本地流量管理配置指南

版本9.0

http://blog.s135.com/book/f5/

MAN-0122-01

产品版本

本指南适用于 9.0 版的 BIG-IP® Local Traffic Manager™、BIG-IP® Load Balancer Limited™和 BIG-IP® SSL Accelerator™。

法律声明

致谢

本产品包含 Bill Paul 开发的软件。
本产品包含 Jonathan Stone 开发的软件。
本产品包含 Manuel Bouyer 开发的软件。
本产品包含 Paul Richards 开发的软件。
本产品包含 NetBSD Foundation, Inc.及其无偿贡献者开发的软件。
本产品包含意大利都灵理工学院及其无偿贡献者开发的软件。

本产品包含瑞典计算机科学研究所及其无偿贡献者开发的软件。
本产品包含美国加利福尼亚大学伯克利分校及其无偿贡献者开发的软件。
本产品包含计算机系统工程小组在美国劳伦斯·伯克利国家实验室开发的软件。
本产品包含 Christopher G. Demetriou 为 NetBSD Project 开发的软件。
本产品包含 Adam Glass 开发的软件。
本产品包含 Christian E. Hopps 开发的软件。
本产品包含 Dean Huxley 开发的软件。
本产品包含 John Kohl 开发的软件。
本产品包含 Paul Kranenburg 开发的软件。
本产品包含 Terrence R. Lambert 开发的软件。
本产品包含 Philip A. Nelson 开发的软件。
本产品包含 Herb Peyerl 开发的软件。
本产品包含 Jochen Pohl 为 NetBSD Project 开发的软件。
本产品包含 Chris Provenzano 开发的软件。
本产品包含 Theo de Raadt 开发的软件。
本产品包含 David MuirSharnoff 开发的软件。
本产品包含 Sigmasoft 公司的 Th. Lockert 开发的软件。
本产品包含 Jason R. Thorpe 为 NetBSD Project 开发的软件。
本产品包含 Jason R. Thorpe 为 And Communications（http://www.and.com）开发的软件。
本产品包含 Frank Van der Linden 为 NetBSD Project 开发的软件。
本产品包含 John M. Vinopal 为 NetBSD Project 开发的软件。
本产品包含 Christos Zoulas 开发的软件。
本产品包含美国佛蒙特大学暨州立农学院与 Garrett A. Wollman 开发的软件。
在以下声明中，“本软件”是指 Mitsumi CD-ROM 驱动程序：本软件由 Holger Veit 和 Brian Moore 共同开发，用于“386BSD”和类似操作系统。“类似操作系统”主要包括供研究和教育之用的非营利性操作系统，包括但不限于“NetBSD”、“FreeBSD”和“Mach”（由 CMU 开发）。
本产品包含 Apache Group 为在 Apache HTTP 服务器项目（http://www.apache.org/）中使用而开发的软件。
本产品包含根据“GNU Library General Public License”，从 Richard H. Porter 处获得许可的软件（©1998，Red Hat Software）。“GNU Library General Public License”发布在 www.gnu.org/copyleft/lgpl.html 上。
本产品包含根据“Perl Artistic License”进行许可的 Perl 软件的标准版本（©1997，1998 Tom Christiansen and Nathan Torkington）。保留所有权利。您可以在网站 http://www.perl.com 上找到 Perl 软件的最新标准版本。
本产品包含 Jared Minch 开发的软件。

本产品包含 OpenSSL Project 为在 OpenSSL Toolkit（http://www.openssl.org/）中使用而开发的软件。
本产品包含 Eric Young（eay@cryptsoft.com）编写的加密软件。
本产品包含基于 oprofile 的软件，该软件受“GNU Public License”的保护。
本产品包含由 Tobi Oetiker（http://www.rrdtool.com/index.html）开发、根据“GNU General Public License”进行许可的软件。
本产品包含根据“GNU General Public License（GPL）”，从 Brian Gladman 博士处获得许可的软件。
本产品包含 Apache Software Foundation（http://www.apache.org/）开发的软件。
本产品包含 Hypersonic SQL。
本产品包含美国加利福尼亚大学董事会、Sun Microsystems, Inc.、Scriptics Corporation 和其它单位共同开发的软件。
本产品包含 Internet Software Consortium 开发的软件。
本产品包含 Nominum, Inc.（http://www.nominum.com）开发的软件。
本产品包含由 Broadcom Corporation 开发的软件，该软件受“GNU 公共许可证”的保护。

目录

1

本地流量管理简介

- 了解BIG-IP本地流量管理
- 本地流量管理配置概述
- 《本地流量管理配置指南》简介

了解BIG-IP本地流量管理

BIG-IP®本地流量管理（LTM）系统专为管理本地网络流量而设计。***本地流量管理***是指管理流入或流出局域网（LAN）的网络流量的过程，此处所说的LAN包括内联网。

本配置指南适用于全套本地流量管理产品，这些产品是BIG-IP®产品系列的一部分。

LTM系统的一个常用特性是它截听和重新引导流入的网络流量，以便对网络服务器的负载进行智能调节的功能。但是，调节服务器负载不是本地流量管理的唯一内容。LTM系统包括各种特性，可以执行的功能包括检测与转换标头和内容数据、管理基于SSL证书的认证、压缩HTTP响应等。这样一来，LTM系统不仅将流量引导至适当的服务器资源，而且增强了网络安全性，并通过执行通常由Web服务器执行的那些任务来释放服务器资源。

本地流量管理功能概述

如果配置得当，LTM系统能够执行各种流量管理功能，例如：

- 通过来调节和分配网络上的服务器负载，从而实现可扩展性。
- 卸载标准的服务器任务，例如 HTTP 数据压缩、SSL 认证和 SSL 加密，以提高服务器性能。
- 监视网络中服务器的状态和性能，以实现出色的可用性。
- 建立和管理会话及连接持续性。
- 根据用户名/密码和 SSL 证书的认证信息，执行应用流量的认证和授权功能。
- 管理数据包吞吐率，以优化特定连接类型的性能。
- 将多个客户机请求汇聚到服务器端的连接 Pool，以提高性能。汇聚客户机请求是 LTM 系统 OneConnect™特性的一部分。
- 应用配置设置来定制特定应用的流量（例如 HTTP 和 SSL 流量）。
- 根据用户基于业界标准的工具命令语言（Tcl）编写的脚本，定制对特定连接的管理。

此列表中的一些功能提供平衡网络服务器负载的基本功能，而列表中的其它功能则提供值得一提的专用功能。这些功能包括管理特定类型的应用流量、优化服务器性能和增强网络安全性。以下几节内容介绍了这些专用功能。

管理特定类型的应用流量

应用配置设置来定制特定应用的流量是本地流量管理的一个关键特性。LTM系统能够控制多种不同类型的流量，每种类型都对应一种不同的方法。这是通过为每种网络流量类型的管理制定一个政策来实现的。以下这些都是系统能够管理的流量类型的实例：TCP、UDP、HTTP、FTP、SSL、会话启动协议（SIP）、i-mode®和Microsoft®远程桌面协议（MSRDP）。

除了创建独立的政策来系统管理这些不同的流量类型之外，您还可以实现以下功能：

- 编写 iRules™，为各个应用分配特定行为（特定连接）。iRule 能够搜索特定流量类型（例如 HTTP 请求或响应）的内容，然后相应地引导流量。
- 将标头数据插入特定应用的请求（例如 HTTP 请求），然后根据该标头数据引导请求。
- 实施会话持续性。使用 LTM 系统功能强大的配置工具，您可以根据数据（例如 HTTP cookie、源 IP 地址、目的地 IP 地址和 SSL 会话 ID）来配置会话持续性。
- 监视 pool 中服务器的状态或性能。例如，LTM 系统能够监视网络上的小型目录访问协议（LDAP）服务器。如果系统确定目标 LDAP 服务器无法正常发挥作用，LTM 系统能够将请求重新引导至其它 LDAP 服务器。
- 使用动态比率负载平衡算法来评估特定服务器类型（例如 Windows 管理基础结构（WMI）服务器）上的当前负载，然后根据该评估重新引导请求。对与特定应用类型相应的服务器进行监视的功能是维护网络最佳性能的关键工具。

优化性能

LTM系统包括若干为优化服务器性能而设计的特性。这些特性或者卸载占用大量资源的流量管理任务（例如SSL证书验证），或者支持服务器端连接的建pool、复用和整体持续性。

卸载服务器任务

LTM系统能够卸载网络服务器中的以下这些任务：

- 基于 SSL 证书的认证，包括通过 OCSP 检查证书撤销状态；
- SSL 加密和解密；
- 使用远程 LDAP 服务器进行基于 SSL 证书的授权；
- HTTP 数据压缩；
- MSRDP 连接的重写。

优化TCP和HTTP连接

LTM系统以特定的方式来管理TCP和HTTP连接，以优化服务器性能。网络优化的主要特性包括：OneConnect™、HTTP流水线技术和速率调整。

OneConnect

OneConnect™特性包括以下几个部分：

◆ **内容转换**
HTTP客户机在单一连接中发送多个请求时，LTM系统能够分别处理其中的每个请求，根据需要将这些请求发送至不同的目的地服务器。此特性自动启用，无需配置。

◆ **连接Pool**
通过此特性，LTM系统将未使用的服务器端连接组合在一起，以便其它客户机能够使用。这显著降低了处理客户机请求所需的服务器数量。在缺省模式下，此特性是禁用的，但使用OneConnect Profile

可以轻松将其启用。

- **OneConnect转换**
  对于HTTP/1.0请求，有时可能希望为HTTP **Connection**标头添加**Keep-Alive**支持，以确保服务器端连接保持在打开状态。对HTTP **Connection**标头的这一操作称为OneConnect转换特性。此特性在与连接Pool一起使用时效果最佳。

有关OneConnect™的详细信息，请参阅第5章“了解Profile”和第6章“管理HTTP和FTP流量”。

HTTP流水线技术

除了OneConnect™特性，LTM系统还能够处理流程化的请求。这表示，即使前一个请求尚未收到响应，LTM系统也能处理下一个客户机请求。流水线技术是仅适用于HTTP/1.1请求的优化特性。有关HTTP流水线技术的详细信息，请参阅第6章“管理HTTP和FTP流量”。

速率调整

速率调整 这一特性允许您将特定连接类型按照速率级别进行分类，以便定制这些连接的吞吐率。举例来说，希望为首选互联网客户优化Web服务器性能时，该特性便非常有用。

TCP优化

LTM系统带有效果显著的TCP优化功能，例如依次交付和内容缓冲。

增强网络安全性

管理本地网络流量时，安全性是一个重要的考虑因素。LTM系统相应地包含了众多特性，用于帮助预防安全隐患。这些特性不仅涉及对用户和应用的认证与授权，还涉及检测入侵与缓和DOS攻击。

一般说来，当LTM系统检测到安全问题时，它可以采取类似以下这些的行动：

- 根据 SSL 证书的验证结果拒绝客户机请求；
- 拒绝并抛弃未经授权的数据包；
- 向系统管理员发出关于攻击或入侵企图的警告；
- 将可疑的流量引导至特定目标服务器；
- 记录认证故障；
- 阻止 SYN 泛滥攻击

对于任何联网环境而言，一个重要的考虑因素是用来对用户及其客户机请求进行认证，同时用来控制用户和应用对服务器资源的访问的认证和授权机制。为此，LTM系统支持可插拔认证模块（PAM）技术，并提供一组完整的PAM认证模块，您可以从中进行选择，以满足自己认证或授权的需要。LTM系统提供的认证模块如下：

- **LDAP 模块**

使用远程LDAP服务器来执行用户名/密码的用户认证。

- **RADIUS 模块**
  使用远程拨入用户服务（RADIUS）服务器来执行用户名/密码的用户认证。
- **TACACS+模块**
  使用远程终端访问控制器访问控制系统（TACACS+）服务器来执行用户名/密码的用户认证。
- **SSL 客户机证书 LDAP 模块**
  使用远程LDAP服务器执行基于SSL证书的客户机SSL流量授权。
- **OCSP 模块**
  使用远程在线证书状态协议（OCSP）服务器提供最新的SSL证书撤销状态，以便对客户机和服务器的SSL流量进行认证。

本地流量管理配置概述

在设置好基础网络、并拥有对LTM系统的管理访问权限、以及为每个接口至少分配一个缺省VLAN之后，下一步就是配置网络，管理以内部服务器为目标的流量。

LTM系统的核心部分是Real Server与负载平衡Pool。Real Server接收入站流量、执行源IP地址与目的地IP地址的基本转换，并将流量引导至以编组形式位于负载平衡Pool中的服务器。

要配置基本的本地流量管理系统，请使用Configuration工具。通过该工具可以创建一整套配置对象，这些对象共同执行本地流量管理任务。每个对象都有一组配置设置，这些设置可以按原样使用，也可以根据需要进行修改。这些对象包括：

- **Real Server**
  Real Server接收请求，然后分发给Pool成员。
- **负载平衡 Pool**
  负载平衡Pool包含可以将请求发送到其中进行处理的服务器。
- **节点**
  节点代表网络上的服务器IP地址，您可以启用和禁用节点，还可以获得节点状态。
- **Profile**
  Profile包含定义各种流量类型的行为的设置。
- **Monitor**
  Monitor跟踪Pool成员的当前状态或者性能。
- **iRule**
  iRule可以定义Pool成员的选择标准，还可以执行内容转换、记录、定制协议支持等。
- **速率调整**
  速率调整控制带宽的使用。
- **SSL 证书**
  SSL证书对象允许您生成SSL证书请求以及在LTM系统上安装SSL证书，以便终止和启动SSL连接。
- **SNAT**
  安全网络地址转换（SNAT）负责转换客户机请求中的源IP地址，从而允许多台主机共享同一个地址。

- **统计数据**
  统计数据显示与各种连接类型相关的指标。

创建配置对象时，您可以选择执行基本配置还是执行高级配置：

- **基本配置**
  希望主要使用对象设置的缺省值时，请选择***基本配置***。选择基本配置时，Configuration工具仅显示那些最有可能需要修改的少数设置。其它设置保持隐藏状态，并保留各自的缺省值。选择基本配置是一种轻松创建配置对象的方式。
- **高级配置**
  希望修改对象设置的多个值时，请选择***高级配置***。选择高级配置时，Configuration工具对象的所有设置允许您任意修改。

在LTM系统中，您必须针对本地流量管理进行配置的三个最重要的对象是：

- Real Server
- 负载平衡 Pool
- Profile

配置Real Server

创建Real Server时，请指定所需Real Server的类型（主机Real Server或者网络Real Server）。然后，您可以为该Real Server附加各种属性和资源，例如特定应用的Profile、会话持续性和用户编写的脚本，这些脚本调用定义pool选择标准的iRule。与Real Server关联之后，所有这些属性和资源共同确定了LTM系统管理本地流量的方式。
创建和配置Real Server时，需要使用第1-8页图1.1中的部分Configuration工具屏幕。

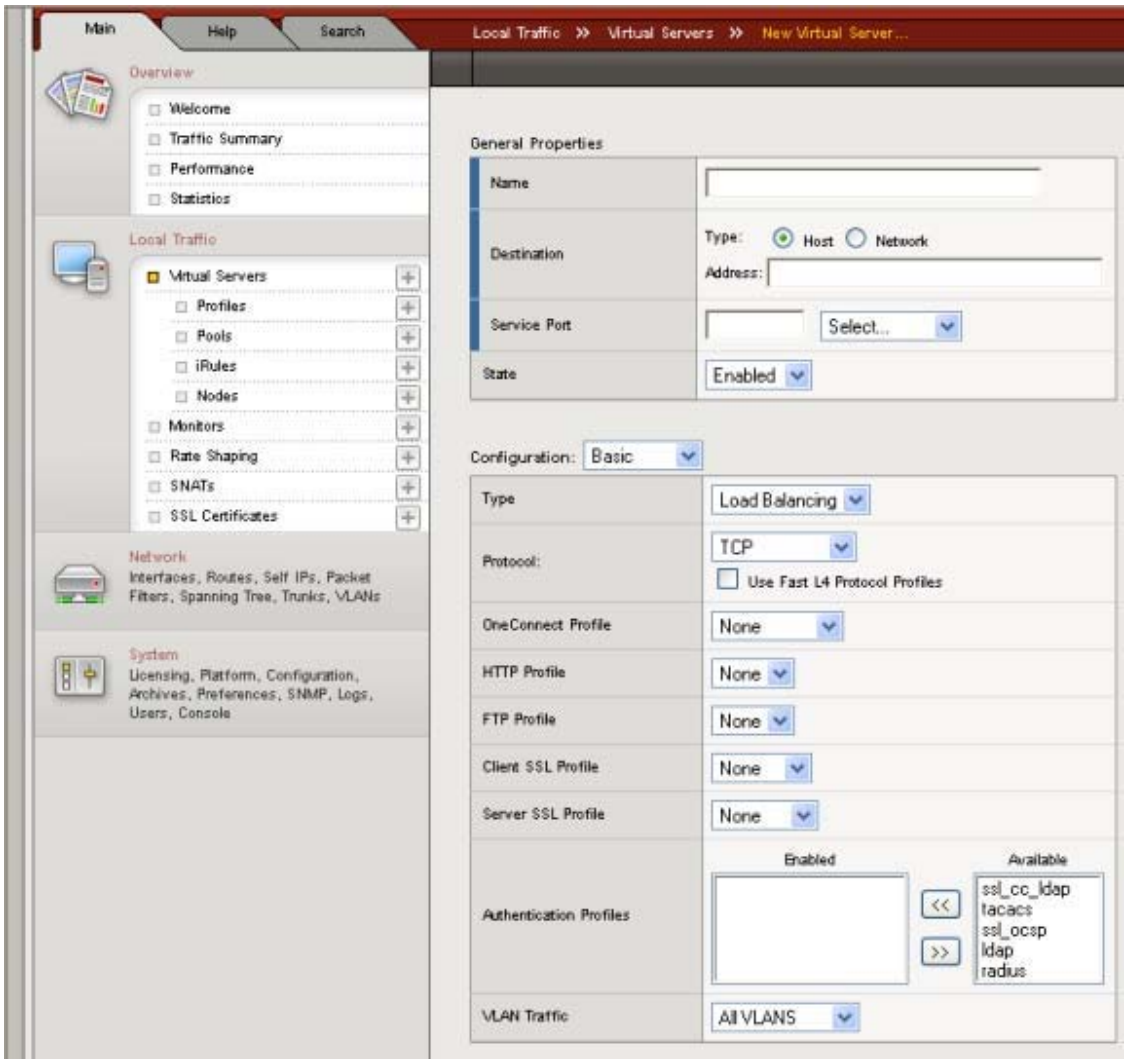

图1.1 *创建Real Server的Configuration工具屏幕*

有关Real Server的详细信息，请参阅第2章“配置Real Server”。

配置负载平衡Pool

*负载平衡Pool*是一些内部服务器的集合，这些服务器为了处理客户机请求而编组在一起。pool中的服务器称为***Pool成员***。LTM系统使用称为“轮循”的缺省负载平衡算法，将客户机请求发送至Pool成员。

每个pool都必须与一台Real Server关联。Real Server将客户机请求发送至与自己关联的一个或多个pool。第1-8页上的图1.1中显示的Real Server包括用于指定pool名的设置：**缺省pool**。

pool具有与自己相关的设置，例如Pool成员的IP地址、负载平衡模式以及状态与性能Monitor。创建pool时，可以针对这些设置中的一些使用缺省值，也可以更改这些缺省值，以更好地满足您的需要。

