LoadMaster Ansible Reference Guide

Reference Guide

UPDATED: 28 August 2020

Copyright Notices

Table of Contents

1 Introduction

Ansible is an open source automation platform. It can help with configuration management, application deployment, and task automation. In Kemp, we use Ansible to configure LoadMasters by running playbook configurations that are pushed out to LoadMasters through Kemp 360 Central.

First you define your layout in the Ansible playbook. When you run the playbook it calls Application Program Interface (API) commands on Kemp 360 Central, which then configures the LoadMasters connected to Kemp 360 Central.

Kemp have developed the following modules to be used in Ansible playbooks:

- Virtual Service
- Sub Virtual Service (SubVS)
- Real Server
- Add LDAP Authentication
- Add or Modify an LDAP-based SSO
- Add or Modify a RADIUS-based SSO
- Add or Modify a RADIUS-LDAP-based SSO
- Add or Modify a Certificate-based SSO
- Add or Modify a SAML-based SSO
- Add GEO FQDN Data
- Update GEO Maps and Clusters
- Update GEO Miscellaneous Options and GEO Partnership
- Upload Certificate
- Add Header Rule
- Delete Header Rule
- Replace Body Rule
- Replace Header Rule

- Match Content Rule
- Modify URL Rule
- Update Global Parameters

Requesting the API Key

To get the API key for Ansible, execute the following API command using your Kemp 360 Central credentials:

Make a curl request against your installation of Kemp 360 Central in the following way:

```
curl "https://{CENTRAL}/api/v1/user/authenticate/" --data "
{""username"":""admin"",""password"":""{PASSWORD}""}"
```

You should see a response similar to below:

```
{
"apikey": "abc123",
"id": 1,
"success": true
}
```

2 Modify a Virtual Service on a LoadMaster

2.1 Synopsis

This module adds or modifies a Virtual Service on a LoadMaster. The minimum supported LoadMaster firmware version is 7.2.47.0.

2.2 Parameters

Parameter	Choices/ Defaults	Comments
allow_https_2 str	**Choices:** • Y: Enabled • N: Disabled	Enable HTTP/2 for this Virtual Service. SSL Acceleration must be enabled before HTTP/2 can be enabled. The **BestPractices** cipher set should be used when HTTP/2 is enabled.
cache int	**Choices:** • 0: Disabled • 1: Enabled	Enable or disable the caching of URLs.
cache_percent str	**Choices:** • 0: Disabled • 1: Enabled	Specify the maximum percentage of cache space permitted for this Virtual Service. This is only relevant if **cache** is enabled. The maximum value is 100.
central_address str/required		The IP address of the Kemp 360 Central that the LoadMaster is added to.
central_api_key str/required		Admin-level API Key to access API services on Kemp 360 Central.
central_ username str/required		Username for Kemp 360 Central that is linked to the given API key.
cert_name		Identifier (name) of a preexisting certificate

str		on the LoadMaster to assign to the Virtual Service.
check_host str		The **check_use_11** parameter must be enabled to set the **check_host** value. When using HTTP/1.1 checking, the Real Servers require a Hostname be supplied in each request. If no value is set then this value is the IP address of the Virtual Service.
check_pattern str		When the **check_type** is set to http or https, this corresponds to the **Reply 200 Pattern** in the WUI. This parameter only applies when the HTTP Method is set to GET or POST. When the **check_type** is set to **bdata**: Specify the hexadecimal string that will be searched for in the response. Specify an empty value to unset **check_pattern**.
check_port int		The port to be checked. If a port is not specified, the Real Server port is used. Specify 0 to unset **check_port**.
check_post_data str		This parameter is only relevant if the **HTTP Method** is set to **POST**. When using the **POST** method, up to 2047 characters of POST data can be sent to the server.
check_type str	**Choices:** • icmp • https • http • tcp • smtp • nntp • ftp • telnet	Specify which protocol is to be used to check the health of the Real Server. The default value is dependent on the Virtual Service port.

	• pop3 • imap • rdp • bdata • ldap • none	
check_url str		When the **check_type** is set to **http** or **https** - by default, the health checker tries to access the URL / to determine if the machine is available. A different URL can be set in the **check_url** parameter. When the **check_type** is set to **bdata**: Specify a hexadecimal string to send to the Real Server. The maximum character length for the **check_url** parameter value is 126 characters.
check_use_11 str	**Choices:** • N: Disabled • Y: Enabled	By default, the health checker uses HTTP/1.0 when checking the Real Server status. Enabling **check_use_11** means HTTP/1.1 is used (which is more efficient).
check_use_get int	**Choices:** • 0: HEAD • 1: GET • 2: POST	When accessing the health check URL - the system can use the HEAD, the GET, or the POST method.
compress int	**Choices:** • 0 - Disabled • 1 - Enabled	When enabled, files sent from the LoadMaster are compressed with Gzip.
copy_hdr_from str	**Choices:** • 0 - Disabled • 1 - Enabled	The source header field to copy from when the request is sent to the LoadMaster.
copy_hdr_to		The name of the header field into which the source header is copied. This is used with

str		the **copy_hdr_from** variable.
cipher_set str	**Choices:** • Default • Default_NoRc4 • BestPractices • Intermediate_compatibility • Backward_compatibility • WUI • FIPS • Legacy • Null_Ciphers-<NameOfCustomCipherSet>	This parameter can be used to assign a cipher set to a Virtual Service. System-defined cipher sets and custom cipher sets can be assigned using this parameter.
ciphers str		Multiple ciphers can be assigned by inserting a colon between each cipher. When ciphers are assigned in this way, a Cipher Set called **Custom_ <VirtualServiceID>** is created/updated. Note: The assigned ciphers list is overwritten when ciphers are added in this way. Ensure to include all ciphers to be assigned.
default_gw str		Set the default gateway for this Virtual Service.
enable str/required	**Choices:** • N: Disabled • Y: Enabled (default)	Specify if the Virtual Service should be created in a live (enabled) state.
enhanced_ health_checks int	**Choices:** • 0: Disabled • 1: Enabled	Enabling the **enhanced_health_checks** parameter provides an additional health check parameter - **rs_minimum**. If the **enhanced_health_checks** parameter is disabled, the Virtual Service is considered

		available if at least one Real Server is available. If the **enhanced_health_checks** parameter is enabled, you can specify the minimum number of Real Servers that should be available to consider the Virtual Service to be available.
ensure str/required	Present (default)	Value set to indicate to Kemp 360 Central that this Virtual Service should always exist. This is set automatically by the module.
error_code int		If no Real Servers are available, the LoadMaster can terminate the connection with a HTTP error code. Specify the error code number in this parameter. Valid values are in the range 200-505.
error_url str		When no Real Servers are available and an error response is sent back to the client, you can also specify a redirect URL.
follow_vsid int		Specify the ID of the Virtual Service to follow. This is used for redirects.
force_l7 int	**Choices:** • 0: Disabled • 1: Enabled	Enabling **force_l7** means the Virtual Service runs at Layer 7 and not Layer 4. This may be needed for various reasons, including that only Layer 7 services can be non-transparent.
vs_ip str/required		The IPv4 Address to assign to the Virtual Service.
ldap_endpoint str		Specify the name of an LDAP endpoint to use for the health checks. If LDAP is selected as the **check_type**, the server IP address (or addresses) and ports from the LDAP endpoint configuration are used instead of the Real Server IP address and port.
lm_address str/required		IP address and port of the LoadMaster that contains the Virtual Service or SubVS that the Real Server should be created or modified on. The format is 'ip:port'.
match_body_		Names (Identifiers) of Match Body type

rules list		Content Rules to assign to the Virtual Service. These content rules must exist on the LoadMaster before being assigned to a Virtual Service.
match_length int		This parameter is only relevant when the **check_type** is set to **bdata**. By setting this you can specify the number of bytes to find the **check_pattern** within.
need_host_name int	**Choices:** • 0: Disabled • 1: Enabled	When this parameter is enabled, the hostname is always required to be sent in the TLS client hello message. If it is not sent, the connection is dropped.
nickname str/required	**Choices:** • 0: Disabled • 1: Enabled	The nickname to assign to the Virtual Service. It must be unique.
ocsp_verify int	**Choices:** • 0: Disabled • 1: Enabled	Verify (using Online Certificate Status Protocol (OCSP)) that the client certificate is valid.
persist str	**Choices:** • ssl • cookie • active-cookie • cookie-src • cookie-hash • cookie-hash-src • url • query-hash • hash • host • header	Specify the type of persistence (stickiness) to be used for this Virtual Service.

	• super • super-src • src • rdp • rdp-src • rdp-sb • rdp-sb-src • udpsip • none	
persist_timeout int		The length of time (in seconds) after the last connection that the LoadMaster remembers the persistence information. Timeout values are rounded down to an even number of minutes. Setting a value that is not a number of whole minutes results in the excess being ignored. Setting a value to less than 60 seconds results in a value of 0 being set, which disables persistency.
vs_port int/required		The port on which the Virtual Service must be active. Can be any valid port number from 3 to 65530, or a wildcard `*`.
preprocess_rules list		Names (Identifiers) of Preprocess type Content Rules to assign to the Virtual Service. These content rules must exist on the LoadMaster before being assigned to a Virtual Service.
vs_protocol str/required	**Choices:** • tcp: Use the TCP protocol • udp: Use the UDP protocol	The protocol type that this Virtual Service uses.
qos str	**Choices:** • Normal-Service • Minimize-Cost	Quality of Service sets a type of service that deals with packets, which treats and prioritizes the traffic.

	• Maximize-Reliability • Maximize-Throughput • Minimize-Delay	
request_rules list		Names (Identifiers) of Request type Content Rules to assign to the Virtual Service. These content rules must exist on the LoadMaster before being assigned to a Virtual Service.
response_rules list		Names (Identifiers) of Response type Content Rules to assign to the Virtual Service. These content rules must exist on the LoadMaster before being assigned to a Virtual Service.
rs_minimum int		An integer that specifies how many Real Servers must be up for a Virtual Service or SubVS to be considered up. It is an integer from 0 to *N*, where *N* is the number of Real Servers on this particular service. In practice, this value is usually 1.
rs_rule_ precedence int		This parameter should be used in conjunction with **rs_rule_precedence_pos**. This parameter is used to specify the name of the existing rule whose position you want to change.
rs_rule_ precedence_pos str		This parameter, in conjunction with the **rs_ rule_precedence** parameter, is used to change the position of the rule in a sequence of rules. For example, a position of 2 means the rule will be checked second.
schedule str	**Choices:** • Round-Robin • Weighted-Round-Robin • Least-Connection • Weighted-Least-Connection • Fixed-Weighting • Adaptive-Resource-Based	Specify the type of scheduling of new connections to Real Servers that is to be performed.

