Let's Encrypt enables Web encryption for all with AMD EPYC™ CPUs

Reduced database latency for security certification from Let's Encrypt with AMD EPYC processors

AMD EPYC

CUSTOMER

Let's Encrypt

INDUSTRY

Web security certificate authority

CHALLENGES

Reduce latency for certification database API while staying within the same server footprint

SOLUTION

Deploy AMD EPYC™ 7002 Series processors in data centers

RESULTS

Threefold reduction in overall database latency

AMD TECHNOLOGY AT A GLANCE

AMD EPYC 7542 CPU with 32 cores

TECHNOLOGY PARTNER

DELL Technologies

Let's Encrypt is the largest Internet security certificate authority in the world, created by the Internet Security Research Group (ISRG). It is a non-profit organization that provides secure connectivity for everyone, not just those who can afford it. Since Let's Encrypt delivers services for a massive number of the world's websites, it really needs to provide its certification system via the fastest and most efficient means possible. Using AMD EPYC™ processors in its data centers enabled ISRG to realize significant improvements in server latency and therefore meaningfully increase the volume of services the organization can provide in the same amount of time, as well as laying the groundwork for their future growth.

"The overall database latency also dropped from 0.45ms to 0.15ms – three times faster with the EPYC CPUs."

Josh Aas, Executive Director, Internet Security Research Group, provider of Let's Encrypt

Encryption certificates for all

Josh Aas is Executive Director of the Internet Security Research Group. He founded Let's Encrypt around the idea that the entire web could be encrypted. "We concluded that the only way to do it was to start a certificate authority," he says. "That's an organization that gives out the digital certificates that you need to encrypt a website's communication. We needed to start one that made it free and easy to do. Prior to Let's Encrypt, it was quite expensive, and it was very technically complicated, so a lot of people and organizations felt like they couldn't do it and privacy on the web suffered a lot as a result."

"When we started Let's Encrypt, only the biggest websites typically had secure connections," says Aas. "Only 39 percent of all web page loads in 2015 were encrypted. Five years later, in the US, that number is approaching 92 percent and globally the number is about 84 percent. So that is a huge amount of progress." Let's Encrypt has been a big part of this effort and operates with a very lean set of resources. "We operate out of two data centers, one in Salt Lake and one in Denver, on a budget of about $4 million a year. We have a strong reputation for being reliable and secure on an efficient budget. Our money comes primarily from corporate sponsors, who have an interest in seeing a much safer and more secure Web. If your goal is to make the Web safer, it is hard to find a better place to invest the dollar than Let's Encrypt."

Massive growth drives need for efficiency

Since its creation, Let's Encrypt has grown its breadth of service dramatically and now serves a huge volume of the Web. "Automation and efficiency are really important because today we're serving over 230 million websites out of three racks of hardware," says Aas. "That is over 40 percent of the entire Web. We issue more certificates every day than any other organization in the world. Almost every organization around the world uses us, from small businesses, governments, and educational institutions to just about every Fortune 500 company. At Let's Encrypt, we provide services to companies in almost every country around the world."

"We're always looking at what we can do to be more efficient and simplify our systems," continues Aas. "Simplicity means less likelihood of making mistakes. We're trusted to run all the security infrastructure for the Web, and we need to be careful about how we do it.

One of the reasons we're able to serve the number of websites we do with almost zero error rate and very low latency today is because a few months ago we replaced our database server with an AMD EPYC platform. We didn't want to use more space, and our options for upgrading prior to EPYC were not good. It would have been just incremental upgrades of 10 or 20 percent. We wanted to more than double everything in the box but in the same form factor."

Lower latency with AMD EPYC processors

The hardware upgrade provided a significant increase in resources. "We went from 24 Xeon cores to 64 EPYC cores. That's 128 threads between two chips. We doubled the RAM from 1TB to 2TB. Most important is the PCIe® lanes in EPYC. We keep all the storage for this database local to the machine, and we wanted to use NVMe because it is fast. You can't stick 24 NVMe drives in an Intel machine. EPYC makes such a huge difference for us because we could put 24 high-capacity, incredibly fast NVMe drives in the front of the server. Having all these PCIe lanes on EPYC is a huge deal and it really changes the game for what you can do with storage."

