NetIQ Directory and Resource Administrator インストールガイド

2021 年 6 月

保証と著作権

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

目次

本書の内容

『*インストールガイド*』では、NetIQ Directory and Resource Administrator (DRA) およびその統合コンポーネントの計画、インストール、設定に関する情報が取り上げられています。

このマニュアルでは、インストール手順について説明し、DRA をインストールおよび設定する際に正しい決定ができるようにします。

本書の読者

このマニュアルには、DRA をインストールするユーザにとって必要な情報が記載されています。

その他のマニュアル

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

連絡先情報

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

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

はじめに

NetIQ Directory and Resource Administrator(DRA) のすべてのコンポーネントをインストールして構成する前に、企業のために DRA が果たす基本理念と、製品アーキテクチャにおける各 DRA コンポーネントの役割について理解しておく必要があります。

1 Directory and Resource Administrator とは

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

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

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

- **Azure とオンプレミスの Active Directory、Exchange、および Skype for Business へのサポート :** Azure とオンプレミスの Active Directory、オンプレミスの Exchange Server、オンプレミスの Skype for Business、Exchange Online、および Skype for Business Online を管理できます。
- **ユーザおよび管理者の特権アクセスの細かい制御 :** 特許取得済みの ActiveView テクノロジにより、特定の責務に必要な権限だけを委任し、特権格上げを防止することができます。
- **カスタマイズ可能な Web コンソール :** 直観的な方法により、技術者でなくても、限定された (そして割り当てられた) 機能および権限を通して、簡単かつ安全に管理タスクを行えます。
- **詳細なアクティビティの監査およびレポーティング :** 製品で実行されたすべてのアクティビティが包括的に監査レコードに記録されます。長期データを安全に保管でき、AD へのアクセスを制御するためのプロセスを実施していることを監査機関 (PCI DSS、FISMA、HIPAA、NERC CIP など) に証明できます。
- **IT プロセスの自動化 :** プロビジョニングや認証の取り消し、ユーザとメールボックスの操作、ポリシーの適用、セルフサービスタスクの制御など、さまざまなタスクのワークフローを自動化できます。これにより、ビジネスの効率を高め、手動で繰り返し行う管理作業を削減することができます。
- **運用上の完全性 :** 管理者にきめ細かいアクセスコントロールを提供し、システムおよびリソースへのアクセスを管理することで、システムおよびサービスのパフォーマンスと可用性に影響する悪意のある変更や間違った変更を防止できます。
- **プロセスの適用 :** 重要な変更管理プロセスの完全性を維持し、生産性の向上、エラーの減少、時間の節約、管理効率の向上に貢献します。

- **Change Guardian との統合 :** DRA および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。

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

特権アクセスを管理するために一貫して使用する DRA のコンポーネントには、プライマリサーバおよびセカンダリサーバ、管理コンソール、レポーティングコンポーネント、ワークフロープロセスを自動化する Workflow Automation Engine などがあります。

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

DRA ユーザのタイプ	ユーザインタフェース	管理サーバ
DRA 管理者 (本製品の構成を管理する人)	Delegation and Configuration Console (委任および環境設定コンソール)	プライマリサーバ
上級管理者	DRA Reporting Center セットアップ (NRC) PowerShell*(オプション)* CLI*(オプション)* DRA ADSI プロバイダ *(オプション)*	任意の DRA サーバ
ヘルプデスクの臨時管理者	Web コンソール	任意の DRA サーバ

DRA 管理サーバ

DRA 管理サーバは、構成データ (環境、委任されたアクセス、およびポリシー) を保管し、オペレータのタスクおよび自動化タスクを実行し、システム全体のアクティビティを監査します。このサーバは、コンソールおよび API レベルのクライアントをいくつかサポートしながらも、マルチマスタセット (MMS) のスケールアウトモデルにより、冗長性と地理的分離に対しても高い可用性を実現できるように設計されています。このモデルでは、すべての DRA 環境に、複数のセカンダリ DRA 管理サーバと同期する 1 つのプライマリ DRA 管理サーバが必要になります。

Active Directory ドメインコントローラには管理サーバをインストールしないようにすることを強くお勧めします。DRA が管理するドメインごとに、管理サーバと同じサイトにドメインコントローラを 1 つ以上配置してください。デフォルトでは、管理サーバはすべての読み込み / 書き込み操作で最も近いドメインコントローラにアクセスします。そのため、パスワードリセットなどのサイト固有のタスクを実行する場合は、サイト固有のドメイン

コントローラを指定して操作を処理できます。ベストプラクティスとして、セカンダリ管理サーバ 1 台をレポーティング、バッチ処理、自動化されたワークロードのために専用で使用することを検討してください。

