グループの作成 (P. 92)
システム グループ (P. 77)
手動で管理対象アイテムをグループに追加 (P. 103)
ルールに従って管理対象アイテムをグループに追加 (P. 96)

グループ メンバシップの表示

［グループの管理］ページのシステム グループまたはカスタム グループに追加されたすべてのアイテムの並べ替え可能なリストを表示します。グループ ルールを検証したり、カスタム スクリプトによってグループが適切に作成および入力されたことを確認したりできます。 選択したグループ内に、すべてのアイテム、またはアイテムのフィルタされたリストを表示できます。

グループ ツリーのカスタム グループ、サイト グループおよびシステム グループは、アイコンによって区別されます。 詳細については、「グループのタイプ (P. 76)」を参照してください。

フィルタを使用すると、グループに手動で追加されたすべてのアイテムなど、表示するアイテムのタイプを選択できます。 デフォルトでは、［アイテム］タブ上のリストは、グループに直接追加されたアイテムのみを表示します。 アイテムの追加は、手動で、またはルールの適用（直接アイテム）によって行われます。

以下の手順に従います。

1. 管理者の役割を持ったユーザとしてログインするか、または有効な「マイ カスタム グループ」機能を持ったオペレータアカウントを使用します。
2. ［管理］-［カスタム設定］を選択し、［グループ］をクリックします。また、［マイ設定］、［マイ カスタム グループ］をクリックできます。

   ［グループ管理］ページが表示されます。

   注: テナント管理者は自分のテナントに関連付けられたアイテムしか参照できません。
3. メンバシップを表示するグループを検索するには、左ペイン内の［グループ］ツリーのノードを展開します。

   注: サブグループが含まれるグループには、［アイテム］タブにメンバが表示されません。 メンバを表示するには、これらのグループを展開し、サブグループを選択します。

4. グループを選択します。

   右ペインの［アイテム］タブが選択されています。

   注: カスタム グループの場合も［ルール］タブが表示されます。

   デフォルトでは、アイテムが表示されません。

5. 表示するアイテムを指定するには、［アイテムの表示］リストからフィルタを選択します。

6. ［アイテムの表示］リストのアイテム タイプ名の隣にある矢印をクリックします。 選択したグループのタイプに応じて、以下のメンバシップ タイプが適用可能です。

   直接アイテム

   手動でまたはルールの適用によってグループに直接追加されたアイテムが含まれます。 ［直接アイテム］が選択されている場合のみ、アイテムを追加および削除できます。 「追加元」列は、アイテムが手動（ユーザ）またはグループ ルール（ルール）によって追加されたかを示します。

   直接および継承アイテム

   直接追加されたか、または直接追加されたアイテムの子として継承されたかにかかわらず、グループのすべてのアイテムが含まれます。

   ［プロパティ］タブの設定によって、アイテムを継承できるかどうかが決定します。 除外されるアイテムは、継承されません。

   継承されたアイテム

   グループ内の管理対象アイテムの子のみを含みます。 このグループに対する継承を有効にし、ルータを追加した場合、ルータと関連付けられるインターフェースはすべてグループに追加されます。

   継承されたアイテムは個別に削除できません。 親アイテムが削除されると、自動的に削除されます。

除外

ルールによってグループに追加されたが、その後グループ ルールによって除外されたアイテムを意味します。 これらのアイテムを表示するには、この設定を選択します。

7. リストからアイテム タイプを選択します。

   グループに含まれている選択したタイプのすべてのアイテムのリストが表示されます。 必要に応じてリンクをクリックし、アイテムを数ページスクロールします。

詳細:

カスタム グループの作成 (P. 92)
グループ (P. 75)
グループのタイプ (P. 76)
グループ管理 (P. 89)
ルールに従って管理対象アイテムをグループに追加 (P. 96)

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 (P. 94)」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 (P. 118) 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 (P. 90)。

   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:

カスタム グループ (P. 80)
権限グループとコンテキスト グループ (P. 86)
手動で管理対象アイテムをグループに追加 (P. 103)
ルールに従って管理対象アイテムをグループに追加 (P. 96)

サイト グループの作成

サイト グループは、都市、地域、支社またはキャンパスなど物理的な場所に基づくカスタム グループです。サイト グループには［タイム ゾーン］および［営業時間］パラメータが含まれており、ビジネス上重要な時間のデータを正確にフィルタすることができます。

サイト グループは、［グループ］ツリーの［すべてのグループ］ノードの下、あるいは既存のカスタム グループまたはサイト グループ内に作成します。 システム グループにはグループを追加できません。システム グループには、ロック アイコンによって読み取り専用ステータスが示されています。

サイト グループにはサブグループを含めることができます。 IT インフラストラクチャの地理的な場所およびアーキテクチャを反映するような階層構造を作成します。

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 (P. 118) 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 (P. 90)。

   ツリー構造内にページの現在のグループが表示されます。

3. ［グループ］ツリーのノードを展開して、新規グループを作成する場所を見つけます。

4. 右クリックし、［新規グループの追加］を選択します。

   ［グループの追加］ウインドウが表示されます。

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. ［グループ タイプ］リストから［サイト］を選択します。

   ［場所］および［タイム ゾーン］フィールドが表示されます。

7. このサイト グループが表す地理的な場所の名前を入力します。

   このグループ内の管理対象アイテムを適切なタイム ゾーンに調整できるように、物理的な場所を使用します。

   注: この名前は、サイト グループの説明としてデータ ビューに表示されます。

8. このサイト グループのタイム ゾーンをリストから選択します。

   注: UTC からの時間差が 30 分および 15 分のタイム ゾーンはサポートされていません。最も近い 1 時間単位のタイム ゾーンを選択してください。

   ［営業時間］パラメータが有効になります。

9. カスタマイズした営業時間の定義をリストから選択します。 営業時間の定義は、別の手順で作成されます。

10. ［保存］をクリックします。

    新しいサイト グループが、［グループ］ツリーに表示されます。

11. この手順を繰り返して、企業内のすべてのサイトおよびタイム ゾーンを表すのに必要なサイト グループをすべて作成します。

    ユーザが追加するまで、サイト 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 (P. 103)。
    - グループ メンバシップを管理するルールを作成します (P. 96)。

詳細:

カスタム グループの作成 (P. 92)
グループのタイプ (P. 76)
営業時間の定義の作成 (P. 71)

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 (P. 90)。

   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。

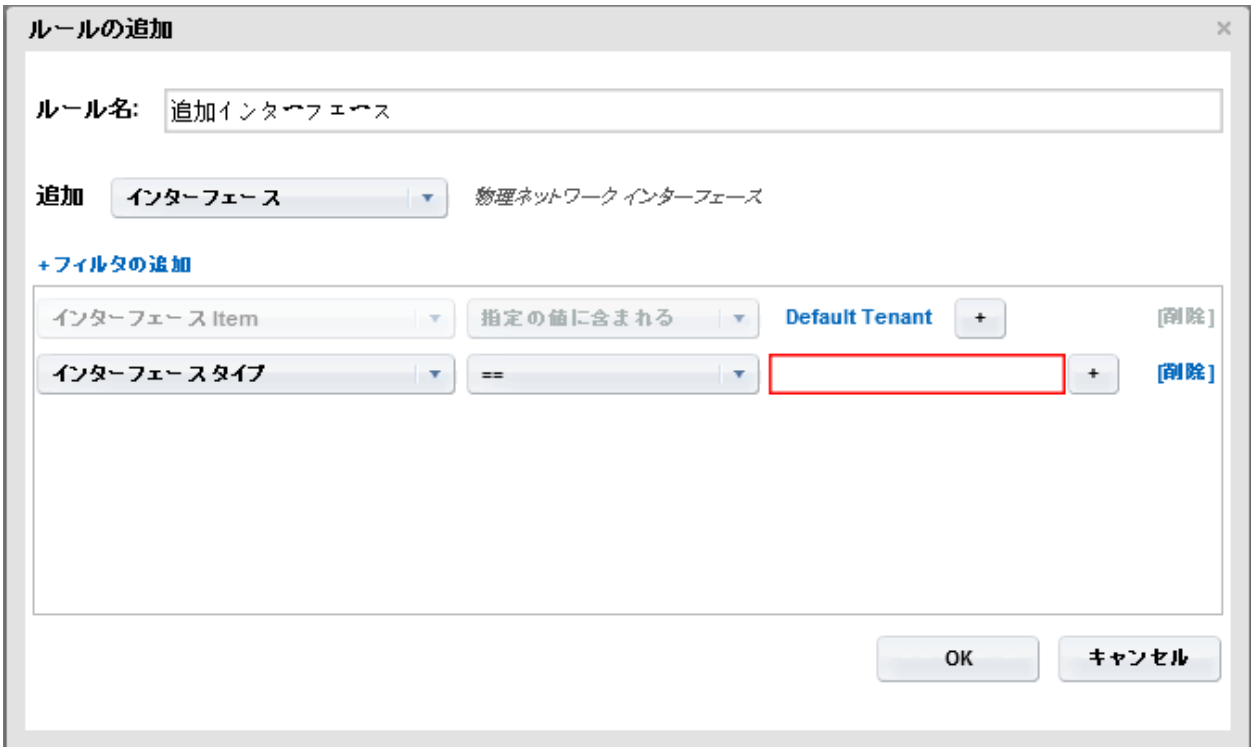
6. ［ルール］タブをクリックして、［ルールの追加］をクリックします。

   ［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。

グループ ルールの編集

監視中に管理対象アイテムが検出されると、アイテムはグループ ルールによって自動的にカスタム グループに追加されます ルールを作成したら、それを編集できます。 ルールを編集する場合は、フィルタを変更または削除するか、サブルールを追加します。

以下の手順に従います。

1. 管理用に必要な役割の権限 (P. 118) 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 (P. 90)。

   ツリー構造内に現在のグループが表示されます。
3. グループ ツリーの［すべてのグループ］ノードを展開します。
4. 編集するルールのあるグループを選択します。
5. ［ルール］タブをクリックします。
6. ルール上にマウス ポインタを置きます。

   ルールを編集または削除するオプションが表示されます。
7. ［編集］をクリックします。

   ［ルールの編集］ウィンドウが表示されます。
8. 必要に応じ、既存のフィルタに希望の変更を加えるか、フィルタまたはサブルールを追加するか、フィルタまたはサブルールを削除します。
9. ［OK］をクリックします。
10. ［プレビュー結果］をクリックし、変更したルールによって適切なアイテムがグループに追加されることを確認します。 必要に応じ、再度ルールを編集します。

11. ルールの編集が完了したら、以下のいずれかのオプションをクリックします。

    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、すぐにグループを自動入力します。

サブルールのグループ ルールへの追加

サブルールは、作成したあらゆるグループ ルールに追加できます。 監視中に管理対象アイテムアイテムが検出されると、アイテムはグループ ルールによって自動的にカスタム グループに追加されます。 サブルールは、ルール インテリジェンスを他のアイテムに拡張するか、または元のルール内に、より厳密にフィルタを定義します。

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 (P. 118)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 (P. 90)。

   ツリー構造内に現在のグループが表示されます。
3. 変更したいルールを含むグループを選択します。
4. ［ルール］タブをクリックします。
5. ルールをクリックして展開します。

   ルール定義テキストおよび［サブルールの追加］リンクが表示されます。
6. ［サブルールの追加］をクリックします。

   ［ルールの追加］ウィンドウが表示されます。

   オプションは、元のルールに適用されたオプションと同一です。
7. ドロップダウンから追加するアイテムの［タイプ］を選択して希望のオプションを選択し、必要に応じてフィルタをセットアップし。
8. ［OK］をクリックします。

9. ［プレビュー結果］をクリックし、変更したルールによって適切なアイテムがグループに追加されることを確認します。

   必要に応じ、再度ルールを編集します。

10. ルールの編集が完了したら、以下のいずれかのオプションをクリックします。

    - ［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。

グループ ルールの削除

管理対象アイテムをグループに自動的に追加するために作成したルールは削除できます。グループ ルールを削除すると、ルールを適用するグループに追加されたいずれのアイテムも削除されます。 アイテムはインベントリから削除されませんが、影響を受けるグループの［アイテム］タブでは利用できなくなります。

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 (P. 118)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 (P. 90)。

   ページには、ツリー構造内に現在のグループが表示されます。
3. グループ ツリーで削除するルールのあるグループを選択します。
4. ［ルール］タブをクリックします。
5. ルールの上にマウス カーソルを置きます。

   ［編集］および［削除］のオプションがリンクとして表示されます。
6. ［削除］をクリックします。

   確認ダイアログ ボックスが表示されます。
7. ［削除］をクリックします。

   ルールは、グループに適用されなくなりました。 グループ ルールに一致するすべての管理対象アイテムも、グループから削除されます。

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 (P. 90)。

   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。

グループにサブグループをコピー

カスタム グループを作成すると、管理対象アイテムが含まれるサブグループを追加することで、グループに入力できます。 新規グループを既存グループに追加できます。 新規グループは、階層構造のサブグループになります。 また、システム グループまたはその他のカスタム グループを高レベル グループにコピーし、サブグループを作成することもできます。

グループをコピーする場合は、実際には*グループ参照*を作成します。 グループ参照は変更できませんが、削除できます。 コピーされたグループには、右ペインに追加のタブが表示されます。 このグループのコピーが置かれている場所を参照するには、[参照の削除]タブをクリックします。

元のグループに対して行った変更は、そのグループの参照先にすべて反映されます。グループを削除した場合も、その参照がすべて削除されます。

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。

以下の手順に従います。

1. 管理用に必要な役割の権限 (P. 118) 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 (P. 90)。

   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. グループ ツリーのノードを展開し、コピーするグループを見つけて選択します。 そのグループのすべてのサブグループは、選択内容に自動的に含まれます。
4. 右クリックし、［グループのコピー］を選択します。
5. サブグループを追加する親グループを選択します。
6. 右クリックし、［グループの貼り付け］を選択します。

   既存グループと、そのすべてのサブグループが、選択された親グループにコピーされます。

   読み取り専用のグループ参照であることを示すアイコンが表示されます。 

グループへのサブグループの追加

階層構造を作成するには、以前に作成したカスタム グループ内に新規グループを作成します。また、既存グループを別のグループへの追加して、サブグループにすることもできます。

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。

以下の手順に従います。

1. 管理用に必要な役割の権限 (P. 118) 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 (P. 90)。

   ツリー構造内に現在のグループが表示されます。
3. グループ ツリーのノードを展開し、親グループを見つけて選択します。

4. 右クリックし、［新規グループの追加］を選択します。

   ［グループの追加］ダイアログ ボックスが表示されます。

5. ［既存］タブを選択します。

   グループ ツリーが表示されます。

6. サブグループとして追加するグループに移動し、それを選択します。

   選択したグループのすべてのサブグループが、選択内容に自動的に含まれます。

7. ［選択］をクリックします。

   既存グループと、そのすべてのサブグループが、選択された親グループに追加されます。

（新規関連グループ 1）

グループ参照の削除 (P. 108)

グループの削除

CA Performance Center グローバル管理者は、テナントが所有しているグループを含む、カスタム グループを削除できます。 またテナント管理者は、そのテナント定義に属するカスタム グループを削除できます。 削除されたグループのサブグループも削除されます。

注: システム グループは削除できません。同様に、デフォルト ドメイン グループも削除できません。

次の手順に従ってください:

1. 管理者の役割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 (P. 90)。

   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. グループ ツリーから削除したいグループを選択します。サブグループが含まれているグループを削除するには、削除するグループの最上位レベルを選択します。
4. 右クリックし、［グループの削除］を選択します。

   確認ダイアログ ボックスが表示されます。

5. ［はい］をクリックし、削除を確定します。

   選択したグループと、そのすべてのサブグループが削除されます。

注:「グループ参照の削除 (P. 108)」の手順とは若干異なる手順に従います。グループ参照は別のグループのコピーです。 コピーであることを示すアイコンが表示されます： 

グループ参照の削除

グループ参照は別のグループのコピーです。 コピーであることを示すアイコンが表示されます。  グループ参照を削除するには、元のグループの［参照］タブを使用します。 ［グループ］ツリーのどこかで参照されているグループにはすべて、右ペインに追加タブが表示されます。 そのグループへの参照を表示して削除するには、［参照の削除］タブを使用します。

参照されているグループを削除すると、その参照がすべて削除されます。対照的に、グループ参照を削除する場合は、元のグループは影響されません。

参照であるサブグループを削除しても、元のグループにも、またそのグループが含まれるグループにも影響しません。 サブグループ参照を含むグループを削除するには、グループを削除する前にすべての参照を削除します。そうでないと、参照を削除しようとした場合に問題が発生します。

たとえば、いくつかのオフィスが一か所に統合される場合は、クローズされるオフィスが検索結果に表示されるのを防ぐためにそれらの参照をすべて削除します。 1 つの参照を削除しても、すべての参照を削除するわけではありません。

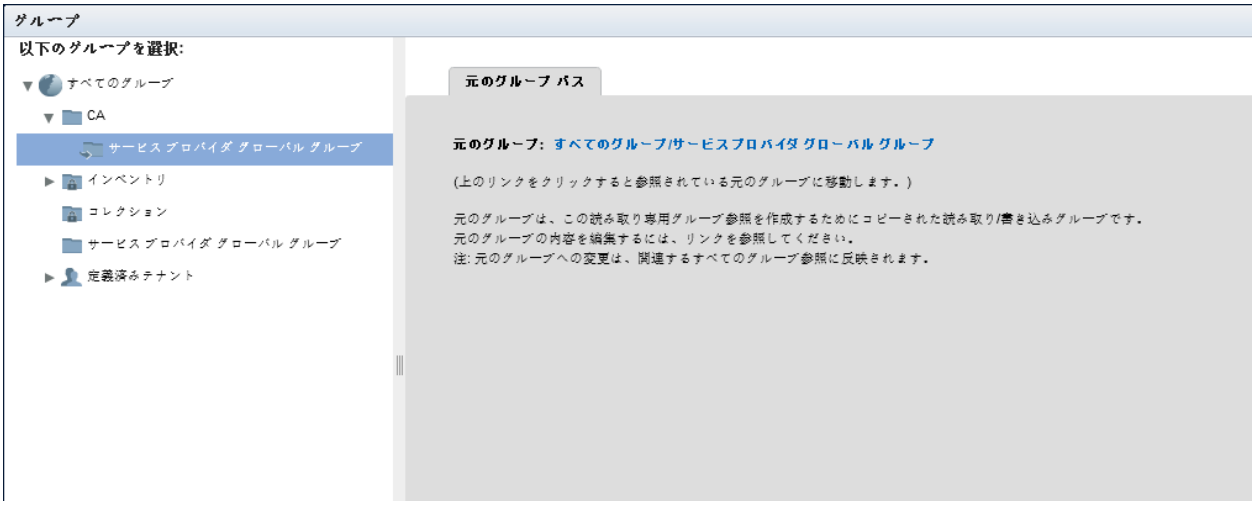
次の手順に従ってください:

1. 管理用に必要な役割の権限 (P. 118)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 (P. 90)。

   ツリー構造内に現在のグループが表示されます。
3. 削除するグループ参照を検索します。

4. グループ参照を選択します。

   右ペインに、コピーされた元のグループへのリンクが表示されます。



5. ［元のグループ］リンクをクリックして、元のグループに移動します。

   元のグループが、右ペインの新しいタブに表示されます。

6. ［参照の削除］タブを選択します。

   このグループへのすべての参照がリスト表示されます。参照のパスは［グループ］ツリーに含まれています。

7. 削除するグループ参照を選択します。

8. ［グループ参照の削除］をクリックします。

   確認ダイアログ ボックスが表示されます。

9. ［OK］をクリックして、削除を確定します。

   選択したグループ参照が削除されます。

第 4 章: 役割の作成と管理

このセクションには、以下のトピックが含まれています。

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。

CA Performance Center は登録済みのデータ ソースと役割を共有しています。ユーザの役割は、データ ソースへのドリルダウン パスに従った場合、ユーザがデータ ソース インターフェースで何を参照および実行できるかを決定します。

