Scenario

Review the following scenario. Then complete the step-by-step instructions.

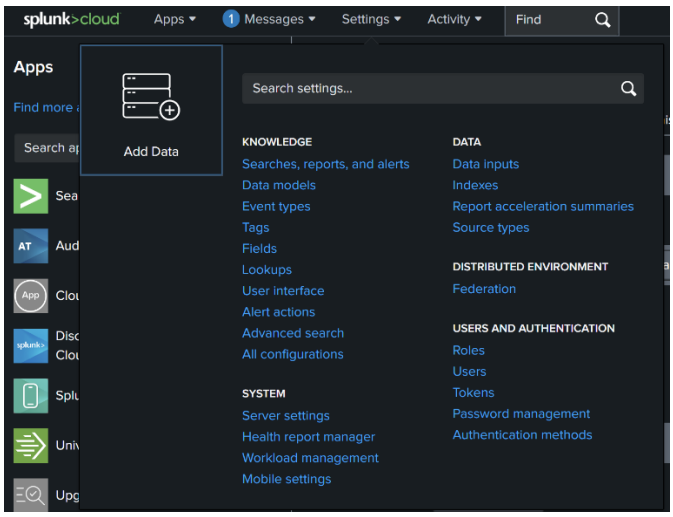
You are a security analyst working at the e-commerce store Buttercup Games. You've been tasked with identifying whether there are any possible security issues with the mail server. To do so, you must explore any failed SSH logins for the root account.

Step 1: Upload data into Splunk

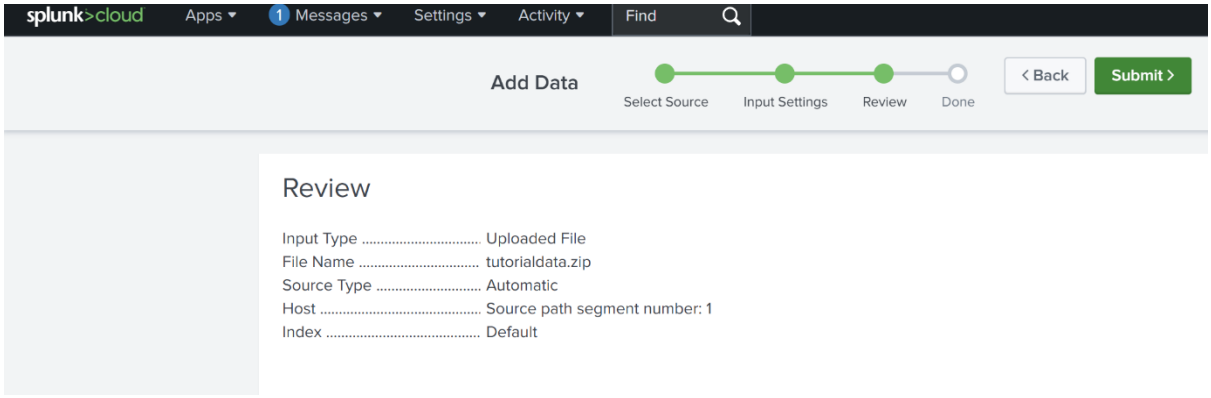
To operate effectively, it's essential that SIEM tools ingest and index data. SIEM tools collect and process data so that it becomes searchable events that can be queried, viewed, and analyzed.

So far, you've created a Splunk account and activated and accessed the Splunk Cloud free trial, but your Splunk Cloud instance does not contain any data. Next, you'll need to upload data into Splunk to start querying. Complete the following steps to upload data into Splunk:

1. If you haven't already, download the data file from Step 1: tutorialdata.zip. Click the link then click the download icon. Do not uncompress the file.
2. Navigate to Splunk Home from your Splunk Cloud free trial instance. You might need to log in again using your credentials from Step 3.
3. On the Splunk bar, click **Settings.** Then click the **Add Data** icon.



