УДК 004.01,004.02,004.4,004.6,004.7

СИСТЕМА МОНИТОРИНГА ЛОКАЛЬНЫХ И ОБЛАЧНЫХ СЕРВИСОВ

Желудкович В.В., магистрант гр.067041

Белорусский государственный университет информатики и радиоэлектроники, г.Минск Республика Беларусь

Бобов М.Н. – профессор , доцент технических наук

Аннотация. Предложен алгоритм перехода к системе мониторинга локальных и облачных сервисов. С помощью нижеописанного алгоритма перехода, становится возможным осуществлять мониторинг как локальных сетей, приложений, серверов, так и развёрнутых в облаке, с удалённого рабочего места, используя один инструмент, сохраняя безопасность, обеспеченную Microsoft Active Directory.

Ключевые слова: локальные сервисы, служба каталогов, службы авторизации, служба аутентификации, облачные сервисы.

ВведениеДля мониторинга локальный и облачных сервисов на базе операционных систем семейства Windows существует огромное количество, как стороннего, так и встроенного программного обеспечения. С переносом сервисов в облако появляется задача одностороннего мониторинга двух систем, как облачной, так и локальной с использованием общего инструмента с одинаковым набором метрик. Это необходимо для скорейшего выявления неполадок, сетевых атак. Кроме того, необходим такой инструмент, который может быть использован любым среднестатистическим специалистом, не обладающим специфическими знаниями. Также данное программное обеспечение должно соответствовать всем нормам сетевой безопасности. Для осуществления всего вышеописанного необходимо подключить все свои сервисы к системе мониторинга Microsoft Azure arc. Для этого необходима подготовка, обновление программного обеспечения, а также знание скриптового языка Microsoft PowerShell.

Подключение к общей системе мониторинга сетевых сервисов. Подготовка текущей системы заключается в обновлении систем каталогов Windows Active Directory до минимально необходимой версии 2016 года. Обновление привычным способами Microsoft приводит к потере данных, изменению схемы каталогов, некорректной работе службы групповых политик. Что в свою очередь часто приводит к нарушению безопасности. Уровень доступа пользователей может манятся. А отследить внесённые изменения не всегда представляется возможным. Identity сервисы являются наиболее важными сервисами в сегодняшнее время. Наиболее правильным путём будет добавление нового мастер сервера в существующий домен и передача ему роли мастера операций посредством PowerShell с параметрами. Сервер должен находится в одной подсети со старым для корректного ввода в домен. Также можно использовать средства виртуализации для создания сервера ADDS.

PowerShell код выполняемый в командной оболочке: Move-ADDirectoryServerOperation MasterRole -Identity "USER01-DC01" -OperationMasterRole PDCEmulator.

Предварительно необходима установка module Active Directory. Этот метод позволяет сохранить без изменений базу данных Active Directory.

Далее, чтобы проверить, перемещены ли роли, нужно перейти на новый сервер Windows. В Диспетчер сервера в разделе средства выбрать Active Directory модуль для Windows PowerShell Get-ADDomain. Командлет Get-ADForest для просмотра владельцев ролей FSMO. Далее после репликации контролёра домена можно выводить из работы старый сервер и проверить аутентификацию на любом пользователе.

После осуществления обновления необходимо синхронизировать Azure Active Directory с Active Directory Domain Services. В облачном портале появляется функция SSO - Single Sign-On. Другими словами, появляется возможность авторизации и аутентификации при помощи логина и пароля пользователя, созданного на локальном сервере. Но вместе с тем у этого пользователя отсутствует доступ к управлению локальной сетью. Для этого системным администратором необходимо настраивать VPN-тоннель для установки взаимоотношений двух сетей облачной и локальной. У пользователя в облачном портале есть доступ только к мониторингу сервисов.

Далее необходима настройка системы мониторинга на стороне облака. В портале Azure, в строке поиска ресурсов устанавливаем все необходимое (рис. 1).

