

Active Directoryの展開前に確認すべき9つの事項

著者

Dmitry Sotnikov
Development Product Manager
Windows Management
Quest Software, Inc.



ホワイトペーパー

© Copyright Quest[®] Software, Inc. 2006. All rights reserved.

このガイドには著作権で保護されている機密情報が含まれています。このガイドで説明されているソフトウェアは、ソフトウェアライセンスまたは守秘義務契約の下に提供されています。このソフトウェアは、適用される契約の条項に準拠している場合のみ使用またはコピーできます。このマニュアルの一部または全部を複製または転送することは、購入者による個人使用以外の目的では、Quest Software, Inc.の書面による許可がない場合、複写および記録を含む電子的または機械的ないかなる手段でも禁じられています。

保証

この文書に含まれている情報は、予告なく変更されることがあります。クエスト・ソフトウェアは、この情報に関するいかなる保証もいたしません。クエスト・ソフトウェアは、商品性および特定目的への適合性に関する黙示的な保証については一切免責されるものとします。クエスト・ソフトウェアは、この情報の提供または使用に起因して申し立てられた、直接的、間接的、付随的、または結果的ないかなる損害についても責任を負わないものとします。

商標

このガイドで使用されているすべての商標および登録商標は、その所有者の財産です。

ワールドワイド本社
5 Polaris Way
Aliso Viejo, CA 92656
www.quest.com
電子メール: info@quest.com
米国およびカナダ: 949.754.8000

各地域および海外の所在地情報については、本社サイトを参照してください。

最終更新日 - 2005年1月10日

目次

ACTIVE DIRECTORY の展開前に確認すべき 9 つの事項	1
1. 現在のディレクトリに存在するもの	2
2. グループはどのように変化するか	4
3. アクセス許可の割当ては適切か	6
4. どのようなサイトを作成すべきか	7
5. サービスはどこで実行されているか	8
6. 名前の変更が必要か	10
7. 不必要なユーザアカウントまたはグループが存在するか	11
8. ソフトウェアとハードウェアのアップグレードは必要か	13
9. 移行中にどのようにしてネットワーク構成を監視するか	16
結論	18
QUEST SOFTWARE, INC. について	19
クエスト・ソフトウェア (QUEST SOFTWARE, INC.) へのお問い合わせ	19
クエストサポートへのお問い合わせ	19

ACTIVE DIRECTORY の展開前に確認すべき 9 つの事項

Windows 2000とWindows Server 2003のどちらを展開する場合でも、Windows NTからActive Directoryへの移行を成功させるために重要なのは事前の計画です。また、既存のActive Directory設計を大幅に変更する場合にも、事前の計画が必要です。適切な計画を立てることにより、移行の一環として実行する必要があるすべてのタスクを特定し、環境ごとのニーズに最も適したActive Directory設計を作成することが可能になります。事前の計画は、Active Directoryの展開時に陥りがちな、多くの潜在的な落とし穴を確実に回避するためにも役立ちます。

しかしながら、正しいとわかっている事柄は往々にして実践が難しいものです。そうしなければならないすべての理由にもかかわらず、計画段階が駆け足で済まされたり、不完全であったり、十分に実施されないことがよくあります。不十分な計画の原因には、以下を含めさまざまなものがあります。

- 適切で正確なデータを収集できない
- 移行に関連する問題についての経験または情報が不足している
- プロジェクトのスケジュールの都合で計画に十分な時間を割けない

移行を成功させるためには、現在の環境に存在するドメイン、グループ、ユーザ、アクセス許可をすべて網羅したインベントリを作成する必要があります。作成したインベントリによって、不必要なデータを移行したり、本来付与すべきでないアクセス許可を誤ってユーザに付与したりすることを防ぐことができます。環境内のオブジェクト間の関係は複雑である可能性があるため、既存の構造の詳細を把握することにより、Active Directoryへの移行を計画および実行する過程で時間とリソースを節約できます。

Active Directoryの機能を十分に活用するために、現在の環境にあるハードウェアやソフトウェアの一部についてアップグレードが必要な場合があります。移行の前に、アップグレードが必要なコンピュータ、アプリケーションソフトウェア、デバイスを把握する必要があります。ここでも同様に、移行を計画する過程でこれらのリソースを把握しておくことにより、時間とコストを節約して将来の問題を防ぐことができます。

