Platform Wintel SOE

DIRECTORY SERVICES UNATTENDED CONFIGURATION

ABSTRACT

This document details the information on execution & results of the Directory Services unattended configuration (Windows PowerShell script). The custom solution and this document is specifically custom made and meant for MyWorkStyle Service Mesh Agility team.

DOCUMENT DETAILS

Author:	Tarun Rajvanshi / Umesh C Thakur
Date:	27 Feb, 2015
Document Reference:	PWS-1-1232
Previous Document Reference:	None
Document Type:	Operations Guide
Document keywords:	Directory Services, DSSOE, Command Line, Windows Server 2012 R2
File Reference:	PWS-1-1232-DSUnattendedConfig-v0.2.docx
Issue:	v0.2
Review Period:	As Required
Template Version:	PWS-Template-v3.0.dotx
Authorizer:	Patrick Tse

Microsoft, Active Directory, Microsoft Management Console, Windows Installer, Windows, Windows XP, Windows Vista, Windows 7, Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012 and Windows Server 2012 R2 are registered trademarks of Microsoft Corporation. Citrix XenDesktop, XenApp, XenServer are registered Citrix Systems, Inc. Other products and company names may be the trademarks of their respective owners.

The latest approved version of this document resides in the
CSC Platform Wintel SOE Wiki

TABLE OF CONTENTS

TABLE OF FIGURES

AMENDMENT HISTORY

Issue	Date	Author	Notes
v0.1	27-Feb-2015	Tarun Rajvanshi & Umesh C Thakur	Written, Reviewed and send to Patrick for final review
v0.2	27-Feb-2015	Tarun Rajvanshi & Umesh C Thakur	Updated document with Patrick's suggestions. Converted to PDF for distribution.

APPROVAL SCHEDULE

Name	Organization	Function
Patrick Tse	GIS Platform Development Studio – x86 SOE Core Engineering	Manager

CONTRIBUTORS

Name	Position
Umesh C Thakur	Professional 2 : System Engineer

REFERENCES

[1]   Directory Services SOE Operations Guide   CSC WPS Wiki
[2]   Domain Controller Antivirus Exclusion List   CSC WPS Wiki

TYPESTYLE CONVENTIONS

The following typestyle conventions are used within this document:

- **Black bold text** is used to designate:
    - client tools
    - Dialog titles and Dialog sections
    - names of buttons, options, check boxes, menus, fields
    - file and folder paths
    - Active Directory paths
    - A reference to a table heading
- **Dark red bold text** is used to designate implementation specific information. When dark red bold text is used it must not be entered or followed literally, but must be replaced or reference made to the implementation specific information.
- `Monospace text` designates text as it must be entered by the implementer
- "Text enclosed with double-quotes" is used to designate informational text as it is worded on a dialog box, message box or table body
- *Italic text* is used as emphasis

- "*Italic text enclosed with double-quotes*" is used to designate text as it is worded in a referenced document
- <Angled brackets> are used to define parameters. Parameters must not be entered literally but must be replaced with the required information. A parameter will be defined in the Section it is used
- ALL CAPITALS is used to designate keyboard keys. When a key combination, or key and mouse combination is required this is designated by the plus sign (+), which is included between the key, and key and mouse combination; e.g. CTRL+ALT+DELETE, CTRL+CLICK
- An arrow (→) is used to indicate navigation of sequential menus or hierarchical trees.

HIGHLIGHTING STATEMENTS

Note

Supporting information to the preceding paragraph(s).

? Section Applicability

Immediately succeeds a Section Heading and provides information on the Section's applicability depending upon the requirements. In addition, "(Applicability)", without the quotes, is included in the Section Heading Text to highlight in the Table of Contents that the Section is optional and therefore, its applicability needs to be determined.

ⓘ Important

Supporting information that is important to the preceding paragraph(s).

✔ Recommended Practice

Includes a summary of the recommended practice and setting(s) where applicable, based upon Vendor and CSC guidelines.

1 INTRODUCTION

Once a domain controller is built in a new or an existing Active Directory environment, it is very important to perform the post domain controller promotion tasks and configure the Active Directory to a CSC standardized DS-SOE configuration. At the time of writing, current versions of the DS-SOE do not have a full unattended installation feature. This custom interim PowerShell script solution was built to facilitate the unattended execution of the post-promotion tasks and can be utilized in environments that require complete unattended installations such as cloud orchestration software. The streamlined automated configuration sets the configuration to the required CSC DS-SOE standards.

