予定表統合のための Microsoft Exchange の設定

Exchange Web サービスによる Microsoft Exchange 2007 の設定

はじめる前に

Exchange Server 2007 の設定手順は、Windows Server 2003 と Windows Server 2008 のどちらを使用するかによって異なります。

Exchange Server 2007 上のメールボックスへのアクセスを設定する場合、次の手順を実行します。詳細手順については、次の URL で Exchange Server 2007 のマニュアルを参照してください。http://technet.microsoft.com/en-us/library/bb124558(EXCHG.80).aspx

ヒント IM and Presence Service では、Exchange Server への接続時にそのアカウントにログインするために必要なのはアカウントに対する偽装権限のみです。このアカウントは、通常、メールを受信しないため、領域の割り当てについて考慮する必要はありません。

Windows セキュリティポリシーの設定

IM and Presence Service の Microsoft Exchange との統合では、Windows 統合認証（NTLM）などのさまざまな認証方式がサポートされます。

IM and Presence Service は、NTLMv1 と NTLMv2 の両方の Windows 統合認証をサポートし、NTLMv2 がデフォルトとして使用されます。

NTLMv2 応答のみを送信するように **Lan Manager 認証レベル**を設定します。Windows ドメインコントローラで LM と NTLM を拒否すると、ドメインに NTLMv2 認証が適用されます。

（注） IM and Presence Service は NTLMv2 セッションセキュリティをサポートしていません。メッセージの機密性と整合性は、安全な http（https）によって確保されます。

Windows セキュリティ設定の確認

手順

ステップ 1 Exchange を実行している Windows ドメインコントローラおよびサーバーで、**[スタート（Start）] > [管理ツール（Administrative Tools）] > [ローカルセキュリティポリシー（Local Security Policy）]** を選択します。

ステップ 2 **[セキュリティ設定（Security Settings）] > [ローカルポリシー（Local Policies）] > [セキュリティのオプション（Security Options）]** に移動します。

ステップ 3 [ネットワークセキュリティ：NTLM SSPベースクライアント（セキュアなRPCを含む）のサーバー向け最小セッションセキュリティ（Network Security: Minimum session security for NTLM SSP based (including secure RPC) servers）] を選択します。

ステップ 4 [NTLMv2 セッションセキュリティが必要（Require NTLMv2 session security）] チェックボックスがオフになっていることを確認します。

ステップ 5 [NTLMv2 セッションセキュリティが必要（Require NTLMv2 session security）] チェックボックスがオンになっている場合は、次の手順を完了します。

a) [NTLMv2 セッションセキュリティが必要（Require NTLMv2 session security）] チェックボックスをオフにします。

b) [OK] をクリックします。

ステップ 6 新しいセキュリティ設定を適用するには、Exchange を実行している Windows ドメインコントローラとサーバーを再起動します。

（注） 再起動は、セキュリティポリシー設定の変更が実行されたサーバーでのみ必要です。

サービスアカウントにローカルでサインインするアクセス許可をユーザーに付与する

ユーザーがサービスアカウントにローカルにログインするように設定するは、次のいずれかの手順を実行します。

はじめる前に

- Exchange の偽装を正常に機能させるには、すべての Microsoft Exchange Server を Windows Authorization Access Group のメンバーにする必要があります。
- サービスアカウントは、Exchange 管理グループのメンバーであってはなりません。Exchange は、これらのグループのすべてのアカウントの偽装を明示的に拒否します。

Windows Server 2003 での Microsoft Exchange 2007 の設定

手順

ステップ 1 Exchange 表示専用管理者の役割を委任されたサービスアカウントを使用して Exchange Server 2007 ユーザーインターフェイスにログインします。

ステップ 2 左ペインの [セキュリティ設定（Security Settings）] から **[ローカルポリシー（Local Policies）]** > **[ユーザー権利の割り当て（User Rights Assignments）]** の順に選択します。