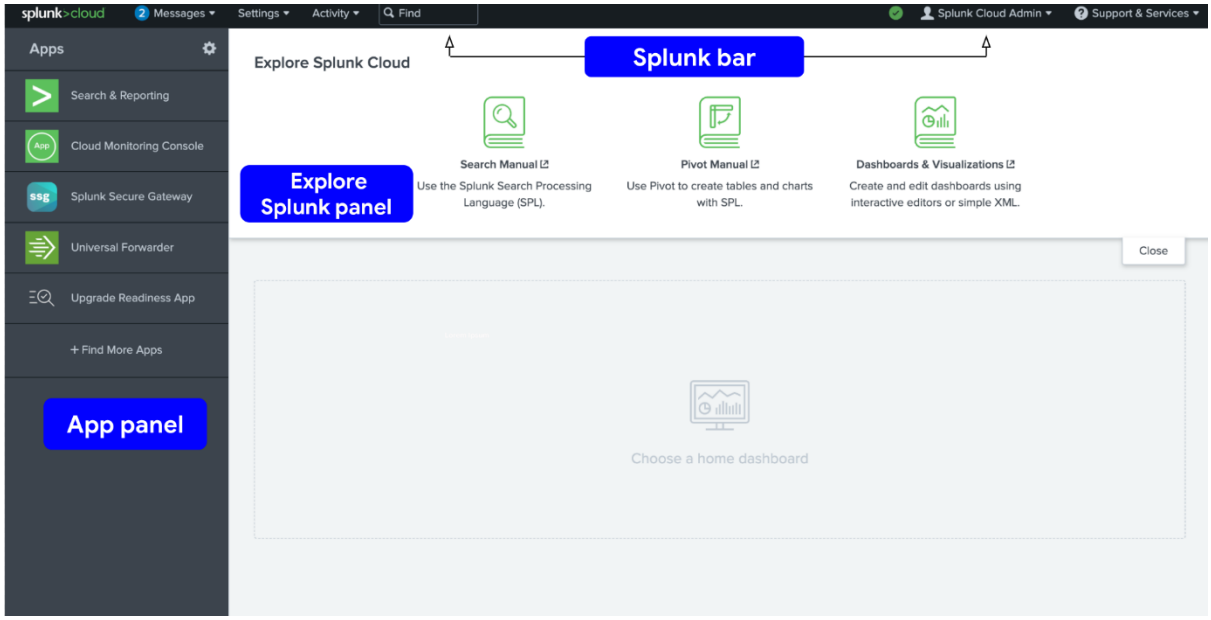
4. Click **Upload**.
5. Click the **Select File** button.
6. Upload the **tutorialdata.zip** file, and click **Open**.
7. Click the **Next** button to continue to **Input Settings**.
8. By the **Host** section, select **Segment in path** and enter **1** as the segment number.
9. Click the **Review** button and review the details of the upload before you submit. The details should be as follows: Input Type: Uploaded File File Name: tutorialdata.zip Source Type: Automatic Host: Source path segment number: 1 Index: Default



10. Click **Submit**. Once Splunk has ingested the data, you will receive confirmation that the file was successfully uploaded.

