NetIQ Directory and Resource Administrator 10.2
管理者ガイド

2022 年 5 月

保証と著作権

法的注意事項と著作権、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/en-us/legal を参照してください。

Micro Focus、関連会社、およびライセンサ (「Micro Focus」) の製品およびサービスに対する保証は、当該製品およびサービスに付属する保証書に明示的に規定されたものに限られます。本書のいかなる内容も、当該保証に新たに保証を追加するものではありません。Micro Focus は、本書に技術的または編集上の誤りまたは不備があっても責任を負わないものとします。本書の内容は、将来予告なしに変更されることがあります。

目次

本書の内容

この『*管理者ガイド*』は、DRA (Directory and Resource Administrator) 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。さらに、設定および操作に関する多くのタスクについて手順を追って説明しています。

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、DRA マニュアルの Web サイト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。

はじめに

Directory and Resource Administrator™(DRA) のすべてのコンポーネントをインストールして構成する前に、企業のために DRA が果たす基本理念と、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。

1 Directory and Resource Administrator とは

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、顧客の AD 環境および Exchange 環境を、リスク (特権の格上げ、エラー、悪意のあるアクティビティ、規制違反など) から保護すると同時に、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して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。

Microsoft Active Directory、Windows、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 へのサポート :** 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、および Exchange 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。

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

特権アクセスを管理するために一貫して使用する DRA のコンポーネントには、プライマリサーバおよびセカンダリサーバ、管理コンソール、レポーティングコンポーネント、ワークフロープロセスを自動化する Workflow Automation Engine 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 Center セットアップ (NRC) PowerShell*(オプション)* CLI*(オプション)* DRA ADSI プロバイダ *(オプション)*	任意の DRA サーバ
ヘルプデスクの臨時管理者	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。

Delegation and Configuration Console (委任および環境設定コンソール)

Delegation and Configuration console (委任および環境設定コンソール) は、インストール可能なユーザインタフェースであり、これを使用してシステム管理者は DRA の構成および管理機能にアクセスできます。

- **Delegation Management:** 管理対象リソースおよびタスクへのアクセスをアシスタント管理者に細かく指定して割り当てることができます。
- **Policy and Automation Management:** 環境の標準および規則に確実に準拠するためのポリシーを定義して適用できます。
- **環境設定管理 :** DRA システムの設定とオプションの更新、カスタマイズの追加、および管理対象サービス (Active Directory、Exchange、Azure Active Directory、など) の設定を行えます。
- **Account and Resource Management:** DRA アシスタント管理者が、Delegation and Configuration Console (委任および環境設定コンソール) から接続されたドメインおよびサービスの委任オブジェクトを表示および管理できるようにします。

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。これを使用してアシスタント管理者が接続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表示および管理できます。企業ブランディングやオブジェクトプロパティのカスタマイズなど、管理者が Web コンソールのインタフェースと使用法をカスタマイズすることができます。

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。

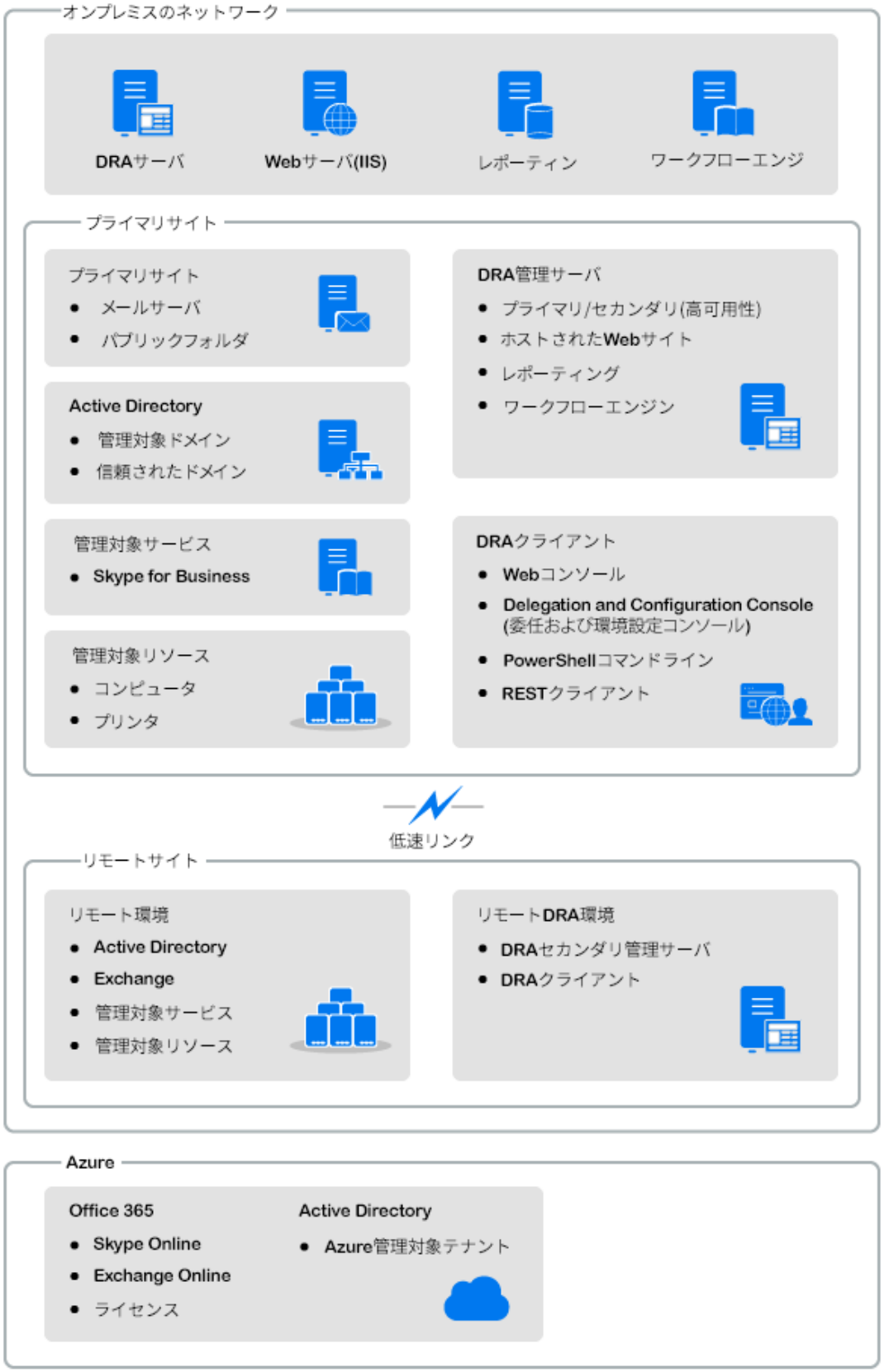
- Active Directory オブジェクトのリソースレポート
- Active Directory オブジェクトデータレポート
- Active Directory サマリレポート
- DRA 構成レポート
- Exchange 構成レポート
- Office 365 Exchange Online レポート
- 詳細なアクティビティトレンドレポート (月別、ドメイン別、ピーク別)
- DRA アクティビティの要約レポート

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。

Workflow Automation Engine

DRA は Workflow Automation Engine 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。Workflow Automation Engine の詳細については、DRA マニュアルサイト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

II 製品のインストールとアップグレード

この章では、Directory and Resource Administrator に必要な推奨ハードウェア、ソフトウェア、およびアカウントの要件について説明します。その後、インストールの各コンポーネントのチェックリストを使用してインストールプロセスをガイドします。

3 展開の計画

Directory and Resource Administrator の展開を計画するときは、このセクションを参照して、ハードウェア環境とソフトウェア環境の適合性を評価し、展開のために構成する必要があるポートおよびプロトコルを確認してください。

テスト済みのリソースの推奨構成

このセクションでは、基本的なリソースの推奨構成のサイジング情報を提供します。使用可能なハードウェア、特定の環境、処理データの特定のタイプなどの要因によって、結果は異なります。より高い負荷に対処するために、より強力で大規模なハードウェア構成にすることもできます。不明な点があれば、NetIQ Consulting Services にお問い合わせください。

約 100 万の Active Directory オブジェクトが存在する環境で実行されます。

コンポーネント	CPU	メモリ	ストレージ
DRA 管理サーバ	8CPU/ コア 2.0GHz	16GB	120GB
DRA Web コンソール	2CPU/ コア 2.0GHz	8GB	100GB
DRA Reporting	4CPU/ コア 2.0GHz	16GB	100GB
DRA ワークフローサーバ	4CPU/ コア 2.0GHz	16GB	120GB

仮想環境リソースのプロビジョニング

DRA は、大きなメモリセグメントを長時間アクティブに保ちます。仮想環境にリソースをプロビジョニングする場合は、以下の推奨事項を考慮する必要があります。

- ストレージを「シックプロビジョニング」として割り当てます

- メモリ予約を［すべてのゲストメモリを予約 (すべてロック)］に設定します
- ページングファイルが、仮想階層でのバルーンメモリの再割り当てをカバーするのに十分な大きさであることを確認します

必要なネットワークポートおよびプロトコル

このセクションでは、DRA 通信のポートとプロトコルについて説明します。

- 設定可能なポートを、アスタリスク 1 つ * で示しています
- 証明書を必要とするポートを、アスタリスク 2 つ ** で示しています

コンポーネントテーブル :

- 24 ページの 「DRA 管理サーバ」
- 26 ページの 「DRA REST サーバ」
- 26 ページの 「Web コンソール (IIS)」
- 27 ページの 「DRA Delegation and Administration コンソール」
- 27 ページの 「ワークフローサーバ」

DRA 管理サーバ

プロトコルとポート	方向	宛先	用途
TCP 135	双方向	DRA 管理サーバ	DRA 通信の基本要件であるエンドポイントマッパーにより、MMS 内で管理サーバは互いを認識
TCP 445	双方向	DRA 管理サーバ	委任モデルの複製、MMS 同期中のファイルの複製 (SMB)
ダイナミック TCP ポート範囲 *	双方向	Microsoft Active Directory ドメインコントローラ	デフォルトでは、DRA は 1024 から 65535 までの TCP ポート範囲から動的にポートを割り当てます。ただし、この範囲はコンポーネントサービスを使用して設定できます。詳細については、「*ファイアウォールでの分散 COM の使用*」を参照してください。
TCP 50000 *	双方向	DRA 管理サーバ	属性のレプリケーションおよび DRA サーバ -AD LDS 通信。(LDAP)
TCP 50001 *	双方向	DRA 管理サーバ	SSL 属性のレプリケーション (AD LDS)

プロトコルとポート	方向	宛先	用途
TCP/UDP 389	アウトバウンド	Microsoft Active Directory ドメインコントローラ	Active Directory オブジェクトの管理 (LDAP)
	アウトバウンド	Microsoft Exchange Server	メールボックスの管理 (LDAP)
TCP/UDP 53	アウトバウンド	Microsoft Active Directory ドメインコントローラ	ネームレゾリューション
TCP/UDP 88	アウトバウンド	Microsoft Active Directory ドメインコントローラ	DRA サーバからドメインコントローラへの認証を許可 (Kerberos)
TCP 80	アウトバウンド	Microsoft Exchange Server	すべてのオンプレミスの Exchange サーバ 2013 以降に必要 (HTTP)
	アウトバウンド	Microsoft Office 365	リモート PowerShell アクセス (HTTP)
TCP 443	アウトバウンド	Microsoft Office 365、Change Guardian	Graph API アクセスおよび Change Guardian Integration(HTTPS)
TCP 443、5986、5985	アウトバウンド	Microsoft PowerShell	ネーティブ PowerShell コマンドレット (HTTPS) と PowerShell リモート処理
TCP 5984	Localhost	DRA 管理サーバ	一時的なグループの割り当てをサポートするための Replication Service (レプリケーションサービス) への IIS アクセス
TCP 8092 * **	アウトバウンド	ワークフローサーバ	ワークフローのステータスとトリガ (HTTPS)
TCP 50101 *	インバウンド	DRA クライアント	変更履歴レポートを右クリックして UI 監査レポートに移動。インストール時に構成可能。
TCP 8989	localhost	ログアーカイブサービス	ログアーカイブ通信 (ファイアウォールで開く必要はありません)
TCP 50102	双方向	DRA コアサービス	ログアーカイブサービス
TCP 50103	localhost	DRA キャッシュ DB サービス	DRA サーバのキャッシュサービス通信 (ファイアウォールで開く必要はありません)
TCP 1433	アウトバウンド	Microsoft SQL Server	レポーティングデータの収集

プロトコルとポート	方向	宛先	用途
UDP 1434	アウトバウンド	Microsoft SQL Server	SQL Server のブラウザサービスは、このポートを使用して名前付きインスタンスのポートを識別。
TCP 8443	双方向	Change Guardian サーバ	Unified Change History
TCP 8898	双方向	DRA 管理サーバ	一時的なグループの割り当てを行うための DRA サーバ間の DRA Replication Service (レプリケーションサービス) 通信
TCP 636	アウトバウンド	Microsoft Active Directory ドメインコントローラ	Active Directory オブジェクトの管理 (LDAP SSL)。

DRA REST サーバ

プロトコルとポート	方向	宛先	用途
TCP 8755 * **	インバウンド	IIS サーバ、DRA PowerShell コマンドレット	DRA REST ベースのワークフローアクティビティを実行 (ActivityBroker)
TCP 135	アウトバウンド	Microsoft Active Directory ドメインコントローラ	サービス接続ポイント (SCP) を使用した自動検出
TCP 443	アウトバウンド	Microsoft AD ドメインコントローラ	サービス接続ポイント (SCP) を使用した自動検出

Web コンソール (IIS)

プロトコルとポート	方向	宛先	用途
TCP 8755 * **	アウトバウンド	DRA REST サービス	DRA Web コンソールと DRA PowerShell の間の通信
TCP 443	インバウンド	クライアントブラウザ	DRA Web サイトを開く
TCP 443 **	アウトバウンド	高度な認証サーバ	高度な認証

DRA Delegation and Administration コンソール

プロトコルとポート	方向	宛先	用途
TCP 135	アウトバウンド	Microsoft Active Directory ドメインコントローラ	SCP を使用した自動検出
ダイナミック TCP ポート範囲 *	アウトバウンド	DRA 管理サーバ	DRA アダプタのワークフローアクティビティ。デフォルトでは、DCOM は 1024 から 65535 までの TCP ポート範囲から動的にポートを割り当てます。ただし、この範囲はコンポーネントサービスを使用して設定できます。詳細については、「*ファイアウォールでの分散 COM の使用* (DCOM)」を参照してください。
TCP 50102	アウトバウンド	DRA コアサービス	変更履歴レポートの生成

ワークフローサーバ

プロトコルとポート	方向	宛先	用途
TCP 8755	アウトバウンド	DRA 管理サーバ	DRA REST ベースのワークフローアクティビティを実行 (ActivityBroker)
ダイナミック TCP ポート範囲 *	アウトバウンド	DRA 管理サーバ	DRA アダプタのワークフローアクティビティ。デフォルトでは、DCOM は 1024 から 65535 までの TCP ポート範囲から動的にポートを割り当てます。ただし、この範囲はコンポーネントサービスを使用して設定できます。詳細については、「*ファイアウォールでの分散 COM の使用* (DCOM)」を参照してください。
TCP 1433	アウトバウンド	Microsoft SQL Server	ワークフローデータストレージ
TCP 8091	インバウンド	Operations Console(オペレーションコンソール) および Configuration コンソール	ワークフロー BSL API(TCP)
TCP 8092 **	インバウンド	DRA 管理サーバ	ワークフロー BSL API(HTTP) および (HTTPS)

プロトコルとポート	方向	宛先	用途
TCP 2219	localhost	Namespace Provider	アダプタを実行するために Namespace Provider で使用
TCP 9900	localhost	Correlation Engine	Workflow Automation Engine および Namespace Provider と通信するために Correlation Engine で使用
TCP 10117	localhost	Resource Management Namespace Provider	Resource Management Namespace Provider で使用

サポートされているプラットフォーム

サポートされているソフトウェアプラットフォームに関する最新情報については、NetIQ Web サイトの Directory and Resource Administrator 製品ページを参照してください。

管理対象システム	前提条件
Azure Active Directory	Azure 管理を有効にするには、次の PowerShell モジュールをインストールする必要があります。 ◆ Azure Active Directory V2(AzureAD)2.0.2.4 バージョン以降 ◆ AzureRM.Profile 5.8.2 バージョン以降 ◆ Exchange Online PowerShell V2.0.3 以降 新しい Azure PowerShell モジュールをインストールするには、PowerShell 5.1 または最新のモジュールが必要です。
Active Directory	◆ Microsoft Server 2012 R2 ◆ Microsoft Server 2016 ◆ Microsoft Windows Server 2019 ◆ Microsoft Server 2022 ◆ Azure Active Directory
Microsoft Exchange	◆ Microsoft Exchange 2013 ◆ Microsoft Exchange 2016 ◆ Microsoft Exchange 2019
Microsoft Office 365	◆ Microsoft Exchange Online O365
Skype for Business	◆ Microsoft Skype for Business 2015
変更履歴	◆ Change Guardian6.0 以降
データベース	◆ Microsoft SQL Server 2016
Web ブラウザ	◆ Google Chrome ◆ Mozilla Firefox ◆ Microsoft Edge

管理対象システム	前提条件
Workflow Automation	◆ Microsoft Server 2012 R2 ◆ Microsoft Server 2016 ◆ Microsoft Server 2019 ◆ Microsoft Server 2022

DRA 管理サーバおよび Web コンソールの要件

DRA コンポーネントには、次のソフトウェアおよびアカウントが必要です。

- 29 ページの 「ソフトウェアの必要条件」
- 31 ページの 「サーバドメイン」
- 31 ページの 「アカウント要件」
- 33 ページの 「最小特権 DRA アクセスアカウント」

ソフトウェアの必要条件

コンポーネント	前提条件
インストールターゲットオペレーティングシステム	**NetIQ 管理サーバおよびオペレーティングシステム :** ◆ Microsoft Windows Server 2012 R2、2016、2019、2022 **注 :** また、サーバは、サポートされる Microsoft オンプレミスの Active Directory ドメインのメンバーでなければなりません。 **DRA のインタフェース :** ◆ Microsoft Windows Server 2012 R2、2016、2019、2022 ◆ Microsoft Windows 10、11
インストーラ	◆ Microsoft .Net Framework 4.8 以降

コンポーネント	前提条件
管理サーバ	**Directory and Resource Administrator:** ◆ Microsoft .Net Framework 4.8 以降 ◆ Microsoft Visual C++ 2015-2019再頒布可能パッケージ(x64および x86) ◆ Microsoft Message Queuing ◆ Microsoft Active Directory ライトウェイトディレクトリサービス役割 ◆ リモートレジストリサービスが開始済みであること ◆ Microsoft Internet Information Services ◆ Microsoft インターネットインフォメーションサービス URL Rewrite Module ◆ Microsoft インターネットインフォメーションサービスアプリケーション要求のルーティング **注 :** DRA REST Endpoint and Service は、管理サーバと一緒にインストールされます。 **Microsoft Office 365/Exchange Online 管理 :** ◆ Windows PowerShell用Windows Azure Active Directoryモジュール ◆ Windows PowerShell モジュール ◆ Exchange Online PowerShell V2.0.3 以降 ◆ Exchange Online タスクのクライアント側で、WinRM for Basic 認証を有効にします。 詳細については、「サポートされているプラットフォーム」を参照してください。
ユーザインタフェース	**DRA のインタフェース :** ◆ Microsoft .Net Framework 4.8 ◆ Microsoft Visual C++ 2015-2019再頒布可能パッケージ(x64および x86)
PowerShell 拡張機能	◆ Microsoft .Net Framework 4.8 ◆ PowerShell 5.1 以降

コンポーネント	前提条件
DRA Web コンソール	**Web サーバ :** ◆ Microsoft .Net Framework 4.x > WCF Services > HTTP Activation (HTTP のアクティベーション) ◆ Microsoft Internet Information Server 8.5、10 ◆ Microsoft インターネットインフォメーションサービス URL Rewrite Module ◆ Microsoft インターネットインフォメーションサービスアプリケーション要求のルーティング **Web Server (IIS) コンポーネント :** ◆ Web サーバ > セキュリティ >URL 認証

サーバドメイン

コンポーネント	オペレーティングシステム
DRA サーバ	◆ Microsoft Windows Server 2022 ◆ Microsoft Windows Server 2019 ◆ Microsoft Windows Server 2016 ◆ Microsoft Windows Server 2012 R2

アカウント要件

アカウント	説明	権限
AD LDS グループ	AD LDS にアクセスするには、このグループに DRA サービスアカウントを追加する必要があります	◆ ドメインローカルセキュリティグループ

アカウント	説明	権限
DRA サービスアカウント	NetIQ 管理サービスを実行するために必要な権限	◆「Distributed COM Users」権限用 ◆ AD LDS 管理者グループのメンバー ◆ アカウントオペレータグループ ◆ ログアーカイブグループ (OnePointOp ConfgAdms & OnePointOp) ◆ STIG 手法を使用して DRA をサーバにインストールする場合、DRA サービスアカウントユーザに対して次の［アカウントタブ］>［**[アカウントオプション]**］のいずれかを選択する必要があります。 　◆ Kerberos AES 128 ビット暗号化 　◆ Kerberos AES 256 ビット暗号化 **注** ◆ 最小特権のドメインアクセスアカウントの設定方法については、「最小特権 DRA アクセスアカウント」を参照してください。 ◆ DRA のグループ管理対象サービスアカウントの設定の詳細については、『*DRA 管理者ガイド*』の「グループ管理対象サービスアカウントの DRA サービスの構成」を参照してください。
DRA 管理者	標準の DRA 管理者役割にプロビジョニングされたユーザアカウントまたはグループ	◆ ドメインローカルセキュリティグループまたはドメインユーザアカウント ◆ 管理対象ドメインまたは信頼されたドメインのメンバー 　◆ 信頼されたドメインのアカウントを指定する場合は、管理サーバコンピュータがそのアカウントを認証できることを確認してください。

アカウント	説明	権限
DRA Assistant Admin アカウント	DRA を介して権限を委任されるアカウント	◆ リモートクライアントから DRA サーバに接続できるように、すべての DRA アシスタント管理者アカウントを「Distributed COM Users」グループに追加してください。これは、シッククライアントまたは Delegation and Configuration console (委任および環境設定コンソール) を使用している場合にのみ必要です。 **注 :** これを自動で実行するように、インストール時に DRA を構成することができます。

最小特権 DRA アクセスアカウント

ここには、各アカウントに必要な権限と特権、および実行する必要がある構成コマンドを記載します。

ドメインアクセスアカウント : ADSI Edit を使用して、ドメインアクセスアカウントに、次の子孫オブジェクトタイプのトップドメインレベルで次の Active Directory 権限を付与します。

- builtInDomain オブジェクトに対するフルコントロール
- コンピュータオブジェクトに対するフルコントロール
- 接続ポイントオブジェクトに対するフルコントロール
- 連絡先オブジェクトに対するフルコントロール
- コンテナオブジェクトに対するフルコントロール
- グループオブジェクトに対するフルコントロール
- InetOrgPerson オブジェクトに対するフルコントロール
- MsExchDynamicDistributionList オブジェクトに対するフルコントロール
- MsExchSystemObjectsContainer オブジェクトに対するフルコントロール
- msDS-GroupManagedServiceAccount オブジェクトに対するフルコントロール
- 部門オブジェクトに対するフルコントロール
- プリンタオブジェクトに対するフルコントロール
- publicFolder オブジェクトに対するフルコントロール
- 共有フォルダオブジェクトに対するフルコントロール
- ユーザオブジェクトに対するフルコントロール

注 : 管理対象ドメインの Active Directory スキーマが Exchange Online に対して拡張されていない場合、次のオブジェクトは表示されません。

- MsExchDynamicDistributionList オブジェクト
- MsExchSystemObjectsContainer オブジェクト
- publicFolder オブジェクト

ドメインアクセスアカウントに、このオブジェクトおよびすべての子孫オブジェクトに対して、トップドメインレベルで次の Active Directory 権限を付与します。

- コンピュータオブジェクトの作成を許可
- 連絡先オブジェクトの作成を許可
- コンテナオブジェクトの作成を許可
- グループオブジェクトの作成を許可
- MsExchDynamicDistributionList オブジェクトの作成を許可
- msDS-GroupManagedServiceAccount オブジェクトの作成を許可
- 部門オブジェクトの作成を許可
- publicFolders オブジェクトの作成を許可
- 共有フォルダオブジェクトの作成を許可
- ユーザオブジェクトの作成を許可
- プリンタオブジェクトの作成を許可
- コンピュータオブジェクトの削除を許可
- 連絡先オブジェクトの削除を許可
- コンテナの削除を許可
- グループオブジェクトの削除を許可
- InetOrgPerson オブジェクトの削除を許可
- MsExchDynamicDistributionList オブジェクトの削除を許可
- msDS-GroupManagedServiceAccount オブジェクトの削除を許可
- 部門オブジェクトの削除を許可
- publicFolders オブジェクトの削除を許可
- 共有フォルダオブジェクトの削除を許可
- ユーザオブジェクトの削除を許可
- プリンタオブジェクトの削除を許可

注

- デフォルトでは、Active Directory 内の一部のビルトインコンテナオブジェクトは、ドメインのトップレベルからアクセス許可を継承しません。そのため、これらのオブジェクトでは、継承を有効にするか、明示的なアクセス許可を設定する必要があります。
- 最小特権アカウントをアクセスアカウントとして使用する場合、DRA で正常にパスワードをリセットするには、アカウントに Active Directory での「パスワードのリセット」許可が割り当てられている必要があります。

Exchange アクセスアカウント : オンプレミスの Microsoft Exchange オブジェクトを管理するには、Organizational Management (組織管理) の役割を Exchange アクセスアカウントに割り当て、Exchange アクセスアカウントをアカウントオペレータグループに割り当てます。

Skype アクセスアカウント : このアカウントが Skype 対応ユーザであり、以下の少なくとも 1 つのメンバーであることを確認してください。

- CSAdministrator 役割
- CSUserAdministrator 役割と CSArchiving 役割

パブリックフォルダのアクセスアカウント : パブリックフォルダのアクセスアカウントには、次の Active Directory 権限を割り当ててください。

- パブリックフォルダ管理
- メールが有効なパブリックフォルダ

Azure テナント : 基本認証では、Azure テナントアクセスアカウントと Azure アプリケーションの両方に対する Azure Active Directory アクセス許可が必要です。証明書ベースの認証では、Azure アプリケーションに対する Azure Active Directory アクセス許可が必要です。デフォルトでは、DRA によって認証に必要な自己署名証明書が自動的に作成されます。

Azure アプリケーション: Azure アプリケーションには、次の役割とアクセス許可が必要です。

役割 :

- ユーザ管理者
- Exchange 管理者

アクセス許可 :

- すべてのユーザのフルプロファイルの読み込みおよび書き込み
- すべてのグループの読み取りおよび書き込み
- ディレクトリデータの読み込み
- Exchange Online リソースにアクセスするためのアプリケーションとして Exchange Online を管理する
- すべてのアプリケーションの読み取りおよび書き込み
- Exchange Recipient 管理者

Azure テナントアクセスアカウント: Azure テナントアクセスアカウントには、次のアクセス許可が必要です。

- 配布グループ
- メール受信者
- メール受信者の作成
- セキュリティグループの作成およびメンバーシップ
- (オプション)Skype for Business 管理者

  Skype for Business Online を管理する場合は、Skype for Business 管理者の権限を Azure テナントアクセスアカウントに割り当てます。
- ユーザ管理者
- 特権認証管理者

NetIQ 管理サービスアカウントの権限:

- ローカル管理者
- 最小特権の上書きアカウントに、ホームディレクトリをプロビジョニングした共有フォルダまたは DFS フォルダに対する「フル権限」を付与します。
- **Resource Management**: 管理されたActive Directoryドメイン内の公開されたリソースを管理するには、そのリソースに対するローカル管理権限をドメインアクセスアカウントに付与する必要があります。

DRA のインストール後: 必要なドメインを管理する前に、次のコマンドを実行する必要があります。

- DRA インストールフォルダの「削除オブジェクトコンテナ」への権限を委任するには、次のようにします (注 : このコマンドはドメイン管理者が実行する必要があります)。

  DraDelObjsUtil.exe /domain:<*NetbiosDomainName*> /delegate:<*Account Name*>
- DRA インストールフォルダから「NetIQReceyleBin OU」に許可を委任するには、次のようにします。

  DraRecycleBinUtil.exe /domain:<*NetbiosDomainName*> /delegate:<*AccountName*>

SAM へのリモートアクセス: DRA によって管理されているドメインコントローラまたはメンバーサーバを割り当てて、次の GPO 設定にリスト化されているアカウントを有効にすることで、セキュリティアカウントマネージャ (SAM) データベースにリモートクエリを実行できるようになります。この構成には、DRA サービスアカウントが含まれている必要があります。

Network access: Restrict clients allowed to make remote calls to SAM (ネットワークアクセス : SAM へのリモートコールを行うことができるクライアントを制限する)

この設定にアクセスするには、次の手順に従います。

1. ドメインコントローラのグループポリシー管理コンソールを開きます。
2. ノードツリー内の［ **[ドメイン]**］> ［ **[ドメインコントローラ]**］> ［ **[グループポリシーオブジェクト]**］を展開します。

3 [[デフォルトのドメインコントローラポリシー]] を右クリックし、[[編集]] を選択して、このポリシーの GPO エディタを開きます。

4 GPO エディタのノードツリーで、[[コンピュータの環境設定]] > [[ポリシー]] > [[Windows の設定]] > [[セキュリティの設定]] > [[ローカルポリシー]] の順に展開します。

5 ポリシーペインの [[Network access: Restrict clients allowed to make remote calls to SAM (ネットワークアクセス : SAM へのリモートコールを行うことができるクライアントを制限する)]] をダブルクリックし、[[Define this policy setting (このポリシー設定を定義する)]] を選択します。

6 [[Edit Security (セキュリティの編集)]] をクリックし、リモートアクセスに対して [[許可]] を有効にします。DRA サービスアカウントがユーザまたは管理者グループの一部として含まれていない場合は、追加します。

7 変更を適用します。これにより、セキュリティデスクリプタである O:BAG:BAD:(A;;RC;;;BA) がポリシー設定に追加されます。

詳細については、「Knowledge Base Article 7023292」を参照してください。

レポーティングの要件

DRA Reporting の要件は次のとおりです。

ソフトウェアの必要条件

コンポーネント	前提条件
インストールターゲット	オペレーティングシステム : ◆ Microsoft Windows Server 2012 R2、2016、2019、2022

コンポーネント	前提条件
NetIQ Reporting Center(v3.3)	**データベース :** ◆ Microsoft SQL Server 2016 ◆ Microsoft SQL Server Reporting Services ◆ SQL Agent ジョブを管理するドメイン管理者は、Microsoft SQL Server Integration Services のセキュリティ権限が必要です。権限がない場合、一部の NRC レポートを処理できない場合があります。 **Web サーバ :** ◆ Microsoft Internet Information Server 8.5、10 ◆ Microsoft IIS コンポーネント ◆ ASP .NET 4.0 **Microsoft .NET Framework 3.5:** ◆ NRC インストーラを実行するために必要です ◆ DRA Reporting Services 設定のために、DRA プライマリサーバにも必要です **注 :** SQL Server コンピュータに NetIQ Reporting Center(NRC) をインストールする場合、NRC をインストールする前に .NET Framework 3.5 を手動でインストールしておかなければならないことがあります。 **Communication Security Protocol(通信セキュリティプロトコル):** ◆ SQL Server は TLS 1.2 をサポートする必要があります。詳細については、TLS 1.2 support for Microsoft SQL Server(Microsoft SQL Server の TLS 1.2 サポート) を参照してください。 ◆ SQL Server には、更新された TLS 対応ドライバが DRA サーバにインストールされている必要があります。推奨ドライバは、最新の Microsoft® SQL Server® 2012 Native Client - QFE です。 ◆ SQL Server と DRA 管理サーバの両方のオペレーティングシステムで同じ TLS プロトコルバージョンがサポートされている必要があります。たとえば、TLS 1.2 だけが有効になっています。
DRA Reporting	**データベース :** ◆ Microsoft SQL Server Integration Services ◆ Microsoft SQL Server エージェント

ライセンスの要件

ライセンスによって、使用できる製品と機能が決まります。DRA では、管理サーバとともにライセンスキーをインストールする必要があります。

管理サーバをインストールした後は、ヘルスチェックユーティリティを使用して、購入したライセンスをインストールすることができます。無制限のユーザアカウントやメールボックスを 30 日間管理できる試用版ライセンスキー (TrialLicense.lic) もインストールパッケージに含まれています。DRA ライセンスの詳細については、「ライセンスのインストールとアップグレード」を参照してください。

ライセンスの定義や制限事項に関する詳細については、製品のエンドユーザ使用許諾契約書 (EULA) を参照してください。

4 製品のインストール

この章では、Directory and Resource Administrator のインストール方法について説明します。インストールまたはアップグレードの計画方法の詳細については、「展開の計画」を参照してください。

DRA 管理サーバのインストール

DRA 管理サーバは、プライマリノードまたはセカンダリノードとして環境にインストールできます。プライマリ管理サーバとセカンダリ管理サーバの要件は同じですが、プライマリ管理サーバはすべての DRA 展開環境に 1 つ用意する必要があります。

DRA サーバパッケージには、次の機能があります。

- **管理サーバ :** 環境設定データ (環境、委任されたアクセス、およびポリシー) の保管、オペレータおよび自動化タスクの実行、そしてシステム全体のアクティビティの監査を実行します。以下の機能が備わっています。
  - **ログアーカイブリソースキット :** 監査情報を表示できます。
  - **DRA SDK:** ADSI のサンプルスクリプトを提供し、独自のスクリプトを作成するのに役立ちます。
  - **一時的なグループの割り当て :** 一時的なグループの割り当ての同期を有効にするコンポーネントを提供します。
- **ユーザインタフェース :** 主にアシスタント管理者が使用する Web クライアントインタフェースですが、カスタマイズのオプションも含まれています。
  - **ADSI プロバイダ :** 独自のポリシースクリプトを作成することができます。
  - **コマンドラインインタフェース :** DRA 操作を実行できるようになります。
  - **Delegation and Configuration:** システム管理者が DRA の環境設定および管理機能にアクセスできるようになります。また、アシスタント管理者に、管理対象リソースおよびタスクへのアクセスを細かく指定して割り当てることができます。
  - **PowerShell 拡張機能 :** 非 DRA クライアントが PowerShell コマンドレットを使用して DRA 操作を要求できるようにする PowerShell モジュールを提供します。
  - **Web コンソール :** 主にアシスタント管理者が使用する Web クライアントインタフェースですが、カスタマイズのオプションも含まれています。

特定の DRA コンソールおよびコマンドラインクライアントを複数のコンピュータにインストールする方法については、「DRA クライアントのインストール」を参照してください。

対話型インストールのチェックリスト :

ステップ	詳細
ターゲットサーバにログオンする	ローカル管理者権限を持つアカウントを使用して、インストール対象の Microsoft Windows サーバにログオンします。
管理者インストールキットをコピーして実行する	DRA インストールキット (NetIQAdminInstallationKit.msi) を実行して、ローカルファイルシステムに DRA インストールメディアを解凍します。 **注 :** このインストールキットは、必要に応じて .Net フレームワークをターゲットサーバにインストールします。
DRA のインストール	[**[Install DRA (DRA のインストール)]**] および [**[次へ]**] をクリックし、インストールオプションを表示します。 **注 :** 後でインストールを実行するには、インストールメディアを解凍した場所 (インストールキットを参照) に移動し、Setup.exe を実行します。
デフォルトのインストール	インストールするコンポーネントを選択し、デフォルトのインストール先 C:\Program Files (x86)\NetIQ\DRA を受け入れるか、別のインストール先を指定します。コンポーネントのオプション : **管理サーバ** ◆ ログアーカイブリソースキット (オプション) ◆ DRA SDK ◆ 一時的なグループの割り当て **ユーザインタフェース** ◆ ADSI プロバイダ (オプション) ◆ コマンドラインインタフェース (オプション) ◆ Delegation and Configuration ◆ PowerShell 拡張機能 ◆ Web コンソール
前提条件の確認	[**[前提条件リスト]**] ダイアログに、インストール対象として選択したコンポーネントに基づいて、必要なソフトウェアのリストが表示されます。インストールを正常に実行するために必要な前提条件ソフトウェアがない場合は、インストーラに従ってインストールすることができます。
EULA 使用許諾契約書に同意する	エンドユーザ使用許諾契約書の条項に同意します。
ログの場所を指定する	DRA がすべてのログファイルを保存する場所を指定します。 **注 :** Delegation and Configuration Console (委任および環境設定コンソール) のログと ADSI ログは、ユーザプロファイルフォルダに保存されます。

ステップ	詳細
サーバ動作モードを選択する	[**[プライマリ管理サーバ]**] を選択してマルチマスタセットの最初の DRA 管理サーバをインストールするか (プライマリは展開環境に 1 つだけ存在します)、[**[セカンダリ管理サーバ]**] を選択して新しい DRA 管理サーバを既存のマルチマスタセットに加えます。 マルチマスタセットの詳細については、『「DRA 管理者ガイド」』の「*Configuring the Multi-Master Set (マルチマスタセットの設定)*」を参照してください。
インストールのアカウントと資格情報を指定する	◆ DRA サービスアカウント ◆ AD LDS グループ ◆ DRA 管理者 アカウント 詳細については、「DRA 管理サーバおよび Web コンソールの要件」を参照してください。
DCOM 権限を構成する	DRA で、認証されたユーザへの「分散 COM」アクセスを構成できるようにします。
ポートを構成する	デフォルトポートの詳細については、「必要なネットワークポートおよびプロトコル」を参照してください。
保管場所を指定する	DRA が監査データとキャッシュデータの保管に使用するローカルファイルの場所を指定します。
DRA レプリケーションデータベースの場所の指定	◆ DRA レプリケーションデータベースおよびレプリケーションサービスポートのファイルの場所を指定します。 ◆ IIS を介してデータベースとの安全な通信を行うために使用する SSL 証明書を指定し、IIS レプリケーションポートを指定します。 **注 :** [**[IIS レプリケーション Web サイト SSL 証明書 (IIS Replication Web Site SSL Certificate)]**] フィールドには、WebHosting ストアとパーソナルストアの両方の証明書が一覧表示されます。
REST サービス SSL 証明書を指定する	REST サービスに使用する SSL 証明書を選択し、REST サービスのポートを指定します。 **注 :** [**[REST サービス SSL 証明書 (REST Service SSL Certificate)]**] フィールドには、WebHosting ストアとパーソナルストアの両方の証明書が一覧表示されます。
Web コンソールの SSL 証明書を指定する	HTTPS のバインドに使用する SSL 証明書を指定します。
インストール構成を確認する	[**[インストール]**] をクリックしてインストールを開始する前に、インストールの概要ページで設定を確認できます。
インストール後の確認	インストールが完了すると、インストールの検証および製品ライセンスの更新のために、正常性検査プログラムが実行されます。 詳細については、『*DRA 管理者ガイド*』の「ヘルスチェックユーティリティ」を参照してください。

DRA クライアントをインストールする

インストールターゲット上で対応する .mst パッケージを指定して DRAInstaller.msi を実行することで、DRA の特定のコンソールやコマンドラインクライアントをインストールできます。

NetIQDRACLI.mst	コマンドラインインタフェースをインストールする
NetIQDRAADSI.mst	DRA ADSI Provider をインストールする
NetIQDRAClients.mst	すべての DRA ユーザインタフェースをインストールする

特定の DRA クライアントを企業全体の複数のコンピュータに展開するには、特定の .MST パッケージをインストールするグループポリシーオブジェクトを設定します。

1. 「Active Directory ユーザとコンピュータ」を開始し、グループポリシーオブジェクトを作成します。
2. このグループポリシーオブジェクトに、DRAInstaller.msi パッケージを追加します。
3. このグループポリシーオブジェクトは、次のいずれかの性質を持つものにする必要があります。
   - グループ内の各ユーザアカウントが、適切なコンピュータに対してパワーユーザ権限を持っている。
   - 「常にシステム特権でインストールする」ポリシー設定を有効にする。
4. このグループポリシーオブジェクトに、ユーザインタフェースの .mst ファイルを追加します。
5. グループポリシーを配布します。

注 : グループポリシーの詳細については、Microsoft Windows のヘルプを参照してください。簡単かつ安全に、グループポリシーをテストして企業全体に展開するには、*Group Policy Administrator* を使用してください。

Workflow Automation のインストールと設定の構成

DRA で Workflow Automation 要求を管理するには、次の手順を実行する必要があります。

- Workflow Automation と DRA アダプタをインストールして設定します。

  詳細については、「*Workflow Automation Administrator Guide(Workflow Automation 管理者ガイド)*」および「*Workflow Automation Adapter Reference for DRA(DRA の Workflow Automation アダプタリファレンス*」を参照してください。
- DRA との Workflow Automation の統合を設定します。

  詳細については、『*DRA 管理者ガイド*』の「「ワークフロー自動化サーバの設定」」を参照してください。

- DRA で Workflow Automation 権限を委任します。

  詳細については、『*DRA 管理者ガイド*』の「「ワークフロー自動化サーバの設定権限を委任する」」を参照してください。

上記で参照したドキュメントは、DRA マニュアルサイトから参照できます。

DRA Reporting のインストール

DRA Reporting を使用するには、NetIQ DRA インストールキットから DRAReportingSetup.exe ファイルをインストールする必要があります。

ステップ	詳細
ターゲットサーバにログオンする	ローカル管理者権限を持つアカウントを使用して、インストール対象の Microsoft Windows サーバにログオンします。このアカウントにローカルおよびドメインの管理者権限と SQL Server のシステム管理者権限があることを確認します。
NetIQ 管理インストールキットをコピーして実行する	DRA インストールキット NetIQAdminINstallationKit.msi をターゲットサーバにコピーし、ファイルをダブルクリックするか、コマンドラインから呼び出して実行します。このインストールキットは、DRA インストールメディアをローカルファイルシステムのカスタマイズ可能な場所に解凍します。さらに、インストールキットは、DRA 製品インストーラの前提条件を満たすために、必要に応じて .Net Framework をターゲットサーバにインストールします。
DRA Reporting のインストールを実行する	インストールメディアを解凍した場所に移動し、DRAReportingSetup.exe を実行して、DRA Reporting の統合のための管理コンポーネントをインストールします。
前提条件を確認してインストールする	[**[前提条件]**] ダイアログに、インストール対象として選択したコンポーネントに基づいて、必要なソフトウェアのリストが表示されます。インストールを正常に実行するために必要な前提条件ソフトウェアがない場合は、インストーラに従ってインストールすることができます。 NetIQ Reporting Center の詳細については、Web のマニュアルサイトにある『*Reporting Center ガイド*』を参照してください。
EULA 使用許諾契約書に同意する	エンドユーザ使用許諾契約書の条項に同意し、インストールの実行を完了します。

5 製品アップグレード

この章は、統制のとれた段階を追って分散環境をアップグレードまたは移行するのに役立つプロセスを提供します。

この章では、環境内に複数の管理サーバがあり、一部のサーバはリモートサイトにあるものと想定しています。この構成は、マルチマスタセット (MMS) と呼ばれます。MMS は、1 つのプライマリ管理サーバと 1 つ以上の関連セカンダリ管理サーバで構成されます。MMS の仕組みについては、『「DRA 管理者ガイド」』の「*Configuring the Multi-Master Set (マルチマスタセットの設定)*」を参照してください。

DRA アップグレードの計画

NetIQAdminInstallationKit.msi を実行して、DRA インストールメディアを解凍し、正常性検査ユーティリティをインストールして実行します。

アップグレードプロセスを開始する前に、DRA の展開計画を作成してください。展開を計画する際には、以下のガイドラインを考慮してください。

- アップグレードを本番環境に適用する前に、アップグレードプロセスを実験環境でテストしてください。テストにより、通常の管理業務に影響を与えることなく、予期しない問題を見つけて解決することができます。
- 「必要なネットワークポートおよびプロトコル」を参照してください。
- 各 MMS に依存するアシスタント管理者の数を調べます。大多数のアシスタント管理者が特定のサーバまたはサーバセットに依存している場合は、まず最初にそれらのサーバをピーク時以外の時間帯にアップグレードします。
- どのアシスタント管理者が Delegation and Configuration console (委任および環境設定コンソール) を必要としているかを調べます。この情報は、次のいずれかの方法で取得できます。
  - どのアシスタント管理者がビルトインアシスタント管理者グループに関連付けられているかを調べます。

- どのアシスタント管理者がビルトインActiveViewに関連付けられているかを調べます。
- Directory and Resource Administrator Reporting を使用して、ActiveView アシスタント管理者の詳細情報やアシスタント管理者グループレポートなどのセキュリティモデルレポートを生成します。

これらのアシスタント管理者に、ユーザインタフェースのアップグレード計画を知らせてください。

- どのアシスタント管理者がプライマリ管理サーバへの接続を必要としているかを調べます。プライマリ管理サーバのアップグレードに対応して、これらのアシスタント管理者のクライアントコンピュータをアップグレードする必要があります。

  これらのアシスタント管理者に、管理サーバおよびユーザインタフェースのアップグレード計画を知らせてください。
- アップグレードプロセスを開始する前に、委任、設定、またはポリシーの変更を実装する必要があるかどうかを調べます。環境によっては、この決定をサイトごとに行うことができます。
- ダウンタイムを最小限に抑えるために、クライアントコンピュータと管理サーバのアップグレードを調整します。同じ管理サーバまたはクライアントコンピュータ上で旧バージョンの DRA と現バージョンの DRA を実行することはできません。

アップグレード前のタスク

アップグレードインストールを開始する前に、以下のアップグレード前のステップを実行して、各サーバセットでアップグレードの準備を行います。

ステップ	詳細
AD LDS インスタンスのバックアップ	ヘルスチェックユーティリティを開き、**[AD LDS インスタンスのバックアップ]** チェックを実行して、現在の AD LDS インスタンスのバックアップを作成します。
展開計画の作成	管理サーバとユーザインタフェース (アシスタント管理者クライアントコンピュータ) をアップグレードするための配備計画を作成します。詳細については、「DRA アップグレードの計画」を参照してください。
セカンダリ管理サーバ 1 台を、前のバージョンの DRA を実行するための専用サーバにする	*オプション:* セカンダリ管理サーバ 1 台を、サイトのアップグレード中に前のバージョンの DRA を実行するための専用のサーバにします。
この MMS にとって必要な変更を加える	この MMS にとって必要な委任、構成、またはポリシー設定に対する変更を加えます。これらの設定を変更するには、プライマリ管理サーバを使用してください。
MMS を同期化する	サーバセットを同期して、すべての管理サーバが最新の構成とセキュリティ設定を持つようにします。
プライマリサーバのレジストリをバックアップする	プライマリ管理サーバのレジストリをバックアップします。レジストリ設定をバックアップしておくと、以前の構成およびセキュリティ設定を簡単に復元できます。

ステップ	詳細
gMSA を DRA ユーザアカウントに変換する	*オプション*:DRA サービスアカウントのグループ管理対象サービスアカウント (gMSA) を使用している場合は、アップグレードの前に gMSA アカウントを DRA ユーザアカウントに変更してください。アップグレード後、アカウントを gMSA に戻す必要があります。

注 : AD LDS インスタンスを復元する必要がある場合、次の操作を行ってください。

1. ［Computer Management］>［Services］で、現在の AD LDS インスタンスを停止します。NetIQDRASecureStoragexxxxx という別のタイトルになります。
2. 以下に示されているように、**現在の** adamnts.dit ファイルを**バックアップの** adamnts.dit ファイルに置き換えます。
   - 現在のファイルの場所 : %ProgramData%/NetIQ/DRA/<DRAInstanceName>/data/
   - バックアップファイルの場所 :%ProgramData%/NetIQ/ADLDS/
3. AD LDS インスタンスを再起動します。

アップグレード前のトピック :

- 49 ページの 「前バージョンの DRA を実行する専用ローカル管理サーバの使用」
- 50 ページの 「前バージョンの DRA サーバセットの同期」
- 51 ページの 「管理サーバのレジストリのバックアップ」

前バージョンの DRA を実行する専用ローカル管理サーバの使用

アップグレードの最中に、１つ以上のセカンダリ管理サーバをローカルで前バージョンの DRA を実行する専用のサーバとして使用すれば、ダウンタイムとリモートサイトへのコストのかかる接続を最小限に抑えることができます。この手順はオプションですが、これによってアシスタント管理者は、展開が完了するまでの間アップグレードプロセス全体を通じて、前バージョンの DRA を使用できるようになります。

以下のアップグレード要件のうち１つ以上があてはまる場合は、このオプションの使用を考慮してください。

- ほとんどまたはまったくダウンタイムが必要ない。
- 多数のアシスタント管理者をサポートする必要があり、すべてのクライアントコンピュータを即座にアップグレードすることは不可能です。
- プライマリ管理サーバをアップグレードした後も、前バージョンの DRA へのアクセスをサポートし続ける必要がある。
- 複数のサイトにまたがる MMS が環境に含まれている。