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

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

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

Web コンソール

Web コンソールは、Web ベースのユーザインタフェースです。これを使用してアシスタント管理者が接続ドメインやサービスの委任オブジェクトを素早く簡単に表示および管理できます。企業ブランディングやオブジェクトプロパティのカスタマイズなど、管理者が Web コンソールのインタフェースと使用法をカスタマイズすることができます。

レポーティングコンポーネント

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

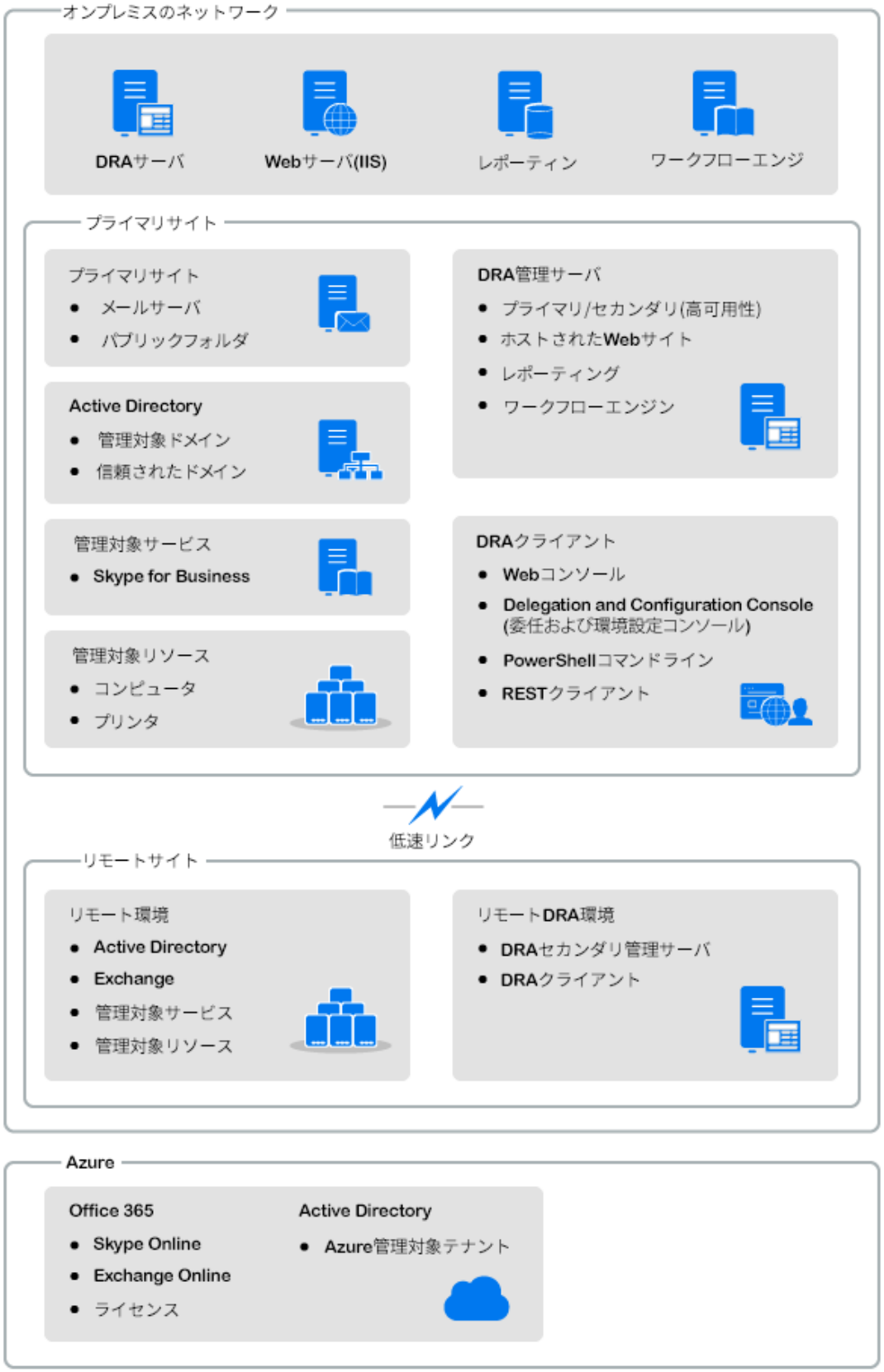
- Active Directory オブジェクトのリソースレポート
- Active Directory オブジェクトデータレポート
- Active Directory サマリレポート
- DRA 構成レポート
- Exchange 構成レポート
- Office 365 Exchange Online レポート
- 詳細なアクティビティトレンドレポート (月別、ドメイン別、ピーク別)
- DRA アクティビティの要約レポート

