Understand Windows DC Configuration Script

Contents

Introduction

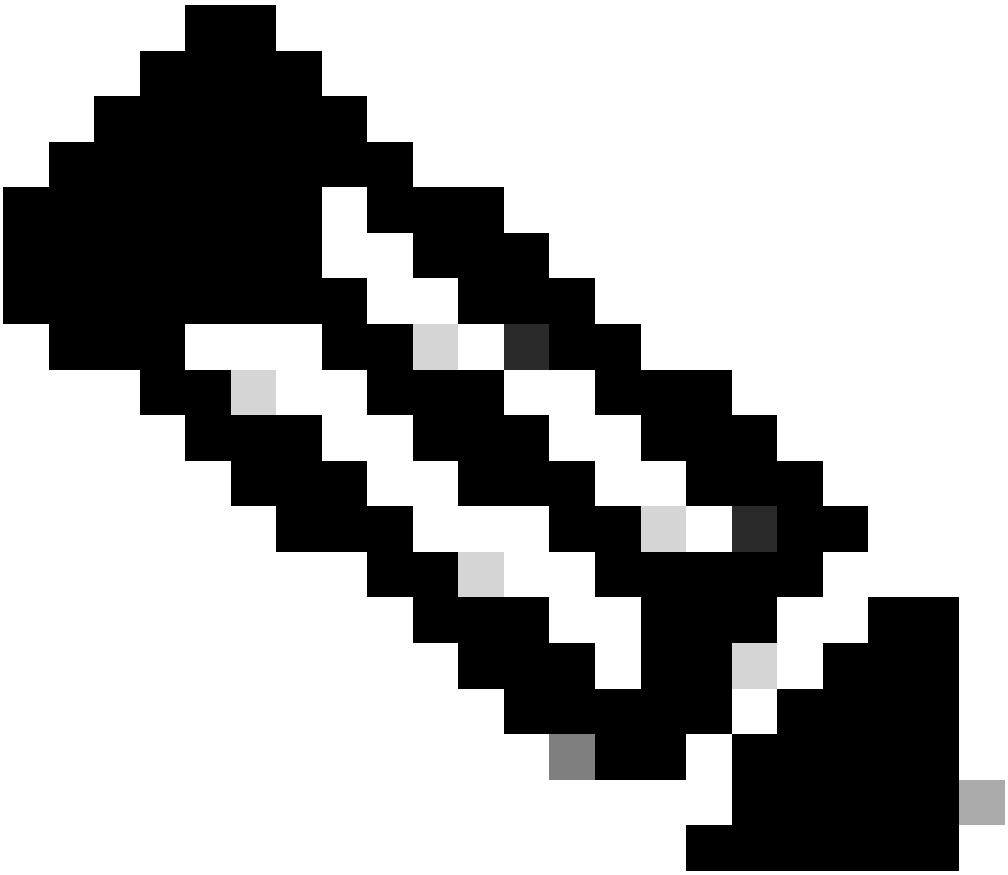
This document describes the changes to your Windows environment that are made by our **Domain Controller Configuration script**.

- For basic pre-requisites please see the Insights documentation: https://docs.umbrella.com/deployment-umbrella/docs/2-prerequisites
- For detailed information on how to set these permissions manually, please see this article: Required Permissions for the OpenDNS_Connector user.

DC Configuration Script Overview

Each domain controller requires a one-time registration with the Umbrella API/Dashboard. Our DC Configuration Script initiates this along with these functions:

1. Check necessary permissions and firewall rules are configured
2. (Optional) Automatically configure those permissions
3. (Optional) Register the Domain Controller with the Umbrella API/Dashboard, only if these checks have succeed.



Note: A list of Domain Controllers can also be manually registered by Umbrella support. This is typically useful in scenarios where the API / Internet access is not possible for the domain controller. However, the described permission changes MUST still be configured, so we still strongly recommend to run the configuration script.

When running the script initially no changes are made to the environment. The script checks if all the necessary permissions are in place. If there is a problem, you are prompted `(Y/N)` but for making changes.

