Zack Heaton
Written Assignment
Started: 29 July at 12:00
Completed: 31 July at 1116 (two sessions of 2 hours each).

Question 1

This is a test. Using any publicly available dataset, write a script that will take data from that source and output it via http in json format to either one of the following inputs: Elastic, Splunk http input, Cribl HTTP input, or s3. We should be able to run the script while passing along the required arguments to make it work with your choice of destination.

The script I wrote required a dataset. A really interesting one that I found was data.gov. If you simply click the search bar with no search context it pulls random datasets published by various government departments. Seeing how the data is formatted you can start to think about how you might pull multiple datasets to correlate. In this example the Economic Research Service (ERS) used Circana (formerly Information Resources Inc. [IRI]) between 2013 and 2020 tracking all items sold in grocery stores nationwide. The data is originally in .csv format. My script can take the URL of the specific dataset, convert it to json, and send it to a test elasticsearch instance that I was able to get for free. If we could imagine this on an elastic dash board or something like a Grafana! Think about how big level data driven decisions could be made to improve our future! It would revolutionize government spending and bureaucracy! The URLs to the respective endpoints are all listed below:

https://catalog.data.gov/dataset/fruit-and-vegetable-prices
https://www.ers.usda.gov/data-products/fruit-and-vegetable-prices.aspx
Fruit Prices 2020.csv (local download)

In addition to describing the simple functionality of my script I did want to provide you with a bit of “where my head was at” as I put it together. Hopefully, this demonstrates how I think a bit better. I start by naming a variable as one of the endpoint data sources from the ERS. I do this with [Invoke-RestMethod -uri] which will connect via http/https. Once the data was pulled down it wasn’t too hard to switch it over to json. It took two tries because originally my syntax just said simply convert TO json there was a struggle with the intake and the data. Once I added a convert FROM .csv it seemed to standardize the input therefore I could do a conversion to json with a uniform input.

I want to explain the last part openly and honestly because I think this is one of my attributes that can help any team! I did not have an elasticsearch instance of my own before this paper, I got one. While the pulling down of data is something sort of in my skill set already; sending it to a a third party like elasticsearch was completely new to me. I went to work reading the following links on Elastic’s Documentation. That is how I got the instance running and therefore built my endpoint. Elastic provided me with those credentials. I think this is important because it shows that I don’t understand something; I will make it my only business to learn it! Check out those links below:

https://zacktestenvironment.kb.us-central1.gcp.cloud.es.io:9243/api/security/saml/callback
https://discuss.elastic.co/t/load-json-to-elasticsearch/195235

See the full script below:

```
$TestData = "https://www.ers.usda.gov/webdocs/DataFiles/51035/Fruit%20Prices%202020.csv?v=499.9"
$response = Invoke-RestMethod -Uri $TestData

if ($response) {
    # Success
    $json_data = $response | ConvertFrom-Csv | ConvertTo-Json
    Write-Output $json_data
}
else {
    echo "Double Check The Link You Provided, It's Not Working."
}

{
Install-Module -Name "Elasticsearch" -Force

    $elasticUrl = "https://zacktestenvironment.kb.us-central1.gcp.cloud.es.io:9243/api/security/saml/callback"
    $elasticUsername = "elastic"
    $elasticPassword = "zPRscsnMd0tfCzk9bQEnNe2g"


    $credentials = [System.Text.Encoding]::UTF8.GetBytes("$($elasticUsername):$($elasticPassword)")
    $base64AuthInfo = [System.Convert]::ToBase64String($credentials)
    $headers = @{ Authorization = "Basic $base64AuthInfo" }


    $result = Invoke-RestMethod -Uri $elasticUrl -Method Post -Headers $headers -Body $json_data -ContentType
"application/json"

    if ($result.created -eq $true) {
        Write-Output "Data sent successfully to Elastic!"
    }

    else {
        Write-Output "Failed to send data to Elastic. Error: $($result.error.type)"
    }
}
```

Question 2

Tell us what your favorite/most-used Linux command is and why. How would you make it even better than it already is? Does it have any negative aspects?

I'm not sure that I have a favorite command. When I think about it I can say that "htop" is my most used. I like it because compared to the normal "top" command it has colors and a better layout. I can also answer the negative features of "top" because when I struggle with Linux I address command shortcomings with further study. That is how I found "htop" over top which usually has to be installed.

There is another command that is specific to Elasticsearch and how LogRhythm leverages it. Around the office we call it the "DX Nurse" and it's sort of like an "htop" but for all things Data Indexer in LogRhythm. The syntax of that is below. I think, to me at least, this highlights my preference for commands that give you a lot of information and ability to study how the machine is performing.

```
watch -n5 'curl -s http://localhost:9200/_cluster/health?pretty; echo; curl -s
http://localhost:9200/_cat/nodes?v; echo; curl -s http://localhost:9200/_cat/recovery?v | grep -v
done'
```

Question 3

A customer submits a case and in it states they have reported the issue multiple times over the course of a month (and now their support renewal is on the horizon) and has already spoken to other TSEs w/o receiving a permanent resolution. You have now taken ownership of the latest case regarding this same topic. You have no context for the issue up until now for various reasons. The customer is frustrated that they have to continue spending time working with us while managing internal pressure to fix it. What steps do you take to begin working on this issue for the first time knowing the customer's patience may be limited? What do you say in your initial reply to the customer?

