JustADC Inc.

F5 BIG-IP SERVICES DATASHEET

JUSTADC

What's Inside

Our Services

Service Delivery

f5 CERTIFIED

amazon web services

Microsoft Azure

Providing The Industry's Most Reliable F5 BIG-IP Solutions.

JustADC focuses on F5 technologies. All of our project resources have a minimum 10+ years of direct practical F5 experience, offering expert level knowledge on the full F5 product suite. We can guarantee that no matter the size or complexity of your project we will be able to provide an optimal solution for your project or break-fix requirements.

Key Benefits

We Do Not Compete With F5 Partners

We partner with F5 partners who sell F5 equipment and licenses to end-customers but do not have the necessary skills to engage in the post-sales deployment. In other words, it's a win-win-win proposition – we profit from pleasing end-customers with our seamless and flawless service delivery, while both partners and customers reap the benefits of strengthening the bonds with each other post-sales.

Our Engineers And F5 Certified, Energetic And Highly Motivated

We hire the only best of the best in the F5 industry. Our staff enjoys the benefits of remote work and flexible hours. They enjoy building their CVs with F5 certifications to better position themselves in the industry as well as increasing their knowledge in fast growing BIG-IP technologies.

We Have A 100% Project Success & Customer Satisfaction Rating

No other vendor can boast 100% project success rate. As a result, all of our customer satisfaction surveys result in 10 on 10 ratings.

We Have The Most Fair And Reasonable Quotes

Given our expertise and efficiency in developing and delivering solutions, we don't take as long as our competitors to fulfill the same requirements, regardless of the complexity. As such you'll find our quotes are often half of what you'll see from our competitors.

Our Services

We do nothing but F5 BIG-IP. Period.

This gives us a focused advantage over other consulting organizations that may not have been exposed to the vast number of environments and scenarios that our team has. With this focus, our experts have the necessary experience to deploy and manage your F5 environments more effectively and efficiently.

Even the most experienced network engineers often lack the expertise to deploy or troubleshoot complex F5 environments. Let us partner with them to avoid any of the most frequent issues we encounter:

1.) Outages due to misconfigurations or design flaws.

2.) Significant delays in your critical projects due to lack of experience in advanced F5 technologies.

3.) Unecessary prolonging of outages due to delays in determining root cause during incidents.

Engage JustADC for every aspect of your BIG-IP projects and ongoing management. Whether introducing F5 into a new environment, migrating away from legacy or other vendor equipment, JustADC will provide the most cost-effective, accurate and efficient solutions to your ADC requirements. We can do this by demystifying every aspect of F5 technologies--Infrastructure, Application Optimization, Authentication and Security.

BIG-IP Infrastructure

Introducing F5 BIG-IPs into your Infrastructure involves two critical phases – accurate sizing and deployment.

Sizing Your BIG-IPs -- Hardware & Licensing

Engage JustADC prior to purchasing your gear and licenses so that we can provide unbiased sizing recommendations. We can help reduce your Return On Investment (ROI) by accurately sizing your F5 hardware. Most resellers do not have the expertise to provide an exhaustive analysis of your current and future growth requirements prior to determining the VE license or hardware platform you require.

Deploying your environment with insufficient horsepower to handle your applications could overload your F5s, resulting in outages and more expensive post facto purchase of additional hardware or licenses to expand capacity. Conversely, over-sizing a platform is a waste of upfront hardware costs and on-going F5 maintenance fees.

To provide sizing recommendations, we collect key sizing metrics from you, such as existing

application, network and firewall statistics, interface bandwidth, SSL Transactions Per Second (TPS), CPU and memory utilization. Using these metrics, we can precisely match the most appropriate F5 Model number to your needs.

Deploying your BIG-IPs -- Base Builds

JustADC can build new BIG-IPs into your existing data center or cloud environments, for the purpose of:

1. Optimizing, Securing and Authenticating your new or existing applications.

2. Migrating off of existing legacy F5s or other vendor ADCs, such as Cisco CSS/ACE, A10, Citrix Netscalers, HAProxy, FortiNet ADC or NGINX

With all of our new hardware or virtual platform base builds, we provide you a JustADC Post-Installation Report including the following items:

1. Confirmation of your base build settings and their test results, including:

    - Custom environnment-specific settings
    - JustADCs recommended settings
    - Industry best practice settings

2. Analysis of F5 BIG-IP iHealth reports for all of your newly deployed devices, included any suspect log file entries or core file dumps created during the build process.