ステップ 3 コンソールの右ペインで [ローカルログオンを許可する（Allow Log On Locally）] をダブルクリックします。

ステップ 4 [ユーザーまたはグループの追加（Add User or Group）] を選択し、作成済みのサービスアカウントに移動して選択します。

ステップ 5 [名前の確認（Check Names）] を選択し、指定されたユーザーが正しいことを確認します。

ステップ 6 [OK] をクリックします。

次のタスク

サーバーレベルでの偽装権限の設定 （4 ページ）

Windows Server 2008 での Microsoft Exchange 2007 の設定

手順

ステップ 1 Exchange 表示専用管理者の役割を委任されたサービスアカウントを使用して Exchange Server 2007 にログインします。

ステップ 2 [スタート（Start）] を選択します。

ステップ 3 gpmc.msc と入力します。

ステップ 4 [Enter] を選択します。

ステップ 5 Exchange Server で [ドメインコントローラセキュリティ設定（Domain Controller Security Settings）] ウィンドウを開きます。

ステップ 6 左ペインの **[セキュリティ設定（Security Settings）]** から **[ローカルポリシー（Local Policies）]** > **[ユーザー権利の割り当て（User Rights Assignments）]** の順に選択します。

ステップ 7 コンソールの右ペインで [ローカルログオンを許可する（Allow Log On Locally）] をダブルクリックします。

ステップ 8 [これらのポリシーの設定を定義する（Define these policy settings）] チェックボックスが選択されていることを確認します。

ステップ 9 [ユーザーまたはグループの追加（Add User or Group）] を選択し、作成済みのサービスアカウントに移動して選択します。次に [OK] をクリックします。

ステップ 10 [名前の確認（Check Names）] を選択し、指定されたユーザーが正しいことを確認します。次に [OK] をクリックします。

ステップ 11 [ローカルログオンを許可する（Allow Log On Locally）] プロパティのダイアログボックスで [適用（Apply）] と [OK] をクリックします。

ステップ 12 ユーザー SMTP アドレスが *alias@FQDN* であることを確認します。そうでない場合は、ユーザープリンシパル名（UPN）を使用して偽装する必要があります。これは *alias@FQDN* と定義されます。

次のタスク

サーバーレベルでの偽装権限の設定　（4 ページ）

サーバーレベルでの偽装権限の設定

次の手順のコマンドを使用すると、サーバーレベルで偽装権限を付与することができます。また、データベース、ユーザー、連絡先レベルでもアクセス許可を付与することもできます。

はじめる前に

- 個々の Microsoft Exchange Server にアクセスするサービスアカウント権限のみを付与する場合は、

```
Get-OrganizationConfig
```

を次の文字列に置き換えます。

```
Get-ExchangeServer -Identity ServerName
```

ここで、*ServerName* は Exchange Server の名前です。

例

```
Add-ADPermission -Identity (Get-ExchangeServer -Identity  exchangeserver1).
DistinguishedName -User (Get-User -Identity user | select-object).identity
-ExtendedRights Send-As
```

- ユーザーの SMTP アドレスが alias@FQDN として定義されていることを確認します。そうでない場合は、ユーザープリンシパル名（UPN）を使用してユーザーアカウントを偽装する必要があります。

手順

ステップ 1 コマンドライン入力を行うために Exchange 管理シェル（EMS）を開きます。

ステップ 2 この Add-ADPermission コマンドを実行し、サーバーに偽装権限を追加します。

構文

```
Add-ADPermission -Identity (Get-OrganizationConfig).DistinguishedName -User (Get-User
-Identity User | select-object).identity -AccessRights GenericAll -InheritanceType
Descendents
```

例

```
Add-ADPermission -Identity (Get-OrganizationConfig).DistinguishedName -User (Get-User
-Identity Ex2007 | select-object).identity -AccessRights GenericAll -InheritanceType
Descendents
```

次のタスク

サービスアカウントの Active Directory サービス拡張権限の設定 （5 ページ）

サービスアカウントの Active Directory サービス拡張権限の設定

始める前に

これらのアクセス許可は、偽装を実行するサービスアカウントに対して設定する必要があります（クライアント アクセス サーバー（CAS）上）。

- CAS がロードバランサの背後に配置されている場合は、ロードバランサの背後にあるすべての CAS の Microsoft Exchange 2007 アカウントに対して **ms-Exch-EPI-Impersonation** 権限を付与します。

- お使いのメールボックス サーバーが CAS サーバーとは異なるマシン上にある場合は、すべてのメールボックスサーバーの Ex2007 アカウントに対して **ms-Exch-EPI-Impersonation** 権限を付与します。
- このアクセス許可は、[Active Directoryサイトとサービス（Active Directory Sites and Services）] または [Active Directory ユーザーとコンピュータ（Active Directory Users and Computers）] ユーザーインターフェイスを使用して設定することもできます。

