Windows DC構成スクリプトについて

内容

はじめに

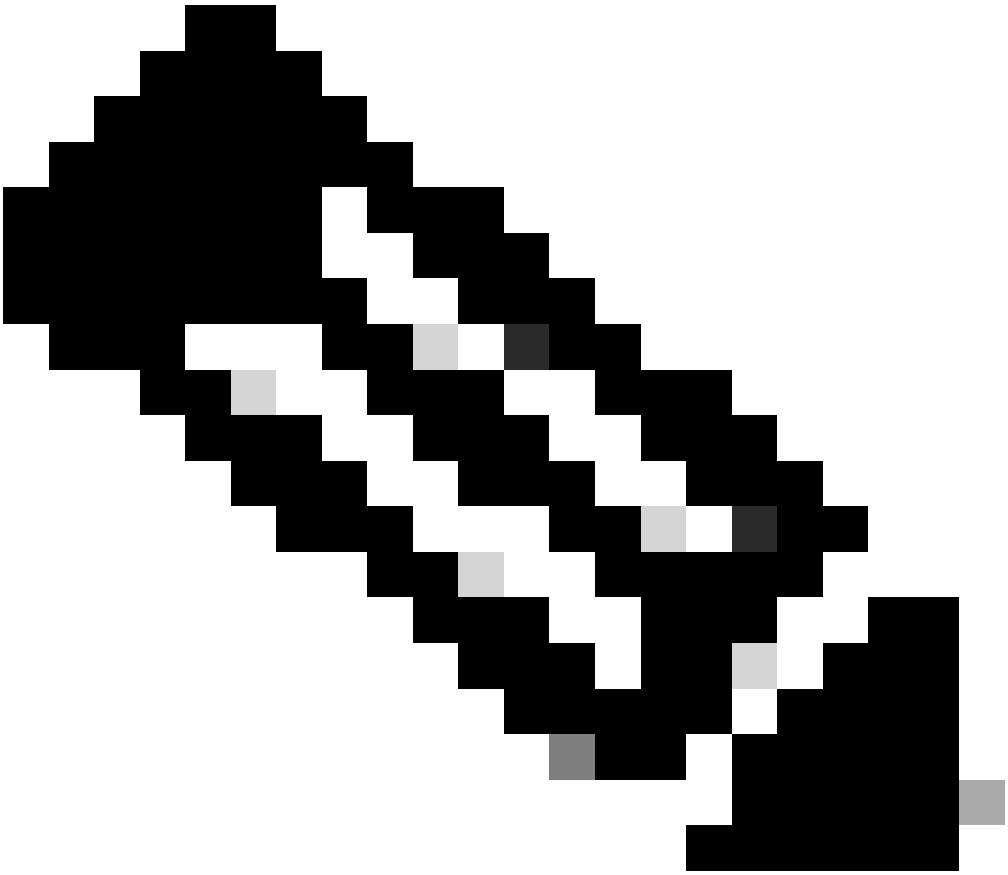
このドキュメントでは、ドメインコントローラ設定スクリプトによって行われたWindows環境への変更について説明します。

- 基本的な前提条件については、Insightsのドキュメントを参照してください。
  https://docs.umbrella.com/deployment-umbrella/docs/2-prerequisites
- これらのアクセス許可を手動で設定する方法の詳細については、次の記事を参照してください。
  OpenDNS_Connectorユーザに必要な権限。

DC設定スクリプトの概要

各ドメインコントローラには、Umbrella API/ダッシュボードへの1回限りの登録が必要です。DC設定スクリプトは、次の関数とともにこれを開始します。

1. 必要なアクセス許可とファイアウォール規則が構成されていることを確認してください
2. （オプション）これらのアクセス許可を自動的に構成する
3. （オプション）これらのチェックが成功した場合にのみ、Umbrella API/ダッシュボードにドメインコントローラを登録します。



注：ドメインコントローラのリストは、Umbrellaサポートによって手動で登録することもできます。 これは通常、ドメインコントローラでAPI/インターネットアクセスが不可能なシナリオで役立ちます。ただし、説明した権限の変更を設定する必要があるため、コンフィギュレーションスクリプトを実行することを強くお勧めします。