このガイドでは、Active Directoryへの移行を開始する前に、対象の環境について理解しておくべき9つの事項を検証します。このガイドには、Quest® Reporter™で出力されたサンプルレポートが含まれています。これらのレポートは、プロジェクトのスムーズな進行と展開の成功を保証するために必要な各種の情報の例を示します。

1 現在のディレクトリに存在するもの

移行は、現在の環境を検証し、組織のニーズをよりの確に反映した設計上の改善点を特定するための機会でもあります。管理面で特別なニーズを持つユーザのグループは存在するでしょうか。特定のグループまたは部署によるリソースへのアクセスを制限するポリシーは存在するでしょうか。Active Directoryでは、物理的または地理的な境界のみに基づいたディレクトリ構造を維持する必要はありません。その代わりに、組織の運営構造を表す論理ディレクトリ構造を作成できます。

新しいディレクトリ構造を計画する過程で、Active Directoryのスケラビリティ機能、管理の委任、グループポリシーをどのように利用するかを考慮してください。たとえば、グループポリシーは、ドメインと組織単位の構築に多大な影響を及ぼす可能性があります。ディレクトリ構造にそのような変更を行うために、ドメインを分割または結合したり、新しい管理境界を決定したり、フォレストを作成したりすることが必要な場合があります。新しいディレクトリ構造については、以下のような設計上の問題を考慮してください。

- フォレスト
 - ドメインはセキュリティの分離を実現しますが、セキュリティと管理の全面的な分離は、複数のフォレストを利用する展開でのみ可能です。
 - フォレスト内のすべてのドメインは同じスキーマを共有する必要があります。特定のドメインが異なるスキーマを必要とする場合、そのドメインを別のフォレストに配置する必要があります。
- ドメイン
 - Active DirectoryドメインはWindows NTドメインよりもずっとスケラブルであるため、多くの場合、Active Directoryの展開中にいくつかのドメインを結合することになります。ただし、Active Directoryドメインにはまだサイズの制限があるため、ドメインの結合を決定する前にドメイン統計を分析する必要があります。
 - 他のユーザと異なるセキュリティポリシーまたは管理ポリシー（ユーザ名やパスワードの制限など）を必要とするユーザは、異なるドメインに配置する必要があります。
 - 新しいドメイン構造は地理的条件を反映しているとは限らず、このことは管理権限を割当て方法に影響を及ぼす可能性があります。
- 組織単位
 - Active Directoryでは、リソースドメインとアカウントドメインが独立している必要はありません。リソースドメインとアカウントドメインを結合し、組織単位を使用して、ドメイン内部の共通オブジェクトに対する独立したコンテナを作成することができます。
 - Active DirectoryのドメインはWindows NTよりも多くのオブジェクトを保持できるため、ドメインを結合して組織単位を使用することにより、管理を委任できる場合があります。

現在のドメインの分析

新しいディレクトリ構造の計画を開始する前に、現在の環境を分析する必要があります。既存のドメイン構造を理解することは、移行方針を定義し、Active Directory設計を決定する上で役立ちます。現在の環境に存在するすべてのドメインを把握し、各ドメインについての以下のような情報を収集する必要があります。

- 各ドメインのタイプ(リソースまたはアカウント)
- 各ドメインに関連付けられたすべてのユーザ、グループ、ドメインコントローラ、リソースサーバ
- ドメイン間の信頼関係

現在のドメイン構造を完全に理解したら、Active Directory内に作成する必要があるフォレスト、ツリー、ドメイン、組織単位が何であるか、また、現在のディレクトリ(「移行元ドメイン」)からこれらのコンテンツに移動するオブジェクトがどれであることを特定する作業を開始できます。



Quest Reporter Domain Statistics

Domain	Reporter.com
Number of Computers	1
Number of Groups	822
Number of Users	6517



