INTRODUCTION

This README will provide a baseline introduction into the Secure Cloud Computing Architecture (SCCA), Infrastructure as Code (IaC), and summarize a portion of the guidance to comply with the guidance provided. Links will be provided for more in-depth explanations.

WHAT IS SECURE CLOUD COMPUTING ARCHITECTURE (SCCA)?

Moving to the Cloud can be tough. The Department of Defense (DoD) still has requirements to protect the Defense Information System Networks (DISN) and DoD Information Networks (DoDIN), even when living in a Cloud Service Provider (CSP). Per the SCCA Functional Requirements Document, the purpose of SCCA is to provide a barrier of protection between the DISN and commercial cloud services used by the DoD.

"It specifically addresses attacks originating from mission applications that reside within the Cloud Service Environment (CSE) upon both the DISN infrastructure and neighboring tenants in a multi-tenant environment. It provides a consistent CSP independent level of security that enables the use of commercially available Cloud Service Offerings (CSO) for hosting DoD mission applications operating at all DoD Information System Impact Levels (i.e. 2, 4, 5, & 6)." * https://iasecontent.disa.mil/stigs/pdf/SCCA_FRD_v2-9.pdf

WHAT IS SECURE AZURE CLOUD ARCHITECTURE (SACA)?

F5 and Microsoft partnered to streamline a baseline Infrastructure as Code / Azure Resource Manager template to ease the deployment and adoption of SCCA in the Azure Government CSP. The template addresses, from a baseline, the main security and functionality requirements of the SCCA guidelines and completes the deployment in about 10 minutes.

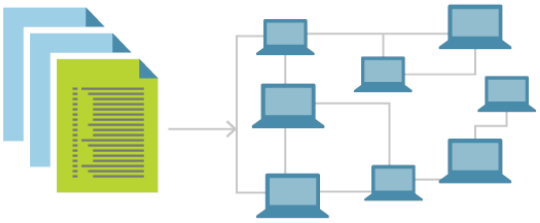
This solution uses an ARM template to launch a three NIC deployment for a cloud-focused BIG-IP Virtual Edition (BIG-IP VE) cluster (Active/Active) in Microsoft Azure Government.

The cluster is configured in a traditional Active/Standby mode. Alternately, you can configure multiple traffic groups in the traditional Active/Active mode to allow each device to process traffic for the traffic group to which it is associated. Azure Load Balancer probes determine which BIG-IP VE device will receive application traffic.

F5 Networks, Inc. 401 Elliott Avenue West, Seattle, WA 98119 888-882-4447 www.f5.com

Americas	Asia-Pacific	Europe/Middle-East/Africa	Japan
info@f5.com	apacinfo@f5.com	emeainfo@f5.com	F5j-info@f5.com

WHAT IS INFRASTRUCTURE AS CODE?



Infrastructure as Code (IaC) is the management of infrastructure (networks, virtual machines, load balancers, and connection topology) in a descriptive model, using the same versioning as DevOps team uses for source code. Like the principle that the same source code generates the same binary, an IaC model generates the same environment every time it is applied. IaC is a key DevOps practice and is used in conjunction with continuous delivery.

Infrastructure as Code evolved to solve the problem of environment drift in the release pipeline. Without IaC, teams must maintain the settings of individual deployment environments. Over time, each environment becomes a snowflake, that is, a unique configuration that cannot be reproduced automatically. Inconsistency among environments leads to issues during deployments. With snowflakes, administration and maintenance of infrastructure involves manual processes which were hard to track and contributed to errors.

Idempotence is a principle of Infrastructure as Code. Idempotence is the property that a deployment command always sets the target environment into the same configuration, regardless of the environment's starting state. Idempotency is achieved by either automatically configuring an existing target or by discarding the existing target and recreating a fresh environment.

For information on getting started using F5's ARM templates on GitHub, see Microsoft Azure: Solutions 101.

DOD CLOUD SECURITY GUIDANCE

An important note for most customers, just moving to an approved CSP environment for a specific impact level does not mitigate the requirements for Risk Management Framework (RMF), meaning, you still need to STIG/SRG your environment and get an Authorization to Operate (ATO).

"In accordance with the DoD Cloud Computing SRG, DoD cloud access systems will enable CSP connections to the DISN consistent with security objectives identified by the information impact levels described therein. The SRG provides guidance for the implementation of cloud access systems3. An Internal CAP (ICAP) allows connectivity between the DISN and a non-DoD (US Commercial) "On-Premise" CSP such as milCloud 2.0. JIE requirements and DoD Data Center architectures govern security capabilities for "On-Premise" CSP

connectivity and to the DISN.4 The Boundary CAP (BCAP) allows connectivity between the DISN and a non-DoD (US Commercial) "Off-Premise" CSP."

WHAT IS INCLUDED IN THIS TEMPLATE?

The BIG-IP VE cluster is deployed with Local Traffic Manager (LTM), Application Security Manager (ASM), Advanced Firewall Manager (AFM), and IP Intelligence (IPI) features enabled by default.