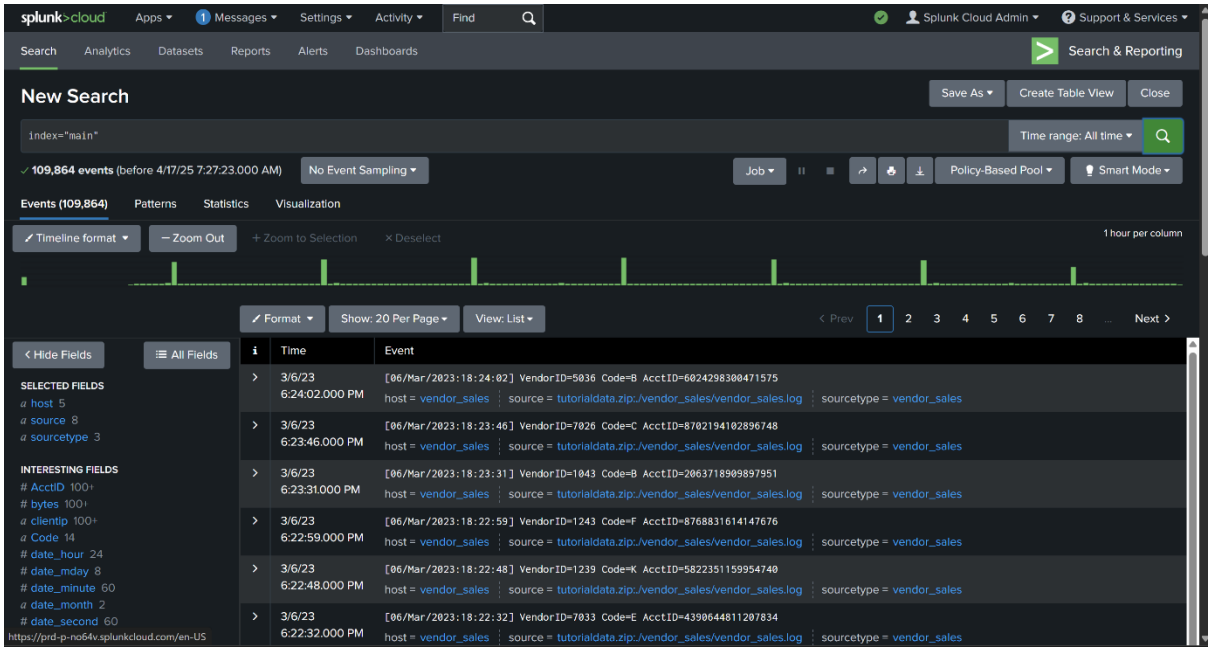
Step 2: Perform a basic search

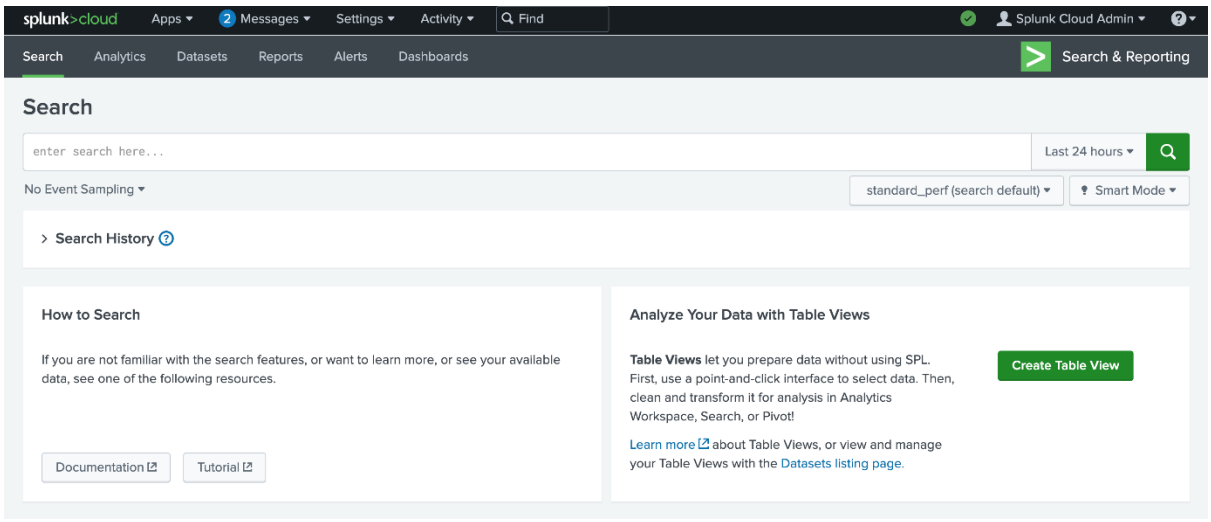
Take a moment to examine the Splunk Cloud interface by locating the app panel, the Explore Splunk panel, and the Splunk bar.



Now that you've uploaded the data into Splunk, perform your first query to confirm that the data has been ingested, indexed, and is searchable. Follow these steps to perform a query:

1. Navigate to Splunk Home. (To return to Splunk Home, click the Splunk Cloud logo on the Splunk Cloud page.)
2. Click **Search & Reporting**. You may close any pop ups that appear.
3. In the search bar, enter your search query: **index="main"** This search term specifies the index. An **index** is a repository for data. Here, the index is a single dataset containing events from an index named main.
4. Select **All Time** from the time range dropdown to search for all the events across all time.
5. Click the search button. Note that the search button is represented by the magnifying glass icon. Your search should retrieve thousands of events.