> (i) **Important**
>
> This custom unattended solution is specifically made for the PDS MyWorkStyle (MWS) Team and it satisfies certain requirements specific to the MWS program requesting this interim capability. It is Best Effort Support and should not be used by any other team or in production without the consent of Platform Wintel SOE team and respective Cybersecurity ASMs, and if used otherwise its execution can lead to problems in the AD environment.

1.1 DOCUMENT PURPOSE

The purpose of this document is to communicate the details of the custom solution, information on Powershell script & its components, step by step implementation and standard results. For any clarification feel free to e-mail us at Platform Wintel SOE.

1.2 SCOPE

This document is made to detail the solution i.e. custom Powershell script and its components, specifically built for the PDS MyWorkStyle team and thus its scope is limited to that specific program only.

The following is under the scope of this document:

- What comprises the custom solution package?
- How a user can provide the input values?
- How to execute the package?
- What is the result of the execution?
- Any item not specifically listed in the table of contents is deemed out of scope of the document.

1.3 ASSUMPTIONS & PRE-REQUISITES

- The domain controller is already built before using the unattended solution i.e. the solution is only to be used on an already built domain controller as it only does the post DC promotion tasks. The custom script does not promote a domain controller and hence the domain controller should be manually created first.
- Implementer must make sure that the domain controller is built properly and does not have any issues.
- The implementer should have adequate knowledge of Active Directory and its terminologies.
- The Implementer has appropriate rights / credentials for the execution of the custom script.
- Read the instructions in the document very carefully as a spelling mistake or human error can lead to failure of the execution.
- Where any changes to a production environment are planned, correct CSC GIS operational procedures will be followed. Typically, this would include change control, verified backups prior to implementing changes, implementing a change in a test environment and ramped deployment if possible.
- The domain controller is running on Windows Server 2012 R2 operating system.

The latest approved version of this document resides in the
CSC Platform Wintel SOE Wiki
CSC Proprietary

2   CUSTOM SOLUTION PACKAGE

2.1   WHAT THE SOLUTION PACKAGE COMPRISES OF?

The solution package comprises of the following files and folders:
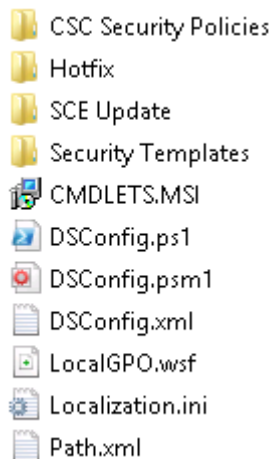
Figure 1 – Custom Solution Folder

Implementer should make sure that above mentioned files and folders must exist in the solution package folder. All of the above shown files are a must for the script to run and complete the post DC promotion tasks. Implementer must make sure that none of the above files are renamed.

2.2   DOWNLOAD LOCATION & CREDENTIALS

The download location and credentials for the custom script package folder is provided below. We recommend that you use a robust FTP client with retry capability.

Utilize our Self Service Portal (accessible from the CSC 20 net) to obtain the credentials.
http://pws.can-kan.csc.com/

Alternatively, send an email to Platform Wintel SOE for the credentials.

Select "Log In" to create an account. Within the "Self Service Portal" you will be able to request the most current FTP password and product updates.

Important:
Please refer to following document on how to configure FTP client properly to access the FTP server mentioned above.
https://c3.csc.com/docs/DOC-736198

If you still have any FTP download related issues, please contact SOE Support.

3 CUSTOM SCRIPT CONFIGURATION FILE

The custom script solution package includes a configuration XML file called the DSConfig.xml. Implementer has to modify the configuration file as per their requirements before running the actual script. The script reads the configuration file and based on the added parameter values the script performs the post promotion configurations accordingly.

> **Note**
>
> It is highly recommended that the implementer must go through the configuration file and provide parameter values as per their requirements. If parameters are not correctly specified, it may lead to unexpected misconfigurations; result in failures and unstable AD environment.

The configuration XML file is self-explanatory. Comments have been included in the XML file for each configurable parameter. Implementer must open the XML file in Notepad.exe, read the comments attentively and pass the parameters; once done the file must be saved and closed.

