Directory and Resource Administrator

インストールガイド

2018年7月

NetIQ

保証と著作権

本書の内容

『*インストールガイド*』では、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、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。

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、特権昇格、エラー、悪意のあるアクティビティ、規制違反のリスク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。

Exchange Administrator(ExA)は、DRAの強力な機能の拡張により、Microsoft Exchangeのシームレスな管理を可能にします。ExAでは、単一の共通ユーザインターフェイスで、Microsoft Exchange環境全体の受信箱、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できます。

DRAおよびExAを一緒に使用すると、Active Directory、Microsoft Windows、Microsoft Exchange、およびMicrosoft Office 365環境の制御と管理に必要なソリューションが得られます。

- **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、特権昇格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。

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ーフェイスと管理サーバを示しています。

DRAユーザのタイプ	ユーザインターフェイス	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

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ーフェイスであり、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:** Assistant Administrator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。
- **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。

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ーフェイスであり、これを使用してDRA Assistant Administratorは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できます。

Webコンソール

Webコンソールは、Webベースのユーザインターフェイスであり、これを使用してDRA Assistant Administratorは接続ドメインやサービスの委任オブジェクトを簡単に素早く表示および管理できます。

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

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

Webコンソールのもう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...

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。

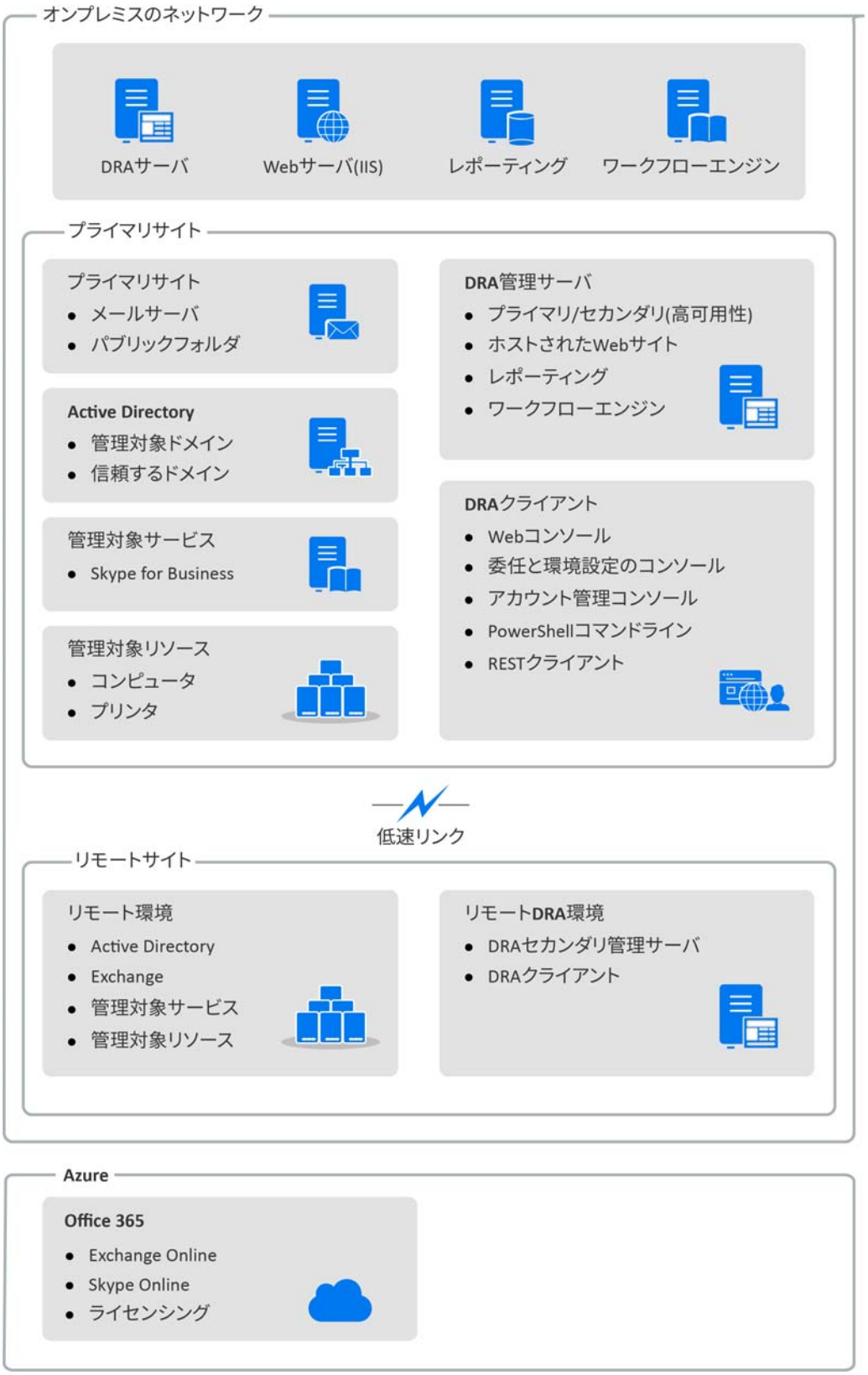
- ADオブジェクトのリソースレポート
- ADオブジェクトデータレポート
- ADサマリレポート
- DRA構成レポート
- Exchange構成レポート
- Office 365 Exchange Onlineレポート
- 詳細なアクティビティトレンドレポート(月別、ドメイン別、ピーク別)
- DRAアクティビティの要約レポート

