Greyson Spencer

grsncd

CS 3530 - Unix Operating System

A Taste of System Administration with AWS

Topic

The topic I chose for this report was a combination of a small introduction into system administration as well as some work in the realm of Amazon Web Services. Working this semester with user manipulation, AWS virtual machines in EC2, and shell scripting piqued my interest in system administration as a career because I liked creating and managing an environment for users to interact with.

This is a very applicable topic because system administration is an important line of work for any organization with an internal computing system. The work with AWS is also incredibly relevant because it's the industry standard at this point for cloud computing.

This report covers some ideas within the cloud computing space, some information about being a system administrator, and a simple script I wrote to demonstrate some automation that could be implemented within AWS.

Research

One of the more important topics I came across in my cloud computing research was the idea of least-privilege access. Amazon Web Services' security policies are largely based on this concept due to its simplicity and effectiveness. I found my information on this topic their best practice security documentation **(source 1)**. The basic idea is to provide only the permissions required to complete the job at hand and this is applied to both users and AWS services. This is to help mitigate the damage users or services can inflict on a system in case of a security breach.

An important part to remember about this is to start with a small amount of privileges and work your way up to what is required. For example, say you're a system administrator setting up the privileges for a virtual machine hosted in an EC2 instance that needs to access the contents of an S3 bucket with important data to be analyzed inside. If you start by giving the EC2 instance full read and write permissions, it's possible an inexperienced developer could accidentally overwrite the data within the bucket, rendering it useless. If you start by giving only read permissions, and they mistakenly attempt to write over the data in the bucket, then they will be prevented from doing so.

I also learned that permissions in AWS are managed through a service called Identity and Access Management (IAM) and allows for the management of access to different services within AWS in a very understandable way. On the AWS IAM documentation **(source 6)** I discovered that Custom permissions can be created and managed with ease by an administrator. Then the groups of permissions can be applied to services with the use of roles.

System administration is an important line of work when it comes to managing the infrastructure needed by an organization, whether it be on-site, or cloud based. The information located at **source 5** shows some of the common requirements of being a system administrator including the maintenance of infrastructure and fixing problems with the system as they arise. Another very important task that system administrators undergo is the creation of new workstations for users.

I also used a few sources to find some more information to write a script for use in AWS. **Source 2** is the Raspberry Pi documentation on the .bashrc and .bash_aliases files, and I used it to understand how the two files interact. Basically, the .bash_aliases file isn't created by default for users but the .bashrc file implements it if it exists. To create a .bash_aliases file, you just need to add aliases line by line in a text file. This allows your list of aliases to be organized and portable.

I used **source 3** to learn the conventional way to update debian and fedora based systems. For debian, you usually can use "apt-get update", while for fedora you can use "yum update".

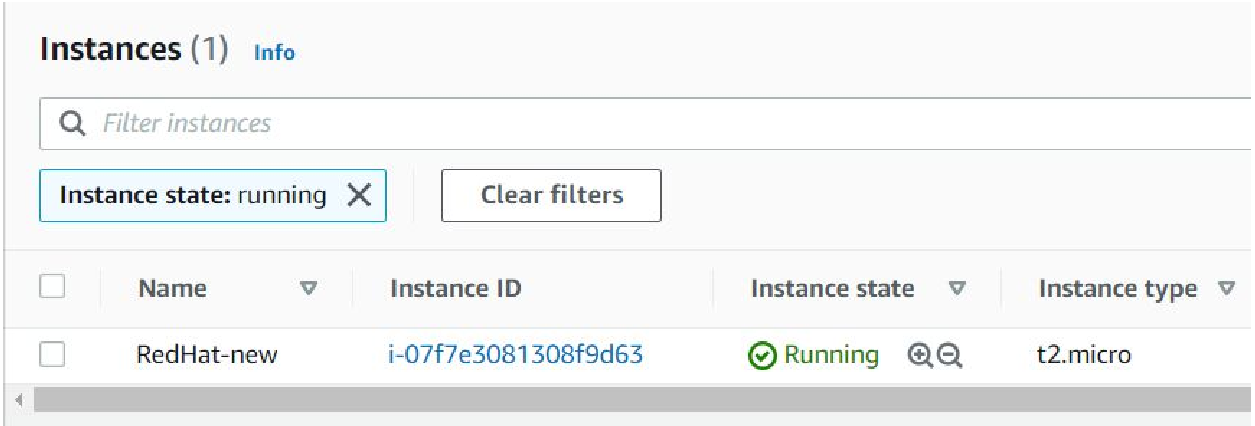
Finally, I used **source 4** to learn how to access the contents of S3 buckets while using an EC2 instance. What I found was that as long as the instance has permissions to access the bucket, it can pull files similar to a normal server. The command that I found most useful was utilizing the wget utility and the path to the file like so:

```
"wget https://{bucket-name}.s3.amazonaws.com/{path}"
```