CA Performance Center にユーザを追加する場合は、そのユーザ アカウントの役割を選択します。 以下を実行できます 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。環境内でユーザの一意の要件を満たす既存の役割。

新しい役割の権限を含めるように役割を編集できます。 また、それらの役割に割り当てられたユーザが CA Performance Center を使用できないように役割を無効にすることもできます。

事前定義済みまたは出荷時の役割を利用すると、必要なカスタマイズを判断し、新規ユーザを迅速に追加できます。

事前定義済み役割

以下の表では、デフォルトで CA Performance Center に含まれている役割（「ファクトリ」役割）について説明します。

役割名	メニュー	権限
管理者	すべて	データ ソースを管理する一意な役割の権限を含む、すべての権限。 対応する役割の権限が存在しない機能へもアクセスできます。 たとえば、この役割を持つユーザのみが、テナント、IP ドメイン、SNMP プロファイル、および共有カスタム グループを作成できます。 **注**: この役割はグローバル管理者です。 SNMP セキュリティ データをクリア テキストで表示する役割権限のみ変更できます。
テナント管理者	すべて	この役割は、Data Aggregator データ ソースのみをサポートします。 一意の「テナントの管理」役割の権限を含む、すべての権限。 ［デフォルト テナント］ワークスペースの一部であるグループへのアクセスは含まれていません。 デフォルト ドメインへのアクセス権はありません。

役割名	メニュー	権限
デザイナ	すべて	■ メニューの管理 ■ 役割の管理 ■ 共有ダッシュボードの管理 ■ ダッシュボードの作成 ■ ビューへのドリル イン ■ コンテキスト ページの編集 ■ 共有ビューの編集 ■ タイム ゾーンの編集 ■ CSV にエクスポート ■ ビューから URL を生成 ■ ダッシュボードの印刷 ■ ユーザのプロキシ ■ 共有ビューへの変更の保存 ■ 電子メールでレポートを送信 ■ スケジュールに従ってレポートを送信 ■ 通信の表示 ■ ホストの表示 ■ インベントリと検索の表示 ■ プロトコルの表示 ■ ToS の表示

役割名	メニュー	権限
IT アーキテクト	すべて	■ 共有ダッシュボードの管理 ■ ダッシュボードの作成 ■ 通知の作成 ■ データ ソースへのドリル イン ■ ビューへのドリル イン ■ 共有ビューの編集 ■ タイム ゾーンの編集 ■ CSV にエクスポート ■ ビューから URL を生成 ■ ダッシュボードの印刷 ■ 共有ビューへの変更の保存 ■ 電子メールでレポートを送信 ■ スケジュールに従ってレポートを送信 ■ データを表示するためのすべての権限。 すべてのリストについては、デザイナの役割を参照してください。
IT ディレクタ	すべて	■ 共有ダッシュボードの管理 ■ ダッシュボードの作成 ■ ビューへのドリル イン ■ タイム ゾーンの編集 ■ CSV にエクスポート ■ ビューから URL を生成 ■ ダッシュボードの印刷 ■ 電子メールでレポートを送信 ■ スケジュールに従ってレポートを送信 ■ データを表示するためのすべての権限。 すべてのリストについては、デザイナの役割を参照してください。

役割名	メニュー	権限
IT エンジニア	マイ ダッシュボード エンジニアリング 操作の表示 アプリケーション	■ 共有ダッシュボードの管理 ■ ダッシュボードの作成 ■ ビューへのドリル イン ■ 共有ビューの編集 ■ タイム ゾーンの編集 ■ ビューから URL を生成 ■ ダッシュボードの印刷 ■ 共有ビューへの変更の保存 ■ 電子メールでレポートを送信 ■ データを表示するためのすべての権限。 すべてのリストについては、デザイナの役割を参照してください。
IT マネージャ	マイ ダッシュボード 操作の表示 キャパシティ計画 管理 アプリケーション	■ 共有ダッシュボードの管理 ■ ダッシュボードの作成 ■ 通知の作成 ■ ビューへのドリル イン ■ 共有ビューの編集 ■ タイム ゾーンの編集 ■ ビューから URL を生成 ■ ダッシュボードの印刷 ■ 共有ビューへの変更の保存 ■ 電子メールでレポートを送信 ■ スケジュールに従ってレポートを送信 ■ データを表示するためのすべての権限。 すべてのリストについては、デザイナの役割を参照してください。

役割名	メニュー	権限
IT オペレータ	インフラストラクチャ ヘルス 操作の表示	■ 通知の作成 ■ ビューへのドリル イン ■ タイム ゾーンの編集 ■ ダッシュボードの印刷 ■ 電子メールでレポートを送信 ■ データを表示するためのすべての権限。 すべてのリストについては、デザイナの役割を参照してください。
運用センター管理者	マイ ダッシュボード 操作の表示	■ ダッシュボードの作成 ■ 通知の作成 ■ ビューへのドリル イン ■ 共有ビューの編集 ■ タイム ゾーンの編集 ■ CSV にエクスポート ■ ビューから URL を生成 ■ ダッシュボードの印刷 ■ ユーザのプロキシ ■ 共有ビューへの変更の保存 ■ 電子メールでレポートを送信 ■ スケジュールに従ってレポートを送信 ■ データを表示するためのすべての権限。 すべてのリストについては、デザイナの役割を参照してください。

役割名	メニュー	権限
IT の VP	マイ ダッシュボード キャパシティ計画 管理	■ ダッシュボードの作成 ■ ビューへのドリル イン ■ 共有ビューの編集 ■ タイム ゾーンの編集 ■ CSV にエクスポート ■ ダッシュボードの印刷 ■ 共有ビューへの変更の保存 ■ 電子メールでレポートを送信 ■ データを表示するためのすべての権限。 すべてのリストについては、デザイナの役割を参照してください。

注: 事前定義済みの管理者アカウント「admin」には、管理者の役割があります。 事前定義済みのユーザ アカウント「user」には、IT オペレータの役割があります。 2 つの事前定義済みユーザ アカウント、admin および user は、名前とパスワードなどを変更できます。「管理者」の役割で可能な変更は限られています。セキュリティを強化するために、デフォルト パスワードを変更することを推奨します。

詳細情報:

役割の権限 (P. 118)
現在の役割の表示 (P. 128)

役割の権限

各役割に割り当てられた権限によって、ダッシュボードとメニューへのユーザ アクセスが決定します。 役割の権限によって、ユーザに表示されるビュー タイプと、ユーザがデータをエクスポートし、設定をカスタマイズできるかどうかが決定します。

管理者は、それらの役割を編集することで、ユーザに追加の権限を許可できます。 ［役割の編集］ダイアログ ボックスに、役割に現在割り当てている役割の権限がリスト表示されます。 さらに、［ユーザの管理］ページでは、各ユーザに割り当てられた役割が表示されます。

注: 管理の役割の権限はプライマリ管理者アカウントから削除しないでください。 コンソールへの管理アクセス権は必須です。

以下のリストでは、CA Performance Center 機能で利用可能なアクセス権限について説明します。

管理の役割の権限

以下の役割の権限があると、ユーザが管理機能アクセスすることが可能になります。セキュリティを強化するには、これらの役割の権限を持つユーザ数を制限します。

データ ソースの管理

新しいデータ ソースの登録、データ ソース接続のテスト、データ ソース ステータスの表示、データ ソース パラメータの変更、およびデータ ソースの削除が可能です。 また、データ ソース ログの表示が可能です。

グループの管理

完全な管理者権限を持たないユーザに、［グループ］ツリーの特定のブランチの管理権限を与えます。 この役割の権限では、ユーザは指定されたブランチでのみグループを作成、変更、削除できます。 「管理者」の役割および「テナント管理者」の役割にはデフォルトでこの役割の権限が割り当てられ、管理者は［すべてのグループ］を、テナント管理者は［テナント］ルート グループを管理できます。

管理者および管理対象ブランチ内のグループの所有者（作成者）のみが、そのブランチ内のグループを削除できます。 管理対象グループが別のグループ (すなわちサブグループ) の子である場合、その親グループを削除すると、管理対象グループも削除されます。 所有者のユーザアカウントを削除しても、管理対象グループは削除されません。

注:

- この役割の権限は、［グループ］ツリーに対する*完全*な管理者権限ではなく、特定のブランチに限定された管理者権限を必要とするユーザに割り当ててください。 組織によっては、このユーザは「パワー ユーザ」または「スーパー ユーザ」になります。
- ［マイ カスタム グループ］機能は［グループの管理］の役割の権限とは異なり、管理者によりアクセスを許可されたグループを編成するためのユーザ用ツールにすぎません。 ［マイ カスタム グループ］は、［グループ］ツリーの特定のブランチに対する管理者権限を与えません。

メニューの管理

メニューの作成、編集、および削除が可能です。 この役割の権限はメニューに新しいダッシュボードを割り当てるために必要となります。 ユーザ アカウントにメニューを割り当てるには、「役割の管理」の役割の権限が必要です。

役割の管理

ユーザ アカウントの役割を作成、編集、および削除できます。 役割を編集することにより、ユーザ アカウントに新しいメニューを割り当てることができます。

共有ダッシュボードの管理

ユーザ独自のダッシュボードと他のユーザのダッシュボードを管理できます。既存のダッシュボード ページを編集して変更内容を保存すれば、他のユーザがその内容を確認できます。

- ダッシュボードを作成するには、「ダッシュボードの作成」の役割の権限が必要です。
- メニューにダッシュボードを割り当てるには、「メニューの管理」の役割の権限が必要です。

テナントの管理

ユーザ ウィザードで選択されているテナントに対するユーザ管理者権限を付与します。この役割を持ったユーザには、デフォルト テナントへのアクセスは制限されていますが、テナントを管理する権限があります。この役割はマルチテナント環境でのみ使用されます。テナント管理には、以下を管理する機能が含まれます。

- ユーザ
- メニュー
- ダッシュボード
- ビュー

ユーザの管理

ユーザ アカウントを作成、編集、および削除できます。 ユーザ アカウントに新しい役割を割り当てることができます。

ダッシュボードの作成

新しいダッシュボードを作成して、それらをビューに表示できます。他のユーザはこれらのダッシュボードを参照できません。他のユーザ用のダッシュボードを作成するには、「共有ダッシュボードの管理」の役割権限が必要です。

通知の作成

［管理］-［通知］メニューから［通知の作成/編集］ウィザードを使用して、電子メール通知を設定します。通知は、一部のデータ ソースではサポートされていません。 CA Performance Center Readme ファイルには、最新のリストが含まれています。

オンデマンド レポート テンプレートの作成

ユーザはオン デマンドのレポート テンプレートを作成、編集、削除できます。 この役割権限は、［オンデマンド レポート テンプレートの実行］権限と常に一緒に割り当てられます。ユーザはオンデマンド レポート テンプレートをユーザ レベルで保存できます。その場合、ユーザのみがテンプレートを表示できます。また、オンデマンド レポート テンプレートをテナント レベルで保存することもできます。その場合、テナント内の全ユーザがテンプレートを表示できます。

データ ソースの削除

管理者の役割を持つユーザがデータ ソースを削除（登録解除）できるようにします。デフォルトではどのユーザや役割にも割り当てられていません。 管理者の役割にのみ割り当てることができます。

ビューから DA 管理ページへのドリル イン

ユーザが Data Aggregator 関連ページから Data Aggregator 管理者ページに直接アクセスすることができます。 この役割権限が正しく動作するには、ユーザは［データ ソースの管理］権限も有することが必要です。 Data Aggregator 管理者ページにアクセスする機能は、Data Aggregator のデバイス、インターフェース、およびコンポーネントに対するビューに制限されています。Data Aggregator インターフェースまたはコンポーネントを選択すると、ギヤ  ボタンおよび［デバイス管理］をクリックした場合に表示される関連親デバイス用の管理者ページを開きます。

コンテキスト ページの編集

コンテキスト ページ上のタブを編集、削除、追加、または並べ替えできます。 *コンテキスト*とは、デバイス、ルータ、スイッチ、またはインターフェースなどの管理対象アイテムです。コンテキスト ページはコンテキストが固定されたダッシュボードのようなものです。デフォルトでこの権限があるのは、デザイナと管理者の役割のみです。

ユーザのプロキシ

選択されたユーザとしてログインし、ユーザ アカウント設定を表示して確認できます。

共有ビューへの変更の保存

共有ページ上のビューに対する編集を保存できます。 これらのビューを参照可能な他のユーザは、「すべてのユーザ用のデフォルト」として適用されている変更を参照できます。 ログアウト後も残るように、変更内容をユーザ アカウントに保存することもできます。

SNMP クリア テキスト

ユーザが SNMP プロファイルをトラブルシュートしてセキュリティ情報を参照できるようにします。

ダッシュボードおよびビュー アクセス用の役割の権限

以下の役割権限を持つユーザはレポート機能にアクセスできます。 ほとんどのユーザ アカウントにはこれらの権限が必要です。

データ ソースへのドリル イン

ドリル ダウンしながらデータ ソース インターフェースに移動して、選択されたアイテムの詳細データを参照できます。

ビューへのドリル イン

CA Performance Center コンテキスト ビューにドリル インして、選択されたアイテムの詳細データを参照できます。「コンテキスト ページの編集」の役割権限を有効にする必要があります。

共有ビューの編集

共有ページ上のビューを自分用に編集できます。これらのビューを参照可能な他のユーザは、この変更内容を参照することはできません。変更内容は、現在のログイン セッションに適用することも、現在のユーザ アカウントに保存することもできます。

タイム ゾーンの編集

ダッシュボードに表示されたデータに関する独自のタイム ゾーン設定を編集できます。

通信の表示

特定のクライアント通信を参照できます。

ホストの表示

特定のクライアント ホスト情報を参照できます。

アイテム表示名または名前エイリアスを表示

アイテムの表示名またはエイリアスを参照できます。

注: この役割の権限を与えられるユーザは、［マイ設定］、［表示設定］メニュー アイテム内のダッシュボードおよびビューにどの名前を表示するかを選択できます。

アイテム名エイリアスのみ表示

アイテムのエイリアスのみを参照できます。

インベントリと検索の表示

ユーザが［インベントリ］タブと［検索］フィールドにアクセスしてアイテムを検索できるかどうかを決定します。

プロトコルの表示

使用可能なプロトコル情報を参照できます。

ToS の表示

適用可能なビュー内のサービスのタイプ情報を参照できます。

エクスポートおよび印刷するための役割の権限

以下の役割の権限がダッシュボード データをさまざまな形式でエクスポートできるようにします。

CSV にエクスポート

選択されたビューの内容をカンマ区切り値（CSV）形式でファイルにエクスポートできます。

ビューから URL を生成

URL を使用してビューを外部と共有できます。

ダッシュボードの印刷

現在のダッシュボード ページを PDF としてエクスポートし、選択されたプリンタに送信できます。

電子メールでレポートを送信

コンソールから、ダッシュボードをレポートとしてエクスポートし、電子メール メッセージで他のユーザに送信できます。

スケジュールに従ってレポートを送信

定期的に、ダッシュボードをレポートとしてエクスポートし、自動的に電子メールで送信するスケジュールをセットアップできます。

注: この権限には「電子メールでレポートを送信」の役割の権限も必要です。

オンデマンド レポート テンプレートの実行

ユーザがオン デマンドのレポート テンプレートを実行できます。 この役割権限は、［オンデマンド レポートテンプレートの作成］権限と常に一緒に与えられます。 ただし、［オンデマンド レポートテンプレートの作成］権限が取り消されても、ユーザはそれらのオン デマンドのダッシュボードを編集および削除する機能を失いません。［オンデマンド テンプレートの作成］権限がないものの［オンデマンド レポートテンプレートの作成］権限を有するユーザは、テナント レベルでオンデマンド レポート テンプレートを実行できます。

より高い解像度でのダッシュボードの実行

ダッシュボードを表示する場合にユーザはより高い解像度を選択できます。 デフォルトでは、CA Performance Center 内の役割にこの役割の権限は与えられません。 この役割権限を持つユーザは、より長い時間範囲にわたってレポートを作成する場合に通常許容される値よりも高い値に解像度を設定して保存することができます。 ユーザがより高い解像度をテナント レベルで保存した場合、その解像度はこの役割権限を持つユーザにしか表示されません。

注: より高い解像度が設定されても、一部のチャートは NULL データに対して引き続きその他の解像度で表示される場合があります。

また、役割の権限にはメニューも含まれます。 役割の権限を編集することで、選択したカスタムおよび事前定義済みメニューへのアクセスを許可できます。

詳細:

役割の追加 (P. 129)
データ ソース固有の役割の権限 (P. 124)
事前定義済み役割 (P. 112)

データ ソース固有の役割の権限

CA Performance Center に登録された各データ ソースには、そのインターフェース内の機能およびデータに対する一意の権限を持つ独自の役割セットがあります。管理者は、CA Performance Center からそのデータ ソース内の役割の権限を割り当てることができます。ユーザが CA Performance Center データ ビューから特定のデータ ソースのドリル ダウン パスに進む場合に、これらのデータ ソース権限が適用されます。 ただし、このようにして付与された権限はいずれも、データ ソースのインスタンスに固有です。 たとえば、複数の CA Application Delivery Analysis データ ソースが登録される場合、各管理コンソールの権限は別々に管理されます。

たとえば、管理者は、CA Network Flow Analysis データ ソースでレポートを生成する権限を許可できますが、CA Performance Center のダッシュボードを編集する権限の保留もできます。 各データ ソースの「*管理者ガイド*」には、役割の権限の適用方法に関する詳細情報が提供されています。

各データ ソースの管理者は、そのデータ ソース内にユーザ アカウントを作成し、機能にアクセスするユーザの役割の権限を許可できます。 登録した後、それらの権限は CA Performance Center で同期され、［役割の編集］ページに表示されます。

注: 個々のデータ ソースに対する役割の権限と CA Performance Center 機能へのアクセス権限は異なるものですが、同じ名前が付けられることがよくあります。

以下のトピックでは各データ ソースのユーザが利用可能な権限の概要について説明します。

Data Aggregator 役割の権限

役割権限の名前	説明
ビューから DA 管理ページへのドリル イン	Data Aggregator ビューから監視対象デバイスの［管理］ページにドリルダウンして、データが表示されないビューのトラブルシューティングを行います。
テナントの管理	テナント（ユーザ アカウントを含む）を管理し、Data Aggregator 用のデバイスを検出および削除します。
DA しきい値プロファイルの管理	Data Aggregator しきい値プロファイルを管理します。管理の内容は、しきい値プロファイルの作成、任意のしきい値プロファイルの編集、すべてのしきい値プロファイルの所有権の変更などです。
DA しきい値プロファイルの作成	イベント プロファイルを作成および管理できる Data Aggregator しきい値プロファイルを作成します。 イベント プロファイルにはイベント ルールが含まれ、グループと関連付けられます。 これらのプロファイルで生成されるイベントに関するレポートを作成できます。 この役割では、しきい値プロファイルの作成、独自プロファイルの編集、すべてのしきい値プロファイルの表示が可能です。

CA Network Flow Analysis 役割の権限

以下のテーブルでは CA Network Flow Analysis （以前の名称： CA ReporterAnalyzer）コンソールに適用可能な役割の権限の概要について説明します。