创建和配置负载平衡Pool时，您将使用Configuration工具的“pool”屏幕。图1.2显示了该屏幕的一部分。

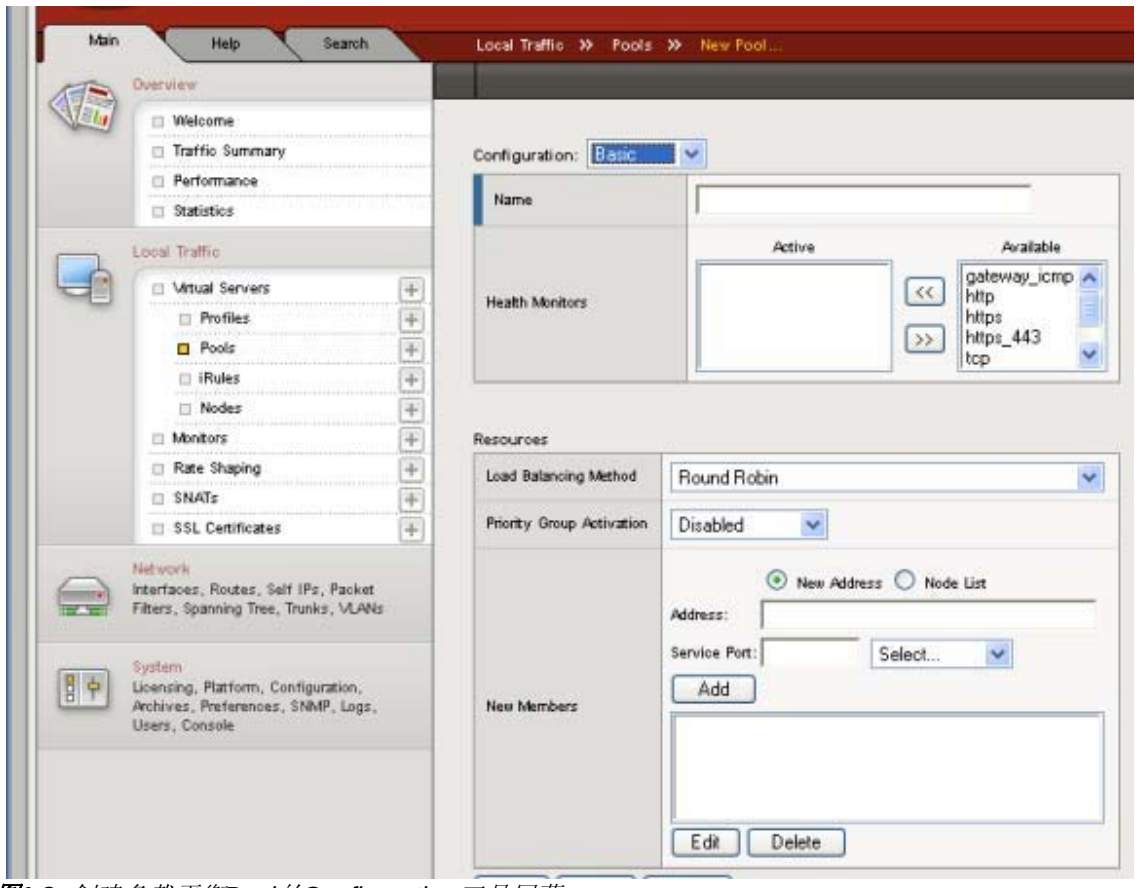

图1.2 *创建负载平衡Pool的Configuration工具屏幕*

有关负载平衡Pool的详细信息，请参阅第4章“配置负载平衡Pool”。

配置Profile

Profile是应用于特定网络流量类型（例如HTTP连接）的一组配置设置。如果希望Real Server管理某种类型的流量，可以将相关适用的Profile与Real Server进行关联，随后Real Server便会将该Profile的设置应用到该类型的所有流量。

例如，您可能希望LTM系统压缩HTTP响应数据。在此情形中，您可以将一个HTTP Profile配置成启用压缩，然后将该Profile与Real Server关联。这样，Real Server处理HTTP请求时，LTM系统将压缩响应。您可以根据自己的需要创建若干种类型的Profile。其中包括：FastL4、TCP、UDP、OneConnect、流、HTTP、FTP、客户机SSL、服务器SSL、持续性和认证。创建Profile时，可以使用设置的缺省值，也可以更改这些缺省值，以更好地满足您的需要。

例如，创建和配置HTTP Profile时，您将使用显示在第1-11页的图1.3中的部分Configuration工具屏幕。

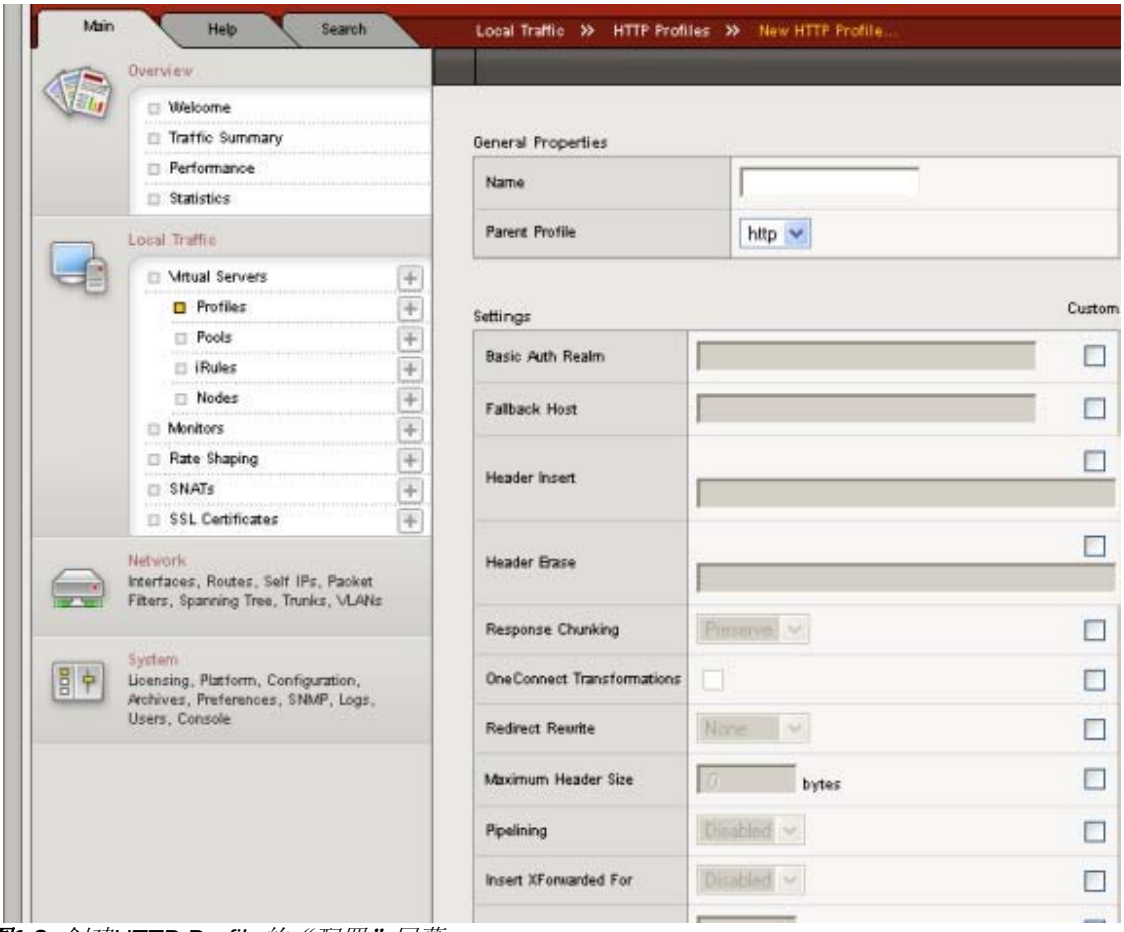

***图1.3** 创建HTTP Profile的“配置”屏幕*

有关对Profile进行配置的详细信息，请参阅第5章“了解Profile”和以下各章节：

第6章“管理HTTP和FTP流量”
第7章“管理SSL流量”
第8章“认证应用流量”
第9章“启用会话持续性”

《本地流量管理配置指南》简介

本指南介绍了配置BIG-IP本地流量管理系统，以便对本地通信网络的入站流量和出站流量进行管理的方法。您必须安装BIG-IP系统、对系统进行授权激活、使用“设置”工具执行管理网络配置，然后才能配置本指南中描述的特性。有关这些任务的信息，请参阅**《平台指南：1500、3400和6400》**与**《BIG-IP系统的安装、授权激活与升级》**指南。

使用Configuration工具

首次使用时，所有用户都需要使用基于Web的Configuration工具对系统进行授权激活。

除了设置管理网络和流量管理软件的初始配置，Configuration工具还用于配置和监视LTM系统。使用Configuration工具可以执行您的配置所需的其它配置步骤。在Configuration工具中，您还可以监视当前系统性能。本指南中的大部分操作过程都使用Configuration工具。

Configuration工具支持7.1版的Netscape® Navigator™或建立在同一引擎基础上的其它浏览器（例如Mozilla™、Firefox™和Camino™）；同时还支持6.x版或更高版本的Microsoft® Internet Explorer™。

其它信息

除了本指南，您还可以参考其它一些文档资源来使用BIG-IP系统。以下介绍的指南和文档中提供了相关信息。BIG-IP系统附带了以下印刷文档。

- **配置工作表**
  此工作表供您规划BIG-IP系统的基本配置之用。
- **BIG-IP快速入门指南**
  此手册介绍了顺利启动BIG-IP系统并在网络中运行所需的基本配置步骤。

BIG-IP系统附带的光盘上也提供了这些PDF格式的指南；登录BIG-IP系统的管理Web服务器时看到的第一个网页上也有这些指南。

- **平台指南**
  此指南包含有关BIG-IP系统的信息，以及重要的环境警告。
- **BIG-IP系统的安装、授权激活与升级**
  此指南提供有关为BIG-IP系统安装升级的详细信息，以及有关对BIG-IP系统软件进行授权激活和将系统连接到管理工作站或网络的信息。

格式规则

为帮助轻松地为辨别和了解重要信息，我们的文档使用下述格式规则。

使用解决方案实例

本文档中的所有实例均仅使用无法路由的IP地址。设置我们介绍的解决方案时，必须使用适合您的网络的IP地址来代替我们的实例地址。

辨别新术语

为帮助辨别定义术语的地方，术语以粗斜体显示。例如：Real Server是虚拟地址与虚拟端口的特定组合，与由BIG-IP系统或由其它类型的主机服务器管理的内容站点相关联。

辨别对对象、名称和命令的引用

为帮助轻松地将某些条目从一段文字中挑出，对它们应用了粗体。这些条目包括Web地址、IP地址、工具名称和命令的一部分（例如变量和关键字）。例如：您可以将**Idle Time**值设置为5。

辨别对其它文档的参考

我们使用特殊形式来标注对其它文档的参考。如果参考中同时提供书名和该书的特定章节名，那么书名以粗体形式包含在中文书名号中，章/节名以常规形式包含在中文引号中，以帮助对这两者进行快速区分。例如：有关安装说明，请参阅《BIG-IP系统的安装、授权激活与升级》指南中的第1章“安装软件”。

查找其它帮助和技术支持资源

在以下位置可以找到有关本产品的其它技术信息：

- **发行说明**
  针对本产品最新版本的发行说明可从产品Web服务器的首页上获得，技术支持网站上也提供了该发行说明。发行说明中包含针对当前版本的最新信息，包括最新特性和增强特性的列表以及漏洞修复列表，在某些情形中还包括已知问题列表。
- **在线帮助**
  您可以在三个不同位置找到在线帮助：
  - 产品上的Web服务器在软件光盘中包含了PDF版本的指南。
  - 基于Web的Configuration工具为每个屏幕都提供了在线帮助。仅需点击“帮助”菜单便可调出在线帮助。
- **“Ask F5”技术支持网站**
  F5 Networks技术支持网站（**http://tech.f5.com**）提供产品的最新文档，包括技术说明、常见问题解答、PDF格式的指南更新以及“ASK F5”自然语言问答引擎。要访问此站点，需在**http://tech.f5.com**注册。
- **F5解决方案中心**
  F5解决方案中心包含经过证明的互操作性与集成解决方案，它们帮助组织在不可预测的网络环境中交付安全、可预测的应用。F5解决方案中心提供了详尽的资料文档，这些文档将向您演示如何通过出色的可靠性、安全性和性能来提高在应用和网络基础设施方面的投资回报（ROI）。如要访问此站点，请登录**http://www.f5.com/solutions**。

◆ 注

本指南中提及的硬件平台均特指F5 Networks公司提供的系统。如果您的硬件是由其它厂商提供的，那么遇到硬件相关的问题时，请参考该厂商提供的文档。

2

配置 Real Server

- Real Server介绍
- 了解Real Server的类型
- 创建和修改Real Server
- 配置Real Server和虚拟地址设置
- 管理Real Server和虚拟地址

Real Server介绍

Real Server是BIG-IP®本地流量管理（LTM）配置中最重要的组件。***Real Server***收到客户机请求后，不是直接将请求发送到数据包标头中指定的目的地IP地址，而是发送到组成负载平衡Pool的内容服务器上。Real Server可提高用于处理客户机请求的资源的可用性。

根据您的流量管理需要，Real Server不仅可以对多台服务器分配流量，还可以分别处理各种不同类型的流量。例如，Real Server可以在HTTP请求数据通过LTM系统时对其进行压缩，或者解密和重新加密SSL连接以及验证SSL证书。对于每种类型的流量，如TCP、UDP、HTTP、SSL和FTP，Real Server都可以应用一整套设置来影响LTM系统管理该类流量的方式。

Real Server同样也支持多种不同流量类型的持续会话。借助Real Server，您可以为HTTP、SSL、SIP和MSRDP等连接建立持续的会话。

最后，Real Server还可以应用iRule，这是一个用户编写的脚本，旨在通过专门的方法来检查和引导单独的连接。例如，您可以创建iRule用来在某个TCP连接的内容中查找一个特定的字符串，并且如果找到该字符串，您还可以引导Real Server将此连接发送至具体的pool或pool的成员。

总之，Real Server能够：

- 在多台服务器中分配客户机请求，以便平衡服务器负载；
- 针对多种流量类型实施不同的设置；
- 支持多种流量类型的持续性；
- 根据用户编写的iRule™引导流量。

您可以采用以下3种截然不同的方法来使用Real Server：

- **将流量引导至负载平衡Pool**
  负载平衡Real Server是一种最基本的Real Server，负责将客户机流量引导至负载平衡Pool。在您第一次创建这种Real Server时，您可以为其分配一个现有的缺省pool。之后，这种Real Server就可以自动地将流量引导至该缺省pool。
- **将流量转发至特定的目的地IP地址**
  转换型Real Server 和其它Real Server一样，但是没有用于负载平衡的Pool成员。这种Real Server能够直接将数据包转发至客户机请求中具体指定的目的地IP地址。在您使用转换型Real Server将请求引导至其最初指定的目的地IP地址时，LTM系统可以像使用其它Real Server一样，来添加、跟踪和获取这些连接。您还可以查看转换型Real Server的统计数据。
- **二级转换**
  您可以设置一台转换型Real Server来与相关的虚拟局域网（VLAN）中的某个节点共享相同的IP地址。为此，您必须进行一些额外的配置工作。这些工作包括：创建一个VLAN组，其中包含驻留该节点的虚拟局域网（VLAN）；为这个VLAN组分配Self-IP地址，并禁用相应VLAN上的Real Server。

在创建Real Server时，您可以为源自该Real Server的任何流量指定一个或多个作为目的地的pool。您还可以为其配置常规属性、一些配置选项以及其它您希望分配的资源，例如iRule或会话持续性类型。

下面描述的是您可以创建的Real Server的类型，以及他们的常规属性、配置选项和资源。

了解Real Server的类型

您可以创建2种截然不同的Real Server：主机Real Server和网络Real Server。

主机Real Server

主机Real Server代表一个具体的站点，比如一个互联网站点或一个FTP站点，它可以负载平衡以内容服务器（并属于Pool成员）为目的地的流量。您分配给主机Real Server的IP地址应该与DNS与站点域名相对应的IP地址相匹配。在LTM系统收到指向该站点的连接请求时，LTM系统将识别客户机的目的地IP地址是否匹配Real Server的IP地址，并随后将客户机请求转发至Real Server负载平衡范围内的内容服务器。

网络Real Server

网络Real Server是指IP地址的主机部分中没有位元（bits set）的Real Server，即其IP地址的主机部分为**0**。网络Real Server有两种类型：根据一系列目的地IP地址引导客户机流量的服务器，以及根据LTM系统不能识别的具体目的地IP地址引导客户机流量的服务器。

引导指向一系列目的地IP地址的流量

借助主机位为**0**的IP地址，Real Server可以引导指向所有IP地址，而不是单个目的地IP地址的客户机连接（就像主机Real Server一样）。这样，当任何客户机连接以Real ServerIP地址在网络中指定的目的地IP地址为目标时，LTM系统就可以将该连接引导至一个或多个与网络Real Server相连的pool。

例如，这种Real Server可以将指向**192.168.1.0**网络上任意节点的客户机流量引导至一个具体的负载平衡Pool，比如**入站防火墙**。或者，该Real Server还可以将指向子网**192.168.1.0/24**内任意地址的web连接引导至pool **default_webservers**。

引导指向透明设备的流量（通配符Real Server）

除了引导指向特定网络或子网的客户机连接之外，网络Real Server还可以引导拥有Real Server无法识别的特定目的地IP地址的客户机连接，比如透明设备。这样的网络Real Server就称为通配符Real Server。
通配符Real Server是设计用于管理指向透明网络设备的网络流量的一种特殊网络Real Server。这里的透明设备包括防火墙、路由器、代理服务器以及高速缓存服务器。通配符Real Server主要管理拥有LTM系统不能识别的目的地IP地址的网络流量。

处理不能识别的客户机IP地址

主机类Real Server通常负责管理通往特定站点的流量。当LTM系统收到指向该站点的连接请求时，LTM系统会识别客户机的目的地IP地址是否匹配Real Server的IP地址，并随后将客户机转接至Real Server可以负载平衡的内容服务器。

但是，在对透明节点进行负载平衡时，LTM系统也许不能识别客户机的目的地IP地址。客户机可能正与防火墙、路由器或代理服务器的另一侧上的IP地址相连。在这种情况下，LTM系统不能将客户机的目的地IP地址与Real Server的IP地址进行匹配。

通配符网络Real Server解决了这一难题，那就是不在LTM系统的Real Server层上转换入站IP地址。例如，在LTM系统没有为客户机的目的地IP地址找到可以匹配的特定Real Server时，LTM系统就会将客户机的目的地IP地址匹配到一个通配符Real Server，并指定一个具体为**0.0.0.0**的IP地址。 LTM系统然后将客户机的数据包转发到通配符Real Server可负载平衡的一个防火墙或路由器，这个防火墙或路由器再反过来将客户机的数据包转发到实际的目的地IP地址。

了解缺省端口和指定端口的通配符服务器

您可以创建两种通配符Real Server：

- **缺省的通配符Real Server**
  缺省的通配符Real Server 是一个使用端口**0**并可处理面向所有服务的流量的通配符Real Server。缺省情况下通配符Real Server能支持所有的VLAN。但是，您也可以禁用一些您不希望让缺省通配符Real Server支持的VLAN。禁用缺省通配符Real Server所支持的VLAN可以通过创建VLAN禁用列表来完成。注意VLAN禁用列表仅适用于缺省通配符Real Server。您不能为仅与一个VLAN相连的通配符Real Server创建VLAN禁用列表。关于创建缺省通配符服务器的步骤，请参见2-7页“创建通配符Real Server”。
- **指定端口的通配符Real Server**
  指定端口的通配符Real Server 处理的是仅面向特定服务的流量，您可以使用一个服务名称或端口号来对其进行定义。您可以使用指定端口的通配符Real Server来跟踪特定类型网络流量的统计数据，或者使用它避开防火墙或路由器直接路由输出流量（如HTTP流量）至高速缓存服务器。对于创建指定端口的通配符Real Server的步骤，请参见2-8页“创建指定端口的通配符Real Server”。

如果您同时使用缺省的通配符Real Server和指定端口的通配符Real Server，则那些既不匹配标准Real Server又不匹配任何一个指定端口的通配符Real Server的任何流量，都将由缺省通配符Real Server进行处理。

我们建议您在定义需要处理多种服务的透明节点（如防火墙或路由器）时，最好为节点指定一个实际端口并关闭Real Server的端口转换。

创建多台通配符服务器

您可以定义同步运行的多个通配符Real Server。每个通配符Real Server必须指定一个单独的VLAN，以便它能够专门处理该VLAN的数据包。

在某些配置中，您需要在LTM系统的一侧安装一台通配符Real Server，以负载平衡跨透明设备的连接。您可以在LTM系统的另一侧创建另一台通配符Real Server，用于将数据包转发至接收来自透明设备的连接并将其转发至其目的地的Real Server。

创建并修改Real Server

利用Configuration工具，您可以创建Real Server，或者修改现有Real Server的设置。以下章节将介绍创建和修改Real Server的步骤。如欲了解具体的Real Server属性和设置，请参见2-10页“配置Real Server和虚拟地址设置”。关于如何查看现有Real Server配置的信息，请参见2-14页“管理Real Server和虚拟地址”。

创建Real Server

在创建Real Server的时候，既可以创建主机或网络Real Server，也可以创建称做通配符Real Server的特殊网络Real Server。

创建主机或网络Real Server

在创建主机Real Server和网络Real Server时，可以使用相同的步骤。以下步骤可以帮助您创建出全部采用缺省设置的最基本的主机或网络Real Server。完成这些步骤之后，您就将拥有一个可使用缺省设置将流量引导至负载平衡Pool的负载平衡Real Server。

在多数情况下，创建基本的Real Server就能够满足负载平衡或者转发的需要。在创建基本的Real Server时，为简化创建过程，绝大多数的设置都已被隐藏。如果您希望调整基本设置之外的其它设置，您可以查看和配置更高级的设置。有关配置具体设置的信息，请参见2-10页“配置Real Server和Real Server地址设置”，或者参阅在线帮助。

创建主机或网络Real Server的步骤

1. 在Main选项卡上，展开**Local Traffic**。
2. 点击**Real Server**。
   出现“Real Server”屏幕。
3. 在屏幕的右上方，点击Create按钮。
   出现“New Real Server”屏幕。
4. 配置所有必需的设置。
   如果您创建的是网络Real Server，您必须将IP地址的主机位设置为**0**。
5. 保留或改变任何可选设置的值。
6. 点击**Finished**。

◆ **注**

如果Real Server与相连VLAN中某节点的IP地址相同，那您就须进行一些额外的配置。这些配置包括：创建VLAN组，其中包含驻留该节点的VLAN；为VLAN组分配Self-IP地址；以及禁用相连VLAN上的Real Server。如欲了解更多信息，请参见关于VLAN的在线帮助。

创建通配符Real Server

通配符Real Server是一种特殊的网络Real Server。创建通配符Real Server需要完成三项工作：

- 首先，您必须创建一个含有透明设备的地址的pool。
- 其次，您必须创建通配符Real Server（缺省或指定端口）。
- 最后，您必须禁用每个Real Server的端口转换功能。端口转换功能缺省为禁用。

以下步骤讲述的就是如何使用Configuration工具来完成这些工作。

创建透明设备pool的步骤

要创建透明设备pool，应打开pool屏幕并点击**Create**按钮。如欲了解更多信息，请参见第4章“配置负载平衡Pool”。

创建缺省通配符Real Server的步骤

1. 在Main选项卡上，展开**Local Traffic**。
2. 点击**Real Servers**。
   出现**Real Servers**屏幕。
3. 在屏幕的右上方，点击**Create**按钮。
   出现New Real Server屏幕。
4. 配置所有必需的设置。
   记住在**Destination Address**框中输入IP地址“**0.0.0.0**”，如果您选择了网络类型的Real Server，则请在**Mask**会话框中输入网络掩码“**0.0.0.0**”。
5. 点击Finished。

创建指定端口的通配符Real Server的步骤

1. 在Main选项卡上，展开**Local Traffic**。
2. 点击**Real Servers**。
   出现Real Servers屏幕。
3. 在屏幕的右上方，点击**Create**。
   出现New Real Server屏幕。
4. 在**Address**框中，输入通配符IP地址**0.0.0.0**。
5. 对于**Service Port**设置，请输入端口号，或者从列表中选择一个服务名称。注意端口**0**定义的通配符Real Server能够处理所有的服务类型。如果您指定一个端口号，您就可创建一个指定端口的通配符Real Server。通配符Real Server处理仅指定端口的流量。
6. 对于Resources部分中的**Default Pool**设置，请选择您希望应用该Real Server的透明设备pool。
7. 点击**Finished**。

关闭通配符Real Server的端口转换功能

在定义好一个带有通配符端口的Real Server之后，您应该验证一下是否已禁用该Real Server的端口转换功能。

1. 在Main选项卡上，展开**Local Traffic**。
2. 点击**Real Servers**。
   出现Real Servers屏幕。
3. 在Name栏中，点击您想关闭端口转换功能的Real Server。
   出现Real Servers屏幕。
4. 在Enable Transformation中，验证**Port**框是否已清空。

修改Real Server

您可以使用Configuration工具，轻松地修改现有Real Server的设置。如欲了解关于虚拟设置的信息，请参见2-10页“配置Real Server和Real Server地址设置”，或者参阅在线帮助。

修改现有Real Server的步骤

1. 在Main选项卡上，展开**Local Traffic**。
2. 点击**Real Servers**。
   出现Real Servers屏幕。
3. 在Name栏内，点击您想修改的Real Server的名称。
   出现该Real Server的属性屏幕。
4. 在Configuration列表中，选择**Advanced**。
5. 在Configuration部分，保存或修改任一Real Server设置。
6. 点击**Update**。
7. 在菜单栏上，点击Resource。
   屏幕显示所选Real Server的其它设置。

8. 在Load Balancing部分，保存或修改任一Real Server资源。
9. 点击**Update**。
10. 如果您想修改分配给Real Server的iRule，请点击**Manage**按钮，然后使用左或右箭头（**<<或>>**）来激活或禁用任何现有的iRule。
11. 点击**Finished**。

配置Real Server和虚拟地址设置

Real Server及其Real Server地址都有许多属性和设置，您可以对它们进行配置来改变Real Server管理流量的方式。您也可以为Real Server分配一定的资源，比如负载平衡Pool和持续性Profile。这些属性、设置和资源共同组成了Real Server或其地址的定义，并且它们在绝大多数情况下均为缺省值。在创建Real Server时，您既可以保留缺省值，又可以对它们进行修改以适应您的具体需要。

以下内容将列出并描述定义Real Server和虚拟地址的所有属性、配置设置和资源。有关创建Real Server的详细信息，请参见2－6页“创建主机或网络Real Server”。

配置Real Server的属性、设置和资源

在Configuration程序中，Real Server设置被分为三个类别：常规属性、配置设置（基本和高级）和资源（基本和高级）下面我们分别讨论这三个类别所包含的设置。

常规属性

在创建Real Server的时候，可以定义一些常规属性。表2.1列出并描述了这些常规属性。

属性	描述	缺省值
Name	您分配给Real Server的一个独有的名称。	无缺省值
Destination Type	您想创建的Real Server及其IP地址的类型。如果您选择的类型为**network**，那么该属性还包括用于该IP地址的掩码。如欲了解有关Real Server类型的更多信息，请参见2－3页“了解Real Server的类型”。该属性是必需属性。	**Host**
Destination Address	Real Server的IP地址。	无缺省值
Destination Mask	网络Real Server的网络掩码。该属性仅适用于网络Real Server，并且是必需属性。网络掩码说明主机位实际为零还是为通配符。	无缺省值
Service Port	您希望用来引导流量的服务名称或端口编号。该属性为必需属性。	无缺省值
State	Real Server的状态包括：**Enabled**或**Disabled**。作为一个选项，您可以启用或禁用Real Server与指定虚拟局域网（VLAN）的连接状态。请注意当Real Server处于禁用状态时，它将无法再接收新的连接请求。不过，它会在当前的连接完成处理之后，才进入**Down**状态。 **注意：**如果没有指定具体的虚拟局域网，那么**Enabled**	**Enabled**

	或**Disabled**设置将适用于所有虚拟局域网。	

表2.1 *Real Server的常规属性*

配置设置

在创建Real Server的时候，您可以配置多项设置。表2.2列出并描述了这些Real Server配置设置。由于所有这些设置均有缺省值，因此没有必要对其进行改动。

设置	说明	缺省值
Type	Real Server 配置的类型。选项有：**Load Balancing**、**IP Forwarding** 和 **L2 Forwarding**。	**Load Balancing**
Protocol	您希望用来引导流量的服务名称或端口编号。示范的协议名称为TCP和UDP其对应的编号分别为**6**和**17**。您还可以启用**Use Fast L4 Protocol Profiles**选项。该选项可适用于转换型Real Server或非转换型Real Server。 该特性的一大优势在于，您可以在几个虚拟专用网（VPN）之间负载平衡虚拟专用网客户端连接，避免出现单点故障的可能性。该特性通常用于借助非转换型 Real Server，在 IPSEC VPN 夹层中对多个虚拟专用网（VPN）网关进行的负载平衡。 需要着重说明的是尽管此类协议的地址转换是可以选择的，但是有些协议比如 AH 模式下的 IPSEC，就需要 IP 标头保持原样。在这种情况下，您应当使用非转换网络 Real Server。	**TCP 和 6**
Client Protocol Profile	指定被选中的 Profile 作为客户端 Profile 的设置。仅适用于 TCP 和 UDP 连接。	**TCP**
Server Protocol Profile	指定被选中的 Profile 作为服务器端 Profile 的设置。仅适用于 TCP 和 UDP 连接。	**（使用 Client Profile）**
HTTP Profile	管理 HTTP 流量的现有 HTTP Profile 的名称。	**None**
FTP Profile	管理 FTP 流量的现有 FTP Profile 的名称。	**None**
Client SSL Profile	管理客户端 SSL 流量的现有 SSL Profile 的名称。	**None**
Server SSL Profile	管理服务器端 SSL 流量的现有 SSL Profile 的名称。	**None**
Authentication Profile	管理认证机制的现有Authentication Profile的名称。比如远程LDAP或RADIUS服务器。	**None**
Stream Profile	管理实时流协议（RTSP）流量的现有 Stream Profile 的名称。	**None**
VIAN Traffic	Real Server 启用或禁用的虚拟局域网的名称。	**All VLANS**
Rate Class	现有速率等级的名称，用于强化关于入站网络流量的	**None**

	吞吐率政策。	
Connection Limit	Real Server 允许的最大同步连接数目。将此设置为 **0** 即可关闭连接限制。	**0**
Address Translation	启用或禁用 LTM 系统地址转换的设置。LTM 系统在负载平衡含有相同 IP 地址的设备时，该选项特别有用。它通常还带有 nPath 路由配置，在该配置中几台服务器的回路设备上配置了相同的 IP 地址。	**Enabled**
Port Translation	启用或禁用 LTM 系统端口转换的设置。如果您希望使用 Real Server 负载平衡通向任何服务的连接，您最好关闭端口转换。	**Enabled**
SANT pool	现有 SANT pool 的名称，用于实施有选择性的智能 SNAT。	**None**
Clone pool (Client)	该特性使 Real Server 复制所有流量发送到指定克隆 pool 部分。该特性用于侵扰检测。	**None**
Clone pool (Server)	可复制 Real Server 为多个具体克隆 pool，所有流量都可发往一个 pool 的特性。该特性用于入侵检测。	**None**
Last Hop pool	使用上一中继 pool 引导返回流量至上一中继路由器的设置。它将使 **auto_lasthop** 设置无效。如果您有多个向 LTM 系统发送连接的路由器，连接将通过接收连接的同一路由器自动返回，前提是 **auto_lasthop** 全部变量必须被启用（缺省状态）。如果您想从 **auto_lasthop** 剔除一个或多个路由器，或出于某种原因全部 **auto_lasthop** 被禁用（比如您不想将其用于 SSL 网关），您可使用上一中继 pool 代替。（如果 **auto_lasthop** 被启用，上一中继 pool 优先。） 在配置上一中继 pool 之前，您必须首先创建一个包含路由器内部地址的 pool。	**None**

***表 2.2** Real Server 配置设置*

资源

如果您已创建一个负载平衡 Real Server，就必须为其分配一个缺省的负载平衡 Pool。如果计划使用 iRule 来引导某些类型的流量，您还必须为 Real Server 和其它在 iRule 中被指定的 pool 分配 iRule。这些 pool 和 iRule 的分配就称作***资源***。

表 2.3 列出并描述了您可以为负载 Real Server 分配的具体资源。

资源	说明	缺省值
Default Pool	您希望 Real Server 将其用做缺省 pool 的 pool 的名称。负载平衡 Real Server 将自动向这个 pool 发送流量，除非有 iRule 来引导服务器将流量发送到另一 pool。	无缺省值
Default Persistence Profile	您希望 LTM 系统使用的暂留类型。	**None**
Fallback Persistence Profile	LTM 系统在不能使用指定缺省暂留时，它所应当使用的暂留类型。	**None**

Rule	您希望 Real Server 在负载平衡其连接时所使用的 iRule 列表。注意您必须在 Real Server 上为所有选中的 iRule 配置相应的 Profile。比如：如果您指定一个含 HTTP 指令的 iRule，您必须在 Real Server 上配置一个缺省的或自定义 HTTP Profile。同理，如果您实施一个认证 iRule，您必须配置缺省的或自定义认证 Profile。	无缺省值

表 2.3 *分配到负载平衡 Real Server 的资源*

配置虚拟地址属性和设置

Configuration 程序可显示虚拟地址属性和设置。表 2.4 列出并描述了虚拟地址的常规属性和配置设置。

属性	说明	缺省值
Address	Real Server 的 IP 地址，不包括服务。	无缺省值状态
State	虚拟地址的状态包括：**启用**或**禁用**。	**Enabled**
Conection Limit	LTM 系统允许在虚拟地址上的最大同步连接数目。	**0**
ARP	启用或禁用 ARP 请求的配置。	**Enabled**

表 2.4 *虚拟地址的常规属性和配置设置*

管理Real Server和虚拟地址

在对 Real Server 和虚拟地址进行常规管理时，您通常需要查看现有 Real Server 配置或虚拟地址配置。有时还可能需要删除 Real Server。

对于已创建的 Real Server，您可以：

- 查看Real Server配置
- 查看虚拟地址配置
- 删除Real Server

查看Real Server配置

有时您可能需要确定应该调整 Real Server 设置，还是创建新的 Real Server。在查看 Real Server 配置时，您可以查看：

- Real Server列表
- Real Server属性和设置
- Real Server资源
- Real Server统计信息

查看 Real Server 列表

您可以查看一列已经创建的 Real Server。当打开 Real Server 列表时，Configuration 程序会显示以下相关信息：

- 状态
- Real Server名称
- 目的地（虚拟地址）
- 服务端口
- 协议
- 资源类型（负载平衡、转发或二级转换）

查看 Real Server 列表的步骤

1. 在Main选项卡上，展开**Local Traffic**。
2. 点击**Real Servers**。
   屏幕将出现一张包含所有现有 Real Servers 的列表。

查看 Real Server 属性和设置

您可以查看 Real Server 属性，比如分配至 Real Server 的 Profile 类型。

查看 Real Server 属性的步骤

1. 在Main选项卡上，展开**Local Traffic**。
2. 点击**Real Servers**。
   屏幕将出现一张包含所有现有Real Server的列表。
3. 在Name栏中，点击一个Real Server名称。
   屏幕将显示该Real Server的属性。

查看 Real Server 资源

您可查看作为资源分配至 Real Server 的缺省 pool、default persistence Profile 和 fallback persistence Profile。您还可以查看与 Real Server 相连的所有 iRule。以下就是如何查看这些资源的步骤。

查看 Real Server 资源的步骤

1. 在Main选项卡上，展开**Local Traffic**。
2. 点击**Real Server**。
   屏幕将出现一张包含所有现有Real Server的列表。
3. 点击一个Real Server名称。
   屏幕将显示该Real Server的属性。
4. 点击Resource菜单。
   屏幕将显示分配至Real Server的各种资源。

查看 Real Server 统计信息

您可以使用 Configuration 程序查看任一现有 Real Server 的统计信息。

查看 Real Server 统计信息的步骤

1. 在Main选项卡上，展开**Local Traffic**。
2. 点击**Real Servers**。
   屏幕将出现一张包含所有现有Real Server的列表。
3. 在Name栏中，点击一个Real Server的名称。
4. 从Statistics菜单中选择Real Server。
   屏幕将显示该Real Server的统计信息。

查看虚拟地址配置

有时候，您可能需要查看虚拟地址设置，以便确定是否需要对其进行调整。对于虚拟地址配置，您可以查看：

- 虚拟地址列表
- 虚拟地址属性
- 虚拟地址统计信息

查看虚拟地址列表

您可以查看一列已经创建的虚拟地址，并调整其任何设置。当打开虚拟地址列表的时候，“配置”程序也会显示该地址的状态（启用或禁用）。

查看虚拟地址列表的步骤

1. 在Main选项卡上，展开**Local Traffic**。
2. 点击**Real Servers**。
   缺省情况下，屏幕将出现一张包含所有现有Real Server的列表。
3. 在菜单栏，点击Virtual Address List。
   屏幕将出现一张包含所有现有虚拟地址的列表。

查看虚拟地址属性

以下是查看虚拟地址属性的步骤。

查看或调整虚拟地址属性的步骤

1. 使用前一步骤打开现有虚拟地址列表。
2. 点击一个虚拟地址。
   屏幕将显示该虚拟地址的属性。

查看虚拟地址统计信息

您可以使用 Configuration 程序查看任一现有虚拟地址的统计信息。

查看虚拟地址统计信息的步骤

1. 在Main选项卡上，展开**Local Traffic**。
2. 点击**Real Servera**。
   缺省情况下，屏幕将出现一张包含所有现有Real Server的列表。
3. 在菜单栏，点击Virtual Address List。
   屏幕将出现一张包含所有现有虚拟地址的列表。
4. 从Statistics菜单中选择**Virtual Address**。
   屏幕将显示该虚拟地址的统计信息。

删除Real Server

您可以从配置中永久性删除 Real Server 及其虚拟地址。

删除 Real Server

1. 在Main选项卡上，展开**Local Traffic**。
2. 点击**Real Server**。
   屏幕将显示现有Real Server的列表。
3. 从左边的复选框中选中您想删除的Real Server。
4. 点击**Delete**。
   将显示Delete Confirmation屏幕。
5. 点击**Delete**。
   删除Real Server。

3

配置节点

- 节点介绍
- 创建和修改节点
- 配置节点设置
- 管理节点

节点介绍

*节点*就是帮助BIG-IP®本地流量管理（LTM）系统传输流量的网络设备。当向负载平衡 Pool 中添加 Pool 成员时，可以显式创建一个节点，也可以指示 LTM 系统自动创建一个节点。

节点与 Pool 成员之间的区别在于，节点仅由设备的 IP 地址指定（**10.10.10.10**），而 Pool 成员则由 IP 地址和服务（如 **10.10.10:80**）共同指定。

节点的主要特性就是与状态 Monitor 关联。与 Pool 成员一样，节点能够与状态 Monitor 关联，作为确定服务器状态的方式。然而，Pool 成员的状态 Monitor 报告设备上运行的服务的状态，而与节点关联的状态 Monitor 则报告设备自身的状态。

例如，如果 ICMP 状态 Monitor 与节点 **10.10.10.10**（对应的 Pool 成员 10.10.10.10:80）关联，并且 Monitor 报告节点处于 **Down** 状态，那么 Monitor 报告 Pool 成员也处于 **Down** 状态。相反，如果 Monitor 报告节点处于 **Up** 状态，那么 Monitor 就会根据运行在其上的服务的状态，报告 Pool 成员处于 **Up** 或 **Down** 状态。

您可以使用 Configuration 工具创建节点，然后根据需要调整设置。使用相同的工具，您还可以显示节点信息，启用和禁用节点以及删除节点。

创建和修改节点

节点是创建负载平衡 Pool 的基础。对于任何您希望成为负载平衡 Pool 一部分的服务器，都必须首先创建一个节点，即将该服务器指定为一个节点。在将服务器指定为节点后，就可以将该节点作为 Pool 成员添加到 pool 中。此外，您也可以将状态 Monitor 与节点关联起来，以报告该服务器的状态。有关将节点添加到负载平衡 Pool 的详细信息，请参阅第 4 章“配置负载平衡 Pool”。

您可以使用 Configuration 工具创建节点。创建节点时，LTM 系统自动为该节点指定一组缺省设置。您可以保留或修改这些缺省设置。也可以在创建了节点之后修改这些设置。有关这些设置的详细信息，请参阅第 3-3 页上的“配置节点设置”或在线帮助。

了解 LTM 系统将一些设置指定为基本设置、而将其它设置指定为高级设置是很有帮助的。如果您在创建节点时决定修改某些缺省设置，请务必在屏幕上选择高级选项，以查看全部可配置的设置。有关基本和高级设置的详细信息，请参阅第 1 章“本地流量管理介绍”。

创建节点

1. 在 Main 选项卡上，展开 **Local Traffic**。
2. 点击 **Nodes**。
   将打开 Node 屏幕。
3. 在屏幕的右上角，点击 **Create**。
   将打开 New Node 屏幕。
4. 对于 **Address** 设置，输入节点的 IP 地址。

5. 指定、保留或修改其它任何设置。
6. 点击 **Finished**。

修改现有节点

1. 在 Main 选项卡上，展开 **Local Traffic**。
2. 点击 **Nodes**。
   将打开 Node 屏幕。
3. 在 Address 栏中，点击一个地址。
   此操作显示该节点的设置。
4. 保留或修改任何节点设置。
5. 点击 **Update**。

配置节点设置

您可以配置节点设置，以便根据具体需要定制节点。对于那些具有缺省值的设置，您可以保留或修改缺省设置。同样，您也可以在创建节点时或创建节点后随时修改这些设置。

表 3.1 列出了这些可配置的设置及其缺省值。该表的下面是具体设置说明。

节点设置	说明	缺省值
Adress	指定节点的 IP 地址。该设置是必需的。	无缺省值
Name	指定节点的名称。	无缺省值
Health Monitor	将状态或性能 Monitor 与节点关联。	无缺省值
Select Monitor	指定将 LTM 系统与节点关联的 Monitor。	无缺省值
Availability Requirement	指定满足以下条件的状态 Monitor 的最小数量：这些 Monitor 必须在 LTM 系统报告节点处于**开启**状态之前，报告节点可用来接收流量。	**All**
Ratio	指定您希望分配到节点的比率权重。	**1**
Connection Limit	指定一个节点上允许的并发连接的最大数量。	**0**

表3.1 *节点配置设置*

在配置节点之前，说明您可能需要修改的特定节点设置是很有帮助的。

指定节点的地址

对于每个配置的节点，都必须指定一个IP地址。例如，节点IP地址为**10.10.10.10**。这是唯一必需的设置。

指定节点名

对于每个配置的节点，您都可以指定唯一的节点名，如Node_1。节点名要区分大小写，并且只能包含字母、数字和下划线（_）。不允许使用保留的关键字。

指定Monitor关联

利用LTM系统，您可以通过将状态或性能Monitor与这些节点关联，监视节点的性能状态。这类似于将Monitor与负载平衡Pool关联，只是在与节点关联的情况下，您监视的是IP地址；而在与pool关联的情况下，您监视的是在Pool成员上激活的服务。

