CISDSC v0.0.1

Brown University Computing & Information Services, Windows Team
Authored by Yujun Qin, *Systems Administration Intern*

May 5, 2017

Contents

Chapter 1

Project Overview

1.1 Introduction

CISDSC is an internal tool for the Windows Team at Brown University Computing & Information Services. It serves to set up an HTTP DSC pull server, and to monitor server compliance states. To utilize its maximal functionality, only three lines of code are required.
Many thanks to Mike R, Mike D, Tony, Adam, Geoff and Robert for the help.

1.2 Usage

Unless you want to customize your installation, or make changes to the template, this part should be sufficient to guide you through the installation process. Suppose the DSC pull server is to be installed on DWINSERVERNAME.ad.brown.edu. Also, suppose DWINS1.ad.brown.edu and DWINS2.ad.brown.edu are the servers we want to make compliant.
First check the prerequisites.

(i) Make sure you have WMF 5 on both the server and the clients. To check WMF version, run
`$PSVersionTable.PSVersion | % Major;`

(ii) Make sure you are in the administrators group for each machine.

(iii) Make sure you can access `\\files`.

Now install the pull server. **You should run each script as administrator.**

1. Put CisDsc.ps1 in a local drive. You can find it at
`\\files\dfs\CISWindows\Software\DSCBackup\Scripts\DSC`.
In this example, we put it under C drive.

2. Open PowerShell as administrator and run
   `. C:\CisDsc.ps1`;
   `Install-CisDscPullServer -ComputerName DWINSERVERNAME`;
   By default it is installed at C:\DSC.

3. Check that the pull server is up and running by visiting `http://DWINSERVERNAME.ad.brown.edu:8080/psdscpullserver.svc`.

4. To check if DWINS1 and DWINS2 are compliant, run
   `Check-CisDscCompliance -ComputerName DWINS1, DWINS2`;
   The first time your run this command, it should prompt you to build the localhost.mof file first. Give it a valid credential and proceed.

5. To see reports of compliance state, go to `C:\DSC\Reports`. There should be an overall report as well as detailed reports for each server.

6. To force DWINS1 to be compliant, run
   `Install-PsDscConfiguration -ComputerName DWINS1`
   `-PullServerName -DWINSERVERNAME`;

Turn on `-Verbose` flag for debugging purposes.

1.3 Support

Tony is in charge of the standard build doc, which the template is based on. You can find it at the SharePoint site. For more information, email Tony: anthony_jaworsky [at] brown.edu.
For help with installing and updating DSC pull server, email Yujun: yujun_qin [at] brown.edu.

Chapter 2

Script Files

2.1 CisDsc.ps1

This file is essentially a wrapper for all the functions in the other files. As long as you have this file, you should be able to fetch the other files and set up DSC.

2.1.1 Install-CisDscPullServer

Paramters:

- `ComputerName`: Mandatory, name of the computer you want to install server on;
- `PullPort`: Port for pull server, 8080 be default;
- `CompliancePort`: Port for compliance server, 8081 by default;
- `InstallDest`: Installation location, `C:\` by default.

This command copies DSC modules from `\\files` and installs DSC pull server.

2.1.2 Install-CisDscConfiguration

Parameters:

- `ComputerName[]`: Mandatory, names of the servers you want to make compliant;
- `PullServerName`: Mandatory, name of the pull server;
- `Port`: Pull server port, 8080 by default;
- `InputDSC`: The directory that contains Template.ps1, `C:\DSC` by default;
- `Force`: Flag to force DSC configuration.

This command enforces template configuration on clients. **It should be run on the pull server specified by `PullServerName`.**

2.1.3 Check-CisDscCompliance

Parameters:

- `ComputerName[]`: Mandatory, names of the servers you want to check compliance state on;
- `UseDefault`: Whether default setting (i.e. installation location) is applied on pull server, true by default;
- `MofFile`: The "golden image" MOF file, default not specified;
- `OutputPath`: Path for outputting compliance reports, `C:\DSC\Reports` by default.

This command checks the compliance state on clients, based on the MOF it is given. By defualt it uses the Server 2016 template MOF. It generates an overview report and machine-specific detailed reports.

2.2 Template.ps1

This is the Server 2016 template based on the standard build doc. It comprises the following modules.

2.2.1 [File]AdminFiles

`C:\AdminFiles` should be present.

2.2.2 [Script]BrownNetwork

There should be a network interface called BrownNetwork. Use Network and Sharing Center to check this.

2.2.3 [Script]DNSServer

DNS server addresses should be set to 10.4.21.{2, 3, 4, 5}, and 10.1.1.10. Use Network and Sharing Center to check this.

2.2.4 [Registry]DNSSuffix

DNS suffixes should be in this order: ad.brown.edu, brown.edu, qad.brown.edu, services.brown.edu. Use Network and Sharing Center to check this.

2.2.5 [Script]WINSServer

WINS address should be 10.4.21.5. Use Network and Sharing Center to check this.