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。

ワークフローエンジン

DRAは、Aegisワークフローエンジンとの統合により、Webコンソールでワークフロータスクを自動化することができます。Webコンソールで、Assistant Administratorは、ワークフローサーバを構成し、カスタマイズされたワークフロー自動化フォームを実行し、それらのワークフローのステータスを表示することができます。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。

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)
レポーティング
ワークフローエンジン
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
信頼するドメイン
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
委任と環境設定のコンソール
アカウント管理コンソール
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
Exchange Online
Skype Online
ライセンシング

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。

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	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

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

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、DRAクライアント	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)を参照してください(DCOM)
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	ネイティブ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)を参照してください(DCOM)
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)を参照してください(DCOM)
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

プロトコルとポート	方向	宛先	用途
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)
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

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サイトのDirectory and Resource Administrator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
Webブラウザ	◆ Microsoft Internet Explorer 11、Edge ◆ Google Chrome ◆ Mozilla Firefox

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。

ソフトウェア要件:

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のネイティブドメインのメンバーでなければなりません。 **Windows DRAインターフェイス:** ◆ 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

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。

コンポーネント	前提条件
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インターフェイス:** ◆ 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
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。

アカウント	説明	権限
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。

- ユーザ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
- グループ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
- 組織単位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
- プリンタオブジェクトに対するフルコントロール
- ビルトインドメイン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
- MsExchSystemObjectContainer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
- パブリックフォルダに対するフルコントロール

ドメインサービスアカウントには、「このオブジェクトとすべての子オブジェクト」のスコープで次の特権を指定してください。

- コンピュータオブジェクトの作成を許可
- 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作成を許可
- 連絡先オブジェクトの削除を許可
- グループオブジェクトの作成を許可
- 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
- 組織単位オブジェクトの作成を許可
- 組織単位オブジェクトの削除を許可

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

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。

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。

ソフトウェア要件:

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
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

レポーティングの要件

DRA Reportingの要件は次のとおりです。

ソフトウェア要件:

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
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:** DRAReporting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

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、正常性検査ユーティリティを使用して、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(License1.lic)を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。

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。

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** **ユーザインターフェイス** ◆ Account and Resource Management ◆ DRA ADSI Provider ◆ コマンドラインインターフェイス ◆ 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、「「Configuring the Multi-Master Set?」」(『*Directory and Resource Administrator管理者ガイド*』)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。