"Within the next three to five years, we're going to move everything over to AMD EPYC CPUs."

Josh Aas, Executive Director, Internet Security Research Group, provider of Let's Encrypt

The result of this was a dramatic improvement in latency. Comparing Let's Encrypt's original dual 12-core Intel Xeon E5-2650 processors against a new Dell EMC PowerEdge R7525 rack server equipped with dual 32-core AMD EPYC 7542 CPUs, the median time to process the certification API request dropped from 90ms to 9ms – a tenfold reduction. "This was with CPU utilization falling from 90 to 25 percent," says Aas. "The overall database latency also dropped from 0.45ms to 0.15ms – three times faster with the EPYC CPUs."

Let's Encrypt has specific limitations on how it can deliver its services due to the level of security required. "We're not allowed to use the cloud," explains Aas. "We don't even use normal datacenter rooms. We have special high security rooms with their own walls built inside data centers with biometric access." The advanced security features from AMD EPYC processors have therefore been another valuable feature.

An all-EPYC future for Let's Encrypt

"We're going to start phasing out all our Intel Xeon servers, including our compute boxes," says Aas. "We have a whole bunch of 1U compute boxes. We've started the process of replacing them with EPYC systems. The new [EPYC powered] 2U servers are easily more than three times as powerful." Let's Encrypt has chosen 32-core AMD EPYC CPUs as the best balance between core count and clock speed. "For the database server, we do need higher frequencies," explains Aas. "So 32 is the most cores we could get without sacrificing too much on frequency. But when we go to the compute machines that run all the VMs, that's a very different workload, where core count has a higher priority. We will look at 48 or 64 cores."

"We launched in December of 2015 and now we are serving 230 million websites," concludes Aas. "We serve everybody from small businesses, news organizations, NGOs, governments to Fortune 500. Some of our users have been with us for a long time. We don't know yet where it's going to level off, but it's clear that we're going to be the majority provider for this service on the Web for a long time. Within the next three to five years, we're going to move everything over to AMD EPYC CPUs."

About Let's Encrypt

Let's Encrypt is a free, automated, and open certificate authority (CA), run for the public's benefit. It is a service provided by the Internet Security Research Group (ISRG). ISRG was founded in May 2013 to serve as a home for public-benefit digital infrastructure projects, the first of which was the Let's Encrypt certificate authority. The group's founding sponsors and partners were Mozilla, the Electronic Frontier Foundation, the University of Michigan, Cisco, and Akamai. Let's Encrypt gives its users the digital certificates they need in order to enable HTTPS (SSL/TLS) for websites, for free, in the most user-friendly way possible, in order to create a more secure and privacy-respecting Web. For more information visit letsencrypt.org.

About Dell Technologies

Dell Technologies is committed to transforming businesses, shaping the future of innovation and developing technologies to drive human progress. We are passionate about driving human progress through greater access to better technology, for people with big ideas around the world. Dell Technologies is at the forefront of driving the digital future. With the combined power of industry leaders: Dell, Dell EMC, Secureworks, Virtustream and VMware, we're committed to transforming lives with world-class technologies. Partnering with dynamic and agile companies is what fuels our desire to drive digital transformation. Together, we create iconic solutions to modernize the technologies, people and processes of today. For more information about how Dell Technologies is enabling today and inspiring tomorrow, visit delltechnologies.com.

About AMD

For 50 years AMD has driven innovation in high-performance computing, graphics, and visualization technologies—the building blocks for gaming, immersive platforms, and the data center. Hundreds of millions of consumers, leading Fortune 500 businesses, and cutting-edge scientific research facilities around the world rely on AMD technology daily to improve how they live, work, and play. AMD employees around the world are focused on building great products that push the boundaries of what is possible. For more information about how AMD is enabling today and inspiring tomorrow, visit amd.com/EPYC.