WHITE PAPER

Optimizing Government Websites for Peak Traffic Events

Akamai

TD SYNNEX
Public Sector

DLT

Contents

Analyze potential bottlenecks and review site workflow 4

Don’t neglect development standards 5

Maximize traffic offload 6

Build a layered security posture 7

Ensure DNS is covered 8

Set up friendly error pages 9

Implement site-monitoring protocols 10

Additional follow-up 11

Want more tips to improve your site’s performance? 12

Government websites provide the public with vital and market-sensitive information that must be released to the general public in a timely manner with no hiccups and must be equally available to all end users. The handling of peak traffic events/releases to ensure the appropriate flow of information to the general public is critical for the agencies Akamai supports.

Although many websites (particularly ecommerce) deal with increased traffic during the "big three" American shopping holidays — Thanksgiving, Black Friday, and Cyber Monday — government websites can encounter both planned and unplanned traffic spikes at any time of year from constituents.

If not handled properly, these spikes can trigger site slowdowns, outages, errors, and have other negative impacts on the user experience.

Government-specific website content with potential for higher traffic include:

- Election sites containing constituent registration and election results
- Healthcare open enrollment and vaccine or disease awareness information
- Press release content, including document releases and court decisions
- Tax guidance and tax return submissions during tax season
- Social media and television announcements that direct users to government sites

Government agencies are prime targets for high-traffic events that, if not handled properly, can cause lasting effects to constituent trust. Whether it's performance-related concerns, distributed denial-of-service (DDoS) attacks that can bring the site down, or even credential stuffing attacks, paying attention to the performance and security of these critical websites is crucial.

In this white paper, we will discuss some key steps to help ensure that your website can proactively withstand peak traffic events and give your website the highest possibility for success.

Analyze potential bottlenecks and review site workflow

The exercise of analyzing potential bottlenecks is critical to understand the main pathways that your users are expected to navigate to use your website. This exercise should include all members of your application and infrastructure teams to ensure that reliable infrastructure is in place to handle heavy traffic loads.

This analysis should include questions such as:

- What are the main entry points to your website? (home page, login pages, forms, newsletters, etc)
- What sort of operations does your site rely on? (form submissions, account creation, back-end processing)
- Do you have adequate infrastructure to handle peak traffic, potentially including disaster recovery locations for failover?
- Have you performed load testing to confirm your resources will support the increased traffic?

Your Akamai Account Team can also assist in performing site, delivery, and security reviews to help ensure that all configurations meet Akamai best practices and are optimized for successful releases.

Knowing the lay of the land before you're under attack can help everyone be ready to go when the site is under duress. The more that can be understood and addressed under normal traffic conditions means the less you need to worry about during peak events and releases.

Don’t neglect development standards

Site performance is not just about infrastructure. You can increase page load times and lower site bloat via periodic audits of your website to ensure that you are only using required resources. These five tips can help you minimize the number of requested assets on your pages and optimize the ones you require.

1. Combine and minify CSS and JavaScript files where possible
2. Use compression mechanisms to reduce the bytes to transfer
3. Enable new protocols like HTTP/3 to streamline asset delivery
4. Use Akamai Image & Video Manager to optimize images according to your users’ devices
5. Minimize the use of third-party assets; a failure here can break your site

Maximize traffic offload

One of the easiest ways to help your government site remain available is to cache as much content as possible. You'll need to identify which content is safe to cache and which content cannot be cached.

Caching content on the Akamai platform allows the content to be served closer to your end users while also limiting the number of requests your infrastructure receives. This enhances the end-user experience, improves scalability, improves site load times, and protects your origin during peak traffic events. A few key recommendations are to:

- **Cache as much content as possible**; pay particular attention to pages that you expect to see increased traffic.
- **Limit the use of user-specific, dynamic pages**
- **Remove cache busting query strings from the cache key** (e.g., common marketing query parameters)
- **Consider hosting** truly static content on Akamai NetStorage (content such as common embedded HTML objects, such as images, CSS, JavaScript, form templates, etc) for 100% origin offload and to avoid downtime
- **Review API and other AJAX-based traffic** to determine if those responses can be cached for further offload
- **Develop a cache-purging strategy** to help ensure that content updates are received in a timely manner
- **Implement SureRoute for Performance races and build traffic-limiting strategies** for content that cannot be cached
- **Improve your customer experience** by using Queue-It waiting rooms to limit traffic to your origin

The more traffic the Akamai platform can offload for you, the more your applications can focus on the workloads that are critical to user functionality. Work with your Akamai Account Team to develop a robust caching strategy that will maximize site offload.

Build a layered security posture

Managing peak traffic events is not just about handling legitimate user traffic — under high traffic conditions, your government site is likely to see all sorts of malicious traffic, as well. Akamai App and API Protector provides site protection at the edge, before it reaches your infrastructure.