手順

ステップ 1 Exchange 管理シェル（EMS）を開きます。

ステップ 2 EMS で次の Add-ADPermission コマンドを実行して、指定したサービスアカウント（Exchange 2007 など）のサーバーに対する偽装権限を追加します。

構文

```
Add-ADPermission -Identity (Get-OrganizationConfig).DistinguishedName -User (Get-User
-Identity User | select-object).identity -ExtendedRight ms-Exch-EPI-Impersonation
```

例

```
Add-ADPermission -Identity (Get-OrganizationConfig).DistinguishedName -User (Get-User
-Identity Ex2007 | select-object).identity -ExtendedRight ms-Exch-EPI-Impersonation
```

ステップ 3 EMS で次の Add-ADPermission コマンドを実行して、サービスアカウントに偽装する各メールボックスへの偽装権限を追加します。

構文

```
Add-ADPermission -Identity (Get-OrganizationConfig).DistinguishedName -User (Get-User
-Identity User | select-object).identity -ExtendedRight ms-Exch-EPI-Impersonation
```

例

```
Add-ADPermission -Identity (Get-OrganizationConfig).DistinguishedName -User (Get-User
-Identity Ex2007 | select-object).identity -ExtendedRight ms-Exch-EPI-May-Impersonate
```

次のタスク

サービスアカウントおよびユーザーメールボックスへの Send As 権限の付与 （6 ページ）

サービスアカウントおよびユーザーメールボックスへの Send As 権限の付与

サービスアカウントおよびユーザーメールボックスに Send As 権限を付与するには、次の手順に従います。

（注） この手順を実行するために、Microsoft Exchange 管理コンソール（EMC）を使用することはできません。

手順

ステップ 1 Exchange 管理シェル（EMS）を開きます。

ステップ 2 EMS で次の Add-ADPermission コマンドを実行して、サービスアカウントおよび関連するすべてのユーザー メールボックス ストアに Send As 権限を付与します。

構文

```
Add-ADPermission -Identity (Get-OrganizationConfig) .DistinguishedName -User (Get-User
-Identity User | select-object) .identity -ExtendedRights Receive-As
```

例

```
Add-ADPermission -Identity (Get-OrganizationConfig).DistinguishedName -User (Get-User
-Identity Ex2007 | select-object).identity -ExtendedRights Send-As
```

次のタスク

サービスアカウントおよびユーザーメールボックスへの偽装権限の付与 （7 ページ）

サービスアカウントおよびユーザーメールボックスへの偽装権限の付与

サービスアカウントおよびユーザーメールボックスに偽装権限を付与するには、次の手順に従います。

（注） この手順を実行するために、Microsoft Exchange 管理コンソール（EMC）を使用することはできません。

手順

ステップ 1 Exchange 管理シェル（EMS）を開きます。

ステップ 2 EMS で次の **Add-ADPermission** コマンドを実行して、サービスアカウントおよび関連するすべてのメールボックスストアに偽装権限を付与します。

構文

```
Add-ADPermission -Identity (Get-OrganizationConfig) .DistinguishedName -User (Get-User
-Identity User | select-object) .identity -ExtendedRights Receive-As
```

例

```
Add-ADPermission -Identity (Get-OrganizationConfig) .DistinguishedName -User (Get-User
-Identity EX2007 | select-object) .identity -ExtendedRights Receive-As
```

（注） IM and Presence Service では、Exchange Server への接続時にそのアカウントにログインするために必要なのはアカウントに対する偽装権限のみです。このアカウントは、通常、メールを受信しないため、領域の割り当てについて考慮する必要はありません。

次のタスク

Microsoft Exchange 2007 アカウントでのアクセス許可の確認 （8 ページ）

Microsoft Exchange 2007 アカウントでのアクセス許可の確認

Exchange 2007 アカウントにアクセス許可を割り当てた後で、そのアクセス許可がメールボックスのレベルまで伝播し、選択されたユーザーがメールボックスにアクセスしたり別のユーザーのアカウントを偽装したりできることを確認する必要があります。Exchange 2007 では、アクセス許可がメールボックスに伝播されるまでに多少時間がかかります。