	• Source-IP-Hash • Weighted-Response-Time • SDN-Adaptive • URL-Hash	
ssl_acceleration int	**Choices:** • 0: Disabled • 1: Enabled	Enable SSL handling services for the Virtual Service.
ssl_reencrypt int	**Choices** • 0: Disabled • 1: Enabled	When this option is enabled, the SSL data stream is re-encrypted before sending to the Real Server. This parameter is only valid if SSL Acceleration is enabled.
ssl_rewrite str	**Choices** • None • http • https	When the Real Server rejects a request with a HTTP redirect, the requesting Location URL may need to be converted to specify HTTPS instead of HTTP (the opposite also applies).
subnet_ originating int	**Choices** • 0: Disabled • 1: Enabled	When transparency is disabled for a Virtual Service, the source IP address of connections to Real Servers is the Virtual Service. When enabled, the source IP address is the local address of the LoadMaster. If the Real Server is on a subnet, the subnet address of the LoadMaster is used.
tls_type list	**Choices** • SSLv3 • TLS1.0 • TLS1.1 • TLS1.2 • TLS1.3	Specify which of the following protocols to support; SSLv3, TLS1.0, TLS1.1, TLS1.2, or TLS1.3.
transparent int	**Choices** • 0: Disabled	(Layer 7 only) When transparency is enabled, connections at the Real Server appear to

	• 1: Enabled	originate at the client. With transparency disabled, connections originate at the LoadMaster.
use_for_snat int	**Choices** • 0: Disabled • 1: Enabled	By default, when the LoadMaster is being used to NAT Real Servers, the source IP address used on the internet is that of the LoadMaster. Enabling this option allows the Real Servers configured to use the Virtual Service as the source IP address instead. If the Real Servers are configured on more than one Virtual Service which has this option set, only connections to destination port 80 will use this Virtual Service as the source IP address.
vs_type str/required	**Choices** • gen • http • http/2 • log • ts • tls	This specifies the type of service being load balanced.
allowed_hosts str		This parameter is only relevant when ESP is enabled. Specify all the virtual hosts that can be accessed using this Virtual Service.
allowed_ directories str		This parameter is only relevant when ESP is enabled. Specify all the virtual directories that can be accessed using this Virtual Service. You can specify up to 254 characters for this parameter.
domain str		The Single Sign On (SSO) domain in which this Virtual Service will operate.
logoff str		This parameter is only relevant when ESP is enabled and when the Client Authentication Mode is set to Form Based. Specify the

		string that the LoadMaster should use to detect a logout event. Multiple logoff strings can be specified by using a space-separated list. If the URL to be matched contains sub-directories before the specified string, the Logoff String will not be matched. Therefore, the LoadMaster will not log the user off. You can specify up to 255 characters for this parameter.
add_auth_header str		This option is only available if SAML is selected as the **input_auth_mode**. Specify the name of the HTTP header. This header is added to the HTTP request from the LoadMaster to the Real Server and its value is set to the user ID for the authenticated session. You can specify up to 255 characters for this parameter.
display_pub_priv int	**Choices** • 0: Disabled • 1: Enabled	Display the public/private option on the login page. Based on the option the user selects on the login form, the session timeout value is set to the value specified for either the public or private timeout.
disable_ password_form int	**Choices** • 0: Disabled • 1: Enabled	Enabling this option removes the password field from the login page. This may be needed when password validation is not required, for example if using RSA SecurID authentication in a singular fashion.
captcha str		Enable this parameter to allow CAPTCHA verification on the login page. The LoadMaster only supports CAPTCHA v2. The **input_auth_mode** must be set to **2** (Form Based) for the CAPTCHA parameters to be relevant.

		All CAPTCHA parameters must be set before it can be used. Both the LoadMaster and the client machine must be able to access Google for this to work. Before the CAPTCHA has been correctly answered, the submit button on the login form is disabled. If the user does not submit the form within two minutes of answering the CAPTCHA, the CAPTCHA times out (Google-specified timeout), and the user must verify a new CAPTCHA (the submit button is disabled until the new CAPTCHA has been verified).
captcha_private_key str		The key that was provided as the private key when you signed up for the CAPTCHA service.
captcha_access_url int	**Choices** • 0: Disabled • 1: Enabled	The URL of the service that provides the CAPTCHA challenge. Usually: **www.google.com/recaptcha/api.js** Do not start this URL with https. Only CAPTCHA V2 is currently supported.
captcha_verify_url str		The URL of the service that verifies the response to the CAPTCHA challenge. Usually: **www.google.com/recaptcha/api/siteverify** Do not start this URL with

		https. Only CAPTCHA V2 is currently supported.
esp_logs int	**Choices:** • 0 • 1 • 2 • 3 • 4 • 5 • 6 • 7	Enable ESP logging. Valid values are below: 0 - Logging off 1 - User Access 2 - Security 3 - User Access and Security 4 - Connection 5 - User Access and Connection 6 - Security and connection 7 - User Access, Security and Connection **Note:** The only valid values for SMTP services are 0 and 4. For SMTP services, security issues are always logged. Nothing is logged for user access because there are no logins.
smtp_allowed_domains str		Specify all the permitted domains that are allowed to be received by this Virtual Service.
excluded_directories str		This parameter is only relevant when ESP is enabled. Any virtual directories specified within this field will not be pre-authorized on this Virtual Service and are passed directly to the relevant Real Servers.
esp_enabled int	**Choices** • 0: Disabled • 1: Enabled	Enable or disable the Edge Security Pack (ESP) features.
input_auth_mode int	**Choices:** • 0	Specify the client authentication method to be used: 0 - Delegate to Server

	• 1 • 2 • 3 • 4 • 5 • 6	1 - Basic Authentication 2 - Form Based 4 - Client Certificate 5 - NTLM 6 - SAML
output_auth_mode int	**Choices:** • 0 • 1 • 2 • 3 • 4	Specify the server authentication mode to be used: 0 - None 1 - Basic Authentication 2 - Form Based 3 - KCD 4 - Server Token
server_fba_path str		Only relevant when using form-based authentication as the Server Authentication Mode (**output_auth_mode**). Set the authentication path for server-side Form Based Authentication (FBA). When used in Exchange environments, this does not need to be set.
out_conf str		Enter the name of the outbound SSO domain.
single_sign_on_dir str		This parameter relates to the **SSO Image Set** drop-down in the **ESP Options** section of the modify Virtual Service screen in the LoadMaster User Interface (UI). Specify the name of the image set to be used for the login screen. If no image set is specified, the default Exchange image set will be used.
single_sign_on_message str		Specifies the SSO message that is displayed. The **single_sign_on_message** parameter accepts HTML code, so you can insert an image if required.

		There are several characters that are not supported. These are the grave accent character (` ) and the single quote ('). If a grave accent character is used in the SingleSignOnMessage, the character will not display in the output, for example a`b`c becomes abc. If a single quote is used, users will not be able to log in.
allowed_groups str		Specify the groups that are allowed to access this Virtual Service. If the parameter value is longer than the maximum length of a HTTP GET query (1024 characters), you must set the **HTTP Method** to **POST**. You can specify up to 2048 characters for this parameter.
group_sids str		Specify the group security identifiers (SIDs) that are allowed to access this Virtual Service. Each group is separated by a semi-colon. Spaces are used to separate bytes in certain group SIDs. Here is an example: **S-1-5-21-703902271-2531649136-2593404273-1606** SIDs can be found by using the **get-adgroup-Identity GroupName** command.

		If the parameter value is longer than the maximum length of HTTP GET query (1024 characters), you must set the HTTP Method to POST.
include_nested_groups str		This parameter relates to the **AllowedGroups** parameter. Enable this option to include nested groups in the authentication attempt. If this option is disabled, only users in the top-level group will be granted access. If this option is enabled, users in both the top-level and first sub-level group will be granted access.
steering_groups str		Enter the Active Directory group names that will be used for steering traffic. Use a semi-colon to separate multiple group names. The steering group index number corresponds to the location of the group in this list. If the parameter value is longer than the maximum length of a HTTP GET query (1024 characters), you must set the **HTTP Method** to **POST**.
excluded_domains str		Any virtual directories specified within this field will not be pre-authorized on this Virtual Service and will be passed directly to the relevant Real Servers. Multiple excluded domains can be specified by using a space-separated list.
alt_domains str		Specify alternative domains to be assigned to a Virtual Service when configuring multi-domain authentication. To specify multiple alternative domains, use a space-separated

		list.
user_pwd_change_url str		This is relevant when using form-based LDAP authentication. Specify the URL that users can use to change their password. If a user's password has expired, or if they must reset their password, this URL and the **user_pwd_change_msg** is displayed on the login form. This URL must be put into the exception list for authentication, if required.
user_pwd_change_msg str		This parameter is only relevant if the **user_pwd_change_url** parameter is set. Specify the text to be displayed on the login form when the user must reset their password.
user_pwd_expiry_warn int	**Choices** • 0: Disabled • 1: Enabled	By default, SSO users are notified about the number of days before they must change their password. If you disable this option, the password expiry notification will not appear on the login forms. This parameter is only relevant if the **input_auth_mode** is set to **Form Based** (**2**) and the **user_pwd_change_url** is set. The language of the warning text is based on the **SSO Image Set** that is selected (English, French, or Portuguese).
user_pwd_expiry_warn_days int		Specify the number of days to show the warning before the password is expired. This parameter is only relevant if the **input_auth_mode** is set to **Form Based** (**2**) and the **user_pwd_change_url** is set.
intercept int	**Choices** • 0: Disabled (default) • 1: Enabled	Enable or disable the Web Application Firewall (WAF).
intercept_opts list		A list of strings to enable or disable certain WAF features.
intercept_post_other_content_		Enter a comma-separated list of POST content types allowed for WAF analysis, for

types list		example **text/plain,text/css**. By default, all types (other than XML/JSON) are enabled. To set this to any other content types, set the value to **any**. Enabling the inspection of any other content types may increase system resource utilization (CPU and memory). A specific list of content types should be considered.
alert_threshold int		This is the threshold of incidents per hour before sending an alert. Setting this to 0 disables alerting. Range: 0 - 100000
waf_rules list		List of WAF rules and which group they belong to with the name of the rule and IDs to disable in the format: **G\<rule_name>:208080:2000023**

2.3 Examples

```
- name: Create a Virtual Service
  hosts: localhost

  vars:
    central_address: '10.35.23.180'
    central_username: 'admin'
    central_api_key: '4ef39d110474a18639bab'
    lm_address: '10.35.23.2:443'
    ip: '10.35.23.156'
    port: 443
    prot: 'tcp'

  tasks:
    - name: Create Virtual Service Pathos on LM
      virtual_service:
        central_address: '{{ central_address }}'
```

```
        central_username: '{{ central_username }}'
       central_api_key: '{{ central_api_key }}'
        lm_address: '{{ lm_address }}'
        enable: 'Y'
        nickname: 'Pathos'
        ip: '{{ ip }}'
        port: '{{ port }}'
        protocol: '{{ prot }}'
       vs_type: 'http'
        ssl_acceleration: 1
        check_type: 'icmp'
        qos: 'Maximize-Reliability'
        transparent: 1
```

2.4 Return Values

The following are the fields unique to this module:

Key	Returned	Description
message str	always	The message response indicating whether the task created or modified the Virtual Service. **Sample:** VS Updated
changed bool	always	A Boolean to indicate whether changes were made during the task **Sample:** true
dataChanged str	when changed is true	The parameters that were changed during the task. **Sample:** {"check_type": "icmp","NickName": "Pathos","SSLAcceleration": "Y", "TlsType": "3", "Transparent": "Y"}
msg str	when task failed	The error message related to why the task failed. **Sample:** The minimum supported LoadMaster firmware version is 7.2.47.0.

2.5 Status

This module is maintained by Kemp Technologies.

3 Modify a SubVS on a LoadMaster

3.1 Synopsis

This module configures a SubVS on a LoadMaster. The minimum supported LoadMaster firmware version is 7.2.47.0. To configure a SubVS on a Virtual Service, the Virtual Service must be defined in your playbook before the SubVS.

