Entender o Script de Configuração de DC do Windows

Contents

Introdução

Visão geral do script de configuração DC

Etapa 1 - Testes

Etapa 1b - Resultados do teste

Estágio 2 - Alterações de configuração automática

Estágio 2b - Avisos de configuração automática

Etapa 3 - Registro

Introdução

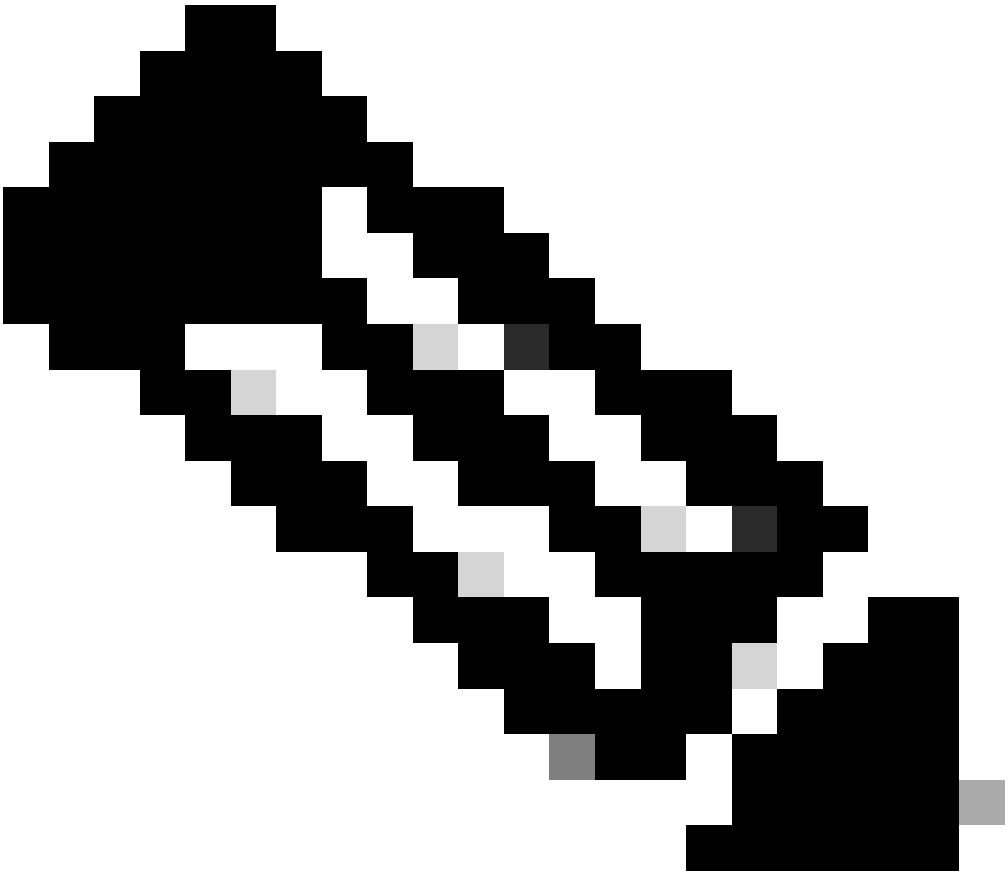
Este documento descreve as alterações em seu ambiente Windows que são feitas pelo nosso script de Configuração do Controlador de Domínio.

- Para obter os pré-requisitos básicos, consulte a documentação do Insights: https://docs.umbrella.com/deployment-umbrella/docs/2-prerequisites
- Para obter informações detalhadas sobre como definir essas permissões manualmente, consulte este artigo: Permissões necessárias para o usuário do OpenDNS_Connector.

Visão geral do script de configuração DC

Cada controlador de domínio requer um registro único com a Umbrella API/Dashboard. Nosso script de configuração de DC inicia isso junto com estas funções:

1. Verifique se as permissões necessárias e as regras de firewall estão configuradas
2. (Opcional) Configure automaticamente essas permissões
3. (Opcional) Registre o controlador de domínio com a API/painel Umbrella, somente se essas verificações forem bem-sucedidas.



Note: Uma lista de controladores de domínio também pode ser manualmente registrada pelo suporte do Umbrella. Isso geralmente é útil em cenários onde o acesso à API/Internet não é possível para o controlador de domínio. No entanto, as alterações de permissão descritas AINDA DEVEM ser configuradas, portanto, recomendamos que você execute o script de configuração.