役割権限の名前	説明
ToS の表示	サービス タイプのデータの表示
レポートの管理	レポートの作成、変更、削除、実行
レポートの実行	定義されたレポートの実行
通信の表示	通信データの表示
ホストの表示	ホスト データの表示
プロトコルの表示	プロトコル データの表示

CA Application Delivery Analysis 役割の権限

以下のテーブルでは CA Application Delivery Analysis （以前の名称： NetQoS SuperAgent）管理コンソールに適用可能な役割の権限の概要について説明します。

役割権限の名前	説明
エンジニアリング	［エンジニアリング］セクションに移動し、エンジニアリング レポートを作成します。
操作	［オペレーション］セクションに移動し、オペレーション レポートを作成します。
管理	［管理］セクションに移動し、管理レポートを作成します。
インシデント	［インシデント］セクションに移動し、インシデント レポートを表示します。
調査	［調査］を起動し、［調査］のデータにドリル ダウンします。

役割の権限は、CA Application Delivery Analysis ユーザに以下の許可を与えません。

- CA Application Delivery Analysis 管理コンソール の［環境管理］ページにアクセスする権限。

  ユーザに［環境管理］ページへのアクセスを許可するには、CA Application Delivery Analysis データ ソースに対する［管理者］製品権限または［パワー ユーザ］製品権限を付与します。

- CA Application Delivery Analysis 管理コンソール 内の実際のレポート データへのアクセス。

  ユーザがレポート データを参照できるようにするには、適切なグループをユーザに割り当てます。

CA Unified Communications Monitor 役割の権限

以下のテーブルでは、CA Unified Communications Monitor 管理コンソールに適用可能な役割の権限の概要について説明します。

役割の権限	説明
コール詳細	CSV ファイルへのコール詳細のエクスポート
コールのパフォーマンス	コールのパフォーマンス レポートへのアクセス
コール品質およびボリューム	コール品質およびボリューム レポートへのアクセス
コール監視	コール監視レポートへのアクセス
コール監視セットアップ	選択された電話でのコール監視のセットアップと起動
コレクタ インシデント	コレクタ インシデント レポートへのアクセス
インシデント	インシデント レポートへのアクセス
調査	調査レポートへのアクセス
調査の起動	調査の起動、生成されたデータの表示
電話詳細	電話詳細レポートへのアクセス
品質	品質レポートへのアクセス
トランク グループ	トランク グループ レポートへのアクセス

役割の権限	説明
音声インターフェース	音声インターフェース レポートへのアクセス
中間デバイス	中間デバイスおよび中間レグ レポートへのアクセス

現在の役割の表示

CA Performance Center には、カスタム ユーザ アカウントに割り当てることができる、事前定義済み（「ファクトリ」）役割 1 セットが含まれます。［役割の管理］ページでは、これらの役割に関するサマリ情報にアクセスできます。 このページには、作成するすべてのカスタム役割もリスト表示されます。

以下の手順に従います。

1. 管理の役割の権限 (P. 118)を持つユーザとしてログインします。
2. ［管理者］-［ユーザ設定］を選択し、［役割］をクリックします。

   ［役割の管理］ページでは、ユーザ アカウントへの割り当てに利用可能な、現在定義されている役割のリストが表示されます。

   注: テナント管理者は自分のテナントに関連付けられたアイテムしか参照できません。

   テーブルには、各役割に関する以下の情報が表示されます。

   役割名

   役割の名前です。 ファクトリ役割の名前は、共通の情報技術ジョブ カテゴリに基づいています。

   説明

   特定の役割に関連付けられるユーザの職務権限を示します。

   ステータス

   この役割のステータス（有効または無効のいずれか）を表示します。 役割はセキュリティ上の理由で無効にできます。

   ユーザ

   現在この役割割り当てがあるユーザ アカウントの数を表示します。

   このページ上でいずれかのアクションを実行するには、役割を選択し、次にボタンをクリックします。 割り当てられたメニューおよび役割の権限のリストを表示するには、役割を編集します。

詳細:

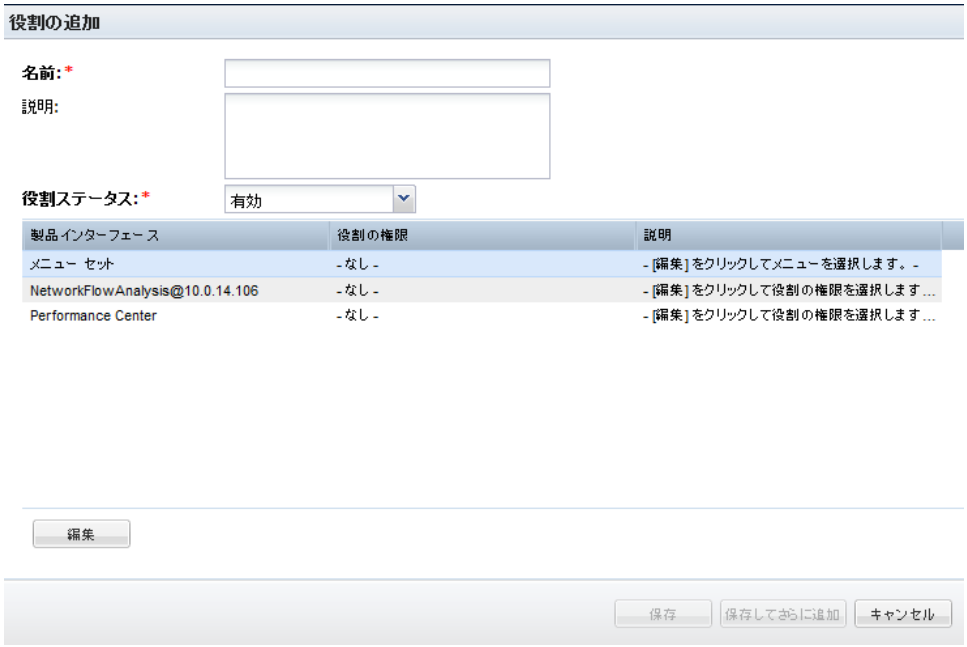
役割の追加 (P. 129)
事前定義済み役割 (P. 112)
役割の編集 (P. 132)

役割の追加

CA Performance Center で提供される事前定義済みユーザ役割 (P. 112)がユーザ要件に適合しない場合は、カスタム ユーザ役割を追加できます。理想的には、それぞれの製品オペレータが責務を実行するために必要とする役割を作成します。

カスタム役割は、カスタム グループのシステムで最適に動作します。 カスタム グループを使用すると、機密データへのアクセスを制限しながら、ダッシュボードおよび製品機能へのアクセスを正確に与えることができます。 データを構成するために作成したグループは、ユーザ アカウント権限をセットアップする場合に「権限グループ」として利用できます。

新しい役割には、役割の権限を追加するまでは権限がありません。



注: 役割を作成し終わったら、それを別の手順でユーザ アカウントに割り当てます。 役割は、ユーザ アカウントに割り当てられるまでは動作しません。「ユーザの管理」および「役割の管理」の役割の権限を持ったユーザのみが、役割をユーザ アカウントに割り当てることができます。

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 (P. 118)を持つユーザとしてログインします。
2. ［役割の管理］ページに移動します (P. 128)。

   役割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。

   ［役割の追加］ダイアログ ボックスが表示されます。
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

   （オプション）役割を識別します。45 文字までに制限されてます。

   説明

   （オプション）役割に関する説明です。 たとえば、関連付けられたユーザが実行するジョブに関連した義務を指定します。

   役割の有効化

   役割を有効にしてアクティブにします。 この役割を持つユーザに役割の権限によって付与されたアクセス権を与える必要があります。
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。 ［利用可能なメニュー］リスト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。

   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。

   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。

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. ［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。「利用可能な権限」リストに表示された役割の権限は、役割に追加できます。 詳細については、「役割の権限 (P. 118)」を参照してください。

10. 左側のアイテムをクリックして、役割に追加するアイテムを選択します。 右方向矢印ボタンをクリックし、［選択された権限］リストに移動します。

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。

    新しい役割が作成され、［役割リスト］に表示されます。

詳細:

役割の権限 (P. 118)
データ ソース固有の役割の権限 (P. 124)

役割の編集

事前定義済みユーザ役割 (P. 112)を利用することで、オペレータは CA Performance Center の使用を開始することができます。 事前定義された役割を変更したり、新しいルールを作成して、固有の環境や製品オペレータの責任に合わせることができます。

グローバル管理者および必要な役割の権限を持つユーザは、事前定義済みの役割とカスタム役割を変更できます。 テナント管理者は、自身のテナントに関連付けられた役割に対してのみアクセス権があります。

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 (P. 118) を持つユーザとしてログインします。
2. ［役割の管理］ページに移動します (P. 128)。

   役割の現在のリストがページに表示されます。
3. （オプション）変更する役割の現在の使用を確認するには、以下の手順を行います。
   a. 役割を選択します。
   b. ［ユーザ］をクリックして［ユーザ リスト］ページを開きます。選択した役割に割り当てられたユーザのみがフィルタ表示されます。
   c. ［役割］をクリックして、［役割の管理］ページに戻ります。
4. 編集する役割を選択します。
5. ［編集］をクリックします。

   ［役割の編集］ダイアログ ボックスが表示されます。
6. 必要に応じて、役割設定を変更 (P. 129) します。

   テーブルに、役割用に選択された役割の権限がリスト表示されます。
7. ［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。 詳細については、「役割の権限 (P. 118)」を参照してください。

8. 左側のアイテムから、役割に追加するものを選択します。 右方向矢印をクリックして、［利用可能な権限］リストから［選択された権限］リストにアイテムを移動します。

   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。

9. （オプション）この役割に新しいメニューを追加するには、以下の手順に従います。

   a. ［メニュー セット］を選択し、［編集］をクリックします。

   b. ［利用可能な権限］リスト内の新しいメニューを選択します。

   c. 右方向矢印ボタンをクリックし、［選択された権限］リストに移動します。

   d. （オプション）選択したメニューのリスト内でメニュー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。

   e. メニューを追加し終わったら、［OK］をクリックします。

   注: 1 つの役割に対して、［マイ ダッシュボード］メニューを含む、最大 6 つのメニューを割り当てることができます。

10. ［保存］をクリックします。

    役割への変更が保存されます。

詳細

役割の追加 (P. 129)
役割の権限 (P. 118)

役割の削除

作成したあらゆるカスタムの役割は削除できます。 役割を削除するには、どのユーザ アカウントにも役割が割り当てられていないことが必要です。

注: 管理者の役割は、削除または無効にできません。その他の役割は、ユーザに割り当てられていなければ削除できます。

以下の手順に従います。

1. 管理用に必要な役割の権限 (P. 118) を持つユーザとしてログインします。

2. ［管理者］-［ユーザ設定］を選択し、［役割］をクリックします。

   役割リスト ページが表示されます。

3. 削除する役割の現在の使用状況を確認するために、テーブル内の［ユーザ］列を確認します。
4. ユーザ アカウントがこの役割を使用している場合は、以下の手順に従って役割の割り当てを削除します。
   a. 役割を選択します。
   b. ［ユーザ］をクリックします。

      ［ユーザ リスト］ページが開き、選択された役割に割り当てられたユーザのみがフィルタされて表示されます。

   c. ユーザ アカウントを選択し、［編集］をクリックします。
   d. ［役割］リストから別の役割を選択します。
   e. ユーザ アカウントへの変更を保存します。
   f. ［役割リスト］ページに戻ります。
5. 削除する役割を選択します。
6. ［削除］をクリックします。

   ［役割の削除］ページが表示されます。

7. ［削除］をクリックして、削除を確定します。

   役割がリストから削除されます。

製品権限

ユーザ アカウント役割は、管理など CA Performance Center 機能へのユーザ アクセスを許可または制限するために使用します。

ただし、各データ ソースを製品アクセスに個別に割り当てます。 管理機能を持ったユーザを作成するには、データ ソースに「製品権限」設定を適用します。たとえば、管理アクセス権限のない CA Performance Center のユーザを作成できます。そのユーザは、CA Network Flow Analysis の特定のインスタンスに対して管理者製品権限を持つことができます。 そのユーザは、CA Network Flow Analysis 管理対象アイテムへのドリル ダウン パスに進んだ場合に、そのデータ ソースに対して完全な管理者権限があります。

以下のタイプの製品権限は、データ ソースで利用可能で、CA Performance Center に同期できます。

管理者

SNMP プロファイルおよび他の設定の作成および編集を含め、すべての機能を実行します。

パワー ユーザ

メニューとダッシュボードを作成します。 役割を作成して編集することもできます。

ユーザ

管理者またはパワー ユーザによって指定されたメニューとダッシュボードを表示します。

なし

データ ソースにアクセス権がありません。 この設定は、ユーザが CA Performance Center 内のビューからドリル ダウン パスを使用してデータ ソースのユーザ インターフェースに移動できないようにします。 デフォルトでは、すべてのユーザに、すべてのデータ ソースに対してこの製品権限が設定されています。

ユーザが特定のデータ ソースへアクセスすることを拒否しながら、その他のデータ ソースへのアクセス権を与えることができます。

CA Performance Center 管理者は、適切な役割の権限を選択することで、ユーザのアクセス レベルをカスタマイズできます。詳細については、「役割の権限 (P. 118)」を参照してください。

役割の権限設定で製品権限設定を調整します。 ユーザがデータ ソースへのドリル ダウン パスに進むには、そのデータ ソースの適切な役割の権限および製品権限が必要です。

事前定義済み管理者アカウント「管理者」には、登録済みのあらゆるデータ ソース用の管理者権限があります。 事前定義済みユーザ アカウント「ユーザ」には、それらのデータ ソース用の限られた（ユーザ レベルの）権限があります。

データ ソースの製品権限

CA Performance Center に登録された各データ ソースには、そのインターフェース内で固有の権限を持つ独自の製品権限があります。 管理者は、CA Performance Center を通じてデータ ソースに製品権限を割り当てることができます。 CA Performance Center のデータ ビューから特定のデータ ソースへのドリル ダウン パスを進む場合に、データ ソース製品権限が適用されます。 ただし、このようにして付与されたすべての権限は、データ ソースのインスタンスに固有です。 たとえば、複数の CA Application Delivery Analysis データ ソースが登録される場合、各管理コンソールの製品権限は別々に管理されます。

デフォルトの管理者アカウント admin は、製品権限の変更を防ぐためにロックされます。 このアカウントは、すべての登録済みデータ ソースで管理者権限を得るために必要です。 管理者アカウントを含むアカウントのグループを選択すると、選択されたいずれのアカウントの製品権限も編集できません。

CA Application Delivery Analysis の製品権限

以下のリストで、CA Application Delivery Analysis （以前の名称： CA SuperAgent）管理コンソールに適用できる製品権限の概要を説明します。

管理コンソール にログインするには、CA Application Delivery Analysis データ ソースに対する製品権限が必要です。 製品権限は、［環境管理］ページへのアクセスも指定します。

ユーザ

［環境管理］ページ以外の、管理コンソール のすべてのページへのアクセスが許可されます。

管理者

［環境管理］ページを含め、管理コンソール のすべてのページへのアクセスが許可されます。

パワー ユーザ

ユーザ レベルの製品権限、および［表示項目］メニューから［環境管理］ページの［SNMP プロファイル］、［ネットワーク デバイス］、および［デバイス グループ］へのアクセスが許可されます。

ヒント： ユーザが 管理コンソール ユーザ インターフェースにログインできない場合は、CA Application Delivery Analysis データ ソース上の製品権限を与えられているかを確認します。

CA Network Flow Analysis の製品権限

NFA コンソールにログインするには、CA Network Flow Analysis データ ソースの製品権限が必要です。 また、ユーザが［環境管理］ページにアクセスして特定の機能を実行できるかどうかは、製品権限によって決まります。

管理者

NFA コンソール内の［環境管理］ページおよびすべての機能にアクセスできます。これには、ユーザ アカウント、役割、グループ、SNMP プロファイル、およびレポートのスケジュールの作成および管理が含まれます。

パワー ユーザ

ユーザ レベルのアクセス権と、［役割］設定によって付与される追加の権限が与えられます。 CA Network Flow Analysis では、パワー ユーザ権限は管理者権限と同等です。

ユーザ

［企業の概要］ページの［トップ インターフェース］レポートおよび［インターフェース使用率］レポートにアクセスできます。

適切な権限グループ設定を持つユーザは、以下のレポートにもアクセスできます。

- ［企業の概要］ページの［トップ ホスト］および［トップ プロトコル］レポート（「すべてのグループ」へのアクセス権限も持っている場合）
- ユーザがアクセス可能なインターフェース用のインターフェース ページ レポート
- ［カスタム レポート］、［フロー監視］、および［分析］ページの既存のレポート
- 管理者が「ユーザ」役割に割り当てたメニュー

［役割］と［権限グループ］の設定は、ユーザが既存レポートの実行、レポートの作成、およびレポートの管理も行うことができるかどうかを決定します。 レポートを作成するには、ユーザは「すべてのグループ」のアクセス権を持っている必要があります。

なし

データ ソースにアクセス権がありません。この製品権限を持つユーザは、NFA コンソールにログインすることも、Performance Center ビューから NFA コンソールにドリルダウンすることもできません。デフォルトでは、すべてのユーザに、すべてのデータ ソースに対してこの製品権限が設定されています。

注: 同じユーザ アカウントに対して、異なるデータ ソースごとに異なる権限を与えることができます。

CA Unified Communications Monitor の製品権限

以下のリストで、CA Unified Communications Monitor 管理コンソールに適用できる製品権限の概要を説明します。

管理者

すべての機能にアクセスできます。以下のすべての管理タスクを含みます： 場所、メディア デバイス、しきい値、Call Watch 定義、インシデント レスポンス、役割、およびユーザ アカウントの作成および編集など。

ユーザ

レポート ページへのアクセス、および管理者によって選択された基本機能を実行できます。 ユーザ権限では、管理機能へアクセスできません。

製品アクセスの管理

各ユーザ アカウントを作成し、製品機能とデータへのアクセスを割り当てます。 特定のユーザの役割の権限を確認するには、以下の方法に従います。 必要に応じて変更することもできます。

以下の手順に従います。

1. 管理用に必要な役割の権限 (P. 118)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. 編集するユーザ アカウントを選択します。

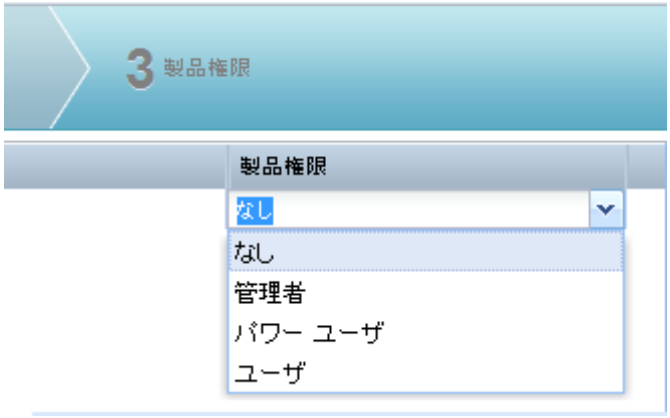
   注: 事前定義の管理者アカウント 'admin' に割り当てられた権限および権利は変更できません。このユーザ アカウントは、すべての登録済みデータ ソースに対する管理者アクセス権を持っている必要があります。

