Probe Configuration Mode Commands

Probe configuration mode commands allow you to configure health monitoring on the ACE to track the state of a server by sending out probes. Also referred to as out-of-band health monitoring, the ACE verifies the server response or checks for any network problems that can prevent a client from reaching a server. Based on the server response, the ACE can place the server in or out of service and can make reliable load-balancing decisions. You can also use health monitoring to detect failures for a gateway or host in high availability configurations. The ACE identifies the health of a server in the following categories:

- **Passed**—The server returns a valid response.
- **Failed**—The server fails to provide a valid response to the ACE or the ACE is unable to reach a server for a specified number of retries.

By configuring the ACE for health monitoring, the ACE sends active probes periodically to determine the server state. The ACE supports 4096 (ACE module) or 1000 (ACE appliance) unique probe configurations, which includes ICMP, TCP, HTTP, and other predefined health probes. The ACE can execute only up to 200 concurrent script probes at a time. The ACE also allows the opening of 2048 sockets simultaneously.

You can associate the same probe with multiple real servers or server farms. Each time that you use the same probe again, the ACE counts it as another probe instance. You can allocate a maximum of 16 K (ACE module) or 4000 (ACE appliance) probe instances.

To configure probes and access probe configuration mode for that probe type, use the `probe` command. The CLI prompt changes to `(config-probe-probe_type)`. For information about the commands in all probe configuration modes, see the commands in this section. See the “Command Modes” section for each command to find out to which probe-type configuration modes a specific command applies.

Use the `no` form of this command to remove a probe from the configuration.

```
probe probe_type probe_name

no probe probe_type probe_name
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>probe_type</code></td>
<td>Type of probe to configure. The probe type determines what the probe sends to the server. Enter one of the following types:</td>
</tr>
<tr>
<td></td>
<td>- <code>dns</code>—Sends a request to a DNS server that passes a configured domain to the server (by default, the domain is <a href="http://www.cisco.com">www.cisco.com</a>). To determine whether the server is up, the ACE must receive one of the configured IP addresses for that domain.</td>
</tr>
<tr>
<td></td>
<td>- `echo {tcp</td>
</tr>
<tr>
<td></td>
<td>- <code>finger</code>—Uses a Finger query to a server for an expected response string. The ACE searches the response for the configured string. If the ACE finds the expected response string, the server is marked as passed. If you do not configure an expected response string, the ACE ignores the server response.</td>
</tr>
</tbody>
</table>
- **ftp** —Establishes a TCP connection to the server and then issues a `quit` command.
- **http**—Establishes a TCP connection and issues an HTTP request to the server for an expected string and status code. The ACE can compare the received response with configured codes, looking for a configured string in the received HTTP page, or verifying hash for the HTTP page. If any of these checks fail, the server is marked as failed.

  For example, if you configure an expected string and status code and the ACE finds them both in the server response, the server is marked as passed. However, if the ACE does not receive either the server response string or the expected status code, it marks the server as failed.

  If you do not configure a status code, any response code from the server is marked as failed.
- **https**—Similar to an HTTP probe except that it uses Secure Sockets Layer (SSL) to generate encrypted data.
- **icmp**—Sends an ICMP echo request and listens for a response. If a server returns a response, the ACE marks the server as passed. If the server does not send a response, causing the probe to time out, or if the server sends an unexpected ICMP echo response type, the ACE marks the probe as failed.
- **imap**—Makes a server connection and sends user credential (login, password, and mailbox) information. The ACE can send a configured command. Based on the server response, the ACE marks the probe as passed or failed.
- **pop**—Initiates a session and sends the configured credentials. The ACE can send a configured command. Based on the server response, the ACE marks the probe as passed or failed.
- **radius**—Sends a query using a configured username, password, and shared secret to a RADIUS server. If the server is up, it is marked as passed. If you configure a Network Access Server (NAS) address, the ACE uses it in the outgoing packet. Otherwise, the ACE uses the IP address associated with the outgoing interface as the NAS address.
- **rtsp**—Establishes a TCP connection and sends a request packet to the server. The ACE compares the response with the configured response code to determine whether the probe has succeeded.
- **scripted**—Allows you to run a script to execute the probe that you created for health monitoring. You can author specific scripts with features not present in standard health probes.
- **sip {tcp | udp}**—Establishes a TCP or UDP connection and sends an OPTIONS request packet to the user agent on the server. The ACE compares the response with the configured response code or expected string, or both, to determine whether the probe has succeeded. If you do not configure an expected status code, any response from the server is marked as failed.
- **smtp**—Initiates an SMTP session by logging into the server, sends a HELLO message, and then disconnects from the server.
- **snmp**—Establishes a UDP connection and sends a maximum of eight SNMP OID queries to probe the server. The ACE weighs and averages the load information that is retrieved and uses it as input to the least-loaded algorithm for load-balancing decisions. If the retrieved value is within the configured threshold, the server is marked as passed. If the threshold is exceeded, the server is marked as failed.

- **tcp**—Initiates a TCP 3-way handshake (SYN, SYN-ACK, ACK) and expects the server to send a response. By default, a successful response causes the probe to mark the server as passed and send a FIN to end the session. If the response is not valid or if there is no response, the probe marks the server as failed.

- **telnet**—Establishes a connection to the server and verifies that a greeting from the application was received.

- **udp**—Sends a UDP packet to a server and marks the server as failed only if the server returns an ICMP Port Unreachable message. If the ACE does not receive any ICMP errors for the UDP request that was sent, the probe is marked as passed. Optionally, you can configure this probe to send specific data and expect a specific response to mark the server as passed. If the IP interface of the server is down or disconnected, the UDP probe by itself would not know that the UDP application is not reachable.

- **vm**—Sends a query to the VM controller (Vcenter) to obtain the load information of the local VMs.

| `probe_name` | Identifier for the probe. Use the probe name to associate the probe to the server. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters. |

**Command Modes**

Configuration mode

Admin and user contexts

**Command History**

<table>
<thead>
<tr>
<th>ACE Module Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.0(0)A1(2)</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>A2(1.0)</td>
<td>This command was revised.</td>
</tr>
<tr>
<td>A4(2.0)</td>
<td>Added the VM probe type.</td>
</tr>
<tr>
<td>A5(1.0)</td>
<td>Added IPv6 support.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ACE Appliance Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1(7)</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>A3(1.0)</td>
<td>This command was revised.</td>
</tr>
<tr>
<td>A4(2.0)</td>
<td>Added the VM probe type.</td>
</tr>
<tr>
<td>A5(1.0)</td>
<td>Added IPv6 support.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command requires the probe feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Virtualization Guide, Cisco ACE Application Control Engine*. 
You can associate only IPv4 probes with IPv4 real servers and only IPv6 probes with IPv6 real servers. For IPv6, the ACE supports the following probe types:

- DNS
- HTTP
- HTTPs
- ICMP
- TCP
- UDP
- Scripted

### Examples

To define a TCP probe named PROBE, and access its mode, enter:

```
host1/Admin(config)# probe tcp PROBE1
host1/Admin(config-probe-tcp)#
```

To delete the TCP probe named PROBE1 for TCP and access its mode, enter:

```
host1/Admin(config)# probe tcp PROBE1
```

### Related Commands

- `clear stats`
- `show probe`
- `show running-config`
- `show stats`

### (config-probe-`probe_type`) append-port-hosttag

(ace appliance only) To append port information in the HTTP Host header when you configure a non-default destination port for an HTTP or HTTPS probe, use the `append-port-hosttag` command. Use the `no` form of this command to reset the default behavior of not appending the port information in the HTTP Host header.

```
append-port-hosttag
```

```
no append-port-hosttag
```

### Syntax Description

This command has no keywords or arguments.

### Command Modes

HTTP and HTTPS probe configuration mode

Admin and user contexts

### Command History

<table>
<thead>
<tr>
<th>ACE Appliance Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A3(2.7). Not applicable for A4(1.0) or A4(2.0).</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
Usage Guidelines

This command has no usage guidelines.

Examples

To configure the ACE to append the port information, enter the following command:

```
host1/Admin(config-probe-http)# append-port-hosttag
```

To reset the default behavior, enter the following:

```
host1/Admin(config-probe-http)# no append-port-hosttag
```

Related Commands

This command has no related commands.
(config-probe-probe_type) community

To change the community string used by an SNMP probe, use the **community** command. Use the **no** form of this command to remove the community string.

