Directory and Resource Administrator

管理者ガイド

2018年7月

NetIQ

保証と著作権

本書の内容

この『*開発者ガイド*』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。このリリースに対応する資料の一覧については、Documentation Webサイト (https://www.netiq.com/documentation/directory-and-resource-administrator-92/)をご覧ください。

セールスサポートへのお問い合わせ

製品、価格、および機能についてのご質問は、地域のパートナーへお問い合わせください。パートナーに連絡できない場合は、弊社のセールスサポートチームへお問い合わせください。

各国共通:	www.netiq.com/about_netiq/officelocations.asp
米国およびカナダ:	1-888-323-6768
電子メール:	info@netiq.com
Webサイト:	www.netiq.com

テクニカルサポートへのお問い合わせ

特定の製品に関する問題については、弊社のテクニカルサポートチームへお問い合わせください。

各国共通:	www.netiq.com/support/contactinfo.asp
北米および南米:	1-713-418-5555
ヨーロッパ、中東、アフリカ:	+353 (0) 91-782 677
電子メール:	support@netiq.com
Webサイト:	www.netiq.com/support

マニュアルサポートへのお問い合わせ

弊社の目標は、お客様のニーズを満たすマニュアルの提供です。マニュアルを改善するためのご提案がございましたら、本マニュアルのHTML版で、各ページの下にある**comment on this topic**をクリックしてください。Documentation-Feedback@netiq.com宛てに電子メールを送信することもできます。貴重なご意見をぜひお寄せください。

オンラインユーザコミュニティへのお問い合わせ

NetIQのオンラインコミュニティであるNetIQ Communitiesは、他のユーザやNetIQのエキスパートとやり取りできるコラボレーションネットワークです。より迅速な情報、有益なリソースへの役立つリンク、NetIQエキスパートとのやり取りを提供するNetIQ Communitiesは、信頼のおけるIT投資が持つ可能性を完全に実現するために必要な知識を習得するために役立ちます。詳細については、http://community.netiq.comを参照してください。

1 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。

1.1 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権限だけを受け取るようにします。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。

DRAには、Active Directory、Microsoft Windows、Microsoft Exchange、およびMicrosoft Office 365の各環境を制御および管理するために必要なソリューションが用意されています。

- **Active Directory、Office 365、Exchange、およびSkype for Businessのサポート:** Active Directory、オンプレミスのExchange Server、オンプレミスのSkype for Business、Exchange Online、およびSkype for Business Onlineを管理できます。
- **ユーザおよび管理者の特権アクセスの細かい制御:** 特許取得済みのActiveViewテクノロジにより、特定の責務に必要な権限だけを委任し、特権格上げを防止することができます。
- **カスタマイズ可能なWebコンソール:** 直観的な方法により、技術者でなくても、限定された(そして割り当てられた)機能および権限を通して、簡単かつ安全に管理タスクを行えます。
- **詳細なアクティビティの監査およびレポーティング:** 製品で実行されたすべてのアクティビティが包括的に監査レコードに記録されます。長期データを安全に保管でき、ADへのアクセスを制御するためのプロセスを実施していることを監査機関(PCI DSS、FISMA、HIPAA、NERC CIPなど)に証明できます。
- **ITプロセスの自動化:** プロビジョニングやプロビジョニング解除、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:** 管理者のアクセスを細かく制御し、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およびワークフロー自動化機能とは無関係にActive Directoryで生成されたイベントの監査を強化します。

1.2 Directory and Administrator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Aegisワークフローエンジンなどがあります。

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

DRAユーザのタイプ	ユーザインタフェース	管理サーバ
DRA管理者 (本製品の構成を管理する人)	Delegation and Configurationコンソール	プライマリサーバ
	DRA ReportingCenterセットアップ(NRC) CLI*(オプション)* DRA ADSIプロバイダ*(オプション)*	セカンダリサーバ
ヘルプデスクの臨時管理者	Account and Resource Managementコンソール	セカンダリサーバ
ヘルプデスクの臨時管理者	Webコンソール	DRARESTがインストールされている任意のDRAサーバ

1.2.1 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。

1.2.2 Delegation and Configurationコンソール

Delegation and Configuration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、Office 365など)の設定を行えます。

1.2.3 Account and Resource Managementコンソール

AccountandResourceManagement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す。これを使用すれば、DRAの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表示および管理することができます。

1.2.4 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。

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

Webコンソールのもう1つの機能である「Unified Change History」では、変更履歴サーバと統合して、DRAの外部でADオブジェクトに対して行われた変更を監査できます。変更履歴レポートのオプションには、次のものがあります。

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

1.2.5 レポーティングコンポーネント

DRAReporting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管理ドメインおよびシステムの詳細を確認できます。

- ADオブジェクトのリソースレポート
- ADオブジェクトデータレポート
- ADサマリレポート

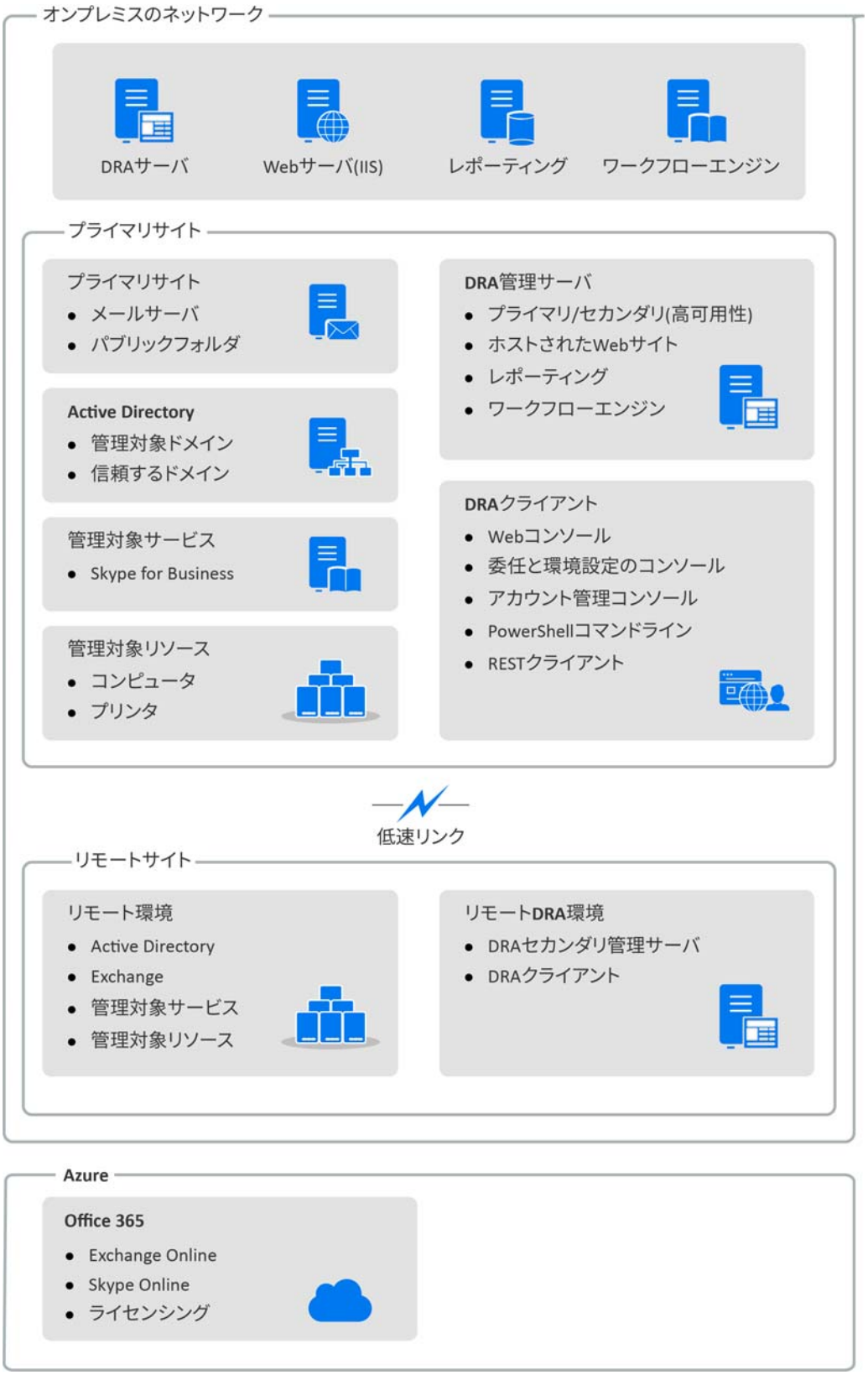
- DRA構成レポート
- Exchange構成レポート
- Office 365 Exchange Onlineレポート
- 詳細なアクティビティトレンドレポート(月別、ドメイン別、ピーク別)
- DRAアクティビティの要約レポート