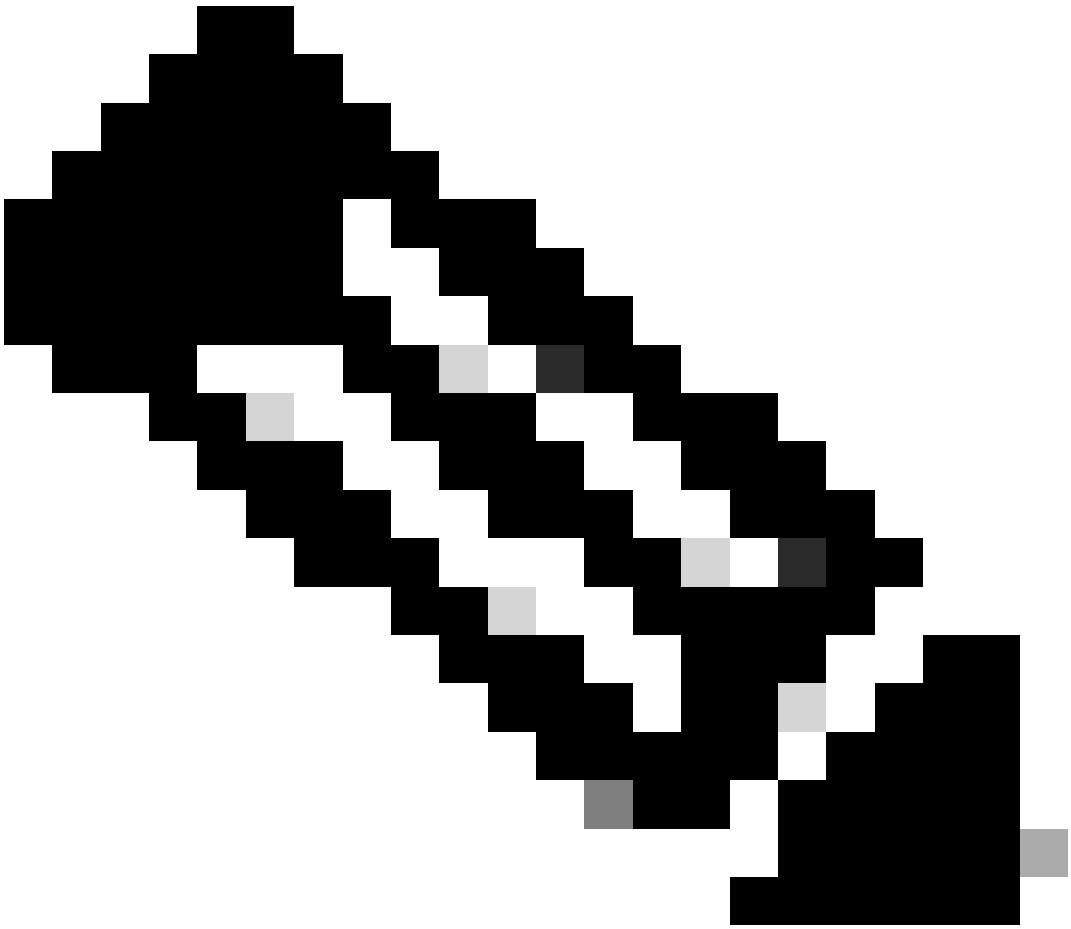
Ao executar o script inicialmente, nenhuma alteração é feita no ambiente. O script verifica se todas as permissões necessárias estão em vigor. Se houver um problema, você será avisado `(S/N)`, mas para fazer alterações.

Após a conclusão do script de registro, nenhum software é necessário para ser executado no próprio Controlador de domínio. No entanto, o serviço OpenDNS Connector deve ser instalado em pelo menos um computador (por exemplo, Controlador de Domínio ou Servidor Membro).

Etapa 1 - Testes

O roteiro reúne inicialmente estas informações:

- Verifica a versão do SO e o nível funcional da floresta
- Verifica se o script está sendo executado como Administrador.
- Obtém as informações de Endereço IP, Nome de Host e Nome de Domínio dos servidores
- Verifique se o Firewall do Windows está habilitado e se a regra interna de 'Administração Remota' é permitida
- Verifica a conta de usuário de domínio necessária 'OpenDNS_Connector'



Note: Se o usuário do OpenDNS_Connector não existir, o script imprimirá os resultados e anulará. Este usuário de domínio deve ser criado manualmente antes da execução do script. Se a conta OpenDNS_Connector existir, o script continuará com essas verificações.

- Verifica se o usuário do OpenDNS_Connector tem permissões para 'Remote Enable' e 'Read Security' no namespace raiz\cimv2 WMI.
- Verifica se a conta OpenDNS_Connector tem a permissão 'Replicating Diretory Changes' do Ative Diretory, que normalmente é concedida pela associação do grupo Controladores de Domínio Somente Leitura Corporativos.

