了解Windows DC配置脚本

目录

简介

DC配置脚本概述

阶段1 — 测试

阶段1b — 测试结果

阶段2 — 自动配置更改

第2b阶段 — 自动配置警告

阶段3 — 注册

简介

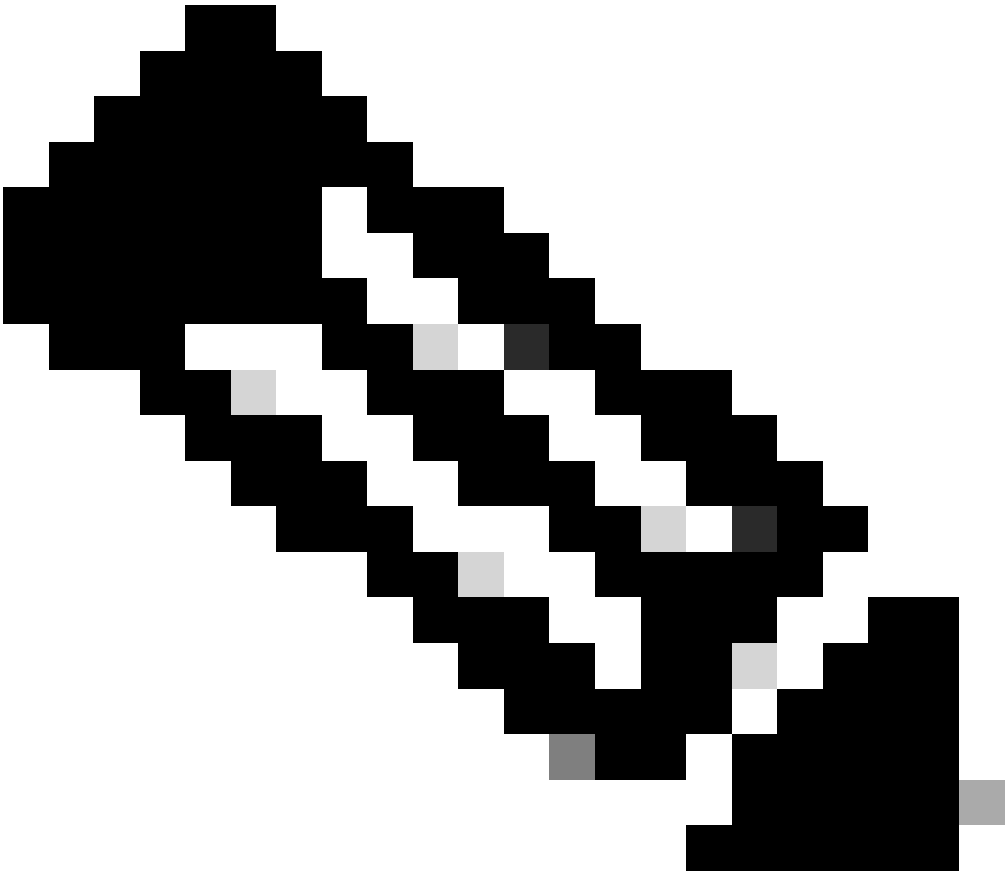
本文档介绍由我们的域控制器配置脚本对您的Windows环境进行的更改。

- 有关基本前提条件，请参阅见解文档：https://docs.umbrella.com/deployment-umbrella/docs/2-prerequisites
- 有关如何手动设置这些权限的详细信息，请参阅以下文章：OpenDNS_Connector用户所需的权限。

DC配置脚本概述

每个域控制器都需要向Umbrella API/控制面板进行一次性注册。我们的DC配置脚本将启动此脚本以及以下功能：

1. 检查必要的权限和防火墙规则已配置
2. （可选）自动配置这些权限
3. （可选）仅当这些检查成功时，才向Umbrella API/控制面板注册域控制器。



注意：还可以通过Umbrella支持手动注册域控制器列表。 这通常适用于域控制器无法进行API/Internet访问的情况。但是，上述权限更改仍然必须配置，因此我们仍然强烈建议运行配置脚本。