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

1.2.6 ワークフローエンジン

DRAはワークフローエンジン「Aegis」との統合により、Webコンソールでワークフロータスクの自動化が可能です。アシスタント管理者がワークフローサーバの構成、カスタマイズされたワークフロー自動化フォームの実行、およびワークフローのステータスの表示をWebコンソールで行うことができます。ワークフローエンジンの詳細については、DRAマニュアルサイト (https://www.netiq.com/documentation/directory-and-resource-administrator-92/)を参照してください。

1.2.7 製品アーキテクチャ



2 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。

2.1 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。

2.1.1 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	4CPU(x64)/コア2.0GHz	16GB	100GB
DRA Webコンソール	2CPU(x64)/コア2.0GHz	8GB	100GB
DRA Reporting	4CPU(x64)/コア2.0GHz	16GB	100GB
DRAワークフローサーバ	4CPU(x64)/コア2.0GHz	16GB	100GB

2.1.2 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

2.1.3 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

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 (http://go.microsoft.com/fwlink/?LinkID=46088)(DCOM)」を参照してください。
TCP 50000 *	双方向	DRA管理サーバ	属性の複製、DRAサーバとADAMの通信。(LDAP)
TCP 50001 *	双方向	DRA管理サーバ	SSL属性のレプリケーション(ADAM)
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	オンプレミスのすべてのExchangeサーバ2010から2013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)

プロトコルとポート	方向	宛先	用途
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 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
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

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 11192 * **	アウトバウンド	DRAホストサービス	DRA RESTサービスとDRA管理サービスの間の通信
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	DRAWebコンソール、DRAPowerShell、およびDRAホストサービスの間の通信
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 (http://go.microsoft.com/fwlink/?LinkID=46088)(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	DRAREST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 (http://go.microsoft.com/fwlink/?LinkID=46088)(DCOM)」を参照してください。

プロトコルとポート	方向	宛先	用途
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)
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	ワークフローエンジンおよび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

2.1.4 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、NetIQWebサイトでDirectory and Resource Administratorのページを参照してください。 https://www.netiq.com/support

管理対象システム	前提条件
Active Directory	◆ Microsoft Server 2012 ◆ Microsoft Server 2012 R2 ◆ Microsoft Server 2016
Microsoft Exchange	◆ Microsoft Exchange 2010 SP3(パブリックフォルダを除く) ◆ Microsoft Exchange 2013 ◆ Microsoft Exchange 2016 ◆ Microsoft Skype Online
Microsoft Office 365	◆ Microsoft Exchange Online ◆ Microsoft Skype Online ◆ Windows PowerShell用Windows Azure Active Directoryモジュール https://docs.microsoft.com/en-us/office365/enterprise/powershell/connect-to-office-365-powershell ◆ Skype for Business Online、Windows PowerShellモジュール https://www.microsoft.com/en-us/download/details.aspx?id=39366
Skype for Business	◆ Microsoft Skype for Business 2015
変更履歴	◆ Change Guardian 5.0、5.1

管理対象システム	前提条件
Webブラウザ	◆ Microsoft Internet Explorer 11、Edge ◆ Google Chrome ◆ Mozilla Firefox
ワークフローの自動化	◆ Microsoft Server 2012 ◆ Microsoft Server 2012 R2

2.1.5 DRA管理サーバの要件

DRAには、ソフトウェアおよびアカウントに関する次のサーバ要件があります。

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	**NetIQ管理サーバおよびオペレーティングシステム:**
オペレーティングシステム	◆ Microsoft Windows Server 2012、2012 R2、2016 ◆ MicrosoftWindows2008R2はアップグレードする場合のみサポートされます。 **注:** また、サーバは、サポートされるMicrosoft Windows Serverのネーティブドメインのメンバーでなければなりません。
	Windows DRAインタフェース:
	◆ Microsoft Windows Server 2012、2012 R2、2016 ◆ Microsoft Windows 8.1(x86 & x64)、10(x86 & x64)
インストーラ	◆ Microsoft .Net Framework 4.5.2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 4.5.2以降 ◆ 次のいずれか: ◆ Microsoft Visual C++ 2015(Update 3)再頒布可能パッケージ(x64およびx86) ◆ Microsoft Visual C++ 2017(Update 3)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 Office 365/Exchange Online管理:** ◆ Windows PowerShell用Windows Azure Active Directoryモジュール ◆ IT Professional用Microsoft Online Servicesサインインアシスタント ◆ Skype for Business Online、Windows PowerShellモジュール 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。
レガシWebコンポーネント	**Webサーバ:** ◆ Microsoft Internet Information Services(IIS)バージョン8.0、8.5、10 **Microsoft IISコンポーネント:** ◆ Microsoft Active Service Pages(ASP) ◆ Microsoft Active Service Pages .NET(ASP .Net) ◆ Microsoft IISセキュリティ役割サービス **Windows DRAインタフェース:** ◆ Microsoft .Net Framework 4.5.2 ◆ Microsoft Visual C++ 2015(Update 3)再頒布可能パッケージ(x86)

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 ◆ 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) **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。
DRA Assistant Adminアカウント	DRAで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 Assistant Adminアカウントを「DistributedCOMUsers」グループに追加してください。 **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: ドメイン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。

- 組み込みのドメイン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
- 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
- 動的配布グループ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
- MsExchSystemObjectContainer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
- パブリックフォルダ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

ドメインアクセスアカウントには、次に挙げる特権を「このオブジェクトとすべての子オブジェクト」の範囲で指定してください。

- 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
- コンテナの作成を許可
- グループオブジェクトの作成を許可
- MsExchDynamicDistiributionListの作成を許可
- 部門オブジェクトの作成を許可
- パブリックフォルダの作成を許可
- サービス接続ポイントの作成を許可
- ユーザ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
- MsExchDynamicDistiributionListの削除を許可
- 部門オブジェクトの削除を許可
- パブリックフォルダの削除を許可
- サービス接続ポイントの削除を許可
- ユーザオブジェクトの削除を許可

Office 365テナントのアクセスアカウント: Office 365テナント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。

- Office 365のユーザ管理の管理者
- Exchange Onlineの受信者管理

Exchangeアクセスアカウント: Exchange 2010を管理するには、Exchangeアクセスアカウントに**組織管理**役割を割り当ててください。

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

DRAのインストール後:

- 次のコマンドを実行して、DRAインストールフォルダの「削除済みオブジェクトコンテナ」への権限を委任します(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*>

- 次のコマンドを実行して、DRAインストールフォルダの「NetIQReceyleBOU」への権限を委任します(注:これは、DRAで管理する各ドメインを追加した後に初めて実行できます)。

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

- 最小特権のオーバーライドアカウントを、DRAでプリンタ、サービス、イベントログ、デバイスなどのリソースを管理する各コンピュータの「ローカル管理者」グループに追加します。
- 最小特権のオーバーライドアカウントに、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。
- Exchangeオブジェクトを管理するには、最小特権のオーバーライドアカウントを「組織管理」役割に追加します。

2.1.6 DRA Webコンソールおよび拡張の要件

Webコンソールおよび REST拡張機能には、次のような要件があります。

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 2016、Microsoft Windows 10(Microsoft IIS 10搭載) ◆ Microsoft Windows Server 2012、2012 R2(Microsoft IIS 8.0、8.5搭載)
DRAホストサービス	◆ Microsoft .Net Framework 4.5.2 ◆ DRA管理サーバ
DRA RESTエンドポイントおよびサービス	◆ Microsoft .Net Framework 4.5.2
PowerShell拡張機能	◆ Microsoft .Net Framework 4.5.2 ◆ PowerShell 4.0

コンポーネント	前提条件
DRA Webコンソール	**Webサーバ:** ◆ Microsoft Internet Information Server 8.0、8.5、10 ◆ Microsoft Internet Information Services WCF(アクティブ化) **Microsoft IISコンポーネント:** ◆ Webサーバ ◆ 一般的なHTTP機能 ◆ 静的なコンテンツ ◆ デフォルトのドキュメント ◆ ディレクトリブラウザ ◆ HTTPエラー ◆ アプリケーション開発 ◆ ASP ◆ 健全性と診断 ◆ HTTPログ ◆ 要求の監視 ◆ セキュリティ ◆ 基本認証 ◆ パフォーマンス ◆ 静的なコンテンツの圧縮 ◆ Webサーバの管理ツール

