Appendix A: Schema Reference¶

This page is a reference for the objects you can use in your Declarations for Declarative Onboarding. For more information on BIG-IP objects and terminology, see the BIG-IP documentation at https://support.f5.com/csp/home (https://support.f5.com/csp/home).

Analytics¶

Global analytics properties for onboarding a BIG-IP.

Properties:

Name (Type)	Default	Values	Description
class (*string*)	•	"Analytics"	Indicates that this property contains global analytics configuration
debugEnabled (*boolean*)	false	true, false	Enable debug mode. If debug mode is disabled, internal statistics are collected only if interval is set to the default value (300 seconds)
interval (*integer*)	300	[20, 300]	Analytics data collection interval in seconds. If this interval is different from the default value (300 seconds), internal statistics are not collected unless debugEnabled is set to true. Minimum interval is 20 seconds, maximum interval is 300 seconds.
offboxEnabled (*boolean*)	false	true, false	Enables all communication with the offbox application on the global level
offboxProtocol (*string*)	•	"https", "tcp"	Protocol for communication with offbox analytics application
offboxTcpAddresses (*array<string>*)	•	•	Server IP addresses used only if the 'tcp/https' protocol is chosen
offboxTcpPort (*number*)	•	•	Server TCP port for the server IP addresses used only if the 'tcp' protocol is chosen
sourceId (*string*)	•	•	Unique value to signify the source of data
tenantId (*string*)	•	•	Unique id for the tenant using the analytics backend system

Authentication¶

Authentication properties for onboarding a BIG-IP.

Properties:

Name (Type)	Default	Values	Description
class (*string*)	•	"Authentication"	Indicates that this property contains authentication configuration.
enabledSourceType (*string*)	"local"	"radius", "local", "tacacs", "ldap", "activeDirectory"	Type of remote authentication source to enable for the system.

Name (Type)	Default	Values	Description
fallback (*boolean*)	false	true, false	Specifies that the system uses the Local authentication method if the remote authentication method is not available.
ldap (*Authentication_ldap*)	•	•	Remote LDAP authentication info
radius (*Authentication_radius*)	•	•	Remote RADIUS authentication info.
remoteUsersDefaults (*Authentication_remoteUsersDefaults*)	•	•	The default values that the BIG-IP system applies to any user account that is not part of a remotely-stored user group.
tacacs (*Authentication_tacacs*)	•	•	TACACS+ authentication info

Authentication_ldap¶

Authentication ldap possible properties

Properties:

Name (Type)	Default	Values	Description
bindDn (*string*)	•	•	Distinguished name of the server account. If server is a Microsoft Windows Active Directory server, the name must be an email address
bindPassword (*string*)	•	•	Password for the server account
bindTimeout (*integer*)	30	[0, 4294967295]	Timeout limit in seconds to bind to remote authentication server
checkBindPassword (*boolean*)	false	true, false	Confirms the password for the server account
checkRemoteRole (*boolean*)	false	true, false	Verifies a user’s group membership based on the remote-role definition, formatted as *member*of=”group-dn”
filter (*string*)	•	•	Filter used for authorizing client traffic
groupDn (*string*)	•	•	Group distinguished name for authorizing client traffic
groupMemberAttribute (*string*)	•	•	Group member attribute for authorizing client traffic
idleTimeout (*integer*)	3600	[0, 4294967295]	Connection timeout limit in seconds
ignoreAuthInfoUnavailable (*boolean*)	false	true, false	Ignores authentication information if not available
ignoreUnknownUser (*boolean*)	false	true, false	Ignores a user that is unknown
loginAttribute (*string*)	•	•	Logon attribute. If server is a Microsoft Windows Active Directory server, the value must be the account name “samaccountname”
port (*integer*)	389	[0, 65535]	Port number for the LDAP service
searchBaseDn (*string*)	•	•	Search base distinguished name

Name (Type)	Default	Values	Description
searchScope (*string*)	"sub"	"base", "one", "sub"	Level of remote server's directory to search for user authentication, either base object, one level, or subtree
searchTimeout (*integer*)	30	[0, 4294967295]	Search timeout limit in seconds
servers (*array<string>*)	•	•	IP addresses or hostnames of the remote authentication servers.
ssl (*string*)	"disabled"	"enabled", "disabled", "start-tls"	Enables SSL
sslCheckPeer (*boolean*)	false	true, false	Specifies whether the system checks an SSL peer
sslCiphers (*array<string>*)		"ECDHE-RSA-AES128-GCM-SHA256", "ECDHE-RSA-AES128-CBC-SHA", "ECDHE-RSA-AES128-SHA256", "ECDHE-RSA-AES256-GCM-SHA384", "ECDHE-RSA-AES256-CBC-SHA", "ECDHE-RSA-AES256-SHA384", "ECDHE-RSA-CHACHA20-POLY1305-SHA256", "ECDH-RSA-AES128-GCM-SHA256", "ECDH-RSA-AES128-SHA256", "ECDH-RSA-AES128-SHA", "ECDH-RSA-AES256-GCM-SHA384", "ECDH-RSA-AES256-SHA384", "ECDH-RSA-AES256-SHA", "AES128-GCM-SHA256", "AES128-SHA", "AES128-SHA256", "AES256-GCM-SHA384", "AES256-SHA",	Specifies SSL ciphers

Name (Type)	Default	Values	Description
		“AES256-SHA256”, “CAMELLIA128-SHA”, “CAMELLIA256-SHA”, “ECDHE-ECDSA-AES128-GCM-SHA256”, “ECDHE-ECDSA-AES128-SHA”, “ECDHE-ECDSA-AES128-SHA256”, “ECDHE-ECDSA-AES256-GCM-SHA384”, “ECDHE-ECDSA-AES256-SHA”, “ECDHE-ECDSA-AES256-SHA384”, “ECDHE-ECDSA-CHACHA20-POLY1305-SHA256”, “ECDH-ECDSA-AES128-GCM-SHA256”, “ECDH-ECDSA-AES128-SHA”, “ECDH-ECDSA-AES128-SHA256”, “ECDH-ECDSA-AES256-GCM-SHA384”, “ECDH-ECDSA-AES256-SHA”, “ECDH-ECDSA-AES256-SHA384”, “DHE-RSA-AES128-GCM-SHA256”, “DHE-RSA-AES128-SHA”, “DHE-RSA-	