LTM系统包含许多不同的预先配置的Monitor。您可以根据要监视的流量类型，将这些Monitor与节点关联。您也可以创建自己的定制Monitor，并将它们与节点关联。唯一不能与节点关联的预先配置的Monitor，是那些专门为监视pool或Pool成员而非节点设计的Monitor。

将Monitor与节点关联有两种方式：创建缺省Monitor关联，或者在创建节点时，将Monitor与每个节点进行显式关联。有关状态与性能Monitor的详细信息，请参阅第10章“配置Monitor”。

创建缺省 Monitor 关联

您可以对LTM系统进行配置，以自动将一个或多个Monitor类型与您创建的每个节点关联。在这种情况下，您需要在创建节点前选择Monitor，然后在缺省模式下，LTM系统将这些Monitor与您创建的每个节点关联。这样就消除了必须将Monitor与您创建的每个节点进行显式关联的工作。

通过导航到Nodes页面和使用缺省Monitor菜单，您可以为节点指定缺省Monitor。然后，当创建节点时，您可以将状态Monitor设置的值设为节点缺省。

◆ 注

如果您希望将缺省Monitor分配到现有节点上，那么可以使用相同的缺省Monitor菜单来完成分配任务。

将 Monitor 与节点进行显式关联

您不必配置LTM系统来自动将一个或多个Monitor与您创建的每个节点关联，只需在创建节点时将特定Monitor与该节点关联。

在创建节点或修改节点设置时，通过将状态Monitor设置的值设为节点特定，可以将Monitor与特定节点关联（而不是像在缺省Monitor关联的情况下那样，与所有节点关联）。然后，Configuration工具使您能够从可用来与该节点关联的Monitor列表中进行选择。

指定可用性要求

通过配置可用性要求设置，您可以指定满足以下条件的状态Monitor的最小数量：这些Monitor必须在LTM系统报告节点处于开启状态之前，报告节点可用来接收流量。可接受的值为全部或您指定的一个数。如果选择最小值（At Least），则需指定一个数。

指定比率权重

比率设置指定节点的比率权重。缺省设置为1。有关比率权重的详细信息，请参阅第4章“配置负载平衡Pool”。

设置连接限制

利用连接限制设置，您可以指定节点上允许的并发连接的最大数量。注意缺省值0（零）意味着节点能够接收的并发连接的数量没有限制。

管理节点

在创建了节点并根据需要对其设置进行配置后，您可能需要执行一些额外的管理任务。您可以通过以下方式管理现有节点：

- 查看现有节点
- 启用或禁用现有节点
- 删除现有节点
- 禁用Monitor关联
- 显示节点状态

查看现有节点

您可以通过以下步骤查看已经创建的节点。

查看现有节点

1. 在 Main 选项卡上，展开 **Local Traffic**。
2. 点击 **Nodes**。
   此操作将显示现有节点列表。
3. 在 Address 栏中，点击您希望查看的节点的地址。此操作将显示该节点的设置。

启用和禁用节点

为了接受流量，必须启用节点。当节点禁用时，LTM系统允许现有连接中断或者正常结束。在这种情况下，只要这些连接属于现有持续性会话，节点便能够接受新的连接。（这样，禁用的节点便与设置为关闭的节点区别开来。关闭节点允许现有连接中断，但是不接受新的连接。）

启用或禁用节点

1. 在 Main 选项卡上，展开 **Local Traffic**。
2. 点击 **Nodes**。
   此操作将显示现有节点列表。
3. 查找您希望启用或禁用的节点的地址。
4. 在左栏中，检查 Select 框。
5. 在屏幕底部，点击 **Enable** 或 **Disable** 按钮。

删除节点

如果不再在pool中使用节点，可以删除节点。

删除节点

1. 在 Main 选项卡上，展开 **Local Traffic**。
2. 点击 **Nodes**。
   此操作将显示现有节点列表。
3. 查找您希望启用或禁用的节点的地址。
4. 在左栏中，检查 Seclect 框。
5. 在屏幕底部，点击 **Delete**。
   显示确认屏幕。
6. 点击 **Delete**。

取消Monitor关联

利用配置工具，您可以取消与某个特定节点显式关联的Monitor。当取消与某个特定节点关联的Monitor时，您既可以完全取消Monitor关联，也可以对其进行修改，以便只有缺省Monitor与该节点关联。此外，您也可以取消任何缺省Monitor，即LTM系统自动与您创建的任何节点关联的Monitor。有关Monitor或关联的详细信息，请参阅第3-4页上的“指定Monitor关联”。

取消节点与Monitor的显式关联

1. 在Main选项卡上，展开**Local Traffic**。
2. 点击**Nodes**。
   此操作将显示现有节点列表。
3. 点击您希望管理的节点的地址。
4. 在屏幕的Configuration部分查找Health Monitor设置。
5. 选择**Node Default**或**None**。
6. 点击**Update**。

取消缺省Monitor

1. 在Main选项卡上，展开**Local Traffic**。
2. 点击**Node**。
   此操作将显示现有节点列表。
3. 点击Default Monitor菜单。
4. 使用右箭头（**>>**），将任何活动Monitor从**Active**框移动到**Available**框。
5. 点击**Update**。

显示节点状态

Nodes屏幕自动显示所有现有节点的状态。可用的状态值包括：

- All
- Available
- Unavailable
- Offline
- Unknown

4

配置负载平衡 Pool

- 负载平衡Pool简介
- 创建和修改负载平衡Pool
- 配置pool设置
- 配置Pool成员设置
- 管理pool和Pool成员

负载平衡Pool简介

在典型的客户端-服务器情形下，客户请求到达在请求标头中指定的目的地IP地址。对于输入流量很大的站点来说，由于目的地服务器要处理大量请求，因而很快就会出现过载现象。为解决这一难题，BIG-IP® 本地流量管理（LTM）系统将客户机请求分配到多个服务器上，而并非只是指定的目的地IP地址。当创建负载平衡Pool时，您可以对LTM系统进行配置来解决此类问题。

什么是负载平衡Pool？

负载平衡Pool是您组合起来接收和处理流量的一组设备，如Web服务器。LTM系统将客户机流量请求发送到Pool成员中的任一服务器上，而不是发送到客户机请求指定的目的地IP地址。

当创建负载平衡Pool时，将服务器（称作Pool成员）分配到pool中，然后将pool与LTM系统中的Real Server相关联。然后，LTM系统将进入Real Server中的流量传输到Pool成员。单个服务器可隶属于一个或多个pool，这取决于您希望如何管理您的网络流量。

LTM系统选择将请求发送给哪个Pool成员由您指定给该pool的负载平衡法决定。负载平衡法是一种算法，LTM系统利用它来选择处理请求的Pool成员。例如，缺省负载平衡法是轮循，采用这种方法，LTM系统将每个输入请求发送到下一个可用的Pool成员，从而将请求平均分配到pool中的所有服务器上。有关负载平衡法的完整列表，请参阅第4-9页上的“指定负载平衡法”。

负载平衡Pool的特性

您可以配置LTM系统，以便对pool执行多种不同的操作。您可以：

- 将状态Monitor和pool及Pool成员相关联；
- 激活或禁用SNAT连接；
- 若原定目标Pool成员不可用，重新连接到其它Pool成员；
- 在数据包内设置“服务质量”或“服务类型”级别；
- 指定pool的负载平衡运算法；
- 将Pool成员分配到pool内的优先组别。

创建和修改负载平衡Pool

您可以使用Configuration工具创建负载平衡Pool，或修改pool及其成员。当创建pool时，LTM系统自动将一组缺省设置分配到该pool及其成员。您可以保留这些缺省设置，也可以对它们进行修改。此外，您也可以在创建pool后随时修改这些设置。

了解LTM系统将一些设置指定为基本设置、而将其它设置指定为高级设置是很有帮助的。如果您在创建pool时决定修改某些缺省设置，请务必在屏幕上选择**Advanced**选项，以查看全部可配置的设置。有关基础和高级设置的详细信息，请参阅第1章“本地流量管理介绍”。

创建和实施负载平衡Pool

创建和实施负载平衡Pool包括两项任务：

- 首先，您必须创建pool。
- 其次，您必须将pool与Real Server相关联。

创建负载平衡Pool

1. 在Main选项卡上，展开**Local Traffic**。
2. 点击**Pools**。
   将打开Pools屏幕。
3. 在屏幕的右上角，点击**Create**。
   将打开New pool屏幕。
4. 在Configuration列表中，选择**Advanced**。
5. 在**Name**设置中，输入pool名称。
6. 指定、保留或更改其它各项设置。
   有关pool设置的详细信息，请参阅第4-5页上的“配置pool设置”，或参考该屏幕上的在线帮助。
7. 点击**Finished**。

实施负载平衡Pool的步骤

1. 在Main选项卡上，点击**Real Server**。将打开“Real Server”屏幕。
2. 点击相应Real Server的名称。
   此操作显示该Real Server的设置。
3. 在菜单栏中，点击Resources。
4. 在**Default Pool列表**中，选择您最新创建的pool的名称。
5. 点击**Update**。

修改负载平衡Pool

您可以修改任何为现有Pool配置的设置，包括负载平衡法。有关pool设置的详细信息，请参阅第4-5页上的“配置pool设置”或在线帮助。有关向现有Pool添加成员的详细信息，请参阅以下部分的“修改Pool成员”。

修改pool设置

1. 在Main选项卡上，展开**Local Traffic**。
2. 点击**pools**。
   将打开pools屏幕。
3. 点击现有Pool的名称。
   此操作显示该pool的现有设置。
4. 在Configuration列表中，选择**Advanced**。
   此操作将显示pool设置。
5. 修改或保留所有设置。
6. 点击**Update**。
7. 如果您希望修改负载平衡方法，或者启用或禁用优先组别设置，找到菜单栏并点击Members。
8. 修改或保留**Load Balancing Method**和**Priority Group Activation**设置。
9. 点击**Update**。

修改Pool成员

对于现有负载平衡Pool，您既可修改现有Pool成员，也可以向pool中添加

新成员。

修改现有Pool成员

当修改Pool成员设置时，您可以：

- 启用或禁用Pool成员；
- 从pool中删除成员；
- 修改Pool成员设置值。

修改现有Pool成员的步骤

1. 在Main选项卡上，展开**Local Traffic**。
2. 点击**pools**。
   将打开pools屏幕。
3. 在Members栏中，点击显示的数量。
   此操作列出了现有Pool成员。
4. 在屏幕中查找Current Members部分。
5. 修改Pool成员。
   a) 如果您希望激活或禁用Pool成员或者从pool中删除Pool成员，点击成员地址左侧的框。然后，点击**Enable**、**Disable**或**Remove**。
   b) 如果您想修改Pool成员设置，点击一个地址，然后根据需要保留或修改Pool成员设置。有关Pool成员设置的详细信息，请参阅第4-14页上的“配置Pool成员设置”。
6. 点击**Update**。

向现有负载平衡Pool中添加成员

您不仅可以在创建pool时指定Pool成员，也可以在创建完成后随时添加Pool成员。当向现有Pool中添加Pool成员时（与创建pool时指定Pool成员相反），您可以为该Pool成员配置多种设置。您必须明确指定的唯一设置是**Adress**和**Service Port**设置。所有其它设置均有缺省值，您可以根据自己的需要保留或调整缺省值。

◆ **注**

如果您在创建pool时指定Pool成员，那么您不会看到这些设置，而是由LTM系统自行分配缺省值。然而，您可通过修改Pool成员属性过后修改这些设置。有关详细信息，请参阅第4-18页上的“管理pool和Pool成员”。

向负载平衡Pool添加成员

1. 在Main选项卡上，展开**Local Traffic**。
2. 点击**pools**。
   将打开pools屏幕。
3. 在Members栏中，点击显示的数量。
   此操作列出了现有Pool成员。
4. 在屏幕的右侧，点击**Add**。
   将打开New pool Members屏幕。
5. 在**Address**框中，选择**New Address**，然后输入一个IP地址，或者选择**Node List**，从中选择一个IP地址。
6. 在**Service Port**框中，输入端口号或者从列表中选择一个服务。
7. 保留或配置所有其它设置。有关Pool成员设置的详细信息，请参阅第4-14页上的“配置Pool成员设置”。

8. 点击**Finished**。

配置pool设置

您可以根据具体需要配置pool设置来定制pool。对于那些具有缺省值的设置，您可以保留或修改缺省设置。同样，您也可以在创建pool时或创建pool后随时修改这些设置。有关如何使用Configuration工具配置这些设置的详细信息，请参阅第4-2页上的“修改负载平衡Pool”。

表4.1列出您可以为pool配置的设置及每项设置的说明。

pool设置	**说明**	**缺省值**
Name	您可采用用户提供的pool名称。指定pool名称是必需的。	无缺省值
Health Monitors	您可将状态或性能Monitor与整个pool相关联，而不是只与单个Pool成员相关联。这就减轻了为多个Web服务器配置状态和性能监视的任务。	无缺省值
Availability Requirement	您可以指定满足以下条件的Monitor的数量：这些Monitor必须在Pool成员定义为Up状态前，报告Pool成员可用。	**All**
Allow SNAT	您可对pool进行配置，以便SNAT自动启用或禁用使用该pool的任何连接。	**Yes**
Allow NAT	您可对pool进行配置，以便NAT自动启用或禁用使用该pool的任何连接。	**Yes**
Action on Service Down	如果启用该设置，当目标Pool成员出现故障时，LTM系统会选择另一个Pool成员，将客户机连接到一台新的服务器。可能的值包括**None**、**Reject**、**Drop**和**Reselect**。	**None**
Link QoS	您可以对pool进行配置，根据目标pool在数据包内设置特定的服务质量级别。	**0**
IP ToS	您可对pool进行配置，根据目标pool在数据包内设置特定的服务类型级别。	**0**
Load Balancing Method	您可使用缺省负载平衡法或定义其它负载平衡法，您还可以配置基于优先级别的成员激活。不同的pool可通过不同的负载平衡法配置。	**Round Robin**
Priority Group Activation	您可以将Pool成员分配到pool内的优先组别。	**Disabled**
New Members	对于您创建的每个pool，都必须指定将成为该Pool成员的服务器。Pool成员必须由其IP地址指定。对于每个Pool成员，您还可以为其分配服务端口、比率权重和优先组别。	无缺省值

表4.1 负载平衡Pool的设置

在配置pool之前，说明您可能需要修改的特定pool设置是很有帮助的。

指定pool名称

您可以对pool进行配置的最基本设置就是pool名称。pool名称要区分大小写，并且只能包含字母、数字和下划线(_)。不允许使用保留的关键字。

您定义的每个pool都必须有唯一的名称。

将状态Monitor与pool关联

Monitor是LTM系统的一个关键特性。Monitor有助于确保服务器处于开启

状态，并且能够接收流量。如果您想将Monitor与整个服务器pool相关联上，无需明确地将Monitor与每个独立服务器相关联。相反，您只需使用pool设置**Health Monitors**来将Monitor分配到pool本身。然后，LTM系统将自动监视pool中的每个成员。

LTM系统包含许多不同的预先配置的Monitor。您可根据自己希望监视的流量类型将这些Monitor与pool关联。您还可创建自己的定制Monitor，并将其与pool关联。唯一不能与pool关联的Monitor类型就是那些专门设计用来监视节点而不是pool或Pool成员的Monitor。这些Monitor类型有：

- ICMP
- TCP Echo
- Real Server
- SNMP DCA
- SNMP DCA Base
- WMI

使用LTM系统，您可以通过许多有效的方式配置您的Monitor关联：

- 您可以将Monitor与整个pool相连而不是单个服务器关联。这样，LTM系统自动将Monitor与所有Pool成员关联，包括您后来添加的那些成员。同样，当从pool中删除某个成员时，LTM系统将不再监视该服务器。
- 当一个指定为Pool成员的服务器允许在同一个IP地址和端口上存在多个处理流程时，您可检查每个流程的状态。为了做到这一点，您可以将服务器添加到多个pool，然后在每个pool内，将Monitor与该服务器关联。与每个服务器关联的Monitor可以检查在该服务器上运行的流程的状态或性能。
- 当将Monitor与整个pool关联时，您可以撤消与该Monitor连接的单个Pool成员。这样，您就可以将这个特殊的Pool成员与其它Monitor关联，或者完全取消对该Pool成员的状态监视。例如，您可将Pool成员A、B和D与httP Monitor关联，同时将Pool成员C与httpS Monitor关联。
- 您也可以将多个Monitor与同一个pool关联。例如，您可以将http和httpS Monitor与同一个pool关联。

有关状态和性能Monitor的详细信息，请参阅第10章“配置Monitor”。

指定可用性要求

该设置指定状态Monitor的最小数量。在LTM系统报告Pool成员处于**up**状态之前，最小数量的Monitor必须报告一个Pool成员可用来接收流量。

为了配置该设置，在**Availability Requirement**框中键入一个数字。

支持SNAT与NAT

当配置pool时，您可以特别禁用针对任何使用该pool的连接的任何安全网络地址转换（SNAT）或网络地址转换（NAT）。您可以通过配置**Allow SNAT**和**Allow NAT**设置做到这一点。在默认模式下，可以启用这些设置。您可以通过显示现有Pool的属性屏幕更改关于该pool的设置。

当您希望pool禁用某种服务的SNAT或NAT连接时，您可能需要配置pool来禁用SNAT或NAT连接。在这种情况下，您可以创建一个独立的pool来

处理该服务的所有连接，然后禁用该pool的SNAT或NAT。

有关SNAT和NAT的一般信息，请参阅第11章“配置SNAT和NAT”。

当某个服务不可用时采取的措施

当某Pool成员上的服务不可用时，您可通过**Action on Service Down**设置来执行您希望LTM系统采取的措施。可能的设置有：

- **None**－－LTM不采取措施。该选项为缺省设置。
- **Reject**－－LTM系统发送RST或ICMP信息。
- **Drop**－－LTM系统简单地清除连接。
- **Reselect**－－LTM系统选择其它节点。

为了配置该设置，找到服务停止措施设置并从列表中选择一个值。

配置服务质量（QoS）级别

pool的另一个设置是服务质量（QoS）级别。QoS级别是网络设备根据标识符确认和处理不同的流量的方法。从根本上说，在数据包中指定的QoS级别加强了该数据包的吞吐率要求。

当流量输入站点时，LTM系统可以根据数据包所指向的pool的QoS级别，来设置该数据包的QoS级别。LTM系统还可以根据服务质量级别，应用iRule将流量发送到不同的服务器pool。

LTM系统可根据在pool中设置的QoS值，标记流出流量（基于HTTP GET的返回数据包）。然后，由上游设备检查该值，并赋予其相应的优先级。根据iRule，LTM系统可检查流入流量在标头中是否含有特殊QoS或ToS标记。然后，LTM系统可根据该标记做出科学的iRule负载平衡决策。

例如，通过配置pool为发送到该pool的数据包设置QoS级别，您可将**Client**级别设为3，**Server**设为4。这样，当将数据包发送到客户机时，QoS级别为3，而当将数据包发送到服务器时，QoS级别为4。

除了配置pool来设置数据包的QoS级别之外，您可以配置iRule，根据数据包内现有QoS值选择pool。有关详细信息，请参阅第13章“编写iRule”。

配置服务类型（ToS）级别

另一个pool设置是服务类型（ToS）级别。除QoS级别之外，ToS级别是网络设备根据标识符确认和处理不同流量的另一种途径。当流量输入站点时，LTM系统可根据数据包所指向的pool的ToS级别，来设置该数据包的ToS级别。LTM系统还可以根据ToS级别，应用iRule将流量发送到不同的服务器pool。

LTM系统可根据在pool中设置的ToS值，标记流出流量（基于HTTP GET的返回数据包）。然后，由上游设备检查该值，并赋予其相应地优先级。根据iRule，LTM系统可检查流入流量的标头中是否含有特殊的ToS标记。然后，LTM系统可根据该标记做出科学的iRule负载平衡决策。

例如，通过配置pool为发送到该pool的数据包设置ToS级别，您可将**Client**级别和**Server**级别均设置为16。这样，当将数据包发送到客户机时，ToS

级别为16，而当将数据包发送到服务器时，ToS级别也为16。

◆ 注

如果您更改客户机或服务器pool的ToS级别时，现有连接继续使用原来的设置。

除了配置pool来设置数据包的ToS级别之外，你可以配置iRule，根据数据包内现有ToS值来选择pool。有关详细信息，请参阅第13章“编写iRule”。

指定负载平衡法

负载平衡是LTM系统不可分割的一部分。在LTM系统上配置负载平衡意味着决定您的负载平衡方案，即决定哪个Pool成员应当接收由特殊Real Server支持的连接。当决定了负载平衡方案后，您就可以为该方案指定适当的负载平衡法。

负载平衡法是一种算法或公式，LTM系统可以使用它来决定发送流量的节点。独立的负载平衡法考虑了一种或多种动态因素，如当前连接计数等。由于LTM系统的每个应用都是唯一的，而且节点性能取决于诸多不同的因素，因此我们建议您尝试使用不同的负载平衡法，并选择能够在您的特定环境下提供最佳性能的方法。

使用缺省负载平衡法

LTM系统的缺省负载平衡法为Round Robin，可以简单地将每个新的连接请求一致地传递到下一服务器。所有其它负载平衡法均考虑了服务器容量和/或状态。

如果您用来平衡负载的设备的处理速度和内存基本相同，Round Robin模式在大多数配置中都会运行良好。如果您希望使用Round Robin方法，那么您可以跳过本节的其它内容，并开始配置您希望添加到基本pool配置的其它pool设置。

