データシート

Active Roles

ハイブリッドActive Directoryなどにおける管理とセキュリティ

メリット

- 重要なActive DirectoryおよびAzure Active Directoryのデータを保護
- 最小限の特権だけを付与することで管理アクセスを規制
- ネイティブツールの制約を克服
- ユーザ/グループアカウントの作成と削除を自動化
- Exchange Online、Lync、SharePoint Online、Office 365などの多数のアカウントを管理
- ハイブリッド環境に対応した、単一の直感的なツールを提供
- 監査に対応したレポート生成
- 価値を早期実現するための迅速な導入
- 誰が、何を、いつ変更したかを特定
- モジュラー型アーキテクチャによって現在および将来のビジネス要件に対応
- AD重視のID管理を非WindowsおよびSaaSシステムの多くへ拡張

概要

Active Directory（AD）およびAzure ADにおけるアカウント管理には、多くのさまざまな課題があります。さらに、これらのクリティカルなシステムのセキュリティを保護することは、たいていの場合、重要な課題となります。ネイティブツールによるハイブリッドADの管理とセキュリティでは不十分で整合性がなく、エラーが起こりがちです。

今日の慌ただしいビジネスシーンで、組織はハイブリッドAD環境へのアクセス権の作成、変更、削除の対応に悪戦苦闘しています。さらに、セキュリティに関する課題もあります。例えば、解雇された従業員による貴重な知的財産へのアクセス保持、厳しいビジネス要件、監査レポートへのリクエスト対応などです。また、Active DirectoryとAzure Active Directoryの管理アクセスの制御を強化し、非WindowsとSaaSアプリケーションの爆発的増加についても策を講じなければなりません。

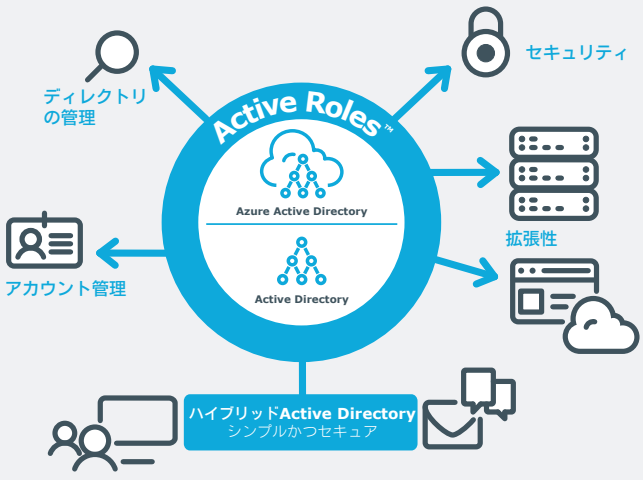
しかし、有効な解決策があります。One Identity Active Rolesを使用すれば、手間がかかりミスの発生しがちなこれらの管理タスクが自動化されるため、セキュリティに関する課題を解決できます。Active Rolesは、アカウントおよびグループ管理を自動化して一元管理し、同時にすべての重要な管理アクセスを安全に保護します。

Active Rolesのユーザ/グループアカウント管理の自動化ツールによって、Active DirectoryとAzure Active Directoryの標準ツールでは満たせない欠点が補われます。これにより業務の効率性と正確性が向上し、手動介入もほとんど必要なくなります。Active Rolesはモジュラー型アーキテクチャに基づいて設計されているため、組織は現在および将来のビジネス要件に簡単に対応できます。

特長

ハイブリッドAD環境に対応

Active Rolesは、オンプレミスのADおよびAzure ADの両方のハイブリッドな導入に関するニーズに応える、最適なソリューションです。お使いのハイブリッド環境全体での作業を1つのコンソールで行うことができるため、ワークフローを統合し、一貫性のある管理が可能になります。異なる複数のツールを使用したり、手動で処理したりという制約がないことから、煩雑さやミスの多発も避けられます。



安全なアクセス

Active Rolesが提供するActive DirectoryとAzure Active Directoryの包括的な特権アカウント管理では、最小特権モデルを使用した委任によってアクセスをコントロールできます。定義済みの管理ポリシーと関連付けられた権限に基づいてアクセスルールを生成し、それを厳密に適用することによって、ハイブリッドのAD管理における標準的なアプローチで起こりやすいエラーや不整合をなくします。さらに、お客様に合わせてカスタマイズされた堅牢な承認手続きにより、ディレクトリデータの自動管理を補完する責任の連鎖を構築し、ビジネス要件に沿ったITプロセスと監視を実現できます。

アカウント管理の自動化

Active Rolesでは、次のようなさまざまなタスクを自動化できます。

- ADおよびAADのユーザとグループのアカウント作成
- AD/AADベースのアカウント管理のアクションを非Windowsシステムおよびサードパーティ製SaaSアプリケーションに簡単に拡張
- ExchangeおよびExchange Onlineのメールボックス作成
- ADおよびAADでのグループ構成
- Windowsのリソース割り当て