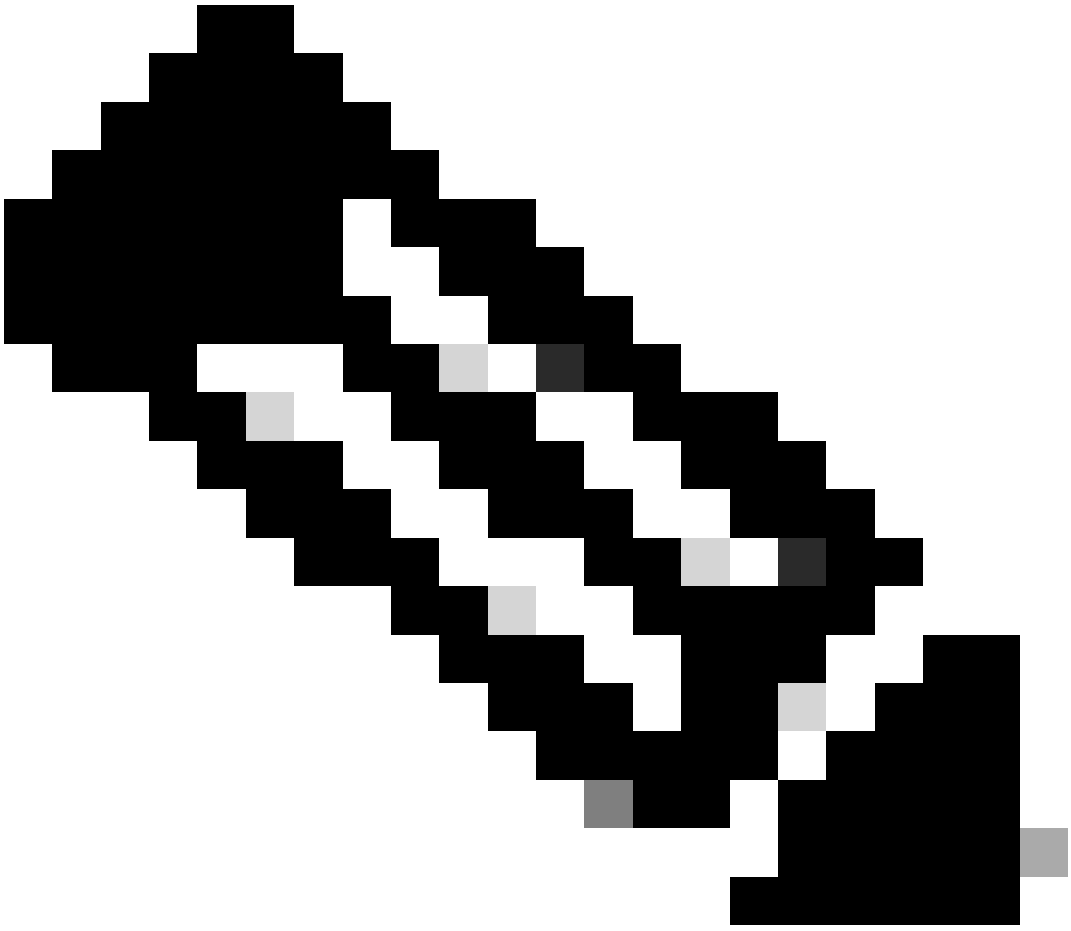
Once the registration script has completed no software is required to run on the Domain Controller itself. However, the OpenDNS Connector service must be installed on at least one computer (eg. Domain Controller or Member Server).

Stage 1 - Tests

The script initially gathers this information:

- Checks **OS version** and forest functional level
- Checks if the script is being **run as Administrator**.
- Gets the servers **IP Address, Hostname, and Domain name** information
- Check if Windows Firewall is enabled, and if the built-in **'Remote Administration'** rule is permitted

- Checks for the required domain user account **'OpenDNS_Connector'**



Note: If the OpenDNS_Connector user does not exist, the script prints the results and abort. This domain user must be created manually before running the script. If the OpenDNS_Connector account exists, the script proceeds to these checks.

- Checks if the OpenDNS_Connector user has permissions for 'Remote Enable' and 'Read Security' in the root\cimv2 **WMI** namespace.
- Checks if the OpenDNS_Connector account has the Active Directory **'Replicating Directory Changes'** permission, which is normally granted by membership of the Enterprise Read-Only Domain Controllers group.
- Checks if the OpenDNS_Connector account is a member of the **'Event Log Readers'** group
- Checks if the OpenDNS_Connector account is a member of the **'Distributed COM Users'** group
- Checks the resultant set of policy (RSOP) to see if **'Audit Logon Events'** is enabled via group policy
- Checks the resultant set of policy (RSOP) to see if the OpenDNS_Connector account has the **'Manage audit and security log'** right assigned

Stage 1b - Test Results

The results printed by the configuration script differs depending on OS version.