手順

ステップ 1 Exchange Server 2007 の Exchange 管理コンソール（EMC）で、コンソールツリーの [Active Directory サイトとサービス（Active Directory Sites and Services）] を右クリックします。

ステップ 2 [表示（View）] をポイントし、[サービスノードの表示（Show Services Node）] を選択します。

ステップ 3 サービスノード（`Services/MS Exchange/First Organization/Admin Group/Exchange Admin Group/Servers` など）を展開します。

ステップ 4 クライアント アクセス サーバー（CAS）が、選択したサービスノードに表示されていることを確認します。

ステップ 5 各 CAS サーバーの [プロパティ（Properties）] を表示し、[セキュリティ（Security）] タブで次の点を確認します。「」

a) サービス アカウントがリストされている。

b) サービスアカウントに付与されているアクセス許可が（チェックされているボックスにより）アカウントに Exchange Web サービスの偽装権限が付与されていることを示している。

（注） アカウントまたは偽装権限が手順 5 のとおりに表示されない場合は、サービスアカウントを再度作成し、必要な偽装権限をアカウントに付与する必要があります。

ステップ 6 サービスアカウント（Ex2007 など）にストレージグループおよびメールボックス ストアに対する Allow impersonationpermission が付与され、個人情報の交換や別のユーザーアカウントでの送受信が可能であることを確認します。

ステップ 7 変更を有効にするために、Exchange Server の再起動が必要となる場合があります。これはテストによって確認されています。

次のタスク

Windows Server 2003 を実行する Exchange 2007 での認証の有効化 （18 ページ）

Exchange Web サービスによる Microsoft Exchange 2010 および 2013 の設定

Microsoft Exchange 2010 および 2013 サーバー上のメールボックスへのアクセスを設定する場合は、次のタスクを実行します。

はじめる前に

Exchange 2010 および 2013 サーバーを IM and Presence Service と統合するために Exchange Web サービス（EWS）を使用する前に、Exchange Server にスロットリング ポリシー パラメータ値を設定していることを確認します。これらの値は、EWS の予定表と IM and Presence Service との統合を正常に機能させるために必要な値です。

これらは、Exchange Server 2010 および 2013 向けのコマンドと設定です。

表 *1 : Exchange Server 2010* で推奨されるスロットリングポリシーの設定

パラメータ	推奨設定値：Exchange Server 2010
EWSFastSearchTimeoutInSeconds	60
EWSFindCountLimit	1000
EWSMaxConcurrency	100[1]
EWSMaxSubscriptions	Null
EWSPercentTimeInAD	50
EWSPercentTimeInCAS	90
EWSPercentTimeInMailboxRPC	60

[1] シスコが行ったテスト時には、予定表を使用するユーザー 50% に対応するにはデフォルトのスロットリング ポリシー値で十分でした。ただし、Client Access Server（CAS）への EWS リクエストの負荷が高い場合は、パラメータを 100 に引き上げることを推奨します。

表 *2 : Exchange Server 2013* または *2016* で推奨されるスロットリングポリシーの設定

パラメータ[1]	推奨設定値：**Exchange Server 2013** および **2016**
EwsCutoffBalance	3000000
EwsMaxBurst	300000
EwsMaxConcurrency	**100**
EwsMaxSubscriptions	**無制限**
EwsRechargeRate	900000

[1] これらは、Exchange Server 2013 で変更できる唯一の EWS パラメータです。

関連トピック

Exchange Server 2010
Exchange Server 2013

Windows セキュリティポリシーの設定

IM and Presence Service の Microsoft Exchange との統合では、Windows 統合認証（NTLM）などのさまざまな認証方式がサポートされます。

IM and Presence Service は、NTLMv1 と NTLMv2 の両方の Windows 統合認証をサポートし、NTLMv2 がデフォルトとして使用されます。

NTLMv2 応答のみを送信するように **Lan Manager 認証レベル**を設定します。Windows ドメインコントローラで LM と NTLM を拒否すると、ドメインに NTLMv2 認証が適用されます。

（注） IM and Presence Service は NTLMv2 セッションセキュリティをサポートしていません。メッセージの機密性と整合性は、安全な http（https）によって確保されます。

Windows セキュリティ設定の確認

手順

ステップ 1 Exchange を実行している Windows ドメインコントローラおよびサーバーで、**[スタート（Start）] > [管理ツール（Administrative Tools）] > [ローカルセキュリティポリシー（Local Security Policy）]** を選択します。