新規のセカンダリ管理サーバをインストールすることも、前バージョンの DRA を実行している既存のセカンダリサーバを指定することもできます。このサーバをアップグレードする場合は、このサーバを最後にアップグレードしなければなりません。アップグレードしない場合は、アップグレードが正常に完了した後で、このサーバから完全に DRA をアンインストールします。

新規のセカンダリサーバの設定

新規のセカンダリ管理サーバをローカルサイトにインストールすれば、コストのかかるリモートサイトへの接続が不要になり、アシスタント管理者が中断なしで前バージョンの DRA の使用を続行できます。複数のサイトにまたがる MMS が環境に含まれている場合は、このオプションを考慮する必要があります。たとえば、ロンドンサイトにあるプライマリ管理サーバと東京サイトにあるセカンダリ管理サーバで MMS が構成されている場合は、ロンドンサイトにセカンダリサーバをインストールして対応する MMS に追加するのが得策です。この追加されたサーバにより、ロンドンサイトからのアシスタント管理者はアップグレードが完了するまでの間、前バージョンの DRA を使い続けられるようになります。

既存のセカンダリサーバの使用

既存のセカンダリ管理サーバを、前バージョンの DRA 専用のサーバとして使用することができます。セカンダリ管理サーバをアップグレードする予定がないサイトについては、このオプションを考慮する必要があります。既存のセカンダリサーバを専用サーバにできない場合は、新規の管理サーバをこの目的のためにインストールすることを考慮してください。1 つ以上のセカンダリサーバを前バージョンの DRA を実行するための専用サーバにすれば、アップグレードが完了するまでの間、アシスタント管理者が中断なしで前バージョンの DRA を使い続けることができます。このオプションは、中央管理モデルを採用している非常に大規模な環境に適しています。

前バージョンの DRA サーバセットの同期

前バージョンの DRA のレジストリをバックアップする前、つまりアップグレードプロセスを開始する前に、サーバセットの同期をとって各管理サーバの設定およびセキュリティ設定を最新の状態にする必要があります。

注 : この MMS の委任、設定、またはポリシーの設定に必要な変更を加えてください。これらの設定の変更には、プライマリ管理サーバを使用してください。プライマリ管理サーバをアップグレードした後で、委任、設定、またはポリシーの設定を、前バージョンの DRA を実行している管理サーバと同期させることはできません。

既存のサーバセットを同期させるには、次の手順を実行します。

1. プライマリ管理サーバに Built-in Admin としてログオンします。
2. Delegation and Configuration Console (委任および環境設定コンソール) を開き、[**[Configuration Management (環境設定管理)]**] を展開します。
3. **[[管理サーバ]]** をクリックします。
4. 右側のウィンドウで、このサーバセットに属する適切なプライマリ管理サーバを選択します。

5 ［[プロパティ]］をクリックします。

6 ［同期スケジュール］タブで、［[今すぐ更新]］をクリックします。

7 同期が正しく完了したことと、すべてのセカンダリ管理サーバが使用可能であることを確認します。

管理サーバのレジストリのバックアップ

管理サーバのレジストリをバックアップすれば、確実に以前の構成に戻すことができます。たとえば、現バージョンの DRA を完全にアンインストールして前バージョンの DRA を使用しなければならなくなった場合、前のレジストリ設定のバックアップがあれば、前の構成とセキュリティ設定を簡単に復旧できます。

ただし、レジストリの編集には注意が必要です。レジストリ内にエラーがあると、管理サーバが予期したとおりに動作しない場合があります。アップグレードプロセス中にエラーが発生した場合は、レジストリ設定のバックアップを使用して、レジストリを復元できます。詳細については、『*レジストリエディタのヘルプ*』を参照してください。

重要 : レジストリを復元するときは、DRA サーバのバージョン、Windows の OS 名、および管理対象のドメイン構成が完全に同じである必要があります。

重要 : アップグレードする前に、DRA をホストしているマシンの Windows OS をバックアップするか、マシンの仮想マシンスナップショットイメージを作成してください。

管理サーバのレジストリをバックアップするには、次の手順を実行します。

1 regedit.exe を実行します。

2 HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Mission Critical Software\OnePoint ノードを右クリックし、［[エクスポート]］を選択します。

3 レジストリキーを保存するファイルの名前と場所を指定し、［[保存]］をクリックします。

DRA 管理サーバのアップグレード

次のチェックリストで、アップグレードプロセス全体について説明します。このプロセスを使用して、環境内の各サーバセットをアップグレードしてください。まだ行っていない場合は、正常性検査ユーティリティを使用して、現在の AD LDS インスタンスのバックアップを作成します。

警告 : セカンダリ管理サーバは、その MMS のプライマリ管理サーバをアップグレードするまでアップグレードしないでください。

アップグレードプロセスを複数の段階に分けて、一度に 1 つの MMS をアップグレードすることもできます。アップグレードプロセスでは、旧バージョンの DRA を実行するセカンダリサーバと現バージョンの DRA を実行するサーバを一時的に同じ MMS に含めることもできます。DRA は、旧バージョンの DRA を実行する管理サーバと現バージョンの DRA を実

行するサーバとの同期をサポートしています。ただし、同じ管理サーバまたはクライアントコンピュータ上で旧バージョンの DRA と現バージョンの DRA を実行することはできません。

重要 : セカンダリサーバで一時的なグループの割り当てを正常に複製するには、**[マルチマスタ同期スケジュール]** を手動で実行、またはスケジュールされた実行を待機します。

ステップ	詳細
正常性検査ユーティリティを実行する	スタンドアロンの DRA 正常性検査ユーティリティをインストールし、サービスアカウントを使用して実行します。問題があれば解決します。
テストアップグレードを実行する	潜在的な問題を見つけて実働時のダウン時間を最小限に抑えるために、実験環境でテストアップグレードを実行します。
アップグレードの順序を決定する	サーバセットをアップグレードする順序を決定します。
アップグレードのために各 MMS を準備する	アップグレードに備えて各 MMS の準備を整えます。詳細については、「アップグレード前のタスク」を参照してください。
プライマリサーバをアップグレードする	適切な MMS 内のプライマリ管理サーバをアップグレードします。詳細については、「プライマリ管理サーバのアップグレード」を参照してください。
新規セカンダリサーバをインストールする	*(オプション)* リモートサイトでのダウンタイムを最小限に抑えるには、最新バージョンの DRA を実行するローカルのセカンダリ管理サーバをインストールします。詳細については、「現バージョンの DRA のローカルセカンダリ管理サーバのインストール」を参照してください。
ユーザインタフェースを展開する	ユーザインタフェースをアシスタント管理者に展開します。詳細については、「DRA ユーザインタフェースの展開」を参照してください。
セカンダリサーバをアップグレードする	MMS 内のセカンダリ管理サーバをアップグレードします。詳細については、「セカンダリ管理サーバのアップグレード」を参照してください。
DRA Reporting をアップグレードする	DRA Reporting をアップグレードします。詳細については、「Reporting のアップグレード」を参照してください。
正常性検査ユーティリティを実行する	アップグレードの一部としてインストールされた正常性検査ユーティリティを実行します。問題があれば解決します。
Azure テナントの追加 *(アップグレード後)*	*(オプション、アップグレード後)* アップグレード前に Azure テナントの管理をしていた場合は、アップグレード中にテナントが削除されます。これらのテナントを再度追加し、Delegation and Configuration Console (委任および環境設定コンソール) から完全なアカウントキャッシュの更新を実行する必要があります。詳細については、『*DRA 管理者ガイド*』の「「Azure テナントの設定」」を参照してください。

ステップ	詳細
Web コンソールの環境設定の更新 *(アップグレード後)*	*(条件付き、アップグレード後)* アップグレード前に以下のいずれかの Web コンソール環境設定がある場合は、アップグレードインストールの完了後に更新する必要があります。 ◆ デフォルトサーバ接続が有効 ◆ 変更された設定ファイル 詳細については、「Web コンソール環境設定の更新 - インストール後」を参照してください。

サーバのアップグレードに関するトピック :

- 53 ページの 「プライマリ管理サーバのアップグレード」
- 53 ページの 「現バージョンの DRA のローカルセカンダリ管理サーバのインストール」
- 54 ページの 「DRA ユーザインタフェースの展開」
- 55 ページの 「セカンダリ管理サーバのアップグレード」
- 55 ページの 「Web コンソール環境設定の更新 - インストール後」

プライマリ管理サーバのアップグレード

MMS の準備が整ったら、プライマリ管理サーバをアップグレードします。プライマリ管理サーバのアップグレードが完了するまでは、クライアントコンピュータ上のユーザインタフェースをアップグレードしないでください。詳細については、「DRA ユーザインタフェースの展開」を参照してください。

注 : アップグレードの考慮事項と手順については、『*Directory and Resource Administrator リリースノート*』を参照してください。

アップグレードを始める前に、アップグレードの開始時期をアシスタント管理者に通知してください。セカンダリ管理サーバを前バージョンの DRA を実行するための専用サーバにした場合は、アシスタント管理者がアップグレード中に前バージョンの DRA を使い続けられるようにするために、そのサーバのことも知らせてください。

注 : プライマリ管理サーバをアップグレードした後に、そのサーバの委任、構成、またはポリシー設定を、前バージョンの DRA を実行している管理サーバと同期することはできません。

現バージョンの DRA のローカルセカンダリ管理サーバのインストール

ローカルサイトで現バージョンの DRA を実行する新規のセカンダリ管理サーバをインストールすれば、コストのかかるリモートサイトへの接続を最小限に抑えるとともに全体的なダウンタイムを短縮することができ、ユーザインタフェースの展開をより迅速に進めら

れます。この手順はオプションですが、これによってアシスタント管理者は、展開が完了するまでの間アップグレードプロセス全体を通じて、現行バージョンと前バージョンの両方の DRA を使用できるようになります。

以下のアップグレード要件のうち 1 つ以上があてはまる場合は、このオプションの使用を考慮してください。

- ほとんどまたはまったくダウンタイムが必要ない。
- 多数のアシスタント管理者をサポートする必要があり、すべてのクライアントコンピュータを即座にアップグレードすることは不可能です。
- プライマリ管理サーバをアップグレードした後も、前バージョンの DRA へのアクセスをサポートし続ける必要がある。
- 複数のサイトにまたがる MMS が環境に含まれている。

たとえば、ロンドンサイトにあるプライマリ管理サーバと東京サイトにあるセカンダリ管理サーバで MMS が設定されている場合は、東京サイトにセカンダリサーバをインストールして対応する MMS に追加するのが得策です。この追加されたサーバは東京での日常的な管理負荷のバランスをとり、アップグレードが完了するまでの間、どちらのサイトのアシスタント管理者も前バージョンの DRA と現バージョンの DRA の両方を使用できるようになります。さらに、現在の DRA のユーザインタフェースを即座に展開できるので、アシスタント管理者がダウンタイムを経験することもありません。ユーザインタフェースのアップグレードの詳細については、「DRA ユーザインタフェースの展開」を参照してください。

DRA ユーザインタフェースの展開

通常は、プライマリ管理サーバと 1 つのセカンダリ管理サーバをアップグレードした後で、現在の DRA のユーザインタフェースを展開しなければなりません。ただし、プライマリ管理サーバを使用する必要があるアシスタント管理者のクライアントコンピュータは、Delegation and Configuration console (委任および環境設定コンソール) をインストールして最初にアップグレードしてください。詳細については、「DRA アップグレードの計画」を参照してください。

CLI、ADSI プロバイダ、PowerShell を通じて頻繁にバッチ処理を実行する場合や、頻繁にレポートを生成する場合は、これらのユーザインタフェースを専用のセカンダリ管理サーバにインストールすることを考慮してください。それにより、MMS 全体の負荷バランスが適切に保たれます。

DRA ユーザインタフェースのインストールをアシスタント管理者に任せることも、グループポリシーを通じてこれらのインタフェースを展開することもできます。また、Web コンソールを複数のアシスタント管理者に簡単かつ迅速に配備できます。

注 : 同じ DRA サーバ上に複数のバージョンの DRA コンポーネントを同時に実行することはできません。アシスタント管理者のクライアントコンピュータを徐々にアップグレードするよう計画している場合、現バージョンの DRA を実行する管理サーバに即座にアクセスできるようにするために、Web コンソールの展開を考慮してください。

セカンダリ管理サーバのアップグレード

セカンダリ管理サーバのアップグレードでは、管理上のニーズに合わせて各サーバを必要に応じてアップグレードできます。また、DRA ユーザインタフェースのアップグレードと展開の計画についても検討してください。詳細については、「DRA ユーザインタフェースの展開」を参照してください。

たとえば、典型的なアップグレードパスには、次の手順が含まれます。

1. 1 つのセカンダリ管理サーバをアップグレードします。
2. このサーバを使用するアシスタント管理者に、Web コンソールなどの適切なユーザインタフェースのインストールを指示します。
3. MMS 全体をアップグレードするまで、上記のステップ 1 とステップ 2 を繰り返します。

アップグレードを始める前に、アップグレードの開始時期をアシスタント管理者に通知してください。セカンダリ管理サーバを前バージョンの DRA を実行するための専用サーバにした場合は、アシスタント管理者がアップグレード中に前バージョンの DRA を使い続けられるようにするために、そのサーバのことも知らせてください。この MMS のアップグレードが完了し、すべてのアシスタント管理者クライアントコンピュータがアップグレード済みのユーザインタフェースを実行するようになったら、残っている前バージョンのサーバをオフラインにしてください。

Web コンソール環境設定の更新 - インストール後

DRA 環境に適用可能な場合は、アップグレードのインストール後に、以下のアクションのいずれかまたは両方を実行します。

デフォルト DRA サーバ接続

DRA REST サービスコンポーネントは、DRA 10.1 から始まる DRA サーバと統合されています。DRA 10.0.x 以前のバージョンからアップグレードする前にデフォルトの DRA サーバ接続が設定されている場合は、DRA サーバ接続という接続設定が 1 つしか存在しなくなるため、アップグレード後にこれらの設定を確認する必要があります。この環境設定には、Web コンソールの［**[管理]**］>［**[構成]**］>［**[DRA サーバ接続]**］でアクセスできます。

アップグレード後に、DRA Web コンソールサーバの C:\inetpub\wwwroot\DRAClient\rest にある web.config ファイルで、次のように設定を更新することもできます。

```
<restService useDefault="Never">
<serviceLocation address="<REST server name>" port="8755"/>
</restService>
```

Web コンソールのログイン設定

DRA 10.0.x 以前のバージョンからアップグレードする場合、DRA REST サービスが DRA サーバなしでインストールされている場合は、DRA REST サービスをアンインストールする必要があります。アップグレード前に変更されたファイルのコピーは、サーバ上の C:\ProgramData\NetIQ\DRA\Backup\ に作成されます。これらのファイルを参照して、アップグレード後に関連するファイルを更新できます。

Workflow Automation のアップグレード

クラスタ化されていない 64 ビット環境でインプレースアップグレードを実行するには、既存の Workflow Automation コンピュータで Workflow Automation セットアッププログラムを実行します。実行中の Workflow Automation サービスを停止する必要はありません。

Workflow Automation インストーラに組み込まれていない Workflow Automation アダプタは、アップグレード後にアンインストールして再インストールする必要があります。

Workflow Automation のアップグレードの詳細については、『*Workflow Automation Administrator Guide(Workflow Automation 管理者ガイド)*』の「「Upgrading from a Previous Version(旧バージョンからのアップグレード)」」を参照してください。

Reporting のアップグレード

DRA Reporting をアップグレードする前に、環境が NRC 3.3 の最低要件を満たしていることを確認します。インストール要件とアップグレードの考慮事項の詳細については、『*NetIQ Reporting Center Reporting Guide*』を参照してください。

ステップ	詳細
DRA Reporting サポートを無効にする	レポーティングコレクタがアップグレード処理中に実行されないように、Delegation and Configuration console (委任および環境設定コンソール) の［Reporting Service Configuration］ウィンドウで DRA Reporting サポートを無効にします。
適切な資格情報を使用して SQL インスタンスサーバにログオンする	レポーティングデータベース用の SQL インスタンスをインストールした Microsoft Windows サーバに、管理者アカウントを使用してログオンします。このアカウントにローカル管理者権限と SQL Server のシステム管理者権限があることを確認します。
DRA Reporting セットアップを実行する	インストールキットの DRAReportingSetup.exe を実行し、インストールウィザードの指示に従います。
DRA Reporting サポートを有効にする	プライマリ管理サーバで、Delegation and Configuration Console (委任および環境設定コンソール) でレポートを有効にします。

SSRS 統合を使用している場合は、レポートを再展開する必要があります。レポートの再展開の詳細については、Web のマニュアルサイトにある『*Reporting Center ガイド*』を参照してください。

委任モデル

DRA では、管理者が「最小特権」パーミッションのスキームを実装することができます。企業内の特定の管理対象オブジェクトにきめ細かい権限が付与できる柔軟なコントロールセットが用意されています。このように委任を行うことで、管理者は各アシスタント管理者の役割および責任遂行に必要なパーミッションのみをアシスタント管理者に与えることができます。

6 ダイナミック委任モデルについて

DRA では、委任モデルのコンテキストで企業への管理アクセスを管理することができます。委任モデルでは、企業の変遷と発展に順応できるダイナミックなコントロールを使用してアシスタント管理者のために「最小特権」の権限を設定することができます。委任モデルで使用する管理アクセスコントロールは、次に挙げるように、より精密に企業の活動に対応します。

- 範囲設定ルールに柔軟性があるため、管理者は企業構造ではなく事業ニーズに基づき、特定の管理対象オブジェクトに狙いを定めてパーミッションを設定できます。
- 委任を役割ベースにすることで、一貫性をもって確実にパーミッションが付与され、プロビジョニングも簡単になります。
- すべてのドメイン、クラウドテナント、および管理対象アプリケーションに関し、特権の割り当てを 1 カ所から管理できます。
- 権限がきめ細かいため、特定のアクセスを特注してアシスタント管理者に付与することができます。

委任モデルのコントロール

管理者は、次に示すコントロールを使用して委任モデルによるアクセスの設定を行います。

- **委任 :** 管理者は、対象範囲を提供する ActiveView のコンテキストでパーミッションを指定しておいた役割を割り当てることによって、ユーザおよびグループへのアクセスを設定します。
- **ActiveView:** ActiveView は、1 つまたは複数のルールで定義される特定範囲の管理対象オブジェクトを表します。ActiveView で各ルールにより特定される管理対象オブジェクトは、1 つの統一範囲内に集約されます。
- **ActiveView のルール :** ルールは式で定義されます。式は、オブジェクトタイプ、場所、名前など多数の条件に基づいて一連の管理対象オブジェクトと一致させます。
- **役割 :** 役割とは、特定の管理機能を実行するために必要となる特定の権限の集まり (パーミッション) です。DRA には、一般的な業務機能に利用できる多くの役割が用意されています。また、自社のニーズに最適となるように役割を定義してカスタマイズすることもできます。
- **権限 :** 権限は、管理対象オブジェクトのサポート対象のタスクに関して特定のパーミッションを定義します。管理対象オブジェクトの変更に関連するパーミッションは、変更可能な特定のプロパティにさらに分割できます。DRA は、サポート対象の管理対象オブジェクトに使用できる権限が数多く用意され、カスタムの権限を定義して委任モデルを通じて設定可能領域を拡大することができます。

DRA の要求の処理方法

管理サーバがアクションの要求を受け取ると、ユーザのパスワード変更など、次の手順を使用します。

1. その操作のターゲットオブジェクトを管理するように設定されている ActiveView を検索します。
2. そのアクションを要求しているアカウントに割り当てられた権限を検証します。
   a. その操作を要求しているアシスタント管理者が含まれている ActiveView の割り当てをすべて評価します。
   b. そのリストが完了したら、ターゲットオブジェクトとアシスタント管理者の両方が含まれる ActiveView の全リストを作成します。
   c. すべての権限を、求めている操作に必要な権限と比較します。
3. *アカウントに正しい権限がある場合*、管理サーバがアクションの実行を許可します。
   アカウントに正しい権限がない場合、管理サーバはエラーを返します。
4. Active Directory を更新します。

DRA の委任割り当て処理方法の例

次に、DRA による要求処理時の委任モデルの評価方法で発生する一般的なシナリオについて、例を挙げて説明します。

例 1: ユーザのパスワード変更

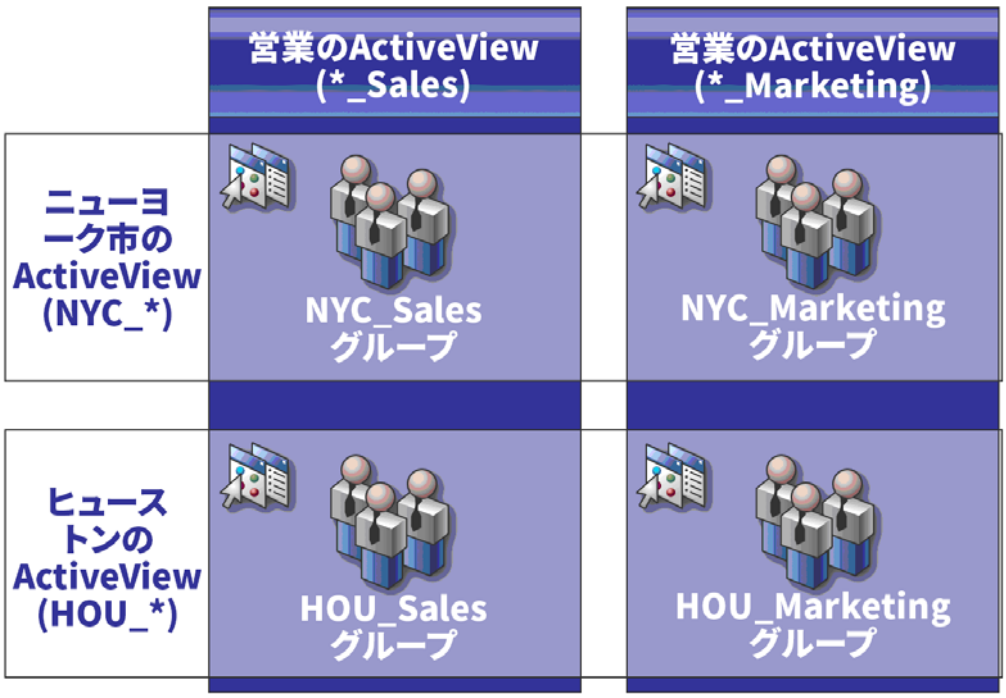
アシスタント管理者が JSmith さんのユーザアカウントに新しいパスワードを設定しようとすると、管理サーバは 「JSmith」を含む ActiveView をすべて見つけます。この検索は、ワイルドカードルールまたはグループメンバーシップを通じて直接 JSmith さんを指定する ActiveView を探します。ある ActiveView が他の ActiveView を含んでいる場合、管理サーバはこれらの ActiveView も追加で検索対象にしてください。これらの ActiveView のいずれかでそのアシスタント管理者が *Reset User Account Password* という権限を持っているかどうかを管理サーバが判断します。アシスタント管理者が *Reset User Account Password* という権限を持っている場合、管理サーバは JSmith さんのパスワードをリセットします。この権限がない場合、管理サーバが要求を拒否します。

例 2: ActiveView の重ね合わせ

権限は、管理対象ドメインまたはサブツリー内でアシスタント管理者が表示、変更、または作成できるオブジェクトプロパティを定義します。2 つ以上の ActiveView が同じオブジェクトを含めることができます。この設定を「**ActiveView の重ね合わせ**」と呼びます。

ActiveView が重なり合うと、同じオブジェクトに対して異なる一連の権限を累積することができます。たとえば、1 つの ActiveView でドメインにユーザアカウントが追加でき、別の ActiveView で同じドメインからユーザアカウントが削除できる場合、そのドメイン内のユーザアカウントを追加または削除できます。このようにして、特定のオブジェクトに対する権限が累積されます。

ActiveView が重なり合ったり、これらの ActiveView に含まれるオブジェクトに対する権限が増したりすることを理解することが重要です。次の図に示すような ActiveView の構成を検討します。



白いタブでは、ActiveView を場所で識別します (*ニューヨーク市*と *ヒューストン*)。黒いタブでは、ActiveView を組織の機能で識別します (*営業*と *拡販*)。各 ActiveView に含まれるグループが各セルに表示されます。

NYC_Sales グループと HOU_Sales グループはどちらも営業の ActiveView に表示されています。営業 ActiveView への権限を持っている場合、NYC_Sales グループと HOU_Sales グループのすべてのメンバーを管理できます。ニューヨーク市 ActiveView への権限も持っている場合、これらの追加権限が NYC_Marketing グループに適用されます。この方法により、ActiveView が重なり合うたびに権限が積み重なります。

ActiveView の重ね合わせにより、強力で柔軟な委任モデルとなります。ただし、この機能は予期しない結果を生む可能性もあります。ActiveView を慎重に計画し、各アシスタント管理者がユーザアカウント、グループ、OU、連絡先、またはリソースのそれぞれに対し本当に必要な権限のみ有している状態にしてください。

複数の Activeview 内のグループ

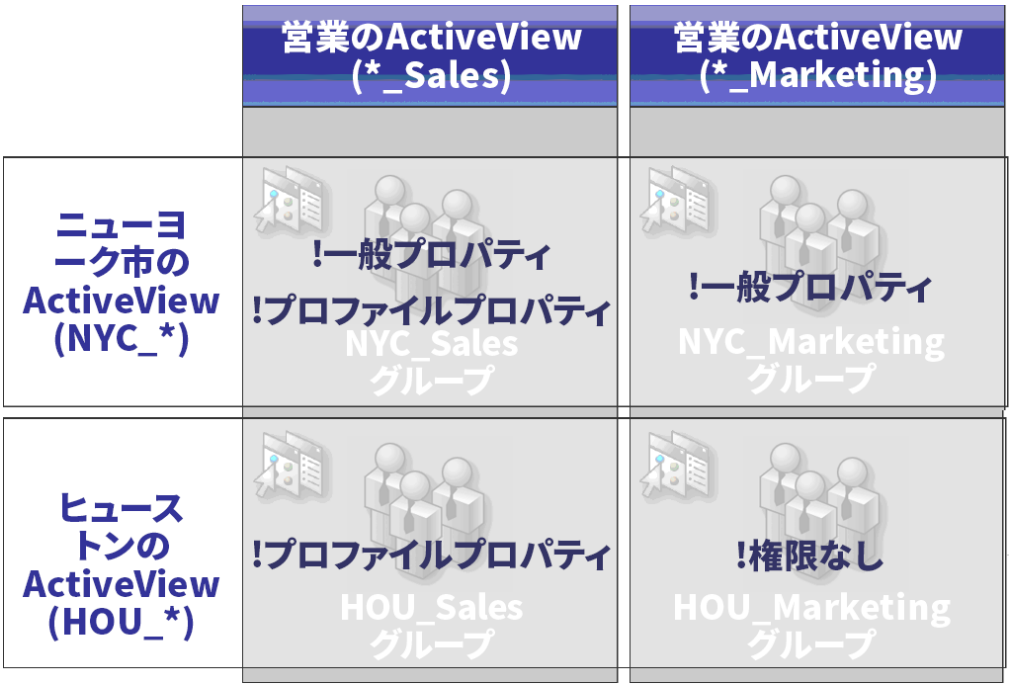
この例では、NYC_Sales グループが複数の ActiveView に表示されます。NYC_Sales グループのメンバーは、そのグループ名が NYC_* という ActiveView ルールと一致するため、ニューヨーク市 ActiveView に表示されています。このグループは、*_Sales という ActiveView ルールと一致するため、営業 ActiveView にも含まれます。同じグループを複数の ActiveView に含めることで、同一のオブジェクトを別々に管理することを異なるアシスタント管理者に許可することができます。

複数の ActiveView での権限使用

ニューヨーク市の ActiveView で *Modify General User Properties* という権限を持つ「JSmith」というアシスタント管理者がいるとします。この最初の権限によって JSmith さんは、ユーザプロパティウィンドウの［全般］タブですべてのプロパティを編集することができま

す。JSmith さんは、営業 ActiveView で *Modify User Profile Properties* という権限を持っています。2 つ目の権限によって JSmith さんは、ユーザプロパティウィンドウの［プロファイル］タブですべてのプロパティを編集することができます。

次の図に、各グループで JSmith さんの持つ権限を示します。



JSmith さんには、次の権限があります。

- NYC_* ActiveView の全般プロパティ
- *_Sales ActiveView のプロファイルプロパティ

このような重なり合う ActiveView の権限委任により、JSmith さんは NYC_Sales グループの［全般］と［プロファイル］の各プロパティを変更できます。そのため、JSmith さんは、NYC_Sales グループを表示するすべての ActiveView で付与された権限をすべて持っています。

7 ActiveView

ActiveView により、次に示す特徴を持った委任モデルを実装することができます。

- 既存の Active Directory 構造から独立している
- 既存のワークフローと相関関係のある権限割り当てとポリシー定義ができる
- 企業の更なる統合化およびカスタマイズ化に役立つ自動化を提供する
- 変更に動的に対応する

1 つの ActiveView が 1 つまたは複数の管理対象ドメイン内の一連のオブジェクトセットを表示します。1 つのオブジェクトを複数の ActiveView に含めることができます。複数のドメインまたは OU からの多数のオブジェクトを含めることもできます。

組み込み ActiveView

組み込み ActiveView とは、DRA に含まれているデフォルトの ActiveView です。これらの ActiveView は、現在のオブジェクトとセキュリティ設定のすべてを表します。したがって、すべてのオブジェクトおよび設定、およびデフォルトの委任モデルに、組み込み ActiveView で直接アクセスすることができます。これらの ActiveView を使用すれば、ユーザアカウントやリソースなどのオブジェクトを管理したり、現在の企業構成にデフォルトの委任モデルを適用することができます。

DRA には、必要な委任モデルと同等の組み込み ActiveView がいくつか用意されています。組み込み ActiveView のノードには、次に示す ActiveView が含まれています。

すべてのオブジェクト

すべての管理対象ドメイン内のすべてのオブジェクトが含まれています。この ActiveView を通じて、企業のすべての側面が管理できます。この ActiveView は、管理者に、または全社に対し監査を行う権限が必要なアシスタント管理者に割り当ててください。

現在のユーザが Windows 管理者として管理するオブジェクト

現在の管理対象ドメインのオブジェクトが含まれます。この ActiveView を通じて、ユーザアカウント、グループ、連絡先、OU、およびリソースが管理できます。この ActiveView は、管理対象ドメイン内のアカウントおよびリソースのオブジェクトを管理する責任のあるネーティブの管理者に割り当ててください。

管理サーバと管理対象ドメイン

管理サーバのコンピュータと管理対象ドメインを含みます。この ActiveView により、管理サーバの毎日の保守を管理できます。キャッシュ更新の実行や同期化ステータスの監視などを担当するアシスタント管理者に、この ActiveView を割り当ててください。

DRA のポリシーと自動化トリガ

すべての管理対象ドメイン内のすべてのポリシーおよび自動化トリガオブジェクトが含まれます。この ActiveView から、自動化トリガのプロパティに加え、ポリシーのプロパティや適用範囲が管理できます。会社のポリシーの作成および維持管理を担当するアシスタント管理者に、この ActiveView を割り当ててください。

DRA のセキュリティオブジェクト

すべてのセキュリティオブジェクトが含まれます。この ActiveView から、ActiveView、アシスタント管理者グループ、および役割が管理できます。セキュリティモデルの作成および維持管理を担当するアシスタント管理者に、この ActiveView を割り当ててください。

すべての管理対象ドメインと信頼されたドメインからの SPA ユーザ

管理対象ドメインと信頼されたドメインからのすべてのユーザアカウントが含まれます。この ActiveView からは、SPA (Secure Password Administrator) を介してユーザのパスワードが管理できます。

組み込みの ActiveView へのアクセス

ActiveView にアクセスして、デフォルトの委任モデルを監査したり、自分のセキュリティ設定を管理します。

組み込みの ActiveView にアクセスするには :

1 [**[Delegation Management]**] > [**[Manage ActiveViews (ActiveView を管理)]**] の順に選択します。
2 検索フィールドが空であることを確認し、[**[List items that match my criteria (自分の基準に一致する項目をリスト表示)]**] ペインで [**[Find Now (今すぐ検索)]**] をクリックします。
3 適切な ActiveView を選択します。

組み込みの ActiveView の使用

組み込みの ActiveView は削除、クローン作成、変更ができません。ただし、これらの ActiveView を既存の委任モデルに組み込むことや、これらの ActiveView を使用して独自モデルの設計を行うことができます。

組み込みの ActiveView は次の方法で使用できます。

- 適切なアシスタント管理者グループに個々のビルトインActiveViewを割り当ててください。この関連付けで、アシスタント管理者グループのメンバーが適切な権限を使って、対応するオブジェクトセットを管理することができます。
- 組み込み ActiveView のルールと関連付けを、委任モデルの設計と実装を始める際のガイドラインとして参照してください。

ダイナミック委任モデルの設計の詳細については、「ダイナミック委任モデルについて」を参照してください。

カスタム ActiveView の実装

ActiveView では、1 つまたは複数のドメインまたは OU の中の特定のオブジェクトにリアルタイムにアクセスできます。ActiveView からオブジェクトを、その裏側にあるドメインまたは OU の構造を変更せずに、追加または削除することができます。

ActiveView は、仮想ドメインまたは仮想 OU だと考えてもよいし、リレーショナルデータベースの場合は select ステートメントまたはデータベースビューの結果とみなすこともできます。ActiveView では、任意のオブジェクトセットを含めたり除外したり、他の ActiveView を内包したり、重なり合うコンテンツを持つこともできます。ActiveView には、異なるドメイン、ツリー、フォレストからでもオブジェクトを含めることができます。ActiveView は、その設定次第でどのような企業管理ニーズにも応えることができます。

Activeview に含めることができるオブジェクトタイプは次のとおりです。

アカウント :

- ユーザ
- グループ
- コンピュータ
- 連絡先
- ダイナミック配布グループ
- グループ管理対象サービスアカウント
- 公開プリンタ
- 公開プリンタのプリントジョブ
- リソースメールボックス
- 共有メールボックス
- パブリックフォルダ

ディレクトリオブジェクト :

- 部門 (OU)
- ドメイン
- メンバーサーバ

委任オブジェクト :

- ActiveView
- 自己管理
- ダイレクトレポート
- 管理対象のグループ

リソース :

- 接続ユーザ

- デバイス
- イベントログ
- オープンファイル
- プリンタ
- プリントジョブ
- サービス
- 共有

Azure オブジェクト :

- Azure ユーザ
- Azure ゲストユーザ
- Azure グループ
- Azure テナント
- Azure 連絡先

企業の変化と成長に合わせて、ActiveView も新しいオブジェクトを含めたり除外しながら変化します。したがって、ActiveView を使用すれば、現モデルの複雑さが軽減され、必要なセキュリティが確保でき、他企業の整理ツールよりもはるかに優れた柔軟性を得ることができます。

ActiveView のルール

アクティブビューは、ユーザアカウント、グループ、OU、連絡先、リソース、コンピュータ、リソースメールボックス、共有メールボックス、ダイナミック配布グループ、グループ管理対象サービスアカウント、アクティブビュー、および Azure ユーザ、Azure ゲストユーザ、Azure グループ、Azure 連絡先などの Azure オブジェクトを含めるルール、または排除するルールで構成することができます。この柔軟性により ActiveView がダイナミックになります。

このような一致を「**ワイルドカード**」と呼びます。たとえば、DOM* と一致する名前を持つすべてのコンピュータを含めるようなルールを定義することができます。このようにワイルドカードで指定すると、名前が文字列「DOM」で始まるコンピュータアカウントをすべて検索します。ワイルドカード一致では、アカウントがルールと一致したときにそれが自動的に含まれるため、管理がダイナミックなものになります。そのため、ワイルドカードを使用すると、組織変更があっても、ActiveView を再設定する必要がありません。

もう 1 つの例は、グループメンバーシップに基づいた ActiveView の定義です。「NYC」の 3 文字で始まるグループメンバーをすべて含めるルールを定義することができます。その後で、メンバーがこのルールに一致するあらゆるグループに追加されたときに、これらのメンバーは自動的にこの ActiveView に含まれます。企業が改変されたり成長した際に、新しいオブジェクトを適切な ActiveView 内に含めるルール、またはそこから除外するルールを DRA が再び適用します。

8 役割

このセクションでは、DRA に組み込まれている役割の説明のリスト、これらの役割を使用する方法、およびカスタム役割の作成と管理に関する情報を掲載します。

各役割についての説明と一般的な使用法は、「委任モデルのコントロール」を参照してください。

組み込みの役割

ビルトインアシスタント管理者という役割により、一般的に使用される一連の権限に直接アクセスできます。これらデフォルトの役割を使用して権限を特定のユーザアカウントまたは他のグループに委任することによって、現在使用中のセキュリティ構成を拡張することができます。

これらの役割には、共通管理タスクを実行するために必要な権限が含まれています。たとえば、DRA の管理役割にはオブジェクトの管理に必要な権限がすべて含まれています。ただし、これらの権限を使用するには、ユーザアカウント (またはアシスタント管理者グループ) および管理対象の ActiveView に役割が関連付けられている必要があります。

組み込みの役割がデフォルトの委任モデルの一部であるため、組み込みの役割を使用して素早く権限を委任でき、セキュリティを実装できます。これらの組み込み役割は、DRA のユーザインタフェースから実行できる共通タスクに対処します。以下のセクションで、組み込みの役割を説明し、その役割に関連付けられた権限についてまとめます。

Azure Active Directory 管理

Azure 連絡先管理

Azure 連絡先のプロパティを作成、変更、削除、および表示するために必要なすべての権限を提供します。Azure 連絡先の管理を担当するアシスタント管理者全員にこの役割を割り当てることができます。

Azure グループの管理

Azure グループおよび Azure メンバーシップの管理に必要なすべての権限を提供します。

Azure ユーザの管理

Azure ユーザのプロパティを作成、変更、削除、有効化、無効化、および表示するために必要なすべての権限を提供します。Azure ユーザの管理を担当するアシスタント管理者に、この役割を割り当ててください。

Azure ゲストユーザの管理

Azure ゲストユーザを管理するために必要なすべての権限を提供します。Azure ゲストユーザの管理を担当するアシスタント管理者に、この役割を割り当ててください。

管理

連絡先の管理

新しい連絡先の作成、連絡先プロパティの変更、連絡先の削除に必要な権限がすべて用意されています。連絡先の管理を担当するアシスタント管理者に、この役割を割り当ててください。

DRA の管理

アシスタント管理者にすべての権限を提供します。この役割では、DRA 内のすべての管理タスクを実行するパーミッションがユーザに与えられます。この役割は、管理者のパーミッションに相当します。DRA の管理の役割に関連付けられたアシスタント管理者は、Directory and Resource Administrator のすべてのノードにアクセスできます。

gMSA の管理

グループ管理対象サービスアカウント (gMSA) のプロパティを作成、変更、削除、および表示するために必要な権限を提供します。gMSA の管理を担当するアシスタント管理者全員にこの役割を割り当てることができます。

カスタムツールの管理と実行

カスタムツールの作成、管理、および実行に必要な権限がすべて用意されています。カスタムツールの管理を担当するアシスタント管理者に、この役割を割り当ててください。

クローン例外を管理する

クローン例外の作成および管理に必要な権限がすべて用意されています。

ポリシーおよび自動化トリガを管理する

ポリシーおよび自動化トリガを定義するために必要な権限がすべて用意されています。企業ポリシーを維持管理してワークフローを自動化することを担当するアシスタント管理者に、この役割を割り当ててください。

セキュリティモデルを管理する

ActiveView、アシスタント管理者、役割など、管理ルールを定義するために必要な権限がすべて用意されています。セキュリティモデルの実装と維持管理を担当するアシスタント管理者に、この役割を割り当ててください。

仮想属性を管理する

仮想属性の作成および管理に必要な権限がすべて用意されています。仮想属性の管理を担当するアシスタント管理者に、この役割を割り当ててください。

OU の管理

部門 (OU) を管理するために必要な権限がすべて用意されています。Active Directory の構造の管理を担当するアシスタント管理者に、この役割を割り当ててください。

パブリックフォルダの管理

メールの作成、変更、削除、有効化、無効化、およびパブリックフォルダのプロパティ表示のための権限が用意されています。パブリックフォルダの管理を担当するアシスタント管理者全員にこの役割を割り当てることができます。

ファイルを複製する

ファイルの情報をアップロード、削除、および変更するために必要な権限がすべて用意されています。プライマリ管理サーバから MMS の他の管理サーバや DRA のクライアントコンピュータにファイルを複製することを担当するアシスタント管理者に、この役割を割り当ててください。

ローカル管理者パスワードをリセットする

ローカルの管理者アカウントのパスワードをリセットしたり、コンピュータ管理者の名前を表示するための権限がすべて用意されています。管理アカウントの管理を担当するアシスタント管理者に、この役割を割り当ててください。

自己管理

電話番号など、自分のユーザアカウントの基本プロパティを変更するために必要な権限がすべて用意されています。アシスタント管理者が自分の個人情報を管理できるようにする場合に、この役割をアシスタント管理者に割り当ててください。

詳細クエリの管理

詳細クエリを実行する

保存された詳細クエリの実行に必要な権限がすべて用意されています。詳細クエリの実行を担当するアシスタント管理者に、この役割を割り当ててください。

詳細クエリを管理する

詳細クエリの作成、管理、および実行に必要な権限がすべて用意されています。詳細クエリの管理を担当するアシスタント管理者に、この役割を割り当ててください。

監査管理

すべてのオブジェクトを監査する

企業内のオブジェクト、ポリシー、構成の各プロパティを表示するために必要な権限がすべて用意されています。この役割でアシスタント管理者がプロパティを変更することはできません。社内のアクションの監査を担当するアシスタント管理者に、この役割を割り当ててください。カスタムツールのノードを除くすべてのノードをアシスタント管理者が表示できます。

制限付きアカウントおよびリソースプロパティを監査する

すべてのオブジェクトプロパティに対する権限が用意されています。

リソースを監査する

管理対象リソースのプロパティを表示するために必要な権限がすべて用意されています。リソースオブジェクトの監査を担当するアシスタント管理者に、この役割を割り当ててください。

ユーザとグループを監査する

ユーザアカウントとグループプロパティの表示に必要な権限はすべて用意されていますが、これらのプロパティを変更する権限はありません。アカウントプロパティの監査を担当するアシスタント管理者に、この役割を割り当ててください。

コンピュータ管理

コンピュータ管理

コンピュータのプロパティを変更するために必要な権限がすべて用意されています。この役割により、アシスタント管理者がコンピュータを追加、削除、シャットダウンでき、ドメインコントローラの同期化もできます。ActiveView 内のコンピュータの管理を担当するアシスタント管理者に、この役割を割り当ててください。

コンピュータアカウントを作成および削除する

コンピュータアカウントの作成と削除に必要な権限がすべて用意されています。コンピュータの管理を担当するアシスタント管理者に、この役割を割り当ててください。

コンピュータのプロパティを管理する

コンピュータアカウントのすべてのプロパティを管理するために必要な権限がすべて用意されています。コンピュータの管理を担当するアシスタント管理者に、この役割を割り当ててください。

すべてのコンピュータプロパティを表示する

コンピュータアカウントのプロパティを表示するために必要な権限がすべて用意されています。コンピュータの監査を担当するアシスタント管理者に、この役割を割り当ててください。

Exchange の管理

メールボックスのあるユーザのクローンを作成する

アカウントのメールボックスを伴う既存のユーザアカウントのクローンを作成するために必要な権限がすべて用意されています。ユーザアカウントの管理を担当するアシスタント管理者に、この役割を割り当ててください。

注 : クローン作成タスクの間にアシスタント管理者に新しいユーザアカウントをグループに追加することを許可するには、Manage Group Memberships (グループメンバーシップの管理) という役割も割り当ててください。

リソースメールボックスを作成および削除する

メールボックスの作成と削除に必要な権限がすべて用意されています。メールボックスの管理を担当するアシスタント管理者に、この役割を割り当ててください。

メールボックスの管理

Microsoft Exchange のメールボックスプロパティの管理に必要な権限がすべて用意されています。Microsoft Exchange を使用する場合は、Microsoft Exchange のメールボックス管理を担当するアシスタント管理者に、この役割を割り当ててください。

Exchange メールボックスの権限を管理する

Microsoft Exchange メールボックスのセキュリティと権限を管理するために必要な権限がすべて用意されています。Microsoft Exchange を使用する場合は、Microsoft Exchange メールボックス権限の管理を担当するアシスタント管理者に、この役割を割り当ててください。

グループの電子メールを管理する

グループの電子メールアドレスの表示、有効化、無効化に必要な権限がすべて用意されています。アカウントオブジェクトのグループまたは電子メールアドレスの管理を担当するアシスタント管理者に、この役割を割り当ててください。

メールボックスの移動要求を管理する

メールボックスの移動要求の管理に必要な権限がすべて用意されています。

リソースメールボックスのプロパティを管理する

メールボックスのすべてのプロパティを管理するために必要な権限がすべて用意されています。メールボックスの管理を担当するアシスタント管理者に、この役割を割り当ててください。

ユーザの電子メールを管理する

ユーザアカウントの電子メールアドレスの表示、有効化、無効化に必要な権限がすべて用意されています。アカウントオブジェクトに関するユーザアカウントまたは電子メールアドレスの管理を担当するアシスタント管理者に、この役割を割り当ててください。

ユニファイドメッセージング PIN のプロパティをリセットする

ユーザアカウントに関するユニファイドメッセージング PIN のプロパティをリセットするために必要な権限がすべて用意されています。

リソースメールボックスの管理

リソースメールボックスを管理するために必要な権限がすべて用意されています。

共有メールボックスの管理

共有メールボックスのプロパティを作成、変更、削除、および共有するために必要な権限がすべて用意されています。共有メールボックスの管理を担当するアシスタント管理者の全員に、この役割を割り当ててください。

すべてのリソースメールボックスプロパティを表示する

リソースメールボックスのプロパティを表示するために必要な権限がすべて用意されています。リソースメールボックスの監査を担当するアシスタント管理者に、この役割を割り当ててください。

グループ管理

グループを作成および削除する

グループの作成と削除に必要な権限がすべて用意されています。グループの管理を担当するアシスタント管理者に、この役割を割り当ててください。

ダイナミックグループの管理

Active Directory のダイナミックグループの管理に必要な権限がすべて用意されています。

グループ管理

グループとグループメンバーシップの管理、および対応するユーザプロパティの表示に必要な権限がすべて用意されています。グループの管理、またはグループを通じて管理されるアカウントとリソースオブジェクトの管理を担当するアシスタント管理者に、この役割を割り当ててください。

ダイナミック配布グループを管理する

Microsoft Exchange のダイナミック配布グループの管理に必要な権限がすべて用意されています。

グループメンバーシップのセキュリティを管理する

Microsoft Windows のグループメンバーシップを Microsoft Outlook から表示および変更できるユーザを指定するのに必要な権限がすべて用意されています。

グループメンバーシップを管理する

ユーザアカウントまたはグループを既存のグループから追加および削除し、ユーザまたはコンピュータアカウントのプライマリグループを表示するために必要な権限がすべて用意されています。グループまたはユーザアカウントの管理を担当するアシスタント管理者に、この役割を割り当ててください。

グループのプロパティを管理する

グループのすべてのプロパティを管理するために必要な権限がすべて用意されています。グループの管理を担当するアシスタント管理者に、この役割を割り当ててください。

一時グループ割り当てを管理する

一時グループ割り当ての作成および管理に必要な権限がすべて用意されています。グループの管理を担当するアシスタント管理者に、この役割を割り当ててください。

グループ名を変えて説明を変更する

グループの名前と説明を変更するために必要な権限がすべて用意されています。グループの管理を担当するアシスタント管理者に、この役割を割り当ててください。

すべてのグループプロパティを表示する

グループのプロパティを表示するために必要な権限がすべて用意されています。グループの監査を担当するアシスタント管理者に、この役割を割り当ててください。

レポーティング管理

Active Directory コレクタ、DRA コレクタ、および管理レポートコレクタを管理する

Active Directory コレクタ、DRA コレクタ、および管理レポートコレクタの管理に必要なデータ収集用の権限がすべて用意されています。レポーティングの設定の管理を担当するアシスタント管理者に、この役割を割り当ててください。

Active Directory コレクタ、DRA コレクタ、管理レポートコレクタ、およびデータベース構成を管理します。

Active Directory コレクタ、DRA コレクタ、管理レポートコレクタ、およびデータベース構成の管理に必要なデータ収集用の権限がすべて用意されています。レポーティングおよびデータベース構成の管理を担当するアシスタント管理者に、この役割を割り当ててください。

UI レポート機能を管理する

ユーザ、グループ、連絡先、コンピュータ、部門、権限、役割、ActiveView、コンテナ、公開プリンタは、およびアシスタント管理者に関する Activity Detail レポートの生成およびエクスポートに必要な権限がすべて用意されています。レポート生成を担当するアシスタント管理者に、この役割を割り当ててください。

データベースの構成を管理する

管理レポート用のデータベースの構成を管理するために必要な権限がすべて用意されています。レポーティングデータベースの構成管理を担当するアシスタント管理者に、この役割を割り当ててください。