Networking Stack Type: This solution deploys into a new networking stack, which is created along with the solution.

PREREQUISITES

- Important: When you configure the admin password for the BIG-IP VE in the template, you cannot use the character #. Additionally, there are a number of other special characters that you should avoid using for F5 product user accounts. See K2873 for details.

- Since you are deploying the BYOL template, you must have valid BIG-IP license keys.

REQUIREMENTS

An important note on the following requirement mappings; many of the requirements can be met on the single BIG-IP devices, while some features reside outside the BIG-IP systems. Systems that have Required Ancillary Systems will be marked as BIG-IP [Module] / 3rd Party RAS. For example, BIG-IP is not a SEIM, but integrates with almost every SEIM today, so this would be a BIG-IP Core / 3rd Party SEIM.

If there is an Infrastructure as a Service (IaaS) feature covered by the CSP, Azure in this case, it will be marked as Azure in the requirement mappings.

BOUNDARY CLOUD ACCESS POINT REQUIREMENTS (BCAP)

The main purpose of the BCAP is to protect the DISN. It serves as a point of defense to detect and prevent intrusion, unauthorized routes, known malicious code, and malicious network activity. It security event capture data is intended for use by JFHQ-DoDIN Situational Awareness (SA) systems.

Requirement ID	BCAP Security Requirement	Aligned Feature
2.1.1.1.1	The BCAP shall provide the capability to detect and prevent malicious code injection into the DISN originating from the CSE	BIG-IP ASM
2.1.1.1.2	The BCAP shall provide the capability to detect and thwart single and multiple node DOS attacks	BIG-IP ASM / AFM
2.1.1.1.3	The BCAP shall provide the ability to perform detection and prevention of traffic flow having unauthorized source and destination IP addresses, protocols, and Transmission Control Protocol (TCP)/User Datagram Protocol (UDP) ports	BIG-IP ASM / ASM
2.1.1.1.4	The BCAP shall provide the capability to detect and prevent IP Address Spoofing and IP Route Hijacking	BIG-IP AFM
2.1.1.1.5	The BCAP shall provide the capability to prevent device identity policy infringement (prevent rogue device access)	BIG-IP APM
2.1.1.1.6	The BCAP shall provide the capability to detect and prevent passive and active network enumeration scanning originating from within the CSE	BIG-IP Core / AFM
2.1.1.1.7	The BCAP shall provide the capability to detect and prevent unauthorized data exfiltration from the DISN to an end-point inside CSE	BIG-IP Core / 3rd Party RAS
2.1.1.1.8	The BCAP and/or BCAP Management System shall provide the capability to sense, correlate, and warn on advanced persistent threats	BIG-IP ASM / AFM
2.1.1.1.9	The BCAP shall provide the capability to detect custom traffic and activity signatures	BIG-IP ASM / AFM
2.1.1.1.10	The BCAP shall provide an interface to conduct ports, protocols, and service management (PPSM) activities in order to provide control for BCND providers	BIG-IP AFM
2.1.1.1.11	The BCAP shall provide full packet capture (FPC) for traversing communications	BIG-IP Core
2.1.1.1.12	The BCAP shall provide network packet flow metrics and statistics for all traversing communications	BIG-IP Core
2.1.1.1.13	The BCAP shall provide the capability to detect and prevent application session hijacking	BIG-IP ASM

INTERNAL CLOUD ACCESS POINT (ICAP)

The ICAP provides a combination of DISN boundary protection and Mission Owner enclave protection similar to what would be expected within a Core Data Center (CDC). As such, its' requirements set is larger than that of the BCAP. From a security perspective, the ICAP must additionally protect against the possible internet backdoor connection that may be present within an on-premises commercial cloud service implementation.

The following assumption with respect to ICAP security requirements are made:

- Existing and planned CDC security systems are capable of delivering ICAP security functionality.
- ICAP requirements can be achieved by deployment of any combination of physical and/or virtual systems.