   ［新規ユーザの作成］ウィザードが表示されます。

4. ［製品権限］をクリックします。

   CA Performance Center に登録されたすべてのデータ ソースが［製品権限］ページに表示されます。

5. ［製品権限］列に表示される値をクリックし、ドロップダウン リストを有効にします。



   登録済みのデータ ソースには、それぞれ別のリストがあります。

6. ドロップダウン リストから、以下の製品権限のうちの 1 つを選択します。

管理者

グループ、メニュー、ダッシュボード、役割、およびユーザ アカウントの作成と編集を含む、すべての機能を実行します。

パワー ユーザ

メニューとダッシュボードを作成します。 役割を作成して編集することもできます。

ユーザ

管理者またはパワー ユーザによって指定されたメニューとダッシュボードを表示します。

なし

データ ソースにアクセス権がありません。 この設定は、ユーザが CA Performance Center 内のビューからドリル ダウン パスを使用してデータ ソースのユーザ インターフェースに移動できないようにします。 デフォルトでは、すべてのユーザに、すべてのデータ ソースに対してこの製品権限が設定されています。

7. ［保存］をクリックします。

製品権限への変更は選択したユーザ アカウントに保存されます。

第 5 章: ユーザ アカウントの作成と管理

このセクションには、以下のトピックが含まれています。

ユーザ アカウント

カスタム ユーザ アカウントを使用すれば、オペレータは、日常業務を実行する必要のあるデータ、メニュー、およびダッシュボードを表示できます。管理者の役割の権限を持つオペレータは、ユーザ アカウントの作成、および既存のアカウントの管理ができます。 テナント管理者は、自分のテナント用のユーザ アカウントしか管理できません。

ユーザ アカウントを作成または編集する前に、必要なカスタム グループと役割を作成することをお勧めします。グループおよび役割は、ユーザ アカウントごとに必要なパラメータの一部です。

ユーザ アカウント パラメータ

ユーザ アカウントには以下の関連付けが必要です。

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。

CA Performance Center には、役割の権限が異なる複数の事前定義の役割が用意されています。 必要な役割の権限を持つユーザは、新しい役割を作成して、それらをユーザ アカウントに割り当てることができます。

権限グループ

*権限グループ*は、各ユーザが監視できる管理対象アイテムの範囲で構成されます。 管理者は、各ユーザの責任領域を反映するために、アプリケーション、サーバ、ネットワーク、ルータおよびインターフェースなど管理対象アイテムのカスタム グループを作成できます。カスタム グループは、権限としてユーザ アカウントに割り当てられると、権限グループと呼ばれます。

デフォルトで、新しいユーザ アカウントにはグループが割り当てられません。新しいユーザが管理対象アイテムを表示できるようにするには、そのユーザ アカウントに 1 つ以上のグループを割り当てる必要があります。 事前定義の「admin」アカウントと「user」アカウントはすべてのグループにアクセスできます。作成されたユーザ アカウントの場合は、ユーザが、その責任に基づいて参照可能なグループを制限します。

製品権限

*製品権限*は、ユーザ アカウントに関連付けられた権限セットの一種です。製品権限は、選択したデータ ソースの機能にユーザがアクセスすることを許可し、CA Performance Center の機能には適用されません。

注: 以前のバージョンの NetQoS Performance Center では、製品権限は、カスタム グループを作成できる機能などの製品設定への管理アクセス権を意味していました。現在は、ユーザ アカウントに割り当てられた役割の権限によって、CA Performance Center 内でのこれらの機能へのアクセスが決定されます。

事前定義のユーザ アカウント

CA Performance Center には 2 つの事前定義の（ファクトリ）ユーザ アカウントが用意されています。 これらのアカウントは初期セットアップの実行時に役立ちます。 最低限の役割の権限を持つ LDAP アクセスを割り当てることや、カスタム ユーザ アカウント用のテンプレートとして使用することができます。ただし、これらのアカウントはすべての CA Performance Center インストールに共通しているため、あまり安全ではありません。

重要: ファクトリ ユーザ アカウントはカスタム ユーザ アカウントの代用ではありません。 セキュリティを強化するために、インストール直後にデフォルト パスワードを変更することをお勧めします。

注: 2 つの事前定義のユーザ アカウント（**admin** と **user**）は削除できません。

ファクトリ ユーザ アカウントには以下のパラメータが設定されます。

admin

すべての管理者権限を付与します。

役割： 管理者

特別な役割の権限： すべて（「グローバル管理者」またはデフォルト テナント管理者）

権限グループ： すべてのグループからのデータを表示できます。

デフォルト パスワード： admin

user

データの表示などの標準的なオペレータ権限を指定します。

役割： IT オペレータ

特別な役割の権限： なし

権限グループ： すべてのグループからのデータを表示できます。

デフォルト パスワード： user

ユーザ アカウントのステータスは有効か無効です。 アカウントを無効にすると、ユーザが製品にアクセスできなくなります。

権限グループとユーザ アカウント

事前定義のグループ（またはシステム グループ）を使用すれば、パフォーマンス データの構成と、そのデータへのオペレータ アクセスの割り当てが容易にできます。ただし、より安全でよりよく管理されたシステムは、権限としてユーザに割り当てられるカスタム グループに基づいて構築されます。

*権限グループ*は、各ユーザが監視できる管理対象アイテムの範囲で構成されます。 管理者は、各ユーザの責任領域を反映するために、アプリケーション、サーバ、ネットワーク、ルータおよびインターフェースなど管理対象アイテムのカスタム グループを作成できます。カスタム グループは、権限としてユーザ アカウントに割り当てられると、権限グループと呼ばれます。

ユーザ アカウントの作成時に、複数の権限グループを各ユーザに割り当てることができます。 たとえば、1 つのユーザ アカウントに「North American Core Routers」と「North American Critical Applications」の 2 つの権限グループを割り当てることができます。

注: ベスト プラクティスとして、「コレクション」グループをユーザの権限グループの一部として割り当てないでください。 このグループはレポート用に使用しないでください。

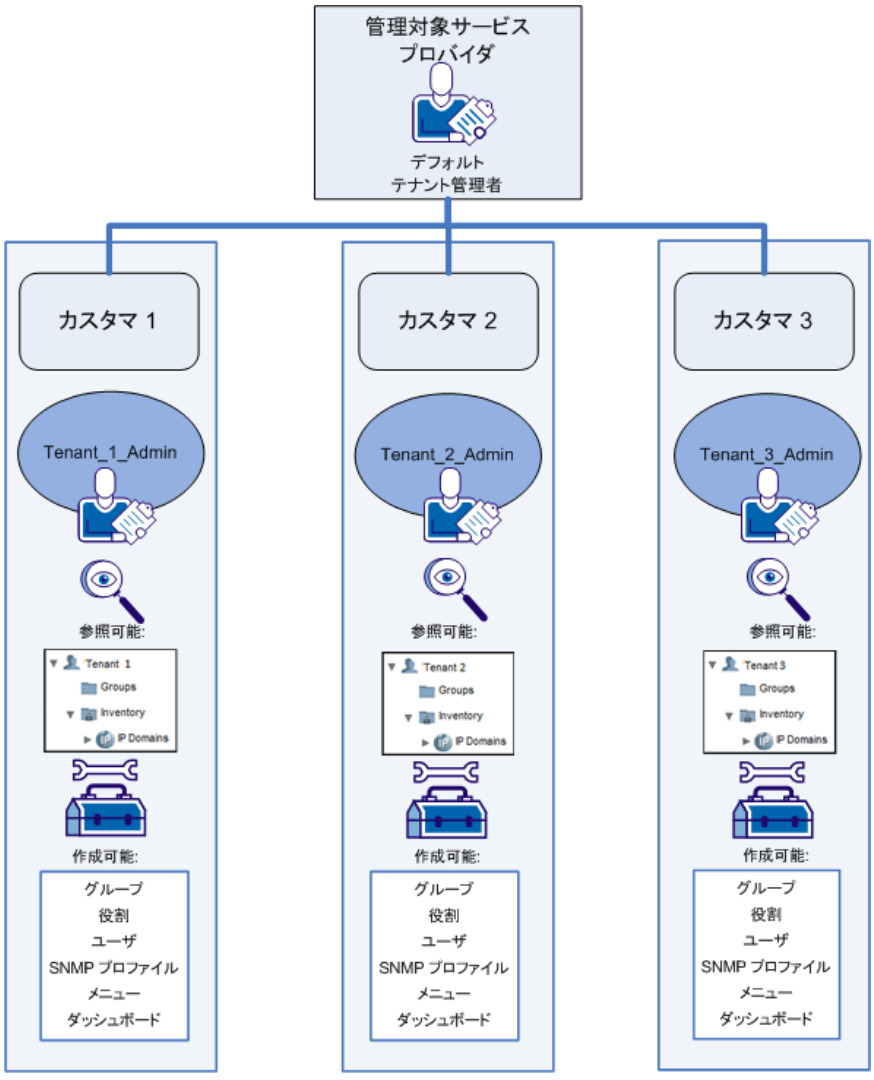
グループ分けや役割構造を作成するための戦略を練るときに CA の技術担当者に相談することをお勧めします。 最適な設定とは、現在の要件を満たすだけでなく、システムの変更に柔軟に対応できる設定です。

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 - 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 - 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. 161)
事前定義済み役割 (P. 112)
テナントの管理 (P. 165)

ユーザ アカウントの作成方法

ユーザ アカウントを作成する前に、管理対象アイテムをカスタム グループ (P. 80)に配置することをお勧めします。各ユーザが表示可能なデータを決定するカスタム グループを「権限グループ」としてユーザ アカウントに割り当てます。 管理対象グループに設定されたユーザ アカウントに対し、［グループ］ツリー内の単一のブランチへの特定の所有権を付与することもできます。

ユーザ アカウントを作成する前に、必要なすべてのカスタム役割を作成します。 通常、事前定義済みの役割 (P. 112)がカスタマイズの出発点となります。

以下のプロセスに従ってユーザ アカウントを作成することをお勧めします。

1. 管理用に必要な役割の権限 (P. 118) を持つユーザとしてログインします。
2. 適切なグループが存在するか確認し、必要な場合はグループを作成 (P. 92) します。

   注: ユーザ アカウント パラメータには、ユーザが *表示*できるすべてのグループのほかに、ユーザが *管理*できるグループ 1 つも含まれます。［グループの管理］の役割権限 (P. 118)は、完全な管理者権限を持たないユーザに［グループ］ツリーの特定のブランチの管理権限を与えます。
3. 適切な役割が存在することを確認するか、必要に応じて、それらを作成します。
4. ユーザを追加して、基本的なユーザ情報 (P. 151) を入力します。
5. 役割を割り当てます。
6. 権限グループを割り当てます。

   注: 新しいユーザ アカウントは、デフォルトではどのグループにもアクセスできません。 権限グループが割り当てられるまで、新規ユーザのダッシュボードにはデータが表示されません。

7. ユーザが［グループ］ツリーの 1 つのブランチでグループを作成および変更できるように、グループの所有権を割り当てます。

   注: この特定のグループ所有権は、［グループの管理］の役割の権限を持ったユーザ アカウントのみに割り当てることができます。

8. 登録されたデータ ソースへのアクセスを可能にするために製品権限を割り当てます。
9. 一時的にユーザ アカウントをプロキシしてテストします。

詳細:

ユーザ アカウント パラメータ (P. 143)
ユーザ アカウントの追加 (P. 151)

ユーザ アカウントのリストの表示

［ユーザの管理］ページでは、ユーザ アカウントの高水準設定を参照できます。 マルチテナント環境では、グローバル管理者は、テナントに明示的に関連付けられていないユーザ アカウントのリストを参照します。テナント管理者は、自分が管理するテナントのユーザ アカウントしか参照できません。

カスタム ユーザ アカウントを作成する前は、2 つのファクトリ ユーザ アカウントしか使用できません。

次の手順に従ってください:

1. 必要な管理の役割の権限（P. 118）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。 このページには、現在のユーザ アカウントのリストが表示されます。

   注: テナント管理者は自分のテナントに関連付けられたアイテムしか参照できません。

このテーブルには、各ユーザ アカウントに関する以下の情報が表示されます。

名前

ユーザ アカウントのログイン名です。

役割

ユーザ アカウントに割り当てられた役割です。

CAPC 権限

CA Performance Center に登録されたデータ ソースへのアクセスのレベルを識別します。

権限

このアカウントに割り当てられた権限グループをリスト表示します。 権限グループはグループ ツリー内にネストされた場所として表示されます。 このユーザが他のユーザから見えないカスタム グループを作成できる場合、「マイ カスタム グループ」が表示されます。

デフォルトは、「/All Groups」です。

ステータス

ユーザ アカウントが有効か、または無効かを示します。

このページ上でいずれかのアクションを実行するには、ページ下部に並んでいるボタンの 1 つをクリックします。

詳細情報:

役割の権限 (P. 118)
事前定義のユーザ アカウント (P. 144)
ユーザ アカウントの追加 (P. 151)
役割 (P. 111)

ユーザ アカウントの追加

CA Performance Center を操作する各ユーザのユーザ アカウントを追加します。 セキュリティ上の理由により、ユーザ アカウントは共有しないでください。

注: ユーザ アカウントを作成する前に、必要な役割およびグループが存在することを確認します。

以下の手順に従います。

1. 管理用に必要な役割の権限 (P. 118) を持つユーザとしてログインします。
2. ［ユーザの管理］ページに移動します (P. 149)。

   ページに、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］ウィザードが表示されます。
4. 次のアカウント 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います。

   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。

   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。

   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。

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。

5. ［アクセス権］をクリックして、ウィザードを進めます。
6. 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］ツリーで目的のグループを展開します。
   - グループまたはサブグループを選択します。
   - 右矢印をクリックし、選択内容を右側の選択済み領域に追加します。
   - 必要に応じて、手順を繰り返します。

注: ベスト プラクティスとして、「コレクション」グループをユーザの権限グループの一部として割り当てないでください。 このグループはレポート用に使用しないでください。

7. （オプション）マイ カスタム グループ機能を有効化するオプションをクリックします。

   このオプションを使用すると、トラブルシューティングや分析のために管理対象アイテムを整理するカスタム グループを作成できます。これらのグループは、［マイ カスタム グループ］ページでのみ利用可能です。 メインの［グループ］ツリーには表示されません。

   デフォルト グループは、自動的に選択されます。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。

8. （オプション）［デフォルト グループ］ドロップダウン リストから別のグループを選択します。

9. ［グループの管理］をクリックして、ウィザードを進めます。［グループの管理］ダイアログ ボックスでは、［グループの管理］の役割の権限を持ったユーザに対して、グループを割り当てることができます。

10. 以下の手順に従って、ユーザが管理するグループを選択します。

    - 左側の［利用可能グループ］ツリーにあるグループを展開します。
    - グループまたはサブグループを選択します。 ユーザは、選択されたグループまたはサブグループの下にグループを作成でき、それら管理対象グループのみを変更および削除できます。 他のユーザが所有しているグループの変更や削除はできません。 ［グループの管理］の役割の権限について、詳しくは「役割の権限 (P. 118)」を参照してください。
    - 右矢印をクリックし、選択した項目を右側の［選択したグループ］に追加します。

    注:

    - ［利用可能なグループ］ツリーは［アクセス権］ダイアログ ボックスで選択されたグループによりフィルタされます。このフィルタは、禁止されているツリーの一部に対する管理者権限をユーザが持つことを阻止します。
    - ［グループの管理］ダイアログ ボックスは、「管理者」の役割を持ったユーザには無効です。

11. ［製品権限］をクリックして、ウィザードを進めます。

12. ［製品］リスト内の各データ ソース製品に対して、以下の製品権限から 1 つ選択します。

    管理者

    グループ、メニュー、ダッシュボード、役割、およびユーザ アカウントの作成と編集を含む、すべての機能を実行します。

    パワー ユーザ

    メニューとダッシュボードを作成します。 役割を作成して編集することもできます。

    ユーザ

    管理者またはパワー ユーザによって指定されたメニューとダッシュボードを表示します。

    なし

    データ ソースにアクセス権がありません。 この設定は、ユーザが CA Performance Center 内のビューからドリル ダウン パスを使用してデータ ソースのユーザ インターフェースに移動できないようにします。 デフォルトでは、すべてのユーザに、すべてのデータ ソースに対してこの製品権限が設定されています。

    注: 同じユーザ アカウントに、別のデータ ソースの別の権限を与えることができます。

13. ［保存］をクリックします。

    新規ユーザ アカウントが［ユーザの管理］ページに表示されます。

詳細:

権限グループとユーザ アカウント (P. 145)
製品権限 (P. 135)
ユーザ アカウントの作成方法 (P. 148)
テナントのクローン作成 (P. 164)

第 6 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

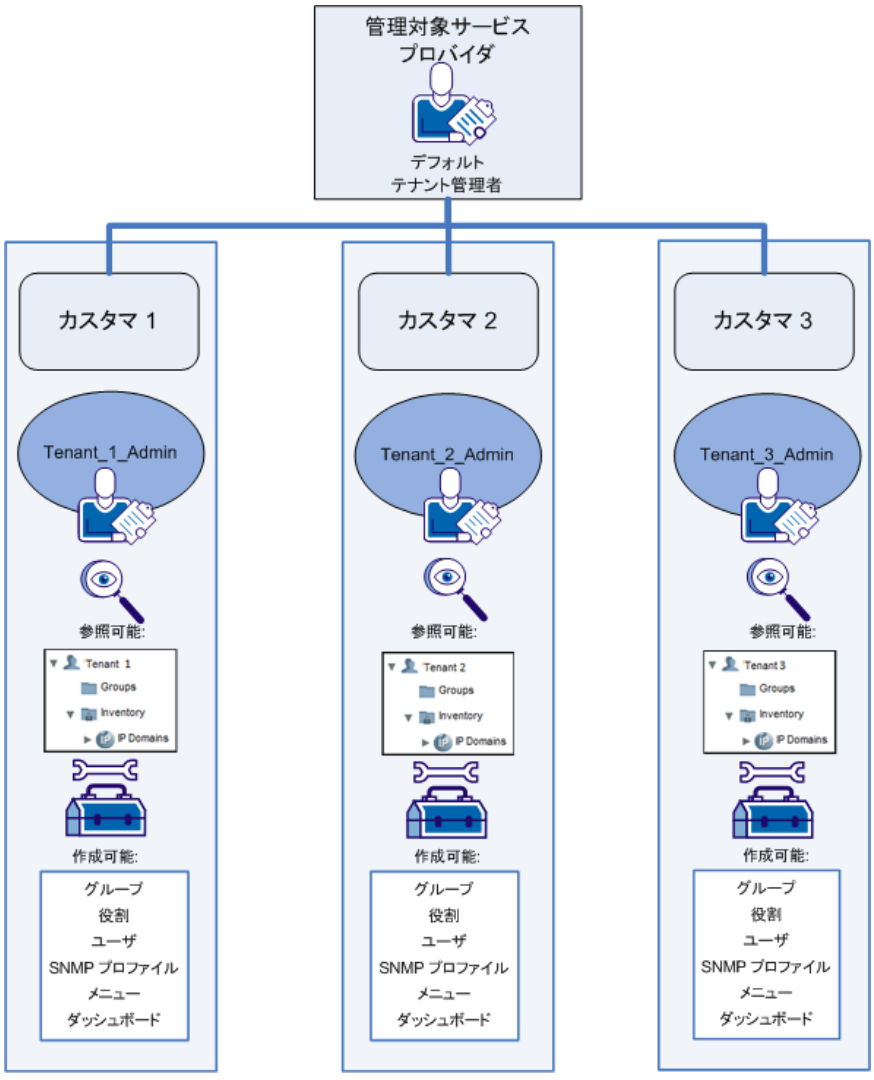
カスタム IP ドメイン (P. 45)は、管理対象アイテムをテナントと関連付ける方法を提供します。有効なテナント定義には、少なくとも 1 つのカスタム IP ドメインが含まれます。 有効なテナントを CA Performance Center に追加すると、IP アドレスがテナント ドメインに一致するすべてのアイテムが、そのテナントにすぐに関連付けられます。

