1. **Parameter Store**

Переменные окружения, которые можно добавить в EC2

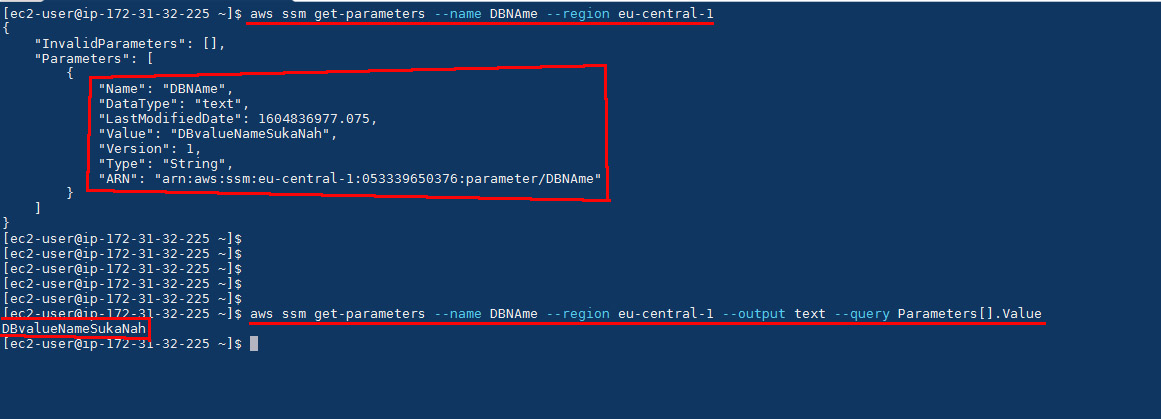
|  |  |
| --- | --- |
|  |  |

Как добавить в EC2:

Создать новую роль в IAM

|  |  |  |
| --- | --- | --- |
|  |  | |
|  | |  |

На EC2 добавить переменную:



***Вывести значения на EC2***

aws ssm get-parameters --name DBNAme --region eu-central-1

aws ssm get-parameters --name DBNAme --region eu-central-1 --output text --query Parameters[].Value

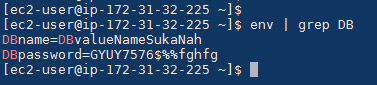
***добавить переменную с обычным текстом:***

export DBname=`aws ssm get-parameters --name DBNAme --region eu-central-1 --output text --query Parameters[].Value`

***переменная с зашифрованным текстом:***

aws ssm get-parameters --name DBPassword --region eu-central-1 --with-decryption --output text --query Parameters[].Value