On server **2003** and newer you see these results:

```
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
```

On Server **2008** and newer (only when the forest functional level is 2008+) this information is also displayed. (This group does not exist in earlier versions):

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

Stage 2 - Auto-Configuration Changes

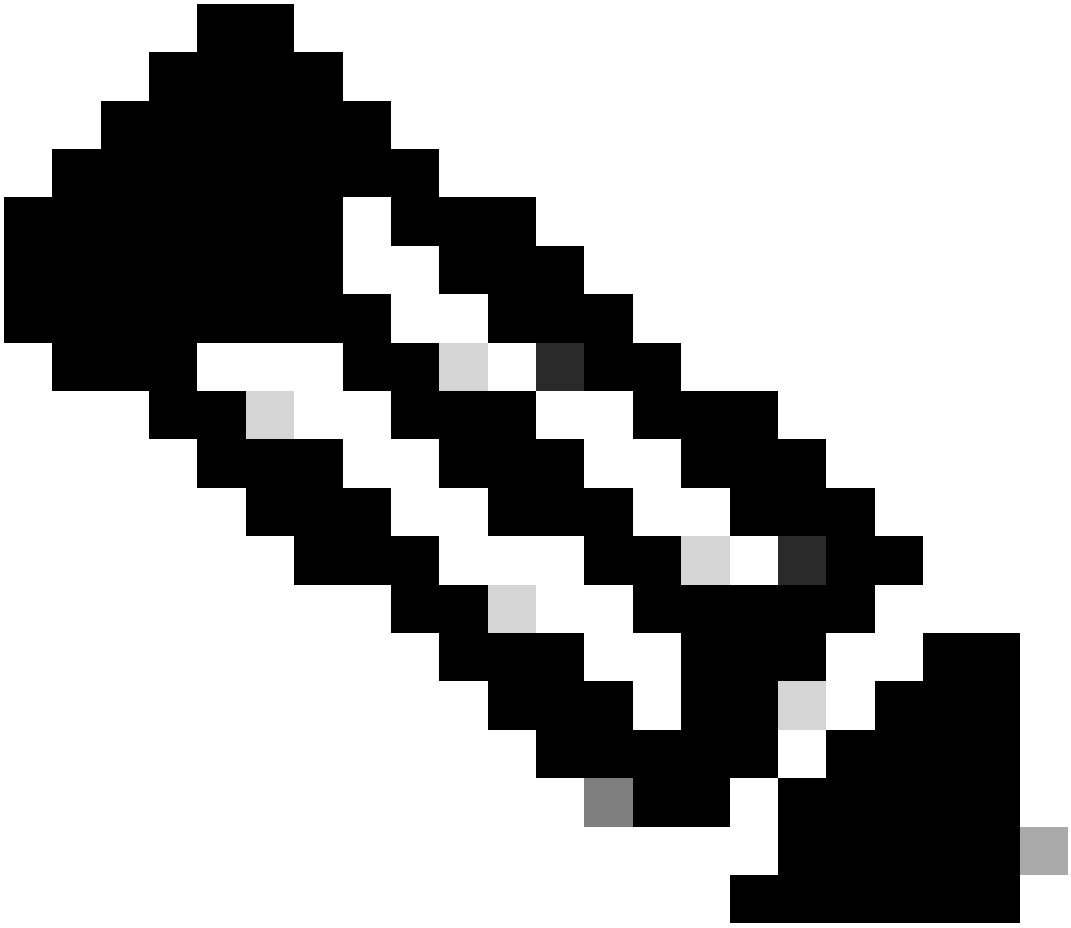
If this checks fail, you are prompted `"Do you want us to auto configure this Domain Controller (y or n)?"` before making any changes.

These **changes** are made:

- Enables the built-in **'Remote Administration'** Windows Firewall rule, if necessary
- Explicitly grants the 'OpenDNS_Connector' account 'Remote Enable' and 'Read Security' permissions in the root\cimv2 **WMI** namespace.
- Explicitly grants the 'OpenDNS_Connector' account **'Replicating Directory Changes'** permissions
- Adds the 'OpenDNS_Connector' account to the **'Distributed COM users**' group

On **2008+** this change is also performed:

- Adds the 'OpenDNS_Connector' account to the '**Event Log Readers**' group



Note: If Auto-Configuration is declined, or these changes fail, the script does not proceed to registration.