最初运行脚本时，不会对环境进行任何更改。 脚本会检查是否所有必要的权限都已就位。 如果出现问题，系统会提示您(Y/N)，但要求您进行更改。

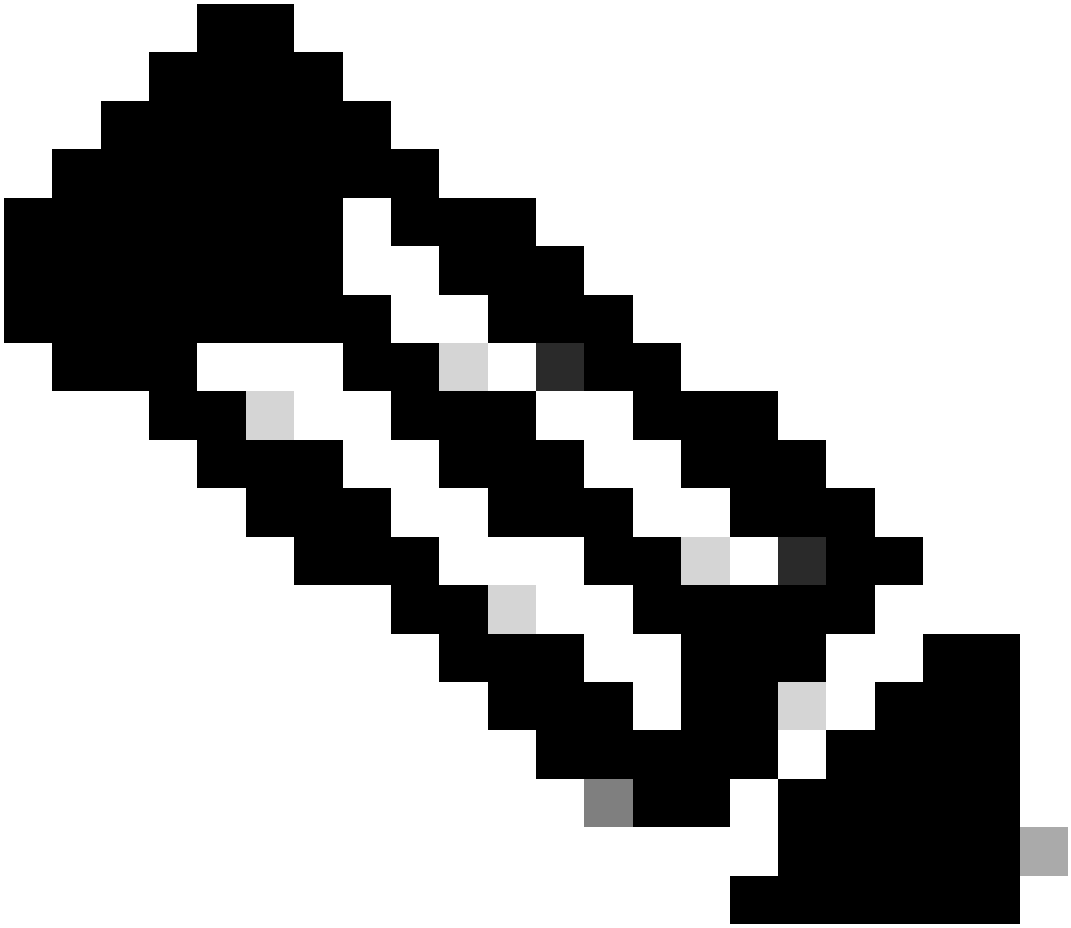
注册脚本完成后，无需在域控制器本身上运行任何软件。但是，OpenDNS Connector服务必须安装在至少一台计算机上(例如，域控制器或成员服务器)。

阶段1 — 测试

该脚本最初收集以下信息：

- 检查OS版本和林功能级别
- 检查脚本是否以管理员身份运行。
- 获取服务器的IP地址、主机名和域名信息

- 检查是否启用了Windows防火墙，以及是否允许内置的“远程管理”规则
- 检查所需的域用户帐户“OpenDNS_Connector”



注意：如果OpenDNS_Connector用户不存在，脚本将打印结果并中止。 在运行脚本之前，必须手动创建此域用户。如果OpenDNS_Connector帐户存在，脚本将继续进行这些检查。

- 检查OpenDNS_Connector用户是否具有根\cimv2 WMI命名空间中的“远程启用”和“读取安全”的权限。
- 检查OpenDNS_Connector帐户是否具有Active Directory “Replicating Directory Changes”权限，该权限通常由企业只读域控制器组的成员授予。
- 检查OpenDNS_Connector帐户是否是“事件日志读取器”组的成员。
- 检查OpenDNS_Connector帐户是否是“分布式COM用户”组的成员
- 检查策略的结果集(RSOP)，以查看“审核登录事件”是否通过组策略启用
- 检查策略的结果集(RSOP)，以查看是否为OpenDNS_Connector帐户分配了“管理审核和安全日志”权限