As an example, a screenshot of the XML file is given below.

```xml
1  <?xml version="1.0"?>
2  <DS>
3      <!-- Location where DS script will generate logs and other output. If this folder does not exist, DS script
4          will automatically crete it.  -->
5      <OutputFolder>C:\DSOutput</OutputFolder>
6
7
8      <!-- Indicate whether DS script should set pagefile settings as per DSSOE standards -->
9      <ConfigurePageFile>true</ConfigurePageFile>
10
11
12     <!-- If path and size is given, DS script will create a reserve file with given size. It can be later used
13         in case server is experiencing low disk space. In such case, this file can be deleted to claim some space.
14         Reserve file is created only when you specify a valid file path and size
15         example: <ReserveFile Path="C:\Reserved.RSV" SizeMB="1024" />
16     -->
17     <ReserveFile Path="" SizeMB="" />
18
19
20     <!-- If external time server name is given, it will be configured by DS script. Only one time server name
21         or IP address should be specified. If you do not specify any value (left blank), external time server
22         will not be configured. You must ensure that a valid time server name or IP is given.  -->
23     <ExternalTimeServer Name="" />
24
25
```

Figure 2 – Custom Script Configuration xml File

3.1 CAVEATS

In the XML file following two configurable parameters must be passed with caution as actual script configuration is dependent on them.

```
<ServerIsFirstDCInNewForest></ServerIsFirstDCInNewForest>
```

```
<ServerIsAdditionalDC></ServerIsAdditionalDC>
```

Consider the following points:

- Both the options are mandatory. Leaving them blank in the configuration file will lead to following error message and the script will exit without doing any configuration.
  `DS_REQUIRED_PARAMS_MISSING`
- Leaving either of them blank will lead to the same error message as mentioned above.
- The value of both the parameters cannot be logically "True"; this will lead to the same error message as defined above.
- If the server is a first DC in child domain or tree domain then the value for both the parameters should be set to "False".

The latest approved version of this document resides in the
CSC Platform Wintel SOE Wiki

4   SCRIPT EXECUTION

The actual script file is DSConfig.ps1. Implementer must run DSConfig.ps1 on the Window
PowerShell prompt to execute the commands within it.

Follow the below mentioned steps to execute the script; DSConfig.ps1:

1. Open the Windows PowerShell in elevated mode (**run as administrator**)
2. From within the PowerShell browse to the directory having the DSConfig.ps1 script file. For
   example if the DSConfig.ps1 is stored in C:\DSCMD folder. Then run the following command
   to execute the script
   PS C:\DSCMD\DSConfig.ps1

> **Note**
>
> If powershell script execution is restricted on the server then as an example run the
> following command to execute the script. Change the path accordingly.
> ```
> C:\DSCMD>
> C:\DSCMD>powershell.exe -executionPolicy bypass c:\DSCMD\DSConfig.ps1
> ```

3. Hit ENTER to execute the script
4. The script will run and perform all the post promotion tasks listed in section 2 and ultimately
   presents a message that the server will be rebooted in 15 seconds.
5. The server will be rebooted
6. Logon to the server and verify the post promotion configuration.

4.1 CAVEATS

- The script file DSConfig.ps1 should only be run when the configuration XML file has been
  appropriately modified / configured.
- The script file should only be executed on an already built domain controller. The script file
  does not build the domain controller; it only configures the post promotion options.
- If the PowerShell was not opened in elevated mode, running the DSConfig.ps1 script will
  result in following error and the script will exit without any modifications
  DS_NO_ADMIN_PRIVILEGES
- If the implementer changed name of the configuration XML file; running the DSConfig.ps1 will
  result in the following error and the script will exit without any modifications
  DS_NO_CONFIG_XML_FILE
- If the implementer changed name of the module file DSConfig.psm1; running the
  DSConfig.ps1 will result in the following error and the script will exit without any modifications
  DS_NO_MODULE_FILE
- If the script determines that the domain controller was not properly built, it will throw the
  following error and the script will exit without any modifications
  DS_NOT_PROPERLY_SETUP

4.2 SCRIPT LOG FILE

The script log file is saved at C:\DSOutput\ with "DSConfig- MMddyyyy-hhmmss.log "name and
format. A text message about every configuration done by the script goes into the log file.
Implementer must check the log file to see the progress of the script or to determine the reason for
non-execution of a particular task or tasks.

