VPN Authentication

Problem Impact Analysis

Event Occurrence: 2018-03-26

Background

Set the context for the service and the value it provides.

OIT-Security provides an authentication, authorization, and accounting (AAA) service to a number of customer facing network devices that support well known functions such as VPN, WiFi (eduroam, UAlaska), etc.

Recently the AAA-service was adjusted, as part of a strategic realignment (i.e. retire edir), to use Active Directory as the store for credentials. This adjustment entailed a major software upgrade and re-configuration.

Break Down of the Problem

Describe the problem and the impact and scope of said problem.

There were at least two primary problems.

a. Customer VPN login attempts were not successful even when the correct username and password were supplied, and the customer was a member of the correct group that granted authorization. No reason or error was logged for the unsuccessful authentication / authorization attempt.

b. The VPN concentrators were internally marking AAA-servers as “dead” due to AAA-server response-latency. When all AAA-servers were marked dead, the VPN concentrators entered a cool down period of no less than sixty seconds where all authentication attempts were failed internally by the vpn concentrators (without being sent to the AAA-service). Since the AAA-servers were not responding within the timeout configured on the vpn concentrators, all AAA-servers were frequently being marked dead. It is unknown how many sessions the vpn concentrators rejected because the AAA-subsystem within the vpn concentrator software was in a cool down state; there were 2,538 timeout warnings in the vpn concentrator logs.

Target State / Goal

What is the desired future state. (What will prevent this from occurring in the future?)

Unsuccessful authorizations via ldap should log an error or reason. Network equipment should be updated with longer timeouts and AAA-service should attempt to respond within these timeouts regardless of ldap authorization issues. Status of AAA should be monitored on network equipment.

Root Cause Analysis

Describe details of what happened. Use a common analysis tool, i.e. 5 Whys, Fishbone, etc.

It appears that the ldap authorization response latency spiked beyond the timeout configured in each of the AAA-server’s internal load-balancers. The internal load-balancer was responsible for ensuring the AAA-server instance always reached a living AD DC. As a result of exceeding the timeout interval, the internal load-balancer would have marked all AD DC’s dead one after the next, however the logging level needed to understand the specifics was not enabled. The AAA-service opens a pool of connections in order to handle a large number of requests per second. Due to the high turn over of pool connections, due to lack of connection being available, back-off behavior appears to have also been triggered in the AAA-service which further increased the response latency.

Develop Countermeasures

What specific action items will be done to reach the Target State / Goal?

1. Configure the ldap module to log a reason or error for all unsuccessful authorizations.
2. Increase vpn concentrator AAA timeout: 5 seconds → 10 seconds.
3. Configure strict timeouts in the AAA-service for ldap authorization. Network connection: 1 second max. Server-side processing: 3 seconds max. Query response: 6 seconds max.
4. It may be prudent to monitor the AAA-subsystem within each networking device for indications that timeouts are causing customer facing problems.
5. Remove internal load-balancer from the AAA-server configurations in favor of *auth.alaska.edu*.
6. Request guidance as to what availability and latency may reasonably be expected from the credential and authorization store, in order to further improve timeouts.

Implementation of Countermeasures

When will action items be implement?

OIT-Security completed items 1, 3, and 5 Monday, March 26th.

OIT-Telecommunications, for item 2, indicated Monday, March 26th, that the timeout configuration on vpn concentrators had been updated.

Items 4 and 6 are TBD.

Follow Up / Review

Goals dates to follow up on implementation of countermeasures, and what specifically you are reviewing.

Configuration changes to reduce and appropriately communicate issues arising ldap connectivity were implemented the same day as the problem surfaced by the groups noted in the aforementioned implementation section.

Items 4 and 6 are TBD.