3. Layer 2 and 3 Connectivity test results. We work directly with your Network teams for establishing F5 Layer 2 and 3 connectivity and configurations that meet and exceed industry best practices.

4. Proof that network failover and configuration synchronization is functioning. JustADC will gaurantee that if any of the following items fail, that the BIG-IP system will remain available for your applications.

    - Any port on any one of the BIG-IPs in the device cluster.
    - Any port on any switch connected to the BIG-IPs in the device cluster.

This report gives you the confidence that your BIG-IPs are ready to start managing your production application traffic .

In addition to experience in deploying all F5 hardware models, we have extensive experience with installing F5 Virtual Edition (VE) on all industry leading hypervisors, such as Microsoft Hyper-V, VMware, Citrix XenServer and the popular Infrastructure as a Service (IaaS) providers Microsoft Azure and Amazon Web Services. JustADC will ensure that your F5 builds continue to follow industry best practices for Layer 2 and 3 connectivity, high availability failover and synchronization, regardless of the intricacies and nuances of the underlying virtual or IaaS environment.
Depending on your environment, we may make the following design recommendations

during your base build engagements:

TMOS Version Upgrades – For your production environments, JustADC recommends installing version N minus 1 plus the most recent hotfix, where N is the most recent major TMOS version.

DMZ segmentation -- For environments where you require logical segmentation, depending on our virtual or hardware recommendations, we may suggest deploying F5 Application Firewall Module (AFM), F5 Route-Domains/Partitions, or vCMP Guests.

Existing Environment Health Checks

Engage JustADC for a comprehensive environment health check for your existing F5 BIG-IP environment, if you are uncertain of its current health in terms of the following items:

1. Memory, CPU and disk utilization.
2. BIG-IP TMOS Bug and security vulnerabilities.
3. Configuration adherence to industry and customer best practices.
4. Network, Power supply and Hardware errors.

For all of our environment audits, we provide a comprehensive JustADC Audit Report, including:

1. Analysis of your configurations for inconsistencies, misconfigurations and adherence to industry best practices.
2. Establishing base-line TMOS versions.
3. Functioning failover and configuration synchronization.
4. F5 iHealth analysis, including analysis of log and core file dumps.
5. High-level change recommendations, if needed, to address any issues resulting from the Healthcheck.

Custom Traffic Management Operating System (TMOS) Certifications
Engage JustADC for deep lab certification and testing of new TMOS releases prior to deploying into your environments. We have extensive customized testing experience for setting up lab scenarios, testing and documenting of any of your required F5 BIG-IP LTM, DNS, ASM and APM features.

We can afford you peace of mind that your new TMOS release will behave as documented prior to deploying in your unique environments.

With all of our custom TMOS certifications, we provide a JustADC TMOS Certification Report including the following:

1. Summary list of required features to test.
2. Summary list of third-party or in-house automation and SNMP-based tools to test integration with BIG-IP.
3. Detailed list of features with test use cases, expected & actual results and

pass or fail result for each test.

Application Optimization

All web applications can benefit from optimization of some kind. We can help you to optimize your application deployments using the F5 BIG-IP Local Traffic Manager (LTM) and DNS (formerly Global Traffic Manager), and customized automation.

BIG-IP LTM and DNS Optimization

A prime candidate for application optimization is your Microsoft Exchange deployments. We have optimized MS Exchange for many organizations running hundreds of thousands of mailboxes within and across their datacenters. We can provide granular tuning of parameters to ensure flawless email delivery. If you're running existing versions of Exchange, or deploying Exchange for the first time, we can configure your BIP-IP LTM to optimize your Client Access Servers (CAS). Using F5 iApps or manual configuration for Outlook Web Access (OWA), Exchange Web Services (EWS), Outlook Anywhere (OA), Outlook Offline Address Book (OAB), JustADC can configure load balancing to distribute your user requests across multiple instances of your CAS servers, offload SSL, and perform web caching and compression of your user requests.

Our team also has vast development experience with iRule and iRuleLX programming to meet any of your custom application optimization needs, using iRule TCL and Node.js programming.

We also have experience in large-scale DNS environments. The BIG-IP DNS is an intelligent DNS server, capable of handling upwards of 1.5 million queries per second, making it a very attractive solution to mitigate against DNS Distributed Denial of Service (DDoS) attacks.

