NetIQ Directory and Resource Administrator ユーザーガイド

2021 年 6 月

保証と著作権

保証と著作権、商標、免責事項、保証、輸出およびその他の使用制限、米国政府の規制による権利、特許ポリシー、および FIPS コンプライアンスの詳細については、https://www.microfocus.com/about/legal/ を参照してください。

目次

本書の内容

この『*ユーザガイド*』は、NetIQ Directory and Resource Administrator (DRA) という製品について概説します。本書では、用語とさまざまな関連する概念について定義しています。

本書の読者

本書は、管理に関する概念を理解し、安全な分散管理モデルを実装する担当者を対象とします。

その他のマニュアル

本書は、Directory and Resource Administrator のマニュアルセットの一部です。このガイドの最新バージョンおよびその他の DRA 関連のドキュメントリソースについては、NetIQ DRA マニュアルの Web サイト (https://www.netiq.com/documentation/directory-and-resource-administrator/index.html) を参照してください。

連絡先情報

本書またはこの製品に付属するその他のドキュメントについて、お客様のご意見やご提案をお待ちしています。オンラインヘルプの各ページの下部にある **[comment on this topic (このトピックに関するコメント)]** リンクを使用するか、または Documentation-Feedback@microfocus.com に電子メールを送信してください。

特定の製品の問題については、Micro Focus ご注文と配送 (https://www.microfocus.com/support-and-services/) にお問い合せください。

1 はじめに

NetIQ Directory and Resource Administrator(DRA) で Active Directory のオブジェクト管理を始める前に、DRA の動作の基本理念と、製品アーキテクチャにおける各 DRA コンポーネントの役割について理解しておく必要があります。

Directory and Resource Administrator とは

NetIQ Directory and Resource Administrator は、Microsoft Active Directory(AD) の安全で効率的な特権 ID 管理を可能にします。DRA では、「最小特権」を細かく委任することで、管理者およびユーザが特定の責務に必要なパーミッションだけが付与されるようにします。また、DRA は、ポリシーの遵守を徹底し、詳細なアクティビティの監査およびレポーティングを提供し、IT プロセスの自動化によって繰り返しの作業を簡素化します。これらの各機能により、特権昇格、エラー、悪意のあるアクティビティ、規制違反などのリスクから顧客の AD および Exchange の環境を保護できるだけでなく、ユーザ、ビジネスマネージャ、ヘルプデスク担当者にセルフサービス機能を付与することで管理者の負担を軽減することができます。

また、DRA は Microsoft Exchange の強力な機能を拡張し、Exchange オブジェクトのシームレスな管理を実現します。DRA では、単一の共通ユーザインタフェースから、Microsoft Exchange 環境全体のメールボックス、パブリックフォルダ、および配布リストをポリシーベースで管理することができます。

Active Directory、Microsoft Windows、Microsoft Exchange、および Azure Active Directory の各環境の制御と管理に関する課題が DRA ですべて解決できます。

- **Azure とオンプレミスの Active Directory、Exchange、および Skype for Business に対するサポート :** Azure とオンプレミスの Active Directory、オンプレミスの Exchange Server、オンプレミスの Skype for Business、Exchange Online、および Skype for Business Online を管理できます。
- **ユーザおよび管理者の特権アクセスの細かい制御 :** 特許取得済みの ActiveView テクノロジにより、特定の責務に必要な権限だけを委任し、特権格上げを防止することができます。
- **カスタマイズ可能な Web コンソール :** 直観的な方法により、技術者でなくても、限定された (そして割り当てられた) 機能および権限を通して、簡単かつ安全に管理タスクを行えます。
- **詳細なアクティビティの監査およびレポーティング :** 製品で実行されたすべてのアクティビティが包括的に監査レコードに記録されます。長期データを安全に保管でき、AD へのアクセスを制御するためのプロセスを実施していることを監査機関 (PCI DSS、FISMA、HIPAA、NERC CIP など) に証明できます。

- **IT プロセスの自動化** : プロビジョニングや認証の取り消し、ユーザとメールボックスの操作、ポリシーの適用、セルフサービスタスクの制御など、さまざまなタスクのワークフローを自動化できます。これにより、ビジネスの効率を高め、手動で繰り返し行う管理作業を削減することができます。
- **運用上の完全性** : 管理者にきめ細かいアクセスコントロールを提供し、システムおよびリソースへのアクセスを管理することで、システムおよびサービスのパフォーマンスと可用性に影響する悪意のある変更や間違った変更を防止できます。
- **プロセスの適用** : 重要な変更管理プロセスの完全性を維持し、生産性の向上、エラーの減少、時間の節約、管理効率の向上に貢献します。
- **Change Guardian との統合** : DRA および Workflow Automation 機能とは無関係に Active Directory で生成されたイベントの監査を強化します。

Directory and Administrator のコンポーネントについて

特権アクセスの管理に一貫して使用される DRA のコンポーネントには、プライマリとセカンダリのサーバ、管理コンソール、レポートコンポーネント、およびワークフロープロセスを自動化するワークフローエンジンなどがあります。

次の表は、各タイプの DRA ユーザが使用する典型的なユーザインタフェースと管理サーバを示しています。

DRA ユーザのタイプ	ユーザインタフェース	管理サーバ
DRA 管理者 (本製品の構成を管理する人)	Delegation and Configuration Console (委任および環境設定コンソール)	プライマリサーバ
上級管理者	DRA Reporting PowerShell CLI DRA ADSI Provider	任意の DRA サーバ
ヘルプデスクの臨時管理者	Delegation and Configuration Console (委任および環境設定コンソール) の Account and Resource Management ノード Web コンソール	任意の DRA サーバ

DRA 管理サーバ

DRA 管理サーバは、構成データ (環境、委任されたアクセス、およびポリシー) を保管し、オペレータのタスクおよび自動化タスクを実行し、システム全体のアクティビティを監査します。このサーバは、コンソールおよび API レベルのクライアントをいくつかサポートしながらも、マルチマスタセット (MMS) のスケールアウトモデルにより、冗長性と地理的

分離に対しても高い可用性を実現できるように設計されています。このモデルでは、すべての DRA 環境に、複数のセカンダリ DRA 管理サーバと同期する 1 つのプライマリ DRA 管理サーバが必要になります。

Active Directory ドメインコントローラには管理サーバをインストールしないようにすることを強くお勧めします。DRA が管理するドメインごとに、管理サーバと同じサイトにドメインコントローラを 1 つ以上配置してください。デフォルトでは、管理サーバはすべての読み込み / 書き込み操作で最も近いドメインコントローラにアクセスします。そのため、パスワードリセットなどのサイト固有のタスクを実行する場合は、サイト固有のドメインコントローラを指定して操作を処理できます。ベストプラクティスとして、セカンダリ管理サーバ 1 台をレポーティング、バッチ処理、自動化されたワークロードのために専用で使用することを検討してください。

Account and Resource Management

Account and Resource Management は、Delegation and Configuration Console (委任および環境設定コンソール) のノードです。これを通じて DRA のアシスタント管理者が、接続されたドメインやサービスの委任オブジェクトを表示および管理することができます。

Web コンソール

Web コンソールは、Web ベースのユーザインタフェースです。これを通じて DRA のアシスタント管理者が、接続されたドメインやサービスの委任オブジェクトを素早く簡単に確認し、管理することができます。

管理者は、Web コンソールの外観と使用方法をカスタマイズして、カスタマイズした企業ブランドとカスタマイズしたオブジェクトプロパティを組み込むことができます。また、DRA の外部で行われた変更監査を可能にするために Change Guardian サーバとの統合を構成することもできます。

DRA 管理者は、自動ワークフローフォームを作成および変更して、トリガされたときにルーチンの自動タスクを実行することもできます。

Web コンソールには「統合された変更履歴」という機能もあります。この機能により変更履歴サーバとの統合が可能になり、DRA の外部で AD オブジェクトに対して行われた変更を監査することができます。変更履歴レポートのオプションには、次のものがあります。

- 次に対して行われた変更 ...
- 次によって行われた変更 ...
- 次によって作成されたメールボックス ...
- 次によって作成されたユーザ、グループ、および連絡先の電子メールアドレス ...
- 次によって削除されたユーザ、グループ、および連絡先の電子メールアドレス ...
- 次によって作成された仮想属性 ...
- 次によって移動されたオブジェクト ...

レポーティングコンポーネント

DRA Reporting には DRA 管理のためにカスタマイズ可能な標準のテンプレートが用意されており、DRA 管理対象ドメインおよびシステムの詳細が確認できます。

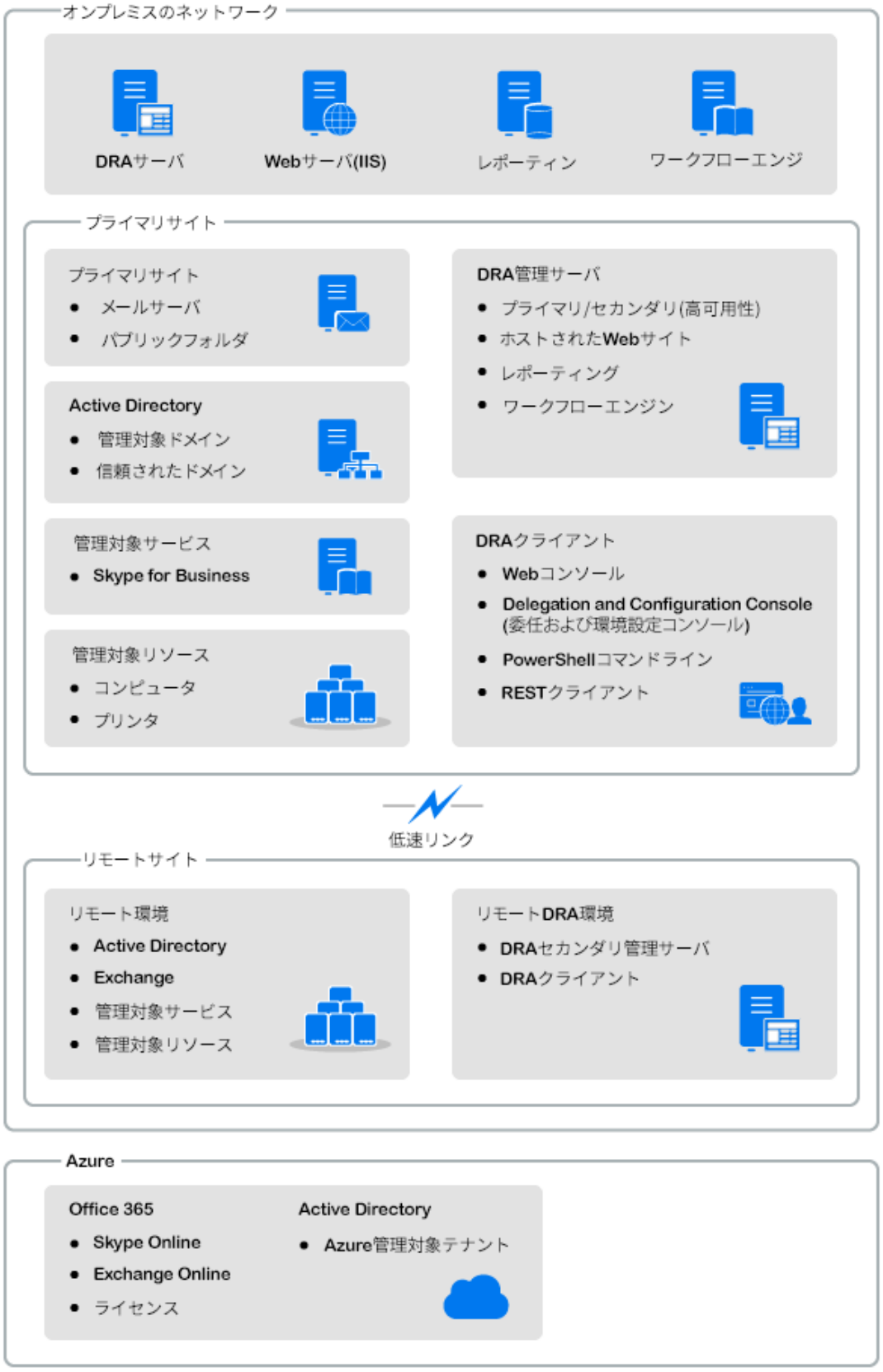
- AD オブジェクトのリソースレポート
- AD オブジェクトデータレポート
- AD サマリレポート
- DRA 構成レポート
- Exchange 構成レポート
- Office 365 Exchange Online レポート
- 詳細なアクティビティトレンドレポート (月別、ドメイン別、ピーク別)
- DRA アクティビティの要約レポート

DRA レポートは、SQL Server Reporting Services を使用してスケジュールおよび公開できるので、関係者に簡単に配布できます。

ワークフローエンジン

DRA はワークフローエンジンとの統合により、Web コンソールでワークフロータスクの自動化が可能です。アシスタント管理者がワークフローサーバの構成、カスタマイズされたワークフロー自動化フォームの実行、およびワークフローのステータスの表示を Web コンソールで行うことができます。ワークフローエンジンについての詳細は、NetIQ DRA マニュアルサイトで Workflow Automation のマニュアルを参照してください。

製品アーキテクチャ


オンプレミスのネットワーク
DRAサーバ
Webサーバ(IIS)
レポーティン
ワークフローエンジ
プライマリサイト
プライマリサイト
メールサーバ
パブリックフォルダ
Active Directory
管理対象ドメイン
信頼されたドメイン
管理対象サービス
Skype for Business
管理対象リソース
コンピュータ
プリンタ
DRA管理サーバ
プライマリ/セカンダリ(高可用性)
ホストされたWebサイト
レポーティング
ワークフローエンジン
DRAクライアント
Webコンソール
Delegation and Configuration Console (委任および環境設定コンソール)
PowerShellコマンドライン
RESTクライアント
低速リンク
リモートサイト
リモート環境
Active Directory
Exchange
管理対象サービス
管理対象リソース
リモートDRA環境
DRAセカンダリ管理サーバ
DRAクライアント
Azure
Office 365
Skype Online
Exchange Online
ライセンス
Active Directory
Azure管理対象テナント

2 ユーザインタフェースの使用

DRA のユーザインタフェースはさまざまな管理ニーズに対応しています。主なインタフェースは次のとおりです。

Web コンソール

Web ベースのインタフェースを通じて、アカウントおよびリソースに関する一般的な管理タスクを行うことができます。Web コンソールには、Internet Explorer、Chrome、または Firefox を実行している任意のコンピュータからアクセスできます。

PowerShell

PowerShell は、DRA 以外のクライアントでも PowerShell のコマンドレットを使って DRA の操作の要求を可能にするモジュールです。

NetIQ Reporting Center コンソール

管理レポートを表示し、展開することができます。これにより、企業セキュリティの監査および管理活動の追跡監視を行うことができます。管理レポートには、アクティビティレポート、環境設定レポート、および要約レポートなどがあります。これらのレポートは多くが図表形式で表示できます。

Web コンソール

Web コンソールは、ユーザアカウント、グループ、コンピュータ、リソース、Microsoft Exchange メールボックスに関する多くのタスクにすばやく簡単にアクセスできる Web ベースのユーザインタフェースです。オブジェクトのプロパティはカスタマイズ可能なため、繰り返し行う業務の効率を向上させることができます。また、所在地や携帯電話番号など、自分のユーザアカウントの一般プロパティを管理することもできます。

Web コンソールには、自分に実行権限があるタスクのみが表示されます。

- 16 ページの 「Web コンソールの起動」
- 17 ページの 「Web コンソールの設定」
- 20 ページの 「Web コンソールのカスタマイズ」
- 22 ページの 「Web コンソールでオブジェクトを管理する」
- 23 ページの 「変更履歴レポートの生成」
- 24 ページの 「Workflow Automation の使用」

Web コンソールの起動

Web コンソールは、次のいずれかのサポートされるブラウザを実行している任意のコンピュータから起動できます。

- Google Chrome
- Mozilla Firefox
- Microsoft Edge

Web コンソールを起動するには、Web ブラウザのアドレスフィールドで適切な URL を指定してください。たとえば、HOUserver というコンピュータに Web コンポーネントをインストールした場合、Web ブラウザのアドレスフィールドに「https://HOUserver.entDomain.com/draclient」と入力します。

注 : アカウントおよび Microsoft Exchange の最新情報を Web コンソールに表示するには、キャッシュされたページが更新されていないかどうかをアクセスのたびにチェックするように Web ブラウザを設定してください。

DRA サーバへの接続

3 つのオプションのいずれかを使用して、Web コンソールにログインできます。ログイン時の各オプションの振る舞いは次の表に示されています。

ログイン画面 - オプション	接続オプションの説明
自動ディスカバリの使用	DRA サーバを自動的に検出します。設定オプションはありません。
デフォルトの DRA サーバに接続する	事前設定済みのサーバおよびポートの詳細が使用されます。 **注 :** このオプションは、Web コンソールでデフォルトの DRA サーバを設定した場合にのみ表示されます。また、クライアントが常にデフォルトの DRA サーバに接続するように指定した場合は、ログイン画面で［**[デフォルトの DRA サーバに接続する]**］オプションのみを表示できます。
特定の DRA サーバに接続する	ユーザがサーバとポートを設定します。
特定のドメインを管理する DRA サーバに接続する	ユーザが管理対象ドメインを指定し、次の接続オプションから選択します。 ◆ 自動ディスカバリの使用 (指定のドメイン内) ◆ このドメインのプライマリサーバ ◆ DRA サーバの検索 (指定のドメイン内)

Web コンソールの設定

DRA の管理権限を持っている場合は、Advanced Authentication、クライアントのブランディングとセッション設定、および Web コンソールに必要なすべてのサーバ接続を設定できます。これらの設定にアクセスするには、Web コンソールにログインし、[**[管理]**] > [**[構成]**] に移動します。

注 : 必要な管理権限を持ってない場合は、マストヘッドの [**[管理]**] タブは表示されません。

- 17 ページの 「Advanced Authentication」
- 17 ページの 「Web コンソールのブランディング」
- 19 ページの 「クライアントセッションの設定」
- 19 ページの 「サーバ接続」

Advanced Authentication

Advanced Authentication では、ユーザ名とパスワードのみの単純な保護ではなく、多要素認証を使用することでより安全に機密情報を保護します。多要素認証とは、カテゴリの異なる資格情報に基づき、複数の認証方法でユーザが本人であることを確認することが求められる、コンピュータへのアクセスコントロールの 1 方式です。

DRA 管理者がチェーンとイベントを構成した後に、必要な権限を持つユーザが Web コンソールにログインして Advanced Authentication を有効にすることができます。認証が有効になると、Advanced Authentication による認証がすべてのユーザに求められ、その後に Web コンソールへのアクセス権が付与されます。

Advanced Authentication を有効にするには、[構成] タブから [**[Advanced Authentication]**] を選択し、[**[Advanced Authentication を有効にする]**] をクリックして、各フィールドに表示される指示に従ってフォームを設定します。

Advanced Authentication の詳細については、『*DRA 管理者ガイド*』の「「認証」」を参照してください。

Web コンソールのブランディング

次のように、DRA Web コンソールのログイン画面とマストヘッドをカスタマイズできます。

- **マストヘッド** : ログイン後の Web コンソールの上部にある高レベルのナビゲーションバーです。
  - *ロゴイメージまたは代替テキスト* : マストヘッドバーの左端に表示されます。ロゴイメージまたは代替テキストを表示できますが、両方表示することはできません。
  - *マストヘッドカラー* : ロゴイメージ領域を除き、この色でマストヘッド全体をオーバーレイします。

- **テーマ付きログイン画面** : ブラウザで Web コンソールの URL にアクセスしたときの、ログインページの表示方法。DRA テーマはデフォルトで設定および有効化されています。
  - *ロゴイメージまたは代替テキスト* : 製品タイトルおよび資格情報フィールドの上に表示されます。ロゴイメージまたは代替テキストを表示できますが、両方表示することはできません。
  - *アプリケーションタイトル* : 資格情報フィールドとロゴイメージの間に表示されます。
  - *通知モーダル* : ユーザが［ **[OK]**］をクリックするまでログインページをオーバーレイして覆い隠すメッセージボックスです。これは通常、コンソールへのアクセスが会社のセキュリティポリシーに従うことに同意することを意味することをユーザに通知するために使用されます。このオプションを一度有効にすると、Web コンソールにアクセスするユーザ全員にプロンプトが表示されます。

マストヘッドの設定

マストヘッドの設定を行うには、次の手順に従ってください。

1 Web コンソールにログインし、［ **[管理]**］>［ **[構成]**］>［ **[ブランディング]**］に移動します。

2 次のいずれかを実行します。テキストとイメージファイルの両方を追加すると、イメージだけが表示されます。
  - ロゴイメージの更新 :
    1. ［ **[マストヘッド]**］タイルの［ロゴイメージ］フィールドにファイル拡張子を含む保存したイメージファイル名を追加します。
    2. ロゴイメージを Web サーバの「アセット」ディレクトリに保存します。例 :

       C:\inetpub\wwwroot\DRAClient\assets

       最適なイメージサイズは 56x56 ピクセルです。
  - 必要に応じて、**[マストヘッド]** タイルの［ロゴ画像の代替テキスト］フィールドの既存のテキストに入力または上書きします。

3 ページの下部の［ **[保存]**］をクリックし、設定の変更を完了します。

ログイン画面の設定

次の手順では、会社ロゴ、アプリケーションタイトル、および通知モーダルという 3 つの設定可能なオプションすべてについて説明します。これらのオプションの 1 つ、2 つ、または 3 つすべてのオプションを変更できます。

ログイン画面でデフォルトテーマを変更するには、次の方法を実行します。

1 Web サーバの「アセット」フォルダに会社のロゴを保存します。例 :

  C:\inetpub\wwwroot\DRAClient\assets

  最適なイメージサイズは 115x28 ピクセルです。

2 Web コンソールにログインし、［ **[管理]**］>［ **[構成]**］>［ **[ブランディング]**］に移動します。

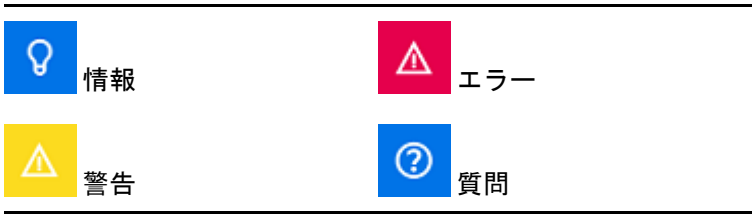
3 [**ログイン**] タイルの［会社ロゴイメージ］フィールドのファイル名を、ファイル拡張子を含む保存済みイメージファイルの名前に置き換えます。

4 必要に応じて、[**アプリケーションタイトル**] フィールドのテキストを変更します。

5 [**ログイン時に通知モーダルを表示する**] をクリックしてこの設定を有効にし、通知プロンプトのタイトルを入力します。ユーザに表示するメッセージの内容を［ [**コンテンツ**]］フィールドに入力または貼り付けます。例 :

セキュリティ保護されたネットワークにログインしています。このシステムにログインすることにより、ネットワークアクセスに関する会社のセキュリティポリシーに従うことに同意したことになります。

6 メッセージの表示形式を選択します。スタイルによって、メッセージボックス (次に示す) に添付されているイメージフラグが変更されます。必要に応じて、［プレビュー］をクリックして、メッセージの表示方法を確認できます。



7 ページの下部の［ [**保存**]］をクリックし、設定の変更を完了します。

クライアントセッションの設定

クライアントセッションの設定で、Web コンソールを自動ログアウトさせる非アクティブ期間の時間増分を定義したり、自動ログアウトを一切しないように設定することができます。

Web コンソールで自動ログアウトを設定するには、[**管理**]］> [**構成**]］> [**クライアントセッションの設定**]］の順に選択します。トグルスイッチを使用して自動ログアウト機能を有効にし、必要に応じて、非アクティブ期間の設定を分単位で変更します。

サーバ接続

ブラウザで Web コンソールのログインページにアクセスする場合、DRA への接続方法を定義するために設定できる [**オプション**] 設定があります。これらの設定は、Web コンソールのユーザプロファイルメニューの［ [**サーバ接続**]］オプションにもあります。DRA サーバのサービスポートのデフォルト設定は 8775 です。デフォルトが有効になっていない場合は、ユーザプロファイルまたはログイン画面の［オプション］で DRA サーバの新しいデフォルトを設定できます。サーバ接続設定の接続設定は、Windows ユーザプロファイルに保持されます。

ログイン画面の［オプション］メニューまたはログイン後のユーザプロファイルメニューから、[**サーバ接続**] 設定から変更できる設定に関する情報は次の通りです。

DRA サーバ設定	説明
自動ディスカバリの使用	DRA サーバを自動的に検出します。設定オプションはありません。
デフォルトの DRA サーバに接続する (サーバ接続設定でデフォルトが有効になっている場合にのみ表示されます)	(有効な場合) サーバ接続設定のデフォルト設定を使用します。使用できる設定オプションはありません。
特定の DRA サーバに接続する	ユーザがサーバとポートを設定します。