```
community text

no community
```

**Syntax Description**

- `text` Name of the SNMP community string for the server. Enter a text string with a maximum of 255 alphanumeric characters.

**Command Modes**

- SNMP probe configuration mode
- Admin and user contexts

**Command History**

<table>
<thead>
<tr>
<th>ACE Module Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A2(1.0)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ACE Appliance Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A3(1.0)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

An ACE Simple Network Management Protocol (SNMP) probe accesses the server through its community string. By default, the community string is not set.

**Examples**

To configure the private community string, enter:

```
host1/Admin(config-probe-snmp)# community private
```

To reset the community string to its default value of public, enter:

```
host1/Admin(config-probe-snmp)# no community
```

**Related Commands**

- **show probe**
**connection term forced**

**no connection term forced**

**Syntax Description**
This command has no keywords or arguments.

**Command Modes**
ECHO TCP, Finger, FTP, HTTP, HTTPS, IMAP, POP, RTSP, SIP TCP, SMTP, TCP, and Telnet probe configuration modes
Admin and user contexts

**Command History**

<table>
<thead>
<tr>
<th>ACE Module Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.0(0)A1(2)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ACE Appliance Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1(7)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
This command applies only to TCP-based probes. By default, the ACE terminates a TCP connection gracefully by sending a FIN to the server.

**Examples**
To terminate a TCP connection by sending a RST for a TCP probe, enter:

```
host1/Admin(config-probe-tcp)# connection term forced
```

To reset the method to terminate a connection gracefully, enter:

```
host1/Admin(config-probe-tcp)# no connection term forced
```

**Related Commands**
show probe
(config-probe-probe_type) credentials

To configure the credentials for username and password authentication of a probe to access a server, use the `credentials` command. For a Remote Authentication Dial-In User Service (RADIUS) probe, a shared secret may also be required. For an Internet Message Access Protocol (IMAP) probe, you can provide a mailbox username. Use the `no` form of this command to remove the credentials from the configuration.

For HTTP, HTTPS, and POP probes, the syntax is as follows:

```
credentials username [password]
```

For RADIUS probes, the syntax is as follows:

```
credentials username password [secret shared_secret]
```

For IMAP probes, the syntax is as follows:

```
credentials {username password} | {mailbox name}
```

For HTTP, HTTPS, POP, and RADIUS probes, the syntax is as follows:

```
no credentials
```

For IMAP probes, the syntax is as follows:

```
no credentials {username | mailbox}
```

### Syntax Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>username</td>
<td>User identifier used for authentication. Enter an unquoted text string with a maximum of 64 alphanumeric characters.</td>
</tr>
<tr>
<td>password</td>
<td>(Optional except for RADIUS and IMAP probes) Password used for authentication. Enter an unquoted text string with a maximum of 64 alphanumeric characters.</td>
</tr>
<tr>
<td>mailbox name</td>
<td>(IMAP probe) Specifies the user mailbox name from which to retrieve e-mail for an IMAP probe. Enter an unquoted text string with a maximum of 64 alphanumeric characters.</td>
</tr>
<tr>
<td>secret shared_secret</td>
<td>(RADIUS probe) Specifies the password used for the MD5 hash encryption algorithm. Enter an unquoted text string with a maximum of 64 alphanumeric characters.</td>
</tr>
</tbody>
</table>

### Command Modes

HTTP, HTTPS, IMAP, POP, and RADIUS probe configuration modes

Admin and user contexts

### Command History

<table>
<thead>
<tr>
<th>ACE Module Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.0(0)A1(2)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ACE Appliance Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1(7)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
Usage Guidelines
You must configure the credentials for an IMAP probe using the credentials command before you configure the mailbox or the ACE will ignore the specified user mailbox name.

Examples
To configure the username ENG1 and a password TEST for an HTTP probe, enter:
host1/Admin(config-probe-http)# credentials ENG1 TEST
To delete the credentials for a probe, enter:
host1/Admin(config-probe-http)# no credentials
To configure the user mailbox LETTERS for an IMAP probe, enter:
host1/Admin(config-probe-imap)# credentials mailbox LETTERS
To delete the mailbox for the IMAP probe, enter:
host1/Admin(config-probe-imap)# no credentials mailbox

Related Commands
show probe

(config-probe-probe_type) description
To provide a description for a probe, use the description command. Use the no form of this command to remove the description for the probe.

description text

no description

Syntax Description
text Description for the probe. Enter a text string with a maximum of 240 alphanumeric characters.

Command Modes
All probe-type configuration modes
Admin and user contexts

Command History

<table>
<thead>
<tr>
<th>ACE Module Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.0(0)A1(2)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ACE Appliance Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1(7)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines
This command has no usage guidelines.
Examples
To configure a description THIS PROBE IS FOR TCP SERVERS for a TCP probe, enter:
host1/Admin(config-probe-tcp)# description THIS PROBE IS FOR TCP SERVERS

To remove the description THIS PROBE IS FOR TCP SERVERS for a TCP probe, enter:
host1/Admin(config-probe-tcp)# no description

Related Commands show probe
(config-probe-probe_type) domain

To configure the domain name that the probe sends to the DNS server to resolve, use the domain command. Use the no form of this command to reset the default domain (www.cisco.com) that the probe sends to the server.

```
domain name

no domain
```

**Syntax Description**

| name | Domain that the probe sends to the DNS server. Enter an unquoted text string with a maximum of 255 alphanumeric characters. |

**Command Modes**

DNS probe configuration mode
Admin and user contexts

**Command History**

<table>
<thead>
<tr>
<th>ACE Module Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.0(0)A1(2)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ACE Appliance Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1(7)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The DNS probe sends a domain name for the DNS server to resolve. By default, the probe uses the www.cisco.com domain name.

**Examples**

To configure the domain name of MARKET, enter:
```
host1/Admin(config-probe-dns)# domain MARKET
```

To reset the default domain that the probe sends to the DNS server, enter:
```
host1/Admin(config-probe-dns)# no domain
```

**Related Commands**

show probe
(config-probe-probe_type) expect address

To configure one or more IPv6 or IPv4 addresses that the ACE expects as a server response to a DNS request, use the `expect address` command. The probe matches the received IP address with the configured addresses. Use the **no** form of this command to remove the expected IP address from the configuration.

```
expect address ip_address

no expect address ip_address
```

**Syntax Description**

- `ip_address`: IPv6 or IPv4 address expected from the DNS server in response to the DNS probe request for a domain.

**Command Modes**

- DNS probe configuration mode
  - Admin and user contexts

**Command History**

<table>
<thead>
<tr>
<th>ACE Module Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.0(0)A1(2)</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>A5(1.0)</td>
<td>Added IPv6 support.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ACE Appliance Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1(7)</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>A5(1.0)</td>
<td>Added IPv6 support.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

A DNS probe sends a request for a domain to a DNS server. The ACE uses the IP address specified in the `expect address` command to decide whether to pass or fail the DNS probe for the server based on the server response. You can specify multiple IP addresses with this command by entering the command with a different address separately.

**Examples**

**IPv6 Example**

To configure an expected IPv6 address of 2001:DB8:15::/64, enter:

```
host1/Admin(config-probe-dns)# expect address 2001:DB8:15::/64
```

To remove an IPv6 address, use the **no expect address** command. For example, enter:

```
host1/Admin(config-probe-dns)# no expect address 2001:DB8:15::/64
```

**IPv4 Example**

To configure an expected IPv4 address of 192.8.12.15, enter:

```
host1/Admin(config-probe-dns)# expect address 192.8.12.15
```

To remove an IPv4 address, use the **no expect address** command. For example, enter:
host1/Admin(config-probe-dns)# no expect address 192.8.12.15

Related Commands: show probe
To configure what the ACE expects as a response from the probe destination server, use the `expect regex` command. Use the `no` form of this command to remove the expectation of a response expression.