- Verifica se a conta OpenDNS_Connector é membro do grupo 'Leitores do Log de Eventos'
- Verifica se a conta OpenDNS_Connector é membro do grupo 'Usuários COM Distribuídos'
- Verifica o conjunto de políticas resultante (RSOP) para ver se 'Auditoria de Eventos de Logon' está habilitada por meio da política de grupo
- Verifica o conjunto de políticas resultante (RSOP) para ver se a conta OpenDNS_Connector tem o direito 'Gerenciar log de auditoria e segurança' atribuído

Etapa 1b - Resultados do teste

Os resultados impressos pelo script de configuração variam de acordo com a versão do SO.

No servidor 2003 e mais recente você verá estes resultados:

```
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
```

No Server 2008 e mais recente (somente quando o nível funcional da floresta é 2008+), essas informações também são exibidas. (Este grupo não existe em versões anteriores):

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

Estágio 2 - Alterações de configuração automática

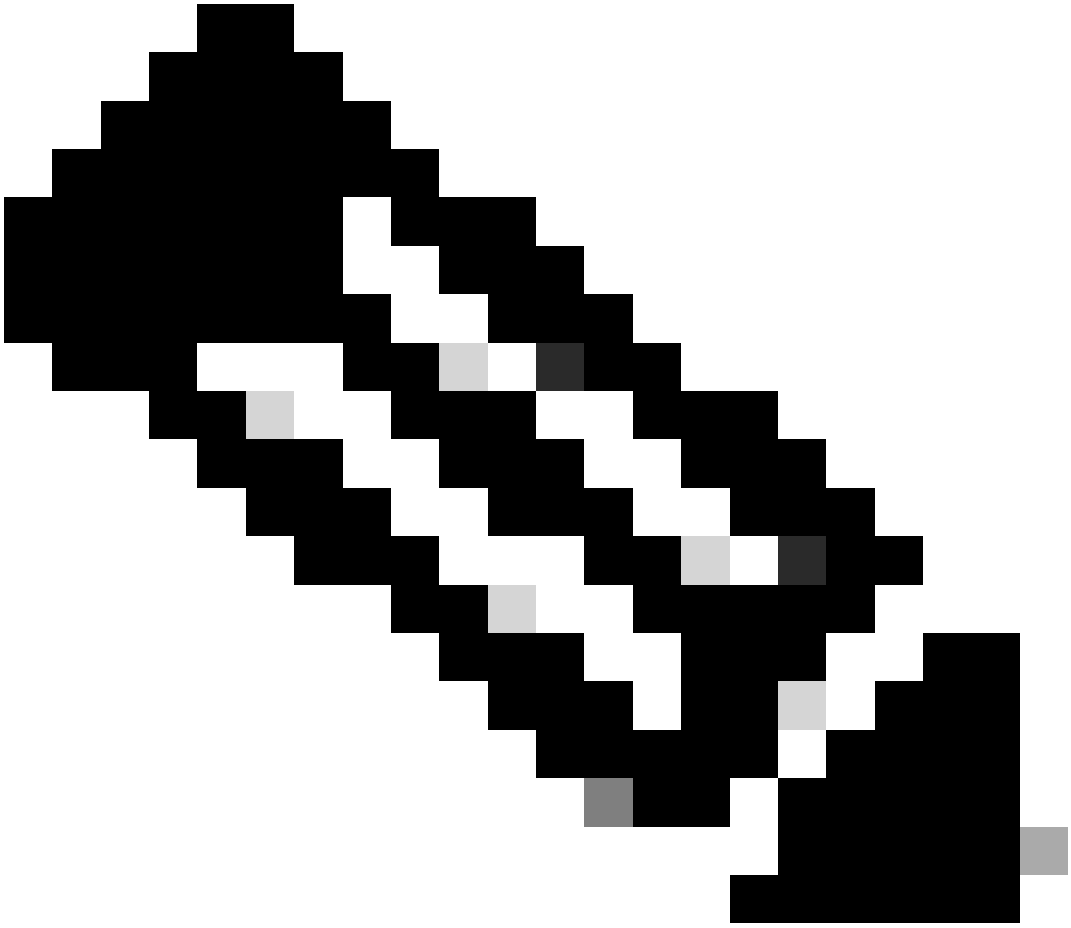
Se essa verificação falhar, você será solicitado a `"Deseja que configuremos automaticamente este controlador de domínio (s ou n)?"` antes de fazer qualquer alteração.

Estas alterações são feitas:

- Habilita a regra interna do Firewall do 'Administração Remota' do Windows, se necessário
- Concede explicitamente as permissões 'Remote Enable' e 'Read Security' para a conta 'OpenDNS_Connector' no namespace raiz\cimv2 WMI.
- Concede explicitamente as permissões da conta 'OpenDNS_Connector' 'Replicando Alterações de Diretório'
- Adiciona a conta 'OpenDNS_Connector' ao grupo 'Usuários COM distribuídos'

Em 2008+, esta alteração também é efetuada:

- Adiciona a conta 'OpenDNS_Connector' ao grupo 'Leitores do Log de Eventos'



Note: Se a configuração automática for recusada ou essas alterações falharem, o script não continuará o registro.