选择负载平衡法

如果您运行的服务器的处理速度和内存差别较大，您可能需要采用一种比率或动态方法。

- **Round Robin**
  该模式为缺省负载平衡法。Round Robin模式将每个新连接请求一致地传递到下一个服务器，最终将连接平均分配到负载平衡的一组设备上。Round Robin模式在大多数配置中运行良好，特别是在负载平衡设备的处理速度和内存基本相同的情况下。

- **Ratio (member)和Ratio (node)**
  LTM系统按照您所设定的比率权重在设备中分配连接，每个设备随时间变化接收的连接的数量与您为每个设备定义的比率权重成一定比例。这些属于静态负载平衡法，根据与服务器容量成比例的静态用户分配比率权重进行分配。关于Ratio负载平衡：

  负载平衡计算对每个pool可以本地化（基于成员的计算），也可以应用到将服务器作为成员的所有pool（基于节点计算）。

采用Ratio法时，这种区别尤为重要。采用Ratio (member)法时，实际比率权重在pool定义中为成员设置；而当采用Ratio (node)法时，比率权重为节点设置。

任何节点的缺省比率设置为1。如果您采用Ratio（与Ratio (node)相对）负载平衡法，必须在配置中至少为一个节点设置不是1的其它比率。

如果您未更改任何比率设置，那么负载平衡法就会与Round Robin负载平衡法具有相同的功效。

警告： *如果您将负载平衡法设置为Ratio (node)（与Ratio (member)），您就必须为每个节点定义比率设置。*

- **Dynamic Ratio**
  Dynamic Ratio方法与Ritio方法相似，只是前者的比率权重以持续监控服务器为基础，因此可持续改变。

  这是一种动态负载平衡法，根据多个方面的实时服务器性能分析分配连接，如每个节点当前的连接数量或最短节点响应时间。

  Dynamic Ratio方法专门用于RealNetworks® RealSystem® Server平台、配备了Windows管理架构（WMI）的Windows®平台或任何配备了SNMP代理（如UC Davis SNMP代理或Windows 2000 Server SNMP代理）的服务器的负载平衡流量。为了实施Dynamic Ratio负载平衡，您必须首先为这些系统安装和配置必需的服务器软件，然后安装相应的性能Monitor。有关详细信息，请参阅附录A“关于Monitor的补充信息”。

- **Fastest (node)和Fastest (application)**
  Fastest方法是根据当前所有运行节点的最快响应速度传递新的连接。在节点分布到不同逻辑网络的环境下，这些方法非常有用。负载平衡计算对每个pool可以本地化（基于成员的计算），也可以应用到将服务器作为成员的所有pool（基于节点计算）。

- **Least Connections (member)和Least Connections (node)**
  Least Connections方法相对比较简单，因为采用此方法，LTM系统可以将新连接传递到当前连接数量最少的节点。Least Connections方法的最佳工作环境为您正在平衡的服务器或其它设备具有相近的功能。

  这些方法属于动态负载平衡法，根据多个方面的实时服务器性能分析分配连接，如每个节点当前的连接数量或最短节点响应时间。

  负载平衡计算对每个pool可以本地化（基于成员的计算），也可以应用到将服务器作为成员的所有pool（基于节点计算）。

- **Observed (member)和Observed (node)**
  Observed方法结合使用了在Least Connections和Fastest模式下使用的逻辑。采用Observed方法，可以结合当前连接的数量和响应时间对节点进行排序。那些能够很好地平衡最少连接和最短响应时间的节点接收连接的比例更大。Observed模式在任何环境下运行良

好，尤其适用于节点性能变化较大的环境下。

这些方法属于动态负载平衡法，根据多个方面的实时服务器性能分析分配连接，如每个节点当前的连接数量或最短节点响应时间。

负载平衡计算对每个pool可以本地化（基于成员的计算），也可以应用到将服务器作为成员的所有pool（基于节点计算）。

- **Predictive (member)和Predictive (node)**
  Predictive方法也采用Observed方法所采用的排序方法，结合当前连接的数量和响应时间排列节点。然而，采用Predictive方法，LTM系统可以排序随时间的变化趋势，从而决定某个节点的性能当前是提高还是下降。具有更好性能等级（当前是提高而非下降）的节点可接收连接的比例更大。Predictive方法可在任何环境下很好地运行。

  Predictive方法属于动态负载平衡法，根据多个方面的实时服务器性能分析分配连接，如每个节点当前的连接数量或最短节点响应时间。

  负载平衡计算对每个pool可以本地化（基于成员的计算），也可以应用到将服务器作为成员的所有pool（基于节点计算）。

指定基于优先级的成员激活

您可以根据成员的优先级别，平衡一个pool所有成员之间的负载流量，或者只平衡当前激活的成员之间的负载流量。在基于优先级的成员激活中，pool中的每个成员都被分配一个优先级号，以便将成员安排到由该号码指定的优先组别中。

当所有Pool成员可用时（意味着它们处于**up**状态，标记为运行且并未超过其连接限制），LTM系统只将连接分配给优先级别最高的组别的所有成员，也就是说，该组别是由优先级号最高的成员指定的。**Priority Group Activation**值决定必须对限制到该组别的流量可用的成员最小数量。如果优先级别最高的组别中可用成员的数量低于最小数量，LTM系统还可以将流量分配到下一个优先级别较高的组别，依此类推。

```
pool my_pool {
    lb_mode fastest
    min active members 2
    member 10.12.10.1:80 priority 3
    member 10.12.10.2:80 priority 3
    member 10.12.10.3:80 priority 3
    member 10.12.10.4:80 priority 2
    member 10.12.10.5:80 priority 2
    member 10.12.10.6:80 priority 2
    member 10.12.10.7:80 priority 1
    member 10.12.10.8:80 priority 1
    member 10.12.10.9:80 priority 1
    }
```

图4.1 *优先负载平衡Pool配置示例*

图4.1中显示的配置有三个优先组别**3**、**2**和**1**。连接首先被分配到优先级为**3**的所有Pool成员。如果优先级为**3**的成员数少于两个，流量将直接分配到优先级为**2**的成员。如果优先级为**3**和优先级为**2**的组别的可用成员数均少于两个，流量将传输到优先级为**1**的组别。LTM系统持续监视优先级较高

的组别，每次当优先级较高的组别具有最小数量的可用成员时，LTM系统会再次限制到达该组别的流量。

指定Pool成员

当您配置该设置时，您需要指定组成负载平衡Pool的服务器（即Pool成员）。为了指定Pool成员，您必须指定服务器的IP地址和服务端口。一个可选设置是比率权重，当您选择**Ratio (member)**、**Ratio (node)**或**Dynamic Ratio**负载平衡法时适用。

配置Pool成员设置

在添加Pool成员时，您可为该Pool成员配置许多设置。在您创建负载平衡Pool后，可对这些设置的大多数进行配置。在创建pool期间，必须指定的唯一设置是**Address**和**Service Port**设置。所有其它设置均有缺省值，您可以根据需要保留或修改这些设置。

有关在创建pool期间添加Pool成员的详细信息，请参阅第4-2页“创建和实施负载平衡Pool”。有关向现有Pool添加成员的详细信息，请参阅第4-4页“向现有负载平衡Pool添加成员”。

表4.2列出了您可以为Pool成员配置的设置及每项设置的说明。

常规属性	说明	缺省值
Address	指定Pool成员的IP地址。您可自己输入一个IP地址或从节点列表中选择。	无缺省值
Service Port	为该Pool成员指定服务。	无缺省值
Ratio	指定您希望分配到Pool成员的比率权重。	**1**
Priority	可以将Pool成员分配到pool中的优先组别。	**1**
Connection Limit	设定允许Pool成员并发连接的最大数量。	**0**
Health Monitors	指定Pool成员是继续使用与pool关联的Monitor还是使用其它Monitor。	**Inherit From Pool**
Select Monitors	指定您希望与该Pool成员关联的一个或多个Monitor。只有当**状态Monitor**行设置为**特定于成员**时才使用该行。	无缺省值

表4.2 *单个Pool成员设置*

在向pool中添加Pool成员之后，要想修改该Pool成员的设置，请参阅第4-18页上的“显示Pool成员属性”。

在添加Pool成员之前，说明您可能需要修改的特定Pool成员设置是很有帮助的。

指定地址

添加Pool成员时，您可以使用**Address**设置指定该Pool成员的IP地址。您可以输入一个IP地址或从节点列表中选择。该设置是必需的。

指定服务端口

Service Port设置可提供与Pool成员关联的服务的名称或端口号。该设置是必需的。

指定Pool成员的比率权重

当使用基于比率的负载平衡法将流量分配到pool中的服务器时，您可以使用**Ratio**设置为服务器指定比率权重。比率权重决定服务器接收流量的数量。

基于比率的负载平衡法包括：**Ratio (member)**、**Ratio (node)**和**Dynamic Ratio**。有关基于比率的负载平衡法的详细信息，请参阅第4-9页“指定负载平衡法”和附录A“附加Monitor信息”。

指定基于优先级的成员激活

Priority设置为Pool成员指定优先级号。然后，根据指定给Pool成员的优先级号在pool中平衡负载流量。因此，指定为高优先级的成员优先接收流量直到负载达到一定水平，此时，流量将转至分配到下一个优先级较低的组别的成员。您可通过pool设置**Priority Group Activation**配置负载量，从而决定LTM系统何时开始将流量转至优先级较低的组别的成员。有关详细信息，请参阅第4-12页上的“指定基于优先级的成员激活”。

指定连接限制

使用**Connection Limit**设置，您可以指定允许Pool成员并发连接的最大数量。注意：缺省值**0**（零）表示Pool成员可以接收的并发连接的数量没有限制。

选择显式Monitor关联

当您将Monitor与pool关联时，LTM系统将自动使该Monitor与每个Pool成员关联，包括那些您后来添加到pool中的成员。然而，有些情况下您可能希望某个特定Pool成员的Monitor与分配到pool的Monitor不同。在这种情况下，您必须使用**Health Monitors**设置来说明您希望将特定Monitor与Pool成员进行显式关联。

您也可以通过该Pool成员来配置该设置，以防止LTM系统将任何其它Monitor与该Pool成员关联。

为了将Monitor与Pool成员显示关联，找到**Health Monitors**设置并选择特定**Member**，这将会显示**Select Monitors**设置。然后，按照以下部分的描述配置**Select Monitors**设置。

为确保LTM不将任何Monitor与该Pool成员关联，需要将**Helath Monitors**设置为**None**。

为Pool成员创建显式Monitor关联

LTM系统包含许多不同的Monitor，您可以根据要监视的流量类型将这些Monitor与Pool成员关联。您也可以创建自己的定制Monitor，并将其与Pool成员关联。唯一不能与Pool成员相关联的Monitor类型就是那些专门设计用来监视节点而不是pool或Pool成员的Monitor。这些Monitor类型有：

- ICMP
- TCP Echo
- Real Server
- SNMP DCA

- SNMP DCA Base
- WMI

有关状态与性能Monitor的详细信息，请参阅第10章“配置Monitor”。

为了将Monitor与单个Pool成员关联，您只需打开Pool成员设置并将**Health Monitors**设置为**Member Specific**。此操作将显示**Select Monitors**设置。选择您希望与Pool成员关联的Monitor，并使用左箭头（**<<**）将Monitor名移动到**Active**框。点击**Finish**或**Update**可激活只与该Pool成员关联的Monitor。

将多个Monitor与同一个Pool成员关联

LTM系统使您能够将多个Monitor与同一个服务器关联。使用Configuration工具，您可以：

- **将多个Monitor与一个pool中的一个成员关联**。例如，您可以创建Monitorhttp1、http2和http3（每个Monitor的配置不同），并将所有这三个Monitor与同一个Pool成员关联。在这种情况下，一旦任何检查失败，该Pool成员将被标记为关闭。
- **将一个IP地址和服务指定为多个pool的成员。**然后，您可以在每个pool中将另一个Monitor与该Pool成员关联。例如，假设您将服务器**10.10.10:80**指定给三个不同的pool：**my_pool1**、**my_pool2**和**my_pool3**。然后，您可以将所有这三个定制HTTP Monitor与该服务器关联（每pool一个Monitor）。结果是LTM系统使用**http1** Monitor检查服务器**10.10.10.:80**在pool **my_pool1**中的状态，**http2** Monitor检查服务器**10.10.10.:80**在pool **my_pool2**中的状态，**http3** Monitor监视服务器**10.10.10:80**在pool **my_pool3**中的状态。

您可以在将Pool成员添加到每个pool时设定多个Monitor关联，也过后修改Pool成员的属性。

管理pool和Pool成员

通常，当管理pool和Pool成员时，您首先需要查看现有Pool或Pool成员配置。有时您可能还需要执行其它管理任务。使用Configuration工具，您可以：

- 显示pool或Pool成员属性；
- 禁用Monitor关联；
- 删除负载平衡Pool；
- 查看pool和Pool成员统计。

显示pool或Pool成员属性

您可以通过以下步骤显示为pool或单个Pool成员配置的设置。有关修改pool属性的详细信息，请参阅第4-3页上的“修改负载平衡Pool”；有关修改Pool成员属性的详细信息，请参阅第4-3页上的“修改现有Pool成员”。

显示pool属性的步骤

1. 在Main选项卡上，展开**Local Traffic**。

2. 点击**pools**。
   将打开Pools屏幕。
3. 点击pool名称。
   此操作将显示该pool的属性。

显示Pool成员属性的步骤

1. 在Main选项卡上，展开**Local Traffic**。
2. 点击**Pools**。
   此操作将显示现有Pool列表。
3. 在Member栏中，点击显示的数量。
   此操作列出了该pool的所有成员。
4. 在Current Members列表中，点击一个Pool成员地址。此操作将显示该Pool成员的属性。

取消Monitor关联

您可以取消Pool或Pool成员的任何现有Monitor关联。

如果从Pool中删除一个Monitor，请访问该Pool的属性页面，并通过将**Active**框中的Monitor名移动到**Enable**框来更改**Health Monitors**设置。

如要取消单个Pool成员的显式Monitor关联，请访问该Pool成员的属性页面，并将**Health Monitors**设置更改为**Inherit From Pool**或**None**。选择**None**不包括您在该Pool中已配置的任何监视的Pool成员。

删除Pool

通过以下步骤删除现有Pool。有关删除Pool中单个Pool成员的详细信息，请参阅第4-3页上的“修改现有Pool成员”。

在删除Pool之前，您必须首先从Real Server中删除作为资源的Pool。

删除Pool的步骤

1. 在Main选项卡上，展开**Local Traffic**。
2. 点击**Pools**。
   此操作将显示现有Pools列表。
3. 在与Pool名称相邻的左侧栏中，检查Seclect框。
4. 点击**Delete**。
   此操作将显示Delete Confirmation屏幕。
5. 点击**Delete**。

查看Pool和Pool成员统计

使用Configuration工具，您可以查看与现有Pool和Pool成员相关的统计信息。

如果要查看Pool和Pool成员统计，打开现有Pool列表或现有Pool成员列表。然后，点击菜单栏上的统计。此操作将打开**Statistics**屏幕，显示所有现有Pool及其Pool成员的统计。

显示的统计类型有：

- 位（进入和发出）

- 数据包（进入和发出）
- 连接（当前数量、最大数量和总数）

5

了解 Profile

- Profile简介
- 创建和修改Profile
- 实施Profile
- 配置协议Profile的设置
- 管理Profile
- 通过iRule使用Profile

Profile简介

BIG-IP®本地流量管理（LTM）系统可以多种方式管理特定应用的网络流量，具体取决于正在使用的协议与服务。例如，您可以将 LTM 系统配置为压缩 HTTP 响应数据，也可以将系统配置为在将请求传递给目标服务器之前，对 SSL 客户机证书进行认证。

对于您希望管理的每类流量，LTM 系统都包含相应的配置工具，您可以使用这些工具对该流量的行为进行智能控制。这些工具称为 Profile。***Profile*** 是系统提供的配置工具，用于增强对特定应用的流量的管理能力。更确切地说，一个 Profile 就是一个对象，其中包含可由用户配置的设置，这些设置具有缺省值，用于控制特定网络流量类型（例如 HTTP 连接）的行为。使用 Profile 可以加强对网络流量管理的控制，使流量管理任务更轻松、更有效。

Profile类型

LTM 系统提供若干种类型的 Profile。其中一些 Profile 类型对应特定的协议（例如 HTTP、SSL 和 FTP），而另一些 Profile 则对应适用于多种协议的流量的行为。后一类 Profile 的实例包括连接持续性 Profile 和认证 Profile。表 5.1 列出了可用的 Profile 类型及其说明。

Profile 类型	说明
协议 Profile	
FastL4	定义第 4 层 IP 流量的行为。
TCP	定义 TCP 流量的行为。
UDP	定义 UDP 流量的行为。
OneConnect	允许客户机请求复用服务器端连接。LTM 系统复用服务器端连接的功能称为 Connection Pooling™（连接 Pool）。
Stream	定义实时流协议（RTSP）流量的行为。
服务 Profile	
HTTP	定义 HTTP 流量的行为。
FTP	定义 FTP 流量的行为。
SSL Profile	
Client SSL	定义客户机端SSL流量的行为。请参阅**持续性Profile**。
Server SSL	定义服务器端SSL流量的行为。请参阅**持续性Profile**。
持续性Profile	
Cookie	使用HTTP cookie实施会话持续性。
Destination Address	根据客户机请求的标头中指定的目的地IP地址实施会话持续性。也称为粘着持续性。
Hash	以类似通用持续性的方式实施会话持续性，不同之处在于LTM系统使用散列来查找持续性条目。
MSRDP	针对微软远程桌面协议会话实施会话持续性。
SIP	针对使用会话启用协议呼叫ID的连接实施会话持续性。
Source Address	根据客户机请求的标头中指定的源IP地址实施会话持续性。也称为简单持续性。
SSL	针对非端接的SSL会话，使用会话ID实施会话持续性。

通用	使用LTM系统的通用检查引擎（UIE）实施会话持续性。
认证Profile	
LDAP	允许LTM系统根据存储在远程小型目录访问协议（LDAP）服务器上的认证数据对流量进行认证。
RADIUS	允许LTM系统根据存储在远程RADIUS服务器上的认证数据对流量进行认证。
TACACS+	允许LTM系统根据存储在远程TACACS+服务器上的认证数据对流量进行认证。
SSL Client Authentication LDAP	允许LTM系统根据存储在远程LDAP服务器上的数据控制客户机对服务器资源的访问权限。客户机授权证书基于SSL证书和已定义的用户群与角色。
SSL OCSP	允许LTM系统使用存储在远程在线证书状态协议（OCSP）服务器上的数据检查客户机证书的撤销状态。客户机证书基于SSL证书。

***表5.1** LTM系统中的可用Profile*

缺省Profile

对于表 5.1 中列出的每种 Profile 类型，LTM 系统都带有一个缺省 Profile。***缺省 Profile*** 是系统提供的 Profile，其中包括自身设置的缺省值。http 缺省 Profile 便是缺省 Profile 的一个实例。您可以按原状使用缺省 Profile，也可以基于缺省 Profile 创建定制 Profile。

使用缺省 Profile 的方式有多种：

- **您可以按原状使用缺省Profile。**
  您只需将Real Server配置为参考缺省Profile。
- **您可以修改缺省Profile设置（不建议）。**
  修改缺省Profile时，原始缺省Profile的设置将丢失。因此，今后基于该缺省Profile创建的任何定制Profile都将继承经过修改的设置。
- **您可以基于缺省Profile创建定制Profile（建议）。**
  这允许您保留缺省Profile，改为在定制Profile中配置个性化的设置。定制Profile继承您指定的上级Profile的部分设置值。创建定制Profile之后，您可以将Real Server配置为参考定制Profile，而不是参考缺省Profile。有关定制Profile的详细信息，请参阅下面的“定制Profile与上级Profile”。

◆ **注**

可以修改缺省 Profile，但不能创建或删除缺省 Profile。

◆ **警告**

一旦修改了缺省 Profile，那么将设置恢复为原始值的唯一方法是对 Profile 进行手动配置，指定那些值。

定制Profile与上级Profile

定制 Profile 是您创建的 Profile。创建 Profile 时，您指定的设置之一是 **Parent Profile** 设置。***上级 Profile*** 也是一个 Profile，您的定制 Profile 从中继承设置和设置的缺省值。

一般而言，定制 Profile 自动继承其上级 Profile 的设置和相应的值。因此，创建定制 Profile 时不必逐个地对设置进行配置，您只需指定上级 Profile，这将令 LTM 系统自动为定制 Profile 的设置分配值。所分配的值是上级

Profile 对应的值。

◆ 注

如果创建定制Profile 时未指定上级Profile，那么LTM 系统自动将相应的缺省Profile 指定为上级Profile。

创建定制 Profile 时，可以指定为上级 Profile 的典型 Profile 是缺省 Profile。例如，如果创建称为 my_http_profile 的 HTTP 类 Profile，那么可以将缺省 Profilehttp 指定为上级 Profile。在此情形中，LTM 系统自动创建 Profilemy_http_profile，以便其包含与 Profilehttp 相同的设置和缺省值。这样，新的下级 Profile 从其上级 Profile 中继承相应的设置和值。