ステップ 2 **[セキュリティ設定（Security Settings）] > [ローカルポリシー（Local Policies）] > [セキュリティのオプション（Security Options）]** に移動します。

ステップ 3 [ネットワークセキュリティ：NTLM SSPベースクライアント（セキュアなRPCを含む）のサーバー向け最小セッションセキュリティ（Network Security: Minimum session security for NTLM SSP based (including secure RPC) servers）] を選択します。

ステップ 4 [NTLMv2 セッションセキュリティが必要（Require NTLMv2 session security）] チェックボックスがオフになっていることを確認します。

ステップ 5 [NTLMv2 セッションセキュリティが必要（Require NTLMv2 session security）] チェックボックスがオンになっている場合は、次の手順を完了します。

a) [NTLMv2 セッションセキュリティが必要（Require NTLMv2 session security）] チェックボックスをオフにします。

b) [OK] をクリックします。

ステップ 6 新しいセキュリティ設定を適用するには、Exchange を実行している Windows ドメインコントローラとサーバーを再起動します。

（注） 再起動は、セキュリティポリシー設定の変更が実行されたサーバーでのみ必要です。

Exchange 2010 の特定のユーザーまたはグループへの Exchange の偽装権限の設定

特定のユーザーまたはユーザーグループに Exchange の偽装権限を設定するには、Microsoft Exchange 管理シェル（EMS）を使用して次の手順を実行します。

これらは、Exchange Server 2010 向けのコマンドと設定です。Exchange Server 2013 を使用している場合は、Exchange 2013 または 2016 の特定のユーザーまたはグループに Exchange の偽装権限を設定 （13 ページ） の手順に従います。

手順

ステップ 1 Active Directory でアカウントを作成します。

ステップ 2 コマンド ライン入力を行うために EMS を開きます。

ステップ 3 EMS で New-ManagementRoleAssignment コマンドを実行し、他のユーザーアカウントを偽装する権限を指定サービスアカウント（*Ex2010* など）に付与します。

構文

```
New-ManagementRoleAssignment -Name:_suImpersonateRoleAsg -Role:ApplicationImpersonation
-User:user@domain
```

例

```
New-ManagementRoleAssignment -Name:_suImpersonateRoleAsg -Role:ApplicationImpersonation
-User:Ex2010@contoso.com
```

ステップ 4 この New-ManagementRoleAssignment コマンドを実行し、偽装権限が適用される範囲を定義します。この例では、指定された Exchange Server のすべてのアカウントを偽装する権限が、*Exch2010* アカウントに対して与えられます。

構文

```
New-ManagementScope -Name:_suImpersonateScope -ServerList:server_name
```

例

```
New-ManagementScope -Name:_suImpersonateScope -ServerList:nw066b-227
```

ステップ 5 New-ThrottlingPolicy コマンドを実行し、下の表の推奨値を使用して新しいスロットリングポリシーを作成します。

構文

```
New-ThrottlingPolicy -Name:Policy_Name -EwsMaxConcurrency:100 -EwsPercentTimeInAD:50
-EwsPercentTimeInCAS:90 -EwsPercentTimeInMailboxRPC:60 -EwsMaxSubscriptions:NULL
-EwsFastSearchTimeoutInSeconds:60 -EwsFindCountLimit:1000
```

例

```
New-ThrottlingPolicy -Name:IM_and_Presence_ThrottlingPolicy -EwsMaxConcurrency:100
-EwsPercentTimeInAD:50 -EwsPercentTimeInCAS:90 -EwsPercentTimeInMailboxRPC:60
-EwsMaxSubscriptions:NULL -EwsFastSearchTimeoutInSeconds:60 -EwsFindCountLimit:1000
```

表 *3 : Exchange Server 2010* で推奨されるスロットリングポリシーの設定

パラメータ	推奨設定値：**Exchange Server 2010**
EWSFastSearchTimeoutInSeconds	60
EWSFindCountLimit	1000
EWSMaxConcurrency	100[1]
EWSMaxSubscriptions	Null
EWSPercentTimeInAD	50
EWSPercentTimeInCAS	90
EWSPercentTimeInMailboxRPC	60

