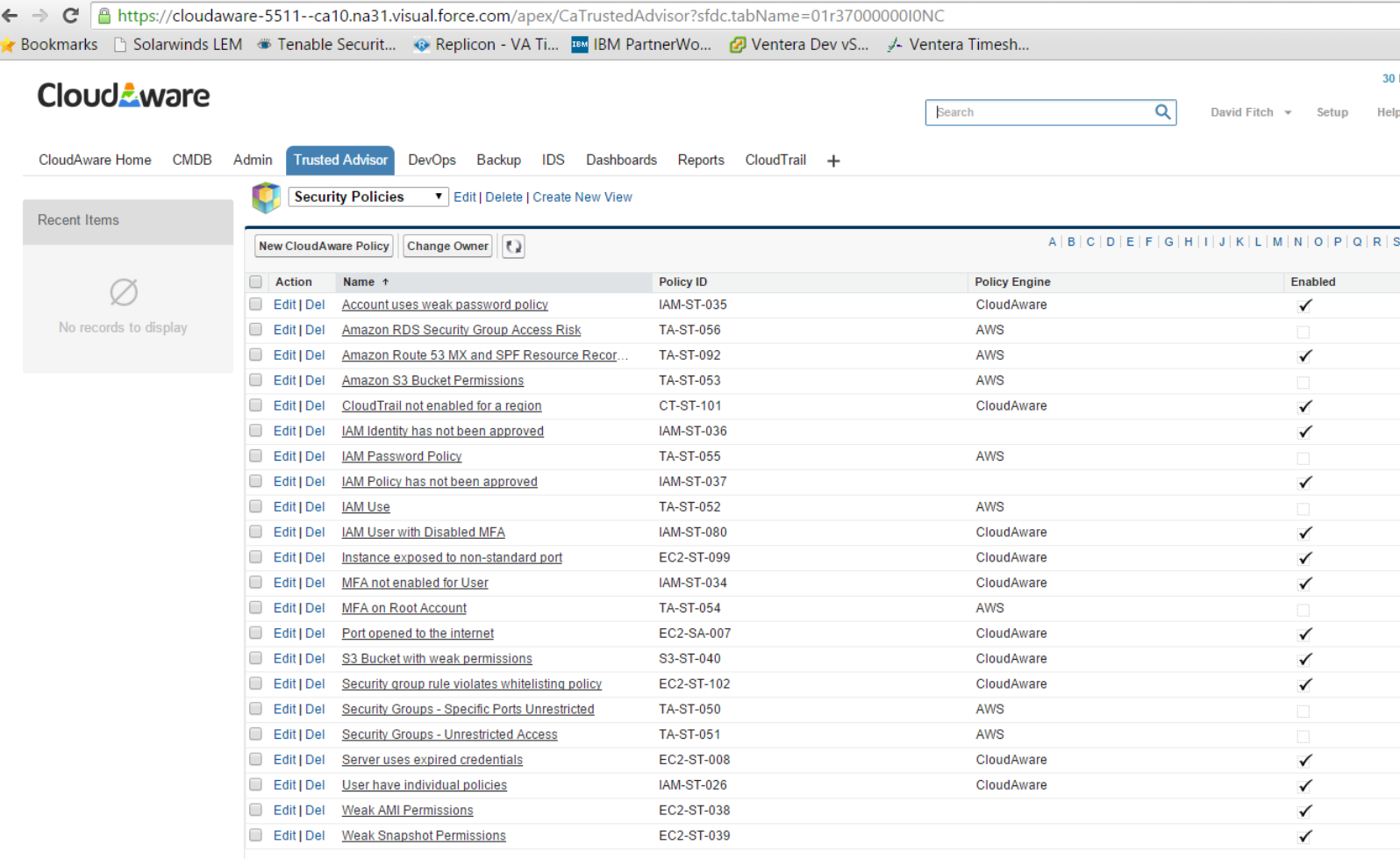
The Ventera team has taken a 3-pronged approach to Continuous Monitoring: CloudAware, CloudWatch, and Monit. This document contains evidence demonstrating how we are ensuring the integrity and availability of the system.