2.1.7 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、2012 R2、2016

コンポーネント	前提条件
NetIQ Reporting Center(v3.2)	**データベース:** ◆ Microsoft SQL Server 2012、2014、2016 ◆ Microsoft SQL Server Reporting Services **Webサーバ:** ◆ Microsoft Internet Information Server 8.0、8.5、10 ◆ Microsoft IISコンポーネント ◆ ASP .NET 4.0 **Microsoft .NET Framework 3.5:** DRA Reportingに接続するすべてのDRA管理サーバには.NET Framework 3.5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。
DRA Reporting	**データベース:** ◆ Microsoft SQL Server Integration Services ◆ Microsofte SQL Serverエージェント

2.1.8 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、無制限の数のユーザアカウントとメールボックスを30日間管理できる試用ライセンスキー(TrialLicense.lic)を、正常性検査ユーティリティを使用してインストールすることができます。

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。

2.2 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。

2.2.1 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。

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。
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インストールを実行する	DRAインストールを起動します。 **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に移動し、Setup.exeを実行します。
NetIQ管理サーバのコンポーネントおよびインストール先を選択する	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: **NetIQ管理サーバ** ◆ ログアーカイブリソースキット ◆ NetIQ DRA SDK **レガシWebコンポーネント** **ユーザインタフェース** ◆ Account and Resource Management ◆ DRA ADSI Provider ◆ コマンドラインインタフェース ◆ Delegation and Configuration
前提条件の確認	［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。
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。

ステップ	詳細
サーバ動作モードを選択する	［プライマリ］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］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、「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 詳細については、「DRA管理サーバの要件」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。
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。

2.2.2 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。

NetIQDRAUserConsole.mst	AccountandResourceManagementコンソールをインストールする
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、NetIQDRAUserConsole.mstなどの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。

2.2.3 DRA REST拡張機能をインストールする

DRA REST拡張機能パッケージには、4つの機能が含まれています。

- **NetIQ DRAホストサービス:** DRA管理サービスとの通信に使用されるゲートウェイ。このサービスは、DRA管理サービスがインストールされているコンピュータで実行する必要があります。
- **DRA RESTサービスおよびエンドポイント:** DRA Webコンソールと非DRAクライアントからDRA操作を要求できるようにするRESTfulインタフェースを提供します。このサービスは、DRAコンソールまたはDRA管理サービスがインストールされているコンピュータで実行する必要があります。
- **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。
- **DRA 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。

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。
SSL証明書をインストールする	SSL証明書がまだWindowsサーバにインストールされていない場合は、インストールを実行する前に証明書をインストールしておく必要があります。
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。
DRA REST拡張機能インストーラを実行する	DRAインストールキットは、インストールメディアの解凍が完了すると、DRAインストールの起動を求めるメッセージを表示します。インストールメディアが解凍された場所に移動し、DRARESTExtensionsInstaller.exeファイルを右クリックし、［**管理者として実行**］を選択します。
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。

ステップ	詳細
コンポーネントを選択し、インストール先を指定する	インストールの［コンポーネントの選択］ダイアログで、DRAホストサービス、DRAREST エンドポイントとサービス、PowerShell拡張機能、およびDRAWebコンソールのすべてのオプションをインストールします。 デフォルトのインストール先C:\Program Files (x86)\NetIQ\DRA Extensionsを受け入れるか、別のインストール先を指定します。
前提条件の確認	［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。
実行者にするサービスアカウントを指定する	デフォルトでは、DRAサーバの既存のサービスアカウントが表示されます。サービスアカウントのパスワードを指定します。DRA管理サーバのサービスアカウントのセットアップの詳細については、「DRA管理サーバの要件」を参照してください。
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およびホストサービスのポートを指定します。
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。

2.2.4 ワークフローサーバのインストール

ワークフローサーバのインストールの詳細については、『ワークフロー自動化管理者ガイド』を参照してください。

2.2.5 DRA Reportingのインストール

DRA Reportingをインストールするには、NetIQ DRAインストールキットにあるNRCSetup.exeとDRAReportingSetup.exeの2つの実行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。
NetIQ Reporting Center(NRC)インストールを実行する	DRAインストールキットがインストールメディアの解凍を完了したら、インストールメディアが解凍された場所に移動し、NRCSetup.exeを実行してください。

ステップ	詳細
NetIQ Reporting Centerコンポーネントを選択する	インストールの［**コンポーネントの選択**］ダイアログ ボックスで、デフォルトの「NetIQ Reporting Center」コンポーネントを使用してNRCの4つのコンポーネントをインストールします。
インストール先を指定する	デフォルトのインストール先C:\Program Files (x86)\NetIQ\Reporting Centerを使用するか、別のインストール先を指定します。
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。 **重要:** NRCをインストールする前に、.NET Framework 3.5をReportingサーバに手動でインストールしておく必要があります。
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。
構成データベースをインストールする	［**構成データベースインストール - SQL Serverログオン**］ダイアログのデフォルトを使用するか、SQL認証を指定してNRCインストールを実行します。SQL Serverのインストールでデフォルトのインスタンスを使用した場合は、［インスタンス］フィールドは空白のままにしてください。
DRAReporting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。
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。

2.3 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の動作の詳細については、「マルチマスタセットの設定」を参照してください。

2.3.1 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組み込みの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組み込みのActiveViewに関連付けられているかを調べます。
  - DRAのレポート機能を使用して、セキュリティモデルレポート(ActiveView Assistant Admin DetailsレポートやAssistant Admin Groupsなど)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。

2.3.2 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。

ステップ	詳細
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の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展開計画を作成します。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。

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。

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、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。
- 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. MMCインタフェースを起動します。
3. 左側のウィンドウで、［**環境設定管理**］を展開します。
4. ［**管理サーバ**］をクリックします。
5. 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。
6. ［**プロパティ**］をクリックします。
7. ［同期スケジュール］タブで、［**今すぐ更新**］をクリックします。
8. 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WindowsOS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\MissionCritical 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。

2.3.3 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。

アップグレードプロセスを複数の段階に分けて、一度の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。

DRA 9.2以降のバージョンでは、ワークフロー自動化サーバの構成は、レジストリではなくAD LDSに保存されます。DRA9.1以前からDRA9.2以降に更新すると、レジストリ構成が自動的にAD LDSに移動し、すべてのセカンダリサーバに複製されます。

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。

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。

ステップ	詳細
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。
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。
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。
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。
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。
REST拡張機能をアップグレードする	DRA REST拡張機能インストーラを実行します。
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。

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、アシスタント管理者の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の詳細については、『*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。
- 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またはADSIプロバイダ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展開できます。

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対して、適切なユーザインタフェース(Account and Resource Managementコンソールなど)をインストールするように指示します。
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のアップグレード完了後、アシスタント管理者のクライアントコンピュータすべてがアップグレード済みのユーザインタフェースを実行しているときに、残っている前バージョンのDRAサーバをオフラインにしてください。

2.3.4 DRA REST拡張機能をアップグレードする

WebコンソールおよびREST拡張機能をDirectory and Resource Administator 9.2にアップグレードするには、DRA 9.0.1以降のバージョンを使用している必要があります。要件については、「DRA Webコンソールおよび拡張の要件」を参照してください。

DRA Webコンソールおよび拡張機能をアップグレードするには、次の手順を実行します。

1. DRAインストールキットをダウンロードした後、インストールメディアを解凍した場所に移動し、DRARESTExtensionsInstaller.exeファイルを右クリックし、［**管理者として実行**］を選択します。
2. インストールウィザードの指示に従い、インストールが完了したら［**終了**］をクリックします。

インストールウィザードの手順の詳細については、新しいインストールの手順:「DRA REST拡張機能をインストールする」を参照してください。

カスタムコンテンツのアップグレード

新しいバージョンのDRAにアップグレードするときに、WebサーバでWebコンソールに対して加えたすべてのカスタマイズを保持したい場合があります。これを簡単に行えるように、DRAREST拡張機能インストーラには、カスタマイズアップグレードユーティリティが組み込まれています。このユーティリティは、REST拡張機能をアップグレードするためにWebサーバでDRARESTExtensionsInstaller.exeを実行したときに、自動的に実行されます。また、このユーティリティは、インストールとは無関係にDRAインストールディレクトリから手動で再実行することもできます。

カスタマイズアップグレードユーティリティのプロセスの一部として、アップグレード開始前にカスタマイズがバックアップされます。アップグレードプロセス中、このユーティリティは、アップグレードによって加えられたすべての変更をログファイルに記録し、自動更新できないカスタマイズ項目についての警告も記録します。

ベストプラクティスとして、アップグレード後にログを確認することをお勧めします。必要に応じて、バックアップフォルダからアップグレード前のカスタマイズをコピーしてカスタマイズをロールバックすることができます。カスタマイズアップグレードユーティリティが開いたら、アップグレードされたカスタマイズを入れるフォルダパスを定義できます。また、自動入力されるデフォルトのパスを使用することもできます。