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 - 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 - 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. 161)
事前定義済み役割 (P. 112)
テナントの管理 (P. 165)

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. 75)」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。

テナントのリストの表示

テナントはすべての展開で必須という訳ではありません。 テナントを作成するのは、単一のユーザ インターフェースから管理できる CA Performance Center 監視環境を個別に構築するためです。 マルチテナンシー機能では、MSP によって CA Performance Center の単一のインスタンスから個別のカスタマ ネットワークおよびシステムを監視できます。 詳細については、「テナントについて (P. 155)」を参照してください。

グローバル管理者は、テナント リストを使用して、すべてのテナントの識別情報を参照できます。

次の手順に従ってください:

1. 管理者の役割を持つユーザとしてログインします。
2. ［管理］-［カスタム設定］を選択し、［テナント］をクリックします。

   ［テナントの管理］ページが開きます。

   ページに、現在のテナントのリストが表示されます。

   カスタム テナントを作成していない場合は、事前定義済み［デフォルト テナント］のみがリスト内に表示されます。

   重要: この事前定義済みテナントは、通常はほとんどのデータ ソースのデータを収集しません。 このテナントにログインするユーザには、どのデータも表示されない可能性があります。

作成したすべてのカスタム テナントには、以下のパラメータの値があります。

名前

テナントの名前です。 45 文字までに制限されてます。

アカウント ID

このテナントを識別します。通常は、MSP を含むテナント アカウント番号またはサービス層と一致します。

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。

このページ上でいずれかのアクションを実行するには、ページ下部に並んでいるボタンの 1 つをクリックします。

詳細情報:

テナントの追加 (P. 161)
テナントについて (P. 155)
テナント範囲の設定 (P. 167)
テナントの管理 (P. 165)

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 (P. 164)］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 (P. 159)。

   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. 167)」を参照してください。

詳細情報:

テナントのクローン作成 (P. 164)
マルチ テナンシーをサポートするための管理者役割 (P. 146)

テナントの編集

グローバル管理者は、すでに作成されたテナント定義を変更できます。

テナント定義を変更しても、その変更はテナントと関連付けられた監視定義には影響しません。テナントの SNMP プロファイル、IP ドメイン、またはその他の設定を変更するには、テナント管理者としてログインするか、テナントを管理するためのテナント範囲を設定する必要があります。 詳細については、「テナントの管理 (P. 165)」を参照してください。

以下の手順に従います。

1. 管理者の役割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 (P. 159)。

   ページに、現在のテナントのリストが表示されます。
3. リストのテナント定義を選択し、［編集］をクリックします。

   ［テナントの編集］ページが開きます。
4. 必要に応じて、テナント パラメータ (P. 161)を変更します。
5. ［保存］をクリックします。

   テナント定義への変更が保存されます。新しい値が［テナント リスト］に表示されます。

テナントのクローン作成

同様のパラメータを持つ複数のテナントを最もすばやく作成するには、［テナントのクローン作成］機能を使用します。 すでに作成したテナント定義を選択して［クローン］を実行し、必要に応じて作成された新しい定義のパラメータを変更できます。

次の手順に従ってください:

1. 管理者の役割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 (P. 159)。

   ページに、現在のテナントのリストが表示されます。
3. クローンを作成するテナント定義を選択し、［クローン］をクリックします。

   ［テナントのクローン作成］ページが開きます。
4. 表示されているフィールドに、必要な情報を入力します。デフォルトでは、［名前］と［アカウント ID］のパラメータ以外の、基本的なパラメータのクローンが作成されます。

   名前

   テナントの名前です。 45 文字までに制限されてます。

   アカウント ID

   このテナントを識別します。通常は、MSP を含むテナント アカウント番号またはサービス層と一致します。
5. テナント管理者アカウントのユーザ名およびパスワードを入力します。
6. テナント ユーザ アカウントのユーザ名およびパスワードを入力します。
7. ［保存］をクリックします。

   新しいテナント定義は、クローンされたテナント定義に基づいて作成されます。 ただし、IP ドメインなど必要なパラメータが不足しています。次にテナント環境をセットアップする必要があります。詳細については、「テナントの設定 (P. 165)」を参照してください。

テナントの設定

「テナントの追加 (P. 161)」では、基本的なテナントの作成方法について説明します。 ただし、ユーザが必要な監視パラメータおよびユーザ アクセスを設定しない限り、基本的な定義は役に立ちません。

そ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すると、テナント環境を設定できます。 または、グローバル管理者である場合は、［テナントの管理］機能を使用してテナントの観点から CA Performance Center にアクセスできます。

選択されたテナントにテナント範囲を設定すると、そのテナントで使用可能な設定アイテムのみ表示されます。次に、必要な IP ドメイン、ユーザ アカウント、その他を作成して、テナントを管理します。 それらは、そのテナントに属するアイテムを表示する権限を持ったユーザのみ使用可能です。

詳細情報:

テナントの追加 (P. 161)
テナント範囲の設定 (P. 167)
テナントの管理 (P. 165)
マルチ テナンシーをサポートするための管理者役割 (P. 146)

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. 167)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. 167)
テナント役割の設定 (P. 172)
テナント ユーザの設定 (P. 175)
テナント グループの設定 (P. 170)
テナント SNMP プロファイルの設定 (P. 169)
テナント メニューの設定 (P. 177)

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 (P. 159)。

   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. 167)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 (P. 49)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. 167)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 (P. 38)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 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. 167)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。

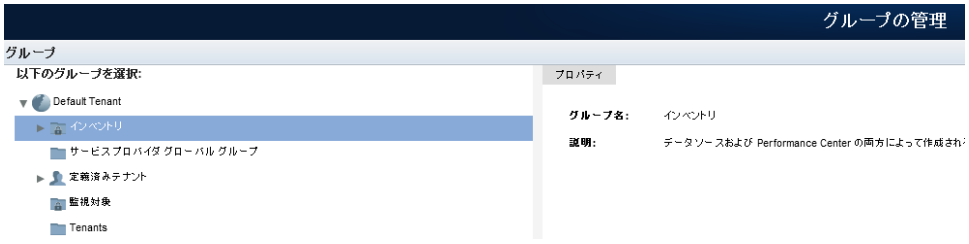
   ［テナント名］ページの［グループの管理］が開きます。

   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. 77)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. 103)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. 96)します。

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. 146)」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. 167)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。

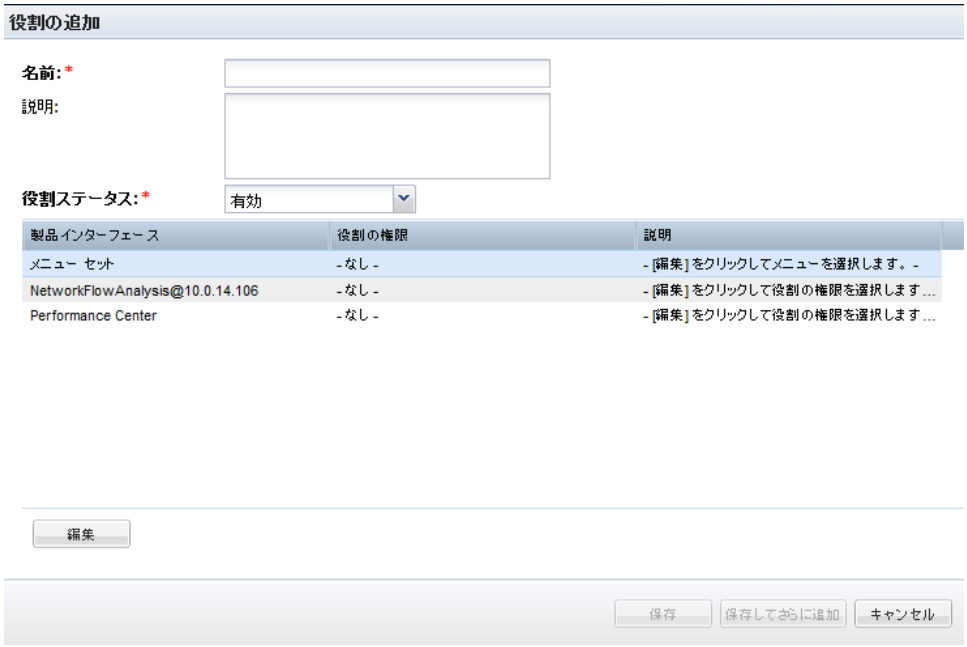
説明

（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。

詳細情報:

役割の追加 (P. 129)
役割の権限 (P. 118)
ユーザ アカウント パラメータ (P. 143)
ユーザ アカウントの追加 (P. 151)

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. 167)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。

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. 167)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。

テナントの削除

テナント定義を削除できるのは、グローバル管理者のみです。 テナント管理者には、この機能はありません。

テナント定義を削除すると、以下のすべてを含め、そのテナントに関連付けられたすべての定義が削除されます。

- データ ソース
- SNMP プロファイル
- IP ドメイン
- ユーザ アカウント
- 役割
- グループ
- カスタム ダッシュボード
- カスタム メニュー

以下の手順に従います。

1. 管理者の役割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 (P. 159)。

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

   操作を確定するかどうかを尋ねられます。
4. ［はい］をクリックし、削除を確定します。

   テナント定義が削除されます。［テナント リスト］に表示されなくなります。

第 7 章: ログとトラブルシューティング

このセクションには、以下のトピックが含まれています。

ログ

ログ ファイルを日単位または週単位確認することで、通常の操作に影響が出る前に問題を解決できます。すべてのログは、サービス（またはデーモン）に対応するサブフォルダ内に格納されます。以下のパスのログ ファイルを検索します。

```
CA/PerformanceCenter/servicename/logs
```

servicename パラメータを以下のいずれかのサービス名に置換します。

DM

デバイス マネージャ。

- DMService.log - デバイス マネージャからの出力（主に同期に関連）。
- wrapper.log - caperfcenter_devicemanager プロセスのログ。

EM

イベント マネージャ。

- EMService.log - イベント マネージャからの出力。イベントおよびアラームの詳細を含みます。
- wrapper.log - caperfcenter_eventmanager プロセスのログ。

PC

メインのコンソール プログラム。

- PCService.log - CA Performance Center 関連のログ。ユーザ インターフェースとビュー コンポーネントで構成されます。
- wrapper.log - caperfcenter_console プロセスのログ。

SSO

Single Sign-On 認証ソフトウェア。

- SSOService.log - Single Sign-On のログ。HTTPS（Secure Sockets Layer ）の設定に関する HTTPS 情報が含まれます。
- wrapper.log - caperfcenter_sso プロセスのログ。

Single Sign-On 設定ツールに関する問題については、以下の場所にあるアプリケーション ログを確認します。

```
/opt/CA/PerformanceCenter/sso/logs/application.log
```

ログ ファイル名には、関連する日付と時間が含まれます。

新しいログ ファイルは、毎日自動的に生成されます。 ディスク領域を過剰に消費しないよう、14 日を経過すると古いログ ファイルから順に自動的に削除されます。

データベースまたはデータ ソースの同期に関連するエラーを見つけるには、最新のログ ファイルにアクセスします。まず始めに、［ダッシュボード］タブの［イベント］ダッシュボードを開き、［ステータス］でソートします。 関連するログ ファイルを確認する場合は、イベント タイプおよび障害の日時に注意します。 ログ ディレクトリで、ファイル名に対応する日付のログ ファイルを開きます。

ロギング レベルの設定

デフォルトでは、CA Performance Center ログ ファイルには、ユーザの監視システムに関するエラーと警告についての概要情報のみが含まれます。トラブルシューティングの状況をより高度にすると、ロギング レベルを変更して、より多くの情報を収集し、日単位のログ ファイルに書き込むことができます。

次の手順に従ってください:

1. CA Performance Center アプライアンス上の Linux コマンド ライン インターフェースで、root としてログインします。
2. 変更するログ レベルのサービスに対応する、以下のディレクトリに移動します。 *servicename* パラメータのオプションのリストについては、「ログ (P. 181)」を参照してください。

   ```
   /opt/CA/PerformanceCenter/servicename/etc/
   ```

3. log4j.xml という名前のログ設定ファイルを開きます。
4. グローバル ログ レベルを変更するには、**<root>**エレメントを見つけます。
5. **<root>** エレメントの **<priority value>** を、以下のログ レベルのいずれかに変更します。
   - FATAL。アプリケーションの失敗の原因となる可能性がある重大なエラー イベントを特定します。
   - ERROR。深刻だが、アプリケーションの実行は継続できる可能性が高いエラー イベントを特定します。
   - WARN。障害を引き起こす可能性がある状況を特定します。
   - INFO。アプリケーションの進捗状況に関する情報メッセージを提供します。
   - DEBUG。問題のデバッグに役立つ情報を提供します。
6. 特定のログのログ レベルを変更するには、関連する **<logger>** エレメントを見つけます。
7. ログ レベルの値を、手順 5 にリストされている値のいずれかに変更します。

複数ログ ファイルの検索

CA Performance Center サーバにアクセス権がある場合、複数のログ ファイルを同時に検索できます。 複数のファイルを検索することで、特定のタイプのエラーのインスタンスをすべて検索できます。 関連するサブディレクトリ内の各コンポーネントのログ ファイルを探します。 たとえば、「DM」サブフォルダ内のデバイス マネージャ ログを探します。

次の手順に従ってください:

1. CA Performance Center アプライアンス上の Linux コマンド ライン インターフェースで、root としてログインします。
2. 検索対象のログに対応するサービスのログ ディレクトリに移動します。*servicename* パラメータのオプションのリストについては、「ログ (P. 181)」を参照してください。

   ```
   opt/CA/PerformanceCenter/servicename/logs
   ```

3. 以下のコマンドを入力します。

   ```
   grep -i keyword *
   ```

4. *キーワード*は、以下のいずれかを代入できます。
   - 「error」
   - 「warn」
   - 「failed」
   - 「no data」

   指定したキーワードが含まれているログ ファイルのリストが返されます。
5. ログ ファイルを表示するには、ローカル サーバ上でテキスト エディタ プログラムを使用します。

データ ソースの登録に失敗

問題の状況:

新しいデータ ソースを追加しようとしたのですが、登録に失敗しました。

「データ ソースの作成に失敗しました。データ ソース通信失敗。」というメッセージが表示されました。

解決方法:

このメッセージは、データ ソースに到達不可であることを示します。 以下を実行します。

- データ ソースが実行されていることを確認してください。
- データ ソースのデータベースがインストールされているサーバの DNS ホスト名または IP アドレスが正しいことを確認してください。この情報を表示するには、データ ソースを編集します。
- 介在するファイアウォールを確認してください。 CA Performance Center 通信がデータ ソースに到達できるようファイアウォールが設定されることを確認します。 開くポートの詳細については、「*インストール ガイド*」を参照してください。

解決方法:

CA Infrastructure Management Data Aggregator データ ソースで障害が発生した場合は、データ ソースが実行されていることを確認します。 以下の URL にアクセスします。

```
http://<host>:<port_number>/rest
```

「host」は Data Aggregator がインストールされているサーバの IP アドレスであり、「port_number」は、RESTful Web サービスにアクセスするために使用されるポートで、通常は 8181 です。

Web サービスのステータスは、Data Aggregator が実行されているかどうかを示します。

解決方法:

デバイス マネージャの application.log ファイルを確認します。 ファイルは以下のディレクトリに書き込まれます。

```
CA¥PerformanceCenter¥PC¥logs
```

ログ エントリは、スタック トレースと共にデータ ソースと通信するために CA Performance Center によって使用される URI を参照します。

データ ソースの同期の失敗

問題の状況:

データ ソースの同期を実行しようとしましたが「同期失敗」というメッセージが表示されました。

解決方法:

同期失敗は、データ ソースが到達不可であることを示す可能性があります。 以下を実行します。

- データ ソースが実行されていることを確認してください。
- ［データ ソースの追加］で、データ ソースのデータベースがインストールされているサーバの DNS ホスト名または IP アドレスが正しいことを確認してください。

解決方法:

同期失敗は、同期中にデータ ソースが送信されたデータを処理できないことを示す可能性があります。

まず、データ ソースの［データ ソース ログ］を確認します。 詳細については、「データ ソース ログの表示 (P. 30)」を参照してください。

問題のソースをまだ特定できない場合は、デバイス マネージャの application.log ファイルを確認します。 このファイルは、以下のディレクトリに書き込まれます。

```
CA¥PerformanceCenter¥PC¥logs
```

同期中にデータ ソースが CA Performance Center から受信されたデータを処理できなかった場合、ログ エントリには一般的な SOAP 例外が表示されます。

解決方法:

同期の試行中に CA Performance Center に問題が発生しました。

上記の説明に従い、ログ ファイルを確認します。 同期の以下の段階で例外およびスタック トレースを探します。

- プル
- グローバル同期
- バインド（データ ソースと最初に同期する場合のみ実行する）
- プッシュ

ログには、各段階に実行される手順の詳細情報が含まれます。 この情報から、同期失敗の原因を特定できます。

解決方法:

システムの時間が同期されていません。NTP サーバ、または各サーバ(データ ソースおよび CA Performance Center サーバを含む) のシステム時間を確認します。

詳細情報:

データ ソース ログの表示 (P. 30)
同期 (P. 25)
データ ソースの登録に失敗 (P. 184)

データ ソース テストの失敗

問題の状況

登録処理中にデータ ソースをテストしましたが、テストは失敗しました。

解決方法

以下を実行します。

- データ ソースのデータベースがインストールされているサーバの DNS ホスト名または IP アドレスが正しいことを確認してください。
- とにかく、データ ソースの登録を試してみてください。テストが失敗したとしても、データ ソース登録は成功する場合があります。
- 登録失敗情報のログを確認します。詳細については、「データ ソース テストの失敗 (P. 184)」を参照してください。

解決方法

CA Infrastructure Management Data Aggregator データ ソースで障害が発生した場合は、データ ソースが実行されていることを確認します。 以下の URL にアクセスします。

```
http://<host>:<portnumber>/rest
```

「host」は Data Aggregator がインストールされているサーバの IP アドレスであり、「portnumber」は、RESTful Web サービスにアクセスするために使用されるポートで、通常は 8181 です。

Web サービスのステータスは、Data Aggregator が実行されているかどうかを示します。

解決方法

CA Infrastructure Management Data Aggregator 以外のデータ ソースで障害が発生した場合は、対応するイベントのアプリケーション ログ ファイル（PC/logs/application.log）を確認します。 ログ エントリには、スタック トレースと共にデータ ソースと通信するために CA Performance Center が使用した URI が含まれます。

詳細情報:

データ ソースの登録 (P. 31)

インベントリが空

症状:

データ ソースをインストールして登録しましたが、インベントリに管理対象アイテムが表示されません。

解決方法:

データ ソースが登録されステータスがアクティブであることを確認します。 以下を実行します。

1. 管理者権限を持つユーザとしてログオンします。
2. ［管理］-［データ ソース設定］を選択し、［データ ソース］をクリックします。

   ［データ ソースの管理］ページが表示されます。 リストに、登録済みの各データ ソースと、そのステータスが表示されます。

解決方法:

以下のいずれかが発生した可能性があります。

- データ ソースの登録に失敗しました。詳細については、「データ ソース テストの失敗 (P. 184)」を参照してください。
- データ ソースの同期に失敗しました。詳細については、「データ ソースの同期の失敗 (P. 185)」を参照してください。

解決方法:

ログインに使用したユーザ アカウントの権限を確認します。 そのユーザ アカウントに権限グループが割り当てられていない場合は、管理対象アイテムは表示されません。 詳細については、「ユーザ アカウントの追加 (P. 151)」を参照してください。