Estágio 2b - Avisos de configuração automática

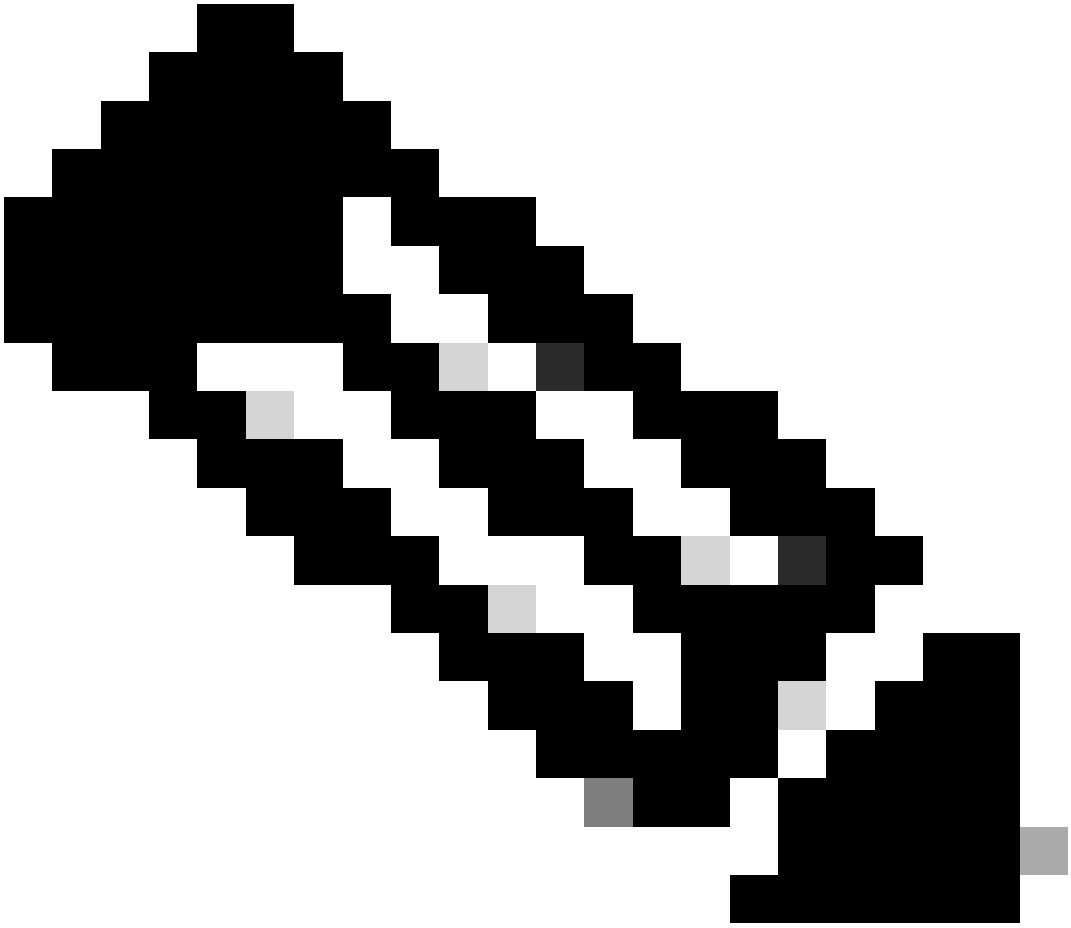
O script produzirá avisos se as configurações de Diretiva de Grupo não estiverem definidas corretamente. O script não pode corrigir esses problemas.

Todos os sistemas operacionais:

- O script AVISA se a configuração "Auditoria de Eventos de Logon" não estiver configurada corretamente na Diretiva de Grupo, mas não modifica a Diretiva de Grupo.

Em 2003 (E nível funcional em 2003):

- O script AVISA se o direito 'Gerenciar log de auditoria e segurança' não está configurado corretamente na Diretiva de Grupo, mas não modifica a Diretiva de Grupo.



Note: Corrija manualmente esse problema e execute novamente o script de configuração. O script não prossegue com o registro até que eles sejam corrigidos.

Etapa 3 - Registro

O script avisa antes de registrar o Controlador de Domínio com o Umbrella "`Deseja registrar este Controlador de Domínio (s ou n)?`".Estas informações são enviadas para o Umbrella:

- Rótulo/nome de host do controlador de domínio
- Nome de domínio
- IP Address
- A ID e o token exclusivos da sua empresa (contidos no seu script) para identificar exclusivamente o DC com a sua empresa de guarda-chuva.

O registro ocorre com segurança via https://api.opendns.com

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.