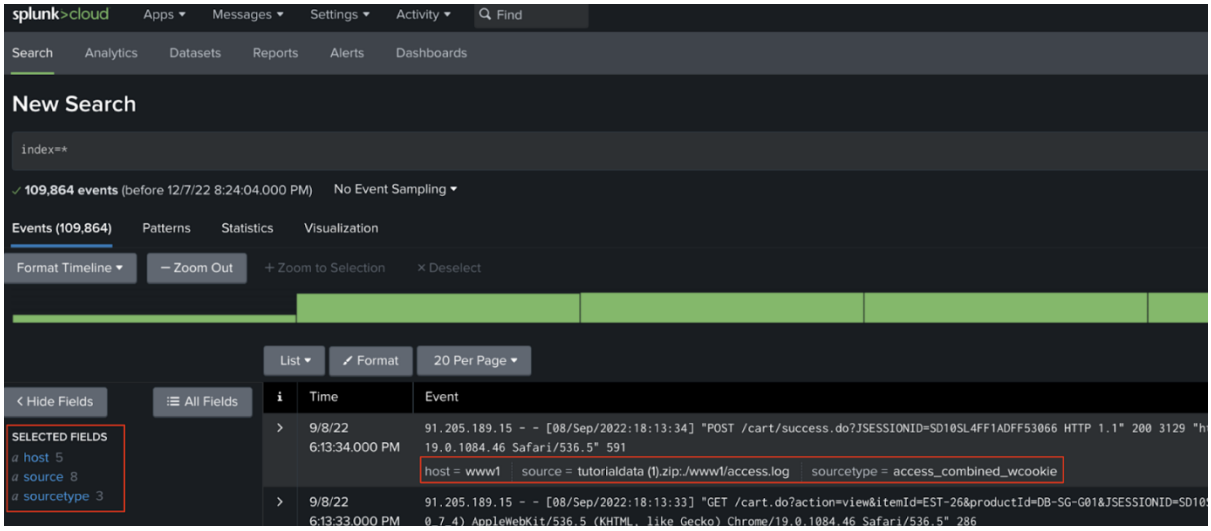

splunk>cloud
Apps
Messages
Settings
Activity
Find
Splunk Cloud Admin
Support & Services
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
New Search
Save As
Create Table View
Close
index="main"
Time range: All time
109,864 events (before 4/17/25 7:27:23.000 AM)
No Event Sampling
Job
Policy-Based Pool
Smart Mode
Events (109,864)
Patterns
Statistics
Visualization
Timeline format
Zoom Out
Zoom to Selection
Deselect
1 hour per column
Format
Show: 20 Per Page
View: List
Prev
1 2 3 4 5 6 7 8
Next
Hide Fields
All Fields
SELECTED FIELDS
a host 5
a source 8
a sourcetype 3
INTERESTING FIELDS
AcctID 100+
bytes 100+
a clientip 100+
a Code 14
date_hour 24
date_mday 8
date_minute 60
a date_month 2
date_second 60
Time
Event
3/6/23 6:24:02.000 PM
[06/Mar/2023:18:24:02] VendorID=5036 Code=B AcctID=6024298300471575
host = vendor_sales source = tutorialdata.zip:./vendor_sales/vendor_sales.log sourcetype = vendor_sales
3/6/23 6:23:46.000 PM
[06/Mar/2023:18:23:46] VendorID=7026 Code=C AcctID=8702194102896748
host = vendor_sales source = tutorialdata.zip:./vendor_sales/vendor_sales.log sourcetype = vendor_sales
3/6/23 6:23:31.000 PM
[06/Mar/2023:18:23:31] VendorID=1043 Code=B AcctID=2063718909897951
host = vendor_sales source = tutorialdata.zip:./vendor_sales/vendor_sales.log sourcetype = vendor_sales
3/6/23 6:22:59.000 PM
[06/Mar/2023:18:22:59] VendorID=1243 Code=F AcctID=8768831614147676
host = vendor_sales source = tutorialdata.zip:./vendor_sales/vendor_sales.log sourcetype = vendor_sales
3/6/23 6:22:48.000 PM
[06/Mar/2023:18:22:48] VendorID=1239 Code=K AcctID=5822351159954740
host = vendor_sales source = tutorialdata.zip:./vendor_sales/vendor_sales.log sourcetype = vendor_sales
3/6/23 6:22:32.000 PM
[06/Mar/2023:18:22:32] VendorID=7033 Code=E AcctID=4390644811207834
host = vendor_sales source = tutorialdata.zip:./vendor_sales/vendor_sales.log sourcetype = vendor_sales
https://prd-p-no64v.splunkcloud.com/en-US