Requirement ID	ICAP Security Requirements	Aligned Feature
2.1.1.2.1	The ICAP shall provide the capability to detect and prevent malicious code injection into the DISN originating from the CSE	BIG-IP ASM
2.1.1.2.2	The ICAP shall provide the capability to detect and thwart single and multiple node DOS attacks	BIG-IP Core / ASM
2.1.1.2.3	The ICAP shall provide the ability to perform detection and prevention of traffic flow having unauthorized source and destination IP addresses, protocols, and Transmission Control Protocol (TCP)/User Datagram Protocol (UDP) ports	BIG-IP Core /AFM
2.1.1.2.4	The ICAP shall provide the capability to detect and prevent IP Address Spoofing and IP Route Hijacking	BIG-IP AFM
2.1.1.2.5	The ICAP shall provide the capability to prevent device identity policy infringement (prevent rogue device access)	BIG-IP APM
2.1.1.2.6	The ICAP shall provide the capability to detect and prevent passive and active network enumeration scanning originating from within the CSE	BIG-IP ASM / AFM
2.1.1.2.7	The ICAP shall provide the capability to detect and prevent application session hijacking	BIG-IP ASM
2.1.1.2.8	The ICAP shall provide the capability to detect and prevent unauthorized data exfiltration from the DISN to an end-point inside CSE	BIG-IP ASM / 3rd Party RAS
2.1.1.2.9	The ICAP and/or ICAP Management System shall provide the capability to sense, correlate, and warn on advanced persistent threats	BIG-IP ASM / AFM
2.1.1.2.10	The ICAP shall provide the capability to write and detect custom traffic and activity signatures	BIG-IP ASM / AFM
2.1.1.2.11	The ICAP shall provide the capability to detect and/or prevent VoIP call eavesdropping, modification, and hijacking	Limited
2.1.1.2.12	The ICAP shall provide an interface to conduct ports, protocols, and service management (PPSM) activities in order to provide bi-directional control.	BIG-IP Core / AFM
2.1.1.2.13	The ICAP shall maintain separation of all management, user, and data traffic.	BIG-IP Core
2.1.1.2.14	The ICAP shall allow the use of encryption for segmentation of management traffic.	BIG-IP Core
2.1.1.2.15	The ICAP shall provide a reverse proxy capability to handle service access requests from client systems	BIG-IP Core

Requirement ID	ICAP Security Requirements	Aligned Feature
2.1.1.2.16	The ICAP shall provide a capability to inspect and filter application layer conversations based on a predefined set of rules (including HTTP) to identify and block malicious content	BIG-IP ASM
2.1.1.2.17	The ICAP shall provide a capability that can distinguish and block unauthorized application layer traffic	BIG-IP ASM
2.1.1.2.18	The ICAP shall provide a capability that monitors network and system activities to detect and report malicious activities	BIG-IP AFM
2.1.1.2.19	The ICAP shall provide a capability that monitors network and system activities to stop or block detected malicious activity	BIG-IP ASM / AFM
2.1.1.2.20	The ICAP shall perform break and inspection of Secure Socket Layer (SSL)/Transport Layer Security (TLS) communication traffic supporting single and dual authentication for traffic destined to systems hosted within the CSE. Decryption of message payloads is not implied.	BIG-IP Core
2.1.1.2.21	The ICAP shall provide a monitoring capability that captures log files and event data for cyberspace analysis	BIG-IP Core
2.1.1.2.22	The ICAP shall provide an archiving system for common collection, storage, and access to event logs by Boundary and Mission cyberspace privileged users	BIG-IP Core
2.1.1.2.23	The ICAP shall provide a FIPS-140-2 compliant encryption key management system for storage of DoD generated and assigned server private encryption key credentials for access and use by the Web Application Firewall (WAF) in the execution of SSL/TLS break and inspection of encrypted communication sessions	BIG-IP Core
2.1.1.2.24	The ICAP shall provide a DoD DMZ Extension to support connection from the NIPRNet DoD DMZ COI of supported mission owners	BIG-IP Core
2.1.1.2.25	The ICAP shall provide full packet capture (FPC) for traversing communications	BIG-IP Core
2.1.1.2.26	The ICAP shall provide network packet flow metrics and statistics for all traversing communications	BIG-IP Core
2.1.1.2.27	The ICAP shall provide for the inspection of traffic entering and exiting the CSE.	BIG-IP ASM / AFM

VIRTUAL DATACENTER SECURITY STACK (VDSS)

The Virtual Datacenter Security Stack (VDSS) serves to protect Mission Owner enclaves and applications hosted in an off-premises CSO. VDSS services may be offered by a DoD Component, Mission Owner, or Enterprise Service Provider. Such services may be provisioned from application CSP, the CSP market place, or other third-party authorized provider. VDSS functionality may be deployed within the CSE, the MeetMe

Point, CAP, or supporting Core Data Center (CDC), as required. VDSS requirements apply to all IaaS, PaaS, and SaaS offerings of a CSP.

The VDSS will maintain the separation of communication traffic between virtual subnets operating within the user, data, and management planes of the DISN. The VDSS will perform traffic inspection and filtering of traffic to provide cybersecurity for cloud resident enclaves and mission owner applications. The VDSS will support the Cyber Security Service Provider (CSSP) organizations having either Boundary or Mission Owner defense objectives. VDSS security requirements are provided in the following table. VDSS requirements are anticipated to apply to all cloud service models including IaaS, PaaS, and SaaS. VDSS requirements are not specific as to provider and can be delivered by either the responsible DoD organization, a DoD authorized CSP, or an authorized 3rd party provider.