Applications

For my application, I created a simple script that a system administrator could use to create the environment they need to set up the rest of the instance. I stored the script and a personal .bash_aliases file in an S3 bucket entitled 3530-init-bucket-gs that can be accessed by my EC2 instance because I attached a role with the permissions required.

The idea is a system administrator creates a new debian or fedora based EC2 instance, logs in with their credentials, downloads the script from S3 using wget, and then runs it. The script creates the sysadmin user, adds the user to the root or wheel group (depends on the distribution), downloads a personal .bash_aliases file from S3, and then attempts to update the system with the command corresponding to the distribution.



Instances (1) Info

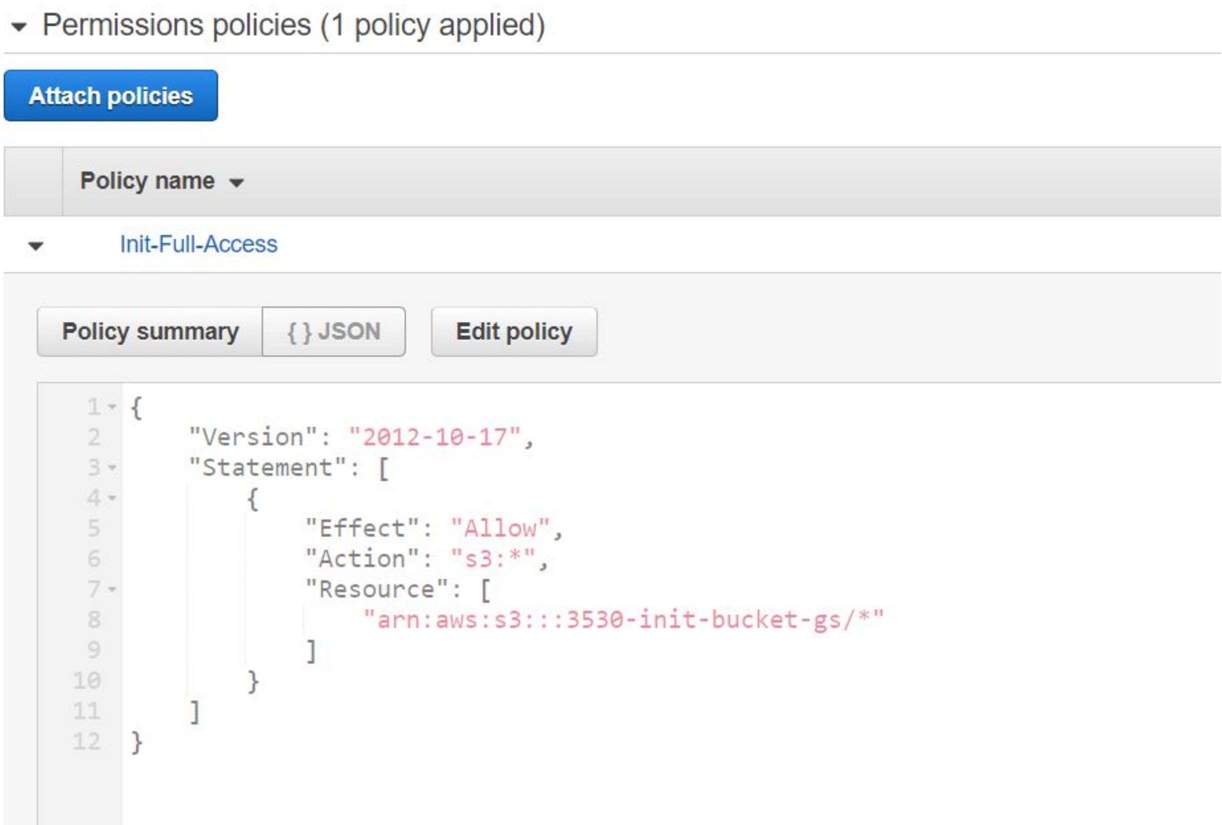
Filter instances

Instance state: running

Clear filters

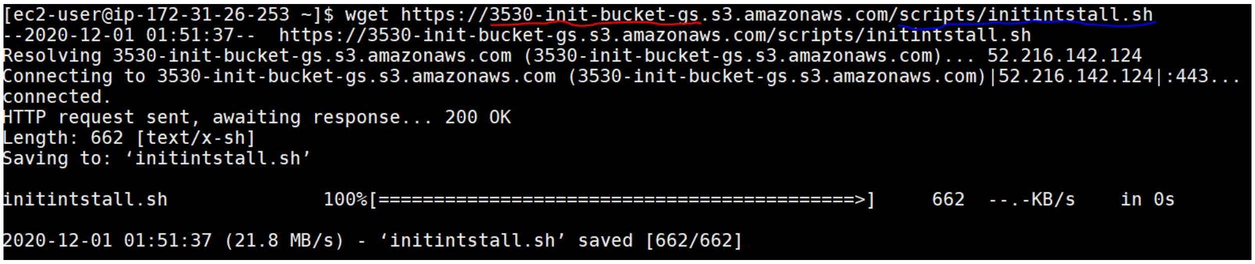
□	Name	Instance ID	Instance state	Instance type
□	RedHat-new	i-07f7e3081308f9d63	Running	t2.micro