アップグレードされたカスタマイズおよびカスタマイズのバックアップのためのデフォルトパスは次のとおりです。

- デフォルトのカスタムフォルダパス: C:\inetpub\wwwroot\DRAClient\components\lib\ui-templates\custom
- デフォルトのバックアップフォルダ: $CustomFolderPath\custom_upgrade_$VERSIONFROM_to_$VERSIONTO_backup

2.3.5 Reportingをアップグレードする

DRA Reportingをアップグレードする前に、環境がNRC 3.2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
DRAReporting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。
DRAReporting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。
NRCセットアップを実行する	*条件付き:* NRC Webサービスを別のコンピュータにインストールした場合は、Webサービスをインストールしたコンピュータにログオンし、NRCSetup.exeを実行してNRC Webサービスをアップグレードします。 **注:** 構成データベースを別のサーバにインストールした場合は、構成データベースを先にアップグレードする必要があります
クライアントコンピュータでNRCセットアップを実行する	すべてのNRCWebサービスクライアントコンピュータでNRCSetup.exeを実行します。
DRAReportingサポートを有効にする	プライマリ管理サーバで、Delegation and Configuration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。

3 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、Office 365、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。

3.1 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。

3.1.1 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。
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。

3.1.2 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。管理サーバをインストールした後に、ヘルスチェックユーティリティを使用して、NetIQ Corporationから提供された試用ライセンスキーファイル(.lic)をインストールします。

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コンソールを開き、［**環境設定管理**］>［**Update License**］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コンソールまたはAccount and Resource Managementコンソールで表示することができます。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。

3.1.3 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。

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。

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。セカンダリサーバを追加するには、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。

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、Configuration Managementノードで［**管理サーバ**］を右クリックして、［**Add Secondary Server (セカンダリサーバを追加)**］を選択します。

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

andDomains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 ［**Configuration Management**］>［**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 ［**Configuration Management**］>［**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、基本的に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、［**Configuration Management (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クライアント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。

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コンソール内の［File Replication (ファイルレプリケーション)］というユーザインタフェースを使用して、1度に1つのファイルをレプリケーションのために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、次の自動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。

イベントスタンプ

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のドメインサービス監査の設定についての詳細は、「AD DS auditing (https://technet.microsoft.com/en-us/library/cc731607(v=ws.10).aspx)」を参照してください。
- ChangeGuardian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コンソールを開き、次の操作を行ってください。
  1. ［**ConfigurationManagement**］>［**UpdateAdministrationServerOptions(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。

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［CommonTasks(共通タスク)］で、［**UpdateAdministrationServerOptions(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のクライアント、ARMのクライアントと管理サーバの間での暗号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、［**EncryptedCommunications (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ADLDS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。

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、［**ConfigurationManagement**］>［**仮想属性**］>［**ManagedAttributes(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、［**Configuration Management**］>［**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、［**Configuration Management**］>［**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Deleted Objects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。Deleted Objects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。

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、「ConfigureServersandDomains」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. ［**ConfigurationManagement**］>［**ManagedDomains(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. ［**Full refresh (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

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、［**ConfigurationManagement**］>［**UpdateAdministrationServerOptions(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、［**AccountandResourceManagement**］>［**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**］>［**AdldsCleanupRefreshSchedule(ADLDS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。

ADLDS(ADAM)の設定情報を表示するには、［**ConfigurationManagement**］>［**UpdateServerOptions (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、［**AccountandResourceManagement**］>［**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、DRAAdmins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［**EnableRecycleBin(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［**DisableRecycleBin(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。

Office 365 Tenantコレクタの設定

Office 365 Tenantコレクタでは、Office 365と同期する管理対象ユーザの情報を収集し、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。

Office 365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: Office 365 Tenant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。直近ログオン統計収集の有効化とスケジュールを行うには、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。

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。

統合された変更履歴

デフォルトでは、UCH (Unified Change History)の機能により、DRAの行った変更に関するレポートが生成できます。

統合された変更履歴の権限委任

統合された変更履歴を管理するには、Unified Change History Server Administration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

UCHの権限を委任するには:

1. 委任管理ノードで［**権限**］をクリックし、オブジェクト検索を使用して目的のUCHオブジェクトを見つけ、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. ［**Active Views**］をクリックし、**オブジェクトセレクタ**を使用して必要なオブジェクト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

UCHサーバを構成するには:

1. Webコンソールを起動し、アシスタント管理者の資格情報でログインします。
2. ［**管理**］>［**統合**］>［**統合された変更履歴**］の順に選択し、［**追加**］アイコンをクリックします。
3. 統合された変更履歴の設定で、UCHのサーバ名またはIPアドレス、ポート番号、サーバタイプ、アクセスアカウントの詳細を指定します。
4. サーバへの接続をテストし、［**OK**］をクリックして設定を保存します。
5. 必要に応じて、さらにサーバを追加します。

ワークフローサーバ

DRAでワークフローの自動化を使用するには、WindowsサーバでWorkflow Engineをインストールしてから Webコンソールからワークフロー自動化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構成するには、Webコンソールにログインし、［**管理**］>［**統合**］>［**ワークフロー自動化**］の順に選択します。

Workflow Engineのインストール情報については、『*Workflow Automation Administrator Guide*』を参照してください。

3.1.4 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

3.1.5 Webクライアントを設定する

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。

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

Webコンソールを自動ログアウトさせる無アクティビティ期間を定義したり、自動ログアウトを一切しないように設定することができます。

Webコンソールで自動ログアウトを設定するには、［管理］>［構成］>［自動ログアウト］の順に選択します。

DRAサーバへの接続

Webコンソールで3つのオプションのうち1つを設定してログイン時のDRAサーバへの接続オプションを定義することができます。設定されれば、Webコンソールにログインしたときの［オプション］ドロップダウンパネルでの接続設定は、管理者とアシスタント管理者の両方で同じになります。

- DRAサーバのデフォルトの場所を常に使用する(［常に］)
- DRAサーバのデフォルトの場所を常に使用しない(［なし］)
- DRAサーバのデフォルトの場所が選択されている場合にのみ、それを使用する(［選択した場合のみ］)

ログイン時の各オプションの動作は次のとおりです。

接続の設定	ログイン画面 - オプション	接続オプションの説明
常に	なし	オプション設定は無効です。
なし	自動ディスカバリを使用する	DRAサーバを自動的に検出します。使用できる設定オプションはありません。
	特定のDRAサーバに接続	ユーザがサーバとポートを設定します。

接続の設定	ログイン画面 - オプション	接続オプションの説明
	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、接続オプションを選択します。 ◆ 自動ディスカバリを使用する(指定のドメイン内) ◆ このドメインのプライマリサーバ ◆ DRAサーバを検索する(指定のドメイン内)
選択した場合のみ	自動ディスカバリを使用する	DRAサーバを自動的に検出します。使用できる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	デフォルトのサーバが選択され、DRAサーバ設定が無効になっています。
	特定のDRAサーバに接続	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、接続オプションを選択します。 ◆ 自動ディスカバリを使用する(指定のドメイン内) ◆ このドメインのプライマリサーバ ◆ DRAサーバを検索する(指定のドメイン内)

WebコンソールでDRAサーバへ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。

RESTサーバの接続

RESTサービスの接続設定には、デフォルトのサーバの場所および接続タイムアウト時間(単位は秒)の設定が含まれています。Webコンソールで3つのオプションのうち1つを設定してログイン時のRESTサービスへの接続オプションを定義することができます。設定されれば、Webコンソールにログインしたときの［**オプション**］ドロップダウンパネルでの接続設定は、管理者とアシスタント管理者の両方で同じになります。

- RESTサービスのデフォルトの場所を常に使用する(［**常に**］)
- RESTサービスのデフォルトの場所を常に使用しない(［**なし**］)
- RESTサービスのデフォルトの場所が選択されている場合にのみ、それを使用する(［**選択した場合のみ**］)

ログイン時の各オプションの動作は次のとおりです。

接続の設定	ログイン画面 - オプション	接続オプションの説明
常に	なし	オプション設定は無効です。
なし	自動ディスカバリを使用する	RESTサーバを自動的に検出します。使用できる設定オプションはありません。
	特定のRESTサーバに接続	ユーザがサーバとポートを設定します。