1. **Cloud Aware**

Ventera is using CloudAware for continuous monitoring of our application to ensure that the confidentiality, integrity, and availability of the application is maintained as needed to meet its system categorization (FISMA Low). Because the application is hosted on the AWS Cloud, we would use the CloudAware FedRAMP Continous Monitoring module after a provisional FedRAMP authorization is received to ensure that the security posture and situational awareness of the application is maintained and risk is managed and reduced to acceptable levels. The CloudAware service is also fully supported in the AWS GovCloud region. As part of a typical deployment, information from other security tools and systems such as vulnerability management, patch management, event management, incident management, malware detection, asset management, configuration management, software assurance, etc. would also feed into the continuous monitoring system so that risk to the application and the overall organization can be managed effectively. Below is a screenshot which shows Cloudaware configured for our application:



1. **Monit – Continuous Integration**

Monit (<https://mmonit.com/monit/>) is a small open source utility used to manage and monitor Unix-based systems. Monit is installed and configured on both the Test/Production Servers, and is mainly used for monitoring the Apache HTTP (web) servers. Monit has been configured to start/restart each Apache server, in situations where a server was not started correctly or the application cannot be accessed. Equally, if the server fails to start five times consecutively, Monit will halt the server process. If this situation did occur, Amazon Web Services (AWS) CloudWatch could allocate additional resources to meet the load demand.

**Monit configuration file for Apache HTTP Servers**

*check process apache*

*with pidfile "/opt/bitnami/apache2/logs/httpd.pid"*

*group apache*

*start program = "/opt/bitnami/apache2/scripts/ctl.sh start" with timeout 90 seconds*

*stop program = "/opt/bitnami/apache2/scripts/ctl.sh stop" with timeout 90 seconds*