Active Directory コレクタ、DRA コレクタ、管理レポートコレクタ、およびデータベース構成の情報を表示します。

AD コレクタ、DRA コレクタ、管理レポートコレクタ、およびデータベース構成の情報を表示するために必要な権限がすべて用意されています。

Resource Management

リソースを作成および削除する

共有とコンピュータアカウントを作成および削除しイベントログをクリアするために必要な権限がすべて用意されています。リソースオブジェクトとイベントログの管理を担当するアシスタント管理者に、この役割を割り当ててください。

プリンタとプリントジョブを管理する

プリンタ、プリントキュー、およびプリントジョブの管理に必要な権限がすべて用意されています。ユーザアカウントに関連付けられたプリントジョブを管理するには、プリントジョブとユーザアカウントを同じ ActiveView に追加する必要があります。プリンタの保守およびプリントジョブの管理を担当するアシスタント管理者に、この役割を割り当ててください。

管理対象ユーザのリソースを管理する

特定のユーザアカウントに関連付けられているリソースを管理するために必要な権限がすべて用意されています。アシスタント管理者およびユーザアカウントは同じ ActiveView に含める必要があります。リソースオブジェクトの管理を担当するアシスタント管理者に、この役割を割り当ててください。

サービスを管理する

サービスを管理するために必要な権限がすべて用意されています。サービスの管理を担当するアシスタント管理者に、この役割を割り当ててください。

共有フォルダを管理する

共有フォルダを管理するために必要な権限がすべて用意されています。共有フォルダの管理を担当するアシスタント管理者に、この役割を割り当ててください。

リソースの管理

ユーザアカウントに関連付けられたリソースを含め、管理対象リソースのプロパティを変更するために必要な権限がすべて用意されています。リソースオブジェクトの管理を担当するアシスタント管理者に、この役割を割り当ててください。

リソースを開始および停止する

サービスの一時停止、開始、再開、または停止、デバイスまたはプリンタの開始または停止、コンピュータのシャットダウン、およびドメインコントローラの同期化に必要な権限がすべて用意されています。また、サービスの一時停止、再開、および開始、デバイスまたはプリントキューの停止、およびコンピュータのシャットダウンに必要な権限がすべて用意されています。リソースオブジェクトの管理を担当するアシスタント管理者に、この役割を割り当ててください。

サーバ管理

組み込みスケジューラ - 社外秘

DRA がキャッシュを更新するときにスケジュールを行う権限が用意されています。

アプリケーションサーバの管理

アプリケーションサーバの設定を構成、表示、削除するために必要な権限が用意されています。

サーバとドメインを設定する

管理サーバのオプションおよび管理対象ドメインを変更するために必要な権限がすべて用意されています。さらに、Azure テナントを構成および管理するために必要な権限もあります。管理サーバの監視および保守の担当、また Azure テナントの管理を担当するアシスタント管理者に、この役割を割り当ててください。

統合された変更履歴のサーバの管理

統合された変更履歴のサーバの設定を構成、表示、削除するために必要な権限が用意されています。

ワークフロー自動化サーバの管理

ワークフロー自動化サーバの設定を構成、表示、削除するために必要な権限が用意されています。

ユーザアカウントの管理

ユーザアカウントを作成および削除する

ユーザアカウントの作成と削除に必要な権限がすべて用意されています。ユーザアカウントの管理を担当するアシスタント管理者に、この役割を割り当ててください。

ヘルプデスクの管理

ユーザアカウントプロパティの表示、およびプロパティ関連のパスワードとパスワードの変更に必要な権限がすべて用意されています。この役割でアシスタント管理者はユーザアカウントの無効化、有効化、およびロック解除ができます。この役割は、ユーザに自分のアカウントに適切にアクセスできる権限を持たせることが必要なヘルプデスク任務を担当するアシスタント管理者に割り当ててください。

プロパティでユーザのダイヤルを管理する

ユーザアカウントのプロパティでダイヤルを変更するために必要な権限がすべて用意されています。会社へのリモートアクセスが可能なユーザアカウントの管理を担当するアシスタント管理者に、この役割を割り当ててください。

ユーザのパスワードを管理しアカウントをロック解除する

パスワードのリセット、パスワード設定の指定、ユーザアカウントのロック解除に必要な権限がすべて用意されています。ユーザアカウントのアクセス権の維持管理を担当するアシスタント管理者に、この役割を割り当ててください。

ユーザプロパティを管理する

Microsoft Exchange のメールボックスプロパティを含め、ユーザアカウントのプロパティすべてを管理するために必要な権限がすべて用意されています。ユーザアカウントの管理を担当するアシスタント管理者に、この役割を割り当ててください。

ユーザ名を変えて説明を変更する

ユーザアカウントの名前と説明を変更するために必要な権限がすべて用意されています。ユーザアカウントの管理を担当するアシスタント管理者に、この役割を割り当ててください。

パスワードをリセットする

パスワードのリセットと変更に必要な権限がすべて用意されています。パスワード管理を担当するアシスタント管理者に、この役割を割り当ててください。

SPA を使用してパスワードをリセットしアカウントをロック解除する

Secure Password Administrator を使用してパスワードのリセットとユーザアカウントのロック解除を行うために必要な権限がすべて用意されています。

ユーザを変換する

テンプレートアカウントで見つかったユーザのグループへの追加とグループからの削除に必要な権限がすべて用意されています。これには、そのユーザを変換しつつ、そのユーザのプロパティを変更する能力も含まれます。

ユーザ管理

ユーザアカウント、関連の Microsoft Exchange メールボックス、およびグループメンバーシップを管理するために必要な権限がすべて用意されています。ユーザアカウントの管理を担当するアシスタント管理者に、この役割を割り当ててください。

すべてのユーザプロパティを表示する

ユーザアカウントのプロパティを表示するために必要な権限がすべて用意されています。ユーザアカウントの監査を担当するアシスタント管理者に、この役割を割り当ててください。

WTS の管理

WTS 環境のプロパティを管理する

ユーザアカウントに関する WTS 環境のプロパティを変更するために必要な権限のすべてが用意されています。ユーザアカウントの管理または WTS 環境の維持管理を担当するアシスタント管理者に、この役割を割り当ててください。

WTS リモート管理のプロパティを管理する

ユーザアカウントに関する WTS リモート管理のプロパティを変更するために必要な権限がすべて用意されています。ユーザアカウントの管理または WTS アクセスの維持管理を担当するアシスタント管理者に、この役割を割り当ててください。

WTS セッションのプロパティを管理する

ユーザアカウントに関する WTS セッションのプロパティを変更するために必要な権限がすべて用意されています。ユーザアカウントの管理または WTS セッションの維持管理を担当するアシスタント管理者に、この役割を割り当ててください。

WTS ターミナルのプロパティを管理する

ユーザアカウントに関する WTS ターミナルのプロパティを変更するために必要な権限がすべて用意されています。ユーザアカウントの管理または WTS 端末プロパティの維持管理を担当するアシスタント管理者に、この役割を割り当ててください。

WTS の管理

ActiveView 内のユーザアカウントに関し WTS (Windows Terminal Server) プロパティの管理に必要な権限がすべて用意されています。WTS を使用する場合に、ユーザアカウントの WTS プロパティの維持管理を担当するアシスタント管理者に、この役割を割り当ててください。

組み込み役割へのアクセス

組み込み役割にアクセスしてデフォルトの委任モデルの監査や自分のセキュリティの設定を管理します。

組み込みの役割にアクセスするには :

1 ［ **[Delegation Management]**］ > ［ **[Manage Roles (役割を管理)]**］の順に選択します。

2 検索フィールドが空であることを確認し、［ **[List items that match my criteria (自分の基準に一致する項目をリスト表示)]**］ペインで ［ **[Find Now (今すぐ検索)]**］をクリックします。

3 適切な役割を選択します。

組み込みの役割の使用

組み込みの役割は削除および変更できません。ただし、組み込みの役割を既存の委任モデルに組み入れたり、これらの役割を使用して独自のモデルを設計および実装することはできます。

組み込みの役割は次の方法で使用できます。

- ビルトインの役割をユーザアカウントやアシスタント管理者グループに関連付けます。この関連付けで、ユーザまたはアシスタント管理者グループのメンバーがタスクのための適切な権限を得ることができます。
- 組み込み役割のクローンを作成し、カスタマイズする役割のベースとしてそのクローンを使用してください。その他の役割や権限をこの新しい役割に追加して、組み込み役割に元々含まれていた権限を削除することができます。

ダイナミック委任モデルの設計の詳細については、「ダイナミック委任モデルについて」を参照してください。

カスタムの役割の作成

役割を作成すると、管理タスクまたはワークフローを表す権限のセットを簡単かつ迅速に委任できます。Delegation and Configuration Console (委任および環境設定コンソール) で［[Delegation Management]］>［[役割]］ノードからロールの作成および管理します。このノードでは次の操作を行うことができます。

- 新しい役割を作成する
- 既存の役割のクローンを作成する
- 役割のプロパティを変更する
- 役割を削除する
- 役割割り当てを管理する
  - 新しい割り当てを委任する
  - 既存の割り当てを削除する
  - 割り当てられたアシスタント管理者のプロパティを表示する
  - 割り当てられた ActiveView のプロパティを表示する
- 役割と役割内の権限を管理する (役割はネスト可能)
- 役割変更レポートを生成する

このセクションで確認したアクションのいずれかを実行するには、［[役割]］ノードを選択してから、次に示す操作のうち 1 つを行うのが一般的な流れです。

- ［[タスク]］メニューまたは右クリックメニューを使用して、該当するウィザードまたはダイアログボックスを開き、後続の必要なアクションを行います。
- ［[List items that match my criteria (自分の基準に一致する項目をリスト表示)]］ペインで役割オブジェクトを見つけて、［[タスク]］メニューか右クリックメニューを使用して該当するウィザードまたはダイアログボックスを選択して開き、後続の必要な操作を実行します。

上のアクションのいずれかを実行するには、Manage Security Model という役割に含まれている権限のような、適切な権限が必要です。

9 権限

権限は、「最小特権」管理において最初の構成要素です。ユーザに権限を割り当てておくと、ダイナミックセキュリティモデルの実装と維持に役立ちます。これらの手順は、Delegation and Configuration console (委任および環境設定コンソール) で実行します。

組み込みの権限

役割定義および委任割り当てを行うときに使う可能性のある管理共通タスクの実行やオブジェクト管理のための組み込み権限が 390 以上もあります。組み込み権限は削除できませんが、そのクローンを作成してカスタム権限を作ることはできます。次に、組み込み権限の例をいくつか示します。

グループを作成してすべてのプロパティを変更する

グループを作成してグループ作成中にプロパティをすべて指定するための権限があります。

ユーザアカウントを削除する

ごみ箱が有効であれば、ユーザアカウントをごみ箱に移動する権限があります。ごみ箱が無効であれば、ユーザアカウントを永久に削除する権限があります。

すべてのコンピュータプロパティを変更する

コンピュータアカウントのプロパティをすべて変更する権限があります。

Azure の権限

次の権限を使用して、Azure ユーザ、グループ、および連絡先の作成および管理を委任します。

Azure User Account Powers (Azure ユーザアカウント権限):

- Azure ユーザの作成およびすべてのプロパティの変更
- Azure ユーザアカウントの完全削除
- Azure ユーザのサインインの管理
- Azure テナントと同期される Azure ユーザのサインインの管理
- すべての Azure ユーザプロパティの変更
- Azure ユーザアカウントのパスワードのリセット
- すべての Azure ユーザプロパティの表示

Azure Group Powers (Azure グループの権限):

- Azure グループへのオブジェクトの追加

- Azure グループの作成およびすべてのプロパティの変更
- Azure グループアカウントの削除
- すべての Azure グループのプロパティの変更
- Azure グループからオブジェクトの削除
- すべての Azure グループプロパティの表示

Azure 連絡先の権限 :

- Azure 連絡先の作成およびすべてのプロパティの変更
- Azure 連絡先アカウントの削除
- すべての Azure 連絡先のプロパティの変更
- すべての Azure 連絡先プロパティの表示

Azure ゲストユーザアカウントの権限 :

- Azure ゲストユーザの招待

Azure ユーザアカウントに一覧表示されている権限は、Azure ゲストユーザアカウントにも適用されます。

Azure オブジェクトの詳細なレベルのプロパティを管理するには、特定のオブジェクト属性を選択することでカスタム権限を作成します。

カスタム権限の実装

カスタム権限を作成するには、新しい権限を作成するか既存の権限のクローンを作成します。既存の権限を新しい権限委任のテンプレートとして使用できます。権限は、管理対象ドメインまたはサブツリー内でアシスタント管理者が表示、変更、または作成できるオブジェクトプロパティを定義します。カスタム権限には、*View All User Properties* という権限のような、複数のプロパティへのアクセス権を含めることができます。

注 : 組み込み権限はどれもクローン作成できません。

カスタム権限は、Delegation and Configuration Console (委任および環境設定コンソール) の［ **[Delegation Management]**］>［ **[権限]**］ノードから実装します。このノードでは次の操作を行うことができます。

- すべての権限プロパティの表示
- 新しい権限の作成
- 既存の権限のクローン作成
- カスタム権限の変更
- 権限変更のレポート生成

これらのアクションを実行するには、Manage Security Model という役割に含まれている権限のような、適切な権限が必要です。

新しい権限を作成する前に、以下のプロセスを考慮してください。

1. DRA に付属している権限を確認する。
2. カスタム権限が必要かどうかを判断する。それが適切な場合は、既存のカスタム権限のクローンを作成して利用できます。
3. ウィザードを使った適切な手順を実行する。たとえば、New Power ウィザードを完了します。
4. 新しい権限を表示する。
5. 必要に応じて、新しい権限を変更する。

このセクションで紹介するアクションはいずれも、実行する際に［**[権限]**］ノードを選択してから次に示す操作のいずれかを行うという流れが一般的です。

- ［タスク］メニューまたは右クリックメニューを使用して、該当するウィザードまたはダイアログボックスを開き、後続の必要なアクションを行います。
- ［**[List items that match my criteria (自分の基準に一致する項目をリスト表示)]**］ペインで権限オブジェクトを見つけて、［**[タスク]**］メニューまたは右クリックメニューを使用して該当するウィザードまたはダイアログボックスを選択して開き、後続の必要な操作を実行します。

権限の拡張

権限を拡張することで、その権限にパーミッションまたは機能を追加することができます。

たとえば、アシスタント管理者にユーザアカウントの作成を許可するために、*Create User and Modify All Properties (ユーザを作成してすべてのプロパティを変更する)* という権限と *Create User and Modify Limited Properties (ユーザを作成し限定プロパティを変更する)* という権限のいずれかを割り当てることができます。*Add New User to Group* という権限も割り当てる場合、この新しいユーザアカウントをアシスタント管理者が［ユーザの作成］ウィザードの使用中にグループに追加することができます。この場合、*Add New User to Group* という権限により、ウィザードの機能が追加されます。*Add New User to Group* という権限は**拡張権限**です。

拡張権限では、単独でパーミッションや機能を追加できません。拡張権限を含むタスクを正常に委任するには、その拡張権限を、拡張する権限とともに割り当てる必要があります。

注

- グループの作成および ActiveView への新規グループの追加を正常に行うには、指定された ActiveView に、*Add New Group to ActiveView* という権限を持っている必要があります。指定された ActiveView には、新しいグループを入れる組み込みコンテナまたは OU も含める必要があります。
- グループのクローン作成および ActiveView への新規グループの追加を正常に行うには、指定された ActiveView に *Add Cloned Group to ActiveView(複製されたグループを ActiveView に追加する)* という権限を持っている必要があります。指定された ActiveView には、新しいグループを入れる組み込みコンテナまたは OU の他に、ソースグループも含める必要があります。

次の表に、権限の新規作成時または既存の権限のプロパティ変更時に設定が可能なアクションの例をいくつか列挙します。

委任するタスク	割り当てる権限	拡張権限
グループを複製し、指定された ActiveView に新しいグループを含める	グループのクローンを作成してすべてのプロパティを変更する	複製されたグループを ActiveView に追加する
グループを作成し、指定された ActiveView に新しいグループを含める	グループを作成してすべてのプロパティを変更する	新しいグループを ActiveView に追加する
メールが有効な連絡先を作成する	連絡先を作成しすべてのプロパティを変更する 連絡先を作成し制限されたプロパティを変更する	新しい連絡先の電子メールを有効にする
メールが有効なグループを作成する	グループを作成してすべてのプロパティを変更する	新しいグループの電子メールを有効にする
メールが有効なユーザアカウントを作成する	ユーザを作成してすべてのプロパティを変更する ユーザを作成し限定プロパティを変更する	新しいユーザの電子メールを有効にする
ユーザアカウントを作成し、特定のグループに新しいアカウントを追加する	ユーザを作成してすべてのプロパティを変更する ユーザを作成し限定プロパティを変更する	新しいユーザをグループに追加する

10 委任の割り当て

委任割り当ては、Delegation and Configuration Console (委任および環境設定コンソール) で［ [Delegation Management]］>［ [アシスタント管理者]］ノードから管理します。このノードでは、アシスタント管理者に割り当てられた権限と役割の表示と、役割および ActiveView の割り当て管理が可能です。アシスタント管理者のグループでは、次の操作を行うことができます。

- グループメンバーを追加する
- グループを作成する
- グループのクローンを作成する
- グループを削除する
- グループプロパティを変更する

割り当ての表示と管理およびアシスタント管理者グループへの変更を行うには、Manage Security Model という役割に含まれる権限のような、適切な権限を持っている必要があります。

このセクションで確認したアクションのいずれかを実行するには、［ [アシスタント管理者]］ノードを選択してから、次に示す操作のうち 1 つを行うのが一般的な流れです。

- ［タスク］メニューまたは右クリックメニューを使用して、該当するウィザードまたはダイアログボックスを開き、後続の必要なアクションを行います。
- ［ [List items that match my criteria (自分の基準に一致する項目をリスト表示)]］ペインでグループまたはアシスタント管理者を見つけて、［ [タスク]］メニューか右クリックメニューで該当のウィザードかダイアログボックスを選んで開き、後続の必要な操作を実行します。

IV コンポーネントおよびプロセスの設定

この章では、サーバとコンソールについて、さらにサーバとコンソールのカスタマイズや、Azure 管理、パブリックフォルダの管理、サーバへの接続など、DRA を初めて設定する人のための情報を提供します。

11 初期設定

このセクションでは、Directory and Resource Administrator を初めてインストールする場合に必要な設定手順について概説します。

設定チェックリスト

次のチェックリストを使用し、初めて DRA を設定する手順を説明します。

ステップ	詳細
DRA ライセンスをインストールする	正常性検査ユーティリティを使用して、DRA ライセンスを適用します。DRA ライセンスの詳細については、「ライセンスの要件」を参照してください。
DRA サーバと機能を設定する	MMS、クローン例外、ファイルのレプリケーション、イベントスタンプ、キャッシュ動作、AD LDS、ダイナミックグループ、ごみ箱、レポート機能、統合された変更履歴、およびワークフローサーバを設定します。
変更履歴レポーティングの設定 (オプション)	Change Guardian サーバと統合して、DRA の内部および外部の両方のユーザイベントの変更履歴データを収集する場合は、変更履歴レポーティングの設定をします。
DRA サービスを gMSA アカウントに設定する (オプション)	複数のサーバと単一のサーバで認証プロトコルを管理する場合は、DRA サービスをグループ管理対象サービスアカウント (gMSA) 用に設定します。
Delegation and Configuration のクライアントを設定する	Delegation and Configuration のクライアントで項目がどのようにアクセスされ表示されるかを設定します。
Web クライアントを設定する	自動ログアウト、証明書、サーバ接続、および認証コンポーネントを設定します。

ライセンスのインストールまたはアップグレード

DRA にはライセンスキーファイルが必要です。このファイルにはライセンス情報が収められており、管理サーバにインストールされます。管理サーバのインストールが完了した後、ヘルスチェックユーティリティを使用して購入したライセンスをインストールします。必要に応じて、無制限のユーザアカウントやメールボックスを 30 日間管理できる試用版ライセンスキーファイル (TrialLicense.lic) もインストールパッケージに含まれています。

既存のライセンスまたは試用ライセンスをアップグレードする場合、Delegation and Configuration Console (委任および環境設定コンソール) を開き、[**[環境設定管理]**] > [**[Update License (ライセンスのアップデート)]**] と移動します。ライセンスをアップグレードするときには、各管理サーバ上のライセンスファイルをアップグレードします。

製品のライセンスは、Delegation and Configuration コンソールで確認できます。製品のライセンスを表示するには、[**[ファイル]**] メニュー > [**[DRA プロパティ]**] > [**[ライセンス]**] の順に選択します。

DRA サーバと機能を設定する

DRA を使用して Active Directory のタスク用に最小特権アクセスを管理する場合、多くのコンポーネントおよびプロセスを設定する必要があります。これには一般的なコンポーネントの設定と、クライアントコンポーネントの設定があります。このセクションでは、DRA 用に設定する必要のある一般的なコンポーネントとプロセスについての情報を記載します。

- 91 ページの 「マルチマスタセットの設定」
- 94 ページの 「クローン例外の管理」
- 94 ページの 「ファイルのレプリケーション」
- 97 ページの 「Azure Sync」
- 97 ページの 「グループに複数のマネージャを有効にする」
- 98 ページの 「暗号通信」
- 98 ページの 「仮想属性の定義」
- 100 ページの 「キャッシュ動作の設定」
- 102 ページの 「Active Directory のプリンタのコレクションの有効化」
- 102 ページの 「AD LDS」
- 103 ページの 「ダイナミックグループ」
- 103 ページの 「ごみ箱の設定」
- 104 ページの 「レポーティング環境設定」
- 106 ページの 「ワークフロー自動化サーバの設定権限を委任する」
- 107 ページの 「ワークフロー自動化サーバの設定」
- 107 ページの 「LDAP 検索権限を委任する」

マルチマスタセットの設定

MMS 環境では、ドメインとメンバーサーバの同じセットを複数の管理サーバで管理します。MMS は、1 つのプライマリ管理サーバと複数のセカンダリ管理サーバで構成されます。

管理サーバのデフォルトモードはプライマリです。セカンダリサーバを MMS 環境に追加するときは、セカンダリ管理サーバが 1 つのサーバセットにしか所属できないので注意してください。

セット内の各サーバが確実に同じデータを管理できるようにするために、定期的に各セカンダリサーバをプライマリ管理サーバと同期させる必要があります。保守の手間を減らすために、ドメインフォレスト内のすべての管理サーバに対して同じサービスアカウントを使用してください。

重要

- セカンダリサーバをインストールしている間は、インストーラで［[セカンダリ管理サーバ]］を選択してください。
- プライマリサーバで使用できる機能がすべてセカンダリサーバでも使用できるようにするため、新しいセカンダリの DRA バージョンをプライマリ DRA サーバと同じにする必要があります。

- 91 ページの 「セカンダリ管理サーバの追加」
- 92 ページの 「セカンダリ管理サーバの格上げ」
- 93 ページの 「プライマリ管理サーバの格下げ」
- 93 ページの 「同期のスケジューリング」

セカンダリ管理サーバの追加

Delegation and Configuration のクライアント内の既存の MMS にセカンダリ管理サーバを追加することができます。

注 : 新しいセカンダリサーバを追加するためには、まずその管理サーバコンピュータに Directory and Resource Administrator 製品をインストールする必要があります。詳細については、「DRA 管理サーバのインストール」を参照してください。

セカンダリ管理サーバを追加するには、以下の手順を実行します。

1. 環境設定管理ノードで［[管理サーバ]］を右クリックし、［[Add Secondary Server(セカンダリサーバの追加)]］を選択します。
2. セカンダリサーバの追加ウィザードで、［次へ］をクリックします。
3. ［セカンダリサーバ］タブで、MMS に追加するセカンダリ管理サーバの名前を指定します。

4 ［アクセスアカウント］タブで、セカンダリ管理サーバのサービスアカウントを指定します。DRA は、セカンダリ管理サーバを MMS に追加するためだけにこのアカウントを使用します。

5 ［マルチマスタアクセスアカウント］タブで、プライマリ管理サーバが MMS 操作に使用するアクセスアカウントを指定します。セカンダリ管理サーバのサービスアカウントは、マルチマスタアクセスアカウントとして使用しないことをお勧めします。セカンダリ管理者サーバに関連付けられたドメインの任意のユーザアカウントを指定できます。マルチマスタアクセスアカウントは、セカンダリサーバ上のローカル管理者グループの一部である必要があります。マルチマスタアクセスアカウントに MMS 操作を実行するための十分な権限がない場合、DRA サーバは必要な権限をマルチマスタアクセスアカウントに自動的に委任します。

セカンダリ管理サーバの格上げ

セカンダリ管理サーバをプライマリ管理サーバに格上げすることができます。セカンダリ管理サーバをプライマリ管理サーバに格上げすると、既存のプライマリ管理サーバはそのサーバセット内のセカンダリ管理サーバになります。セカンダリ管理サーバを格上げするには、Configure Servers and Domains という組み込みの役割に含まれている権限など、適切な権限が必要です。セカンダリ管理サーバを格上げする前に MMS を同期させてください。こうすることで MMS の設定が最新になります。

MMS を同期方法の詳細については、「同期のスケジューリング」を参照してください。

注 : 新しく格上げされたプライマリサーバは、格上げ処理中に使用できたセカンダリサーバにのみ接続できます。格上げ処理中にセカンダリサーバが使用不能になった場合は、テクニカルサポートに連絡してください。

セカンダリ管理サーバを格上げするには :

1 ［ **[環境設定管理]**］ > ［ **[管理サーバ]**］ノードの順に選択します。

2 右側のペインで、格上げするセカンダリ管理サーバを選択します。

3 ［タスク］メニューで、［ **[Advanced (詳細情報)]**］ > ［ **[Promote Server (サーバを格上げ)]**］をクリックします。

重要 : セカンダリサーバのサービスアカウントがプライマリサーバと異なる場合、またはセカンダリサーバがプライマリサーバ (信頼済みドメイン / 信頼できないドメイン) と異なるドメインにインストールされている場合、まず **[Audit All Objects]**、**[Configure Servers and Domains]**、および **[Generate UI Reports]** の各役割を確実に委任しておいてから、セカンダリサーバを格上げしてください。その後で MMS の同期が成功したか確認してください。

プライマリ管理サーバの格下げ

プライマリ管理サーバをセカンダリ管理サーバに格下げすることができます。プライマリ管理サーバを格下げするには、Configure Servers and Domains という組み込みの役割に含まれている権限など、適切な権限が必要です。

プライマリ管理サーバを格下げするには :

1 ［ [環境設定管理]］> ［ [管理サーバ]］ノードの順に選択します。
2 右側のペインで、格下げするプライマリ管理サーバを選択します。
3 ［タスク］メニューから ［ [Advanced (詳細情報)]］> ［ [Demote Server (サーバを格下げ)]］をクリックします。
4 新しいプライマリ管理サーバに任命するコンピュータを指定して、［ [OK]］をクリックします。

同期のスケジューリング

同期によって、MMS 内のすべての管理サーバが同じ設定データを使用することが保証されます。サーバの同期化はいつでも手動でできますが、デフォルトでは 4 時間ごとに MMS を同期するようにスケジュールされています。このスケジュールを各企業のニーズに合うように変更してください

この同期化スケジュールを変更する場合、または手動で MMS サーバを同期化するには、Configure Servers and Domains という組み込みの役割に含まれている権限など、適切な権限が必要です。

同期スケジュールにアクセスする場合、または手動の同期化に関しては、［ [Configuration Management]］> ［ [管理サーバ]］の順に選択して、［ [タスク]］メニューを使用するか、選択したサーバ上で右クリックしてオプションを選択してください。同期化のスケジュールは、選択したサーバのプロパティの中にあります。

同期化オプションについて

MMS サーバを同期化するためのオプションは、4 種類です。

- プライマリサーバを選択しセカンダリサーバをすべて同期化する「Synchronize All Servers」
- セカンダリサーバを選択して、そのサーバだけを同期化する
- プライマリサーバとセカンダリサーバの同期化スケジュールを別々に設定する
- 設定した同期化スケジュールをすべてのサーバに適用するこのオプションは、プライマリサーバの同期化スケジュールの設定で次の項目を選択した場合に有効になります。

  ［ [Configure secondary Administration servers when refreshing the primary Administration server (プライマリ管理サーバの更新時にセカンダリ管理サーバを設定)]］

注 : このオプションを選択しなかった場合、設定ファイルがプライマリスケジュール上のセカンダリサーバにコピーされますが、コピーの時点でセカンダリによってロードされることはありません。セカンダリサーバ上に設定されたスケジュールに基づい

てロードされます。これは、タイムゾーンの異なる各地にサーバが配備されている場合に便利です。たとえば、すべてのサーバについて、それぞれのタイムゾーンにおける真夜中に構成を更新するように設定することも可能です。

クローン例外の管理

クローン例外とは、オブジェクト (ユーザ、グループ、連絡先、コンピュータ) のうち 1 つに対しクローンが作成されたときにコピーされないプロパティを定義することのできる機能です。

適切な権限を持つ人がクローン例外を管理することができます。Manage Clone Exceptions という役割は、クローン例外を表示、作成、および削除する権限が与えられます。

既存のクローン例外の表示または削除、および新規のクローン例外の作成には、[**[環境設定管理]**] > [**[Clone Exceptions (クローン例外)]**] > [**[タスク]**] の順に選択するか、右クリックしてメニューから選択します。

ファイルのレプリケーション

カスタムツールを作成する場合は、それを実行する前に DRA Delegation and Configuration Console (委任および環境設定コンソール) コンピュータ上にカスタムツールが使用するサポートファイルのインストールが必要となることがあります。カスタムツールのサポートファイルは、DRA のファイルレプリケーション機能を使用してプライマリ管理サーバから MMS 内のセカンダリ管理サーバや DRA クライアントコンピュータへと複製することができます。ファイルのレプリケーションは、プライマリサーバからセカンダリサーバにトリガスクリプトを複製するときにも使用できます。

カスタムツール機能とファイルレプリケーション機能は、Delegation and Configuration Console(委任および環境設定コンソール) でのみ使用できます。

カスタムツールとファイルレプリケーション機能を合わせて使用することにより、DRA のクライアントコンピュータが確実にカスタムツールファイルにアクセスすることができます。DRA がカスタムツールファイルをセカンダリ管理サーバに複製して、セカンダリ管理サーバに接続する DRA クライアントコンピュータがカスタムツールにアクセスできるようにします。

カスタムツールファイルは、MMS の同期処理中に DRA によってプライマリ管理サーバからセカンダリ管理サーバへと複製されます。DRA のクライアントコンピュータが管理サーバに接続するときに、DRA によってカスタムツールファイルがダウンロードされます。

注 : カスタムツールファイルは、DRA クライアントコンピュータ上の次に示すディレクトリにダウンロードされます。

{DRAInstallDir}\{MMS ID}\Download

MMSID は、DRA がカスタムツールファイルをダウンロードするマルチマスタセットの ID です。

- 95 ページの 「レプリケーションのためのカスタムツールファイルのアップロード」
- 96 ページの 「管理サーバ間で複数のファイルを複製する」
- 96 ページの 「複数ファイルの DRA クライアントコンピュータへの複製」

レプリケーションのためのカスタムツールファイルのアップロード

プライマリ管理サーバにファイルをアップロードするときに、プライマリ管理サーバと MMS セット内のすべてのセカンダリ管理サーバとの間でアップロードし、複製するファイルを指定します。DRA でアップロードが許可されているのは、ライブラリファイル、スクリプトファイル、および実行ファイルです。

Replicate Files という役割を使用すると、プライマリ管理サーバから MMS 内のセカンダリ管理サーバおよび DRA のクライアントコンピュータへとファイルを複製することができます。Replicate File という役割には、次の権限が含まれています。

- **サーバからファイルを削除する** : この権限を使用すると、プライマリ管理サーバ上、セカンダリ管理サーバ上、および DRA のクライアントコンピュータ上にもはや存在しないファイルを DRA に削除させることができます。
- **ファイル情報を設定する** : この権限では、DRA がセカンダリ管理サーバ上のファイルに関するファイル情報を更新することができます。
- **ファイルをサーバにアップロードする** : この権限では、DRA が DRA のクライアントコンピュータからプライマリ管理サーバにファイルをアップロードすることができます。

注 : Delegation and Configuration Console (委任および環境設定コンソール) の中の［File Replication (ファイルのレプリケーション)］ユーザインタフェースを使用して、レプリケーションのために 1 度に 1 つのファイルをアップロードすることができます。

カスタムツールファイルをプライマリ管理サーバにアップロードする手順は、次のとおりです。

1 ［ **[Configuration Management]**］> ［ **[File Replication (ファイルレプリケーション)]**］の順に選択します。
2 ［タスク］メニューで ［ **[Upload File (ファイルをアップロード)]**］をクリックします。
3 アップロードするファイルを検索して選択するために、［ **[参照]**］をクリックします。
4 *選択したファイルをすべての DRA クライアントコンピュータにダウンロードする場合は*、［ **[Download to all client computers (すべてのクライアントコンピュータにダウンロード)]**］チェックボックスを選択します。
5 *COM ライブラリを登録する場合*は、［ **[Register COM library (COM ライブラリを登録)]**］チェックボックスを選択します。
6 ［ **[OK]**］をクリックします。

注

- DRA は、他のセカンダリ管理サーバに複製する必要のあるサポートファイルまたはスクリプトファイルを、プライマリ管理サーバの *{DRAInstallDir}*\FileTransfer\Replicate フォルダにアップロードします。*{DRAInstallDir}*\FileTransfer\Replicate フォルダは *{DRA_Replicated_Files_Path}* とも呼ばれます。
- DRA は、DRA のクライアントコンピュータに複製する必要のあるサポートファイルまたはスクリプトファイルを、プライマリ管理サーバの *{DRAInstallDir}*\FileTransfer\Download フォルダにアップロードします。
- プライマリ管理サーバにアップロードされたカスタムツールファイルは、(自動か手動かを問わず) 次の同期化処理のときにセカンダリ管理サーバに配布されます。

管理サーバ間で複数のファイルを複製する

MMS 内のプライマリ管理サーバとセカンダリ管理サーバとの間でアップロードおよび複製するファイルが複数ある場合は、次のプライマリ管理サーバのレプリケーションディレクトリにファイルをコピーすることによって、手動でこれらのファイルをアップロードすることができます。

{DRAInstallDir}\FileTransfer\Replicate

レプリケーションディレクトリは DRA インストール時に作成されます。

レプリケーションディレクトリ内のファイルは、管理サーバによって自動的に識別され、次の自動同期の間に管理サーバ間で複製されます。アップロードされたファイルは、同期後に Delegation and Configuration console (委任および環境設定コンソール) の［File Replication (ファイルレプリケーション)］ウィンドウに表示されます。

注 : 登録が必要な COM ライブラリを含むファイルを複製する場合、そのファイルを管理サーバのレプリケーションディレクトリに手動でコピー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) を使用して各ファイルをアップロードして、COM ライブラリを登録する必要があります。

複数ファイルの DRA クライアントコンピュータへの複製

プライマリ管理サーバと DRA クライアントコンピュータとの間で複製するファイルが複数ある場合、プライマリ管理サーバのクライアントレプリケーションディレクトリにファイルをコピーすることができます。コピー先のディレクトリは次のとおりです。

{DRAInstallDir}\FileTransfer\Download

クライアントレプリケーションディレクトリは DRA インストール時に作成されます。

［ダウンロード］フォルダ内のファイルは、管理サーバによって自動的に識別され、次のスケジュール設定された同期の間にセカンダリ管理サーバへと複製されます。アップロードされたファイルは、同期後に Delegation and Configuration console (委任および環境設定コン

ソール) の［File Replication (ファイルレプリケーション)］ウィンドウに表示されます。レプリケーション後に初めて DRA クライアントコンピュータが管理サーバに接続すると、複製されたファイルが DRA クライアントにダウンロードされます。

注 : 登録が必要な COM ライブラリを含むファイルを複製する場合、そのファイルを管理サーバのダウンロードディレクトリに手動でコピー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) を使用して各ファイルをアップロードして、COM ライブラリを登録する必要があります。

Azure Sync

Azure Sync はディレクトリ同期の失敗を防ぐために、無効な文字と文字長のポリシーを規定することができます。このオプションを選択すると、Azure Active Directory と同期されているすべてのプロパティで無効な文字が制限され、文字の長さの制限が適用されます。

Azure Sync を有効にするには :

1. 左側のペインで、[**[Configuration Management]**］をクリックします。
2. 右側のペインの［Common Tasks (共通タスク)］で、[**[Update Administration Server Options (管理サーバオプションを更新)]**］をクリックします。
3. ［Azure Sync］タブで、[**[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)]**］を選択します。

グループに複数のマネージャを有効にする

複数のマネージャがグループを管理するためのサポートを有効にした場合、デフォルトの 2 つの属性のうち 1 つがグループのマネージャを保存するために使用されます。Microsoft Exchange を実行するときの属性は、msExchCoManagedByLink という属性です。Microsoft Exchange を実行しないときのデフォルト属性は、nonSecurityMember という属性です。2 つ目のオプションは変更することができます。ただし、この設定を変更する必要がある場合は、技術サポートに連絡して適切な属性を決めることをお勧めします。

グループに複数マネージャのサポートを有効にするには :

1. 左側のペインで、[**[Configuration Management]**］をクリックします。
2. 右側のペインの［Common Tasks (共通タスク)］で、[**[Update Administration Server Options (管理サーバオプションを更新)]**］をクリックします。
3. ［Enable Support for Group Multiple Managers (グループの複数管理者のサポートを有効)］タブで、[**[Enable support for group's multiple managers (グループの複数管理者のサポートを有効にする)]**］チェックボックスを選択します。

暗号通信

この機能では、Delegation and Configuration クライアントと管理サーバの間での暗号化通信の使用を有効または無効にできます。デフォルトでは、DRA はアカウントパスワードを暗号化します。この機能は、Web クライアントや PowerShell の通信の暗号化に対応しません。これは別個にサーバ証明書で処理されます。

暗号通信を使用すると、パフォーマンスに影響する場合があります。暗号通信は、デフォルトでは無効になっています。このオプションを有効にすると、ユーザインタフェースと管理サーバの間での通信中にデータが暗号化されます。DRA では、リモートプロシージャコール (RPC) に Microsoft の標準暗号を使用します。

通信の暗号化を有効にするには、[**[Configuration Management]**] > [**[Update Administration Server Options (管理サーバオプションを更新)]**] > [**[全般]**] タブの順に選択し、[**[Encrypted Communications (暗号化して通信)]**] チェックボックスを選択します。

注 : 管理サーバとユーザインタフェースの間での通信をすべて暗号化するには、Configure Servers and Domains という組み込みの役割に含まれる権限など、適切な権限が必要です。

仮想属性の定義

仮想属性を使用すると、新しいプロパティを作成して、それらをユーザ、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 に関連付けることができます。仮想属性を使用すると、Active Directory スキーマを拡張しなくても新しいプロパティが作成できます。

仮想属性を使用して、Active Directory 内のオブジェクトに新しいプロパティを追加できます。仮想属性の作成、有効化、無効化、関連付け、および関連付けの解除は、プライマリ管理サーバでしかできません。DRA は、作成された仮想属性を AD LDS に保存します。仮想属性は、MMS 同期プロセス中に DRA によってプライマリ管理サーバからセカンダリ管理サーバへと複製されます。

適切な権限があれば、仮想属性を管理することができます。Manage Virtual Attributes という役割は、仮想属性を作成、有効化、関連付け、関連付け解除、無効化、および表示する権限を付与します。

- 99 ページの 「仮想属性の作成」
- 99 ページの 「仮想属性のオブジェクトへの関連付け」
- 99 ページの 「仮想属性の関連付けの解除」
- 99 ページの 「仮想属性の無効化」

仮想属性の作成

仮想属性を作成するには *Create Virtual Attributes* という権限が、仮想属性を表示するには *View Virtual Attributes* という権限が必要です。

仮想属性を作成するには、[**[Configuration Management]**] > [**[仮想属性]**] > [**[Managed Attributes (管理対象の属性)]**] ノードの順に選択し、[タスク] メニューの [**[New Virtual Attribute (新しい仮想属性)]**] をクリックします。

仮想属性のオブジェクトへの関連付け

Active Directory オブジェクトと関連付けることができるのは、有効になっている仮想属性だけです。仮想属性をオブジェクトと関連付けると、その仮想属性をオブジェクトのプロパティの一部として使用できるようになります。

DRA のユーザインタフェースから仮想属性を表示させるには、カスタムプロパティページを作成する必要があります。

オブジェクトと仮想属性を関連付けるには、[**[Configuration Management]**] > [**[仮想属性]**] > [**[Managed Attributes (管理対象の属性)]**] ノードの順に選択し、使用したい仮想属性を右クリックし、[**[Associate (関連付ける)]**] > (オブジェクトタイプ) を選択します。

注

- 仮想属性を関連付けることができるのは、ユーザ、グループ、ダイナミック配布グループ、コンピュータ、連絡先、および OU だけです。
- 仮想属性をオブジェクトと関連付けると、DRA がデフォルトのカスタム権限を自動的に 2 つ作成します。アシスタント管理者がその仮想属性を管理するためには、これらのカスタム権限が必要です。

仮想属性の関連付けの解除

仮想属性と Active Directory オブジェクトとの関連付けは解除できます。関連付けを解除した仮想属性は、その後新規に作成するオブジェクトではオブジェクトプロパティの一部として表示されなくなります。

Active Directory オブジェクトから仮想属性の関連付けを解除するためには、[**[環境設定管理]**] > [**[仮想属性]**] > [**[Managed Classes (管理対象のクラス)]**] > [(オブジェクトタイプ)] ノードの順に選択します。仮想属性を右クリックし、[**[解除]**] を選択します。

仮想属性の無効化

Active Directory オブジェクトに関連付けられていない仮想属性は、無効にできます。仮想属性を無効にすると、管理者がその仮想属性を表示したりオブジェクトと関連付けることはできなくなります。

仮想属性を無効にするには、[**[環境設定管理]**] > [**[Managed Attributes (管理対象の属性)]**] の順に選択します。リストのペインで該当する属性を右クリックして [**[無効]**] を選択します。

キャッシュ動作の設定

管理サーバは**アカウントキャッシュ**を構築および維持し、そこに管理対象ドメインの Active Directory の一部が収められます。DRA はアカウントキャッシュを使用して、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管理する際のパフォーマンスを向上させています。

キャッシュの更新をスケジュールするか、キャッシュステータスを表示するには、Configure Servers and Domains という組み込みの役割に含まれる権限など、適切な権限が必要です。

注 : 管理対象サブツリーが含まれているドメインでアカウントキャッシュの増分更新を実行するには、サービスアカウントが削除オブジェクトコンテナと当該サブツリーのドメイン内の全オブジェクトに対する読み込みアクセス権を持っている必要があります。削除オブジェクトユーティリティを使用すれば、権限をチェックして適切な権限を委任することができます。

- 100 ページの 「完全更新と増分更新」
- 101 ページの 「デフォルトスケジュールの時刻」

完全更新と増分更新

アカウントキャッシュの増分更新では、直近の更新以降に変更されたデータだけが更新されます。増分更新は、Active Directory の変化に対応してキャッシュを最新の状態に保つための能率的な手段を提供します。増分更新を使用すると、会社への影響を最小限に抑えつつ、アカウントキャッシュをすばやく更新できます。

重要 : Microsoft Server では、WinRM/WinRS のセッションに同時に接続できるユーザ数を 5 に、ユーザごとのシェル数を 5 に制限しています。このため、同じユーザアカウントが DRA のセカンダリサーバで 5 シェルに限定されるようにしてください。

増分更新では、以下のデータが更新されます。

- 新規のオブジェクトとクローンとして作成されたオブジェクト
- 削除されたオブジェクトと移動したオブジェクト
- グループメンバーシップ
- 変更されたオブジェクトに関するキャッシュされたすべてのオブジェクトプロパティ

アカウントキャッシュの完全更新では、指定されたドメインに関して DRA のアカウントキャッシュが再構築されます。

注 : アカウントキャッシュ完全更新の実行中、DRA ユーザはドメインを使用できません。

アカウントキャッシュの完全更新の実行

アカウントキャッシュを更新するには、「Configure Servers and Domains」という組み込みの役割に含まれている権限など、適切な権限が必要です。

アカウントキャッシュの完全更新を即時実行するには、以下の手順を実行します。

1 ［ [Configuration Management]］ > ［ [Managed Domains (管理対象のドメイン)]］の順に選択します。
2 目的のドメインを右クリックして、［ [プロパティ]］を選択します。
3 ［ [完全更新]］タブの ［ [今すぐ更新]］をクリックします。

デフォルトスケジュールの時刻

アカウントキャッシュを更新するべき頻度は、企業が変化する頻度によって決まります。増分更新を使用してアカウントキャッシュを頻繁に更新し、DRA が Active Directory について最新の情報を持つようにしてください。

デフォルトでは、管理サーバが次に示す時刻にアカウントキャッシュの増分更新を実行します。

ドメインタイプ	デフォルトでスケジュールされた更新時刻
管理対象ドメイン	5 分ごと
信頼されたドメイン	1 時間おき
Azure テナント	15 分ごと

FACR をスケジュールすることはできません。ただし、次のような状況では DRA が自動 FACR を実行します。

- 初めて管理対象ドメインを設定した後。
- 以前のバージョンから新しい完全バージョンに DRA をアップグレードした後。
- DRA サービスパックをインストールした後。

アカウントキャッシュの完全更新には数分かかることがあります。

注意事項

DRA に常に最新情報があるようにするために、アカウントキャッシュは定期的に更新する必要があります。アカウントキャッシュの更新を実行またはスケジュールする前に、以下の留意点を確認してください。

- アカウントキャッシュの増分更新を実行するには、管理サーバサービスアカウントまたはアクセスアカウントが管理対象ドメインまたは信頼関係があるドメインの Active Directory 内にある削除されたオブジェクトにアクセスする権限を持っている必要があります。

- DRA がアカウントキャッシュの更新を実行するとき、管理サーバは信頼関係があるドメインからのドメインローカルセキュリティグループを対象に含めません。キャッシュがこれらのグループを含んでいないため、信頼関係があるドメインからのドメインローカルセキュリティグループを管理対象メンバーサーバ上のローカルグループに追加することはできません。
- 信頼関係のあるドメインをアカウントキャッシュの更新から除外した場合は、そのドメインがドメイン構成の更新からも除外されます。
- 以前は除外した信頼関係のあるドメインをアカウントキャッシュの更新に含める場合は、管理対象ドメインに対してアカウントキャッシュの完全更新を実行してください。これにより、管理対象ドメインに関する管理対象サーバ上のアカウントキャッシュが、管理対象ドメインおよび信頼関係のあるドメイン内のグループメンバーシップを正確に反映するようになります。
- アカウントキャッシュの増分更新の間隔を［**[なし]**］に設定すると、アカウントキャッシュの完全更新だけが実行されるようになります。アカウントキャッシュの完全更新には時間がかかる場合があり、その間はそのドメイン内のオブジェクトを管理できません。
- Microsoft Directory Services など、他のツールから変更が行われた場合、それを DRA で自動的に判断することはできません。DRA の外で実行される操作が、キャッシュされた情報の正確さに影響する場合があります。たとえば、別のツールを使ってメールボックスをユーザアカウントに追加した場合、アカウントキャッシュを自分で更新するまで Exchange でそのメールボックスを管理することができません。
- アカウントキャッシュの完全更新を実行すると、キャッシュ内に保持されていた直近のログオン統計情報が削除されます。その後、管理サーバがすべてのドメインコントローラから最新のログオン情報を収集します。

Active Directory のプリンタのコレクションの有効化

AD のプリンタコレクションはデフォルトで無効になっています。これを有効にするには、［**[Configuration Management]**］>［**[Update Administration Server Options (管理サーバオプションを更新)]**］>［**[全般]**］タブの順に選択し、［Collect Printers (プリンタを収集)］チェックボックスをオンにします。

AD LDS

スケジュールに従って特定のドメインに対して AD LDS のクリーンアップ更新が実行されるように設定できます。デフォルトでは、更新「しない」に設定されています。クリーンアップのステータスも、AD LDS (ADAM) の設定に関連した特定の情報も表示することができます。

スケジュールを設定するには、または AD LDS クリーンアップのステータスを表示するには、［**[Account and Resource Management]**］>［**[すべての管理対象オブジェクト]**］ノードで目的のドメインを右クリックし、［**[プロパティ]**］>［**[Adlds Cleanup Refresh Schedule (AD LDS クリーンアップ更新スケジュール)]**］(または［**[Adlds Cleanup status (AD LDS クリーンアップステータス)]**］) の順に選択します。

AD LDS (ADAM) の設定情報を表示するには、[[Configuration Management]] > [[Update Server Options (サーバオプションを更新)]] > [[ADAM Configuration (ADAM の設定)]] の順に選択します。

ダイナミックグループ

ダイナミックグループとは、グループプロパティで設定しておいた定義済み条件セットに基づいてメンバーシップが変わるグループです。ドメインプロパティで特定のドメインに対し、スケジュールに従ってダイナミックグループの更新が実行されるように設定できます。デフォルトでは、更新「しない」に設定されています。更新のステータスを表示することもできます。