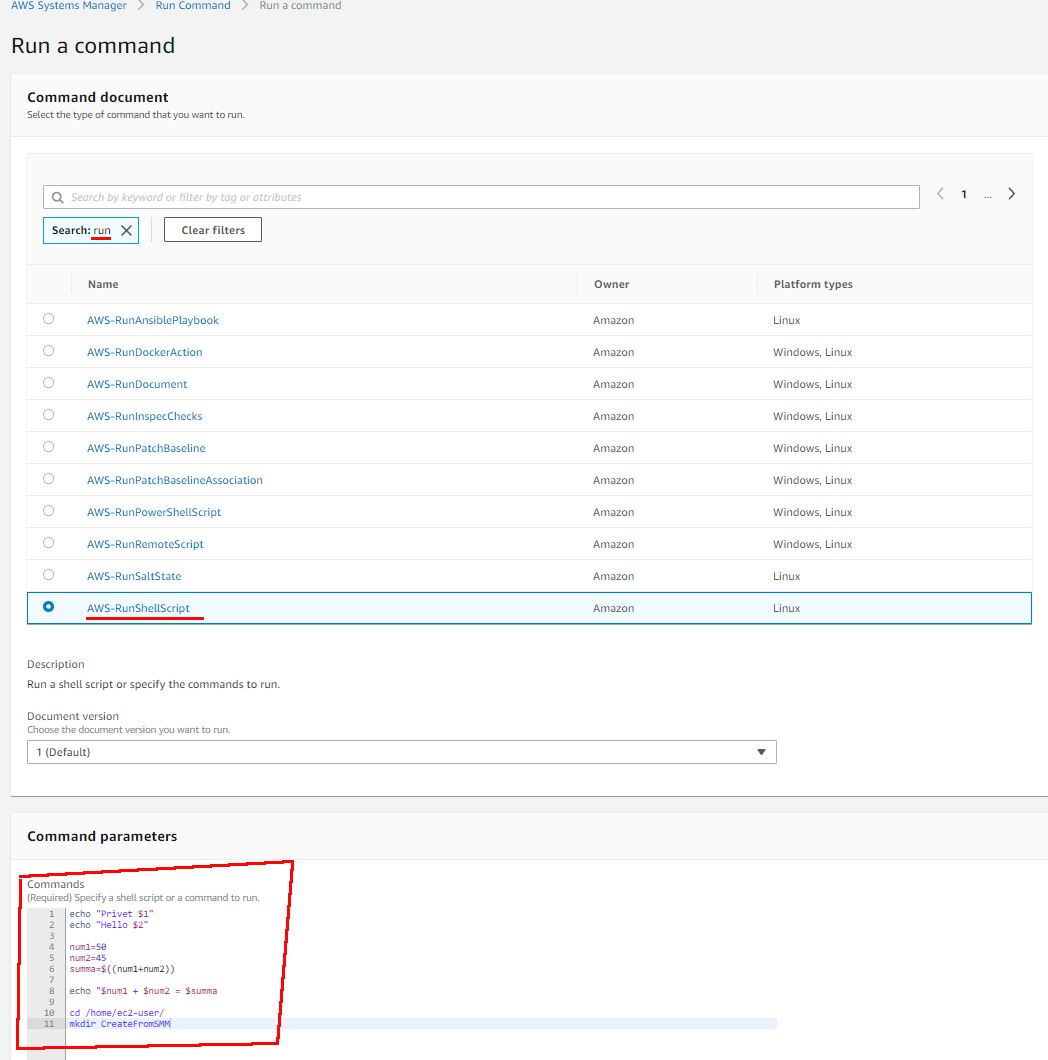
export DBpassword=`aws ssm get-parameters --name DBPassword --region eu-central-1 --with-decryption --output text --query Parameters[].Value`

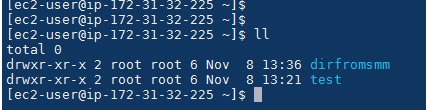


1. **Run Command**

Запустить скрипт (EC2 должен быть с ролью посмотреть подключенные к SSM в Managed Instances):

AWS System Manager – Instances & Nodes





1. **Hybrid Infrastructure - Управление Серверами не в AW*S***

[**https://docs.aws.amazon.com/systems-manager/latest/userguide/sysman-install-managed-linux.html**](https://docs.aws.amazon.com/systems-manager/latest/userguide/sysman-install-managed-linux.html)

*команды для запуска агента SMM на сервере НЕ AWS*

mkdir /tmp/ssm

curl https://s3.amazonaws.com/ec2-downloads-windows/SSMAgent/latest/debian\_amd64/amazon-ssm-agent.deb -o /tmp/ssm/amazon-ssm-agent.deb