阶段1b — 测试结果

配置脚本打印的结果因操作系统版本而异。

在server 2003和更高版本上，您可以看到以下结果：

```
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
```

在Server 2008和更高版本上（仅当林功能级别为2008+时）也会显示此信息。 （此组在早期版本中不存在）：

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

阶段2 — 自动配置更改

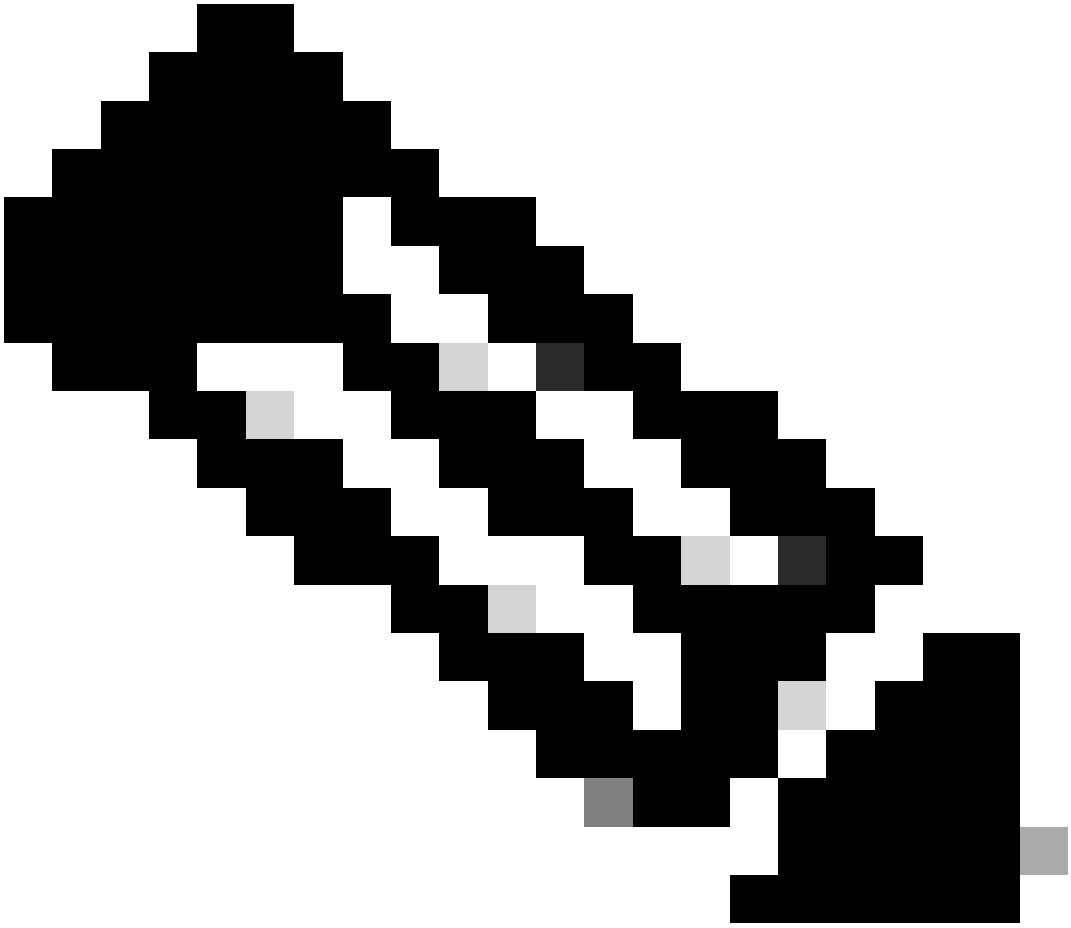
如果检查失败，系统将提示“是否希望我们自动配置此域控制器（y或n）？” 进行更改之前。

进行以下更改:

- 如有必要，启用内置“远程管理”Windows防火墙规则
- 在root\cimv2 WMI命名空间中显式授予“OpenDNS_Connector”帐户“Remote Enable”和“Read Security”权限。
- 明确授予“OpenDNS_Connector”帐户“复制目录更改”权限
- 将“OpenDNS_Connector”帐户添加到“分布式COM用户”组