5 POST DC PROMOTION CONFIGURATIONS

The unattended execution of the custom script solutions configures the following DS-SOE post-promotion options:

1. Creates a new output folder at the user defined path (configurable within DSConfig.xml). The default path is C:\DSOutput. This folder will store the log files and other files the script will create. For the purpose of demonstration C:\DSOutput is used as the default output path throughout this document.
2. Creates the script log file in C:\DSOutput folder with "DSConfig- MMddyyyy-hhmmss.log "name and format.
3. Checks whether the server was properly built as a domain controller or not, if not, the script will exit. Script will add text in the script log file accordingly.
4. Checks if the server is an Additional DC or the First DC in the new forest and goes ahead accordingly. Text is added in the script log file.
5. Configures the page file as per CSC standards. Initial Size (MB) is 300 + Actual RAM size and Maximum Size (MB) is 1.5 times the Actual RAM size. Setting page file or not is given as a user configurable option in the custom script. For more information see reference [1].
6. Creates a reserve file. The reserve file is a simple file that captures space on the drive and it can be deleted if there is a scarcity of free space to quickly recover some space on the server. Reserve file path and its size are user configurable options in the custom script.
7. Configures external time sync server as per the CSC defined standards. This is a user configurable option. A user can input either name or IP of the external time sync server in the custom script. For more information see reference [1].
8. Creates the CSC standard or multitenant OU structure. OU structure creation is a user configurable option in the script. The OU creation will not execute if the server is an Additional Domain Controller. For more information see reference [1].
9. Creates and configure CSC standard security baseline group policies for domain and domain controller. GPO creation is a user configurable option in the script. GPO creation will not execute if the server is an Additional Domain Controller. For more information see reference [1].
10. Configures DNS scavenging. This is not a user configurable options i.e. the DNS scavenging will apply always. If the server is the first DC in the forest the scavenging on _msdcs zone will be configured else not. The server level and zone level configuring will be configured always. For more information see reference [1].
11. Configures system state backup and maintenance tasks in the task scheduler. This is a use configurable option in the script. System state backup will be configured to trigger every day at 10:00 pm and the backup maintenance task will delete the backup files keeping the latest 3 versions. For more information see reference [1].
12. Configures DNS forwarders as defined by the implementer. User must specify the DNS forwarder IP addresses in the script. For more information see reference [1].
13. Configures the directory services repair mode option, available at the boot time. This is not a user configurable option. For more information see reference [1].
14. Adds the DFS Management tools for the management of SYSVOL folder replication. This is not a user configurable option. For more information see reference [1].
15. Creates the DS server configuration text file in the C:\DSOutput folder. The file contains the inventory information of the DS server. This is not a user configurable option.
16. Installs the Directory Services specific hotfixes automatically. This is not a user configurable option. For more information see reference [1].
17. Generates best practices analyzer reports and save them in the C:\DSOutput folder. This is not a user configurable option. For more information see reference [1].

The latest approved version of this document resides in the
CSC Platform Wintel SOE Wiki
CSC Proprietary

6 ADDITIONAL CONSIDERATIONS

The following DSSOE post-promotion options are not added in this custom solution. Implementer must make sure to configure these options manually if required, after the completion of script execution.

1. McAfee Antivirus Exclusions for the domain controller: See reference [2] for the complete list of exclusions which must be added in the McAfee antivirus for a Windows Server 2012 R2 domain controllers.
2. Start up and recovery settings: See reference [1] for details on it.
3. Clear all events in the event logs except setup log: For this custom solution this is not required. However if required implementer can perform this. See reference [1] for details on it.
4. First DC in forest subnet association with site: See reference [1] for details on it.
5. DC new subnet association with site: See reference [1] for details on it.
6. Create users in bulk: See reference [1] for details on it.

7 DOCUMENT ADMINISTRATION

7.1 FEEDBACK

The information contained in this document is not region specific. Any customizations or variants of this publication that occur at the regional/account level are not under the management of this team.

General or technical feedback/updates/errors/suggestions regarding this publication can be submitted by emailing the responsible team listed in Table 1. This feedback will then be assessed, in terms of criticality, for addition to either the current version of the document or as part of the next review cycle.