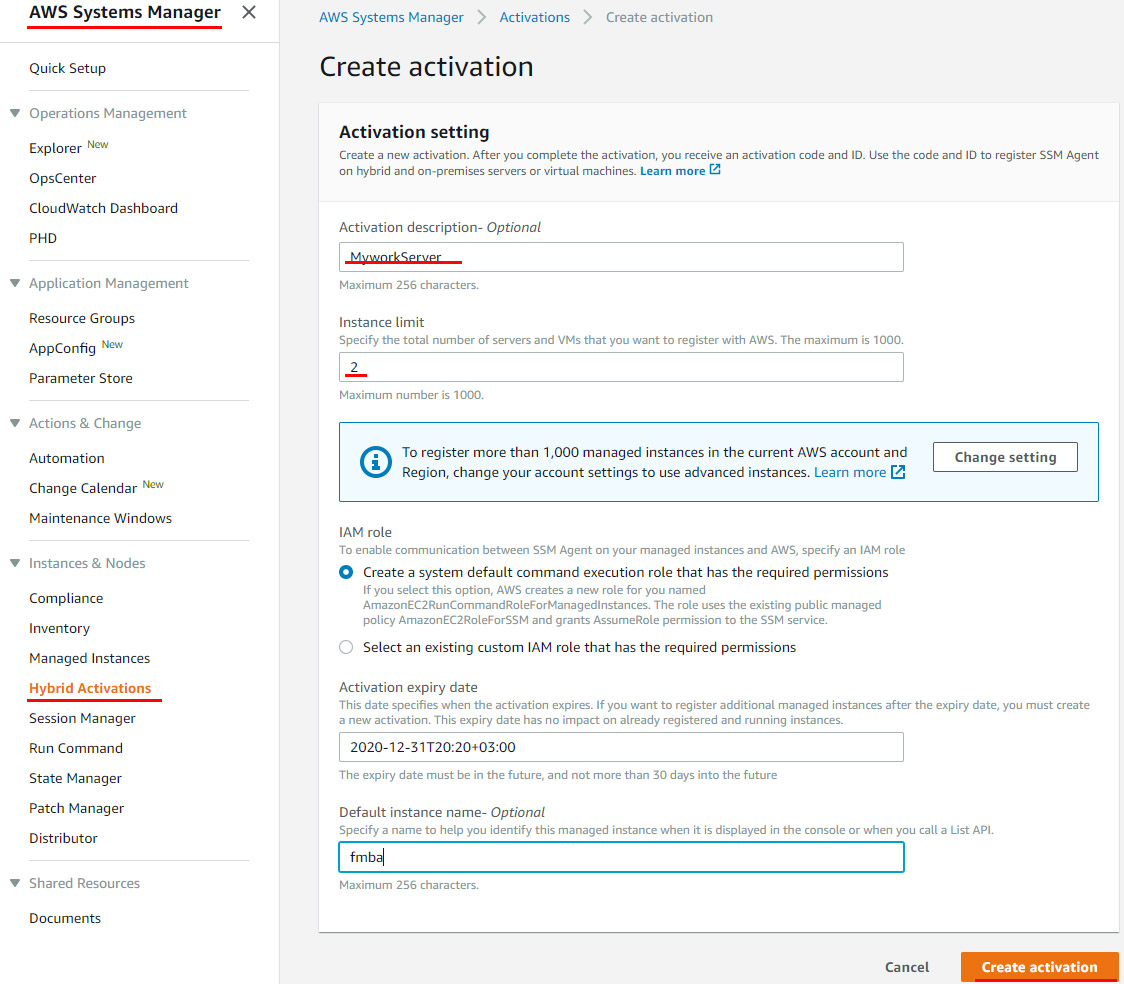
sudo dpkg -i /tmp/ssm/amazon-ssm-agent.deb

sudo service amazon-ssm-agent stop

sudo amazon-ssm-agent -register -code "activation-code" -id "activation-id" -region "region"