Quest Reporter Domain Controllers

Domain	Reporter.com
Domain Controller	RCPORTER.Reporter.com

現在のドメインの詳細な分析は、新しいActive Directoryの設計と移行の計画に欠かせない最初のステップです。

2 グループはどのように変化するか

グループを使用すると、環境内のユーザとリソースを効率的に管理できます。グループはディレクトリ設計の重要な要素です。Active Directoryでは、新しい種類のグループ(ユニバーサルグループ)が導入され、グループが機能する仕組みが変更されています。たとえば、リソースに対してドメイン全体でのアクセス許可を設定する目的で、ドメインローカルグループをActive Directory内で使用できます。結果として、Active Directoryを展開するときに、サーバローカルグループをドメインローカルグループに移行することが必要な場合があります。また、Windows NTで、アクセス許可の管理を容易にする目的でファイルまたはプリントサーバをドメインコントローラとして設定していた場合、これらのサーバをActive Directory内のメンバーサーバに格下げし、それらのドメインローカルグループを、Active Directory内の対応する移行先ドメインのドメインローカルグループに結合することが必要な場合もあります。

新しいActive Directoryグループ構成を効果的に計画するには、Windows NTとActive Directoryでグループがどのように異なっているかを理解する必要があります。

Windows NTの場合:

- グループの使用目的は、ファイル、共有、プリンタなどのNTリソースに対するアクセス許可を付与してセキュリティを施行することに限定されます。Exchange 5.5では、グループの代わりにメール配布のための配布リストを使用します。
- グループの範囲はグローバルグループとローカルグループに限定されます。
- ドメインローカルグループは、ドメインコントローラに対するアクセス許可を設定する目的にのみ使用できます。

Active Directoryの場合:

- セキュリティと配布の両方の目的にグループを使用できるため、グループ管理が簡素化されません。
- グローバルグループとローカルグループに加えて、フォレストの複数のドメインからのメンバーを含むことができるユニバーサルグループが存在します。
- リソースに対するドメイン全体でのアクセス許可を設定する目的で、ドメインローカルグループを使用できます。

グループの把握

Active DirectoryのグループはWindows NTのグループとは異なるため、既存のグループを検証し、何らかの変更が必要かどうかを決定する必要があります。移行中および移行後にも、ユーザのリソースアクセスとメール配布を維持するためには、グループを理解することが重要です。グループのネストは複雑になる可能性があります。アクセス許可がどのように割当てられたのかを完全に理解し、これから変更する必要があるかどうかを判断するために、グループ構造を把握する必要があります。その後、グループのメンバーシップや、結合または削除されるグループなど、新しいグループ構造を決定する作業を開始できます。

現在の環境に存在するすべてのグループを把握し、各グループについて以下のような情報を収集する必要があります。

- 各グループのタイプ
- 各グループに割当てられているすべてのユーザ
- 各グループへのすべての参照
- グループのネスト(ローカルグループにネストされたグローバルグループのユーザなど)
- Exchange 5.5の配布リスト

The screenshot displays the Quest Reporter interface for Local Group Membership. It shows details for the 'Account Operators' group, including its domain (Reporter.com), scope (Domain Local Security), and type (Security). Below this, it lists other groups like 'Administrators' and 'Users - Member Of'. The 'Group Membership' section shows nested group relationships with their respective domain and security identifiers. The 'Group Statistics' section provides a summary of groups across different domains and types.

リソースに対するユーザの適切なアクセス権を確実に維持するためには、ネストを含めて既存のグループ構造を完全に理解する必要があります。

The screenshot displays the Quest Reporter interface for Local Groups by Computer. It shows a list of groups on the computer \\REPORTER, including their descriptions and group names. The groups listed are WINS Users, DnsAdmins, RAS and IAS Servers, Administrators, and Users.

既存のサーバローカルグループを分析して、それらのグループを移行するかどうか、またはActive Directory内のドメインローカルグループと結合するかどうかを決定します。

3 アクセス許可の割当ては適切か

移行は、現在の環境で付与されているアクセス許可を見直し、必要なクリーンアップを実行するためのよい機会でもあります。移行の前に、本来割当てられるべきでないアクセス許可が割当てられたユーザがないかどうかを調べ、不適切な割当てを変更して、そのような割当てがActive Directoryに継承されることを防ぐ必要があります。移行がユーザに及ぼす影響を減らすには、ファイル、フォルダ、プリンタなどのネットワークリソースに対するアクセス許可が正しく再割当てされることを保証する必要があります。加えて、アクセス許可が割当てられていないグループの削除や、同じアクセス許可を付与するグループの結合についても検討する必要があります。

アクセス許可割当ての把握

リソースに対するユーザのアクセス権を移行中に、そして移行後も確実に維持するためには、現在のアクセス許可構造を分析する必要があります。現在の環境で、以下の事項を把握する必要があります。