splunk>cloud
Apps
Messages
Settings
Activity
Find
Splunk Cloud Admin
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Search
enter search here...
Last 24 hours
No Event Sampling
standard_perf (search default)
Smart Mode
Search History
How to Search
If you are not familiar with the search features, or want to learn more, or see your available data, see one of the following resources.
Documentation
Tutorial
Analyze Your Data with Table Views
Table Views let you prepare data without using SPL. First, use a point-and-click interface to select data. Then, clean and transform it for analysis in Analytics Workspace, Search, or Pivot!
Create Table View
Learn more about Table Views, or view and manage your Table Views with the Datasets listing page.

Step 3: Evaluate the fields

When Splunk indexes data, it attaches fields to each event. These fields become part of the searchable index event data. This helps security analysts easily search for and find the specific data they need. Now that you've run your first query, examine the search results and the fields.

For each event the fields are **host**, **source**, and **sourcetype**. Under **SELECTED FIELDS**, examine the same fields.



Examine the field values by clicking on the field under **SELECTED FIELDS**. You should observe the following:

- **host**: The host field specifies the name of the network host from which the event originated. In this search there are five hosts:
    - **mailsv** - Buttercup Games' mail server. Examine events generated from this host.
    - **www1** - This is one of Buttercup Games' web applications.
    - **www2** - This is one of Buttercup Games' web applications.
    - **www3** - This is one of Buttercup Games' web applications.
    - **vendor_sales** - Information about Buttercup Games' retail sales.
- **source**: The source field indicates the file name from which the event originates. You should identify eight sources. Notice **/mailsv/secure.log**, which is a log file that contains information related to authentication and authorization attempts on the mail server.

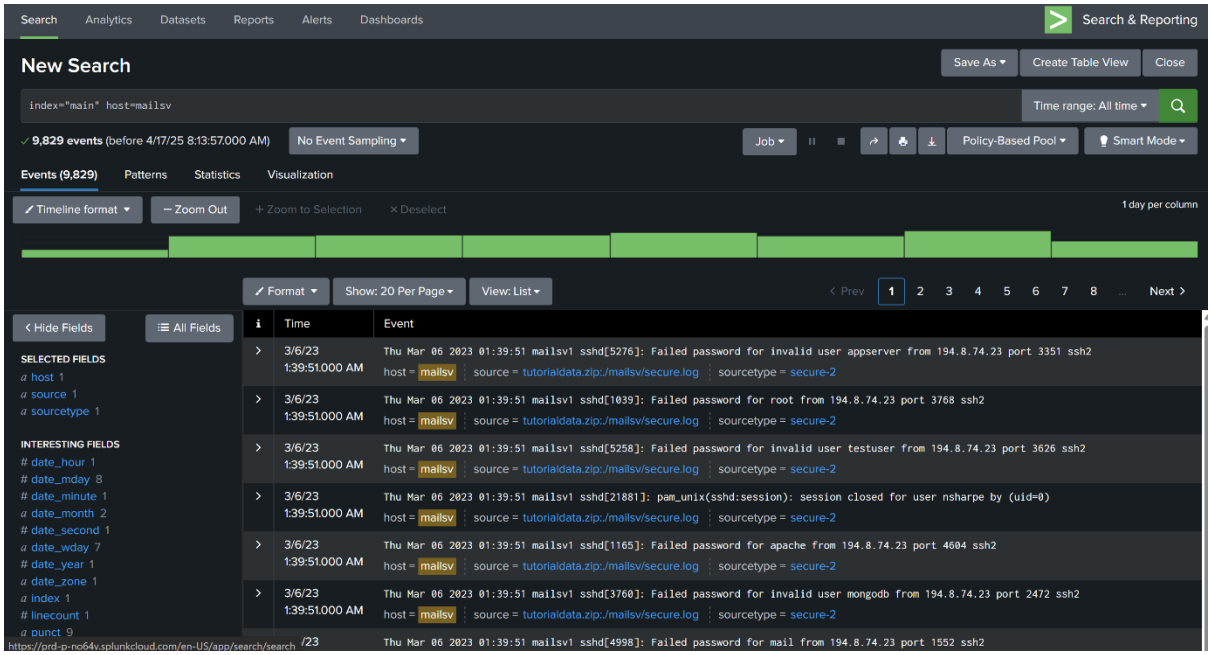
- **sourcetype**: The sourcetype determines how data is formatted. You should observe three sourcetypes. Examine **secure-2**.