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

Workflow Automation Engine

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

製品アーキテクチャ


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

II 製品のインストールとアップグレード

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

3 展開の計画

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

テスト済みのリソースの推奨構成

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

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

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

仮想環境リソースのプロビジョニング

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

- ストレージを「シックプロビジョニング」として割り当てます

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

必要なネットワークポートおよびプロトコル

このセクションでは、DRA 通信のポートとプロトコルについて説明します。

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

コンポーネントテーブル :

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

DRA 管理サーバ

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

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

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

DRA REST サーバ

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

Web コンソール (IIS)

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

DRA Delegation and Administration コンソール

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

ワークフローサーバ

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

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

サポートされているプラットフォーム

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

管理対象システム	前提条件
Azure Active Directory	Azure 管理を有効にするには、次の PowerShell モジュールをインストールする必要があります。 ◆ Azure Active Directory V2(AzureAD)2.0.2.4 バージョン以降 ◆ AzureRM.Profile 5.8.2 バージョン以降 ◆ Exchange Online PowerShell V2 1.0.1 以降 新しい Azure PowerShell モジュールをインストールするには、PowerShell 5.1 または最新のモジュールが必要です。
Active Directory	◆ Microsoft Server 2012 R2 ◆ Microsoft Server 2016 ◆ Microsoft Windows Server 2019
Microsoft Exchange	◆ Microsoft Exchange 2013 ◆ Microsoft Exchange 2016 ◆ Microsoft Exchange 2019
Microsoft Office 365	◆ Microsoft Exchange Online
Skype for Business	◆ Microsoft Skype for Business 2015
変更履歴	◆ Change Guardian5.1 以降
データベース	◆ Microsoft SQL Server 2016
Web ブラウザ	◆ Google Chrome ◆ Mozilla Firefox ◆ Microsoft Edge

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

DRA 管理サーバおよび Web コンソールの要件

DRA コンポーネントには、次のソフトウェアおよびアカウントが必要です。

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

ソフトウェアの必要条件

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

コンポーネント	前提条件
管理サーバ	**Directory and Resource Administrator:** ◆ Microsoft .Net Framework 4.8 以降 ◆ Microsoft Visual C++ 2015-2019再頒布可能パッケージ(x64および x86) ◆ Microsoft Message Queuing ◆ Microsoft Active Directory ライトウェイトディレクトリサービス役割 ◆ リモートレジストリサービスが開始済みであること ◆ Microsoft インターネットインフォメーションサービス URL Rewrite Module ◆ Microsoft インターネットインフォメーションサービスアプリケーション要求のルーティング **注 :** DRA REST Endpoint and Service は、管理サーバと一緒にインストールされます。 **Microsoft Office 365/Exchange Online 管理 :** ◆ Windows PowerShell用Windows Azure Active Directoryモジュール ◆ Windows PowerShell モジュール ◆ Exchange Online PowerShell V2 モジュール ◆ Exchange Online タスクのクライアント側で、WinRM for Basic 認証を有効にします。 詳細については、「サポートされているプラットフォーム」を参照してください。
ユーザインタフェース	**DRA のインタフェース :** ◆ Microsoft .Net Framework 4.8 ◆ Microsoft Visual C++ 2015-2019再頒布可能パッケージ(x64および x86)
PowerShell 拡張機能	◆ Microsoft .Net Framework 4.8 ◆ PowerShell 5.1 以降
DRA Web コンソール	**Web サーバ :** ◆ Microsoft .Net Framework 4.x > WCF Services > HTTP Activation (HTTP のアクティベーション) ◆ Microsoft Internet Information Server 8.0、8.5、10 ◆ Microsoft インターネットインフォメーションサービス URL Rewrite Module ◆ Microsoft インターネットインフォメーションサービスアプリケーション要求のルーティング

サーバドメイン

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

アカウント要件

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

DRA サービスアカウント	NetIQ 管理サービスを実行するために必要な権限	◆「Distributed COM Users」権限用
		◆ AD LDS 管理者グループのメンバー
		◆ アカウントオペレータグループ
		◆ ログアーカイブグループ (OnePointOp ConfgAdms & OnePointOp)
		◆ STIG 手法を使用して DRA をサーバにインストールする場合、DRA サービスアカウントユーザに対して次の［アカウントタブ］>［**[アカウントオプション]**］のいずれかを選択する必要があります。
		  ◆ Kerberos AES 128 ビット暗号化
		  ◆ Kerberos AES 256 ビット暗号化
		注
		◆ 最小特権のドメインアクセスアカウントの設定方法については、「最小特権 DRA アクセスアカウント」を参照してください。
		◆ DRA のグループ管理対象サービスアカウントの設定の詳細については、『*DRA 管理者ガイド*』の「グループ管理対象サービスアカウントの DRA サービスの構成」を参照してください。

