**8. Whitelisting Alerts in AWS GuardDuty**

--- Reference (GuardDuty Alert Lists) - <https://docs.aws.amazon.com/guardduty/latest/ug/guardduty_finding-types-active.html>

**Handling Guard Duty Alerts**

--- Amazon GuardDuty can generate a wide variety of alerts.

--- Some of these might be true but you might want to ignore them.

--- Example:

* + There is a central Security server that performs port-scans as part of penetration testing on all the production servers.
  + This can lead to GuardDuty alerts like port scans or brute force being triggered.

--- **note** - in order to distinguish between a genuine one and the real one, there are certain ways in which you can handle the alert. one of the ways that can be used is to manage a trusted IP list. the guard duty allows customers to add their own trusted IP list.

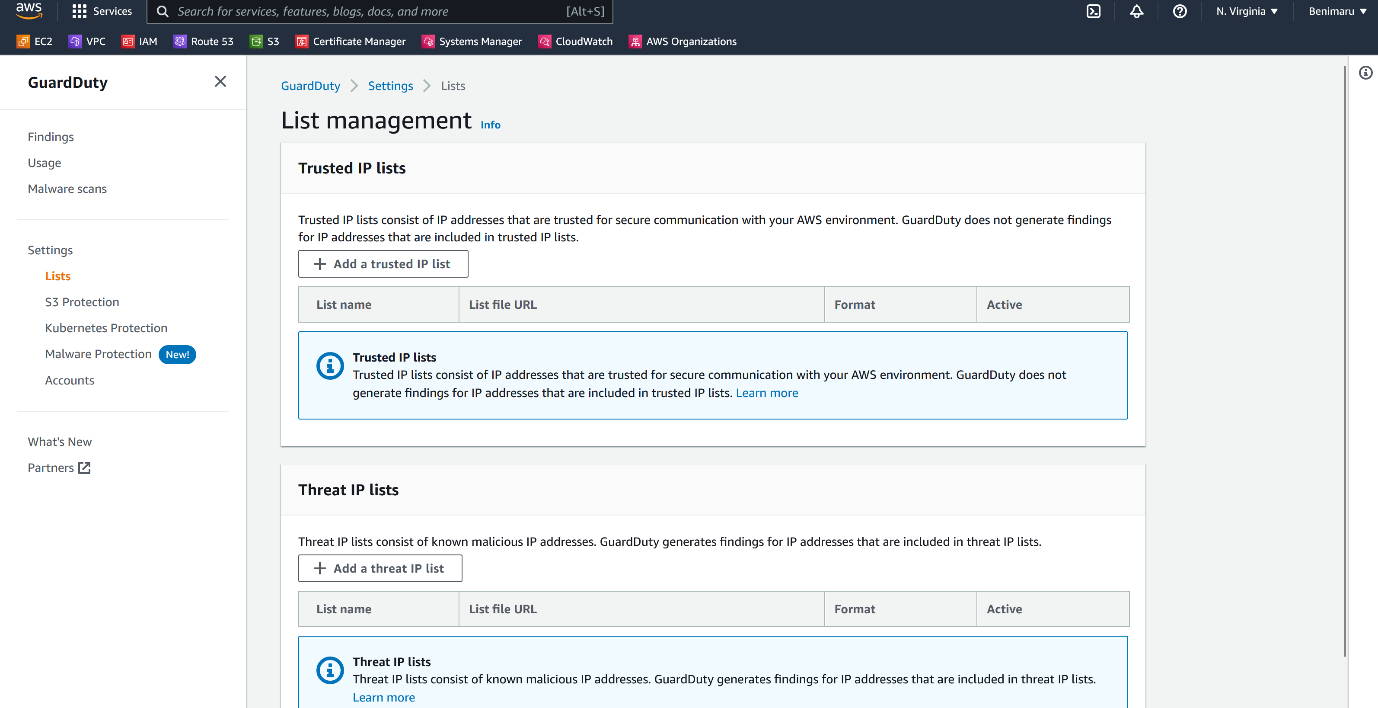
**Managing Trusted IP List**

* AWS GuardDuty allows customers to add their own “Trusted IP” list.
* GuardDuty does not generate findings for IP addresses on trusted IP lists.
* Example Trusted IP List:

116.75.25.50/32

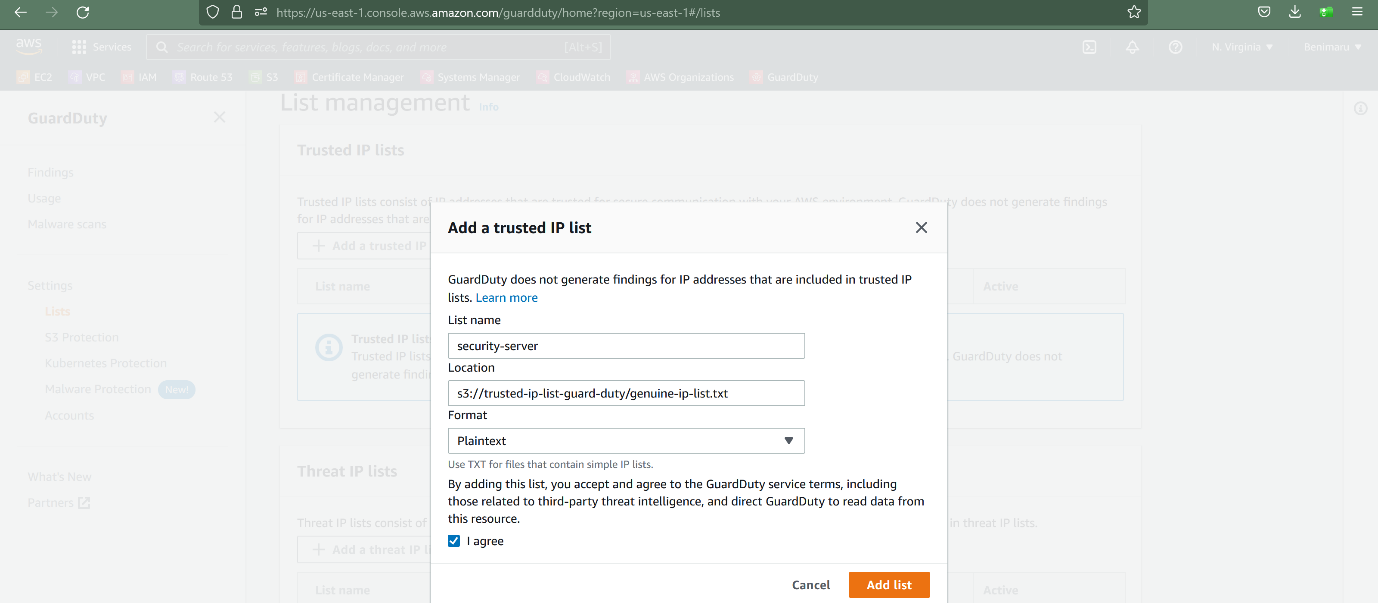
**Guard duty**

--- go to aws guard duty console.