Step 4: Narrow your search

Because you've been tasked with exploring any failed SSH logins for the root account on the mail server, you'll need to narrow the search results for events from the mail server.

Under **SELECTED FIELDS**, click **host** and click **mailsv**.

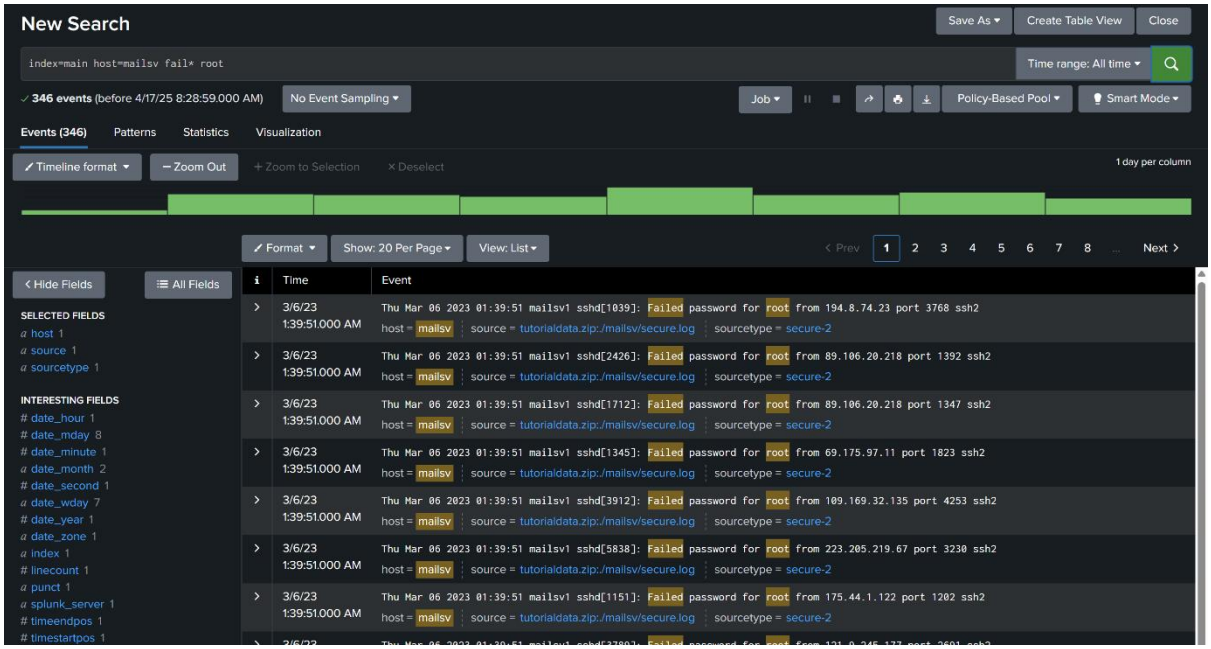
Notice that a new term has been added to the search bar: **index=main host=mailsv**. The search results have narrowed to over 9000 events that are generated by the mail server.



Step 5: Search for a failed login for root

Now that you've narrowed your search results to events generated by the mail server, continue to narrow the search to locate any failed SSH logins for the root account.

1. Clear the search bar.
2. Enter **index=main host=mailsv fail* root** into the search bar. This search expands on the search from the previous task and searches for the keyword **fail***. The wildcard tells Splunk to expand the search term to find other terms that contain the word *fail* such as *failure*, *failed*, etc. Lastly, the keyword **root** searches for any event that contains the term root.
3. Click **search**.



Step 6: Evaluate the search results

Your search from the previous task should have retrieved search results for over 300 events. Navigate to other pages of the search results to observe the events not listed on the first page of results.

- **Over 100,000** events are contained in main index across all time
- **Host** field identifies the name of a network device/system from which event originates
- **Vendor_sales** contains log information relevant to financial transactions
- **346 Failed SSH logins** are found in the root account on mail server