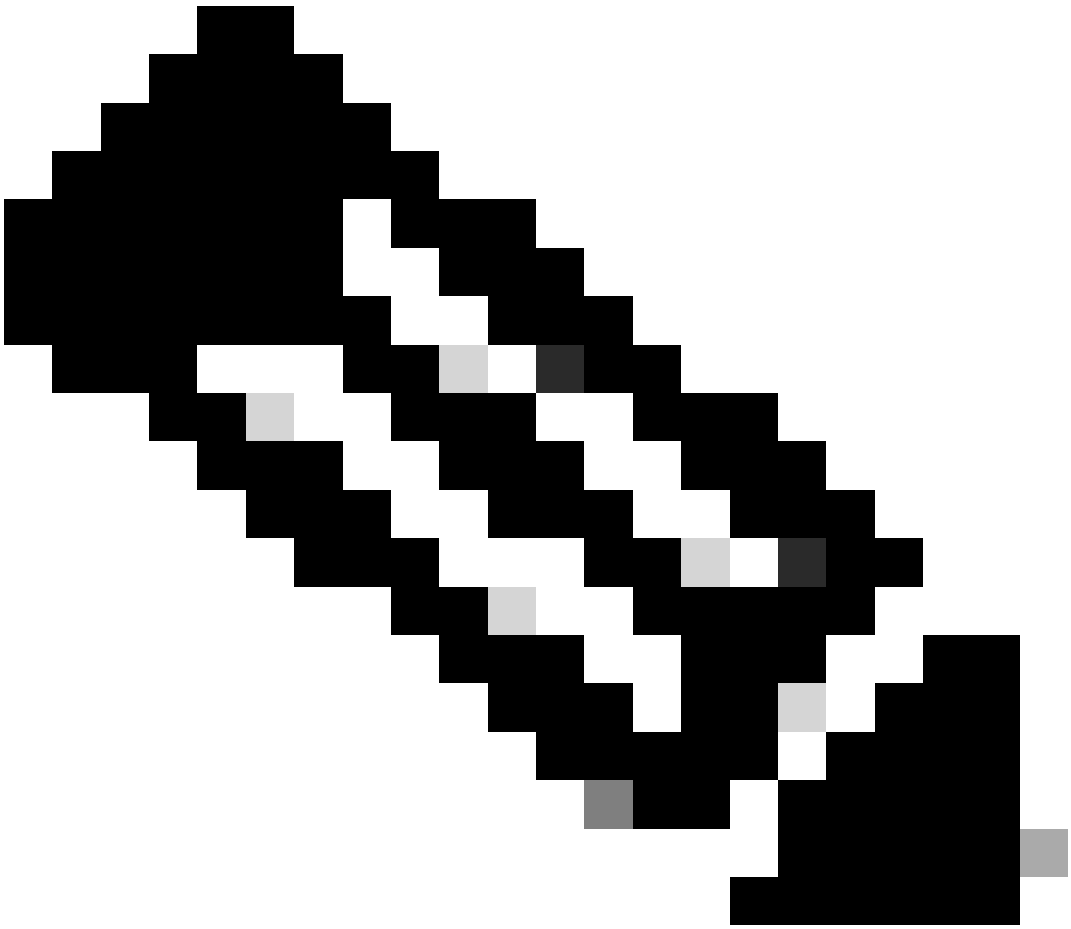
最初にスクリプトを実行しても、環境は変更されません。 スクリプトは、必要な権限がすべて設定されているかどうかをチェックします。 問題がある場合は、変更を求めるプロンプトが表示されます(Y/N)。

登録スクリプトが完了したら、ドメインコントローラ自体で実行するソフトウェアは必要ありません。ただし、OpenDNS Connectorサービスは少なくとも1台のコンピュータ（例：ドメインコントローラまたはメンバサーバ）にインストールする必要があります。

ステージ1 – テスト

スクリプトは最初に次の情報を収集します。

- OSバージョンとフォレストの機能レベルを確認します
- スクリプトが管理者として実行されているかどうかを確認します。
- サーバのIPアドレス、ホスト名、およびドメイン名情報を取得します。
- Windowsファイアウォールが有効になっているかどうか、および組み込みの「リモート管理」ルールが許可されているかどうかを確認します
- 必要なドメインユーザーアカウント'OpenDNS_Connector'を確認します



注:OpenDNS_Connectorユーザが存在しない場合、スクリプトは結果を出力して中止します。 このドメインユーザーは、スクリプトを実行する前に手動で作成する必要があります。 OpenDNS_Connectorアカウントが存在する場合、スクリプトはこれらのチェックに進みます。

- OpenDNS_Connectorユーザがroot\cimv2 WMI名前空間で「Remote Enable」および「Read Security」の権限を持っているかどうかを確認します。
- OpenDNS_ConnectorアカウントにActive Directoryの'Replicating Directory Changes'権限があるかどうかを確認します。この権限は、通常、Enterprise Read-Only Domain Controllersグループのメンバーシップによって付与されます。

- OpenDNS_Connectorアカウントが「Event Log Readers」グループのメンバーであるかどうかを確認します
- OpenDNS_Connectorアカウントが「Distributed COM Users」グループのメンバーであるかどうかを確認します
- ポリシーの結果セット(RSOP)をチェックして、グループポリシーで'ログオンイベントの監査'が有効になっているかどうかを確認します
- ポリシーの結果セット(RSOP)を確認して、OpenDNS_Connectorアカウントに「監査およびセキュリティログの管理」権限が割り当てられているかどうかを確認します