接続の設定	ログイン画面 - オプション	接続オプションの説明
	特定のドメイン内のRESTサーバに接続する	ユーザが管理対象ドメインを指定し、接続オプションを選択します。 ◆ 自動ディスカバリを使用する(指定のドメイン内) ◆ RESTサーバを検索する(指定のドメイン内)
選択した場合のみ	自動ディスカバリを使用する	RESTサーバを自動的に検出します。使用できる設定オプションはありません。
	デフォルトのRESTサーバに接続	デフォルトのRESTサーバが選択され、RESTサーバ設定が無効になっています。
	特定のRESTサーバに接続	ユーザがサーバとポートを設定します。
	特定のドメイン内のRESTサーバに接続する	ユーザが管理対象ドメインを指定し、接続オプションを選択します。 ◆ 自動ディスカバリを使用する(指定のドメイン内) ◆ RESTサーバを検索する(指定のドメイン内)

WebコンソールでRESTサービスの接続を設定するには、［**管理**］>［**構成**］>［**RESTサービス接続**］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。

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 <system.serviceModel>という行のすぐ下に、次に示す数行を追加します。

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

8d <serviceDebug includeExceptionDetailInFaults="false"/>という行のすぐ下に、次に示す数行を追加します。

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

8e <serviceHostingEnvironment multipleSiteBindingsEnabled="true" />という行のすぐ**上**に、次に示す数行を追加します。

```
<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. 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。
6. 値の"None"を"Windows"に変更し、ファイルを保存します。
7. 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、ユーザ本人であることを検証するために、カテゴリの異なる資格情報による2種類以上の認証メソッドを必要とするコンピュータアクセス制御手法です。

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、多因子認証を使って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、［**Syncnow(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. ［**Roles & Groups (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に適用させたい場合は、［**Roles&Groups(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［**All Users (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**］>［**AdvancedAuthentication**］の順に選択します。［**Enabled(有効)**］チェックボックスを選択し、各フィールドに用意された説明に従ってフォームを構成します。

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。

3.2 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。

3.2.1 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には、以下の手順を実行します。

1. ［**Configuration Management**］>［**New Managed Domain (新しい管理対象ドメイン)**］の順に選択します。
2. 管理対象にするドメインまたはコンピュータの名前を指定し、［**次へ**］をクリックします。
3. ［Access account (アクセスアカウント)］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を指定します。デフォルトでは、DRAは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、Deleted Objects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 Managed 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 ［**Configuration Management**］>［**Managed Domains**］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。

3.2.2 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サポートの有効化」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。
   - **Directory and Resource Administratorのサービスアカウントを使用する:** DRAのサービスアカウントを使用する場合です。
   - **次のアカウントを使用してこのドメインにアクセスする:** ドメインアクセスアカウントを使用する場合です。

   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。
   - **すべてのExchangeサーバにドメインアクセスアカウントを使用する:** ドメインアクセスアカウントを使用する場合です。
   - **次のアカウントを使用してすべてのExchangeサーバにアクセスする:** Exchangeアクセスアカウントを使用する場合です。

   重要: セカンダリサーバを使用している場合、［**UsethePrimaryAdministrationServerExchange 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。

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。

3.2.3 Microsoft Exchangeサポートの有効化

Microsoft Exchangeのサポートを有効にすると、Microsoft Exchangeのポリシー、統合化されたメールボックス、メールが有効なオブジェクト管理など、Exchangeの機能を最大限に利用できます。Microsoft Exchange Server 2010、Microsoft Exchange Server 2013以降のバージョンのプラットフォームで、管理サーバごとにMicrosoft Exchangeのサポートを有効または無効にすることができます。

Microsoft Exchangeサポートを有効にするには、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、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。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のサポートを有効にするには:

1 ［**PolicyandAutomationManagement(ポリシーと自動化の管理)**］>［**ConfigureExchangePolicies (Exchangeポリシーを設定)**］の順に選択します。

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。

   DRAがExchange管理サーバにどのバージョンの管理ツールがインストールされているかを検証し、適切なバージョンでのExchangeサポートが選択できるオプションを有効にします。

3 *Enable Exchange Policyがすでに選択され、Exchangeサポートが選択できるオプションが有効になっていない場合、*［**更新**］をクリックしてExchange管理サーバにどのバージョンの管理ツールがインストールされているかをDRAに検証させてください。

4 Exchange管理サポートを有効にするには、オプションを選択して、この管理サーバで管理するつもりのバージョンのExchangeのサポートを有効にしてください。

5 ［**OK**］をクリックします。

3.2.4 Exchange OnlineおよびSkype for Business Onlineの有効化

Office 365のSkype for Business OnlineとExchange Onlineのメールボックスを有効にするには、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。

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 OnlineとSkype for Business Onlineのサポートを有効にするには:

1 まだインストールしていない場合は、以下に示すMicrosoftコンポーネントをインストールしてください。
   - PowerShell 5.0+
   - IT Professional RTW用Microsoft Online Servicesサインインアシスタント

     https://www.microsoft.com/en-us/download/details.aspx?id=41950
   - Skype for Business Online、Windows PowerShellモジュール

     https://www.microsoft.com/en-us/download/details.aspx?id=39366
     - PowerShellを開き、Install-Module MSOnlineを実行します。

   詳細については、https://docs.microsoft.com/en-us/office365/enterprise/powershell/connect-to-office-365-powershellを参照してください。
2 Computer Managementコンソールを開き、**NetIQ Administration Service**を再起動します。
3 左のペインで［**Policy and Automation Management (ポリシーと自動化の管理)**］をクリックします。
4 ［**Policy and Automation Management (ポリシーと自動化の管理)**］>［**Configure Office 365 Policies (Office 365のポリシーを設定)**］の順に選択し、［**Enable Exchange Online Administration support (Exchange Online管理のサポートを有効にする)**］をクリックします。

3.2.5 Office 365のテナント追加

Exchange OnlineおよびSkype for Business Onlineを管理するためには、Office 365のテナントを1つまたは複数管理する必要があります。Office 365のテナントを管理できるようにするには、その前にExchange OnlineまたはSkype for Business Onlineのサポートを有効にしておく必要があります。

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。

Exchange OnlineまたはSkype for Business Onlineを有効にする方法の詳細については、次を参照してください。

- Microsoft Exchangeサポートの有効化
- Exchange OnlineおよびSkype for Business Onlineの有効化

Exchange Onlineのテナントを管理するようにDRAを設定する前に、Office 365のポータルに、次に挙げるパーミッションを持つアカウントを作成する必要があります。

DRAはこのアカウントを使用して、Exchange Onlineのすべての管理タスクを実行します。

- Office 365のユーザ管理の管理者
- Exchange Onlineの受信者管理

注: このアカウントは、Active Directory環境との同期化、または Microsoft Office 365のクラウドでホストされることのいずれかが可能です。DRAでは、Active Directoryに入っていなくとも管理タスクを実行できます。

アカウントの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。

Office 365のテナント管理とサービスプリンシパルの作成

DRAでオンラインポリシーを有効にしたら、新しいOffice 365テナントが管理可能な「**Office 365 Tenants**」という名称の設定管理から、新しいノードにアクセスできるようになります。

Office 365テナントを追加するには、［**Configuration Management**］>［**Office 365 Tenants (Office 365テナント)**］の順に選択し、ウィザードの指示に従ってOffice 365テナントのアクセスアカウントの追加や各種更新スケジュールの設定などの操作を行ってください。

DRAには、テナント内のオブジェクトに関するデータを収集するために、Directory Readersというパーミッションを持つサービスプリンシパルが必要です。

サービスプリンシパルを作成するには、Office 365で企業管理者の役割を持つユーザアカウントの資格情報をDRAに入力してDRAに自分用のサービスプリンシパルを作成させてもよいし、またはオフラインでサービスプリンシパルを作成することもできます。

注

- サービスプリンシパル作成のために入力された企業管理者の資格情報はDRA内に保存されません。
- オフラインでサービスプリンシパルを作成する場合は、ウィザードでサービスプリンシパルのIDとパスワードを指定する必要があります。

Office 365テナントの追加には数分かかる場合があります。テナントが正常に追加されると、DRAがそのテナントのためにFACR (Full Accounts Cache Refresh)を実行します。キャッシュの更新が完了すると、そのテナントに関するOffice 365ライセンスとメールボックスの管理を始めることができます。

4 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。

4.1 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。

4.1.1 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。

4.1.2 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。

4.1.3 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

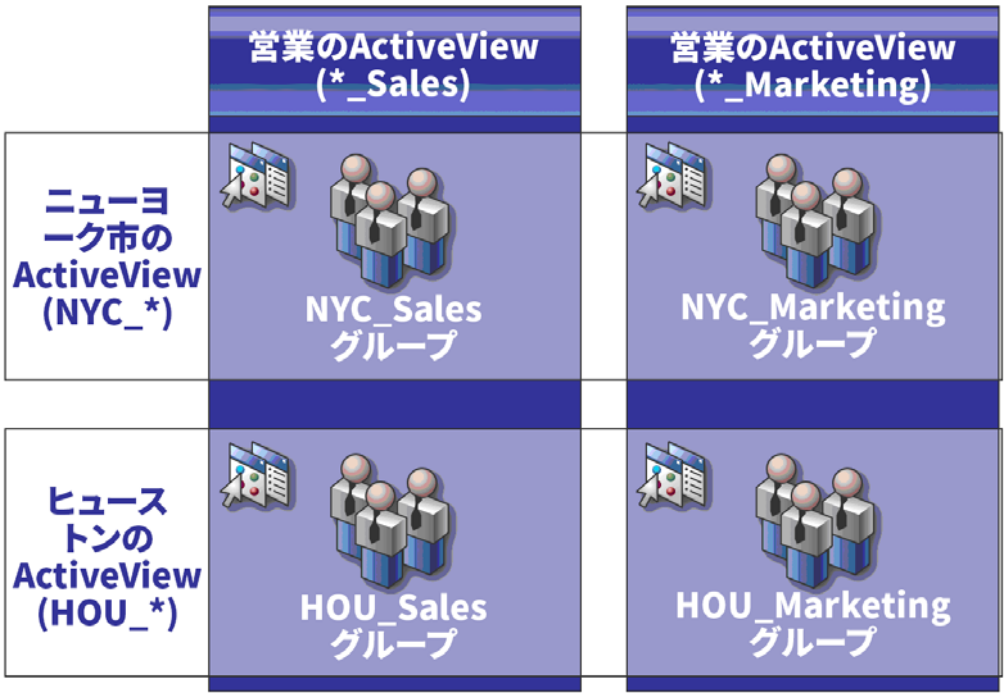
アシスタント管理者がJSmithさんのユーザアカウントに新しいパスワードを設定しようとすると、管理サーバは 「JSmith」を含むActiveViewをすべて見つけます。この検索は、ワイルドカードルールまたはグループメンバーシップを通じて直接JSmithさんを指定するActiveViewを探します。あるActiveViewが他のActiveViewを含んでいる場合、管理サーバはこれらのActiveViewも追加で検索対象にしてください。これらのActiveViewのいずれかでそのアシスタント管理者が*Reset User Account Password*という権限を持っているかどうかを管理サ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

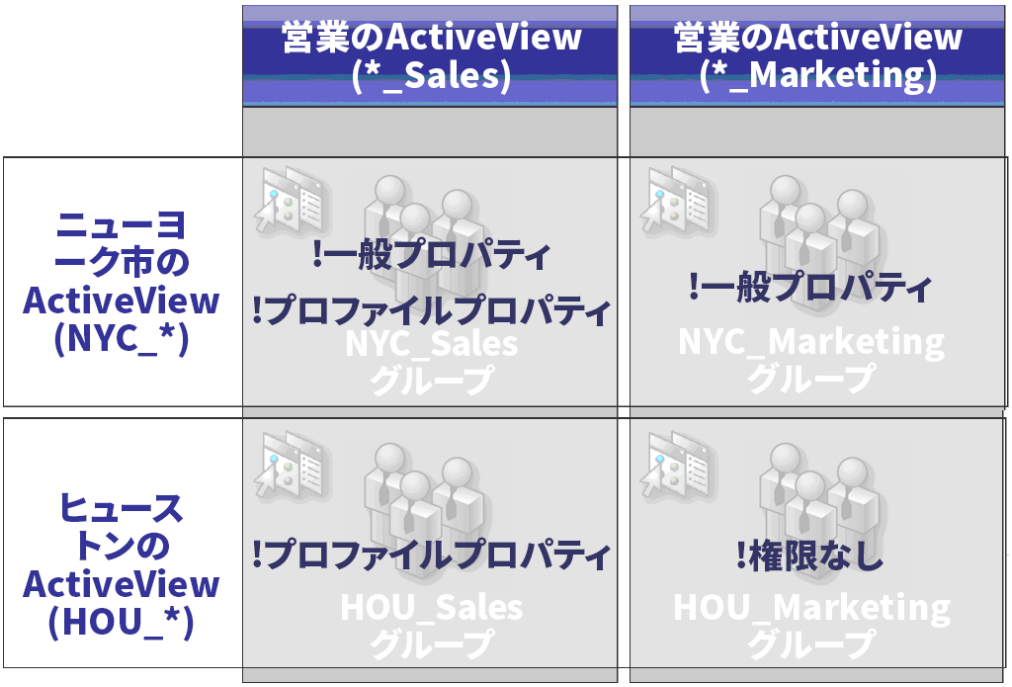
この例では、NYC_Salesグループが複数のActiveViewに表示されます。NYC_Salesグループのメンバーは、そのグループ名がNYC_*というActiveViewルールと一致するため、ニューヨーク市ActiveViewに表示されています。このグループは、*_SalesというActiveViewルールと一致するため、営業ActiveViewにも含まれます。同じグループを複数のActiveViewに含めることで、同一のオブジェクトを別々に管理することを異なるアシスタント管理者に許可することができます。

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。

4.2 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。