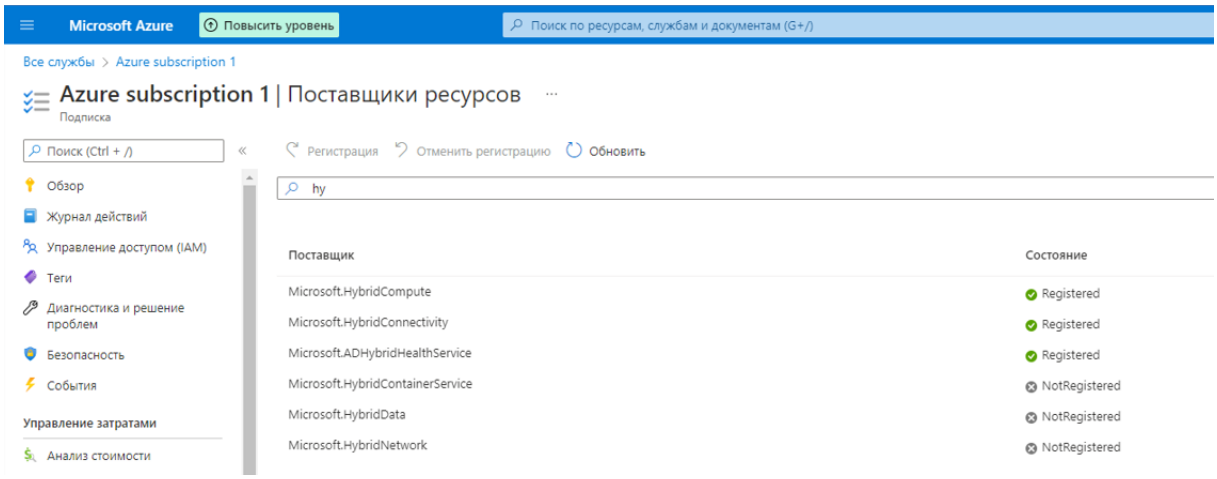

Рис. 1. Ресурсы системы мониторинга

Hybrid Compute, Hybrid Connectivity – отвечают за подключение гибридных серверов (локальных, облачных).
Hybrid HealthCare – панель мониторинга гибридной системы.
После установки ресурсов необходимо осуществить подключение серверов. Подключение осуществляется при помощи скриптового языка PowerShell, на стороне сервера, который необходимо подключить. Пример скрипта описан на рис. 2.

C: > Users > zhalu > OneDrive > Рабочий стол > ExitTask > ip.ps1

```
# Скачивание и установка пакетов
Invoke-WebRequest -Uri "https://aka.ms/azcmagent-windows" -TimeoutSec 30 -OutFile "$env:TEMP\install_windows_azcmagent.ps1"
# Установка гибридного агента
& "$env:TEMP\install_windows_azcmagent.ps1"
if($LASTEXITCODE -ne 0) {
throw "Failed to install the hybrid agent"
}
# Запуск подключённой программы
& "$env:ProgramW6432\AzureConnectedMachineAgent\azcmagent.exe" connect --resource-group "ADDS" --tenant-id "f6ce8ba2-89a1-4442-b939-1ddbbb7c2e47" --`
location "eastus" --subscription-id "d8272f6f-327a-4dd9-9754-f2a0fa035a2b" --cloud "AzureCloud" --correlation-id "c8a00abe-747a-4d22-919a-c2609c4b5001"`
if($LastExitCode -eq 0){Write-Host -ForegroundColor yellow "To view your onboarded server(s), navigate to`
https://portal.azure.com/#blade/HubsExtension/BrowseResource/resourceType /Microsoft.HybridCompute%2Fmachines"}
```

Рис. 2. Пример кода для подключения к системе мониторинга Azure

В данном коде осуществляется запрос на удалённый сервер, для скачивания сгенерированного скриптового файла под определённый сервер, его дальнейшая установка и запуск. Всё это происходит в командной оболочке.
После выполнения скриптового кода на сервере должны отобразиться сообщения о успешном выполнении этапов установки и запуска (рис.3). При неверном исполнении будут выводиться ошибки со всей необходимой информацией. Это описано в коде для устранения проблем установки.

```
PS C:\Users\Administrator> # Download the installation package
PS C:\Users\Administrator> Invoke-WebRequest -Uri "https://aka.ms/azcmagent-windows" -TimeoutSec 30 -OutFile "$env:TEMP\instal
l_windows_azcmagent.ps1"
PS C:\Users\Administrator>
PS C:\Users\Administrator> # Install the hybrid agent
PS C:\Users\Administrator> & "$env:TEMP\install_windows_azcmagent.ps1"
VERBOSE: Installing Azure Connected Machine Agent
VERBOSE: Downloading agent package
VERBOSE: Installing agent package
Installation of azcmagent completed successfully
PS C:\Users\Administrator> if($LASTEXITCODE -ne 0) {
>>     throw "Failed to install the hybrid agent"
>> }
PS C:\Users\Administrator>
PS C:\Users\Administrator> # Run connect command
PS C:\Users\Administrator> & "$env:ProgramW6432\AzureConnectedMachineAgent\azcmagent.exe" connect --resource-group "Arc" --ten
ant-id "f6ce8ba2-89a1-4442-b939-1ddbbb7c2e47" --location "westeurope" --subscription-id "d8272f6f-327a-4dd9-9754-f2a0fa035a2b"
 --cloud "AzureCloud" --correlation-id "87d902f2-b789-46ba-ab1a-1deb9c02f00b"
time="2022-02-15T09:09:26-08:00" level=info msg="Loading AgentConfig file from: C:\\ProgramData\\AzureConnectedMachineAgent\\C
onfig\\agentconfig.json"
time="2022-02-15T09:09:26-08:00" level=info msg="Onboarding Machine. It usually takes a few minutes to complete. Sometimes it
may take longer depending on network and server load status."
time="2022-02-15T09:09:26-08:00" level=info msg="Check network connectivity to all endpoints..."
time="2022-02-15T09:09:27-08:00" level=info msg="All endpoints are available... continue onboarding"
To sign in, use a web browser to open the page https://microsoft.com/devicelogin and enter the code CSWLJDMS6 to authenticate.
time="2022-02-15T09:10:26-08:00" level=info msg="Successfully Onboarded Resource to Azure" VM Id=dc4e026d-e60e-45c0-99c2-4db3c
d1c89e2
PS C:\Users\Administrator>
PS C:\Users\Administrator> if($LastExitCode -eq 0){Write-Host -ForegroundColor yellow "To view your onboarded server(s), navig
ate to https://portal.azure.com/#blade/HubsExtension/BrowseResource/resourceType/Microsoft.HybridCompute%2Fmachines"}
To view your onboarded server(s), navigate to https://portal.azure.com/#blade/HubsExtension/BrowseResource/resourceType/Micros
oft.HybridCompute%2Fmachines
PS C:\Users\Administrator>
```