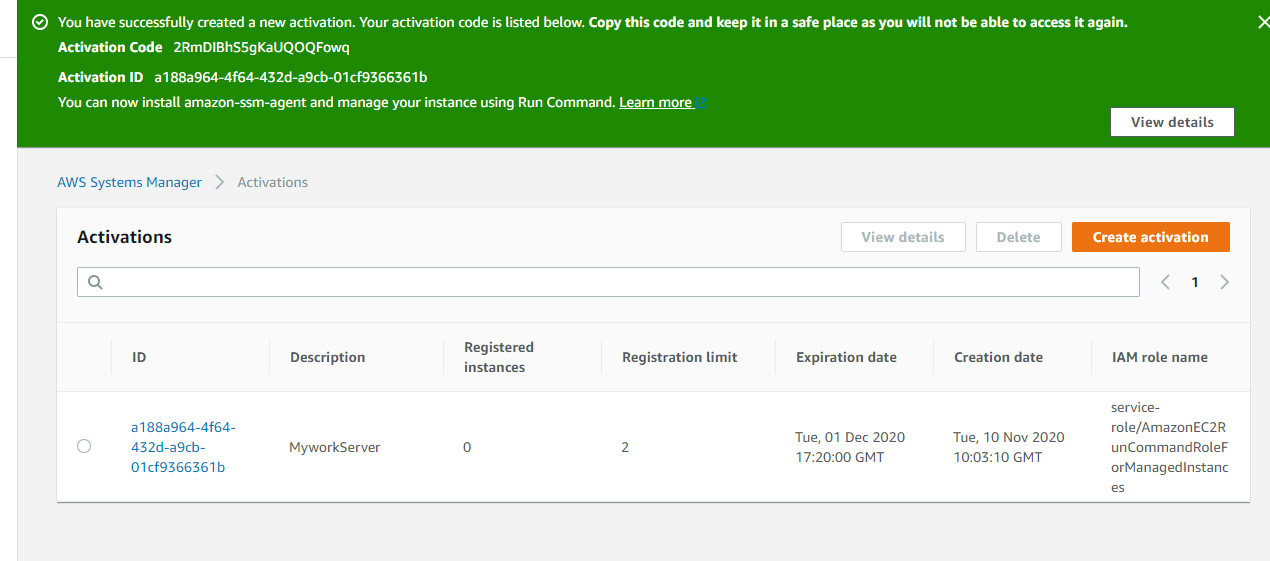
sudo service amazon-ssm-agent start

*где взять activation-code и activation-id:*

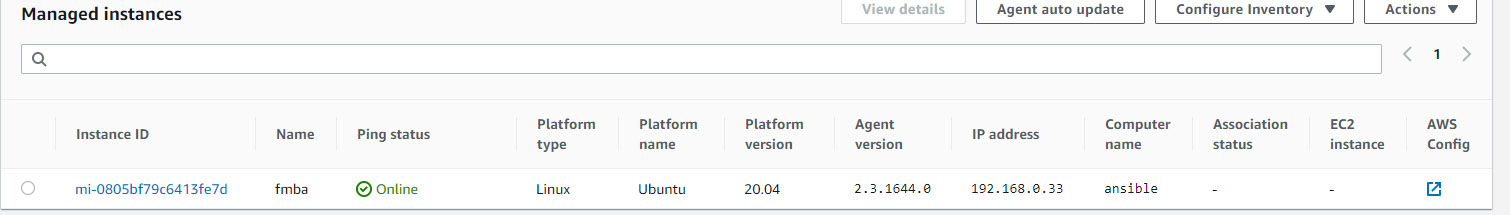


Activation Code 2RmDIBhS5gKaUQOQFowq

Activation ID a188a964-4f64-432d-a9cb-01cf9366361b



Поочередно вводим команды выше, сервер появится в Managed instances



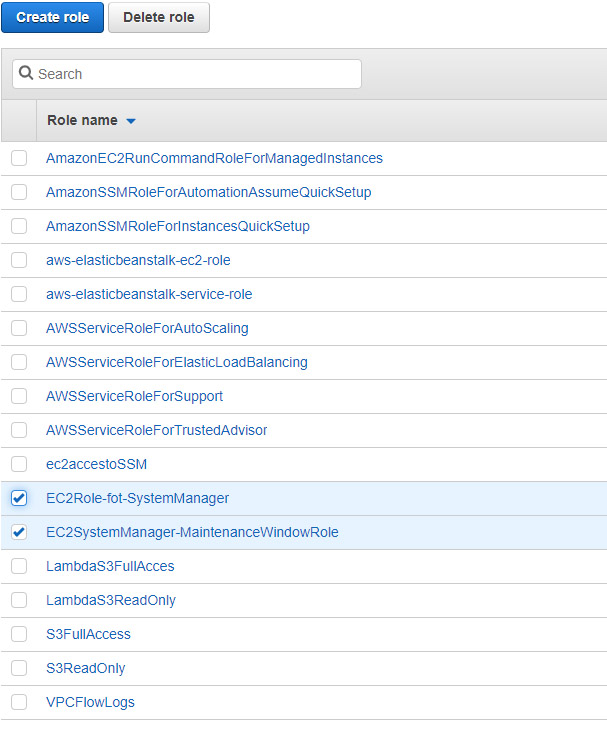
Теперь можно запускать команды как для амазоновских EC2