The following assumptions are made with respect to implementation of a VDSS solution:

- Routing within the CSP is accomplished via CSP's Software Defined Networking (SDN).
- Routing of public IP space within the DISN for the purpose of application advertisement and whitelisting is prohibited, unless specifically authorized.
- Security information and event data from the VDSS can be made available to either the DISN Boundary CSSP or the Mission Owner. For example, SSL/TLS session data could be used to support both the MO CSSP to protect the end-point system and the Boundary CSSP to protect the DISN.
- A single DoD-managed network security enclave deployed to an IaaS or PaaS CSE may support multiple Mission Owners while maintaining virtual separation between Mission Owner virtual environments. For SaaS providers, this assumption is validated by the DoD Provisional Authorization.

Important: Management of FIPS 140-2 compliance for cryptographic components deployed to virtualized systems is the responsibility of the VDSS system owner in collaboration with the CSP and applicable 3rd party vendors. Associated risks should be addressed at Authorization.

Requirement ID	VDSS Security Requirement	Aligned Feature
2.1.2.1	The VDSS shall maintain virtual separation of all management, user, and data traffic.	BIG-IP Core
2.1.2.2	The VDSS shall allow the use of encryption for segmentation of management traffic.	BIG-IP Core
2.1.2.3	The VDSS shall provide a reverse proxy capability to handle access requests from client systems	BIG-IP Core
2.1.2.4	The VDSS shall provide a capability to inspect and filter application layer conversations based on a predefined set of rules (including HTTP) to identify and block malicious content	BIG-IP ASM / AFM
2.1.2.5	The VDSS shall provide a capability that can distinguish and block unauthorized application layer traffic	BIG-IP ASM
2.1.2.6	The VDSS shall provide a capability that monitors network and system activities to detect and report malicious activities for	BIG-IP ASM / AFM

Requirement ID	VDSS Security Requirement	Aligned Feature
	traffic entering and exiting Mission Owner virtual private networks/enclaves	
2.1.2.7	The VDSS shall provide a capability that monitors network and system activities to stop or block detected malicious activity	BIG-IP ASM / AFM
2.1.2.8	The VDSS shall inspect and filter traffic traversing between mission owner virtual private networks/enclaves.	BIG-IP AFM
2.1.2.9	The VDSS shall perform break and inspection of SSL/TLS communication traffic supporting single and dual authentication for traffic destined to systems hosted within the CSE12.	BIG-IP LTM / APM
2.1.2.10	The VDSS shall provide an interface to conduct ports, protocols, and service management (PPSM) activities in order to provide control for MCD operators	BIG-IP AFM
2.1.2.11	The VDSS shall provide a monitoring capability that captures log files and event data for cybersecurity analysis	BIG-IP Core
2.1.2.12	The VDSS shall provide or feed security information and event data to an allocated archiving system for common collection, storage, and access to event logs by privileged users performing Boundary and Mission CND activities	BIG-IP Core
2.1.2.13	The VDSS shall provide a FIPS-140-2 compliant encryption key management system for storage of DoD generated and assigned server private encryption key credentials for access and use by the Web Application Firewall (WAF) in the execution of SSL/TLS break and inspection of encrypted communication sessions.	BIG-IP Core
2.1.2.14	The VDSS shall provide the capability to detect and identify application session hijacking	BIG-IP ASM
2.1.2.15	The VDSS shall provide a DoD DMZ Extension to support to support Internet Facing Applications (IFAs)	BIG-IP Core
2.1.2.16	The VDSS shall provide full packet capture (FPC) or cloud service equivalent FPC capability for recording and interpreting traversing communications	BIG-IP Core
2.1.2.17	The VDSS shall provide network packet flow metrics and statistics for all traversing communications	BIG-IP Core
2.1.2.18	The VDSS shall provide for the inspection of traffic entering and exiting each mission owner virtual private network.	BIG-IP Core

MANAGEMENT NETWORK CONNECTIVITY FOR OFF-PREMISES CSO

There is a template provided that configures the F5 Privileged User Access (PUA) Solution, used extensively

by DoD today, that provides secure multi-factor authentication (MFA) and authorization to Management Interfaces.

The standard template deploys "bastion host" systems, which are basically jump boxes, which are only accessible by traversing the security stack.

Connectivity requirements are met based on how access to the CSP is configured.

Requirement ID	Management Connectivity Requirements	Aligned Feature
2.2.3.2	The VDMS shall allow DoD privileged user access to mission owner management interfaces inside the CSO	BIG-IP PUA
2.2.3.3	The VDMS shall provide secure connectivity to mission owner management systems inside the CSO that is logically separate from mission application traffic.	BIG-IP Core

COMPONENT MANAGEMENT

All components of the template were designed around the aspect of Highly Available Hybrid and/or Multi-cloud integration and allow integration and interoperability with On-Premises solutions.