Name (Type)	Default	Values	Description
		AES128-SHA256”, “DHE-RSA-AES256-GCM-SHA384”, “DHE-RSA-AES256-SHA”, “DHE-RSA-AES256-SHA256”, “DHE-RSA-CAMELLIA128-SHA”, “DHE-RSA-CAMELLIA256-SHA”, “DHE-DSS-AES128-GCM-SHA256”, “DHE-DSS-AES128-SHA”, “DHE-DSS-AES128-SHA256”, “DHE-DSS-AES256-GCM-SHA384”, “DHE-DSS-AES256-SHA”, “DHE-DSS-AES256-SHA256”, “DHE-DSS-CAMELLIA128-SHA”, “DHE-DSS-CAMELLIA256-SHA”, “ADH-AES128-GCM-SHA256”, “ADH-AES128-SHA”, “ADH-AES256-GCM-SHA384”, “ADH-AES256-SHA”, “ECDHE-RSA-DES-CBC3-SHA”, “ECDH-RSA-DES-CBC3-SHA”, “DES-CBC3-SHA”, “ECDHE-ECDSA-DES-CBC3-SHA”, “ECDH-ECDSA-	

Name (Type)	Default	Values	Description
		DES-CBC3-SHA”, “DHE-RSA-DES-CBC3-SHA”, “ADH-DES-CBC3-SHA”, “DHE-RSA-DES-CBC-SHA”, “DES-CBC-SHA”, “ADH-DES-CBC-SHA”, “RC4-SHA”, “RC4-MD5”, “ADH-RC4-MD5”, “EXP1024-DES-CBC-SHA”, “EXP1024-RC4-SHA”, “EXP-RC4-MD5”, “EXP-DES-CBC-SHA”, “TLS13-AES128-GCM-SHA256”, “TLS13-AES256-GCM-SHA384”, “TLS13-CHACHA20-POLY1305-SHA256”, “NULL-SHA”, “NULL-MD5”	
userTemplate (*string*)	•	•	Specifies a user template for the LDAP application to use for authentication.
version (*integer*)	3	[2, 3]	Specifies the version number of the LDAP application.

Authentication_radius¶

Authentication radius possible properties

Properties:

Name (Type)	Default	Values	Description
servers (*reference*)	•	•	RADIUS servers settings

Name (Type)	Default	Values	Description
serviceType (*string*)	“default”	“administrative”, “authenticate-only”, “call-check”, “callback-administrative”, “callback-framed”, “callback-login”, “callback-nas-prompt”, “default”, “framed”, “login”, “nas-prompt”, “outbound”	Type of service used for the RADIUS server.

Authentication_remoteUsersDefaults¶

Authentication remoteUsersDefaults possible properties

Properties:

Name (Type)	Default	Values	Description
partitionAccess (*string*)	“all”	“Common”, “all”	Default accessible partitions for remote users.
role (*string*)	“no-access”	“acceleration-policy-editor”, “admin”, “application-editor”, “auditor”, “certificate-manager”, “firewall-manager”, “fraud-protection-manager”, “guest”, “irule-manager”, “manager”, “no-access”, “operator”, “resource-admin”, “user-manager”, “web-application-security-administrator”, “web-application-security-editor”	Role for the remote users.

Name (Type)	Default	Values	Description
terminalAccess (*string*)	"disabled"	"tmsh", "disabled"	Default terminal access for remote users.

Authentication_tacacs¶

Authentication tacacs possible properties

Properties:

Name (Type)	Default	Values	Description
accounting (*string*)	"send-to-first-server"	"send-to-all-servers", "send-to-first-server"	Specifies how the system returns accounting information, such as which services users access and how much network resources they consume, to the TACACS+ server. The default setting is Send to first available server.
authentication (*string*)	"use-first-server"	"use-all-servers", "use-first-server"	Specifies the process the system employs when sending authentication requests. The default is Authenticate to first server.
debug (*boolean*)	false	true, false	Specifies whether to log Syslog debugging information at the LOG_DEBUG level. We do not recommend enabling this setting for normal use. The default is Disabled.
encryption (*boolean*)	true	true, false	Specifies whether to use encryption of TACACS+ packets. The default is Enabled.
protocol (*string*)	•	"lcp", "ip", "ipx", "atalk", "vines", "lat", "xremote", "tn3270", "telnet", "rlogin", "pad", "vpdn", "ftp", "http", "deccp", "osicp", "unknown"	Specifies the protocol associated with the value specified in Service Name, which is a subset of the associated service being used for client authorization or system accounting. You can use following values: lcp, ip, ipx, atalk, vines, lat, xremote, tn3270, telnet, rlogin, pad, vpdn, ftp, http, deccp, osicp, and unknown. Note that the majority of TACACS+ implementations are of protocol type ip, so try that first.
secret (*string*)	•	•	Type the secret key used to encrypt and decrypt packets sent or received from the server. Do not use the pound sign (#) in the secret for TACACS+ servers.
servers (*array<string>*)	•	•	Specifies a list of the IPv4 addresses for servers using the Terminal Access Controller Access System (TACACS)+ protocol with which the system communicates to obtain authorization data. For each address, an alternate TCP port number may be optionally specified by entering the address in the format address:port. If no port number is specified, the default port 49 is used.
service (*string*)	•	"slip", "ppp", "arap", "shell", "tty-daemon", "connection", "system", "firewall"	Specifies the name of the service that the user is requesting to be authorized to use. Identifying what the user is asking to be authorized for, enables the TACACS+ server to behave differently for different types of authorization requests. You can use following values: slip, ppp, arap, shell, tty-daemon, connection, system, and firewall. Specifying this setting is required. Note that the majority of TACACS+ implementations are of service type ppp, so try that first.

ConfigSync¶

Clustering properties for onboarding a BIG-IP.

Properties:

Name (Type)	Default	Values	Description
class (*string*)	•	"ConfigSync"	Indicates that this property contains config sync IP configuration.
configsyncIp (*string*)	•	•	ConfigSync IP

DagGlobals¶

Network properties for onboarding a BIG-IP.

Properties:

Name (Type)	Default	Values	Description
class (*string*)	•	"DagGlobals"	Indicates that this property contains DAG Globals configuration.
icmpHash (*string*)	"icmp"	"icmp", "ipicmp"	Specifies ICMP hash for ICMP echo request and ICMP echo reply in SW DAG.
ipv6PrefixLength (*integer*)	128	[0, 128]	Specifies whether SPDAG or IPv6 prefix DAG should be used to disaggregate IPv6 traffic when vlan cmp hash is set to src-ip or dst-ip.
roundRobinMode (*string*)	"global"	"global", "local"	Specifies whether the round robin disaggregator (DAG) on a blade can disaggregate packets to all the TMMs in the system or only to the TMMs local to the blade.

DbVariables¶

System properties for onboarding a BIG-IP.

Properties:

Name (Type)	Default	Values	Description
class (*string*)	•	"DbVariables"	Indicates that this property contains global db variable configuration.

Device¶

Top level schema for onboarding a BIG-IP.