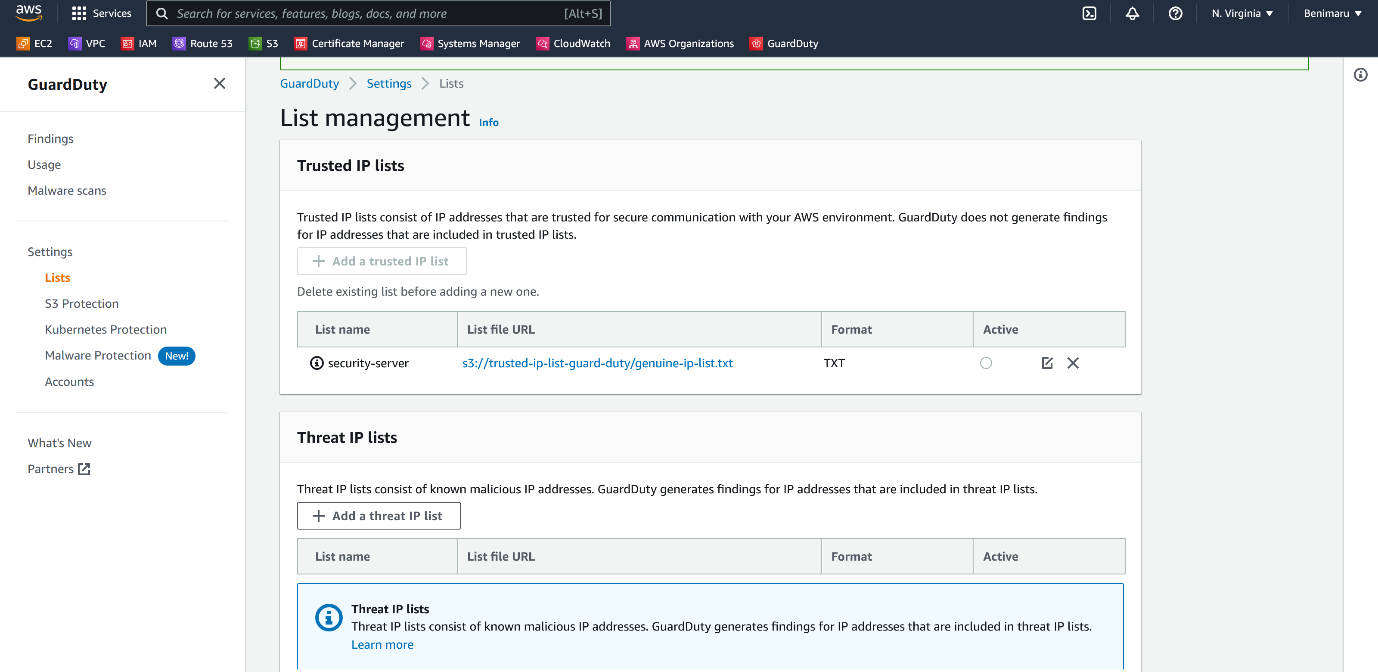


--- click on lists.

--- click on add a trusted ip list.



--- click on add list.



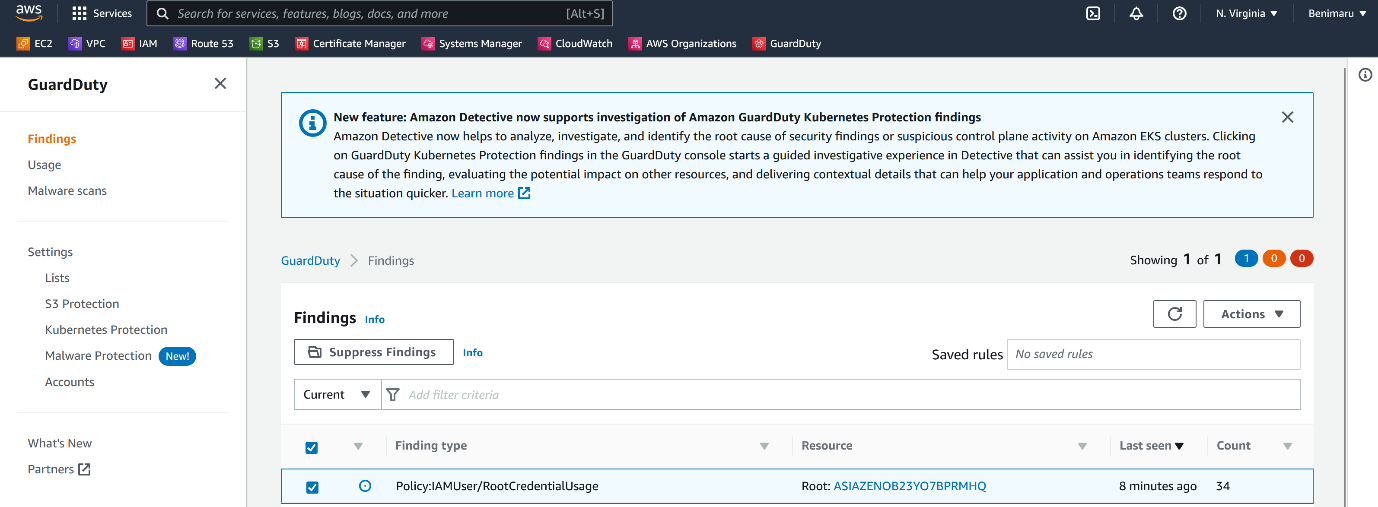
--- trusted ip list successfully added.