[1] シスコが行ったテスト時には、予定表を使用するユーザー 50% に対応するにはデフォルトのスロットリング ポリシー値で十分でした。ただし、Client Access Server（CAS）への EWS リクエストの負荷が高い場合は、パラメータを 100 に引き上げることを推奨します。

注：サポートされる Exchange SP1 でのみ使用可能です。

ステップ 6 Set-ThrottlingPolicyAssociation コマンドを実行し、新しいスロットリングポリシーと手順 2 で使用したサービスアカウントを関連付けます。

構文

```
Set-ThrottlingPolicyAssociation -Identity Username -ThrottlingPolicy Policy_Name
```

例

```
Set-ThrottlingPolicyAssociation -Identity Ex2010 -ThrottlingPolicy
IM_and_Presence_ThrottlingPolicy
```

次のタスク

Microsoft Exchange 2010 アカウントのアクセス許可の確認 （14 ページ）

関連トピック

Exchange Server 2010
Exchange Server 2013

Exchange2013または2016の特定のユーザーまたはグループにExchangeの偽装権限を設定

特定のユーザーまたはユーザーグループに Exchange の偽装権限を設定するには、Microsoft Exchange 管理シェル（EMS）を使用して次の手順を実行します。

これらは、Exchange Server 2013 または 2016 向けのコマンドと設定です。Exchange Server 2010 を使用している場合は、Exchange 2010 の特定のユーザーまたはグループへの Exchange の偽装権限の設定 （11 ページ） の手順に従います。

手順

ステップ 1 Active Directory でアカウントを作成します。

ステップ 2 コマンド ライン入力を行うために EMS を開きます。

ステップ 3 EMS で New-ManagementRoleAssignment コマンドを実行し、他のユーザーアカウントを偽装するアクセス許可を指定サービスアカウント（*Ex2013* など）に付与します。

構文

```
New-ManagementRoleAssignment -Name:_suImpersonateRoleAsg -Role:ApplicationImpersonation
-User:user@domain
```

例

```
New-ManagementRoleAssignment -Name:_suImpersonateRoleAsg -Role:ApplicationImpersonation
-User:Ex2013@contoso.com
```

ステップ 4 この New-ManagementRoleAssignment コマンドを実行し、偽装権限が適用される範囲を定義します。この例では、指定された Exchange Server のすべてのアカウントを偽装するアクセス許可が、*Exch2013* アカウントに対して与えられます。

構文

```
New-ManagementScope -Name:_suImpersonateScope -ServerList:server_name
```

例

```
New-ManagementScope -Name:_suImpersonateScope -ServerList:nw066b-227
```

ステップ 5 New-ThrottlingPolicy コマンドを実行し、下の表の推奨値を使用して新しいスロットリングポリシーを作成します。

構文

```
New-ThrottlingPolicy -Name:Policy_Name -EwsMaxConcurrency:100  -EwsMaxSubscriptions:NULL
-EwsCutoffBalance 3000000 -EwsMaxBurst 300000 -EwsRechargeRate 900000
```

例

```
New-ThrottlingPolicy -Name IMP_ThrottlingPolicy -EwsMaxConcurrency 100
-EwsMaxSubscriptions unlimited -EwsCutoffBalance 3000000 -EwsMaxBurst 300000
-EwsRechargeRate 900000
```

表 *4 : Exchange Server 2013* または *2016* で推奨されるスロットリングポリシーの設定

パラメータ[1]	推奨設定値：**Exchange Server 2013** および **2016**
EwsCutoffBalance	3000000
EwsMaxBurst	300000
EwsMaxConcurrency	**100**
EwsMaxSubscriptions	**無制限**
EwsRechargeRate	900000

[1] これらは、Exchange Server 2013 で変更できる唯一の EWS パラメータです。

注：サポートされる Exchange SP1 でのみ使用可能です。

ステップ 6 Set-ThrottlingPolicyAssociation コマンドを実行し、新しいスロットリングポリシーと手順 2 で使用したサービスアカウントを関連付けます。

構文

```
Set-ThrottlingPolicyAssociation -Identity Username -ThrottlingPolicy Policy_Name
```

例

```
Set-ThrottlingPolicyAssociation -Identity ex2013 -ThrottlingPolicy IMP_ThrottlingPolicy
```