1. **Windows maintenance**

Создать две роли в IAM

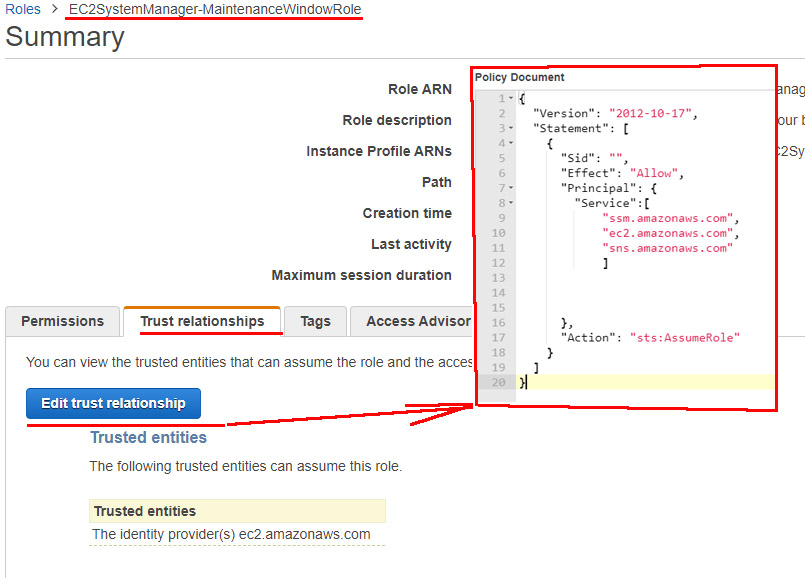
Первая для EC2 с политикой *AmazonEC2RoleforSSM*

Вторая для EC2 с политикой *AmazonSSMMaintenanceWindowRole*



Во вторую роль добавить Trust Relationship

<https://docs.aws.amazon.com/systems-manager/latest/userguide/sysman-maintenance-perm-console.html>



------------------------------------------начало кода-------------------------------------------------------------

{

"Version": "2012-10-17",

"Statement": [

{

"Sid": "",

"Effect": "Allow",

"Principal": {

"Service":[

"ssm.amazonaws.com",

"ec2.amazonaws.com",

"sns.amazonaws.com"

]

},

"Action": "sts:AssumeRole"

}

]

}------------------------------------------конец кода-------------------------------------------------------------