在2008+年，还进行了以下更改：

- 将“OpenDNS_Connector”帐户添加到“Event Log Readers”组



注意：如果拒绝自动配置，或者这些更改失败，脚本不会继续注册。

第2b阶段 — 自动配置警告

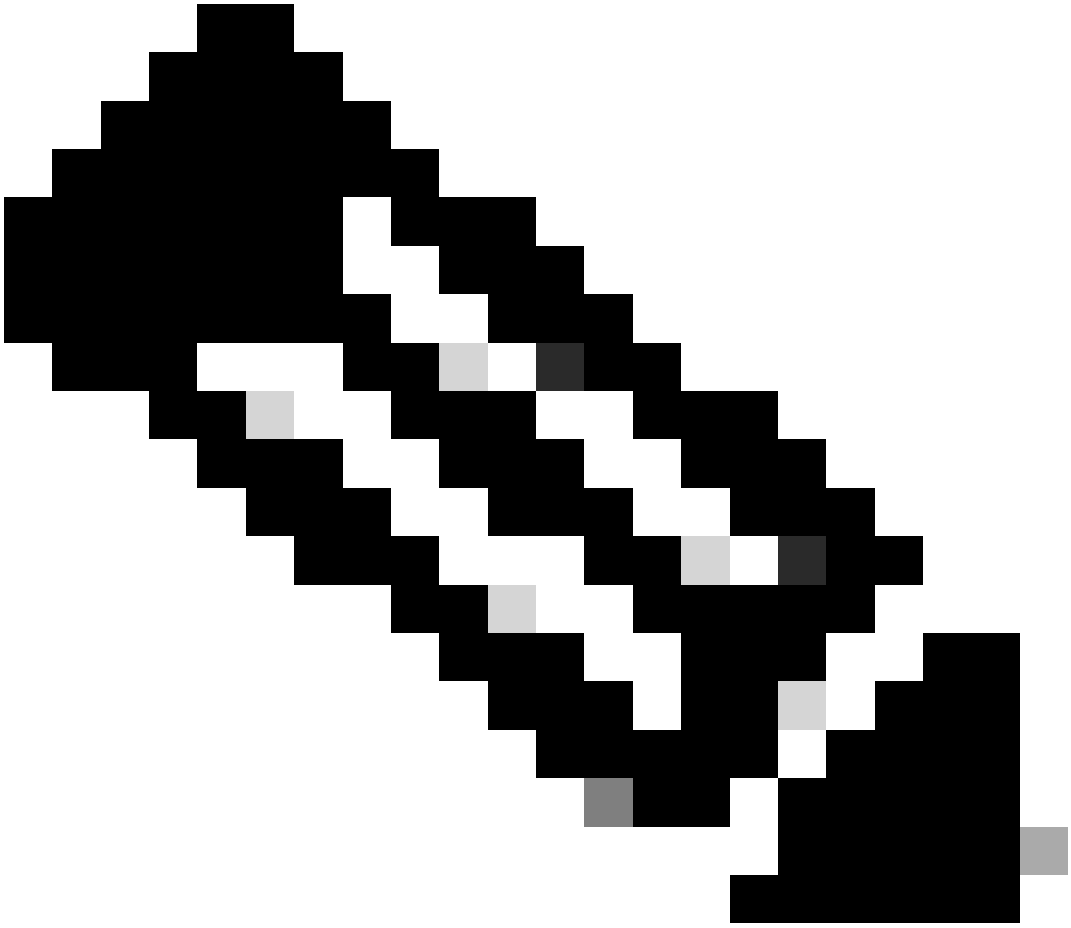
如果组策略设置配置不正确，脚本将生成警告。 脚本无法更正这些问题。

所有操作系统：

- 如果“审核登录事件”设置未在组策略中正确配置，但未修改组策略，脚本将发出警告。

在2003（和2003功能级别）上：

- 如果“管理审核和安全日志”权限未在“组策略”中正确配置，但不会修改组策略，脚本将发出警告。



注意：请手动更正这些问题，然后重新运行配置脚本。在更正这些错误之前，脚本不会继续注册。

阶段3 — 注册

脚本会在向Umbrella注册域控制器之前提示“是否要注册此域控制器(y或n)？”。此信息将发送到Umbrella:

- 域控制器主机名/标签
- 域名
- IP Address
- 您的唯一组织ID和令牌（包含在脚本中），用于通过Umbrella组织唯一标识DC。

通过https://api.opendns.com安全进行注册

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。