JustADC can assist you in deploying BIG-IP DNS to:

1. Dynamically distribute user's DNS requests across your mulltiple Data Centers or cloud locations using BIG-IP WideIPs. JustADC can provision granulaar DNS routing policies on your BIG-IP DNS to decide which site to send requests to based on requirements. We can also migrate your legacy BIG-IP GTM or other ADC vendor technologies to the new BIG-IP DNS. We can configure BIG-IP DNS and LTMs on the same device/VE or separately, using iQuery or application health checks to determine your aplication statuses.

2. Migrate your static DNS zone files to the BIG-IP DNS. If you're currently running legacy DNS servers such as Microsoft DNS, you can engage Just ADC to stage your zone files and migrate your DNS requests by delegating your domains to the BIG-IP DNS.

BIG-IP LTM and DNS Migrations

JustADC provides migration and transformation services from legacy BIG-IP versions, such as versions 4, 9, and 10, and from all major ADC vendors such as Citrix Netscaler, Cisco CSS/ACE, A10, HAProxy , FortiNet or NGINX. We have experience with migration methods, including:

1. VIP Address Migrations – By placing your new BIG-IPs in the same Layer 2 VLAN, we can convert and stage new configurations by re-using existing VIP addresses. We then migrate VIPs during a scheduled maintenance window, by disabling your legacy VIPs and enabling them on the new platform.

2. DNS alias or WideIP member update Migrations – JustADC can scan your zone files and identify aliases associated with your BIG-IP DNS WideIPs for the purpose of incrementally migrating your applications one at a time, from one platform to the other.

BIG-IP Automation

Rely on our extensive development experience with iControl programming to automate the following:

1. Day-to-Day Engineering – For your custom applications that require enhanced F5 application integration, automation and control, you can rely on JustADC's extensive iControl Rest and SOAP development experience. We also have experience deploying new VIPs, WideIPs and BIG-IP ASM policies using the BIG-IQ automation platform.

2. BIG-IP new deployments and upgrades-- Your environments may be candidates for custom developed automation in the form of:

   - **BIG-IQ automation** – We can automate deploying new BIG-IPs using F5s BIG-IQ platform.

   - **iWorkFlow & OpenStack automation** -- For your Openstack environments, we are experienced in deploying the Load Balancer as a Service (LBaaS) Neutron plug-in for integrating the BIG-IP into your OpenStack environment.

Authentication

Take advantage of your BIG-IP APM to replace existing Virtual Private Networks (VPNs), Web Application Portals, Remote Desktop gateways and Single Sign-On (SSO) functions. Replacing these functions saves you vendor maintenance costs as well as specialized staff to support them.

Additionally, you can use the BIG-IP APM to obfuscate authentication for your DMZ facing applications such as, Microsoft Exchange, Mobile Device Management (MDM --

AirWatch) and Microsoft Lync.

We have expert-level experience with deploying the following functions on the BIG-IP APM.

Web Application Portals

Use the BIG-IP APM to provide a unique webtop experience for individuals or groups of users, providing granular application access, based on Windows Active Directory account or Organization Unit (OU) group settings.
We design custom webtops that contain any of the following resources, ensuring your users only ever login once -- the BIG-IP APM will automatically authenticate your users into all of your application resources thereafter, such as:

- **Local Web applications** – For your in-house web applications, we can configure the BIG-IP APM to use server-side NTLMv2 or Kerberos SSO to supress pesky HTTP basic login prompts. Your applications will typically prompt external users in this manner who want to access your applications from computers that are not joined to your Microsoft Active Directory (AD).

- **Cloud Applications** – Using Security Assertion Markup Language (SAML), we can provide client-side Single-Sign-on (SSO) Federation services for Could applications, such as ServiceNow, WorkDay, SalesForce, Microsoft Outlook 365, or any other clould-based employee service.

- **Virtual Desktop/Application Security Gateways** - We have extensive experience deploying the F5 BIG-IP APM to replace the security gateway function of major virtual desktop and application vendors, including the two most popular -- Citrix Storefront / Access Gateway and VMware Horizon View Unified Access Gateways (UAG). We can provide HTML5, ICA Proxy, PCoIP proxy cabilities for your thick client applications or web browser access needs.

- **Traditional SSL VPNs** – If you are currently using your Cisco ASA, Checkpoint or F5 Firepass, for traditional remote access VPNs, we can provide seamless migration to the BIG-IP APM, while also providing more granular access to your users with any of the Authentication features mentioned previously.