```
expect regex string [offset number] [cache [length]]
```

For TCP and UDP probes, the syntax is as follows:

```
no expect
```

For Finger, HTTP, HTTPS, and SIP probes, the syntax is as follows:

```
no expect regex
```

### Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>string</code></td>
<td>Expected response string from the probe destination. Enter an unquoted text string with no spaces. If the string includes spaces, enclose the string in quotes. The string can be a maximum of 255 alphanumeric characters.</td>
</tr>
<tr>
<td><code>offset number</code></td>
<td>(Optional) Sets the number of characters into the received message or buffer where the probe starts searching for the defined expression. Enter an number from 1 to 4000. (ACE appliance only) If you do not include the <code>cache</code> keyword when entering this command, the <code>number</code> argument is from 1 to 4000. However, if you include the <code>cache</code> keyword, the offset maximum number is 163840.</td>
</tr>
<tr>
<td><code>cache</code></td>
<td>(ACE appliance only, Optional for HTTP and HTTPS probes only) Enables caching when regex parsing long web pages. By default, when you configure the <code>expect regex</code> command for HTTP or HTTPS probes in probe configuration mode, the ACE does not cache the web page parsed by the probes. If the web page is longer than 4kBytes and the regex matching string exceeds this length, the probe fails.</td>
</tr>
<tr>
<td><code>length</code></td>
<td>(ACE appliance only, Optional) Cache length. Enter a number from 1 to 1000. The default cache length is 1000.</td>
</tr>
</tbody>
</table>

### Command Modes

Finger, HTTP, HTTPS, SIP, TCP, and UDP probe configuration modes

Admin and user contexts

### Command History

<table>
<thead>
<tr>
<th>ACE Module Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.0(0)A1(2)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ACE Appliance Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1(7)</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>A3(2.7). Not applicable to A4(1.0) or A4(2.0).</td>
<td>Added the <code>cache [length]</code> option for regex parsing of long web pages.</td>
</tr>
</tbody>
</table>
Usage Guidelines

When you configure a probe to expect a string from a server, it searches the response for a configured string. If the ACE finds the expected string, the server is marked as passed. If you do not configure an expected string, the ACE ignores the server response.

If you configure the `expect regex` command for TCP probes, you must configure the `send-data` command. Otherwise, the probe performs a connection open and close without checking the response from the server.

For HTTP or HTTPS probes, the server response must include the Content-Length header for the `expect regex` command to function. Otherwise, the probe does not attempt to parse the regex.

(ACE appliance only) For the `cache` option, consider the following:

- The HTML file configured with the `request method` command cannot exceed the length of the offset plus the length of the cache. If the file exceeds this length, the probes fail.
- For HTTP and HTTPS probes with active and standby ACEs that are running different software versions, any incremental changes made for the `expect regex` command are not synchronized. Any synchronization changes to the other ACE occur through bulk synchronization. Bulk synchronization takes place as expected.

Examples

To configure a TCP probe to expect an ACK response, enter:

```
host1/Admin(config-probe-tcp)# expect regex ack
```

(ACE appliance only) To configure the expected response string with caching with the default cache length of 1000, enter:

```
host1/Admin(config-probe-http)# expect regex test cache
```

To remove the expectation of a response expression for a TCP probe, enter:

```
host1/Admin(config-probe-tcp)# no expect
```

To remove the expectation of a response expression for an HTTP probe, enter:

```
host1/Admin(config-probe-http)# no expect regex
```

Related Commands

`show probe`
(config-probe-probe_type) expect status

To configure a single status code or a range of status code responses that the ACE expects from the probe destination, use the `expect status` command. You can specify multiple status code ranges with this command by entering the command with different ranges separately. Use the `no` form of this command to remove the expected status code or codes from the configuration.

```
expect status min_number max_number

no expect status min_number max_number
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>min_number</code></td>
<td>Single status code or the lower limit of a range of status codes. Enter an integer from 0 to 999.</td>
</tr>
<tr>
<td><code>max_number</code></td>
<td>Upper limit of a range of status codes. Enter an integer from 0 to 999. When configuring a single code, reenter the <code>min_number</code> value.</td>
</tr>
</tbody>
</table>

**Command Modes**

FTP, HTTP, HTTPS, RTSP, SIP, and SMTP probe configuration modes  
Admin and user contexts

**Command History**

<table>
<thead>
<tr>
<th>ACE Module Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.0(0)A1(2)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ACE Appliance Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1(7)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When the ACE receives a response from the server, it expects a status code to mark a server as passed. By default, no status codes are configured on the ACE. If you do not configure a status code, any response code from the server is marked as failed.

For HTTP and HTTPS, if you configure the `expect-regex` command without configuring a status code, the probe will pass if the regular expression response string is present.

You can specify multiple status code ranges with this command by entering the command with different ranges one at a time. Both the `min_number` and the `max_number` values can be any integer between 0 and 999 if the `max_number` is greater than or equal to the `min_number`. When the `min_number` and `max_number` values are the same, the ACE uses a single status code number.

**Examples**

To configure an expected status code of 200 that indicates that the HTTP request was successful, enter:

```
host1/Admin(config-probe-http)# expect status 200 200
```

To configure a range of expected status codes from 200 to 202, enter:

```
host1/Admin(config-probe-rtsp)# expect status 200 202
```
To configure multiple ranges of expected status codes from 200 to 202 and 204 to 205, configure each range separately. Enter:

```plaintext
code snippet
host1/Admin(config-probe-http)# expect status 200 202
host1/Admin(config-probe-http)# expect status 204 205
```

To remove a single expected status code of 200, enter:

```plaintext
code snippet
host1/Admin(config-probe-sip-udp)# no expect status 200 200
```

To remove a range of expected status codes, enter:

```plaintext
code snippet
host1/Admin(config-probe-http)# no expect status 200 202
```

To remove multiple ranges of expected status codes, you must remove each range separately. If you have set two different ranges (200 to 202 and 204 to 205), enter:

```plaintext
code snippet
host1/Admin(config-probe-http)# no expect status 200 202
host1/Admin(config-probe-http)# no expect status 204 205
```

**Related Commands**  
`show probe`

### (config-probe-probe_type) faildetect

To change the number of consecutive failed probes, use the `faildetect` command. Use the `no` form of this command to reset the number of probe retries to its default.

```plaintext
code snippet
faildetect retry-count
no faildetect
```

**Syntax Description**

<table>
<thead>
<tr>
<th>retry_count</th>
<th>Consecutive number of failed probes before marking the server as failed. Enter a number from 1 to 65535. The default is 3.</th>
</tr>
</thead>
</table>

**Command Modes**

All probe-type configuration modes

Admin and user contexts

**Command History**

<table>
<thead>
<tr>
<th>ACE Module Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.0(0)A1(2)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ACE Appliance Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1(7)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Before the ACE marks a server as failed, it must detect that probes have failed a consecutive number of times. By default, when three consecutive probes have failed, the ACE marks the server as failed.
Examples

To set the number of failed probes to 5 before declaring the server as failed for a TCP probe, enter:

```
host1/Admin(config-probe-tcp)# faildetect 5
```

To reset the number of probe failures to the default of 3, enter:

```
host1/Admin(config-probe-tcp)# no faildetect
```

Related Commands

`show probe`

(config-probe-
probe_type) hash

To configure the ACE to dynamically generate the MD5 hash value or manually configure the value, use the `hash` command. By default, no hash value is configured on the ACE. Use the `no` form of this command to configure the ACE to no longer compare the referenced hash value to the computed hash value.

```
hash [value]
no hash
```

Syntax Description

(value) (Optional) The MD5 hash value that you want to manually configure. Enter the MD5 hash value as a hexadecimal string with exactly 32 characters (16 bytes).

Command Modes

HTTP and HTTPS probe configuration mode
Admin and user contexts

Command History

<table>
<thead>
<tr>
<th>ACE Module Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.0(0)A1(2)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ACE Appliance Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1(7)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

If you do not use this command to configure the hash value, the ACE does not calculate a hash value on the HTTP data returned by the probe.

When you enter this command with no argument, the ACE generates the hash on the HTTP data returned by the first successful probe. If subsequent HTTP server hash responses match the generated hash value, the ACE marks the server as passed. If a mismatch occurs due to changes to the HTTP data, the probe fails and the `show probe ... detail` command displays an MD5 mismatch error in the Last disconnect error field.

To clear the reference hash and have the ACE recalculate the hash value at the next successful probe, change the URL or method by using the `request method` command.
The server response must include the Content-Length header for the `hash` command to function. Otherwise, the probe does not attempt to parse the hash value.

You can configure the `hash` command on a probe using the HEAD method, however there is no data to hash and has no effect causing the probe to always succeed.

**Examples**

To configure the ACE to generate the hash on the HTTP data returned by the first successful probe, enter:

```
host1/Admin(config-probe-http)# hash
```

To manually configure a hash value, enter:

```
host1/Admin(config-probe-http)# hash 0123456789abcdef0123456789abcdef
```

To configure the ACE to no longer compare the referenced hash value to the computed hash value, enter:

```
host1/Admin(config-probe-http)# no hash
```

**Related Commands**

- `show probe`
- `(config-probe-probe_type) request method`

**(`config-probe-probe_type) header**

To configure a header field value for a probe, use the `header` command. Use the `no` form of this command to remove the header field from the probe configuration.