修改下级 Profile 的设置时，此自动继承特性将出现异常。此时，下级 Profile 任何经过修改的设置都不再继承上级值。这样做的目的是防止 LTM 系统覆盖下级 Profile 中任何您已经修改的设置。

然而，对于下级 Profile 中没有修改的所有设置，下级 Profile 继续从上级 Profile 中继承相应的值。

使用定制 Profile 作为上级 Profile

创建定制 Profile 时，可以将其它定制 Profile（而不是缺省 Profile）指定为上级 Profile。唯一的限制是：您指定为上级的定制 Profile 必须与其下级具有相同的 Profile 类型。一旦创建了下级 Profile，那么指定为上级的定制 Profile 的设置和缺省值将自动成为该下级 Profile 的设置和缺省值。

例如，如果创建称为 my_http_profile2 的 Profile，那么可以将定制 Profilemy_http_profile 指定为它的上级 Profile。结果是，Profilemy_http_profile2 的缺省设置值是上级 Profilemy_http_profile 的缺省设置值。

如果随后修改上级 Profile 的设置，LTM 系统会自动将这些变化传播到下级 Profile。例如，如果创建定制 Profilemy_http_profile，然后将其用作上级 Profile 来创建定制 Profilemy_http_profile2，那么以后对 Profilemy_http_profile 所做的任何更改都将自动传播到 Profilemy_http_profile2。同样，修改下级 Profile 中的任何设置时，此自动传播特性将出现异常。对于那些经过修改的设置，下级 Profile 不再继承其上级 Profile 的值。

Profile小结

Profile 是一种配置工具，可以用来影响特定网络流量类型的行为。默认情况下，LTM 系统提供了一组可以按原样使用的 Profile。这些 Profile 包含定义 FastL4、TCP、UDP、RSTP、HTTP、FTP 和 SSL 流量行为的各种设置。此外，通过 Profile 还可以启用连接和会话的持续性以及管理客户机应用认证。将 Profile 分配到 Real Server 之后，LTM 系统将根据该 Profile 中定义的设置，管理任何与该 Profile 类型对应的流量。

Profile 可能的类型有两种：缺省 Profile 和定制 Profile。缺省 Profile 由 LTM 系统提供，定制 Profile 由您创建。缺省 Profile 中包含的值能够满足您的需要时，请使用缺省 Profile。如果希望您的值与缺省 Profile 中包含的值不同，请使用定制 Profile。为使配置和维护 Profile 的任务变得轻松，LTM

系统保证定制 Profile 自动从上级 Profile 中继承设置和相应的值。

创建 Profile 来管理一类网络流量时，可以通过以下方式使用这些 Profile：

- 您无需执行任何动作来使用缺省Profile，该文件在默认情况下已经启用。LTM系统根据这些Profile中指定的值，使用这些缺省Profile来自动引导相应的流量类型。
- 您可以使用缺省Profile作为上级Profile，修改该Profile中的部分或全部值，从而创建定制Profile。
- 您可以创建一个定制Profile，然后将其用作其它定制Profile的上级Profile。

创建和修改Profile

如上一节中所述，Profile 是用来帮助管理应用流量的配置工具。使用 Profile 时，您可以使用 LTM 系统提供的缺省 Profile，也可以创建自己的定制 Profile。此外，您还可以根据需要修改现有的 Profile。确切地说，您可以：

- 按原状使用缺省Profile。
- 修改缺省Profile。
- 创建定制Profile。
- 修改定制Profile。

以下数节包括创建和修改 Profile 的操作流程。如要了解各个 Profile 设置及其对不同流量类型的影响，请参阅本章剩余部分，或参阅以下各章之一：

- 第6章“管理HTTP和FTP流量”
- 第7章“管理SSL流量”
- 第8章“认证应用流量”
- 第9章“启用会话持续性”

有关缺省 Profile 和定制 Profile 的背景信息，请参阅第 5-1 页上的“Profile 简介”。

按原状使用缺省Profile

LTM 系统提供了一个对于每种流量类型，都可以按原状使用的缺省 Profile。缺省 Profile 包含与管理该类流量相关的任何属性和设置的缺省值。要实施缺省 Profile，只需使用 Configuration 工具将该 Profile 分配给 Real Server。您不需要配置设置的值。有关详细信息，请参阅第 5 - 10 页上的“实施 Profile”。

有关创建或修改 Real Server 的信息，请参阅第 2 章“配置 Real Server”。

修改缺省Profile

您可以使用 Configuration 工具来修改缺省 Profile 的值，但我们不建议这样做。虽然修改缺省 Profile 比创建定制 Profile 看似更加简单、快捷，但请记住，这样做将丢失原始值。之后，如果希望将 Profile 重新设置回其原始状态，必须以手动方式进行重新设置，再次修改缺省 Profile 的设置，以指定原始值。（要查找原始缺省值，请参阅本指南中相关 Profile 的章节，或参阅在线帮助。）

修改与实施缺省 Profile 共分两步：

- 首先，必须使用Configuration工具修改缺省Profile的设置。有关详细信息，请参阅后面的“修改缺省Profile”。
- 其次，必须将该Profile与Real Server关联。有关将Profile与Real Server进行关联的信息，请参阅第5 - 10页上的“实施Profile”。

修改缺省 Profile 的步骤

1. 在Main选项卡上，展开**Local Traffic**。
2. 点击**Profiles**。
   将打开HTTP Profile”屏幕。
3. 选择要修改的缺省Profile：
   - 如果要修改http Profile，请点击名称http。
     此操作将显示缺省http Profile的属性和设置。
   - 如果要修改除HTTP Profile之外的缺省Profile，请在菜单栏上点击相应的Profile菜单，选择Profile类型，然后点击Profile名称。
     此操作将显示该缺省Profile的属性和设置。
4. 根据需要修改设置。
5. 点击**Update**。

创建定制Profile

如果不想按原状使用缺省 Profile，也不想更改其设置，那么可以创建定制 Profile。创建定制 Profile 并将其与 Real Server 进行关联，这样便可以实施一组特定的流量管理政策。

创建定制 Profile 时，该 Profile 是一个下级 Profile，它自动继承您指定的上级 Profile 的设置值。但是，您可以更改下级 Profile 中的任何值，以更好地满足自己的需要。有关定制 Profile 和继承设置值的背景信息，请参阅第 5 - 3 页上的“定制 Profile 与上级 Profile”。

如果没有指定上级 Profile，LTM 系统将使用与所创建的 Profile 类型相匹配的缺省 Profile。

实施定制 Profile 共分两步：

- 首先，必须使用Configuration工具创建定制Profile。有关详细信息，请参阅后面的“创建定制Profile的步骤”。
- 其次，必须将该Profile与Real Server关联。有关将Profile与Real Server进行关联的信息，请参阅第5 - 10页上的“实施Profile”。

◆ 重要信息

在 Configuration 工具的每个 Profile 创建屏幕中，每个 Profile 设置的右侧都有一个复选框。选中设置的复选框，然后应用该设置的值时，Profile 将保留该值，即使您以后更改了上级 Profile 的相应值。因此，选中设置的复选框可以确保继承过程中，上级 Profile 不会覆盖该值。

创建定制 Profile 的步骤

1. 在Main选项卡上，展开**Local Traffic**。
2. 点击**Profiles**。
   默认情况下，将打开Profiles屏幕，并列表显示任何现有的HTTP Profile。
3. 选择要创建的Profile类型：

- 如果要创建HTTP类型的Profile，请继续执行步骤4。
- 如果要创建其它类型的Profile，请在菜单栏上点击Profile目录，然后选择Profile类型。

4. 在屏幕的右侧，点击**Create**。
   此操作将显示创建新Profile的屏幕。
5. 在**Name**框中，为Profile键入一个唯一的名称。
6. 对于**Parent Profile**，从列表中选择一个Profile。
   您可以选择缺省Profile，也可以选择其它定制Profile。
7. 指定、修改或保留所有设置的值：
   - 如果要指定或修改值，请找到相应的设置，点击屏幕右侧“定制”栏中的复选框，然后键入或修改值。
   - 如果要保留继承自上级Profile的值，请将设置保持不变，且不要选中“定制”栏中的复选框。
8. 点击**Finished**。

◆ **提示**

*访问 New Profile 屏幕的另一种方法是展开 Main 选项卡上的 **Local Traffic**，点击 **Profiles** 菜单项旁边的 **Create** 按钮，然后选择 Profile 类型。*

修改定制Profile

创建定制 Profile 之后，可以根据需要使用 Configuration 工具来调整该定制 Profile 的设置。如果已将 Profile 与 Real Server 进行关联，则无需再次执行该任务。

◆ **重要信息**

在 Configuration 工具的每个 Profile 创建屏幕中，每个 Profile 设置的右侧都有一个复选框。选中设置的复选框，然后应用该设置的值时，Profile 将保留该值，即使您以后更改了上级 Profile 的相应值。因此，选中设置的复选框可以确保继承过程中，上级 Profile 不会覆盖该值。

修改定制 Profile 设置的步骤

1. 在Main选项卡上，展开**Local Traffic**。
2. 点击**Profiles**。
   将打开“HTTP Profile”屏幕。
3. 找到要修改的Profile类型（服务、持续性、协议、SSL或认证）对应的菜单，然后选择Profile类型。
   此操作将列表显示现有的该类型Profile。
4. 在Name栏中，点击要修改的Profile的名称。
   此操作将显示该Profile的设置与值。
5. 修改或保留所有设置的值：
   - 如果要修改值，请找到相应的设置，点击屏幕右侧Custom栏中的复选框，然后修改值。
   - 如果要保留继承自上级Profile的值，请将设置保持不变，且不要选中Custom栏中的复选框。
   - 如果要将值重新设置回上级Profile的值，请清除屏幕右侧Custom栏中的复选框。
6. 点击**Update**按钮。

实施Profile

针对特定流量类型创建 Profile 之后，通过将该 Profile 与一个或多个 Real Server 进行关联来实施该 Profile。

将某个 Real Server 配置为参考某个 Profile，便可将该 Profile 与该 Real Server 进行关联。只要 Real Server 接收到该类型的流量，LTM 系统便将 Profile 的设置应用到该流量，从而控制其行为。因此，Profile 不仅按网络流量类型定义功能，而且确保 Real Server 可以得到这些功能。

将 Profile 分配给 Real Server 的步骤

1. 在Main选项卡上，展开**Local Traffic**。
2. 点击**Real Servers**。
   此操作将列表显示现有的Real Server。
3. 点击一个Real Server名称。
   此操作将显示该Real Server的属性和设置。
4. 找到要分配的Profile类型的设置，然后选择缺省Profile或定制Profile的名称。
5. 在屏幕底部，点击**Update**。

◆ **注**

也可以在创建 Real Server 时为其分配 Profile。

因为有些特定类型的流量使用多种协议与服务，所以用户通常创建多个 Profile，然后将它们与一个 Real Server 进行关联。例如，客户机应用可能使用 TCP、SSL 和 HTTP 协议与服务来发送请求。因此，此类流量需要基于三种 Profile 类型（TCP、客户机 SSL 和 HTTP）的三个 Profile。

每个 Real Server 都会列出当前与自己关联的 Profile 的名称。使用 Configuration 工具可以从 Profile 列表中添加或删除 Profile。

对于给定的 Real Server，LTM 系统对允许的 Profile 类型组合有着特定的要求。表 5.2 显示了可在 Real Server 上配置的 Profile 类型的特定组合。

Profile类型	**先决Profile**	**不兼容的Profile**
协议Profile		
FastL4	无	全部
TCP	无	UDP和FastL4
UDP	无	FastL4和TCP
OneConnect	TCP	不适用
Stream	TCP	FastL4和UDP
服务Profile		
HTTP	TCP	FTP
FTP	TCP	HTTP、客户机SSL或服务器SSL
SSL Profile		
Client SSL	TCP	FTP
Server SSL	TCP	FTP
持续性Profile		
Cookie	HTTP	不适用
Destination Address Affinity	任意	无
Hash	FastL4、TCP和	不适用

	UDP	
MSRDP	TCP	不适用
SIP	TCP或UDP	FTP
Source Address Affinity	任意	无
SSL	TCP	FTP
Universal	无	不适用
认证Profile		
LDAP	TCP	不适用
RADIUS	TCP	不适用
TACACS+	TCP	不适用
SSL Client Certificate LDAP	TCP	不适用
OCSP	TCP	不适用

***表 5.2** LTM 系统允许和不允许的 Profile 组合*

引导流量时，如果 Real Server 需要其 Profile 列表中没有的特定 Profile 类型，LTM 系统将利用相关的缺省 Profile，将 Profile 自动添加到 Profile 列表。例如，如果客户机应用通过 TCP、SSL 和 HTTP 发送流量，同时您只分配了 SSL 和 HTTP Profile，那么 LTM 系统会自动将缺省 Profile tcp 添加到其 Profile 列表中。

作为最低限度，一个 Real Server 必须参考一个 Profile，且该 Profile 必须与 UDP、FastL4 或 TCPProfile 类型关联。因此，如果没有将 Profile 与 Real Server 进行关联，LTM 系统会自动将 UDP、FastL4 或 TCP 缺省 Profile 添加到 Profile 列表。

LTM 系统选择的缺省 Profile 取决于 Real Server 协议设置的配置。如果协议设置为 UDP，LTM 系统将 udp Profile 添加到其 Profile 列表。如果协议设置为 UDP 之外的其它设置，LTM 系统将 FastL4 Profile 添加到其 Profile 列表。

配置协议Profile的设置

您可以配置的那些 Profile 称为协议 Profile。协议 Profile 的类型包括：

- FastL4
- TCP
- UDP
- OneConnect
- Stream

对于每种协议 Profile 类型，LTM 系统都提供一个带有缺省设置的预配置的 Profile。在大多数情形中，您可以按原状使用这些缺省 Profile。如果要更改这些设置，您可以在创建 Profile 时配置协议 Profile 的设置，也可以在创建之后通过修改 Profile 的设置来进行更改。

以下各节列出了包含在 FastL4、TCP、UDP、OneConnect 和流 Profile 中的流量管理设置。

FastL4 Profile类型

FastL4Profile 的用途是帮助管理第 4 层流量。对于典型的需要，大部分

FastL4Profile 的设置均能满足。您可能希望修改的特定设置包括：**Reset on Timeout**、**Idle Timeout** 和 **PVA Acceleration**。表 5.3 列出并介绍了 FastL4 Profile 类型的设置。

设置	说明	缺省值
Name	此设置为Profile指定一个唯一的名称。	无缺省值
Parent Profile	此设置指定希望用作上级Profile的Profile。您的新Profile从指定的上级Profile中继承所有非定制的设置和值。	**fastL4**
Reset on Timeout	如果启用此设置，且TCP连接超出空闲连接的超时值，LTM系统将删除连接，并发送复位指令。	**Enable**
Reassemble IP Fragments	如果启用此设置，LTM系统将重组IP字段。	**Disable**
Idle Timeout	此设置指定可以删除某个连接之前，该连接空闲的秒数。	**300**
Max Segment Size Override	如果设置为非零的值，此设置将覆盖最大字段尺寸1450。	**0**
PVA Acceleration	此设置指定首选的PVA加速模式。可能的值包括**Full**、**Assisted**或**None**。	**Full**
IP ToS to Client	此设置指定将UDP数据包发送到客户机时，LTM系统为这些数据包分配的服务类型的级别。	**65535**
IP ToS to Server	此设置指定将UDP数据包发送到服务器时，LTM系统为这些数据包分配的服务类型的级别。	**65535**
Link QoS to Client	此设置指定将UDP数据包发送到客户机时，LTM系统为这些数据包分配的服务质量的级别。	**65535**
Link QoS to Server	此设置指定将UDP数据包发送到服务器时，LTM系统为这些数据包分配的服务质量的级别。	**65535**
TCP Timestamp Mode	指定LTM系统应对TCP时间戳执行何种动作。可能的值包括：**Preserve**、**Strip**和**Rewrite**。	**Preserve**
TCP Window Scale Mode	指定LTM系统应对TCP窗口执行何种动作。可能的值包括：**Peserve**、**Strip**和**Rewrite**。	**Preserve**
Generate Internal Sequence	允许LTM系统根据RFC 1984，生成自己的SYN数据包序列号。启用时，此设置允许时间戳循环。	**Disable**
Strip SackOK	允许LTM系统阻止TCP SackOK选项在启动SYN上向服务器进行传递。	**Disable**
RTT From Client	指定LTM系统应使用TCP时间戳选项来衡量到客户机的往返时间。	**Disable**
RTT From Server	指定LTM系统应使用TCP时间戳选项来衡量到服务器的往返时间。	**Disable**

***表5.3** FastL4Profile的设置*

TCP Profile类型

TCP Profile 是用来管理 TCO 网络流量的配置工具。多数 TCPProfile 的设置都是标准的 SYSCTL 类设置，但其它一些是 LTM 系统特有的。

对于绝大多数 TCP Profile 设置，缺省值通常便可以满足您的需要。您可能希望修改的特定设置包括：**Reset on Timeout**、**Idle Timeout**、**IP ToS 和 Link QoS**。表 5.3 列出并介绍了 TCPP rofile 类型的设置。

设置	说明	缺省值

Name	此设置为Profile指定一个唯一的名称。	无缺省值
Parent Profile	此设置指定希望用作上级 Profile 的 Profile。您的新 Profile 从指定的上级 Profile 中继承所有非定制的设置和值。	Tcp
Reset on Timeout	如果启用此设置，且 TCP 连接超出空闲连接的超时值，LTM 系统将删除连接，并发送复位指令。	**Enabled**
Time Wait Cycle	如果在 TIME-WAIT 状态下接收到 SYN 数据包，此设置将循环利用连接。	**Enabled**
Delayed ACKs	如果启用此设置，LTM 系统将允许多个确认（ACK）响应的融合。	**Enabled**
Proxy Maximum Segment	将已与客户机协商的最大字段通知服务器。	**Enabled**
Proxy Options	仅将已与客户机协商的选项（例如时间戳）通知服务器。	**Disabled**
Proxy Buffer Low	指定打开接收窗口的代理缓冲级别。	**4096**
Proxy Buffer High	指定关闭接收窗口的代理缓冲级别。	**16384**
Idle Timeout	此设置指定可以删除某个连接之前，该连接空闲的秒数。	**300**
Time Wait	此设置指定连接进入CLOSED状态之前，处于TIME-WAIT状态的毫秒数。	**2000**
FIN Wait	此设置指定退出连接之前，该连接处于FIN-WAIT或CLOSING状态的秒数。**0**值代表永不退出（或直到FIN状态规定的值）。	5
Close Wait	此设置指定退出连接之前，该连接保持在LAST-ACK状态的秒数。**0**值代表永不退出(或直到FIN状态规定的值)。	5
Send Buffer	此设置令LTM系统发送缓冲区大小（字节数）。	**8192**
Receive Window	此设置令LTM系统接收窗口大小（字节）。	**4096**
Keep Active Interval	此设置令LTM系统将探测间隔保持在激活状态（毫秒）。	**1800**
Maximum SYN Retransmissions	此设置指定LTM系统允许的最大SYN字段重发次数。	4
Maximum Segment Retransmissions	此设置指定LTM系统允许的最大数据字段重发次数。	8
IP ToS	此设置指定将TCP数据包发送到客户机时，LTM系统为这些数据包分配的服务类型的级别。	0
Link QoS	此设置指定将TCP数据包发送到客户机时，LTM系统为这些数据包分配的服务质量的级别。	0

***表5.4** TCPProfile的设置*

UDP Profile类型

UDP Profile 是用来管理 UDP 网络流量的配置工具。表 5.5 列出并介绍了 UDP Profile 类型的设置。

设置	说明	缺省值
Name	此设置为Profile指定一个唯一的名称。	无缺省值
Parent Profile	此设置指定希望用作上级Profile的Profile。您的新Profile从指定的上级Profile中继承所有非定制的设置和值。	Udp
Idle Timeout	此设置指定可以删除某个连接流之前，该连接空闲的秒数。	60
IP ToS	此设置指定将UDP数据包发送到客户机时，LTM系统为这些数据包分配的服务类型的级别。	0
Link QoS	此设置指定将UDP数据包发送到客户机时，LTM系统为这些数据包分配的服务质量的级别。	0

***表5.5** UDP Profile的设置*

OneConnect Profile类型

OneConnect™ Profile 是用于在 LTM 系统上启用连接 Pool 的配置工具。作为 LTM 系统 OneConnect 特性的一个组成部分，连接 Pool 可以优化 LTM 系统处理连接的方式。在 LTM 系统上启用连接 Pool 后，客户机请求便可以利用现有的服务器端连接，从而减少服务器必需打开，以便为那些请求提供服务的服务器端连接数。

LTM 系统可以将多个 Real Server 中的连接纳入 Pool 中，只要那些 Real Server 参考同一个 OneConnect Profile 和同一个 Pool。表 5.5 列出并介绍了 OneConnect Profile 类型的设置。