ステージ1b – テスト結果

コンフィギュレーションスクリプトによって出力される結果は、OSのバージョンによって異なります。

サーバ2003以降では、次の結果が表示されます。

```
AD User Exists:                true/false
WMI Permissions Set:           true/false
DCOM Permissions Set:          true/false
RDC Permissions Set:           true/false
Audit Policy Set:              true/false
Manage Event Log Policy Set:   true/false
Distributed COM MemberOf:      true/false
```

サーバ2008以降（フォレストの機能レベルが2008+の場合のみ）では、この情報も表示されます。 （このグループは以前のバージョンには存在しません）:

```
Event Log Readers MemberOf:     true/false
```

ステージ2：自動設定の変更

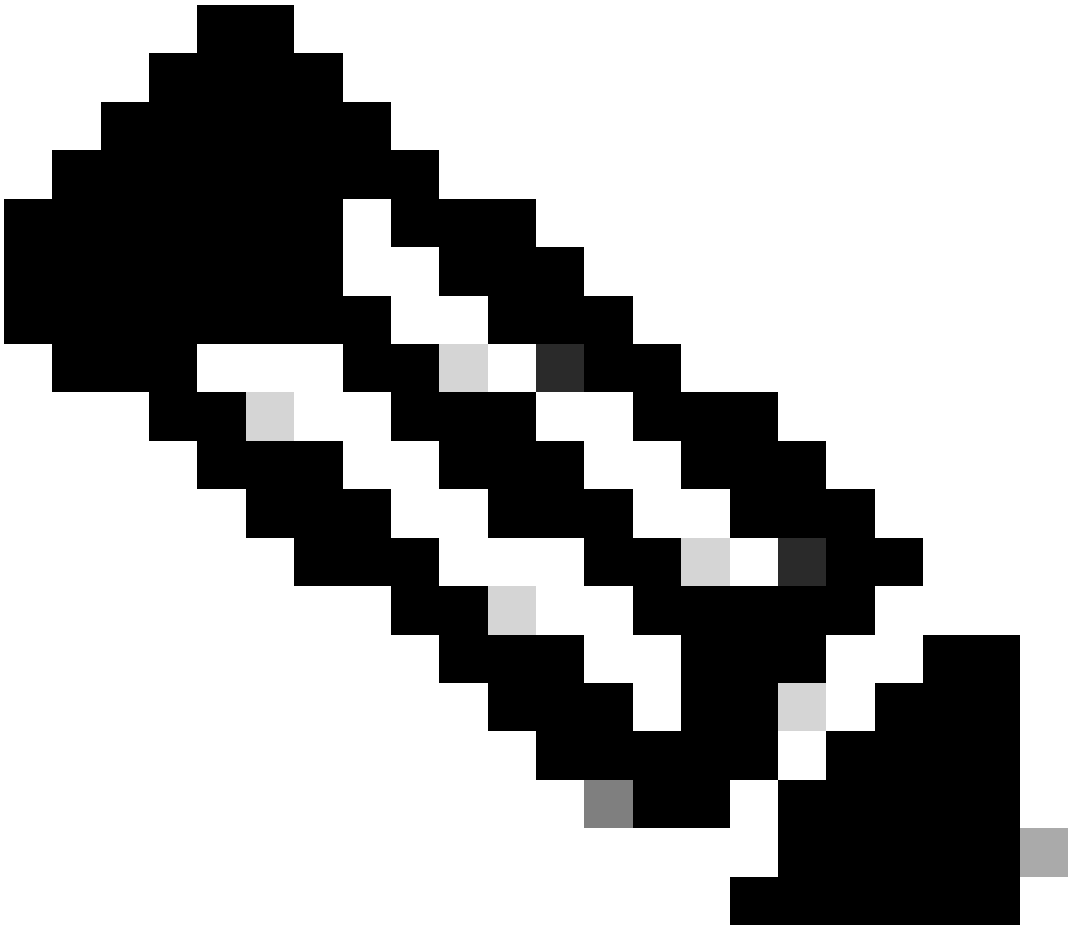
このチェックに失敗すると、変更を行う前に「このドメインコントローラ（yまたはn）を自動設定しますか。」というメッセージが表示されます。

次の変更が行われます。

- 必要に応じて、組み込みのリモート管理Windowsファイアウォール規則を有効にします
- root\cimv2 WMI名前空間で'OpenDNS_Connector'アカウント'Remote Enable'および'Read Security'アクセス許可を明示的に付与します。
- 'OpenDNS_Connector'アカウントに'Replicating Directory Changes'アクセス許可を明示的に付与します
- 'OpenDNS_Connector'アカウントを'Distributed COM users'グループに追加します