Requirement ID	Component Management System Requirements	Aligned Feature
2.3.2.1	SCCA components shall provide element managers to manage the configuration of system elements comprising the CAP, VDSS, and the VDMS	BIG-IQ/ AS3
2.3.2.2	SCCA component managers shall be able to manage (e.g., set security, configuration, & routing policies and install patches) SCCA system security and network components	BIG-IQ/ AS3
2.3.2.3	SCCA component managers shall allow for the configuration, control, and management of Ports, Protocols, and Services Management (PPSM) in accordance with DoDI 8551.0120	BIG-IQ/ AS3
2.3.2.4	SCCA component managers shall provide a capability to implement and control system configuration, report configuration change incidents, and support DoD Component change configuration management systems and processes	BIG-IQ/ AS3
2.3.2.5	SCCA management systems shall support the sharing of Combatant Commands, Services, Agencies (CC/S/A) SIEM event & correlation data with the CC/S/A and CND Service Providers	BIG-IP Core
2.3.2.6	SCCA components shall provide logically separate network interfaces for access from the management network infrastructure that is logically separate from production	BIG-IP Core

Requirement ID	Component Management System Requirements	Aligned Feature
2.3.2.7	SCCA components shall support management administration from the DISN management system and/or DISA Datacenter Management System	BIG-IP PUA
2.3.2.9	SCCA components shall provide for management traffic segmentation from user and data plane traffic	BIG-IP Core

PERFORMANCE MANAGEMENT

Performance Management is the monitoring and management of performance and availability of SCCA systems and components. Performance Management operates to detect and diagnose complex system performance problems to maintain an expected level of service. SCCA management systems will operate within the management network (DISN or Cloud side) to provide a performance management capability for monitoring the performance and health of SCCA security components.

Requirement ID	Performance Management Requirements	Aligned Feature
2.3.3.1	SCCA security elements (i.e., BCAP, ICAP, VDSS, and VDMS) shall provide a performance management capability to monitor the health and status of security elements.	BIG-IP Core / BIG-IQ/ iHealth
2.3.3.2	SCCA security elements shall provide performance data, such as CPU, bandwidth, memory and disk I/O, and storage utilization to SCCA management systems for performance analysis and reporting	BIG-IP Core
2.3.3.3	The SCCA security elements shall be able to generate reports and alerts based on performance information provided by SCCA systems.	BIG-IP Core / BIG-IQ/ AVR

PERFORMANCE REQUIREMENTS

QoS and performance requirements affecting the CSP infrastructure and service offerings will be defined by Service Level Agreement (SLA) between the CSP and the acquiring DoD Mission Owner at the time of procurement. Specifications on CSO performance are out of scope for this document.

The following assumptions are made with respect to implementation of SCCA performance requirements:

- The BCAP/ICAP will maintain DISN Service Level Agreement (SLA) objectives21
- The BCAP/ICAP and design will not degrade RTT latency performance between DISN nodes as defined in the DISN SLA for Intra-CONUS, Intra-EUR, and Intra-PAC

BCAP / ICAP PERFORMANCE

Requirement ID	BCAP / ICAP Performance Requirement	Aligned Feature
2.4.1.1	The BCAP shall support scalability of up to 10 Gigabit/second throughput between the DISN and CSP	BIG-IP Core
2.4.1.2	The ICAP shall start with 1 Gigabit/second throughput and have ability to scale up to 10G.	BIG-IP Core
2.4.1.3	The BCAP/ICAP shall support assured bandwidth (Quality of Service)	BIG-IP Core / 3rd Party RAS
2.4.1.4	The BCAP/ICAP shall support IP packet forwarding in accordance with Mission Owner Differentiated Services Code Point (DSCP) tagged QOS prioritization	BIG-IP Core / 3rd Party RAS
2.4.1.5	The BCAP/ICAP shall meet NIPRNet backbone availability of 99.5%	BIG-IP Core
2.4.1.6	The BCAP/ICAP unit processing latency shall be no greater than 35 milliseconds	BIG-IP Core
2.4.1.7	The BCAP (location/performance) design shall provide Round-Trip Time (RTT) in accordance with DISN SLA latency between the CSP and DISN services nodes: <100msec for Intra-CONUS <150msec for Intra-EUR <150msec for Intra-PAC (Oahu, HI-Western Pacific)	BIG-IP Core
2.4.1.8	The BCAP/ICAP unit packet loss shall be <1%	BIG-IP Core

VDSS PERFORMANCE

Requirement ID	VDSS Performance Requirements	Aligned Feature
2.4.2.1	The VDSS unit processing latency shall be no greater than 35 milliseconds	BIG-IP Core
2.4.2.2	The VDSS unit packet loss shall be <1%	BIG-IP Core
2.4.2.3	The VDSS shall achieve availability of 99.5%	BIG-IP Core
2.4.2.4	The VDSS shall support NIPRNet assured bandwidth (Quality of Service) for mission owner systems residing within the commercial cloud	BIG-IP Core
2.4.2.5	The VDSS shall support IP packet forwarding in accordance with Mission Owner Differentiated Services Code Point (DSCP) tagged QOS prioritization	BIG-IP Core

F5 Networks, Inc. 401 Elliott Avenue West, Seattle, WA 98119 888-882-4447 www.f5.com