また［デフォルト テナント］に関連付けられているユーザとしてログインしていないことも確認してください。 通常このテナントには、管理対象アイテムは表示されません。

ビューにデータが表示されない

症状:

一部のインターフェース ビューで、データが欠落したり、テーブル列が空になります。 たとえば、インターフェースおよびデバイス名、インターフェース速度、および使用率データがビューに表示されません。

解決方法:

一部のデータ ソースでは、最小長より短い認証パスワードやプライバシー パスワードをサポートしません。

SNMPv3 形式を使用する SNMP プロファイルでは、認証とプライバシー オプションを有効になります。SNMPv3 プロファイルを作成するときに、8 文字以上の長さの認証パスワードを指定します。 これより短い認証パスワードを指定すると、パスワードおよび SNMP プロファイルは無効になります。 これらのプロファイルは、デバイスとの通信に成功しない場合があります。 この場合、影響を受けたインターフェースの SNMP データが欠落します。

同様に、認証プロトコルとして MD5 または SHA を使用する SNMP v3 プロファイルでは、空のパスワードはサポートされていません。

解決方法:

SNMPv3 プロファイルを編集して、8 文字以上の長さの認証パスワードを指定します。

詳細情報:

SNMP プロファイルの追加 (P. 38)

ビューの「データがありません」メッセージ

症状:

ダッシュボード上のいくつかのビューが空になっています。 「表示するデータがありません」というメッセージが表示されます。

解決方法:

ダッシュボード上のグラフまたはテーブル ビューに「表示するデータがありません」と表示される場合、以下のような多くの理由が考えられます。

- ビューのデータ ソースがインストールされていないか登録されていません。

  各ビューは、単一のデータ ソースからデータを受信します。 対応するデータ ソースが登録されていない場合でも、一部のビュー コンテナはダッシュボードに表示されます。 データ ソースが登録されるまで、それらのビュー コンテナは空のままです。

  このようなビューがダッシュボードに表示されないように、表示設定を変更できます。 詳細については、「［ビューの非表示］の無効化 (P. 19)」を参照してください。

  ヒント： 通常、ビュー上の［?］ボタンをクリックすることで、ビューに関連付けられているデータ ソースを 確認できます。

- データ ソースは登録されていますが、一時的に無効になっています。

  無効なデータ ソースはデータがポーリングされません。 管理者は、データ ソースを編集して有効にすることができます。詳細については、「データ ソースの登録 (P. 31)」を参照してください。

- データを表示するには、先にビュー タイプを編集する必要があります。

  一部のビュー タイプには、デフォルト設定がありません。 たとえば、マルチビューやマルチトレンド ビューでは、データを表示する前にカスタマイズする必要があります。

- 選択された時間範囲内にデータがありません。 この仮定が正しいかどうかを検証するには、別の時間範囲を選択します。

- レポート対象のデバイスに対するポーリングを開始してから、十分な時間が経過していません。

  ポーリング間隔がかなり長い場合、最初のデータポイントが表示されるまで時間がかかることがあります。 ポーリング レートはデータ ソースに設定されています。

- サービスが実行されていません。

  デバイス マネージャ サービスが実行されていない場合、「データがありません」というメッセージが表示される可能性が高いです。 CA Performance Center デーモンのステータスを確認する手順は、「インストール ガイド」に説明されています。

- このビューで必要なタイプのアイテムが、現在のグループに含まれていません。

  ダッシュボードでレポートされるデータのアイテム グループは、［期間］セレクタの上に表示されます。 たとえば、ルータ グループからのデータをサーバ レポートに表示しようとしていないかなど、ビューを確認してください。

- グループが新しいか、または最近変更されました。

  グループ メンバシップを確認してください。グループのルールが誤って設定されている場合があります。

  ユーザ アカウントに必要な役割の権限がある場合は、ビューを編集して別のグループ コンテキストを選択します。 または、［期間］セレクタの上にある［グループ フィルタ］リンクをクリックして、ダッシュボード用に別のグループ コンテキストを選択します。

- ログイン ユーザのユーザ アカウントに、データがレポートされた監視対象アイテムを表示する権限がありません。 詳細については、「ユーザ アカウントの作成方法 (P. 148)」を参照してください。

- データ ソースが CA Performance Center と正しく同期されていません。詳細については、「データ ソースの同期の失敗 (P. 185)」を参照してください。

- コンポーネントが検出されなかったか、または、管理対象アイテムのディスカバリに失敗しました。

  この問題はデータ ソースに固有であるため、該当するデータ ソースについてオンライン ヘルプで確認してください。Data Aggregator データ ソースについては、インベントリ ディスカバリの履歴を確認できます。［ディスカバリ プロファイル リスト］ページで、初回のディスカバリで作成したディスカバリ プロファイルを選択し、［履歴］ボタンをクリックします。

- メトリック ファミリが設定されていないか、有効ではありません。

  Data Aggregator データ ソースでは、事前定義済み（ファクトリ）監視プロファイルは自動的に［All Routers］コレクションなどの事前定義済みコレクションに適用されます。ただし、カスタム グループおよびカスタム コレクションは、誤って設定されたカスタム監視プロファイルによって影響を受けることがあります。

- データベース クエリがタイムアウトしました。 CA Performance Center サーバとデータ ソース間のネットワーク接続問題によって、この問題が発生する場合があります。

NetQoS--NPC--Troubleshooting--チャートまたは画像が表示されない

症状:

一部のチャートまたは画像が CA Performance Center に表示されません。赤い X は、チャートまたは画像が壊れていることを示します。

解決方法:

Internet Explorer （IE）で CA Performance Center を実行している場合、安全な HTTP （HTTPS）を使用しています。 IE で、HTTPS に必要とされたトランスポート レイヤ セキュリティ（TLS）設定は、デフォルトでは TLS 1.0 のみに設定されます。 壊れたチャートまたは表示されない画像を表示するには、TLS 1.1 をオンにします。

次の手順に従ってください:

1. ブラウザ上部の［ツール］をクリックするか、または右上でギヤ アイコンをクリックします。
2. ［インターネット オプション］をクリックします。
3. ［詳細設定］タブをクリックし、TLS 1.1 チェック ボックスを選択します。
4. ［適用］をクリックします。

   TLS 設定が保存されます。

CA Remote Engineer の使用

CA Remote Engineer（CARE）ツールは、問題のトラブルシューティングに CA サポートの担当エンジニアが使用するデータを収集します。 CARE のスクリプト ディレクトリには、CARE がサポートする製品それぞれの設定ファイルが入っています。

CARE は、CA Infrastructure Management コンポーネントと同時にインストールされます。

コンポーネント	Installation Directory
CA Performance Center	/opt/CA/PerformanceCenter/RemoteEngineer
Data Aggregator	/opt/IMDataAggregator/RemoteEngineer
Data Collector	/opt/IMDataCollector/RemoteEngineer
Data Repository	Data Repository インストーラは、/opt/CA/IMDataRepository_vertica7 ディレクトリに CARE を抽出します。 **dr_install.sh** を実行して、/opt/CA/RemoteEngineer ディレクトリにあるクラスタ内の各ノードに CARE をコピーします。

CA サポートの担当エンジニアから指示があった場合には、以下の手順を実行して、CARE を実行し、トラブルシューティング用のデータを収集してください。

次の手順に従ってください:

1. コマンド プロンプトで、インストール ディレクトリに移動します。

   ```
   cd install dir
   ```

2. 以下のコマンドを入力します。

   ```
   ./re.sh
   ```

3. プロンプトが表示されたら、CARE を実行している場所に応じて、以下のいずれか 1 つを入力します。
   - CAPC
   - IMDataAggregator
   - IMDataCollector
   - IMDataRepository
4. CARE ファイルを CA Support に FTP で送信するかどうかを尋ねるプロンプトが表示されたら、以下のいずれかの応答を行います。
   - **y** CARE ファイルは CA Support に送信されます。
   - **n** CARE ファイルは、CA Support に手動で配信できる ZIP ファイルに保存されます。

第 8 章: ダッシュボードとレポートの操作

このセクションには、以下のトピックが含まれています。

CA Performance Center でのデータの表示

ダッシュボード ページには、CA Performance Center が登録済みのデータ ソースから受信し、解釈およびフォーマットするデータの動的ビューが表示されます。 *ビュー*、または*データ ビュー*は通常、グラフまたは表形式で統計データを示します。 各ビューは、収集されたデータの個別のセットを表します。 ユーザ アカウントの役割の権限に応じて、ダッシュボード ページに個別のビューを追加および編集、または削除できます。 場合によっては、データを CSV 形式のファイルにエクスポートできます。

ダッシュボード ページ上のビューの配置は自由に変更できます。 必要な役割の権限を持つユーザはダッシュボードをカスタマイズできます。 たとえば、ボリューム データ ビューの横にアプリケーション パフォーマンス データのビューを配置することにより、問題のトラブルシューティングを 1 つのページで行うことができます。

事前定義のダッシュボードは、ワークフロー内に整理されています。トップ N ビューから、個別のデバイスなど、絞り込まれたコンテキストから得られる詳細なメトリックにドリルダウンできます。 標準で提供されるワークフローによって、ユーザは参照しているメトリックに関連のあるデータに移動されます。 たとえば、インターフェース使用率のビューからドリル ダウンして、廃棄のビューを参照できます。

カスタム グループを作成することにより、サイト、デバイス、またはインターフェースの特定のセットに関するデータを表示できます。 グループ セレクタ（左上にある［変更］リンク）を使用して、これらのグループをダッシュボードに適用できます。 特定のグループ化に対するデータを分析するためにダッシュボードの「コンテキスト」を変更することができます。 また、管理対象アイテムまたはアイテム グループを選択し、選択されたメトリック ファミリおよびタイムフレームに対してオン デマンドのレポート (P. 217)を生成できます。

グループのデータが表示されるビューには、データ ソースからのロールアップ データが含まれます。 1 つの管理対象アイテムに関するデータ ビューでは、通常データ ソースに直接ドリルダウンするためのパスが提供されています。 Single Sign-On 機能を使用すると、ダッシュボードからデータ ソースのインターフェースに移動できます（ただし、ユーザ アカウントに「データ ソースへのドリル イン」役割権限がある場合のみ）。

詳細情報:

ダッシュボードおよびレポート (P. 208)

コンテキスト ページ ナビゲーション

ダッシュボードから、個々の管理対象アイテムに関する詳細情報へ頻繁にアクセスできます。 大半のダッシュボードは、時間ごとのロールアップやアイテム グループの平均などのサマリ データのビューで構成されています。データ ソースから追加のデータを利用できる場合は、ダッシュボードのページでリンクされているアイテムをクリックして、*コンテキスト ページ*へドリル ダウンすることができます。

注: ビューへのドリル ダウンを実行するための役割権限が必要です。

コンテキスト ページ上のビューには、限られたコンテキストからのフィルタされたデータ（単一の管理対象アイテムのデータのビューなど）が表示されます。 このリンクを使用して、特定のデータ、およびパフォーマンス問題のソースにおける特定のデータおよびホームへドリル ダウンします。

いくつかのデータ ソースのデータ ビューで、テーブル ビューのアイテム名を右クリックしてメニューにアクセスすることもできます。 たとえば、［インベントリ］セクション内のアイテム名に対応するリンクを右クリックします。 メニューを使用して、より詳細なデータが含まれている、関連コンテキスト ページを選択することができます。

最終的には、いくつかのコンテキスト ページに、詳細データの追加ページのタブが含まれています。 タブをクリックして、選択した管理対象アイテムまたはアイテムのタイプによってフィルタされたデータを表示します。

デバイス名の表示

事前定義済みの管理者の役割を持ったユーザは、デバイス名のエイリアスを定義できます。 エイリアスは、必要に応じて CA Performance Center ビューに表示されます。

デバイス エイリアスは、CA Performance Center 内の関連付けられた管理対象アイテムに適用されるユーザ設定名です。 エイリアスが定義されていない場合、検出されたデバイス名が表示されます。 エイリアスを使用する場合でも、インターフェースまたはデバイスのコンテキスト ページの［詳細］タブで、検出された名前を参照できます。

インターフェースの説明の表示

インターフェースの説明は、必要に応じて CA Performance Center ビューに表示されます。たとえば、インベントリ内のインターフェースのリスト、およびインベントリ内のインターフェース アドレスのリストには、［説明］列が含まれています。インターフェース ビューでは、インターフェースの説明は以下のように表示されます。

- ビューにサブタイトルが含まれる場合、インターフェースの説明はサブタイトル内に含まれます。
- ビューに［名前］列が含まれているが、［説明］列が含まれていない場合、インターフェースの説明は［名前］列のインターフェース名に追加されます。
- インターフェースの説明は、説明が表示されていないすべてのビュー内のインターフェース名に追加されます。

管理対象アイテムのインベントリ

［インベントリ］ページは［インベントリ］タブから使用できます。 インベントリには、すべてのデータ ソースが検出および監視するすべてのアイテム、つまり *管理対象アイテム*のリストが含まれています。 アプリケーション、デバイス、インターフェースなどのすべてのタイプの管理対象アイテムは、インベントリ ページのリスト ビューに表示されます。 インベントリは、オンデマンド レポート (P. 217)の作成に使用します。

このページの「コンソール」セクションには、別のコンソールを持つ登録済みのデータ ソースへのリンク一覧が含まれています。 アクセスするには、各データ ソースの製品権限が必要です。

［インベントリ］リストには、登録済みデータ ソースの中で CA Performance Center で現在使用できるアイテムのカテゴリのみが表示されます。またこのリストには、アカウント権限セットに含まれるグループ メンバのアイテムのみが表示されます。 カテゴリは、選択したタイプのすべての管理対象アイテムが示されている、フィルタされたリストへアクセスするためのリンクです。

リスト ページは、デバイスのホスト名や IP アドレスなど、各アイテムを識別するための最小限の情報を提供します。 管理対象アイテムのオンデマンド レポートを有効化するには、チェック ボックスをオンにします。

複数のデータ ソースが 1 つの管理対象アイテムを監視している場合、CA Performance Center はそのアイデンティティを一致させて、インベントリ内に 1 つのアイテムを作成します。

詳細:

検索の実行 (P. 198)
インベントリが空 (P. 188)

検索の実行

展開規模によっては、何千もの管理対象アイテムがある場合があります。複数の検索機能を使用することで、特定のアイテムまたはアイテム グループのデータを見つけることができます。

ユーザ アカウントに必要な役割の権限がある場合は、［インベントリ］タブから検索を開始できます。 このタブで、管理対象アイテム タイプのリストを表示できます。 アイテムのリストを表示するには、リンクをクリックします。 次に、リスト ビュー下の検索フィールドと、ソートおよびページング機能を使用して、リストのアイテムを検索します。

［インベントリ］ページおよび［検索結果］ページからは、オンデマンド レポート (P. 217)にもアクセスできます。

注: ［インベントリ］を表示してグローバル検索を実行する機能は、それらの役割を持った個別のオペレータに許可されます。 ［インベントリと検索の表示］役割の権限を持ったユーザのみに、［インベントリ］タブが表示されます。

グローバル検索を実行するには、任意のページの一番上にある検索フィールドを使用します。このタイプの検索は、すべてのデータ ソースで、データベース内のすべてのアイテムをスキャンします。 グローバル検索は、［インベントリ］内の検索に一致するすべてのアイテムのリストを、アイテム タイプによってソートして返します。各ビューで、結果をさらにフィルタすることもできます。 詳細については、「フィルタによる検索結果の絞り込み (P. 200)」を参照してください。

テーブル ビューでは、さらに限定された検索機能が使用可能です。この機能は、特別な役割の権限を必要としません。 テーブル フッタから検索を実行すると、管理対象アイテムをフィルタして、そのビューに表示されるアイテムを限定します。 その他のビューまたはダッシュボードからのアイテムは、表示されません。

管理対象アイテムの検索

ネットワーク問題に関連する可能性のあるルータなど、単一のアイテムのコンテキストに関する情報に直接移動できます。 データ ビューの検索フィールドでは、選択されたビュー内のアイテムを検索できます。 ダッシュボード ページ、および［管理］および［インベントリ］ページ（ユーザ アカウントに必要な役割の権限がある場合）で、検索できます。

次の手順に従ってください:

1. 検索を開始するダッシュボードまたはインベントリ ページに移動します。

   注: 必要な役割の権限がある場合は、［グループの管理］ページのグループ ツリーなど、［管理］ページでも検索できます。

2. 検索フィールドに検索文字列を入力し、Enter キーを押します。

   テキスト文字列、数を含む検索文字列、またはこれらの組み合わせを指定できます。

   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。

   詳細については、「フィルタによる検索結果の限定 (P. 200)」を参照してください。

   検索結果が、同様のアイテムのカテゴリに表示されます。

3. リストのアイテムのうち 1 つをクリックします。

   選択したアイテムの情報を含んだ［コンテキスト］ページが表示されます。

フィルタによる検索結果の絞り込み

［検索］フィールドにワイルドカード文字またはフィルタ テキストを追加することで、実行する検索結果を狭める、または広げることができます。フィルタは、グローバル検索またはビュー レベル検索に適用できます。

検索には、ワイルド カード文字としてアスタリスク (*) を使用できます。以下に例を示します。

- 「serv*」は、「serv」で始まるエントリのあるすべての行を返します。
- 「*erver」は、「erver」で終わるエントリのあるすべての行を返します。
- 「*server*」は「server」と同様で、たとえば my_server、server1、または単に server など、「server」という単語が含まれるすべての単語を返します。
- 「ser*ver」は、「server」など、「ser」で始まり、「ver」で終わるすべての単語を検索します。

検索結果を狭めるには、複数の検索語を追加します。 たとえば、「server 192.168*」という検索文字列を使用してデバイスを検索した場合、検索は 192.168.0.0/16 のネットワーク上のすべてのサーバを返します。

ユーザの環境に 400 万のサーバなど多数の管理対象アイテムが含まれる場合は、グローバル検索のフィルタリングを推奨します。そうしないと、グローバル検索を行うたびに、ユーザ インターフェースのパフォーマンスが制限されてしまいます。

複数の監視対象デバイスに対するエイリアス名の設定

CA Performance Center には、複数の監視対象デバイスにエイリアス名を設定するスクリプトが含まれます。 このスクリプトを使用して、一度に複数の監視対象デバイスのエイリアス名を設定できます。 エイリアス名は、デバイスのインベントリ リストとインターフェースのインベントリ リストに表示されます。

注: このスクリプトを使用して設定されるエイリアスは、IP ドメインの追加時に CSV ファイルをインポートして設定されるエイリアスよりも優先されます。CSV ファイルのインポートの詳細については、「*CA Performance Center 管理者ガイド*」を参照してください。

このスクリプトには 2 つの機能があります。まず、スクリプトは、デバイス アイテム ID とデバイス名のリストを .csv 形式で返します。 各監視対象デバイスに設定したいエイリアス名を含めるには、この .csv ファイルを変更します。スクリプトの 2 番目の機能は、更新された .csv ファイルを取り込んで、監視対象デバイスのエイリアス名を設定することです。

次の手順に従ってください:

1. コマンド プロンプトを開き、*Performance_Center_installation_directory*/PerformanceCenter/Tools/bin ディレクトリにアクセスします。
2. スクリプトを呼び出して監視対象デバイスのエイリアス名を設定するには、以下のコマンドを入力します。

   ```
   ./update_alias_name.sh
   ```

   スクリプト パラメータのリストと説明が表示されます。
3. 監視対象デバイスの全リストを返すには、以下のコマンドを入力します。

   ```
   ./update_alias_name.sh -h host_name -u username -p password [-T item_type] [-o output_filename]
   ```