スケジュールを設定するためには、ダイナミックグループの更新のステータスを表示するには、[[Account and Resource Management]] > [[すべての管理対象オブジェクト]] ノードで目的のドメインを右クリックし、[[プロパティ]] > [[Dynamic group refresh (ダイナミックグループの更新)]] (または [[Dynamic group status (ダイナミックグループのステータス)]]) の順に選択します。

ダイナミックグループの詳細については、「DRA のダイナミックグループ」を参照してください。

ごみ箱の設定

ごみ箱を Microsoft Windows の各ドメインまたは各ドメイン内のオブジェクトに対し有効または無効に設定することができ、ごみ箱のクリーンアップの実行方法と時期も設定できます。

ごみ箱の使用の詳細については、「ごみ箱」を参照してください。

ごみ箱の有効化

特定の Microsoft Windows ドメイン、およびそれらのドメイン内のオブジェクトに対し、ごみ箱を有効にすることができます。デフォルトで DRA は、管理対象の各ドメインと、そのドメインのオブジェクトすべてに対し、ごみ箱を有効にします。ごみ箱を有効にするには、DRA Admins または DRA Configuration Admins というグループのメンバーである必要があります。

ご使用の環境が次に示す設定を含む場合、ごみ箱ユーティリティを使用してこの機能を有効にしてください。

- DRA はこのドメインのサブツリーを管理している。
- ごみ箱コンテナを作成し、このコンテナにアカウントを移動させ、このコンテナ内のアカウントを変更することのできるパーミッションが、管理サーバのサービスまたはアクセスアカウントに与えられていない。

また、ごみ箱ユーティリティを使用すれば、管理サーバのサービスの検証をしたり、ごみ箱コンテナに対するアカウントパーミッションにアクセスすることもできます。

ごみ箱を有効にするには、[[ごみ箱]] ノードの目的のドメインを右クリックし [[Enable Recycle Bin (ごみ箱を有効にする)]] を選択します。

ごみ箱の無効化

特定の Microsoft Windows ドメイン、およびそれらのドメイン内のオブジェクトに対し、ごみ箱を無効にすることができます。無効にしたごみ箱にアカウントが入っている場合、これらのアカウントの表示、永久削除、回復ができません。

ごみ箱を無効にするには、DRA Admins または DRA Configuration Admins というアシスタント管理者グループのメンバーである必要があります。

ごみ箱を無効にするには、[**[ごみ箱]**] ノードの目的のドメインを右クリックし [**[Disable Recycle Bin (ごみ箱を無効にする)]**] を選択します。

ごみ箱のオブジェクトとクリーンアップの設定

ごみ箱のクリーンアップはデフォルトで「毎日」に設定されています。この設定は、ドメインのごみ箱を任意の日数ごとにクリーンアップするように変更することができます。スケジュールされたクリーンアップの間ごみ箱は、オブジェクトタイプごとに、設定しておいた日数以上が経過したオブジェクトを削除します。各タイプのデフォルトの設定では、1 日以上が経過したオブジェクトが削除されます。ごみ箱のクリーンアップの動作は、設定を無効にし、再度有効にして、オブジェクトの削除猶予期間をオブジェクトタイプごとに設定することでカスタマイズすることができます。

ごみ箱のクリーンアップを設定するには、Delegation and Configuration console (委任および環境設定コンソール) で目的のドメインを選択し、[**[タスク]**] > [**[プロパティ]**] > [**[ごみ箱]**] タブの順に移動します。

レポーティング環境設定

以下のセクションでは、DRA 管理レポートと、有効にできるレポートコレクタについて概説します。コレクタが設定できるウィザードを表示するには、[**[Configuration Management]**] > [**[Update Reporting Service Configuration (レポーティングサービスの設定を更新)]**] の順に選択します。

Active Directory Collector の設定

Active Directory コレクタは Active Directory から、DRA 内にある管理対象ユーザ、グループ、連絡先、コンピュータ、OU、およびダイナミックグループの指定された属性セットを収集します。これらの属性は、レポーティングデータベースに保存され、Reporting コンソールでレポートを生成するために使用されます。

レポーティングデータベースにどの属性を収集および保存させるかを Active Directory コレクタを設定することができます。コレクタの実行場所となる DRA 管理サーバを設定することもできます。

DRA コレクタの設定

DRA コレクタは、DRA の設定についての情報を収集し、その情報をレポーティングコンソールがレポート生成に使用するレポーティングデータベースに保存します。

DRA コレクタを有効にするには、コレクタを実行させる DRA 管理サーバを指定する必要があります。最良の方法として、Active Directory コレクタが正常に実行された後で、サーバの通常稼働時間帯以外の期間または負荷最小期間に DRA コレクタが実行されるようにスケジュール設定することを推奨します。

Azure テナントコレクタの設定

Azure テナントコレクタでは、Azure Active Directory テナントに同期されている Azure ユーザ、連絡先、およびグループの情報を収集し、その情報を Reporting コンソールがレポート生成に使用するレポーティングデータベースに保存します。

Azure テナントコレクタを有効にするには、コレクタの実行場所となる DRA 管理サーバを指定する必要があります。

注 : Azure テナントによる収集は、対応するドメインの Active Directory コレクタが収集を正常に実行した後でのみ、正常に実行することができます。

管理レポートコレクタの設定

管理レポートコレクタは、DRA の監査情報を収集し、その情報をレポーティングコンソールがレポート生成に使用するレポーティングデータベースに保存します。コレクタを有効にすると、DRA のレポーティングツールで実行されるクエリ用のデータベースのデータ更新頻度を設定できます。

この設定をするには、DRA サービスのアカウントがレポーティングサーバに対し SQL サーバで **[sysadmin]** というパーミッションを持っている必要です。設定可能なオプションは、次のように定義されます。

- **監査エクスポートデータの時間間隔 :** これは、DRA のトレースログ (LAS) から監査データが SQL サーバ内の「SMCubeDepot」データベースにエクスポートされる時間間隔です。
- **管理レポート概要の時間間隔 :** これは、監査データが SMCubeDepot データベースから、DRA のレポーティングツールによるクエリが可能な DRA レポーティングデータベース内に、供給される時間間隔です。

直近ログオン統計の収集

管理対象ドメイン内のすべてのドメインコントローラから直近のログオン時の統計情報を収集するように、DRA を設定することができます。最終ログオン統計情報の収集の有効化とスケジュールを行うには、適切な権限 (Configure Servers and Domains ビルトイン役割に含まれる権限など) が必要です。

デフォルトでは、直近ログオン情報の収集機能は無効になっています。直近ログオン情報を収集するには、この機能を有効にする必要があります。直近ログオン情報の収集を有効にすると、特定ユーザの直近のログオン情報を表示したり、直近ログオン情報の収集状況を表示することができます。

直近ログオン統計を収集するには :

1 ［ **[Configuration Management]**］ > ［ **[Managed Domains (管理対象のドメイン)]**］の順に選択します。
2 目的のドメインを右クリックして、［ **[プロパティ]**］を選択します。
3 ［ **[Last logon schedule (直近ログオンスケジュール)]**］タブをクリックして、直近ログオン統計の収集を設定します。

ワークフロー自動化サーバの設定権限を委任する

ワークフローを管理するには、ワークフロー自動化サーバ管理の役割または次の該当する権限を管理者に割り当てます。

- ワークフローイベントを作成しすべてのプロパティを変更する
- Delete Workflow Automation Server Configuration (ワークフロー自動化サーバ設定の削除)
- Set Workflow Automation Server Configuration Information (ワークフロー自動化サーバの環境設定情報の設定)
- Start Workflow (ワークフローの開始)
- View All Workflow Event Properties (すべてのワークフローイベントのプロパティの表示)
- View All Workflow Properties (すべてのワークフロープロパティの表示)
- View Workflow Automation Server Configuration Information (ワークフロー自動化サーバの環境設定情報の表示)

ワークフロー自動化サーバの設定権限を委任するには、次のようにします。

1 Delegation Management ノードで ［ **[権限]**］をクリックし、オブジェクト検索機能を使用して目的のワークフロー権限を見つけ、それを選択します。
2 選択されているワークフロー権限のいずれかを右クリックして、［ **[Delegate Roles and Powers (役割と権限を委任)]**］を選択します。
3 権限の委任先となる特定のユーザ、グループ、またはアシスタント管理者グループを検索します。
4 **[オブジェクトセレクタ]** を使用して目的のオブジェクトを見つけて追加し、**[ウィザード]** で ［ **[Roles and Powers (役割と権限)]**］をクリックします。

5 [[ActiveViews]] をクリックし、[オブジェクトセレクタ] を使用して必要な ActiveView を見つけて追加します。

6 [[次へ]] をクリックしてから [[完了]] で委任プロセスを完了します。

ワークフロー自動化サーバの設定

DRA で Workflow Automation を使用するには、Windows サーバで Workflow Automation Engine をインストールしてから Delegation and Configuration console (委任および環境設定コンソール) を介して Workflow Automation サーバを構成する必要があります。

ワークフロー自動化サーバを設定するには、次のようにします。

1 Delegation and Configuration Console (委任および環境設定コンソール) にログインします。

ワークフロー自動化権限については、「ワークフロー自動化サーバの設定権限を委任する」を参照してください。

2 [[Configuration Management (環境設定管理)]] > [[Integration Servers (統合サーバ)]] を展開します。

3 [[ワークフローの自動化]] を右クリックし、[[新しいワークフロー自動化サーバ]] を選択します。

4 [[ワークフロー自動化サーバの追加]] ウィザードで、サーバ名、ポート、プロトコル、アクセスアカウントなどの詳細を指定します。

5 サーバへの接続をテストし、[[完了]] をクリックして設定を保存します。

Workflow Automation Engine のインストールの詳細については、『DRA マニュアルサイト』の「*Workflow Automation 管理者ガイド*」を参照してください。

LDAP 検索権限を委任する

DRA では、LDAP サーバからユーザ、連絡先、コンピュータ、グループ、および OU などのオンプレミスの Active Directory ドメインに含まれる LDAP オブジェクトを検索できます。DRA サーバは引き続き操作を処理し、検索が実行されるのはドメインコントローラです。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。また、検索クエリを保存して後で使用することもできます。検索クエリをパブリッククエリとして共有したり、プライベートとしてマークすることで自分で使用したりできます。保存されているクエリを編集できます。LDAP 詳細クエリ役割は、アシスタント管理者に、LDAP 検索クエリを作成および管理する権限を与えます。次に示す権限を使用して、LDAP 検索クエリの作成および管理を委任します。

- プライベートの詳細クエリを作成する
- パブリックの詳細クエリを作成する
- パブリックの詳細クエリを削除する
- 詳細クエリの実行
- 詳細クエリの保存の実行

- パブリッククエリの変更
- 詳細クエリの表示

LDAP クエリ権限を委任するには、次のようにします。

1. Delegation Management ノードで［[権限]］をクリックし、オブジェクト検索機能を使用して目的の詳細 LDAP クエリ権限を見つけ、それを選択します。
2. 選択されている LDAP 権限のいずれかを右クリックして、［[Delegate Roles and Powers (役割と権限を委任)]］を選択します。
3. 権限の委任先となる特定のユーザ、グループ、またはアシスタント管理者グループを検索します。
4. [オブジェクトセレクタ] を使用して目的のオブジェクトを見つけて追加し、[ウィザード] で［[Roles and Powers (役割と権限)]］をクリックします。
5. ［[ActiveViews]］をクリックし、[オブジェクトセレクタ] を使用して必要な ActiveView を見つけて追加します。
6. ［[次へ]］をクリックしてから［[完了]］で委任プロセスを完了します。

Web コンソールの検索機能にアクセスするには、［[管理] > ［LDAP 検索]］に移動します。

変更履歴レポーティングの設定

DRA は企業組織内の管理対象変更の委任を可能にし、Change Guardian(CG) は、Active Directory で発生した管理対象および管理されていない変更の監視を可能にします。DRA と CG を統合すると、次の機能が提供されます。

- DRA を介して行われた変更に対して、DRA から委任されたアシスタント管理者が、Active Directory に変更を加えたイベントを表示する機能。
- DRA で行われた変更と、DRA の外部で発生した SDRA によってキャプチャされた変更の両方について、DRA 内のオブジェクトの最近の変更履歴を表示する機能。
- DRA を介して行われた変更は、CG で「管理対象」の変更として指定されます。

DRA 変更履歴レポーティングを設定するには、次の手順に従います。

1. Change Guardian Windows エージェントのインストール。
2. Active Directory ライセンスキーの追加。
3. Active Directory の設定。
4. Active Directory ポリシーの作成と割り当て。
5. Active Directory ドメインの管理。
6. イベントスタンプを有効にする。
7. 統合された変更履歴サーバの設定。

Change Guardian をインストールし、DRA と CG 統合を設定する手順を完了すると、ユーザは Web コンソールで UCH レポートを生成および表示できます。

詳細については、『*Directory and Resource Administrator ユーザガイド*』の「「変更履歴レポートの生成」」を参照してください。

Change Guardian Windows エージェントのインストール

DRA と CG の統合を開始する前に、Change Guardian Windows エージェントをインストールします。詳細については、『*Change Guardian Installation and Administration Guide*』を参照してください。

Active Directory ライセンスキーの追加

Change Guardian サーバと、監視する予定のアプリケーションまたはモジュールの両方にライセンスを追加する必要があります。詳細については、『*Change Guardian Installation and Administration Guide*』を参照してください。

Active Directory の設定

Active Directory を変更履歴用に設定するには、次のセクションを参照してください。

セキュリティイベントログの設定

セキュリティイベントログを設定して、Change Guardian がイベントを処理するまで、Active Directory イベントがイベントログに残るようにします。

セキュリティイベントログを設定するには、次の手順を実行します。

1. 構成するドメイン内のコンピュータに管理者としてログインします。
2. グループポリシー管理コンソールを開く場合は、コマンドプロンプトで「gpmc.msc」と入力します。
3. [**[フォレスト]**]> [**[ドメイン]**] > [***[domainName]***] > [**[ドメインコントローラ]**] の順序で開きます。
4. [**[デフォルトのドメインコントローラポリシー]**] を右クリックし、[**[編集]**] をクリックします。

   注 : デフォルトのドメインコントローラポリシーを変更することは重要です。これは、リンク順序がより高いドメインコントローラ（DC）組織単位（OU）にリンクされた GPO が、コンピュータを再起動したり、gpUpdate を再度実行したりすると、この設定を上書きする可能性があるためです。企業標準の関係でデフォルトのドメインコントローラポリシーを変更できない場合は、Change Guardian 設定用の GPO を作成し、これらの設定を GPO に追加して、ドメインコントローラ OU 内で最も高いリンク順序を持つように設定をします。

5. [**[コンピュータの環境設定]**]> [**[ポリシー]**]> [**[Windows の設定]**]> [**[セキュリティの設定]**] を展開します。

6 [イベントログ] を選択し、次の項目を設定します。

- [最大セキュリティログサイズ] は 10240KB(10MB) 以上
- [必要に応じてイベントを上書きする]> [セキュリティログの保持方法]

7 ポリシー設定を更新するには、コマンドプロンプトで gpUpdate コマンドを実行します。

設定が正常に実行されたことを確認するには、次の手順を実行します。

1 コンピュータの管理者としてコマンドプロンプトを開きます。

2 イベントビューアの開始 : eventvwr

3 Windows のログで［ [セキュリティ]］を右クリックし、［ [プロパティ]］を選択します。

4 設定に 10240KB(10MB) 以上の最大ログサイズが表示され、[「必要に応じてイベントを上書きする」]］が選択されていることを確認します。.

AD 監査の設定

AD 監査を設定して、セキュリティイベントログへの AD イベントのログを有効にします。

監査ディレクトリサービスアクセスを使用してデフォルトのドメインコントローラポリシー GPO を設定し、成功イベントと失敗イベントの両方を監視します。

AD 監査を設定するには、次の手順を実行します。

1 構成するドメイン内のコンピュータに管理者としてログインします。

2 グループポリシー管理コンソールを開く場合は、コマンドプロンプトで gpmc.msc を実行します。

3 ［ [フォレスト]]> [［ドメイン]］ > ［ [*domainName*]］ > ［ [ドメインコントローラ]］を展開します。

4 ［ [デフォルトのドメインコントローラポリシー]］を右クリックし、［ [編集]］をクリックします。

注 : デフォルトのドメインコントローラポリシーを変更することは重要です。これは、リンク順序がより高いドメインコントローラ（DC）組織単位（OU）にリンクされた GPO が、コンピュータを再起動したり、gpUpdate を再度実行したりすると、この設定を上書きする可能性があるためです。企業標準の関係でデフォルトのドメインコントローラポリシーを変更できない場合は、Change Guardian 設定用の GPO を作成し、これらの設定を GPO に追加して、ドメインコントローラ OU 内で最も高いリンク順序を持つように設定をします。

---

5 [[コンピュータの環境設定]]> [[ポリシー]]> [[Windows 設定]]> [[セキュリティ設定]]> [[Advanced Audit Policy Configuration(高度な監査ポリシー環境設定)]]> [[監査ポリシー]] を展開します。

5a AD およびグループポリシーを設定するには、[[アカウント管理]] および [[ポリシーの変更]] で、各サブカテゴリに対して次の [[Configure the following audit events(次の監査イベントの設定)]]、[[成功]]、および [[失敗]] 項目を選択します。

5b AD のみを設定するには、[DS Access] の下で、各サブカテゴリに対して次の [[Configure the following audit events(次の監査イベントの設定)]]、[[成功]]、および [[失敗]] 項目を選択します。

6 [[コンピュータの環境設定]]> [[ポリシー]]> [[Windows 設定]]> [[セキュリティ設定]]> [[ローカルポリシー]]> [[監査ポリシー]] を展開します。

6a 次の各ポリシーについて、[[セキュリティポリシー設定]] タブで、[[これらのポリシー設定を定義する]]、[[成功]]、および [[失敗]] を選択します。

- [監査アカウント管理]
- [監査ディレクトリサービスアクセス]
- [監査ポリシーの変更]

7 ポリシー設定を更新するには、コマンドプロンプトで gpUpdate コマンドを実行します。

詳細については、Microsoft マニュアルサイトの「*Active Directory の侵害の兆候を監視する*」を参照してください。

ユーザおよびグループ監査の設定

ユーザおよびグループの監査を設定して、次のアクティビティを監査します。

- ローカルユーザおよびActive Directoryユーザのログオンおよびログオフアクティビティ
- ローカルユーザ設定
- ローカルグループの設定

ユーザおよびグループの監査を設定するには、次の手順を実行します。

1 構成するドメイン内のコンピュータに管理者としてログインします。

2 Microsoft 管理コンソールを開き、[[ファイル]]> [[Add/Remove Snap-in(スナップインの追加 / 削除)]] を選択します。

3 [[グループポリシーの管理エディタ]] を選択し、[[追加]] をクリックします。

4 [Select Group Policy Object(グループポリシーオブジェクトの選択)] ウィンドウで、[[参照]] をクリックします。

5 [[Domain Controllers.*FQDN*] を選択します。ここで *FQDN* はドメインコントローラコンピュータの完全修飾ドメイン名です。

6 [[デフォルトドメインコントローラポリシー]] を選択します。

7 Microsoft 管理コンソールで、[[デフォルトドメインコントローラポリシー *FQDN*]]> [[コンピュータの環境設定]]> [[ポリシー]]> [[Windows 設定]]> [[セキュリティ設定]]> [[ローカルポリシー]]> [[監査ポリシー]] を展開します。

8 [[Audit Account Logon Events(アカウントログオンイベントの監査)]] および [[Audit Logon Events(ログオンイベントの監査)]] の下で、[[Define these policy setting(これらのポリシー設定を定義する)]]、[[成功]]、および [[失敗]] を選択します。

9 Microsoft 管理コンソールで、[[デフォルトドメインコントローラポリシー *FQDN*] > [コンピュータの環境設定] > [ポリシー] > [Windows 設定] > [セキュリティ設定] > [Advanced Audit Policy Configuration(高度な監査ポリシー環境設定)] > [監査ポリシー] > [ログオン / ログオフ]] を展開します。

10 [[ログオンの監査]] の下で、[[ログオンの監査]]、[[成功]]、および [[失敗]] を選択します。

11 [[ログオフの監査]] の下で、[[監査ログオフ]]、[[成功]]、および [[失敗]] を選択します。

12 ポリシー設定を更新するには、コマンドプロンプトで gpupdate/force コマンドを実行します。.

セキュリティアクセス制御リストの設定

Active Directory 内の現在のオブジェクトと今後のオブジェクトのすべての変更を監視するには、ドメインノードを設定します。

SACL を設定するには、次の手順を実行します。

1 構成するドメイン内のコンピュータに管理者としてログインします。

2 ADSI Edit 設定ツールを開く場合は、コマンドプロンプトで adsiedit.msc を実行します。

3 [ADSI Edit] を右クリックし、[[Connect to(接続先)]] を選択します。

4 [Connection Settings(接続設定)] ウィンドウで、次の内容を指定します。

- [名前] を Default naming context(デフォルトの名前付けコンテキスト) として名前付けする。
- 設定するドメインへの [パス]。
- この手順を初めて実行する場合は、[[Default naming context(デフォルトの名前付けコンテキスト)]] を選択します。
- 2 回目の実行を行う場合は、[[スキーマ]] を選択します。
- 3 回目の実行を行う場合は、[[設定]] を選択します。

注 : [Default naming context(デフォルトの名前付けコンテキスト)]、[スキーマ]、および [設定] の接続ポイントを設定するには、手順 4 からステップ 11 を 3 回実行する必要があります。

---

5 [[接続ポイント]] で、[[Select a well known Naming Context(よく知られているネーミングコンテキストを選択する)]] を [[Default naming context(デフォルトの名前付けコンテキスト)]] に設定します。

6 ADSI Edit ウィンドウで、[[Default naming context(デフォルトの名前付けコンテキスト)]] を展開します。

7 (DC= または CN= で始まる) 接続ポイントの下のノードを右クリックし、[[プロパティ]] をクリックします。

8 [[セキュリティ]] タブで、[[詳細]> [[監査]> [[追加]] をクリックします。

9 [[Applies to(適用対象)]] または [[Apply onto(適用先)]] で、[[This object and all descendant objects(このオブジェクトおよびすべての子孫オブジェクト)]] を選択します。

10 すべてのユーザを監視する監査を設定します。

10a [[Select a principal(プリンシパルの選択)]] をクリックし、[[Enter the object name to select(選択するオブジェクト名を入力)]] に「全員」と入力します。

10b 次のオプションを指定します。

- [[入力]] を [[すべて]]
- 次のように [[許可]] を選択します。
  - [すべてのプロパティを書き込む]
  - [削除]
  - [許可の変更]
  - [所有者の変更]
  - [すべての子オブジェクトの作成]

    子オブジェクトに関連するその他のノードは自動的に選択されます
  - [すべての子オブジェクトの削除]

    子オブジェクトに関連するその他のノードは自動的に選択されます

11 [[Apply these auditing entries to objects and/or containers within this container only(これらの監査エントリをこのコンテナ内のオブジェクトおよび / またはコンテナにのみ適用する)]] オプションを選択解除します。

12 手順 4 からステップ 11 をあと 2 回繰り返します。

Active Directory ポリシーの作成と割り当て

事前設定なしで新規ポリシーを作成できます。

ポリシーを作成するには、次を実行します。

1 ポリシーエディタで、Active Directory などのアプリケーションの 1 つを選択します。

2 ポリシーのリストを展開し、作成するポリシータイプを選択します。たとえば、[[Active Directory ポリシー]]> [[AD オブジェクト]] を選択します。

3 [構成ポリシー] 画面で、適切な変更を行います。

4 (条件付き) ポリシーをすぐに有効にする場合は、[[Enable this policy revision now(このポリシーリビジョンを今すぐ有効にする)]] を選択します。.

割り当てるには :

1. [[設定]]> [[ポリシー]]> [[ポリシーの割り当て]] をクリックします。
2. (条件付き) エージェントグループに割り当てるには、[[エージェントグループ]] と [[デフォルトグループ]] または [[カスタムグループ]] をクリックし、グループ名をクリックします。
3. (条件付き) エージェントに割り当てるには、[[エージェント]] をクリックしてエージェント名を選択します。
4. [[割り当て / 割り当て解除]] の下にあるアイコンをクリックします。
5. [[ポリシーセット]]、[[ポリシー]]、またはその両方からポリシーを選択し、[[適用]] をクリックします。

注 : Azure AD、AWS for IAM、Dell EMC、Microsoft Exchange、Microsoft Office 365 のアセットタイプでは、エージェントグループを使用してポリシーを割り当てすることはできません。

Active Directory ドメインの管理

DRA 内のドメインを管理対象ドメインとして設定するには、「Active Directory ドメインの管理」を参照してください。

DRA でイベントスタンプを有効にする

AD のドメインサービスの監査を有効にすると、DRA のサービスアカウントまたはドメインアクセスアカウントが設定されていれば、そのいずれかによってイベントが発生したときに、DRA イベントが記録されます。この機能を応用したのがイベントスタンプです。イベントスタンプでは、AD のドメインサービスイベントを追加で生成し、それによってその操作を実行したアシスタント管理者を特定します。

このようなイベントを発生させるには、AD のドメインサービス監査を設定し、DRA の管理サーバでイベントスタンプを有効にしておく必要があります。イベントスタンプが有効になると、アシスタント管理者が加えた変更が Change Guardian イベントのレポート内に表示されます。

- AD DS の監査を設定するには、Microsoft マニュアルの『*AD DS Auditing Step-by-Step Guide (AD DS 監査のステップバイステップガイド)*』を参照してください。
- Change Guardian の統合を設定するには、「統合された変更履歴サーバの構成」を参照してください。
- イベントスタンプを有効にするには、DRA 管理者として Delegation and Configuration console (委任および環境設定コンソール) を開き、次の操作を行ってください。
  1. [[環境設定管理]] > [[Update Administration Server Options (管理サーバオプションを更新)]] > [[Event Stamping (イベントスタンプ)]] の順に選択します。
  2. オブジェクトタイプを選択し、[[更新]] をクリックします。
  3. そのオブジェクトタイプでイベントスタンプに使用する属性を選択します。

DRA は現段階でユーザ、グループ、連絡先、コンピュータ、および部門のイベントスタンプをサポートしています。

また、使用する管理対象ドメインのそれぞれで属性が AD スキーマ内に存在していることも、DRA の必須要件です。イベントスタンプを設定した後に管理対象ドメインを追加する場合は、この点に注意する必要があります。選択した属性が含まれていない管理対象ドメインを追加してしまった場合、そのドメインからの操作の監査でイベントスタンプのデータが使用されません。

これらの属性は DRA によって変更されるため、DRA にも環境内のどのアプリケーションにも使用されていない属性を選択する必要があります。

イベントスタンプの詳細については、「イベントスタンプの仕組み」を参照してください。

統合された変更履歴サーバの設定

統合された変更履歴 (UCH) サーバ機能を使用すると、DRA の外部で行った変更についてのレポートを生成することができます。

統合された変更履歴サーバの設定権限を委任する

統合された変更履歴サーバを管理するには、Unified Change History Server Administration(統合された変更履歴サーバ管理) という役割、または次に示す権限のうち該当するものをアシスタント管理者を割り当ててください。

- 統合された変更履歴の設定を削除する
- 統合された変更履歴の情報を設定する
- 統合された変更履歴の設定情報を表示する

統合された変更履歴サーバの権限を委任するには、次のようにします。

1. Delegation Management ノードで［ **[権限]**］をクリックし、オブジェクト検索機能を使用して目的の UCH 権限を見つけ、それを選択します。
2. 選択されている UCH 権限のいずれかを右クリックして、［ **[Delegate Roles and Powers (役割と権限を委任)]**］を選択します。
3. 権限の委任先となる特定のユーザ、グループ、またはアシスタント管理者グループを検索します。
4. **[オブジェクトセレクタ]** を使用して目的のオブジェクトを見つけて追加し、**[ウィザード]** で［ **[Roles and Powers (役割と権限)]**］をクリックします。
5. ［ **[ActiveViews]**］をクリックし、**[オブジェクトセレクタ]** を使用して必要な ActiveView を見つけて追加します。
6. ［ **[次へ]**］をクリックしてから［ **[完了]**］で委任プロセスを完了します。

統合された変更履歴サーバの構成

統合された変更履歴サーバを設定するには、次のようにします。

1. Delegation and Configuration Console (委任および環境設定コンソール) にログインします。
2. [[Configuration Management (環境設定管理)]] > [[Integration Servers (統合サーバ)]] を展開します。
3. [[統合された変更履歴]] を右クリックし、[[新しい統合された変更履歴サーバ]] を選択します。
4. 変更履歴の統合の設定で、UCH サーバ名または IP アドレス、ポート番号、サーバタイプ、アクセス用アカウントの詳細を指定します。
5. サーバへの接続をテストし、[[完了]] をクリックして設定を保存します。
6. 必要に応じてサーバを追加します。

統合された変更履歴レポートへのアクセス

Change Guardian を介して、Active Directory オブジェクトに関する統合された変更履歴レポートを生成および表示するには、『*Directory and Resource Administrator ユーザガイド*』の「「変更履歴レポートの生成」」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 DRA サービスの設定

必要に応じて、DRA サービスに対してグループ管理対象サービスアカウント (gMSA) を使用することができます。gMSA の使用方法の詳細については、Microsoft リファレンス「*グループ管理対象サービスアカウントの概要*」を参照してください。このセクションでは、Active Directory にアカウントを追加した後に gMSA の DRA を設定する方法について説明します。

重要 : DRA のインストール中は、gMSA をサービスアカウントとして使用しないでください。

DRA プライマリ管理サーバを gMSA に設定するには、次のようにします。

1. 次のグループのメンバーとして gMSA を追加します。
   - DRA サーバ上の Local Administrators (ローカル管理者) グループ
   - DRA 管理ドメイン内の AD LDS グループ
2. 次の各サービスのサービスプロパティでログオンアカウントを gMSA に変更します。
   - NetIQ 管理サービス
   - NetIQ DRA 監査サービス
   - NetIQ DRA キャッシュサービス
   - NetIQ DRA コアサービス

- NetIQ DRA ログアーカイブ
- NetIQ DRA レプリケーションサービス
- NetIQ DRA Rest サービス
- NetIQ DRA Skype サービス

3 すべてのサービスを再起動します。

4 次のコマンドを実行して、「すべてのオブジェクトの監査」役割を gMSA に委任します。

```
Add-DRAAssignments -Identifier "All Objects" -Users "CN=<gMSA_name>,
CN=Managed Service Accounts, DC=MyDomain, DC=corp" -Roles "Audit All
Objects"
```

gMSA の DRA セカンダリ管理サーバを設定するには、次のようにします。

1 セカンダリサーバをインストールします。

2 プライマリサーバで、セカンダリサーバのサービスアカウントの［ **[Administration Servers and Managed Domains (管理サーバと管理対象ドメイン)]**］の ActiveView に［ **[Configure Servers and Domains]**］役割を割り当てます。

3 プライマリサーバで、新しいセカンダリサーバを追加し、セカンダリサーバサービスアカウントを指定します。

4 DRA セカンダリ管理サーバのローカル管理者グループに gMSA を追加します。

5 セカンダリサーバで、すべての DRA サービスのログオンアカウントを gMSA に変更してから、DRA サービスを再起動します。

Delegation and Configuration のクライアントを設定する

Delegation and Configuration のクライアントは、構成タスクや委任タスクへのアクセスを提供し、分散型管理からポリシーの強制まで企業の管理ニーズに対応します。Delegation and Configuration Console (委任および環境設定コンソール) から、企業の効果的な管理に必要なセキュリティモデルとサーバ構成を設定できます。

Delegation and Configuration のクライアントを設定するには :

1 Delegation and Configuration のクライアントを起動するには、［ **[Configuration Management]**］>［ **[Update Administration Server Options (管理サーバオプションを更新)]**］の順に選択します。

2 ［ **[Client Options (クライアントオプション)]**］タブをクリックして、表示される設定オプションの中から所望の設定を定義します。

- ユーザに ActiveView での検索を許可する
- コンソールのリストからソース専用のオブジェクトの非表示にする
- 高度な Active Directory オブジェクトを表示する
- セキュリティコマンドを表示する

- ユーザの検索時にリソースと共有メールボックスを表示する
- 現在のドメインへのデフォルトのユーザ UPN サフィックス
- 一度に編集可能な最大項目数 (複数選択)
- 検索オプション
- キャリッジリターンのオプション
- Exchange メールボックスのストレージ制限の単位

Web クライアントの設定

Web コンソールをスマートカードまたは多要素認証を使用して認証するように設定したり、独自のロゴやアプリケーションタイトルを使ったブランディングでカスタマイズしたりすることもできます。

- 118 ページの 「Web コンソールの起動」
- 118 ページの 「自動ログアウト」
- 118 ページの 「DRA サーバへの接続」
- 119 ページの 「認証」

Web コンソールの起動

Web コンソールは、Web ブラウザを実行していれば、どのコンピュータからでも、iOS や Android のデバイスからでも起動できます。コンソールを起動するには、適切な URL を Web ブラウザのアドレスフィールドに指定してください。たとえば、Web コンポーネントを HOUserver というコンピュータにインストールした場合は、Web ブラウザのアドレスフィールドに https://HOUserver/draclient とタイプ入力します。

注 : アカウントと Microsoft Exchange に関する最新の情報を Web コンソールに表示するには、キャッシュされているページにそれより新しいバージョンがある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。

自動ログアウト

何もせずに時間が経過したら Web コンソールを自動的にログアウトするように時間を設定することができます。また、自動ログアウトしないように設定することもできます。

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]**] > [**[自動ログアウト]**] の順に選択します。

DRA サーバへの接続

次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 コンソールで DRA サーバの接続を設定するには、［**[管理]**］>［**[構成]**］>［**[DRA サーバ接続]**］の順に選択します。

認証

このセクションには、Advanced Authentication の統合を使用してスマートカード認証、Windows 認証、および多要素認証を設定するための情報が記載されています。

- 119 ページの 「スマートカード認証」
- 121 ページの 「Windows 認証」
- 122 ページの 「Advanced Authentication による多要素認証」

スマートカード認証

スマートカードからのクライアント資格情報に基づいてユーザを受け入れるように Web コンソールを設定するには、IIS (Internet Information Services) および REST サービスの設定ファイルを設定する必要があります。

重要 : スマートカード上の証明書が Web サーバ上のルートの証明書ストアにもインストールされているか確認してください。IIS がカードの証明書と一致する証明書を参照する必要があるためです。

1 Web サーバで認証コンポーネントをインストールします。

1a サーバマネージャを起動します。

1b ［**[Web サーバ (IIS)]**］をクリックします。

1c［Role Services (役割サービス)］セクションに移動し、［ [Add Role Services (役割サービスを追加)]］をクリックします。

1d Security という役割サービスのノードに移動し、［ [Windows Authentication (Windows 認証)]］>［ [Client Certificate Mapping Authentication (クライアント証明書割り付け認証)]］の順に選択します。

2 Web サーバで認証を有効にします。

2a [IIS Manager] を起動します。

2b ご使用の Web サーバを選択します。

2c IIS セクションの下にある [認証] アイコンを見つけて、それをダブルクリックします。

2d「Active Directory クライアント証明書認証」と「Windows 認証」を有効にします。

3 DRA クライアントを設定します。

3a ご使用の DRA クライアントを選択します。

3b IIS セクションの下にある [認証] アイコンを見つけて、それをダブルクリックします。

3c「Windows 認証」を有効にし、「匿名認証」を無効にします。

4 DRA クライアントに対し SSL 証明書およびクライアント証明書を有効にします。

4a IIS セクションの下の [SSL サービス] のアイコンを見つけて、それをダブルクリックします。

4b［ [Require SSL (SSL を要求)]］を選択し、クライアント証明書の下の［ [Require (要求する)]］を選択します。

ヒント : このオプションが使用可能な場合、［ [Require 128-bit SSL (128 ビット SSL を要求)]］を選択します。

---

5 REST サービスの Web アプリケーションを設定します。

5a REST サービスの Web アプリケーションを選択します。

5b IIS セクションの下にある [認証] アイコンを見つけて、それをダブルクリックします。

5c「Windows 認証」を有効にし、「匿名認証」を無効にします。

6 REST サービスの Web アプリケーション上で SSL 証明書およびクライアント証明書を有効にします。

6a IIS セクションの下の [SSL サービス] のアイコンを見つけて、それをダブルクリックします。

6b［ [Require SSL (SSL を要求)]］を選択し、クライアント証明書の下の［ [Require (要求する)]］を選択します。

ヒント : このオプションが使用可能な場合、［ [Require 128-bit SSL (128 ビット SSL を要求)]］を選択します。

---

7 WCF の Web サービスのファイルを設定します。

7a REST サービスの Web アプリケーションを選択し、Content View に切り替えます。

7b .svc ファイルを見つけて、それを右クリックします。

7c [**[Switch to Features View (フィーチャービューに切り替える)]**] を選択します。

7d IIS セクションの下にある **[認証]** アイコンを見つけて、それをダブルクリックします。

7e「匿名認証」を有効にし、その他の認証メソッドをすべて無効にします。

8 REST サービスの設定ファイルを編集します。

8a C:\inetpub\wwwroot\DRAClient\rest\web.config というファイルをテキストエディタで開きます。

8b その中の <authentication mode="None" /> という行を見つけて、その行を削除します。

8c 以下に指定されている行のコメントを外します。

- <system.serviceModel> 行の下 :

```
<services> <service name="NetIQ.DRA.DRARestProxy.RestProxy">
<endpoint address="" binding="webHttpBinding"
bindingConfiguration="webHttpEndpointBinding"
name="webHttpEndpoint"
contract="NetIQ.DRA.DRARestProxy.IRestProxy" /> </service> </
services>
```

- <serviceDebug includeExceptionDetailInFaults="false"/> 行の下 :

```
<serviceAuthorization impersonateCallerForAllOperations="true" /
> <serviceCredentials> <clientCertificate> <authentication
mapClientCertificateToWindowsAccount="true" /> </
clientCertificate> </serviceCredentials>
```

- <serviceHostingEnvironment multipleSiteBindingsEnabled="true" /> 行の上 :

```
<bindings> <webHttpBinding> <binding
name="webHttpEndpointBinding"> <security mode="Transport">
<transport clientCredentialType="Certificate" /> </security> </
binding> </webHttpBinding> </bindings>
```

9 ファイルを保存して、IIS サーバを再起動します。

Windows 認証

Web コンソールで Windows 認証を有効にするには、IIS (Internet Information Services) と REST サービスの設定ファイルを設定する必要があります。

1 IIS Manager を開きます。

2 [接続] ペインで、REST サービスの Web アプリケーションを見つけて、それを選択します。

3 右側のペインで、IIS セクションに移動し、[**[認証]**] をダブルクリックします。

4 **[Windows 認証]** を有効にし、その他の認証メソッドをすべて無効にします。

5 Windows 認証を有効にすると、マネージャウィンドウの右側にある右クリックメニューと［アクション］パネルに［[プロバイダ]］オプションが追加されます。［プロバイダ］ダイアログボックスを開き、[NTLM] をリストの一番上に移動します。

6 C:\inetpub\wwwroot\DRAClient\rest\web.config というファイルをテキストエディタで開き、<authentication mode="None" /> という行を探します。

7 値の "None" を "Windows" に変更し、ファイルを保存します。

8 IIS サーバを再起動します。

Advanced Authentication による多要素認証

AAF (Advanced Authentication Framework) は、単純なユーザ名とパスワードから、より安全に機密情報を保護できる多要素認証方式へと移行できるようにする、弊社のプレミアソフトウェアパッケージです。

Advanced Authentication では、セキュリティ向上のために次に示す通信プロトコルをサポートしています。

- TLS 1.2 (デフォルト設定)、TLS 1.1、TLS 1.0
- SSL 3.0

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制御の 1 方式です。

次に示すように、認証には 3 種類のカテゴリ (要素) があります。

- *知識 :* このカテゴリでは、パスワードまたはアクティベーションコードなど、特定の情報を知っている必要があります。
- *所有物 :* このカテゴリでは、スマートカードまたはスマートフォンなど、認証デバイスを用意する必要があります。
- *身体 :* このカテゴリでは、指紋など、体の一部を検証手段として使用することが必要です。

各認証要素には、少なくとも 1 つの認証メソッドが含まれています。認証メソッドとはユーザの識別に使用できる特定の技法であり、指紋を使用したりパスワードを要求するといった手法があります。

たとえば、パスワードとともに指紋を要求する場合のように、2 つ以上の認証メソッドを使用すると、認証プロセスが強いとみなすことができます。

Advanced Authentication でサポートされるのは、次に示す認証メソッドです。

- LDAP パスワード
- RADIUS (Remote Authentication Dial-In User Service)
- スマートフォン

ヒント : スマートフォンメソッドでは、ユーザが iOS または Android のアプリをダウンロードする必要があります。詳細については、『*Advanced Authentication - Smartphone Applications User Guide*』を参照してください。このガイドは、NetIQ のマニュアル Web サイトから入手できます。

以降のセクションの情報を使用して、多要素認証が使用できるように Web コンソールを設定してください。

重要 : 次のセクションの手順には、Web コンソール内部で行われるものもありますが、多要素認証の環境設定プロセスの多くで AAF へのアクセスが必要です。これらの手順では、AAF がすでにインストール済みで、AAF のヘルプマニュアルにアクセスできるユーザを対象にしています。

Advanced Authentication Framework へのリポジトリの追加

最初のステップは、DRA 管理者および DRA で管理されるアシスタント管理者を含んでいる Active Directory ドメインのすべてを、多要素認証を使って AAF に追加できるように Web コンソールを設定することです。これらのドメインはリポジトリと呼ばれ、認証対象のユーザおよびグループの ID 属性が含まれています。

1 管理者レベルのユーザ名とパスワードを使って AAF の管理ポータルにログインします。
2 左側のパネルに移動し、[**[リポジトリ]**] をクリックします。
3 [**[追加]**] をクリックします。
4 フォームを記入します。

ヒント : **[LDAP タイプ]** は **[AD]** です。

ヒント : 対応するフィールドに管理者レベルのユーザ名とパスワードを入力します。

5 [**[サーバを追加]**] をクリックします。
6 LDAP サーバの IP アドレスを [**[アドレス]**] フィールドに入力します。
7 [**[保存]**] をクリックします。
8 DRA によって管理される他のすべての AD リポジトリにも、手順 3 から 7 を繰り返し実行してください。
9 [リポジトリ] ページに表示されている各リポジトリに対し、[**[Sync now (今すぐ同期化)]**] をクリックして AAF サーバと同期化します。

認証チェーンの作成

認証チェーンには、少なくとも 1 つの認証メソッドが含まれています。チェーンに追加された順序で、チェーン内のメソッドが呼び出されます。ユーザが認証されるためには、ユーザがチェーン内のすべてのメソッドを渡す必要があります。たとえば、LDAP パスワードメソッドと SMS メソッドを含むチェーンが作成されているとしましょう。この場合、ユーザがこのチェーンを使用して認証を試みたときに、このユーザはまず自分の LDAP パ

スワードを使用して認証する必要があります。そしてパスワード認証に続いて、1 回限り使用可能なパスワードが記載されたテキストメッセージがそのユーザの携帯電話に送信されます。このユーザがそのパスワードを入力したら、チェーン内のすべてのメソッドが履行されたことになり、認証が成功します。認証チェーンは、特定のユーザまたはグループに割り当てることができます。

認証チェーンを作成するには :

1 管理者レベルのユーザ名とパスワードを使って AAF の管理ポータルにログインします。
2 左側のパネルに移動し、[**[チェーン]**] をクリックします。右側のパネルに現在使用可能なチェーンがリスト表示されます。
3 [**[追加]**] をクリックします。
4 フォームを記入します。すべてのフィールドが必須です。

重要 : メソッドは、実動作で呼び出されるべき順序で追加してください。つまり、最初にユーザに LDAP パスワードを入力させたい場合は、最初に LDAP パスワードをチェーンに追加します。

重要 : [**[Apply if used by endpoint owner (エンドポイント所有者が使用する場合に適用)]**] がオフになっていることを確認します。

---

5 [**[Is enabled (有効)]**] をオンにします。
6 [**[役割とグループ]**] フィールドに、認証リクエストの対象となる役割またはグループの名前を入力します。

ヒント : チェーンをすべてのユーザタイプに適用したい場合は、[役割とグループ] フィールドに 「 **[all users]**」と入力し、ドロップダウンリストから [**[すべてのユーザ]**] を選択します。

選択したユーザまたはグループが [**[Roles & Groups (役割とグループ)]**] フィールドの下に追加されます。

7 [**[保存]**] をクリックします。

認証イベントの作成

認証イベントは、ユーザ認証を行うアプリケーション (この場合は Web コンソール) がトリガとなって開始します。そのイベントに少なくとも 1 つの認証チェーンが割り当てられる必要があります。そうすることで、イベントの発生時にそのイベントに関連付けられたチェーン内のメソッドがユーザ認証するために呼び出されます。

エンドポイントとは、コンピュータやスマートフォンのような、認証イベントのトリガとなるソフトウェアを実行している実際のデバイスです。DRA はイベント作成後に AAF でエンドポイントを登録します。

エンドポイントのホワイトリストボックスを使用すると、イベントへのアクセスを特定のエンドポイントに制限することができます。また、イベントへのアクセスをすべてのエンドポイントに許可することもできます。

認証イベントを作成するには :

1 管理者レベルのユーザ名とパスワードを使って AAF の管理ポータルにログインします。
2 左側のパネルに移動し、[**[イベント]**] をクリックします。右側のパネルに、現在使用可能なイベントのリストが表示されます。
3 [**[追加]**] をクリックします。
4 フォームを記入します。すべてのフィールドが必須です。

重要 : [**[Is enabled (有効)]**] というスイッチが ON になっていいることを確認します。

---

5 特定のエンドポイントにアクセスを制限する場合は、エンドポイントのホワイトリストセクションに移動し、対象となるエンドポイントを［*Available (使用可能)*］リストから［*Used (使用済み)* ］リストに移動させます。

ヒント : [*Used (使用済み)*] リストにエンドポイントがない場合、そのイベントはすべてのエンドポイントで使用可能になります。

Web コンソールの有効化

チェーンとイベントの設定後、Web コンソールに管理者でログインし、Advanced Authentication を有効にできます。

認証が有効になると、すべてのユーザが Web コンソールへのアクセス権を得る前に AAF で認証を行う必要があります。

重要 : Web コンソールを有効にする前に、Web コンソールがユーザ認証に使用する認証メソッドに登録済みである必要があります。認証メソッドへの登録方法については、『*Advanced Authentication Framework User Guide*』を参照してください。

Advanced Authentication を有効にするには、Web コンソールにログインし［**[管理]**］> ［**[設定]**］> ［**[Advanced Authentication]**］の順に選択します。［**[有効]**］チェックボックスを選択し、各フィールドの指示に従ってフォームを記入します。

ヒント : 設定を保存した後に、エンドポイントが AAF に作成されます。表示または編集するには、管理者レベルのユーザ名とパスワードで AAF 管理ポータルにログオンし、左側のペインの［**[エンドポイント]**］をクリックします。

最後のステップ

1 管理者レベルのユーザ名とパスワードで AAF 管理ポータルにログオンし、左側のペインの［[イベント]］をクリックします。

2 Web コンソールのイベントをそれぞれ編集します。

2a 編集するイベントを開きます。

2b ［エンドポイント］ホワイトリストのセクションに移動し、Web コンソールを設定したときに作成したエンドポイントを［[Available (使用可能)]］リストから［[Used (使用済み)]］リストに移動します。これにより、Web コンソールのみがこれらのイベントを使用できるようになります。

3 ［[保存]］をクリックします。

12 管理対象システムの接続

このセクションでは、パブリックフォルダ、Exchange、Office 365、Skype for Business Online を含む Microsoft Exchange コンポーネントや、ドメインに関係する管理対象システムの接続と設定について説明します。

Active Directory ドメインの管理

管理サーバのインストール後に Delegation and Configuration のクライアントを介し新しい管理対象ドメインおよびコンピュータを追加できます。信頼されたドメインとサブツリーを追加し、それらのドメインと Exchange アクセスアカウントを設定することもできます。管理対象ドメインおよびコンピュータを追加するには、Configure Servers and Domains という組み込みの役割に含まれる権限など、適切な権限が必要です。

注 : 管理対象ドメインの追加が完了した後、それらのドメインのアカウントキャッシュ更新のスケジュールが正しいことを確認してください。

管理対象ドメインおよびコンピュータを追加する

管理対象ドメインまたはコンピュータを追加するには :

1 [[環境設定管理]] > [[New Managed Domain (新しい管理対象ドメイン)]] に移動します。

2 追加するコンポーネントを指定するには、該当するラジオボタンを選択して、ドメイン名またはコンピュータ名を指定します。

- [ドメインの管理]
  - ドメインのサブツリーを管理する場合は、「管理対象サブツリーの追加」を参照してください。
  - セキュリティ保護された LDAP を有効にした新しいドメインをドメインコントローラで追加し、DRA が SSL を使用してドメインコントローラと通信するようにしたい場合は、[[This domain is configured for LDAP over SSL (このドメインは SSL 経由の LDAP 用に構成されています)]] を選択します。詳細については、「セキュリティ保護された Active Directory を実行するための DRA の設定」を参照してください。
- [コンピュータを管理する]