Akamai's security controls provide you with the flexibility to block malicious traffic with traditional network firewall controls (such as IP, GEO, and ASN blocks), build rate limiting policies to protect against DDoS attacks, use our Adaptive Security Engine ruleset to block malicious application attacks, and block IP addresses with poor reputations (as determined by Akamai AI and our robust bot detection capabilities).

Work with your Akamai Account Team to help review and optimize your security configurations. Consider:

- Ensuring that all your sites and endpoints are covered under match targets
- Performing site analysis to ensure all controls are tuned in a deny state to proactively block malicious traffic
- Developing a policy for handling IP, GEO, and ASN blocks (and allows) using client lists to block known threat actors
- Reviewing web application firewall (WAF) policies to ensure the attack groups are in a deny state where appropriate
- Creating custom rules to block traffic based on patterns that are unique to your specific application at the edge
- Using Client Reputation profiles to dynamically block IPs based on their reputation scores, as determined by Akamai AI, before they can cause a problem for your application
- Using bot visibility and management to deny custom bots, Akamai-known bots (where appropriate), and transparent detections
- Implementing Bot Manager Premier and Akamai Account Protector to protect any transactional endpoints (such as site logins, password resets, account creations, etc)
- Restricting access to your origin infrastructure by implementing Site Shield firewall rules, allowing only
- Akamai IPs to access your servers
- Performing tabletop exercises with your security team and your Akamai Account Team to ensure that all parties are prepared to respond in the event of a security incident

Security is a critical component for any peak traffic event given their high-profile nature. Building a layered strategy is important to the success of the event and the availability of your website. Tuning security configurations ahead of these events will provide peace of mind that everything will run smoothly during the event.

Ensure that DNS is covered

DNS is the entry point for all requests to your government website and is one of the most critical pieces of infrastructure to maintain. Without DNS, no one can access your website. Onboarding your domain's zone to Akamai DNS is a quick and easy way to ensure the availability and reliability of DNS traffic.

Using the vast Akamai network, your zone will be served from Akamai regions across the globe, increasing overall resiliency and availability compared with using traditional DNS providers.

Additionally, don't neglect the time to live (TTL) on your DNS resource records. Under high traffic conditions, the last thing you want your users to do is constantly querying your hostname in DNS. Using longer TTL on your hostnames will improve caching of these records and the overall perceived performance of your website, resulting in a better user experience.

Set up friendly error pages

If your site returns an error, it's a good practice to use a branded page to indicate to the user that some sort of error occurred. Akamai delivery configurations support this with Site Failover, a feature included with Akamai Ion. Failover content can be hosted directly on Akamai NetStorage and returned to users in the event that an error is returned by the origin infrastructure.

Additionally, Queue-It waiting room pages can be configured for high-traffic endpoints, providing a branded experience for users to wait in while site resources free up for them to access the site.

Implement site-monitoring protocols

Traffic over the Akamai platform can be monitored in many ways. The Akamai Control Center provides numerous traffic reports and security consoles to view your traffic use, as well as real-time event dashboards that can be configured to monitor CDN traffic.

You can also use Akamai DataStream, SIEM, and TrafficPeak services to retrieve delivery and security logs directly from the Akamai platform for real-time monitoring with tools familiar to your organization. This speeds up investigation time for errors and allows rapid analysis and triage, which is critical during peak events. Gathering these metrics lets you document the results of the event and prepare for future traffic spikes.

Additional follow-up

It's important to know that each peak traffic event is unique. The items we discussed in the previous sections are excellent springboards for starting a review. Additional items to consider are:

- Ensuring that you have robust testing mechanisms in place to handle high traffic
- Testing your applications to ensure proper functionality, as well as validating that your infrastructure can handle the increased traffic volume, which will help build confidence during peak traffic events
- Developing runbooks for specific scenarios (such as when to block sectors of traffic, when to enable a waiting room, and how to reach out to specific application teams for releases), which will help to ensure a consistent process is followed
- Knowing how to monitor your applications during the peak event, as well as who and how to escalate during the event; these are paramount to the overall success of the event
- Reporting on the outcome of the event to validate that it achieved the expected outcomes as well as to document the lessons learned can continuously optimize your releases; attack vectors and targets are always evolving so you must maintain a state of constant vigilance to meet these threats proactively and maintain successful releases

Want more tips to improve your site's performance?

Using these tips, you can be sure that your government website can handle high traffic and maintain your expected user experience. If you have any questions, reach out to your Akamai Account Team for help with reviewing properties.

Your Account Team has the expertise and knowledge to effectively review your website and make recommendations to improve site performance and security posture, giving your users the best possible experience.

Contact us

Akamai

TD SYNNEX Public Sector

DLT

Akamai Security protects the applications that drive your business at every point of interaction, without compromising performance or customer experience. By leveraging the scale of our global platform and its visibility to threats, we partner with you to prevent, detect, and mitigate threats, so you can build brand trust and deliver on your vision. Learn more about Akamai's cloud computing, security, and content delivery solutions at **akamai.com** and **akamai.com/blog**, or follow Akamai Technologies on **X** and **LinkedIn**. Published 08/25.