必要に応じて、Web コンソールの **[サーバ接続]** 設定から DRA サーバのデフォルトの場所、サーバ、およびドメインを設定できます。

デフォルト設定を有効にするには、Web コンソールにログインし、［**[管理]**］>［**[構成]**］>［**[DRA サーバへの接続]**］の順に移動します。使用する接続設定を有効にし、［**[保存]**］をクリックします。

DRA サーバへの接続

DRA サービスへの接続の設定には、デフォルトサーバの場所の設定、ポートの変更 (必要な場合)、および接続タイムアウト (秒単位) が含まれます。また、トグルスイッチを使用して設定を無効にできます。

DRA サーバの場所を指定する場合は、次の例に示すフォーマットを使用します。

ServerName.DomainName.com

Web コンソールのカスタマイズ

Web コンソールでオブジェクトのプロパティをカスタマイズできます。プロパティを適切にカスタマイズすると、オブジェクト管理を伴うタスクの自動化に役立ちます。

プロパティページのカスタマイズ

DRA 管理権限がある場合、Active Directory の管理の役割で使用するオブジェクトプロパティフォームをオブジェクトタイプごとにカスタマイズすることができます。たとえば、DRA に組み込まれているオブジェクトタイプに基づいた新しいオブジェクトページを作成しカスタマイズすることもできます。また、組み込みオブジェクトタイプに合わせてプロパティを変更することもできます。

プロパティオブジェクトは Web コンソールの［プロパティページ］リストに明確に定義されています。このリストを見れば、どのオブジェクトページが組み込み済みで、どの組み込みページがカスタマイズされ、どのページが組み込みではなく管理者によって作成されたかが簡単に識別できます。

オブジェクトプロパティページのカスタマイズ

オブジェクトプロパティのフォームは、ページの追加または削除、既存のページやフィールドの変更、およびプロパティ属性のためのカスタムハンドラの作成といったカスタマイズを行うことができます。フィールドのカスタムハンドラは、フィールドの値が変更されるたびに実行されます。タイミングを設定することもできます。これにより、管理者は、ハンドラを (キーを押すたびに) すぐに実行するかどうか、フィールドがフォーカスを失ったとき、または指定した時間遅延後に実行するかを指定できます。

プロパティページのオブジェクトリストには、オブジェクトタイプごとに操作タイプ (オブジェクトの作成とプロパティの編集) があります。これらは、アシスタント管理者が Web コンソールで実行する主要な操作です。これらの操作を実行するには、[**[管理]**] > [**[検索]**] または [**[詳細検索]**] に移動します。ここでは、[作成] プルダウンメニューからオブジェクトを作成したり、[プロパティ] アイコンを使用して検索結果テーブルで選択されている既存のオブジェクトを編集することができます。

Web コンソールでオブジェクトプロパティページをカスタマイズするには :

1. DRA 管理特権で Web コンソールにログインします。
2. [**[管理]**] > [**[カスタマイズ]**] > [**[プロパティページ]**] の順に選択します。
3. [プロパティページ] のリストからオブジェクトと操作タイプ (オブジェクトの作成または編集) を選択します。
4. [**[プロパティ]**] アイコンをクリックします。
5. 次のうち 1 つまたは複数の方法でオブジェクトプロパティのフォームをカスタマイズし、変更を適用します。
   - 新しいプロパティページを追加する : [**[+ ページの追加]**]
   - プロパティページの並べ替えおよび削除
   - プロパティページを選択し、そのページをカスタマイズする
     - ページ内の設定フィールドの順序を変える ( )
     - フィールドまたはサブフィールドを編集する ( )
     - 1 つまたは複数のフィールドを追加します : [ ] または [**[新しいフィールドの挿入]**]
     - 1 つまたは複数のフィールドを削除する ( )
   - スクリプト、メッセージボックス、クエリ (LDAP、DRA、REST) のいずれかを使用してプロパティのカスタムハンドラを作成する

     カスタムハンドラの使用に関する詳細については、『*DRA 管理者ガイド*』の「「Adding Custom Handlers(カスタムハンドラの追加)」」を参照してください。

オブジェクトプロパティページの新規作成

オブジェクトプロパティページを新規に作成するには :

1. DRA 管理権限を使用して Web コンソールにログインし、[[管理]> [[カスタマイズ]] > [[プロパティページ]] に移動し、[✚ [作成]] をクリックします。
2. 名前、アイコン、オブジェクトタイプ、操作の設定を定義して最初のオブジェクトプロパティフォームを作成します。

   [[OK]] をクリックした後、[作成] アクションは [作成] ドロップダウンメニューに追加され、[プロパティ] アクションはユーザが検索リストからオブジェクトを選択して編集したときにオブジェクトフォームに表示されます。
3. 必要に応じて、その新規のフォームをカスタマイズします。「オブジェクトプロパティページのカスタマイズ」を参照してください。

Web コンソールでオブジェクトを管理する

Web コンソールでは、管理者のマストヘッドに移動することによってオブジェクトを管理します。ここから、管理対象ドメイン、Azure テナント、コンテナ、およびごみ箱のオブジェクトをオブジェクトタイプで検索できます。ドメインまたは Azure テナント内では、DRA を使用して、Active Directory および Azure Active Directory オブジェクトを管理およびアクションを実行できます。

検索結果リストでオブジェクトを選択すると、そのオブジェクトに対して実行できるすべての該当するアクションが、グリッド上のタスクバーで使用可能になります。使用可能なオプションは、選択されたオブジェクトタイプ、現在 DRA 用に設定されているコンポーネント、および割り当てられた管理者特権に基づいています。

オブジェクトのプロパティを編集するには、オブジェクトの上にマウスのカーソルを合わせて、オブジェクト行に表示される [[プロパティ]] アイコン✎をクリックします。ここから、左のナビゲーションペインにあるすべてのオブジェクトのプロパティページにアクセスできます。

重要 : オブジェクトが [誤って削除されないように保護] するには、[[全般]] プロパティページの下部までスクロールし、チェックボックスをオンにして、この機能を有効にし、変更内容を [適用] します。

オブジェクトに対して実行できるアクションの詳細については、次のトピックを参照してください。

- Active Directory オブジェクトの管理
- Azure オブジェクトの管理
- Exchange のメールボックスとパブリックフォルダの管理
- リソースの管理

変更履歴レポートの生成

変更履歴が DRA 管理者によって設定され、[UI レポートの生成] 権限を持っている場合は、変更履歴レポートを生成し、DRA の管理対象オブジェクトのレポートをエクスポートできます。これには、DRA および DRA の外部で行われた変更が含まれます。変更履歴レポートは、次のタイプのレポートを含む Web コンソールからのみ生成できます。

- ユーザが行った変更
- ユーザに行われた変更
- ユーザが作成したユーザのメールボックス
- ユーザが削除したユーザのメールボックス
- ユーザが設定したグループおよび連絡先電子メールアドレス
- ユーザが削除したグループおよび連絡先電子メールアドレス
- ユーザが作成または無効化した仮想属性
- ユーザが移動したオブジェクト

統合された変更履歴 (UCH) レポートを生成するには :

1. Web コンソールを起動します。
2. [[管理] > [検索]] の順に選択します。
3. [[検索方法]]、[[検索語]]、および [[フィルタ]] オプションを使用して検索条件を定義します。
4. [[検索]] ボタンをクリックして、検索結果を表示します。
5. 生成するレポートに含める必要のあるオブジェクトを選択します。
6. [[変更履歴レポートの表示]] アイコンをクリックします。

   統合された変更履歴レポートフォームでは、[タイプ]、[ターゲットオブジェクト]、および [フィルタ] オプションからレポート条件を編集および生成して、変更が検出されたサーバ (DRA および Change Guardian) の定義を含めることができます。
7. [[生成]] をクリックすると、監査データにアクセスして UCH レポートを生成します。
8. レポートは、ソートしたり、CSV や HTML などの必要な形式でエクスポートすることができます。

表示されたレポートの CSV ファイルを作成するには、上記の手順を使用してレポートを生成した後に次のいずれかのオプションを実行して、生成された変更または現在のページに表示されている変更をエクスポートできます。

- [[すべてをエクスポート]] をクリックし、エクスポートしたレポートを保存します。
- [[現在のページをエクスポート]] をクリックし、エクスポートしたレポートを保存します。

  必要に応じて、ページに表示される変更の数を最大 200 項目まで変更できます。

Workflow Automation の使用

ワークフローの自動化を使うと、ワークフローフォームを起動することで IT プロセスを自動化することができます。ワークフローフォームは、ワークフローを実行したとき、または Workflow Automation サーバで作成された名前付きワークフローイベントが発生したときに実行されます。

ワークフローのフォームは、その作成時または変更時に Web サーバに保存されます。このサーバの Web コンソールにログオンするときに、委任された権限とフォームの構成方法に基づいてフォームが利用できます。フォームは Web サーバの資格情報を持つすべてのユーザが利用できます。フォームを送信するには適切な権限が必要です。

ワークフローフォームを起動するには : ワークフローは、Web コンソール経由で DRA と統合された Workflow Automation サーバ内に作成されます。新しいフォームを保存するには、フォームのプロパティで設定される［**[特定のワークフローの起動]**］または［**[イベントによるワークフローのトリガ]**］のいずれかのオプションが必要です。これらのオプションに関する詳細は以下のとおりです。

- **特定のワークフローの起動 :** このオプションでは、DRA のワークフローサーバで稼働中の利用可能なワークフローをすべてリストで表示します。このリストに表示されるためには、ワークフローが Workflow Automation サーバ内の DRA_Workflows というフォルダに作成される必要があります。
- **イベントによるワークフローのトリガ :** このオプションは、事前に定義されたトリガでワークフローを実行するために使用されます。トリガを用いるワークフローも Workflow Automation サーバ内に作成されます。

注 : ［特定のワークフローの起動］で設定したワークフローフォームのみ実行履歴が付きます。履歴に対しては、［**[タスク]**］> ［**[要求]**］からアクセスする検索のメインの表示枠内からクエリを行うことができます。

Workflow Automation の詳細については、DRA マニュアルサイトの次のガイドを参照してください。

- *DRA 管理者ガイド*
- *WFA 管理者ガイド*
- *WFA ユーザガイド*
- *WFA プロセスオーサリングガイド*

Account and Resource Management

Delegation and Configuration Console (委任および環境設定コンソール) の Account and Resource Management ノードは、DRA のアシスタント管理者が行うタスクのほとんどに対応します。基本的なシステム管理から高度なヘルプデスクでの問題まで企業の管理ニーズ

を満たします。Account and Resource Management を使用し、アカウントおよびリソースの管理タスクを実行したり、Microsoft Exchange のメールボックスを管理することができます。

Account and Resource Management には、次のノードが含まれています。

すべての管理対象オブジェクト

ユーザアカウント、グループ、連絡先、リソース、ダイナミックグループ、ダイナミック配布グループ、リソースのメールボックス、パブリックフォルダなど、操作権限のあるドメインの中のオブジェクトが管理できます。

一時グループの割り当て

特定の期間だけグループメンバーシップを必要とするユーザのためのグループメンバーシップが管理できます。

詳細クエリ

個人およびパブリックの LDAP および仮想属性クエリの両方を構築、保存、インポート、エクスポート、コピー、および管理できます。

ごみ箱

ごみ箱が有効になっているすべての Microsoft Windows ドメインに関し、削除されたユーザアカウント、グループ、連絡先、およびリソースが管理できます。

Account and Resource Management ノードにアクセスするには、NetIQ 管理者プログラムフォルダの［ **[Delegation and Configuration]**］をクリックし、コンソールの Delegation and Configuration ノードを展開します。

Delegation and Configuration console (委任および環境設定コンソール) を起動すると、ローカルドメイン内で利用できる最善な管理サーバに初期接続します。利用できる最善な Administration サーバは最も近くにあるサーバです。一般的にそれはネットワークサイト内のサーバです。DRA は、利用できる最善な管理サーバを探すことで、接続スピードとパフォーマンスを向上させています。

Account and Resource Management の操作の詳細については、次のトピックを参照してください。

- 26 ページの 「管理サーバまたは管理対象ドメインへの接続」
- 26 ページの 「コンソールのタイトル変更」
- 27 ページの 「リストの列のカスタマイズ」
- 27 ページの 「Account and Resource Management におけるオブジェクトの管理」
- 28 ページの 「保存された高度なクエリの実行」
- 29 ページの 「コンソール設定の復元」
- 29 ページの 「特殊文字の制限」
- 30 ページの 「ワイルドカード文字の使用」
- 31 ページの 「割り当てられた権限と役割の表示」
- 32 ページの 「製品のバージョン番号とインストール済みのホットフィックスの表示」

- 32 ページの 「現在のライセンスの表示」
- 32 ページの 「BitLocker パスワードの回復」

管理サーバまたは管理対象ドメインへの接続

デフォルトで DRA は、管理対象のドメインまたはコンピュータの管理サーバのうち、利用できる最善なものに接続します。利用できる最善な Administration サーバは最も近くにあるサーバです。一般的にそれはネットワークサイト内のサーバです。サイト内に管理サーバがない場合、DRA はその次に最も利用可能なサーバを管理対象ドメインまたは管理対象サブツリー内から探して接続します。また、接続先の管理サーバまたはドメインを指定することもできます。

ユーザインタフェースを最初に起動すると、DRA はまず、その起動に使用されたログオンアカウントのドメインに接続します。管理サーバの管理していないドメインにログオンしている場合や、DRA がそのドメインの管理サーバに接続できない場合は、DRA がエラーメッセージを表示することがあります。管理サーバが利用可能であることを確認して、再試行します。

管理サーバに接続には :

1. ［ファイル］メニューから［ **[Connect to DRA server (DRA サーバに接続する★)]**］をクリックします。
2. ［ **[Connect to this DRA server (この DRA サーバに接続する★)]**］をクリックします。
3. 管理サーバの名前を入力します。入力形式 : *computername*
4. ［ **[OK]**］をクリックします。

管理対象のドメインまたはコンピュータに接続するには :

1. ［ファイル］メニューから［ **[Connect to DRA server (DRA サーバに接続する★)]**］をクリックします。
2. 適切なオプションを選択してから、管理対象のドメインまたはコンピュータの名前を入力します。
3. たとえば、HOULAB というドメインに接続するには、［ **[Connect to a DRA server that manages this domain (このドメインを管理する DRA サーバに接続する★)]**］をクリックしてから、「HOULAB」と入力します。
4. 管理対象のドメインまたはコンピュータの管理サーバを指定するには、［ **[Advanced(詳細設定★)]**］をクリックしてから、適切なオプションを選択します。
5. ［ **[OK]**］をクリックします。

コンソールのタイトル変更

Delegation and Configuration console (委任および環境設定コンソール) のタイトルバーは、そこに表示される情報を変更することができます。便利さと明確さを向上させるために、コンソール起動時のユーザ名や、コンソール接続先の管理サーバを追加することができま

す。また、複数の管理サーバに異なる資格情報を使用して接続する必要のある複雑な環境では、この機能を応用することで、今どのコンソールを使用すべきかがすぐに判別できるようになります。

コンソールのタイトルバーを変更するには :

1 Delegation and Configuration console (委任および環境設定コンソール) を起動します。

2 ［ **[表示]**］> **[［オプション］]** の順にクリックします。

3 ［Window Title (ウィンドウタイトル★)］タブを選択します。

4 適切なオプションを指定してから、［ **[OK]**］をクリックします。

リストの列のカスタマイズ

どのオブジェクトプロパティを DRA のリストカラムに表示させるかを選択することができます。この柔軟性のある機能により、検索結果のリスト表示などのユーザインタフェースをカスタマイズでき、企業のシステム管理における特定のニーズを満たすことができます。たとえば、カラムにユーザのログオン名またはグループの種類を表示されるよう設定できます。これにより、必要なデータを迅速かつ効率的に特定しソートすることができます。

リストカラムをカスタマイズするには :

1 適切なノードを選択します。たとえば、管理対象オブジェクトに関する検索結果を表示する場合に、結果を表示させるカラムを選択するには、［ **[すべての管理対象オブジェクト]**］を選択します。

2 ［表示］メニューから［ **[Choose Columns (カラムを選択★)]**］をクリックします。

3 このノードで使用可能なプロパティのリストから、表示するオブジェクトプロパティを選択します。

4 カラムの順序を変更するには、カラムを選択し、［ **[上に移動]**］または［ **[下に移動]**］をクリックします。

5 カラムの幅を指定するには、カラムを選択し、所定のフィールドに適切なピクセル数を入力します。

6 ［ **[OK]**］をクリックします。

Account and Resource Management におけるオブジェクトの管理

Account and Resource Management のオブジェクトを管理するには、ディレクトリツリー内の［ **[すべての管理対象オブジェクト]**］またはサブノードを選択します。ここから、ドメイン、コンテナ、および OU 内のオブジェクトをオブジェクトタイプで検索できます。

検索結果リストでオブジェクトを選択すると、そのオブジェクトに対して実行できるすべての該当するアクションがツールバーの［ **[タスク]**］メニューまたは右クリックメニューから使用できるようになります。使用可能なオプションは、選択されたオブジェクトタイプ、現在 DRA 用に設定されているコンポーネント、および割り当てられた管理者特権に基づいています。

オブジェクトのプロパティを編集するには、オブジェクトを選択し、[[タスク]] メニューで [[プロパティ]] をクリックします。ここから、左のナビゲーションペインにあるページのリンクをクリックすることによって、すべてのオブジェクトのプロパティページにアクセスすることができます。

重要 : オブジェクトが [誤って削除されないように保護] するには、オブジェクトを選択し、[[プロパティ]」を開き、ナビゲーションペインで [[全般]] を選択します。チェックボックスをオンにしてこの機能を有効にし、変更内容を [[適用]] します。

オブジェクトに対して実行できるアクションの詳細については、次のトピックを参照してください。

- Active Directory オブジェクトの管理
- Exchange のメールボックスとパブリックフォルダの管理
- リソースの管理

保存された高度なクエリの実行

高度なクエリを使用すると、ユーザ、連絡先、グループ、コンピュータ、プリンタ、OU はもとより、DRA がサポートするオブジェクトならすべて検索することができます。「Execute Saved Advanced Querie」という権限があれば、Account and Resource Management のノード内のどのコンテナに対しても [[Saved Queries (保存済みクエリ★)]] リストで利用可能な高度なクエリを実行できます。自分に割り当てられた権限の詳細については、「割り当てられた権限と役割の表示」を参照してください。

保存済みの高度なクエリを実行するには :

1. [[Account and Resource Management]] > [[すべての管理対象オブジェクト]] の順に開きます。
2. 適切なコンテナを選択します。たとえば、DRA にユーザアカウント情報を検索させたい場合、[[ユーザ]] を選択します。
3. 詳細検索の表示枠を表示するには、[[Advanced Search (詳細検索★)]] をクリックします。
4. 詳細検索の表示枠内の [[Saved Queries (保存済みクエリ)]] リストから詳細検索クエリを 1 つ選択します。
5. [[Load Query (クエリをロード★)]] をクリックして、[[Find Now (今すぐ検索★)]] をクリックします。

コンソール設定の復元

DRA では、ウィンドウサイズの変更とウィンドウサイズの保持が可能です。この他にも DRA は、前回接続した管理サーバ、リスト結果から追加または削除されたカラム、カラムの幅など、多くの設定を保持します。これらの設定を DRA インストール直後の設定に戻す必要が生じた場合、[Restore Default Settings (デフォルトの設定に復元★)] というオプションを使用すれば戻すことができます。

デフォルトのコンソール設定に復元するには :

1. [**[表示]**] > [**[オプション]**] の順にクリックします。
2. [**[Saved Settings (保存済みの設定★)]**] タブを選択します。
3. ウィンドウに表示される情報を確認してから、[**[Restore Default Settings (デフォルトの設定に復元★)]**] をクリックします。

特殊文字の制限

ユーザアカウント、グループ、連絡先、OU、コンピュータ、ActiveView、AA グループ、役割、ポリシー、または自動化トリガに名前を付ける場合、次に挙げる特殊文字は名前に使用できません。これらの命名制限は、オブジェクト名にも、オブジェクトを定義するルールの名前にも適用されます。

ユーザアカウント、グループ、コンピュータの命名

Windows 2000 以前の名前を指定する場合、次に挙げる特殊文字が使用できません。

円記号	\
コロン	:
カンマ	,
二重引用符	"
等号 (=)	=
スラッシュ (/)	/
大なり記号	>
左角カッコ	[
小なり記号	<
プラス記号 (+)	+
右角カッコ	]
セミコロン	;
縦線	|

重要 : パブリックフォルダ管理にはバックスラッシュ (\) 文字がサポートされていません。

ユーザアカウント、グループ、および Microsoft Windows ドメイン内のコンピュータに名前を付ける場合は、任意の特殊文字が使用できます。

連絡先と OU の命名

連絡先や OU に名前を付ける場合、任意の特殊文字が使用できます。

Activeview、AA グループ、役割の命名

ActiveViews、AA グループ、および役割に名前を付ける場合、バックスラッシュ (\) が使用できません。

ポリシーと自動化トリガの命名

ポリシーおよび自動化トリガに名前を付ける場合は、バックスラッシュ (\) が使用できません。

Azure で無効な文字

無効な文字を使用すると、Azure Active Directory と企業内システムのディレクトリとの同期が失敗する原因となります。無効な文字の詳細については、Microsoft Office サポートの Web サイトにアクセスし、*Directory object and attribute preparation (ディレクトリオブジェクトと属性の準備)* というサブトピックを参照してください。

オンラインメールボックスのプロパティでこれらの文字が使用されないようにするには、次の操作を行います。

1. Delegation and Configuration console (委任および環境設定コンソール) の［Configuration Management (環境設定管理)］ノードをクリックし、［ **[Update Administration Server Options (管理サーバオプションの更新)]**］を選択します。
2. タブメニューの［ **[Azure Sync (Azure 同期)]**］をクリックします。
3. ［ **[Enforce online mailbox policies for invalid characters and character length (無効な文字や文字数に対してオンラインメールボックスポリシーを強制する)]**］をクリックして、［ **[OK]**］をクリックします。

ワイルドカード文字の使用

DRA では、CLI コマンドと DRA コンソールの多くのフィールドでワイルドカード文字が使用できます。ワイルドカードを使って、複数のオブジェクトを特定の条件または規格 (命名規則など) に一致させるルールを定義することができます。ルールの範囲を広げたり絞り込む場合、正規表現の代わりにワイルドカードが使用できます。ワイルドカードの照合では大文字と小文字を区別しません。疑問符 (?)、アスタリスク (*)、番号記号 (#) といった

ワイルドカード文字の直前に円記号 (\) を付けることで、そのワイルドカード文字を通常の文字として使用することもできます。たとえば、「abc*」を検索するには、検索文字列として「abc*」を入力します。

DRA では、次に示すワイルドカード文字が使用できます。ワイルドカード文字を名前に使用することはできません。

一致項目	文字	定義
任意の文字	疑問符 (?)	1 文字とだけ一致する
任意の桁	シャープ記号 (#)	1 桁一致
任意の文字、0 個以上の一致	アスタリスク (*)	一致する文字がないか複数の文字と一致する

次の表に、ワイルドカード文字による指定例とそれぞれで一致する例と一致しない例を示します。

例	一致する	一致しない
Den???	Denton and Dennis	Denison
El ????o	El Campo and El Indio	El Paso
Houston, TX #####	Houston, TX 77024	Houston, TX USOFA

DRA は論理演算子を含むワイルドカード指定をサポートしません。

割り当てられた権限と役割の表示

役割と権限によってオブジェクトの管理方法が決まります。役割とは、特定の管理タスク (ユーザアカウントの作成や共有ディレクトリの移動など) を実行するために必要なパーミッションを提供する権限のセットです。

DRA 管理者がユーザに役割を割り振り、特定の AA グループに追加し、ActiveView (管理可能なドメインオブジェクトのセット) に関連付けます。これらの割り当ては、Delegation and Configuration console (委任および環境設定コンソール) で確認することができます。自分に割り当てられた役割と権限を確認するために補助的な権限は必要ありません。

割り当てられた権限と役割を表示するには :

1. ［ファイル］メニューから［ **[DRA Properties (DRA プロパティ★)]**］をクリックします。
2. ［ **[権限]**］をクリックします。
3. 適切なビューを選択します。たとえば、AA グループのメンバーシップ、各メンバーの権限と役割、および関連付けられた ActiveView で構成されるテーブルを表示するには、［ **[Flat View (フラット表示★)]**］をクリックします。
4. 適切な項目を開きます。たとえば、「 **[Has Power]**」という列で［ **[Roles and Powers (役割と権限★)]**］を開いて個々の役割と権限を表示します。
5. ［ **[OK]**］をクリックします。