Properties:

Name (Type)	Default	Values	Description
$schema (*string*)	•	format: uri	URL of schema against which to validate. Used by validation in your local environment only (via Visual Studio Code, for example)
async (*boolean*)	false	true, false	Tells the API to return a 202 HTTP status before processing is complete. User must then poll for status.
class (*string*)	•	"Device"	Indicates this JSON document is a Device declaration
Common (*Device_Common*)	•	•	Special tenant Common holds objects other tenants can share

Name (Type)	Default	Values	Description
controls (*Device_controls*)	•	•	Options to control configuration process
Credentials (*array<Device_Credentials>*)	•	-, -	Credentials which can be referenced from other parts of the declaration or the remote wrapper.
label (*string*)	•	•	•
result (*Device_result*)	•	•	Status of current request. This is set by the system.
schemaVersion (*string*)	•	"1.15.0", "1.14.0", "1.13.0", "1.12.0", "1.11.1", "1.11.0", "1.10.0", "1.9.0", "1.8.0", "1.7.0", "1.6.1", "1.6.0", "1.5.1", "1.5.0", "1.4.1", "1.4.0", "1.3.0", "1.2.0", "1.1.0", "1.0.0"	Version of Declarative Onboarding schema this declaration uses.
webhook (*string*)	•	format: uri	URL to post results to

Device_Common¶

Device Common possible properties

Properties:

Name (Type)	Default	Values	Description
class (*string*)	•	"Tenant"	•
hostname (*string*)	•	format: hostname	Hostname to set for the device. Note: If you set the hostname as part of the System class, you CANNOT set a hostname in the Common class (they are mutually exclusive).

Device_controls¶

Device controls possible properties

Properties:

Name (Type)	Default	Values	Description
class (*string*)	•	"Controls"	•
trace (*boolean*)	false	true, false	If true, create a detailed trace of the configuration process for subsequent analysis (default false). Warning: trace files may contain sensitive configuration data.

Name (Type)	Default	Values	Description
traceResponse (*boolean*)	false	true, false	If true, the response will contain the trace files.
userAgent (*string*)	•	•	User Agent information to include in TEEM report.

Device_Credentials¶

Device Credentials possible properties when object type

Properties:

Name (Type)	Default	Values	Description
password (*string*)	•	regex: ^.{0,254}$	Password for username account. This is generally not required to configure 'localhost' and is not required when you populate tokens
tokens (*object*)	•	•	One or more HTTP headers (each a property, like 'X-F5-Auth-Token': 'MF6APSRUYKTMSDBEOOEWLCNSO2') you want to send with queries to the device management service as authentication/authorization tokens
username (*string*)	•	regex: ^[^:]{0,254}$	Username of principal authorized to modify configuration of device (may not include the character ':'). NOTE: this is generally not required to configure 'localhost' because client authentication and authorization precede invocation of DO. It is also not required for any host if you populate tokens

Device_result¶

Device result possible properties

Properties:

Name (Type)	Default	Values	Description
class (*string*)	•	"Result"	•
code (*string*)	•	"OK", "ERROR"	Status code.
message (*string*)	•	•	Further detail about the status.

DeviceCertificate¶

System properties for onboarding a BIG-IP.

Properties:

Name (Type)	Default	Values	Description
certificate (*reference*)	•	•	X.509 public-key certificate
class (*string*)	•	"DeviceCertificate"	Indicates that this property contains device certificate information
privateKey (*reference*)	•	•	Private key matching certificate's public key (optional)

DeviceGroup¶

Clustering properties for onboarding a BIG-IP.

Properties:

Name (Type)	Default	Values	Description
asmSync (*boolean*)	false	true, false	Whether or not the device group should sync ASM properties
autoSync (*boolean*)	false	true, false	Whether or not the device group should auto sync
class (*string*)	•	“DeviceGroup”	Indicates that this property contains device group configuration.
fullLoadOnSync (*boolean*)	false	true, false	Whether or not the device group should do a full load on sync
members (*array<string>*)	•	•	Members to add to the device group if they are already in the trust domain
networkFailover (*boolean*)	false	true, false	Whether or not the device group supports network failover
owner (*string*)	•	•	Owning device. Config will be pushed from this device. If this is present, device group will only be created if the current device is the owner. If not present, device group will be created if it does not exist
saveOnAutoSync (*boolean*)	false	true, false	Whether or not the device group should save on auto sync
type (*string*)	•	“sync-failover”, “sync-only”	Type of the device group

DeviceTrust¶

Clustering properties for onboarding a BIG-IP.

Properties:

Name (Type)	Default	Values	Description
class (*string*)	•	“DeviceTrust”	Indicates that this property contains device trust configuration.
localPassword (*string*)	•	•	The password for the localUsername
localUsername (*string*)	•	•	The username for the local device
remoteHost (*string*)	•	•	The remote hostname or IP address
remotePassword (*string*)	•	•	Password for the remote user in remoteUsername
remoteUsername (*string*)	•	•	An admin user on the remote host

Disk¶

System properties for onboarding a BIG-IP.

Properties:

Name (Type)	Default	Values	Description
applicationData (*integer*)	•	[0, infinity]	Specifies the size in kilobytes for the application data. This size should be less than the current size. This API is experimental and subject to change.
class (*string*)	•	"Disk"	Indicates this contains Disk configuration. This API is experimental and subject to change.

DNS¶

System properties for onboarding a BIG-IP.

Properties:

Name (Type)	Default	Values	Description
class (*string*)	•	"DNS"	Indicates that this property contains DNS configuration.
nameServers (*array<string>*)	•	•	IP addresses of name servers to use for DNS.
search (*array<string>*)	•	format: hostname	Search domain to use for DNS.

DNS_Resolver¶

Network properties for onboarding a BIG-IP.

Properties:

Name (Type)	Default	Values	Description
answerDefaultZones (*boolean*)	false	true, false	Specifies whether the resolver answers queries for default zones: localhost, reverse 127.0.0.1, ::1, and AS112 zones.
cacheSize (*integer*)	5767168	[10, 9437184]	Specifies the maximum cach size in bytes of the DNS Resolver object
class (*string*)	•	"DNS_Resolver"	Indicates that this property contains DNS Resolver configuration.
forwardZones (*array<DNS_Resolver_forwardZones>*)	•	•	Forward zones on a DNS Resolver. A given zone name should only use the symbols allowed for a fully qualified domain name (FQDN), namely ASCII letters a through z, digits 0 through 9, hyphen, nad period. For example site.example.com would be a valid zone name. A DNS Resolver configured with a forward zone will forward any queries that resulted in a cache-miss and which also match a configured zone name, to the nameserver specified on the zone.
randomizeQueryNameCase (*boolean*)	true	true, false	Specifies whether the resolver randomizes the case of query names.
routeDomain (*string*)	"0"	•	Specifies the name of the route domain the resolver uses for outbound traffic.
useIpv4 (*boolean*)	true	true, false	Specifies whether the resolver sends DNS queries to IPv4

Name (Type)	Default	Values	Description
useIpv6 (*boolean*)	true	true, false	Specifies whether the resolver sends DNS queries to IPv6
useTcp (*boolean*)	true	true, false	Specifies whether the resolver sends DNS queries over TCP
useUdp (*boolean*)	true	true, false	Specifies whether the resolver sends DNS queries over UDP

DNS_Resolver_forwardZones¶

DNS_Resolver forwardZones possible properties when object type

Properties:

Name (Type)	Default	Values	Description
name (*string*)	•	format: hostname	Name of a forward zone.
nameservers (*array<string>*)	•	•	Specifies the IP address and service port of a recursive nameserver that answers DNS queries when the response cannot be found in the internal DNS resolver cache. Enter each address in the format address:port (IPv4) or addrss.port (IPv6). The port is usually 53.