設定が完了したら、[[次へ]] をクリックします。

3 [[Domain access (ドメインアクセス)]] タブで、このドメインまたはコンピュータにアクセスするために DRA が使用するアカウント資格情報を指定します。デフォルトでは、DRA が管理サーバのサービスアカウントを使用します。

4 サマリの内容を確認し [[完了]] をクリックします。

5 このドメインまたはコンピュータにあるオブジェクトの管理を開始するために、ドメイン構成を更新します。

ドメインアクセスアカウントの指定

管理対象ドメインまたは管理対象サブツリーのそれぞれに、管理サーバのサービスアカウントの代わりに使うそのドメインへのアクセス用のアカウントを指定できます。この代替アカウントを「アクセスアカウント」と呼びます。アクセスアカウントを設定するには、Configure Servers and Domains という組み込みの役割に含まれる権限など、適切な権限が必要です。

メンバーサーバに対しアクセスアカウントを指定するには、ドメインメンバーが存在するドメインを管理するためのパーミッションが必要です。管理サーバからアクセスできる管理対象ドメインの中にドメインメンバーが存在する場合、管理できるのはドメインメンバーのみです。

アクセスアカウントを指定するには :

1 [[Configuration Management]] > [[Managed Domains (管理対象ドメイン)]] ノードの順に選択します。

2 アクセス アカウントを指定する必要のあるドメインまたはサブツリーを右クリックし、[[プロパティ]] を右クリックします。

3 [Domain access account (ドメインアクセスのアカウント)] タブで [[Use the following account to access this domain (このドメインへのアクセスに次のアカウントを使用)]] をクリックします。

4 このアカウントの資格情報を指定および確認し、[[OK]] をクリックします。

この最小特権アカウントの設定について詳細は、「最小特権 DRA アクセスアカウント」を参照してください。

Exchange のアクセスアカウントの指定

DRA の各ドメインに対し、DRA のドメインアクセスアカウントまたは別の Exchange アクセスアカウントを使用して Exchange オブジェクトを管理できます。Exchange のアクセスアカウントを設定するには、Configure Servers and Domains という組み込みの役割に含まれている権限など、適切な権限が必要です。

重要 : Microsoft Server では、WinRM/WinRS のセッションに同時に接続できるユーザ数を 5 に、ユーザごとのシェル数を 5 に制限しています。このため、同じユーザアカウントが DRA のセカンダリサーバで 5 シェルに限定されるようにしてください。

Exchange のアクセスアカウントを指定するには :

1. ［**[Configuration Management]**］>［**[Managed Domains (管理対象ドメイン)]**］ノードの順に選択します。
2. アクセス アカウントを指定する必要のあるドメインまたはサブツリーを右クリックし、［**[プロパティ]**］を右クリックします。
3. ［Exchange access account (Exchange のアクセスアカウント)］タブで［**[Use the following account to access all Exchange servers (すべての Exchange サーバへのアクセスに次のアカウントを使用)]**］をクリックします。
4. このアカウントの資格情報を指定および確認し、［**[OK]**］をクリックします。

この最小特権アカウントの設定について詳細は、「最小特権 DRA アクセスアカウント」を参照してください。

管理対象サブツリーの追加

管理サーバをインストールした後、管理対象サブツリーおよび欠けているサブツリーを特定の Microsoft Windows ドメインから追加することができます。管理対象サブツリーを追加するには、Configure Servers and Domains という組み込みの役割に含まれている権限など、適切な権限が必要です。

Microsoft Windows のサポート対象バージョンについては、「DRA 管理サーバおよび Web コンソールの要件」を参照してください。

Windows のドメインのサブツリーを管理することにより、DRA を使って大規模な企業ドメイン内の部門のセキュリティを確保できます。

たとえば、SOUTHWEST ドメイン内の Houston サブツリーを指定して、ヒューストン OU とその子 OU に属しているオブジェクトだけを安全に管理することができます。この柔軟性により、ドメイン全体に対する管理権限がなくても、1 つまたは複数のサブツリーを管理することが可能になります。

注

- 指定したアカウントがこのサブツリーの管理とアカウントキャッシュの増分更新の実行ができるパーミッションを持っているかどうか確認するには、削除オブジェクトというユーティリティを使用してください。このユーティリティで、適切なパーミッションをチェックおよび委任することができます。
- 管理対象サブツリーの追加が完了した後、対応するドメインのアカウントキャッシュ更新のスケジュールが正しいことを確認してください。

管理対象サブツリーを追加するには、以下の手順を実行します。

1. [[Configuration Management]] > [[New Manage Domain (新しい管理対象ドメイン)]] の順に選択します。
2. ドメインまたはサーバのタブで、[[Manage a domain (ドメインを管理)]] をクリックし、管理する必要のあるサブツリーのドメインを指定します。
3. 管理の対象とするサブツリーのドメインを指定します。
4. [[Manage a subtree of this domain (このドメインのサブツリーを管理)]] を選択し、[[次へ]] をクリックします。
5. [サブツリー] タブで [[追加]] をクリックして、管理対象にするサブツリーを指定します。複数のサブツリーを指定できます。
6. [Access account (アクセスアカウント)] タブで、このサブツリーにアクセスするために DRA が使用することになるアカウントを指定します。デフォルトでは、DRA が管理サーバのサービスアカウントを使用します。
7. サマリの内容を確認し [[完了]] をクリックします。
8. このサブツリーにあるオブジェクトの管理を開始するために、ドメイン構成を更新します。

信頼済みドメインの追加

信頼済みのドメインでは、管理対象の環境全体で管理対象システムでのユーザ認証が可能です。信頼済みドメインを追加すれば、管理対象ドメインと同じように、ドメインと Exchange アクセスアカウントの指定、キャッシュ更新のスケジュール、およびそのドメインのプロパティでの各種アクションの実行が可能です。

信頼済みドメインを追加するには :

1. [[環境設定管理]] > [[管理対象ドメイン]] ノードの順に選択し、そのノードで、関連付けられている管理対象ドメインを持つ管理対象ドメインを選択します。
2. 詳細ペインで [[Trusted domains (信頼済みドメイン)]] をクリックします。詳細ペインは、[表示] メニューで表示非表示を切り替える必要があります。
3. 信頼済みドメインを右クリックして [[プロパティ]] を選択します。
4. [[Ignore this trusted domain (この信頼済みドメインを除外する)]] のチェックを外し、変更を適用します。

注 : 信頼済みのドメインを追加するとアカウントキャッシュの完全更新が始まりますが、[[適用]] をクリックしたときに通知として確認プロンプトが表示されます。

セキュリティ保護された Active Directory を実行するための DRA の設定

セキュリティ保護された Active Directory は、LDAPS (SSL を介した LDAP) プロトコルを使用して実行するように構成された DRA 環境によって定義され、DRA と Active Directory 間の通信を暗号化し、より安全な環境を提供します。

バージョン 9.x から DRA 10.x にアップグレードする場合、アップグレード後にセキュリティ保護された Active Directory を使用するには、LDAPS が有効になっている必要があります。この機能を使用するには、DRA および REST サーバを検出して接続するための自動ディスカバリ機能も設定する必要があります。

SSL 経由の LDAP を有効にする (LDAPS)

バージョン 9.x から DRA 10.x にアップグレードする場合は、次の手順に従います。DRA を新規インストール用に設定する場合は、「管理対象ドメインおよびコンピュータを追加する」を参照してください。

1. DRA Delegation and Configuration console (委任および環境設定コンソール) の［ [環境設定管理]］>［ [管理対象ドメイン]］に移動します。
2. ドメインを右クリックし、［プロパティ］を開きます。
3. ［General (一般)］タブで［ [This domain is configured for LDAP over SSL (このドメインは SSL 経由の LDAP 用に構成されています)]］を有効にして、［ [OK]］をクリックします。
4. NetIQ 管理サービスを再起動します。

注 : セキュリティ保護された Active Directory を使用するように自動ディスカバリを設定する場合は、その構成が完了するまでサービスの再起動を待つことができます。詳細については、「LDAPS の自動ディスカバリを設定する」を参照してください。

LDAPS の自動ディスカバリを設定する

自動ディスカバリは、使用可能な DRA 環境に自動的に接続するためにクライアントが使用するメカニズムです。

セキュリティ保護された Active Directory が実行されている環境に対して DRA を設定するには、ClientSSLAllDomains レジストリキーを設定します。

1. レジストリエディタユーティリティを起動します。
2. HKEY_LOCAL_MACHINE SOFTWARE\Wow6432Node\Mission Critical Software\RestExtentions ノードを右クリックします。
3. ［ [新規]］>［ [DWORD (32 ビット) 値]］を選択します。

4 新しいキーの名前を ClientSSLAllDomains にします。

5 レジストリキーの値を 1 に設定します。

6 ClientSSLAllDomains レジストリキーを追加した後、次のサービスを再起動します。

- World Wide Web Publishing サービス
- NetIQ DRA Rest サービス

パブリックフォルダの接続

DRA では、Microsoft Exchange のパブリックフォルダが管理できます。パブリックフォルダのフォレストドメインの設定およびアシスタント管理者への権限付与により、DRA を使用してパブリックフォルダのプロパティの一部を管理することができます。

重要 : パブリックフォルダ管理を管理するには、まず DRA で Microsoft Exchange のサポートを有効にし、該当する権限を持つ必要があります。

- Microsoft Exchange を有効にする方法については、「Microsoft Exchange の有効化」を参照してください。
- アカウントパーミッションの詳細については、「最小特権 DRA アクセスアカウント」を参照してください。

Exchange のパブリックフォルダのサポートを設定するには :

1 Configuration and Management ノードの［ **[Managed Public Folder Forests (管理対象のパブリックフォルダフォレスト)]**］を右クリックし、［ **[New Public Folder Forest (新しいパブリックフォルダフォレスト)]**］をクリックします。

2 ［ **[Forest Domain (フォレストドメイン)]**］をクリックし、パブリックフォルダオブジェクトがあるアクティブディレクトリフォレストを指定してから、［ **[次へ]**］をクリックします。

3 ［ **[Domain access (ドメインアクセス)]**］で、次のようにアクセスアカウントを指定します。

重要 : セカンダリサーバを使用している場合、［ **[Use the Primary Administration Server domain access account (プライマリ管理サーバのドメインアクセスアカウントを使用)]**］オプションが使用可能になります。

---

4 ［ **[Exchange access (Exchange のアクセス)]**］で、Exchange サーバへの保護されたアクセスに DRA が使用すべきアカウントを指定します。

重要 : セカンダリサーバを使用している場合、［ **[Use the Primary Administration Server Exchange access account (プライマリ管理サーバの Exchange アクセスアカウントを使用)]**］というオプションが使用可能になります。

---

5 ［ **[Exchange サーバ]**］で、パブリックフォルダの管理に DRA が使用するべき Exchange サーバを選択します。

6 ［[Summary (サマリー)]］で、アカウントの詳細と Exchange Server の詳細を確認し、［[完了]］をクリックしてプロセスを完了します。

DRA サーバは、パブリックフォルダのアカウントキャッシュの完全更新を実行します。パブリックフォルダの新しいフォレストは、キャッシュの更新が完了してしばらくすると (数分かかる場合あり)、コンソールに表示されます。

注 : 選択したパブリックフォルダフォレストドメインを［[タスク]］メニューまたは右クリックメニューから削除することができます。

- 133 ページの 「パブリックフォルダのドメインプロパティの表示と変更」
- 134 ページの 「パブリックフォルダの権限委任」

パブリックフォルダのドメインプロパティの表示と変更

パブリックフォルダのドメインプロパティを表示または変更するには :

1 ［Configuration Management］ノードで［[Managed Public Folder Forests (管理対象のパブリックフォルダフォレスト)]］をクリックして、パブリックフォルダを表示します。

2 表示するパブリックフォルダのアカウントを右クリックして［[プロパティ]］を選択します。

3 ［[Public Folder Forest (パブリックフォルダフォレスト)]］プロパティで、次に挙げる操作を行うことができます。

- **全般 :** パブリックフォルダのアカウントの詳細を表示したり［[Exchange サーバ]］フィールドを更新できます。これは DRA サーバがパブリックフォルダのサーバ上での Exchange のアクティビティの実行に使用します。
- **統計 :** パブリックフォルダの数と、メール可能なパブリックフォルダの数を表示します。
- **増分更新ステータス :** 増分アカウントキャッシュのステータスを表示または更新できます。
- **増分更新スケジュール :** キャッシュの増分更新スケジュールを表示し、キャッシュ更新のスケジュールが変更できます。
- **完全更新ステータス :** アカウントキャッシュの完全更新のステータスを表示します。
- **完全更新 :** アカウントキャッシュの更新更新をすぐに実行します。

  NetIQ では、パブリックフォルダのキャッシュデータが破損している場合にのみ [完全更新] を実行することを推奨しています。
- **ドメインへのアクセス :** DRA サービスアカウントの詳細を表示したり、アクセスアカウントを上書きできます。
- **Exchange へのアクセス :** Exchange サーバへのセキュリティで保護されたアクセスを表示または更新できます。

パブリックフォルダの権限委任

権限を定義しパブリックフォルダの委任を管理するために ActiveView を使用します。管理対象オブジェクトの追加、ドメインの選択、権限の割り当てのルールを指定し、それらのパブリックフォルダの権限をアシスタント管理者に委任することができます。

ActiveView を作成して、パブリックフォルダの権限を委任するには :

1 ［ [Delegation Management]］ノードで ［ [ActiveViews]］ をクリックします。

2 ［ [Create ActiveView (ActiveView を作成)]> [] ウィザード] で ［ [次へ]］ をクリックし、［ [追加]］ ドロップダウンリストから目的のルールを選択し、オブジェクトタイプとしてパブリックフォルダを選択します。たとえば、オブジェクトマッチングルールを作成するには、［ [Objects that match a rule (ルールと一致するオブジェクト)]］ を選択し、オブジェクトタイプとして ［ [パブリックフォルダ]］ を選択します。

3 パブリックフォルダに追加する ActiveView ルールを指定してから ［ [次へ]］ をクリックします。

4 ActiveView の名前を指定してから ［ [完了]］ をクリックします。

5 ［ [ActiveViews]］ を右クリックして、［ [Delegate Administration]］ > ［ [アシスタント管理者]］ の順に選択し、[ウィザード] で ［ [追加]］ ドロップダウンリストから管理者タイプを指定します。

6 権限の委任先となる特定のユーザ、グループ、またはアシスタント管理者グループを検索します。

7 [オブジェクトセレクタ] を使用して目的のオブジェクトを見つけて追加し、[ウィザード] で ［ [Roles and Powers (役割と権限)]］ をクリックします。

8 ［ [追加]］ ドロップダウンリストから ［ [役割]］ を選択し、パブリックフォルダ管理の役割を追加します。

9 ［ [追加]］ ドロップダウンリストから権限を選択し、パブリックフォルダ管理者の役割に入っていないアシスタント管理者に対して割り当てたい権限があれば、それらを見つけて追加します。

10 ［ [次へ]］ をクリックしてから ［ [完了]］ で委任プロセスを完了します。

パブリックフォルダの権限委任が完了したら、設定されたドメイン内のパブリックフォルダのプロパティに対して作成、読み取り、更新、削除の各操作を、認可されたユーザが Web コンソールから実行することができます。

Microsoft Exchange の有効化

Microsoft Exchange を有効化することにより、Microsoft Exchange ポリシー、統合メールボックス、およびメールが有効なオブジェクトの管理を含めた Exchange および Exchange Online 機能を活用することができます。Microsoft Exchange Server 2013 以降のバージョンについては、各管理サーバで Microsoft Exchange サポートを有効または無効にすることができます。

Exchange を有効にするには、Manage Policies and Automation Triggers という組み込みの役割に含まれている権限のような、必要とされる権限が必要です。また、ご使用のライセンスが Exchange 製品をサポートしている必要があります。Microsoft Exchange の要件の詳細については、「サポートされているプラットフォーム」を参照してください。

Microsoft Exchange および Exchange Online のサポートを有効にするには、次のようにします。

1 Delegation and Configuration console (委任および環境設定コンソール) の［ **[Policy and Automation Management]**］>［ **[Configure Exchange Policies (Exchange ポリシーの設定)]**］の順に移動します。

2 ［ **[Exchange ポリシーを有効にする]**］を選択し、［ **[適用]**］をクリックします。

Azure テナントの設定

DRA では、証明書を使用した基本認証または多要素認証を使用して、Azure テナントを管理できます。

1 つ以上の Azure テナントに対して、Azure Active Directory を使用して Azure オブジェクトを管理するように DRA を設定できます。これらのオブジェクトには、Azure で作成されたユーザ、ゲストユーザ、連絡先、およびグループ、DRA 管理対象ドメインからの Azure テナントと同期されたユーザ、連絡先、およびグループなどが含まれます。

委任された役割「サーバとドメインの設定」を持つ DRA 管理者またはアシスタント管理者は、Azure テナントを管理できます。Web コンソールで Azure オブジェクトを管理するには、Azure ビルトイン役割が必要です。

Azure タスクを管理するには、Azure PowerShell モジュール、Azure Active Directory、Azure Resource Manager プロファイル、および Exchange Online が必要です。詳細については、「サポートされているプラットフォーム」を参照してください。

Azure Active Directory のアカウントも必要です。Azure テナントアクセスアカウントの許可の詳細については、「最小特権 DRA アクセスアカウント」を参照してください。

Delegation and Configuration Console (委任および環境設定コンソール) で、次に示す設定タスクを実行します。Azure オブジェクトに対する操作は、Web コンソールでのみ実行されます。詳細については、『NetIQ DRA ユーザガイド』の「Azure オブジェクトの管理」を参照してください。

- 136 ページの 「新しい Azure テナントの追加」
- 137 ページの 「手動での証明書のアップロード」

- 138 ページの 「10.2 へのアップグレード後の、Azure アプリケーションの証明書ベース認証の設定」
- 139 ページの 「Azure アプリケーションのクライアントシークレットのリセット」
- 140 ページの 「Azure ゲストユーザの招待の設定」

新しい Azure テナントの追加

新しい Azure テナントを管理するには、DRA が提供する PowerShell スクリプトを使用して、オフラインで Azure アプリケーションを作成する必要があります。DRA は、テナント内のオブジェクトを管理するために必要な許可を、Azure アプリケーションに自動的に付与します。Azure アプリケーションで必要な許可のリストについては、「最小特権 DRA アクセスアカウント」を参照してください。

DRA 用の Azure アプリケーションを作成して Azure テナントを追加するには :

1 Delegation and Configuration Console (委任および環境設定コンソール) で、[**[環境設定管理 (Configuration Management)]**] > [**[Azure テナント]**] に移動します。

2 [**[Azure テナント]**] を右クリックして、[**[新しい Azure テナント]**] を選択します。[**[次へ]**] をクリックします。

3 Azure アプリケーションを作成し、[**[Azure アプリケーション]**] タブで必要な詳細 を指定します。

3a DRA 管理サーバで PowerShell セッションを起動し、C:\Program Files (x86)\NetIQ\DRA\SupportingFiles に移動します。

3b . .\NewDraAzureApplication.ps1 を実行し、PowerShell をロードします。

3c 次のパラメータを指定して、New-DRAAzureApplication コマンドレットを実行します。

- <name>- テナントウィザードのアプリケーション名。

  重要 : Micro Focus では、DRA コンソールで指定された名前を使用することをお勧めします。

- (オプション)<environment>- 使用しているテナントに応じて、AzureCloud、AzureChinaCloud、AzureGermanyCloud、または AzureUSGovernment を指定します。

3d [資格情報] ダイアログボックスで、グローバル管理者の資格情報を指定します。Azure テナント ID、オブジェクト ID、アプリケーション ID、およびクライアントシークレット (アプリケーションパスワード) が生成されます。

注 : DRA は、Azure AD および Exchange Online PowerShell の両方のモジュールと、Microsoft Graph API を使用してデータにアクセスします。アプリケーション ID とアプリケーションシークレットは、Microsoft Graph API を使用して Azure Active Directory にアクセスする場合に使用されます。

3e 新しい Azure テナントの追加ウィザードの［**[Azure アプリケーション]**］タブにテナント ID、オブジェクト ID、アプリケーション ID、およびクライアントシークレットをコピーして、［**[次へ]**］をクリックします。DRA は、Azure アプリケーションを検証します。

4 ［**[認証]**］タブで、認証タイプを選択します。

DRA は、Azure AD モジュールと Exchange Online PowerShell モジュールを使用するときに、証明書ベースの認証と基本認証の両方をサポートします。

- **[証明書ベースの認証]**: これはデフォルトのオプションです。DRA は自己署名証明書を作成し、その証明書を Azure アプリケーションに関連付けます。自己署名証明書を使用しない場合は、テナントの管理後に独自の証明書をアップロードできます。詳細については、「手動での証明書 のアップロード」を参照してください。
- **[基本認証]**: これはレガシオプションです。DRA は、指定したユーザアカウントを使用して、Azure Active Directory を認証します。

［**[次へ]**］をクリックします。

5 (オプション) ［**[カスタム Azure テナントソースアンカー属性 (Custom Azure Tenant Source Anchor Attribute)]**］タブで、同期中に Active Directory オブジェクトを Azure にマップするために使用するソースアンカー属性を指定します。**[次へ]** をクリックします。

6 ［**[完了]**］をクリックします。

Azure テナントを追加するには数分かかることがあります。テナントが正常に追加されると、DRA はテナントに対する完全なアカウントキャッシュの更新を実行し、次に［Azure テナントビュー］ペインに追加されたテナントが表示されます。

Azure テナントの認証タイプを表示するには、テナントを右クリックし、[**[プロパティ]**] > [**[認証]**] に移動します。

証明書情報を表示するには、テナントを右クリックし、[[**[プロパティ]**] > ［**[証明書情報]**］に移動します。

手動での証明書のアップロード

独自の証明書を使用する場合、または既存のカスタム証明書の有効期限が切れている場合に新しい証明書を指定する場合は、Azure テナントプロパティのページから証明書をアップロードできます。サポートされている証明書ファイル形式は、.pfx および .cer です。

重要 : 指定する手動証明書が強力なパスワードで保護されていることを確認してください。

証明書をアップロードするには :

1. Delegation and Configuration Console (委任および環境設定コンソール) を開き、[[環境設定管理 (Configuration Management)]] > [[Azure テナント]] に移動します。
2. Azure テナントを右クリックし、[[プロパティ]] > [[認証]] に移動 します。[[手動顧客証明書 (Manual customer certificate)]] オプションが選択されていることを確認します。
3. [[証明書情報]] タブを 選択します。
4. [[新しい証明書]] で、[[参照]] をクリックして証明書ファイルを選択します。.cer 証明書ファイルを指定する場合は、プライベートキーを持つ証明書がサービスアカウントユーザの個人ストアにインストールされていることを確認します。
5. 必要に応じて、証明書のパスワードを指定します。
6. 変更を適用します。証明書の詳細が更新されます。

重要 :

- プライマリ管理サーバが [[基本認証 (Basic authentication)]] を使用して設定されている場合は、アカウントキャッシュの完全更新を正常に実行するために、セカンダリ管理サーバで [[基本認証 (Basic authentication)]] の資格情報を手動で指定してください。アクセスアカウントは、MMS セット内の各管理サーバで固有である必要があります。
- プライマリ管理サーバが [[手動顧客証明書 (Manual customer certificate)]] 認証タイプか [[自動自己署名証明書 (Automatic self-signed certificate)]] 認証タイプで設定されている場合、セカンダリ管理サーバは認証タイプを [[自動自己署名証明書 (Automatic self-signed certificate)]] として表示します。独自の証明書をアップロードするには、セカンダリ管理サーバで認証タイプを [[手動顧客証明書 (Manual customer certificate)]] に手動で変更する必要があります。証明書は、MMS セット内の各管理サーバで一意である必要があります。

10.2 へのアップグレード後の、Azure アプリケーションの証明書ベース認証の設定

DRA 10.2 にアップグレードした後、基本認証から証明書ベースの認証に切り替え、証明書ベースの認証を使用するように Azure アプリケーションを設定できます。Azure アプリケーションでは、証明書ベースの認証に追加の許可が必要です。Azure アプリケーションに必要な許可を適用するには、UpdateDraAzureApplicationPermission.ps1 スクリプトを実行する必要があります。

アップグレード後に証明書ベースの認証を使用するように Azure アプリケーションを設定するには、次の手順を実行します。

1. Delegation and Configuration Console (委任および環境設定コンソール) を開き、[[環境設定管理 (Configuration Management)]] > [[Azure テナント]] に移動します。
2. Azure テナントを右クリックして、[[プロパティ]]> [[認証]] を選択します。デフォルトでは、[[基本認証 (Basic authentication)]] オプションが選択されています。

3 認証タイプを［[自動自己署名証明書 (Automatic self-signed certificate)]］または［[手動顧客証明書 (Manual customer certificate)]］に変更します。

4 ［[証明書情報 (Certificate Info)]］タブをクリックします。

5 証明書ベースの認証に必要な許可を適用して、Azure アプリケーションを更新します。

5a DRA 管理サーバで PowerShell セッションを起動し、C:\Program Files (x86)\NetIQ\DRA\SupportingFiles に移動します。

5b . .\UpdateDraAzureApplicationPermission.ps1 を実行し、PowerShell をロードします。

5c ［[Azure アプリケーション]］タブで使用可能な Azure アプリケーションの名前を指定して、UpdateDraAzureApplicationPermission コマンドレットを実行します。

5d ［資格情報］ダイアログボックスで、グローバル管理者の資格情報を指定します。アプリケーションオブジェクト ID が生成されます。

5e アプリケーションオブジェクト ID を［[証明書情報 (Certificate Info)]］タブにコピー します。［[手動顧客証明書 (Manual customer certificate)]］オプションを選択した場合は、［新しい証明書 (New Certificate)］エリアに証明書をアップロードします。

6 変更を適用します。証明書の詳細が更新されます。

Azure アプリケーションのクライアントシークレットのリセット

Azure アプリケーションのクライアントシークレットをリセットする必要がある場合は、次の手順に従います。

Azure アプリケーションのクライアントシークレットをリセットするには :

1 DRA 管理サーバで PowerShell セッションを起動し、C:\Program Files (x86)\NetIQ\DRA\SupportingFiles に移動します。

2 . .\ResetDraAzureApplicationClientSecret.ps1 を実行し、PowerShell をロードします。

3 ResetDraAzureApplicationClientSecret コマンドレットを実行して、パラメータを要求するプロンプトを表示します。

4 Reset-DraAzureApplicationClientSecret に次のパラメータを指定します。

- <name>- テナントウィザードのアプリケーション名。
- (オプション)<environment>- 使用しているテナントに応じて、AzureCloud、AzureChinaCloud、AzureGermanyCloud、または AzureUSGovernment を指定します。

5 ［資格情報］ダイアログボックスで、グローバル管理者の資格情報を指定します。

Azure アプリケーション ID とクライアントシークレットが生成されます。

6 クライアントシークレットを DRA コンソール (テナントウィザード) にコピーします。

6a Delegation and Configuration Console (委任および環境設定コンソール) を開き、[[環境設定管理 (Configuration Management)]] > ［[Azure テナント]］に移動します。

6b Azure テナントを右クリックし、[[プロパティ]] > ［[Azure アプリケーション]］の順にクリックします。

6c スクリプトから生成された Azure アプリケーションクライアントシークレットを［ [クライアントシークレット]］フィールドに貼り付けます。

6d 変更を適用します。

Azure ゲストユーザの招待の設定

Azure ゲストユーザを Azure Active Directory に招待すると、DRA は招待リンクを含むカスタマイズされたようこそメッセージとともに、電子メールを Azure ゲストユーザに送信します。このようこそメッセージと、招待に表示する招待リンクまたはリダイレクト URL は設定が可能です。Azure ゲストユーザは招待を受け入れると、設定済みの URL にリダイレクトされます。この URL で、Azure ゲストユーザは資格情報を使用してログインすることができます。

ゲストユーザの招待を設定するには :

1 Delegation and Configuration Console (委任および環境設定コンソール) で、［ [環境設定管理 (Configuration Management)]］> ［ [Azure テナント]］に移動します。

2 招待を設定する管理対象 Azure テナントを選択し、右クリックして［ [プロパティ]］を選択します。

3 ［ [ゲスト招待の設定 (Guest Invite Config)]］タブをクリックします。

4 ようこそメッセージと招待リンクを指定します。

5 変更を適用します。

アクセスアカウントのパスワードの管理

DRA からドメイン、セカンダリサーバ、Exchange、または Azure テナントを管理するために使用されるアクセスアカウントのパスワードをリセットできます。これらのアクセスアカウントのパスワードの期限が切れた場合、またはパスワードを忘れた場合は、次の方法でアクセスアカウントのパスワードをリセットできます。

- Delegation and Configuration Console (委任および環境設定コンソール) で手動でパスワードをリセットします。
- アクセスアカウントのパスワードの有効期限を監視し、期限切れになるアクセスアカウントのパスワードをリセットするジョブをスケジュールします。

プライマリサーバとセカンダリサーバの両方からアクセスアカウントのパスワードをリセットできます。Exchange メールボックスやセカンダリサーバの管理など、同じドメイン内の複数のインスタンスで同じアクセスアカウントが使用されている場合、DRA サーバはアクセスアカウントの使用のすべてのインスタンスのパスワードを自動的に更新するため、各インスタンスのパスワードを手動で更新する必要がなくなります。セカンダリ管理サーバがプライマリ管理サーバのドメインアクセスアカウントを使用している場合、DRA サーバはセカンダリ管理サーバのアクセスアカウントのパスワードを自動的に更新します。

- 141 ページの 「パスワードを手動でリセットする」
- 142 ページの 「パスワードをリセットするジョブのスケジュール」

パスワードを手動でリセットする

Delegation and Configuration Console (委任および環境設定コンソール) を使用して、アクセスアカウントのパスワードを手動でリセットします。

アクセスアカウントのパスワードを手動でリセットするには、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) で、[**[環境設定管理]**] をクリックします。
2. 管理対象ドメインまたは Azure テナントを選択し、プロパティを表示します。
3. [プロパティ] ページで、次の情報を指定します。
   - ドメインアクセスアカウントのパスワードを更新するには、[ドメインアクセス] タブで、ドメインアクセスアカウントの新しいパスワードを指定します。[**[Update password in Active Directory(Active Directory のパスワードを更新する)]**] を選択します。
   - Exchange アクセスアカウントのパスワードを更新するには、[Exchange アクセス] タブで、Exchange アクセスアカウントの新しいパスワードを指定します。[**[Active Directory のパスワードを更新する (Update password in Active Directory)]**] を選択します。
   - Azure テナントアクセスアカウントのパスワードを更新するには、[テナントアクセス] タブで、テナントアクセスアカウントの新しいパスワードを指定します。[**[Update Azure tenant access account password(Azure テナントアクセスアカウントパスワードの更新)]**] を選択します。
   - セカンダリ管理サーバのアクセスアカウントのパスワードを更新するには、プライマリ管理サーバで [**[環境設定管理]**] > [**[管理サーバ]**] を選択します。パスワードを更新するセカンダリ管理サーバを選択し、右クリックして [**[プロパティ]**] を選択します。[アクセスアカウント] タブで、アクセスアカウントの新しいパスワードを指定します。[**[Update password in Active Directory(Active Directory のパスワードを更新する)]**] を選択します。

注

- セカンダリ管理サーバのアクセスアカウントがセカンダリ管理サーバのサービスアカウントではないことを確認します。アクセスアカウントは、セカンダリ管理サーバ上のローカル管理者グループの一部である必要があります。
- 最小特権アカウントをアクセスアカウントとして使用する場合、DRA でパスワードのリセットを成功させるためには、アカウントに Active Directory での「パスワードのリセット」許可が割り当てられている必要があります。

パスワードをリセットするジョブのスケジュール

［パスワードのリセット］ジョブを事前定義された間隔で実行するようにスケジュールして、アクセスアカウントの期限切れパスワードをリセットすることができます。ジョブは、スケジュールされている次のジョブの実行の前に期限切れになるアクセスアカウントパスワードをリセットします。新しいパスワードは、パスワードポリシーに従って自動的に生成されます。

ジョブはデフォルトでは無効になっています。要件に応じて、1 週間に 1 回、または特定の間隔でジョブをスケジュールできます。MMS 環境で、プライマリサーバでジョブを設定する場合は、そのジョブが MMS 内のすべてのサーバで設定されていることを確認します。

ジョブを設定する場合

1 ジョブをスケジュールするサーバで、レジストリエントリ HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Mission Critical Software\OnePoint\Administration\Modules\Accounts\UpdateAccessAccPWD.Freq に移動します。

2 右クリックして［**[変更]**］を選択します。

3 ［**[Value data (値のデータ)]**］フィールドで、ジョブを実行する頻度を指定します。

- 週単位のジョブをスケジュール設定するには、［Weekly(毎週)< 曜日 ><24 時間形式の時刻 >］の形式で頻度を指定します。たとえば、毎週土曜日の午後 6 時にジョブを実行するスケジュールを設定するには、次のコマンドを入力します。

  毎週 06 18:00

  6 は曜日を示し、18:00 は 24 時間形式の時刻を示します。

- ジョブを特定の間隔で実行するスケジュールを設定するには、［Interval(間隔)<24 時間形式の時刻 >］の形式で頻度を指定します。たとえば、8 時間ごとにジョブを実行するスケジュールを設定するには、次のコマンドを入力します。

  間隔 08:00

週末にジョブを実行するようにスケジュールすることをおすすめします。

注 : パスワードのリセットジョブでは、毎日の頻度はサポートされていません。毎日の頻度を設定すると、DRA 管理サービスを再起動すると、DRA Server はスケジュールを自動的に毎週 06 00:00 にリセットします。

---

4 ［**[OK]**］をクリックします。

5 変更を有効にするために DRA 管理サービスを再起動します。

注 : 設定されている各 Azure テナントについて、デフォルトのパスワードポリシーの次のレジストリキーが作成され、有効期間は 90 日となります。
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Mission Critical Software\OnePoint\Administration\Modules\Accounts\<tenantName>.ValidityPeriod。テナントアクセスアカウントのパスワードの有効期限は、テナントの有効期間に基づいて計算されます。パスワードの期限が切れると、ジョブはテナントアクセスアカウントのパスワードをリセットします。

LDAP 上書き認証を有効にする

Web コンソールで LDAP カスタムハンドラ変更の LDAP 上書き認証を設定できます。この機能を有効にすると、カスタム LDAP クエリハンドラの認証タイプを設定して、接続認証に LDAP 上書きアカウントを要求することができます。

この機能を有効にするには :

1. Delegation and Configuration Console (委任および環境設定コンソール) で、[**[環境設定管理]**] > [**[Update Administration Server Options (管理サーバオプションを更新)]**] に移動します。
2. [管理サーバオプション] ウィンドウで [**[LDAP 上書きアカウント]**] タブを選択します。
3. アカウント名、ドメイン、およびパスワードを入力し、変更を適用します。

   例 : name@domain または domain\name

Web コンソールのカスタマイズでこの機能を使用する方法については、「カスタムハンドラ作成の基本手順」を参照してください。

V ポリシーおよびプロセスの自動化

この章には、DRA 環境でのポリシーの働きとポリシーオプションを内容を理解するのに役立つ情報が記載されています。また、Active Directory でオブジェクトを使用するときの、プロセスを自動化するためのトリガと自動ワークフローの使用法についても説明しています。

13 DRA ポリシーについて

DRA では、会社のセキュリティ確保とデータ破壊防止に役立つさまざまなポリシーが設定できます。これらのポリシーは動的セキュリティモデルのコンテキスト内で機能し、ポリシーの強制が会社の変化に自動的に対応するようになっています。命名規則、ディスク使用量の制限、プロパティ検証などのポリシーを確立することで、企業データの整合性の維持を助けるルールを強制できます。

DRA では、次に示す企業管理領域に対し、ポリシーのルールが素早く定義できます。

- Microsoft Exchange
- Office 365 ライセンス
- ホームディレクトリ
- パスワード生成

DRA は、グループ、ユーザアカウント、およびコンピュータに関する組み込みポリシーも提供します。

ポリシーを管理または定義するには、DRA 管理者の役割または Manage Policies and Automation Triggers という役割に含まれている権限のような、適切な権限が必要です。ポリシーの管理を助けるために、DRA は Policy Details レポートを提供しています。このレポートは以下の情報を提供します。

- ポリシーが有効になっているかどうか
- 関連付けられた操作のリスト
- 当該ポリシーによって制御されるオブジェクトのリスト
- ポリシー適用範囲の詳細

このレポートを使用すれば、ポリシーが適切に定義されているかどうかを確認できます。また、このレポートを使用してポリシーのプロパティを比較し、競合を把握することにより、会社全体にポリシーをより適切に強制することもできます。

管理サーバはポリシーをどのように強制するか

各タスク (つまり管理操作) を 1 つ以上のポリシーと関連付けることができます。ポリシーに関連した操作を実行すると、管理サーバがそのポリシーを実行し、指定されたルールを強制します。サーバはポリシー違反を検出すると、エラーメッセージを返します。ポリシー違反を検出しなかった場合、サーバはその操作を完了します。ポリシーを特定の ActiveView グループまたはアシスタント管理者グループに関連付けることにより、ポリシーの適用範囲が制限できます。

操作が複数のポリシーと関連している場合、管理サーバはそれらのポリシーをアルファベット順に強制します。つまり、ポリシー A は、指定されたルールに関係なくポリシー B より先に強制されます。

ポリシーどうしが互いに競合しないようにするために、以下のガイドラインを使用してください。

- 各ポリシーが正しい順序で実行されるように、各ポリシーの名前を付けてください。
- 各ポリシーが他のポリシーによって実行される検証またはアクションに干渉しないことを確認してください。
- カスタムポリシーは、本番環境に実装する前に徹底的にテストしてください。

管理サーバは、ポリシーが実行されるたびにそのポリシーのステータスを監査ログに記録します。これらのログエントリは、戻りコード、関連する操作、操作対象オブジェクト、およびカスタムポリシーの実行が成功したかどうかを記録します。

警告 : ポリシーは、管理サービスアカウントを使って実行されます。サービスアカウントは管理者権限を持っているので、ポリシーはすべての会社データへの完全なアクセス権を持っています。したがって、Manage Policies and Automation Triggers という組み込みの役割に関連付けられたアシスタント管理者が、意図より大きな権限を持つ可能性があります。

組み込みのポリシー

組み込みポリシーは、管理サーバのインストール時に実装されます。これらのポリシーに対する操作を行うときには、以下の用語を理解しておく必要があります。

ポリシーの適用範囲

DRA がポリシーを適用するオブジェクトまたはプロパティを定義します。たとえば、一部のポリシーは、特定の ActiveView 内の特定のアシスタント管理者に対して適用できます。ユーザアカウントやグループなど、異なるクラスのオブジェクトから適用対象を選択できるポリシーもあります。

グローバルポリシー

管理対象ドメイン内にある指定されたクラスまたはタイプのすべてのオブジェクトに対してポリシールールを強制します。グローバルポリシーでは、ポリシーが適用されるオブジェクトの適用範囲を制限することはできません。

ポリシーの関係

ポリシーが他のポリシーとともに適用されるか、それとも単独で適用されるかを定義します。ポリシーの関係を確立するには、同じアクションに適用される複数のルールを定義し、ポリシーグループオプションのメンバーを選択します。操作のパラメータかプロパティがいずれかのルールと一致すると、その操作は成功します。

ビルトインポリシーのトピック :

- 149 ページの 「組み込みポリシーについて」
- 150 ページの 「使用可能なポリシー」
- 152 ページの 「組み込みポリシーの使用」

組み込みポリシーについて

組み込みポリシーは、一般的なセキュリティとデータ整合性の問題に対処するビジネスルールとなります。これらのポリシーはデフォルトのセキュリティモデルの一部ですので、企業の既存のシステム構成に DRA のセキュリティ機能を統合することができます。

DRA には、ポリシーを強制する手段が 2 つあります。カスタムポリシーを作成するという方法と、組み込みポリシーの中から選択するという方法です。込み込みポリシーを利用すれば、カスタムスクリプトを開発しなくても、簡単にポリシーを適用できます。カスタムポリシーを実装する必要がある場合は、既存の組み込みポリシーをニーズに合わせてカスタマイズすることができます。ほとんどのポリシーでは、エラーメッセージのテキストの変更、ポリシーの名前変更、説明の追加、ポリシーの適用方法の指定ができます。

DRA をインストールしたときに、いくつかの組み込みポリシーが有効になります。以下のポリシーがデフォルトで実装されます。これらのポリシーを強制させない場合は、そのポリシーを無効にすることも削除することもできます。

ポリシー名	デフォルト値	説明
$ComputerNameLengthPolicy	64 15 (Windows 2000 以前と互換)	コンピュータ名の文字数または Windows 2000 以前と互換のコンピュータ名を制限します。
$GroupNameLengthPolicy	64 20 (Windows 2000 以前と互換)	グループ名または Windows 2000 以前と互換のグループ名の文字数を制限します。
$GroupSizePolicy	5000	グループのメンバー数を制限します。
$NameUniquenessPolicy	なし	Windows 2000 以前と互換の名前と共通名がすべての管理対象ドメイン内で他と重複しないようにします。
$SpecialGroupsPolicy	なし	環境内で権限が勝手に格上げされることを防ぎます。
$UCPowerConflictPolicy	なし	User Clone 権限と User Create 権限を相互に排他的にすることで、権限の格上げを防ぎます。
$UPNUniquenessPolicy	なし	UPN 名がすべての管理対象ドメイン内で一意であるようにする
$UserNameLengthPolicy	64 20 (ダウンレベルのログイン名)	ユーザログイン名またはダウンレベルログイン名の文字数を制限します。

使用可能なポリシー

DRA には、独自のセキュリティモデル用にカスタマイズできるポリシーがいくつかあります。

注 : 現在は DRA のユーザインタフェースから利用できないプロパティに関し入力を求めるポリシーを作成することも可能です。ポリシーが入力を必要とし、その値 (たとえば新しいユーザカウントの部門名など) を入力するためのフィールドがユーザインタフェース内に存在しない場合は、そのオブジェクトを作成することも管理することもできません。この問題を回避するために、ユーザインタフェースからアクセスできるプロパティのみ要求するポリシーを設定してください。

カスタムポリシーを作成する

スクリプトまたは実行ファイルを DRA または Exchange の操作にリンクさせることができます。カスタムポリシーを使用すれば、任意の操作を検証できます。

名前の最大長を強制する

ユーザアカウント、グループ、OU、連絡先、またはコンピュータの名前の最大長をグローバルに強制することができます。

名前コンテナ (共通名、または cn) と Windows 2000 以前と互換の名前 (ユーザログオン名) をポリシーでチェックします。

最大グループメンバー数を強制する

グループのメンバー数をグローバルに制限することができます。

Windows 2000 以前と互換の一意のアカウント名を強制する

Windows 2000 以前と互換の名前がすべての管理対象ドメイン内で重複していないことを検証します。Microsoft Windows ドメインでは、Windows 2000 以前と互換の名前はドメイン内で一意でなければなりません。このグローバルポリシーによってこのルールがすべての管理対象ドメインで強制されます。

一意の UPN (User Principal Names) を強制する

UPN (User Principal Names) がすべての管理対象ドメイン内で重複していないか検証します。Microsoft Windows ドメインでは、UPN はドメイン内で他と重複しない固有の名前でなければなりません。このポリシーは、このルールをすべての管理対象ドメインにわたって強制します。これはグローバルポリシーなので、DRA がポリシー名、説明、およびポリシーの関係を提供しています。

特別グループのメンバーへのアクションを制限する

管理者グループのメンバー以外はその管理者グループのメンバーを管理できないようにします。このグローバルポリシーは、デフォルトで有効になっています。

管理者グループのメンバーに対するアクションを制限する場合、Create Policy ウィザードは追加情報を要求しません。独自のエラーメッセージを指定できます。これはグローバルポリシーなので、DRA がポリシー名、説明、およびポリシーの関係を提供しています。

アシスタント管理者が同一 AV でユーザの作成およびクローンの作成を防止する

権限のエスカレーションを防ぎます。このポリシーが有効になっている場合、1 人の管理者がユーザアカウントの作成とクローン作成のいずれかを行うことはできますが、その両方の権限を持つことはできません。このグローバルポリシーは、同一人物が同じ ActiveView 内でアカウントの作成とクローン作成の両方を行うことはできないようにします。

このポリシーは、追加情報を必要としません。

命名規則ポリシーを設定する

特定のアシスタント管理者、ActiveView、およびオブジェクトクラス (ユーザアカウントやグループなど) に適用される命名規則を確立できます。

このポリシーによって監視する名前を正確に指定することもできます。

特定のプロパティを検証するポリシーを作成する

OU またはアカウントオブジェクトのプロパティを検証するためのポリシーを作成できます。デフォルト値、プロパティの形式マスク、および有効な値と範囲を指定できます。

このポリシーは、特定のオブジェクトのプロパティが作成、クローン作成、または変更が行われたときに特定の入力フィールドを検証することによってデータの整合性を確保するために使用します。このポリシーは、さまざまなプロパティフィールドについて、入力を検証するための大きな柔軟性と力を提供し、デフォルトの入力を提供し、入力の選択肢を制限します。このポリシーを使用すれば、タスクが完了する前に正しい入力が行われるように強制することができるので、すべての管理対象ドメインにおいてデータの整合性を維持できます。

たとえば、製造、営業、および管理という 3 部門があるとします。DRA がこの 3 つの値しか受け付けないように、入力を制限することができます。また、このポリシーを使用して、正しい電話番号形式を強制したり、有効なデータの範囲を提示したり、電子メールアドレスフィールドの入力を要求することもできます。(123)456 7890 と 456 7890 のように電話番号に複数の形式マスクを指定する場合は、プロパティ形式マスクを「(###)### ####,### ####」と定義してください

Office 365 ライセンスを強制するためのポリシーを作成する

Active Directory グループのメンバーシップに基づいて Office 365 ライセンスを割り当てるためのポリシーが作成できます。このポリシーは、メンバーを関連の Active Directory グループから削除するときに Office 365 ライセンスの削除の強制も行います。

クラウドと同期していないユーザが Active Directory グループに追加される場合、そのユーザの同期化が、Office 365 ライセンスがそのユーザに割り当てられる前に行われます。

ポリシーの作成時に、ポリシーの名前や、このポリシーに違反するアクションをアシスタント管理者が試みたときに表示されるエラーメッセージの内容など、いくつかのプロパティと設定を指定できます。

[Ensure only licenses assigned by DRA (DRA によって割り当てられたライセンスのみ確認する) ポリシーはアカウントで有効になっています。その他のライセンスはすべて削除されます。] 設定は、［テナントプロパティ］ページに含まれており、このページはテナントごとに設定できます。この設定は、DRA Office 365 ライセンスポリシーで使用され、ライセンス割り当ての適用方法を構成します。

この設定が有効になっている場合、DRA ライセンスの適用により、DRA ポリシーを通じて割り当てられたライセンスのみがアカウントにプロビジョニングされます (DRA の外部に割り当てられたライセンスは、ライセンスポリシーに割り当てられたアカウントから削除されます)。この設定が無効になっている場合 (デフォルト)、DRA ライセンスの適用により、Office 365 ポリシーに含まれている特定のライセンスのみがアカウントにプロビジョニングされます (アカウントがライセンスポリシーから割り当てられていない場合は、そのポリシーによって割り当てられたライセンスのみがプロビジョニング解除されます)。

組み込みポリシーの使用

組み込みポリシーはデフォルトセキュリティモデルの一部であり、これらのポリシーを使用して現在のセキュリティモデルを強制することも、ニーズに合わせて組み込みポリシーを変更することもできます。いくつかの組み込みポリシーについては、その名前、ルール設定、適用範囲、ポリシーの関係、エラーメッセージを変更できます。組み込みポリシーは、それぞれ有効または無効にすることができます。

また、簡単に新しいポリシーを作成することもできます。

カスタムポリシーの実装

カスタムポリシーを使用すると、デフォルトのセキュリティモデルの能力と柔軟性をフルに活用できます。カスタムポリシーを使用することで、DRA を既存の企業コンポーネントと統合しつつ、同時に独自ルールも強制することができます。カスタムポリシー機能を利用して、会社のポリシーを拡張できます。

実行可能ファイルまたはスクリプトを管理操作と関連付けることにより、カスタムポリシーを作成および強制します。たとえば、ポリシースクリプトを UserCreate という操作に関連付けることによって、指定された従業員が存在するかどうかを人事データベースでチェックすることが可能です。人事データベース内にその従業員が存在し、既存のアカウントを持っていない場合、そのスクリプトはデータベースから従業員 ID、姓、および名を取得します。操作は正常に完了し、ユーザアカウントのプロパティウィンドウに適切な情報が表示されます。ただし、従業員がすでにアカウントを持っている場合には、この操作は失敗します。

スクリプトは大きな柔軟性と能力を提供します。独自のポリシースクリプトを作成するには、Directory Resource Administrator の ADSI Provider (ADSI プロバイダ)、ソフトウェア開発キット (SDK)、および PowerShell のコマンドレットが使用できます。独自のポリシースクリプトの作成の詳細については、DRA マニュアルのサイトでリファレンスセクションを参照してください。