Active RolesはAD、AAD、およびADを組み合わせたシステムにおけるユーザのアクセス権の再付与と削除のプロセス（ユーザとグループのプロビジョニング解除を含む）も自動化し、ユーザやグループのライフタイム全体にわたって効率的で安全な管理プロセスを実現します。ユーザアクセスを変更または削除する必要がある場合、AD/AADのハイブリッド環境内のあらゆる関連システムやアプリケーションに加え、ADを組み合わせたシステム（Unix、Linux、Mac OS Xなど）、さらに、増え続ける一般的なSaaSアプリケーション（One Identity Starling Connectソリューションを介して）においても、アップデートが自動的に行われます。

日常的なディレクトリ管理

Active Rolesを使えば、オンプレミス環境やAzure AD環境でのさまざまな管理作業を簡単に行えます。主な管理対象は次の通りです。

- Exchange受信者（メールボックスやOCSの割り当て、作成、移動、削除、アクセス許可、配布リストの管理など）
- グループ
- コンピュータ（共有、プリンタ、ローカルユーザ、ローカルグループなど）
- Active DirectoryおよびAzure Active Directory

Active Rolesでは直感的に使えるインターフェイスが採用されており、MMCスナップインとWebインターフェイスにより、AD/AADのハイブリッド環境での日常的な管理業務やヘルプデスクの業務をより効率的に行えます。

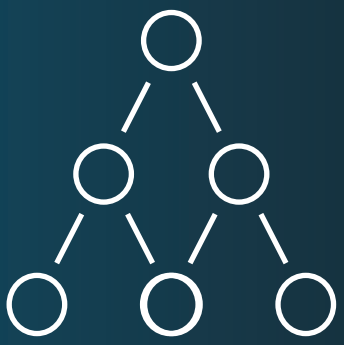
また、Active Rolesは最も一般的で関連性のあるカスタマイズオプションもサポートします。例えば、組織が最適にActive Rolesを利用するのに必要な最大の柔軟性と機能を提供するPowerShellなどです。

管理範囲が拡張

Active RolesはSCIM標準に対応するため、SCIM対応のすべてのSaaSアプリケーション（One Identity Starling Connectを介して）を、Active RolesのADベースのアカウントおよびグループ管理機能で利用できます。

ホスト環境のグループとユーザの管理

Active Directoryドメインクライアントを、ホスト環境のActive Directoryホストドメインと同期させることができます。Active Rolesを使うと、クライアントのドメインからホストされたドメインへのユーザおよびグループアカウントを管理することができ、さらに属性やパスワードの同期も可能です。すぐに利用可能なコネクタを使って、オンプレミスのADアカウントを、Microsoft Office 365、Lync Online/Skype for Business、SharePoint Onlineと同期できます。



ユーザアクセスを変更または削除する必要がある場合、アップデートが自動的に行われます。

対象となるのは、AD、AAD、Exchange Online、SharePoint Online、OCS、Skype for Business、Windowsに加え、ADを組み合わせたシステム（Unix、Linux、Mac OS Xなど）、およびSaasアプリケーションです。

統合による管理ポイントの集約

Active Rolesは、既存のテクノロジーとアイデンティティ管理およびアクセス管理戦略を補完します。Identity Manager、Safeguard、Authentication Services、Password Manager、ChangeAuditorなど、さまざまなOne Identity製品を簡単に統合できるため、管理ポイントをシンプル化して統合できます。さらに、Active Rolesでは、PowerShell、ADSI、SPML、およびカスタマイズ可能なWebインターフェイスの各機能の自動化や拡張も可能です。

Active Rolesには、管理やセキュリティ維持に必要なあらゆる同期技術が搭載されています。

- Lync/Skype for Business
- Exchange
- One Drive
- SharePoint
- AD LDS
- Office 365（ロールとグループを含む）
- Azure AD
- Microsoft SQL Server
- OLE DB（MS Access）
- フラットファイル

One Identityについて

One Identity（Quest Softwareグループ）は、組織のIDを重視したセキュリティ戦略の実現をお手伝いします。他には見られないほど幅広いOne IdentityのIDおよびアクセス管理製品のポートフォリオには、IDガバナンス、特権アクセス管理、およびアカウント管理が含まれます。これらすべてがハイブリッド・クラウド・デリバリ戦略によって強化されるため、組織にとってOne Identityを利用することは、脅威に対する保護を確保しながらもセキュリティによる制限のない環境を最大限実現するのに役立ちます。お客様の長期的な成功に対するOne Identityの取り組みは、他に例を見ないことが証明されています。世界で7,500を超える組織がOne Identityソリューションを利用し、1億2500万を超えるIDが管理されています。これらの組織はそのアジリティと効率性を向上させ、オンプレミス、クラウド、ハイブリッドを問わず、システムおよびデータへのセキュアなアクセスを確保しています。詳細については、次のWebサイトをご覧くださいwww.oneidentity.com。

© 2019 One Identity LLC ALL RIGHTS RESERVED. One IdentityおよびOne Identityロゴは、米国およびその他の国におけるOne Identity LLCの商標または登録商標です。One Identityの商標の一覧については、当社のWebサイト（www.oneidentity.com/legal）をご覧ください。その他すべての商標、サービスマーク、登録商標および登録サービスマークは各所有者に帰属します。
Datasheet_2019_ActiveRoles74_US_RS_42104