Cloud Federation / Single Sign On (SSO)

As an alternative to using Web Application Portals, your users can retain their URLs and bookmarks to existing cloud services, such as ServiceNow, WorkDay, SalesForce, and Microsoft Outlook 365. We can configure the BIG-IP APM as either a SAML Service-Provider (SP) or Identity Provider (iDP) so your users can login to any of these cloud providers using their local Active Directory login credentials. JustADC will configure the BIG-IP APM to consume SAML assertions from your Cloud providers and offer SAML tokens for a seamless user login experience. For those of you who may be using Microsoft Active Directory Federation Services (ADFS) for your SSO already, JustADC can migrate to BIG-IP APM, to reduce your operating costs and vendor footprint .

Authentication Offloading and Obfuscation

Use the BIG-IP APM to obfuscate and offload your application authentication functions – fronting applications with your BIG-IP APM will prevent attackers from attempting logins directly against your application servers. Examples of applications that BIG-IP APM can offload authentication are Exchange Outlook Web Access (OWA), Exchange Web Services (EWS), Outlook Anywhere (OA), Outlook Offline Address Book (OAB), Mobile Device Management (MDM) and Microsoft Lync authentication. JustADC can configure your BIG-IP APM to offloading the authentication function, using LDAP or AD from these application servers.

Multi-factor Authentication (MFA)

You may have enforced complex password selection requirements for your users, but security experts have shown that your systems are still susceptible to brute force password guessing attacks. Providing an additional layer of` login security with MFA can prove to greatly reduce your risk of malicious logins to your systems.

JustADC has experience integrating BIG-IP APM with traditional hard or softoken MFA solutions. However what distinguishes JustADC from our competitors is our experience integrating your applications with cloud based MFA solutions. Cloud MFA solutions allow users to use their mobile phones for your MFA requirements instead of expensive hardware token or on premise software token solutions. With cloud based MFA users can utilize SMS, phone-calls or push notifications to prove they are who they claim to be.

Some of the vendors we've successfully integrated the BIG-IP APM with are:
- RSA SecurID
- Microsoft Azure MFA
- Amazon Web Services (AWS) MFA
- OneLogin Security
- DUO Security

Migrating From Microsoft's End-of-Life Threat Management Gateway (TMG)

Migrating Microsoft's retired TMG product to the BIG-IP APM module is a popular use of the BIG-IP APM. Whether you're currently using the TMG as a reverse proxy or for your Microsoft Exchange Outlook Web Access (OWA) gateway, we can migrate your TMG system to the BIG-IP APM with zero impact to your users.

Security

Is your network security keeping you awake at night? F5 tackles security from a number of fronts – JustADC has your back on these fronts.
Web application Firewall (WAF) with BIG-IP Application Security Module (ASM)

Whether you're deploying applications you've developed internally or third-party web

applications, on premise or in the cloud, the BIG-IP ASM can meet your security needs. We can configure the BIG-IP ASM to help you mitigate against the known OWASP top 10 attacks, such as cross-site scripting, or SQL injection or fulfilling your Payment Card Industries (PCI) compliance audit requirements.

Your JustADC F5 resources are application, network and security experts. As such, we can speak the language of all of your various IT departments to make sure we completely understand your requirements to maximize the potential of your BIG-IP ASM.

We determine based on your applications and security posture the following requirements:

1. Do you have any sensitive parameters or information that is suseptible to web scraping?
2. Do you require a policy that learns automatically or do you require a manually built policy?
3. Do you prefer a Positive, Negative security model or a combination of the two?
4. Do you have any login pages that you require to protect from web bots and brute force attacks?

Does your organization require a 100% Positive and Manual security policy? JustADC will ensure all of your application entities, including URLs, file types, parameters, headers, flows and login pages of your applications have been properly incorporated into your security policies. We ensure your entities traverse your environments from development, test, non-production through to production. This ensures that no false positives will occur once your applications have reached production release.

For PCI compliance audits, we can rapidly deploy a strictly negative policy and provide you with the necessary PCI reports within one week of our engagement.

Layer 4 Firewalling with Advanced Firewall Module (AFM)

Do you have an existing third-party firewall that is approaching end-of-life and requires refresh? If so, you can migrate your existing firewall rules seamlessly to the BIG-IP Advanced Firewall Module (AFM). JustADC can provide rule conversion from all major firewall vendors, such as Checkpoint, Cisco, Fortinet, and Palo Alto Networks.