ネーティブの組み込みセキュリティグループの制限

さらに安全な環境を実現するために、DRA は与えられた権限を Microsoft Windows の組み込みセキュリティグループに制限できます。グループメンバーシップ、組み込みセキュリティグループのプロパティ、またはグループメンバーシップのプロパティを変更できることはセキュリティ的に重要な意味合いがあります。たとえば、サーバオペレータグループ内のユーザのパスワードを変更できる場合、そのユーザとしてログオンでき、この組み込みセキュリティグループに委任された権限を行使します。

DRA は、ネーティブの組み込みセキュリティグループとそのメンバーに対してどのような権限を持っているかを検証するポリシーを用意することで、このセキュリティの問題を防止します。この検証では、要求したアクションによって権限が増すことがないことを確認しています。このポリシーを有効にした後は、サーバオペレータグループなど、ビルトインセキュリティグループのメンバーであるアシスタント管理者は、同じグループの他のメンバーの管理のみできます。

制限可能なネーティブの組み込みセキュリティグループ

次に示す Microsoft Windows 組み込みセキュリティグループの権限を、DRA のポリシーで制限することができます。

- アカウントオペレータ
- 管理者
- バックアップオペレータ
- 証明書の発行元
- DNS 管理者
- ドメイン管理者
- 企業管理者
- グループポリシー作成元の所有者
- プリントオペレータ
- スキーマ管理者

注 : DRA は内部識別子で組み込みのセキュリティグループを参照します。その結果、グループ名が変更されても、DRA がこれらのグループをサポートします。この機能により、さまざまな国々で異なる名前を使った組み込みセキュリティグループを DRA がサポートします。たとえば、DRA は管理者グループと、同じ内部 ID の *Administratoren* というグループを参照します。

ネーティブの組み込みセキュリティグループに対するアクション制限

DRA はポリシーを使用してネーティブの組み込みセキュリティグループとそのメンバーが実行できる権限を制限することができます。このポリシーは、$SpecialGroupsPolicy と呼ばれ、ネーティブの組み込みセキュリティグループのメンバーが他のメンバーまたは他の

ネーティブの組み込みセキュリティグループに対して実行できるアクションを制限します。DRA ではデフォルトでこのポリシーが有効になります。ネーティブの組み込みセキュリティグループとそのメンバーに対するアクションを制限したくない場合は、このポリシーを無効にすることができます。

このポリシーを有効にすると、DRA は次に示す検証テストを使用して、ネーティブの組み込みセキュリティグループまたはそのメンバーに対してのアクションが許可されているかどうかを判断します。

- Microsoft Windows の管理者の人であれば、適切な権限のあるネーティブの組み込みセキュリティグループとそのメンバーに対しアクションを実行できます。
- 組み込みのセキュリティグループのメンバーであれば、適切な権限を持っている限り、同じ組み込みセキュリティグループとそのメンバーに対してアクションを実行できます。
- 組み込みセキュリティグループのメンバーでない人は、組み込みのセキュリティグループやそのメンバーを変更することができません。

たとえば、適切な権限を持ち、サーバオペレータグループとアカウントオペレータグループのメンバーの人であれば、サーバオペレータのメンバーに、アカウントオペレータのグループのメンバーに、または両グループのメンバーに対してアクションを実行できます。ただし、その人はプリントオペレータグループとアカウントオペレータグループのメンバーのユーザアカウントに対してアクションを実行できません。

DRA はネーティブの組み込みセキュリティグループに対し次に挙げる操作の実行を制限します。

- グループのクローン作成
- グループの作成
- グループの削除
- グループへのメンバー追加
- グループからのメンバー削除
- OU のグループへの移動
- グループのプロパティ変更
- メールボックスのコピー
- メールボックスの削除
- ユーザアカウントのクローン作成
- ユーザアカウントの作成
- ユーザーアカウントの削除
- OU へのユーザアカウントの移動
- ユーザアカウントのプロパティ変更

DRA は、あるオブジェクトに対しユーザが権限を獲得しないように、アクションも制限します。たとえば、あるユーザアカウントをグループに追加するときに、それがそのグループのメンバーであるため、DRA がその操作をした人がそのユーザアカウントに対し追加の権限を獲得しないようチェックします。この検証は権限格上げの防止に役立ちます。

ポリシーの管理

Policy and Automation Management ノードを通じて、Exchange ポリシー、ホームディレクトリポリシー、組み込みポリシー、およびカスタムポリシーにアクセスできます。以下の一般的なタスクを使用して、会社のセキュリティとデータの整合性を向上させることができます。

Exchange ポリシーを設定する

Microsoft Exchange の設定、メールボックスポリシー、自動命名、およびプロキシ生成ルールを定義することができます。これらのルールは、アシスタント管理者がユーザアカウントを作成、変更、または削除したときに、メールボックスがどのように管理されるかを定義できます。

ホームディレクトリポリシーを設定する

アシスタント管理者によってユーザアカウントが作成、名前変更、または削除されたときに、ホームディレクトリおよびホーム共有を自動的に作成、名前変更、または削除することができます。ホームディレクトリポリシーを使って、Microsoft Windows のサーバおよび Windows ではないサーバのホームディレクトリについてディスククォータのサポートを有効または無効にすることもできます。

パスワード生成ポリシーの設定

DRA によって生成されたパスワードの要件を定義できます。

DRA でポリシーを管理する方法の詳細については、次のセクションを参照してください。

- 155 ページの 「Microsoft Exchange ポリシー」
- 157 ページの 「Office 365 ライセンスポリシー」
- 158 ページの 「ホームディレクトリポリシーの作成と実装」
- 165 ページの 「パスワード生成機能の有効化」
- 165 ページの 「ポリシーのタスク」

Microsoft Exchange ポリシー

Exchange には、Microsoft Exchange のオブジェクトをより効率的に管理するために役立つポリシーがいくつか用意されています。Microsoft Exchange のポリシーを使用すれば、メールボックス管理の自動化、エイリアスとメールボックスストアの命名規則適用、および電子メールアドレスの自動生成が可能です。

これらのポリシーは、ワークフローの整理統合とデータの整合性の維持に役立ちます。たとえば、ユーザカウントが作成、変更、または削除されたときに Exchange がメールボックスをどう管理するのかを指定することができます。Microsoft Exchange ポリシーを設定するには、Manage Policies and Automation Triggers という組み込みの役割に含まれている権限のような、適切な権限が必要です。

デフォルトの電子メールアドレスポリシーの指定

電子メールアドレスのデフォルトのポリシーを指定するには、Manage Policies and Automation Triggers という組み込みの役割に含まれている権限のような、適切な権限が必要です。また、使用しているライセンスが Exchange をサポートしている必要があります。

デフォルトの電子メールアドレスポリシーを指定するには :

1 [[Policy and Automation Management]> [[Configure Exchange Policies (Exchange ポリシーを設定)]] > [[Proxy Generation (プロキシの生成)]] の順に選択します。

2 Microsoft Exchange サーバのドメインを指定します。

   2a [[参照]] をクリックします。

   2b 必要に応じて追加の検索条件を指定し、[[Find Now (今すぐ検索)]] をクリックします。

   2c 設定するドメインを選択して [[OK]] をクリックします。

3 選択されたドメインに対するプロキシ生成ルールを指定します。

   3a [[追加]] をクリックします。

   3b プロキシタイプを選択します。たとえば、[[インターネットアドレス]] をクリックします。

   3c デフォルトの値を受け入れるか、新しいプロキシ生成ルールをタイプ入力してから、[[OK]] をクリックします。

   プロキシ生成ルールで使用できる置換文字列の詳細については、「委任およびクライアントのクライアントのポリシー」を参照してください。

4 [[カスタム属性]] をクリックして、カスタムメールボックスプロパティのカスタム名を編集します。

   4a 属性を選択して [[編集]] ボタンをクリックします。

   4b [Attribute Properties (属性プロパティ)] ウィンドウで [[Custom name (カスタム名)]] フィールドに属性名を入力し、[[OK]] をクリックします。

5 [[OK]] をクリックします。

注 : Microsoft Exchange のポリシー内のカスタム属性を変更するには、DRA のポリシー管理者が *Manage Custom Tools* という権限を持っている必要があります。

メールボックスルール

メールボックスルールを使用すれば、アシスタント管理者によってユーザアカウントが作成、クローン作成、変更、または削除されたときに Exchange にメールボックスをどのように管理させるかを指定することができます。メールボックスルールは、関連付けられたユーザアカウントをアシスタント管理者がどのように管理したかに基づいて、Microsoft Exchange メールボックスを自動的に管理します。

注 : Microsoft Windows ドメインで［ **[Do not allow Assistant Admins to create a user account without a mailbox (メールボックス無しのユーザアカウントの作成をアシスタント管理者に許可しない)]**］というオプションを有効にする場合、確実にアシスタント管理者にユーザアカウントの作成またはクローン作成のいずれかを行う権限を付与してください。このオプションを有効にするには、アシスタント管理者がメールボックスを持つ Windows ユーザアカウントを作成できる必要があります。

Microsoft Exchange のメールボックスのルールを指定するには、Manage Policies and Automation Triggers という組み込みの役割に含まれている権限のような、適切な権限が必要です。また、使用しているライセンスが Exchange 製品をサポートしている必要があります。

Exchange のメールボックスルールを指定するには :

1. ［ **[Policy and Automation Management]**>［ **[Configure Exchange Policies (Exchange ポリシーを設定)]**］>［ **[Mailbox Rules (メールボックスルール)]**］の順に選択します。
2. ユーザアカウントを作成または変更したときに Exchange に強制させるメールボックスポリシーを選択します。
3. ［ **[OK]**］をクリックします。

Office 365 ライセンスポリシー

Office 365 のライセンスポリシーを指定するには、Manage Policies and Automation Triggers というビルトインの役割に含まれている権限のような、適切な権限が必要です。使用しているライセンスが Microsoft Exchange をサポートしている必要もあります。

DRA による Office 365 ライセンス管理の許可 (オプション)

DRA に Office 365 のライセンスの管理を許可する場合は、次の操作を行う必要があります。

- ライセンス強制ポリシーを作成する
- テナントプロパティのページで［ **[ライセンスの更新スケジュール]**］を有効にします。

Office 365 ライセンスを強制するポリシーの作成

Office 365 ライセンスを強制するポリシーを作成するには、Delegation and Configuration console (委任および環境設定コンソール) で［ **[Policy and Automation Management]**］ノードをクリックし、［ **[New Policy (新規のポリシー)]**］>［ **[Create New Policy to Enforce Office 365 Licenses (Office 365 のライセンスを強制する新規のポリシーを作成)]**］の順に選択します。

ポリシーが強制されユーザが Active Directory に追加されているときは、DRA がグループメンバーシップを使用して Office 365 のライセンスをユーザに自動的に割り当てます。

Office 365 ライセンスの更新スケジュール

Office 365 のライセンス強制に作成するポリシーは、テナントプロパティページで［[License update schedule (ライセンス更新スケジュール)]］も有効にしていない限り、変更が DRA の外で行われたときは適用されません。ライセンス更新ジョブでは、ユーザに割り当てられた Office 365 のライセンスが Office 365 のライセンスポリシーと一致することを確認しています。

ライセンス更新ジョブと Office 365 のライセンスポリシーが連携し合って、すべての管理対象ユーザが確実に各自の持つべき Office 365 ライセンスのみに割り当てられるようにします。

注

- DRA では、オンライン専用のユーザアカウントに関しては Office 365 ライセンスを管理しません。Office 365 ライセンスを持つユーザを DRA に管理させるには、そのようなユーザと Active Directory とを同期化する必要があります。
- DRA を使用して Office 365 ライセンスを管理することを選択した場合、DRA の外で行われた Office 365 ライセンスへの手動による変更が、次回ライセンス更新ジョブが実行されるときにすべて DRA によって上書きされます。
- Office 365のライセンスポリシーが正しく設定されているか確認する前にOffice 365ライセンス更新ジョブを有効にすると、ライセンス更新ジョブの実行後に、割り当てられたライセンスが正しくなくなる可能性があります。

ホームディレクトリポリシーの作成と実装

多数のユーザアカウントを管理する場合、それらのホームディレクトリおよび共有を作成して管理するには長い時間がかかり、セキュリティエラーの原因になる可能性があります。その後も、ユーザが作成、名前変更、または削除されるたびに、追加の保守が必要になります。ホームディレクトリポリシーは、ホームディレクトリとホーム共有の保守管理を助けます。

DRA では、ユーザホームディレクトリの作成と保守を自動化できます。たとえば、ユーザアカウントが作成されたときに管理サーバがホームディレクトリを作成するように、DRA を設定することができます。このケースでは、ユーザアカウントを作成したときにホームディレクトリパスを指定すると、サーバがそのパスに自動的にホームディレクトリを作成します。パスを指定しなかった場合、ホームディレクトリは作成されません。

DRA は、許容される親パス内のユーザについて、ユーザのホームディレクトリの作成時や、ホームディレクトリポリシーの設定時に、DFS (Distributed File System) のパスをサポートします。Netapp フィルタおよび DFS パスまたはパーティション上でのホームディレクトリの作成、名前変更、削除を実行できます。

ホームディレクトリポリシーの設定

ホームディレクトリ、共有、ボリュームディスククォータのポリシーを設定するには、Manage Policies and Automation Triggers という組み込みの役割に含まれている権限のような、適切な権限が必要です。各ポリシーは、関連付けられたユーザアカウントをどのように管理するかに基づいて、ホームディレクトリ、共有、およびボリュームディスククォータを自動的に管理します。

ホームディレクトリのポリシーを設定するには、[**[Policy and Automation Management]**] > [**[Configure Home Directory Policies (ホームディレクトリのポリシーを設定)]**] の順に選択してください。

- ホームディレクトリ
- ホーム共有
- ホームボリュームディスククォータ

管理サーバの要件

ホーム共有を作成する必要がある各コンピュータに対して、管理サーバサービスアカウントまたはアクセスアカウントがそのコンピュータの管理者になっているか、対応するドメイン内で Administrators グループのメンバーになっている必要があります。

管理共有 (C$ や D$) は、DRA がホームディレクトリを管理および保存する各ドライブに存在している必要があります。DRA は管理共有を使用して、一部のホームディレクトリおよびホーム共有自動化タスクを実行します。これらの共有が存在しないと、DRA はホームディレクトリおよびホーム共有の自動化を提供できません。

NetApp フィルタの許容可能なホームディレクトリパスの設定

NetApp フィルタに許容可能な親パスを設定する手順は次のとおりです。

1 [**[Policy and Automation Management]**] > [**[Configure Home Directory Policies (ホームディレクトリのポリシーを設定)]**] の順に選択します。

2 [**[Allowable parent paths (指定可能な親パス)]**] テキストボックスに、次の表に示す指定可能なパスのいずれかを入力します。

共有の種類	指定可能なパス
Windows	(\\ *ファイル名* *adminshare*:\ *ボリュームのルートパス* \ *ディレクトリパス*)
Windows 以外	(*non-windows**share*)

3 [**[追加]**] をクリックします。

4 ホームディレクトリポリシーを適用する許容可能な親パスのそれぞれに手順 1 ～ 3 を繰り返します。

ホームディレクトリポリシーについて

適切な Microsoft Windows セキュリティポリシーと矛盾しないように、DRA はディレクトリレベルでのみアクセス制御の制限を作成します。共有名レベルとファイルまたはディレクトリオブジェクトレベルの両方でアクセス制御の制限を課すると、多くの場合、管理者およびユーザーにとって混乱を招くアクセススキームとなります。

ホーム共有に対するアクセス制御の制限を変更しても、DRA はそのディレクトリに対する既存のセキュリティを変更しません。この場合は、変更者が、ユーザアカウントが自分自身のホームディレクトリに対して適切なアクセス権を持つように設定する必要があります。

ホームディレクトリの自動化とルール

DRA は、ユーザアカウントが変更されたときにホームディレクトリを管理することにより、ホームディレクトリ保守タスクを自動化します。DRA は、ユーザアカウントが作成、クローン作成、変更、名前変更、または削除されたときに、それぞれ異なるアクションを実行できます。

ホームディレクトリポリシーを適切に実装するために、以下のガイドラインを使用してください。

- 正しい形式でパスを指定してください。
  - 単一のホームディレクトリのパスを指定するには、次の表に示すテンプレートのうち 1 つを使用してください。

共有の種類	パスのテンプレート
Windows	*computer**share*\. たとえば、server01 というコンピュータ上の Home Share というフォルダ内にホームディレクトリを DRA に自動的に作成させたい場合、「\\server01\Home Share\」とタイプ入力します。
Windows 以外	*non-windows**share*

  - 対応するホーム共有のルートディレクトリに対するホームディレクトリ管理を標準化するためには、汎用命名規則 (Universal Naming Convention) の構文を使用してください。たとえば、「\\ *サーバ名* *C:*\ *ルートディレクトリへのパス*」のような形式です。
  - 入れ子になったホームディレクトリのパスを指定するには、次の表に示すテンプレートのうち 1 つを使用してください。

共有の種類	パスのテンプレート
Windows	*computer**share*\ *最初のディレクトリ**2 番目のディレクトリ*\
	たとえば、server01 というコンピュータ上の Home Share というフォルダ内にある JSmith\Home という既存ディレクトリに自動的にホームディレクトリが作成されるようにしたい場合は、「\\server01\Home Share\JSmith\Home」とタイプ入力します。
Windows 以外	*non-windows**share*\ *最初のディレクトリ**2 番目のディレクトリ*\

注 : DRA は「*computer**share*\ *ユーザ名*」および「*computer**share**% ユーザ名 %*」という形式もサポートしています。どちらの場合も、DRA は関連付けられたユーザアカウントのホームディレクトリを自動的に作成します。

- NetApp Filer 上のホームディレクトリを管理するためにポリシーまたは自動化トリガを定義する際には、異なる形式でディレクトリを指定する必要があります。
  - NetApp ファイラを使用している場合は、親ディレクトリを次の形式で指定します。\\ *ファイル名**adminshare:*\ *ボリュームのルートパス*\ *ディレクトリパス*
  - adminshare という変数は、*c$* などのように、NetApp ファイラ上のルートボリュームにマップする非表示の共有です。たとえば、NetApp ファイラの共有が usfiler という名前で、そのローカルパスが c$\vol\vol0\mydirectory だった場合、その NetApp ファイラのルートパスを「\\usfiler\c:\vol\vol0\mydirectory」に指定することができます。
- ユーザのホームディレクトリを作成するとき、またはユーザのためにホームディレクトリのポリシーを設定するときに DFS パスを指定するには、「\\ *サーバ*\ *ルート*\< *リンク*> という形式を使用してください。ここで、ルートは管理対象ドメインでも、「\\ *ファイル名**adminshare:*\ *ボリュームのルートパス*\ *ディレクトリパス*」という形式であればスタンドアロンのルートディレクトリでも構いません。
- このユーザカウントのホームディレクトリを保存する共有ディレクトリを作成してください。
- パス内で参照されているコンピュータまたは共有に DRA がアクセスできるようにしてください。

ユーザアカウント作成時にホームディレクトリを作成する

このルールは、DRA が新しいユーザアカウントに対してホームディレクトリを自動的に作成できるようにします。DRA がホームディレクトリを作成するとき、管理サーバは［ユーザの作成］ウィザードの［**[ホームディレクトリ]**］フィールドで指定されたパスを使用します。ユーザプロパティウィンドウの［プロファイル］タブを使ってこのパスを後で変更でき、DRA はホームディレクトリを新しい場所に移動します。これらのフィールドに値を指定しなかった場合、そのユーザアカウントのホームディレクトリは作成されません。

DRA は、[[Home directory permissions (ホームディレクトリ権限)]] という選択されたオプションに基づいて新しいディレクトリのセキュリティを設定します。これらのオプションを使用することで、すべてのホームディレクトリに対する一般的なアクセスを制御できます。

たとえば、各自のユーザホームディレクトリが属している共有に対して、管理者グループのメンバーはフルコントロール権限を持ち、ヘルプデスクグループのメンバーは読み込みアクセス権限を持つように指定することができます。その後 DRA がユーザホームディレクトリを作成すると、その新しいホームディレクトリは親ディレクトリからこれらの権限を継承できます。したがって、管理者グループのメンバーはすべてのユーザホームディレクトリに対してフルコントロール権限を持ち、ヘルプデスクグループのメンバーはすべてのユーザホームディレクトリに対して読み込みアクセス権限を持つことになります。

すでに存在するホームディレクトリを指定した場合、新しいホームディレクトリは作成されず、既存のディレクトリに対する権限は変更されません。

ユーザアカウントの名称変更時にホームディレクトリを名称変更する

このルールは、DRA が以下のアクションを自動的に実行できるようにします。

- 新しいホームディレクトリパスが指定されたときにホームディレクトリを作成する
- ホームディレクトリパスが変更されたときにホームディレクトリの内容を移動する
- ユーザカウントの名前が変更されたときにホームディレクトリの名前を変更する

ユーザカウントの名前を変更すると、新しいアカウント名に基づいて既存のホームディレクトリの名前も変更されます。既存のホームディレクトリが使用中の場合は、新しいホームディレクトリが作成され、既存のホームディレクトリは変更されません。

ホームディレクトリのパスを変更すると、指定したホームディレクトリが新しく作成され、元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。また、元のホームディレクトリから内容を移動せずにホームディレクトリを作成するように、ホームディレクトリのポリシーを設定することもできます。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。すでに存在するホームディレクトリを指定した場合、新しいホームディレクトリは作成されず、既存のディレクトリに対する権限は変更されません。元のホームディレクトリがロックされていなければ、そのディレクトリは削除されます。

DRA がホームディレクトリの名前変更に失敗した場合、DRA は新しい名前で新しいホームディレクトリを作成し、元のホームディレクトリの内容を新しいホームディレクトリにコピーしようとします。その後、元のホームディレクトリを削除しようと試みます。元のホームディレクトリの内容を新しいホームディレクトリにコピーしないように DRA を設定し、元のホームディレクトリの内容を手動で新しいホームディレクトリに移動することもできます。これにより、開いているファイルをコピーするなどの問題を回避できます。

DRA が元のホームディレクトリを削除する際には、元のホームディレクトリから読み取り専用ファイルおよびサブディレクトリを削除するための明示的な権限を必要とします。元のホームディレクトリを読み取り専用ファイルおよびサブディレクトリを削除する権限を、DRA に明示的に与えることができます。

ホーム共有で親ディレクトリまたはパスを許可する

DRA では、ファイルサーバ上のホーム共有について、許可される親ディレクトリまたはパスを指定できます。指定するディレクトリまたはファイルサーバパスが多い場合は、それらのパスを CSV ファイルにエクスポートして、DRA コンソールを使って CSV ファイルから DRA にパスを追加することができます。DRA は、以下のことを保証するために、[**[Allowable parent paths (指定可能な親パス)]**] というフィールドに入力された情報を使用します。

- アシスタント管理者がユーザアカウントとユーザアカウントのホームディレクトリを削除したときに、DRA はファイルサーバ上の親ディレクトリを削除しない。
- ユーザアカウントの名前が変更されるか、ユーザアカウントのホームディレクトリパスが変更されたときに、DRA がホームディレクトリを有効な親ディレクトリまたはファイルサーバ上のパスに移動する。

ユーザアカウントの削除時にホームディレクトリを削除する

このルールは、ユーザアカウントが削除されたときに、それに関連付けられたホームディレクトリを DRA が自動的に削除できるようにします。ごみ箱が有効になっている場合には、ユーザアカウントがごみ箱から削除されるまでは、ホームディレクトリは削除されません。DRA がホームディレクトリを削除する際には、そのホームディレクトリから読み取り専用ファイルおよびサブディレクトリを削除するための明示的な権限を必要とします。元のホームディレクトリを読み取り専用ファイルおよびサブディレクトリを削除する権限を、DRA に明示的に与えることができます。

ホーム共有の自動化とルール

DRA は、ユーザアカウントが変更されるかホームディレクトリが管理されたときにホーム共有を管理することによって、ホーム共有保守タスクを自動化します。DRA は、ユーザアカウントの作成、クローン作成、変更、名前変更、または削除が行われたときに、それぞれ異なるアクションを実行できます。

適切な Microsoft Windows セキュリティポリシーと矛盾しないように、DRA は共有名レベルではアクセス制御の制限を作成しません。代わりに、ディレクトリレベルでのみアクセス制御の制限を作成します。共有名レベルとファイルまたはディレクトリオブジェクトレベルの両方でアクセス制御の制限を課すると、多くの場合、管理者およびユーザにとって混乱を招くアクセススキームとなります。

注 : 指定する場所は、HOMEDIRS のような共通のホーム共有をホームディレクトリの 1 レベル上に持っている必要があります。

たとえば、次のパスは有効です。*HOUSERV1**HOMEDIRS**%username%*

次のパスは無効です。*HOUSERV1**%username%*

共有ホームディレクトリ名の指定

共有ホームディレクトリの自動化ルールを定義するときに、自動的に作成される各共有ホームディレクトリについてプレフィックスおよびサフィックスを指定できます。プレフィックスまたはサフィックスを指定することにより、共有ホームディレクトリに命名規則を強制できます。

たとえば、Create home directory および Create home share という自動化ルールを有効にしたとします。さらに、共有ホームディレクトリについて、プレフィックスとしてアンダスコア (_)、サフィックスとしてドル記号 ($) を指定したとします。TomS という名前のユーザを作成するとき、このユーザの新しいディレクトリを U ドライブにマッピングして、ディレクトリパスとして \\HOUSERV1\HOMEDIRS\%username% と指定します。この例では、DRA が _TomS$ という名前のネットワーク共有を作成し、それが \\HOUSERV1\HOMEDIRS\TomS というディレクトリが指しています。

新規ユーザアカウントのホーム共有の作成

DRA がホーム共有を作成すると、管理サーバは［ユーザの作成］ウィザードの［[ホームディレクトリ]］フィールドで指定されたパスを使用します。その後、ユーザプロパティウィンドウの［プロファイル］タブを使ってこのパスを変更できます。

DRA は、プレフィックスとサフィックスが指定されていれば、それらをユーザ名に付け加えて共有名を作成します。長いユーザカウント名が使用された場合は、指定されたホーム共有プレフィックスおよびサフィックスを付け加えられないことがあります。プレフィックスとサフィックス、および許可される接続の数は、選択されたホーム共有作成オプションに基づいて決められます。

クローン作成されたユーザアカウントのホーム共有の作成

新しく作成されたユーザアカウント名から生成された共有ホームディレクトリ名がすでに存在する場合、DRA は既存の共有を削除して、指定されたホームディレクトリに対して新しい共有を作成します。

ユーザアカウントのクローンを作成するときには、既存のユーザアカウントの共有名が存在していなければなりません。ユーザアカウントのクローンが作成されると、DRA はホームディレクトリ情報のクローンも作成して、その情報を新しいユーザ用にカスタマイズします。

ホーム共有のプロパティの変更

ホームディレクトリの場所を変更すると、既存の共有は削除され、新しいホームディレクトリに対して新しい共有が作成されます。元のホームディレクトリが空の場合、元のディレクトリは削除されます。

名前が変更されたユーザアカウントの共有ホームディレクトリ名の変更

ユーザアカウントの名前を変更すると、既存のホーム共有は削除され、新しいアカウント名に基づいて新しい共有が作成されます。新しい共有ディレクトリは、既存のホームディレクトリをポイントします。

削除されたユーザアカウントの共有ホームディレクトリの削除

ユーザアカウントを永久に削除すると、その共有ホームディレクトリも削除されます。

ホームボリュームディスククォータ管理ルール

DRA では、ホームボリュームのディスククォータを管理できます。このポリシーは、Microsoft Windows コンピュータにある、ホームディレクトリが存在するネーティブドメイン内で実装できます。このポリシーを実装する場合は、十分な領域を確保するために、ディスククォータを少なくとも 25MB に指定する必要があります。

パスワード生成機能の有効化

この機能では、DRA の生成するパスワードのポリシー設定を指定することができます。DRA はユーザ作成のパスワードに対するこれらの設定を強制しません。パスワードポリシーのプロパティを設定する場合、パスワードの長さは 6 文字未満で、127 文字以下でなければなりません。パスワードの長さと上限を除き、すべての値を 0 に設定することができます。

パスワード生成ポリシーを設定するには、[[Policy and Automation Management]] > [[Configure Password Generation Policies (パスワード生成ポリシーを設定)]] の順に選択し、[[Enable Password Policy (パスワードポリシーを有効にする)]] チェックボックスを選択してください。[[Password Settings (パスワード設定)]] をクリックし、パスワードポリシーのプロパティを設定します。

ポリシーのタスク

ポリシーを消去、有効化、無効化するには、Manage Policies and Automation Triggers という組み込みの役割に含まれている権限のような、適切な権限が必要です。

これらのアクションのいずれかを実行するには、[[Policy and Automation Management]] > [[ポリシー]] の順に選択します。右側のペインで削除、有効化、または無効化するポリシーを右クリックし、目的のアクションを選択します。

組み込みポリシーの実装

組み込みポリシーを実装にするには、Manage Policies and Automation Triggers という組み込みの役割に含まれている権限のような、適切な権限が必要です。組み込みのポリシーの詳細については、「組み込みポリシーについて」を参照してください。

注 : ビルトインポリシーをアシスタント管理者および ActiveView と関連付ける前に、まずそのアシスタント管理者がその ActiveView に割り当てられているか確認してください。

組み込みポリシーを実装するには :

1. [[Policy and Automation Management]] > [[ポリシー]] の順に選択します。
2. [タスク] メニューで [[New Policy (新規のポリシー)]] をクリックし、作成する組み込みポリシーのタイプを選択します。

3 各ウィザードウィンドウで適切な値を指定して［[次へ]］をクリックします。たとえば、この新しいポリシーを特定の ActiveView に関連付けて、その ActiveView に含まれるオブジェクトにこのポリシーが強制されるようにすることができます。

4 サマリの内容を確認し［[完了]］をクリックします。

カスタムポリシーの実装

カスタムポリシーを実装するには、Manage Policies and Automation Triggers という組み込みの役割に含まれている権限のような、適切な権限が必要です。

カスタムポリシーを正しく実装するには、特定の操作 (管理タスク) の最中に実行されるスクリプトを作成する必要があります。実行ファイルまたはスクリプトを操作に関連付けできます。DRA は、32 ビット PowerShell スクリプトと 64 ビット PowerShell スクリプトの両方をサポートしています。カスタムポリシースクリプトの中では、アクションがポリシーに違反したときに表示されるエラーメッセージを定義できます。また、Create Policy ウィザードでデフォルトのエラーメッセージを指定することもできます。

カスタムポリシーの作成方法、管理操作のリスト、および引数配列の使用方法については、SDK を参照してください。詳細については、「カスタムポリシースクリプトまたは実行ファイルの作成」を参照してください。

注

- カスタムポリシーをアシスタント管理者および ActiveView と関連付ける前に、まずそのアシスタント管理者がその ActiveView に割り当てられているか確認してください。
- カスタムポリシースクリプトまたは実行ファイルのパスにスペースが含まれている場合は、パス全体を引用符 (") で囲んでください。

カスタムポリシーを実装するには :

1 ポリシースクリプトまたは実行ファイルを作成します。

2 管理対象ドメイン内で Manage Policies and Automation Triggers という組み込みの役割を割り当てられているアカウントを使って、DRA のクライアントコンピュータにログオンします。

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

4 プライマリ管理サーバに接続します。

5 左側のペインで、[Policy and Automation Management] を展開します。

6 ［[ポリシー]］をクリックします。

7 ［タスク］メニューで［[New Policy (新規のポリシー)］>［Create a Custom Policy (カスタムポリシーを作成)]］の順にクリックします。

8 各ウィザードウィンドウで適切な値を指定して［[次へ]］をクリックします。たとえば、この新しいポリシーを特定の ActiveView に関連付けて、その ActiveView に含まれるオブジェクトにこのポリシーが強制されるようにすることができます。

9 サマリの内容を確認し［[完了]］をクリックします。

ポリシーのプロパティの変更

ポリシーのプロパティを変更するには、Manage Policies and Automation Triggers という組み込みの役割に含まれている権限のような、適切な権限が必要です。

ポリシーのプロパティを変更するには :

1 ［ [Policy and Automation Management]］>［ [ポリシー]］の順に選択します。
2 変更するポリシーを右クリックして［ [プロパティ]］を選択します。
3 このポリシーについて適切なプロパティと設定を変更します。

カスタムポリシースクリプトまたは実行ファイルの作成

カスタムポリシースクリプトまたは実行ファイルの作成方法については、SDK を参照してください。

SDK にアクセスする手順は、次のとおりです。

1 コンピュータに SDK がインストールされていることを確認します。セットアッププログラムが Directory and Resource Administrator プログラムグループの中に SDK のショートカットを作成しています。詳細については、「DRA 管理サーバのインストール」のインストール時チェックリストを参照してください。
2 Directory and Resource Administrator プログラムグループ内の SDK のショートカットをクリックします。

委任およびクライアントのクライアントのポリシー

自動命名ポリシーには、Exchange ポリシーのうちの Delegation and Configuration のクライアント専用のポリシー設定が 3 つ含まれます。これはクライアント側のポリシーであることを意味します。

自動命名ポリシーを使用すると、メールボックスの特定のプロパティについて、自動化された命名ルールを指定することができます。これらのオプションを使用すると、命名規則を確立し、表示名、ディレクトリ名、およびエイリアスのプロパティの標準値を迅速に生成することができます。Exchange では、いくつかの自動命名オプションとして、%First や %Last などの置換文字列が指定できます。

Exchange は、ディレクトリ名またはエイリアスを生成するときに、生成された値が他と重複しない固有のものであるかどうかをチェックします。生成された値が他と重複する場合、Exchange はその値を固有の値にするために値の最後にハイフン (-) と 2 桁の番号を付け加えます (そのような値は -01 から始まる)。Exchange は、表示名を生成するときに、その値が他と重複しない固有のものであるかどうかをチェックしません。

Exchange は、自動命名ポリシーとプロキシ生成のポリシーに関し、次に挙げる置換文字列をサポートしています。

% 最初の列	**関連付けられたユーザアカウントの First name（名）プロパティの値を示します。**
% 最終	関連付けられたユーザアカウントの Last name（姓）プロパティの値を示します。
%Initials	関連付けられたユーザアカウントの Initials（頭文字）プロパティの値を示します。
% 別名	メールボックスプロパティ Alias（エイリアス）の値を示します。
%DirNam	メールボックスプロパティ Directory name（ディレクトリ名）の値を示します。Exchange は、Microsoft Exchange のメールボックス用に電子メールアドレスを生成する際に、変数 %DirName を指定するプロキシ生成文字列をサポートしません。
% ユーザ名	関連付けられたユーザアカウントの User name（ユーザ名）プロパティの値を示します。

パーセント記号 (%) と置換文字列名の間に数値を指定することもできます。その数値は、置換文字列のうち何文字まで含めるかを示します。たとえば %2First は、ユーザアカウントの「 [First]」という名前プロパティの文字列の最初の 2 文字を示します。

各自動命名ルールまたはプロキシ生成ポリシーには、1 つ以上の置換文字列を含めることができます。また、各ルールの中で文字を特定の置換文字列のプレフィックスまたはサフィックスとして指定することもできます。たとえば、置換文字列 %Initials の後に付けるピリオドとスペース (.) などです。Exchange では、置換文字列のプロパティが空白の場合、そのプロパティのサフィックスを含めません。

たとえば、名前プロパティの [Display] に関して、次に示す自動命名ルールについて考えてみましょう。

```
%First %1Initials. %Last
```

名前プロパティの [First] が Susan、[Initials] が May、[Last] が Smith だった場合、Exchange は名前プロパティの [Display] を「Susan M. Smith」に設定します。

名前プロパティの [First] が Michael、[Initials] が空白、[Last] が Jones だった場合、Exchange は名前プロパティの [Display] を「Michael Jones」に設定します。

メールボックス自動命名ポリシーの指定

メールボックス自動命名オプションを指定するには、Manage Policies and Automation Triggers という組み込みの役割に含まれている権限のような、適切な権限が必要です。また、ご使用のライセンスが Exchange 製品をサポートしている必要があります。

メールボックス自動命名ポリシーを指定するには :

1 [[Policy and Automation Management]] > [[Configure Exchange Policies (Exchange ポリシーを設定)]] > [[Alias naming (エイリアスの命名)]] の順に選択します。
2 適切な名前生成情報を指定します。
3 [[Enforce alias naming rules during mailbox updates (メールボックスの更新中にエイリアス命名ルールを強制する)]] を選択します。
4 [[OK]] をクリックします。

リソースの命名ポリシーの指定

リソース自動命名オプションを指定するには、Manage Policies and Automation Triggers という組み込みの役割に含まれている権限のような、適切な権限が必要です。また、使用しているライセンスが Exchange 製品をサポートしている必要があります。

リソースの命名ポリシーを指定するには :

1 [[Policy and Automation Management]] > [[Configure Exchange Policies (Exchange ポリシーを設定)]] > [[Resource naming (リソースの命名)]] の順に選択します。
2 適切なリソース名生成情報を指定します。
3 [[Enforce resource naming rules during mailbox updates (メールボックスの更新中にリソース命名ルールを強制する)]] を選択します。
4 [[OK]] をクリックします。

アーカイブの命名ポリシーの指定

アーカイブ自動命名オプションを指定するには、Manage Policies and Automation Triggers という組み込みの役割に含まれている権限のような、適切な権限が必要です。また、使用しているライセンスが Exchange 製品をサポートしている必要があります。

アーカイブの命名ポリシーを指定するには :

1 [[Policy and Automation Management]] > [[Configure Exchange Policies (Exchange ポリシーを設定)]] > [[Archive naming (アーカイブの命名)]] の順に選択します。
2 ユーザアカウントに対する適切なアーカイブ名生成情報を指定します。
3 [[Enforce archive naming rules during mailbox updates (メールボックスの更新中にアーカイブ命名ルールを強制する)]] を選択します。
4 [[OK]] をクリックします。

14 タスク前とタスク後のトリガ自動化

自動化トリガは、スクリプトまたは実行ファイルを 1 つ以上の操作と関連付けるルールです。そのスクリプトまたは実行ファイルを通じて、既存のワークフローを自動化したり、DRA と他のデータリポジトリとの間に情報の橋をかけたりすることができます。自動化トリガを使用すると、DRA が提供する機能とセキュリティが拡張できます。

自動化トリガを定義するときには、ルールパラメータを設定し、どの操作をそのトリガと関連付けるか、どのスクリプトまたは実行可能ファイルを実行するか、および (該当する場合は) どの ActiveView またはアシスタント管理者をそのトリガと関連付けるかを設定します。これらのルールは、管理サーバがトリガをどのように適用するかを決定します。

また、トリガについて取り消しスクリプトまたは実行ファイルを指定することもできます。**取り消しスクリプト**を使用すれば、操作が失敗したときに変更をロールバックできます。

DRA では、VBscript と PowerShell の各スクリプトをサポートします。

管理サーバはプロセスをどのように自動化するか

DRA では、ActiveView のルールベースの管理に加えて、既存のワークフローを自動化し、自動化トリガを通じて関連タスクを自動的に実行することができます。既存のワークフローを自動化すると、会社の能率化に寄与するとともに、より優れたサービスをより早く提供することができます。

管理サーバは、自動化トリガに関連付けられた操作を実行するときに、トリガスクリプトまたは実行ファイルも実行します。トリガがタスク前トリガの場合、そのスクリプトまたは実行ファイルは操作が実行される前に実行されます。トリガがタスク後トリガの場合、そのスクリプトまたは実行ファイルは操作が実行された後に実行されます。このプロセスをトランザクションと呼びます。**トランザクション**は、管理サーバが実行する各タスク (つまり操作) の実装サイクル全体を表します。トランザクションには、操作を完了するために必要なアクションと、その操作が失敗した場合に管理サーバが実行するべき取り消しアクション (もしあれば) が含まれます。

管理サーバは、自動化トリガが実行されるたびにそのトリガのステータスを監査ログに記録します。これらのログエントリは、戻りコード、関連する操作、操作対象オブジェクト、およびトリガスクリプトの実行が成功したかどうかを記録します。

警告 : 自動化トリガは、管理サーバサービスアカウントを使って実行されます。サービスアカウントは管理者権限を持っているので、ポリシーと自動化トリガはすべての会社データへの完全なアクセス権を持っています。自動化トリガを定義するには、Manage Policies and Automation Triggers という組み込みの役割に含まれている権限のような、適切な権限が必要です。これらの自動化トリガは、サービスアカウントのセキュリティコンテキストの

中で実行されます。したがって、Manage Policies and Automation Triggers という組み込みの役割に関連付けられたアシスタント管理者が、意図より大きな権限を持つ可能性があります。

自動化トリガの実装

自動化トリガを実装するには、まずトリガスクリプトまたは実行ファイルを作成する必要があり、さらに Manage Policies and Automation Triggers という組み込みの役割に含まれている権限のような、適切な権限が必要です。

カスタムトリガを正しく実装するには、特定の操作 (管理タスク) の最中に実行されるスクリプトを作成する必要があります。実行ファイルまたはスクリプトを操作に関連付けできます。DRA は、32 ビット PowerShell スクリプトと 64 ビット PowerShell スクリプトの両方をサポートしています。トリガを操作が実行される前 (タスク前) に適用するか後 (タスク後) に適用するかを指定できます。トリガスクリプトでは、トリガが失敗したときに表示されるエラーメッセージを定義することができます。また、Create Automation Trigger ウィザードでデフォルトのエラーメッセージを指定することもできます。

カスタムトリガの作成、管理操作のリスト表示、および引数配列の使用については、「*SDK*」を参照してください。

注

- カスタム自動化トリガをアシスタント管理者および ActiveView と関連付ける前に、まずそのアシスタント管理者がその ActiveView に割り当てられているか確認してください。
- カスタムトリガスクリプトまたは実行可能ファイルのパスにスペースが含まれている場合は、パス全体を引用符 (") で囲んでください。
- 現在、**[UserSetInfo]** 操作がスクリプト自動化トリガに使用され、ユーザ属性が変更された場合 (トリガを実行している場合)、ユーザオブジェクトに対して［ **[Find Now (今すぐ検索)]**］操作が実行されるまでは、変更された属性はエンタープライズ全体に増殖されません。

自動化トリガを実装するには :

1. トリガスクリプトまたは実行可能ファイルを書き込みます。
2. 管理対象ドメイン内で **[Manage Policies and Automation Triggers]** という組み込みの役割が割り当てられているアカウントを使って、DRA クライアントコンピュータにログオンします。
3. Delegation and Configuration console (委任および環境設定コンソール) を起動します。
4. プライマリ管理サーバに接続します。
5. トリガファイルを DRA プライマリおよびセカンダリサーバにアップロードするために ファイルのレプリケーションを使用します。

   フォルダパスは、管理対象ドメイン内のすべての DRA サーバにすでに存在している必要があります。ファイルを含むこのパスは、自動化トリガウィザードの **[実行ファイルパス]** で使用されます。

6 左側のペインで、[Policy and Automation Management] を展開します。

7 ［ [Automation Triggers (自動化のトリガ)]］をクリックします。

8 ［タスク］メニューで［ [New Trigger (新規のトリガ)]］をクリックします。

9 各ウィザードウィンドウで適切な値を指定して［ [次へ]］をクリックします。たとえば、この新しいトリガを特定の ActiveView に関連付けて、その ActiveView に含まれるオブジェクトをアシスタント管理者が管理するときにこのトリガが適用されるようにすることができます。

10 サマリの内容を確認し［ [完了]］をクリックします。

重要 : ActiveView の間にカンマを追加することにより、トリガに対して 1 つ以上の ActiveView を構成している場合、DRA の新しいバージョンにアップグレードすると、それらの ActiveView がトリガで分岐し、トリガは実行されません。アップグレード後に操作を実行するには、トリガを再構成するか、新しいトリガを作成する必要があります。

---

15 自動ワークフロー

ワークフローの自動化を使用すると、カスタマイズしたワークフローフォームを作成することで IT プロセスが自動化できます。これらのフォームが、ワークフローを実行したときに、またはワークフロー自動化サーバで作成される名前付きワークフローイベントがトリガとなって発生したときに作動します。ワークフローフォームを作成するときは、フォームを表示できる管理者グループを定義します。フォーム送信またはワークフロープロセスの実行は、ワークフローフォーム作成時に含まれているグループに委任された権限に依存します。

ワークフローフォームは、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しているアシスタント管理者は、フォームの設定の仕方に基づいて、フォームにアクセスできます。フォームは一般的に Web サーバの資格情報を持つすべてのユーザが利用可能です。特定のフォームへのアクセスを制限するには、アシスタント管理者のグループを追加してから他のユーザに対しそのフォームを非表示に設定します。フォーム送信ができるようにするには、次に示す権限のうち 1 つが必要です。

- ワークフローイベントを作成しすべてのプロパティを変更する
- ワークフローの開始

ワークフローフォームの起動するには : ワークフローは、Delegation and Configuration Console (委任および環境設定コンソール) 経由で DRA と統合されたワークフロー自動化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［**[イベントによるワークフローのトリガ]**］または［**[特定のワークフローの起動]**］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要求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。

既存の要求を変更したり、新しい要求を作成したりできます。既存の要求を変更するには、［**[タスク]**］> ［**[要求]**］に移動します。

ワークフロー要求を作成するには、［**[管理]**］> ［**[カスタマイズ]**］> ［**[要求]**］に移動します。

要求を作成するには、次の基本手順に従います。

1. フォームが送信されたときに*指定のワークフロー*を実行するように要求を設定するか、事前定義された*名前付きイベント*がトリガとして発生したときに実行するように要求を設定します。
2. ワークフロープロセスに含まれているアシスタント管理者グループを選択し、[**[全般]**] タブで［ **[フォームは非表示]**］というオプションを有効にして、このようなユーザへのフォームによるアクセスを制限します。
3. プロパティフィールドが必要な場合やプロパティページを追加する必要があれば、それをフォームに追加します。
4. 該当する場合は、カスタムハンドラを作成してワークフローのプロセスとその実行方法をさらに詳しく定義してください。

   注 : カスタムハンドラのオプションは、要求が最初に保存されるまで、新しいワークフロー要求として表示されません。[**[フォームプロパティ]**] でカスタムハンドラをアクセス、作成、および変更します。

   ---

5. ユーザがフォームを表示できるようにするには、[**[フォームは非表示]**] オプションを無効にします。

Workflow Automation サーバの設定の詳細については、「ワークフロー自動化サーバの設定」を参照してください。ワークフロー要求のカスタマイズについては、「要求フォームのカスタマイズ」を参照してください。

VI 監査とレポート

ユーザアクションの監査は、確固としたセキュリティ対策を実施する上で最も重要な要素です。アシスタント管理者のアクションを確認しレポートできるように、DRA はユーザによるすべての操作を管理サーバのコンピュータ上にログアーカイブとして記録しています。DRA は、監査対象イベントの前と後の値を含む明確で包括的なレポートを提供し、何が変わったかを正確に把握する手助けをします。

16 監査アクティビティ

イベントログ内の動作記録を監査することは、環境で発生した問題の隔離、診断、解決に役立ちます。このセクションでは、イベントログ機能の有効化と理解に役立つ情報やログアーカイブの使用方法を記載しています。

ネーティブの Windows イベントログ

アシスタント管理者のアクションを確認しレポートできるように、DRA はユーザによるすべての操作を管理サーバのコンピュータ上にログアーカイブとして記録しています。ユーザによる操作には、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、定義を変更するすべての操作が含まれます。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。

Windows イベントログでの DRA 監査の有効化 / 無効化

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。

イベントの監査を有効にするには、次の手順を実行します。

1 ［**[スタート]** > ［**ファイル名を指定して実行]**］の順にクリックします。

2 [[開く]] フィールドに「regedit」と入力し、[[OK]] をクリックします。

3 展開するレジストリキー : HKLM\Software\WOW6432Node\Mission Critical Software\OnePoint\Administration\Modules\ServerConfiguration\.

4 [[編集] > [新規] > [DWORD 値]] の順にクリックします。

5 「IsNTAuditEnabled」と入力します。

6 [[編集] > [修正]] の順にクリックします。

7 [[Value data (値のデータ)]] フィールドに「1」と入力し、[[OK]] をクリックします。

8 レジストリエディタを終了します。

イベントの監査を無効にするには、次の手順を実行します。

1 [[スタート] > [ファイル名を指定して実行]] の順にクリックします。

2 [[開く]] フィールドに「regedit」と入力し、[[OK]] をクリックします。

3 展開するレジストリキー : HKLM\Software\WOW6432Node\Mission Critical Software\OnePoint\Administration\Modules\ServerConfiguration\.