DRAクライアントのインストール

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ーフェイ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ユーザインターフェイ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ーフェイスの.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。

DRA REST拡張機能のインストール

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インターフェイスを提供します。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Assistant Administratorが使用するWebクライアントインターフェイスですが、カスタマイズ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。

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、『Aegis管理者ガイド』を参照してください。

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つの実行可能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。

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、『*Directory and Resource Administrator管理者ガイド*』の「「Configuring the Multi-Master Set」」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AAの数を調べます。大多数のAA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AA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AAがビルトインAAグループに関連付けられているかを調べます。
  - どのAAがビルトイン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AAに、ユーザインターフェイスのアップグレード計画を知らせてください。
- どのAA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AA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AAに、管理サーバおよびユーザインターフェイスのアップグレード計画を知らせてください。
- アップグレードプロセスを開始する前に、委任、設定、またはポリシーの変更を実装する必要があるかどうかを調べます。環境によっては、この決定をサイトごとに行うことができます。
- ダウンタイムを最小限に抑えるために、クライアントコンピュータと管理サーバのアップグレードを調整します。同じ管理サーバまたはクライアントコンピュータ上で旧バージョンのDRAと現バージョンのDRAを実行することはできません。

アップグレード前のタスク

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

ステップ	詳細
AD LDSインスタンスのバックアップ	ヘルスチェックユーティリティを開き、**AD LDSインスタンスのバックアップ**チェックを実行して、現在のAD LDSインスタンスのバックアップを作成します。
展開計画の作成	管理サーバとユーザインターフェイス(AA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インスタンスのバックアップを復元する必要がある場合、次の操作を行います。

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AA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AA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、AA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AA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、AA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インターフェイスを起動します。
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。

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。
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。
ユーザインターフェイスを展開する	ユーザインターフェイスをAssistant Administrator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。

ステップ	詳細
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、AAクライアントコンピュータ上のユーザインターフェイ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ユーザインターフェイ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、アップグレードが開始されることをAA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、AA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、ユーザインターフェイ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AA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AA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AA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のユーザインターフェイスを即座に展開できるので、AAがダウンタイムを経験することもありません。ユーザインターフェイスのアップグレードの詳細については、DRAユーザインターフェイスの展開を参照してください。

DRAユーザインターフェイスの展開

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のユーザインターフェイ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AA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ーフェイ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ユーザインターフェイスのインストールをAA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ーフェイ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AA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。AA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は、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ユーザインターフェイ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ユーザインターフェイ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AAに対して、適切なユーザインターフェイス(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、アップグレードが開始されることをAA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、AA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AA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ーフェイ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。

DRA Reportingコンポーネントのアップグレード

DRA Reportingをアップグレードする前に、環境がNRC 3.2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、DRAマニュアルサイトの『*Reporting Center 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、DRAマニュアルサイトの『*NetIQ Reporting Center Reporting Guide*』を参照してください。

DRA REST拡張機能のアップグレード

WebコンソールおよびREST拡張機能をDirectory and Resource Administrator 9.2にアップグレードするには、DRA9.0.1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拡張機能のインストール)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

3 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。

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。

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。

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、『*Directory and Resource Administrator管理者ガイド*』の「「キャッシングの構成」」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、特定のMicrosoft Windowsドメインから管理対象サブツリーを追加できます。欠けているサブツリーを管理対象として追加するには、Delegation and Configurationコンソールの［詳細設定］ノードを使用します。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、委任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、『*Directory and Resource Administrator管理者ガイド*』の「「委任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、『*Directory and Resource Administrator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、『*Directory Resource Administrator管理者ガイド*』の「「キャッシングの構成」」を参照してください。

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。

Distributed COM Usersグループの設定

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とすべてのAssistant Admin (AA)を含めなければなりません。

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クライアントコンピュータにログオンします。
2. Delegation and Configuration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。

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、［**設定**］>［**システムとセキュリティ**］>［**コントロールパネル**］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。