- ディレクトリ全体でユーザとグループに付与されているファイル、フォルダ、共有、プリンタのアクセス許可
- あるドメイン内に存在し、別のドメインのユーザがアクセスできるリソース
- 管理権限を持つユーザ

Quest Reporter Share and Folder Permissions

Object Path	Permissions
Account	SYSTEM
Ace String	Allow Full Control, subfolders and files
Account	Authenticated Users
Ace String	Allow Read & Execute, subfolders and files
Account	REPORTER0\Server Operators
Ace String	Allow Modify, this folder only

Quest Reporter Group - Members

Domain	Reporter.com
Group Name	Administrators
Members	
CN=Administrator,CN=Users,DC=Reporter,DC=com	
CN=Administrator,CN=Users,DC=Reporter,DC=com (CN=Domain Admins,CN=Users,DC=Reporter,DC=com)	
CN=Administrator,CN=Users,DC=Reporter,DC=com (CN=Enterprise Admins,CN=Users,DC=Reporter,DC=com)	
CN=Domain Admins,CN=Users,DC=Reporter,DC=com	

移行の前に、ユーザとグループに割当てられているアクセス許可を評価します。

4 どのようなサイトを作成すべきか

Active Directoryでは、ネットワークの論理構造を表現する目的でフォレストとドメインを作成する一方で、ネットワークの物理構造を表現する目的でサイトを作成します。Windows NT 3.xまたは4.0ネットワークの論理構造は、ほとんどがその物理構造を反映したものです。一方Active Directoryでは、ネットワークの論理構造と物理構造は一致する必要はありません。組織のドメイン名前空間を形成しているツリーとフォレストは、ネットワークの論理構造を表します。ネットワークの物理構造を定義するには、Active Directory内で1つ以上のサイトオブジェクトを構成する必要があります。

サイトオブジェクトは、良好なネットワーク接続の領域を定義するために使用されます。Active Directory内でサイトオブジェクトを構成するには、サイトを1つ以上のTCP/IPサブネットと関連付けます。サイトに対して定義する各TCP/IPサブネットが、高帯域幅リンク(512Kbps以上)を共有するようにしてください。一般的には、低帯域幅によって分離されるネットワークの各領域に対して1つのサイトオブジェクトを作成します。

サイトの役割は、ネットワーク上のレプリケーショントラフィックの経路を決定することです。Active Directoryでは、ドメイン内のすべてのドメインコントローラ間ですべてのデータがレプリケートされますが、ドメイン間では特定のデータのみがレプリケートされます。サイトを使用して、ネットワーク内でのレプリケーションの効率を最大化することができます。

IPサブネットの把握

サイト構造を計画するには、現在のネットワーク内のIPサブネットについて理解する必要があります。多くの場合、既存のIPサブネットのほとんどがActive Directoryのサイトオブジェクトになります。

Quest Reporter		Computers by Network Configuration
Common Name	REPORTER	
Domain	Reporter.com	
IP Address	192.168.64.156	
Role	<ul style="list-style-type: none"> A LAN Manager server A LAN Manager workstation Any server running with Microsoft SQL Server Primary domain controller Server running the master browser service Server running the Timesource service Server sharing print queue Terminal Server Windows NT/Windows 2000 workstation or server 	
WINS Primary Server	127.0.0.0	
WINS Secondary Server	127.0.0.0	

Active Directoryサイトを計画するために、現在のネットワークのコンピュータ構成を把握します。

5 サービスはどこで実行されているか

Active Directory構造を計画する過程で、ネットワークサーバ上で現在実行されているサービスを把握する必要があります。ネットワーク構造の変更やオペレーティングシステムのアップグレードは、これらのサービスに影響を及ぼす可能性があります。たとえば、DHCPやWINSの設定を変更する場合は、それらのサービスがどのサーバで実行されているかを調べる必要があります。