For HTTP and HTTPS probes, the syntax is as follows:

```
header field_name header-value field_value
```

```
no header field_name
```

For RTSP probes, the syntax is as follows:

```
header {require | proxy-require} header-value field_value
```

```
no header {require | proxy-require}
```

**Syntax Description**

- `field_name` (HTTP and HTTPS probes) Identifier for a standard header field. Enter a text string with a maximum of 64 alphanumeric characters. If the header field includes spaces, enclose the string in quotation marks (" "). You can also enter one of the following header keywords:
  - `Accept`—Accept request header
  - `Accept-Charset`—Accept-Charset request header
  - `Accept-Encoding`—Accept-Encoding request header
  - `Accept-Language`—Accept-Language request header
  - `Authorization`—Authorization request header
  - `Cache-Control`—Cache-Control general header
  - `Connection`—Connection general header
Chapter 2 CLI Commands

Probe Configuration Mode Commands

Command Modes

HTTP, HTTPS, and RTSP probe configuration mode

Admin and user contexts

Command History

<table>
<thead>
<tr>
<th>ACE Module Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.0(0)A1(2)</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>A2(1.0)</td>
<td>This command was revised.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ACE Appliance Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1(7)</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>A3(1.0)</td>
<td>This command was revised.</td>
</tr>
</tbody>
</table>

Usage Guidelines

For each HTTP or HTTPS probe in your configuration, you can configure multiple header fields.

Examples

To configure the Accept-Encoding HTTP header with a value of identity, enter:

```
host1/Admin(config-probe-http)# header Accept-Encoding header-value identity
```

To remove the header with the Accept-Encoding field name from the probe, enter:

```
host1/Admin(config-probe-http)# no header Accept-Encoding
```

To configure the RTSP REQUIRE header with a field value of implicit-play, enter:

```
host1/Admin(config-probe-rtsp)# header require header-value implicit-play
```
To remove the header configuration for the RTSP probe, enter:

```
host1/Admin(config-probe-rtsp)# no header require
```

To remove a Proxy-Require header, enter:

```
host1/Admin(config-probe-rtsp)# no header proxy-require
```

**Related Commands**

`show probe`
(config-probe-probe_type) interval

To change the time interval between probes, use the interval command. The time interval between probes is the frequency that the ACE sends probes to the server marked as passed. Use the no form of this command to reset the default time interval of 15 seconds.

    interval seconds

    no interval

**Syntax Description**

| seconds | Time interval in seconds. Enter a number from 2 to 65535. The default is 15. |

**Command Modes**

All probe-type configuration modes
Admin and user contexts

**Command History**

<table>
<thead>
<tr>
<th>ACE Module Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.0(0)A1(2)</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>A4(1.0)</td>
<td>The default is 15. Previously, it was 120.</td>
</tr>
<tr>
<td>A4(2.0)</td>
<td>Added the interval command for VM probes.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ACE Appliance Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1(7)</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>A4(2.0)</td>
<td>Added the interval command for VM probes.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The open timeout value for TCP-based probes and the receive timeout value can impact the execution time for a probe. When the probe interval is less than or equal to these timeout values and the server takes a long time to respond or it fails to reply within the timeout values, the probe is skipped. When the probe is skipped, the No. Probes skipped counter through the show probe detail command increments.

**Examples**

To configure a time interval of 50 seconds for a TCP probe, enter:

```
host1/Admin(config-probe-tcp)# interval 50
```

To reset the time interval to the default of 15 seconds, enter:

```
host1/Admin(config-probe-tcp)# no interval
```

**Related Commands**

show probe
(config-probe-
probe_type) ip address

To override the destination address that the probe uses, use the ip address command. By default, the
probe uses the IP address from the real server or server farm configuration for the destination IP address.
Use the no form of this command to reset the default of the probe.

ip address ip_address [routed]

no ip address

Syntax Description

| ip_address | Destination IP address. The default is the IP address from the real
server or server farm configuration. Enter a unique IPv4 address in
dotted-decimal notation (for example, 192.168.12.15). |
|------------|--------------------------------------------------------------------------------------------------|
| routed     | (Optional) Routes the address according to the ACE internal routing table. If you are configuring a probe under a redirect server, you must configure this option. 
(ACE module only) Hardware-initiated SSL probes do not support this option. |

Command Modes

All probe-type configuration modes except scripted probe configuration mode
Admin and user contexts

Command History

<table>
<thead>
<tr>
<th>ACE Module Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.0(0)A1(2)</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>A5(1.0)</td>
<td>Added IPv6 support.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ACE Appliance Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1(7)</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>A3(2.7). Not applicable for A4(1.0).</td>
<td>Support added to configure a probe under a redirect server or server farm.</td>
</tr>
<tr>
<td>A5(1.0)</td>
<td>Added IPv6 support.</td>
</tr>
</tbody>
</table>

Usage Guidelines

This command has no usage guidelines.

Examples

IPv6 Example

To configure an IPv6 address of 2001:DB8:12::15, enter:

host1/Admin(config-probe-type)# ip address 2001:DB8:12::15

To reset the default behavior of the probe using the IPv6 address from the real server or server farm configuration, use the no ip address command. For example, enter:

host1/Admin(config-probe-type)# no ip address
**IPv4 Example**

To configure an IP address of 192.8.12.15, enter:

```
host1/Admin(config-probe-type)# ip address 192.8.12.15
```

To reset the default behavior of the probe using the IP address from the real server or server farm configuration, use the `no ip address` command. For example, enter:

```
host1/Admin(config-probe-type)# no ip address
```

**Related Commands**  
`show probe`
(config-probe-probe_type) nas ip address

To configure a Network Access Server (NAS) address, use the **nas ip address** command. Use the **no** form of this command to remove the NAS address.

```plaintext
nas ip address ip_address

no nas ip address
```

### Syntax Description

- **ip_address**
  
  NAS IP address. Enter a unique IPv4 address in dotted-decimal notation (for example, 192.168.12.15). By default, if a NAS address is not configured for the Remote Authentication Dial-In User Service (RADIUS) probe, the ACE uses the IP address associated with the outgoing interface as the NAS address.

### Command Modes

- RADIUS probe configuration mode
- Admin and user contexts

### Command History

<table>
<thead>
<tr>
<th>ACE Module Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.0(0)A1(2)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ACE Appliance Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1(7)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

If a NAS address is not configured for the RADIUS probe, the ACE performs a route lookup on the RADIUS server IP address.

### Examples

To configure a NAS address of 192.168.12.15, enter:

```plaintext
host1/Admin(config-probe-radius)# nas ip address 192.168.12.15
```

To remove the NAS IP address, enter:

```plaintext
host1/Admin(config-probe-radius)# no nas ip address
```

### Related Commands

- **show probe**
To configure an Object Identifier (OID) for an SNMP probe, use the `oid` command. When you enter this command, the CLI prompt changes to (config-probe-snmp-oid). For information about the commands available in probe SNMP OID configuration mode, see the **Probe SNMP OID Configuration Mode Commands** section. Use the `no` form of this command to remove the OID from the probe configuration.

```
oid string
```

```
no oid string
```

**Syntax Description**

`string`  
OID that the probe uses to query the server for a value. Enter an unquoted string with a maximum of 255 alphanumeric characters in dotted-decimal notation. The OID string is based on the server type.

**Command Modes**

SNMP probe configuration mode  
Admin and user contexts

**Command History**

<table>
<thead>
<tr>
<th>ACE Module Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A2(1.0)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ACE Appliance Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A3(1.0)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

When the ACE sends a probe with an SNMP OID query, the ACE uses the retrieved value as input to the least-loaded algorithm for load-balancing decisions. Least-loaded load balancing bases the server selection on the server with the lowest load value. If the retrieved value is within the configured threshold, the server is marked as passed. If the threshold is exceeded, the server is marked as failed.

You can configure a maximum of eight OID queries to probe the server.