製品のバージョン番号とインストール済みのホットフィックスの表示

製品のバージョン番号とインストール済みのホットフィックスを［DRA Properties (DRA プロパティ★)］ウィンドウに表示できます。このウィンドウには、管理サーバーと DRA のクライアントコンピュータに関するインストール済みのホットフィックスの一覧とバージョン番号が表示されます。

製品のバージョン番号とインストール済みのホットフィックスを表示するには :

1 ［ファイル］メニューから［ **[DRA Properties (DRA プロパティ★)]**］をクリックします。

2 ［ **[全般]**］をクリックします。

3 必要な情報を確認します。

4 ［ **[OK]**］をクリックします。

現在のライセンスの表示

DRA にはライセンスキーファイルが必要です。製品のライセンスを任意の管理サーバのコンピュータから確認することができます。製品のライセンスの確認をするために特別な権限は必要ありません。

自分のライセンスを表示するには :

1 ［ファイル］メニューから［ **[DRA Properties (DRA プロパティ★)]**］をクリックします。

2 ［ **[ライセンス]**］をクリックします。

3 ライセンスのプロパティを確認したら［ **[OK]**］をクリックします。

BitLocker パスワードの回復

Microsoft BitLocker では、Active Directory に回復パスワードを格納しています。必要な権限を持つユーザなら、DRA の BitLocker 回復機能を使用してエンドユーザの紛失した BitLocker パスワードを検索し回復することができます。

重要 : BitLocker 回復パスワードの機能を使用する前に、自分のコンピュータがドメインに割り当てられ、BitLocker がオンになっているか確認してください。

BitLocker 回復パスワードの表示とコピー

コンピュータの BitLocker パスワードが失われた場合、Active Directory でそのコンピュータのプロパティから回復用パスワードのキーを入手し、それを使用してリセットすることができます。そのパスワードキーをコピーし、エンドユーザに渡してください。

回復用パスワードを表示しコピーするには :

1. Delegation and Configuration console (委任および環境設定コンソール) を起動し、[[Account and Resource Management]] > ［[すべての管理対象オブジェクト]］に移動します。
2. ドメインを選択し、検索を実行して、ドメイン内のすべてのコンピュータのリストを表示します。
3. コンピュータのリストから回復が必要なコンピュータを右クリックし、[[プロパティ]］> ［[BitLocker 回復パスワード]］の順に選択します。
4. 右クリックして BitLocker 回復パスワードをコピーし、テキストファイルにパスワードのテキストを貼り付けます。

回復パスワードの検索

コンピュータの名前が変更されていた場合、パスワード ID の最初の 8 文字を使用してドメイン内で回復パスワードを検索する必要があります。

パスワード ID を使用して回復用パスワードを検索するには :

1. Delegation and Configuration console (委任および環境設定コンソール) を起動し、[[Account and Resource Management]] > ［[すべての管理対象オブジェクト]］に移動します。
2. 右クリックし、[［管理対象ドメイン］] を右クリックしてから、[［BitLocker 回復パスワードの検索］] をクリックします。

   回復用パスワードの先頭から 8 文字を検索する方法については、「BitLocker 回復パスワードの表示とコピー」を参照してください。
3. ［[BitLocker 回復パスワードの検索]］のページで、コピーした文字を検索フィールドに貼り付けてから ［[検索]］クリックします。

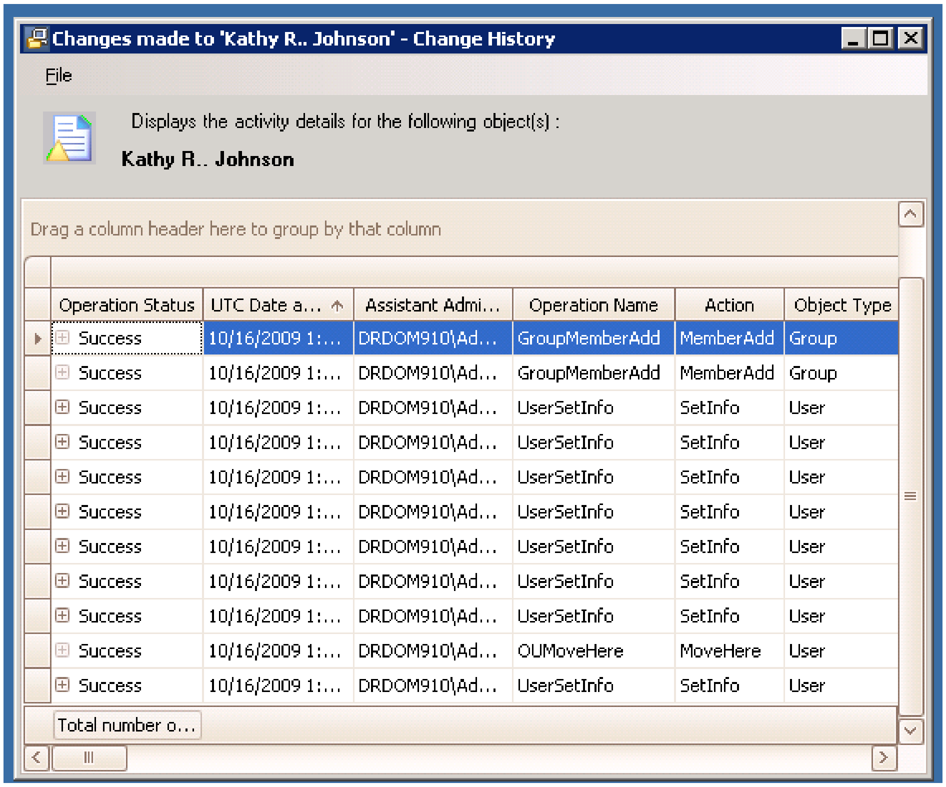
DRA Reporting

DRA Reporting は、すぐに利用できる組み込みのレポート機能です。これを使用して、重複アカウント、アカウントの直近のログオン、Microsoft Exchange メールボックスの詳細など、多くの内容を迅速に追跡することができます。また、Reporting は、変更前と変更後のプロパティの値を含め、使用中の環境に加えられた変更の詳細をリアルタイムに提供します。レポートをエクスポート、印刷、表示でき、SQL Server のレポーティングサービスにレポートを発行することもできます。

DRA には、ユーザアカウント、グループ、およびドメイン内のリソース定義を収集し確認できるレポートの生成方法が 2 つあります。それは、**Activity Detail レポート**と **DRA Management レポート**です。Activity Detail レポートは、Delegation and Configuration console

(委任および環境設定コンソール) に表示され、ドメイン内のオブジェクトに関する変更情報がリアルタイムに確認できます。たとえば、Activity Detail レポートを使用すれば、指定した期間中にオブジェクトに対して加えられた変更またはオブジェクトが加えた変更のリストを表示できます。

次の図に Activity Detail レポートのサンプルを示します。



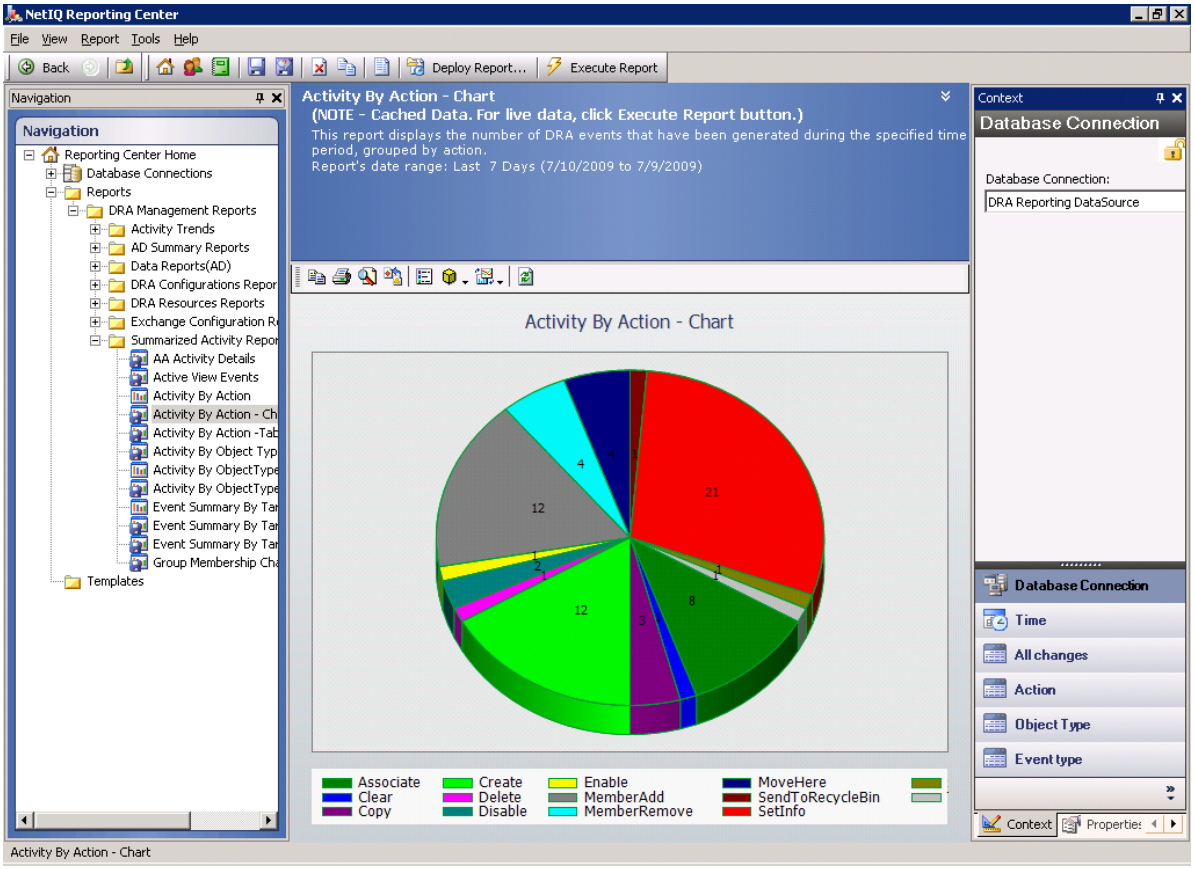
オプションの **DRA 管理レポート**は、NetIQ Reporting Center (レポーティングセンター) に表示でき、管理対象ドメイン内のイベントに関する情報の要約、構成、およびアクティビティが確認できます。管理レポートの中にはデータがグラフ表示できるものがあります。これらの組み込みレポートは、必要とされる情報が正確に得られるようにカスタマイズすることもできます。

たとえば、管理レポートを使用して、指定した期間中の各管理対象ドメインにおけるイベントの数をグラフで表示することができます。Reporting では、ActiveView の定義や AA グループの定義など、DRA のセキュリティモデルに関する詳細が表示できます。

これらのレポートを表示するには、事前にオプションの管理レポートをインストールし構成しておく必要があります。レポーティングコンポーネントのインストールの詳細については、『*インストールガイド*』を参照してください DRA のレポート機能の詳細については、「33 ページの 「DRA Reporting」」を参照してください。

NetIQ > Reporting Center プログラムグループの中にある Reporting Center コンソールを起動します。

次の図は、DRA 管理レポートが選択されたときの Reporting Center のインタフェースを示しています。



DRA Reporting の詳細については、次のトピックを参照してください。

- 35 ページの 「DRA Reporting について」
- 36 ページの 「DRA によるログアーカイブの使用」
- 37 ページの 「日付と時刻について」
- 37 ページの 「DRA Reporting タスク」

DRA Reporting について

DRA Reporting にはレポート生成方法が 2 つあり、使用中の環境で最近変更された内容を確認するレポートと、ドメイン内のユーザアカウント、グループ、およびリソースの定義を収集し確認するためのレポートが生成できます。

Activity Detail のレポート

Account and Resource Management ノードおよび Delegation and Configuration console (委任および環境設定コンソール) からアクセスできるこれらのレポートは、ドメイン内のオブジェクトの変更情報をリアルタイムで提供します。

DRA 管理レポート

NetIQ Reporting Center (レポーティングセンター) からアクセスできるこれらのレポートは、管理対象ドメイン内のイベントに関するアクティビティ、構成、および要約情報を提供します。一部のレポートでは、データがグラフで表現されます。

たとえば、Activity Detail レポートを使用すれば、指定した期間中にオブジェクトに対して加えられた変更またはオブジェクトが加えた変更のリストを表示できます。また、管理レポートを使用して、指定した期間中の各管理対象ドメインにおけるイベントの数をグラフで表示することもできます。Reporting では、ActiveView の定義や AA グループの定義など、DRA のセキュリティモデルに関する詳細も表示できます。

ライセンスでサポートされていない機能やレポートは、自動的に無効にされます。また、レポートの実行と表示には、適切な権限が必要です。このため、一部のレポートを使用できないことがあります。

DRA 管理レポートは、オプション機能としてインストールして設定することができ、Reporting Center で表示できます。データの収集を有効にして設定すると、定義したスケジュールに従って、DRA が監査対象イベントに関する情報を収集して SQL Server データベースにエクスポートするようになります。Reporting Center でこのデータベースに接続すると、以下をはじめとする 60 以上の組み込みレポートにアクセスできます。

- 誰がいつ何をしたかを示すアクティビティレポート
- 特定の時点での AD または DRA の状態を示す構成レポート
- アクティビティの量を示す要約レポート

管理レポート用にデータ収集を設定する方法については、『*管理者ガイド*』を参照してください。

DRA によるログアーカイブの使用

アシスタント管理者のアクションを調査したりレポートが生成できるように、DRA はユーザのあらゆる操作を管理サーバのコンピュータ上にあるログアーカイブに記録しています。ユーザ操作とは、ユーザアカウントの更新、グループの削除、ActiveView の再定義など、定義の変更を試みるすべての操作を指します。DRA は、管理サーバの初期化など、内部操作や関連するサーバの詳細情報も記録します。DRA は、これらの監査イベントをログに記録するだけでなく、そのイベントの前と後の値も記録して、何が変わったかを正確に把握できるようにします。

アーカイブしたログデータを安全に保存するために、DRA は **[NetIQLogArchiveData]** というフォルダを使用しています。このフォルダを「**[ログアーカイブ]**」といいます。DRA は長期間にわたってログをアーカイブし、グルーミングというプロセスを通じて古いデータを削除して新しいデータのための場所を確保します。

DRA は、ログアーカイブファイルに保存された監査イベントを使用して、たとえば指定した期間中にオブジェクトに対してどのような変更が加えられたかを示す Activity Detail レポートを表示します。また、これらのログアーカイブファイルから、NetIQ Reporting Center が管理レポートの表示に使用する SQL Server データベースに、情報をエクスポートするように DRA を設定することもできます。

DRA は、常に監査イベントをログアーカイブに書き込みます。DRA が Windows のイベントログにもイベントを書き込む機能を、有効または無効にすることができます。

DRA の監査の詳細については、『*管理者ガイド*』を参照してください。

日付と時刻について

DRA はレポートを表示するときに、コントロールパネルの［地域と言語のオプション］で指定されている［**短い形式**］と［**時刻**］を使用します。DRA のレポートには、イベントのローカル日付および時刻として UTC 日付および時刻が表示されます。DRA レポートでは、次の日付形式がサポートされます。

- m/d/yy
- m-d-yy
- m/d/yyyy
- m-d-yyyy
- mm/dd/yy
- mm-dd-yy
- mm/dd/yyyy
- mm-dd-yyyy
- dd/mm/yy
- dd-mm-yy
- dd/mm/yyyy
- dd-mm-yyyy

DRA Reporting タスク

DRA 管理レポートを生成するには、Reporting Center をインストールし、DRA でデータ収集を有効にします。データ収集を有効にする方法については、『*管理者ガイド*』を参照してください。Activity Detail のレポートを生成するには、オブジェクトを右クリックして［[レポーティング]］をクリックします。そのオブジェクトについて生成できるレポートの選択肢が表示されます。以下の各セクションで、さまざまなレポーティングタスクについて説明します。

Activity Detail レポートの表示

Activity Detail レポートには、環境内の変化に関する情報が表示されます。レポートを表示したり印刷するほかに、Excel、CSV、または TXT 形式でレポートを保存することもできます。レポートを表示または印刷するには、Reporting Administration という役割を持っている必要があります。

レポートを表示するときには、情報表示の対象にする期間を指定するために基準を入力します。レポートに表示する対象を特定の DRA サーバに加えられた変更だけに制限したり、レポートに含める行数を制限することもできます。レポートのサイズが次のいずれかの制限を超えると、レポートが完成しなかったことを知らせるメッセージが表示されます。

- サイズが 500MB を超えた
- すべての DRA サーバに対してクエリを実行するために要した時間が 5 分を超えた
- 表示される行の数が 1000 を超えた

いずれかの制限に達するまでに取得された情報だけを含んだレポートを表示することも、レポートの基準を変更してこれらの制限条件を満たすレポートを表示することもできます。

レポートを表示するには、次の手順を実行します。

1 左側の表示枠にある［**[すべての管理対象オブジェクト]**］を開きます。

2 レポート表示の対象にするオブジェクトを指定するには、次の手順を実行します。

2a ***オブジェクトの場所が分かっている***場合は、このオブジェクトを含むドメインと OU を選択します。

2b 検索の表示枠でオブジェクトの属性を指定してから［**[Find Now (今すぐ検索★)]**］をクリックします。

3 リストの表示枠内で、オブジェクトを右クリックして［**[Reporting (レポート生成★)]**］をクリックします。

4 ［**[Changes made to objectName (オブジェクト名への変更★)]**］や［**[Changes made by objectName (オブジェクト名による変更★)]**］など、レポートの種類を選択します。使用できるレポートは、選択したオブジェクトの種類によって異なります。

5 変更を表示する期間の開始日と終了日を選択します。

6 ***表示する行数を変更したい場合***は、デフォルトの値 (250) を必要な値に書き換えます。

注 : 表示される行数は、環境内の各管理サーバに適用されます。レポートに 3 つの管理サーバを含めてデフォルト値の 250 行を使用すると、そのレポートに表示できる行数は最大で 750 行になります。

---

7 ***特定のサーバだけをレポートに含めたい場合***は、［**[Restrict query to these DRA servers (クエリをこれらの DRA サーバに制限★)]**］を選択し、レポートに含めるサーバの名前を (1 つまたは複数) 入力します。複数のサーバ名を指定する場合はカンマで区切ります。

8 ［**[OK]**］をクリックします。

注 : DRA が最新の変更をレポートに表示するまでに、最大で 5 秒かかることがあります。したがって、行った変更をレポートに表示するには、その変更から少なくとも 5 秒たってからレポートを実行してください。

Activity Detail レポートのエクスポート

Activity Detail レポートは、XLS、CSV、および TXT 形式でエクスポートできます。デフォルトの形式は、Microsoft Excel 形式です。

Activity Detail レポートをエクスポートするには、次の手順を実行します。

1. レポートのウィンドウで、[ファイル] メニューから [**[Preview and Export (プレビューとエクスポート★)]**] をクリックします。
2. プレビューウィンドウの [ファイル] メニューから、[**[Export Document (Export ドキュメントをエクスポート★)]**] > [**[Excel File (Excel ファイル★)]**] の順にクリックします。
3. エクスポートのオプションを選択し、[**[OK]**] をクリックします。
4. [名前を付けて保存] ウィンドウで、ファイルの名前を入力して [**[保存]**] をクリックします。

Activity Detail レポートの印刷

レポートを印刷するには、Reporting Administration という役割を持っている必要があります。レポートを表示したり印刷するほかに、さまざまな形式で保存することもできます。

Activity Detail レポートを印刷するには、次の手順を実行します。

1. レポートのウィンドウで、[ファイル] メニューから [**[Preview and Export (プレビューとエクスポート★)]**] をクリックします。
2. [プレビュー] ウィンドウで [ファイル] メニューから [**[印刷]**] をクリックします。

管理レポートの表示

Reporting Center で管理レポートを表示できるようにするには、DRA Reporting をインストールして DRA データコレクタを設定する必要があります。DRA Reporting のインストールと DRA Collector の設定については、『*管理者ガイド*』を参照してください。

Reporting Center にログオンすると、インストール時に設定した方法に従って Web サービスが IIS を使用してアカウントの資格情報を検証します。

管理レポートを表示するには、次の手順を実行します。

1. Reporting Center コンソールを実行しているコンピュータにログオンします。
2. NetIQ > Reporting Center プログラムグループの順に選択し、その中の **[Reporting Center コンソール]** を起動します。
3. [Logon (ログオン★)] ダイアログボックスに必要な情報を入力し、[**[Logon (ログオン★)]**] をクリックします。

4 ナビゲーションの表示枠内で、[[レポート]] > [[DRA Management Reports (DRA Management のレポート★)]] の順に開きます。

5 表示したいレポートに到達するまで、レポートのカテゴリを開いていきます。

6 [ナビゲーション] 表示枠内でレポート名をクリックすると、そのレポートが中央の結果表示枠内に読み込まれ、キャッシュされたデータが表示されます。

7 ***最新のデータを使ってレポートを表示したい場合***は、結果の表示枠内で [[Execute Report (レポートを実行★)]] をクリックします。

デフォルトのコンテキスト設定を変更して、異なるレポート結果が表示されるようにすることができます。Reporting Center でのコンテキスト設定の詳細については、『*管理者ガイド*』を参照してください。

管理レポートのカスタマイズ

DRA には、出荷時に 60 以上の管理レポートが付属しています。Reporting Center は、これらのレポートをさまざまな方法でカスタマイズおよび展開できる柔軟性を備えています。Reporting Center での管理レポートのカスタマイズと展開の詳細については、『*管理者ガイド*』を参照してください。

管理レポートをカスタマイズするには :

1 作成したいレポートに似たレポートを表示します。詳細については、「管理レポートの表示」を参照してください。

2 レポートのプロパティとコンテキスト設定を変更し、必要な情報を表示するようにレポートをカスタマイズします。

3 [[Execute Report (レポートを実行★)]] をクリックします。

4 [Report (レポート★)] メニューで、[[Save Report As (名前を付けてレポートを保存★)]] をクリックし、レポートのタイトルと、新しいレポートを保存する場所を指定します。

5 [[保存]] をクリックします。

Reporting Center での管理レポートの操作の詳細については、『*管理者ガイド*』を参照してください。

3 オブジェクトの検索

この章では、検索および LDAP 検索機能に関する概念と手順について説明します。

検索

DRA では、オンプレミスの Active Directory ドメイン、Microsoft Exchange、および Azure テナントのオブジェクトを検索することができます。Azure テナントのユーザ、グループ、および連絡先、Active Directory ドメインのユーザ、グループ、連絡先、コンピュータ、プリンタ、OU、グループ管理対象サービスアカウント (gMSA) などのオブジェクト、および Exchange におけるルームメールボックス、備品のメールボックス、共有メールボックス、ダイナミック配布グループなどのオブジェクトを検索できます。検索フィルタを使用して、より効率的で効果的な検索を行うことができます。DRA は、検索入力の先頭または末尾のスペースを自動的に切り捨て、検索結果を返します。

Web コンソールの検索機能にアクセスするには、[**[管理]**] > [**[検索]**] の順に移動します。検索を実行するには、1 つまたは複数のフィルタを選択し、[検索方法] オプションを選択して検索語を入力し、[**[検索]**] をクリックします。

たとえば、次で実行された検索では、選択したドメインまたはコンテナ内で、名字が「Beck」、または名字がその 4 文字で終わるすべてのユーザが返されます。

検索方法	入力された検索語	選択したフィルタ
• 名前 • 次で終わる	beck	ユーザ

注 : フィルタ使用時に検索されたオブジェクトを正確に返すには、フィルタを適用して検索を実行する前に、改ページ調整の変更を行う必要があります。オブジェクトタイプフィルタが適用されている場合は、Web コンソールの下部にある [**[ページ当たりの項目]**] の設定を変更することはできません。

Delegation and Configuration Console (委任および環境設定コンソール) の検索機能にアクセスするには、Account and Resource Management に移動し、表示枠で [**[Accounts and Resources(アカウントとリソース)]**] をクリックします。

- 43 ページの 「列の追加およびソート」
- 44 ページの 「検索結果のエクスポート」

ワイルドカード文字を使用する

DRA は、検索結果を最大化するために、疑問符 (?)、アスタリスク (*)、およびシャープ記号 (#) などのワイルドカード文字をサポートしています。ワイルドカードの照合では大文字と小文字を区別しません。

次の表に、ワイルドカード文字による指定例とそれぞれで一致する例と一致しない例を示します。

文字	一致項目
疑問符 (?)	任意の 1 文字または 1 桁の数字
シャープ記号 (#)	任意の 1 桁の数字
アスタリスク (*)	任意の数の文字または数字

複数フィールドの検索

複数フィールドの一致オプションを使用すると、1 回の検索で複数の属性に一致する検索を行うことができます。複数フィールドの一致を使用して検索を実行する場合、検索文字列は、名前、表示名、名、および姓などの複数の属性と比較されます。検索文字列がこれらのいずれかの属性と一致する場合、オブジェクトは検索結果に返されます。