2008+では、この変更も行われます。

- 'OpenDNS_Connector'アカウントを'Event Log Readers'グループに追加します



> 注：自動設定が拒否された場合、またはこれらの変更が失敗した場合、スクリプトは登録に進みません。

ステージ2b – 自動設定の警告

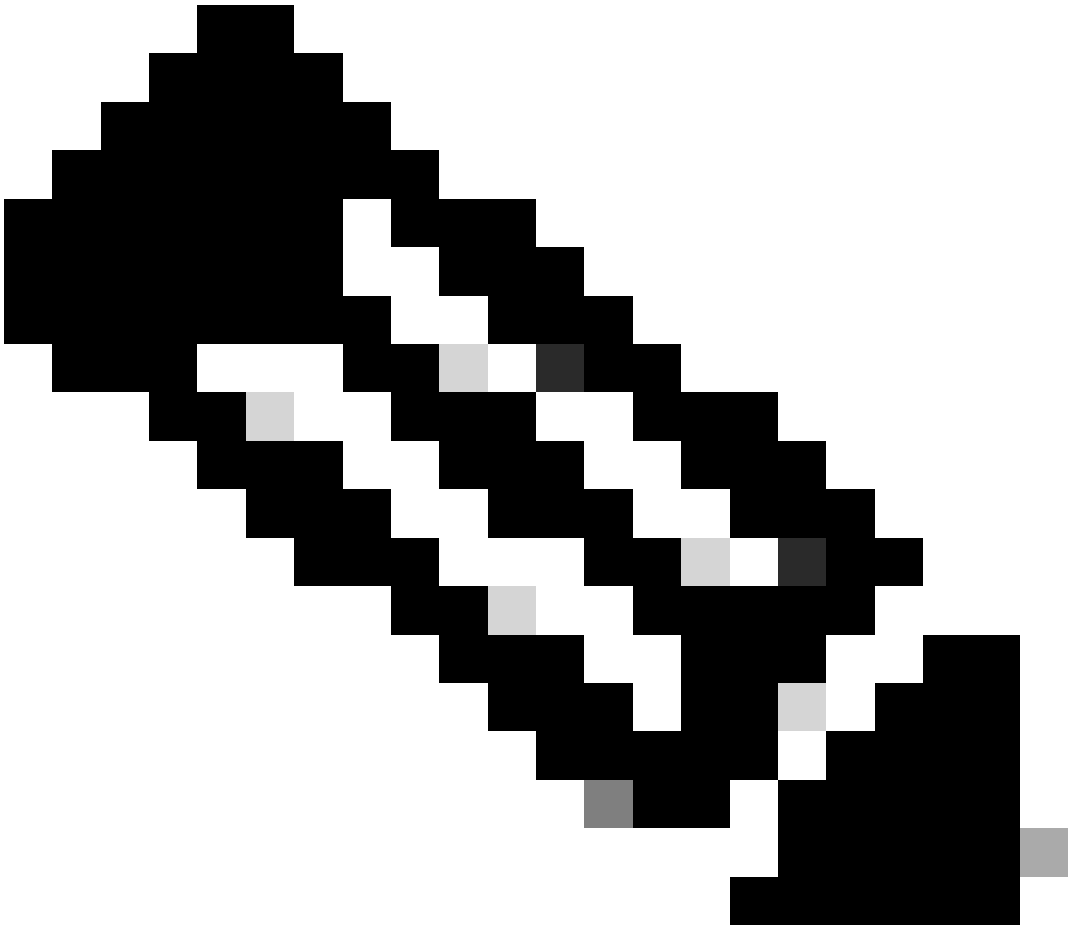
グループポリシー設定が正しく構成されていない場合、スクリプトは警告を生成します。 スクリプトでは、これらの問題を修正できません。

すべてのオペレーティングシステム：

- [ログオンイベントの監査]設定がグループポリシーで正しく構成されていない場合は警告が表示されますが、グループポリシーは変更されません。

2003 (および2003年の機能レベル) :

- このスクリプトは、「監査およびセキュリティログの管理」権限がグループポリシーで正しく設定されていない場合に警告しますが、グループポリシーは変更されません。



注：これらの問題を手動で修正し、設定スクリプトを再実行してください。スクリプトは、これらを修正するまで登録に進みません。

ステージ3 – 登録

スクリプトは、Umbrellaを使用してドメインコントローラを登録する前に、「`Would you like to register this Domain Controller (y or n)?`」というメッセージを表示します。この情報はUmbrellaに送信されます。

- ドメインコントローラのホスト名/ラベル
- ドメイン名
- IP アドレス

- Umbrella組織でDCを一意に識別するための一意の組織IDおよびトークン（スクリプトに含まれる）。

登録は、https://api.opendns.com経由で安全に行われます。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。