サービスについての情報が重要な理由には、以下のものがあります。

- DNS、DHCP、WINSなどのサービスはネットワーク運用の根幹であり、移行中の扱いに特別な配慮が必要になります。たとえば、DHCPサービスを実行しているサーバを移行する場合、事前にDHCPを無効にする必要があります。
- サービスが特定のユーザアカウントによって実行されている場合、そのアカウントを無効にする過程でサービスを更新する必要があります。ユーザアカウントがサービスによって使用中である場合、そのアカウントを無効にする前に、移行先ドメイン内の対応するアカウントにサービスを再割当てする必要があります。
- 一部のサービスはActive Directoryとの互換性がない可能性があります。新しい環境で実行されるすべてのサービスがActive Directoryに対応していることを確認する必要があります。

サービスの把握

ネットワークで実行されているサービスを把握することは、予期しない問題が移行中に発生することの回避に役立ちます。現在の環境について、サービスに関する以下の情報を把握する必要があります。

- 各サービスの名前
- 各サービスの実行に使用されているアカウント
- サービスを実行しているコンピュータ

Quest Reporter Services	
Domain	Reporter.com
SAM Account Name	REPORTER\$
Binary Path Name	C:\WINNT\System32\services.exe
Start Type	Automatic
Current State	Running
Service Display Name	Alerler
Interact With Desktop	False
Load Order Group Name	Alerler
Type	Win32 shared process
Account Name	LocalSystem
Dependencies	LanmanWorkstation
Binary Path Name	C:\WINNT\system32\services.exe
Start Type	Star: on demand
Current State	Stopped
Service Display Name	Application Managemert
Interact With Desktop	False
Load Order Group Name	AppMgm:
Type	Win32 shared process
Account Name	LocalSystem
Dependencies	

ネットワークの問題を防ぐために、サーバ上で実行されている各サービスについて把握します。

6 名前の変更が必要か

状況によっては、新しいActive Directory内のユーザアカウント、グループ、コンピュータの名前の変更が必要になる場合があります。Active Directoryでの問題を防ぐために、以下のような状況について理解しておく必要があります。

- Active DirectoryとWindows NTでは、コンピュータ、グループ、ユーザアカウントの命名規則が異なります。Windows NTでの一部の名前はActive Directoryで禁止されている可能性があり、そのような名前を変更する必要があります。
- 同じ名前のオブジェクトを含む複数のドメインを結合するときに、名前付けの問題が発生する可能性があります。この状況は、以下のいずれかの方法で解決できます。
 - 複数のオブジェクトが偶然に同じ名前を使用していた場合、移行中に一方のオブジェクトの名前を変更できます。
 - 同じ人物（複数のドメインに1つのアカウントを持つ人物など）または同じグループ（「営業」のような同じ目的のグループが2つのドメインに存在する場合など）を表す複数のオブジェクトが存在する場合、移行中にこれらのユーザオブジェクトまたはグループを結合できます。
 - 複数のオブジェクトが同じ人物を表すが、（重複した管理者アカウントなどの）何らかの理由で一方のアカウントが必要でない場合、移行前に一方のオブジェクトを削除するか、または移行中にそのオブジェクトをスキップすることができます。

名前の分析

Active Directoryでの名前付けの競合を避けるには、既存のディレクトリオブジェクトの名前を把握しておく必要があります。この情報を使用して、名前の変更、結合、削除またはスキップが必要なオブジェクトが存在するかどうかを調べることができます。現在の環境で、以下の事項を識別する必要があります。

- 同じ名前を持つユーザアカウント
- 同じ名前を持つグループ
- Active Directoryで使用できない名前が付けられたすべてのコンピュータ、グループ、ユーザ

Duplicate Users

This report shows users that have the same name in the selected domains. You must select users from more than 1 domain in order to see any results. Note: The report looks for duplicate pre-Windows 2000 names.

Duplicate Groups

This report shows groups that have the same name in the selected domains. You must select groups from more than 1 domain in order to see any results. Note: The report looks for duplicate pre-Windows 2000 names.