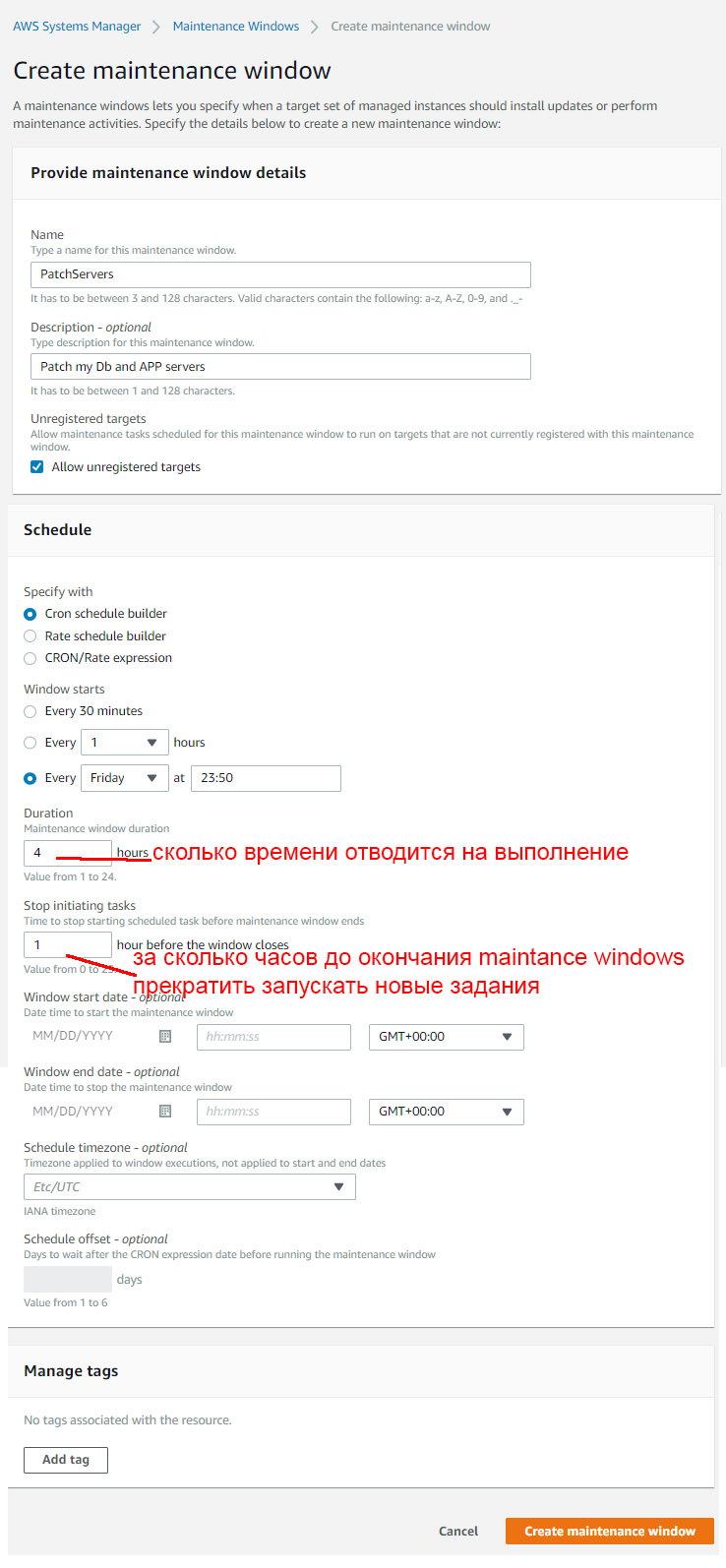
* Привязать роли к EC2, правой кнопкой – security – modify IAM role, добавить первую созданную роль для SMM, теперь сервера появятся в Managed Instances
* Добавить тэги в EC2 с ключом Patch Group (SMM понимает этот ключ)

