

TESTINGGGGGGGGGGGGGGGG

Guía de resolución de problemas de Cisco Application Control Engine (ACE): resolución de problemas de supervisión de estado de ACE

Contenido

- 1 Descripción general de la supervisión de estado de ACE
 - 1.1 Tipos de sondeos
 - 1.2 Configuración de sondas
 - 1.3 Ejemplo de configuración de una sonda
- 2 Solución de problemas de supervisión de estado ACE
 - 2.1 Resolución de problemas de sonda básica
 - 2.2 Resolución de problemas de un error de sonda TCP
 - 2.3 Resolución de problemas de un error de sonda UDP
 - 2.4 Resolución de problemas de un error de sonda HTTP
 - 2.5 Resolución de problemas de un error de sonda HTTPS
 - 2.6 Resolución de problemas de una sonda SNMP
 - 2.7 Uso del campo Último código de estado
 - 2.8 Depuraciones de sondeo

Descripción general de la supervisión de estado de ACE

En esta sección se describe la supervisión del estado de la ACE.

La ACE utiliza sondeos como supervisión de estado fuera de banda (OOB) para realizar un seguimiento del estado de un servidor. De forma predeterminada, no se configura ningún sondeo en la ACE. La ACE verifica la respuesta del servidor a una sonda (o si no hay respuesta en absoluto) para comprobar si hay algún problema de red o de aplicación que pueda impedir que un cliente llegue a un servidor. Según la respuesta del servidor, la ACE puede colocar el servidor dentro o fuera de servicio y puede tomar decisiones confiables de balanceo de carga.

También puede utilizar la supervisión de estado para detectar fallos de una puerta de enlace o un host en configuraciones de alta disponibilidad (redundantes). Para obtener más información, vea la [Guía de Administración del Módulo Cisco Application Control Engine](#).

La ACE evalúa el estado de un servidor marcando los sondeos de la siguiente manera:

- Pasado: el servidor devuelve una respuesta válida.
- Error: el servidor no puede proporcionar una respuesta válida a la ACE y la ACE no puede alcanzar un servidor durante un número especificado de reintentos.

Al configurar la ACE para la supervisión de estado, la ACE envía sondeos activos periódicamente para determinar el estado del servidor. La ACE admite configuraciones de sondeo únicas 4096, que incluyen ICMP, TCP, HTTP y otros sondeos de estado predefinidos. La ACE sólo puede ejecutar hasta 200 sondas con scripts a la vez. El ACE también permite la apertura de 2048 sockets simultáneamente.

Puede asociar la misma sonda con varios servidores reales o conjuntos de servidores. Cada vez que utilice el mismo sondeo de nuevo, la ACE lo cuenta como otra instancia de sondeo. Puede asignar un máximo de 16 000 instancias de sondeo.

ACE también admite una función de supervisión de estado en banda (deshabilitada de forma predeterminada), que realiza un seguimiento de los errores de conexión en los servidores reales de un conjunto de servidores:

- Para TCP, restablece (RST) los tiempos de espera del servidor o SYN
- Para mensajes UDP, ICMP Host, Network, Port, Protocol y Source Route inalcanzable

Cuando configura un umbral de recuento de fallas y el número de estas fallas excede el umbral dentro del intervalo de tiempo de restablecimiento, la ACE inmediatamente marca al servidor como fallado, lo saca de servicio y lo elimina del balanceo de carga. El servidor no se tiene en cuenta para el equilibrio de carga hasta que caduque el intervalo de reanudación de servicio opcional.

Para obtener más información sobre la supervisión del estado dentro de la banda, vea la [Guía de Balanceo de Carga del Servidor del Módulo Cisco Application Control Engine](#).

Tipos de sondeo

- Sonda ICMP
 - Envía una solicitud de eco
 - Espera una respuesta de Eco
- Sonda TCP genérica
 - Abrir una conexión con el servidor y desconectar con TCP FIN (predeterminado)
 - TCP RST se puede utilizar para cerrar la sonda TCP si se desea
- Sonda UDP genérica
 - Envía un paquete, la sonda se considera exitosa, si no se recibe ningún error icmp
- Sonda HTTP
 - Envía una solicitud "GET / HTTP 1.1"

- Se espera una respuesta HTTP con el código devuelto configurado

- Sonda HTTPS

- Establece una conexión SSL, envía una consulta HTTP y la elimina
- La solicitud/respuesta HTTP funciona como con la sonda HTTP

- Sondeo FTP

- De forma similar a la sonda TCP, envíe un mensaje "QUIT"

- Sonda Telnet

- Realiza una conexión, envía un mensaje "QUIT"

- Sonda DNS

- Envía una consulta DNS, utiliza un dominio predeterminado de " www.cisco.com
- Espera una respuesta IP para el dominio consultado

- Sondeo SMTP

- Envía un mensaje "HELO" seguido de un mensaje "QUIT"

- Sonda POP3

- Similar a la sonda TCP, puede enviar credenciales de usuario

- Sonda IMAP

- Similar a la sonda TCP, puede enviar credenciales de usuario

- Sonda SIP

- Puede estar basado en TCP o UDP. Enviar una solicitud de opciones
- Puede comparar la respuesta con el código de respuesta configurado o la cadena esperada, o con ambos

- Sonda RTSP

- Similar a la sonda HTTP. Enviar una solicitud OPTIONS o DESCRIBE

- Sonda Radius

- Similar a la sonda UDP. NAS-IP se puede configurar

Configuración de sondeos

Puede configurar sondeos de estado en la ACE para realizar conexiones de forma activa y enviar tráfico explícitamente a los servidores. Los sondeos determinan si el estado de un servidor pasa o falla según la respuesta del servidor.

La configuración de sondas activas es un proceso de tres pasos:

1. Configure el sondeo de estado con un nombre, un tipo y atributos.
2. Asocie la sonda a una de las siguientes opciones:
 - Un servidor real.
 - Instancia de servidor real dentro de un conjunto de servidores específico. Puede asociar uno o varios sondeos a servidores reales dentro de un conjunto de servidores.
 - Un conjunto de servidores. Todos los servidores del conjunto de servidores reciben sondeos de los tipos de sondeo asociados.
3. Ponga en servicio el servidor real o conjunto de servidores.

Para obtener más información, vea la [Guía de equilibrio de carga del servidor del módulo Cisco Application Control Engine](#).

Ejemplo de configuración de una sonda

El siguiente ejemplo muestra una configuración en ejecución que equilibra la carga del tráfico DNS a través de varios servidores reales y transmite y recibe datos UDP que abarcan varios paquetes. La configuración utiliza una sonda de mantenimiento UDP.

```
access-list ACL1 line 10 extended permit ip any any

probe udp UDP
  interval 5
  passdetect interval 10
  description THIS PROBE IS INTENDED FOR LOAD BALANCING DNS TRAFFIC
  port 53
  send-data UDP_TEST

rserver host SERVER1
  ip address 192.168.10.45
  inservice
rserver host SERVER2
  ip address 192.168.10.46
  inservice
rserver host SERVER3
  ip address 192.168.10.47
```

```

inservice

serverfarm host SFARM1
  probe UDP
  rserver SERVER1
    inservice
  rserver SERVER2
    inservice
  rserver SERVER3
    inservice

class-map match-all L4UDP-VIP_114:UDP_CLASS
  2 match virtual-address 192.168.120.114 udp eq 53

policy-map type loadbalance first-match L7PLBSF_UDP_POLICY
  class class-default
    serverfarm SFARM1
policy-map multi-match L4SH-Gold-VIPs_POLICY
  class L4UDP-VIP_114:UDP_CLASS
    loadbalance vip inservice
    loadbalance policy L7PLBSF_UDP_POLICY
    loadbalance vip icmp-reply
  nat dynamic 1 vln 120
  connection advanced-options 1SECOND-IDLE

interface vln 120
  description Upstream VLAN_120 - Clients and VIPs
  ip address 192.168.120.1 255.255.255.0
  fragment chain 20
  fragment min-mtu 68
  access-group input ACL1
  nat-pool 1 192.168.120.70 192.168.120.70 netmask 255.255.255.0 pat
  service-policy input L4SH-Gold-VIPs_POLICY
  no shutdown

ip route 10.1.0.0 255.255.255.0 192.168.120.254

```

Solución de problemas de supervisión de estado ACE

Esta sección describe cómo resolver problemas comunes de configuración de sonda.

Resolución de problemas de sonda básica

El resultado más importante del comando para verificar la resolución de problemas de sonda básica es `show probe detail`:

```
<#root>
```

```
ACE_module5/Admin#
```

```
show probe detail
```

```

probe      : icmp-probe
type       : ICMP, state :

```

ACTIVE

description :

```
-----
port      : 0      address      : 0.0.0.0      addr type : -
interval  : 10     pass intvl   : 10           pass count : 3
fail count: 5     recv timeout: 5
```

```
----- probe results -----
probe association  probed-address  probes
```

failed

passed

health

```
-----+-----+-----+-----+
rserver      : rs1
              10.7.107.51    230      6      224
```

FAILED

Socket state : RESET

No. Passed states : 1 No. Failed states : 1

No. Probes skipped : 0 Last status code : 0

Last disconnect err :

Host Unreachable, no route found to destination

Last probe time : Sat Feb 18 18:24:18 2006

Last fail time : Sat Feb 18 18:24:08 2006

Last active time : Sat Feb 18 17:46:08 2006

- Estado de la sonda: "INIT", "FAILED", "PASSED", "DISABLED"
- Estado del socket: "RESTABLECER", "ABRIR", "RECIBIR", "CERRADO"

- Último error de desconexión: Mensajes de error genéricos o específicos del tipo de sonda:
 - "Restablecimiento de la conexión por el servidor"
 - "Conexión rechazada por el servidor"
 - "Respuesta no reconocida o no válida"
 - "Tiempo de espera de apertura del servidor (sin SYN ACK)"
 - "Tiempo de espera de respuesta del servidor (sin respuesta)"
 - "Se espera una discordancia de código de estado"
 - "Código de estado no válido recibido"
 - "Error interno: El script se ha finalizado debido a un tiempo de espera agotado"
 - "Error interno de ICMP: No hay espacio, la ruta de transmisión está llena"
 - "Error interno: Error al crear la sesión SSL"
 - "Paquete obsoleto ICMP recibido"
 - ...

Resolución de problemas de un error de sondeo TCP

Los campos "Socket State" y "Last disconnect err" en el resultado de show probe detail deben proporcionar la mayor parte de la información necesaria. Revise esto junto con un rastro del sabueso del tráfico de la sonda.

Resolución de problemas de un error de sondeo UDP

Los campos "Socket State" y "Last disconnect err" en el resultado de show probe detail deben proporcionar la mayor parte de la información necesaria. Revise esto junto con un rastro del sabueso del tráfico de la sonda.

Solución de problemas de un error de sondeo HTTP

En este primer escenario, ha configurado un sondeo HTTP, pero el estado del servidor real se muestra como FAILED y el campo Last disconnect err indica que se recibió un código de estado no válido como se muestra en el resultado del comando show probe detail. Ha comprobado el servidor y está en funcionamiento. Una captura de paquetes en el servidor también muestra que todo está bien. ¿Dónde está el problema?

1. Muestre los detalles del estado de la sonda introduciendo el siguiente comando:

```
<#root>
```

ACE_module5/Admin#

show probe detail

probe : HTTP_PROBE
type : HTTP
state : ACTIVE
description :

port : 80 address : 0.0.0.0 addr type : -
interval : 10 pass intvl : 10 pass count : 3
fail count: 3 recv timeout: 10
http method : GET
http url : /
conn termination : GRACEFUL
expect offset : 0 , open timeout : 1
expect regex : -
send data : -

----- probe results -----
associations ip-address port porttype probes failed passed health
-----+-----+-----+-----+-----+-----+-----
rserver : SERVER1
192.168.10.45 80 -- 2 2 0 FAILED

Socket state : CLOSED
No. Passed states : 0 No. Failed states : 1

No. Probes skipped : 0 Last status code : 200 <----- Last status code from server

No. Out of Sockets : 0 No. Internal error: 0

Last disconnect err : Received invalid status code <-----

Last probe time : Tue Apr 7 16:17:26 2009
Last fail time : Tue Apr 7 16:17:16 2009
Last active time : Never

El campo Last disconnect err indica que la ACE recibió un código de estado no válido. Este error significa que no ha configurado el comando Expect Status para la sonda.

2. Confirme esta conclusión introduciendo el siguiente comando:

<#root>

ACE_module5/Admin#

show running-config probe

Generating configuration....

```
probe http HTTP_PROBE
  interval 10
  passdetect interval 10
  open 1
```


3. Corrija el problema introduciendo los siguientes comandos:

```
<#root>
```

```
ACE_module5/Admin#
```

```
config
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
ACE_module5/Admin(config)#
```

```
probe http HTTP_PROBE
```

```
ACE_module5/Admin(config-probe-http)#
```

```
expect status 200 200
```

```
<----- 200 indicates the 200 OK message from the server
```

```
ACE_module5/Admin(config-probe-http)#
```

```
end
```

4. Confirme la configuración introduciendo el siguiente comando:

```
<#root>
```

```
ACE_module5/Admin#
```

```
show running-config probe
```

```
Generating configuration....
```

```
probe http HTTP_PROBE
  interval 10
  passdetect interval 10
  expect status 200 200
  open 1
```

5. Muestre de nuevo los detalles del estado de la sonda y observe que el valor del estado del servidor es CORRECTO introduciendo el siguiente comando:

```
<#root>
```

```
ACE_module5/Admin#
```

```
show probe HTTP_PROBE detail
```

```
probe      : HTTP_PROBE
type       : HTTP
state      : ACTIVE
description :
-----
```

```

port      : 80      address      : 0.0.0.0      addr type : -
interval  : 10      pass intvl   : 10          pass count : 3
fail count: 3      rcv timeout: 10
http method      : GET
http url         : /
conn termination : GRACEFUL
expect offset    : 0      , open timeout      : 1
expect regex     : -
send data        : -

----- probe results -----
associations ip-address      port porttype probes  failed  passed  health
-----+-----+-----+-----+-----+-----+-----
rserver      : SERVER1
              192.168.10.45  80    --      24      15      9      SUCCESS

Socket state      : CLOSED
No. Passed states : 1      No. Failed states : 1
No. Probes skipped : 0      Last status code : 200
No. Out of Sockets : 0      No. Internal error: 0

Last disconnect err : - <----- No error indicated now. The probe is successful.

Last probe time    : Tue Apr  7 16:21:05 2009
Last fail time     : Tue Apr  7 16:17:16 2009
Last active time   : Tue Apr  7 16:20:05 2009

```

Resolución de problemas de un error de sondeo HTTPS

Además de los métodos para [Troubleshooting de un Error de Sondeo HTTP](#), utilice las estadísticas de SSL para resolver los fallos de sondeo HTTPS. El tráfico de sondeo HTTPS se ejecuta en el contexto virtual Admin, por lo que debe ver la salida del comando [show stats crypto client](#) en ese contexto.

También de manera diferente a todos los otros sondeos, los sondeos HTTPS se ejecutan en el plano de datos de la ACE. Por lo tanto, están sujetos a asignaciones de recursos para el tráfico SSL en ACE.

Resolución de problemas de una sonda SNMP

En este escenario, ha configurado una sonda SNMP, pero el campo Last disconnect err indica que la suma de los pesos no suma al valor de peso máximo como se muestra en la salida del comando show probe detail.

1. Muestre los detalles del estado de la sonda introduciendo el siguiente comando:

```
<#root>
```

```
ACE_module5/test#
```

```
show probe detail
```

```
probe      : SNMP_PROBE
```

```
type      : SNMP
state     : ACTIVE
description : snmp probe
```

```
-----
port      : 161      address      : 0.0.0.0      addr type : -
interval  : 15      pass intvl  : 10      pass count : 3
fail count: 3      recv timeout: 10
version   : 2c      community   : test_comm
oid string #1 : .1.3.6.1.2.1.4.3.0
type      : ABSOLUTE      max value : 1000000000
weight    : 10000      threshold : 1000000000
```

```
----- probe results -----
associations ip-address      port porttype probes  failed  passed  health
-----+-----+-----+-----+-----+-----+-----
serverfarm   : least-loaded, predictor least-loaded
  real       : SERVER1[0]
              192.168.10.45  161  --      0      0      0      INIT
```

```
Socket state      : CLOSED
No. Passed states : 0      No. Failed states : 0
No. Probes skipped : 0      Last status code : 0
No. Out of Sockets : 0      No. Internal error: 30
```

Last disconnect err : Sum of weights don't add up to max weight value <----- Error condition

```
Last probe time    : Never
Last fail time     : Never
Last active time   : Never
```

Server load : 16000 <----- Note the server load value

La razón de este error es que el comando weight debe configurarse cuando tiene varios OID configurados para una sola sonda y desde esos OID si desea dar prioridad a un OID específico.

La suma de los pesos debe ser igual a 16000 (consulte el campo Server Load). Para un solo OID, el comando weight no tiene ninguna importancia.

2. Muestre la configuración de la sonda introduciendo el siguiente comando:

<#root>

ACE_module5/Admin#

show running-config probe

```
probe snmp SNMP_PROBE
  description snmp probe
  port 161
  interval 15
  passdetect interval 10
  version 2c
  community TEST_COMM
  oid .1.3.6.1.2.1.4.3.0
  type absolute max 1000000000
```

```
weight 10000 <-----
```

En la configuración anterior, el peso se configura como 10000 para un solo OID. La ACE espera que se configure otro OID en la sonda y que la suma de ambos pesos sea igual a 16000.

La configuración no está completa y la ACE espera parámetros adicionales en la configuración de la sonda. Debido a que no hay otro OID en la configuración, la ACE no puede calcular la carga y es por eso que aparece el mensaje de error "Suma de pesos no suma el valor de peso máximo".

3. Resuelva el problema modificando la configuración de la sonda de la siguiente manera:

```
<#root>
```

```
probe snmp SNMP_PROBE
  description test
  port 161
  interval 15
  passdetect interval 60
  version 2c
  community test_comm
  oid .1.3.6.1.2.1.4.3.0
    type absolute max 1000000000
    weight 10000
  oid .1.3.6.1.2.1.4.10.0
    type absolute max 1000000000
```

```
weight 6000 <----- 10000 + 6000 = 16000
```

4. Vuelva a mostrar los detalles del estado de la sonda introduciendo el siguiente comando:

```
<#root>
```

```
ACE_module5/test#
```

```
show probe SNMP_PROBE detail
```

```
probe      : snmp1
type       : SNMP
state      : ACTIVE
description : snmp probe
```

```
-----
port       : 161      address      : 0.0.0.0      addr type : -
interval   : 15      pass intvl   : 10      pass count : 3
fail count : 3      rcv timeout : 10
version    : 2c      community   : test_comm
```

```
oid string #1 : .1.3.6.1.2.1.4.3.0
type          : ABSOLUTE      max value : 1000000000
weight        : 10000         threshold : 1000000000
```

```
oid string #2 : .1.3.6.1.2.1.4.10.0
type          : ABSOLUTE      max value : 1000000000
```

```

weight      : 6000                threshold : 1000000000
----- probe results -----
associations ip-address      port porttype probes  failed  passed  health
-----+-----+-----+-----+-----+-----+-----
serverfarm   : least-loaded, predictor least-loaded
  real       : SERVER1[0]
              192.168.10.45  161  --      4143    0      4143    SUCCESS

Socket state      : CLOSED
No. Passed states : 1           No. Failed states : 0
No. Probes skipped : 0         Last status code : 0
No. Out of Sockets : 0         No. Internal error: 0

Last disconnect err : - <----- No error indicated now. The probe is successful.

Last probe time    : Mon Apr  6 09:12:54 2009
Last fail time     : Never
Last active time   : Sun Apr  5 15:57:28 2009
Server load        : 0

```

Uso del campo Último código de estado

Se pueden proporcionar detalles sobre el último campo de código de estado para sondeos no triviales. Por ejemplo, en el caso de la sonda con scripts PROBENOTICE_PROBE, el código de estado 30001 significa que la sonda es correcta y el valor 30002 indica un error en los argumentos de la sonda. El último error de desconexión para el código de estado 30002 muestra "No recibió una respuesta correcta del servidor", pero el problema real está relacionado con los argumentos de la configuración de sondeo, que se pueden comprobar consultando la secuencia de comandos para el sondeo.

<#root>

ACE_module5/Admin#

show probe TEST detail

```

probe      : TEST
type       : SCRIPTED
state      : ACTIVE
description :
-----
port       : 0          address      : 0.0.0.0          addr type : -
interval   : 15         pass intvl  : 20                pass count : 3
fail count : 3          recv timeout: 10
script filename : PROBENOTICE_PROBE
----- probe results -----
probe association  probed-address  probes  failed  passed  health
-----+-----+-----+-----+-----+-----
serverfarm   : sf1
  real       : rs2[0]
              23.0.0.5      4082    54      4028    SUCCESS

Socket state      : RESET
No. Passed states : 6           No. Failed states : 5
No. Probes skipped : 8

```

Last status code : 30001 <----- Indicates success

No. Out of Sockets : 0 No. Internal error: 0
Last disconnect err : -
Last probe time : Wed Apr 8 04:44:41 2009
Last fail time : Tue Apr 7 12:02:10 2009
Last active time : Tue Apr 7 12:03:45 2009

Depuraciones de sondeo

Para una investigación más detallada de los fallos de sondeo, se puede realizar el siguiente plan de acción:

- Obtenga un show tech del contexto ACE Admin así como del contexto donde se configuran los sondeos
- Iniciar rastreos de sabueso capturando tráfico de sonda
- Recopilar depuraciones de sondeo:

1) crear un archivo de registro de depuración:

```
debug logfile probe.log
```

2) habilitar depuración:

```
debug hm errors  
debug hm events  
debug hm info
```

3) capturar fallas de sondeo, luego detener seguimientos de sabueso y desactivar la depuración:

```
no debug hm all  
-O-  
undebug all
```

4) para recopilar la salida del registro, ejecute el siguiente comando y copie la salida en un archivo de texto:

```
show debug logfile probe.log
```

5) Elimine el archivo de la ACE una vez que lo haya copiado:

```
clear debug-logfile test.log
```

- Obtenga otro show tech del contexto ACE Admin así como del contexto donde se configuran las

sondas después de la prueba

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).