3.2 Parameters

Parameter	Choices/ Defaults	Comments
add_via int	**Choices:** • 0 • 1 • 2 • 3 • 4 • 5 • 6	Corresponds to the add http headers in LM
central_username str/required		The Kemp 360 Central username.
central_api_key str/required		The API key for the user of the Kemp 360 Central machine.
central_address str/required		The IP address of the Kemp 360 Central that the LoadMaster is added to.

enable str	**Choices:** • Y • N	Enable the SubVS.
lm_address str/required		IP address and port of the LoadMaster that contains the Virtual Service or SubVS that the Real Server should be created or modified on. The format is 'ip:port'.
vs str/required		The IP address of the parent Virtual Service on the LoadMaster.
port int/required		The port of the parent Virtual Service on the LoadMaster value between 3 and 65530.
limit int		The maximum number of open connections that can be sent to a Real Server before it is taken out of rotation; values 0-100000.
nickname str/required		Nickname of a SubVS.
qos int	**Choices** • 0 • 1 • 2 • 4 • 8	Quality of Service sets a type of service that deals with how packets treat and prioritize the traffic.
subnet_originating int	**Choices:** • 0 • 1	When transparency is not enabled, the source IP address of connections to the Real Servers is that of the Virtual Service. When transparency is enabled, the source IP address is the IP address that is initiating

		connection to the Virtual Service. If the Real Server is on a subnet, and the Subnet Originating Requests option is enabled, then the subnet address of the LoadMaster is used as the source IP address.
vs_type str	**Choices:** • gen • http • http/2 • tls • log	This specifies the type of service being load balanced.
critical int	**Choices:** • 0 • 1	Enabling this parameter indicates that the Real Server is required for the Virtual Service to be considered available. The Virtual Service is marked as down if the Real Server has failed or is disabled.
check_type str	**Choices:** • icmp • http • https • tcp • smtp • nntp • ftp • telnet • pop3 • imap	Specify which protocol is to be used to check the health of the Real Server.

	• rdp • bdara • ldap • none	
check_codes str		A space-separated list of HTTP status codes that should be treated as successful when received from the Real Server.
check_port int		The port to be checked. If a port is not specified, the Real Server port is used. Specify 0 to unset **check_port**.
weight int		When using weighted round robin scheduling, the weight of a Real Server is used to indicate what relative proportion of traffic should be sent to the server. Servers with higher values receive more traffic. The weight of a SubVS can also be updated using the **modrs** command - set the Real Server to the number that appears in the Id column for the relevant SubVS in the parent Virtual Service modify screen; values 1-65535.
check_host str		The **check_use_11** parameter must be enabled to set the **check_host** value. When using HTTP/1.1 checking, the Real Servers require a Hostname be supplied in each request. If no value is set, then this value is the IP address of the Virtual Service.
check_pattern str		When the **check_type** is set to **http** or **https** - this corresponds to the **Reply 200 Pattern** in the

		WUI. This parameter only applies when the **HTTP Method** is set to **GET** or **POST**. When the **check_type** is set to **bdata**: Specify the hexadecimal string, which is searched for in the response. Specify an empty value to unset **check_pattern**.
check_headers str		Specify up to four additional headers/fields that will be sent with each health check request. Separate the pairs with a pipe, for example; **Host:xyc|UserAgent:prq**.
check_use_11 str	**Choices:** • 0 • 1	By default, the health checker uses HTTP/1.0 when checking the Real Server status. Enabling **check_use_11** means HTTP/1.1 is used (which is more efficient).
enhanced_health_checks int	**Choices** • 0 • 1	Enabling the **enhanced_health_checks** parameter provides an additional health check parameter - **rs_minimum**. If the **enhanced_health_checks** parameter is disabled, the Virtual Service is considered available if at least one Real Server is available. If the **enhanced_health_checks** parameter is enabled, you can specify the minimum number of Real Servers that should be available to consider the Virtual Service to be available.
rs_minimum int		An integer that specifies how many Real Servers must be up for a Virtual Service or SubVS to be considered up. It is an integer from 0 to *N*, where *N* is the

		number of Real Servers on this particular service. In practice, this value is usually 1.
extra_header_key str		Specify the key for the extra header to be inserted into every request sent to the Real Servers.
extra_header_value str		Specify the value for the extra header to be inserted into every request sent to the Real Servers.
error_code int		If no Real Servers are available, the LoadMaster can terminate the connection with a HTTP error code. Specify the error code number in this parameter. To unset the error code, set the parameter to an empty string.
error_url str		When no Real Servers are available and an error response is sent back to the client, a redirect URL can also be specified.
ldap_endpoint str		Specify the name of an LDAP endpoint to use for the health checks. If LDAP is selected as the **check_type**, the server IP address (or addresses) and ports from the LDAP endpoint configuration are used instead of the Real Server IP address and port.
copy_header_from str		This is the name of the source header field to copy into the new header field before the request is sent to the Real Servers.
copy_header_to str		Used in conjunction with the **copy_header_from** parameter. The name of the header field into which the source header is to be copied.

transparent int	**Choices:** • 0 • 1	When using Layer 7, when this is enabled - the connection arriving at the Real Server appears to come directly from the client. Alternatively, the connection can be non-transparent, which means that the connections at the Real Server appear to come from the LoadMaster. If a Virtual Service (with or without a SubVS) has SSL re-encrypt enabled, the transparency flag of the Virtual Service has no meaning (re-encryption forces transparency to be off). The transparency setting can still be modified by the API and is honored when re-encrypt is disabled on the Virtual Service.
multi_connect int	**Choices:** • 0 • 1	Enabling this option permits the LoadMaster to manage connection handling between the LoadMaster and the Real Servers. Requests from multiple clients are sent over the same TCP connection. Multiplexing only works for simple HTTP GET operations. This parameter cannot be enabled in certain situations, for example if WAF, ESP, or SSL Acceleration is enabled.
non_local int	**Choices:** • 0 • 1	By default only Real Servers on local networks can be assigned to a Virtual Service. Enabling this option allows a non-local Real Server to be assigned to the Virtual Service. This option is only available if a non local Real Server is enabled and the

		Transparent option is disabled on the relevant Virtual Service.
check_url str		When the **check_type** is set to http or https - by default, the health checker tries to access the URL / to determine if the machine is available. A different URL can be set in the **check_url** parameter. When the **check_type** is set to **bdata**: Specify a hexadecimal string to send to the Real Server. The maximum character length for the **check_url** parameter value is 126 characters.
check_post_data str		This parameter is only relevant if the HTTP Method is set to POST. When using the POST method, up to 2047 characters of POST data can be sent to the server.
check_use_get int	**Choices:** • 0 • 1 • 2	When accessing the health check URL - the system can use the HEAD, the GET, or the POST method.
persist str	**Choices:** • ssl • cookie • active-cookie • cookie-src • cookie-hash • cookie-hash-src • url • query-hash	Specify the type of persistence (stickiness) to be used for this Virtual Service.

	• hash • host • header • super • super-src src • rdp • rdp-src • rdp-sb • rdp-sb-src • udpsip • none	
persist_timeout int		The length of time (in seconds) after the last connection that the LoadMaster remembers the persistence information. Timeout values are rounded down to an even number of minutes. Setting a value that is not a number of whole minutes results in the excess being ignored. Setting a value to less than 60 seconds results in a value of 0 being set, which disables persistency.
match_len int		This parameter is only relevant when the **check_type** is set to **bdata**. Specify the number of bytes to find the **check_pattern** within; values 0-8000.
stand_by_addr str		Specify the IP address of the 'Sorry' server that is to be used when no other Real Servers are available. This server will not be health checked and is assumed

		to be always available.
stand_by_port int		Specify the port of the 'Sorry' server.
schedule str	**Choices:** • Round-Robin • Weighted-Round-Robin • Least-Connection • Weighted-Least-Connection • Fixed-Weighting • Adaptive-Resource-Based • Source-IP-Hash • Weighted-Response-Time • SDN-Adaptive • URL-Hash	Specify the type of scheduling of new connections to Real Servers that is to be performed.
rs_rule_precedence str		This parameter should be used in conjunction with **rs_rule_precedence_pos**. This parameter is used to specify the name of the existing rule whose position you want to change.
rs_rule_precedence_pos int		This parameter, in conjunction with the **rs_rule_precedence** parameter, is used to change the position of the rule in a sequence of rules. For example, a position of 2 means the rule is checked second.
selection_rules str		Specify a list of selection rules to add to the SubVS.
request_header_rules		Add a list of request rules to a SubVS.

str		
response_header_rules str		Add a list of response rules to a SubVS.

3.3 Examples

```
- name: Create a Sub VS
  hosts: localhost

  vars:
   central_address: '10.35.23.180'
   central_username: 'admin'
   central_api_key: '4ef39d1104767e18639bab'
   lm_address: '10.35.23.2:443'

 tasks:
 - name: Create SubVS
   sub_virtual_service:
       central_address: '{{ central_address }}'
       central_api_key: '{{ central_api_key }}'
       central_username: '{{ central_username }}'
       lm_address: '{{ lm_address }}'
       vs: 10.35.23.100'
       port: 80
       prot: 'tcp'
       nickname: 'Beta'
       vs_type: 'http'
       enable: 'Y'
       enhanced_health_checks: 1
       schedule: 'Round-Robin'
       content_rules: ['matchRedHeader']
```

3.4 Return Values

The following are the fields unique to this module:

Key	Returned	Description
message str	always	The message response indicating whether the task created or modified the SubVS.

		Sample: SubVS Updated
changed bool	always	A Boolean to indicate whether changes were made during the task true
dataChanged str	when changed is true	The parameters that were changed during the task. **Sample:** {"Transparent": "N", "UseforSnat": "N", "VSPort": "0", "VStype": "http", "NickName": "Epsilon"}
msg str	when task failed	The error message related to why the task failed. **Sample:** The minimum supported LoadMaster firmware version is 7.2.47.0.

3.5 Status

This module is maintained by Kemp Technologies.

4 Modify a Real Server on a LoadMaster

4.1 Synopsis

This module adds or modifies a Real Server to Virtual Services and SubVS on a LoadMaster. The minimum supported LoadMaster firmware version is 7.2.47.0. To configure a Real Server on a Virtual Service, the Virtual Service must be defined in your playbook before the Real Server. To configure a Real Server on a SubVS, the SubVS must be defined in your playbook before the Real Server.

4.2 Parameters

Parameter	Choices/ Defaults	Comments
lm_address str/required		The IP address and port of the LoadMaster that contains the Virtual Service or SubVS that the Real Server should be created or modified on.
lm_port str		The port of the LoadMaster.
central_address str/required		The IP address of the Kemp 360 Central that the LoadMaster is added to.
username str/required		The Kemp 360 Central username.
api_key str/required		The API key for the user of the Kemp 360 Central machine.
vs_ip str/required		The IP address of the Virtual Service on the provided LoadMaster.
vs_port int/required		The port of the Virtual Service on the provided LoadMaster. Values are between 3 and 65530.

vs_prot str/required	**Choices** • udp • tcp	The protocol of the Virtual Service on the provided LoadMaster.
rs_ip str/required		The IP address of the Real Server that is being created or modified.
rs_port str/required		The port of the Real Server that is being created or modified. Values are between 3 and 65530.
rs_limit int		The maximum number of open connections that can be sent to a Real Server before it is taken out of rotation. Values are between 0 and 100000.
rs_weight int		When using weighted round robin scheduling, the weight of a Real Server is used to indicate what relative proportion of traffic should be sent to the server. Servers with higher values receive more traffic. The weight of a SubVS can also be updated using the **modrs** command; set the Real Server to the number that appears in the Id column for the relevant SubVS in the parent Virtual Service modify screen.
rs_fw_method str	**Choices** • nat • route	The type of forwarding method used. The default method is NAT. Direct server return can only be used with Layer 4 services.
rs_enable str	**Choices** • Y (default) • N	Enable or disable the Real Server.
rs_critical int	**Choices** • 0: Disabled	Enabling this parameter indicates that the Real Server is required for the Virtual Service to be considered

	• 1: Enabled	available. The Virtual Service is marked as down if the Real Server has failed or is disabled.
sub_vs_nickname str		To create or modify a Real Server on a SubVS; the nickname of the SubVS must be provided.
addtoallsubvs int	**Choices** • 0: Disabled • 1: Enabled	Enable this option when adding a Real Server to all SubVSs of a Virtual Service; values are 0 or 1.
newport int		The port on the Real Server to be used. Values are between 3 and 65535.
follow int		Specify what Real Server the health check is based on by setting this parameter to the **RsIndex** of the Real Server to be followed. This can either be set to the **RsIndex** of the same Real Server to health check based on that particular Real Server status, or another Real Server can be specified. For example, if Real Server 1 is down, any Real Servers that have their health check based on Real Server 1 are also marked as down, regardless of their actual Real Server status.
content_rules list		A list of content rule names to be added to a Real Server. The names provided must be previously added to the LoadMaster and must be Content Matching rules.