--- note – click on activate.

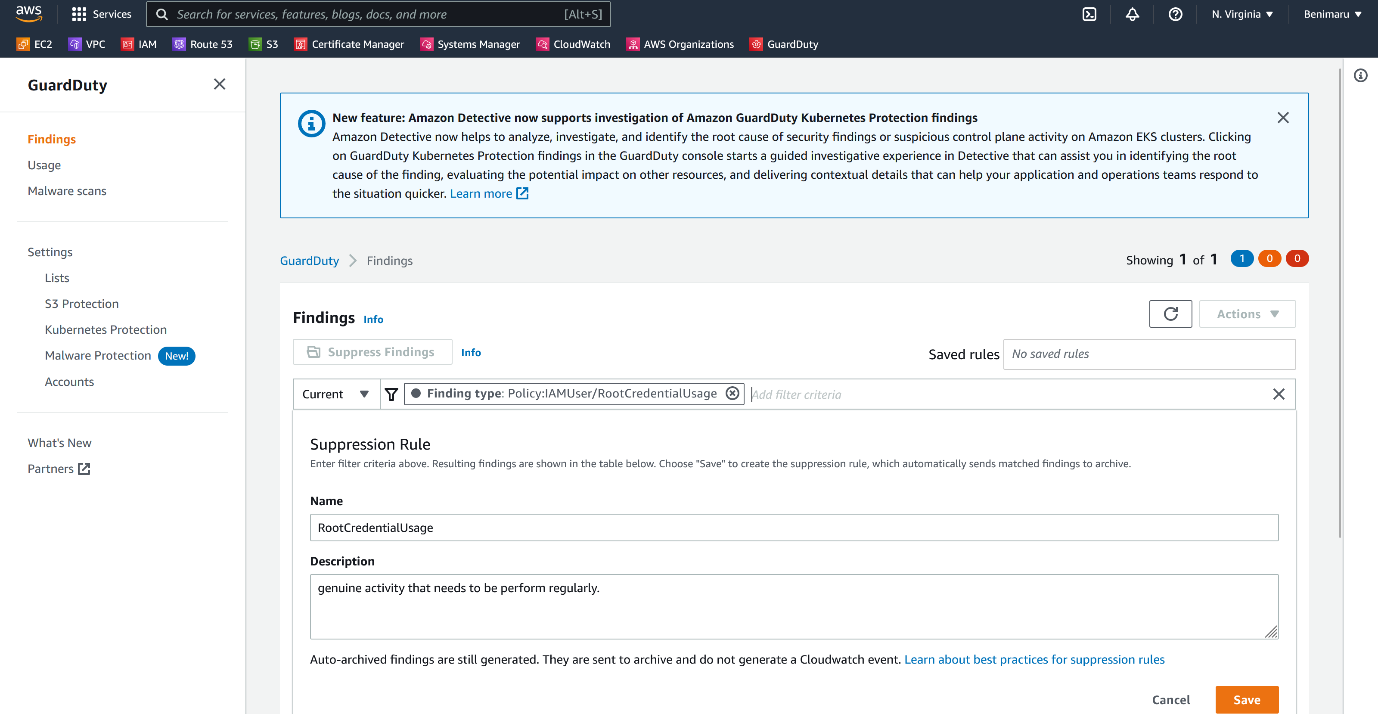
--- **important** - In a similar way, you can also add a threat ip list where if you know that there are certain IP addresses that have been known to attack your servers, you can add them within that threat list.

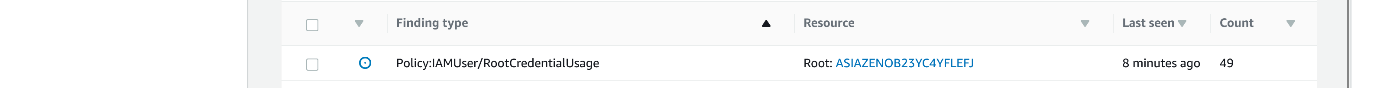
**Supress findings**

--- click on findings.



--- click on suppress findings.





--- **note** - in current – select finding type, then paster finding type.

--- click on save.

--- **note** - you have basically suppressed these types of findings from appearing.