CA Advanced Authentication version 8.1 Performance Test Brief

Dec 21, 2015

Introduction

Enterprises today are faced with a dilemma. How do they enable access to their users from anywhere on any device thereby enhancing user convenience while lowering security risk and keeping costs in check? CA Advanced Authentication offers a flexible and scalable solution that incorporates behavior and credential based authentication methods that allows enterprises to meet regulatory requirements in authenticating employees, partners and consumers while providing a simple user experience, higher security and lower total cost of ownership (TCO). The solution covers both conventional use cases like web portals, VPN and the rapidly expanding user cases of Mobile and IoT.

The purpose of this report is to assess the performance capability of CA Advanced Authentication Server 8.1 Release.

Performance Factors

The two most important performance factors in an authentication solution are scalability and latency. Scalability is the ability of the server to provide service that scales to millions of users with minimal/acceptable impact on response time. Latency describes the delay as introduced in the system by the different components that make up the authentication service.

CA Advanced Authentication Server provides excellent horizontal and vertical scalability through increasing the number of server instances and the memory[1], disk and processing speed of each instance. It achieves full-featured horizontal scalability and low latency by using the following techniques

Stateless Servers

CA Advanced Authentication Servers eliminate the need to store state information on any server instance, allowing deployments behind load balancers. In addition to providing scalability this deployment configuration also provides high availability.

Connection Pooling

CA Advanced Authentication Server uses proprietary connection pooling technology to avoid expensive connects and reconnects to database servers, crypto devices, and remote servers

Data cache

Accessing the database is much slower than accessing local memory. The CA Advanced Authentication Server caches often-used data to minimize database interactions.

Optimized database interface

Inefficient database interaction can cause even the fastest software to a crawl. CA Advanced Authentication Server has highly optimized database schemas and SQL statements that allow exceptionally efficient database interactions.

[1] Note, the CA Advanced Authentication servers are delivered as 32-bit applications and thus subject to a 4 GByte memory limit. We plan in a future release to switch to 64-bit, however at present we do not find the 4 Gig limit to be a significant performance limiter.

Test Environment Description

To demonstrate the performance of CA Advanced Authentication Server version 8.1 was tested for the performance of authentication using a scenario that included Risk assessment and authentication using the CA Auth ID™ credential. The performance was measured using a Windows 2k12 R2 and MS-SQL 2014 database. The details of the test environment configuration is given in Table 1

Table 1Test Configuration

Component	OS	CPU	RAM	Disk
CA Advanced Authentication Servers	Windows 2k12 R2	16 cores - Intel(R) Xeon(R) CPU E5-2470 0 @ 2.30GHz	4 x 16 GB	600 GB 15K RPM
Database MSSQL 2014	Windows 2k12 R2	16 cores - Intel(R) Xeon(R) CPU E5-2470 0 @ 2.30GHz	4 x 16 GB	600 GB 15K RPM
Clients	Windows 2k12 R2	8 cores Intel(R) Xeon(R) CPU E3-1280 v2 @ 3.60GHZ	4 x 4 GB	600 GB 15K RPM

The database was populated with 100,000 pre-created users and CA Auth ID™ credentials. Sixteen concurrent (multi-threaded) clients sent 100,000 authentication requests to the server. Time was noted at the start and end of the tests in order to calculate the Transactions Per Second (TPS) values.

The figure below shows the deployment configuration of the test system.