4.3 Examples

```
- name: Create Real Server
  hosts: localhost

  vars:
   central_address: '10.35.39.21'
```

```
   lm_address: '10.35.39.20:443'
   username: 'admin'
   api_key: '699129a26ad34466a4cc'

  tasks:
- name: Create Real Server
  hosts: localhost
  tasks:
  - name: Create RS for VS 10.35.39.25:8010
    real_server:
      lm_address: '{{ lm_address }}'
      central_address: '{{ central_address }}'
      username: '{{ username }}'
      api_key: '{{ api_key }}'
      vs_ip: '10.35.39.25'
      vs_port: 8010
      vs_prot: 'tcp'
      rs_ip: '10.35.39.6'
      rs_port: 4006
      rs_limit: 220
```

4.4 Return Values

The following are the fields unique to this module:

Key	Returned	Description
message str	always	The message response indicating whether the task created or modified the Real Server. **Sample:** Real Server 10.35.39.180:8010 created successfully
changed bool	always	A Boolean to indicate whether changes were made during the task **Sample:** true
dataChanged str	when changed is true	The parameters that were changed during the task. **Sample:** {"Addr": "10.35.39.180", "Critical": "N", "DnsName": null, "Enable": "Y", "Follow": "0", "Forward": "nat"}

msg str	when task failed	The error message related to why the task failed. **Sample:** The minimum supported LoadMaster firmware version is 7.2.47.0.

4.5 Status

This module is maintained by Kemp Technologies.

5 Add LDAP Authentication on the LoadMaster

5.1 Synopsis

Module to add LDAP authentication on LoadMaster.

5.2 Parameters

Parameter	Choices /Defaults	Comments
lm_address str		The IP address and port of the LoadMaster. The format is 'ip:port'.
central_address str		The IP address of the Kemp 360 Central machine that the LoadMaster is added to.
username str		The username of the Kemp 360 Central user.
api_key str		The API key for the Kemp 360 Central machine.
name str		The name of the LDAP service.
ldaptype str	**Choices:** • 0 - Unencrypted (default) • 1 - StartTLS • 2 - LDAPS	Specify the transport protocol to use when communicating with the LDAP server.
adminuser str		The username that is used to check the LDAP server.
adminpass		The password that is used to

str		check the LDAP server.
server str		Specify the address, or addresses, of the LDAP server to be used. You can also specify a port number, if desired. Separate multiple addresses with a space.
vinterval str		Specify how often to revalidate the user the with the LDAP server. Range: 10 - 86400 seconds
referralcount str		Multiple hops may increase authentication latency. There is a performance impact that depends on the number and depth of referrals required in your configuration. You must have intimate knowledge of your Active Directory structure to set the referral limit appropriately. The same credentials are used for all lookups, and so on. The use of Active Directory Global Catalog (GC) is the preferred configuration as the primary means of resolution instead of enabling LDAP referral chasing. A GC query can be used to query the GC cache instead of relying on LDAP and the referral process. Using Active Directory GC has little or no performance drag on the LoadMaster. For steps on how to add/remove the GC, refer to the following TechNet article: Add or Remove the Global Catalog.

timeout str		Specify the LDAP server timeout in seconds. The default value is 5. Valid values range from 5 to 60.

5.3 Examples

```
- name: Create a small configuration for LoadMaster
  hosts: localhost

  vars:
       central_address: '10.35.60.27'
       central_username: 'admin'
       central_api_key: '7291f46c25094ee5edc8ef4bf54c3144050e2717'
       lm_address: '10.35.60.30'
       lm_port: '443'
       vs_ip: '10.35.60.123'
       vs_port: 443
       vs_prot: 'tcp'
       rs_ip: '10.35.60.112'

  tasks:
       - name: Set SSO LDAP
         sso_ldap:
               central_address: '{{ central_address }}'
               username: '{{ central_username }}'
               api_key: '{{ central_api_key }}'
               lm_address: '{{ lm_address }}'
               lm_port: '{{ lm_port }}'
               name: 'TestLdap'
               ldaptype: '2'
               server: 'ldap://10.35.23.154'
               vinterval: '240'
               adminuser: 'user123'
               adminpass: 'test'
               referralcount: 0
               timeout: 3600
```

5.4 Return Values

The following are the fields unique to this module:

Key	Returned	Description
message str	always	The message response indicating whether the task created or modified. **Sample:** LDAP auth was configured successfully
changed bool	always	A Boolean to indicate whether changes were made during the task. **Sample:** true
dataChanged	when changed is true	The error message related to why the task failed.
msg str	when task fails	The error message relating to why the task failed. **Sample:** The minimum supported LoadMaster firmware version is 7.2.47.0

5.5 Status

This module is maintained by Kemp Technologies.

6 Add or Modify an LDAP-based SSO on the LoadMaster

6.1 Synopsis

Module to add or modify a Certificate based SSO on LoadMaster.

6.2 Parameters

Parameter	Choices /Defaults	Comments
lm_address str		The IP address and port of the LoadMaster. The format is 'ip:port'.
central_address str		The IP address of the Kemp 360 Central machine that the LoadMaster is added to.
username str		The username of the Kemp 360 Central user.
api_key str		The API key for the Kemp 360 Central machine.
domain str		Set the name for the logon domain you are providing.
auth_type str		Set the authentication type for the LoadMaster. For **sso_ldap** this can only be **LDAP-Unencrypted**.
ldap_endpoint str		The name of an existing LDAP endpoint. Specify the LDAP endpoint to use.
logon_domain str		This parameter corresponds with the **Domain/Realm** field in

		the WUI. This is the login domain to be used. This is also used with **logon_fmt** to construct the normalized user name.
logon_fmt str	**Choices:** • Principalname • Username • Not Specified	Specify the logon string format used to authenticate to the LDAP server.
logon_transcode str	**Choices:** • 0: Disabled • 1: Enabled	Enable or disable the transcode of logon credentials from ISO-8859-1 to UTF-8, when required.
ldapephc str	**Choices:** • 0: Disabled • 1: Enabled	Enable this parameter to use the LDAP endpoint admin username and password for the health check.
max_failed_auths str		The maximum number of failed login attempts before the user is locked out. Range: 0-999
unblock_tout str		The timeout value (in seconds) before a blocked account is automatically unblocked. This must be greater than the **reset_fail_tout** value.
sess_tout_type str	**Choices:** • idle time • max duration	Specify the type of session timeout to be used.
sess_tout_idle_pub str		The session idle timeout value in seconds. This value is used in a public environment.
sess_tout_idle_priv str		The session idle timeout value in seconds. This value is used in a private environment.

sess_tout_duration_priv str		The maximum duration timeout value for the session in seconds. This value is used in a private environment.

6.3 Examples

```
- name: Create a small configuration for LoadMaster
  hosts: localhost

  vars:
       central_address: '10.35.60.27'
       central_username: 'admin'
       central_api_key: '7291f46c25094ee5edc8ef4bf54c3144050e2717'
       lm_address: '10.35.60.30'
       lm_port: '443'
       vs_ip: '10.35.60.123'
       vs_port: 443
       vs_prot: 'tcp'
       rs_ip: '10.35.60.112'

  tasks:
    - name: Set SSO LDAP
         sso_ldap:
               central_address: '{{ central_address }}'
               username: '{{ central_username }}'
               api_key: '{{ central_api_key }}'
               lm_address: '{{ lm_address }}'
               lm_port: '{{ lm_port }}'
               domain: 'TestLdap'
               ldap_endpoint: 'LDAP1'
               auth_type: 'LDAP-Unencrypted'
               logon_domain: 'logondomain'
               logon_fmt: 'Not Specified'
               logon_transcode: '0'
               max_failed_auths: '18'
               unblock_tout: '2020'
               sess_tout_idle_pub: '706'
               sess_tout_duration_pub: '700'
               sess_tout_idle_priv: '702'
               sess_tout_duration_priv: '700'
               sess_tout_type: 'idle time'
```

```
        ldapephc: '0'
        testuser: 'user123'
        testpass: 'test'
```

6.4 Return Values

Common return values are documented here; the following are the fields unique to this module:

Key	Returned	Description
message str	always	The message response indicating whether the task created or modified. **Sample:** Successfully updated SSO Parameters
changed bool	always	A Boolean to indicate whether changes were made during the task. **Sample:** true
dataChanged str	when changed is true	The parameters that were changed during the task.
msg str	when task fails	The error message relating to why the task failed. **Sample:** The minimum supported LoadMaster firmware version is 7.2.47.0

6.5 Status

This module is maintained by Kemp Technologies.

7 Add or Modify a RADIUS-based SSO on the LoadMaster

7.1 Synopsis

Module to add or modify a RADIUS based SSO on LoadMaster.

7.2 Parameters

Parameter	Choices /Defaults	Comments
lm_address str		IP address and port of the LoadMaster. The format is 'ip:port'.
central_address str		The Kemp 360 Central IP address where the LoadMaster is added to.
username str		The username of the Kemp 360 Central user.
api_key str		The API key for the Kemp 360 Central user.
domain str		An identifer for the domain you are creating.
auth_type str		The type of SSO domain this will be. For RADIUS this should be 'RADIUS'.
radius_shared_secret str		The shared secret to be used between the RADIUS server and the LoadMaster.
radius_send_nas_id str	**Choices:** • 0: Disabled • 1: Enabled	If enabled, a NAS identifer string (radius_nas_id) is sent to the RADIUS server.
radius_nas_id		The Network Access Server (NAS) identifer

str		string.
server str		The address(s) of the server(s) to use to validate this domain. (IPv4 only)
logon_domain str		The domain/realm used to construct normalized username for login.
logon_fmt str		Specify the logon string format used to authenticate to the LDAP/RADIUS server.
logon_fmt2 str		Specify an alternate logon string format used to authenticate to the LDAP/RADIUS.
logon_transcode str	**Choices:** • 0: Disabled • 1: Enabled	Enable or disable the transcode of logon credentials from ISO-8859-1 to UTF-8, when required.
max_failed_auths str		The maximum number of failed login attempts before the user is locked out. Range: 0-999
unblock_tout str		The timeout value (in seconds) before a blocked account is automatically unblocked. This must be greater than the **reset_fail_tout** value.
sess_tout_idle_pub str		The session idle timeout value in seconds. This value is used in a public environment.
sess_tout_duration_pub str		The maximum duration timeout value for the session in seconds. This value is used in a public environment.
sess_tout_idle_priv str		The session idle timeout value in seconds. This value is used in a private environment.
sess_tout_duration_priv str		The maximum duration timeout value for the session in seconds. This value is used in a private environment.
sess_tout_type str	**Choices:** • idle time	Specify the type of session timeout to be used.