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

最小特権 DRA アクセスアカウント

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

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

- builtInDomain オブジェクトに対するフルコントロール
- コンピュータオブジェクトに対するフルコントロール
- 接続ポイントオブジェクトに対するフルコントロール
- 連絡先オブジェクトに対するフルコントロール
- コンテナオブジェクトに対するフルコントロール
- グループオブジェクトに対するフルコントロール
- InetOrgPerson オブジェクトに対するフルコントロール
- MsExchDynamicDistributionList オブジェクトに対するフルコントロール
- MsExchSystemObjectsContainer オブジェクトに対するフルコントロール
- msDS-GroupManagedServiceAccount オブジェクトに対するフルコントロール

- 部門オブジェクトに対するフルコントロール
- プリンタオブジェクトに対するフルコントロール
- publicFolder オブジェクトに対するフルコントロール
- 共有フォルダオブジェクトに対するフルコントロール
- ユーザオブジェクトに対するフルコントロール

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

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

注

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

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

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

- CSAdministrator 役割
- CSUserAdministrator 役割と CSArchiving 役割

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

- パブリックフォルダ管理
- メールが有効なパブリックフォルダ

Azure テナントアクセスアカウント : Azure テナントのアクセスアカウントには、次の Azure Active Directory 権限を割り当ててください。

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

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

NetIQ 管理サービスアカウントの権限 :

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

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

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

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

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

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

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

この設定にアクセスするには、次の手順に従います。

1. ドメインコントローラのグループポリシー管理コンソールを開きます。
2. ノードツリー内の［ **[ドメイン]**］> ［ **[ドメインコントローラ]**］> ［ **[グループポリシーオブジェクト]**］を展開します。
3. ［ **[デフォルトのドメインコントローラポリシー]**］を右クリックし、［ **[編集]**］を選択して、このポリシーの GPO エディタを開きます。
4. GPO エディタのノードツリーで、［ **[コンピュータの環境設定]**］> ［ **[ポリシー]**］> ［ **[Windows の設定]**］> ［ **[セキュリティの設定]**］> ［ **[ローカルポリシー]**］の順に展開します。
5. ポリシーペインの［ **[Network access: Restrict clients allowed to make remote calls to SAM (ネットワークアクセス : SAM へのリモートコールを行うことができるクライアントを制限する)]**］をダブルクリックし、［ **[Define this policy setting (このポリシー設定を定義する)]**］を選択します。
6. ［ **[Edit Security (セキュリティの編集)]**］をクリックし、リモートアクセスに対して［ **[許可]**］を有効にします。DRA サービスアカウントがユーザまたは管理者グループの一部として含まれていない場合は、追加します。
7. 変更を適用します。これにより、セキュリティデスクリプタである O:BAG:BAD:(A;;RC;;;BA) がポリシー設定に追加されます。

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

レポーティングの要件

DRA Reporting の要件は次のとおりです。

ソフトウェアの必要条件

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

コンポーネント	前提条件
NetIQ Reporting Center(v3.3)	**データベース :** ◆ Microsoft SQL Server 2016 ◆ Microsoft SQL Server Reporting Services ◆ SQL Agent ジョブを管理するドメイン管理者は、Microsoft SQL Server Integration Services のセキュリティ権限が必要です。権限がない場合、一部の NRC レポートを処理できない場合があります。 **Web サーバ :** ◆ Microsoft Internet Information Server 8.0、8.5、10 ◆ Microsoft IIS コンポーネント ◆ ASP .NET 4.0 **Microsoft .NET Framework 3.5:** ◆ NRC インストーラを実行するために必要です ◆ DRA Reporting Services 設定のために、DRA プライマリサーバにも必要です **注 :** SQL Server コンピュータに NetIQ Reporting Center(NRC) をインストールする場合、NRC をインストールする前に .NET Framework 3.5 を手動でインストールしておかなければならないことがあります。 **Communication Security Protocol(通信セキュリティプロトコル):** ◆ SQL Server は TLS 1.2 をサポートする必要があります。詳細については、TLS 1.2 support for Microsoft SQL Server(Microsoft SQL Server の TLS 1.2 サポート) を参照してください。 ◆ SQL Server には、更新された TLS 対応ドライバが DRA サーバにインストールされている必要があります。推奨ドライバは、最新の Microsoft® SQL Server® 2012 Native Client - QFE です。 ◆ SQL Server と DRA 管理サーバの両方のオペレーティングシステムで同じ TLS プロトコルバージョンがサポートされている必要があります。たとえば、TLS 1.2 だけが有効になっています。
DRA Reporting	**データベース :** ◆ Microsoft SQL Server Integration Services ◆ Microsoft SQL Server エージェント