**Examples**

To configure the OID string `.1.3.6.1.4.1.2021.10.1.3.1` and access probe SNMP OID configuration mode, enter:

```
host1/Admin(config-probe-snmp)# oid .1.3.6.1.4.1.2021.10.1.3.1
host1/Admin(config-probe-snmp-oid)#
```

To remove the OID string, enter:

```
host1/Admin(config-probe-snmp)# no oid .1.3.6.1.4.1.2021.10.1.3.1
```
Related Commands

- `show probe`
- `(config-probe-snmp-oid) threshold`
- `(config-probe-snmp-oid) type absolute max`
- `(config-probe-snmp-oid) weight`
(config-probe-probe_type) open

To configure the time interval for a connection to be established through a TCP three-way handshake, use the open command. By default, when the ACE sends a probe, it waits 1 second to open and establish the connection with the server. Use the no form of this command to reset its default of 1 second.

    open timeout

    no open

Syntax Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>timeout</td>
<td>Time in seconds. Enter an integer from 1 to 65535. The default is 1.</td>
</tr>
</tbody>
</table>

Command Modes

Echo TCP, Finger, FTP, HTTP, HTTPS, IMAP, POP, RTSP, scripted, SIP TCP, SMTP, TCP, and Telnet probe configuration mode

Admin and user contexts

Command History

<table>
<thead>
<tr>
<th>ACE Module Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.0(0)A1(2)</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>A4(1.0)</td>
<td>The default is 1. Previously, it was 10.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ACE Appliance Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1(7)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

The open timeout value for TCP-based probes and the receive timeout value can impact the execution time for a probe. When the probe interval is less than or equal to these timeout values and the server takes a long time to respond or it fails to reply within the timeout values, the probe is skipped. When the probe is skipped, the No. Probes skipped counter increments through the show probe detail command.

Examples

To configure the wait time interval to 25 seconds for a TCP probe, enter:

```
host1/Admin(config-probe-tcp)# open 25
```

To reset the time interval to its default of 1 second, enter:

```
host1/Admin(config-probe-tcp)# no open
```
(config-probe-
probe_type) passdetect

To configure the time interval to send a probe to a failed server and the number of consecutive successful probe responses required to mark the server as passed, use the passdetect command. Use the no form of this command to reset the default of waiting 60 seconds before sending out a probe to a failed server and marking a server as passed if it receives 3 consecutive successful responses.

```
passdetect {interval seconds | count number}
no passdetect {interval | count}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interval seconds</td>
<td>Specifies the wait time interval in seconds. Enter a number from 2 to 65535. The default is 60.</td>
</tr>
<tr>
<td>count number</td>
<td>Specifies the number of successful probe responses from the server. Enter a number from 1 to 65535. The default is 3.</td>
</tr>
</tbody>
</table>

**Command Modes**

All probe-type configuration modes except scripted probe configuration mode

Admin and user contexts

**Command History**

<table>
<thead>
<tr>
<th>ACE Module Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.0(0)A1(2)</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>A4(1.0)</td>
<td>The default is 60. Previously, it was 300.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ACE Appliance Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1(7)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

For best results, we recommend that you do not configure a passdetect interval value of less than 30 seconds. If you configure a passdetect interval value of less than 30 seconds, the open timeout and receive timeout values are set to their default values, and a real server fails to respond to a probe, overlapping probes may result, which can cause management resources to be consumed unnecessarily and the No. Probes skipped counter to increase.

After the ACE marks a server as failed, it waits a period of time and then sends a probe to the failed server. When the ACE receives a number of consecutive successful probes, it marks the server as passed. By default, the ACE waits 60 seconds before sending out a probe to a failed server and marks a server as passed if it receives 3 consecutive successful responses.

The receive timeout value can impact the execution time for a probe. When the probe interval is less than or equal to this timeout value and the server takes a long time to respond or it fails to reply within the timeout value, the probe is skipped. When the probe is skipped, the No. Probes skipped counter increments through the show probe detail command.

**Examples**

To configure a wait interval of 10 seconds for a TCP probe, enter:

```
host1/Admin(config-probe-tcp)# passdetect interval 10
```
To configure five success probe responses from the server before declaring it as passed, enter:

```
host1/Admin(config-probe-tcp)# passdetect count 5
```

To reset the wait interval to its default, enter:

```
host1/Admin(config-probe-tcp)# no passdetect interval
```

To reset the successful probe responses to its default, enter:

```
host1/Admin(config-probe-tcp)# no passdetect count
```

**Related Commands**

- `show probe`
(config-probe-probe_type) port

To configure the port number that the probe uses, use the port command. Use the no form of this command to reset the port number based on the probe type.

```
port port-number
no port
```

**Syntax Description**

```
port-number
```

Port number for the probe. Enter an integer from 1 to 65535.

**Command Modes**

All probe-type configuration modes except ICMP probe configuration mode

Admin and user contexts

**Command History**

<table>
<thead>
<tr>
<th>ACE Module Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.0(0)A1(2)</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>A4(1.0)</td>
<td>This command was revised to support probe port inheritance.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ACE Appliance Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1(7)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Table 2-22 lists the default port numbers for each probe type.

**Table 2-22 Default Port Numbers for Probe Types**

<table>
<thead>
<tr>
<th>Probe Type</th>
<th>Default Port Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS</td>
<td>53</td>
</tr>
<tr>
<td>Echo</td>
<td>7</td>
</tr>
<tr>
<td>Finger</td>
<td>79</td>
</tr>
<tr>
<td>FTP</td>
<td>21</td>
</tr>
<tr>
<td>HTTP</td>
<td>80</td>
</tr>
<tr>
<td>HTTPS</td>
<td>443</td>
</tr>
<tr>
<td>ICMP</td>
<td>Not applicable</td>
</tr>
<tr>
<td>IMAP</td>
<td>143</td>
</tr>
<tr>
<td>POP</td>
<td>110</td>
</tr>
<tr>
<td>RADIUS</td>
<td>1812</td>
</tr>
<tr>
<td>RTSP</td>
<td>554</td>
</tr>
<tr>
<td>SIP (TCP and UDP)</td>
<td>5060</td>
</tr>
<tr>
<td>SMTP</td>
<td>25</td>
</tr>
</tbody>
</table>
If you choose not to specify a port number for a probe, the ACE can dynamically inherit the port number specified:

- From the real server specified in a server farm (see the `(config-sfarm-host) rserver` command).
- From the VIP specified in a Layer 3 and Layer 4 class map (see the `(config-cmap) match virtual-address` command).

In this case, all you need is a single probe configuration, which will be sufficient to probe a real server on multiple ports or on all VIP ports. The same probe inherits all of the real server’s ports or all of the VIP ports and creates probe instances for each port.

**Note**

Probe port inheritance is not applicable for the server farm predictor method, a probe assigned to a standalone real server, or a probe configured on the active FT group member in a redundant configuration.

For a Layer 3 and Layer 4 class map, a VIP port will be inherited only if a `match` command consists of a single port. If you specify a wildcard value for the IP protocol value (the `any` keyword) or a port range for the port, port inheritance does not apply for those match statements.

The order of precedence for inheriting the probe’s port number is as follows:

1. Probe's configured port
2. Server farm real server's configured port
3. VIP's configured port
4. Probe's default port

For example, if the configured probe does not contain a specified port number, the ACE will look for the configured port associated with the real server specified in a server farm. If a port number is not configured, the ACE looks for the configured port associated with the VIP specified in a Layer 3 and Layer 4 class map. If a port number is also not configured, the ACE then uses the probe's default port to perform health monitoring on the back-end real server.

### Examples

To configure a port number of 88 for an HTTP probe, enter:

```
host1/Admin(config-probe-HTTP)# port 88
```

To reset the port number to its default, in this case, port 80 for an HTTP probe, enter:

```
host1/Admin(config-probe-HTTP)# no port
```

### Related Commands

`show probe`
(config-probe-probe_type) receive

To configure the time period that the ACE expects to receive a server response to the probe, use the receive command. Use the no form of this command to reset its default of 10 seconds.

receive seconds

no receive

Syntax Description

| seconds | Time to wait in seconds. Enter an integer from 1 to 65535. The default is 10. |

Command Modes

All probe-type configuration modes
Admin and user contexts

Command History

<table>
<thead>
<tr>
<th>ACE Module Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.0(0)A1(2)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

ACE Appliance Release Modification

<table>
<thead>
<tr>
<th>ACE Appliance Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1(7)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

By default, when the ACE sends a probe, it expects a response within a time period of 10 seconds. For example, for an HTTP probe, the timeout period is the number of seconds to receive an HTTP reply for a GET or HEAD request. If the server fails to respond to the probe, the ACE marks the server as failed.

The open timeout value for TCP-based probes and the receive timeout value can impact the execution time for a probe. When the probe interval is less than or equal to these timeout values and the server takes a long time to respond or it fails to reply within the timeout values, the probe is skipped. When the probe is skipped, the No. Probes skipped counter increments through the show probe detail command.

Examples

To configure the timeout period for a response at 5 seconds for a TCP probe, enter:

```
host1/Admin(config-probe-TCP)# receive 5
```

To reset the time period to receive a response from the server to its default of 10 seconds, enter:

```
host1/Admin(config-probe-TCP)# no receive
```

Related Commands

show probe
To configure the request command used by an Internet Message Access Protocol (IMAP) or POP probe, use the `request command` command. Use the `no` form of this command to remove the request command from the configuration.