4 IsNTAuditEnabled キーを選択します。

5 [[編集] > [修正]] の順にクリックします。

6 [[Value data (値のデータ)]] フィールドに「0」と入力し、[[OK]] をクリックします。

7 レジストリエディタを終了します。

監査の整合性の確保

DRA は、すべてのユーザアクションが監査されるようにするために、製品がログ活動を検証できないときに代替ログ手段を提供します。DRA をインストールすると、次のアクションが実行されるようにするために、AuditFailsFilePath キーおよびパスがレジストリに追加されます。

- DRA が監査イベントがログアーカイブに記録されていないことを検出した場合は、監査イベントを管理サーバ上のローカルファイルに記録する。
- 監査イベントをローカルファイルに書き込めない場合、DRA は Windows イベントログに監査イベントを書き込む。
- 監査イベントを Windows イベントログに書き込めない場合、DRA は監査イベントを DRA のログに書き込む。
- 監査イベントがログに記録されていないことを検出した場合、DRA はそれ以降のユーザー操作をブロックする。

ログアーカイブが使用不能の場合に書き込み操作を有効にするには、AllowOperationsOnAuditFailure キーのレジストリキー値も設定する必要があります。

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。

書き込み操作を有効にするには :

1 ［[スタート］>［ファイル名を指定して実行]］の順にクリックします。
2 ［[開く]］フィールドに「regedit」と入力し、［[OK]］をクリックします。
3 レジストリを展開します。レジストリキー : HKLM\Software\WOW6432Node\Mission Critical Software\OnePoint\Administration\Audit\
4 ［[編集］>［新規］>［DWORD 値]］の順にクリックします。
5 キー名には「AllowOperationsOnAuditFailure」と入力します。
6 ［[編集］>［修正]］の順にクリックします。
7 ［[Value data (値のデータ)]］フィールドに「736458265」と入力します。
8 ［[Base (基数)]］フィールドで［[Decimal (10 進)]］を選択し、［[OK]］をクリックします。
9 レジストリエディタを終了します。

ログアーカイブについて

DRA は、ユーザアクティビティのデータを管理サーバ上のログアーカイブに記録します。DRA は毎日、その日に収集されて標準化されたデータを保存するために日ごとのログアーカイブパーティションを作成します。DRA は、毎日のログアーカイブパーティションの命名に、管理サーバのローカル時間による日付 (*YYYYMMDD*) を使用します。

管理レポートコレクタが有効になっている場合、DRA はログアーカイブデータを DRA 管理レポートのソースとして SQL サーバのデータベースにエクスポートします。

初期状態では、DRA はデフォルトでログデータをログアーカイブ内に無期限に保持します。この状態では、ログアーカイブのサイズが、インストール時にハードドライブ容量に基づいて決定された最大サイズに達する可能性があります。ログアーカイブがこの最大サイズを超過すると、新規の監査イベントが保存されなくなります。データを保持する期間の制限を設定することができます。時間制限を設定すると、グルーミングと呼ばれるプロセスを通じてデータが古い順に削除されて新しいデータのための場所が確保されるようになります。グルーミングを有効にする前に、バックアップ戦略を確立してください。ログアーカイブ保持期間を設定するには、Log Archive Configuration ユーティリティを使用します。詳細については、「ログアーカイブのグルーミング設定の変更」を参照してください。

Log Archive Viewer ユーティリティの使用

ログアーカイブファイルに保存されたデータを表示するには、Log Archive Viewer ユーティリティを使用します。NetIQ DRA の LARK (Log Archive Resource Kit) は、DRA でインストールするよう選択できますが、Log Archive Viewer ユーティリティを提供します。詳細については、『*NetIQ DRA Log Archive Resource Kit Technical Reference*』を参照してください。

ログアーカイブファイルのバックアップ

[ログアーカイブファイル] とは、レコードブロックの集まりです。ログアーカイブファイルは物理データベースの外にある圧縮されたバイナリファイルなので、ログアーカイブをバックアップするのに Microsoft SQL Server Management Studio を使用する必要はありません。自動化されたファイルバックアップシステムを使用している場合は、ログアーカイブファイルも他のファイルと同様に自動的にバックアップされます。

バックアップ戦略を計画するときには、次のベストプラクティスを頭に置いてください。

- イベントデータを保存するために、1 日に 1 つのパーティションが作成されます。グルーミングを有効にすると、デフォルトの設定で、Log Archive Service がこれらのパーティションからのデータを 90 日ごとに自動的にグルーミングします。バックアップ戦略では、バックアップの頻度を決めるときにグルーミングのスケジュールを考慮に入れる必要があります。ログアーカイブパーティションがグルーミングされるときに、DRA はバイナリファイルを削除します。グルーミングされたデータを取り戻すことはできません。グルーミングされたデータは、バックアップから復元するしかありません。詳細については、「ログアーカイブのグルーミング設定の変更」を参照してください。
- パーティションのバックアップは、そのパーティションが閉じられた後にのみ行ってください。通常の状態では、パーティションは夜中に日付が変わってから 2 時間以内に閉じられます。
- パーティションフォルダとそのすべてのサブフォルダを、1 つの単位としてバックアップしてください。パーティションバックアップの一環として、VolumeInfo.xml というファイルをバックアップします。
- レポート用にログアーカイブパーティションを復元する場合は、バックアップされたログアーカイブが元のままの形式を保っているか、または元の形式に復元できることを確認してください。
- ログアーカイブファイルをバックアップするプロセスを設定するときには、NetIQ では、メインのログアーカイブフォルダにある index_data と CubeExport の両サブフォルダを除外することを推奨しています。これらは一時データが収められるサブフォルダなので、バックアップするべきではありません。

ログアーカイブのグルーミング設定の変更

DRA のインストール時に、ログアーカイブのグルーミングはデフォルトで無効にされます。ログアーカイブファイルの定期的なバックアップ手順を確立する場合は、ディスクスペースがいっぱいにならないようにログアーカイブのグルーミングを有効にする必要があります。ログアーカイブパーティションがグルーミングされるまでの日数は、Log Archive Configuration を使って変更できます。

ログアーカイブパーティションがグルーミングされるまでの日数を変更するには、次の手順を実行します。

1. ローカルの管理者グループのメンバーであるアカウントを使用して、管理サーバにログオンします。
2. NetIQ 管理プログラムグループ内の [Log Archive Configuration] を起動します。
3. [[Log Archive Server Settings (ログアーカイブサーバーの設定)]] をクリックします。

4 *パーティションのグルーミングを有効にする場合*は、[**[Partition Grooming Enabled (パーティショングルーミングが有効)]**] フィールドの値を「True」に設定します。

5 グルーミングされるまでログアーカイブパーティションを保持する日数を [**[Number of Days before Grooming (グルーミングまでの日数)]**] フィールドに入力します。

6 [**[適用]**] をクリックします。

7 [**[はい]**] をクリックします。

8 [**[閉じる]**] をクリックします。

9 *NetIQLogArchiveData*\<*Partition Name*> フォルダのパスの場所を見つけます。これは通常の場合、C:\ProgramData\NetIQ\DRA\NetIQLogArchiveData です。

指定されたパーティション内のファイルまたはフォルダに対して「File is ready for archiving」という属性が (ファイルまたはフォルダプロパティで) 選択されていない場合、ログアーカイブのグルーミングが有効になるように CONFIG ファイルを編集する必要があります。この属性が選択された理由、または選択されなかった理由を理解するためには、ナレッジベースの記事の「*How do you configure the data retention period for DRA Logarchival Data? (DRA ログアーカイブデータのデータ保持期間の設定方法)*」の「**Additional Information (追加情報)**」セクションを参照してください。

値	
オン	確認メッセージに対して [**[はい]**] をクリックして NetIQ Security Manager Log Archive サービスを再起動します。 **注 :** ログアーカイブの設定を何か変更した場合、その変更を有効にするにはログアーカイブサービスを再起動する必要があります。
チェックなし	確認メッセージで [**[いいえ]**] をクリックします。詳細については、「アーカイブされなかったデータをグルーミングするために DRA のログアーカイブサーバを有効にするには :」を参照してください。

アーカイブされなかったデータをグルーミングするために DRA のログアーカイブサーバを有効にするには :

1 ローカル管理者グループのメンバーとして、DRA サーバのウィンドウコンソールそれぞれにローカルにログオンします。

2 テキストエディタを使用して「C:\ProgramData\NetIQ\Directory Resource Administrator\LogArchiveConfiguration.config file and locate the <Property name="GroomUnarchivedData" value="false" />」という行を開きます。

3 値の "false" を "true" に変更し、ファイルを保存します。

4 NetIQ DRA LogArchive サービスを再起動します。

注 : ログアーカイブの設定を何か変更した場合、その変更を有効にするにはログアーカイブサービスを再起動する必要があります。

17 レポーティング

このセクションでは、DRA のレポート機能の理解と有効化、データ収集のレポート生成、ActiveView アナライザの収集とレポート、および組み込みレポートの利用に関して説明します。

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。

ネットワークの変更に関する最新の詳細情報を提供するために DRA をインストールすると、アクティビティ詳細レポートを Delegation and Configuration console (委任および環境設定コンソール) ですぐに使用できるようになります。

- 185 ページの 「レポート用のデータ収集の管理」
- 187 ページの 「組み込みのレポート」

レポート用のデータ収集の管理

DRA Reporting は、環境内の最新の変化を知り、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確認できるように、2 種類のレポート生成方法を提供しています。

Activity Detail レポート

Delegation and Configuration console (委任および環境設定コンソール) からアクセスした場合、これらのレポートにドメイン内のオブジェクトに関する変更内容がリアルタイムで表示されます。

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 の定義やアシスタント管理者グループの定義など、DRA セキュリティモデルに関する詳細を表示することもできます。

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、「レポーティング環境設定」を参照してください。

コレクタのステータスの表示

［Collectors Status (コレクタのステータス)］タブで各データコレクタの詳細が確認できます。

コレクタのステータスを表示するには :

1 ［ **[Configuration Management]**］を展開し、**[［Update Reporting Service Configuration (レポーティングサービスの設定を更新)]]** をクリックします。

2 ［Collectors Status (コレクタのステータス)］タブで各エントリをクリックすると、データが最後に収集された日時や最後のデータ収集が成功したかどうかなど、データ収集に関する追加情報が表示されます。

3 ［サーバ］リストにデータが表示されない場合は［ **[更新]**］をクリックしてくださいい。

レポート生成とデータ収集の有効化

DRA Reporting のコンポーネントをインストールした後に、Reporting Center のレポートにアクセスするために、レポート生成のデータ収集を有効にして設定を行ってください。

レポート生成とデータ収集を有効にするには :

1 ［ **[Configuration Management]**］> ［ **[Update Reporting Service Configuration (レポーティングサービスの設定を更新)]**］の順に選択します。

2 ［SQL サーバ］タブで［ **[Enable DRA Reporting support (DRA レポーティングのサポートを有効にする)]**］を選択します。

3 ［サーバ名］フィールドで［ **[参照]**］をクリックし、SQL Server がインストールされているコンピュータを選択します。

4 ［資格情報］タブで、SQL Server に対する操作に使用する適切な資格情報を指定します。

5 データベースの作成とスキーマの初期化に使用できるものと同じアカウントを使用する場合は、［Use the above credentials for creating a database and initializing the database schema (上の資格情報をデータベース作成とデータベーススキーマの初期化に使用する)］チェックボックスを選択します。

6 データベース作成用のアカウントとは別のアカウントを指定する場合は、[Admin Credentials (管理者資格情報)] タブでそのユーザアカウントとパスワードを指定します。

7 [[OK]] をクリックします。

特定のコレクタを設定する方法の詳細については、「レポーティング環境設定」を参照してください。

組み込みのレポート

組み込みのレポートで、オブジェクトの変更、オブジェクトのリスト、およびオブジェクトの詳細に関する各レポートを生成できます。これらのレポートは、DRA Reporting Services の一部ではないため、ビルトイン変更履歴レポートを有効にするために設定する必要はありません。これらのレポートのアクセス方法については、このセクションのトピックを参照してください。

注 : DRA が Change Guardian に統合されている場合は、DRA の外部からのイベントに対する変更履歴レポートにアクセスすることもできます。これらのレポートの種類、および Change Guardian サーバの設定に関する詳細については、「115 ページの 「統合された変更履歴サーバの設定」」を参照してください。

オブジェクトの変更に関するレポート

Activity Detail レポートを生成することで、ドメイン内のオブジェクトに関する変更情報をリアルタイムで確認できます。たとえば、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がリスト表示されます。Activity Detail レポートはエクスポートや印刷することもできます。

オブジェクトの変更のレポートを生成するには :

1 所望の条件に一致するオブジェクトを検索します。

2 オブジェクトを右クリックして、[[レポーティング] > [次に対して行われた変更 ...objectName]] (または [[Reporting] > [次によって行われた変更 ...objectName]]) の順に選択します。

3 変更を表示する期間の開始日と終了日を選択します。

4 *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。

---

5 *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。

6 [[OK]] をクリックします。

オブジェクトリストのレポート

オブジェクトのリストからデータをエクスポートおよび印刷することができます。この機能により、管理対象オブジェクトの一般情報に関するレポートの生成や配布が素早く簡単にできます。

オブジェクトリストをエクスポートする場合は、ファイルの場所、名前、および形式を指定することができます。DRA では、HTML、CSV、XML の各形式がサポートされています。オブジェクトの一般情報をデータベースアプリケーションにエクスポートすることも、リスト出力の結果を Web ページに投稿することもできます。

注 : リスト内の複数の項目を選択して項目をメモ帳などのテキストアプリケーションにコピーすることもできます。

オブジェクトのリストを表示するには :

1. 所望の条件に一致するオブジェクトを検索します。
2. このオブジェクトのリストをエクスポートするには、［ファイル］メニューから［**[Export List (リストをエクスポート)]**］をクリックします。
3. このオブジェクトのリストを印刷するには、［ファイル］メニューから［ **[Print List (リストを印刷)]**］をクリックします。
4. 適切な情報を指定して、このリストを保存または印刷します。

オブジェクトの詳細に関するレポート

グループメンバーシップなど、オブジェクト属性をリスト表示する詳細タブからデータをエクスポートおよび印刷することができます。この機能により、特定のオブジェクトに関し必要な詳細情報を素早く簡単に頻繁にレポート生成および配布することができます。

オブジェクトの詳細のタブをエクスポートする場合は、ファイルの場所、名前、および形式を指定することができます。DRA では、HTML、CSV、XML の各形式がサポートされています。オブジェクトの一般情報をデータベースアプリケーションにエクスポートすることも、リスト出力の結果を Web ページに投稿することもできます。

オブジェクトの詳細のレポートを生成するには :

1. 所望の条件に一致するオブジェクトを検索します。
2. ［表示］メニューの［ **[詳細]**］をクリックします。
3. 詳細ペインで適切なプロセスを選択します。
4. これらのオブジェクト詳細情報をエクスポートするには、［ファイル］メニューの［ **[Export Details List (詳細情報のリストをエクスポート)]**］をクリックします。
5. これらのオブジェクト詳細情報を印刷するには、［ファイル］メニューの［ **[Print Details List (詳細情報のリストを印刷)]**］をクリックします。
6. 適切な情報を指定して、このリストを保存または印刷します。

VII その他の機能

一時グループ割り当て、ダイナミックグループ、イベントスタンプ、および BitLocker 回復パスワードは、個々の企業環境に導入できる DRA の追加機能です。

18 一時グループ割り当て

DRA では、権限を与えられたユーザが一時的にリソースにアクセスすることを可能にする一時グループ割り当てが使用できます。アシスタント管理者は、一時グループ割り当て機能を使用して指定期間のみターゲットグループにユーザを割り当てることができます。指定の期間が終了すると、DRA はそのユーザをグループから自動的に除外します。

Manage Temporary Group Assignments という役割により、アシスタント管理者は一時グループ割り当ての作成と管理を行う権限を持ちます。

アシスタント管理者がメンバーを追加または削除する権限を持っているグループに対する一時的なグループの割り当てのみを表示することができます。

次に示す権限を使用して、一時グループ割り当ての作成および管理を委任します。

- 一時グループ割り当てを作成する
- 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を変更する
- 一時的なグループの割り当て状態をリセットする
- 一時的なグループの割り当てを表示する
- オブジェクトをグループに追加する
- オブジェクトをグループから削除する

ターゲットグループおよびユーザは、同じ ActiveView に所属している必要があります。

注

- すでにターゲットグループのメンバーになっているユーザに対しては一時グループ割り当てを作成できません。すでにターゲットグループのメンバーになっているユーザに対しては一時グループ割り当てを作成しようとしても、DRA に警告メッセージが表示され、そのユーザには一時グループ割り当てが作成できません。
- ターゲットグループのメンバーではないユーザに一時グループ割り当てを作成した場合、一時グループ割り当ての期間が終了した時点で DRA がそのユーザをグループから削除します。

例 :

人事マネージャのボブは、プロジェクトを完了するために特定の期間、ジョーという臨時社員と契約をしたことをヘルプデスク管理者のジョンにお知らせします。ジョンは次のことを行います。

- 一時的なグループの割り当て (TGA) を作成します。
- 臨時社員の人事グループを TGA に追加します。

- ジョーを臨時社員グループのメンバーとして追加します。
- TGA 期間を 1 カ月に設定します (2019 年 7 月 3 日から 2019 年 8 月 2 日)

予期された結果 :

デフォルトでは、TGA が期限切れになると、ジョーのメンバーシップは人事グループから削除されます。[**[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]**] オプションをジョンが選択した場合を除き、TGA は 7 日間利用できます。

一時的なグループの割り当ての作成や使用の詳細については、『*DRA ユーザガイド*』を参照してください。

19 DRA のダイナミックグループ

ダイナミックグループとは、グループプロパティで設定しておいた定義済み条件セットに基づいてメンバーシップが変わるグループです。どのグループでもダイナミックにすることができ、設定したグループのいずれからでもダイナミックフィルタを削除することができます。この機能は、グループメンバーをスタティックリストや除外リストに追加する場合に使用することもできます。これらのリストに含まれるグループメンバーに、ダイナミックの条件による影響はありません。

ダイナミックグループを正規のグループに戻すと、スタティックメンバーのリスト内のすべてのメンバーがグループメンバーシップに追加され、除外されたメンバーおよびダイナミックフィルタは無視されます。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、既存のグループをダイナミックにしたり、新規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を作成するには :

1 該当するコンソールでグループを探します。

- Delegation and Configuration: ［ **[すべての管理対象オブジェクト]**］> ［ **[Find Now (今すぐ検索)]**］の順に選択します。

  注 : クエリビルダを有効にするには、［ **[検索]**］をクリックし、ドメイン、コンテナ、または OU を選択します。

- Web コンソール : ［ **[管理]**］> ［ **[検索]**］の順に選択します。

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］タブで［ **[グループをダイナミックにする]**］を選択します。

3 必要な LDAP と仮想属性を追加してグループメンバーシップをフィルタします。

4 任意の必要なスタティックメンバーや除外メンバーをダイナミックグループに追加し、変更を適用します。

新しいダイナミックグループを作成するには :

- **Delegation and Configuration:**［すべての管理対象オブジェクト］でドメインまたはサブノードを右クリックし、［ **[新規]**］> ［ **[ダイナミックグループ]**］の順に選択します。
- **Web コンソール :** ［ **[管理]**］> ［ **[作成]**］> ［ **[新しいダイナミックグループ]**］の順に選択します。

20 イベントスタンプの仕組み

オブジェクト タイプに属性を設定し DRA がサポートする操作のうちの 1 つを実行すると、その操作を誰が行ったかなど、DRA 固有の情報がその属性に追加されて (スタンプが押されて) 更新されます。これにより、AD がその属性変更に関する監査イベントを生成します。

例として、extensionAttribute1 という属性をユーザ属性に選択し、AD DS 監査を設定していた場合を考えてみましょう。アシスタント管理者がユーザを更新するたびに、DRA は extensionAttribute1 という属性をイベントスタンプのデータを使って更新します。つまり、アシスタント管理者が更新した各属性の AD DS イベント (たとえば、説明や名前など) に加えて、extensionAttribute1 属性のために追加の AD DS イベントが存在することになります。

これらのイベントのそれぞれに、相関性 ID が含まれます。この ID は、ユーザが更新されたときに変更された各属性のものと同一です。こうして、アプリケーションがイベントスタンプのデータと更新された別の属性を関連付けることができるのです。

イベントスタンプを有効にする手順については、「DRA でイベントスタンプを有効にする」を参照してください。

AD DS イベントとサポートされる操作タイプの例については、次を参照してください。

- 195 ページの 「AD DS イベント」
- 196 ページの 「サポートされている操作」

AD DS イベント

このようなイベントは、DRA がサポート対象の操作を実行したときにいつでも、Windows ログのセキュリティで確認することができます。

LDAP の表示名 :	**extensionAttribute1**
構文 (OID): 2.5.5.12	2.5.5.12
値 :	<dra-event **user**="DRDOM300\drauseradmin" **sid**="S-1-5-21-53918190-1560392134-2889063332-1914" **tid**="E0E257E6B4D24744A9B0FE3F86EC7038" **SubjectUserSid**="S-1-5-21-4224976940-2944197837-1672139851-500" **ObjectDN**="CN=admin_113,OU=Vino_113,DC=DRDOM113,DC=LAB"/ >+a+02ROO+bJbhyPbR4leJpKWCGTp/ KXdqI7S3EBhVyniE7iXvxIT6eB6IdcXQ5StkbIAHJgKzLN5FCOM5fZcITxyAPLWhbstaA7ZA0VbVC9MGlVIaAcjl3z7mpF9GKXsfDogbSeNlmHliXvH5KpOX3/29AKMPj/zvf6Yuczoos=

イベントの値は、2 つの部分で構成されています。1 つ目はイベントスタンプのデータを含んだ XML 文字列です。2 つ目はデータの署名です。これはデータが実際に DRA によって生成されたことを検証するために使用できます。署名を認証するには、アプリケーションがその署名の公開鍵を持っている必要があります。

XML の文字列は、次に示す情報で構成されています。

User	操作を実行したアシスタント管理者
Sid	操作を実行したアシスタント管理者の SID
Tid	各イベントを一意にするための DRA 監査トランザクションの ID
SubjectUserSid	実際に AD を更新した DRA サービスアカウントまたはアクセスアカウントの SID
ObjectDN	変更されたオブジェクトの識別名

サポートされている操作

ユーザ	◆ 作成 ◆ 名称変更 ◆ 変更 ◆ クローン作成
グループ	◆ 作成 ◆ 名称変更 ◆ 変更 ◆ クローン作成
連絡先	◆ 作成 ◆ 名称変更 ◆ 変更 ◆ クローン作成
コンピュータ	◆ 作成 ◆ 有効化 ◆ 無効化 ◆ 名称変更 ◆ 変更
部門	◆ 作成 ◆ 名称変更 ◆ クローン作成

21 BitLocker 回復パスワード

Microsoft BitLocker は回復パスワードを Active Directory に格納します。BitLocker 回復という DRA の機能を使用すると、アシスタント管理者にエンドユーザが紛失した BitLocker パスワードを見つけて復旧できるように権限を委任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、必ず、使用するコンピュータをドメインに割り当てて、BitLocker をオンにしてください。

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。

回復パスワードを表示およびコピーするには :

1. [Delegation and Configuration] コンソールを起動し、ツリービュー構造を展開します。
2. [[Account and Resource Management]] ノードで、[[すべての管理対象オブジェクト]] > [[ドメイン]] > [[コンピュータ]] の順に選択します。
3. 必要なコンピュータをコンピュータリストから右クリックし、[[プロパティ]] を選択します。
4. [[BitLocker 回復パスワード]] タブをクリックして BitLocker の回復パスワードを表示します。
5. BitLocker の回復パスワードを右クリックし、[[コピー]] をクリックしてから、必要なテキストファイルやスプレッドシートに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。

注 : 回復パスワードを検索するには、アシスタント管理者が、委任されたコンピュータオブジェクトを含むドメインに対して [BitLocker 回復パスワードの表示] 権限を持っている必要があります。

パスワード ID を使用して回復パスワードを検索するには :

1. [Delegation and Configuration] コンソールを起動し、ツリービュー構造を展開します。
2. [[Account and Resource Management]] ノードで、[[すべての管理対象オブジェクト]] に移動し、[[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。

   回復パスワードの最初の 8 文字を検索するには、「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。

22 ごみ箱

そのようなドメイン内の Microsoft Windows ドメインまたはオブジェクトのそれぞれでごみ箱を有効または無効にして会社全体のアカウント管理をコントロールすることができます。ごみ箱を有効にしてからユーザアカウント、グループ、ダイナミック配布グループ、ダイナミックグループ、リソースメールボックス、連絡先、またはコンピュータアカウントを削除すると、選択されたアカウントは管理サーバが無効にして、ごみ箱コンテナに移動します。DRA がアカウントをごみ箱に移動すると後、そのアカウントは属していた ActiveView に表示されません。ごみ箱が無効であるときにユーザアカウント、グループ、連絡先、またはコンピュータアカウントを削除すると、選択されたアカウントを管理サーバが永久に削除します。以前に削除したアカウントの入ったごみ箱を無効にすることができます。ただし、ごみ箱を無効にすると、中に入っていたアカウントはそれ以降ごみ箱ノードから使用できません。

ごみ箱権限の割り当て

[すべての管理対象オブジェクト] ノードからアシスタント管理者がアカウントをごみ箱内を含め永久に削除できるようにするには、次に示すリストから関連の権限を割り当てます。

- アカウントを永久に削除する
- グループを永久に削除する
- コンピュータを永久に削除する
- 連絡先を永久に削除する
- ダイナミック配布グループを永久に削除する
- ダイナミックグループアカウントを永久に削除する
- リソースメールボックスを永久に削除する
- 共有メールボックスを永久に削除する
- Azure ユーザアカウントを永久に削除する
- グループ管理対象サービスアカウントを永久に削除する

複数の管理サーバが同じ Microsoft Windows ドメインの異なるサブツリーを管理している場合、どの管理サーバがそのアカウントを管理しているかを問わず、このドメインからごみ箱を使用して削除されたアカウントを確認することができます。

ごみ箱の使用

アカウントの永久消去、アカウントの復元、削除されたアカウントのプロパティ表示にごみ箱を使用します。特定のアカウントを検索することや、削除されたアカウントがごみ箱に入って経過した日数を追跡することもできます。[ごみ箱] タブは選択されたドメイン

の［プロパティ］ウィンドウにも含まれています。このタブから、ドメイン全体または特定のオブジェクトに対しごみ箱を無効または有効にでき、ごみ箱クリーンアップをスケジュールすることもできます。

Restore All または **Empty Recycle Bin** というオプションを使用して、これらのアカウントを素早く簡単に復元または削除します。

DRA では、アカウントを復元すると、アカウントのパーミッション、権限委任、ポリシー割り当て、グループメンバーシップ、および ActiveView メンバーシップなどがすべて回復します。アカウントを永久に削除すると、DRA はそのアカウントを Active Directory から削除します。

アカウントが確実に安全に削除されるために、次の権限を持つアシスタント管理者だけが、ごみ箱からアカウントを完全に削除できます。

- アカウントを永久に削除する
- ごみ箱からユーザを削除する
- グループアカウントを永久に削除する
- ごみ箱からグループを削除する
- コンピュータアカウントを永久に削除する
- ごみ箱からコンピュータを削除する
- 連絡先のアカウントを永久に削除する
- ごみ箱から連絡先を削除する
- ダイナミック配布グループを永久に削除する
- ごみ箱からダイナミック配布グループを削除する
- ダイナミックグループを永久に削除する
- ごみ箱からダイナミックグループを削除する
- リソースメールボックスを永久に削除する
- ごみ箱からのリソースのメールボックスを削除する
- 共有メールボックスを永久に削除する
- ごみ箱からの共有メールボックスを削除する
- すべてのごみ箱オブジェクトを表示する

ごみ箱からのアカウントを復元するには、アカウントを含む OU で、アシスタント管理者が次に示す権限を持っている必要があります。

- ごみ箱からユーザを復元する
- ごみ箱からグループを復元する
- ごみ箱からダイナミック配布グループを復元する
- ごみ箱からダイナミック グループを復元する
- ごみ箱からリソースのメールボックスを復元する
- ごみ箱から共有メールボックスを復元する
- ごみ箱からコンピュータを復元する

- ごみ箱から連絡先を復元する
- すべてのごみ箱オブジェクトを表示する

注

- アシスタント管理者のアカウントをごみ箱に削除した場合、DRA は引き続きこのアカウントに関する ActiveView と役割の割り当てを表示します。削除されたアシスタント管理者のアカウントの名前を表示する代わりに、DRA は SID(Security Identifier) を表示します。これらの割り当てを、アシスタント管理者のアカウントを完全に削除する前に削除することができます。
- ユーザアカウントをごみ箱から削除した後に、DRA がホームディレクトリを削除します。
- Office 365 ライセンスを持つユーザが削除された場合、そのユーザアカウントはごみ箱に移動し、そのライセンスは削除されます。削除後でユーザアカウントを復元した場合、Office 365 ライセンスも復元されます。

VIII クライアントのカスタマイズ

Delegation and Configuration クライアントおよび Web コンソールをカスタマイズすることができます。各クライアントに関しては、物理アクセスまたはリモートアクセスと、アカウント資格情報が必要です。コンソールに関しては、サーバの URL と、Web ブラウザからログインするためのアカウント資格情報が必要です。

23 Delegation and Configuration クライアント

このセクションは、Delegation and Configuration クライアントのカスタマイズに役立つ情報を記載しており、カスタムプロパティページの作成方法、ネットワーク上のクライアントおよびサーバコンピュータ上で実行できるカスタムツールを DRA で作成する方法、およびユーザインタフェースの設定をカスタマイズする方法などを理解するのに役立ちます。

プロパティページのカスタマイズ

カスタムプロパティを実装することで、Delegation and Configuration console (委任および環境設定コンソール) をカスタマイズおよび拡張できます。カスタムプロパティでは、Active Directory のスキーマ拡張と仮想属性など、独自のアカウントおよび OU のプロパティを特定のウィザードとプロパティウィンドウに追加できます。これらの拡張機能では、特定の要件が満足できるように DRA をカスタマイズ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) 内の［New Custom Page (新規のカスタムページ)］ウィザードで、カスタムページを素早く簡単に作成して適切なユーザインタフェースを拡張することができます。

カスタムページを安全に管理するために各アシスタント管理者が固有の権限を必要とする場合は、カスタム権限を作成および委任することもできます。たとえば、ユーザアカウントの管理をカスタムページ上のプロパティのみに制限するほうがよいでしょう。詳細については、「カスタム権限の実装」を参照してください。

カスタムプロパティページの仕組み

ユーザインタフェース拡張機能は、DRA が適切なウィザードとプロパティウィンドウで表示するカスタムページです。Active Directory の属性、スキーマ拡張および仮想属性を表示させるようにカスタムページを Delegation and Configuration console (委任および環境設定コンソール) で構成することができます。

サポート対象の Active Directory 属性、スキーマ拡張、または仮想属性を選択すると、次に示す方法でカスタムページを使用できます。

- アシスタント管理者を、明確に定義され制御された一連のプロパティに制限します。このプロパティセットには、*標準プロパティ*とスキーマ拡張を含めることができます。標準プロパティは、Accounts and Resource Management コンソールを通じてデフォルトで表示されている Active Directory の属性です。
- DRA が管理する標準プロパティではなく Active Directory 属性を表示させます。
- Delegation and Configuration console (委任および環境設定コンソール) を拡張して、専有プロパティを含めます。

これらのプロパティを DRA が表示および適用する方法を設定することもできます。たとえば、デフォルトのプロパティの値を使ってユーザインタフェースコントロールを定義することができます。

企業内の該当する管理対象オブジェクトのすべてに、DRA がカスタムページを適用されます。たとえば、Active Directory のスキーマ拡張を［グループのプロパティ］ウィンドウに追加するためにカスタムページを作成する場合、DRA がこのページ上のプロパティを、指定したスキーマ拡張をサポートするドメイン内の各管理対象グループに適用します。各カスタムページに一意のプロパティセットが必要です。Active Directory の属性を 2 つ以上のカスタムページに追加することはできません。

既存のユーザインタフェース内のウィンドウまたはタブを個別に無効にすることはできません。アシスタント管理者は、デフォルトのユーザインタフェースとカスタムページのいずれかを使用してプロパティ値を選択できます。プロパティの最近選択した値を DRA が適用されます。

DRA はカスタムプロパティに完全な監査証跡を提供します。DRA は、次に示すデータをアプリケーションのイベントログに記録しています。

- カスタムページへの変更

  重要 : Windows アプリケーションのログ監査を手動で設定する必要があります。詳細については、「Windows イベントログでの DRA 監査の有効化 / 無効化」を参照してください。

- カスタムページの作成と削除
- カスタムページに含まれる公開スキーマ拡張、Active Directory の属性、および仮想属性

カスタムプロパティの設定変更を監視するために変更アクティビティのレポートを実行することもできます。

プライマリ管理サーバからカスタムページを実装および変更します。同期化の期間、DRA はマルチマスタセット全体でカスタムページの設定を複製します。詳細については、「マルチマスタセットの設定」を参照してください。

サポート対象のカスタムページ

作成するカスタムページごとに、Active Directory のプロパティ、スキーマ拡張、または仮想属性を一式で選択でき、これらのプロパティをカスタムタブとして表示させることができます。次のタイプのカスタムページが作成できます。

カスタムユーザページ

次に示すウィンドウにカスタムタブを表示させることができます。

- ［ユーザのプロパティ］ウィンドウ
- ［ユーザの作成］ウィザード
- ［ユーザのクローンを作成する］ウィザード

カスタムグループページ

次に示すウィンドウにカスタムタブを表示させることができます。

- ［グループのプロパティ］ウィンドウ
- ［グループの作成］ウィザード
- ［グループのクローンを作成する］ウィザード

カスタムコンピュータページ

次に示すウィンドウにカスタムタブを表示させることができます。

- ［コンピュータのプロパティ］ウィンドウ
- ［コンピュータの作成］ウィザード

カスタム連絡先ページ

次に示すウィンドウにカスタムタブを表示させることができます。

- ［連絡先のプロパティ］ウィンドウ
- ［連絡先の作成］ウィザード
- ［連絡先のクローンを作成する］ウィザード

カスタムの OU ページ

次に示すウィンドウにカスタムタブを表示させることができます。

- ［部門のプロパティ］ウィンドウ
- ［部門の作成］ウィザード
- ［部門のクローンを作成する］ウィザード

カスタムリソースメールボックスのページ

次に示すウィンドウにカスタムタブを表示させることができます。

- ［リソースメールボックスのプロパティ］ウィンドウ

- ［リソースメールボックスの作成］ウィザード
- ［リソースメールボックスのクローンを作成する］ウィザード

カスタムダイナミック配布グループのページ

次に示すウィンドウにカスタムタブを表示させることができます。

- ［ダイナミック配布グループのプロパティ］ウィンドウ
- ［ダイナミック配布グループの作成］ウィザード
- ［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

カスタム共有メールボックスのページ

次に示すウィンドウにカスタムタブを表示させることができます。

- ［共有メールボックスのプロパティ］ウィンドウ
- ［共有メールボックスの作成］ウィザード
- ［共有メールボックスのクローンを作成する］ウィザード

サポートされているカスタムプロパティコントロール

Active Directory 属性、スキーマ拡張、または仮想属性をカスタムページに追加する場合、アシスタント管理者がプロパティ値の入力に使用するユーザインタフェースコントロールも設定します。たとえば、次の方法でプロパティの値を指定できます。

- 特定の値の範囲を定義する
- デフォルトのプロパティ値を設定する
- プロパティが必須項目かどうかを示す

固有の情報や天順を表示するユーザインタフェースコントロールを設定することもできます。たとえば、従業員識別番号に特定の範囲を定義する場合、**[Specify employee identification number (001 to 100)]** と表示されるようにテキストボックスコントロールラベルを設定できます。

ユーザインタフェースの各コントロールは、単一の Active Directory 属性、スキーマ拡張、または仮想属性のサポートを提供しています。プロパティのタイプに基づき次に示すユーザインタフェースコントロールを設定します。

Active Directory 属性の種類	サポート対象のユーザインタフェースコントロール
ブール	[チェックボックス]
日付	カレンダコントロール
整数	テキストボックス (デフォルト) 選択リスト
文字列	テキストボックス (デフォルト) 選択リスト オブジェクトセレクタ
複数値の文字列	選択リスト

カスタムページの操作

カスタムページは［User Interface Extensions (ユーザインタフェースの拡張)］ノードから作成できます。ページが作成されたら、Active Directory の属性プロパティを追加または削除でき、ページを無効にしたり削除したりすることができます。設定したいカスタマイズ項目それぞれに対し、カスタムページを作成し、適切な権限または役割をアシスタント管理者に割り当ててください。以下にベストプラクティスを示します。カスタムページの使用を開始するときに考慮に入れてください。

1. DRA に確実に Active Directory の属性、スキーマの拡張属性、または仮想属性を認識させるには、NetIQ Administration Service というサービスを各管理サーバで再起動します。
2. どのタイプのカスタムページを作成するのか、このカスタムページでどのプロパティをアシスタント管理者に管理させたいかを特定してください。Active Directory の属性をどれでも選択できます。これには、スキーマ拡張属性も、DRA の既存のウィザードおよびプロパティウィンドウ内の属性も、または作成する任意の仮想属性も含まれます。ただし、各カスタムページに一意のプロパティセットが必要です。Active Directory の属性を 2 つ以上のカスタムページに追加することはできません。

   カスタムページが既存のユーザインタフェースを置き換えることはありません。詳細については、「カスタムプロパティページの仕組み」および「サポート対象のカスタムページ」を参照してください。
3. アシスタント管理者にこれらのプロパティを指定させる方法を決めてください。たとえば、指定したプロパティで可能な値を 3 つに制限してもよいでしょう。プロパティごとに、適切なユーザインタフェースコントロールを定義することができます。詳細については、「サポートされているカスタムプロパティコントロール」を参照してください。
4. これらのプロパティを管理するために専有の情報や指示をアシスタント管理者が必要としているかを判断してください。たとえば、DN (Distinguished Name) や LDAP パスなど、プロパティ値の構文が Active Directory に必要かどうか判断します。

5. これらのプロパティをカスタムページに表示させる順序を指定します。表示順序はいつでも変更できます。
6. DRA によるこのカスタムページの使用法を決めてください。たとえば、［新しいユーザ］ウィザードと［ユーザのプロパティ］ウィンドウにユーザカスタムページを追加できます。
7. ［Assistant Admin details (アシスタント管理者の詳細情報)］ペインの［割り当て］タブを使用して、正しいオブジェクトセットに対してアシスタント管理者が適切な権限を持っているか検証します。このカスタムページのためにカスタム権限を作成していた場合、その権限を適切なアシスタント管理者に委任してください。
8. このページでプロパティを管理するためにカスタム権限をアシスタント管理者が必要としているかを判断してください。たとえば、カスタムページを［ユーザのプロパティ］ウィンドウに追加する場合、［*Modify All User Properties (すべてのユーザプロパティを変更)*］という権限を委任すると、アシスタント管理者が必要以上の権限を得る可能性があります。カスタムページの実装に必要なカスタム権限があれば、それを作成します。詳細については、「カスタム権限の実装」を参照してください。
9. これまでの手順の中で判断したことを使って、適切なカスタムページを作成してください。
10. 実装したカスタムプロパティページに関する情報を、ヘルプデスクなど、適切なアシスタント管理者に配布してください。

プロパティのカスタマイズを実装するには、DRA の管理役割に含まれる権限が必要です。カスタムページの詳細については、「カスタムプロパティページの仕組み」を参照してください。

カスタムプロパティページの作成

異なるカスタムページを作成することで、さまざまなカスタムプロパティを作成できます。デフォルトでは、新規のカスタムページは有効になっています。

カスタムのページを作成するときは、それを無効にすることができます。カスタムのページを無効にすると、ユーザインタフェースに表示されなくなります。複数のカスタムページを作成している場合は、カスタマイズ内容をテストし、テストが完了するまでは、ページを無効にしておいたほうがよいでしょう。

注 : コンピュータアカウントは、ユーザアカウントから Active Directory の属性を継承します。Active Directory のスキーマを拡張してユーザアカウントの追加属性を含める場合、コンピュータアカウントを管理するためのカスタムページを作成するときに、これらの属性を選択することができます。

カスタムプロパティ ページを作成するには :

1 ［**[環境設定管理]**］> ［**[User Interface Extensions (ユーザインタフェースの拡張)]**］ノードの順に選択します。

2 ［タスク］メニューで ［**[新規]**］をクリックし、作成したいカスタムページに適したメニュー項目をクリックします。

3 ［全般］タブで、このカスタムページの名前をタイプ入力してから、［ [OK]］をクリックします。このページを無効にする場合は、［ [有効]］チェックボックスをクリアします。

4 このカスタムページに含めたいプロパティごとに、次の操作を行ってください。

4a ［プロパティ］タブで［ [追加]］をクリックします。

4b プロパティを選択するには［ [参照]］をクリックします。します。

4c ［ [Control label (コントロールのラベル)]］フィールドで、ユーザインタフェースコントロールのラベルとして DRA が使用すべきプロパティ名をタイプ入力します。コントロールのラベルは、見て用途が分かる使いやすい名前にしてください。手順、有効な値の範囲、および構文の例を含めることもできます。

4d ［ [Control type (コントロールのタイプ)]］メニューから、適切なユーザインタフェースコントロールを選択します。

4e DRA にこのカスタムページを Delegation and Configuration console (委任および環境設定コンソール) 内のどこに表示させたいか、その位置を選択します。

4f 最小長やデフォルト値など、追加属性を指定するには、［ [Advanced (詳細設定)]］をクリックします。

4g ［ [OK]］をクリックします。

5 これらのプロパティを DRA がカスタムページに表示する順番を変えるには、適切なプロパティを選択し、［ [上に移動]］または［ [下に移動]］をクリックします。

6 ［ [OK]］をクリックします。

カスタムプロパティの変更

カスタムページは、カスタムプロパティを変更することで変更できます。

カスタムプロパティを変更するには :

1 ［ [環境設定管理]］> ［ [User Interface Extensions (ユーザインタフェースの拡張)]］ノードの順に選択します。

2 リストペインで、目的のカスタムページを選択します。

3 ［タスク］メニューで [［プロパティ］] をクリックします。

4 このカスタムページについて適切なプロパティと設定を変更します。

5 ［ [OK]］をクリックします。

カスタムページで管理される Active Directory の属性の識別

特定のカスタムページを使用してどの Active Directory 属性、スキーマ拡張、または仮想属性が管理されているかを素早く識別できます。

カスタムページを使用して管理される Active Directory のプロパティを識別するには :

1 ［ [環境設定管理]］> ［ [User Interface Extensions (ユーザインタフェースの拡張)]］ノードの順に選択します。

2 リストペインで、目的のカスタムページを選択します。

3 ［詳細］ペインの［[プロパティ]］タブをクリックします。［詳細］ペインを表示するには、［表示］メニューの［[詳細]］をクリックします。

4 DRA がプロパティを表示および適用する方法を確認するには、適切な Active Directory 属性、スキーマ拡張、または仮想属性をリストから選択してから、［[プロパティ]］アイコンをクリックします。

カスタムページの有効化、無効化、および削除

カスタムページを有効にすると、DRA がこのカスタムページを関連するウィザードとウィンドウに追加します。カスタムページを表示させるウィザードやウィンドウを指定するには、カスタムページページを変更します。

注 : 各カスタムページが一意のプロパティセットを確実に表示させるには、DRA は、他のカスタムページ上に表示されるプロパティを含んでいるカスタムページを有効にしません。

カスタムページを削除すると、DRA が関連するウィザードとウィンドウからカスタムページを無効にします。カスタムページは削除されません。カスタムページがユーザインタフェースに一切表示されないようにするには、カスタムページを削除します。

カスタムページを削除すると、DRA が関連するウィザードとウィンドウからカスタムページを削除します。削除されたカスタムページを復元することはできません。ユーザインタフェースからカスタムページを一時的に削除するには、カスタムのページを無効化します。

カスタムページを有効化、無効化、削除するには、［[環境設定管理]］>［[User Interface Extensions (ユーザインタフェースの拡張)]］ノードの順に選択し、［タスク］メニューまたは右クリックメニューで目的のアクションを選択します。

コマンドラインインタフェース

CLI を使用すると、コマンドまたはバッチファイルを使用して強力な管理製品の機能がアクセスおよび適用できます。CLI では、1 つのコマンドを発行して複数のオブジェクトに変更を加えることができます。

たとえば、200 人の従業員のホームディレクトリを新しいサーバに再配置する必要がある場合、CLI を使用すれば、次に示すように、わずか 1 つのコマンドを入力するだけで 200 個のユーザアカウントをすべて変更することができます。

```
EA USER @GroupUsers(HOU_SALES),@GroupUsers(HOU_MIS) UPDATE HOMEDIR:\\HOU2\USERS\@Target()
```

このコマンドは、HOU_SALES と HOU_MIS の各グループ内にある 200 個のユーザアカウントそれぞれのホームディレクトリフィールドを \\HOU2\USERS*user_id* に変えるよう DRA に指示しています。Microsoft Windows のネーティブの管理ツールでこのタスクを実行するには、最低でも 200 種類の異なるアクションを実行する必要があります。

注 : PowerShell に多くの機能が追加されたため、CLI ツールは今後のリリースで廃止される予定です。

カスタムツール

カスタムツールを使用すると、DRA 管理下の任意の Active Directory アカウントを選択することで任意のアプリケーションを呼び出してネットワーク内のクライアントコンピュータおよびサーバコンピュータ上で実行させることができます。

DRA は 2 種類のカスタムツールをサポートしています。

- Microsoft Office など、共通のデスクトップユーティリティを起動するカスタムツール
- ユーザが作成し DRA の各クライアントコンピュータに配布するカスタムツール

DRA クライアントがインストールされているすべてのコンピュータからウィルス対策スキャンを起動するカスタムツールを作成することができます。DRA によるスクリプトの定期的更新を必要とする外部アプリケーションやツールを起動するカスタムツールを作成することができます。これらの定期的更新には、構成の変更やビジネスルールの変更などが含まれます。定期的な更新の後に、DRA はプライマリ管理サーバからセカンダリ管理サーバおよび DRA クライアントコンピュータへとカスタムツールを複製します。

カスタムツールをサーバのマルチマスタセットに複製させる方法を理解するには、「ファイルのレプリケーション」を参照してください。

カスタムツールの作成

選択した Active Directory オブジェクトか、カスタムツール作成用ウィザード内に表示される Active Directory の全オブジェクトのいずれかに関連付けることによって、DRA のプライマリサーバ内にカスタムツールを作成することができます。同じものが、MMS のセカンダリサーバに複製され、さらにファイルレプリケーションを通じて DRA クライアントに複製されます。

新しいカスタムツールが、必要に応じて、DRA 内の関連 Active Directory オブジェクトに対して操作を開始するためのメニューとサブメニューを作成します。

アシスタント管理者に委任して、カスタムツールの作成と実行およびアプリケーションへのアクセスと実行を行うことができます。

カスタムツールを作成する場合、次のように各パラメータを入力する必要があります。

[全般] タブ

1. **名前 :** ツールの必須顧客名。
2. **メニューとサブメニュー :** 新しいカスタムツールのメニュー項目を作成するには、[**[Menu and Submenu Structure (メニューとサブメニューの構造)]**] フィールドにメニュータイトルを入力します。カスタムツールを作成してオブジェクトを選択すると、DRA は [タスク] メニュー、[ショートカット] メニュー、および DRA ツールバーで指定するメニューとサブメニューから成る構造を使用したカスタムツールメニュー項目を表示します。

   メニューとサブメニューのサンプル構造 : メニュー項目の名前、円記号 (\)、サブメニュー項目の名前をタイプ入力します。

ショートカットキーを設けるには : メニュー項目の名前の前にアンパーサンド文字 (&) をタイプ入力します。

a. 例 : SendEmail\ApproveAction ---- SendEmail がメニューで ApproveAction がサブメニューで、ApproveAction の最初の文字「A」はショートカットキーとして有効になっています。

3. **有効 :** カスタムツールを有効にするにはこのボックスにチェックマークを入れます。
4. **説明 :** 説明が必要であれば、その値を追加できます。
5. **コメント :** コメントが必要であれば、カスタムツールに追加することができます。

[Supported Objects (サポート対象オブジェクト)] タブ

必要な AD オブジェクト、または作成済みカスタムツールと関連付けられるべき AD オブジェクトのすべてを選択します。

現在サポートされているカスタムツールのオプションは、管理対象ドメイン、コンテナ、ユーザ、連絡先、グループ、コンピュータ、部門 (OU)、および公開プリンタなどです。

注 : その他の新しく導入されたオブジェクト、すなわちリソースメールボックス、ダイナミックグループ、および Exchange のダイナミックグループなどは、カスタムツールではサポートされていません。

[Application Settings (アプリケーションの設定)] タブ

アプリケーションの場所 : アプリケーションがインストールされた場所のパス / 位置を指定する必要があります。方法は、アプリケーションのパス自体をコピーして貼り付けても、[**[挿入]**] オプションを使用しても構いません。

この同じパスは、MMS 内のすべての DRA サーバにすでに存在している必要があります。必要に応じて、新しいカスタムツールを作成する前に、ファイルのレプリケーションを使用して MMS サーバ上の使用可能なパスにファイルをアップロードして複製することができます。

また、[Location of the application (アプリケーションの場所)] フィールドで外部アプリケーションの場所を指定する際に、DRA 変数、環境変数、およびレジストリ値が使用できます。これらの変数を使用するには、[**[挿入]**] をクリックし、使用する変数を選択します。