ライセンスの要件

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

管理サーバをインストールした後は、ヘルスチェックユーティリティを使用して、購入したライセンスをインストールすることができます。無制限のユーザアカウントやメールボックスを 30 日間管理できる試用版ライセンスキー (TrialLicense.lic) もインストールパッケージに含まれています。

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

4 製品のインストール

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

DRA 管理サーバのインストール

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

DRA サーバパッケージには、次の機能があります。

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

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

対話型インストールのチェックリスト :

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

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

DRA クライアントをインストールする

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

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

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

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

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

Workflow Automation のインストールと設定の構成

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

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

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

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

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

上記で参照したドキュメントは、DRA マニュアルサイトから参照できます。

DRA Reporting のインストール

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

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

5 製品アップグレード

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

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

DRA アップグレードの計画

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

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

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

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

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

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

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

重要

- 以前のバージョンの DRA に Account and Resource Management(ARM) コンソールがインストールされている場合は、アップグレードする際に ARM コンソールが削除されます。
- DRA 9.x バージョンから DRA サーバをアップグレードすると、管理対象テナントが DRA から削除されます。Azure を使用してこれらのテナントを継続して使用するには、アップグレード後にテナントを追加する必要があります。テナント追加の詳細については、『*DRA 管理者ガイド*』の「Azure アプリケーションの作成および Azure テナントの追加」を参照してください。
- Exchange 2010 は DRA 10.1 ではサポートされていないため、DRA 9.x からアップグレードした場合、Exchange が無効になります。アップグレード後も引き続き Exchange の操作を実行するには、Delegation and Configuration Console (委任および環境設定コンソール) の［ **[Enable Exchange Policy (Exchange ポリシーの有効化]**］オプションを無効にし、再度有効にします。ポリシーをリセットするには、両方の変更が「適用」されている必要があります。

  このポリシーの設定の詳細については、『*DRA 管理者ガイド*』の「「Enabling Microsoft Exchange (Microsoft Exchange の有効化)」」を参照してください。

アップグレード前のタスク

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

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

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

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

アップグレード前のトピック：

前バージョンの DRA を実行する専用ローカル管理サーバの使用

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

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

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

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

新規のセカンダリサーバの設定

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

既存のセカンダリサーバの使用

既存のセカンダリ管理サーバを、前バージョンの DRA 専用のサーバとして使用することができます。セカンダリ管理サーバをアップグレードする予定がないサイトについては、このオプションを考慮する必要があります。既存のセカンダリサーバを専用サーバにできな

い場合は、新規の管理サーバをこの目的のためにインストールすることを考慮してください。1 つ以上のセカンダリサーバを前バージョンの DRA を実行するための専用サーバにすれば、アップグレードが完了するまでの間、アシスタント管理者が中断なしで前バージョンの DRA を使い続けることができます。このオプションは、中央管理モデルを採用している非常に大規模な環境に適しています。

前バージョンの DRA サーバセットの同期

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

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

既存のサーバセットを同期させるには、次の手順を実行します。

1. プライマリ管理サーバに Built-in Admin としてログオンします。
2. Delegation and Configuration Console (委任および環境設定コンソール) を開き、[**[Configuration Management (環境設定管理)]**] を展開します。
3. **[[管理サーバ]]** をクリックします。
4. 右側のウィンドウで、このサーバセットに属する適切なプライマリ管理サーバを選択します。
5. [**[プロパティ]**] をクリックします。
6. [同期スケジュール] タブで、[**[今すぐ更新]**] をクリックします。
7. 同期が正しく完了したことと、すべてのセカンダリ管理サーバが使用可能であることを確認します。

管理サーバのレジストリのバックアップ

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

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

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

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

管理サーバのレジストリをバックアップするには、次の手順を実行します。

1. regedit.exe を実行します。
2. HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Mission Critical Software\OnePoint ノードを右クリックし、[**[エクスポート]**] を選択します。
3. レジストリキーを保存するファイルの名前と場所を指定し、[**[保存]**] をクリックします。