|  |  |
| --- | --- |
|  |  |

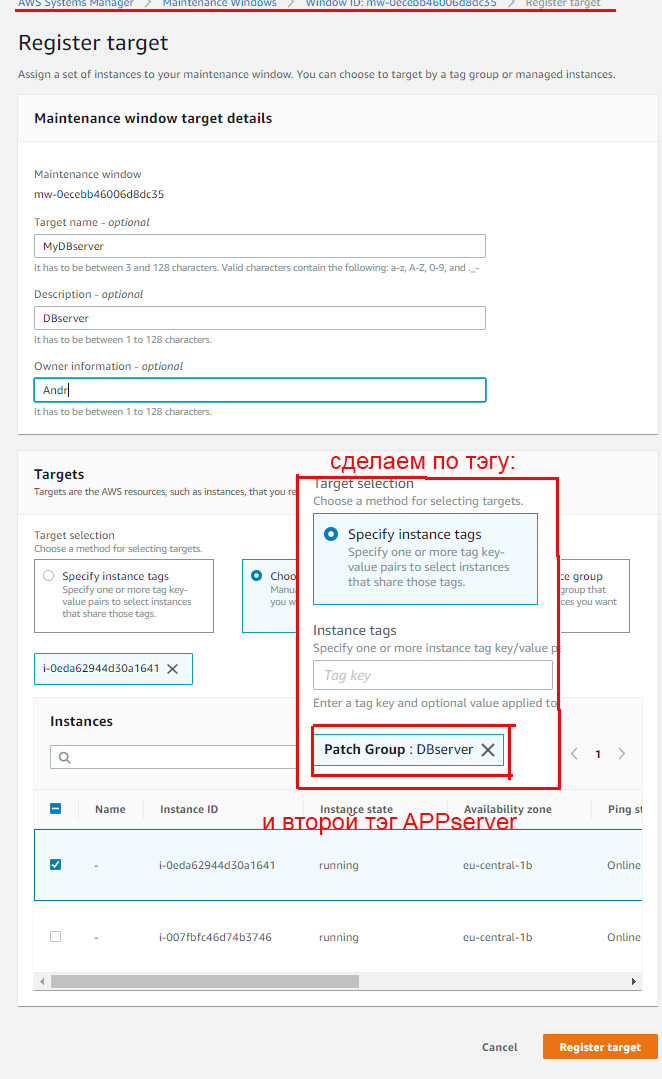
В State manager добавить ассоциацию:

|  |  |
| --- | --- |
|  |  |

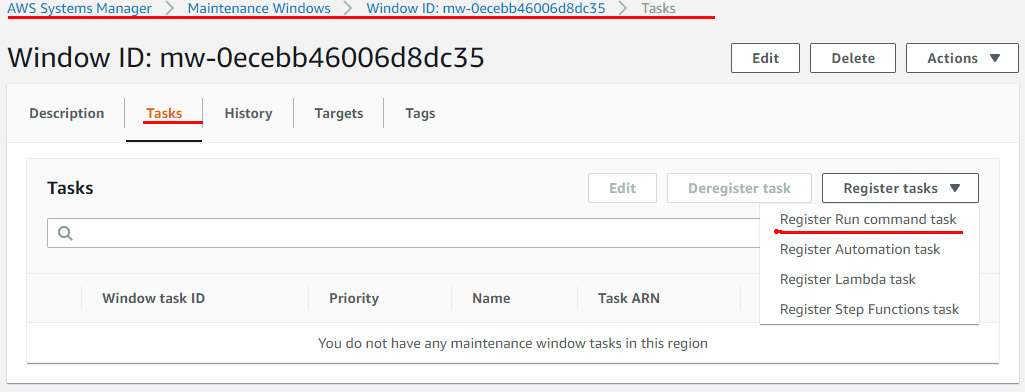
Создаем Maintenance Windows



Добавить задачи в созданное окно, target – на каких серверах запускать, сделаем две цели на два разных сервера по тегам



Добавляем задачи:



|  |  |
| --- | --- |
|  |  |

|  |  |
| --- | --- |
|  | Команда:  Add-Content -patch c:\log.txt -Value "$(Get-Date)---Start of Patching"  Working directory – c:\ |