4.2.1 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 (自分の基準と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割り当ててください。個々の組み込み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。

4.2.2 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
- 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

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

ActiveView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、および Activeviewなどの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。

4.3 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。

4.3.1 組み込みの役割

組み込みの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。以下のリストで、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。

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。

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。

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。

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という役割も割り当ててください。

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。

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、Office 365の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。

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。

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。

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。

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。

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。

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。

DRAの管理

アシスタント管理者にすべての権限が与えられます。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。

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。

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。

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。

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。

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。

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、Office 365 Tenant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。

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。

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。

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。

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。

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。

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メールボックスのパーミッション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。

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。

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。

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。

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。

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。

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。

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。

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。

共用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。

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。

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。

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。

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。

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ターミナル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。

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。

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。

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。

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。

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。

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。

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。

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。

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。

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。

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。

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。

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。

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。

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。

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。

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。

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。

- 組み込み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。

4.3.2 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。

4.4 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コンソールで実行します。

4.4.1 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。

4.4.2 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。

4.4.3 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*という権限と*Create User and Modify Limited Properties*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*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

委任するタスク	割り当てる権限	拡張権限
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

4.5 委任の割り当て

委任割り当ては、Delegation and Configuration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。

5 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。

5.1 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
- 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。

5.1.1 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という組み込み役割に関連付けられたアシスタント管理者は、意図より大きな権限を持つことになる可能性があります。

5.1.2 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。

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	Windows2000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。

同一AVでのユーザの作成とクローン作成を防止する

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。

デフォルトでは、DRAの外で変更が行われた場合、テナントプロパティページでライセンス更新スケジュールも有効にしていない限り、Office 365のライセンス強制のために作成するポリシーが適用されません。

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。

5.1.3 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。

5.1.4 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、組み込み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。

5.1.5 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。

Office 365のポリシーの設定

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。

Office 365ルールにより、ユーザアカウントの作成および削除時のExchange OnlineによるOffice 365のメールボックスの管理方法を指定できます。

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。

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のポリシー

Office 365のメールボックス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。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。

無効な文字および文字長をOffice 365と同期するプロパティで制限するには、［**Office 365 Rules (Office 365ルール)**］をクリックし、［**Enforce online mailbox policies for invalid characters and character lengths (無効な文字と文字長についてオンラインメールボックスポリシーを強制する)**］チェックボックスを選択します。

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. ［**PolicyandAutomationManagement**］>［**ConfigureHomeDirectoryPolicies(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\HomeShare\」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HomeShare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、［**Homedirectorypermissions(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。

元のホームディレクトリと新しいホームディレクトリの名前と場所が同じ場合は、ホームディレクトリの名前を変更できます。ただし、ディレクトリの名前変更が失敗すると、新しいホームディレクトリが作成され、元のホームディレクトリの内容が新しいホームディレクトリに移動されて、元のホームディレクトリは削除されます。

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、［**Allowableparentpaths(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、パスワードの長さを6文字以上で127文字以下にする必要があります。パスワード長以外のすべての値がゼロに設定できます。

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: 組み込み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。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。

SDKの詳細については、DRAマニュアルのサイトで『「DRA REST Service Guide」』を参照してください。

5.1.6 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Username（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 ［**Enforcearchivenamingrulesduringmailboxupdates(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。

5.2 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。

5.2.1 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。

5.2.2 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。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。