	• max duration	
reset_fail_count str		The number of seconds that must elapse before the Failed Login Attempts counter is reset to 0. This value must be less than the **unblock_tout**.

7.3 Examples

```
- name: Create a small configuration for LoadMaster
  hosts: localhost

  vars:
       central_address: '10.35.60.27'
       central_username: 'admin'
       central_api_key: '7291f46c25094ee5edc8ef4bf54c3144050e2717'
       lm_address: '10.35.60.30'
       lm_port: '443'
       vs_ip: '10.35.60.123'
       vs_port: 443
       vs_prot: 'tcp'
       rs_ip: '10.35.60.112'

  tasks:
  - name: Set Radius SSO list
       sso_radius:
               central_address: '{{ central_address }}'
               username: '{{ central_username }}'
               api_key: '{{ central_api_key }}'
               lm_address: '{{ lm_address }}'
               lm_port: '{{ lm_port }}'
               domain: 'TestRadius'
               auth_type: 'RADIUS'
               server: '10.35.60.111'
               radius_shared_secret: 'def'
               radius_send_nas_id: '0'
               radius_nas_id: '1'
               logon_domain: 'domainTestABC'
               logon_fmt: 'Username Only'
               logon_fmt2: 'Principalname'
               logon_transcode: 0
               max_failed_auths: '1'
```

```
            unblock_tout: '71'
            sess_tout_idle_pub: '1301'
            sess_tout_duration_pub: '1301'
            sess_tout_idle_priv: '1302'
            sess_tout_duration_priv: '1302'
            sess_tout_type: 'idle time'
            reset_fail_count: '79'
            testuser: '123'
            testpass: '123'
```

7.4 Return Values

The following are the fields unique to this module:

Key	Returned	Description
message str	always	The message response indicating whether the SSO domain was created successfully.
changed bool	always	A Boolean to indicate whether changes were made during the task.
dataChanged str	when changed is true	The parameters that were changed during the task.
msg str	when task fails	The error message relating to why the task failed.

7.5 Status

This module is maintained by Kemp Technologies.

8 Add or Modify a RADIUS-LDAP-based SSO on the LoadMaster

8.1 Synopsis

Module to add or modify a RADIUS-LDAP based SSO on LoadMaster.

8.2 Parameters

Parameter	Choices /Defaults	Comments
lm_address str		IP address and port of the LoadMaster. The format is 'ip:port'.
central_address str		The IP address of the Kemp 360 Central machine that the LoadMaster is added to.
username str		The username of the Kemp 360 Central user.
api_key str		The API key of the Kemp 360 Central user.
domain str		Set the name for the logon domain you are providing.
auth_type str		Set the authentication type for the LoadMaster. For **sso_radius** this can only be **RADIUS and LDAP-Unencrypted**.
ldap_endpoint str		The name of an existing LDAP endpoint. Specify the LDAP endpoint to use.
radius_shared_secret		The shared secret to be used between the RADIUS server and the LoadMaster.

str		
radius_send_nas_id str	**Choices:** • 0: Disabled • 1: Enabled	If this parameter is disabled (default), a NAS identifier is not sent to the RADIUS server. If it is enabled, a Network Access Server (NAS) identifier string is sent to the RADIUS server. By default, this is the hostname. Alternatively, if a value is specified in the **radius_nas_id** parameter, this value is used as the NAS identifier. If the NAS identifier cannot be added, the RADIUS access request is still processed. This field is only available if the **auth_type** is set to a RADIUS option.
radius_nas_id str		If the **radius_send_nas_id** parameter is enabled, the **radius_nas_id** parameter is relevant. When specified, this value is used as the NAS identifier. Otherwise, the hostname is used as the NAS identifier. If the NAS identifier cannot be added, the RADIUS access request is still processed. This parameter is only relevant if the auth_type is set to a RADIUS option and the **radius_send_nas_id** parameter is enabled.
server str		The address (or addresses) of the server(s) that are to be used to validate this domain. IPv6 is not supported for RADIUS authentication.
ldapephc str	**Choices:** • 0: Disabled • 1: Enabled	Enable this parameter to use the LDAP endpoint admin username and password for the health check.
testuser str		The username to check the authentication server(s), if you are not using an LDAP endpoint.
testpass str		The password of the user to check the authentication server(s), if you are not using an LDAP endpoint.
logon_domain		This parameter corresponds with the

str		**Domain/Realm** field in the WUI. The login domain to be used. This is also used with logon format to construct the normalized user name.
logon_fmt str	**Choices:** • Principalname • Username • Not Specified	Specify the logon string format used to authenticate to the LDAP server.
logon_transcode str	**Choices:** • 0: Disabled • 1: Enabled	Enable or disable the transcode of logon credentials from ISO-8859-1 to UTF-8, when required.
max_failed_auths str	**Choices:** • 0: Disabled • 1: Enabled	The maximum number of failed login attempts before the user is locked out.
unblock_tout str		The timeout value (in seconds) before a blocked account is automatically unblocked. This must be greater than the **reset_fail_tout** value.
sess_tout_idle_pub str		The session idle timeout value in seconds. This value is used in a public environment.
sess_tout_duration_pub str		The maximum duration timeout value for the session in seconds. This value is used in a public environment.
sess_tout_idle_priv str		The session idle timeout value in seconds. This value is used in a private environment.
sess_tout_duration_priv str		The maximum duration timeout value for the session in seconds. This value is used in a private environment.
sess_tout_type str	**Choices:** • idle time • max duration	Specify the type of session timeout to be used.

reset_fail_tout int		The number of seconds that must elapse before the **Failed Login Attempts** counter is reset to 0. This value must be less than the **unblock_tout**. Range: 60-86400

8.3 Examples

```
- name: Create a small configuration for LoadMaster
  hosts: localhost

  vars:
       central_address: '10.35.60.27'
       central_username: 'admin'
       central_api_key: '7291f46c25094ee5edc8ef4bf54c3144050e2717'
       lm_address: '10.35.60.30'
       lm_port: '443'
       vs_ip: '10.35.60.123'
       vs_port: 443
       vs_prot: 'tcp'
       rs_ip: '10.35.60.112'

  tasks:
       - name: Set Radius LDAP SSO
         sso_radius_ldap:
               central_address: '{{ central_address }}'
               username: '{{ central_username }}'
               api_key: '{{ central_api_key }}'
               lm_address: '{{ lm_address }}'
               lm_port: '{{ lm_port }}'
               domain: 'TestLdapRadius'
               auth_type: 'RADIUS and LDAP-Unencrypted'
               ldap_endpoint: 'LDAP1'
               radius_shared_secret: 'def'
               radius_send_nas_id: '1'
               radius_nas_id: 'ABC123'
               server: '10.35.60.111'
               ldapephc: '0'
               testuser: 'user123'
               testpass: 'test'
               logon_domain: 'domainTestABC'
```

```
                logon_fmt: 'Username Only'
                logon_fmt2: 'Username'
                logon_transcode: '0'
                max_failed_auths: '1'
                unblock_tout: '70'
                sess_tout_idle_pub: '701'
                sess_tout_duration_pub: '1201'
                sess_tout_idle_priv: '702'
                sess_tout_duration_priv: '1202'
                sess_tout_type: 'idle time'
                reset_fail_tout: '95'
```

8.4 Return Values

The following are the fields unique to this module:

Key	Returned	Description
message str	always	The message response indicating whether the task created or modified. **Sample:** Successfully updated SSO Parameters
changed bool	always	A Boolean to indicate whether changes were made during the task. **Sample:** true
msg str	when task fails	The error message relating to why the task failed. **Sample:** The minimum supported LoadMaster firmware version is 7.2.47.0

8.5 Status

This module is maintained by Kemp Technologies.

9 Add or Modify a Certificate-based SSO on the LoadMaster

9.1 Synopsis

Module to add or modify a certificate-based SSO on LoadMaster.

9.2 Parameters

Parameter	Choices /Defaults	Comments
lm_address str		The IP address and port of the LoadMaster. The format is 'ip:port'.
central_address str		The IP address of the Kemp 360 Central machine that the LoadMaster is added to.
username str		The username of the Kemp 360 Central user.
api_key str		The API key for the Kemp 360 Central machine.
domain str		An identifer for the domain you are creating.
logon_domain str		The domain/realm used to construct the normalized username for login.
auth_type str		The type of SSO domain this will be. For RADIUS this should be 'RADIUS'.
logon_fmt str		Specify the logon string format used to authenticate to the LDAP/RADIUS server.
logon_fmt2 str		Specify an alternate logon string format used to authenticate to the LDAP/RADIUS.

logon_transcode bool	**Choices:** • 0: Disabled • 1: Enabled	Enable or disable the transcode of logon credentials from ISO-8859-1 to UTF-8, when required.
reset_fail_tout str		The number of seconds that must elapse before the Failed Login Attempts counter is reset to 0. This value must be less than the **unblock_tout**.
unblock_tout str		The timeout value (in seconds) before a blocked account is automatically unblocked. This must be greater than the **reset_fail_tout** value.
max_failed_auths int		The maximum number of failed login attempts before the user is locked out. (0-999)
sess_tout_idle_pub str		The session idle timeout value in seconds. This value is used in a public environment.
sess_tout_duration_pub str		The maximum duration timeout value for the session in seconds. This value is used in a public environment.
sess_tout_idle_priv str		The session idle timeout value in seconds. This value is used in a private environment.
sess_tout_duration_priv str		The maximum duration timeout value for the session in seconds. This value is used in a private environment.
sess_tout_type str	**Choices:** • idle time • max duration	Specify the type of session timeout to be used.

9.3 Example

```
- name: Create a small configuration for LoadMaster
  hosts: localhost

  vars:
       central_address: '10.35.60.27'
```

```
      central_username: 'admin'
      central_api_key: '7291f46c25094ee5edc8ef4bf54c3144050e2717'
      lm_address: '10.35.60.30'
      lm_port: '443'
      vs_ip: '10.35.60.123'
      vs_port: 443
      vs_prot: 'tcp'
      rs_ip: '10.35.60.112'

tasks:
- name: Set SSO Certificates list
  sso_certificate:
              central_address: '{{ central_address }}'
              username: '{{ central_username }}'
              api_key: '{{ central_api_key }}'
              lm_address: '{{ lm_address }}'
              lm_port: '{{ lm_port }}'
              domain: 'TestCert'
              ldap_endpoint: 'LDAP1'
              auth_type: 'Certificates'
              ldapephc: '0'
              logon_domain: 'test'
              logon_fmt: 'Not Specified'
              logon_transcode: '1'
              max_failed_auths: '18'
              unblock_tout: '4022'
              sess_tout_idle_pub: '503'
              sess_tout_duration_pub: '303'
              sess_tout_idle_priv: '903'
              sess_tout_duration_priv: '503'
              sess_tout_type: 'max duration'
              reset_fail_tout: '63'
              cert_check_asi: '1'
              cert_check_cn: '1'
              testuser: 'user123'
              testpass: 'test'
```

9.4 Return Values

The following are the fields unique to this module:

Key	Returned	Description
message	always	The message response indicating whether the SSO data was updated.

str		**Sample:** Successfully updated SSO Parameters
changed bool	always	A Boolean to indicate whether changes were made during the task. **Sample:** true
msg str	when task fails	The error message relating to why the task failed. **Sample:** Could not update SSO

9.5 Status

This module is maintained by Kemp Technologies.