PWS Mailing List	Core Technology Areas of Responsibilities
Platform Wintel SOE	CSC Global Active Directory Standards, CSC Global Presentation Virtualization Server Standards, strategic initiatives, best practices, recommendations and process.
WPS Enterprise Toolsets	CSC Global Windows Distributed Cluster Server Standards, Server Disk Defragmentation standards, WAFS and WAN Optimization standards. Recommendations, best practices and miscellaneous server environment enterprise utilities.

Table 1 - Mailing List Table

7.1.1 Naming Conventions of Documents

Global Directory Engineering has changed the document naming convention to be applied to its documents. Thus, documents created with a prefix of GDE or WPS will be renamed with a PWS (Platform Wintel SOE) prefix as they get reviewed or new ones are created. To ensure that access to previously published documents is still possible, whenever a previous document with GDE-x-icy or WPS-x-icy document has been updated, the previous document reference will also be listed in the Document Details section of the new or updated document. All updates and new documents published by Platform Wintel SOE will use the new naming convention of PWS-x-icy.

7.2 KNOWN ISSUES

7.2.1 IP Address & Server Names

The script code does not validate the correctness of the user specified IP addresses and Server names. Thus, implementer must be extra cautious when specifying IP or server names in the configuration XML file and make sure they enter the valid values.

7.2.2 Page File Error

When following parameter in DSConfig.xml is set to true and c:\pagefile.sys file already exists: <ConfigurePageFile>true</ConfigurePageFile> below mentioned error is written to output device. This error is displayed because script tries to reconfigure it as per DSSOE standards. You can safely ignore this error message.

```
ERROR:
Description = Object or property already exists
```

7.2.3 PDF Attachments

Where a file has been attached to a PDF document, Adobe Acrobat 7.x and above products have a security feature which prevents the saving or opening of attachments with certain file extensions, e.g. ZIP, exe. If this security feature is preventing the reader from saving any attached files included in our documents, visit the following Adobe website support article:
http://forums.adobe.com/message/2378110

> **Note**
>
> When the Adobe Acrobat 7.x and above product is updated with a critical update, the above mentioned security feature is reset to the default installation setting. The actions taken to grant certain file extensions the ability to be saved must be performed again.

7.3 ATTACHMENTS

Where a file has been attached in this document with a ZIP extension, it will contain other file formats. These formats may require specific Microsoft viewers in order to display the contents of the file properly. These viewers are freely distributed by Microsoft and can be found at http://office.microsoft.com/en-us/downloads/HA010449811033.aspx.

APPENDIX A   ABBREVIATIONS AND ACRONYMS

Abbreviation/Acronym	Definition
AD	Active Directory
AD DS	Active Directory Domain Services
ACL	Access Control List
BDC	Backup Domain Controller
DC or DC(s) or DCs	Domain Controller or Domain Controllers
DNS	Domain Name System
e.g.	Exempli Gratia (Latin: for example)
EMEA	Europe, Middle East and Africa
FQDN	Fully Qualified Domain Name
Gab	Gigabyte
GCARS	Global Change Activity Request System
GDE	Global Directory Engineering
GIS	Global Infrastructure Services
GOS	Global Outsourcing Services
GUI	Graphical User Interface
i.e.	Id Est. (Latin: that is)
IP	Internet Protocol
LAN	Local Area Network
Mb	Megabyte
MS	Microsoft
MSDE	Microsoft SQL Server Desktop Engine
NIC	Network Interface Card
NT	New Technology (Microsoft abbreviation)
OS	Operating System
PDC	Primary Domain Controller
PDS	Platform Development Studio
PWS	Platform Wintel SOE
SBC	Server Based Computing
SID	Security Identifier
SOE	Standard Operating Environment
SP	Service Pack
SQL	Structured Query Language
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VPN	Virtual Private Network

The latest approved version of this document resides in the
CSC Platform Wintel SOE Wiki
CSC Proprietary

Abbreviation/Acronym	Definition
WAAS	Wide Area Application Services
WAN	Wide Area Network
WAFS	Wide Area File Services
WPS	Windows Platform Solutions
XP	experience (Microsoft abbreviation)

The latest approved version of this document resides in the
CSC Platform Wintel SOE Wiki
CSC Proprietary