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. ［**Automation Triggers (自動化のトリガ)**］をクリックします。
7. ［タスク］メニューで［**New Trigger (新規のトリガ)**］をクリックします。
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。
9. サマリの内容を確認し［**完了**］をクリックします。

5.3 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、ワークフロー自動化サーバで作成されます。このサーバはWebコンソールを介してDRAで統合されている必要があります。新しいフォームを設定するには、フォームプロパティで設定された**Launch Specific Workflow**オプションか**Trigger Workflow by Event**オプションのいずれかを持っている必要があります。これらのオプションの詳細を次に示します。

- **特定のワークフローの起動:** このオプションでは、DRAのためのワークフローサーバで動作中の使用可能なワークフローがすべて一覧表示されます。このリストにワークフローが表示されるためには、ワークフローがワークフロー自動化サーバ内のDRA_Workflowsというフォルダに作成されている必要があります。
- **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、定義済みのトリガでワークフローを実行する場合に使用されます。トリガを持つワークフローはワークフロー自動化サーバでも作成されます。

注: ［特定のワークフローの起動］で設定されたワークフローフォームのみに実行履歴が付き、それは［**管理**］>［**要求**］の順に選択して表示されるメイン検索ペインでクエリを行うことができます。

既存のフォームを変更したり新しいフォームを作成できます。新しいワークフローフォームを作成するには、または既存のフォームを変更するには、［**カスタマイズ**］>［**ワークフロー**］の順に選択します。

新しいフォームを作成するときは、次に示す基本手順に従ってください。

1. フォームが送信されたときに*指定のワークフロー*を実行するようにフォームを設定するか、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フォームを設定します。
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、フォームが最初に保存されるまで、新しいワークフローフォーム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。

ワークフローフォームのカスタマイズの詳細については、「ワークフローフォームのカスタマイズ」を参照してください。

6 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(AA)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。

6.1 アクティビティの監査

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。

6.1.1 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の詳細な内部操作や関連のあるサーバの情報も記録します。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。

DRAは、アーカイブしたログデータを安全に保存するために**NetIQLogArchiveData**というフォルダを使用します。このフォルダは「**ログアーカイブ**」と呼ばれます。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が管理レポートを表示するために使用するSQLサーバの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。この種のログ記録は、レジストリキーを修正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。

6.1.2 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 Security Manager > Configurationの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 *<LogArchiveDataへのパス>\<パーティション名>*のフォルダを見つけ、次の表に従って操作します。

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。

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/選択されなかった理由を理解するために、ナレッジベースの記事の「**Additional Information**」セクションを参照してください。記事の表題は「How do you configure the data retention period for DRA Logarchival Data?」です。

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。

6.2 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。

Activity Detailレポートは、ARMコンソールおよびDelegation and Configurationコンソールを通じてDRAをインストールするとすぐに使用でき、ネットワークの変化に関する最新の詳細を表示できます。

- 122ページのセクション6.2.1「レポート用のデータ収集の管理」
- 123ページのセクション6.2.2「組み込みのレポート」

6.2.1 レポート用のデータ収集の管理

DRAReporting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

ARMコンソールおよびDelegation and Configurationコンソールからアクセスできるこれらのレポートは、ドメイン内のオブジェクトの変更情報をリアルタイムで提供します。

DRA管理レポート

NetIQのReporting Center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。

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。

6.2.2 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。

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する場合*は、デフォルトの値(250)をその行数に書き換えます。

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 *特定の管理サーバだけをレポートに含める場合*は、［**Restrict query to these DRA servers (これらのDRAサーバにクエリを限定する)**］を選択し、レポートに含めるサーバの名前(1つまたは複数)を入力します。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。

7 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。

7.1 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。

ManageTemporaryGroupAssignments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。

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
- 一時グループ割り当てを表示する
- 一時グループ割り当てを削除/変更する
- 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とターゲットユーザが同じActiveView内にある必要があります。

注

- アシスタント管理者は、作成、変更、および、プライマリ管理サーバでのみ一時グループ割り当てを削除することができます。セカンダリ管理サーバ上の一時グループ割り当ては管理できません。
- DRAはMMSのレプリケーション中に一時グループ割り当てをプライマリ管理サーバからセカンダリ管理サーバに複製します。
- 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。

一時グループ割り当ての作成や使用の詳細については、『*ユーザガイド*』を参照してください。

7.2 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。

7.3 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、各属性に対し発生するAD DSイベントに伴って(たとえば説明や名前など)、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。

7.3.1 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/ KXdqI7S3EBhVyniE7iXvxIT6eB6IdcXQ5StkbIAHJgKzLN5FCOM5fZcITxyAPLW hbstaA7ZA0VbVC9MGlVIaAcjl3z7mpF9GKXsfDogbSeNlmHliXvH5KpOX3/ 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

7.3.2 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

7.4 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。

7.4.1 BitLocker回復パスワードの表示とコピー

あるコンピュータのBitLockerパスワードを紛失したら、Active Directoryでそのコンピュータのプロパティから回復パスワードキーを使用してリセットすることができます。パスワードキーをコピーし、エンドユーザに提供します。

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. ［**Accounts and Resources 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。

7.4.2 回復パスワードの検索

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

パスワードIDを使用して回復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 ［**Accounts and Resources 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**］をクリックします。

7.5 ActiveViewアナライザ

ActiveViewアナライザは、ActiveViewの問題の診断に役立ちます。たとえば、処理に時間がかかりすぎる、操作が実行されているのに未使用のActiveViews処理があるなど、ActiveView処理で異常がないかを確認できます。ActiveViewアナライザは、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のルールを変更する必要が生じる場合もあります。

7.5.1 ActiveViewデータの収集開始

ActiveViewアナライザを使うと、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 Webコンソールを起動し、管理者の資格情報でログインします。

2 ［**管理者**］>［**ActiveViewアナライザ**］の順に選択します。

3 ActiveViewアナライザのページで、次のように指定します。

   3a **アシスタント管理者:** データ収集対象にするアシスタント管理者を検索機能で見つけて追加します。

   3b **プロパティの表示:** (任意)収集の開始前に［プロパティの表示］の機能を使用してアシスタント管理者のプロパティを表示または変更します。

   3c **収集継続時間:** 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。指定した時間を超えると、データ収集が停止し、Mongoデータベースにインデックスが作成されます。

4 ［**収集を開始**］をクリックしてActiveViewのデータを収集します。

5 (任意)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。Mongoデータベースにインデックスが作成されます。

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。

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、Mongoデータベース内の既存のデータをActiveViewアナライザがクリアします。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。

7.5.2 Analyzerレポートの生成

Analyzerレポートを生成する前に、データ収集を停止したことと、インデックスがMongoデータベースで利用できることを確認してください。

Analyzerのレポートを生成するには:

1 ［**管理者**］>［**ActiveViewアナライザ**］の順に選択します。

2 ActiveViewアナライザのページで、アシスタント管理者が行った操作のリストが表示されます。次の中から選択してください。

- **実行された操作:** Analyzerデータ収集の対象にする操作を選択します。
- **長時間操作の上位:** 最も長く時間がかかった操作から何番目までを表示させるかを選択します。

3 ［**レポートを生成**］をクリックして、一致、不一致、および期間を含めたActiveView操作の詳細を解析レポートとして生成します。

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。

7.5.3 分析されたデータのパージ

パージというアクションは、重複データや未使用データを削除することでMongoデータベースの領域を解放することに役立ちます。

ActiveViewが分析した既存データをMongoデータベースからすべて消去するには、［**データのパージ**］をクリックします。

7.6 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。

7.6.1 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

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。

7.6.2 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永久に削除できます。

- 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
- 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する場合、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永久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。

---

8 クライアントのカスタマイズ

Delegation and ConfigurationのクライアントとARMのクライアント、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。

8.1 Delegation and Configuration and ARM Clientsのクライアント

このセクションは、Delegation and ConfigurationとARMの各クライアントのカスタマイズに役立つ情報を記載し、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が理解できます。

8.1.1 プロパティページのカスタマイズ

カスタマイズしたり、カスタムプロパティを実装することで、委任の構成とARMコンソールを拡張することができます。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コンソールおよびAccount and Resource Management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。