*if DOES NOT exist then start*

*if failed port 80 protocol HTTP request "/web/index.html" then restart*

*if 5 restarts within 5 cycles then timeout*

**Monit Output and Evidence**

*: monit daemon with PID 3797 awakened*

*: 'apache' monitor action done*

*: 'apache' process is not running*

*: 'apache' start: /opt/bitnami/apache2/scripts/ctl.sh*

*: 'apache' process is running with pid 3900*

*: monit summary*

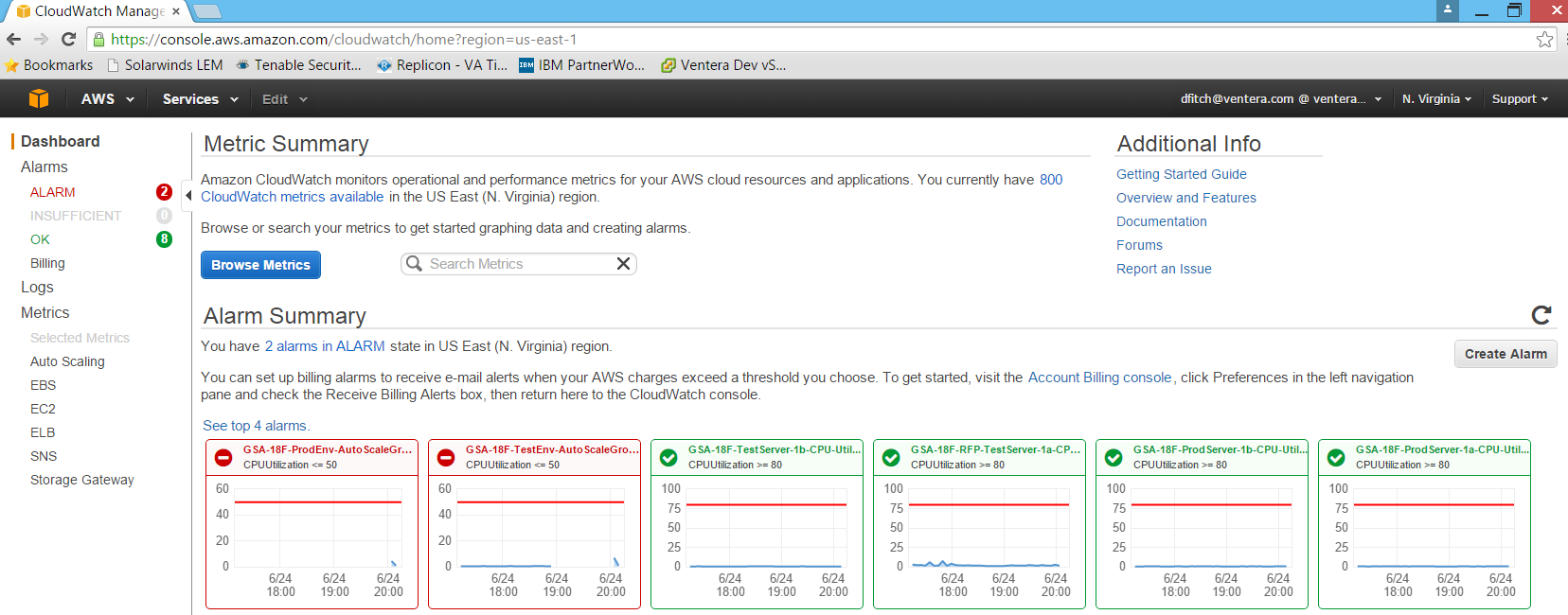
*The Monit daemon 5.6 uptime: 8m*

*Process 'apache' Running*

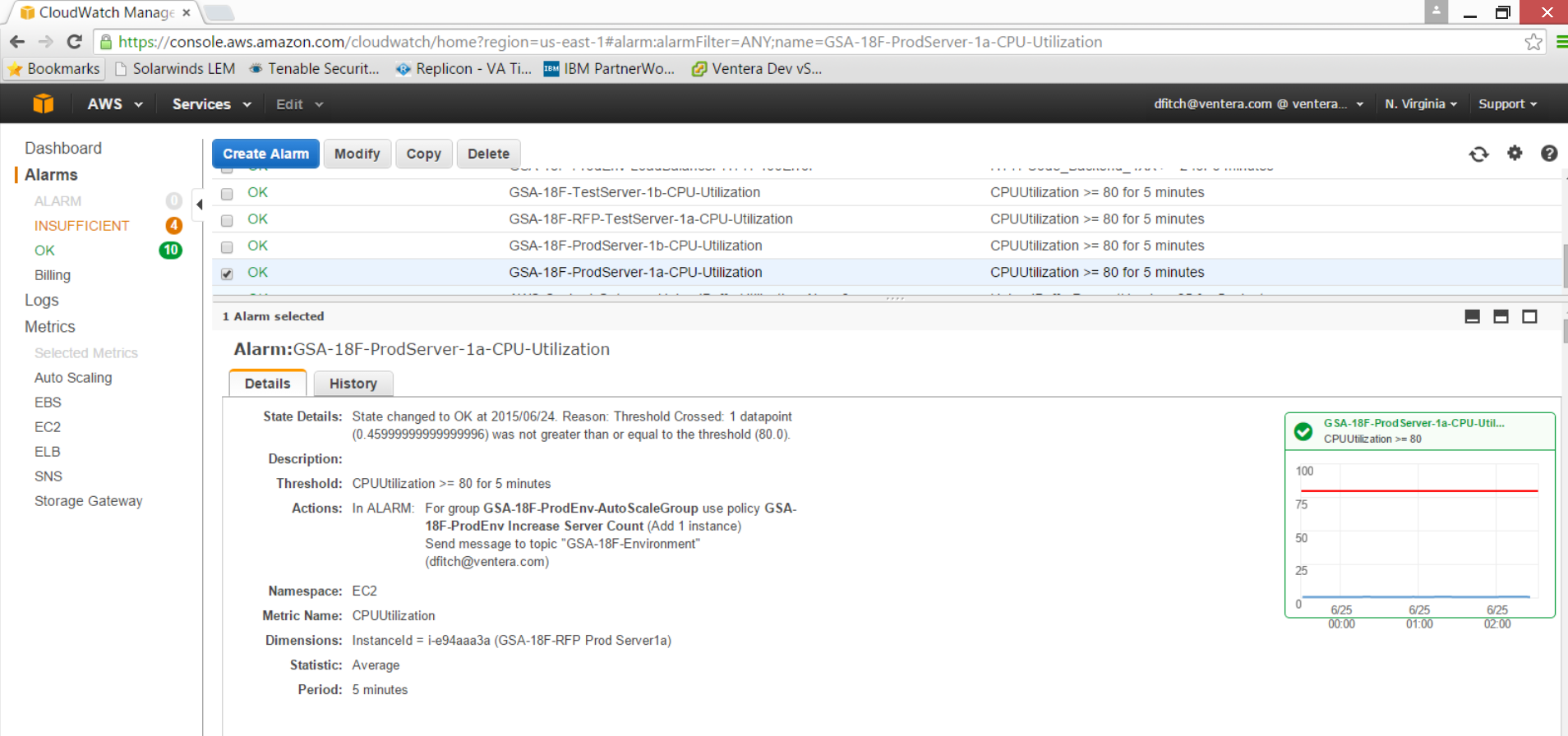
*System 'ip-XXX-XX-X-XX' Running*

1. **CloudWatch**

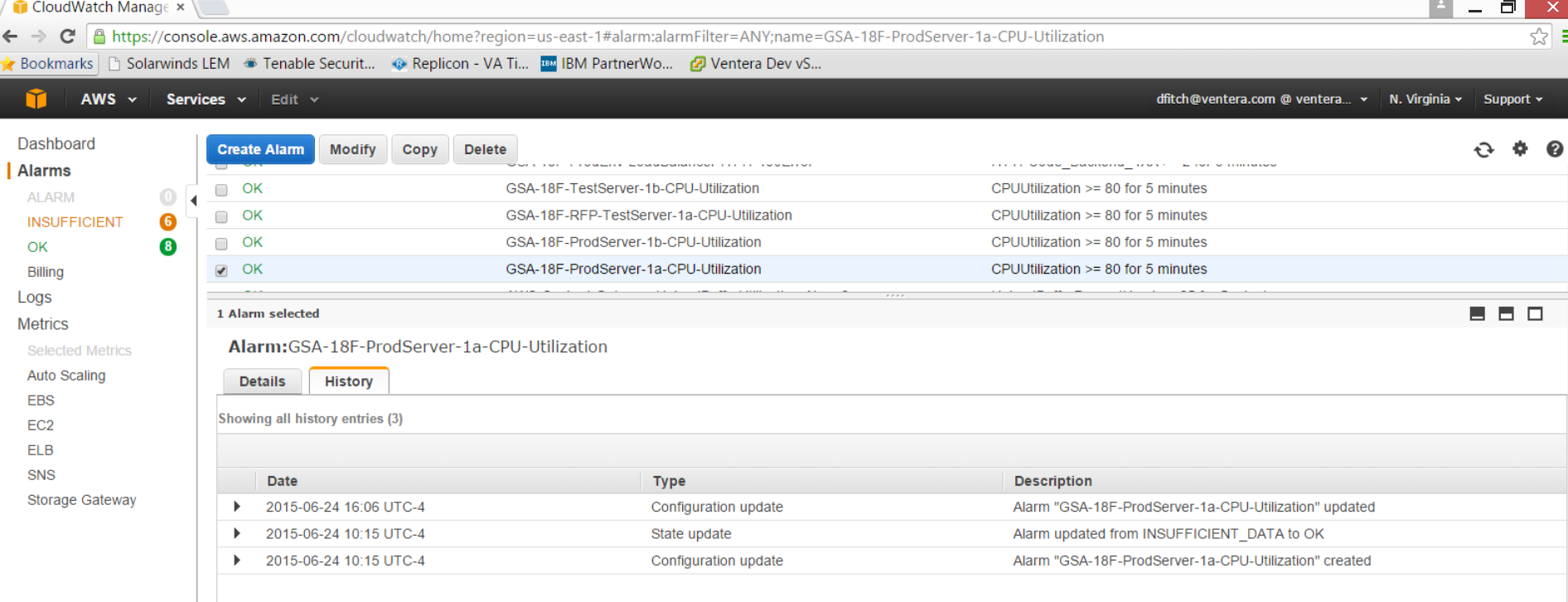
Summary of Alarms for Test and Production Server CPU Utilization and Auto Scale Groups in AWS:



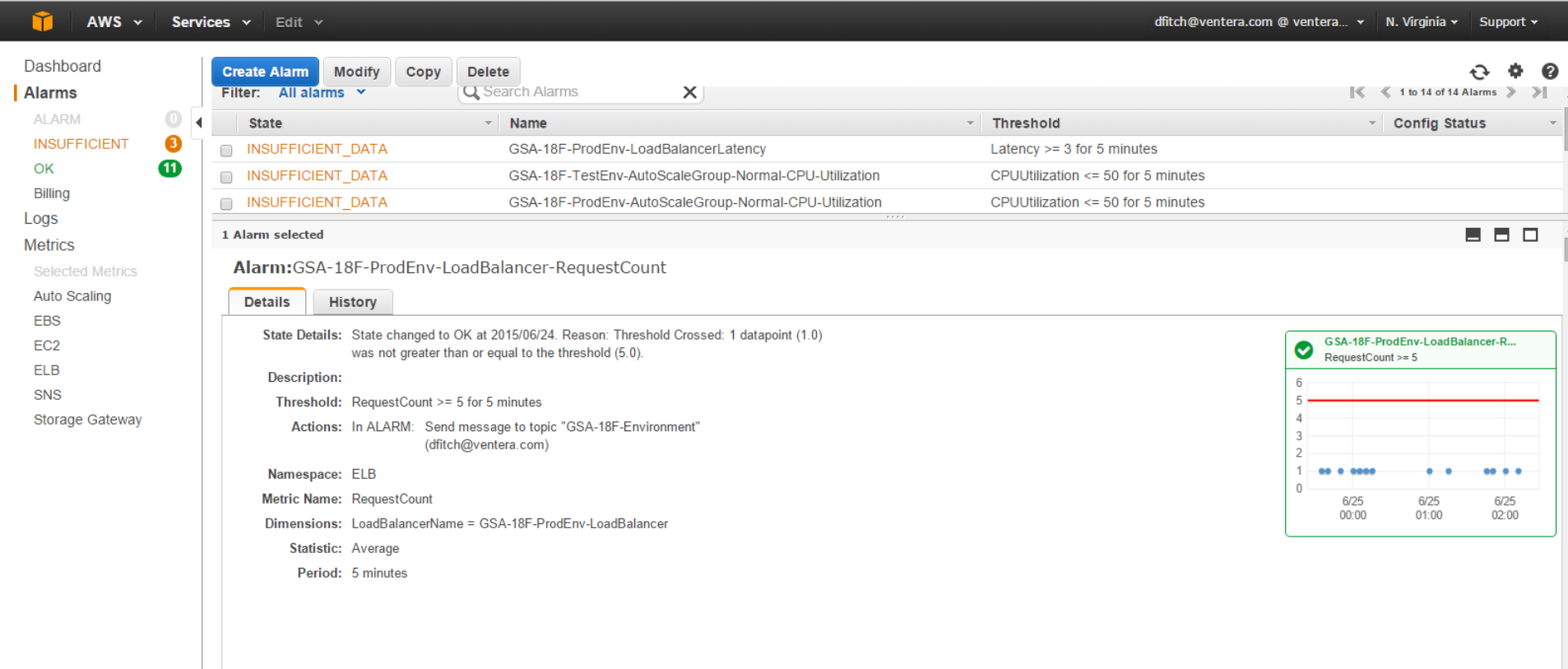
Details of Alarm for Production Environment Server CPU Utilization:



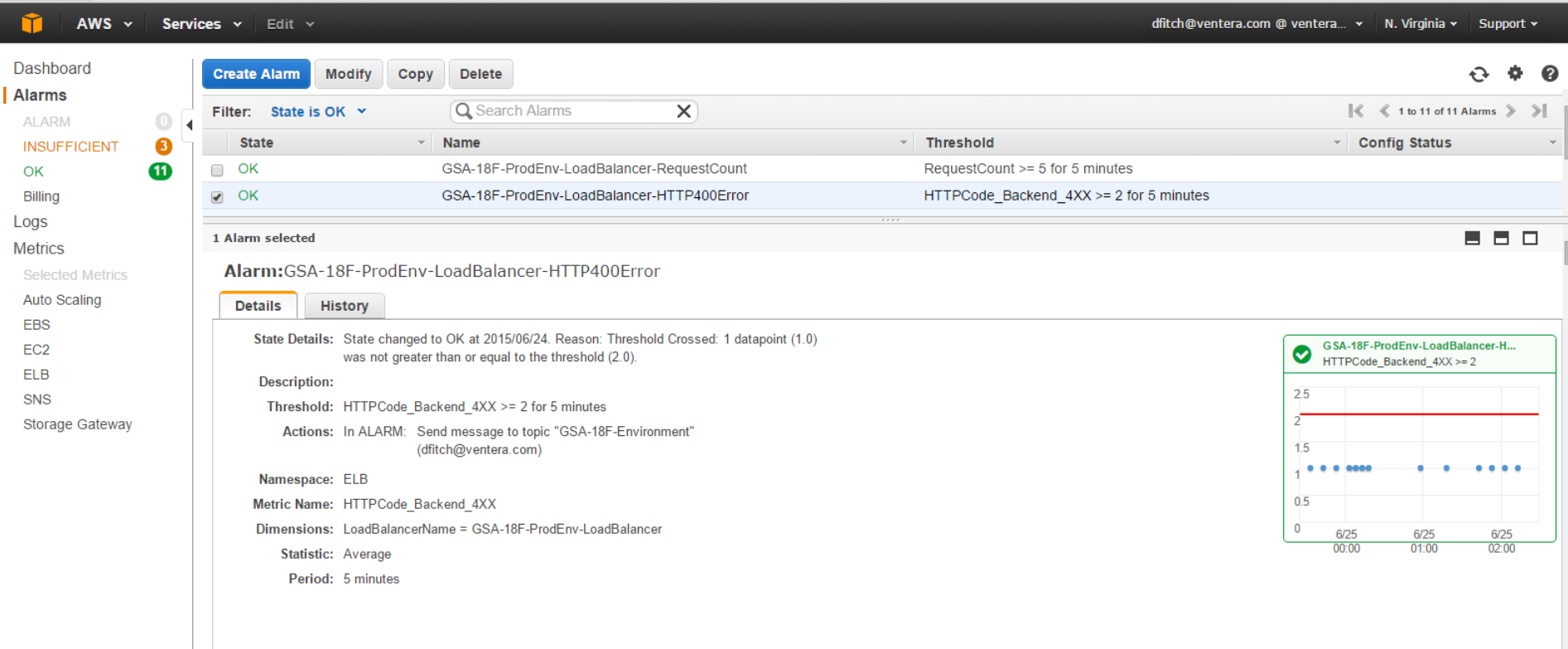
History of Alarm for Production Server CPU Utilization:



Monitoring and Details of Alarm for Production Environment Load Balancer Request Count:



Details of Alarm for Production Environment Load Balancer HTTP 4XX Error Codes:



History of Alarm for Production Environment Load Balancer HTTP 4XX Error Codes:

