Rally Software
ca technologies A Broadcom Company

Root Cause Analysis:
Outage due to auto-patching

The following is a detailed accounting of the service outage that Rally users experienced on October 4th, 2019.

Root Cause Analysis Summary

Event Date	10/4/2019
Event Start	3:12am MDT
Time Detected	3:19am MDT
Time Resolved	4:39am MDT
Event End Time	4:57am MDT
Root Cause	Our DNS hosts all scheduled a normal reboot for security patches, resulting in a simultaneous outage of all DNS servers in our environment. As a result, all connections between all hosts in our environment failed due to DNS lookup issues. We were down for long enough that all reconnects between services and data stores broke, and our services were hard down. We investigated the confusing outage symptoms, and brought up all services.
Customer Impact	● Site was down for approximately one hour ● Authentication service was down for a longer period ● Most recent analytics data was not ingested in a timely fashion. 17 workspaces had stale data until resolved later in the morning ● 2 support cases logged

Future Preventative Measures

Actions that should be taken to prevent this Event in the future.

Actions	Description
Quick restart playbook	Document quick ALM roll script and provide examples of when it should be used
Remove automated reboots for Windows hosts	Stop the servers from rebooting automatically, and add them back into the monthly patching stories.
Additional redundancy	Have one off DC AD as a redundancy for DNS. Add a domain controller in opposite datacenter to the resolvers on our linux hosts.
Documentation update	Update windows configuration documentation to include disabling automatic reboots