Stage 2b - Auto-Configuration Warnings

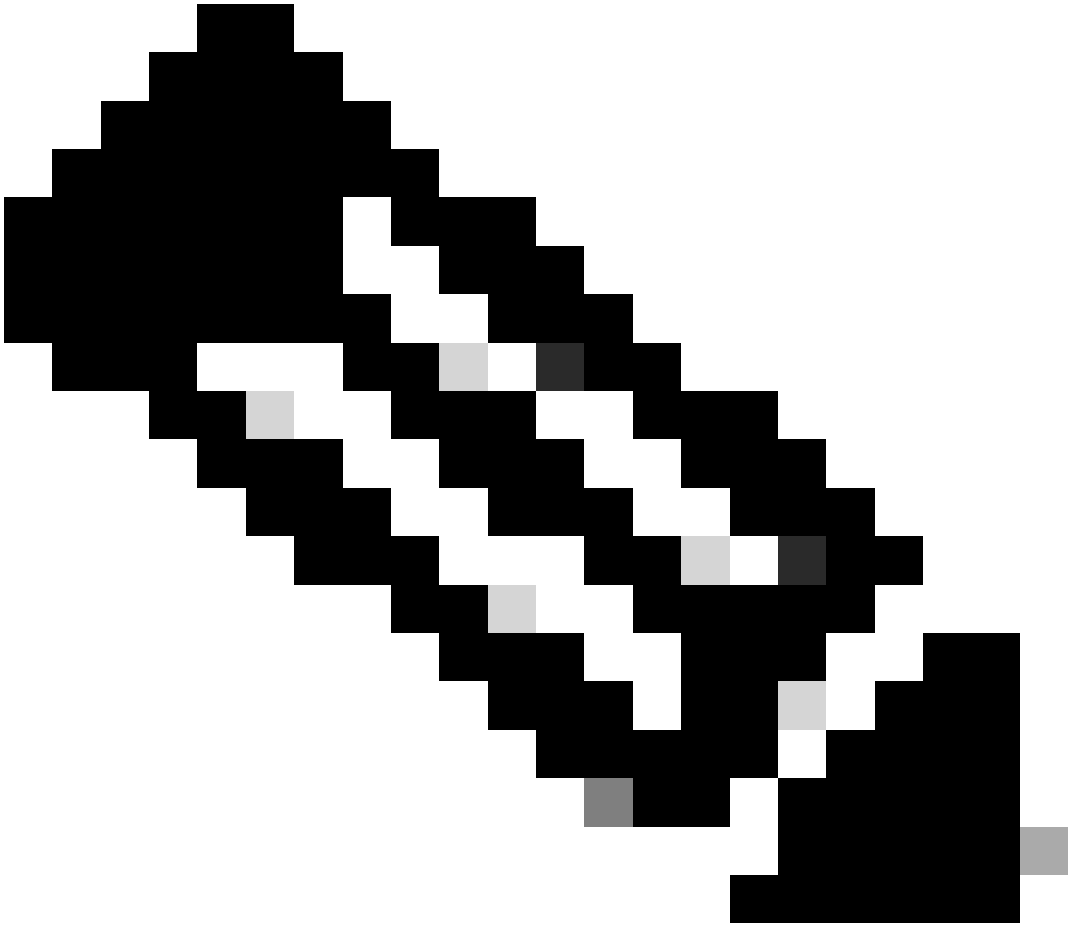
The script produces warnings if Group Policy settings are not correctly configured. The script is unable to correct these issues.

All Operation Systems:

- The script WARNS if the **'Audit Logon Events'** setting is not correctly configured in Group Policy, but does not modify Group Policy.

On **2003** (And 2003 functional-level):

- The script WARNS if the **'Manage auditing and security log'** right is not correctly configured in Group Policy, but does not modify Group Policy.



Note: Please manually correct these issue and re-run the configuration script. The script does not proceed to registration until these are corrected.

Stage 3 - Registration

The script prompts before registering the Domain Controller with Umbrella "`Would you like to register this Domain Controller (y or n)?`".This information is sent to Umbrella:

- Domain Controller Hostname / Label
- Domain Name
- IP Address
- Your unique organization ID and token (contained within your script) to uniquely identify the DC with your Umbrella Organization.

The registration happens securely via **https://api.opendns.com**