複数フィールド一致オプションでは、[**[次の値で始まる]**] 検索条件のみがサポートされます。

たとえば、2 人のユーザが存在し、そのうち 1 人の *表示名* が「Martin Smith」で、もう一方のユーザがユーザプリンシパル名として「martha.jones@acme.com」を使用している場合、「Mart」という文字列を使用して検索を実行すると、両方のユーザが検索結果に返されます。

次の表は、各オブジェクトタイプで検索される属性を示しています。

オブジェクトタイプ	検索された属性
Azure 連絡先	displayName、givenName、mail、mailNickname、surname
Azure グループ	displayName、mail
Azure ユーザ	displayName、employeeId、givenName、mail、surname、userPrincipalName
コンピュータ	displayName、name、sAMAccountName
連絡先	displayName、employeeId、givenName、mail、mailNickname、name、surname

オブジェクトタイプ	検索された属性
ダイナミック配布グループ	displayName、mail、mailNickname、name
グループ	displayName、mail、mailNickname、name、sAMAccountName
グループ管理対象サービスアカウント	displayName、name、sAMAccountName
部門	name
ごみ箱	name、sAMAccountName
ユーザ	displayName、employeeId、givenName、mail、mailNickname、name、sAMAccountName、surname

注 : 複数マッチ機能は、次にリストされている Exchange オブジェクトの委任または許可を追加する場合は、Delegation and Configuration console (委任および環境設定コンソール) のオブジェクトセレクタ検索ではサポートされません。

- ユーザのメールボックス
- メールが有効なユーザ
- メールが有効なグループ
- メールが有効な連絡先
- ダイナミック配布グループ
- 共有メールボックス
- リソースメールボックス

列の追加およびソート

属性の列のヘッダをクリックすると、次のいずれかの属性によって検索結果オブジェクトをソートできます。

- 別名
- 表示名
- 電子メール
- EmployeeID
- 名
- 姓
- 場所
- 名前
- Windows2000 より前の名前
- User Principal Name (ユーザプリンシパル名)

属性の列を追加または削除するには、[column (列)] アイコンをクリックします。

検索結果のエクスポート

DRA を使用すると、アシスタント管理者は Web コンソールの [検索] 結果を CSV ファイルにエクスポートできます。Web コンソールから [検索] 結果をエクスポートするには、[[管理]] > [[検索]] に移動し、[[ダウンロード]] アイコンをクリックします。

注 : 選択した列だけがエクスポートされます。現在表示されていないデータを追加する場合は、まずこれらの列を追加してから [検索] 結果をエクスポートします。

詳細検索

DRA を使用すると、[詳細検索] ページからオンプレミスの Active Directory ドメイン内で LDAP 属性および仮想属性のクエリを実行できます。既存のクエリを使用して検索したり、既存のクエリを変更したり、新しいクエリを作成したり、新しいクエリおよび変更されたクエリを保存して、後でパブリックまたはプライベートクエリとして使用できます。検索フィルタを使用して、より効率的で効果的な検索を行います。

Web コンソールの詳細検索クエリ機能にアクセスするには、[[管理]] > [[詳細検索]] の順に移動します。

Delegation and Configuration Console (委任および環境設定コンソール) で詳細検索クエリにアクセスするには、[Account and Resource Management] の下のドメイン、Azure テナント、またはサブノードを選択し、ツールバーの [[詳細検索]] をクリックします。

詳細検索クエリ

DRA は、仮想属性と LDAP クエリの両方をサポートしており、DRA および Active Directory のオブジェクトを検索することができます。仮想属性は、ユーザ、グループ、ダイナミック配布グループ、連絡先、コンピュータ、および OU などの Active Directory オブジェクトタイプに関連付けることができます。仮想属性クエリを使用すると、LDAP クエリによって返された結果をフィルタして、仮想属性のクエリに一致する結果のみを取得することができます。仮想属性クエリの文字列は、(objectCategory=<object type>) で始まる必要があります。仮想属性クエリを実行するには、LDAP 属性および仮想属性クエリの両方に対して文字列を指定する必要があります。

LDAP クエリの例 :

- DRA で「すべてのコンピュータオブジェクト」を検索するには :

  LDAP クエリ : (objectCategory=computer)
- DRA で「East\West Sales」と記述されたユーザオブジェクトを検索するには :

  LDAP クエリ : (&(objectCategory=user)(description=East\5CWest Sales))
- DRA で「すべてのコンピュータオブジェクト」を検索するには :

  LDAP クエリ : (objectCategory=computer)

重要 : バックスラッシュ文字は LDAP フィルタでエスケープする必要があります。\5C で代用します。

- DRA で「すべての無効なユーザオブジェクトを一覧表示する」には :

  LDAP クエリ :

  (&(objectCategory=person)(objectClass=user)(userAccountControl:1.2.840.113556.1.4.803:=2))

  文字列 1.2.840.113556.1.4.803 は、LDAP_MATCHING_RULE_BIT_AND を指定します。これは、userAccountControl、groupType、systemFlags などのフラグ属性 (整数) およびビットマスク (2、32、または 65536 など) のビット単位の AND を指定します。属性値およびビットマスクのビット単位の AND が 0 以外の場合、この句は True となり、ビットが設定されていることを示します。

仮想属性クエリの例 :

- 会社名が ABC であるすべてのユーザを検索するには :

  クエリ : (&(objectCategory=User)(CompanyName=ABC))

  DRA オブジェクトは「User」で、仮想属性は (ユーザに関連付けられた) 「CompanyName」です。

- ストレージドメインで会社名が ABC であるすべてのユーザを検索するには :

  クエリ : (&(objectCategory=User)(CompanyName=ABC)(Domain=Storage))

  DRA オブジェクトは「User」で、仮想属性は (ユーザに関連付けられた) 「CompanyName」および「Domain」です。

- 製品名が DRA であるすべてのグループ、または会社名が ABC であるすべてのユーザを検索するには :

  クエリ :

  (|(&(objectCategory=Group)(ProductGroupName=DRA))(&(objectCategory=User)(CompanyName=ABC)))

  DRA オブジェクトは、「Group」および「User」であり、仮想属性は (ユーザに関連付けられた)CompanyName、(グループに関連付けられた)ProductGroupName です。

- 製品名が DRA であるすべてのグループ、または会社名が ABC であるストレージドメイン内のすべてのユーザを検索するには :

  クエリ :

  (|(&(objectCategory=Group)(ProductGroupName=DRA))(&(objectCategory=User)(CompanyName=ABC)(Domain=Storage)))

  DRA オブジェクトは、「Group」および「User」であり、仮想属性は (ユーザに関連付けられた)CompanyName、(グループに関連付けられた)ProductGroupName、(ユーザに関連付けられた)Domain です。

詳細クエリの管理

DRA は、LDAP を使って詳細検索クエリ機能をサポートしています。詳細クエリを使用すると、ユーザ、連絡先、グループ、コンピュータ、OU はもとより、DRA がサポートするオブジェクトならすべて検索することができます。保存された詳細クエリを実行する権限がある場合は、任意のコンテナの [過去の検索] および [パブリック検索] リストで利用できる詳細クエリを実行できます。

保存された詳細クエリを使用して検索を実行し、それに該当する権限で詳細を表示することに加えて、[詳細検索] ページから詳細クエリを使用して次の操作を実行することもできます。

新規クエリを作成する

新しい詳細クエリについて、クエリ文字列（LDAP および該当する場合は仮想属性) を指定して、プライマリ管理サーバまたはセカンダリ管理サーバのいずれかに詳細クエリを作成します。検索を実行した後、[[検索]] ドロップダウンメニューを展開して、[過去の検索] リストまたは [パブリック検索] リストのいずれかにクエリを保存します。

クエリの変更

[過去の検索] または [パブリック検索] で既存の詳細クエリを選択し、[[変更]] オプションを使用して検索条件を変更します。更新された検索条件を使用して検索を実行した後、必要に応じて [[検索]] ドロップダウンメニューを展開し、[[保存]] を選択して、そのクエリに対する変更を保存します。

クエリをコピーする

[過去の検索] または [パブリック検索] で既存の詳細クエリを選択し、検索を実行します。検索を実行した後、[[検索]] ドロップダウンメニューを展開し、[[名前を付けて保存]] を選択して、別の名前でクエリを保存できます。

クエリの結果をカスタマイズする

DRA が表示する検索結果リストには、デフォルトの列のセットがあります。保存されたクエリ、または保存されていないクエリから検索結果をカスタマイズするには、ページの右側にある [[列の追加と削除]] アイコンをクリックして、検索結果の表示方法を変更します。

クエリを削除する

[[過去の検索]] リストに表示されている詳細クエリを削除することができます。該当する権限を使用して、[[パブリック検索]] リスト内の詳細クエリを削除することもできます。保存されている詳細なクエリを削除するには、該当するリストでそれを選択し、[検索] ドロップダウンメニューの [[削除]] をクリックします。

クエリをクリアする

Web コンソールで、保存されたクエリまたは保存されていないクエリのフォームフィールドをクリアして、クリーンなフォームから変更を加えることができます。クエリのフィールドをクリアするには、[検索] ドロップダウンメニューの [[クリア]] を選択します。

詳細検索結果のエクスポート

DRA を使用すると、アシスタント管理者は Web コンソールの [詳細検索] 結果を CSV ファイルにエクスポートできます。Web コンソールから [詳細検索] 結果をエクスポートするには、[[管理]] > [[詳細検索]] に移動し、[[ダウンロード]] アイコンをクリックします。

注 : 選択した列だけがエクスポートされます。現在表示されていないデータを追加する場合は、まずこれらの列を追加してから、[詳細検索] 結果をエクスポートします。

---

4 Active Directory オブジェクトの管理

この章では、Delegation and Configuration console (委任および環境設定コンソール) の Account and Resource Management ノードと Web コンソールの両方でユーザアカウント、グループ、ダイナミックグループ、ダイナミック配布グループ、および連絡先を管理するための概念と手続きの情報を記載しています。ユーザアカウントに関しては、両方のクライアントアプリケーションで一般的なオブジェクトの管理方法の例を取り上げて、より包括的に説明します。

ユーザアカウントの管理

Microsoft Windows では、関連するユーザアカウントのアクセス権限がユーザアカウントの種類によって決まります。ユーザアカウントはグローバルかローカルです。DRA は InetOrgPerson オブジェクトもサポートしていますが、InetOrgPerson オブジェクトを通常ユーザとして認識します。

グローバルユーザアカウント

ユーザアカウントが作成されたドメインを信頼するドメインならどこでも使用できるユーザアカウントです。ユーザアカウントに特定のパーミッションを付与することができます。ユーザアカウントをグループのメンバーにしてから、そのグループにパーミッションを割り当てる方法もあります。ユーザアカウントのグループ化により、ユーザアカウントが多数ある場合のネットワークパーミッションの管理プロセスが単純になります。

ローカルユーザアカウント

ローカルユーザアカウントは、Windows オペレーティングシステムにログインする際に使用するアカウントと同じです。これにより、自分のユーザスペースでシステムのリソースにアクセスできます。

ユーザアカウントの管理の詳細については、次のトピックを参照してください。

信頼されたドメイン内のユーザアカウント

Microsoft Windows では、管理対象ドメインのディレクトリ内にユーザアカウントとグループ定義が保存されます。このため、管理サーバは、信頼されたドメインが DRA によって管理されている場合を除き、そのドメインのディレクトリ情報を変更することができません。

たとえば、変更できないユーザアカウントとグループが Account and Resource Management に表示されることがあります。これらのユーザアカウントとグループは、管理対象ドメインのうちの 1 つが信頼するドメインに定義されています。ただし、信頼されたドメインのアカウントとグループを管理対象ドメイン内の別のグループに追加することはできます。

ユーザアカウントの管理タスク

このセクションでは、Delegation and Configuration Console (委任および環境設定コンソール) の Account and Resource Management ノードおよび Web コンソールによるユーザアカウント管理について順を追って説明します。適切な権限があれば、アカウントの作成や削除など、さまざまなユーザアカウント管理タスクを実行することができます。複数のユーザアカウントを選択した場合、グループに対するユーザの追加、削除、移動など、選択したタスクを 1 回の操作で実行できます。自分に割り当てられた権限の詳細については、「割り当てられた権限と役割の表示」を参照してください。

Account and Resource Management でのユーザアカウントタスク

次に示す該当タスクをすべて［[タスク]］メニュー、または右クリックメニューから実行できます。一般に、目的のユーザオブジェクトを見つけてそれを選択するには、［[すべての管理対象オブジェクト]］というノードを選択し、［[Find Now (今すぐ検索★)]］という操作を実行します。1 つまたは複数のユーザアカウントを選択すると、実行できるタスクが［タスク］メニューに表示されます。1 人のユーザに対してさらに多くのオプションを使用できます。

新しいユーザを作成する場合は、ユーザを作成する場所のドメインまたは OU を選択する必要があります。例 :

1. ［すべての管理対象オブジェクト］の下のドメイン内の [ユーザ] コンテナを選択します。
2. タスクメニューから［[新規]］>［[ユーザ]］を選択します。
3. ユーザ作成ウィザードの手順に従います。

自分のアカウントを管理する

電話番号など、一般プロパティを変更することにより、自分のアカウントを管理することができます。自分のアカウントを管理する前に、適切な権限があることを確認してください。

ユーザアカウントを別の ActiveView にコピーする

ユーザアカウントを別の ActiveView にコピーすることができます。この操作を、ユーザアカウントの「転送」と呼びます。ユーザアカウントを別の ActiveView にコピーするには、コピー元とコピー先の ActiveView の両方で Copy User to Another ActiveView という権限を持っている必要があります。ユーザアカウントを別の ActiveView に転送しても、元の ActiveView のユーザアカウントは削除されません。

注 : ユーザアカウントを別の ActiveView にコピーすることは、Delegation and Configuration Console (委任および環境設定コンソール) から Account and Resource Management ノードを介してのみ実行できます。

ユーザアカウントの名前を変更する

管理対象ドメインまたは管理対象サブツリー内のユーザアカウントの名前を変更できます。ユーザのログオン名を変更すると、そのユーザアカウントに対応するメールボックスの名前も変更されます。

Web コンソールでのユーザアカウントタスク

次に挙げるタスクのほとんどが Web コンソールの［ **[管理]**］>［ **[検索]**］タブから実行できます。検索操作は、必要なユーザオブジェクトを見つけて、それを選択する際に実行します。リストで 1 つまたは複数のオブジェクトを選択すると、タスクバーがアクティブになり、［ **[アカウント]**］および［ **[Exchange]**］のツールバーオプションとドロップダウンオプションが表示されます。ツールバーアイコンをマウスオーバーするか、ドロップダウンメニューをクリックして機能またはオプションを表示します。

ユーザアカウントを作成する

管理対象ドメインまたは管理対象サブツリー内にユーザアカウントが作成できます。また、プロパティの変更、メールボックスの作成、電子メールの有効化、および新しいアカウントへのグループメンバーシップの割り当てなどを実行することもできます。

注

- 企業によっては、新規ユーザアカウントに割り当てる名前に対し、ポリシーによって強制的に命名規則が適用される場合があります。
- デフォルトにより、新規ユーザアカウントは管理対象ドメインのユーザ OU の中に置かれます。
- DRA で InetOrgPerson オブジェクトを作成することはできません。

ユーザアカウントのクローンを作成する

ユーザアカウントのクローンを作成すると、そのユーザがメンバーになっているすべてのグループが新しいユーザアカウントに自動的に追加されるため、クローンとして作成されたアカウントのための設定時間が省けます。クローンとして作成されたアカウントに対しては、グループの追加または削除、およびメールの有効化など、様々なプロパティ設定を新規アカウントのときと同様に行うことができます。

注 : InetOrgPerson オブジェクトのクローンを作成するときには、ユーザアカウントを作成します。

ユーザアカウントのプロパティを変更する

管理対象ドメインまたは管理対象サブツリー内のユーザアカウントのプロパティを管理できます。変更できるユーザアカウントのプロパティは、ユーザの権限により異なります。Exchange をインストールし、Microsoft Exchange のサポートを有効にすれば、ユーザアカウントを管理しながら対応するメールボックスのプロパティを変更することができます。

注 : ホームディレクトリのポリシーを有効にすると、そのアカウントを管理するときにユーザアカウントのホームディレクトリが自動的に変更されます。たとえば、ホームディレクトリの場所を変更すると、指定されたホームディレクトリが作成され、前のホームディレクトリの内容が新しい場所に移動されます。元のディレクトリで割り当てられていた ACL も、新しいディレクトリに適用されます。

注 : DRA では、**[所属するグループ]** の結果を CSV ファイルとしてエクスポートできます。Web コンソールから［**[所属するグループ]**］の結果をエクスポートするには、［**[管理]**］>［**[検索]**］に移動し、［**[プロパティ]**］をクリックします。［**[所属するグループ]**］タブに移動し、［**[ダウンロード]**］アイコンをクリックします。保存されていない変更はエクスポートされません。最近の変更を保存して、エクスポートされたファイルで使用できるようにしてください。

ユーザアカウントを有効化する

管理対象ドメインまたは管理対象サブツリー内のユーザアカウントを有効にすることができます。Microsoft Windows アカウントを管理している場合、この変更が適用されるドメインコントローラを指定することができます。

変更を特定のドメインコントローラに適用する場合、その変更は同じ管理対象ドメインのデフォルトのドメインコントローラにも適用されます。デフォルトのドメインコントローラを検証するには、ドメインのプロパティを表示します。

ユーザアカウントを無効にする

管理対象ドメイン内のユーザアカウントを無効にすることができます。Microsoft Windows アカウントを管理している場合、この変更が適用されるドメインコントローラを指定することができます。

変更を特定のドメインコントローラに適用する場合、その変更は同じ管理対象ドメインのデフォルトのドメインコントローラにも適用されます。デフォルトのドメインコントローラを検証するには、ドメインのプロパティを表示します。

ユーザアカウントのロックを解除する

管理対象ドメインまたは管理対象サブツリー内にあるユーザアカウントのロックを解除できます。

DRA ではユーザアカウントのステータスがアカウントキャッシュから取得されるため、選択したアカウントが実際にはロックされているのにロックが解除されているものとしてユーザインタフェースに表示されることがあります。そのような場合でも、DRA ではユーザアカウントのロックを解除することができます。DRA コンソールを使用してユーザアカウントのロックを解除するとき、ドメインコントローラを指定することもできます。このとき、ユーザアカウントのパスワードをリセットする必要はありません。

ユーザアカウントのパスワードをリセットする

管理対象ドメインまたは管理対象サブツリー内のアカウントのパスワードをリセットできます。ユーザアカウントについて変更できるフィールドは、ユーザの権限により異なります。

ユーザアカウントのパスワードをリセットすると、そのアカウントのロックが自動的に解除されます。ユーザアカウントの新しいパスワードが DRA で自動的に生成されるようにするかどうかを選択できます。また、アカウントのパスワード関連のオプションも変更できます。Microsoft Windows のアカウントを管理している場合は、ドメインコントローラを指定して、そこに対して DRA にこれらの変更を適用させることができます。

注 : 変更を特定のドメインコントローラに適用する場合、その変更は同じ管理対象ドメインのデフォルトのドメインコントローラにも適用されます。デフォルトのドメインコントローラを検証するには、ドメインのプロパティを表示します。

ユーザアカウントを別のコンテナに移動する

管理対象ドメインまたは管理対象サブツリー内の別のコンテナ (OU など) にユーザアカウントを移動することができます。

ユーザアカウントを削除する

管理対象ドメインまたは管理対象サブツリー内のユーザアカウントを削除することができます。そのドメインでごみ箱が無効になっている場合、ユーザアカウントを削除すると、そのユーザアカウントは Active Directory から永久に削除されます。そのドメインでごみ箱が有効になっている場合、ユーザアカウントを削除すると、そのユーザアカウントはごみ箱に移動します。

警告 : ユーザアカウントを作成すると、Microsoft Windows によってそのアカウントに SID (Security Identifier) が割り当てられます。SID は、アカウント名からは生成されません。Microsoft Windows は、SID を使用して各リソースの ACL (Access Control Lists) に特権を記録します。ユーザアカウントを削除した場合、同じ名前のユーザアカウントを新規に作成しても、削除前のアクセス権を復活させることはできません。

ユーザアカウントにグループメンバーシップを指定する

管理対象ドメインまたは管理対象サブツリー内の特定グループにユーザアカウントを追加したり削除することができます。このアカウントが属す既存のグループのプロパティを表示し、変更することもできます。

ユーザアカウントの変換

DRA では、ユーザアカウントを簡単かつ効率的に変換できます。ユーザアカウントを持つ個人の職責が変更になったときに、DRA の変換機能が使用できます。職務内容テンプレートを使用して、アカウントに設定されたグループメンバーシップを簡単に追加、削除、または更新することができます。昇進、部署移動、退職のいずれであっても、ユーザアカウントの変換機能により、時間、お金、労力などが節約できます。

変換プロセスの概要

ユーザアカウントの変換機能は、次の目的に使用できます。

- ユーザアカウントに設定されたグループメンバーシップの削除
- ユーザアカウントへのグループメンバーシップの追加
- ユーザプロパティの変更
- 特定のグループメンバーシップを削除して同時に他のグループメンバーシップをユーザアカウントに追加する

ユーザアカウントを変更する前に、次のプロセスを検討してください。

1. グループメンバーシップの追加、削除、またはその両方を行う必要性を判断します。
2. 現在の削除および追加テンプレートを見直して、必要なテンプレートユーザアカウントがあることを確認します。
3. 必要に応じてテンプレートアカウントを作成します。
4. ［Transform User (ユーザの変換★)］ウィザードを終了します。

DRA によるユーザの変換により、削除テンプレートによって指定されたグループメンバーシップはユーザアカウントから削除され、追加テンプレートによって指定されたグループメンバーシップがユーザアカウントに割り当てられます。削除テンプレートまたは追加テンプレートにないメンバーシップは影響を受けません。たとえば、1 人の海外営業部員が米国営業課から欧州営業課へと転属になったとします。その会社には配布グループとセキュリティグループの両方があり、それぞれが対応する営業課独自のグループであり、数はすべての営業課で共有されています。米国営業課には「米国重点地域 DL」および「米国営業管理 DL」という流通グループがあり、欧州営業課には「欧州重点地域」および「欧州営業管理」という流通グループがあります。両課とも「グローバル営業セキュリティ」というセキュリティグループのメンバーですが、個別に地域固有のセキュリティグループも持っています。

削除テンプレート「米国営業テンプレート」には次のグループメンバーシップが指定されています。

- 米国重点地域 DL
- 米国営業管理 DL
- グローバル営業セキュリティ
- 米国セキュリティ

追加テンプレート「欧州営業テンプレート」には次のグループメンバーシップが指定されます。

- 欧州重点地域 DL
- 欧州営業管理 DL
- グローバル営業セキュリティ
- 欧州セキュリティ

変換プロセス中に、転属された営業部員のユーザアカウントはまず、「米国営業テンプレート」によって指定されたすべてのグループメンバーシップから削除され、「欧州営業テンプレート」によって指定されたすべてのグループメンバーシップに追加されます。仮にこの社員が「ポーカー仲間」という配布グループのメンバーでもある場合、このグループメンバーシップは変更されません。

次の権限を付与すれば、アシスタント管理者が変換プロセス中にユーザアカウントをさらに変更することができます。

- ユーザアカウントの変換と同時に所在地プロパティを変更
- ユーザアカウントの変換と同時に説明を変更
- ユーザアカウントの変換と同時に事務所を変更
- ユーザアカウントの変換と同時に電話プロパティを変更

また、グループメンバーシップを追加または削除する権限を限定することもできます。それには、次に挙げる権限のいずれかのみをアシスタント管理者に与えます。

- テンプレート内に存在するグループにユーザを追加
- テンプレート内に存在するグループからユーザを削除

権限を応用したこのような制限オプションのいずれかを使うことで自社のセキュリティに厚みが増します。テンプレートに存在するグループだけを削除するだけの権限を特定の社員に付与する形で、暫定のユーザアカウントが作成できます。これらの暫定アカウントは、別のアシスタント管理者が追加テンプレートのアカウントを使って新しいグループメンバーシップを付与してしまう前に、検証することができます。

ユーザ変換テンプレートの作成

ユーザアカウントの変換は、社内での役割と職務に直接連携しています。社内の役割や職務ごとにテンプレートを作成することを検討してください。DRA では、削除テンプレートとして使用されるユーザアカウントと追加テンプレートとして使用されるユーザアカウントを区別しません。社内での役割ごとにテンプレートユーザアカウントを 1 つ作成してください。変換中に、テンプレートを削除または追加として選択します。削除テンプレートとして選択したテンプレートを、後の変換処理で追加テンプレートとして使用することもできます。

ユーザ変換テンプレートを作成するには、ユーザアカウントを作成し、そのユーザアカウントに適切なグループを割り当てる権限がなければなりません。これらの権限をは、適切な ActiveView で Create and Delete User Accounts および Group Administration という各役割をアカウントに関連付けるか、個々の権限を割り当てることで、取得できます。