FailoverUnicast¶

Clustering properties for onboarding a BIG-IP.

Properties:

Name (Type)	Default	Values	Description
address (*string*)	•	•	IP address to listen on for failover heartbeats
addressPorts (*array<FailoverUnicast_addressPorts>*)	•	•	An array of address and port objects, that will create multiple failover unicast objects in the BIG-IP device. This array is mutually exclusive from using the other address and port features. Available in DO 1.15 and later.
class (*string*)	•	"FailoverUnicast"	Indicates that this property contains failover unicast address configuration.
port (*number*)	•	•	Port to listen on for failover heartbeats. The default is 1026.

FailoverUnicast_addressPorts¶

FailoverUnicast addressPorts possible properties when object type

Properties:

Name (Type)	Default	Values	Description
address (*string*)	•	•	IP address to listen on for failover heartbeats
port (*number*)	1026	•	Port to listen on for failover heartbeats

HTTPD¶

System properties for onboarding a BIG-IP.

Properties:

Name (Type)	Default	Values	Description
allow (*string* | *array<string>*)	all	•	Configures IP addresses for the HTTP clients from which the httpd daemon accepts requests.
authPamIdleTimeout (*integer*)	1200	[120, 2147483647]	Specifies the number of seconds of inactivity that can elapse before the GUI session is automatically logged out.
class (*string*)	•	"HTTPD"	Configures the HTTP daemon for the system. Important: F5 Networks recommends that users of the Configuration utility exit the utility before changes are made to the system using the httpd component. This is because making changes to the system using this component causes a restart of the httpd daemon. Additionally, restarting the httpd daemon creates the necessity for a restart of the Configuration utility.
maxClients (*integer*)	10	[10, 256]	Maximum number of clients allowed to be simultaneously connected.
sslCiphersuite (*array<string>*)	ECDHE-RSA-AES128-GCM-SHA256, ECDHE-RSA-AES256-GCM-SHA384, ECDHE-RSA-AES128-SHA, ECDHE-RSA-AES256-SHA, ECDHE-RSA-AES128-SHA256, ECDHE-RSA-AES256-SHA384, ECDHE-ECDSA-AES128-GCM-SHA256, ECDHE-ECDSA-AES256-GCM-SHA384, ECDHE-ECDSA-AES128-SHA, ECDHE-ECDSA-AES256-SHA, ECDHE-ECDSA-AES128-SHA256, ECDHE-ECDSA-AES256-SHA384, AES128-GCM-SHA256,	"ECDHE-RSA-AES256-GCM-SHA384", "ECDHE-ECDSA-AES256-GCM-SHA384", "ECDHE-RSA-AES256-SHA384", "ECDHE-ECDSA-AES256-SHA384", "ECDHE-RSA-AES256-SHA", "ECDHE-ECDSA-AES256-SHA", "DH-DSS-AES256-GCM-SHA384", "DHE-DSS-AES256-GCM-SHA384", "DH-RSA-AES256-GCM-SHA384", "DHE-RSA-AES256-GCM-SHA384", "DHE-RSA-AES256-SHA256", "DHE-DSS-	Specifies the ciphers that the system uses.

Name (Type)	Default	Values	Description
	AES256-GCM-SHA384, AES128-SHA, AES256-SHA, AES128-SHA256, AES256-SHA256	AES256-SHA256”, “DH-RSA-AES256-SHA256”, “DH-DSS-AES256-SHA256”, “DHE-RSA-AES256-SHA”, “DHE-DSS-AES256-SHA”, “DH-RSA-AES256-SHA”, “DH-DSS-AES256-SHA”, “DHE-RSA-CAMELLIA256-SHA”, “DHE-DSS-CAMELLIA256-SHA”, “DH-RSA-CAMELLIA256-SHA”, “DH-DSS-CAMELLIA256-SHA”, “ECDH-RSA-AES256-GCM-SHA384”, “ECDH-ECDSA-AES256-GCM-SHA384”, “ECDH-RSA-AES256-SHA384”, “ECDH-ECDSA-AES256-SHA384”, “ECDH-RSA-AES256-SHA”, “ECDH-ECDSA-AES256-SHA”, “AES256-GCM-SHA384”, “AES256-SHA256”, “AES256-SHA”, “CAMELLIA256-SHA”, “PSK-AES256-CBC-SHA”, “ECDHE-RSA-AES128-GCM-SHA256”, “ECDHE-ECDSA-	

Name (Type)	Default	Values	Description
		AES128-GCM-SHA256”, “ECDHE-RSA-AES128-SHA256”, “ECDHE-ECDSA-AES128-SHA256”, “ECDHE-RSA-AES128-SHA”, “ECDHE-ECDSA-AES128-SHA”, “DH-DSS-AES128-GCM-SHA256”, “DHE-DSS-AES128-GCM-SHA256”, “DH-RSA-AES128-GCM-SHA256”, “DHE-RSA-AES128-GCM-SHA256”, “DHE-RSA-AES128-SHA256”, “DHE-DSS-AES128-SHA256”, “DH-RSA-AES128-SHA256”, “DH-DSS-AES128-SHA256”, “DHE-RSA-AES128-SHA”, “DHE-DSS-AES128-SHA”, “DH-RSA-AES128-SHA”, “DH-DSS-AES128-SHA”, “DHE-RSA-SEED-SHA”, “DHE-DSS-SEED-SHA”, “DH-RSA-SEED-SHA”, “DH-DSS-SEED-SHA”, “DHE-RSA-CAMELLIA128-SHA”, “DHE-	