Above is the running EC2 instance I planned to set up



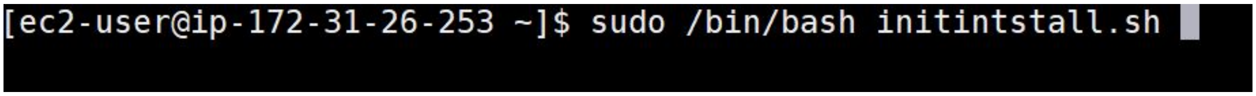
```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "s3:*",
            "Resource": [
                "arn:aws:s3:::3530-init-bucket-gs/*"
            ]
        }
    ]
}
```

The permissions policy in a JSON format that allows access to the S3 bucket



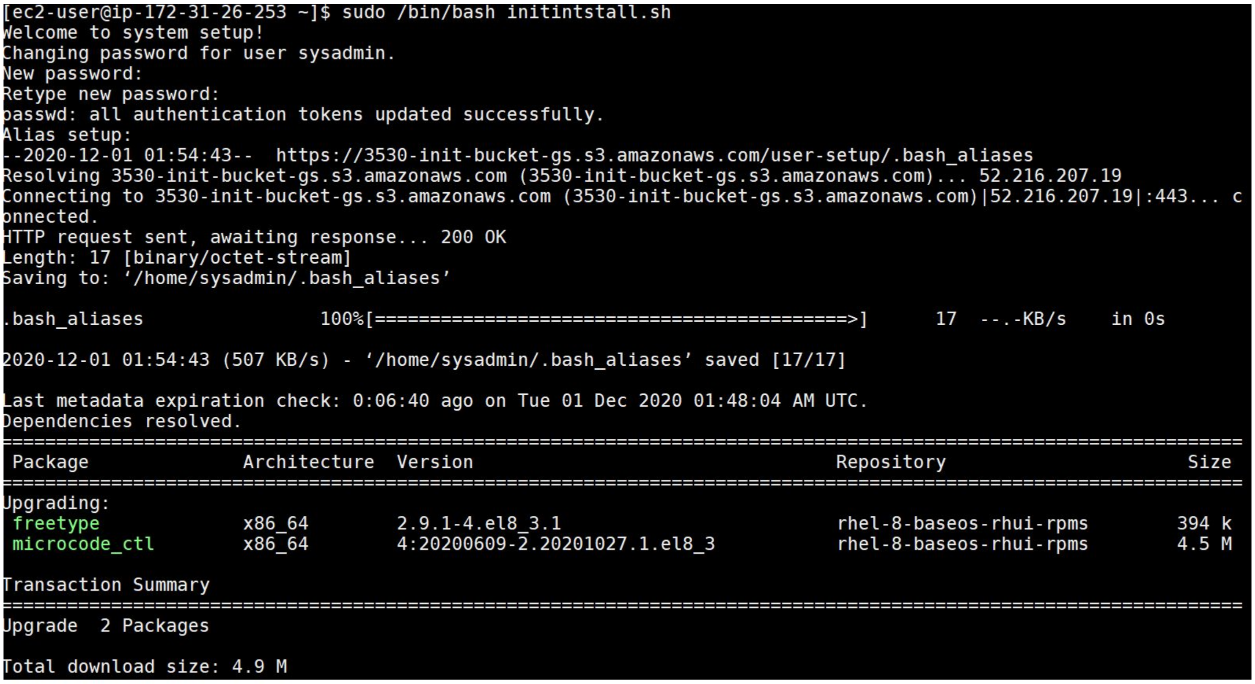
```
[ec2-user@ip-172-31-26-253 ~]$ wget https://3530-init-bucket-gs.s3.amazonaws.com/scripts/initintstall.sh
--2020-12-01 01:51:37--  https://3530-init-bucket-gs.s3.amazonaws.com/scripts/initintstall.sh
Resolving 3530-init-bucket-gs.s3.amazonaws.com (3530-init-bucket-gs.s3.amazonaws.com)... 52.216.142.124
Connecting to 3530-init-bucket-gs.s3.amazonaws.com (3530-init-bucket-gs.s3.amazonaws.com)|52.216.142.124|:443...
connected.
HTTP request sent, awaiting response... 200 OK
Length: 662 [text/x-sh]
Saving to: ‘initintstall.sh’

initintstall.sh              100%[==========================================>]     662  --.-KB/s    in 0s

2020-12-01 01:51:37 (21.8 MB/s) - ‘initintstall.sh’ saved [662/662]
```

The command run by the initial user to pull the script from the S3 bucket



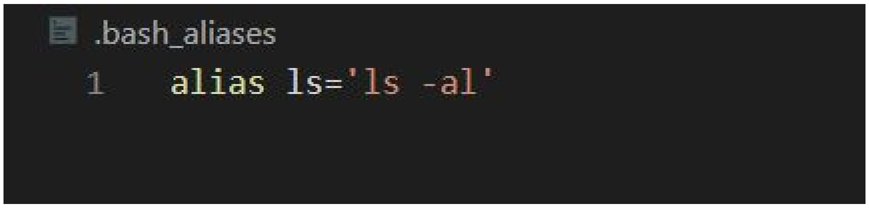
```
[ec2-user@ip-172-31-26-253 ~]$ sudo /bin/bash initintstall.sh
```

Command to run the script once downloaded



```
[ec2-user@ip-172-31-26-253 ~]$ sudo /bin/bash initintstall.sh
Welcome to system setup!
Changing password for user sysadmin.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
Alias setup:
--2020-12-01 01:54:43--  https://3530-init-bucket-gs.s3.amazonaws.com/user-setup/.bash_aliases
Resolving 3530-init-bucket-gs.s3.amazonaws.com (3530-init-bucket-gs.s3.amazonaws.com)... 52.216.207.19
Connecting to 3530-init-bucket-gs.s3.amazonaws.com (3530-init-bucket-gs.s3.amazonaws.com)|52.216.207.19|:443... c
onnected.
HTTP request sent, awaiting response... 200 OK
Length: 17 [binary/octet-stream]
Saving to: ‘/home/sysadmin/.bash_aliases’

.bash_aliases               100%[=========================================>]      17  --.-KB/s    in 0s

2020-12-01 01:54:43 (507 KB/s) - ‘/home/sysadmin/.bash_aliases’ saved [17/17]

Last metadata expiration check: 0:06:40 ago on Tue 01 Dec 2020 01:48:04 AM UTC.
Dependencies resolved.
================================================================================================================
 Package                Architecture  Version                                  Repository                  Size
================================================================================================================
Upgrading:
 freetype               x86_64        2.9.1-4.el8_3.1                          rhel-8-baseos-rhui-rpms    394 k
 microcode_ctl          x86_64        4:20200609-2.20201027.1.el8_3            rhel-8-baseos-rhui-rpms    4.5 M

Transaction Summary
================================================================================================================
Upgrade  2 Packages

Total download size: 4.9 M
```

Output of the script



```
.bash_aliases
alias ls='ls -al'
```

Contents of the .bash_aliases file imported from S3

Sources

1. https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#grant-least-privilege Least Privilege information, as well as additional best-practice security
2. https://www.raspberrypi.org/documentation/linux/usage/bashrc.md about .bash_aliases
3. https://www.cyberciti.biz/faq/linux-update-all-packages-command/ about cross platform updates
4. https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AmazonS3.html working with S3 through EC2
5. https://resources.workable.com/system-administrator-job-description system administrator information
6. https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html AWS IAM docs