ユーザアカウントの変換

ユーザアカウントを変換することで、ユーザアカウントグループメンバーシップの追加と削除のいずれか、またはその両方が実行できます。社内での人事異動の際に、このワークフローを使用します。Transform a User という役割か、ユーザアカウントを変更するための

権限を含んでいる役割を持っていなければなりません。この機能は、Delegation and Configuration console (委任および環境設定コンソール) から Account and Resource Management ノードを介してのみ実行できます。

ユーザアカウントを変更するには、次の手順を実行してください。

1 左側の表示枠にある［ **[すべての管理対象オブジェクト]**］を開きます。

2 管理するユーザアカウントを指定するには、［ **[Find Now (今すぐ検索★)]**］という操作を実行してユーザオブジェクトを見つけ、それを選択します。

3 ［ **[タスク]**］>［ **[変換]**］をクリックします。

4 ［ようこそ］ウィンドウを確認してから、［ **[次へ]**］をクリックします。

5 ［Select User Template (ユーザテンプレートの選択★)］ウィンドウで、［ **[ブラウズ]**］を使用して適切な削除テンプレートユーザを選択します。

6 削除テンプレートのユーザアカウントのプロパティを確認する必要がある場合は、［ **[表示]**］をクリックします。

7 ［ **[ブラウズ]**］を使用して、適切な追加テンプレートユーザを選択します。

8 追加テンプレートユーザアカウントのプロパティを確認するには、［ **[表示]**］をクリックします。

9 適切な権限があるユーザであれば、［ **[Change other properties of the user (このユーザの他のプロパティを変更する★)]**］にチェックマークを入れて、変更するプロパティを選択することができます。［ **[次へ]**］をクリックして、使用可能なプロパティまで移動します。

10 ［ **[次へ]**］をクリックします。

11 ［Summary (概要★)］ウィンドウの内容を確認したら、［ **[Finish (終了★)]**］をクリックします。

グループを管理する

アシスタント管理者として、DRA を使用してグループ管理およびグループプロパティの変更を行うことができます。グループ化により、定義された一連のユーザアカウントに特定のパーミッションを与えることができます。グループを使用して、任意のドメイン内でユーザアカウントがアクセスできるデータとリソースを管理することができます。

任意の種類および範囲のグループを管理することができます。たとえば、グループをネストして、1 つのグループに別のグループのパーミッションを継承させることができます。信頼するドメインのグループを管理対象ドメイン内の別のグループに追加したり、一時的なグループ指定を管理することにより、ドメイン全体のグループメンバーシップを効率的に管理することもできます。

グループの管理の詳細については、次のトピックを参照してください。

- 57 ページの 「グループ管理タスク」
- 60 ページの「Delegation and Configuration Console (委任および環境設定コンソール) での一時的なグループの割り当ての管理」
- 61 ページの 「Web コンソールで一時的なグループの割り当てを管理する」

グループ管理タスク

このセクションでは、Account and Resource Management ノードを介して、Delegation and Configuration console (委任および環境設定コンソール) でグループを管理する方法について説明します。適切な権限があれば、グループメンバーシップの変更など、さまざまなグループ管理タスクを実行することができます。複数のグループを選択した場合、グループに対するメンバーの追加、削除、移動など、選択したタスクを 1 回の操作で実行できます。1 つまたは複数のグループを選択すると、実行できるタスクが［タスク］メニューに表示されます。

グループにアカウントを追加する

ユーザアカウント、連絡先、およびコンピュータを管理グループに追加することができます。

注 : このタスクは、複数のアカウントを指定グループに追加します。1 つのアカウントをグループに追加するには、アカウントを選択して、［タスク］メニューの［グループに追加］をクリックします。

別のグループへのアカウントの追加により、そのアカウントに対する権限が増える場合には、そのアカウントの追加は許可されません。

グループを他のグループに追加する

別の管理対象グループにグループを追加することによってグループを入れ子にすることができます。グループが別のグループの入れ子になっている場合、子のグループは親のグループからパーミッションを継承できます。

注 : 別のグループにグループを追加することにより、そのグループに対する権限が増える場合には、そのグループの追加は許可されません。

グループのプロパティを変更する

ローカルグループとグローバルグループのプロパティを変更することができます。所有する権限により、管理対象ドメインまたは管理対象サブツリー内のグループに対して変更できるプロパティが異なります。Exchange をインストールし、Microsoft Exchange のサポートを有効にすれば、グループを管理しながら配布リストのプロパティを変更することができます。

グループを作成する

管理対象ドメインまたは管理対象サブツリー内にグループを作成することができます。新しいグループのグループメンバーなどのプロパティを変更することもできます。

注

- 企業によっては、新しいグループに割り当てる名前にポリシーを通して命名規則が適用される場合があります。
- デフォルトでは、新しいグループが管理対象ドメインのユーザ OU の中に置かれます。

グループメンバーを指定する

管理グループに対して、ユーザアカウント、連絡先、コンピュータ、または他のグループを追加または削除できます。DRA は、外部のセキュリティプリンシパルの削除のみ許可します。既存グループメンバーのプロパティを表示および変更することもできます (外部のセキュリティプリンシパルを除く)。

グループからメンバーを削除しても、メンバーであるオブジェクトは削除されません。メンバーをグループに追加するときには、追加するメンバーオブジェクトを変更する権限がなければなりません。

注

- Windows の管理者または特別なグループのメンバーでない限り、Windows の特別なグループ (Administrators グループ、アカウントオペレータグループ、バックアップオペレータグループ、サーバーオペレータグループなど) にユーザアカウントやグループを追加することはできません。
- DRA では、[メンバー] の結果を CSV ファイルとしてエクスポートできます。Web コンソールから [メンバー] の結果をエクスポートするには、[[管理]] > [[検索]] に移動し、[[プロパティ]] をクリックします。[[メンバー]] タブに移動し、[[ダウンロード]] アイコンをクリックします。保存されていない変更はエクスポートされません。最近の変更を保存して、エクスポートされたファイルで使用できるようにしてください。

グループにグループメンバーシップを指定する

管理対象ドメインまたは管理対象サブツリー内の別のグループにグループを追加したり削除することができます。グループが属す既存のグループのプロパティを表示し、変更することもできます。

注 : DRA では、[所属するグループ] の結果を CSV ファイルとしてエクスポートできます。Web コンソールから [[所属するグループ]] の結果をエクスポートするには、[[管理]] > [[検索]] に移動し、[[プロパティ]] をクリックします。[[所属するグループ]] タブに移動し、[[ダウンロード]] アイコンをクリックします。保存されていない変更はエクスポートされません。最近の変更を保存して、エクスポートされたファイルで使用できるようにしてください。

グループメンバーシップのセキュリティパーミッションを設定する

グループメンバーシップに Active Directory のセキュリティ権限を設定することができます。これらのパーミッションにより、Microsoft Outlook を使用してグループメンバーシップを表示 (読み込み) および変更 (書き込み) できるユーザが指定されます。これらの設定を使用して、環境内の配布リストおよびセキュリティグループの安全性を高めることができます。継承したセキュリティパーミッションを変更することはできません。

注 : グループメンバーシップのセキュリティを管理するときに、オフになっているパーミッションが継承されたパーミッションを示す場合があります。

グループの所有権を設定する

Microsoft Windows の配布グループおよびセキュリティグループの所有権を設定することができます。グループ所有権のパーミッションは、ユーザアカウント、グループ、または連絡先に付与することができます。グループ所有権が付与されると、ユーザアカウント、グループ、または連絡先がそのグループのメンバーシップを変更することができます。

注 : グループメンバーシップが Microsoft Exchange サーバから隠れている場合は、DRA が［**[Manager can update membership list (マネージャがメンバーシップリストを更新できる★)]**］というチェックボックスを無効にします。このチェックボックスを有効にするには、［Group Properties (グループプロパティ★)］ウィンドウで［Exchange (変換★)］タブの［**[Expose Group Membership (グループメンバーシップを表示する★)]**］をクリックします。

グループのクローンを作成する

管理対象ドメイン内のローカルグループとグローバルグループの両方でクローンが作成できます。グループのクローンを作成することにより、元のグループと同じ種類および属性を持つ新しいグループを作成することができます。また、元のグループのすべてのメンバーが新しいグループに追加されます。

グループのクローンを作成することにより、同様のプロパティを持つ他のグループをベースとして簡単にグループを作成することができます。グループのクローンを作成すると、選択されたグループの値が［Clone Group (グループのクローン作成★)］ウィザードに設定されます。新しいグループのプロパティを変更することもできます。

注

- 企業によっては、新しいグループに割り当てる名前にポリシーを通して命名規則が適用される場合があります。
- デフォルトでは、新しいグループが管理対象ドメインのユーザ OU の中に置かれます。

グループを削除する

管理対象ドメインまたは管理対象サブツリー内のローカルグループとグローバルグループが削除できます。そのドメインでゴミ箱が無効になっている場合は、グループを永久に削除すると、そのグループは Active Directory から削除されます。そのドメインでごみ箱が有効になっている場合は、グループを削除すると、そのグループはごみ箱に移動し、グループのプロパティが無効になります。

ごみ箱の詳細については、「ごみ箱の管理」を参照してください。

警告 : グループを作成すると、Microsoft Windows によってそのグループに SID (Security Identifier) が割り当てられます。SID は、グループ名からは生成されません。Microsoft Windows は、SID を使用して各リソースの ACL (Access Control Lists) に特権を記録します。グループを削除する場合は、同一名を使用して新規のグループを作成することにより、そのグループのアクセス権を戻すことはできません。

別のコンテナにグループを移動する

管理対象ドメインまたは管理対象サブツリー内の別のコンテナ (OU など) にグループを移動することができます。

グループメンバーシップを配布リストに表示させる

管理対象ドメインまたは管理対象サブツリー内のグループのメンバーシップを配布リストに表示させることができます。

配布リストでグループメンバーシップを非表示にする

管理対象ドメインまたは管理対象サブツリー内のグループのメンバーシップを配布リストで非表示にすることができます。

Delegation and Configuration Console (委任および環境設定コンソール) での一時的なグループの割り当ての管理

一時的なグループの割り当てでは、特定の期間だけグループメンバーシップを必要とするユーザのグループメンバーシップを管理することができます。このセクションでは、[Account and Resource Management] の Delegation and Configuration console (委任および環境設定コンソール) で一時的なグループの割り当てを管理する方法について説明します。適切な権限があれば、一時的なグループの割り当ての作成や期限が切れた一時的なグループの割り当ての削除などのタスクを実行できます。

アシスタント管理者は、アシスタント管理者がグループメンバーシップを変更する (メンバーを追加または削除する) 権限を持つグループの一時的なグループの割り当てのみを表示できます。

一時的なグループの割り当てがアクティブ状態にある間は、関連付けられたグループを変更したり、ユーザのリストを変更したりすることはできません。これらの項目を変更する場合は、一時的なグループの割り当てをキャンセルする必要があります。

一時的なグループの割り当てのプロパティを管理する

一時的なグループの割り当てまたは期限切れになった一時的なグループの割り当てのプロパティを管理できます。

一時的なグループの割り当てを再スケジュールするには、割り当ての［[プロパティ]］でスケジュールを変更し、変更内容を保存します。

一時的なグループの割り当てを作成する

プライマリ管理サーバおよびセカンダリ管理サーバに一時的なグループの割り当てを作成することができます。

デフォルトでは、一時的なグループの割り当ての期限が切れると、［[今後の使用に備えて、この一時的なグループの割り当てを保持します]］というオプションを選択しない限り、7 日後に削除されます。この保持期間を変更するには、［すべての管理対象オブジェクト］の下にある［[一時的なグループの割り当て]］ノードを右クリックし、［[プロパティ]］を選択して、一時的なグループの割り当てを保持する日数を変更します。

一時的なグループの割り当てでユーザアカウントを管理する

プライマリ管理サーバおよびセカンダリ管理サーバ上で、一時的なグループの割り当てにユーザアカウントを追加または削除することができます。

注 : まだアクティブになっていない一時的なグループの割り当てのユーザアカウントのみを管理できます。

一時的なグループの割り当てを削除する

一時的なグループの割り当ては、プライマリ管理サーバおよびセカンダリ管理サーバ上で削除することができます。

Web コンソールで一時的なグループの割り当てを管理する

一時的なグループの割り当てにより、特定の期間だけグループメンバーシップを必要とするユーザのグループメンバーシップを管理することができます。Azure Active Directory が DRA 管理者によって設定されている場合、Azure グループの一時的なグループの割り当てを作成し、Azure ユーザと同期されたユーザを Azure グループメンバーシップに追加できます。Web コンソールでは、DRA プライマリサーバとセカンダリサーバの両方からの割り当てを作成および管理できます。ただし、既存の割り当てに対して実行できるアクションは、割り当てがどの状態にあるかによって異なります。

アシスタント管理者は、グループメンバーの追加や削除などの、ActiveView の割り当てによって変更する権限を持つグループに対してのみ一時的なグループの割り当てを表示できます。

Web コンソールで一時的なグループの割り当てを管理するには、[**[タスク]**] > [**[一時的なグループの割り当て]**] の順に移動します。

次のアクションを実行できます。

一時的なグループの割り当てを作成する

ドメインコントローラを変更および指定する権限を持っているグループを使用して、一時的なグループの割り当てを作成できます。ターゲットグループは、Azure 管理対象テナントのグループ、または Active Directory ドメインのグループにできます。一時的なグループの割り当てが期限切れになると、今後の試用に備えて、一時的なグループの割り当てを保持するオプションを選択しない限り、DRA は 7 日後に自動的にそれを削除します。

注 : Azure グループメンバーシップを持つ設定済みの一時的なグループの割り当てが DRA の外部で変更された場合、一時的なグループの割り当ては無効になります。

一時的なグループの割り当てを作成するには、次の手順を実行します。

1. [**[タスク]**] > [**[一時的なグループの割り当て]**] に移動し、[**[作成]**] をクリックします。
2. [**[選択]**] をクリックし、該当するコンテナで検索を実行してグループを検索します。

3. グループにメンバーを追加する必要がある場合は、［一時的なグループの割り当ての作成］ページの［[メンバー]］の下の［[追加]］をクリックし、結果リストの［[追加] ✚］オプションを見つけて使用して、メンバーをグループに追加します。
4. スケジュールを設定します。
5. ［一般情報］の下の TGA に名前を付け、［[作成]］をクリックします。

既存の割り当てを検索する

既存の一時的なグループの割り当て (TGA) を検索すると、割り当てのステータスに基づいて結果にリストされます。これには、次の状態が含まれます。

- **保留中 :** TGA は今後開始されるようにスケジュールされています。キャンセル、削除、および再スケジュールを実行できます。
- **アクティブ :** TGA が開始され、該当するメンバーがグループに追加されました。キャンセルおよび削除を実行できます。
- **アクティブ (エラーあり):** TGA は開始されていますが、該当するすべてのメンバーをグループに追加できませんでした。キャンセルおよび削除を実行できます。
- **完了 :** TGA が期限切れになったため、該当するすべてのメンバーがグループから削除されました。削除および再スケジュールを実行できます。
- **完了 (エラーあり):** TGA は期限切れになっていますが、該当するすべてのメンバーをグループから削除できませんでした。削除および再スケジュールを実行できます。
- **キャンセル :** TGA がユーザによってキャンセルされ、該当するすべてのメンバーがグループから削除されました。削除および再スケジュールを実行できます。
- **キャンセル (エラーあり):** TGA はユーザによってキャンセルされましたが、該当するすべてのメンバーをグループから削除できませんでした。削除および再スケジュールを実行できます。
- **エラー :** TGA はすべてのメンバーを追加または削除できませんでした。削除および再スケジュールを実行できます。

これらの状態、および割り当て名、ターゲットグループ、期間、割り当てを作成した管理者などを含むその他の条件に基づいて結果をフィルタすることができます。

一時的なグループの割り当てのプロパティを表示または変更する

一時的なグループの割り当てが作成されたときに定義された一時的なグループの割り当てを表示したり、変更したりできます。一時的なグループの割り当ての検索を実行した後で、プロパティを表示または変更したい割り当てを選択します。

一時的なグループの割り当てを再スケジュールするには、割り当ての［[プロパティ]］でスケジュールを変更し、変更内容を保存します。割り当てがアクティブ状態である場合は、終了日のみ変更できます。

重要 : 一時的なグループの割り当てがアクティブ状態である場合は、関連付けられたグループを変更したり、ユーザのリストを変更したりすることはできません。これらの項目を変更する場合は、まず割り当てをキャンセルする必要があります。

一時的なグループの割り当てをキャンセルする

一時的なグループの割り当ては、次のいずれかの状態になっている場合のみキャンセルできます。

- アクティブ
- アクティブ (エラーあり)
- 保留中

一時的なグループの割り当てを削除する

複数の一時的なグループの割り当てを選択し、それらを削除できます。選択した一時的なグループの割り当ての状態が［アクティブ］、［アクティブ (エラーあり)］、または［保留中］の場合は、［ **[キャンセル]**］オプションも有効になります。

ダイナミック配布グループの管理

ダイナミック配布グループとは、メールが有効な Active Directory のグループオブジェクトです。電子メールメッセージやその他の情報を迅速に大量送信をするために作成することができます。

ダイナミック配布グループのメンバーシップリストは、グループにメッセージが送信されるたびに、定義するフィルタおよび条件に基づいて計算されます。これは、定義されたメンバーセットを含む正規の配布グループとは異なります。電子メールメッセージがダイナミック配布グループに送信されると、組織内でそのグループに定義されている条件に一致する受信者に届きます。

DRA がサポートする機能は次のとおりです。

- 監査と UI レポーティング
- ダイナミック配布グループの列挙のサポート
- ダイナミック配布グループの NetIQ Reporting Center (NRC) レポート
- ダイナミック配布グループのトリガ操作のサポート
- Exchange のダイナミック配布グループの UI 拡張機能のサポート

ダイナミック配布グループのタスク :

ダイナミック配布グループを作成する

管理対象ドメインまたは管理対象サブツリーの中にダイナミック配布グループを作成することができます。また、新規のダイナミック配布グループに関し、グループメンバーなどのプロパティを変更することもできます。

注

- 企業によってはポリシーで命名規則が定められている場合があります。その場合は、その規則に従って新規のダイナミック配布グループに割り当てられる名前が決まります。
- デフォルトでは、DRA が新規のダイナミック配布グループを管理対象ドメインのユーザ OU の中に配置します。

Delegation and Configuration Console (委任および環境設定コンソール) でダイナミック配布グループを作成するには、次の手順を実行します。

1. Account and Resource Management ノードの［すべての管理対象オブジェクト］からグループを作成するコンテナを選択します。
2. タスクメニューで［[新規]］>［[ダイナミック配布グループ]］を選択します。
3. ウィザードに表示される手順を実行します。

Web コンソールでダイナミック配布グループを作成するには、次の手順を実行します。

1. [管理] のマストヘッドを選択し、Account and Resource Management ノードの［すべての管理対象オブジェクト］からグループを作成するコンテナを選択します。
2. ［作成］ドロップダウンメニューから［[ダイナミック配布グループ]］を選択します。
3. フォームに必要な情報を入力し、［[作成]］をクリックします。

ダイナミック配布グループのクローンを作成する

管理対象ドメイン内のローカルとグローバルのダイナミック配布グループの両方でクローンを作成することができます。ダイナミック配布グループのクローンを作成することにより、元のダイナミック配布グループと同じ種類および属性を持つダイナミック配布グループを新たに作成することができます。

ダイナミック配布グループのクローンを作成することにより、同様のプロパティを持つ別のダイナミック配布グループをベースにして簡単にダイナミック配布グループを作成することができます。ダイナミック配布グループのクローンを作成すると、その選択されたダイナミック配布グループの値を使って［ダイナミック配布グループのクローンを作成する］ウィザードの設定が行われます。新しいダイナミック配布グループのプロパティを変更することもできます。

ダイナミック配布グループを別のコンテナに移動する

管理対象ドメインまたは管理対象サブツリー内にある別のコンテナ (OU など) にダイナミック配布グループを移動することができます。

ダイナミック配布グループを削除する

管理対象ドメインまたは管理対象サブツリーの中のローカルおよびグローバルのダイナミック配布グループを削除できます。そのドメインでごみ箱が無効になっている場合、ダイナミック配布グループを削除すると、そのダイナミック配布グループは Active Directory から永久に削除されます。そのドメインでごみ箱が有効になっている場合、ダイナミック配布グループを削除すると、そのダイナミック配布グループはごみ箱に移動し、ダイナミック配布グループのプロパティが無効になります。

ごみ箱の詳細については、「ごみ箱の管理」を参照してください。

警告 : ダイナミック配布グループを作成するとき、Microsoft Windows によって SID (Security Identifier) がそのダイナミック配布グループに割り当てられます。SID はダイナミック配布グループ名から生成されるものではありません。Microsoft Windows は、SID を使用して各リソースの ACL (Access Control Lists) に特権を記録します。ダイナミック配布グループを削除した場合、それと同じ名前で新規にダイナミック配布グループを作成しても、削除前のダイナミック配布グループのアクセス権を復活させることはできません。

ダイナミック配布グループのプロパティを変更する

ローカルおよびグローバルのダイナミック配布グループのプロパティを変更することができます。所有する権限により、管理対象ドメインまたは管理対象サブツリー内のグループに対して変更できるプロパティが異なります。

フィルタを指定する

ダイナミック配布リストのメンバーシップは、そのフィルタで決まり、そのフィルタはユーザが定義できます。

条件を指定する

条件には、ダイナミック配布グループのメンバーになるためにオブジェクトが満たす必要のある基準が定義されます。

ダイナミックグループの管理

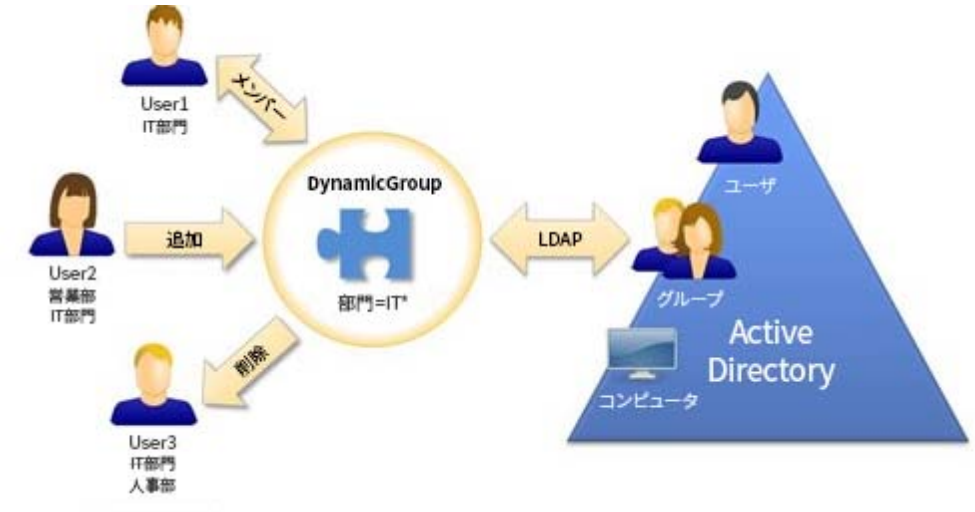
ダイナミックグループとは、定義された一連の基準に基づいてメンバーシップが変わるグループです。DRA では、Exchange 環境がなくてもダイナミックグループを作成することができます。Active Directory でダイナミックグループを管理するために使用されるメンバーシップフィルタは、DRA に固有のものです。

DRA 管理者は、Delegation and Configuration Console (委任および環境設定コンソール) でダイナミックグループのドメイン更新スケジュールを設定します。グループのメンバーフィルタ条件に一致する 1 つ以上のユーザプロパティがアップデートされ、更新が行われると、新しいメンバーがグループに動的に追加されます。同様に、一致するプロパティが変更またはユーザから削除されると、メンバーがグループから動的に削除されることがあります。

シナリオの例

Active Directory のダイナミックグループでの一般的な使用について、次の図で説明します。この図には、ダイナミックグループが 3 つあります。各グループに一連の基準があり、その基準によってそのグループに追加できるユーザとできないユーザが決まります。各グループが、ファイル、フォルダ、およびアプリケーションへのアクセスを制御します。

ヒント : ダイナミックグループの永続メンバーを含める「*スタティックメンバーリスト*」と、特定のユーザにダイナミックグループのメンバーシップを持たせないようにする「*除外されたメンバーリスト*」が作成できます。



最近 User2 が IT 部門に加わりました。そのユーザは、IT 部門のダイナミックグループが更新されると、グループに追加されます。User2 は、営業部のダイナミックグループが更新されるときに、そのメンバーのリストから削除されます。