Name (Type)	Default	Values	Description
		DSS-CAMELLIA128-SHA”, “DH-RSA-CAMELLIA128-SHA”, “DH-DSS-CAMELLIA128-SHA”, “ECDH-RSA-AES128-GCM-SHA256”, “ECDH-ECDSA-AES128-GCM-SHA256”, “ECDH-RSA-AES128-SHA256”, “ECDH-ECDSA-AES128-SHA256”, “ECDH-RSA-AES128-SHA”, “ECDH-ECDSA-AES128-SHA”, “AES128-GCM-SHA256”, “AES128-SHA256”, “AES128-SHA”, “SEED-SHA”, “CAMELLIA128-SHA”, “PSK-AES128-CBC-SHA”, “ECDHE-RSA-RC4-SHA”, “ECDHE-ECDSA-RC4-SHA”, “ECDH-RSA-RC4-SHA”, “ECDH-ECDSA-RC4-SHA”, “RC4-SHA”, “RC4-MD5”, “PSK-RC4-SHA”, “ECDHE-RSA-DES-CBC3-SHA”, “ECDHE-ECDSA-DES-CBC3-SHA”, “EDH-RSA-DES-CBC3-SHA”, “EDH-DSS-DES-CBC3-SHA”, “DH-RSA-DES-	

Name (Type)	Default	Values	Description
		CBC3-SHA”, “DH-DSS-DES-CBC3-SHA”, “ECDH-RSA-DES-CBC3-SHA”, “ECDH-ECDSA-DES-CBC3-SHA”, “DES-CBC3-SHA”, “PSK-3DES-EDE-CBC-SHA”, “EDH-RSA-DES-CBC-SHA”, “EDH-DSS-DES-CBC-SHA”, “DES-CBC-SHA”, “EXP-EDH-RSA-DES-CBC-SHA”, “EXP-EDH-DSS-DES-CBC-SHA”, “EXP-DES-CBC-SHA”, “EXP-RC2-CBC-MD5”, “EXP-RC4-MD5”	
sslProtocol (*string*)	“all -SSLv2 -SSLv3 -TLSv1”	•	The list of SSL protocols to accept on the management console. A space-separated list of tokens in the format accepted by the Apache mod_ssl SSLProtocol directive.

License¶

System properties for onboarding a BIG-IP.

Properties:

Name (Type)	Default	Values	Description
licenseType (*reference*)	•	•	•
unitOfMeasure (*reference*)	“monthly”	•	•

MAC_Masquerade¶

Clustering properties for onboarding a BIG-IP.

Properties:

Name (Type)	Default	Values	Description
class (*string*)	•	“MAC_Masquerade”	Indicates that this property contains MAC masquerade configuration.
source (*MAC_Masquerade_source*)	•	•	MAC address source to use for masquerading.

Name (Type)	Default	Values	Description
trafficGroup (*string*)	"traffic-group-1"	"traffic-group-local-only", "traffic-group-1"	Traffic group to apply the MAC masquerade to.

MAC_Masquerade_source¶

MAC_Masquerade source possible properties

Properties:

Name (Type)	Default	Values	Description
interface (*string*)	•	•	Generate a MAC address from an interface

ManagementRoute¶

System properties for onboarding a BIG-IP.

Properties:

Name (Type)	Default	Values	Description
class (*string*)	•	"ManagementRoute"	Indicates this property contains management route configuration
gw (*string*)	•	•	Gateway for the management route.
mtu (*integer*)	•	[0, 65535]	MTU for the management route.
network (*string*)	"default"	•	IP address/netmask for the management route
type (*string*)	•	"interface", "blackhole"	Type of the management route

NTP¶

System properties for onboarding a BIG-IP.

Properties:

Name (Type)	Default	Values	Description
class (*string*)	•	"NTP"	Indicates that this property contains NTP configuration.
servers (*array<string>*)	•	•	IP addresses of servers to use for NTP.
timezone (*string*)	•	•	The timezone to set.

Provision¶

System properties for onboarding a BIG-IP.

Properties:

Name (Type)	Default	Values	Description

Name (Type)	Default	Values	Description
class (*string*)	•	“Provision”	Indicates that this property contains module provisioning configuration.

RemoteAuthRole¶

Authentication properties for onboarding a BIG-IP.

Properties:

Name (Type)	Default	Values	Description
attribute (*string*)	•	•	Specifies an attribute-value pair that an authentication server supplies to the BIG-IP system to match against entries in /config/bigip/auth/remoterole. The specified pair typically identifies users with access rights in common. This option is required.
class (*string*)	•	“RemoteAuthRole”	Indicates that this property contains RemoteAuthRole configuration.
console (*string*)	“disabled”	“disabled”, “tmsh”	Specifes if the remotely-authenticated users have tmsh console access or not. Accepted values are ‘disabled’ and ‘tmsh’.
lineOrder (*integer*)	•	[0, 4294967295]	The BIG-IP only allows one role per user for each partition/tenant. Because some remote servers allow multiple user roles, the BIG-IP uses the lineOrder parameter to choose one of the conflicting roles for the user at login time. In these cases, the system chooses the role with the lowest line-order number. See line order in the BIG-IP documentation for more information and examples.
remoteAccess (*boolean*)	false	true, false	Enables the specified group of remotely-authenticated users, remote access.
role (*string*)	“no-access”	“admin”, “application-editor”, “auditor”, “certificate-manager”, “firewall-manager”, “fraud-protection-manager”, “guest”, “irule-manager”, “manager”, “no-access”, “operator”, “resource-admin”, “user-manager”, “web-application-security-administrator”, “web-application-security-editor”	Specifies the role that you want to grant to the specified group of remotely-authenticated users.

Name (Type)	Default	Values	Description
userPartition (*string*)	“Common”	“all”, “Common”	Specifies the BIG-IP partition to which you are assigning access to the specified group of remotely-authenticated users. The default value is Common. This option is required.

Route¶

Network properties for onboarding a BIG-IP.

Properties:

Name (Type)	Default	Values	Description
class (*string*)	•	“Route”	Indicates that this property contains Route configuration.
gw (*string*)	•	•	Gateway for the route.
localOnly (*boolean*)	false	true, false	A boolean to indicate if the Route should be added to the LOCAL_ONLY partition. ‘Across Network’ clusters in AWS require this partition to be configured.
mtu (*integer*)	•	[0, 9198]	MTU for the route.
network (*string*)	“default”	•	IP address/netmask for route
target (*string*)	•	•	The VLAN or Tunnel for the Route.

RouteDomain¶

Network properties for onboarding a BIG-IP.

Properties:

Name (Type)	Default	Values	Description
bandWidthControllerPolicy (*string*)	•	•	Specifies the bandwidth controller policy for the route domain.
class (*string*)	•	“RouteDomain”	Indicates that this property contains Route Domain configuration.
connectionLimit (*integer*)	0	[0, 4294967295]	The connection limit for the route domain.
enforcedFirewallPolicy (*string*)	•	•	Specifies an enforced firewall policy on the route domain.
flowEvictionPolicy (*string*)	•	•	Specifies a flow eviction policy for the route domain to use.
id (*integer*)	•	[0, 65534]	Specifies a unique numeric identifier for the route domain.
ipIntelligencePolicy (*string*)	•	•	Specifies an IP intelligence policy for the route domain to use.