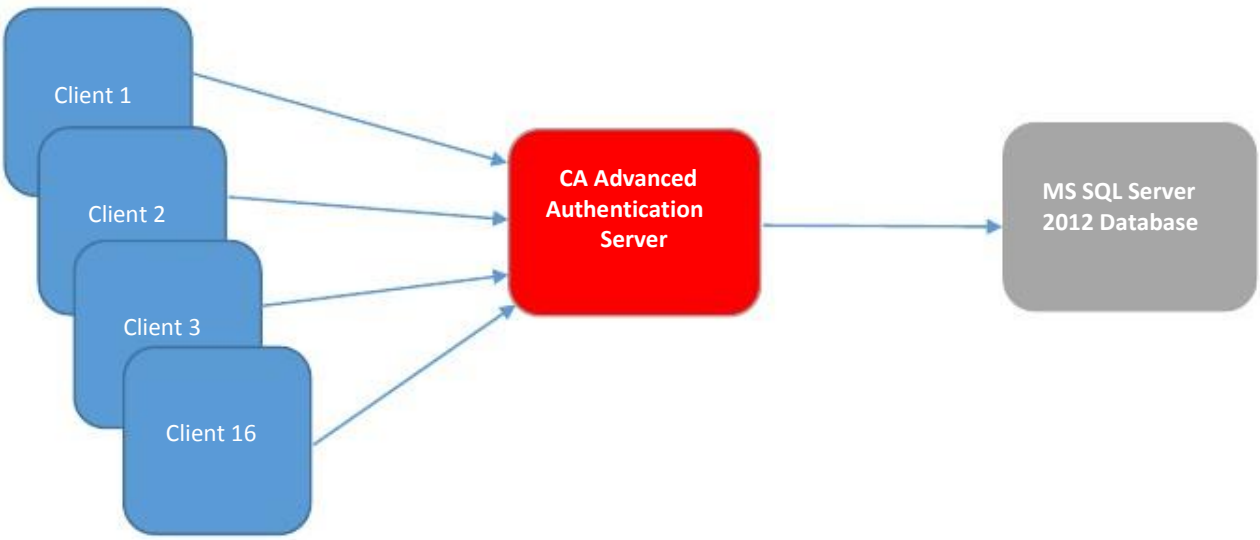

Figure 1 Test Deployment Configuration

Summary of Findings

The test client simulates the work load from the customer's web infrastructure by making calls to the APIs from a test driver that invokes the following APIs of the Risk and Strong Auth Servers in order to perform the authentication requests. These are the APIs called in a typical deployment of the product when using risk-based assessment and the 2-factor CA Auth ID™ credential.

- EvaluateRisk (Sent to the CA Risk Authentication Server, which then evaluates the risk using both the behavior model and rules, calculates a risk score, and recommends action)
- GetChallenge (Sent to retrieve the challenge from the CA Strong Authentication Server)
- SignChallenge (This happens on the client and hence is not counted in the measurement)
- VerifySignChallenge (Sent to verify the signed challenge returned by the client)

API Call	*Time (Sec)*	*Requests per Second*
API – Risk Evaluation	0.0061	163
API - GetChallenge	0.0009	1078
API – Verify Signed Challenge	0.0049	202.9
Total	0.0119	83.78

These APIs are called in sequence to complete a single authentication. Discarding any network latency and delays in client side processing, CA Advanced Authentication Servers delivers a throughput of 84 Requests per second. The response time for these requests ranges from 0.9 to 6.1 milliseconds when measured on the server. The figure below highlights that these response times are done at less than 20% CPU utilization.

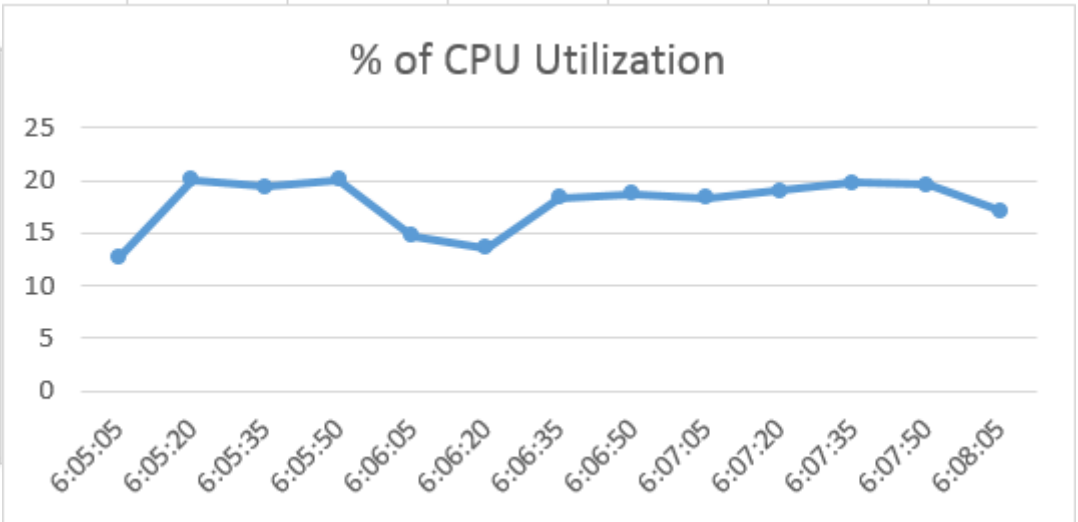

Figure 2CA Advanced Authentication CPU Usage

Conclusion

CA Advanced Authentication Server is able to deliver excellent results in an environment demanding high performance while providing the robust security of two-factor authentication.