DRA 管理サーバのアップグレード

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

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

アップグレードプロセスを複数の段階に分けて、一度に 1 つの MMS をアップグレードすることもできます。アップグレードプロセスでは、旧バージョンの DRA を実行するセカンダリサーバと現バージョンの DRA を実行するサーバを一時的に同じ MMS に含めることもできます。DRA は、旧バージョンの DRA を実行する管理サーバと現バージョンの DRA を実行するサーバとの同期をサポートしています。ただし、同じ管理サーバまたはクライアントコンピュータ上で旧バージョンの DRA と現バージョンの DRA を実行することはできません。

重要 : DRA アップグレードインストールでは、DRA 9.x バージョンから DRA 10.x バージョンに DRA サーバをアップグレードした場合、次の変更が行われます。

- UCH およびワークフロー自動化サーバのユーザ環境設定を Web コンソールから Delegation and Configuration Console (委任および環境設定コンソール) に移動します
- 古い Web コンポーネントをサーバから削除します。
- 管理対象のテナントを削除します。

  テナントの追加の詳細については、『*DRA 管理者ガイド*』の「「Azure テナントの設定」」を参照してください。
- 以前のリリースで Account and Resource Management コンソールをインストールしており、DRA 10.x バージョンにアップグレードする場合には、Account and Resource Management コンソールが削除されます。

- MMS のアップグレード時には、プライマリサーバが最初にアップグレードされ、続いてセカンダリサーバがアップグレードされます。セカンダリサーバで一時的なグループの割り当てを正常に複製するには、**[マルチマスタ同期スケジュール]** を手動で実行、またはスケジュールされた実行を待機します。
- Exchange 2010 は DRA 10 ではサポートされていないため、DRA 9.x からアップグレードした場合、Exchange が無効になります。アップグレード後も引き続き Exchange の操作を実行するには、Delegation and Configuration Console (委任および環境設定コンソール) の［ **[Enable Exchange Policy (Exchange ポリシーの有効化]**］オプションを無効にし、再度有効にします。ポリシーをリセットするには、両方の変更が「適用」されている必要があります。

  このポリシーの設定の詳細については、『*DRA 管理者ガイド*』の「「Enabling Microsoft Exchange (Microsoft Exchange の有効化)」」を参照してください。

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。
テストアップグレードを実行する	潜在的な問題を見つけて実働時のダウン時間を最小限に抑えるために、実験環境でテストアップグレードを実行します。
アップグレードの順序を決定する	サーバセットをアップグレードする順序を決定します。
アップグレードのために各 MMS を準備する	アップグレードに備えて各 MMS の準備を整えます。詳細については、「アップグレード前のタスク」を参照してください。
プライマリサーバをアップグレードする	適切な MMS 内のプライマリ管理サーバをアップグレードします。詳細については、「プライマリ管理サーバのアップグレード」を参照してください。
新規セカンダリサーバをインストールする	*(オプション)* リモートサイトでのダウンタイムを最小限に抑えるには、最新バージョンの DRA を実行するローカルのセカンダリ管理サーバをインストールします。詳細については、「現バージョンの DRA のローカルセカンダリ管理サーバのインストール」を参照してください。
ユーザインタフェースを展開する	ユーザインタフェースをアシスタント管理者に展開します。詳細については、「DRA ユーザインタフェースの展開」を参照してください。
セカンダリサーバをアップグレードする	MMS 内のセカンダリ管理サーバをアップグレードします。詳細については、「セカンダリ管理サーバのアップグレード」を参照してください。
DRA Reporting をアップグレードする	DRA Reporting をアップグレードします。詳細については、「Reporting のアップグレード」を参照してください。
正常性検査ユーティリティを実行する	アップグレードの一部としてインストールされた正常性検査ユーティリティを実行します。問題があれば解決します。

ステップ	詳細
Azure テナントの追加 ***(アップグレード後)***	*(オプション、アップグレード後)* アップグレード前に Azure テナントの管理をしていた場合は、アップグレード中にテナントが削除されます。これらのテナントを再度追加し、Delegation and Configuration Console (委任および環境設定コンソール) から完全なアカウントキャッシュの更新を実行する必要があります。詳細については、『*DRA 管理者ガイド*』の「「Azure テナントの設定」」を参照してください。
Web コンソールの環境設定の更新 ***(アップグレード後)***	*(条件付き、アップグレード後)* アップグレード前に以下のいずれかの Web コンソール環境設定がある場合は、アップグレードインストールの完了後に更新する必要があります。 ◆ デフォルトサーバ接続が有効 ◆ 変更された設定ファイル 詳細については、「Web コンソール環境設定の更新 - インストール後」を参照してください。

サーバのアップグレードに関するトピック :

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

プライマリ管理サーバのアップグレード

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

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

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

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

現バージョンの DRA のローカルセカンダリ管理サーバのインストール

ローカルサイトで現バージョンの DRA を実行する新規のセカンダリ管理サーバをインストールすれば、コストのかかるリモートサイトへの接続を最小限に抑えるとともに全体的なダウンタイムを短縮することができ、ユーザインタフェースの展開をより迅速に進められます。この手順はオプションですが、これによってアシスタント管理者は、展開が完了するまでの間アップグレードプロセス全体を通じて、現行バージョンと前バージョンの両方の DRA を使用できるようになります。

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

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

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

DRA ユーザインタフェースの展開

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

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

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

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

セカンダリ管理サーバのアップグレード

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

たとえば、典型的なアップグレードパスには、次の手順が含まれます。

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

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

Web コンソール環境設定の更新 - インストール後

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

デフォルト DRA サーバ接続

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

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

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

Web コンソールのログイン設定

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

Workflow Automation のアップグレード

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

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

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

Reporting のアップグレード

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

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

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

III 製品の構成

この章では、Directory and Resource Administrator を初めてインストールする場合に必要な構成ステップと手順について大まかに説明します。

6 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 ライセンスを適用する	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。
Delegation and Configuration を開く	DRA サービスアカウントを使用して、Delegation and Configuration Console (委任および環境設定コンソール) がインストールされているコンピュータにログオンします。コンソールを開きます。
最初の管理対象ドメインを DRA に追加する	最初の管理対象ドメインを DRA に追加します。 **注 :** 最初のアカウントのフル更新が完了したら、権限の委任を開始できます。
管理対象ドメインおよびサブツリーを追加する	*オプション:* その他の管理対象ドメインおよびサブツリーを DRA に追加します。管理対象ドメインの詳細については、「管理対象ドメインの追加」を参照してください。
DCOM 設定を構成する	*オプション:* DCOM 設定を構成します。DCOM 設定の詳細については、「DCOM の設定」を参照してください。
ドメインコントローラと管理サーバを設定する	各ドメインコントローラおよび各管理サーバの Delegation and Configuration console (委任および環境設定コンソール) を実行しているクライアントコンピュータを構成します。詳細については、「ドメインコントローラと管理サーバの設定」を参照してください。
DRA サービスを gMSA に設定する	*オプション:* Group Managed Service Account (グループ管理されたサービスアカウント)(gMSA) に対して DRA サービスを設定します。詳細については、「グループ管理対象サービスアカウントの DRA サービスの設定」を参照してください。

7 ライセンスのインストールまたはアップグレード

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

既存のライセンスまたは試用ライセンスをアップグレードする場合、Delegation and Configuration console (委任および環境設定コンソール) を開き、[**[Configuration Management (環境設定管理)]**] > [**[Update License(ライセンスの更新)]**] 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。

8 管理対象ドメインの追加

管理サーバをインストールした後、管理対象ドメイン、サーバ、またはワークステーションを追加できます。最初の管理対象ドメインを追加するときには、DRA サービスアカウントを使用して、Delegation and Configuration Console (委任および環境設定コンソール) がインストールされているコンピュータにログインする必要があります。Domain Administrators グループに付与された権限など、ドメイン内の管理権限も必要です。最初の管理対象ドメインをインストールした後で管理対象のドメインおよびコンピュータを追加するには、適切な権限 (Configure Servers and Domains ビルトイン役割に含まれる権限など) が必要です。

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。アカウントキャッシュ更新スケジュールを変更する方法の詳細については、『「DRA 管理者ガイド」』の「*キャッシュ動作の設定*」を参照してください。

---

9 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または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。これらの機能は、[**[Configuration Management (環境設定管理)]**] > [**[管理対象ドメイン]**] ノードから Delegation and Configuration console (委任および環境設定コンソール) で実行されます。管理サーバをインストールした後で管理対象サブツリーを追加するには、適切な権限 (Configure Servers and Domains ビルトイン役割に含まれる権限など) が必要です。指定したアクセスアカウントがそのサブツリーを管理する権限とアカウントキャッシュの増分更新を実行する権限を持っていることを確認するには、削除オブジェクトユーティリティを使用して、適切な権限をチェックおよび委任します。

このユーティリティの詳細については、『「DRA 管理者ガイド」』の「*削除オブジェクトユーティリティ*」を参照してください。

アクセスアカウントのセットアップの詳細については、『「DRA 管理者ガイド」』の「*ドメインアクセスアカウントの指定*」を参照してください。

注 : 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。アカウントキャッシュ更新スケジュールを変更する方法の詳細については、『「DRA 管理者ガイド」』の「*キャッシュ動作の設定*」を参照してください。