◆ **提示**

通过实施 OneConnect Profile，您还可以启用 ***OneConnect Transmission*** *特性，此特性来自 HTTP Profile。将* ***OneConnect Transmission*** *设置与 OneConnec Profile 一起使用可以优化连接持续性。*

设置	说明	缺省值
Name	此设置为Profile指定一个唯一的名称。	无缺省值
Parent Profile	此设置指定希望用作上级Profile的Profile。您的新Profile从指定的上级Profile中继承所有非定制的设置和值。	**oneconnect**
Source Mask	LTM系统将此设置的值应用于源地址，以确定是否可以复用。掩码**0**令LTM系统在所有客户机上共享复用的连接。主机掩码（即所有的值均为二进制的**1**）令LTM系统仅共享那些从同一客户机IP地址发起的复用连接。	**0.0.0.0**
Max Size	此设置定义LTM系统在连接复用pool中维持的最大连接数。如果pool已满，服务器端连接将在响应完成后关闭。	**10000**
Max Age	此设置定义允许连接在连接复用pool中存在的最大秒数。对于任何生存时间大于此值的连接，LTM系统会将其从复用pool中删除。	**86400**
Max Reuse	此设置指定服务器端连接可复用的最大次数。	**1000**
Idle Timeout Override	此设置指定可以删除某个连接流之前，该连接空闲的秒数。将连接纳入pool中进行复用时，您可以使用此设置增大超时值。可能的值包括**Disabled**、**Indefinite**或您指定的数值。	**Disabled**

表5.6 *OneConnect Profile的设置*

Stream Profile类型

使用 Stream Profile 可以管理实时流协议（RTSP）连接。RTSP 协议通过 TCP 打开一个控制信道，以便设置和控制流会话。此外，RTSP 协议还会打开一个数据信道（通常是通过 UDP），以便传输流数据。表 5.7 列出并介绍了 Stream Profile 类型的设置。

设置	说明	缺省值
Name	此设置为Profile指定一个唯一的名称。	无缺省值
Parent Profile	此设置指定希望用作上级Profile的Profile。您的新Profile从指定的上级Profile中继承所有非定制的设置和值。	**udp**
Source	指定要搜索的源字符串。	无缺省值

Target	指定要替换的目标字符串。	无缺省值

表5.7 流Profile的设置

管理Profile

使用 Configuration 工具，不仅可以创建和实施 Profile，还可以：

- 查看现有Profile的设置
- 删除Profile
- 查看或重设Profile的统计数据

查看Profile

使用 Configuration 工具可以查看 Profile 的设置与值。

查看 Profile 设置的步骤:

1. 在Main选项卡上，展开**Local Traffic**。
2. 点击**Profiles**。
   将打开Profiles屏幕。
3. 找到要查看的Profile类型（服务、持续性、协议、SSL或认证）对应的菜单，然后选择Profile类型。
   此操作将列表显示现有的该类型Profile。
4. 在Name栏中，点击要查看的Profile的名称。
   此操作将显示该Profile的设置与值。

删除Profile

使用 Configuration 工具可以删除现有的 Profile，只要没有 Real Server 正在参考该 Profile。

删除 Profile 的步骤

1. 在Main选项卡上，展开**Local Traffic**。
2. 点击**Profiles**。
   将打开Profiles屏幕。
3. 找到要查看的Profile类型（服务、持续性、协议、SSL或认证）对应的菜单，然后选择Profile类型。
   此操作将列表显示现有的该类型Profile。
4. 对于一个或多个要删除的Profile，在Select栏中选中它们名称旁的复选框。
5. 点击Delete按钮。
   此操作将显示**Delete Confirmation**屏幕。
6. 确定已选中列表中的所有复选框，然后点击**Delete**按钮将那些Profile永久删除。

通过iRule使用Profile

在有些情形中，管理特定连接类型的最佳方法是创建一个 iRule。例如，希望将一个标头插入 HTTP 请求中，然后基于该标头中的信息来引导请求。

iRule 是用户编写的脚本，用于在特定流量连接符合特定条件时，管理该连接。例如，可以编写一个 iRule，声明如果 HTTP 请求的标头中包含某

个特定的字符串，LTM 系统便应将该请求发送至 Pool http_pool。iRule 中指定的事件发生时，便会触发该 iRule。iRule 事件分为一些特定的类型，例如 TCP、SSL 和 HTTP。仅当 Real Server 的 Profile 列表中包含与 iRule 事件类型对应的 Profile 时，LTM 系统才能在发生该类 iRule 事件时真正地触发 Rule。例如，如果 iRule 指定 HTTP 事件，那么 Real Server 必须参考基于 HTTP Profile 类型的 Profile。

下表显示了可能的 iRule 事件类型及其 Profile 要求。

- **IP事件**
  无Profile要求
- **UDP事件**
  要求基于UDP或FastL4的Profile
- **TCP事件**
  要求基于TCP或FastL4的Profile
- **FTP事件**
  要求基于FTP的Profile
- **HTTP事件**
  要求基于HTTP和TCP的Profile
- **SSL事件**
  要求基于客户机SSL或服务器SSL的Profile，具体取决于iRule的内容
- **AUTH事件**
  要求认证Profile

有关 iRule 事件的详细信息，请参阅第 13 章“编写 iRule”。

6

管理 HTTP 和 FTP 流量

- HTTP和FTP流量管理简介
- 配置HTTP Profile的属性
- 配置HTTP Profile的设置
- 配置HTTP压缩设置
- 配置FTP Profile的设置
- 管理HTTP和FTP Profile

HTTP和FTP流量管理简介

BIG-IP®本地流量管理（LTM）系统提供了多项特性，可帮助您智能地控制 HTTP、HTTPS 和 FTP 流量。比如将标头插入 HTTP 请求中，或者对 HTTP 服务器响应进行压缩。

其中一些特性可以通过配置 HTTP 或 FTP 的 Profile 来实现。***Profile*** 是一组带有数值设置信息，对应于一种具体的流量类型，比如 HTTP 流量。Profile 定义了您希望 LTM 系统管理该流量类型的方式。

除了 HTTP 和 FTP Profile 以外，LTM 系统还有其它可以帮您管理应用流量的特性。比如状态监控器可以检查 HTTP 和 FTP 服务的状态，而 iRules™ 则用于查询或处理 HTTP 标头或内容数据。

表 6.1 总结了 LTM 系统管理 HTTP 和 FTP 流量的能力，并为您呈现了用于配置每种特性的 LTM 对象。

特性	说明	配置对象
HTTP compression	您可以创建一个HTTP Profile，以引发LTM系统使用完全定义的算法（如**gzip和deflate**）来压缩服务器响应。	HTTP Profile
Monitoring of HTTP, HTTPS and FTP ports on pool members	您可以将HTTP、HTTPS或FTP监控器与Pool成员进行连接，以确保Pool成员能够随时接受具体端口上的流量。	Load balancing pool HTTP、HTTPS和FTP health monitors
Header insertion and deletion	您可以在HTTP请求中插入标头，或者从HTTP标头中删除内容。	HTTP Profile与iRule
Session persistence	您可以确保HTTP会话在跨越多个连接之后仍然支持同一个Pool成员。	Persistence Profile与iRule
Header and content inspection and modification	用户可以通过编写一个iRule来检查或修改HTTP请求或响应的内容。	iRule
Redirection of HTTP requests	通过配置HTTP Profile或编写iRule，您可以指导LTM系统来根据URI、状态代码或内容来重定向HTTP流量。	HTTP Profile与iRule
Pooling connections	您可以通过配置LTM系统，使多个客户机连接都能重新使用同一空闲服务器端连接。您还可以配置LTM系统来重写HTTP连接标头，以确保连接保持打开状态。	OneConnect Profile
Chunking of requests and reponses	您可以通过配置LTM系统来解除中继或重新中继HTTP响应。	HTTP Profile
Pipelining	LM系统支持HTTP流水线技术。	HTTP Profile
IPV4-to-IPV6 compatibility	确保使用FTP协议时，使用IP第4版和IP第6版的客户机和服务器能够相互兼容。	FTP Profile

***表6.1** LTM系统与HTTP和FTP流量控制相关的特性总结*

配置HTTP Profile的属性

您可以配置 HTTP Profile 的设置，以确保 HTTP 流量管理能够满足您的具体要求。这些配置的设置情况可分为三类，并且显示在配置工具中的新 HTTP Profile 屏幕上：常规属性、设置和压缩。您可以在创建 Profile 时配置这些设置，或者创建 Profile 之后修改 Profile 设置。关于配置 Profile 的具体流程，请参阅第 5 章“了解 Profile”。

表 6.2 显示的是常规属性，也就是名称和上级 Profile，可帮助指定定制的 HTTP Profile。该表下面是这些常规属性的描述。有关 HTTP Profile 设置的信息，请参阅 6-4 页“配置 HTTP Profile 的设置”，有关压缩设置的信息，请参阅 6-11 页“配置 HTTP 压缩设置”。

常规属性	说明	缺省值
Name	详细说明用户提供的Profile的名称。您必须为您的Profile指定一个名称。	无缺省值
Parent Profile	需要指定从您的定制Profile中衍生出来的Profile。	**http**

***表6.2** HTTP Profile的常规属性*

在配置 HTTP Profile 之前，先对其常规属性做出必要的说明将会很有帮助。

指定Profile的名称

在创建 HTTP 配置时，必须为 Profile 指定一个唯一的名称。**Name** 设置是您在创建 HTTP Profile 时必须主动赋值的两项设置之一；所有其它设置都有缺省值。

指定 Profile 名称时，只需简单地定位 **Name** 设置并为 Profile 输入一个独特的名称即可。

指定一个上级Profile

您创建的每个 Profile 都是从一个上级 Profile 衍生而来的。您可以使用缺省 **HTTP Profile** 作为上级 Profile，或者使用另一个已经创建的 HTTP Profile。

指定上级 Profile 时，需要定位该 **Parent Profile** 的设置，并选择一个 Profile 名称。

配置HTTP Profile的设置

对于在 HTTP Profile 设置屏幕上出现的 Profile 设置，您可以在没有数值是指定一个值，或者可以修改任何缺省值来满足您的具体需要。有关其它 HTTP Profile 设置的信息，请参阅 6-3 页“配置 HTTP Profile 的属性”和 6-11“配置 HTTP 压缩设置”。

表 6.3 显示了这些 Profile 设置。对于那些含有缺省值的设置，可以保留或修改这些缺省设置。该表格的下面是设置说明和修改设置的流程。

设置	说明	缺省值
Basic Auth Realm	为客户机身份验证指定一个认证范围。	无缺省值
Fallback Host	当所有结点都停机时指定返回主机发送HTTP 302响应。	无缺省值
Header Insert	指定您希望在HTTP请求中插入的标头字符串。	无缺省值
Header Erase	指定您希望从HTTP请求中删除的标头字符串。	无缺省值
Response Chunking	规定如何对HTTP响应进行中继。可能的值为**Unchunk**、**Retrunk**、**Select**和**Preserve**。	**Preserve**
OneConnect Transmissions	执行HTTP标头转换，以保持连接的开放状态。此特性需要配置One Connect™ Profile。	**Disabled**
Redirect Rewrite	允许您修改HTTP重定向。可能的值为**Matching**、**All**、**Nodes**或**None**。	**无**
Maximum Header Size	指定LTM系统允许HTTP标头的最大尺寸。缺省值用字节表示。	**16**
Pipelining	启用或禁用HTTP流水线技术。	**Disabled**
Insert **XForwarded-For**	指定一个可以供LTM系统在HTTP请求中插入的**XForwarded-For**标头，以便与连接Pool使用。此特性可以将客户机的IP地址作为**XForwarded-For**标头的值进行添加。	无缺省值
LWS Maximum Columns	指定在HTTP请求中插入的HTTP标头的最大宽度限制。	**80**
LWS Separator	指定当标头超过最大宽度限制时LTM系统应该在HTTP标头之间使用的分隔符。	**\r\n**
Pipelining	启用或禁用HTTP流水线技术（HTTP第1.1版的一个特性）。	**Disabled**

***表6.3** HTTP Profile中的配置设置*

在配置 HTTP Profile 之前，先对需要修改的特定设置做出必要的说明将会很有帮助。

指定一个基本认证范围

Basic Auth Realm 设置中的值是一个由您提供的字符串。LTM 系统会将此字符串作为客户机认证的一部分发送至客户机。

配置此设置时，需要找到 **Basic Auth Realm** 设置，然后为其输入一个值。

指定一个返回主机

HTTP 重定向是另一个您可以对 HTTP Profile 进行设置的特性。***HTTP 重定向***允许您将 HTTP 流量重新定向至另一个协议标识符、主机名称、端口号或 URI 路径。例如，如果目标 pool 的所有成员均不可用（也就是说，成员均禁用，标记为 **down**，或者超过了连接限制），则 LTM 系统可以将 HTTP 请求重定向至返回主机，HTTP 回复状态代码为 **302 Found**。

在配置 LTM 系统将 HTTP 流量重定向至返回主机时，您可以指定 IP 地址或完全合格的域名（FQDN）。您指定的值将成为服务器在响应中发送的 **Location** 标头的值。例如，您可以将一个重定向指定为 **http://redirector.siterequest.com**。

在HTTP请求中插入标头

HTTP 标头插入是 HTTP Profile 中的一个可选设置。被插入的 HTTP 标头可以包括一个客户机 IP 地址。当一个连接通过安全网络地址转换（SNAT）

而您需要保留原客户机 IP 地址的时候，HTTP 标头中包含客户机 IP 地址将会非常有用。

您插入的标头的格式通常是用引号将字符串括起来。此外，在能够动态解析为理想值的标头中，您还可以插入工具命令语言（TCL）表达式。在向 Real Server 分配已配置的 HTTP Profile 时，LTM 系统会将 Profile 中指定的标头插入 LTM 系统，并发送给 pool 或 Pool 成员的任何 HTTP 请求中。

注

除在 HTTP 请求中插入一个字符串（如一个客户机 IP 地址）之外，您还可以通过配置 LTM 系统，在 HTTP 请求中插入 SSL 相关标头。例如：客户机证书、密码规范和客户机会话 ID。如果希望插入此类标头，您必须创建一个 iRule。有关使用 iRule 命令来执行标头插入的详细信息，请参阅第 13 章 ***"编写 iRule"****。*

在 HTTP 请求中插入标头时，需要找到 **Header Insert** 设置，然后为其输入一个值。

删除HTTP标头中的内容

另一项可选设置是 **Header Erase** 设置。使用此设置，您可以配置一个 pool 来删除 HTTP 客户机请求标头中的内容。当您使用这一设置时，LTM 系统可以删除指定标头的内容并将内容更换为空白。标头本身保持不变。

凭借这一特性，您可以在通过网络转发请求之前删除 HTTP 请求标头中的内容。这样的标头可能包括重要信息，如用户 ID 或电话号码，必须在转发信息之前删除。

带有需要删除的内容的客户机标头必须指定为用引号括起来的字符串。

删除 HTTP 请求中的标头时，需要找到 **Header Erase** 设置，然后为其输入一个值。

配置中继

您有时可能希望检查和/或修改 HTTP 应用数据，比如当使用 iRule 检查 HTTP 响应内容的时候。这样的检查或修改需要响应进行***解除中继***，也就是使该响应不在中继编码（chunked encoding）内。使用 **Response Chunking** 设置，LTM 系统在执行响应要求的行动前可以将已经中继的响应解除。

此设置的可能值为 **Unchunk**、**Retrunk**、**Selective** 和 **Preserve**。缺省值为 **Preserve**。

表 6.4 描述了 LTM 系统针对原始响应被中继或被解除中继的情况所使用的值和采取的行动。

设置	原始响应已被中继	原始响应已被解除中继
Unchunk	LTM系统可以解除对响应的中继并处理HTTP内容，然后将该响应以解除中继的状态进行传递。当所有数据都发送至	LTM系统处理HTTP内容，并按照原样传

设置	原始响应已被中继	原始响应已被解除中继
	Connection: Closed标头设置中规定的客户机时，连接就会关闭。	递响应。
Retrunk	LTM系统解除对响应的中继，处理HTTP内容、重新添加中继标尾的标头，然后作为中继响应继续传递。任何中继扩展被丢失。	LTM 系统在输出时添加传输编码和中继标头。
Selective	与**Retrunk**相同	LTM系统处理HTTP内容，并按照原样传递响应。
Preserve	LTM系统保持响应的中继状态，处理HTTP内容，并按照原样传递响应。注意即使启用了HTTP压缩，LTM系统也不会压缩响应。	LTM系统处理HTTP内容，并按照原样传递响应。

***表6.4** LTM系统的整合行为*

启用或禁用OneConnect转换

这一设置可以启用或禁用部分 OneConnect™特性。启用之后，此种设置会根据 HTTP/1.0 请求来执行 HTTP **Connection** 标头转换，以便实施 **Keep-Alive** 功能，支持持续性连接。这样，当客户机发送的 HTTP/1.0 请求带有 **Connection**:**Close** 标头时，此特性可通过把标头转换为 **Connection: Keep-Alive** 来迫使连接保持开放状态。

此设置的缺省值为 **Disabled**。

◆ **重要信息**

*为了支持此设置，您还必须支持 OneConnect™特性的连接 Pool 组件。通过配置 OneConnect Profile 可以支持连接 Pool。有关连接 Pool 和配置 OneConnect Profile 的详细信息，请参阅第 5 章“**了解 Profile**”。*

有关 OneConnect™特性的一般信息，请参阅第 1 章“本地流量管理简介”。

启用 OneConnect 转换时，需要找到 **OneConnect Transmissions** 设置及其复选框。

重写HTTP重定向

客户机请求有时会从 HTTPS 协议重定向至 HTTP 协议，但这并不是一个安全的通道。如果您希望确保请求保留在一个安全通道中，您可以重写重定向，将其重新定向回 HTTPS 协议。

注意重写任何重定向时，只能针对那些重定向响应的 HTTP **Locations** 标头，不能涉及重定向的内容。

为了使 LTM 系统重写 HTTP 重定向，您只需通过配置工具来指定您希望系统在重写期间处理的 URI 即可。启用之后，此特性可以重写协议名称和端口号

此设置可能的值为 **Matching**、**All**、**Nodes** 或 **None**。

选择URI进行重写

在配置 LTM 系统重写 HTTP 重定向时，您可以规定系统是应该根据最初客户机的请求仅重写这些 URI 来匹配 URI（去掉可选托尾斜杠），还是应该重写所有的 URI。如果选择后者，则系统总是重写 redirected-to URI，而重写这些 URI 则假设它们符合最初请求的 URI。

如果 URI 包含一个节点 IP 地址而不是主机名称的话，您可以配置 LTM 系统来改变指向 Real Server 地址的 IP 地址。

表 6.5 展示了当 LTM 系统在端口 **443** 上听到内容而 **Rewrite Redirections** 设置为启用的时候，如何转换客户机请求重定向的范例。

原始重定向	重定向重写
http://www.myweb.com/myapp/	**https://www.myweb.com/myapp/**
http://www.myweb.com:8080/myapp/	**https://www.myweb.com/myapp/**

表6.5 *当系统在端口**443**上听内容时重写HTTP重定向的范例*

表 6.6 展示了当 SSL 代理在端口 **4443** 上听到内容而重写特性设置为启用的时候，如何转换客户机请求重定向的范例。

原始重定向	重定向重写
http://www.myweb.com/myapp/	**https://www.myweb.com:4443/myapp/**
http://www.myweb.com:8080/myapp/	**https://www.myweb.com:4443/myapp/**

表6.6 *当系统在端口**4443**上听内容时重写HTTP重定向的范例*

重写协议名称

在配置重写 HTTP 重定向时，LTM 系统将 HTTP 协议名称重写为 HTTPS。例如，客户机可能发送请求至 **https://www.sample.com/bar**，然后被开始重定向至 **http://www.sample.com/bar/，但这不是一个安全的通道。**如果您希望客户机请求保留在安全通道中，您可以配置 LTM 系统来重写重定向 URI，转到 **https://www.sample.com/bar/**。（注意增加托尾斜杠。）

指定最大标头尺寸

通过这一设置，您可以指定 LTM 系统允许 HTTP 标头的最大尺寸限制。缺省值为 **16**，用字节表示。

启用流水线技术支持

通常情况下，客户机必须等到上一个请求收到响应才能再次提出请求。HTTP/1.1 流水线技术可使客户机即使在上一个请求没有收到响应的情况下也可以发出请求。然而，如果想做到这一点，目的地服务器必须支持流水线技术。此特性也可以在 LTM 系统上进行支持。

启用流水线技术时，需要找到 **Pipelining** 设置并选中复选框。此特性缺省设置为 **Disabled**。

插入XForwarded For标头

使用连接 Pool 的时候客户机可以使用现有服务器端连接，此时您可以插入 **XForwarded For** 标头并指定客户机 IP 地址。当您配置 LTM 系统插入此标头时，目标服务器可以识别来自任何客户机（而不仅限于发起连接请求的客户机）的请求。