変数を挿入した後、円記号 (\) 文字を入力し、アプリケーションパスの残りの部分 (アプリケーションの実行ファイル名を含む) を指定します。

例 :

- *例 1:* カスタムツールが実行する外部アプリケーションの場所を指定するために、環境変数 {%PROGRAMFILES%} を選択し、アプリケーションのパスの残りの部分を [Location of the application (アプリケーションの場所)] フィールドに指定します。
  {%PROGRAMFILES%}\ABC Associates\VirusScan\Scan32.exe

注 : DRA はサンプルとして、Office のインストールディレクトリのレジストリ値を指定します。パスが含まれているレジストリキーを値として指定するには、次の構文を使用します。{HKEY_LOCAL_MACHINE\SOFTWARE\MyProduct\SomeKey\(Default)}

- *例2:* カスタムツールが実行するカスタムスクリプトファイルの場所を指定するために、DRA 変数 {DRA_Replicated_Files_Path} を選択し、スクリプトファイルのパスの残り部分を［Location of the application (アプリケーションの場所)］フィールドに指定します。{DRA_Replicated_Files_Path}\cscript.vbs ; ここで、{DRA_Replicated_Files_Path} は複製されたファイルパス、または管理サーバ内の {DRAInstallDir}\FileTransfer\Replicate フォルダです。

注 : カスタムツールを作成する前に、ファイル複製機能を使用してスクリプトファイルをプライマリ管理サーバにアップロードしてください。ファイル複製機能がスクリプトファイルをプライマリ管理サーバ内の {DRAInstallDir}\FileTransfer\Replicate フォルダにアップロードします。

- *例3:* カスタムツールが実行する DRA ユーティリティの場所を指定するために、DRA 変数 {DRA_Application_Path} を選択し、ユーティリティのパスの残りの部分を［Location of the application (アプリケーションの場所)］フィールドに指定します。{DRA_Application_Path}\DRADiagnosticUtil.exe; ここで、{DRA_Application_Path} は DRA のインストール場所です。
- *例 4:* アプリケーションの場所をアプリケーションのファイル名と拡張子とともにコピーし、貼り付けるだけです。

Parameters to pass to the application: 外部アプリケーションに渡すパラメータを定義するために、1 つまたは複数のパラメータをコピーして［Parameters to pass to the application (アプリケーションに渡すパラメータ)］フィールドに貼り付けるか、タイプ入力します。DRA は［Parameters to pass to the application (アプリケーションに渡すパラメータ)］フィールドで使用できるパラメータを提供します。これらのパラメータを使用するには、［挿入］をクリックして、使用するパラメータを選択します。オブジェクトプロパティをパラメータとして指定する場合、オブジェクトプロパティに対し読み取り権限と、カスタムツールの実行に必要な *Execute Custom Tools* という権限を確実にアシスタント管理者に付与してください。

例 :

- *例 1:* グループ名とドメイン名をパラメータとして外部のアプリケーションまたはスクリプトに渡すために、オブジェクトパラメータ名とドメインパラメータ名という各パラメータを選択し、パラメータ名を［Parameters to pass to the application (アプリケーションに渡すパラメータ)］フィールドに指定します。"{Object.Name}""{Domain.$McsName}"
- *例 2:* アプリケーション「C:\Windows\SysWOW64\cmd.exe」に入力パラメータ「ipconfig」を渡すには、そのフィールドに「"{C:\Windows\SysWOW64\cmd.exe}" "{ipconfig}"」と入力します。

Directory where the application will run: これは、クライアントまたはサーバのマシンの、アプリケーションを実行する必要のある場所です。アプリケーションを実行する場所のパスに渡す必要があります。［Location of the application (アプリケーションの場所)］フィールドのパラメータを渡す方法と同じように［挿入］オプションを使用することもできます。このタブの他のパラメータは、その用途を暗示的に説明しています。

ユーザインタフェースのカスタマイズ

Delegation and Configuration Console (委任および環境設定コンソール) の設定方法をカスタマイズするオプションがいくつかあります。これらのオプションのほとんどに、アプリケーション内の様々な機能ペインの機能を非表示にしたり、表示させたり、再構成する機能があります。ツールバーの表示 / 非表示の切り替え、アプリケーションタイトルのカスタマイズ、およびカラムの追加、削除、並べ替えも行うことができます。これらのカスタマイズオプションはすべて［ **[表示]**］メニューにあります。

コンソールタイトルの変更

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 (ウィンドウのタイトル)］タブを選択します。
4. 適切なオプションを指定して［ **[OK]**］をクリックします。詳細については、［ **[?]**］アイコンをクリックしてください。

リストカラムのカスタマイズ

リストカラムに DRA が表示するオブジェクトプロパティが選択できます。この柔軟な機能により、検索結果のリストなど、自社の特定管理ニーズに合うようにユーザインタフェースをカスタマイズすることができます。たとえば、必要なデータを素早く効率的に見つけてソートできるよう、ユーザのログオン名やグループを表示するようにカラムを設定できます。

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。

24 Web クライアント

Web クライアントでは、オブジェクトプロパティ、フォームのワークフロー自動化のフォーム、およびユーザインタフェースのブランディングをカスタマイズすることができます。正しく実装された場合、プロパティおよびワークフローのカスタマイズは、オブジェクト管理および自動ワークフローを送信する際に、アシスタント管理者タスクを自動化するのに役立ちます。

プロパティページのカスタマイズ

オブジェクトタイプごとに Active Directory 管理役割でアシスタント管理者が使用するオブジェクトプロパティフォームをカスタマイズできます。これには、DRA 内に組み込まれた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の作成とカスタマイズが含まれます。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 コンソールにて［カスタマイズ］>［プロパティページ］のリストに明確に定義されているため、どのオブジェクトページがビルトインであり、どのビルトインページがカスタマイズされ、どのページがビルトイン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 管理者として 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の詳細については、「カスタムハンドラの追加」を参照してください。

カスタムフィルタの定義

フィルタを使用して、プロパティページに [[管理対象オブジェクトブラウザ]] フィールドを追加して、各オブジェクトタイプに表示される情報をカスタマイズできます。フィールド設定を行う場合、[管理対象オブジェクトブラウザのオプション] タブを使用して設定にフィルタを追加できます。カスタムフィルタを定義することで、アシスタント管理者のオブジェクトブラウザに表示される情報を制限できます。アシスタント管理者は、定義したフィルタ条件を満たすオブジェクトのみを表示できます。

フィルタを定義するには、[管理対象オブジェクトブラウザのオプション] タブで [[オブジェクトフィルタの指定]] チェックボックスを有効にします。フィルタ条件ごとに、情報のフィルタに使用するオブジェクトタイプ、フィルタする属性、フィルタ条件、および属性値を指定します。同じオブジェクトタイプに対して複数のフィルタを作成する場合は、AND 演算子と組み合わされます。管理対象オブジェクトブラウザのすべての定義済みフィルタを使用すると、アシスタント管理者が検索操作を実行できます。

注

- フィルタの定義には、キャッシュされた属性のみを使用できます。
- カスタムフィルタのカスタムスクリプトを使用してカスタムハンドラを作成する場合、カスタムハンドラが機能するためには、[[管理対象オブジェクトブラウザのオプション]] タブでカスタムフィルタを手動で定義する必要もあります。

オブジェクトプロパティページの新規作成

新しいオブジェクトプロパティページを作成するには :

1 DRA 管理者として 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 [+ [作成]] をクリックします。

4 アクション名、アイコン、オブジェクトタイプ、操作設定を定義して、最初のオブジェクトプロパティフォームを作成します。

[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。

5 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。

要求フォームのカスタマイズ

要求フォームは、その作成時または変更時に Web サーバに保存されます。DRA 管理者は、[[管理]] > [[カスタマイズ]] > [[要求]] から管理します。アシスタント管理者は、これらを [[タスク]] > [[要求]] から管理します。これらのフォームは、ワークフロー自動化サーバで作成された自動ワークフローの送信に使用されます。フォーム作成者は、これらの要求を使用して、オブジェクト管理タスクの自動化および改善を行うことができます。

既存のフォームプロパティおよびカスタムハンドラを追加および変更することができます。プロパティを追加およびカスタマイズするためのインタフェースの動作は、通常、ワークフロー自動化フォームでは、ワークフロー構成オプションおよびフォームを使用できるユーザのコントロールを除いて、オブジェクトプロパティをカスタマイズする場合と同じです。プロパティの追加と変更、カスタムハンドラの追加、およびワークフロー自動化の説明について詳細は、以下のトピックを参照してください。

- プロパティページのカスタマイズ (Web クライアント)
- カスタムハンドラの追加
- 自動ワークフロー

カスタムハンドラの追加

DRA では、プロパティ属性を相互作用させてワークフロータスクを完了するためや、ワークフロー、プロパティ、フォーム作成でのロードと送信をカスタマイズするために、カスタムハンドラを使用します。

プロパティカスタムハンドラ

プロパティカスタムハンドラーのいくつかの例は次のとおりです。

- 他のフィールドの値を照会する
- フィールド値の更新
- フィールドの読み込み専用状態の切り替え
- 設定された変数に基づいてフィールドを表示または非表示にする

ページロードハンドラ

通常、ページロードハンドラは初期化を実行し、主にカスタムプロパティページで使用されます。これらは、ページが最初に選択された時にのみ実行され、プロパティページの場合は、サーバからデータがロードされた後に実行されます。

フォームロードハンドラ

フォームロードハンドラは、通常、初期化コントロールを実行します。これらは、フォームが初めてロードされたときに 1 回だけ実行されます。プロパティページの場合は、選択したオブジェクトのプロパティについてサーバがクエリを実行する前に実行されます。

フォーム送信ハンドラ

フォーム送信ハンドラでは、ユーザがあるタイプの検証を行ったり、場合によって異常の発生時にフォームの送信をキャンセルすることができます。

注 : ベストプラクティスとして、ハンドラを作成した場所とは異なるページ（タブ）にあるフィールドの値を変更するページおよびフォームハンドラでの変更ハンドラを構成することは避けてください。このシナリオでは、ハンドラとは異なるページのデータは、アシスタント管理者がそのページにアクセスするまでロードされません。このページは、変更ハンドラによって設定された値と衝突する可能性があります。

Web コンソールでカスタムハンドラおよびカスタマイズを使用する方法の詳細な例については、DRA マニュアルページにある*製品カスタマイズ*リファレンスの「「Web コンソールのカスタマイズ」」および「「ワークフローのカスタマイズ」」セクションを参照してください。

カスタムハンドラの振る舞いと作成方法の詳細については、次のトピックを参照してください。

- 222 ページの 「カスタムハンドラ作成の基本手順」
- 225 ページの 「カスタム JavaScript の有効化」
- 225 ページの 「スクリプトエディタの使用」
- 226 ページの 「カスタムハンドラの実行について」

カスタムハンドラ作成の基本手順

カスタムハンドラを作成する前に、コンソール設定でカスタム JavaScript が有効になっていることを確認してください。詳細については、「カスタム JavaScript の有効化」を参照してください。

次の手順は、事前に選択済みのカスタムハンドラのページからの操作です。そのポイントに到達するには、次のように異なるハンドラに移動します。

- オブジェクトプロパティのカスタムハンドラ : プロパティフィールドの編集アイコン をクリックします。

- ページロードハンドラ : ページのプロパティを選択します。たとえば、[[全般]] > [▪▪▪ [その他のオプション]] > [[プロパティ]] などです。
- フォームロードおよびフォーム送信ハンドラ : 選択したワークフローフォーム、[オブジェクトの作成] ページ、または [プロパティの編集] ページの [[フォームプロパティ]] ボタンをクリックします。

カスタムハンドラの作成 :

1 カスタマイズするプロパティまたはページを基にして、該当するハンドラタブを選択します。
   - カスタムハンドラ
   - ページロードハンドラ
   - フォームロードハンドラ
   - フォーム送信ハンドラ
2 ハンドラページを有効にします。○ → ● そして、次のいずれかを実行します。
   - **プロパティフィールドカスタムハンドラ :**
      1. 実行時間を選択します。通常は、2 番目のオプションを使用します。

         実行時間は、ユーザ入力に応じて変更ハンドラを実行する時期を制御します。この設定は、フィールドの値が draApi.fieldValues インタフェースを使用して別のカスタムハンドラによって更新される場合には適用されません。
      2. [[+ 追加]] をクリックして、[[カスタムハンドラの追加]] メニューからカスタムハンドラを選択します。
   - **ページまたはフォームハンドラ :** [[+ 追加]] をクリックして、[[カスタムハンドラの追加]] メニューからカスタムハンドラを選択します。

注 : 一般的に、1 つのカスタムハンドラのみが必要な場合もありますが、複数のハンドラを使用することもできます。複数のハンドラは、一覧に載っている順序で順番に実行されます。ハンドラの順序を変更したり、不要なハンドラをスキップしたりする場合は、スクリプト内にフローコントロール API を追加できます。

---

3 その場合、このページに追加するカスタムハンドラごとに設定する必要があります。環境設定オプションはハンドラタイプによって異なります。スクリプトエディタには、ビルトインヘルプと動的な Intellisense コード補完アシスタンスがあり、ヘルプのスニペットも参照します。これらの機能の使い方の詳細については、「スクリプトエディタの使用」を参照してください。

   独自のハンドラタイプを作成できます。

   - **LDAP クエリまたは REST クエリのハンドラ :**
      1. 静的な値を基にクエリを実行する場合、[[接続情報]] と [[クエリパラメータ]] を定義します。

         注 : LDAP クエリの場合、[接続情報] の設定で特定の認証タイプを要求できます。
            - **デフォルトアカウント :** DRA サーバログインで認証します。

- **管理対象ドメイン上書きアカウント**: 既存の管理対象ドメイン上書きアカウントを介して、Active Directory に対して認証します。
- **LDAP上書きアカウント**: 管理対象ドメインのドメインアカウントとは対照的に、LDAP 上書きアカウントを通じて認証されます。このオプションを使用するには、まず Delegation and Configuration Console (委任および環境設定コンソール) でアカウントを有効にする必要があります。詳細については、「LDAP 上書き認証を有効にする」を参照してください。

クエリをダイナミックにする場合、必須フィールドにプレースホルダの値を入力します。これはハンドラの実行に必須です。スクリプトがプレースホルダの値を上書きします。

注: また、REST クエリのヘッダとクッキーも設定できます。

---

2. クエリ前アクションでは、スクリプトエディタを使用して、クエリが送信される前に実行されるカスタム JavaScript コードを書き込みます。このスクリプトは、すべての接続情報およびクエリパラメータにアクセスでき、これらのパラメータを変更してクエリをカスタマイズすることもできます。たとえば、ユーザがフォームに入力した値に基づいて、クエリパラメータを設定します。
3. クエリ後のアクションでは、クエリの結果を処理するためのスクリプトを含めます。一般的なタスクには、エラーの確認、返された結果に基づいたフォーム値の更新、およびクエリによって返されたオブジェクトの数に基づいたオブジェクトの一意性の検証が含まれます。

- **スクリプト**: カスタム JavaScript コードを挿入してスクリプトを構築します。
- **DRA クエリ**: [クエリパラメータ] タブで JSON ペイロードを指定します。ペイロード形式は、DRA サーバに送信される VarSet キーまたは値のペアに一致している必要があります。REST および LDAP クエリと同様に、サーバに送信する前にペイロードを変更するために使用できるクエリ前アクション、また結果を処理するためのクエリ後のアクションを指定することもできます。
- **メッセージボックスハンドラ**: メッセージボックス自体のプロパティを定義した後に、[**[表示前のアクション]**] および [**[閉じた後のアクション]**] に対して JavaScript セグメントを書き込むこともできます。

  これらのアクションは、オプションです。[表示前のアクション] は、ユーザに表示される前に、すべてのメッセージボックスのプロパティをカスタマイズするために使用されます。また、[閉じた後のアクション] は、ユーザのボタン選択の処理、および追加のロジックの実行を行うために使用します。

4 **[OK]** をクリックし、ハンドラを保存します。

Web コンソールでカスタムハンドラおよびカスタマイズを使用する方法の詳細な例については、DRA マニュアルページにある*製品カスタマイズ*リファレンスの「「Web コンソールのカスタマイズ」」および「「ワークフローのカスタマイズ」」セクションを参照してください。

カスタム JavaScript の有効化

セキュリティ上の理由のため、デフォルトではカスタム JavaScript は無効になっています。カスタム JavaScript を有効にすることにより、管理者は JavaScript コードのスニペットを書き込むことができ、Web コンソールはそのまま実行されます。この例外を有効にするのは、そのリスクを理解して受諾した場合のみにしてください。

カスタマイズする際にカスタム JavaScript コードを含めるようにするには、次のようにします。

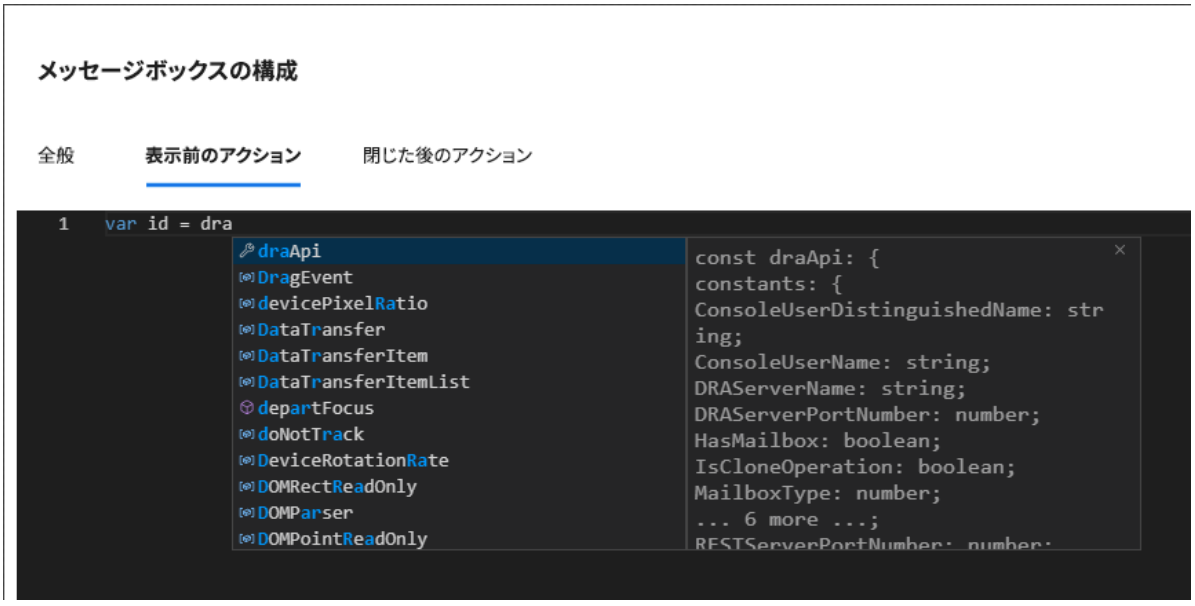
1. C:\ProgramData\NetIQ\DRARESTProxy のロケーションに移動します。
2. restProxy.config ファイルを開きます。
3. allowCustomJavaScript="true" を <consoleConfiguration> エレメントに追加します。

スクリプトエディタの使用

スクリプトエディタでは、DRA API を使用して DRA でカスタムハンドラを作成する JavaScript メソッドの自由形式の入力と貼り付けが可能です。エディタには、動的な Intellisense コード補完とスクリプトを書く際に役立つフライアウトヘルプパネルが含まれています。

Intellisense コード補完

スクリプトエディタの Intellisense は、API の説明を含む、API サマリの選択可能なコード補完スニペット、タブ補完、およびフライアウトパネルを提供します。



注 : Intellisense コード補完は動的です。つまり、スクリプトを定義するハンドラのタイプに基づいた構文オプションが提供されますが、ユーザが以前入力した文字列も格納され、それらのプロンプトも表示されます。

スクリプトエディタのヘルプ

スクリプトエディタで ヘルプ オプションをクリックすると、カスタムハンドラ API の一般的な用途とその使用場所を説明したパネルが開き、API の機能の説明を API タイプ別にリストします。

- グローバル API には次のものが含まれます。
  - フォームアクセス
  - フローコントロール
  - 定数
- メッセージボックス API には次のものが含まれます。
  - 表示前のアクション
  - 閉じた後のアクション
- クエリ API には次のものが含まれます。
  - クエリ結果
  - DRA クエリ
  - LDAP クエリ
  - REST クエリ

カスタムハンドラの実行について

DRA は、カスタムハンドラを通じてフォーム実行ライフサイクルの複数のポイントで Web フォームの振る舞いをカスタマイズする機能を提供します。カスタムハンドラの各タイプには特定の実行ウィンドウがあります。このウィンドウは、次に示されるように、カスタマイズの実行中に利用可能なオブジェクトデータのスコープに影響します。

1. *フォームロードハンドラ*。フォームが接続されているオブジェクト属性のコレクションの前にフォームがロードされると実行されます。これらのハンドラは、ターゲットオブジェクトの属性値にアクセスがありません。
2. *ページロードハンドラ*。DRA は、フォームのページに初めてアクセスした時にページロードハンドラを実行します。これらのハンドラは、そのページに含まれるターゲットオブジェクトの属性値へのアクセスが保証されます。
3. *属性ハンドラ*。フォーム上の属性値にアクセスすると、DRA は属性ハンドラを実行します。さらに、各フォーム属性は、ユーザの操作中に 3 つの特定のポイントの 1 つでカスタムハンドラを実行するように設定できます。(1) 即座に (属性がフォーカスを取得したとき)、(2) 属性がフォーカスを失ったとき、または (3) 属性がフォーカスを失ってから指定した時間が経過したとき。
4. *フォーム送信ハンドラ*。フォーム送信ハンドラは、フォームが保存または変更がフォームに適用されると実行されます。

ユーザインタフェースのブランディングのカスタマイズ

DRA の Web コンソールのタイトルバーを独自のタイトルやロゴイメージにしてカスタマイズすることができます。位置は DRA の製品名の右隣りです。この位置は最上位のナビゲーションにも使用されるため、ログインすると DRA の最上位のナビゲーションリンクに隠れます。ただし、ブラウザのタブにはカスタマイズされたタイトルが引き続き表示されます。

DRA Web コンソールのブランディングをカスタマイズするには、次のようにします。

1. DRA 管理者として Web コンソールにログインします。
2. [**[管理]**] > [**[環境設定]**] > [**[ブランディング]**] に移動します。
3. 会社のロゴ画像を追加する場合は、inetpub\wwwroot\DRAClient\assets の Web サーバにロゴイメージを保存します。
4. 必要に応じて、マストヘッドとログインのタイルの設定を更新します。

   ログイン時にアシスタント管理者への通知を追加する場合は、[**[ログイン時に通知モーダルを表示する]**] ボタンをオンにします。この通知の設定を更新し、[**[プレビュー]**] をクリックして、ログイン時にこの通知がどのように表示されるかを確認します。
5. すべての変更が完了したら、[**[保存]**] をクリックします。

IX ツールとユーティリティ

以下のセクションでは、DRA の提供する ActiveView Analyzer ユーティリティ、診断ユーティリティ、削除オブジェクトユーティリティ、ヘルスチェックユーティリティ、ごみ箱ユーティリティについての情報があります。

25 ActiveView Analyzer ユーティリティ

各 DRA ActiveView には、1 つ以上のルールが含まれています。このルールは、DRA マルチマスタセットによって管理されている Active Directory(AD) オブジェクトに適用されます。ActiveView Analyzer ユーティリティは、特定の DRA 操作内の AD オブジェクトに適用される各 DRA ActiveView ルールの処理時間を監視します。DRA の操作中に、DRA サーバは、その操作のターゲットオブジェクトをすべての ActiveView 内のすべてのルールと比較します。その後、DRA はすべての一致するルールを含む結果リストを作成します。ActiveView Analyzer は、DRA の操作に適用されたときに、各ルールの処理に要した時間を計算します。

この情報を使用して、未使用の ActiveView の処理にかかった時間を含む、ActiveView 処理時間の異常をチェックすることにより、ActiveView の問題を診断できます。ユーティリティは、重複した ActiveView の検知も簡素化します。

データ収集を実行しレポートを確認した後に ActiveView の 1 つ以上のルールを変更する必要が生じる場合もあります。

ActiveView Analyzer ユーティリティには、任意の DRA 管理サーバからアクセスできます。ただし、ActiveView ユーティリティは問題が発生している管理サーバに対して実行する必要があります。

ActiveView Analyzer ユーティリティにアクセスするには、DRA 管理の役割特権を使用して管理サーバにログオンし、スタートメニューから［**[NetIQ 管理]**］>［**[ActiveView Analyzer ユーティリティ]**］に移動します。ActiveViewAnalyzer.exe は、DRA のインストール済みパス Program Files (x86)\NetIQ\DRA\X64 から起動できます。

このユーティリティを使用して、次の操作を実行します。

- ActiveView でデータを収集する
- Analyzer レポートを生成する

例

アシスタント管理者であるポールは、DRA 管理者であるボブに、ユーザを作成するときに通常よりも時間がかかっていることを知らせします。ボブはポールのユーザオブジェクトで ActiveView Analyzer を起動し、ポールにユーザを作成してもらうことにしました。収集が完了したあと、ボブは分析レポートを生成し、［Share MBX］という名前のルールが列挙に 50 ミリ秒かかったことに気づきます。ボブはこのルールを含む ActiveView を識別し、ルールを変更した後に、問題が解決されていることがわかりました。

ActiveView データの収集開始

ActiveView Analyzer ユーティリティを使うと、アシスタント管理者によって実行されたアクションから ActiveView のデータを収集できます。このデータは Analyzer のレポートで確認することができます。データを収集するには、データ収集対象のアシスタント管理者を指定し、ActiveView の収集を開始する必要があります。

注 : 実行中の Analyzer と同じ DRA サーバにデータ収集対象のアシスタント管理者も接続されている必要があります。

ActiveView の収集を開始するには :

1 ［ **[開始]**］> ［ **[NetIQ 管理]**］> ［ **[ActiveView Analyzer ユーティリティ]**］をクリックします。

2 ActiveView Analyzer のページで、次のように指定します。

   2a **ターゲット DRA サーバ :** アシスタント管理者操作でパフォーマンスデータを収集する DRA サーバ。

   2b **ターゲットアシスタント管理者 :** ［参照］をクリックし、データを収集するアシスタント管理者を選択します。

   2c **監視期間 :** Analyzer のデータを収集するために必要な時間の合計を指定します。指定した時間を経過すると、データ収集が停止します。

3 ［ **[収集を開始]**］をクリックして ActiveView のデータを収集します。

   ActiveView データ収集を開始すると、ユーティリティによって既存のデータがクリアされ、最新のステータスが表示されます。

4 (オプション) スケジュールされていた期間が終了する前にデータ収集を手動で停止してレポートを生成することができます。ActiveView でのアシスタント管理者の操作の記録を停止するには ［ **[収集を停止]**］をクリックします。

5 (オプション) 最新のステータスを取得するには、［ **[Collection Status (コレクションステータス)]**］をクリックします。

重要 : 収集を停止してアシスタント管理者を変更した場合、または収集を停止して同一のアシスタント管理者に関するデータ収集を再開した場合、既存のデータを ActiveView Analyzer がクリアします。Analyzer のデータは一度につきデータベース内のアシスタント管理者 1 人のみです。

Analyzer レポートの生成

Analyzer レポートを生成する前に、データの収集を停止していることを確認してください。

［ActiveView Analyzer］ページでは、アシスタント管理者によって実行された操作のリストが表示されます。Analyzer レポートを生成するには :

1 ［ **[レポートの選択]**］をクリックし、表示するレポートを選択します。

2 [[レポートの生成]] をクリックし、操作による影響を受ける AD オブジェクトやリストされたオブジェクト、一致、不一致、および個々の ActiveView ルールの処理にかかった時間などを管理する ActiveView などの ActiveView 操作の詳細を含む分析レポートを生成します。

レポートを使用すれば、操作実行に時間がかかり過ぎるルールを分析して、いずれかを各 ActiveView から変更または削除するかどうか決断することができます。

3 (オプション) グリッドの上にマウスを合わせ、右クリックしてから、[コピー] メニューを使用して、レポートをクリップボードにコピーします。クリップボードから、Notepad や Excel などの別のアプリケーションに列の見出しとデータを貼り付けることができます。

オブジェクトのパフォーマンスを識別する

ActiveView またはルールによって管理されているすべてのオブジェクトのパフォーマンスを識別するには、次のようにします。

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 [[Delegation Management]] に移動し、[[Manage ActiveViews (ActiveView を管理)]] をクリックします。

3 特定の ActiveView を見つけるには、検索を実行します。

ここでは、問題が発生しているルールまたはオブジェクトを検索し、変更を行うことができます。

- ActiveView をダブルクリックして、[[ルール]] を選択し、ルールを一覧表示します。特定のルールは、右クリックメニューから変更できます。
- ActiveView を右クリックし、[[Show Managed Objects (管理対象オブジェクトの表示)]] を選択して、オブジェクトを一覧表示します。オブジェクトを変更するには、右クリックの [[プロパティ]] から実行できます。

4 ルールまたは管理オブジェクトに変更を加え、それらの変更によって問題が解決されるかどうかを確認します。

26 診断ユーティリティ

診断ユーティリティは、ご使用の管理サーバから情報を収集して DRA に起きた問題を診断する際に役立ちます。このユーティリティを使用してログファイルを取得し、それを御社の技術サポート担当者に提供してください。診断ユーティリティはウィザード形式のインタフェースです。ログの詳細度の設定から診断情報の収集までの一連の操作がストレスなく行えます。

任意の管理サーバのコンピュータから診断ユーティリティが利用できます。ただし、診断ユーティリティは問題が発生している管理サーバに対して実行する必要があります。

診断ユーティリティにアクセスするには、ローカル管理者権限を持つ管理者アカウントを使用して管理サーバコンピュータにログオンし、Windows のスタートメニューの NetIQ 管理プログラムグループからユーティリティを開きます。

このユーティリティの使用に関する詳細については、技術サポートに問い合わせてください。

27 削除オブジェクトユーティリティ

このユーティリティでは、ドメインアクセスアカウントが管理者でないときに特定ドメインに対するアカウントキャッシュ増分更新のサポートを有効にすることができます。ドメイン内の削除オブジェクトのコンテナに対する読み取りパーミッションがドメインアクセスアカウントに与えられていない場合、DRA はアカウントキャッシュ増分更新が実行できません。

このユーティリティを使用して実行できるタスクは、次のとおりです。

- 指定したドメイン内の削除オブジェクトのコンテナに対する読み取りパーミッションが指定のユーザアカウントまたはグループに付与されているか検証する
- 指定されたユーザアカウントまたはグループに対し、読み取りパーミッションの委任または削除を行う
- ユーザアカウントに対し、ディレクトリサービスのデータを同期するユーザ権限の委任または削除を行う
- 削除オブジェクトのコンテナのセキュリティ設定を表示する

削除オブジェクトユーティリティの実行ファイル (DraDelObjsUtil.exe) は、ご使用の管理サーバの Program Files (x86)\NetIQ\DRA フォルダから実行することができます。

削除オブジェクトユーティリティに必須のパーミッション

このユーティリティを使用するには、次に示すパーミッションを持っている必要があります。

目的の作業	必要なパーミッション
アカウントのパーミッションを検証する	削除オブジェクトコンテナへのアクセスでの読み取りパーミッション
削除オブジェクトコンテナに対する読み取りパーミッションを委任する	削除オブジェクトコンテナが置かれているドメインの管理者パーミッション
ディレクトリサービスのデータを同期するユーザ権限を委任する	削除オブジェクトコンテナが置かれているドメインの管理者パーミッション
以前委任されたパーミッションを削除する	削除オブジェクトコンテナが置かれているドメインの管理者パーミッション
削除オブジェクトのコンテナのセキュリティ設定を表示する	削除オブジェクトコンテナへのアクセスでの読み取りパーミッション

削除オブジェクトユーティリティの構文

DRADELOBJSUTIL /DOMAIN: *ドメイン名* [/DC: *コンピュータ名*] {/DELEGATE: *アカウント名* | /VERIFY: *アカウント名* | /REMOVE: *アカウント名* | /DISPLAY [/RIGHT]}

削除オブジェクトユーティリティのオプション

次に挙げるオプションが指定できます。

/DOMAIN: ***ドメイン***	削除オブジェクトコンテナが存在するドメインの NETBIOS 名または DNS 名を指定します。
/SERVER: ***コンピュータ名***	指定されたドメインのドメインコントローラの名前または IP アドレスを指定します。
/DELEGATE: ***アカウント名***	指定されたユーザアカウントまたはグループにパーミッションを委任します。
/REMOVE: ***アカウント名***	指定されたユーザアカウントまたはグループに以前委任したパーミッションを削除します。
/VERIFY: ***アカウント名***	指定されたユーザアカウントまたはグループのパーミッションを検証します。
/DISPLAY	指定されたドメイン内の削除オブジェクトコンテナのセキュリティ設定を表示します。
/RIGHT	指定されたユーザアカウントまたはグループにディレクトリサービスのデータを同期するユーザ権限が与えられていることを確認します。この権限の委任または検証に、このオプションが使用できます。ディレクトリサービスのデータを同期するユーザ権限があれば、そのアカウントで Active Directory 内のすべてのオブジェクトとプロパティを読み取ることができます。

注

- 指定するユーザアカウント名またはグループ名にスペースが含まれている場合は、アカウント名を引用符で囲んでください。たとえば、Houston IT というグループを指定する場合は「Houston IT」と入力します。
- グループを指定する場合は、Windows 2000 以前と互換の名前をそのグループに使用してください。

削除オブジェクトユーティリティの例

次に、一般的なシナリオでのコマンド使用例を示します。

例 1

MYCOMPANY\JSmith というユーザアカウントが hou.mycompany.com というドメイン内の削除オブジェクトコンテナに対するパーミッションを読み込んだことを検証するには、次のコマンドを入力してください。

```
DRADELOBJSUTIL /DOMAIN:HOU.MYCOMPANY.COM /VERIFY:MYCOMPANY\JSMITH
```

例 2

MYCOMPANY というドメイン内の削除オブジェクトコンテナに対する読み取りパーミッションを MYCOMPANY\DraAdmins というグループに委任するには、次のコマンドを入力してください。

```
DRADELOBJSUTIL /DOMAIN:MYCOMPANY /DELEGATE:MYCOMPANY\DRAADMINS
```

例 3

MYCOMPANY というドメイン内の削除オブジェクトコンテナに対する読み取りパーミッションと、ディレクトリサービスのデータを同期するユーザ権限を MYCOMPANY\JSmith というユーザアカウントに委任するには、次のコマンドを入力してください。

```
DRADELOBJSUTIL /DOMAIN:MYCOMPANY /DELEGATE:MYCOMPANY\JSMITH /RIGHT
```

例 4

HQDC というドメインコントローラを使用して hou.mycompany.com というドメイン内の削除オブジェクトコンテナに関するセキュリティ設定を表示するには、次のコマンドを入力してください。

```
DRADELOBJSUTIL /DOMAIN:HOU.MYCOMPANY.COM /DC:HQDC /DISPLAY
```

例 5

MYCOMPANY というドメイン内の削除オブジェクトコンテナに対する読み取りパーミッションを MYCOMPANY\DraAdmins というグループから削除するには、次のコマンドを入力してください。

```
DRADELOBJSUTIL /DOMAIN:MYCOMPANY /REMOVE:MYCOMPANY\DRAADMINS
```

28 正常性チェックユーティリティ

正常性チェックユーティリティは、DRA のインストールキットに同梱されているスタンドアロンのアプリケーションです。正常性チェックユーティリティのポストインストールおよび事前アップグレードと事後アップグレードを使用して、DRA サーバ、DRA の Web サイト、および DRA クライアントに関しコンポーネントとプロセスの確認、検証、通知を行います。また、これを使用して製品ライセンスをインストールまたは更新したり、製品アップグレードの前に AD の LDS インスタンスをバックアップしたり、チェックの説明を表示したり、問題を解決したり、問題解決と再検証に必要なアクションの特定することもできます。

正常性チェックユーティリティは、NetIQAdminInstallationKit.msi を実行した後に DRA プログラムのフォルダから利用できます。

正常性チェックユーティリティは、NetIQ.DRA.HealthCheckUI.exe ファイルを実行することで、いつでも実行することができます。特定の操作を行う、特定のコンポーネントのチェックを実行、またはすべてのコンポーネントのチェックを実行するなど、アプリケーションを開いたときに行われる動作を選択することができます。正常性チェックユーティリティを使用して実行する便利な機能について、次を参照してください。

機能	ユーザアクション
すべてを選択またはすべての選択を解除	ツールバーまたは［ファイル］メニューのオプションを使用してすべてのチェック項目を **[選択]** または **[選択解除]** します。特定のチェックを実行する場合はチェックボックスを個別に選択します。
選択されたチェックを実行	このツールバーまたは［ファイル］メニューのオプションを使用して、選択されたチェックを (一括で、または個別に) 実行します。
結果の保存または書き込み	このツールバーまたは［ファイル］メニューのオプションを使用して、実行されたチェックに関する詳細レポートを作成および保存します。
このチェックを実行	項目タイトルを選択してチェックの内容を表示し、このツールバーアイコンをクリックしてチェックを実行します。たとえば、次の操作のいずれかを実行するために使用します。 ◆ ライセンスの検証 (製品ライセンスのインストールまたは更新) ◆ AD LDS インスタンスのバックアップ (AD LDS インスタンスのバックアップ) ◆ レプリケーション (レプリケーションデータベースの検証)
この問題を解決	項目のタイトルを選択し、チェックが失敗したときにこのツールバーのオプションを使用します。チェックを再度実行しても問題が解決しない場合、説明を参照してください。問題解決のために行うべきことや情報が記載されています。

29 ごみ箱ユーティリティ

このユーティリティを使用すると、ドメインのサブツリーを管理しているときに、ごみ箱のサポートを有効にすることができます。指定されたドメイン内の非表示の NetIQRecycleBin コンテナに対するパーミッションがドメインアクセスアカウントに与えられていない場合、DRA は削除されたアカウントをごみ箱に移動することができません。

注 : このユーティリティを使用してごみ箱が有効にした後は、この変更を管理サーバが確実に適用できるよう、アカウントキャッシュ完全更新を実行してください。

このユーティリティを使用して実行できるタスクは、次のとおりです。

- 指定したドメイン内の NetIQRecycleBin コンテナに対する読み取りパーミッションが指定したアカウントに与えられているか検証する
- 指定したアカウントに読み取りパーミッションを委任する
- NetIQRecycleBin コンテナのセキュリティ設定を表示する

ごみ箱ユーティリティに必須のパーミッション

このユーティリティを使用するには、次に示すパーミッションを持っている必要があります。

目的の作業	必要なパーミッション
アカウントのパーミッションを検証する	NetIQRecycleBin コンテナへのアクセスでの読み取りパーミッション
NetIQRecycleBin コンテナに対する読み取りパーミッションを委任する	指定したドメイン内の管理者パーミッション
NetIQRecycleBin コンテナのセキュリティ設定を表示する	NetIQRecycleBin コンテナへのアクセスでの読み取りパーミッション

ごみ箱ユーティリティの構文

DRARECYCLEBINUTIL /DOMAIN: *ドメイン名* [/DC: *コンピュータ名*] {/DELEGATE: *アカウント名* | /VERIFY: *アカウント名* | /DISPLAY}

ごみ箱ユーティリティのオプション

ごみ箱ユーティリティの設定には、次に示すオプションが利用できます。

/DOMAIN: ***ドメイン***	ごみ箱が置かれているドメインの NETBIOS 名または DNS 名を指定します。
/SERVER: ***コンピュータ名***	指定されたドメインのドメインコントローラの名前または IP アドレスを指定します。
/DELEGATE: ***アカウント名***	指定したアカウントにアクセス権を委任します。
/VERIFY: ***アカウント名***	指定したアカウントのパーミッションを検証します。
/DISPLAY	指定したドメイン内の NetIQRecycleBin というコンテナのセキュリティ設定を表示します。

ごみ箱ユーティリティの例

次に、一般的なシナリオでのコマンド使用例を示します。

例 1

MYCOMPANY\JSmith というユーザアカウントが hou.mycompany.com というドメイン内の NetIQRecycleBin というコンテナに対するパーミッションを読み込んだことを検証するには、次のコマンドを入力してください、

```
DRARECYCLEBINUTIL /DOMAIN:HOU.MYCOMPANY.COM /VERIFY:MYCOMPANY\JSMITH
```

例 2

MYCOMPANY というドメイン内の NetIQRecycleBin というコンテナに対する読み取りパーミッションを MYCOMPANY\DraAdmins というグループに委任するには、次のコマンドを入力してください。

```
DRARECYCLEBINUTIL /DOMAIN:MYCOMPANY /DELEGATE:MYCOMPANY\DRAADMINS
```

例 3

HQDC というドメインコントローラを使用して hou.mycompany.com というドメイン内の NetIQRecycleBin というコンテナに関するセキュリティ設定を表示するには、次のコマンドを入力してください。

```
DRARECYCLEBINUTIL /DOMAIN:HOU.MYCOMPANY.COM /DC:HQDC /DISPLAY
```

A 付録

この付録では、DRA サービスと DRA REST サービスの問題のトラブルシュート方法について説明します。

- 245 ページの 「DRA サービス」
- 246 ページの 「DRA REST サービスのトラブルシューティング」

DRA サービス

この表では、DRA サービスに関する情報を示します。これにより、DRA 管理者は DRA の機能に影響を与えることなく、サービスを安全に無効にできるのかを判断できます。

DRA サービス	説明	安全に無効化
NetIQ 管理サービス	このサービスは、すべての DRA 操作を実行し、内部 DRA サーバプロセスを管理します。	非対応
NetIQ DRA 監査サービス	このサービスは、Web コンソールからの統合された変更履歴要求を処理します。 このサービスを無効にすると、 ◆ DRA の機能に影響はありません。 ◆ Delegation and Configuration Console (委任および環境設定コンソール) から統合された変更履歴レポートを生成できます。 ◆ Web コンソールから統合された変更履歴レポートを生成することはできません。	対応
NetIQ DRA キャッシュサービス	このサービスは、NetIQ 管理サーバの永続的なキャッシュとして機能します。	非対応
NetIQ DRA コアサービス	このサービスは、DRA コンソールのレポートを生成し、Active Directory、Office365、DRA、およびリソースコレクタジョブをスケジュールします。 このサービスを無効にすると、 ◆ DRA の機能に影響はありません。 ◆ コレクタジョブは実行されないので、NRC レポートのデータは収集されません。 ◆ DRA コンソールから統合された変更履歴レポートを生成することはできません。	対応

DRA サービス	説明	安全に無効化
NetIQ DRA ログアーカイブ	このサービスは、監査レポーティングをサポートするために、すべての DRA 監査イベントを安全な方法で保存します。	非対応
NetIQ DRA レプリケーションサービス	このサービスは、DRA の一時的なグループの割り当て (TGA) 機能をサポートしています。このサービスが削除または停止された DRA サーバでは、TGA を使用できません。	対応
NetIQ DRA Rest サービス	Web コンソールおよび PowerShell クライアントは、このサービスを使用して NetIQ 管理サーバと通信します。	非対応
NetIQ DRA セキュアストレージ	このサービスは、DRA 設定を保存する DRA の AD LDS インスタンスを管理します。また、この設定データを MMS セットアップ全体で複製します。	非対応
NetIQ DRA Skype サービス	このサービスは、すべての Skype タスクを管理します。 このサービスを無効にすると、 ◆ DRA の機能に影響はありません。 ◆ Skype 操作は処理されません。	対応

DRA REST サービスのトラブルシューティング

このセクションでは、次のトピックのトラブルシューティング情報について説明します。

- 246 ページの 「DRA REST 拡張の証明書の処理」
- 247 ページの 「DRA サーバからのエラーの処理」
- 248 ページの 「すべての PowerShell コマンドで PSInvalidOperation エラーが発生する」
- 248 ページの 「WCF トレースログ記録」

DRA REST 拡張の証明書の処理

DRA エンドポイントサービスでは、通信ポートで証明書のバインドが必要です。インストール中に、インストーラはポートを証明書にバインドするためのコマンドを実行します。このセクションの目的は、バインディングを検証する方法、および必要に応じてバインディングを追加または削除する方法について説明します。

基本情報

デフォルトのエンドポイントサービスポート : 8755

DRA REST 拡張機能のアプリ ID: 8031ba52-3c9d-4193-800a-d620b3e98508

証明書ハッシュ : IIS Manager の［SSL 証明書］ページに表示されます。

既存のバインディングの確認

互換モードドライバ (CMD) ウィンドウで、次のコマンドを実行します : netsh http show sslcert

これにより、このコンピュータの証明書バインドのリストが表示されます。DRA REST 拡張機能のアプリ ID のリストを確認します。ポート番号は設定ポートと一致する必要があります。証明書ハッシュは、IIS Manager に表示される証明書ハッシュと一致する必要があります。

```
IP:port                 : 0.0.0.0:8755
Certificate Hash        : d095304df3d3c8eecf64c25df7931414c9d8802c
Application ID          : {8031ba52-3c9d-4193-800a-d620b3e98508}
Certificate Store Name  : (null)
Verify Client Certificate Revocation    : Enabled
Verify Revocation Using Cached Client Certificate Only    : Disabled
Usage Check             : Enabled
Revocation Freshness Time : 0
URL Retrieval Timeout   : 0
Ctl Identifier          : (null)
Ctl Store Name          : (null)
DS Mapper Usage         : Disabled
Negotiate Client Certificate    : Disabled
```

バインディングの削除

既存のバインディングを削除するには、互換モードドライバ (CMD) ウィンドウで次のコマンドを入力します。

netsh http delete sslcert ipport=0.0.0.0:9999

9999 は削除するポート番号です。netsh コマンドは、SSL 証明書が正常に削除されたことを示すメッセージを表示します。

バインディングの追加

新しいバインディングを追加するには、互換モードドライバ (CMD) ウィンドウで次のコマンドを入力します。

netsh http add sslcert ipport=0.0.0.0:9999 certhash=[HashValue] appid={8031ba52-3c9d-4193-800a-d620b3e98508}

ここで、9999 はエンドポイントサービスのポート番号を表し、[HashValue] は IIS Manager に表示される証明書ハッシュ値です。

DRA サーバからのエラーの処理

メールが有効なオブジェクトの作成中にエラーが発生した場合は、次を参照してください。

EnableEmail が操作の失敗を返す

メールが有効なオブジェクトを作成したり、EnableEmail エンドポイントの 1 つを呼び出したりすると、DRA サーバから「*Server failed to complete the requested operation workflow successfully.Operation UserEnableEmail failed(サーバが要求された操作ワークフローを正常に完了できませんでした。UserEnableEmail 操作に失敗しました。)*」などのエラーが返される場合があります。これは、サーバで定義されたポリシーに準拠しない mailNickname プロパティをペイロードに含めた場合に発生します。

mailNickname プロパティをペイロードから削除し、定義されたポリシーに従って DRA サーバに電子メールエイリアス値を生成させます。

すべての PowerShell コマンドで PSInvalidOperation エラーが発生する

DRA REST サービスが自己署名証明書にバインドされている場合、PowerShell コマンドレットは次のエラーを返します。

```
Get-DRAServerInfo: One or more errors occurred.
An error occurred while sending the request.
The underlying connection was closed: Could not establish trust
relationship for the SSL/TLS secure channel.
The remote certificate is invalid according to the validation procedure.
```

コマンドごとに、-IgnoreCertificateErrors パラメータを含める必要があります。確認メッセージも抑止するには、-Force パラメータを追加します。

WCF トレースログ記録

REST 要求の結果、REST サービスログを読み込んで解決できないエラーが発生する場合は、要求が WCF 層を通過している方法に関する詳細を確認するために、WCF のトレースログのレベルを上げる必要があります。トレースのこのレベルで生成されるデータの量は重要な場合があります。したがって、出荷ログレベルは「Critical, Error(重大、エラー)」に設定されます。

これが役立つ場合の例として、ペイロード内のオブジェクトを送信している場合でも、要求が null 値の例外が発生する場合があげられます。もう 1 つのケースとしては、REST が応答しなりつつある場合があげられます。

WCF トレースログ記録を増やすには、調査中のサービスの設定ファイルを編集する必要があります。ペイロードの例外は、REST サービスの WCF トレースログを確認する場合に明らかになる可能性があります。

詳細ログ記録を有効にする手順

1. Windows ファイルエクスプローラで、DRA Extensions インストールフォルダに移動します。通常、これは C:\Program Files (x86)\NetIQ\DRA です。
2. NetIQ.DRA.RestService.exe.config ファイルを開きます。

3 次の XML パスで <source> 要素を見つけます : <system.diagnostics><sources>。

4 ソース要素で、switchValue 属性値を「Critical, Error(重大、エラー)」から「Verbose, ActivityTracing(詳細、ActivityTracing)」に変更します。

5 ファイルを保存し、NetIQ DRA Rest サービスを再起動します。

EnableEmail が操作の失敗を返す

WCF トレースデータは、専有の形式で書き込まれます。SvcTraceViewer.exe ユーティリティを使用して trace.svslog を読み込むことができます。このユーティリティの詳細については、次を参照してください。