Рис. 3. Успешное добавление сервера в систему мониторинга

В панели Azure в облачном портале появится добавленный сервер (рис.4).

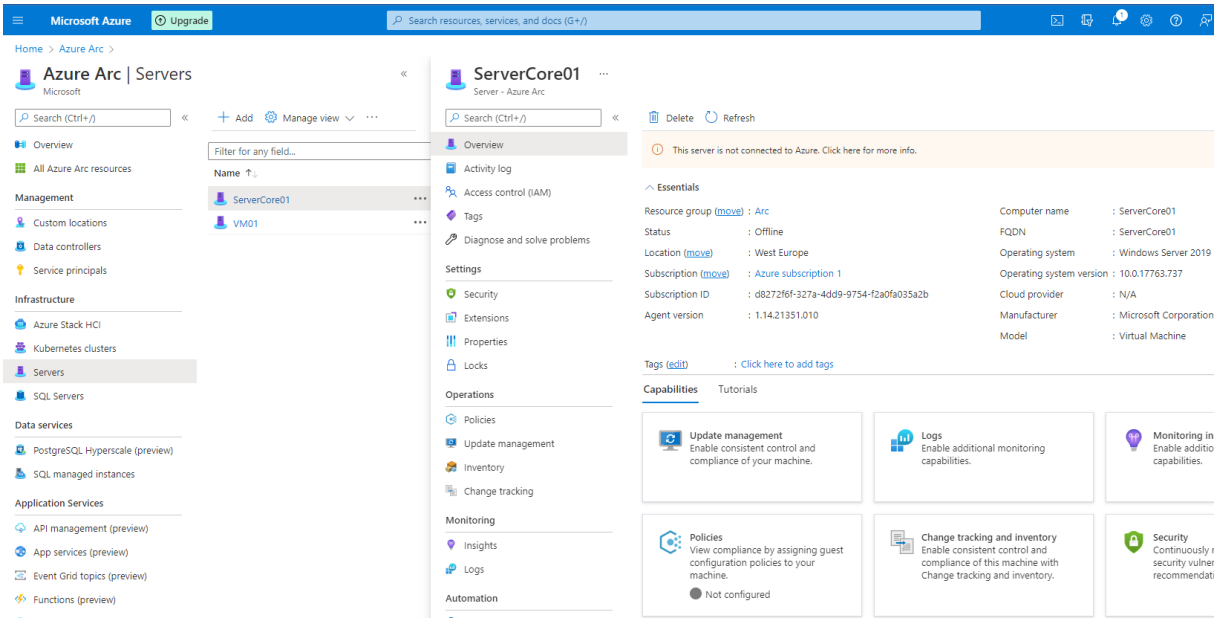

Рис. 4. Панель мониторинга Azure

Дополнительные возможности системы общего мониторинга и управления: централизованное управление широким спектром ресурсов, включая серверы Windows и Linux, SQL Server, кластеры Kubernetes; обеспечение управлением жизненным циклом виртуальных машин для своих сред Azure Stack HCI и VMware из централизованного расположения; создание ориентированных на облако приложений в большом масштабе.

Заключение. Переход на вышеописанную систему мониторинга открывает совершенно новые возможности. Нет необходимости отказываться от существующей локальной сетевой структуры, мониторинг осуществляется удалённо из любой точки планеты, аутентификация и авторизация осуществляется при помощи Active Directory, что в свою очередь обеспечивает безопасность. Существует перспектива роста и переход к новой системе управления. Всё выше описанное позволяет с уверенность сказать, что любую старую сетевую структуру можно безболезненно переносить в облако имея при этом современный доступ к мониторингу всех сервисов. Не нужно иметь несколько инструментов мониторинга для каждой из сетей будь то облако или локальный сервер.

Список литературы

1. Mastering Active Directory 2021. Dishan Francis. // Domen Controllers. 2021. Vol. 3. P. 31–37.
2. PowerShell for system administrators. Adam Bertram //Active Directory. 2021. Vol. 51. P. 100–125.
3. Computer Networking James F.Kurose //. 2008. Vol. 9. P. 35–79.
4. Microsoft Azure Security Center, First Edition. // . 2018. Vol. 48. P. 130–159.