```
request command command
no request
```

### Syntax Description

- **command**: Request command for the probe. Enter a text string with a maximum of 32 alphanumeric characters with no spaces.

### Command Modes

- IMAP and POP probe configuration modes
- Admin and user contexts

### Command History

<table>
<thead>
<tr>
<th>ACE Module Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.0(0)A1(2)</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>A2(1.0)</td>
<td>This command was revised.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ACE Appliance Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1(7)</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>A3(1.0)</td>
<td>This command was revised.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

You must configure the name of the mailbox using the `(config-probe-probe_type) credentials` command before you configure the request command used by an IMAP probe or the ACE will ignore the specified request command.

### Examples

To configure the last request command for an IMAP probe, enter:

```
host1/Admin(config-probe-imap)# request command last
```

To remove the request command for the probe, enter:

```
host1/Admin(config-probe-imap)# no request
```

### Related Commands

- `show probe`
To configure the request method and URL used by a probe, use the `request method` command. Use the `no` form of this command to reset the default request method.

For HTTP and HTTPS probes, the syntax is as follows:

```
request method {get | head} [url url_string]
```

```
no request method {get | head} [url url_string]
```

For RTSP probes, the syntax is as follows:

```
request method {options | describe url url_string}
```

```
no request method
```

For SIP probes, the syntax is as follows:

```
request method options
```

```
no request method
```

### Syntax Description

- **get** (HTTP or HTTPS probe) Configures the HTTP GET request method to direct the server to get the page. This method is the default.
- **head** (HTTP or HTTPS probe) Configures the HTTP HEAD request method to direct the server to get only the header for the page.
- **url url_string** (HTTP or HTTPS probe) Specifies the URL string used by the probe. Enter an alphanumeric string with a maximum of 255 characters. The default string is a forward slash (/).
- **options** (RTSP or SIP probe) Specifies the OPTIONS request method. This is the default method. The ACE uses the asterisk (*) request URL for this method.
- **describe url url_string** (RTSP probe) Specifies the DESCRIBE request method. The `url_string` is the URL request for the RTSP media stream on the server. Enter an alphanumeric string with a maximum of 255 characters.

### Command Modes

HTTP, HTTPS, RTSP, and SIP probe configuration modes

Admin and user contexts

### Command History

<table>
<thead>
<tr>
<th>ACE Module Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.0(0)A1(2)</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>A2(1.0)</td>
<td>This command was revised.</td>
</tr>
</tbody>
</table>
Usage Guidelines

By default, the HTTP request method is a GET with the URL of a forward slash (/). If you do not configure a URL, the HTTP or HTTPS probe functions as a TCP probe.

By default, the RTSP request method is the OPTIONS method. You can also configure the DESCRIBE method.

By default, the SIP request method is the OPTIONS method; this method is the only method available for SIP probes.

Examples

To configure the HTTP HEAD request method and the /digital/media/graphics.html URL used by an HTTP probe, enter:

```
host1/Admin(config-probe-http)# request method head url /digital/media/graphics.html
```

To reset the HTTP method for the probe to HTTP GET with a URL of “/”, enter:

```
host1/Admin(config-probe-http)# no request method head url /digital/media/graphics.html
```

To configure an RTSP probe to use the URL rtsp:///media/video.smi, enter:

```
host1/Admin(config-probe-rtsp)# request method describe url rtsp://192.168.10.1/media/video.smi
```

To reset the default RTSP request method (OPTIONS), use the `no request method` or the `request method options` command. For example, enter:

```
host1/Admin(config-probe-rtsp)# no request method
```

Related Commands

- show probe
- (config-probe-probe_type) hash

(config-probe-probe_type) script

To specify the script name and the arguments to be passed to a scripted probe, use the `script` command. Use the `no` form of this command to remove the script and its arguments from the configuration.

```
script script_name [script_arguments]

no script
```
## Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>script_name</code></td>
<td>Name of the script. Enter an unquoted text string with no spaces and a maximum of 255 alphanumeric characters.</td>
</tr>
<tr>
<td><code>script_arguments</code></td>
<td>(Optional) Data sent to the script. Enter a text string with a maximum of 255 alphanumeric characters including spaces and quotes. Separate each argument by a space. If a single argument contains spaces, enclose the argument string in quotes.</td>
</tr>
</tbody>
</table>

## Command Modes

- Scripted probe configuration mode
- Admin and user contexts

## Command History

<table>
<thead>
<tr>
<th>ACE Module Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.0(0)A1(2)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ACE Appliance Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1(7)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

## Usage Guidelines

Scripted probes run probes from a configured script to perform health probing. You can also configure arguments that are passed to the script. Before you can associate a script file with a probe, you must copy and load the script on the ACE. For information about TCL scripts and instructions for copying and loading script files on the ACE, see the *Server Load-Balancing Guide, Cisco ACE Application Control Engine*.

The ACE allows the configuration of 256 unique script files.

The ACE can simultaneously execute only 200 scripted probe instances. When this limit is exceeded, the `show probe detail` command displays the “Out-of Resource: Max. script-instance limit reached” error message in the Last disconnect err field and the out-of-sockets counter increments.

## Examples

To configure the script name of PROBE-SCRIPT and arguments of double question marks (??), enter:

```
host1/Admin(config-probe-scrptd)# script PROBE-SCRIPT ??
```

To remove the script and its arguments from the configuration, enter:

```
host1/Admin(config-probe-scrptd)# no script
```

## Related Commands

- `show probe`
- `show script`
- `(config) script file name`

### (config-probe-probe_type) send-data

To configure the ASCII data that the probe sends when the ACE connects to the server, use the `send-data` command. Use the `no` form of this command to remove the data from the configuration.
send-data expression

no send-data

**Syntax Description**

| expression | ASCII data that the probe sends. Enter an unquoted text string with no spaces and a maximum of 255 alphanumeric characters. |

**Command Modes**

ECHO, Finger, TCP, and UDP probe configuration modes
Admin and user contexts

**Command History**

<table>
<thead>
<tr>
<th>ACE Module Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.0(0)A1(2)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ACE Appliance Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1(7)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

If you do not configure the `send-data` command for a UDP probe, the probe sends one byte, 0x00.

When you configure the `expect regex` command for a TCP probe, you must configure the `send-data` command for the expect function to work. Otherwise, the TCP probe makes a socket connection and disconnects without checking the data.

**Examples**

To configure a TCP probe to send TEST as the data, enter:

```
host1/Admin(config-probe-tcp)# send-data TEST
```

To remove the data, enter:

```
host1/Admin(config-probe-tcp)# no send-data
```

**Related Commands**

`show probe`

**Command**

`(config-probe-probe_type) ssl cipher`

To configure the probe to expect a specific type of RSA cipher suite from the back-end server, use the `ssl cipher` command. Use the `no` form of this command to reset its default of accepting any RSA configured cipher suites.

```
ssl cipher {RSA_ANY \ cipher_suite}
no ssl cipher
```
**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th><strong>RSA_ANY</strong></th>
<th>Specifies that the probe accepts any of the RSA configured cipher suites. This is the default.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>cipher_suite</strong></td>
<td>RSA cipher suite that the probe expects from the back-end server. Enter one of the following keywords:</td>
</tr>
<tr>
<td></td>
<td><strong>RSA_EXPORT1024_WITH_DES_CBC_SHA</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>RSA_EXPORT1024_WITH_RC4_56_MD5</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>RSA_EXPORT1024_WITH_RC4_56_SHA</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>RSA_EXPORT_WITH_DES40_CBC_SHA</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>RSA_EXPORT_WITH_RC4_40_MD5</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>RSA_WITH_3DES_EDE_CBC_SHA</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>RSA_WITH_AES_128_CBC_SHA</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>RSA_WITH_AES_256_CBC_SHA</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>RSA_WITH_DES_CBC_SHA</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>RSA_WITH_RC4_128_MD5</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>RSA_WITH_RC4_128_SHA</strong></td>
<td></td>
</tr>
</tbody>
</table>

**Command Modes**

HTTPS probe configuration mode

Admin and user contexts

**Command History**

<table>
<thead>
<tr>
<th>ACE Module Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.0(0)A1(2)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ACE Appliance Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1(7)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command has no usage guidelines.

**Examples**

To configure the HTTPS probes with the RSA_WITH_RC4_128_SHA cipher suite, enter:

```
host1/Admin(config-probe-https)# ssl cipher RSA_WITH_RC4_128_SHA
```

To reset the default of the HTTPS probes accepting any RSA cipher suite, enter:

```
host1/Admin(config-probe-https)# ssl cipher RSA_ANY
```

To reset the default by using the **no ssl cipher** command, enter:

```
host1/Admin(config-probe-https)# no ssl cipher
```

**Related Commands**

**show probe**
(config-probe-probe_type) ssl version

To configure the version of Secure Sockets Layer (SSL) that the probe supports, use the `ssl version` command. Use the `no` form of this command to reset the default to SSL version 3.