This is actually a situation I am incredibly familiar with handling! At LogRhythm the Premier Services Team started as an experiment to see how we could give that "additional white glove treatment" to customers. This actually morphed over time into being an incredibly skilled team at handling scenarios like the one described above where the customer has a hot temperature, possibly on the fence, and we are doing everything to restore confidence. Rather than explaining "how" I would respond I decided to type an example of my first email because I send items like this daily.

Hey John,

My name is Zack Heaton and I am one of the Senior Technical Support Engineers here at LogRhythm. I want to start this communication with profound gratitude for your patience as we work together to resolve this issue. I have analyzed Company X's Account and I can understand where frustration could possibly grow in this situation. While I cannot assure you of a successful resolution in my first email; I can commit to you my willingness and ability to create next steps. As a Senior I have access to resources x, y, and z which includes my leadership team. Even if I don't personally resolve the technical challenge (more specific in real context); I can assure you I will find out who can and/or what can be done.

Let's start off with a simple diagnosis session. I have read through months of engineer reports on this situation but I would love to get your personal perspective. Are you available at time x,y,z for an hour WebEx Session? If those times do not work can you provide some that do? I am happy and eager to assist you in getting this resolved.

V/r

Zack

Question 4

What criteria do you use for deciding when to escalate a support case either internally or externally to the Support team? Consider the different reasons that a given support case requires escalation and address each of them in your answer.

The criteria I use to decide escalation or not has a standard structure but gets applied to every case for an individual analysis. There are not two accounts that are the same. While I believe in systems that can produce objective next steps; it would be unwise to blindly apply rules to support cases.

The first part that I would like to address is that at LogRhythm there is a differential between "elevation" and "escalation". When it comes to deciding "elevation" this depends on my position. As a TSE the position is about speed and time to resolution. If I cannot personally resolve the case within two hours; it goes to an advanced Engineer. As an Advanced TSE I can say that my rule of thumb was 3-5 hours or until I was out of education on a topic. As a Senior, I have to acknowledge that I am the last line before engineering. My goal is to absolutely one-hundred percent rule out environmental challenges with every account. The items that I elevate to engineering MUST be product issues. Our limited resources as a single company cannot have our engineering team troubleshooting networks and GPOs. The very rare case that this does not happen returns to the 1:1 basis for each case. If the account is in jeopardy then I see it as my responsibility as a Senior TSE to explain this in a clear way to the leadership and account teams. In the end, my goal is to allow us as a company to decide the best path forward rather than me going rogue on my own plan.

“Escalations” work a bit differently. It goes back to the 1:1 evaluation of accounts. I can say this: if everything is a fire then nothing is a fire. Keeping that in mind, it all comes down to prioritization. What is the customer’s temperature? How did their temperature get there? Is this frustration with the product or is this a personal evaluation that they’re simply a hot-head? It’s going to change with every engagement and I see my role as an intelligence gatherer. I then present it in a clean format that the leadership, account team, and I can have productive conversations to resolve.

Question 5

You have just met someone who recently moved to the area, and they have never heard of a peanut-butter & jelly sandwich. How do they go about making one?

An interesting question deserves a thorough answer. In software, I prefer to start my explanations by checking the audience for understanding. The way that I would teach a middle schooler how to make a pb&j is completely different from the way I would teach an adult which is different from the way I would teach in English vs Spanish. There are so many perspectives and they all work in my mind in sync to provide the best output, hopefully without rambling.

Once I figure out whether my new friend understands the concept of a sandwich and or peanut butter and or jelly; I can start to explain the benefits to making the product and what it will accomplish for them. Assuming they are interested (you can lead a horse to water ... .but if it aint thirsty. . .); I would start by explaining that we are going to make food because it is a fantastic idea to do this. On top of being quick and simple; it is absolutely delicious!

Now that we are established on what PB&J, what it can do for us, and our desire to proceed we can get into the decisions that have to be made that will be different with each person. Are we talking white bread, wheat bread, or other bread? Sourdough PB&J sounds gross to me but that doesn’t mean it’s not possible. Are we creamy peanut butter, crunchy, natural, sun butter (allergies), or one of those cool peanut butters from GNC that have crazy protein levels and flavors like hazelnut? The jelly, are we doing grape, strawberry, or some hipster jam? Are there combinations that we haven’t thought of yet? I would then walk through the exact steps to construct the which. Finally I would wrap that up with how we are doing the crusts and whether they’d like water or another drink with it.

I would add a qualifier to the end of this that it would also start with a personal evaluation. If my new friend is stressed out to crazy levels I might not go through all of this and use up their time. I’d have to check their mindset because if you ask a person starving after a 10 mile walk in contrast to a food critic; you’ll get two different answers. If they want me to slap some food together, I can. If they want the PBJ-Hipster Special, I can do that. It all ends with whatever is going to make them happy!