Configure Umbrella for AD Connectors on Windows Servers

Contents

Introduction

This document describes how to configure the Active Directory (AD) integration for Cisco Umbrella for DCs running Server Core.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on Cisco Umbrella.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Overview

Note: Umbrella does not support installing the Active Directory connector on non-GUI-based Windows servers like Windows Server Core.

This article applies to setting up Active Directory integration for Cisco Umbrella for DCs running Server Core. For all other OS versions, refer to the full setup guide or permissions troubleshooting guide.

Enable Features for Server Core Machine with Umbrella AD

To use a Server Core machine with Umbrella Active Directory, ensure that these features are enabled:

- ServerManager-PSH-Cmdlets
- BestPractices-PSH-Cmdlets

To enable these features, run this command to enable them. Note that this requires a reboot.

```
dism.exe /online /enable-feature /featurename:ServerManager-PSH-Cmdlets /FeatureName:BestPractices-PSH-C
```

Once enabled, after a reboot, run this command:

```
Set-ExecutionPolicy -ExecutionPolicy RemoteSigned
```

```
Configure-SMRemoting.ps1 -enable
```

After setting these, restart the Connector service and validate if the device appears as green within the dashboard within 5 minutes.

DCOM

In order to set DCOM permissions on Server Core, a copy of dcomperm.exe is required. To compile this from the Windows SDK, download Windows SDK and compile dcomperm from this folder location:

```
C:\Program Files\Microsoft SDKs\Windows\v7.1\Samples\com\fundamentals\dcom\dcomperm
```

To set Remote Launch and Remote Activation, run this command:

```
DComPerm.exe -ml set <Domain>\OpenDNS_Connector permit level:rl,ra
```

You can verify this by running DComPerm.exe -ml list:

```
C:\>DComPermEx.exe -ml list
```

An example validation:

```
Machine launch permission list:

Remote and Local launch permitted to BUILTIN\Administrators.
Remote and Local activation permitted to BUILTIN\Administrators.
Local launch permitted to \Everyone.
Local activation permitted to \Everyone.
Remote and Local launch permitted to BUILTIN\Distributed COM Users.
Remote and Local activation permitted to BUILTIN\Distributed COM Users.
Remote and Local launch permitted to BUILTIN\Performance Log Users.
Remote and Local activation permitted to BUILTIN\Performance Log Users.
Local launch permitted to APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES.
Local activation permitted to APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES.
Local launch permitted to APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES.
Local activation permitted to APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES.
Remote launch permitted to MYDOMAIN\OpenDNS_Connector.
Remote activation permitted to MYDOMAIN\OpenDNS_Connector.
```