結合、名前変更、削除またはスキップの対象となる重複したユーザアカウントとグループを識別します。

7 unnecessary ユーザアカウントまたはグループが存在するか

時間の経過とともに、使われていないユーザアカウント、無効なユーザアカウント、空のグループが環境内に発生してそのままになっている場合があります。これらのアカウントやグループは環境に不要であり、インベントリから削除すべきものです。さらに重要なこととして、使われていないアカウントはセキュリティの脅威となります。悪意のある管理者がそのようなアカウントを利用して、自らの身元を隠したまま攻撃を実行できるからです。

Active Directoryへの移行は、そのような不要データとセキュリティの脆弱性をネットワークから取り除く機会です。不要になったユーザアカウントとグループの削除は、移行プロジェクトの所要時間短縮と作業負荷の削減にもつながります。

unnecessary グループの識別

移行の前に、移行すべきでない空のまたは使われていないグループを識別する必要があります。

Quest Reporter	
Groups without members	
Domain	Reporter.com
Group Name	Grp1-1
Description	
Type	Security
Members	
Group Name	Grp1-10
Description	
Type	Security
Members	
Group Name	Grp1-11
Description	
Type	Security
Members	

削除またはスキップすべきである、空のまたは使われていないグループを識別します。

unnecessary アカウントの識別


移行の前に、移行すべきでないアカウントを識別する必要があります。現在の環境に存在する、以下のような unnecessary アカウントを識別する必要があります。

- 使われていないアカウント
- 無効なアカウント
- 有効期限の切れたアカウント



The screenshot shows the 'Quest Reporter' interface for 'Inactive Accounts' in the 'Reporter.com' domain. It lists three user accounts with their User Name, Account Disabled status, and Last Logon information.

Domain	Reporter.com
User Name	1-76
Account Disabled	False
Last Logon	
User Name	111-10
Account Disabled	False
Last Logon	
User Name	113-150
Account Disabled	False
Last Logon	



The screenshot shows the 'Quest Reporter' interface for 'Disabled Accounts' in the 'Reporter.com' domain. It lists three user accounts with their Account Disabled status, Display Name, and User Name information.

Domain	Reporter.com
Account Disabled	True
Display Name	
User Name	Guest
Account Disabled	True
Display Name	
User Name	krbtgt

使われていない、無効である、有効期限が切れている、のいずれかに該当し削除すべきであるアカウントを識別します。

8 ソフトウェアとハードウェアのアップグレードは必要か

Active Directoryのすべての機能を十分に活用するために、ネットワーク内のソフトウェアとハードウェアのアップグレードが必要になる場合があります。移行を計画する過程で、このようなアップグレードにかかる追加の時間、労力、コストを忘れてはなりません。準備として、これらのアップグレードが既存のネットワークに及ぼす影響について検討してください。

- ドメインコントローラのコンピュータに利用しているハードウェアを移行後も利用する予定の場合、現在のハードウェアがWindows 2000/2003のドメインコントローラの要件を満たしているかどうかを確認する必要があります。
- Windows 9xとNT Service Pack 4 (SP4)よりも前のWindows NTは、Active DirectoryクライアントソフトウェアがこれらのOSにインストールされていない限り、Active Directoryの機能を完全にはサポートしません。そのようなコンピュータを特定し、オペレーティングシステムをアップグレードするか、またはActive Directoryクライアントをインストールするかどうかを決定する必要があります。
- コンピュータのオペレーティングシステムをアップグレードする場合は、対象のコンピュータについてハードウェア互換性を確認する必要があります。プリンタ、ビデオカード、モデムなどの一部のハードウェアデバイスは、新しいオペレーティングシステムと互換性がない可能性があります。Microsoftから提供されているハードウェア互換性リスト(HCL)は、互換性のないデバイスの特定に役立ちます。
- 古いバージョンのソフトウェアアプリケーションは、新しいオペレーティングシステムと互換性がない場合があります。
- ハードウェアとソフトウェアのアップグレードは、移行プロジェクトのコストや期間に影響を与えます。移行計画の一環として、アップグレードのコストを見積る必要があります。

コンピュータのオペレーティングシステムの把握

古いオペレーティングシステムを実行しているコンピュータについて、オペレーティングシステムをアップグレードするか、またはActive Directoryクライアントをインストールするかどうかを決定する必要があります。現在の環境で、Windows 9x、またはNT4 SP4よりも前のWindows NTを実行しているコンピュータを特定する必要があります。

Quest Reporter Operating System Information	
Domain	Reporter.com
SAM Account Name	REPORTER\$
Build Number	2'95
Service Pack	Service Pack 4
Windows Product Name	Microsoft Windows 2000
Windows Version	5

古いオペレーティングシステムを実行しているコンピュータを特定します。

インストールされているハードウェアの把握

コンピュータのオペレーティングシステムのアップグレードは、そのコンピュータにインストールされているハードウェアデバイスに影響を及ぼす可能性があります。アップグレードする前に、プリンタ、ビデオカード、モデムなどのコンピュータデバイスが、新しいオペレーティングシステムでも正常に機能することを確認する必要があります。現在の環境で、以下のような情報を把握する必要があります。