10 Add or Modify a SAML-based SSO on the LoadMaster

10.1 Synopsis

Module to add or modify a SAML-based SSO on LoadMaster. The minimum supported LoadMaster firmware version is 7.2.47.0.

10.2 Parameters

Parameter	Choices /Defaults	Comments
lm_address str		IP address and port of the LoadMaster. The format is 'ip:port'.
central_address str		The IP address of the Kemp 360 Central machine that the LoadMaster is added to.
username str		The username of the Kemp 360 Central user.
api_key str		The API key for the Kemp 360 Central user.
domain str		Set the name for the logon domain you are providing.
auth_type str		Set the authentication type for the LoadMaster. For **sso_saml** this can only be **SAML**.
idp_entity_id str		Specify the Identity Service Provider (IdP) Entity ID.
idp_sso_url str		Specify the IdP Single Sign On (SSO) URL.
idp_cert		Specify the IdP certificate to use for

str		verification processing.
sp_cert str		It is optional to sign requests that are sent in the context of logon. Currently, the LoadMaster does not sign those requests. In the context of log off requests - it is mandatory and these requests must be signed. This is to avoid any spoofing and to provide extra security in relation to log off functionality. This ensures that users are not being hacked and not being logged off unnecessarily. In the **sp_cert** parameter, you can choose to use a self-signed certificate or third party certificate to perform the signing. To specify a self-signed certificate, set **sp_cert** to **useselfsigned**. To use a third party certificate, specify the name of the certificate to use (this certificate must be uploaded to the intermediate certificate section of the LoadMaster before it can be selected).
sp_entity_id str		The Service Provider (SP) entity ID is an identifier that is shared to enable the IdP to understand, accept, and have knowledge of the entity when request messages are sent from the LoadMaster. This must correlate to the identifier of the relying party on the AD FS server.
sess_tout_idle_pub str		The session idle timeout value in seconds. This value is used in a public environment.
sess_tout_duration_pub str		The maximum duration timeout value for the session in seconds. This value is used in a public environment.
sess_tout_type str	**Choices:** • idle time • max duration	Specify the type of session timeout to be used.
idp_match_cert	**Choices:**	If this option is enabled, the IdP certificate

str	• 0: Disabled • 1: Enabled	assigned must match the certificate in the IdP SAML response.

10.3 Examples

```
- name: Create a small configuration for LoadMaster
  hosts: localhost

  vars:
       central_address: '10.35.34.2'
       central_username: 'admin'
       central_api_key: 'b54058156b44a6ac818d58e6bc92b3ce57f17aa3'
       lm_address: '10.35.34.134'
       lm_port: '443'
       vs_ip: '10.35.60.123'
       vs_port: 443
       vs_prot: 'tcp'
       rs_ip: '10.35.60.112'

  tasks:
    - name: Set SAML SSO list
         sso_saml:
               central_address: '{{ central_address }}'
               username: '{{ central_username }}'
               api_key: '{{ central_api_key }}'
               lm_address: '{{ lm_address }}'
               lm_port: '{{ lm_port }}'
               domain: 'TestSaml'
               auth_type: 'SAML'
               idp_entity_id: 'test_abc123'
               idp_sso_url: 'https://www.def.com/url/abc123'
               idp_logoff_url: 'https://www.def.com/url/logoff123'
               idp_cert: '1'
               sp_cert: '38FCF8174F0E9FCF1318FC5758E8F5BC5BD6EA6D'
               sp_entity_id: '09876'
               sess_tout_idle_pub: '802'
               sess_tout_duration_pub: '1200'
               sess_tout_type: 'idle time'
               idp_match_cert: '0'
```

10.4 Return Values

Common return values are documented here; the following are the fields unique to this module:

Key	Returned	Description
message str	always	The message response indicating whether the SSO data was updated **Sample:** Successfully updated SSO Parameters
changed bool	always	A Boolean to indicate whether changes were made during the task. **Sample:** true
msg str	when task fails	The error message relating to why the task failed. **Sample:** Could not update SSO

10.5 Status

This module is maintained by Kemp Technologies.

11 Add GEO FQDN Data

11.1 Synopsis

Module to add GEO FQDN data on the LoadMaster.

11.2 Parameters

Parameter	Choices /Defaults	Comments
central_api_key str		The API key for the user of the Kemp 360 Central machine.
central_address str		The Kemp 360 Central IP address.
central_username str		The username of the Kemp 360 Central user.
lm_address str		The IP address of the LoadMaster that is attached to Kemp 360 Central.
lm_port int		The port of the LoadMaster.
fqdn str		The FQDN to be added or edited on the LoadMaster.
fail_over int		This parameter is only relevant if the selection criteria is set to **Location Based**.
selection_criteria str	**Choices:** • rr • wrr • fw • rsr	The selection criteria for addresses associated with the FQDN.

	• prx • lb • all	
fail_time int		If a failure delay is not set, normal health checking is performed. If set, this parameter defines the number of minutes to wait after a failure before finally disabling it.
site_recovery_mode str	**Choices:** • auto • manual	If this is set to automatic, upon site recovery the site is brought back into operation immediately. If this is set to manual, once the site has failed, the site is disabled. Manual intervention is required to restore normal operation.
public_request_value int	**Choices:** • 0 • 1 • 2 • 3	Restrict responses to clients from public IP addresses to specific classes of site. Here is an explanation of the different settings and their values: • 0 - Public Sites Only • 1 - Prefer Public Sites • 2 - Prefer Private Sites • 3 - Any Sites
private_request_value int	**Choices:** • 0 • 1 • 2 • 3	Restrict responses to clients from private IP addresses to specific classes of site. Here is an explanation of the different settings and their values: • 0 - Private Sites Only • 1 - Prefer Private Sites • 2 - Prefer Public Sites • 3 - Any Sites
local_settings	**Choices:**	Enabling this parameter provides two

int	• 0: Disabled • 1: Enabled	additional parameters for the FQDN - **local_ttl** and **local_sticky**.
local_ttl int		The Time To Live (TTL) value dictates how long the reply from the GEO LoadMaster can be cached by other DNS servers or client devices. The time interval is defined in seconds. This value should be as practically low as possible. The default value for this field is 10. Defaults to the value of the global **ttl** value when an FQDN is created. Range: 1 to 86400
local_sticky int		Stickiness, also known as persistence, is the property that enables all name resolution requests from an individual client to be sent to the same resources until a specified period of time has elapsed.
unanimous_checks int	**Choices:** • 0: Disabled • 1: Enabled	When this parameter is enabled, if any IP addresses fail health checking - the other FQDN IP addresses which belong to the same cluster will be forced down.

11.3 Examples

```
- name: Add FQDN to LoadMaster
  hosts: localhost

  vars:
       central_address: '10.35.53.100'
       lm_address: '10.35.53.101'
       lm_port: 443
       username: 'admin'
       api_key: '699129a26ace3fcd34466a4cc'
       domain: 'example.com'

  tasks:
  - name: Add FQDN to LoadMaster
       geo_fqdn:
```

```
            lm_address: '{{ lm_address }}'
            lm_port '{{ lm_port }}'
            central_address: '{{ central_address }}'
            central_username: '{{ username }}'
            central_api_key: '{{ api_key }}'
            fqdn: '{{ domain }}'
            selection_criteria: 'wrr'
            fail_time: 50
            site_recovery_mode: 'auto'
            local_settings: 1
            local_ttl: 302
            local_sticky: 304
            unanimous_checks: 1
```

11.4 Return Values

The following are the fields unique to this module:

Key	Returned	Description
message str	always	The message response indicating whether the GEO FQDN data was updated. **Sample:** Successfully updated FQDN Parameters
changed bool	always	A Boolean to indicate whether changes were made during the task. **Sample:** true
msg str	when task fails	The error message relating to why the task failed. **Sample:** Could not update FQDN, ...

11.5 Status

This module is maintained by Kemp Technologies.

12 Update GEO Maps and Clusters

12.1 Synopsis

Module to update GEO maps and cluster data on the LoadMaster.

12.2 Parameters

Parameter	Choices /Defaults	Comments
central_api_key str		The API key for the user of the Kemp 360 Central machine.
central_address str		The IP address of Kemp 360 Central.
central_username str		The username of the Kemp 360 Central user.
lm_address str		The IP address of the LoadMaster attached to Kemp 360 Central.
lm_port int		The LoadMaster port that is attached to Kemp 360 Central.
fqdn str		The FQDN of the GEO configuration.
cluster_ip str		The cluster IP address to be set.
cluster_name str		The cluster nickname to be set.
cluster_type str	**Choices:** • default	The type of cluster.

	• remoteLM • localLM	
cluster_checker str	**Choices:** • none • tcp • icmp	Specify the method used to check the status of the cluster.
cluster_checker_port int		Specify the port of the cluster.
cluster_enable int	**Choices:** • 0: Disabled • 1: Enabled	Enable or disable the cluster.
cluster_latitude_seconds int		The latitude of the cluster.
cluster_longitude_seconds int		The longitude of the cluster.
map_ip str		The IP address of the cluster.
map_checker str	**Choices:** • none • icmp • tcp • clust	The type of checking to do on the map.
map_weight int		The weight of the map.
map_address str		The map IP address to check.
map_port int		The map port to be addressed.
map_enable	**Choices:**	Enable or disable the map.

int	• 0: Disabled • 1: Enabled	
map_latitude_seconds str		The map longitude.
map_longitude_seconds str		The map longitude.
checker_ip str		Specify the address used to health check the IP address.
checker_port str		The address port used to health check the IP address.
country_code str		The country code.
is_continent int	**Choices:** • 0: Disabled • 1: Enabled	When dealing with a country - the **is_continent** parameter must be set to **0**. When adding a continent - the **is_continent** parameter must be set to **1**.
custom_location str		The custom location.

12.3 Examples

```
- name: Test general geo parameters
  hosts: localhost

  vars:
       central_address: '10.35.53.50'
       central_username: 'Admin'
       central_api_key: '32e0513423f2df63ce7afd5cf5fdb5eda448eb9c'
       lm_address: '10.35.53.6'
       lm_port: '443'
       domain: 'www.example.com'

       name: GEO map Example
              geo_misc:
                     central_address: '{{ central_address }}'
```



```
                    central_username: '{{ central_username }}'
                    central_api_key: '{{ central_api_key }}'
                    lm_address: '{{ lm_address }}'
                    lm_port: '{{ lm_port }}'
                    central_api_key: '{{ central_api_key }}'
                    fqdn: '{{ domain }}'
                    cluster_ip: '10.35.53.100'
                    cluster_type: 'default'
                    cluster_name: 'Cluster'
                    cluster_checker: 'tcp'
                    cluster_checker_port: 8080
                    cluster_enable: 1
                    cluster_latitude_seconds: 360
                    cluster_longitude_seconds: 360
                    map_ip: '10.35.53.101'
                    map_enable: 1
                    map_checker: 'tcp'
                    map_weight: 500
                    checker_ip: '10.35.53.190'
                    checker_port: 7893
                    country_code: 'IE'
                    is_continent: 0
```

12.4 Return Values

The following are the fields unique to this module:

Key	Returned	Description
message str	always	The message response indicating whether the task created or modified the GEO map or cluster. **Sample:** Map cluster and data updated
changed bool	always	A Boolean to indicate whether changes were made during the task. **Sample:** true
dataChanged str	when changed is true	The parameters that were changed during the task.

msg str	when task fails	The error message relating to why the task failed. **Sample:** Could not update cluster and map data

12.5 Status

This module is maintained by Kemp Technologies.