Egress Airgap Inspection with F5 Herculon SSL Orchestrator

The BIG-IP Herculon SSL Orchestrator can be used for creating an air gap for your network security forensic tools. With BIG-IP SSL you can centrally manage your SSL encryption and decryption and leave your forensic tools, such as Intrusion detection systems (IPS), data loss prevention (DLP), and application firewalls, to perform their specific task thus alleviating the SSL burden from them.

JustADC can configure the BIG-IP Herculon SSL Orchestrator as a man-in-the-middle within your network, to centralize all of your SSL decryption and re-encryption needs. JustADC has experience in creating highly customized SSL Orchestrator policies to chain

numerous forensic tools to take action on your unencrypted user data in series or in parallel.

Distributed Denial of Service (DSoS) with LTM

The BIG-IP LTM is a proxy server by nature of establishing unique TCP connections between itself and the client and the server. By employing a full TCP proxy architecture in this manner, the BIG-IP can protect the server from a number of TCP based attacks, including Distributed Denial of Service (DDoS) attacks. The BIG-IP uses the industry standard SYN Cookie approach using specialized imbedded chips in its hardware platforms.

We also have experience with integrating your BIG-IPs with the Silverline DDoS cloud. With TMOS version 13, we can configure your BIG-IPs to automatically detect DDoS attacks and automatically trigger your traffic to route-away to the F5 SilverlineDDoS cloud for DDoS cleansing. We configure your BIG-IP to use Border Gateway Protocol (BGP) to integrate directly with the Silverline cloud. The Silverline cloud can handle over 13 Tbps shared DDoS cleansing protection so you can be sure their cloud can handle your DDoS traffic requirements.

Forward Proxy with Secure Web Gateway (SWG)

To ensure safe web browsing by your users from internal desktops, laptops or virtual desktops, JustADC can deploy the Secure Web Gateway (SWG) in your environment. SWG prevents malware by analyzing context based data from Websense's cloud based intelligence system and filtering on allowed URLs by Websense categories.

Service Delivery Methods

ADC On Demand

The best bang for your buck is through our subscription service. The benefits of subscribing as compared to our project-based delivery method are a reduced hourly rate and resource engagement lead-times.

You can subscribe to one of our two packages:

	Standard	Premium
Discounted rate for after hours Emergency Support	x	x
24 x 7 x 365 coverage for break-fix and operational issues.	x	x
Two hotfix and two security vulnerability upgrades included per year	x	x
Pro-active eyes on glass monitoring with our JustADC monitoring platform		x
Guaranteed Expert level F5 resources assigned to your engagement		x
One to 14 day project engagement lead-times with on-demand project resources		x
Gradually reduced resource rate based on lead-times		x

If you are not currently a subscriber to our managed service but still require emergency support, please contact us. You will have access to immediate support for any after hours emergency incident/break-fix or during work-hours emergency or critically delayed project-style engagements.

If you decide within sixty days of your emergency engagement to subscribe to our managed service, we'll credit you back a percentage of your emergency fees into your contract.

ADC Consulting

Our project consulting engagements are fixed-fee Statement of Work (SOW)-based engagements. These engagements consist of:

1. **Requirements gathering** – Meet with an Expert resource to obtain your F5 Technology predefined requirements.

2. **SOW creation** -- Within two days of call, receive a detailed SOW consisting of the various steps required to fullfill the project requirements.

3. **SOW review** -- Make any adjustments needed to the technical details and terms.

4. **SOW sign-off** -- Agreement of the terms and fixed fee associated with the requirements.

ADC University

All of our engagements include knowledge transfer of the solutions we develop and implement. However, if you require classroom-style remote training for your specific needs, we can provide highly customized technical F5 training on any of the technologies F5 supports.

Similar to our ADC Consulting SOW-based project engagements, we'll collect your training requirements and provide a fixed-fee 100% customized training SOW, that you can sign prior to scheduling the training. All of our training requires 8 weeks lead-time to give us time to develop the course material and lab scenarios.

We will mock up all of the scenarios that you would like to have training on in our remote JustADC lab. During the training sessions we will present the agreed upon training over our remote screen sharing, virtual white board environment. We will not configure your devices during the training engagement. Any actual configuration of your lab, non-prod or production environments will require a Project engagement SOW described here.