- アップグレード対象のコンピュータ
- 各コンピュータにインストールされているデバイスの種類
- デバイスの名前
- デバイスの製造元

Quest Reporter General Computer Information	
Domain	Reporter.com
SAM Account Name	REPORTER\$
Automatic Logon Enabled	False
Bios Date	03/28/03
Bios Version	03/28/03PhoenixBIOS 4.0 Release 6.0
Build Number	2195
Current Date	12/28/2004 12:42:05 PM
Default Browser	Microsoft Internet Explorer
Description	
IP Address	192.168.64.156
SAM Size	20
SID	S-1-5-21-1626555193-7955
Time Zone Daylight Name	Central Daylight Time
Time Zone Standard Name	Central Standard Time
Service Pack	Service Pack 4
System File Checker Disable	Enabled
System File Checker Dll	%SystemRoot%\System32
Cache Dir	
System File Checker Quota	4095
System File Checker Scan	do not scan protected files
System File Checker Show Progress	False
Windows Version	5

Quest Reporter Video Controller (VM	
Domain	Reporter.com
SAM Account Name	REPORTER\$
Adapter DAC Type	VMware SVGA II
Adapter RAM in MB	16777216
Video Controller Caption	VMware SVGA II
Current Bits Per Pixel	32
Current Horizontal Resolution	1024
Current Number of Colors	4294967296
Current Refresh Rate	85
Current Vertical Resolution	768
Video Controller Description	VMware SVGA II
Video Controller Device ID	VideoController1
Device Specific Pens	-1
Video Controller Driver Date	8/20/2003 3:39:24 AM
Video Controller Driver Version	10.10.6.1 - Build build-5592
Video Controller Inf Filename	oem4.inf

オペレーティングシステムをアップグレードするコンピュータ上のハードウェアデバイスを確認します。

インストールされているソフトウェアの把握

ワークステーションまたはサーバ上で実行されているアプリケーションソフトウェアについても、アップグレードが必要な場合があります。古いバージョンのソフトウェアは、新しいオペレーティングシステムと互換性がない場合があります。現在の環境で、アプリケーションソフトウェアの現在のバージョンを確認し、そのソフトウェアが新しいオペレーティングシステムと互換性があるかどうかを調べる必要があります。

 Quest Reporter Installed Software	
Domain	Reporter.com
SAM Account Name	REPORTER\$

Installed Software

dstool
Internet Explorer Q818529
Microsoft .NET Framework 1.1
Microsoft SQL Server 2000
Outlook Express Update Q330994
Quest Reporter
VMware Tools
Windows 2000 Administration Tools

インストールされているソフトウェアについて、アップグレードが必要かどうかを確認します。

9 移行中にどのようにしてネットワーク構成を監視するか

移行が始まった後は、ネットワークセキュリティを強化するために、グループやグループポリシーの使用状況を含め、Active Directoryのアクセス許可の割当てを定期的に見直すようにしてください。移行中にたびたび、異なる管理者によってユーザとグループの移動が行われ、それが原因で意図しない権限割当てが発生する可能性があります。移行対象のすべてのユーザについて、不適切な権限が付与されていないかを確認する必要があります。移行が完了した後も、Active Directoryのアクセス許可の調査を継続し、適用される法的規制や組織のセキュリティポリシーの遵守状況を確認する必要があります。

ACTIVE DIRECTORYの管理権限の監視

Active Directoryで、Administratorsグループのメンバーシップを監視する必要があります。監視の対象には、このグループのメンバーシップを他のグループ経由で取得するアカウントも含まれます。メンバーシップリストを使用して、このグループへのアクセス許可を付与される必要があるユーザだけがグループのメンバーであることを確認できます。加えて、どのユーザに管理権限が付与されたかを確実に把握しておく必要があります。



Quest Reporter	
Group - Members	
Domain	Reporter.com
Group Name	Domain Admins
Members	CN=Administrator,CN=Users,DC=Reporter,DC=com