13 Update GEO Miscellaneous Options and GEO Partnership

13.1 Synopsis

Module to update GEO miscellaneous options and GEO partnership.

13.2 Parameters

Parameter	Choices /Defaults	Comments
central_api_key str		The API key for the user of the Kemp 360 Central machine.
central_address str		The Kemp 360 Central IP address.
central_username str		The username of the Kemp 360 Central user.
lm_address str		The IP address of the LoadMaster that is attached to Kemp 360 Central.
lm_port int		The port of the LoadMaster IP address.
zone str		Specify the zone name.
source_of_authority str		The response set for Source of Authority requests.
soa_email str		Email address of the person responsible for the zone and to which email may be sent to report errors or problems. This

		is the email address of a suitable DNS administrator but more commonly the technical contact for the domain.
name_server str		Set the response sent for Name Server requests.
ttl int		Set the Time To Live (TTL) (in seconds).
persist int		This corresponds with the **Stickiness** WUI field. This determines how long (in seconds) a specific response will be returned to a host.
check_interval int		Set how often (in seconds) that devices will be checked.
conn_timeout int		Set the timeout (in seconds) for the check request.
retry_attempts int		Set the number of times the check will be retried before the device is marked as failed Range: 2-10
ip_range list		The IP range data to be added. This must include the CIDR number per IP range.
latitude str		Latitude data to be added to the IP range.
longtitude str		Longtitude data to be added to the IP range.
country_code str		Country code data to be added to the IP range.
custom_location str		Custom location data to be added to the IP range.
white_list		White list of allowed IP ranges.

list		
algorithm str	**Choices:** • RSASHA256 • NSEC3RSASHA1 • NSEC3RSASHA1	The algorithm to be used in DNS.
key_size int	**Choices:** • 1024 • 2048 • 4096	The key size to be used in DNS.
dns_enable int	**Choices:** • 0: Disabled • 1: Enabled	Enable or disable DNS in GEO.
geo_clients list		Set the addresses of the GEO LoadMasters which can retrieve service status information from the LoadMaster.
geo_partners list		Set the IP address of the GEO LoadMaster partner(s). These GEO LoadMasters will keep their DNS configurations in sync.
geo_ssh_port int		The port over which GEO LoadMasters will communicate with each other.
geo_ssh_interface int		Specify the ID of the GEO interface in which the SSH partner tunnel is created, for example, setting this to 0 means the interface eth0.

13.3 Examples

```
- name: Add FQDN to LoadMaster
```

```
hosts: localhost

vars:
     central_address: '10.35.53.100'
     lm_address: '10.35.53.101'
     lm_port: 443
     username: 'admin'
     api_key: '699129a26ace3fcd34466a4cc'

     tasks:
     - name: Add FQDN to LoadMaster
       geo_fqdn:
            lm_address: '{{ lm_address }}'
            lm_port '{{ lm_port }}'
            central_address: '{{ central_address }}'
            central_username: '{{ username }}'
            central_api_key: '{{ api_key }}'
            geo_clients: ['10.35.53.200']
            geo_partners: ['10.35.53.220']
            geo_ssh_port: 22
```

13.4 Return Values

The following are the fields unique to this module:

Key	Returned	Description
message str	always	The message response indicating whether the miscellaneous data was updated. **Sample:** Successfully updated MISC Parameters
changed bool	always	A Boolean to indicate whether changes were made during the task. **Sample:** true
msg str	when task fails	The error message relating to why the task failed. **Sample:** Could not update MISC, ...

13.5 Status

This module is maintained by Kemp Technologies.

14 Upload a Certificate and Key on a LoadMaster

14.1 Synopsis

This module uploads a certificate and key to a LoadMaster. A certificate and key must be in the same file being uploaded. A certificate upload must be defined in your playbook before being assigned to a Virtual Service.

14.2 Parameters

Parameter	Choices/ Defaults	Comments
api_key str/required		The API key for the user of the Kemp 360 Central machine.
central_ address str/required		The IP address of the Kemp 360 Central that the LoadMaster is added to.
cert_name str/required		The name of the identifier of the cert to upload or replace.
cert_file str/required		Path to the file where the key and cert are stored. This must have both key and cert in the same file.
replace int/required	**Choices:** • 0 • 1	A Boolean to upload the cert to replace the current cert.
username int/required		The Kemp 360 Central username.
intermediate	**Choices:**	A Boolean to specify if the cert is an intermediate or not.

int	• 0 (default) • 1	

14.3 Example

```
- name: Upload a certificate to the LoadMaster
  hosts: localhost

  vars:
   central_address: '10.35.39.21'
   lm_address: '10.35.39.20:443'
   username: 'admin'
   api_key: '699129a26ace3fcd34466a4cc'

  tasks:
  - name: Upload a certificate to the LoadMaster
     cert_management:
      lm_address: '{{ lm_address }}'
      central_address: '{{ central_address }}'
      cert_name: 'cert'
      cert_file: '/path/to/cert/test.pem'
      replace: 0
      username: '{{ username }}'
      api_key: '{{ api_key }}'
```

14.4 Return Values

Common return values are documented here; the following are the fields unique to this module:

Key	Returned	Description
message str	always	The message response indicating whether the certificate was uploaded. **Sample:** Certificate uploaded to LoadMaster
changed bool	always	A Boolean to indicate whether changes were made during the task true
msg	when task	The error message related to why the task failed.

		Sample:
str	failed	Could not add Certificate to LM - Command Failed: Certificate Identifier already exists

14.5 Status

This module is maintained by Kemp Technologies.

15 Add or Modify a Header Rule

15.1 Synopsis

This module adds or modifies addHeaderRules on a LoadMaster. The minimum supported LoadMaster firmware version is 7.2.47.0. Rules must be defined in your playbook before being assigned to Virtual Services, SubVSs, and Real Servers.

15.2 Parameters

Parameter	Choices/ Defaults	Comments
lm_address str/required		The IP address and port of the LoadMaster. The format is 'ip:port'.
central_address str/required		The IP address of the Kemp 360 Central that the LoadMaster is added to.
username str/required		The Kemp 360 Central username.
api_key str/required		The API key for the user of the Kemp 360 Central machine.
name str/required		The name of the AddHeaderRule.
header str/required		The name of the header field to be added.
replacement str/required		The replacement string. You can enter a maximum of 255 characters in this parameter.
only_on_flag		Range: 1-9. Only try to execute this rule if the

int		specified flag is set. Using the **only_on_flag** and **set_on_match** parameters, it is possible to make rules dependent on each other, that is, only execute a particular rule if another rule has been successfully matched.

15.3 Examples

```
- name: Create AddHeaderRule
  hosts: localhost

  vars:
   central_address: '10.35.39.21'
   lm_address: '10.35.39.20:443'
   username: 'admin'
   api_key:'699129a26ace3fcd34466a4cc'

  tasks:
- name: Create AddHeaderRule
  add_header_rule:
    lm_address: '{{ lm_address }}'
    central_address: '{{ central_address }}'
    username: '{{ username }}'
    api_key: '{{ api_key }}'
    name: 'addHeaderRule1'
    header: 'name'
    replacement: 'username'
```

15.4 Return Values

The following are the fields unique to this module:

Key	Returned	Description
message str	always	The message response indicating whether the task created or modified the rule. **Sample:** AddHeaderRule with name addHeaderRule1 was created successfully
changed	always	A Boolean to indicate whether changes were made during the

bool		task **Sample:** true
dataChanged str	when changed is true	The parameters that were changed during the task. **Sample:** {"Header": "name","HeaderValue": "username","Name": "addHeaderRule1"}
msg str	when task failed	The error message related to why the task failed. **Sample:** The minimum supported LoadMaster firmware version is 7.2.47.0.

15.5 Status

This module is maintained by Kemp Technologies.

16 Delete Header Rule

16.1 Synopsis

This module adds or modifies a deleteHeaderRule on a LoadMaster. The minimum supported LoadMaster firmware version is 7.2.47.0. Rules must be defined in your playbook before being assigned to Virtual Services, SubVS, and Real Servers.

16.2 Parameters

Parameter	Choices/ Defaults	Comments
lm_address str/required		The IP address and port of the LoadMaster. The format is 'ip:port'.
central_address str/required		The IP address of the Kemp 360 Central that the LoadMaster is added to.
username str/required		The Kemp 360 Central username.
api_key str/required		The API key for the user of the Kemp 360 Central machine.
name str/required		The name of the DeleteHeaderRule.
pattern str		The pattern to be matched.
only_on_flag int		Range: 1-9. Only try to execute this rule if the specified flag is set. Using the **only_on_flag** and **set_on_match** parameters, it is possible to make rules dependent on each other, that is, only execute a particular rule if another rule has been successfully matched.

16.3 Examples

```
- name: Create DeleteHeaderRule
```

```
hosts localhost

vars:
  central_address: '10.35.39.21'
  lm_address: '10.35.39.20:443'
  username: 'admin'
  api_key: '699129a26ace983fcd34466a4cc'

tasks:
- name: Create DeleteHeaderRule
  delete_header_rule:
       lm_address: '{{ lm_address }}'
       central_address: '{{ central_address }}'
       username: '{{ username }}'
       api_key: '{{ api_key }}'
       name: 'deleteHeaderRule1'
       pattern: '^((http[s]?|ftl):\/)$'
```

16.4 Return Values

The following are the fields unique to this module:

Key	Returned	Description
message str	always	The message response indicating whether the task created or modified the rule. **Sample:** DeleteHeaderRule with name deleteHeaderRule1 was created successfully
changed bool	always	A Boolean to indicate whether changes were made during the task **Sample:** true
dataChanged str	when changed is true	The parameters that were changed during the task. **Sample:** {"Name": "deleteHeaderRule1", "Pattern": "^((http[s]?|ftl):\\/)$"}
msg	when task failed	The error message related to why the task failed.

	Sample:
str	The minimum supported LoadMaster firmware version is 7.2.47.0.

16.5 Status

This module is maintained by Kemp Technologies.

17 Replace Body Rule

17.1 Synopsis

This module adds or modifies a replaceBodyRule on a LoadMaster. The minimum supported LoadMaster firmware version is 7.2.47.0. Rules must be defined in your playbook before being assigned to Virtual Services, SubVS, and Real Servers.

17.2 Parameters

Parameter	Choices/ Defaults	Comments
lm_address str/required		The IP address of the LoadMaster.
lm_port str		The port of the LoadMaster.
central_address str/required		The IP address of the Kemp 360 Central that the LoadMaster is added to.
username str/required		The Kemp 360 Central username.
api_key str/required		The API key for the user of the Kemp 360 Central machine.
name str/required		The name of the ReplaceBodyRule.
replacement str/required		The replacement string.
pattern str		The pattern to be matched.
only_on_flag int		Range: 1-9. Only try to execute this rule if the specified flag is set. Using the **only_on_flag** and **set_on_**

		match parameters, it is possible to make rules dependent on each other, that is, only execute a particular rule if another rule has been successfully matched.
case_independent int	**Choices:** • 0: Disabled • 1: Enabled	Enable this parameter to ignore the case of the strings when comparing.