User3 は、IT 部門から人事部に異動したため、IT 部門のダイナミックグループから削除され、人事部のダイナミックグループに追加されます。

シナリオの準備

次の情報は、上記のシナリオを可能にするために Web コンソールで実行するアクションの例を示しています。既存のグループをダイナミックにしたり、新しいダイナミックグループを作成することができます。簡略化のため、スタティックメンバーや除外メンバーは追加せず、既存の 3 つのグループ (HR グループ、IT グループ、セールスグループ) をダイナミックに設定します。

ダイナミックグループの設定 :

1. 上記の各グループに対して、グループフィルタを有効にした検索操作を実行して、グループを検索します。
2. グループの [**[プロパティ]**] を開き、[**[ダイナミックメンバーフィルタ]**] ページにアクセスします。
3. [**[グループをダイナミックにする]**] スライダをクリックして、この機能を有効にします。
4. [**[変更]**] をクリックし、[LDAP クエリ] フィールドにメンバーフィルタ条件を入力または貼り付けます。この場合は、[**[ユーザ]**]>[**[部門]**] プロパティの条件を探します。次の例は、シナリオの例で各グループに使用する LDAP 条件を示しています。
   - HR グループ : *(&(objectClass=user)(objectCategory=person)(department=HR*))*
   - IT グループ : *(&(objectClass=user)(objectCategory=person)(department=IT*))*
   - セールスグループ : *(&(objectClass=user)(objectCategory=person)(department=Sales*))*
5. **[適用]** をクリックして変更内容を保存します。

選択したユーザのプロパティでユーザのグループ提携を動的に変更するために実行されるアクション :

- User2: [[組織]]>[[部門]] プロパティが「セールス」から「IT」に変更されました。
- User3: [[組織]]>[[部門]] プロパティが「IT」から「HR」に変更されました。

動的な変更は、スケジュールされたダイナミックグループの更新中、または DRA 管理者によって手動で更新された場合に行われます。

ダイナミックグループタスク

Web コンソールで実行できるダイナミックグループタスクについて、次に説明します。

ダイナミックグループを作成する

管理対象ドメインまたは管理対象サブツリーの中にダイナミックグループを作成することができます。また、新しいダイナミックグループのグループメンバーなどのプロパティを変更することもできます。新しいダイナミックグループを作成するには、管理マストヘッドの [[作成]]>[[ダイナミックグループ]] に移動します。

注 : 企業によってはポリシーで命名規則が定められている場合があります。その場合は、その規則によって新規のダイナミックグループに割り当てられる名前が決まります。

フィルタを作成する

ダイナミックグループは、グループが更新されるたびに、[ダイナミックメンバーフィルタ] を使用してメンバーシップリストからユーザを追加または削除します。フィルタに対する LDAP および仮想属性クエリの作成例については、「「詳細検索クエリ」」に示す例を参照してください。フィルタは、検索ではなくグループメンバーシップの条件として機能しますが、クエリの例は引き続き適用できます。

- LDAP クエリの例
- 仮想属性クエリの例

スタティックメンバーリストを管理する

ダイナミックグループのスタティックメンバーリストに入っているユーザは、手動で削除されない限り、永続的にそのグループのメンバーです。このリストは、選択したユーザの [ダイナミックメンバーフィルタ] プロパティページから変更できます。

ダイナミックグループからメンバーを削除しても、メンバーであるオブジェクトは削除されません。メンバーをダイナミックグループに追加するときには、追加するメンバーオブジェクトに対し変更できる権限がなければなりません。

除外されたメンバーリストを管理する

ダイナミックグループの除外されたメンバーリストに入っているユーザは、手動でこのリストから削除されない限り、グループに加わることができません。このリストは、選択したユーザの [ダイナミックメンバーフィルタ] プロパティページから変更できます。

メンバーリストを更新する

ダイナミックグループ内のメンバーを［ [Update Members (メンバーを更新★)]］という操作で更新することができます。

ダイナミックグループのクローンを作成する

管理対象ドメイン内のローカルとグローバルのダイナミックグループの両方でクローンを作成することができます。ダイナミックグループのクローン作成では、元のダイナミックグループと同じ種類および属性を持つダイナミックグループが新たに作成されます。

ダイナミックグループを作成することにより、同様のプロパティを持つ他のダイナミックグループをベースにして簡単にダイナミックグループを作成することができます。ダイナミックグループのクローンを作成するときは、その選択されたダイナミックグループの値を使って［ダイナミックグループのクローンを作成する］ウィザードの設定が行われます。新しいダイナミックグループのプロパティは変更することもできます。

ダイナミックグループのクローンを作成するには、[検索結果] ペインでグループを選択し、ツールバーの [[クローン]] をクリックします。

ダイナミックグループを別のコンテナに移動する

管理対象ドメインまたは管理対象サブツリー内にある別のコンテナ (OU など) にダイナミックグループを移動することができます。

ダイナミックグループを移動するには、[検索結果] ペインでグループを選択し、ツールバーの [[オブジェクトの移動]] をクリックします。

ダイナミックグループを削除する

管理対象ドメインまたは管理対象サブツリーの中のローカルとグローバルのダイナミックグループを削除できます。そのドメインでごみ箱が無効になっている場合、削除されたダイナミックグループは Active Directory から永久に削除されます。そのドメインでごみ箱が有効になっている場合、ダイナミックグループを削除すると、そのダイナミックグループはごみ箱に移動し、ダイナミックグループのプロパティが無効になります。ごみ箱の詳細については、「ごみ箱の管理」を参照してください。

ダイナミックグループを削除するには、[検索結果] ペインでグループを選択し、ツールバーの [[削除]] をクリックします。

警告 : ダイナミックグループを作成するとき、Microsoft Windows によって SID (Security Identifier) がそのダイナミックグループに割り当てられます。SID はダイナミックグループ名から生成されるものではありません。Microsoft Windows は、SID を使用して各リソースの ACL (Access Control Lists) に特権を記録します。ダイナミックグループを削除した場合、それと同じ名前で新規にダイナミックグループを作成しても、削除前のダイナミックグループのアクセス権を復活させることはできません。

ダイナミックグループのプロパティを変更する

ローカルおよびグローバルのダイナミックグループのプロパティを変更することができます。所有する権限により、管理対象ドメインまたは管理対象サブツリー内のグループに対して変更できるプロパティが異なります。

注 : DRA では、[メンバー] および [所属するグループ] の結果を CSV ファイルとしてエクスポートできます。Web コンソールから [メンバー] または [所属するグループ] の結果をエクスポートするには、[[管理]] > [[検索]] に移動し、[[プロパティ]] をクリックします。[[メンバー]] タブまたは [[所属するグループ]] タブに移動し、[[ダウンロード]] アイコンをクリックします。保存されていない変更はエクスポートされません。最近の変更を保存して、エクスポートされたファイルで使用できるようにしてください。

ダイナミックグループのプロパティを変更するには、[検索結果] ペインでグループを選択し、ツールバーの [[プロパティ]] をクリックします。

ダイナミックグループを別のダイナミックグループを追加する

別の管理対象グループにダイナミックグループを追加することによって、ダイナミックグループをネストさせることができます。ダイナミックグループが別のダイナミックグループの中にネストされると、子のダイナミックグループは親のダイナミックグループからパーミッションを継承できます。

ダイナミックグループを別のダイナミックグループに追加するには、[検索結果] ペインでグループを選択し、ツールバーの [[グループに追加]] をクリックします。

注 : ダイナミックグループを別のダイナミックグループに追加することによってそのダイナミックグループに対する権限が増える場合、DRA はそのダイナミックグループの追加を許可しません。

グループメンバーシップのセキュリティパーミッションを設定する

ダイナミックグループのメンバーシップに対し Active Directory のセキュリティパーミッションを設定することができます。これらのパーミッションで、Microsoft Outlook を使用してダイナミックグループのメンバーシップの表示 (読み込み) が行えるユーザと、変更 (書き込み) も行えるユーザを指定します。これらの設定を使用することで、環境内の配布リストおよびセキュリティダイナミックグループの安全性をより効率的に確保することができます。継承したセキュリティパーミッションを変更することはできません。

これらの設定は、選択したダイナミックグループの [[メンバーシップセキュリティ]] プロパティページから更新できます。

注 : ダイナミックグループメンバーシップのセキュリティを管理するとき、オフになっているパーミッションが継承されたパーミッションを示している場合があります。

ダイナミックグループの所有権を設定する

ダイナミックグループの所有者のパーミッションをユーザアカウント、グループ、または連絡先に付与することができます。ダイナミックグループの所有者の権限を付与されると、指定されたユーザアカウント、グループ、または連絡先がそのダイナミックグループのメンバーシップを変更できるようになります。

これらの設定は、選択したダイナミックグループの [[管理者]] プロパティページから更新できます。

ダイナミックグループのメンバーシップを配布リストに公開する

ダイナミックグループのメンバーシップは、管理対象ドメインまたは管理対象サブツリー内のグループのための配布リストに表示させることができます。

このオプションには、選択したダイナミックグループのツールバーの [[Exchange]] ドロップダウンメニューからアクセスできます。

ダイナミックグループのメンバーシップを配布リストで非表示にする

ダイナミックグループのメンバーシップは、管理対象ドメインまたは管理対象サブツリー内のグループのための配布リストに表示されないようにすることができます。

このオプションには、選択したダイナミックグループのツールバーの [[Exchange]] ドロップダウンメニューからアクセスできます。

注 : Microsoft Exchange 2007 の配布リストでは、[[Hide Group Membership (グループのメンバーシップを隠す★)]] というオプションが無効になっています。

連絡先を管理する

連絡先や関連する電子メールアドレスなど、多数のネットワークオブジェクトが DRA で管理できます。連絡先は、混合モードまたはネイティブ Microsoft Windows ドメインでのみ使用できます。連絡先には、ユーザアカウントやグループと同様に、SID (Security Identifier) があります。連絡先を使用して、ネットワークサービスへのアクセスを許可せずにメンバーを配布リストやグループに追加することができます。

混合モードまたはネイティブモードドメインの中のセキュリティまたは配布グループに連絡先を追加することができます。Microsoft Windows では配布リストとしてセキュリティグループを使用できるため、連絡先をこれらのグループに追加すると便利な場合があります。グローバルセキュリティグループに連絡先が含まれていても、ネイティブモードの Microsoft Windows ドメインに移行するときにそのグループをユニバーサルセキュリティグループに変換することができます。

次に挙げるタスクのほとんどが Web コンソールの［ [管理]］>［ [検索]］タブから実行できます。検索操作を実行して、必要な連絡先を見つけて選択します。リストで 1 つまたは複数の連絡先を選択すると、タスクバーがアクティブになり、[[Exchange]］のツールバーオプションとドロップダウンオプションが表示されます。ツールバーアイコンをマウスオーバーするか、ドロップダウンメニューをクリックして機能またはオプションを表示します。

連絡先のプロパティを変更する

連絡先のプロパティは変更することができます。所有する権限により、管理対象ドメイン内の連絡先に対して変更できるプロパティが異なります。Exchange をインストールし、Microsoft Exchange のサポートを有効にすれば、連絡先を管理しながら電子メールアドレスのプロパティを変更することができます。

注 : DRA では、[所属するグループ] の結果を CSV ファイルとしてエクスポートできます。Web コンソールから［ [所属するグループ]］の結果をエクスポートするには、[[管理]］>［ [検索]］に移動し、［ [プロパティ]］をクリックします。[[所属するグ

ループ]］タブに移動し、[[ダウンロード]］アイコンをクリックします。保存されていない変更はエクスポートされません。最近の変更を保存して、エクスポートされたファイルで使用できるようにしてください。

連絡先を作成する

管理対象ドメインまたは管理対象サブツリー内に連絡先を作成できます。また、プロパティの変更、電子メールの有効化、電子メールアドレスの指定、新しい連絡先へのグループメンバーシップの割り当てなどを実行することもできます。

新しい連絡先を作成するには、[[管理]]>[[検索]] に移動し、[作成] ドロップダウンメニューで [[連絡先]] を選択します。

連絡先のクローンを作成する

連絡先のクローンを作成することにより、同様のプロパティを持つ他の連絡先をベースとして簡単に連絡先を作成することができます。連絡先のクローンを作成すると、選択された連絡先から値が取り込まれ、［Clone Contact (連絡先のクローン作成★)］ウィザードに設定されます。また、プロパティの変更、電子メールの有効化、電子メールアドレスの指定、新しい連絡先へのグループメンバーシップの割り当てなどを実行することもできます。

連絡先のグループメンバーシップを管理する

管理対象ドメインまたは管理対象サブツリー内の特定のグループに連絡先を追加したり削除することができます。この連絡先が属す既存のグループのプロパティを表示し、変更することもできます。

別の OU に連絡先を移動する

管理対象ドメインまたは管理対象サブツリー内の別のコンテナ (OU など) に連絡先を移動することができます。

連絡先を削除する

管理対象ドメインまたは管理対象サブツリー内の連絡先を削除することができます。そのドメインでごみ箱が無効になっている場合、連絡先を削除すると、その連絡先は Active Directory から永久に削除されます。そのドメインでごみ箱が有効になっている場合は、連絡先を削除すると、その連絡先はごみ箱に移動します。

ごみ箱の詳細については、「ごみ箱の管理」を参照してください。

グループ管理対象サービスアカウントの管理

グループ管理対象サービスアカウント (gMSA) は、コンピュータリソース上のサービスに割り当て可能な管理対象ドメインアカウントです。Active Directory でこれらのアカウントのパスワードを手動で更新する必要はありません。これらのアカウントのパスワードは Windows サーバによって自動的に管理されます。

DRA Web コンソールから gMSA を作成および管理できます。グループ管理対象サービスアカウントは、複数のコンピュータでサービスを実行するために使用できます。gMSA を使用しているコンピュータは、Active Directory に現在のパスワードを要求してサービスを開始します。

適切な権限を使用して、グループ管理対象サービスアカウントに関連するさまざまなタスクを実行できます。検索操作を実行して、必要な gMSA オブジェクトを見つけて選択します。リストで 1 つまたは複数のオブジェクトを選択すると、タスクバーがアクティブになり、オブジェクトの削除、オブジェクトのグループへの追加、グループからのオブジェクトの削除、あるコンテナから別のコンテナへのオブジェクトの移動、および gMSA プロパティの変更を行うオプションが表示されます。検索結果を CSV ファイルとしてダウンロードできます。それらの機能を表示するには、［オプション］をクリックします。

gMSA の作成

gMSA を作成する場合は、このアカウントを使用するホストと、そのアカウントを使用できるコンピュータオブジェクトを指定する必要があります。メンバーシップポリシーで定義されたコンピュータオブジェクトは、gMSA を使用してサービスを実行できます。または、コンピュータオブジェクトのリストを含むセキュリティグループを指定することもできます。

新しい gMSA を作成するには、[**[管理]**]>[**[検索]**] に移動し、[作成] ドロップダウンメニューから [**[グループ管理対象サービスアカウント]**] を選択します。

gMSA プロパティの変更

gMSA プロパティは変更することができます。所有する権限により、管理ドメインの中の gMSA に対して変更できるプロパティが異なります。

gMSA を有効にする

gMSA を有効にすると、コンピュータサービスのログインアカウント情報として gMSA を使用できます。［アカウント］タブから gMSA を有効または無効にできます。

gMSA のグループメンバーシップを管理する

管理ドメインまたは管理サブツリーの中の特定のグループにグループ管理対象サービスアカウントを追加したり削除することができます。

別のコンテナに gMSA を移動する

gMSA は、デフォルトで、Active Directory の管理対象サービスアカウントコンテナの下に作成されます。グループ管理対象サービスアカウントは、デフォルトのコンテナから、管理対象ドメインまたは管理対象サブツリー内の別のコンテナ (OU など) に移動できます。

gMSA の削除

管理対象ドメインまたは管理対象サブツリーの中のグループ管理対象サービスアカウントを完全に削除することができます。

5 Azure オブジェクトの管理

この章では、Web コンソールで Azure ユーザアカウント、Azure 連絡先、および Azure グループを管理するための概念と手順について説明します。適切な権限があれば、Azure ユーザアカウントオブジェクトの作成や削除など、さまざまな Azure ユーザ、Azure 連絡先、および Azure グループ管理タスクを実行できます。

次のいずれかのノードでオブジェクトを検索することにより、Web コンソールの［**[管理]**］>［**[検索]**］タブから Azure ユーザオブジェクト、Azure 連絡先オブジェクト、および Azure グループオブジェクトのほとんどのタスクを実行できます。

- すべての管理対象オブジェクト
- すべての管理対象テナント
- すべての管理対象テナントのサブノード

トピックには次のものが含まれます。

- 73 ページの 「Azure ユーザアカウントの管理」
- 74 ページの 「Azure グループの管理」
- 76 ページの 「Azure 連絡先の管理」

Azure ユーザアカウントの管理

アシスタント管理者は、DRA を使用して Azure ユーザアカウントを管理し、DRA 管理者が Azure Active Directory を構成した際に Azure ユーザアカウントのプロパティを変更できます。

検索操作を実行して、必要な Azure ユーザオブジェクトを見つけて選択します。リストで 1 つまたは複数のオブジェクトを選択すると、タスクバーがアクティブになり、［削除］、［許可］、［ブロック］、［パスワードリセット］、［プロパティの変更］などのオプションが表示されます。検索結果を CSV ファイルとしてダウンロードできます。それらの機能を表示するには、［オプション］をクリックします。

Azure ユーザアカウントを作成する

Azure Active Directory に Azure のユーザアカウントを作成することができます。また、電子メールの有効化および新しいアカウントへのグループメンバシップの割り当てなどを実行することもできます。

Azure ユーザアカウントプロパティの変更

Azure Active Directory 内の Azure ユーザアカウントのプロパティを管理できます。所有する権限により、Azure ユーザアカウントに対して変更できるプロパティが決定されます。Azure ユーザアカウントに Office 365 メールボックスがある場合、または Azure ユーザアカウントがメールに対応している場合、Azure ユーザアカウントのメー

ルボックス関連およびメール関連のプロパティを管理できます。メールボックスポリシーの管理、配信制限とオプションの設定、ストレージ制限の設定、メールボックス許可の委任、訴訟の保留、電子メールアドレスの管理などが可能です。

注

- 管理者以外の Azure ユーザに対してだけ、携帯電話とオフィスの電話のプロパティを更新できます。
- DRA では、[所属するグループ] の結果を CSV ファイルとしてエクスポートできます。Web コンソールから［[所属するグループ]］の結果をエクスポートするには、[管理]］>［[検索]］に移動し、［[プロパティ]］をクリックします。［[所属するグループ]］タブに移動し、［[ダウンロード]］アイコンをクリックします。保存されていない変更はエクスポートされません。最近の変更を保存して、エクスポートされたファイルで使用できるようにしてください。

Azure ユーザアカウントのサインインの許可

Azure ユーザアカウントが Azure Active Directory にサインインできるように設定できます。

Azure ユーザアカウントのサインインのブロック

Azure ユーザアカウントが Azure Active Directory にサインインするのをブロックできます。

Azure ユーザアカウントのパスワードのリセット

Azure Active Directory 内の Azure ユーザアカウントのパスワードをリセットして、そのアカウントに対して DRA が新しいパスワードを生成するかどうかを選択できます。

Azure ユーザアカウントの削除

Azure Active Directory から Azure ユーザアカウントを削除することはできますが、DRA から復元することはできません。

Azure ユーザアカウントの Azure グループメンバーシップの指定

Azure Active Directory 内の特定の Azure グループの Azure ユーザアカウントを追加または削除することができます。

Azure グループの管理

DRA 管理者が Azure Active Directory を構成した際に、アシスタント管理者は DRA を使用して Azure グループを管理できます。Azure グループ化により、定義された一連のユーザアカウントに特定の許可を与えることができます。Azure グループを使用して、任意のテナントの中のユーザアカウントがアクセスできるデータとリソースを管理することができます。

検索操作を実行して、必要な Azure グループオブジェクトを見つけて選択します。リストで 1 つまたは複数のオブジェクトを選択すると、タスクバーがアクティブになり、オブジェクトの削除、グループへのオブジェクトの追加、グループからのオブジェクトの削

除、他のグループへのグループの追加、既存のグループからのグループの削除、およびグループプロパティの変更を行うオプションが表示されます。それらの機能を表示するには、[オプション] をクリックします。

注 : サポートされているメンバー : Azure グループメンバーには、Azure ユーザ、Azure グループ、Azure 連絡先、同期されたユーザ、同期された連絡先、および同期されたグループを使用できます。

Azure グループへアカウントを追加する

オンプレミスおよび Azure の両方にユーザアカウントを Azure 管理対象グループに追加できます。

このタスクは、複数のアカウントを指定グループに追加します。適切なアカウントを選択することにより、1 つのアカウントをグループに追加できます。別のグループにアカウントを追加することにより、そのアカウントに対する権限が増える場合には、DRA はそのアカウントの追加を許可しません。

Azure でグループをネストする

別のグループ (オンプレミスおよび Azure の両方) を管理対象の Azure グループに追加することによって、グループをネストできます。グループが Azure グループの中にネストされると、子のグループは親のグループから権限を継承します。

別の Azure グループにドメインまたは Azure グループを追加することにより、そのグループに対する権限が増える場合には、DRA はそのグループの追加を許可しません。

Azure グループを作成する

Azure Active Directory に Azure グループを作成することができます。新しいグループに Azure グループメンバーを追加するなど、プロパティを変更することもできます。

所有者が指定されていない場合、デフォルトで DRA は Azure テナントアクセスアカウントを所有者として提供します。

Azure グループプロパティの変更

所有する権限により、Azure Active Directory 内のグループに対して変更できるプロパティが異なります。Exchange ポリシーが有効になっている場合、Office 365 グループ、メール対応セキュリティグループ、配布リストなどのメールが有効な Azure グループの Exchange プロパティを管理できます。グループタイプに応じて、グループの電子メールアドレスの管理、グループに電子メールを送信できるユーザの指定、グループの代わりに電子メールを送信できるユーザの指定、電子メール承認オプションの設定などが可能です。

注 : DRA では、**[メンバー]** および **[所属するグループ]** の結果を CSV ファイルとしてエクスポートできます。[**[メンバー]**] タブまたは [**[所属するグループ]**] タブに移動し、[**[ダウンロード]**] アイコンをクリックします。保存されていない変更はエクスポートされません。最近の変更を保存して、エクスポートされたファイルで使用できるようにしてください。

Azure グループ所有権を設定する

任意のグループの所有権を設定することができます。グループ所有権のパーミッションは、ユーザアカウントまたはグループに付与することができます。グループ所有権のパーミッションを付与すると、指定したユーザアカウントまたはグループは、メンバーシップを含むグループを管理することができます。

Azure グループの削除

Azure Active Directory から Azure グループを削除することはできますが、DRA から復元することはできません。

Azure 連絡先の管理

Azure 連絡先は、外部電子メールアドレスを含むメールが有効なオブジェクトです。アシスタント管理者は、DRA を使用して Azure 連絡先を管理し、DRA 管理者が Azure Active Directory を構成した際に Azure 連絡先のプロパティを変更できます。

検索操作を実行して、必要な Azure 連絡先オブジェクトを見つけて選択します。リストで 1 つまたは複数のオブジェクトを選択すると、タスクバーがアクティブになり、オブジェクトの削除、オブジェクトのグループへの追加、グループからのオブジェクトの削除、連絡先プロパティの変更を行うオプションが表示されます。検索結果を CSV ファイルとしてダウンロードできます。それらの機能を表示するには、［オプション］をクリックします。

Azure 連絡先の作成

管理対象テナントに Azure 連絡先を作成し、新しい Azure 連絡先の連絡先情報と電子メールアドレスを指定できます。

Azure 連絡先プロパティの変更

Azure 連絡先のプロパティは変更することができます。所有する権限により、管理対象テナントの Azure 連絡先に対して変更できるプロパティが異なります。Exchange ポリシーが有効になっている場合は、メッセージの配信制限の設定、この Azure 連絡先の代わりにメッセージを送信できるユーザの指定、Azure 連絡先がアドレスリストに表示されるかどうかなどのメール関連プロパティを管理できます。

メッセージのモデレートの有効化

Azure 連絡先に送信されるメッセージをモデレートするためのオプションを設定できます。モデレーションを有効にした場合、Azure 連絡先に送信されたメッセージは、メッセージが配信される前に定義したモデレータによって承認されます。承認プロセスから除外されるユーザおよびグループを指定することもできます。

Azure 連絡先のグループメンバーシップの管理

メールが有効なセキュリティグループおよび配布リストに対して、Azure 連絡先を追加または削除できます。

注 : DRA では、**[所属するグループ]** の結果を CSV ファイルとしてエクスポートできます。[**[所属するグループ]**] タブに移動し、[**[保存されたメンバーシップのダウンロード]**] アイコンをクリックします。保存されていない変更はエクスポートされません。最近の変更を保存して、エクスポートされたファイルで使用できるようにしてください。