ネットワークのセキュリティを保証するために、Active Directoryで管理権限を持つユーザを監視します。

ACTIVE DIRECTORYのグループメンバーシップの監視

グループメンバーシップの追跡が困難になり、その結果として、不適切なアクセス許可の割当てが発生する可能性があります。グループの詳細なリストを使用して、各グループの目的を確認し、ドメイン内でのアクセス許可の割当てを修正することができます。移行の後で、類似のグループが統合されている場合があります。グループメンバーシップについての情報を利用して、メンバーシップを取消すべきだったユーザまたはグループが存在していないかどうかを調べることができます。

Quest Reporter
Group List by OU

OU	Reporter.com/Builtin
Description	A backward compatibility group which allows read access on all users and groups in the domain
Display Name	
Group Name	Pre-Windows 2000 Compatible Access
Description	Guests have the same access as members of the Users group by default, except for the Guest account which is further restricted
Display Name	
Group Name	Guests
Description	Administrators have complete and unrestricted access to the computer/domain
Display Name	
Group Name	Administrators

Quest Reporter
Group Membership

Domain	Reporter.com
Group Name	Account Operators
Type	Security
Members	
Group Name	Administrators
Type	Security
Members	CN=Administrator,CN=Users,DC=Reporter,DC=com CN=Administrator,CN=Users,DC=Reporter,DC=com (CN=Domain Admins,CN=Users,DC=Reporter,DC=com)

Active Directoryのグループとグループメンバーシップを追跡します。

結論

移行前と移行後の両方にわたってその時点のディレクトリのインベントリ作成を行うことにより、移行の計画を立てるための、新しいActive Directoryを設計するための、またその一方で重大な問題の発生を回避するための有益な情報が得られます。構成データやソフトウェアとハードウェアのインベントリを収集してレポートを生成する、Quest Reporterのようなツールを使用することで、計画作業の効率を大きく高めることができます。Reporterによってデータとインベントリの収集が自動化されるため、より完全で正確なデータの収集が可能になります。Reporterの定義済みレポートには、このガイドでこれまでに示したような、移行とセキュリティに関するベストプラクティスと専門的な知識が反映されています。Reporterのようなツールの利用は、Windows 2000またはWindows Server 2003環境へのActive Directoryの展開を確実に成功させるために役立ちます。

Quest Reporterの詳細については、クエスト・ソフトウェアのWebサイト (<http://www.quest.com/reporter/>) を参照してください。

QUEST SOFTWARE, INC. について

クエスト・ソフトウェア(Quest Software, Inc.)は、アプリケーション、データベース、Windowsインフラストラクチャによるパフォーマンスおよび生産性の向上を支援する革新的な製品を提供しています。IT業務に対する深い専門知識、そして最善を追求する絶え間ない努力によって、クエスト・ソフトウェアは全世界18,000以上の顧客企業のITソリューションに対する高い期待に応えています。クエスト・ソフトウェアは、全世界にオフィスを展開しています。詳細については、www.quest.comを参照してください。

クエスト・ソフトウェア(QUEST SOFTWARE, INC.)へのお問い合わせ

電話: 949.754.8000(米国およびカナダ)

電子メール: info@quest.com

所在地: Quest Software, Inc.
World Headquarters
5 Polaris Way
Aliso Viejo, CA 92656
USA

Webサイト: www.quest.com

各地域および海外の所在地情報については、本社サイトを参照してください。

クエストサポートへのお問い合わせ

クエストサポートは、Quest製品の試用版をお持ちのお客様、または製品版を購入し、有効な保守契約書をお持ちのお客様がご利用いただけます。クエストサポートは、弊社のWebセルフサービスであるSupportLinkで、24時間体制のサービスを提供しています。SupportLink (<http://www.quest.com/japan/support/>)を参照してください。

SupportLinkでは、以下のことが行うことができます。

- 数千ものソリューション(ナレッジベースの記事/文書)をすばやく検索できます。
- パッチとアップグレードをダウンロードできます。
- サポートエンジニアにサポートを依頼できます。
- ユーザ事例をログに記録および更新し、その状況をチェックできます。

サポートプログラム、オンラインサービス、連絡先情報、およびポリシーと手順についての詳細な説明については、『Global Support Guide』を参照してください。このガイドは以下の場所から入手できます：
[http://support.quest.com/pdfs/Global Support Guide.pdf](http://support.quest.com/pdfs/Global%20Support%20Guide.pdf)