次のタスク

Microsoft Exchange 2013 または 2016 のアカウントのアクセス許可の確認 （16 ページ）

Microsoft Exchange 2010 アカウントのアクセス許可の確認

Exchange 2010 アカウントにアクセス許可を割り当てた後で、そのアクセス許可がメールボックスのレベルまで伝播し、選択されたユーザーがメールボックスにアクセスしたり別のユー

ザーのアカウントを偽装したりできることを確認する必要があります。Exchange 2010 では、アクセス許可がメールボックスに伝播されるまでに多少時間がかかります。

これらは、Exchange Server 2010 向けのコマンドです。Exchange Server 2013 を使用している場合は、Microsoft Exchange 2013 または 2016 のアカウントのアクセス許可の確認 （16 ページ）の手順に従います。

手順

ステップ 1 Active Directory サーバーで、偽装アカウントが存在することを確認します。

ステップ 2 コマンドライン入力を行うために Exchange 管理シェル（EMS）を開きます。

ステップ 3 Exchange Server で、サービスアカウントに必要な次の偽装権限が付与されていることを確認します。

a) EMS で次のコマンドを実行します。

```
Get-ManagementRoleAssignment role: ApplicationImpersonation
```

b) コマンド出力で、次のように、指定アカウントに対する役割「ApplicationImpersonation」の割り当てが示されることを確認します。

コマンド出力の例

Name - - - -	Role - - -	Role AssigneeName-	Role AssigneeType-	Assignment Method- - -	Effective UserName
_suImpersonate RoleAs	Application Impersonation	ex2010	User	Direct	ex2010

ステップ 4 サービスアカウントに適用される管理の範囲が正しいことを確認します。

a) EMS で次のコマンドを実行します。

```
Get-ManagementScope _suImpersonateScope
```

b) 次のように、コマンド出力に偽装アカウント名が含まれていることを確認します。

コマンド出力の例

Name - - -	Scope RestrictionType	Exclusive	Recipient Root - -	Recipient Filter -	Server Filter- - -
_suImpersonate Scope	ServerScope	False	User	Direct	Distinguished Name

ステップ 5 次のコマンドを EMS で実行して、ThrottlingPolicy パラメータが EMS で定義されている内容と一致することを確認します。

```
Get-ThrottlingPolicy -Identity Policy_Name | findstr ^EWS
```

表 *5 : Exchange Server 2010* で推奨されるスロットリングポリシーの設定

パラメータ	推奨設定値：Exchange Server 2010
EWSFastSearchTimeoutInSeconds	60
EWSFindCountLimit	1000
EWSMaxConcurrency	100[1]
EWSMaxSubscriptions	Null
EWSPercentTimeInAD	50
EWSPercentTimeInCAS	90
EWSPercentTimeInMailboxRPC	60

[1] シスコが行ったテスト時には、予定表を使用するユーザー 50% に対応するにはデフォルトのスロットリングポリシー値で十分でした。ただし、Client Access Server（CAS）への EWS リクエストの負荷が高い場合は、パラメータを 100 に引き上げることを推奨します。

次のタスク

Exchange 仮想ディレクトリでの認証の有効化 （18 ページ）

関連トピック

Exchange Server 2010
Exchange Server 2013

Microsoft Exchange 2013 または 2016 のアカウントのアクセス許可の確認

Exchange 2013 または 2016 アカウントにアクセス許可を割り当てた後で、そのアクセス許可がメールボックスのレベルまで伝播し、選択されたユーザーがメールボックスにアクセスしたり別のユーザーのアカウントを偽装したりできることを確認する必要があります。アクセス許可がメールボックスに伝播されるまでには多少の時間がかかります。

（注） Exchange Server 2010 を使用している場合は、Microsoft Exchange 2010 アカウントのアクセス許可の確認 （14 ページ） の手順に従います。

手順

ステップ 1 Active Directory サーバーで、偽装アカウントが存在することを確認します。

ステップ 2 コマンドライン入力を行うために Exchange 管理シェル（EMS）を開きます。

ステップ 3 Exchange Server で、サービスアカウントに必要な次の偽装権限が付与されていることを確認します。

a) EMS で次のコマンドを実行します。

```
Get-ManagementRoleAssignment role: ApplicationImpersonation
```

b) コマンド出力で、次のように、指定アカウントに対する役割「ApplicationImpersonation」の割り当てが示されることを確認します。

コマンド出力の例

Name - - - -	Role - - -	Role AssigneeName-	Role AssigneeType-	Assignment Method- - -	Effective UserName
_suImpersonate RoleAs	Application Impersonation	ex2010	User	Direct	ex2010