Americas	Asia-Pacific	Europe/Middle-East/Africa	Japan
info@f5.com	apacinfo@f5.com	emeainfo@f5.com	F5j-info@f5.com

FULL PACKET CAPTURE (FPC)

Full Packet Capture (FPC) is used during analysis of event traffic by the SIEM capability. The capability will capture, store, and provide event correlated session traffic back to the SIEM for use by CND Service Providers engaged in both Boundary and Mission defense. The FPC capability will be implemented at the break and inspection points to provide the greatest CND visibility and situational awareness. However, since FPC may be performed at multiple points within the DISN to include JRSS, the IAP, and the Core Data Centers, the FPC function of the VDSS is intended to be configurable according to traffic flow source and destination points to avoid multiple point capture. Additionally, depending upon the capabilities available within the CSO, FPC equivalent data may also be captured within the CSE.

While a SIEM is not deployed in this template, since the F5 is a Full Proxy, FPC is a standard function of the system.

Requirement ID	Full Packet Capture Requirements	Aligned Feature
2.3.5.1	The FPC shall support integration with SIEM systems to effect data search and retrieval, such as the capability to pull select timeframes of captured data	BIG-IP Core
2.3.5.2	The FPC shall provide the means to reconstruct all network traffic sessions traversing the SCCA Component.	3rd Party RAS
2.3.5.3	The FPC shall provide defined data queries that run against metadata	3rd party RAS
2.3.5.4	The FPC shall provide a capability to request an arbitrary subset of packets	3rd Party RAS
2.3.5.5	The FPC shall locally store captured traffic for 30 days	BIG-IP Core / 3rd Party RAS
2.3.5.6	The FPC data shall be isolated from user and data plane traffic via cryptographic or physical means	Azure
2.3.5.7	The FPC data shall be query-able from a secure remote location on the management network	Azure
2.3.5.8	The FPC function shall be configurable	Azure

SYSTEM SCALABILITY REQUIREMENTS

SCCA components will be built to support scalability both horizontally (add processing components) and vertically (add resources to processing components) to handle a growing amount of work or to improve system performance. Scalability solutions may also address the number and location of nodes.

VDSS SCALABILITY

Requirement ID	VDSS Scalability Requirements	Aligned Feature
2.6.2.1	The VDSS shall be designed to rapidly scale virtual elements up and down in capacity to achieve negotiated (between components provider and Mission Owner) SLA objectives while minimizing metered billing CSO costs incurred by DoD procuring component	BIG-IP Core / Azure
2.6.2.2	The VDSS shall support scalability in increments of 1 Gigabit/second throughput at all points within the design without costly modification	BIG-IP Core / Azure

WHAT IS NOT INCLUDED WITH THE IAAS SACA TEMPLATE?

There are several aspects of the SCCA Guidance that cannot be addressed in a single quick-start template.

- While a subnet is created as part of the template, the Virtual Datacenter Management Stack (VDMS) systems are left unpopulated and should be based on individual customer requirements.
- The Trusted Cloud Credential Manager is also not addressed in the template, as this is a business role and not a technical function that can be addressed in the template.
- DISN Connectivity is also subject to methods used to connect to the CSP, Azure, and is outside the scope of the templates.
- Mission Application Connectivity is not addressed due to it being too complex to estimate most customers' needs when it comes to Mission Owner support. While the template does not create and configure these environments out of the gate, it is possible and recommended to work with your Azure and F5 account teams to architect a proper solution for your requirements.
- Management Network Connectivity for On-Premises CSO is not addressed in the templates because this is outside the scope of the CSP.

F5 Networks, Inc. 401 Elliott Avenue West, Seattle, WA 98119 888-882-4447 www.f5.com

Americas	Asia-Pacific	Europe/Middle-East/Africa	Japan
info@f5.com	apacinfo@f5.com	emeainfo@f5.com	F5j-info@f5.com

- Security Information & Event Management (SIEM) is not addressed in this document to allow for customized SIEM deployment. F5 BIG-IP can integrate with any SIEM desired. https://docs.microsoft.com/en-us/azure/security/security-azure-log-integration-overview

- Continuity of Operations should be discussed with your F5 and Microsoft Account teams to ensure all requirements are met.

- BCAP/ICAP, and VDMS Scalability are not addressed in this template.

- Backup and Restoration Requirements.