   -h *host_name*

   接続先の CA Performance Center ホスト名を指定します。

   -u *username*

   エイリアス名を設定する CA Performance Center 管理者のユーザ名を指定します。

   -p *password*

   エイリアス名を設定する CA Performance Center 管理者のパスワードを指定します。

   -T *item_type*

   エイリアス名を設定するアイテムのタイプを指定します。 有効な値はデバイス、インターフェースまたはコンポーネントです。

   デフォルト： device

   デフォルト値を保持します。

-o *output_filename*

（オプション）ItemID および Device Name で示される監視対象デバイスの総数を含む .csv ファイルを、そのデフォルト ファイル名とは異なるファイル名を使用して作成します。 このパラメータの値を入力しない場合、.csv ファイルにはデフォルト名 DeviceList.csv が使用されます。

.csv ファイルの形式は、「デバイス アイテム ID, デバイス名」となります。

以下に例を示します。

560, MyRouter1

561, MyRouter2

4. 前の手順で作成された .csv ファイルを変更して、監視対象デバイスごとに設定するエイリアス名を表示します。 このファイルの形式は、「デバイス アイテム ID, デバイス エイリアス名」となる必要があります。

   注: .csv ファイルのアイテム ID が無効な場合、エラー メッセージは表示されません。 これらの無効なエントリは無視されます。

   以下に例を示します。

   560, MyRouter1AliasDisplayName

   561, MyRouter2AliasDisplayName

   注: カンマおよびスペースは .csv ファイルの［エイリアス名］フィールドで使用できます。

5. 以下のコマンドを入力します。

   ```
   ./update_alias_name.sh -h host_name -u username -p password [-T device] -i input_file
   ```

   -i *input_file*

   以前にエイリアス名を使用して作成した .csv ファイルのファイル名を指定します。

   エイリアス名は監視対象デバイスに対して設定されます。

   注: -i を指定しなかった場合、スクリプトは指定されたタイプで必要なアイテム ID のすべてをルックアップし、アイテム ID とアイテム名を使って csv ファイルを作成します。

6. （オプション）大量の監視対象デバイスにエイリアス名を設定するには、以下のコマンドを入力してバッチ サイズを調整し、バッチ間で一時停止させます。 このような調整は、作業負荷の制御に役立ちます。

```
./update_alias_name.sh -h host_name -u username -p password -T device -i
input_file -b batch_size –t time_in_seconds
```

–b *batch_size*

各バッチで処理するアイテムの数を示します。

デフォルト： 10000

-i パラメータが設定されていない場合のデフォルト： 150

–t *time_in_seconds*

バッチ間で一時停止する時間（秒単位）を示します。

デフォルト： 1

-i パラメータが設定されていない場合のデフォルト： 1

以下に例を示します。

```
./update_alias_name.sh -h host_name -u username -p password -T device -i
input_file -b 20 –t 2
```

詳細:

IP ドメインの追加 (P. 49)

複数の監視対象デバイスにわたるインターフェースおよびコンポーネントへのエイリアス名の設定

CA Performance Center には、複数の監視対象デバイスにわたるインターフェースおよびコンポーネントへのエイリアス名を設定するためのスクリプトが含まれます。割り当てる役割の権限に応じて、ユーザはインターフェースのインベントリ リスト、およびダッシュボードとビューでエイリアス名を確認します。

このスクリプトには 2 つの機能があります。まず、スクリプトは、インターフェース アイテム ID またはコンポーネント アイテム ID のリスト、およびインターフェース名またはコンポーネント名を.csv 形式で返します。インターフェースまたはコンポーネントに設定するエイリアス名を含めるには、この .csv ファイルを変更します。 スクリプトの 2 番目の機能は、更新された .csv ファイルを取り込んで、インターフェースまたはコンポーネントのエイリアス名を設定することです。

次の手順に従ってください:

1. コマンドプロンプトを開き、*Performance_Center_installation_directory*/PerformanceCenter/Tools/bin ディレクトリにアクセスします。
2. スクリプトを呼び出してインターフェースまたはコンポーネントのエイリアス名を設定するには、以下のコマンドを入力します。

   ```
   ./update_alias_name.sh
   ```

   スクリプト パラメータのリストと説明が表示されます。

例: インターフェースへのエイリアス名の設定

1. Data Aggregator ホストによって監視されているインターフェースの完全なリストを返すには、以下のコマンドを入力します。

   ```
   ./update_alias_name.sh -h host_name -u username -p password -T item_type [-o output_filename]
   ```

   -h *host_name*

   接続先の CA Performance Center ホスト名を指定します。

   -u *username*

   エイリアス名を設定する CA Performance Center 管理者のユーザ名を指定します。

   -p *password*

   エイリアス名を設定する CA Performance Center 管理者のパスワードを指定します。

   -T *item_type*

   エイリアス名を設定するアイテムのタイプを指定します。 有効な値はデバイス、インターフェースまたはコンポーネントです。

   デフォルト： device

   インターフェースを指定します。

   -o *output_filename*

   （オプション）デバイス アイテム ID、インターフェース アイテム ID、およびインターフェース名によりインターフェースの総数を含む .csv ファイルをデフォルトのファイル名とは異なるファイル名で作成します。 このパラメータの値を入力しない場合、.csv ファイルにはデフォルト名 InterfaceList.csv が使用されます。

.csv ファイルの形式は、「デバイス アイテム ID, インターフェース アイテム ID, インターフェース名」となります。

以下に例を示します。

560, 164, MyInterface1

561, 165, MyInterface2

2. インターフェースごとに設定するエイリアス名に注意しながら、前の手順で作成された .csv ファイルを変更します。 このファイルの形式は、「デバイス アイテム ID、インターフェース アイテム ID、インターフェース エイリアス名」である必要があります。

   注: .csv ファイルのアイテム ID が無効な場合、エラー メッセージは表示されません。 これらの無効なエントリは無視されます。

   以下に例を示します。

   560、164、MyInterface1AliasDisplayName

   561、165、MyInterface2AliasDisplayName

   注: カンマおよびスペースは .csv ファイルの［エイリアス名］フィールドで使用できます。

3. 以下のコマンドを入力します。

   ```
   ./update_alias_name.sh -h host_name -u username -p password -T interface -i input_file
   ```

   -i *input_file*

   以前にエイリアス名を使用して作成した .csv ファイルのファイル名を指定します。

   エイリアス名はインターフェースに対して設定されます。

   注: -i を指定しなかった場合、スクリプトは指定されたタイプで必要なアイテム ID のすべてをルックアップし、アイテム ID とアイテム名を使って csv ファイルを作成します。

4. （オプション）大量のインターフェースにエイリアス名を設定するには、以下のコマンドを入力してバッチ サイズを調整し、バッチ間で一時停止させます。 このような調整は、作業負荷の制御に役立ちます。

   ```
   ./update_alias_name.sh -h host_name -u username -p password -T interface -i input_file -b batch_size –t time_in_seconds
   ```

–b *batch_size*

各バッチで処理するアイテムの数を示します。

デフォルト： 10000

-i パラメータが設定されていない場合のデフォルト： 150

–t *time_in_seconds*

バッチ間で一時停止する時間（秒単位）を示します。

デフォルト： 1

-i パラメータが設定されていない場合のデフォルト： 1

以下に例を示します。

```
./update_alias_name.sh -h host_name -u username -p password -T interface -i
input_file -b 20 –t 2
```

例: コンポーネントへのエイリアス名の設定

1. Data Aggregator ホストによって監視されているコンポーネントの完全なリストを返すには、以下のコマンドを入力します。

```
./update_alias_name.sh -h host_name -u username -p password -T item_type [-o
output_filename]
```

-h *host_name*

接続先の CA Performance Center ホスト名を指定します。

-u *username*

エイリアス名を設定する CA Performance Center 管理者のユーザ名を指定します。

-p *password*

エイリアス名を設定する CA Performance Center 管理者のパスワードを指定します。

-T *item_type*

エイリアス名を設定するアイテムのタイプを指定します。 有効な値はデバイス、インターフェースまたはコンポーネントです。

デフォルト： device

コンポーネントを指定します。

-o *output_filename*

（オプション）デバイス アイテム ID、コンポーネント アイテム ID、およびコンポーネント名別コンポーネントの総数を含む .csv ファイルをデフォルトのファイル名とは異なるファイル名で作成します。 このパラメータの値を入力しない場合、.csv ファイルにはデフォルト名 ComponentList.csv が使用されます。

.csv ファイルの形式は、「デバイス アイテム ID, コンポーネント アイテム ID, コンポーネント名」となります。

以下に例を示します。

565, 166, MyComponent1

566, 167, MyComponent2

2. コンポーネントごとに設定するエイリアス名に注意しながら、前の手順で作成された .csv ファイルを変更します。 このファイルの形式は、「デバイス アイテム ID、コンポーネント アイテム ID、コンポーネント エイリアス名」である必要があります。

   注: .csv ファイルのアイテム ID が無効な場合、エラー メッセージは表示されません。 これらの無効なエントリは無視されます。

   以下に例を示します。

   565、166、MyComponent1AliasDisplayName

   566、167、MyComponent2AliasDisplayName

   注: カンマおよびスペースは .csv ファイルの［エイリアス名］フィールドで使用できます。

3. 以下のコマンドを入力します。

   ```
   ./update_alias_name.sh -h host_name -u username -p password -T component -i input_file
   ```

   -i *input_file*

   以前にエイリアス名を使用して作成した .csv ファイルのファイル名を指定します。

   エイリアス名はコンポーネントに対して設定されます。

4. （オプション）大量のコンポーネントにエイリアス名を設定するには、以下のコマンドを入力してバッチ サイズを調整し、バッチ間で一時停止させます。 このような調整は、作業負荷の制御に役立ちます。

   ```
   ./update_alias_name.sh -h host_name -T component -i input_file -b batch_size –t time_in_seconds
   ```

–b *batch_size*

各バッチで処理するアイテムの数を示します。

デフォルト： 10000

-i パラメータが設定されていない場合のデフォルト： 150

–t *time_in_seconds*

バッチ間で一時停止する時間（秒単位）を示します。

デフォルト： 1

-i パラメータが設定されていない場合のデフォルト： 1

以下に例を示します。

```
./update_alias_name.sh -h host_name -u username -p password -T component -i
input_file -b 20 –t 2
```

詳細:

IP ドメインの追加 (P. 49)

ダッシュボードおよびレポート

ダッシュボードは、CA Performance Center ユーザ インターフェース内で動的にレポートを作成するページです。 これらは、［ダッシュボード］タブからアクセス可能なメニュー アイテムとして表示されます。 各ダッシュボードは、単一の Web ページ上の登録済みのデータ ソースからのデータを表示するビューのコレクションです。 各ダッシュボードのレイアウト、ビュー、時間間隔、およびグループ コンテキストは、カスタマイズできます。

注: ユーザ アカウントの役割の権限によって、表示できるダッシュボードが決まります。

レポートは、オン デマンドで選択した内容またはエクスポートされたダッシュボード ページからの静的な出力です。 ダッシュボードからエクスポートしたレポートは、関連するダッシュボードにデータおよび情報から静的なデータ セットを作成します。 オン デマンドのレポートは、インベントリ内の単一の管理対象アイテムまたはそのグループからのデータ セットをキャプチャします。 レポートは、印刷、電子メールでの送信、PDF や CSV 形式でのエクスポートなどが可能です。 各形式に対して、選択したデータ セットがキャプチャされます。

ダッシュボードはメニューで体系化されています。 メニューとは、ダッシュボードをコンテンツによって構成するために使用する［ダッシュボード］タブのセグメントです。 デフォルトでは、管理者とデザイナがメニューをカスタマイズし、それらをユーザ アカウント役割に割り当てることができます。

CA Performance Center には、一連のファクトリ ダッシュボードおよびメニューが用意されています。これは、データ ソースを登録した直後に使用できるようになっています。 必要な役割の権限を備えているユーザは、ダッシュボード、メニュー、およびビューを広範にカスタマイズして、個々のオペレータに対するカスタム システムを作成することもできます。

使用できるメニューおよびダッシュボードは、［ダッシュボード］タブにマウスを置いた場合、［ダッシュボード］タブをクリックしたときに表示されます。

レポート ページのタイプ

ダッシュボードの 2 つのカテゴリは、デフォルトで、またはカスタマイズを通じて使用可能です。

- *サマリ ページ*は、管理対象アイテムのグループの平均など高レベル情報を提供します。サマリ ダッシュボードは、選択されたコンテキストに関連する、より詳細なページへのドリル ダウン パスをしばしば提供します。
- *コンテキスト ページ*は、単一のルータまたはサーバなど絞り込んだコンテキストから特定の焦点を絞ったパフォーマンスまたはステータス データを提供します。 これらのページは、［サマリ］ダッシュボードのドリル ダウン リンクまたはタブから利用可能です。

サマリ ダッシュボードの詳細ビューへドリル インするには、以下の手順のいずれかを実行します。

- アイテムを右クリックして、表示するコンテキスト ページを選択します。
- アイテムをクリックして、デフォルトのコンテキスト ページを開きます。

注: 役割権限 (P. 118)には、ビューにドリル ダウンする機能が含まれている必要があります。

コンテキスト ページのデフォルト セットは、個々のデバイス、インターフェース、およびサーバに対して利用可能です。 これらのページにはカスタマイズ可能なタブのセットが含まれており、これを使用して、選択した管理対象アイテムの特定のコンテキスト データへアクセスすることができます。 たとえば、ルータのコンテキストには、［ヘルス］、［使用率］、［エラー］のデータ タブが含まれます。

ダッシュボードをユーザの［ホーム ページ］に設定

デフォルトでは、ログインすると、CA Performance Center が以下のいずれかのダッシュボードに表示されます。

- ［マイ ダッシュボード］のリストの先頭にあるダッシュボード
- ［インフラストラクチャ概要］ダッシュボード（製品購入時のデフォルト）

別のダッシュボード、*ホーム ページ*を設定して、ログインしたときに表示できます。 このホーム ページには、CA Performance Center コンソール内の別の場所から簡単に戻れます。

次の手順に従ってください:

1. ホーム ページとして設定するダッシュボードに移動します。
2. （*オプション*）ダッシュボードに対してグループ コンテキストを設定するには［変更］リンクをクリックします。 ホーム ページには、このコンテキストが記憶されます。
3. ［詳細］-［ホーム ページとして設定］をクリックします。

4. 確認のダイアログ ボックスで［はい］をクリックします。

   選択されたダッシュボードがホーム ページに設定されます。

5. コンソール内の別の場所からホーム ページに戻るには、コンソール ウィンドウの左上にある CA ロゴをクリックします。

注:

- ダッシュボードと関連付けられているグループをユーザの権限セットから削除した場合、ホーム ページにはユーザのデフォルト権限グループが使用されます。
- ユーザがログオンした、または CA ロゴをクリックした場合、ダッシュボードのビューが非表示であるかどうかを通知するエラー メッセージが表示されます。

コンテキスト ページの変更

*コンテキスト ページ*は、単一のルータまたはサーバなど絞り込んだコンテキストから特定の焦点を絞ったパフォーマンスまたはステータス データを提供します。 これらのページは、［サマリ］ダッシュボードのドリル ダウン リンクまたはタブから利用可能です。

ユーザ アカウントに「コンテキスト ページの編集」および「ビューへのドリル イン」の役割の権限がある場合、コンテキスト ページをカスタマイズできます。事前定義済みの管理者およびデザイナの役割には、デフォルトでこれらの役割の権限があります。

コンテキスト ページでデータ ビューが含まれるタブ ページを追加または削除できます。事前定義済みのタブを編集して、タブに表示されるビューを変更できます。 また、タブを再配置して表示順序を変更することもできます。 ［タブをデフォルトにリストア］を選択すると、現在のコンテキストのすべてのタブに対する変更が元に戻ります。 すべての変更は、現在のテナントに保存されます。

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 (P. 118)を持つユーザとしてログインします。

2. 編集対象のページのアイテム コンテキストに移動します。 たとえば、任意のダッシュボード上のルータのリンクをクリックして、[ルータ] コンテキスト ページを呼び出します。 または、インベントリ ページ上のアイテムをクリックして、アイテム コンテキストに直接移動します。

   デフォルトでは、左側の最初のタブが選択されています。 選択されているタブには [編集] アイコンが含まれており、[編集] メニューにアクセスできます。

3. [編集] をクリックします。
4. 以下のオプションから選択します。

タブの編集

選択されたタブに対する新しいビューを選択し、ビューのアイテム コンテキストを変更できます。

タブの削除

選択したタブをリストから削除できます。

重要: [元に戻す] などのリストア機能は利用できません。 削除したタブは、必要に応じて手動でリストアする必要があります。

タブの追加

タブを作成するオプションにアクセスできます。

タブの並べ替え

既存のタブの表示順序を変更できます。

詳細情報:

コンテキスト ページの追加または編集 (P. 213)
コンテキスト タブの作成 (P. 215)
コンテキスト タブの再配置 (P. 216)

コンテキスト ページの追加または編集

ユーザ アカウントに「コンテキスト ページの編集」および「ビューへのドリル イン」の役割の権限がある場合、コンテキスト ページをカスタマイズできます。事前定義済みの管理者およびデザイナの役割には、デフォルトでこれらの役割の権限があります。

標準的なダッシュボード ページとは異なり、アイテム コンテキスト ページはタブ ページのセットから構成されます。 事前定義済みのタブを編集して、タブに表示されるビューを変更できます。 タブ ページを追加できます。 また、アイテム コンテキスト内のタブを再配置して、表示順序を変更することもできます。 ［タブの編集］メニューから［タブをデフォルトにリストア］を選択すると、現在のコンテキスト内のタブの変更がすべて元に戻ります。

変更は現在のテナントに適用されます。

次の手順に従ってください:

1. 必要な役割の権限 (P. 118) を持つユーザとしてログインします。
2. 編集対象のページのアイテム コンテキストに移動します。 たとえば、任意のダッシュボード上のルータのリンクをクリックして、［ルータ］コンテキスト ページを呼び出します。

   選択されているタブには［編集］アイコンが含まれており、［編集］メニューにアクセスできます。

3. 変更するタブを選択します。

   ［編集］アイコンが表示されます。

4. ［編集］アイコンをクリックし、［タブの追加］または［タブの編集］を選択します。

5. （オプション）メニューから［デフォルト タブ テンプレート］の 1 つを選択します。 各テンプレートは、そのタイプのページに対するデフォルト ビューをページに適用します。

6. タブ タイトルを変更します。 タイトルは必須です。

   タブ タイトルは、タブを含むコンテキスト ページの一番上に表示される名前です。

7. ［レイアウト］ボタンで、ページ用のレイアウト テンプレートを選択します。

8. 必要に応じて、ページから不要なビューを削除します。［レイアウト］ペインで、以下の操作を実行します。

   - ［レイアウトのクリア］をクリックして、ページ上のビューの位置を変更します。
   - ［X］をクリックして、ページから個別のビューを削除します。

   ページに追加可能なビューが、カテゴリ別のリストに表示されます。このリストは選択されたグループまたはアイテム コンテキストでフィルタされます。

   登録済みのすべてのデータ ソースが表示されます。ただし、使用可能なビューは、コンテキストに適用可能なビューに制限されています。

   注: ページのアイテム コンテキストは変更できません。現在のコンテキストに対して事前選択されています。

9. ビューのカテゴリをクリックして展開します。

10. ビューを選択して、［レイアウト］ペインにドラッグし、表示する場所にドロップします。

11. ［保存］をクリックします。

    コンテキスト ページがリフレッシュして変更が反映されます。変更はログイン セッションを通じて保持されますが、現在のテナントのみに適用されます。

コンテキスト タブの作成

ユーザ アカウントに「コンテキスト ページの編集」および「ビューへのドリル イン」の役割の権限がある場合、コンテキスト ページを作成できます。 事前定義済みの管理者およびデザイナの役割には、デフォルトでこれらの役割の権限があります。