Azure 連絡先の削除

Azure Active Directory から Azure 連絡先を削除することはできますが、DRA から復元することはできません。

6 Exchange のメールボックスとパブリックフォルダの管理

DRA を使用すると、Microsoft Exchange のメールボックスをユーザアカウントプロパティの一環として管理することができます。この統合によりシステム管理のワークフローが単純化されるため、Exchange のプロパティが効率的に管理できます。また、ユーザアカウントと Exchange アカウントの各フォレストからメールボックスをリンクでき、リソースメールボックス、共有メールボックス、およびパブリックフォルダの管理もできます。

Delegation and Configuration Console (委任および環境設定コンソール) でのメールボックスタスクの管理

ARM ノードの使用時に、オブジェクトのプロパティの［ **[Exchange Task (Exchange タスク)]**］タブから (［ **[タスク]**］や、選択されたオブジェクトの右クリックメニューからもアクセス可能)、該当するメールボックスタスクを実行します。一般的には、［ **[すべての管理対象オブジェクト]**］ノードを選択し、［ **[Find Now (今すぐ検索★)]**］の操作を実行して目的のオブジェクトを見つけて、それを選択します。

Web コンソールでのメールボックスタスクの管理

Web コンソールを使用している場合、次に挙げる該当メールボックスタスクを［ **[管理]**］>［ **[検索]**］タブから実行します。一般的には、検索操作を実行して目的のメールボックスオブジェクトを見つけて、必要なメールボックスオブジェクトを選択します。リスト内の 1 つまたは複数のオブジェクトを選択すると、タスクバーがアクティブになります。それらの機能を表示するには、［オプション］をクリックします。

ここでは次のトピックについて説明します。

ユーザメールボックスの管理タスク

管理対象ドメインまたは管理対象サブツリー内のユーザアカウントが所有する Microsoft Exchange のメールボックスを管理することができます。Microsoft Exchange メールボックスの各管理機能により必要な権限が異なります。ユーザが持っている権限により、変更可能なメールボックスプロパティの種類や、Exchange メールボックスの作成、クローン作成、

表示、削除が可能かどうかが決まります。また、ユーザアカウントと関連付けられたメールボックスの権限とパーミッションも管理できます。これにより、Microsoft Exchange 環境のセキュリティをコントロールすることができます。選択したメールボックスのタブやフィールドを変更する権限がユーザにない場合、DRA は変更できないタブやフィールドを無効にします。

以下に定義されているタスクに加え、DRA 管理者が Skype および Skype Online の設定を構成するためにオブジェクトのプロパティでユーザアカウントに対しオプションを有効にしている場合があります。Skype の設定は、Delegation and Configuration Console (委任および環境設定コンソール) と Web コンソールの両方でユーザアカウントから行うことができます。Skype Online は Web コンソールからのみ設定できます。

メールボックスを作成する

Microsoft Exchange のメールボックスを既存のユーザアカウント用に作成できます。新しいメールボックスのプロパティを変更することもできます。

注 : メールボックスを作成するとき、Exchange ポリシーの設定に基づいて Exchange が必要なプロキシ文字列を生成します。Microsoft Exchange でも、デフォルトのプロキシ文字列を生成します。この結果、新しく作成されたメールボックスのプロパティを表示すると、2 種類のプロキシ文字列が表示されます。

ユーザアカウントのクローンを作成する

ユーザアカウントのクローンを作成すると、そのユーザがメンバーになっているすべてのグループが新しいユーザアカウントに自動的に追加されるため、クローンとして作成されたアカウントのための設定時間が省けます。クローンとして作成されたアカウントに対しては、グループの追加または削除、およびメールの有効化など、様々なプロパティ設定を新規アカウントのときと同様に行うことができます。

注 : InetOrgPerson オブジェクトのクローンを作成するときには、ユーザアカウントを作成します。

メールボックスを移動する

ユーザアカウント用の Microsoft Exchange のメールボックスを、別のメールボックスストアや Microsoft Exchange のサーバーに移動することができます。

メールボックスのプロパティを変更する

Microsoft Exchange のメールボックスのプロパティを変更しつつ、関連するユーザアカウントの管理を行うことができます。所有する権限により、変更できるメールボックスプロパティが異なります。

注 : メンバーサーバ上で管理されるユーザアカウントのメールボックスプロパティを変更することはできません。

メールボックスのセキュリティパーミッションを設定する

特定の Microsoft Exchange メールボックスを使用して電子メールを送受信する機能を付与する (または付与させない) ユーザアカウント、グループ、またはコンピュータを指定することができます。これらの設定により、Exchange 環境の安全性を高めることができます。継承したセキュリティパーミッションを変更することはできません。

注 : メールボックスのセキュリティを管理するとき、オフになっているパーミッションは継承されたパーミッションを示す場合があります。

メールボックスのセキュリティパーミッションを削除する

Microsoft Exchange メールボックスと関連付けられたユーザアカウント、グループ、またはコンピュータからメールボックスのセキュリティパーミッションを削除することができます。メールボックスのセキュリティパーミッションを削除すると、ユーザアカウント、グループ、またはコンピュータアカウントは、指定されたメールボックスから電子メールを送受信できなくなります。継承したセキュリティパーミッションを削除することはできません。

メールボックスの権限を設定する

他のユーザアカウント、グループ、またはコンピュータに特定の Microsoft Exchange メールボックスへの権限を付与したり付与させないようにすることができます。これらの設定により、Exchange 環境の安全性を高めることができます。継承したメールボックス権限を変更することはできません。

注 : メールボックスの権限を管理するとき、オフになっているパーミッションが継承されたパーミッションを示す場合があります。

メールボックスの権限を削除する

特定の Microsoft Exchange メールボックスと関連付けられたユーザアカウント、グループ、またはコンピュータからメールボックスの権限を削除することができます。メールボックスの権限を削除すると、ユーザアカウント、グループ、またはコンピュータアカウントは、指定されたメールボックスが使用できなくなります。継承したメールボックス権限を削除することはできません。

メールボックスを削除する

管理対象ドメインまたは管理対象サブツリー内のユーザアカウントに関連付けられたメールボックスを削除することができます。メールボックスを削除すると、メールボックスの中のすべてのメッセージが削除されます。

電子メールアドレスを追加または変更する

管理対象ドメインまたは管理対象サブツリー内のユーザアカウントに関連付けられたメールボックスに電子メールアドレスを指定することができます。メールボックスを所有していないユーザアカウントに電子メールアドレスを割り当てることもできます。Microsoft Exchange メールボックスを管理するときに、プロキシ生成ポリシーによって定義された電子メールアドレスの種類だけを追加することができます。

返信アドレスを指定する

管理対象ドメインまたは管理対象サブツリー内のユーザアカウントに関連付けられたメールボックスに返信アドレスを設定することができます。1 つのメールボックスに複数の返信アドレスを設定することができます。ただし、1 つの返信アドレスとして複数種類の電子メールアドレスを設定することはできません。たとえば、1 つの返信アドレスとして複数のインターネットアドレスを指定することはできません。

電子メールアドレスを削除する

メールボックスからアドレスを削除することにより、電子メールアドレスを削除することができます。

配信オプションを指定する

メッセージ送信にユーザが使用できるメールボックスの指定、転送オプションの設定、受信者制限の指定を行うことができます。

配布制限を指定する

配布制限を設定することにより、特定のメールボックスに関する着信および送信メッセージのサイズや着信メッセージの受け取りを制限することができます。

ストレージの制限を指定する

メールボックスのサイズに基づく警告など、保存限度を指定することができます。削除された項目の保持期間を指定することもできます。

メールボックスの移動ステータスをチェックする

メールボックスの移動ステータスを確認してアクション (ステータスのクリア、移動のキャンセル、中断された移動の再開など) を実行することができます。

Office 365 のメールボックスの管理タスク

このセクションでは、Account and Resource Management ノードを介した Delegation and Configuration console (委任および環境設定コンソール) および Web コンソールでの Microsoft Office 365 メールボックスを管理する方法について説明します。適切な権限があれば、訴訟ホールドの配置や電子メール転送の設定など、さまざまなユーザアカウント管理タスクが実行できます。

重要 : DRA は、Office 365 ユーザメールボックスの管理に加え、移行された共有、ルーム、および備品のメールボックスを管理します。DRA でこれらのメールボックスを管理するには、DRA が管理するオンプレミスのユーザおよび Azure ユーザに関連付けられている必要があります。メールボックスのプロパティは、関連付けられたユーザのプロパティページで使用できます。

訴訟ホールドの設定

メールボックスに対し訴訟ホールドを設定すると、削除された項目、変更された項目の元版を含め、メールボックス内のすべてのコンテンツが保持できます。また、ユーザのメールボックスを訴訟ホールドにすることで、ユーザのアーカイブメールボックス (もしあれば) 内のコンテンツも保管できます。このホールドは、指定された期間、または手動でメールボックスの訴訟ホールドを解除するまで、効力を保ちます。

訴訟ホールドを使用するには、適切な Exchange Online のライセンスが必要です。この機能はユーザオブジェクトプロパティ内の［ **[訴訟ホールド]**］タブで設定します。

メールボックスのパーミッションを委任する

ユーザオブジェクトのプロパティの中の［メールボックスの委任］タブで Office 365 のメールボックスパーミッションを委任することができます。メールボックス所有者として送信する、代理送信、およびフルアクセスの委任できる 3 種類の許可があります。委任できる許可のタイプは、受け取るオブジェクトタイプによって異なります。

アーカイブメールボックスステータスの表示

ユーザのアーカイブメールボックスのステータス、およびストレージ制限や警告制限などのアーカイブメールボックス統計情報を表示できます。アーカイブメールボックスがアーカイブ警告制限を超えると、ユーザに通知されます。

メールボックス使用状況統計情報の表示

使用されたメールボックスの割り当て量の合計を表示できます。

メッセージ配信制限の設定

配布制限を設定することにより、特定ユーザのメールボックスに関する着信および送信メッセージのサイズ制限や着信メッセージの受信または拒否をすることができます。

配信オプションの指定

メッセージ転送オプションを設定し、ユーザがメッセージを送信できる最大受信者を指定できます。

電子メールアドレスを追加または削除する

1 つのユーザメールボックスに複数の電子メールアドレスを設定し、プライマリ電子メールアドレスを指定できます。メールボックスを所有していないユーザアカウントに電子メールアドレスを割り当てることもできます。

電子メールアドレスを非表示にする

電子メールアドレスをアドレスリストから非表示にするかどうかを指定できます。

メールのヒントの追加

ユーザにメールを送信するときに表示する情報テキストを追加できます。

メールボックスのポリシーの割り当て

メールボックスの共有ポリシー、電子メール保持ポリシー、役割割り当てポリシー、またはアドレス帳ポリシーを割り当てできます。

リソースメールボックスの管理タスク

Microsoft Exchange のリソースメールボックス機能を使えば、会議室などリソースのメールボックスが作成できます。会議室なら、参加予定の人と共に会議室のメールボックスにも会議招待メールを送ることでその会議室が予約できます。DRA には、一連の役割、権限、およびポリシーが含まれています。これによりリソースのメールボックスが効率的に管理できます。

DRA では、リソースのメールボックスを使うためのインタフェース拡張と、監査やユーザインタフェースレポートの生成がサポートされています。ADSI スクリプトのサポートも DRA に組み込まれています。

リソースメールボックスを作成する

管理対象ドメインまたは管理対象サブツリー内にリソースメールボックスを作成することができます。

リソースメールボックスを別のコンテナに移動する

リソースメールボックスを管理対象ドメインまたは管理対象サブツリー内の別のコンテナ (OU など) に移動することができます。

リソースのメールボックスを別のメールボックスストアまたは Exchange サーバに移動する

リソースのメールボックスを別のメールボックスストアや Microsoft Exchange サーバに移動することができます。

リソースメールボックスのクローンを作成する

リソースのメールボックスのクローンを作成することで、似たプロパティを持つ他のリソースのメールボックスが素早く作成できます。リソースのメールボックスのクローンを作成するときは、選択されたリソースからの値が DRA によって［Clone Resource Mailbox (リソースメールボックスのクローン作成★)］ウィザードに設定されます。

リソースメールボックスの名前を変更する

管理対象ドメインまたは管理対象サブツリー内のリソースメールボックスの名前を変更することができます。ユーザのログオン名を変更すると、そのユーザアカウントに対応するメールボックスの名前も変更されます。

リソースメールボックスをグループに追加する

管理対象ドメインまたは管理対象サブツリー内の特定のグループにリソースメールボックスを追加することができます。

リソースメールボックスを削除する

管理対象ドメインまたは管理対象サブツリー内のリソースメールボックスを削除することができます。リソースメールボックスを削除すると、メールボックス内のすべてのメッセージが削除され、リソースメールボックスに関連付けられた無効なユーザオブジェクトもすべて削除されます。必要に応じて、メールボックスを削除する際に無効なユーザオブジェクトの削除を上書きすることができます。リソースメールボックスに関連付けられたユーザオブジェクトを削除すると、そのリソースメールボックスも削除されます。

削除されたリソースメールボックスを復元する

ドメインでごみ箱が有効になっていれば、削除されていたリソースメールボックスを復元することができます。

リソースメールボックスのプロパティを変更する

管理対象ドメインまたは管理対象サブツリー内のユーザアカウントのプロパティを管理することができます。所有する権限により、変更できるプロパティが異なります。

注 : DRA では、**[所属するグループ]** の結果を CSV ファイルとしてエクスポートできます。Web コンソールから［**[所属するグループ]**］の結果をエクスポートするには、［**[管理]**］>［**[検索]**］に移動し、［**[プロパティ]**］をクリックします。［**[所属するグ**

ループ]］タブに移動し、[[ダウンロード]］アイコンをクリックします。保存されていない変更はエクスポートされません。最近の変更を保存して、エクスポートされたファイルで使用できるようにしてください。

共有メールボックスの管理タスク

共有メールボックスは、複数のユーザがアクセスできる 1 つのメールボックスにすべての応答が入るように設定できるため、ヘルプデスクの管理者やテクニカルサポートのスタッフにとって便利な機能です。このメールボックスは、Exchange ポリシーを有効にした DRA の管理対象ドメイン内に存在する必要があります。使用するには、共有メールボックスの管理権限が委任されている必要があります。

共有メールボックスを作成する場合、ユーザに委任できるパーミッションが 2 種類あり、「メールボックス所有者として送信する」と「フルアクセス」です。「メールボックス所有者として送信する」は、電子メールの閲覧と送信が可能なパーミッションです。パーミッションはユーザに対してもグループオブジェクトに対しても委任することができます。また、配信制限、配信オプション、ストレージ制限、フォルダパーミッション、およびその他のいくつかのオプションをオブジェクトのプロパティで指定することもできます。

注 : 共有メールボックスの管理タスクは、Web コンソールからのみ実行できます。

共有のメールボックスを作成する

管理対象ドメインまたは管理対象サブツリー内に共有メールボックスを作成することができます。

共有メールボックスを別のコンテナに移動する

共有メールボックスを管理対象ドメインまたは管理対象サブツリー内の別のコンテナ (OU など) に移動することができます。

共有メールボックスを別のメールボックスストアに移動する

共有メールボックスを別のメールボックスストアに移動することができます。

共有メールボックスのクローンを作成する

共有メールボックスのクローンを作成することで、プロパティが類似する別の共有メールボックスを素早く作成することができます。

共有メールボックスの名前を変更する

管理対象ドメインまたは管理対象サブツリー内の共有メールボックスの名前を変更することができます。ユーザのログオン名を変更すると、そのユーザアカウントに対応するメールボックスの名前も変更されます。

共有メールボックスを削除する

管理対象ドメインまたは管理対象サブツリー内の共有メールボックスを削除することができます。そのドメインでごみ箱が無効になっている場合、削除された共有メールボックスは Active Directory から永久に削除されます。そのドメインでごみ箱が有効になっている場合、削除された共有メールボックスはごみ箱に移動します。

共有メールボックスを削除すると、メールボックス内のすべてのメッセージが削除され、共有メールボックスに関連付けられた無効なユーザオブジェクトもすべて削除されます。共有メールボックスに関連付けられたユーザオブジェクトを削除すると、その共有メールボックスも削除されます。

削除された共有メールボックスを復元する

共有メールボックスが削除されても、そのドメインからのごみ箱が有効になっていれば、共有メールボックスを復元することができます。

アーカイブ共有メールボックスを作成する

アーカイブ共有メールボックスは管理対象ドメインまたは管理対象サブツリー内に作成することができます。

アーカイブ共有メールボックスを削除する

管理対象ドメインまたは管理対象サブツリー内のアーカイブ共有メールボックスは削除することができます。

共有メールボックスのプロパティを変更する

管理対象ドメインまたは管理対象サブツリー内の共有メールボックスのプロパティは変更することができます。所有する権限により、変更できるプロパティが異なります。

注 : DRA では、[所属するグループ] の結果を CSV ファイルとしてエクスポートできます。Web コンソールから［[所属するグループ]］の結果をエクスポートするには、［[管理]］>［[検索]］に移動し、［[プロパティ]］をクリックします。［[所属するグループ]］タブに移動し、［[ダウンロード]］アイコンをクリックします。保存されていない変更はエクスポートされません。最近の変更を保存して、エクスポートされたファイルで使用できるようにしてください。

リンクされたメールボックスの管理タスク

リンクされたメールボックスは、メールボックスのマイグレーションがよく行われる大規模な組織変更 (企業の合併、買収、分社) の際に便利です。この機能により、異なる Exchange フォレストからメールボックスをリンクさせてユーザの電子メールの混乱を回避することができます。Exchange ポリシーを有効にした DRA の管理対象ドメインにすべてのメールボックスが存在する必要があります。また、使用するには、リンクされたメールボックスを管理する権限が委任されている必要があります。リンクされたメールボックスを作成するとき、［[リンクされたメールボックス]］タブがユーザオブジェクトプロパティに追加されます。

リンクされたメールボックスの管理は、Web コンソールでのみサポートされています。リンクされたメールボックスは、選択したユーザアカウントのツールバーから作成します。このオプションは、選択されたユーザのドメインが DRA の他の管理対象ドメインと外部

フォレストの信頼を有している場合にのみ、有効になります。別の DRA 管理対象ドメインにあるリンク先アカウントを検索する際、無効なユーザアカウントのみがリスト表示されます。

リンクされたメールボックスを作成する

異なる管理対象 Exchange フォレストから選択した 2 つのユーザアカウントで、リンクされたメールボックスが作成できます。

リンクされたメールボックスを削除する

リンクされたメールボックスは、リンクされたメールボックスを持つユーザを選択してから、そのツールバーから削除することができます。

リンクされたメールボックスのプロパティを変更する

リンクされたメールボックスのプロパティは、選択したユーザプロパティ内の［[リンクされたメールボックス]］タブで変更できます。

リンクされたアーカイブメールボックスを作成する

リンクされたアーカイブメールボックスは、リンクされたメールボックスを持つユーザを選択して、そこから作成することができます。

リンクされたアーカイブメールボックスを削除する

リンクされたアーカイブメールボックスは、リンクされたアーカイブメールボックスを持つユーザを選択してから、そのツールバーから削除することができます。

削除されたリンクされたメールボックスを復元する

リンクされたメールボックスが削除されても、そのドメインのごみ箱が有効になっていれば、リンクされたメールボックスを復元することができます。

パブリックフォルダの管理タスク

DRA 管理者が DRA 管理下の企業内にパブリックフォルダのフォレストを作成し、その DRA 管理者から DRA でパブリックフォルダを管理する権限をもらった場合、パブリックフォルダの作成、プロパティの変更、変更履歴のレポート生成ができるようになります。パブリックフォルダの作成および変更は、Web コンソールでのみ実行できます。［検索］オプションを使用して、パブリックフォルダを検索できます。詳細については、「*41 ページの 「検索」*」を参照してください。

パブリックフォルダのタスクは、［[管理]］>［[パブリックフォルダ]］タブから実行します。

パブリックフォルダを作成する

Web コンソールを介して指定のパブリックフォルダのドメイン、サブツリー、およびメールボックスに新規のパブリックフォルダを作成することができます。選択されたドメインのデフォルトのメールボックスを使用することも、1 つを選択することもできます。

パブリックフォルダの電子メールを有効にする

リストツールバーの［[メールを有効にする]］というオプションを使用してパブリックフォルダの電子メールを有効にすることができます。これにより、電子メールアドレスをパブリックフォルダに関連付けて、パブリックフォルダのプロパティを変更することができます。

パブリックフォルダの電子メールを無効にする

リストツールバーの中の［[メールを無効にする]］というオプションを使用すればパブリックフォルダの電子メールを無効にすることができます。

パブリックフォルダのプロパティを変更する

既存のパブリックフォルダに対してメールを有効にした後は、そのフォルダの統計情報を表示したり、そのパブリックフォルダのプロパティを変更することができます。これらのプロパティでは、ユーザ配信と制約のオプション、サイズ制限と割り当て量の警告、メールのプロパティ、ストレージの経過時間制限、承認メールへの管理者の包含、およびカスタム属性が変更できます。

注 : また、複数のフォルダが選択されたとき、複数のパブリックフォルダに関して一部のプロパティ (ストレージの制限など) を更新することもできます。

パブリックフォルダを削除する

サブフォルダが 1 つもなく、電子メールのオプションが無効な場合、パブリックフォルダを削除することができます。

7 リソースの管理

DRA では、コンピュータ、プリンタ、その他のデバイスなどのリソースとともに、これらのリソースに関連付けられているプロセスも管理することができます。たとえば、管理対象コンピュータで特定サービスを起動する必要がある場合、DRA でそのコンピュータオブジェクトを検索してオブジェクトプロパティからそのサービスにアクセスし、そのコンピュータに対し (リモート操作する必要なしに) DRA から特定サービスを再起動できます。

部門 (OU) の管理

このセクションでは、Account and Configuration ノードを介して Delegation and Configuration console (委任および環境設定コンソール) で OU を管理する方法について説明します。適切な権限があれば、OU を別のコンテナへ移動するなど、さまざまな OU 管理タスクを実行することができます。

注 : OU の管理は、Delegation and Configuration Console (委任および環境設定コンソール) からのみ実行できます。

OU プロパティの変更

OU のプロパティを変更することができます。所有する権限により、管理ドメインまたは管理サブツリーの中の OU に対して変更できるプロパティが異なります。

OU の作成

管理ドメインまたは管理サブツリーの中に OU を作成することができます。OU の説明など、一般的なプロパティも変更することができます。

OU の複製

管理ドメインまたは管理サブツリーの中の既存の OU を複製することにより、OU を新規作成することができます。OU の説明など、新しい OU の一般的なプロパティも変更することができます。OU を複製しても、OU の中のオブジェクトは複製されません。

Active Directory ツリーを OU の場所に開く

管理ドメインまたは管理サブツリーの中の特定の OU の場所に Active Directory ツリーを簡単に開くことができます。

別のコンテナへの OU の移動

管理ドメインの中の異なるコンテナに OU を移動することができます。ドメインのサブツリーを管理するときに、そのサブツリーの階層内で OU を移動することができます。

注

- 別のコンテナへの OU の移動により、移動された OU に対するユーザーの権限が増える場合には、その OU の移動は許可されません。
- OU をドラッグすることにより新しい場所に移動することもできます。

OU の削除

管理ドメインまたは管理サブツリーの中の OU を削除することができます。削除できるのは空の OU のみです。OU にオブジェクトが含まれていると、その OU は削除できません。オブジェクトを含む OU を削除するには、最初にすべてのオブジェクトを削除してから、その OU を削除します。

コンピュータの管理

管理対象ドメインまたは管理対象サブツリー内にあるコンピュータを DRA で管理することができます。たとえば、管理対象ドメインへのコンピュータアカウントの追加や削除、各コンピュータ上のリソースの管理が可能です。ドメインにコンピュータを追加すると、DRA によってドメインの中にそのコンピュータのアカウントが作成されます。次に、そのドメインのコンピュータに接続して、そのコンピュータアカウントを使用するようにコンピュータを設定します。コンピュータアカウントのプロパティを表示し、変更することもできます。DRA では、管理対象ドメイン内のコンピュータをシャットダウンしたり、ドメインコントローラを同期させることもできます。

注

- コンピュータの管理は、Delegation and Configuration Console (委任および環境設定コンソール) からのみ実行できます。
- 非表示のドメインコントローラを管理することはできません。ドメインキャッシュには、非表示のドメインコントローラは含まれません。このため、DRA は非表示のドメインコンピュータをリストやプロパティウィンドウに表示しません。

コンピュータにグループメンバーシップを指定する

管理対象ドメインまたは管理対象サブツリー内の特定のグループにコンピュータを追加したり削除することができます。このコンピュータが属する既存のグループのプロパティを表示し、変更することもできます。

注 : DRA では、[所属するグループ] の結果を CSV ファイルとしてエクスポートできます。Web コンソールから［[所属するグループ]］の結果をエクスポートするには、［[管理]］>［[検索]］に移動し、［[プロパティ]］をクリックします。［[所属するグループ]］タブに移動し、［[ダウンロード]］アイコンをクリックします。保存されていない変更はエクスポートされません。最近の変更を保存して、エクスポートされたファイルで使用できるようにしてください。