IMPORTANT CONFIGURATION NOTES

- All F5 ARM templates include Application Services 3 Extension (AS3) v3.5.1 (LTS version) on the BIG-IP VE. As of release 4.1.2, all supported templates give the option of including the URL of an AS3 declaration, which you can use to specify the BIG-IP configuration you want on your newly created BIG-IP VE(s). In templates such as autoscale, where an F5-recommended configuration is deployed by default, specifying an AS3 declaration URL will override the default configuration with your declaration. See the AS3 documentation for details on how to use AS3.
- There are new options for BIG-IP license bundles, including Per App VE LTM, Advanced WAF, and Per App VE Advanced WAF. See the the version matrix for details and applicable templates.
- You have the option of using a password or SSH public key for authentication. If you choose to use an SSH public key and want access to the BIG-IP web-based Configuration utility, you must first SSH into the BIG-IP VE using the SSH key you provided in the template. You can then create a user account with admin-level permissions on the BIG-IP VE to allow access if necessary.
- See the important note about optionally changing the BIG-IP Management port.
- This template supports service discovery. See the Service Discovery section for details.
- F5 has created an iApp for configuring logging for BIG-IP modules to be sent to a specific set of cloud analytics solutions. See Logging iApp.
- This template can be used to create the BIG-IP(s) using a local VHD or Microsoft.Compute image, please see the **customImage** parameter description for more details.
- In order to pass traffic from your clients to the servers, after launching the template, you must create virtual server(s) on the BIG-IP VE. See Creating a virtual server.
- F5 has created a matrix that contains all of the tagged releases of the F5 ARM templates for Microsoft Azure and the corresponding BIG-IP versions, license types and throughputs available for a specific tagged release. See azure-bigip-version-matrix.
- F5 ARM templates now capture all deployment logs to the BIG-IP VE in **/var/log/cloud/azure**. Depending on which template you are using, this includes deployment logs (stdout/stderr), f5-cloud-libs execution logs, recurring solution logs (failover, metrics, and so on), and more.

- This template has some optional post-deployment configuration. See the Post-Deployment Configuration section for details.
- **IMPORTANT:** Customization of the Management subnet is not currently exposed, if this is a requirement, the ARM and the AS3 will need to be customized appropriately. The linux jumpbox automatically adds 50 to the start IP, and Windows Jumpbox adds 51. It is recommended that you fork the repo, edit the AS3, and point your ARM config to the new location. Or Deploy as is and change configuration after everything is up and running.

SUPPORTED BIG-IP VERSIONS

The following is a map that shows the available options for the template parameter **bigIpVersion** as it corresponds to the BIG-IP version itself. The standard F5 version options have been limited in this template to FIPS CMVP and APL certified releases.

Azure BIG-IP Image Version	BIG-IP Version	Important: Boot location options note
13.1.100000	13.1.1 Build 0.0.4	Two Boot Location option available
14.1.100000	14.1.1	This release will be added in the future.

INSTALLATION / DEPLOYMENT

SACAV2 AZURE GOVERNMENT DEPLOY BUTTONS

Use the appropriate button below to deploy:

- **BYOL** (bring your own license): This allows you to use an existing BIG-IP license.
- **1 Tier** This deploys the 3-NIC 1 Tier use-case.

- **1 Tier with Privileged User Access** This deploys the 3-NIC 1 Tier with Privileged User Access use-case.

POST-DEPLOYMENT CONFIGURATION

Use this section for optional configuration changes after you have deployed the template.

ADDING ADDITIONAL PUBLIC IP ADDRESSES TO THE DEPLOYMENT

The deployment template supports creation of 1 initial external public IP addresses for application traffic. Follow the steps below to add **additional** public IP addresses to the deployment:

- Create a new Azure public IP address resource in the deployment resource group
- Create a new, secondary IP configuration resource (for example: MYRESOURCEGROUPNAME-EXT-IPCONFIG9) in the properties of the external Azure network interface (for example: MYRESOURCEGROUPNAME-EXT0)

When you create virtual servers on the BIG-IP VE for these additional addresses, the BIG-IP network virtual server destination IP address should match the private IP addresses of both secondary Azure IP configurations assigned to the backend pool that is referenced by the application's Azure load balancing rule.

DOCUMENTATION

For more information on F5 solutions for Azure, including manual configuration procedures for some deployment scenarios, see the Azure section of Public Cloud Docs.

SERVICE DISCOVERY

Once you launch your BIG-IP instance using the ARM template, you can use the Service Discovery iApp template on the BIG-IP VE to automatically update pool members based on auto-scaled cloud application hosts. In the iApp template, you enter information about your cloud environment, including the tag key and tag value for the pool members you want to include, and then the BIG-IP VE programmatically discovers (or removes) members using those tags. See our Service Discovery video to see this feature in action.

F5 Networks, Inc. 401 Elliott Avenue West, Seattle, WA 98119 888-882-4447 www.f5.com

Americas	Asia-Pacific	Europe/Middle-East/Africa	Japan
info@f5.com	apacinfo@f5.com	emeainfo@f5.com	F5j-info@f5.com

TAGGING

In Microsoft Azure, you have three options for tagging objects that the Service Discovery iApp uses. Note that you select public or private IP addresses within the iApp.

- TAG A VM RESOURCE
  The BIG-IP VE will discover the primary public or private IP addresses for the primary NIC configured for the tagged VM.

- TAG A NIC RESOURCE
  The BIG-IP VE will discover the primary public or private IP addresses for the tagged NIC. Use this option if you want to use the secondary NIC of a VM in the pool.