- Account and Resource ManagementコンソールとDelegation and Configurationコンソールを拡張して独自の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の値を選択できます。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。「How do I re-enable DRA to write events to the Application Event log in DRA 8.5 and later?」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

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固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 ［**Configuration Management**］>［**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 このカスタムページをAccountandResourceManagement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 ［**Configuration Management**］>［**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 ［**Configuration Management**］>［**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、［**ConfigurationManagement**］>［**UserInterface 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。

8.1.2 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。

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。オブジェクトのプロパティをパラメータとして指定する場合、オブジェクトのプロパティに対し読み取りのパーミッションと、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}"
- *Example2:* 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。

8.1.3 ユーザインタフェースのカスタマイズ

Delegation and Configuration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コンソールとAccount and Resource Managementコンソールの両方のタイトルバーに表示される情報を変更することができます。便利さと分かりやすさのために、コンソール起動に使用したユーザ名とコンソールが接続されている管理サーバを追加することができます。異なる資格情報を使用して複数の管理サーバに接続する必要のある複雑な環境では、どのコンソールを使用する必要があるかがすぐに認識できるようにするこの機能は便利です。

コンソールのタイトルバーを変更するには:

1. Delegation and Configuration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、表示を選択する列には、管理対象オブジェクトの検索結果を確認するときに表示させるカラムを選ぶには、［**すべての管理対象オブジェクト**］を選択します。

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

3 このノードで使用できるプロパティの一覧から、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、カラムを選択してから［**上へ移動**］または［**下へ移動**］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。

8.2 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、自動ワークフローの送信を伴うアシスタント管理者タスクの自動化に役立ちます。

8.2.1 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。組み込みのオブジェクトタイプの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組み込みであり、どの組み込みページがカスタマイズされ、どのページが組み込みではなく管理者によって作成されたかが簡単に識別できます。

オブジェクトプロパティページのカスタマイズ

オブジェクトプロパティフォームは、ページを追加または削除する、既存のページとフィールドを変更する、プロパティ属性のカスタムハンドラを作成するなどの方法でカスタマイズすることができます。作成されたカスタムハンドラは、その設定方法によって、プロパティフィールドが変化したときか、クエリ実行のためのプロンプトに管理者が応答したときに、自動的に実行されます。

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2つの操作タイプ(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クライアントで実行する主要な操作です。また、カスタマイズすることで、DRAでActive Directoryオブジェクトを管理するときの管理者の効率と操作性が向上する可能性があります。

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 ［**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(作成または編集)を選択します。

4 ［**編集**］ボタン(✎)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］
   - プロパティページを選択し、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更する: ↑ ↓
     - 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する: ＋ または［フィールドの追加］
     - 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。

新しいオブジェクトプロパティページの作成

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 ［カスタマイズ］>［プロパティページ］の順に選択します。
3 ［タスク］の下の［新しいアクションの作成］をクリックします。
4 名前、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。
5 必要に応じて、新しいフォームをカスタマイズします。詳細については、「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。

8.2.2 ワークフローフォームのカスタマイズ

ワークフローフォームは、作成または変更時にWebサーバに保存され、Webコンソール内でアクセスします(［カスタマイズ］>［ワークフロー］ページ)。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。フォームをカスタマイズすると、一歩進んだ自動化が可能になり、アシスタント管理者がフォームを使ってオブジェクト管理タスクを遂行するときに使い勝手が良いと感じられるフォームにすることができます。

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。プロパティの追加とカスタマイズに対するインタフェースの振る舞いは、ワークフロー自動化フォームの中では、オブジェクトプロパティのカスタマイズと同じです。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。

たとえば、他のフィールド値のクエリ、値の更新、フィールドの読み込み専用状態の切り替え、および設定済み変数に基づいてフィールドを表示または非表示にするときなどにプロパティのカスタムハンドラが使用されます。

フォームのロードハンドラにより、ユーザがフォームをカスタマイズできます(コントロールの初期化が一般的)。フォーム送信ハンドラでは、ユーザが検証を行ったり、場合によって異常の発生時に送信をキャンセルすることができます。

また、DRAではカスタムハンドラの作成が簡単です。選択可能なJavaScript (JS)マクロがいくつか用意されており、そのうちの1つをカスタムハンドラ作成検証プロセスで選ぶことができます。

カスタムハンドラ作成の基本手順:

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。そこまで進むには、プロパティフィールドにある編集ボタン( )からオブジェクトプロパティのカスタムハンドラにアクセスします。ワークフローフォームまたはオブジェクト作成ページの［フォームプロパティ］からフォームロードハンドラおよびフォーム送信ハンドラにアクセスします。

1. 該当するタカスタムハンドラのタブをクリックし、ページ( )を有効にします。
   - カスタムハンドラ
   - フォームロードハンドラ
   - フォーム送信ハンドラ
2. ドロップダウンメニューからカスタムハンドラを選択して、実行時間を選択します。通常、実行時間には2番目か3番目のオプションを使用します。

   注: 一般的にカスタムハンドラは1つで十分ですが、ハンドラ同士がリンクするようにスクリプト内のフロー制御を設定すれば複数のハンドラを使用することもできます。

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。設定オプションがハンドラの種類によって異なりますが、すべてのハンドラがJavaScriptから実行されます。

   独自のVanilla JavaScriptエントリを作成したり、組み込みマクロを使用することもできます。

   - **LDAPまたはRESTのクエリハンドラ:**
     1. 静的な値をベースにしたクエリを実行する場合は、［**接続情報**］および［**クエリパラメータ**］を定義してください。

        動的なクエリが必要な場合は、必須フィールドにプレースホルダのテキストを入力してください。スクリプトの実行にはこれが必須です。スクリプトが仮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. クエリ前のアクションで、**Global**、**Query**、**Form Field**のうちマクロを1つ選択します。

3. ドロップダウンリストからマクロを選択し、マクロを挿入します(**</>マクロの挿入**)。
4. 必要に応じて他のマクロを挿入し、必要な値を指定してスクリプトを完成させます。

   例として、ユーザが入力したグループ名がActive Directoryにすでに存在しないことを、フォームが送信されたときに［クエリ前アクション］のスクリプトで検証します。

   ユーザが入力した名前を使用してLDAPクエリを作成する必要があります。Field()というマクロを使用して名前フィールドの値にアクセスしてクエリ文字列を構築します。それを今度はFilter()マクロを使用するクエリフィルタとして設定します。

   ```
   Filter() = '(&(objectCategory=group)(objectClass=group)(name=' +
   Field(name) + '))';
   ```

5. 前の例を実行して、［クエリ後アクション］でクエリの返す結果をチェックします。結果はクエリに一致したオブジェクトの配列として返されます。そこで、配列の長さが0より大きいかどうかを調べる必要があります。

   一致するグループが見つかると、Cancel()というマクロを使用してフォーム送信をキャンセルし、そのマクロにユーザに表示するオプションメッセージを渡します。

   if (QueryResults().length > 0) { Cancel('A group with that name already exists, please enter a unique name.');}

- **スクリプト:** JavaScriptのカスタムコードを挿入するか、マクロを使用してスクリプトを作成します。
- **DRAクエリ:** クエリパラメータについては、JSON形式でペイロードを定義します。そして、前に説明したLDAPクエリとRESTクエリの場合と同様の方法でマクロを使用します。
- **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ら、LDAPクエリとRESTクエリについて前に説明したように、同じような方法でマクロを使用します。ただし、クエリ前アクションとクエリ後アクションの代わりに、表示前のアクションと閉じた後のアクションのためのマクロスクリプトを作成します。

4 フォームを保存する前に［**ハンドラのテスト**］をクリックしてスクリプトを検証します。

これによりテストの結果の概要が生成され、実行結果が表示されます。

注: そのハンドラがフォームの現在の状態に依存している場合(たとえばフィールドに値がある)、フォームを編集するときにデータがまったくロードされないため、正常に実行されません。そのようなケースではフォームエディタの外でハンドラをテストする必要があります。方法は、カスタマイズの内容を保存してから、適切なフォームを表示し、必要なデータを記入します。

8.2.3 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する

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を使ってカスタマイズすることができます。その位置はDRAの製品名のすぐ右です。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でタイトルのブランディング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 ［**カスタマイズ**］>［**ブランディング**］の順に選択します。

3 会社のロゴを追加するには、ロゴイメージをWebサーバのcomponents\lib\imgに保存します。

4 ブランディングのカスタマイズのページの3つのフィールドに該当する情報があれば、必要な情報を追加して変更内容を保存します。

9 ツールとユーティリティ

以下のセクションでは、DRAの提供する診断ユーティリティ、削除オブジェクトユーティリティ、正常性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説明します。

9.1 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、DRA管理者のアカウントを使って管理サーバのコンピュータにログオンし、Program Files (x86)\NetIQ\DRAフォルダからDRADiagnosticUtil.exeを実行してください。

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。

9.2 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。

9.2.1 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

9.2.2 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]}

9.2.3 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。

9.2.4 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
```

9.3 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。 ◆ 製品ライセンスをインストールまたは更新する(ライセンスの検証) ◆ ADLDSインスタンスをバックアップする(ADLDSインスタンスのバックアップ)
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。

9.4 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

- 155ページのセクション9.4.1「ごみ箱ユーティリティに必須のパーミッション」
- 155ページのセクション9.4.2「ごみ箱ユーティリティの構文」
- 155ページのセクション9.4.3「ごみ箱ユーティリティのオプション」
- 155ページのセクション9.4.4「ごみ箱ユーティリティの例」

9.4.1 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

9.4.2 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}

9.4.3 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。

9.4.4 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
```