```
ssl version {all | SSLv3 | TLSv1}
```

```
no ssl version
```

**Syntax Description**
- `all`: Configures the probe to support all SSL versions.
- `SSLv3`: Configures the probe to support SSL version 3. This is the default.
- `TLSv1`: Configures the probe to support TLS version 1.

**Command Modes**
- HTTPS probe configuration mode
- Admin and user contexts

**Command History**

<table>
<thead>
<tr>
<th>ACE Module Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.0(0)A1(2)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**ACE Appliance Release**

<table>
<thead>
<tr>
<th>ACE Appliance Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1(7)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
The version in the ClientHello message sent to the server indicates the highest supported version.

**Examples**

To configure the probe to support all SSL versions, enter:

```
host1/Admin(config-probe-https)# ssl version all
```

To reset the default of SSL version 3, enter:

```
host1/Admin(config-probe-https)# no ssl version
```

**Related Commands**
- `show probe`

---

( config-probe-probe_type ) version

To configure the version of SNMP that the probe supports, use the `version` command. Use the `no` form of this command to reset the version to its default value of SNMP version 1.

```
version {1 | 2c}
```

```
no version
```
### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Configures the probe to support SNMP version 1. This is the default.</td>
</tr>
<tr>
<td>2c</td>
<td>Configures the probe to support SNMP version 2c.</td>
</tr>
</tbody>
</table>

### Command Modes

- SNMP probe configuration mode
- Admin and user contexts

### Command History

<table>
<thead>
<tr>
<th>ACE Module Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A2(1.0)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ACE Appliance Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A3(1.0)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

The version in the SNMP OID query sent to the server indicates the supported SNMP version. By default, the probe supports SNMP version 1.

### Examples

To configure the probe to use SNMP version 2c, enter:

```
host1/Admin(config-probe-snmp)# version 2c
```

To reset the version of SNMP to the default value, SNMP version 1, enter:

```
host1/Admin(config-probe-snmp)# no version
```

### Related Commands

- `show probe`
(config-probe-sip-udp) rport enable

To force the SIP server to send the 200 OK message from the same port as the destination port of the probe request OPTIONS method per RFC 3581 when you configure the ACE for SIP UDP, use the **rport enable** command. By default, if the SIP server sends the 200 OK message from a port that is different from the destination port of the probe request, the ACE discards the response packet from the server. Use the **no** form of this command to reset the default behavior.

```
rport enable
no rport enable
```

**Syntax Description**
This command has no keywords or arguments.

**Command Modes**
SIP UDP probe configuration modes
Admin and user contexts

**Command History**

<table>
<thead>
<tr>
<th>ACE Module Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A2(2.3)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**ACE Appliance Release**

<table>
<thead>
<tr>
<th>ACE Appliance Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A3(2.5)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
This command has no usage guidelines.

**Examples**
To force the SIP server to send the 200 OK message from the destination port of the probe request OPTIONS method, enter:

```
host1/Admin(config-probe-sip-udp)# rport enable
```

To reset the ACE behavior to the default, enter:

```
host1/Admin(config-probe-sip-udp)# no rport enable
```

**Related Commands**

- `show probe`
Probe SNMP OID Configuration Mode Commands

Probe SNMP OID configuration mode commands allow you to configure an OID for an SNMP probe. To configure an OID for an SNMP probe and access probe SNMP OID configuration mode, use the **oid** command in SNMP probe configuration mode. The CLI prompt changes to (config-probe-snmp-oid). For information about the commands in this mode, see the following commands. Use the **no** form of this command to remove the OID from the SNMP probe configuration.

**oid string**

**no oid string**

### Syntax Description

| **string** | OID that the probe uses to query the server for a value. Enter an unquoted string with a maximum of 255 alphanumeric characters in dotted-decimal notation. The OID string is based on the server type. |

### Command Modes

SNMP probe configuration mode

Admin and user contexts

### Command History

<table>
<thead>
<tr>
<th><strong>ACE Module Release</strong></th>
<th><strong>Modification</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>A2(1.0)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>ACE Appliance Release</strong></th>
<th><strong>Modification</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>A3(1.0)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

When the ACE sends a probe with an SNMP OID query, the ACE uses the retrieved value as input to the least-loaded algorithm for load-balancing decisions. Least-loaded load balancing bases the server selection on the server with the lowest load value. If the retrieved value is within the configured threshold, the server is marked as passed. If the threshold is exceeded, the server is marked as failed.

You can configure a maximum of eight OID queries to probe the server.

### Examples

To configure the OID string `.1.3.6.1.4.2021.10.1.3.1` and access probe SNMP OID configuration mode, enter:

```
host1/Admin(config-probe-snmp)# oid .1.3.6.1.4.2021.10.1.3.1
host1/Admin(config-probe-snmp-oid)#
```

To remove the OID string, enter:

```
host1/Admin(config-probe-snmp)# no oid .1.3.6.1.4.2021.10.1.3.1
```
Related Commands

- `show probe`
- `(config-probe-snmp-oid) threshold`
- `(config-probe-snmp-oid) type absolute max`
- `(config-probe-snmp-oid) weight`
(config-probe-snmp-oid) threshold

To specify the threshold value for an OID, use the `threshold` command. Use the `no` form of this command to remove the threshold value.

```
threshold integer

no threshold integer
```

**Syntax Description**

- `integer`: Threshold value to take the server out of service. When the OID value is based on a percentile, enter an integer from 0 to 100, with a default value of 100. When the OID is based on an absolute value, the threshold range is from 1 to the maximum value specified using the `type absolute maximum` command.

**Command Modes**

- Probe SNMP OID configuration mode
- Admin and user contexts

**Command History**

<table>
<thead>
<tr>
<th>ACE Module Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A2(1.0)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ACE Appliance Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A3(1.0)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

You can configure a threshold for an OID value so that when the threshold is exceeded, the server is taken out of service.

When the ACE sends a probe with an SNMP OID query, the ACE uses the retrieved value as input to the least-loaded load-balancing algorithm for load-balancing decisions. Least-loaded load balancing bases the server selection on the server with the lowest load value. If the retrieved value is within the configured threshold, the server is marked as passed. If the threshold is exceeded, the server is marked as failed.

By default, the OID value is based on a percentile. If you use the `type absolute maximum` command to base the OID on an absolute value, the threshold range is from 1 to the maximum value specified with the `type absolute maximum` command.

**Examples**

To configure a threshold of 90 for the OID, enter:

```
host1/Admin(config-probe-snmp-oid)# threshold 90
```

To remove the threshold from the OID, enter:

```
host1/Admin(config-probe-snmp-oid)# no threshold
```
Related Commands

- `show probe`
- `(config-probe-probe_type) oid`
- `(config-probe-snmp-oid) type absolute max`
- `(config-probe-snmp-oid) weight`
(config-probe-snmp-oid) type absolute max

To specify that the retrieved OID value is an absolute value, use the type absolute max command. Use the no form of this command to remove the absolute value.