Name (Type)	Default	Values	Description
routingProtocols (*array<string>*)	•	“BFD”, “BGP”, “IS-IS”, “OSPFv2”, “OSPFv3”, “PIM”, “RIP”, “RIPng”	Specifies routing protocols for the system to use in the route domain.
securityNatPolicy (*string*)	•	•	Specifies the security NAT policy for the route domain.
servicePolicy (*string*)	•	•	Specifies the service policy for the route domain.
stagedFirewallPolicy (*string*)	•	•	Specifies a staged firewall policy on the route domain.
strict (*boolean*)	true	true, false	Determines whether a connection can span route domains.
vlans (*array<string>*)	•	•	Specifies VLANS for the system to use in the route domain.

SelfIp¶

Network properties for onboarding a BIG-IP.

Properties:

Name (Type)	Default	Values	Description
address (*string*)	•	format: f5ip	IP address.
allowService (*string* | *array<string>*)	“default”	•	Which services (ports) to allow on the self IP. Value should be ‘all’, ‘none’, ‘default’, or array of ‘<service:port (service:port)>
class (*string*)	•	“SelfIp”	Indicates that this property contains Self IP configuration.
trafficGroup (*string*)	“traffic-group-local-only”	“traffic-group-local-only”, “traffic-group-1”	Traffic group for the Self IP.
vlan (*string*)	•	•	VLAN or Tunnel for the self IP.

SnmpAgent¶

System properties for onboarding a BIG-IP.

Properties:

Name (Type)	Default	Values	Description
allowList (*array<string>*)	•	format: f5ip	Allowed client IP addresses.
class (*string*)	•	“SnmpAgent”	Indicates that this property contains basic SNMP agent configuration.
contact (*string*)	•	•	The name of the person who administers the SNMP service for this system.

Name (Type)	Default	Values	Description
location (*string*)	•	•	The description of this system’s physical location.

SnmpCommunity¶

System properties for onboarding a BIG-IP.

Properties:

Name (Type)	Default	Values	Description
access (*string*)	“ro”	“ro”, “rw”	Whether the user’s access level to the MIB is readOnly.
class (*string*)	•	“SnmpCommunity”	Indicates that this property contains SNMP v1 or v2c community configuration.
ipv6 (*boolean*)	false	true, false	Specifies whether the record applies to IPv6 addresses.
name (*string*)	•	•	Overrides using the object name as the community name. Use this if you want special characters in the community name.
oid (*string*)	•	•	Specifies the current object identifier (OID) for the record.
source (*string*)	•	•	Specifies the source address for access to the MIB.

SnmpTrapDestination¶

System properties for onboarding a BIG-IP.

Properties:

Name (Type)	Default	Values	Description
authentication (*SnmpTrapDestination_authentication*)	•	•	Specifies the user’s authentication method and password.
class (*string*)	•	“SnmpTrapDestination”	Indicates that this property contains SNMP trap configuration.
community (*string*)	•	•	Specifies the community name for the trap destination. — *Note: This property is available only when* **version** *is NOT ‘3’* —
destination (*string*)	•	•	Specifies the address for the trap destination.
engineId (*string*)	•	•	Specifies the unique identifier (snmpEngineID) of the remote SNMP protocol engine.
network (*string*)	•	“management”, “other”	Specifies the trap network. The system sends the SNMP trap out the specified network. ‘management’ specifies that the system sends the trap out of the management IP address. ‘other’ specifies that the system sends the trap out of the interface based on the routing tables.
port (*integer*)	•	[0, 65535]	Specifies the port for the trap destination.

Name (Type)	Default	Values	Description
privacy (*SnmpTrapDestination_privacy*)	•	•	Specifies the privacy protcol to use to deliver authentication information for this user.
securityName (*string*)	•	•	Specifies the user name the system uses to handle SNMP v3 traps.
version (*string*)	•	"1", "2c", "3"	Specifies to which Simple Network Management Protocol (SNMP) version the trap destination applies.

SnmpTrapDestination_authentication¶

SnmpTrapDestination authentication possible properties

Properties:

Name (Type)	Default	Values	Description
password (*string*)	•	•	Specifies the password for the user.
protocol (*string*)	•	"sha", "md5"	Authentication protocol.

SnmpTrapDestination_privacy¶

SnmpTrapDestination privacy possible properties

Properties:

Name (Type)	Default	Values	Description
password (*string*)	•	•	Specifies the password for the user.
protocol (*string*)	•	"aes", "des"	Specifies the encryption protocol.

SnmpTrapEvents¶

System properties for onboarding a BIG-IP.

Properties:

Name (Type)	Default	Values	Description
agentStartStop (*boolean*)	true	true, false	Indicates whether to send a trap when the SNMP agent starts/stops.
authentication (*boolean*)	false	true, false	Indicates whether to send authentication warning traps.
class (*string*)	•	"SnmpTrapEvents"	Indicates that this property contains SNMP trap configuration.
device (*boolean*)	true	true, false	Indicates whether to send device warning traps.

SnmpUser¶

System properties for onboarding a BIG-IP.

Properties:

Name (Type)	Default	Values	Description
access (*string*)	"ro"	"ro", "rw"	Whether the user's access level to the MIB is readOnly.
authentication (*SnmpUser_authentication*)	•	•	Specifies the user's authentication method and password.
class (*string*)	•	"SnmpUser"	Indicates that this property contains SNMP v3 user configuration.
name (*string*)	•	•	Overrides using the object name as the username. Use this if you want special characters in the username.
oid (*string*)	".1"	•	Specifies the current object identifier (OID) for the record.
privacy (*SnmpUser_privacy*)	•	•	Specifies the privacy protcol to use to deliver authentication information for this user.

SnmpUser_authentication¶

SnmpUser authentication possible properties

Properties:

Name (Type)	Default	Values	Description
password (*string*)	•	•	Specifies the password for the user.
protocol (*string*)	"sha"	"sha", "md5"	Authentication protocol.

SnmpUser_privacy¶

SnmpUser privacy possible properties

Properties:

Name (Type)	Default	Values	Description
password (*string*)	•	•	Specifies the password for the user.
protocol (*string*)	"aes"	"aes", "des"	Specifies the encryption protocol.

SSHD¶

System properties for onboarding a BIG-IP.

Properties:

Name (Type)	Default	Values	Description
allow (*string* | *array<string>*)	•	•	Specifies the list of IP addresses that are allowed to log in to the system. Allow all addresses by using the 'all' value or disallow all addresses using the 'none' value.
banner (*string*)	•	•	Enables or disabled the display of the banner text field when a user logs in.