ステップ 4 サービスアカウントに適用される管理の範囲が正しいことを確認します。

a) EMS で次のコマンドを実行します。

```
Get-ManagementScope _suImpersonateScope
```

b) 次のように、コマンド出力に偽装アカウント名が含まれていることを確認します。

コマンド出力の例

Name - - -	Scope RestrictionType	Exclusive	Recipient Root - -	Recipient Filter -	Server Filter- - -
_suImpersonate Scope	ServerScope	False	User	Direct	Distinguished Name

ステップ 5 次のコマンドを EMS で実行して、ThrottlingPolicy パラメータが EMS で定義されている内容と一致することを確認します。

```
Get-ThrottlingPolicy -Identity IMP_ThrottlingPolicy | Format-List | findstr ^Ews
```

表 *6 : Exchange Server 2013* または *2016* で推奨されるスロットリングポリシーの設定

パラメータ[1]	推奨設定値：**Exchange Server 2013** および **2016**
EwsCutoffBalance	3000000
EwsMaxBurst	300000
EwsMaxConcurrency	**100**
EwsMaxSubscriptions	**無制限**
EwsRechargeRate	900000

パラメータ[1]	推奨設定値：**Exchange Server 2013** および **2016**
[1] これらは、Exchange Server 2013 で変更できる唯一の EWS パラメータです。	

ステップ 6 ThrottlingPolicy が Exchange アカウントに関連付けられていることを確認します。

```
Get-ThrottlingPolicyAssociation -Identity ex2013
```

Exchange 仮想ディレクトリでの認証の有効化

始める前に

Exchange Web サービス（EWS）の統合が正しく機能するには、基本認証、Windows 統合認証またはその両方を Exchange Server 2007、2010 および 2013 の EWS 仮想ディレクトリ（/EWS）で有効にする必要があります。

Windows Server 2003 を実行する Exchange 2007 での認証の有効化

手順

ステップ 1 [管理ツール（Administrative Tools）] からインターネットインフォメーションサービス（Internet Information Services）を開き、サーバーを選択します。

ステップ 2 [サイト（Web Sites）] を選択します。

ステップ 3 [既定の Web サイト（Default Web Site）] を選択します。

ステップ 4 [EWS] ディレクトリフォルダを右クリックし、[プロパティ（Properties）] を選択します。

ステップ 5 [ディレクトリセキュリティ（Directory Security）] タブを選択します。

ステップ 6 [認証とアクセス制御（Authentication and Access Control）] で [編集（Edit）] をクリックします。

ステップ 7 [認証方法（Authentication Methods）] の下で、次のチェックボックスがオフになっていることを確認します。

- [匿名アクセスを有効にする（Enable anonymous access）]

ステップ 8 [認証済みアクセス（Authenticated Access）] で、次のチェックボックスの両方がオンになっていることを確認します。

- **Integrated Windows Authentication**
- **Basic Authentication (password is sent in clear text)**

ステップ 9 [OK] をクリックします。

次のタスク

Exchange Server の証明書の設定タスクフロー

Windows Server 2008 を実行する Exchange 2010、2013 または 2016 の認証の有効化

手順

ステップ 1 [管理ツール（Administrative Tools）]からインターネットインフォメーションサービス（Internet Information Services）を開き、サーバーを選択します。

ステップ 2 [サイト（Web Sites）] を選択します。

ステップ 3 [既定の Web サイト（Default Web Site）] を選択します。

ステップ 4 [EWS] を選択します。

ステップ 5 [IIS] セクションで、[認証（Authentication）] を選択します。

ステップ 6 次の認証方法が有効になっていることを確認します。

- [匿名認証（Anonymous Authentication）]
- [Windows 認証（Windows Authentication）] および [Basic 認証（Basic Authentication）]（両方またはどちらか）

ステップ 7 適切に設定するには、[操作（Actions）] カラムで [有効にする/無効にする（Enable/Disable）] リンクを使用します。

次のタスク

Exchange Server の証明書の設定タスクフロー

関連トピック

Outlook Web App の仮想ディレクトリの管理

Exchange Web サービス仮想ディレクトリの SSL を有効または無効にする

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。