コンピュータアカウントのプロパティを管理する

コンピュータアカウントのプロパティを管理することができます。所有する権限により、管理対象ドメインまたは管理対象サブツリー内のコンピュータに対して変更できるプロパティが異なります。

ドメインにコンピュータを追加する

新しいコンピュータアカウントを作成することにより、管理対象ドメインまたは管理対象サブツリーにコンピュータを追加することができます。

ドメインからコンピュータを削除する

コンピュータアカウントを削除することにより、管理対象ドメインまたは管理対象サブツリーからコンピュータを削除することができます。

コンピュータを移動する

管理対象ドメインまたは管理対象サブツリー内にある別のコンテナ (OU など) にコンピュータを移動することができます。

コンピュータをシャットダウンまたは再起動する

コンピュータをシャットダウンして、即座にまたは指定された日付と時刻に再起動することができます。

管理者アカウントのパスワードをリセットする

コンピュータの管理者アカウントパスワードをリセットするには、Reset Password for Local Administrator 権限か、この権限を含む役割を持っている必要があります。管理対象ドメインまたは管理対象サブツリー内のメンバーサーバの管理パスワードをリセットすることができます。ドメインコントローラの管理者パスワードをリセットすることはできません。

コンピュータアカウントをリセットする

管理対象ドメインまたは管理対象サブツリー内のメンバーサーバのコンピュータアカウントをリセットすることができます。ドメインコントローラのコンピュータアカウントをリセットすることはできません。

コンピュータアカウントを削除する

管理対象ドメインまたは管理対象サブツリー内のコンピュータアカウントを削除することができます。Microsoft Windows ドメインを管理している場合は、共有リソースなど、他のオブジェクトを含むコンピュータアカウントを削除することができます。Active Directory からコンピュータオブジェクトを削除するには、［[強制削除]］オプションを有効にします。これにより、プリンタや共有フォルダなどを含む、子オブ

ジェクトも削除されます。削除されたコンピュータおよびそれに関連付けられたオブジェクトは、DRA のごみ箱に移動されます。削除された時点でごみ箱が無効になっている場合、そのオブジェクトは完全に削除されます。

注 : 管理対象ドメインまたは管理対象サブツリー内のメンバーサーバのコンピュータアカウントを削除することはできません。

コンピュータアカウントを無効にする

管理対象ドメインまたは管理対象サブツリー内のコンピュータアカウントを無効にすることができます。コンピュータのアカウントを無効にすると、そのコンピュータのユーザはどのドメインにもログオンすることができなくなります。

コンピュータアカウントを有効化する

管理対象ドメインまたは管理対象サブツリー内のコンピュータアカウントを有効にできます。コンピュータのアカウントを有効にすると、そのコンピュータのユーザがどのドメインにもログオンできるようになります。

コンピュータのリソースを管理する

管理対象ドメインまたは管理対象サブツリー内の各コンピュータアカウントごとに、サービス、共有リソース、プリンタ、プリントジョブなど、関連リソースを管理することができます。

サービスの管理

サービスとは、Windows オペレーティングシステムから特別な処理を取得するアプリケーションの種類です。コンピュータにログオンしているユーザが 1 人もいないときでも、サービスが実行されることがあります。適切な権限を持つアシスタント管理者は、管理対象ドメインまたは管理対象サブツリー内のコンピュータで実行されているサービスを管理できます。

サービスのプロパティを管理する

管理対象ドメインまたは管理対象サブツリー内のコンピュータ上で実行されるサービスのプロパティを管理することができます。コンピュータのリソース管理の一貫としてサービスを管理することができます。

サービスを起動する

管理対象ドメインまたは管理対象サブツリー内のコンピュータ上でサービスを起動することができます。

パラメータを使用してサービスを起動する

パラメータを受け入れるサービスを起動すると、起動時にこれらのパラメータを指定することができます。管理対象ドメインまたは管理対象サブツリー内のコンピュータ上でサービスを起動することができます。

注 : パラメータを使用してサービスを開始できるのは、Delegation and Configuration Console (委任および環境設定コンソール) を介した場合のみです。

サービスの起動タイプを指定する

マニュアルでの起動を必要とするなど、サービスの起動タイプを変更することができます。

サービスのログオンアカウントを指定する

サービスログオンアカウントを、現在のシステムアカウント以外のアカウントに変更することができます。ローカルシステムアカウント、特定のユーザアカウント、またはグループ管理対象サービスアカウント (gMSA) をサービスログオンアカウントとして指定できます。

サービスを再開する

管理対象ドメインまたは管理対象サブツリー内のコンピュータ上で実行されるサービスを再起動することができます。

サービスを再起動するには、サービスを停止するおよびサービスを起動する権限の両方か、サービスの起動役割およびサービスの停止役割などのこれらの権限を含む役割を持っている必要があります。

サービスを停止する

管理対象ドメインまたは管理対象サブツリー内のコンピュータ上で実行されるサービスを停止することができます。

サービスを一時停止にする

管理対象ドメインまたは管理対象サブツリー内のコンピュータ上で実行されるサービスを一時停止にすることができます。サービスの種類によっては、サービスを一時停止にできない場合があります。たとえば、他のサービスに依存されているサービスの場合、一時停止にできないことがあります。

一時停止中のサービスを再開する

管理対象ドメインまたは管理対象サブツリー内のコンピュータ上で一時停止になっていたサービスを再開することができます。

プリンタとプリントジョブの管理

プリンタを管理するには、そのプリンタのプリントキューを管理します。DRA でリソースプリンタおよび公開プリンタを一時停止 / 再開、起動、変更、停止、および表示することができます。DRA では、プリントジョブのプロパティや優先順位を変更することもできます。プリンタの追加や削除を実行するには、ネイティブの Windows ツールを使用してください。

プリントサーバとは、1 台以上の論理プリンタがインストールされたコンピュータです。論理プリンタは、プリンタデバイスドライバを持つコンピュータ上に定義されます。論理プリンタには、プリンタドライバ、プリントキュー、およびプリンタポートが含まれます。プリントサーバは、論理プリンタとプリンタデバイスを関連付けます。

接続されたプリンタは、印刷のために文書が選択されたコンピュータ上に定義されます。接続されたプリンタは、ネットワーク上の印刷共有リソースに接続されます。このため、関連付けられたコンピュータを通してプリンタとプリントジョブを管理することができます。

公開プリンタとは、Active Directory 内で公開されたプリンタです。公開プリンタは、サーバに直接接続されていないネットワークプリンタや、クラスタサーバによってホストされたプリンタである場合もあります。

注 : プリンタおよびプリントジョブの管理は、Delegation and Configuration Console (委任および環境設定コンソール) からのみ実行できます。

プリンタおよびプリントタスクの管理の詳細については、次のトピックを参照してください。

- 94 ページの 「プリンタ管理タスク」
- 95 ページの 「プリントジョブ管理タスク」
- 95 ページの 「公開プリンタの管理タスク」
- 96 ページの 「公開プリンタのプリントジョブ管理タスク」

プリンタ管理タスク

管理対象ドメインまたは管理対象サブツリー内のコンピュータと関連付けられたプリンタを管理することができます。DRA では、コンピュータのリソース管理の一貫としてプリンタを管理することができます。

このセクションでは、Account and Configuration コンソールを介して、Delegation and Configuration console (委任および環境設定コンソール) のプリンタを管理する方法について説明します。適切な権限を使用して、プリンタの停止など、さまざまなプリンタ管理タスクを実行することができます。

プリンタのプロパティを管理する

管理対象ドメインまたは管理対象サブツリー内のプリンタのプロパティを管理することができます。DRA では、コンピュータのリソース管理の一貫としてプリンタを管理することができます。

プリンタを一時停止にする

管理対象ドメインまたは管理対象サブツリー内のコンピュータに関連付けられたプリンタを一時停止にすることができます。DRA では、コンピュータのリソース管理の一貫としてプリンタを管理することができます。

プリンタを再開する

管理対象ドメインまたは管理対象サブツリー内のコンピュータに関連付けられたプリンタを再開することができます。DRA では、コンピュータのリソース管理の一貫としてプリンタを管理することができます。

プリントジョブ管理タスク

管理対象ドメインまたは管理対象サブツリー内のプリンタに関連付けられたプリントジョブを管理することができます。プリントジョブはプリンタと関連付けられるため、プリンタ管理の一貫としてプリントジョブを管理することができます。

このセクションでは、Delegation and Configuration console (委任および環境設定コンソール) の Account and Resource Management ノードのプリントジョブを管理する方法について説明します。適切な権限を使用して、プリントジョブのキャンセルなど、さまざまなプリントジョブ管理タスクを実行することができます。

プリントジョブプロパティを管理する

プリントジョブのプロパティは、プリンタ管理ワークフローの一部として変更することができます。プリントジョブはプリンタと関連付けられるため、対応するプリンタの管理の一貫としてプリントジョブを変更することができます。変更可能なプリントジョブのプロパティは、ユーザの権限の種類によって異なります。プリントジョブのプロパティを変更するには、関連するプリンタとコンピュータにアクセスできなければなりません。

プリントジョブを一時停止にする

管理対象ドメインまたは管理対象サブツリー内のプリンタ上のプリントジョブを一時停止にすることができます。プリントジョブを一時停止にするには、関連するプリンタとコンピュータにアクセスできなければなりません。プリントジョブが一時停止になっても、そのプリントジョブはプリントキューから削除されません。

プリントジョブを再開する

一時停止になっていたプリントジョブを再開することができます。プリントジョブを再開するには、関連するプリンタとコンピュータにアクセスできなければなりません。

プリントジョブを再起動する

停止されたプリントジョブを再起動することができます。プリントジョブを再起動するには、関連するプリンタとコンピュータにアクセスできなければなりません。

プリントジョブをキャンセルする

プリンタキューの中のプリントジョブをキャンセルすることができます。プリントジョブをキャンセルすると、DRA はそのプリントジョブをプリンタキューから永久に削除します。プリントジョブをキャンセルするには、関連するプリンタとコンピュータにアクセスできなければなりません。

公開プリンタの管理タスク

管理対象ドメインまたは管理対象サブツリー内の公開プリンタを管理することができます。Active Directory 内で公開されているすべてのプリンタ、またはクラスタサーバによってホストされるプリンタを、追加または検索することができます。

このセクションでは、Account and Resource Management ノードを使用して、公開プリンタを管理する方法について説明します。適切な権限を使用して、プリンタの停止など、さまざまなプリンタ管理タスクを実行することができます。

公開プリンタのプロパティを管理する

管理対象ドメインまたは管理対象サブツリー内の公開プリンタのプロパティを管理することができます。DRA では、リソース管理の一貫として公開プリンタを管理することができます。

公開プリンタの情報を更新する

管理対象ドメインまたは管理対象サブツリー内の公開プリンタの情報を更新することができます。DRA では、リソース管理の一貫として公開プリンタを管理することができます。

公開プリンタを一時停止にする

管理対象ドメインまたは管理対象サブツリー内にある公開プリンタを一時停止させることができます。DRA では、リソース管理の一貫として公開プリンタを管理することができます。

公開プリンタを再開する

管理対象ドメインまたは管理対象サブツリー内にある一時停止中の公開プリンタを再開させることができます。DRA では、リソース管理の一貫として公開プリンタを管理することができます。

公開プリンタを移動する

管理対象ドメイン内の 1 つのコンテナ内にある公開プリンタを同一ドメイン内の別のコンテナに移動させることができます。DRA では、リソース管理の一貫として公開プリンタを管理することができます。

公開プリンタの名前を変更する

Active Directory の中の共有公開プリンタの名前を変更することができます。DRA では、リソース管理の一貫として公開プリンタを管理することができます。

注 : Active Directory の中の公開プリンタの名前を変更しても、リソースプリンタの共有名が変更されることはありません。また、名前の変更が管理するリソースプリンタに伝播されることはありません。たとえば、「Emerald」という名前のリソースプリンタがあり、Active Directory でプリンタ名を「Ruby」に変更する場合、他のユーザに表示されるプリンタ名は Ruby ですが、リソースプリンタ名は Emerald のままです。

公開プリンタのプリントジョブ管理タスク

管理対象ドメインまたは管理対象サブツリー内にある公開プリンタに関連付けられたプリントジョブを管理することができます。プリントジョブはプリンタと関連付けられるため、公開プリンタ管理の一貫としてプリントジョブを管理することができます。

このセクションでは、Account and Resource Management ノードを使用して、公開プリンタを管理する方法について説明します。適切な権限を使用して、プリントジョブのキャンセルなど、さまざまなプリントジョブ管理タスクを実行することができます。

プリントジョブプロパティを管理する

プリントジョブのプロパティは、公開プリンタ管理のワークフローの一部として変更することができます。プリントジョブはプリンタと関連付けられるため、対応する公開プリンタの管理の一貫としてプリントジョブを変更することができます。変更可能なプリントジョブのプロパティは、ユーザの権限の種類によって異なります。プリントジョブのプロパティを変更するには、関連する公開プリンタにアクセスできなければなりません。

プリントジョブを一時停止にする

管理対象ドメインまたは管理対象サブツリー内にある公開プリンタ上のプリントジョブを一時停止させることができます。プリントジョブを一時停止にするには、関連する公開プリンタにアクセスできなければなりません。プリントジョブが一時停止になっても、そのプリントジョブはプリントキューから削除されません。

プリントジョブを再開する

管理対象ドメインまたは管理対象サブツリー内にある一時停止中のプリントジョブを再開させることができます。プリントジョブを再開するには、関連する公開プリンタにアクセスできなければなりません。

プリントジョブを再起動する

管理対象ドメインまたは管理対象サブツリー内にある停止したプリントジョブを再起動することができます。プリントジョブを再起動するには、関連する公開プリンタにアクセスできなければなりません。

プリントジョブをキャンセルする

管理対象ドメイン内または管理対象サブツリー内にあるプリンタキューに入ったプリントジョブをキャンセルすることができます。プリントジョブをキャンセルすると、DRA はそのプリントジョブをプリンタキューから永久に削除します。プリントジョブをキャンセルするには、関連する公開プリンタにアクセスできなければなりません。

共有の管理

共有は、ファイルやプリンタなどのリソースをネットワーク上の他のユーザに使用できるようにする手段です。各共有に共有名があり、共有名がサーバ上の共有フォルダを参照しています。DRA は、管理対象ドメイン内のコンピュータ上にある共有だけを管理します。共有を管理するには、リソースを管理するすべてのコンピュータに対する管理者権限 (ローカル管理者グループのメンバーなど) がアクセスアカウントに付与されていなければなりません。これらのパーミッションを割り当てるには、コンピュータのドメイン内の Domain Admins というネイティブグループにアクセスアカウントを追加します。

注 : 共有の管理は、Delegation and Configuration Console (委任および環境設定コンソール) からのみ実行できます。

共有プロパティを管理する

管理対象ドメインまたは管理対象サブツリー内にある共有のプロパティを管理することができます。DRA では、コンピュータのリソース管理の一貫として共有を管理することができます。

共有を作成する

管理対象ドメインまたは管理対象サブツリー内にあるコンピュータ上で共有を作成することができます。共有のプロパティを変更することもできます。

共有のクローンを作成する

管理対象ドメインまたは管理対象サブツリー内にあるコンピュータ上で共有のクローンを作成することができます。共有のクローンを作成することにより、同様のプロパティを持つ他の共有をベースとして簡単に共有を作成することができます。この機能を利用して、特定のドメインの中に作成するすべての共有を同一の設定にすることができます。

共有のクローンを作成すると、選択された共有から値が取り込まれ、[Clone Share (共有のクローン作成★)] ウィザードに設定されます。新しい共有のプロパティを変更することもできます。

共有を削除する

管理対象ドメインまたは管理対象サブツリー内にあるコンピュータから共有を削除することができます。

接続ユーザの管理

ユーザがリモートコンピュータ上のリソースに接続するたびにセッションが確立されます。接続ユーザとは、ネットワーク上の共有リソースに接続されたユーザです。

DRA は、管理対象ドメインの中のコンピュータ上の接続ユーザだけを管理します。アクセスアカウントには、接続ユーザを管理するすべてのコンピュータに対する管理者権限 (ローカル管理者グループのメンバーなど) がなければなりません。これらのパーミッションを割り当てるには、コンピュータのドメイン内の Domain Admins というネイティブグループにアクセスアカウントを追加します。

ユーザを接続解除する

管理対象ドメインまたは管理対象サブツリー内のコンピュータから接続ユーザを接続解除することができます。ただし、該当するコンピュータとオープンセッションにアクセスできなければなりません。接続ユーザを切断するとオープンセッションが終了します。

接続ユーザのリストを更新する

コンピュータ上のオープンセッションに関して今表示されている情報が最新であることを確信する必要がある場合は、接続されたユーザのリストを手動で更新してください。ただし、該当するコンピュータとオープンセッションにアクセスできなければなりません。

デバイスを管理する

デバイスは、コンピュータ、プリンタ、モデム、またはその他の周辺装置など、ネットワークに接続された装置です。

デバイスがコンピュータ上にインストールされている場合でも、Windows は適切なドライバがインストールされ、構成されるまで、そのデバイスを認識できません。デバイスドライバは、ハードウェアとオペレーティングシステムとの通信を有効にします。

DRA では、管理対象ドメイン内のコンピュータ上でのみデバイスを構成および管理することができます。デバイスを管理するすべてのコンピュータに対する管理者権限 (ローカル管理者グループのメンバーなど) がアクセスアカウントに付与されていなければなりません。これらのパーミッションを割り当てるには、コンピュータのドメイン内の Domain Admins というネイティブグループにアクセスアカウントを追加します。

デバイスのプロパティを管理する

特定のコンピュータ上のデバイスのプロパティを変更することができます。デバイスのデバイスプロパティを変更することにより、デバイスの起動タイプを変更することができます。

デバイスを起動する

管理対象ドメインまたは管理対象サブツリー内にある特定のコンピュータ上のデバイスを起動することができます。

デバイスを停止する

管理対象ドメインまたは管理対象サブツリー内にある特定のコンピュータ上のデバイスを停止させることができます。

イベントログの管理

イベントは、重要なシステムまたはアプリケーションの出来事です。Windows オペレーティングシステムは、イベントに関する情報をイベントログファイルに記録します。各コンピュータ上に複数のイベントログが保管されていることがあります。イベントログを表示するには、ネイティブの Windows イベントビューアを使用します。DRA は、管理対象ドメイン内にあるコンピュータ上のイベントログだけを管理します。

DRA は、ユーザによって行われた操作を、セキュリティが確保されたリポジトリであるログアーカイブに記録します。ユーザによって行われた操作を DRA のログアーカイブだけでなく Windows のイベントログにも記録するように、DRA を設定することもできます。詳細については、「日付と時刻について」を参照してください。

イベントログの種類

Microsoft Windows を実行しているコンピュータでは、さまざまなログに追加情報が記録されます。これらのログについて、以下に簡単に説明します。

ログの種類	説明
ADAM	ADAM リポジトリによって記録されるイベントが書き込まれます。
アプリケーション	サービスの起動や失敗など、コンピュータ上のアプリケーションに関するイベントを記録します。たとえば、DRA ではアプリケーションログにイベントを保存します。
ディレクトリサービス	セキュリティデータベースを管理するドメインコントローラに関するイベントを記録します。
ファイルリプリケーションサービス	オペレーティングシステムによって提供されるファイルリプリケーションサービスに関連するイベントを記録します。
セキュリティ	ログオンの試行、ファイルおよびディレクトリアクセス、監査ポリシーオプションに基づくセキュリティポリシーの変更などのイベントを記録します。
システム	ドライバの失敗やサービスの起動や停止など、Windows システムのコンポーネントによってログ取りされたイベントを記録します。

イベントログ管理タスク

DRA をインストールしても、監査イベントはデフォルトでは Windows イベントログに記録されません。このタイプのログ記録は、レジストリキーを変更することによって有効にできます。

警告 : Windows レジストリを編集するときには十分に注意してください。レジストリ内にエラーがあると、コンピュータが動作不能になる場合があります。エラーが発生した場合は、レジストリを最後にコンピュータを問題なく起動したときの状態に戻すことができます。詳細については、Windows レジストリエディタのヘルプを参照してください。

イベントログファイルの最大サイズおよびイベントログが一杯になったときの処理を指定することができます。プロパティウィンドウには、ログ名、ログファイルのパスとファイル名、ログの作成日付、最終変更日付、最終アクセス日付なども表示されます。ログファイルのバックアップを選択すると、DRA は選択されたコンピュータの標準の場所に一意のファイル名が付いたイベントログを保存します。

DRA では、コンピュータのリソース管理の一貫としてイベントログを管理することができます。適切な権限を使用して、イベントログのプロパティの変更など、さまざまなタスクを実行することができます。

イベントログのプロパティを管理する

特定のコンピュータのイベントログのプロパティを変更することができます。

イベントログのエントリを表示する

管理対象ドメインまたは管理対象サブツリー内にあるコンピュータ上の特定のイベントログに記録されたエントリを表示することができます。Delegation and Configuration Console (委任および環境設定コンソール) では、ネイティブの Windows イベントビューアでイベントログファイルを表示できます。

イベントログをクリアする

管理対象ドメインまたは管理対象サブツリー内にあるコンピュータ上の特定のイベントログに記録されたエントリをクリアすることができます。ログをクリアする前に、イベントログエントリを保存することもできます。

オープンファイルの管理

オープンファイルは、ファイルやパイプなどの共有リソースへの接続です。パイプとは、1 つのプロセスがローカルまたはリモートの別のプロセスと通信できるようにするプロセス間通信メカニズムです。

DRA は、管理対象ドメインまたは管理対象サブツリー内にあるコンピュータ上のファイルだけを管理します。オープンファイルはコンピュータと関連付けられるため、コンピュータのリソース管理の一貫としてオープンファイルを管理することができます。たとえば、システムをシャットダウンしたり、新しいデバイスやサービスをインストールするときに、オープンファイルを閉じる必要があるかもしれません。最も頻繁にユーザにアクセスされるファイルを監視して、ファイルのセキュリティの評価に役立てることもできます。

注 : オープンファイルの管理は、Delegation and Configuration Console (委任および環境設定コンソール) からのみ実行できます。

ファイルを閉じる

ネットワーク上のリソースからオープンファイルを閉じることができます。オープンファイルを閉じるときには、ユーザに通知することをお勧めします。データを保存する時間が必要な場合があります。オープンファイルを閉じるには、該当するコンピュータにアクセスできる必要があります。

オープンファイルのリストを更新する

コンピュータ上のオープンセッションに関して今表示されている情報が最新であることを確信する必要がある場合は、接続されたユーザのリストを手動で更新してください。オープンファイルのリストを更新するには、該当するコンピュータにアクセスできる必要があります。

8 ごみ箱の管理

ごみ箱は、ユーザアカウント、グループ、連絡先、コンピュータアカウントを一時的に削除することができるセーフティーネットです。ごみ箱に入ったこれらのオブジェクトは、SID、ACL、グループメンバーシップなど、データをすべて損なわずに元の状態に戻すこともでき、永久に削除することもできます。この柔軟性により、ユーザアカウント、グループ、連絡先、およびコンピュータアカウントをより安全に管理することができます。検索オプションを使用して、必要なオブジェクトを検索できます。詳細については、「*オブジェクトの検索*」を参照してください。

ごみ箱からオブジェクトを復元する

削除したオブジェクトを元の場所に戻すことができます。DRA は、SID、ACL、グループメンバーシップを含めすべてのデータと共にオブジェクトを元の状態に復元します。オブジェクトとは、ユーザアカウント、グループ、連絡先、ダイナミックグループ、リソースメールボックス、ダイナミック配布グループ、コンピュータアカウントなどです。

すべてのオブジェクトを復元する

管理対象ドメインのためのごみ箱からすべてのオブジェクトを復元することができます。選択したドメインまたはすべての管理対象ドメインのごみ箱からオブジェクトを復元することができます。特定のドメインのごみ箱からオブジェクトを復元するには、そのドメインのごみ箱が有効になっている必要があります。

ごみ箱からオブジェクトを削除する

管理対象ドメインのためのごみ箱からオブジェクトを永久に削除することができます。ごみ箱からオブジェクトを削除すると、そのオブジェクトを元に戻すことはできません。オブジェクトとは、ユーザアカウント、グループ、連絡先、ダイナミックグループ、リソースメールボックス、ダイナミック配布グループ、コンピュータアカウントなどです。

ごみ箱を空にする

管理対象ドメインのためのごみ箱を空にすることができます。ごみ箱を空にすると、ごみ箱の中のオブジェクトはすべて完全に削除されます。ごみ箱を空にする操作は、選択したドメインまたはすべての管理対象ドメインに対して実行できます。特定のドメインのごみ箱を空にするには、そのドメインのごみ箱が有効になっている必要があります。ごみ箱をいったん空にすると、削除されたオブジェクトは復元できなくなります。