2.2.6 [Script]LMHOSTS

LMHOSTS should be turned off. Use Network and Sharing Center to check this.

2.2.7 [Registry]IPv6

IPv6 should be disabled.

2.2.8 [Service]PrintSpooler

Print Spooler should be forbidden from starting up. Use Computer Management - Services to check this.

2.2.9 [Registry]AdminESC

IE Enhanced Security should be disabled for administrators. Use Server Manager - Local Server to check this.

2.2.10 [Registry]UserESC

IE Enhanced Security should be enabled for users. Use Server Manager - Local Server to check this.

2.2.11 [xUAC]UAC

It depends on DSC resource xSystemSecurity. User Account Control should be set to Never Notify. Use Control Panel - User Accounts -Change User Account Control Settings to check this.

2.2.12 [Script]DEP

Data Execution Prevention should be set to "Turn on DEP for essential Windows programs and services only". Use Control Panel - System and Security - System - Advanced System Settings - Advanced - Performance - Data Execution Prevention to check this.

2.2.13 [Registry]AdjustForBestPerformance

Visual Effects should be set to "Adjust for Best Performance". Use Control Panel - System and Security - System - Advanced System Settings - Advanced - Performance - Visual Effects to check this.

2.2.14 [xRemoteDesktopAdmin]RemoteDesktop

It depends on DSC resource xRemoteDektopAdmin. Remote access should be enabled.. Use Control Panel - System and Security - Allow Remote Access to check this.

2.2.15 [Registry]ServerManager

Registry key should be set to disable Server Manager at logon.

2.2.16 [Script]ServerManagerTask

Server Manager should be disabled from auto startup. Use Task Scheduler - Microsoft - Windows - Server Manager to check this.

2.2.17 [File]BGInfo

2.2.18 [Registry]BGInfoKey

2.2.19 [WindowsFeature]SMB1

2.2.20 [Registry]KB3125869_Key1

2.2.21 [Registry]KB3125869_Key2

2.2.22 [Script]NetshReceiveSideScaling

2.2.23 [Script]DeviceManagerReceiveSideScaling

2.3 PullServerConfiguration.ps1

This is the configuration file for pull server installation. You normally need not change its content. However, if you want to enforce HTTPS, you should modify a few properties.
Under `[xDSCWebService]PSDSCPullServer`, set

- `CertificateThumbPrint = Certificate thumbprint for IIS Server`
- `UseSecurityBestPractices = $true`.

Under `[xDSCWebService]PSDSCComplianceServer`, do the same thing with

- `CertificateThumbPrint = Certificate thumbprint for IIS Server`
- `UseSecurityBestPractices = $true`.

After modification, re-install the pull server.

2.4 LCM_HttpPull.ps1

This is the configuration file for DSC Local Configuration Manager. If a client wants to pull DSC Mof files, it has to know where to find them. This file serves that purpose.
To enforce HTTPS, under `[ConfigurationRepositoryWeb]DSCHTTP`, set

- `ServerURL = "https://$PullServerName.ad.brown.edu:$Port/PSDSCPullServer.svc"`
- `CertificateID = Certificate thumbprint for IIS Server`
- `AllowUnsecureConnection = $false`.

And then use `Install-CisDscConfiguration` to re-install settings for the clients.

Chapter 3

Issues & TODOs

3.1 Issues

(i) During installation, CisDsc.ps1 copies backup DSC modules from \\files, rather than using the standard installation method. This is because the command `Install-Module` does not work in CIS network. The error is "Unable to download from URI 'https://go.microsoft.com/fwlink/?LinkID=627338&clcid=0x4'". The Network Team was not able to identify the problem. It is very likely that GPO blocks the connection.

(ii) Credential encryption is not implemented. To justify the use of domain user account, note that DSC Local Configuration Manager by default runs as SYSTEM. It does not have access to SMB share files unless we provide it with domain credentials. This is necessary for `[File]BGInfo`.
Were this project to be continued, this should be top priority.
For instructions, visit https://blogs.msdn.microsoft.com/powershell/2014/01/31/want-to-secure-credentials-in-windows-powershell-desired-state-configuration/.

(iii) HTTPS is not implemented. This can be easily configured once you have a certificate, but it could complicate the logic in `Install-CisDscPullServer`. The best practice would be to configure manually, after the pull server is installed.

3.2 TODOs

(i) Once credential encryption issue is resolved, uncomment the following lines in `[File]BGInfo`.

```
#SourcePath = "\\files\dfs\CISWindows\Software\DSCBackup\BGInfo32-64"
#MatchSource = $true
#Recurse = $true
```

```
#Credential = $Credential
```

(ii) Change current implementation of WMF 5 check. Rather than attempting to install it remotely, which always fails, maybe notify a systems administrator.

(iii) Find out why `[Script]DEP` in the template does not work on Server 2012 machines.

(iv) Add IISCrypto settings in template.