Мне понадобилось хранить информацию о том, какой пользователь и когда логинился или завершал работу на конкретном компьютере в домене. Вариантов решения этой задачи с помощью GPO много: как с помощью стандартного аудита, так и с помощью различных скриптов. Мне необходимо было сохранять полученные данные о логинах в текстовый файл в удобочитаемом виде.

Содержание:

Введение

Готового решения, которое бы меня полностью удовлетворило я не нашел. Есть много вариантов скриптов, которые делают что-то похожее, но мне они показались не очень удобными. Можно воспользоваться стандартным аудитом windows и собирать данные журналов с компьютеров, но у меня нет хранилища для этих журналов, да и разбирать события не очень удобно и наглядно.

Я решил пойти по самому простому и очевидному пути. Сделать сетевую папку с разрешением на запись пользователям, создать 2 скрипта для событий logon и logoff. С помощью групповой политики запускать эти скрипты. Они во время работы записывают в текстовый файл следующие данные:

1. Тип события: **logon** или **logoff**.
2. Имя компьютера.
3. Имя пользователя.
4. Время события

Для каждого компьютера создается отдельная папка с именем компьютера в названии. В этой папке каждый день создается новый файл с датой в названии. С такой структурой можно очень легко и быстро посмотреть в какой день, в какое время и кто заходил на компьютер. Скрипт написан на VBS.

VBS скрипт для аудита входов/выходов в компьютер

Сразу предупреждаю, что писать vbs скрипты я не умею, и практически не знаком с этим языком. Я собирал из разных кусочков то, что мне нужно, читая документацию и правя на ходу чужие куски кода. Может я предвзято отношусь к vbs, но когда я вижу его код, сразу хочу закрыть редактор. Мне он кажется каким-то нелепым и трудночитаемым. Было бы здорово, если кто-нибудь подсказал бы как сделать мой скрипт более правильным и логичным.

Как я уже писал выше, скрипт во время запуска создает в сетевом каталоге папку с именем компьютера, в ней создает текстовый файл с текущей датой в имени. В сам файл записывает информацию о том, кто залогинился или вышел из компьютера. Каждый новый запуск скрипта в один и тот же день дописывает информацию в существующий файл. На следующий день создается новый файл с другой датой в имени.

```
Const MY_COMPUTER = &H11&
Set objNetwork = CreateObject("Wscript.Network")
objComputerName = objNetwork.ComputerName
objUserName = objNetwork.UserName
Set objShell = CreateObject("Shell.Application")
Set objFolder = objShell.Namespace(MY_COMPUTER)
Set objFolderItem = objFolder.Self
MyStroka = "User: " & (objUserName) & vbNewLine & "Компьютер: " & (objComputerName) & vbNewLine & "Время: "'

On Error Resume Next
Const ForWriting = 2
Const ForReading = 1
Const ForAppending = 8
Const TristateFalse = 0
Set fso = CreateObject("Scripting.FileSystemObject")
```

```
Set GObjArgs = WScript.Arguments
GStrCmd = GObjArgs(0)
Call crypt(GStrCmd)

Sub crypt(msg)
n = Len(msg)
c = 0
Do Until c = n
c = c + 1
t1 = Mid(msg,c,1)
ch = Chr(asc(t1)+n)
output = output & ch
Loop

MyComp = objComputerName
MyPath = "\\192.168.0.100\logon-info\"
MyDate = Date
MyTime = Time
MyDir = MyPath & MyComp
If Not FSO.FolderExists(MyDir) Then
  FSO.CreateFolder(MyDir)
End If

Mytxt = ".txt"
My1 = "\"
Myfile = MyDir & My1 & MyDate & Mytxt

Set GObjLocalF = fso.OpenTextFile(Myfile,ForAppending,True)
GObjLocalF.WriteLine "###########LOGON#################"
GObjLocalF.WriteLine MyStroka & Time
GObjLocalF.WriteLine "################################"
GObjLocalF.Close
```

```
End Sub
```

Во втором файле выделенная строка должна быть LOGOFF. Первый файл ставим на событие входа в систему, второй — на выход. В одном текстовом файле мы увидим, когда человек зашел на компьютер, а когда вышел.

Добавление скрипта в групповую политику

Теперь нам нужно распространить выполнение скриптов на компьютеры. Я воспользовался стандартным функционалом GPO. Не буду приводить картинки, как это сделать, в интернете есть масса статей с различными версиями windows. Расскажу словами, как это делаю я.

Для начала я создаю отдельную политику. Я всегда для разных настроек создают отдельные политики. Мне так удобнее управлять ими. Можно оперативно отключить что-то или добавить настройку отдельной группе пользователей. Если добавлять все в одну политику, гибкости в управлении не будет.

Таким образом, создаем отдельную политику. Отключаем в ней конфигурацию компьютера, она не нужна. Скрипты будут добавляться в настройки пользователя. Переименовываем скрипты, к примеру, в logon.vbs и logoff.vbs. Назначаем каждому событию свой скрипт. После этого линкуете в нужное место политику и проверяете.

Проверка работы vbs скрипта

В результате работы скрипта у вас должны быть созданы папки с именами компьютеров. Примерно вот так:

В каждой папке будут накапливаться текстовые файлы с информацией о логинах пользователей конкретного компьютера:

В файлах будет примерно такая информация:

Дальше используете эти файлы на ваше усмотрение.

Во время отладки можно указать локальный путь к файлу и запускать его вручную тут же на компьютере. Все должно корректно отрабатывать. После отладки можно поместить в GPO.

Если у вас нет домена и групповых политик, вы можете вручную или каким-то другим способом добавить указанный файл в автозапуск и регистрировать все входы на компьютер в текстовый файл локально или на сетевую шару.

Заключение

Мне мало приходится работать с windows серверами. Чувствую себя не очень уверенно в этом окружении. Писать скрипты на bash и sh мне несравненно проще, чем на vbs или powershell. Тут вопрос привычки и опыта, но даже с самого начала своей работы с серверами в линуксе мне работать было интереснее и приятнее. Но от винды никуда не деться, приходится быть в тонусе и решать поставленные задачи.

Помогла статья? Есть возможность отблагодарить автора