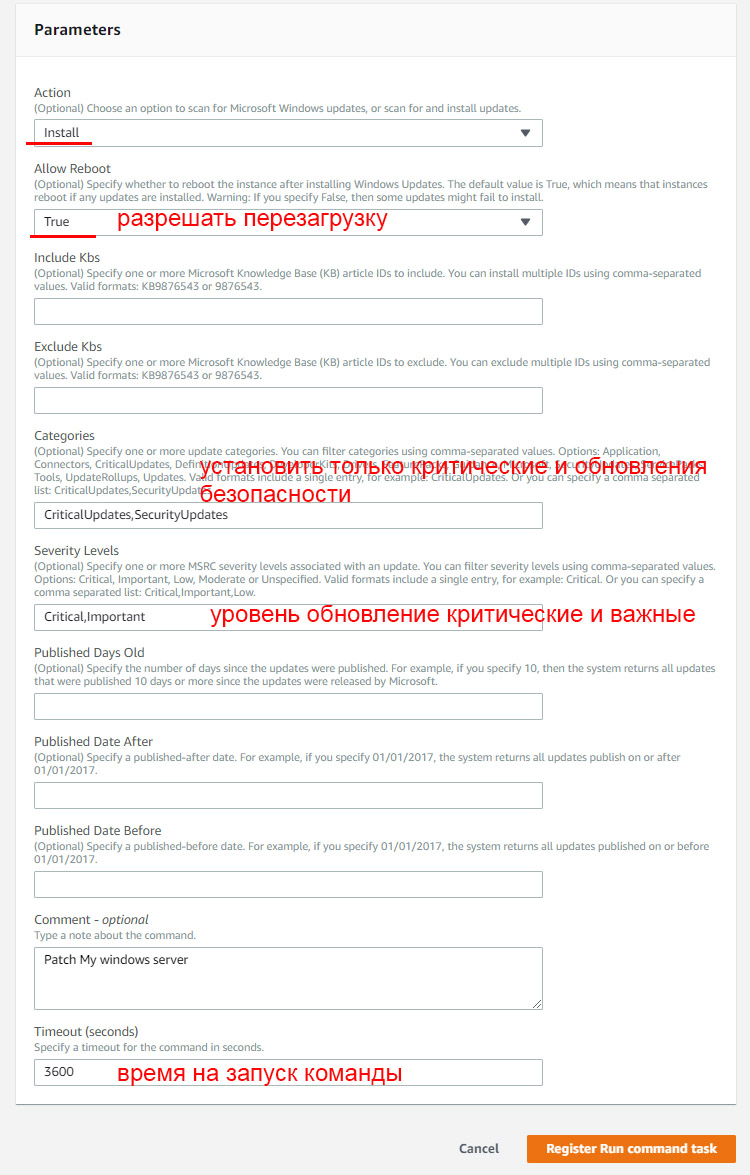
Создаем вторую такую же задачу, только с командой Add-Content -patch c:\log.txt -Value "$(Get-Date)---End of Patching"

Создаем третью задачу по запуску обновлений на серверах:

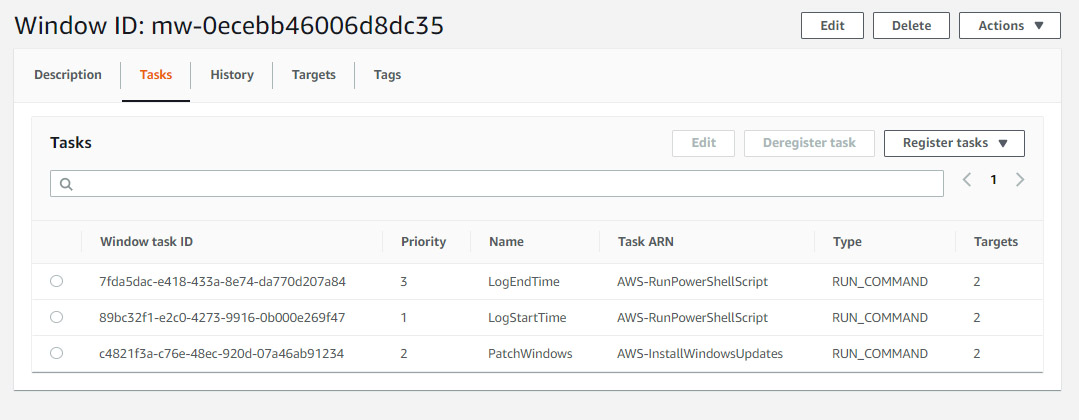
В разделе Command document выбрать *AWS-InstallWindowsUpdates*

Приоритет 2 (1 на задаче старта, 3 на задаче окончания)

Раздел Parameters:



Итого три задачи



Теперь по расписанию будут запускаться обновления