---

10 DCOM の設定

セットアッププログラムでの DCOM 設定を許可しなかった場合は、プライマリ管理サーバで DCOM を設定します。

DRA インストール処理中に分散 COM を設定しないように選択した場合は、Distributed COM Users グループのメンバーシップを更新し、DRA を使用するすべてのユーザアカウントを含める必要があります。このメンバーシップには、DRA サービスアカウント、すべてのアシスタント管理者、および DRA REST、DRA ホスト、DRA 管理者サービスを管理するために使用されるアカウントが含まれている必要があります。

Distributed COM Users グループを設定するには、次の手順を実行します。

1. DRA 管理者として DRA 管理者コンピュータにログオンします。
2. Delegation and Configuration console (委任および環境設定コンソール) を起動します。コンソールが自動的に管理サーバに接続しない場合は、手動で接続を確立します。

   注 : Distributed COM Users グループに Assistant Admin アカウントが 1 つも含まれていない場合は、管理サーバに接続できないことがあります。その場合は、Active Directory Users and Computers スナップインを使用して、Distributed COM Users グループを設定します。Active Directory Users and Computers スナップインの使用方法については、Microsoft 社の Web サイトを参照してください。

   ---

3. 左側のウィンドウで、[[Account and Resource Management]] を展開します。
4. [[すべての管理対象オブジェクト]] を展開します。
5. ドメインコントローラがある各ドメインのドメインノードを展開します。
6. [[ビルトイン]] コンテナをクリックします。
7. Distributed COM Users グループを検索します。
8. 検索結果リストで、[[Distributed COM Users]] グループをクリックします。
9. 下のウィンドウで [[メンバー]] をクリックし、[[メンバーの追加]] をクリックします。
10. DRA を使用するユーザとグループを追加します。このグループに、DRA サービスアカウントを必ず追加してください。
11. [[OK]] をクリックします。

11 ドメインコントローラと管理サーバの設定

Delegation and Configuration を実行するクライアントコンピュータの設定が完了したら、各ドメインコントローラおよび管理サーバを設定する必要があります。

ドメインコントローラと管理サーバを設定するには、次の手順を実行します。

1. ［スタート］メニューから、［[コントロールパネル]］>［[システムとセキュリティ]］の順に移動します。
2. ［管理ツール］、［コンポーネントサービス］の順に開きます。
3. ［[コンポーネントサービス]］>［[コンピュータ]］>［[マイコンピュータ]］>［[DCOM 設定]］の順に展開します。
4. 管理サーバ上で [［MCS OnePoint Administration Service］] を選択します。
5. ［アクション］メニューで [［プロパティ］] をクリックします。
6. ［認証レベル］領域の［全般］タブで、［[パケット]］を選択します。
7. ［アクセス権限］領域の［セキュリティ］タブで、[［カスタマイズ］] を選択して [［編集］] をクリックします。
8. Distributed COM Users グループが使用可能であることを確認します。使用可能でない場合は、Distributed COM Users グループを追加します。すべてのユーザグループが使用可能な場合は、そのグループを削除します。
9. Distributed COM Users グループがローカルおよびリモートアクセス権限を持っていることを確認します。
10. ［起動および有効化権限］領域の［セキュリティ］タブで、[［カスタマイズ］] を選択して [［編集］] をクリックします。
11. Distributed COM Users グループが使用可能であることを確認します。使用可能でない場合は、Distributed COM Users グループを追加します。すべてのユーザグループが使用可能な場合は、そのグループを削除します。
12. Distributed COM Users グループが以下の権限を持っていることを確認します。
    - ローカルからの起動
    - リモートからの起動
    - ローカルからのアクティブ化
    - リモートからのアクティブ化
13. 変更を適用します。

12 グループ管理対象サービスアカウントの DRA サービスの設定

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

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

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

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

     NetIQ DRA キャッシュサービス
   - NetIQ DRA コアサービス
   - NetIQ DRA ログアーカイブ
   - NetIQ DRA レプリケーションサービス
   - NetIQ DRA Rest サービス
   - NetIQ DRA Skype サービス
3. すべてのサービスを再起動します。

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

1. セカンダリサーバをインストールします。
2. プライマリサーバで、セカンダリサーバのサービスアカウントの［ **[Administration Servers and Managed Domains (管理サーバと管理対象ドメイン)]**］の ActiveView に［ **[Configure Servers and Domains]**］役割を割り当てます。
3. プライマリサーバで、新しいセカンダリサーバを追加し、セカンダリサーバサービスアカウントを指定します。

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

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