Name (Type)	Default	Values	Description
ciphers (*array<string>*)	•	“3des-cbc”, “aes128-ctr”, “aes192-ctr”, “aes256-ctr”, “aes128-cbc”, “aes192-cbc”, “aes256-cbc”, “aes128-gcm@openssh.com (mailto:aes128-gcm%40openssh.com)”, “aes256-gcm@openssh.com (mailto:aes256-gcm%40openssh.com)”, “arcfour”, “arcfour128”, “arcfour256”, “blowfish-cbc”, “cast128-cbc”, “chacha20-poly1305@openssh.com (mailto:chacha20-poly1305%40openssh.com)”	Specifies the ciphers to be included.
class (*string*)	•	“SSHD”	Indicates this contains SSH configuration.
inactivityTimeout (*integer*)	0	[0, 2147483647]	Specifies the number of seconds before inactivity causes an SSH session to log out.
loginGraceTime (*integer*)	•	[-infinity, infinity]	Specifies the login grace period that will be included. This is in the number of seconds.

Name (Type)	Default	Values	Description
MACS (*array<string>*)	•	“hmac-sha1”, “hmac-ripemd160”, “hmac-md5”, “hmac-md5-96”, “hmac-sha1-96”, “hmac-sha2-256”, “hmac-sha2-512”, “hmac-md5-etm@openssh.com (mailto:hmac-md5-etm%40openssh.com)”, “hmac-md5-96-etm@openssh.com (mailto:hmac-md5-96-etm%40openssh.com)”, “hmac-ripemd160-etm@openssh.com (mailto:hmac-ripemd160-etm%40openssh.com)”, “hmac-sha1-etm@openssh.com (mailto:hmac-sha1-etm%40openssh.com)”, “hmac-sha1-96-etm@openssh.com (mailto:hmac-sha1-96-etm%40openssh.com)”, “hmac-sha2-256-etm@openssh.com (mailto:hmac-sha2-256-etm%40openssh.com)”, “hmac-sha2-512-etm@openssh.com (mailto:hmac-sha2-512-etm%40openssh.com)”, “umac-64@openssh.com (mailto:umac-64%40openssh.com)”, “umac-128@openssh.com (mailto:umac-128%40openssh.com)”, “umac-64-etm@openssh.com (mailto:umac-64-etm%40openssh.com)”, “umac-128-etm@openssh.com (mailto:umac-128-etm%40openssh.com)”	Specifies the MACs that will be included.
maxAuthTries (*integer*)	•	[-infinity, infinity]	Specifies the max auth tries to be included.
maxStartups (*string*)	•	•	Specifies the max startups to include.
protocol (*integer*)	•	[1, 2]	Specifies the protocol to be included.

SyslogRemoteServer¶

System properties for onboarding a BIG-IP.

Properties:

Name (Type)	Default	Values	Description
class (*string*)	•	“SyslogRemoteServer”	Indicates that this property contains Syslog Remote Server Information
host (*string*)	•	•	Specifies the IP address of a remote server to which syslog sends messages.
localIp (*string*)	•	•	Specifies the IP address of the interface syslog binds with in order to log messages to a remote host.
remotePort (*integer*)	514	[0, 65535]	Specifies the port to which the syslog sends messages.

System¶

System properties for onboarding a BIG-IP.

Properties:

Name (Type)	Default	Values	Description
autoCheck (*boolean*)	•	true, false	Enables the BIG-IP system to check for and recommend software updates.
autoPhonehome (*boolean*)	•	true, false	Enables the BIG-IP system to send non-confidential, high-level device information to F5 in order to help determine product usage to optimize product development.
class (*string*)	•	“System”	Indicates this property contains global system settings
cliInactivityTimeout (*integer*)	0	[0, 128849018820]	Configure automatic logout for idle users in TMSH interactive mode. A setting other than 0 automatically logs a user out after a specified number of seconds, which must be entered in multiples of 60. The default value 0 means that no timeout is set.
consoleInactivityTimeout (*integer*)	0	[0, 2147483647]	Configure automatic logout for idle serial console sessions (command line sessions) in seconds. The default value 0 means that no timeout is set.
guiAuditLog (*boolean*)	•	true, false	Enables audit logging for the GUI. Only available on TMOS v14+
hostname (*string*)	•	format: hostname	Hostname to set for the device. Note: If you set the hostname as part of the Common class, you CANNOT set a hostname in the System class (they are mutually exclusive).
mcpAuditLog (*string*)	•	“disable”, “enable”, “verbose”, “all”	Enables audit logging for MCP.
tmshAuditLog (*boolean*)	•	true, false	Enables audit logging for tmsh.

TrafficControl¶

System properties for onboarding a BIG-IP.

Properties:

Name (Type)	Default	Values	Description
acceptIpOptions (*boolean*)	false	true, false	Specifies whether the system accepts IPv4 packets with IP Options.
acceptIpSourceRoute (*boolean*)	false	true, false	Specifies whether the system accepts IPv4 packets with IP source route options that are destined for TMM. To enable this option, you must also enable the acceptIpOptions option.
allowIpSourceRoute (*boolean*)	false	true, false	Specifies whether the system allows IPv4 packets with IP source route options enabled to be routed through TMM. To enable this option, you must also enable the acceptIpOptions option.
class (*string*)	•	"TrafficControl"	Indicates this property contains traffic control configuration
continueMatching (*boolean*)	false	true, false	Specifies whether the system matches against a less-specific virtual server when the more-specific one is disabled or rejects / drops the packets depending on the value of rejectUnmatched.
maxIcmpRate (*integer*)	100	[0, 2147483647]	Specifies the maximum rate per second at which the system issues ICMP errors.
maxPortFindLinear (*integer*)	16	[0, 61439]	Specifies the maximum of ports to linearly search for outbound connections
maxPortFindRandom (*integer*)	16	[0, 1024]	Specifies the maximum of ports to randomly search for outbound connections
maxRejectRate (*integer*)	250	[1, 1000]	Specifies the maximum rate per second at which the system issues reject packets (TCP RST or ICMP port unreach).
maxRejectRateTimeout (*integer*)	30	[0, 300]	Specifies the time in seconds which the system ignores ICMP port unreach and TCP RST ratelimits on becoming active after a failover.
minPathMtu (*reference*)	296	•	Specifies the minimum packet size that can traverse the path without suffering fragmentation
pathMtuDiscovery (*boolean*)	true	true, false	Specifies that the system discovers the MTU that it can send over a path without fragmenting TCP packets
portFindThresholdTimeout (*integer*)	30	[0, 300]	Specifies the threshold warning's timeout which is the time in seconds since the last trigger value was hit and will drop the tuple if not hit.
portFindThresholdTrigger (*integer*)	8	[1, 12]	Specifies the threshold warning's trigger which is the value of random port attempts when attempting to find an unused outbound port for a connection.
portFindThresholdWarning (*boolean*)	true	true, false	Specifies if the ephemeral port-exhaustion threshold warning is to be monitored.
rejectUnmatched (*boolean*)	true	true, false	Specifies, when enabled, that the system returns a TCP RST or ICMP port unreach packet if no virtual servers on the system match the destination address of the incoming packet. When disabled, the system silently drops the unmatched packet.