- TAG A VIRTUAL MACHINE SCALE SET RESOURCE
  The BIG-IP VE will discover the primary private IP address for the primary NIC configured for each Scale Set instance. Note you must select Private IP addresses in the iApp template if you are tagging a Scale Set.

The iApp first looks for NIC resources with the tags you specify. If it finds NICs with the proper tags, it does not look for VM resources. If it does not find NIC resources, it looks for VM resources with the proper tags. In either case, it then looks for Scale Set resources with the proper tags.

Important: Make sure the tags and IP addresses you use are unique. You should not tag multiple Azure nodes with the same key/tag combination if those nodes use the same IP address.

To launch the template:

1. From the BIG-IP VE web-based Configuration utility, on the Main tab, click **iApps > Application Services > Create**.
2. In the **Name** field, give the template a unique name.
3. From the **Template** list, select **f5.service_discovery**. The template opens.
4. Complete the template with information from your environment. For assistance, from the Do you want to see inline help? question, select Yes, show inline help.
5. When you are done, click the **Finished** button.

CREATING VIRTUAL SERVERS ON BIG-IP

In order to pass traffic from your clients to the servers through the BIG-IP system, you must create a virtual server on the BIG-IP VE. To create a BIG-IP virtual server you need to know the private IP address of the secondary IP configuration(s) for each BIG-IP VE network interface created by the template. If you need additional virtual servers for your applications/servers, you can add more secondary IP configurations on the

Azure network interface, and corresponding virtual servers on the BIG-IP system. See virtual-network-multiple-ip-addresses-portal for information on multiple IP addresses.

In this template, the Azure public IP address is associated with an Azure Load Balancer that forwards traffic to a backend pool that includes secondary IP configurations for *each* BIG-IP network interface. You must create a single virtual server with a destination that matches both private IP addresses in the Azure Load Balancer's backend pool. In this example, the backend pool private IP addresses are 10.0.1.36 and 10.0.1.37.

1. Once your BIG-IP VE has launched, open the BIG-IP VE Configuration utility.
2. On the Main tab, click **Local Traffic > Virtual Servers** and then click the **Create** button.
3. In the **Name** field, give the Virtual Server a unique name.
4. In the **Destination/Mask** field, type the destination address (for example: 10.0.1.32/27).
5. In the **Service Port** field, type the appropriate port.
6. Configure the rest of the virtual server as appropriate.
7. If you used the Service Discovery iApp template: In the Resources section, from the **Default Pool** list, select the name of the pool created by the iApp.
8. Click the **Finished** button.
9. Repeat as necessary.

If network failover is disabled (default), when you have completed the virtual server configuration, you must modify the virtual addresses to use Traffic Group None using the following guidance.

1. On the Main tab, click **Local Traffic > Virtual Servers**.
2. On the Menu bar, click the **Virtual Address List** tab.
3. Click the address of one of the virtual servers you just created.
4. From the **Traffic Group** list, select **None**.
5. Click **Update**.
6. Repeat for each virtual server.

If network failover is enabled (if, for example, you have deployed the HA Cluster 3 NIC template, or manually enabled network failover with traffic groups), when you have completed the virtual server configuration, you may modify the virtual addresses to use an alternative Traffic Group using the following guidance.

1. On the Main tab, click **Local Traffic > Virtual Servers**.
2. On the Menu bar, click the **Virtual Address List** tab.
3. Click the address of one of the virtual servers you just created.
4. From the **Traffic Group** list, select **traffic-group-2** (or the additional traffic group you created previously).
5. Click **Update**.
6. Repeat for each virtual server.

LOGGING IAPP

F5 has created an iApp for configuring logging for BIG-IP modules to be sent to a specific set of cloud analytics solutions. The iApp creates logging profiles which can be attached to the appropriate objects (virtual servers, APM policy, and so on) which results in logs being sent to the selected cloud analytics solution, Azure in this case.

We recommend you watch the Viewing ASM Data in Azure Analytics video that shows this iApp in action, everything from downloading and importing the iApp, to configuring it, to a demo of an attack on an application and the resulting ASM violation log that is sent to ASM Analytics.

Important: Be aware that this may (depending on the level of logging required) affect performance of the BIG-IP as a result of the processing to construct and send the log messages over HTTP to the cloud analytics solution. It is also important to note this cloud logging iApp template is a *different solution and iApp template* than the F5 Analytics iApp template described here.

Use the following guidance using the iApp template (the iApp now is present on the BIG-IP VE image as a part of the templates).

1. Log on to the BIG-IP VE Configuration utility.
2. On the Main tab, from the **iApp** menu, click **Application Services > Applications > Create**.
3. From the **Template** list, select f5.cloud_logger.v1.0.0.tmpl (or later version if applicable).

For assistance running the iApp template, once you open the iApp, from the *Do you want to see inline help?* question, select **Yes, show inline help**.