17.3 Examples

```
- name: Create ReplaceBodyRule
  hosts: localhost

  vars:
   central_address: '10.35.39.21'
   lm_address: '10.35.39.20:443'
   username: 'admin'
   api_key: '699129a26acd34466a4cc'

  tasks:
  - name: Create ReplaceBodyRule
    replace_body_rule:
        lm_address: '{{ lm_address }}'
        central_address: '{{ central_address }}'
        username: '{{ username }}'
        api_key: '{{ api_key }}'
        name: 'replaceBodyRule1'
        case_independent: 1
        replacement: 'username'
        pattern: '^((http[s]?|ftl):\/)$'
```

17.4 Return Values

The following are the fields unique to this module:

Key	Returned	Description
message str	always	The message response indicating whether the task created or modified the rule.

		Sample: ReplaceBodyRule with name replaceBodyRule1 was created successfully
changed bool	always	A Boolean to indicate whether changes were made during the task **Sample:** true
dataChanged str	when changed is true	The parameters that were changed during the task. **Sample:** {"CaseIndependent": "N","Name": "replaceBodyRule1","Pattern": "^((http[s]?|ftl):\\/)$","Replacement": "username"}
msg str	when task failed	The error message related to why the task failed. **Sample:** The minimum supported LoadMaster firmware version is 7.2.47.0.

17.5 Status

This module is maintained by Kemp Technologies.

18 Replace Header Rule

18.1 Synopsis

This module adds or modifies a replaceHeaderRule to a LoadMaster. The minimum supported LoadMaster firmware version is 7.2.47.0. Rules must be defined in your playbook before being assigned to Virtual Services, SubVS, and Real Servers.

18.2 Parameters

Parameter	Choices/Defaults	Comments
lm_address str/required		The IP address of the LoadMaster.
lm_port str		The port of the LoadMaster.
central_address str/required		The IP address of the Kemp 360 Central that the LoadMaster is added to.
username str/required		The Kemp 360 Central username.
api_key str/required		The API key for the user of the Kemp 360 Central machine.
name str/required		The name of the ReplaceHeaderRule.
header str		The header field name where the substitution should be performed.
replacement str/required		The replacement string.
pattern str		The pattern to be matched.
only_on_flag		Range: 1-9. Only try to execute this rule if the specified flag is set. Using the **only_on_flag**

int		and **set_on_match** parameters, it is possible to make rules dependent on each other, that is, only execute a particular rule if another rule has been successfully matched.

18.3 Examples

```
- name: Create ReplaceHeaderRule
  hosts: localhost
  vars:
   central_address: '10.35.39.21'
   lm_address: '10.35.39.20:443'
   username: 'admin'
   api_key: '699129a26ace406fd65ee30a6983fcd34466a4cc'

  tasks:
  - name: Create ReplaceHeaderRule
    replace_header_rule:
        lm_address: '{{ lm_address }}'
        central_address: '{{ central_address }}'
        username: '{{ username }}'
        api_key: '{{ api_key }}'
        name: 'replaceHeaderRule1'
        header: 'name'
        replacement: 'username'
        pattern: '^((http[s]?|ftl):\/)$'
```

18.4 Return Values

The following are the fields unique to this module:

Key	Returned	Description
message str	always	The message response indicating whether the task created or modified the rule. **Sample:** ReplaceHeaderRule with name replaceHeaderRule1 was created successfully
changed	always	A Boolean to indicate whether changes were made during the task

bool		**Sample:** true
dataChanged str	when changed is true	The parameters that were changed during the task. **Sample:** {"Header": "name","Name": "replaceHeaderRule1", "Pattern": "^((http[s]?|ftl):\\/)$",Replacement": "username"}
msg str	when task failed	The error message related to why the task failed. **Sample:** The minimum supported LoadMaster firmware version is 7.2.47.0.

18.5 Status

This module is maintained by Kemp Technologies.

19 Match Content Rule

19.1 Synopsis

This module adds or modifies a matchContentRule on a LoadMaster. The minimum supported LoadMaster firmware version is 7.2.47.0. Rules must be defined in your playbook before being assigned to Virtual Services, SubVS, and Real Servers.

19.2 Parameters

Parameter	Choices/Defaults	Comments
lm_address str/required		The IP address and port of the LoadMaster. The format is 'ip:port'.
central_address str/required		The IP address of the Kemp 360 Central that the LoadMaster is added to.
username str/required		The Kemp 360 Central username.
api_key str/required		The API key for the user of the Kemp 360 Central machine.
name str/required		The name of the MatchContentRule.
match_type str/required	**Choices:** • regex • prefix • postfix	The name of the MatchContentRule.
include_host str		Prepend the hostname to request URI before performing the match.
ignore_case str		Ignore case when comparing the strings.
negate_match		Ignore case when comparing the

str		strings.
include_query str		Append the query string to the URI before performing a match.
header str/required		The header field name that should be matched. If no header field is set, the default is to match in the URL. Set this to body to match on the body of a request.
pattern str/required		The pattern to be matched.
set_on_match int		If the rule is successfully matched, set the specified flag. Accepted values: 0-9.
only_on_flag int		Range: 1-9. Only try to execute this rule if the specified flag is set. Using the **only_on_flag** and **set_on_match** parameters, it is possible to make rules dependent on each other, that is, only execute a particular rule if another rule has been successfully matched.
must_fail int	**Choices:** • 0: Disabled • 1: Enabled	If this rule is matched, then always fail to connect.

19.3 Examples

```
- name: Create ModifyURLRule
  hosts: localhost

  vars:
    central_address: '10.35.39.21'
    lm_address: '10.35.39.20:443'
    username: 'admin'
    api_key: '699129a26acecd34466a4cc'

  tasks:
```

```
    - name: Create ModifyURLRule
      match_content_rule:
      lm_address: '{{ lm_address }}'
      central_address: '{{ central_address }}'
      username: '{{ username }}'
      api_key: '{{ api_key }}'
      name: 'matchContentRule1'
      match_type: 'regex'
      include_host: 'Y'
      ignore_case: 'Y'
      include_query: 'Y'
      header:'username'
      pattern: '^((http[s]?|ftl):\/)$'
```

19.4 Return Values

The following are the fields unique to this module:

Key	Returned	Description
message str	always	The message response indicating whether the task created or modified the rule. **Sample:** MatchContentRule with name matchContentRule1 was created successfully
changed bool	always	A Boolean to indicate whether changes were made during the task **Sample:** true
dataChanged str	when changed is true	The parameters that were changed during the task. **Sample:** {"CaseIndependent": "Y","Header": "username","MatchType": "Regex","Name": "matchContentRule1","Pattern": "^((http[s]?|ftl):\\/)$"}
msg str	when task failed	The error message related to why the task failed. **Sample:** The minimum supported LoadMaster firmware version is 7.2.47.0.

19.5 Status

This module is maintained by Kemp Technologies.

20 Add or Modify a modifyURLRule on a LoadMaster

20.1 Synopsis

This module adds or modifies a modifyURLRule on a LoadMaster. The minimum supported LoadMaster firmware version is 7.2.47.0. Rules must be defined in your playbook before being assigned to Virtual Services, SubVS, and Real Servers.

20.2 Parameters

Parameter	Choices /Defaults	Comments
lm_address str/required		The IP address of the LoadMaster.
lm_port str		The port of the LoadMaster.
central_address str/required		The IP address of the Kemp 360 Central that the LoadMaster is added to.
username str/required		The Kemp 360 Central username.
api_key str/required		The API key for the user of the Kemp 360 Central machine.
name str/required		The name of the ModifyURLRule.
replacement str/required		How the URL is to be modified.

pattern str		The pattern to be matched.
only_on_flag int		Range: 1-9. Only try to execute this rule if the specified flag is set. Using the **only_on_flag** and **set_on_match** parameters, it is possible to make rules dependent on each other, that is, only execute a particular rule if another rule has been successfully matched.

20.3 Examples

```
- name: Create ModifyURLRule
  hosts: localhost

  vars:
    central_address: '10.35.39.21'
    lm_address: '10.35.39.20:443'
    username: admin
    api_key: '699129a26accd34466a4cc'

  tasks:
   - name: Create ModifyURLRule
     modify_url_rule:
      lm_address:'{{ lm_address }}'
      central_address: '{{ central_address }}'
      username: '{{ username }}'
      api_key:'{{ api_key }}'
      name: 'ModifyURLRule1'
      replacement: 'username'
      pattern: '^((http[s]?|ftl):\/)$'
```

20.4 Return Values

The following are the fields unique to this module:

Key	Returned	Description
message str	always	The message response indicating whether the task created or modified the rule. **Sample:**

		ModifyURLRule with name ModifyURLRule1 was created successfully
changed bool	always	A Boolean to indicate whether changes were made during the task **Sample:** true
dataChanged str	when changed is true	The parameters that were changed during the task. **Sample:** {"Name": "ModifyURLRule1","Pattern": "^((http[s]?|ftl):\\/)$","Replacement": "username"}
msg str	when task failed	The error message related to why the task failed. **Sample:** The minimum supported LoadMaster firmware version is 7.2.47.0.

20.5 Status

This module is maintained by Kemp Technologies.

21 Update Global Parameters

21.1 Synopsis

Module to update global parameters such as black list updates, WAF updates, and non-local Real Server.

21.2 Parameters

Parameter	Choices /Defaults	Comments
central_api_key str		The API key for the user of the Kemp 360 Central machine.
central_address str		The Kemp 360 Central IP address.
central_username str		The username of the Kemp 360 Central user.
lm_address str		The IP address of the LoadMaster that is attached to Kemp 360 Central.
lm_port int		The port of the LoadMaster.
non-local_rs int	**Choices:** • 0: Disabled • 1: Enabled	Enable non-local Real Servers on the LoadMaster.
black_list_auto_update int	**Choices:** • 0: Disabled • 1: Enabled	Enable or disable the blacklist auto-update setting.
black_list_auto_install int	**Choices:** • 0: Disabled • 1: Enabled	Enable or disable the blacklist auto-install setting.

black_list_install_time int		The hour of the day to install the blacklist updates.
waf_auto_update int	**Choices:** • 0: Disabled • 1: Enabled	Enable or disable the WAF auto-update setting.
waf_auto_install int	**Choices:** • 0: Disabled • 1: Enabled	Enable or disable the WAF auto-install setting.
waf_install_time int		The hour of the day to install the WAF updates.

21.3 Examples

```
- name: Configure LoadMaster Global Parameters
  hosts: localhost

  vars:
       central_address: '10.35.53.5'
       central_username: 'Admin'
       central_api_key: 'apikey'
       lm_address: '10.35.53.6'
       lm_port: '443'

  tasks:
       - name: Turn on some global settings
         global_params:
               central_address: '{{ central_address }}'
               central_username: '{{ central_username }}'
               central_api_key: '{{ central_api_key }}'
               lm_address: '{{ lm_address }}'
               lm_port: '{{ lm_port }}'
               non_local_rs: 1
               black_list_auto_update: 1
               black_list_auto_install: 1
               black_list_install_time: 10
               waf_auto_update: 1
```

```
                waf_auto_install: 1
                waf_install_time: 8
```

21.4 Return Values

The following are the fields unique to this module:

Key	Returned	Description
message str	always	The message response indicating whether the global data was updated. **Sample:** Successfully updated Global Parameters
changed bool	always	A Boolean to indicate whether changes were made during the task. **Sample:** true
msg str	when task fails	The error message relating to why the task failed. **Sample:** Global setting(s) could not be set, ...

21.5 Status

This module is maintained by Kemp Technologies.

22 Appendix

To install Ansible, refer to the Ansible Quick Start Guide at https://docs.ansible.com/ansible/latest/user_guide/quickstart.html.

Last Updated Date

This document was last updated on 28 August 2020.