TrafficGroup¶

Clustering properties for onboarding a BIG-IP.

Properties:

Name (Type)	Default	Values	Description
autoFailbackEnabled (*boolean*)	false	true, false	Specifies whether the traffic group fails back to the default device.
autoFailbackTime (*integer*)	60	[0, 300]	Specifies the time required to fail back.
class (*string*)	•	“TrafficGroup”	Indicates that this property contains Traffic Group configuration.
failoverMethod (*string*)	“ha-order”	“ha-order”	Specifies the method used to decide if the current device needs to failover the traffic-group to another device. If the failover-method is set to ha-order, a list of devices and their respective HA load is used to decide the next one to take over if the current devices fails.
haLoadFactor (*integer*)	1	[1, 1000]	Specifies a number for this traffic group that represents the load this traffic group presents to the system relative to other traffic groups. This allows the failover daemon to load balance the active traffic groups amongst the devices.
haOrder (*array<string>*)	•	•	This list of devices specifies the order in which the devices will become active for the traffic group when a failure occurs. This list may contain zero, one, or more entries up to the number of devices in the failover device group.

Trunk¶

Network properties for onboarding a BIG-IP.

Properties:

Name (Type)	Default	Values	Description
class (*string*)	•	“Trunk”	Indicates that this property contains Trunk configuration.
distributionHash (*string*)	”dst-mac”	“dst-mac”, “src-dst-ipport”, “src-dst-mac”	Specifies the basis for the hash that the system uses as the frame distribution algorithm. Choices are ‘dst-mac’ (use the destination MAC addresses), ‘src-dist-mac’ (use the source, destination, and MAC addresses), or ‘src-dst-ipport’ (use the source and destination IP addresses and ports).
interfaces (*array<string>*)		•	Interfaces for the Trunk. The number of interfaces used is recommended to be a power of 2 (for example 2, 4, or 8). Interfaces must be untagged.
lacpEnabled (*boolean*)	false	true, false	Specifies, when true, that the system supports the link aggregation control protocol (LACP), which monitors the trunk by exchanging control packets over the member links to determine the health of the links.
lacpMode (*string*)	“active”	“active”, “passive”	Specifies the operation mode for LACP if the lacp option is enabled for the trunk. The values are ‘active’ (specifies the system periodically transmits LACP packets, regardless of the control value of the peer system) and ‘passive’ (specifies the system periodically transmits LACP packets, unless the control value of the peer system is active).

Name (Type)	Default	Values	Description
lacpTimeout (*string*)	“long”	“long”, “short”	Specifies the rate at which the system sends the LACP control packets.
linkSelectPolicy (*string*)	“auto”	“auto”, “maximum-bandwidth”	Sets the LACP policy that the trunk uses to determine which member link (interface) can handle new traffic.
qinqEthertype (*string*)	“0x8100”	regex: ^0x[a-fA-F0-9]{4}$	Specifies the ether-type value used for the packets handled on this trunk when it is a member in a QinQ vlan.
spanningTreeEnabled (*boolean*)	true	true, false	Enables the spanning tree protocols (STP).

Tunnel¶

Network properties for onboarding a BIG-IP.

Properties:

Name (Type)	Default	Values	Description
autoLastHop (*string*)	“default”	“default”, “enabled”, “disabled”	Specifies that packets are returned to the MAC address from which they were sent when enabled. The default setting specifies that the system uses the default route to send back the request.
class (*string*)	•	“Tunnel”	Indicates that this property contains Tunnel configuration.
mtu (*integer*)	0	[0, 65535]	Specifies the maximum transmission unit of the Tunnel.
tunnelType (*string*)	•	“tcp-forward”	Specifies the profile that you want to associate with the Tunnel.
typeOfService (*string* | *integer*)	“preserve”	•	Specifies a value for insertion into the Type of Service octet within the IP header of the encapsulating header of transmitted packets.
usePmtu (*boolean*)	true	true, false	Enable or disable the Tunnel to use Path MTU information provided by ICMP NeedFrag error messages.

User¶

System properties for onboarding a BIG-IP.

Properties:

Name (Type)	Default	Values	Description
class (*string*)	•	“User”	Indicates that this property contains user configuration. — *Note: This property is available only when* **userType** *is NOT ‘root’* —
keys (*array<string>*)		•	An array of public keys for the user. These will overwrite the /home/username/.ssh/authorized_keys if not root. — *Note: This property is available only when* **userType** *is NOT ‘root’* —
newPassword (*string*)	•	•	Password to set for the root user.
oldPassword (*string*)	•	•	Old password for the root user.

Name (Type)	Default	Values	Description
partitionAccess (*User_partitionAccess*)	•	•	Access control configuration. — *Note: This property is available only when* **userType** *is NOT 'root'* —
password (*string*)	•	•	Password for the user. — *Note: This property is available only when* **userType** *is NOT 'root'* —
shell (*string*)	"tmsh"	"bash", "tmsh", "none"	Shell for the user. — *Note: This property is available only when* **userType** *is NOT 'root'* —
userType (*string*)	•	"regular"	The type of user. — *Note: This property is available only when* **userType** *is NOT 'root'* —

User_partitionAccess¶

User partitionAccess possible properties

Properties:

Name (Type)	Default	Values	Description
all-partitions (*partitionAccess*)	•	•	•
Common (*partitionAccess*)	•	•	•

VLAN¶

Network properties for onboarding a BIG-IP.

Properties:

Name (Type)	Default	Values	Description
class (*string*)	•	"VLAN"	Indicates that this property contains VLAN configuration.
cmpHash (*string*)	"default"	"default", "dst-ip", "src-ip"	Specifies how the traffic on the VLAN will be disaggregated.
failsafeAction (*string*)	"failover-restart-tm"	"failover", "failover-restart-tm", "reboot", "restart-all"	Specifies the action for the system to take when the fail-safe mechanism is triggered
failsafeEnabled (*boolean*)	false	true, false	Enables a fail-safe mechanism that causes the active cluster to fail over to a redundant cluster when loss of traiffic is detected on a VLAN
failsafeTimeout (*integer*)	90	[10, 3600]	Specifies the number of seconds that an active unit can run without detecting network traffic on this VLAN before starting a failover
interfaces (*array<VLAN_interfaces>*)	•	•	Interfaces for the VLAN.
mtu (*integer*)	1500	[576, 9198]	MTU for the VLAN.
tag (*integer*)	•	[1, 4094]	Tag for the VLAN.

VLAN_interfaces¶

VLAN interfaces possible properties when object type

Properties:

Name (Type)	Default	Values	Description
name (*string*)	•	•	Name of the interface.
tagged (*boolean*)	•	true, false	Whether or not the interface is tagged. Default is true if a VLAN tag is provided, otherwise false.