注: 「ダッシュボードの作成」の役割の権限は、コンテキスト タブの作成には必須ではありません。

標準的なダッシュボード ページとは異なり、アイテム コンテキスト ページはタブ ページのセットから構成されます。 コンテキスト タブを追加すると、新規タブ ページがアイテム コンテキストに表示されます。 現在のテナントに関連付けられたユーザのみが、この新規タブを参照できます。

次の手順に従ってください:

1. 必要な役割の権限 (P. 118)を持つユーザとしてログインします。
2. ページを追加するアイテム コンテキストに移動します。たとえば、任意のダッシュボード上のルータのリンクをクリックして、［ルータ］コンテキスト ページを呼び出します。

   デフォルトでは、左側の最初のタブが選択されています。 選択されているタブには［編集］アイコンが含まれており、［編集］メニューにアクセスできます。
3. ［編集］アイコンをクリックし、［タブの追加］を選択します。
4. 必要に応じてタブ タイトルを変更します。

   タブ タイトルは、タブを含むコンテキスト ページの一番上に表示される名前です。

5. ［レイアウト］ボタンで、ページ用のレイアウト テンプレートを選択します。
6. 必要に応じて、ページから不要なビューを削除します。［レイアウト］ペインで、以下の操作を実行します。
   - ［レイアウトのクリア］をクリックして、ページ上のビューの位置を変更します。
   - ［X］をクリックして、ページから個別のビューを削除します。

   ページに追加可能なビューが、カテゴリ別のリストに表示されます。このリストは選択されたグループまたはアイテム コンテキストでフィルタされます。

   登録済みのすべてのデータ ソースが表示されます。

   注: ページのアイテム コンテキストは変更できません。現在のコンテキストに対して事前選択されています。
7. ビューのカテゴリをクリックして展開します。
8. ビューを選択して、［レイアウト］ペインにドラッグし、表示する場所にドロップします。
9. ［保存］をクリックします。

   コンテキスト ページがリフレッシュして新しいタブが含まれます。変更はログイン セッション間で保持されます。

コンテキスト タブの再配置

ユーザ アカウントに「コンテキスト ページの編集」および「ビューへのドリル イン」の役割の権限がある場合、コンテキスト ページをカスタマイズできます。事前定義済みの管理者およびデザイナの役割には、デフォルトでこれらの役割の権限があります。

各アイテム コンテキストは、タブ ページのセットから構成されます。 個別のタブ ページの変更に加えて、アイテム コンテキスト内のタブを再配置して表示順序を変更できます。 変更は現在のテナントのみに保存されます。

次の手順に従ってください:

1. 必要な役割の権限 (P. 118)を持つユーザとしてログインします。

2. 編集対象のページのアイテム コンテキストに移動します。 たとえば、任意のダッシュボード上のルータのリンクをクリックして、［ルータ］コンテキスト ページを呼び出します。

   選択されているタブには［編集］アイコンが含まれており、［編集］メニューにアクセスできます。デフォルトでは左側の最初のタブが選択されています。

3. ［編集］アイコンをクリックし、［タブの並べ替え］を選択します。

   ［タブの並べ替え］ダイアログ ボックスに、［現在のコンテキスト ページ タブ］リストが表示されます。

   このリストでは、左から右への現在のタブ順序が反映されています。

4. 移動するタブを選択し、リスト内の別の場所にドラッグします。

5. ［保存］をクリックします。

   コンテキスト ページがリフレッシュして変更が反映されます。タブは左から右に新しい順序で表示されます。

   コンテキストで利用可能なタブが多数あり、表示するのに水平スクロールが必要な場合は、右側に矢印が表示されます。 追加のタブを参照するには矢印をクリックします。

オンデマンド レポート

オンデマンド機能を使用して、選択したグループ、デバイス、またはインターフェースのメトリックをすぐに確認できます。 オンデマンド トレンド レポートは、管理対象アイテムまたはアイテム グループの徹底的な調査を行う際に役立ちます。

オンデマンド レポートには、［インベントリ］ページ、検索結果ページ、または［オンデマンド レポート テンプレートの管理 (P. 223)］ページからアクセスできます。

［インベントリ］ページと検索ページには、ユーザ アカウントの権限グループに含まれているアイテムのみが表示されます。 トレンド レポートに使用する管理対象アイテムを選択し、［オンデマンド］をクリックします。 次に、追加アイテム、メトリック、グラフの形式など、レポートの設定を選択します。

注: ［インベントリ］を表示してグローバル検索を実行する機能は、それらの役割を持った個別のオペレータに許可されます。 ［インベントリと検索の表示］役割の権限を持ったユーザのみに、［インベントリ］タブが表示されます。 このためオンデマンド レポートを有効化するには、この役割の権限 (P. 118)が必要です。

オンデマンドのトレンド レポートが生成された後、他ユーザと結果を共有するための出力形式を選択できます。 共有を有効化するには、レポートを印刷する、およびレポートを電子メールで送信するための役割の権限が必要です。

オンデマンド レポートの生成

何らかの役割を持つユーザは、オンデマンドのトレンド レポートを生成して、絞り込まれたコンテキストから静的データ セットを表示することができます。 オンデマンド レポートは徹底的な調査および、トラブルシューティングに使用します。

オンデマンド レポートの生成は、［インベントリ］ページまたは検索結果のページから開始できます。

次の手順に従ってください:

1. ［インベントリ］タブを選択し、デバイスなどのアイテム タイプをクリックします。
2. レポートに含める管理対象アイテムを見つけます。 または、アイテムの検索を実行し、結果からアイテムを見つけます。
3. アイテムの隣にあるチェック ボックスをオンにして、［オンデマンド］をクリックします。

   設定ダイアログ ボックスが開きます。

   重要: すべての設定オプションを表示するには、ダイアログ ボックスの右側のスクロール バーを使用します。
4. （オプション）デフォルトのビュー タイトルを変更します。タイトルがビューに表示されます。このタイトルはレポートにも表示されます。
5. オンデマンド レポートの名前を指定します。この名前は［オンデマンド レポート テンプレート］リスト内のレポートを特定するもので、レポートのタイトルとして表示されます。
6. （オプション）レポートの説明を指定します。

7. ［ビューのタイプ］オプションを選択します。 これらのオプションにより、グラフの形式が決定されます。 以下のオプションから選択します。

   - **複数メトリックを持つチャート**： このビューは、選択した各メトリックのトレンド ラインを表示する 1 つのチャートから構成されます。
   - **メトリックごとのチャート**： このビューは、選択したメトリックごとの 1 つのチャートから構成されます。各チャートは、メトリックのトレンド ラインを表示します。
   - **複数メトリックを持つアイテムごとのチャート**： このビューは、選択したアイテムまたはグループごとに 1 つのチャートから構成されます。 各チャートは、選択したメトリックごとのトレンド ラインを表示します。
   - **複数アイテムを持つメトリックごとのチャート**： このビューは、選択したメトリックごとの 1 つのチャートから構成されます。 各チャートは、選択したアイテムまたはグループごとのトレンド ラインを表示します。

   ［ビュー タイプ］オプションの詳細については、「オンデマンド レポート オプション (P. 222)」を参照してください。

8. ［間隔］オプションを選択します。

   ［間隔］は、グラフ内の各データ ポイントが表す時間です。

9. （オプション）レポートに含める別の管理対象アイテムを選択します。 以下の手順を実行します。

   a. ［アイテムの追加］をクリックします。

   b. ［アイテムの追加/削除］をクリックします。

      （オプション）ダイアログ ボックスで、［コンテキスト タイプ］を変更できます。

      注: 最初の選択を行った後で、アイテム コンテキストを変更すると、元の選択内容はクリアされます。 詳細については、「オンデマンド レポート オプション (P. 222)」を参照してください。

c. リストから管理対象アイテムを選択し、［追加］をクリックします。 最大で 15 アイテムまで追加します。

注: 権限グループに含まれている管理対象アイテムのみが表示されます。

選択したアイテムが、［選択された <アイテム>］ペインに表示されます。

d. ［OK］をクリックして、［ビュー設定］ダイアログ ボックスに戻ります。

選択したアイテムが、含めるアイテムのリストに表示されます。これらのアイテムのみで、パフォーマンス データのクエリが実行されます。

10. （オプション）レポートに含めるグループを選択します。 以下の手順を実行します。

a. ［グループの追加］をクリックします。

b. ［グループの追加/削除］をクリックし、グループ ツリーを表示します。 ダイアログ ボックスがフィルタリングされ、権限グループに含まれるグループのみが表示されます。

c. グループ ツリー内のノードをクリックして展開します。

d. グループをクリックして選択してから右方向矢印をクリックし、グループを［選択したグループ］ペインに移動します。 最大 15 グループまで追加できます。

注: アイテムまたはグループを削除するには、［追加/削除］ボタンをクリックして［アイテムの追加/削除］または［グループの追加/削除］ダイアログ ボックスに戻ります。［選択済み］ペインでアイテムまたはグループを選択して、［削除］をクリックします。

重要: ［コレクション］カテゴリにあるグループは含めることができません。［コレクション］グループは、現在レポートに含めることはできません。

11. ［OK］をクリックします。
12. （オプション）［メトリック計算レベル］ペインで、集計データを計算する方法（［グループ別］、［デバイス別］、または［コンポーネント別］）を選択します。［ビュー タイプ］フィールドで「複数メトリックを持つアイテムごとのチャート」または「複数アイテムを持つメトリックごとのチャート」が選択されている場合にのみ、このオプションは使用できます。
13. レポートに表示するメトリックを選択します。以下の手順を実行します。
    a. ［使用可能メトリック］画面内のフォルダをクリックして展開します。各フォルダはメトリック ファミリを表します。たとえば、使用可能な CPU 統計を表示するには、「CPU」メトリック ファミリを選択します。
    b. 個々のメトリックをクリックして選択します。最大 15 個までのメトリックを選択できます。

       注: リストには、選択したアイテムに適用するメトリックのみが表示されます。
    c. 矢印をクリックして、選択内容を［選択されたメトリック］画面に移動します。
14. ［変更を適用］ドロップダウンから変更の範囲を選択します。以下のいずれかのオプションを選択します。
    - マイ ユーザ アカウント: このユーザ アカウントに限定してレポートを保存します。
    - すべてのテナント ユーザ用 : テナント（通常はデフォルト テナント）に関連付けられたユーザのみが使用できるようにレポートを保存します。

    注: これらのオプションが使用できるかどうかはユーザ アカウントの役割の権限に依存します。
15. （オプション）レポートをプレビューするには、［実行］ボタンをクリックします。

    プレビュー ダッシュボードには、選択したビュー形式が表示されます。
16. レポート テンプレートを保存するには、プレビュー ページにあるツールバー上の［保存］リンクをクリックします。

    ［設定］ダイアログ ボックスが表示され、保存する前に再度変更できます。

保存したレポート テンプレートは、［オンデマンド レポート テンプレートの管理］ページのリストに表示されます。

17. レポートをエクスポートするには、［印刷］アイコンまたは［電子メール］アイコン、または［編集］アイコンをクリックします（CSV にエクスポートする場合）。

オンデマンド レポートのオプション

オンデマンド レポート テンプレートを作成すると、複数のオプションを使用して、生成されるレポートに含めるチャートの数および外観を選択することができます。

ビュー オプションでは、オンデマンド レポートでデータを表示する方法を決定します。 レポートの設定時には、レポートするアイテムまたはグループを複数選択できます。 ビュー オプションは、選択されたすべての管理対象のアイテムまたはグループから、選択されるすべてのメトリック ファミリをチャートでどのように表現するかを決定します。 グループ ロールアップ データは集計トレンド ラインによって表されます。

以下のオプションを使用できます。

- **複数メトリックを持つチャート**： このビューは、選択した各メトリックのトレンド ラインを表示する 1 つのチャートから構成されます。トレンド ラインを区別するためにさまざまな色が使用されます。
- **メトリックごとのチャート**： このビューは、選択したメトリックごとの 1 つのチャートから構成されます。 各チャートは、メトリックのトレンド ラインを表示します。
- **複数メトリックを持つアイテムごとのチャート**： このビューは、選択したアイテムまたはグループごとに 1 つのチャートから構成されます。各チャートは、選択したすべてのメトリックのトレンド ラインを表示します。

  メトリック ファミリの中には、複数のデバイス コンポーネントについて自動的にレポートするものがあります。 たとえば、CPU メトリック ファミリは、管理対象デバイス上で検出された、すべての CPU からのデータをレポートします。 これらの場合は、CPU ごとに別々のチャートが作成されます。
- **複数アイテムを持つメトリックごとのチャート**： このビューは、選択したメトリックごとの 1 つのチャートから構成されます。 各チャートは、選択したそれぞれのアイテムのトレンド ラインを表示します。

注: グループはレポートにおいて個別のアイテムとして表されます。データは各グループ内のすべての管理対象アイテムからロールアップされます。

互いを補足し合う管理対象アイテムとメトリック ファミリを選択するように注意します。 最初の選択を行った後で、アイテム コンテキストを変更すると、元の選択内容はクリアされます。 たとえば、レポート対象として 3 つのルータを選択してから、インターフェースを追加した場合、ルータはクリアされます。 レポートはインターフェース データを反映しますが、ルータ レベルにはロールアップしません。

ただし、その他のデバイス タイプとコンポーネントは、単一のオンデマンド レポートでレポートされる場合、互換性があります。たとえば、ルータとサーバは同じレポートに含めることができます。

また、オプションの特定の組み合わせで必要になる処理量に注意します。多数の管理対象アイテムが含まれるグループでは、特に各アイテムのグラフが必要になるオプションを選択した場合には、大量の処理が必要になります。 さらに、CPU やメモリなどのコンポーネント メトリックのレポートを選択すると、この状況は悪化します。 たとえば、200 のルータが含まれるグループについてレポートを作成しようとし、［ビュー タイプ］として［複数メトリックを持つアイテムごとのチャート］を選択します。そして、［含めるメトリック］リストから CPU メトリックを選択し、［メトリック計算レベル］を［コンポーネント別］に変更した場合、このビューでは、このグループ内のすべてのルータに含まれるすべての CPU から CPU データを取得しようと Data Aggregator にクエリが送信されます。 さらに、レポートが完全に生成されるまでに 200 のグラフがレンダリングされる必要があります。

レポート テンプレートのリストの表示

［オン デマンド レポート テンプレートの管理］ページには、再利用可能なレポート定義のリストが表示されます。 事前定義済みのレポートはありません。ユーザがオンデマンド レポートを作成していない場合、リストは空です。

ユーザがオンデマンド レポートを作成すると、各レポート テンプレートの主要な機能がリスト表示されます。 オンデマンド レポートを作成するには［新規］をクリックします。

デフォルトでは、ユーザのテナント内で作成されたレポートと同様、作成したレポートの表示、生成、変更が可能です。［マイ レポート］をクリックすると、リストがフィルタされ、作成したレポートのみが表示されます。

次の手順に従ってください:

1. 「レポートの管理」または「レポートの実行」の役割の権限 (P. 118)のいずれかを持ったユーザとしてログインします。
2. ［レポート］を選択し、［オン デマンド レポート テンプレート］をクリックします。

   ［オン デマンド レポート テンプレートの管理］ページが表示されます。

   このページには、現在のレポートのリストが表示されます。 オンデマンド レポートが作成されていない場合、リストは空になっています。

   各レポートには、以下の情報がリスト表示されます。

   名前

   レポート（指定したタイトル）を識別します。

   説明

   レポートの説明です。

   作成日

   レポートの作成日時が表示されます。

   最終変更

   テンプレートの最終変更日時が表示されます。

   所有者

   このレポート テンプレートの所有者（オンデマンド レポートの作成者）であるユーザ アカウントのユーザ名を示します。 レポートを変更または生成するときは、このユーザの許可が必要です。 レポート テンプレートを削除できるのは所有者のみです。

   テナントが作成されていない場合は、すべてのユーザがリスト内のレポートを表示できます。 グローバル管理者は、テナントに明示的に関連付けられていないレポート（すなわち、デフォルト テナントに関連付けられているレポート）のリストを表示できます。 テナント管理者は、自身のテナントに関連付けられたアイテムのみを表示できます。

詳細:

オンデマンド レポートの生成 (P. 218)

ビュー オプション

多くのビューが、検索機能とビューを変更可能なその他の設定を備えています。 ほとんどのデータ ビューで、フィルタリングとタイム フレームオプションに加えて、以下のオプションを使用できます。

- タイトルや重大度カテゴリの変更など、ビュー設定の編集  。
- テーブル ビューの別の「ページ」を選択することによる、より多くのデータの参照。
- 「ページ」単位で表示されるアイテム数の増減。
- データが非表示になるようにするためのビューの折り畳み。
- ビューに表示されるデータに関する管理対象アイテム コンテキストの変更。

  注: 「共有ビューへの変更の保存」の役割の権限 (P. 118)を持つユーザは、ビューの変更を自身のユーザ アカウントに保存できます。 この変更はログアウト後も残ります。 ただし、他のユーザはビューに対する変更を参照できません。

その他のビュー オプションは選択されたビューによって異なります。 利用可能なオプションは形式とデータ ソースに依存します。

トレンド ビュー オプション

コンテキスト ページで利用可能なトレンド ビューでは、グラフに表示されるトレンド ラインを迅速かつ簡単に変更できます。 マルチトレンド ビューには、以下のオプションも適用されます。

- グラフの凡例内のメトリックを右クリックし、［非表示］を選択してビューから削除します。
- 他のすべてのメトリックを除外するには、凡例内のメトリックを右クリックして［フォーカス］を選択します。
- ズーム機能を使用して、正確なタイムフレームにフォーカスを絞り込みます。

トレンド ビューには、パフォーマンス レベルまたはしきい値を視覚的に表示するために「目標ライン」を追加するオプションもあります。 目標ラインの値やラベルを指定できます。また、選択されたトレンド ビューで目標ラインの表示/非表示を設定できます。

テーブル ビュー オプション

テーブル ビューでは、個々のアイテムの詳細データにドリルダウンできます。 長いアイテム リストからメトリックを参照するには、ページ機能を使用します。ビューのサイズ、および 1 ページ当たりのテーブル行数を増やすには、［1 ページあたりの最大数］の値を増加させます。

テーブルのデータ列を選択したメトリックで並べ替えたり、含める列を選択することもできます。 並べ替えるテーブル列をクリックします。 列の上にある白い矢印を使用して、テーブル列オプションのメニューにアクセスできます。 列を選択して、デフォルトでテーブルで有効になっているメトリックを有効または無効にします。

ブラウザ ビュー オプション

ブラウザ ビューは、選択したレポート ページに任意の URL を追加できる一意のビュー タイプです。このビューを使用して、ネットワーク パフォーマンス ビューと共に外部要因を比較できます。 また、ブラウザ ビューによって、内部および外部データを動的に更新できます。

世界の出来事、悪天候などの複数の外部要因は、ネットワークおよびサーバのパフォーマンスに影響を及ぼす場合があります。 単一のレポート ページに、パフォーマンス データ ビューと共に天気図とニュース ヘッドラインを並べて表示する機能により、ネットワーク パフォーマンスのパターンをよりよく理解することができます。

デバイス管理オプション

ビューに Data Aggregator のデータが表示されない場合、このオプションを使用して Data Aggregator の［管理］ページに直接ドリルダウンし、監視対象のデバイスおよびアイテムのトラブルシューティングを行うことができます。