```
type absolute max integer
no type
```

### Syntax Description

<table>
<thead>
<tr>
<th>integer</th>
<th>Expected OID value. Enter an integer from 1 through 4294967295.</th>
</tr>
</thead>
</table>

### Command Modes

Probe SNMP OID configuration mode

Admin and user contexts

### Command History

**ACE Module Release** | Modification
----------------------|------------------
A2(1.0) | This command was introduced.

**ACE Appliance Release** | Modification
-------------------------|------------------
A3(1.0) | This command was introduced.

### Usage Guidelines

When the ACE sends a probe with an SNMP OID query, the ACE uses the retrieved value as input to the least-loaded algorithm for load-balancing decisions. By default, the ACE assumes that the retrieved OID value is a percentile value.

Least-loaded load balancing bases the server selection on the server with the lowest load value. If the retrieved value is within the configured threshold, the server is marked as passed. If the threshold is exceeded, the server is marked as failed.

When you configure the `type absolute max` command, we recommend that you also configure the value for the `threshold` command because the default threshold value is 100 and is not automatically adjusted with respect to the `type absolute max` value.

The `no type` command resets the values of both the `type absolute max` command and the `threshold` command to a value of 100.

### Examples

To specify that the retrieved maximum OID value is 597, enter:
```
host1/Admin(config-probe-snmp-oid) # type absolute max 597
```

To remove the OID value and reset the expected OID to a percentile, enter:
```
host1/Admin(config-probe-snmp-oid) # no type
```
Related Commands

- `show probe`
- `(config-probe-probe_type) oid`
- `(config-probe-snmp-oid) threshold`
- `(config-probe-snmp-oid) weight`
(config-probe-snmp-oid) weight

To configure the weight to be assigned to this OID for the SNMP probe, use the weight command. Use the no form of this command to remove the weight.

weight number

no weight

Syntax Description

| number | Weight value assigned to this OID for the SNMP probe. Enter an integer from 0 to 16000. |

Command Modes

Probe SNMP OID configuration mode
Admin and user contexts

Command History

<table>
<thead>
<tr>
<th>ACE Module Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A2(1.0)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ACE Appliance Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A3(1.0)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

If you configure more than one OID and they are used in a load-balancing decision, you must configure a weight value.

When the ACE sends a probe with an SNMP OID query, the ACE uses the retrieved value as input to the least-loaded algorithm for load-balancing decisions. Least-loaded load balancing bases the server selection on the server with the lowest load value. If the retrieved value is within the configured threshold, the server is marked as passed. If the threshold is exceeded, the server is marked as failed.

Examples

To configure a weight of 90 for the OID, enter:

`host1/Admin(config-probe-snmp-oid)# weight 90`

To remove the threshold from the OID, enter:

`host1/Admin(config-probe-snmp-oid)# no weight`

Related Commands

show probe
(config-probe-probe_type) oid
(config-probe-snmp-oid) threshold
(config-probe-snmp-oid) type absolute max
# Probe VM Configuration Mode Commands

Probe VM configuration mode commands allow you to configure a VM probe that the ACE uses to poll the local VM controller for the load of the local virtual machines (VMs) in a dynamic workload scaling (DWS) configuration. To configure a VM probe and access probe VM configuration mode, use the `probe vm` command in configuration mode. The CLI prompt changes to `(config-probe-vm)`. For information about the commands in this mode, see the commands in this section. Use the `no` form of this command to remove the VM probe from the ACE configuration.

```
probe vm probe_name

no probe vm probe_name
```

## Syntax Description

| `probe_name` | Unique identifier of the probe that the ACE uses to poll the vCenter for the load of the local VMs. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters. |

## Command Modes

VM probe configuration mode

Admin and user contexts

## Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A4(2.0)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

## Usage Guidelines

All commands in this mode require the probe feature in your user role. For details about role-based access control (RBAC) and user roles, see the `Virtualization Guide, Cisco ACE Application Control Engine`.

When the ACE sends a VM probe to a VM controller to retrieve the load of the local VMs, the ACE uses the retrieved load value to make a decision about bursting traffic to the remote data center. If the retrieved load equals or exceeds the configured load threshold, the ACE bursts traffic to the remote data center while it continues to load balance traffic to the local data center. When the VM load drops below the configured threshold for CPU and memory usage, the ACE load balances traffic only to the local data center.

The VM probe is not supported with IPv6.

## Examples

To configure a VM probe, enter the following command:

```
host1/Admin(config)# probe vm VM_PROBE
```

To remove the VM probe and all its attributes from the ACE configuration, enter the following command:

```
host1/Admin(config)# no probe vm
```
To specify the frequency with which the ACE sends probes to the VM controller, use the `interval` command. Use the `no` form of this command to remove the threshold value.

```
interval value

no interval value
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>value</code></td>
<td>Specifies the elapsed time between probes. Enter the time interval in seconds as an integer from 300 to 65535. The default is 300 seconds (5 minutes).</td>
</tr>
</tbody>
</table>

**Command Modes**

- Probe VM configuration mode
- Admin and user contexts

**Command History**

<table>
<thead>
<tr>
<th>ACE Module/Appliance</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>A4(2.0)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command requires the probe feature in your user role. For details about role-based access control (RBAC) and user roles, see the *Virtualization Guide, Cisco ACE Application Control Engine*.

**Examples**

To configure the ACE to send a probe to the VM controller every 420 seconds (7 minutes), enter the following command:

```
host1/Admin(config-probe-vm)# interval 420
```

To reset VM probe interval to the default value of 300 seconds (5 minutes), enter the following command:

```
host1/Admin(config-probe-vm)# no interval
```
(config-probe-vm) load

To specify the interesting load of the local VMs, use the load command. You can specify CPU usage, memory usage, or both. Use the no form of this command to remove the load from the configuration.

```
load {cpu | mem} burst-threshold {max value min value}
```

```
no load {cpu | mem} burst-threshold {max value min value}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>load {cpu</td>
<td>mem}</td>
</tr>
<tr>
<td>burst-threshold {max value min value}</td>
<td>Specifies the threshold values that determine when the ACE starts and stops bursting traffic through the local DCI device over the DCI link to the remote data center. Enter a maximum and a minimum threshold value as a load percentage from 1 to 99. The default value is 99 percent for both the max and the min keywords. A maximum burst threshold value of 1 percent instructs the ACE to always burst traffic to the remote data center. A maximum burst threshold value of 99 percent instructs the ACE to always load balance traffic to the local VMs unless the load value is equal to 100 percent or the VMs are not in the OPERATIONAL state.</td>
</tr>
</tbody>
</table>

If the average load value returned by the VM controller is greater than or equal to the maximum threshold value, the ACE starts bursting traffic to the remote data center. When the load value returned by the VM controller is less than the minimum threshold value, the ACE stops bursting traffic to the remote data center and load balances traffic to the local VMs. Any active connections to the remote data center are allowed to complete.

**Command Modes**

Probe VM configuration mode
Admin and user contexts

**Command History**

<table>
<thead>
<tr>
<th>ACE Module/Appliance Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A4(2.0)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
Usage Guidelines
This command requires the probe feature in your user role. For details about role-based access control (RBAC) and user roles, see the Virtualization Guide, Cisco ACE Application Control Engine.

Examples
To instruct the ACE to start bursting traffic to the remote datacenter when the local average VM load exceeds 80 percent CPU usage and to stop bursting traffic when the local average CPU usage drops below 50 percent, enter the following command:

```
host1/Admin(config-probe-vm)# load cpu burst-threshold max 80 min 50
```

You can configure an additional `load` command under the same VM probe to create an OR statement between the CPU usage and the memory usage of the local VMs. Whichever load type reaches its maximum threshold first will cause the ACE to burst traffic to the remote data center. For example, enter the following commands:

```
host1/Admin(config-probe-vm)# load cpu burst-threshold max 80 min 50
host1/Admin(config-probe-vm)# load mem burst-threshold max 70 min 40
```

In this case, if the average CPU usage reaches 80 percent or the average memory usage reaches 70 percent, the ACE bursts traffic to the remote data center. The ACE does not stop bursting traffic to the remote data center until both the CPU load and the memory load drop below their respective minimum configured values.

To reset the VM probe behavior to the default of checking the average VM CPU usage and memory usage against the maximum and minimum threshold values of 99 percent each, enter the following command:

```
host1/Admin(config-probe-vm)# no load cpu burst-threshold max 80 min 50
host1/Admin(config-probe-vm)# no load mem burst-threshold max 70 min 40
```

Related Commands
- `show probe (config-probe-vm) interval`
- `show probe (config-probe-vm) vm-controller`
(config-probe-vm) vm-controller

To identify the VM controller for the probe, use the vm-controller command. Use the no form of this command to remove the VM controller name from the VM probe configuration.

```
vm-controller name
no vm-controller name
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>name</code></td>
<td>Identifier of the existing VM controller that you previously configured. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.</td>
</tr>
</tbody>
</table>

**Command Modes**

- Probe VM configuration mode
- Admin and user contexts

**Command History**

<table>
<thead>
<tr>
<th>ACE Module/Appliance</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release</td>
<td>Modification</td>
</tr>
<tr>
<td>A4(2.0)</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

This command requires the probe feature in your user role. For details about role-based access control (RBAC) and user roles, see the Virtualization Guide, Cisco ACE Application Control Engine.

**Examples**

To configure the VM controller called VCENTER_1, enter the following command:
```
host1/Admin(config-probe-vm)# vm-controller VCENTER_1
```

To remove the VM controller name from the VM probe configuration, enter the following command:
```
host1/Admin(config-probe-vm)# no vm-controller VCENTER_1
```

**Related Commands**

- `show probe`
- `(config-probe-vm) interval`
- `(config-probe-vm) load`