配置linear white space的最大列数

此设置可为插入 HTTP 请求中的标头指定最大列数。

配置 **LWS Maximum Columns** 设置时，只需指定一个最大值即可。

配置linear white space分隔符

此设置可以指定当标头超过 **LWS Maximum Columns** 设置中规定的最大宽度时，LTM 系统应该用在 HTTP 标头之间的分隔符。

配置 **LWS Separator** 设置时，只需为分隔符赋值即可。

配置HTTP压缩设置

在典型的客户机服务器环境中，可以对浏览器和服务器进行配置，以便压缩和解压缩 HTTP 内容。HTTP 压缩可以减少需要传输的数据量，从而明显降低带宽的使用率。下面两个章节主要说明配置 LTM 系统使其执行 HTTP 压缩任务，将会带来哪些优势。

典型客户机服务器环境中的压缩

当在客户机服务器环境中启用 HTTP 压缩时，浏览器会在客户机请求中插入一个 **Accept-Encoding** 标头。该标头指定了浏览器能够理解的压缩方法。然后，服务器读取标头并使用其中一种压缩方法来压缩响应主体。然后服务器在响应中插入 **Content-Encoding** 标头，说明服务器采用的浏览器压缩方法。收到经过压缩的响应之后，浏览器将会读取 **Content-Encoding** 标头并相应地压缩数据。如果没有 LTM 系统，启用 HTTP 压缩通常需要在目的地服务器上安装和配置压缩软件。

使用LTM系统进行压缩

LTM 系统从目标服务器上卸载 HTTP 压缩任务的能力是一种可选特性。在 LTM 系统上配置 HTTP 压缩时的所有任务，以及压缩软件本身都集中在了 LTM 系统上。

启用 HTTP 压缩选项的主要途径是，将 HTTP Profile 的 **Compression** 设置设为 **Enabled**。这样，LTM 系统可以为符合您在 HTTP Profile 的 **Request-URI** 或 **Content-Type** 设置中规定的值的任何响应，来压缩 HTTP 内容。

如果希望为某些特定的连接启用 HTTP 压缩功能，您可以编写 iRule，并指定 **HTTP:compress enable** 命令。有关更多详细信息，请参阅第 13 章“配置负载平衡 Pool”。

当 LTM 系统能支持 HTTP 压缩的时候，LTM 系统将执行一系列步骤：

1. 首先，LTM系统读取客户机请求的**Accept-Encoding**标头，查看**deflate**或**gzip**压缩方法的规范，并提示哪种方法标记为优先使用。
2. 如果HTTP Profile中**Keep Accept Encoding**设置为**Disabled**，则LTM系统将从请求中移除**Accept-Encoding**标头，然后将请求传输到服务器上。移除**Accept-Encoding**标头可以阻止服务器执行HTTP压缩和在响应中插入**Content-Encoding**标头。
3. 接收服务器响应之后，LTM系统就会插入**Content-Encoding**标头，指定已经选中的压缩方法。LTM系统通过查看客户机请求的**Accept-Encoding**标头中的**gzip**或**deflate**压缩方法规范，来选择压缩方法。如果客户机请求不能指定压缩方法，则LTM系统将使用**deflate**方法来压缩响应数据。
4. 最后，LTM系统将对响应进行压缩并发送给客户机。然后客户机读取响应中的**Content-Encoding**标头，确定所使用的压缩方法，并相应地解压数据。

使用LTM 系统 HTTP 压缩特性，您可以加入或排除您指定的特定类型 URI 或文件。这一点非常实用，因为一些 URI 或文件类型可能已经进行了压缩。使用 CPU 资源来压缩已经压缩的数据并不是明智的选择，因为压缩数据的成本通常会超过其所带来的优势。您可能希望规定排除的常规表达式为**.*.pdf** 或**.*.gif**。

表 6.7 显示了您在 HTTP Profile 中可以指定的压缩设置。配置这些设置意味着为没有缺省值的项目指定一个值，或者更改缺省值。

设置	说明	缺省值
Compression	启用或禁用HTTP压缩特性。	**Disable**
URI Compression	显示加入或排除特定**Request-URI**响应的设置。可能的值为**URI List**或**Not Configured**。	**Not Configured**
URI List	如果**URI Compression**设置为**Enabled**，则需要指定压缩目标的URI，和URI压缩中加入和排除的响应类型。	无缺省值
Content Compression	显示加入或排除特定**Content-Type**响应的设置。可能的值为**Content List**或**Not Configured**。	**Not Configured**
Content List	如果**Content Compression**设置为**Enabled**，则需要指定压缩的目标内容类型，和内容压缩中加入和排除的响应类型。	在**Include List**框中，默认值为： **text/** **application/(xml|x-javascript)**
Minimum Content Length	指定服务器响应的最小字节长度，应该符合压缩响应的可接受范围。字节长度仅适用于内容长度，不包括标头。	**1024**
Compression Buffer Size	指定LTM系统缓冲压缩字节的最大数量，然后决定是否在指定压缩尺寸的响应中插入**Content-Length**标头。	**4096**
gzip Memory Level	指定压缩服务器响应时LTM系统用于内部压缩缓冲的内存千字节数量。	**8**

设置	说明	缺省值
gzip Window Size	指定压缩服务器响应时LTM系统使用的窗口尺寸中的千字节数量。	**16**
gzip Level	指定压缩的数量和速度。	**1**
Vary Header	启用或禁用在使用高速缓存的服务器响应中插入一个Vary标头。	**Enabled**
HTTP/1.0 Requests	启用或禁用HTTP/1.0客户机请求响应压缩。	**Disabled**
Keep Accept Encoding	启用之后，允许目标服务器而不是LTM系统执行HTTP压缩。	**Disabled**

表6.7 *HTTP压缩的可配置设置*

在配置 HTTP Profile 之前，先对需要更改的压缩设置做出必要的说明将会很有帮助。

启用或禁用压缩特性

Compression 设置可以支持 LTM 系统在服务器响应上执行压缩。可能的值包括：

- **Enabled**
  使用这个值，LTM系统可以为符合您在HTTP Profile的**URI List**或**Content List**设置中规定的值的任何响应，来压缩、或阻止压缩HTTP服务器内容。
- **Disabled**
  当**Compression**设置为**Disabled**时，LTM系统不能执行HTTP压缩。
- **Selective**
  在指定了包含**HTTP::compress**命令的iRule之后，这一设置将带动LTM系统单纯执行HTTP压缩。

启用 HTTP 压缩时，需要找到 **Compression** 设置并选择 **Enabled**。如果您通过使用 iRule 命令 **HTTP::compress <enable>**来启用压缩，应该选择 **Selective**。

使用URI压缩

在启用压缩功能之后，您可能不希望 LTM 系统压缩所有类型的服务器响应。使用 **URI Compression** 设置，可以把它的值设为 **URI List**，这样可以指导 LTM 系统将客户机请求的 URI 中所指定的响应加入压缩任务，或者从压缩任务中排除。

您甚至可以输入常用表达式，以指定您希望 LTM 系统加入到压缩任务的服务器响应类型，或希望从压缩任务中排除的响应类型。例如，您可以通过输入常规表达式**.*.htm** 来指定您希望 LTM 系统压缩所有**.htm** 响应。然后 LTM 系统将这个响应类型与每个客户机请求中指定的 URI 进行比较，如果系统发现符合要求，则会采取相应措施。

您指定的任何常规表达式必须采用 Advanced Regular Expression（ARE）语法。

使用 URI 压缩特性时，需要找到 **URI Compression** 设置，并选择 **URI List**。然后您可以使用 **Include List** 框或 **Exclude List** 框来输入常规表达

式。如果您不指定任何列表（URI 或内容），则 LTM 系统将压缩所有响应。有关内容列表的详细信息，请参阅 6-15 “使用内容压缩”。

在HTTP压缩中加入具体的URI响应

当 **URI Compression** 设置启用之后，您可以在 **Include List** 中输入一个或多个值，LTM 系统仅压缩这些符合客户机请求命令行 URI 部分的响应。

您在 **Include List** 中指定的值应该采用常规表达式的形式。例如，如果 **Include List** 框包括**.*.txt**、**.*.htm** 和**.*.html** 等值，而这些表达式与客户机请求中的 URI 相匹配，则 LTM 系统仅压缩带有符合具体常规表达式的 URI 的响应。

为了成功地应用这一设置，LTM 系统必须在 **Include List** 框中发现至少一个指定的值匹配才可以操作。如果 LTM 系统没有发现匹配结果，则不会压缩任何响应。

在HTTP压缩中排除具体的URI响应

当 **URI Compression** 设置启用之后，您可以在 **Exclude List** 中输入一个或多个值，LTM 系统会将这些符合客户机请求命令行 URI 部分的响应排除在压缩任务之外。

您在 **Exclude List** 中指定的值应该采用常规表达式的形式。例如，如果 **Exclude List** 框包含**.*.pdf** 值，而表达式匹配客户机请求中的 URI，则 LTM 系统会将匹配这些 URI 的任何**.pdf** 响应排除在压缩任务之外。

为了成功地应用这一设置，LTM 系统必须在 **Exclude List** 框中发现至少一个指定的值匹配才可以操作。如果 LTM 系统没有发现匹配结果，则不会从压缩中排除任何响应。

使用内容压缩

在启用压缩功能之后，您可能不希望 LTM 系统压缩所有类型的服务器响应。使用 **URI Compression** 设置，可以把它的值设为 **Content List**，这样可以指导 LTM 系统将服务器请求的 **Content-Type** 标头中所指定的响应加入压缩任务，或者从压缩任务中排除。

您甚至可以输入常用表达式，以指定您希望 LTM 系统加入到压缩任务的服务器响应类型，或希望从压缩任务中排除的响应类型。例如，您可以通过输入常规表达式**.*.htm** 来指定您希望 LTM 系统压缩所有**.htm** 响应。然后 LTM 系统将这个响应类型与每个服务器响应中指定的 **Content-Type** 标头进行比较，如果系统发现符合要求，则会采取相应措施。

您指定的任何常规表达式必须采用 Advanced Regular Expression（ARE）语法。

使用内容压缩特性时，需要找到 **Content Compression** 设置，并选择 **Content List**。然后您可以使用 **Include List** 框或 **Exlcude List** 框来输入常规表达式。如果您不指定任何列表（URI 或内容），则 LTM 系统将压缩所有响应。有关内容列表的详细信息，请参阅 6-14“使用 URI 压缩”。

在HTTP压缩中加入内容类型响应

当您启用了压缩并在 **Include List** 框中指定了一个或多个值之后，LTM 系统将仅包含那些与服务器的 **Content-Type** 标头相匹配的响应。这一设置的值是由这些标头的值组成的列表。例如，如果 **Include List** 框包括 **application/pdf** 和 **image/****等值，则只有包含这些内容类型的响应会被压缩。

为了包含所有文本类型，您可以为这个设置赋值为 **text/.***。

在HTTP压缩中排除内容类型响应

当您启用了压缩并在 **Exclude List** 框中指定了一个或多个值之后，LTM 系统将仅排除那些与服务器的 **Content-Type** 标头相匹配的响应。这一设置的值是由这些标头的值组成的列表。例如，如果 **Exclude List** 框包括 **application/pdf** 和 **image/****等值，则只有包含这些内容类型的响应会被排除在压缩任务之外。

为了排除所有文本类型，您可以为这个设置赋值为 **text/.***。

为压缩指定最小内容长度

启用压缩后，LTM 系统可以通过 **Minimum Content Length** 设置，对字节未被压缩的服务器响应规定其最小长度。LTM 系统在服务器响应的 **Content-Length** 标头中查找服务器响应的内容长度信息。这样，如果响应标头中指定的内容长度低于 **Minimum Content Length** 设置中的赋值，则 LTM 系统就不会压缩该响应。字节长度仅指内容长度，不是指标头。

例如，使用缺省值 **1024**，LTM 系统仅压缩那些 HTTP 内容包含至少 1024 个字节的响应。有时候 **Content-Length** 标头并不代表响应的内容长度。在这种情况下，LTM 系统会不考虑大小，统一压缩响应。

指定最小内容长度时，需要找到 **Minimum Content Length** 设置，并为其输入一个数值。

指定压缩缓冲尺寸

启用压缩后，**Compression Buffer Size** 设置将指定 LTM 系统缓冲压缩字节的最大数量，然后决定是否保留 **Keep-Alive** 连接并重写 **Content-Length** 标头。

例如，使用缺省值 **4096**，在决定是否保留连接和重写**内容长度**标头之前，LTM 系统缓冲的压缩数据高达 4096 个字节。

LTM 系统根据响应中继的启用情况来决定是否重写 **Content-Length** 标头（使用 **Response Chunking** Profile 设置）。表 6.8 显示了 LTM 系统对于压缩缓冲尺寸和响应中继的行为。

如果被压缩响应的尺寸	而被压缩的响应	则LTM系统

如果被压缩响应的尺寸	而被压缩的响应	则LTM系统
等于或超过最大缓冲尺寸	已被中继	保持连接的开放状态（如果连接标头没有设置为关闭）。
	未被中继	通过将连接标头的值改为关闭来关闭连接。
小于最大缓冲尺寸	以被中继	不会插入带有压缩响应尺寸的内容长度标头。
	未被中继	插入带有压缩响应尺寸的内容长度标头。

***表6.8** LTM系统根据最大缓冲尺寸做出的行为*

有关更多详细信息，请参阅前面的“为压缩指定最小内容长度”。

指定压缩缓冲尺寸时，只需找到 **Compression Buffer Size** 设置，并输入一个数值。

指定gzip压缩的内存级别

gzip Memory Level 设置规定了一个值，代表在使用 **gzip** 或 **deflate** 压缩方法时，LTM 系统用于压缩数据的内存千字节的数量。**gzip Memory Level** 设置的值必须是 **1** 至 **256** 之间的 2 的整数被倍，以字节表示。

通常，更大的数值会促使 LTM 系统使用更多内存，但结果是压缩的速度更快，比率更高。相反，更小的数值会促使 LTM 系统使用更少的内存，但结果是压缩的速度更慢，比率更低。缺省值为 **8**。

指定内存级别时，只需定位 **gzip Memory Level** 设置并选择一个数值即可。

为gzip压缩指定窗口尺寸

gzip Window Size 设置规定了一个值，代表在使用 **gzip** 或 **deflate** 压缩方法压缩服务器响应时，LTM 系统用在窗口尺寸中的千字节的数量。**gzip Window Size** 设置的值必须是 **1** 至 **128** 之间的 2 的整数倍。

通常，更大的数值会促使 LTM 系统使用更多内存，但结果是压缩的比率更高。相反，更小的数值会促使 LTM 系统使用更少的内存，但结果是压缩的比率更低。缺省值为 **16**。

指定窗口尺寸时，只需找到 **gzip Window Size** 设置，并选择一个数值。

指定一个压缩级别

使用 **gzip Level** 设置，您可以指定数据压缩的程度和压缩比率。

- 指定更高级别可以压缩更多数据，但是比率更低。
- 指定更低级别压缩的数据更少，但是比率更高。

允许的值是 **1** 到 **9** 之间的任何整数。缺省的压缩级别为 **1**。

启用或禁用Vary标头

启用压缩之后，**Vary Header** 设置将把 **Vary:Accept-Encoding** 标头插入已经压缩的服务器响应中。如果响应中已经存在 **Vary** 标头，LTM 系统会为标头添加 **Accept-Encoding** 这个值。

之所以要在服务器响应中插入 **Vary: Accept-Encoding** 标头，主要是我们接受了 RFC2616 的意见，即 **Vary** 标头应该插入到任何以服务器的协商情况而进行高速缓存处理的响应中。基于 HTTP 压缩的服务器响应就属于此类。

如果 **Vary Header** 设置被禁用，LTM 系统不能在服务器响应中插入 **Vary** 标头。

如果禁用 Vary 标头，则需要定位 **Vary Header** 设置并取消选择 **Enabled** 框。

支持面向HTTP/1.0请求的压缩

包含 **HTTP/1.0 Requests** 设置可支持后向兼容性，使 HTTP 压缩能够响应 HTTP/1.0 客户机请求。此设置的缺省值为 **Disabled**。

如果此设置为 **Enabled**，则 LTM 系统仅在下列条件下才压缩响应：

- 当服务器响应**Connection:close** 标头的时候
- 当响应内容没有超过**Compession Buffer Size**设置的时候

启用 HTTP/1.0 请求的压缩时，定位 **HTTP/1.0 Requests** 设置并选中复选框即可。

保持Accept-Encoding标头

通常，当您启用 HTTP 压缩的时候，LTM 系统将从 HTTP 请求中取出 **Accept-Encoding** 标头。这样将促使 LTM 系统而不是目标服务器来执行 HTTP 压缩。

Keep Accept Encoding 设置缺省值为禁用。如果您希望允许目标服务器而不是 LTM 系统来执行 HTTP 压缩的话，只需启用这一设置即可。

配置FTP Profile的设置

您可以定制 FTP Profile 设置以满足您的具体需要。对于那些含有缺省值的设置，您可保留或者修改这些缺省设置。您也能够在创建 Profile 时，或者创建 Profile 以后随时修改设置。有关配置 Profile 的具体流程，请参阅第 5 章“了解 Profile”。

表 6.9 列举出这些可配置的设置，以及每个缺省值的简短说明。该表下面是具体设置的描述。

常规属性	说明	缺省值
Name	指定用户提供的Profile的名称。必须为您的Profile指定一个名称。	无缺省值
Parent Profile	需要指定从您的定制Profile中衍生出来的Profile。	**FTP**
Translate Extended	确保在使用FTP协议时IP第4版和IP第6版客户机和服务器之间的兼容性。	**Enabled**
Data Port	支持FTP服务在冗余端口上运行。	**20**

表6.9 FTP Profile的设置

在配置 FTP Profile 之前，说明您可能需要更改的特定节点设置是非常有帮助的。

指定一个Profile名称

为了创建 FTP Profile，您必须为 Profile 指定独一无二的名称。**Name** 设置是您创建 FTP Profile 时必须主动赋值的两项设置之一；所有其它设置都有缺省值。

指定一个上级Profile

您创建的每个 Profile 都是从上级 Profile 衍生而来的。在 Parent Profile 设置中，您可以选择缺省 FTP Profile 作为上级 Profile，或者您可以选择另一个您已经创建的 FTP Profile。

指定一个Translate Extended值

由于 IP 第 6 版的地址没有限制在 32 位之内（与 IP 第 4 版的地址不同），因此在混合 IP 版本配置中使用 FTP 时会出现兼容性问题。

Translate Extended 设置缺省值为 Enabled，当客户机服务器配置同时包含 IP 第 4 版和 IP 第 6 版系统时，会造成 LTM 系统自动转换 FTP 命令。例如，如果运行 IP 第 4 版的客户机系统向运行 IP 第 6 版的服务器发送 FTP **PASV** 命令，LTM 系统会将 **PASV** 命令自动转换为支持 IP 第 6 版系统的对等 FTP 命令——**EPSV**。LTM 系统也采用此方式转换 FTP 命令 **EPRV** 和 **PORT**。

您不太可能需要更改此设置的缺省值（**Enabled**）。您希望禁用这一设置的唯一情况就是向使用 IP 第 4 版发送 **EPSV** 命令的时候，如测试 FTP 服务器的时候。

指定一个数据端口

数据端口设置可允许 FTP 服务在冗余端口上运行。您可以使用缺省端口号 **20**，或指定另一个端口号。

管理HTTP和FTP Profile

使用配置工具，您可以浏览 HTTP 和 FTP Profile 并删除您已经创建的任何定制 Profile。但是请注意您不能删除缺省 Profile**http** 和 **ftp**。

有关创建和修改 SSL Profile 的流程，请参阅第 5 章“了解 Profile”。

浏览 HTTP 或 FTP Profile 的步骤

1. 在Main选项卡上，展开**Local Traffic**。
2. 点击**Profiles**。
   Profiles屏幕打开。
3. 从**Services**菜单中选择**HTTP**或**FTP**。

这样可以显示任何现有的HTTP或FTP Profile列表。

4. 在Name栏内，点击您希望浏览的Profile的名称。

删除 HTTP 或 FTP Profile 的步骤

1. 在Main选项卡上，展开**Local Traffic**。
2. 点击**Profiles**。
   Profiles屏幕打开。
3. 从**Service**菜单中选择**HTTP**或**FTP**。
   这样可以显示任何客户机端或服务器端Profile的列表。
4. 选中您希望删除的定制Profile左侧的Selective框。
5. 点击**Delete**。
   出现确认屏幕。
6. 点击**Delete**。

7

管理 SSL 流量

- SSL流量管理简介
- 管理密钥和证书
- 了解SSL Profile
- 配置SSL Profile的常规属性
- 对配置的设置进行配置
- 配置客户机或服务器认证设置
- 管理SSL Profile

SSL流量管理简介

BIG-IP®本地流量管理（LTM）系统提供若干可用于智能控制 SSL 流量的特性。其中一些 SSL 流量管理特性如下：

- 能够对客户机和服务器进行认证，以维持客户机系统和BIG-IP系统之间，以及BIG-IP系统和目标Web服务器之间的安全连接
- 能够从客户机和服务器系统中卸载SSL证书验证任务
- iRule命令，这些命令提供插入标头和重新引导HTTP等特性
- 支持在线证书状态协议（OCSP），以便获得最新的证书撤销状态
- 使用小型目录访问协议（LDAP）服务器进行基于证书的客户机授权

得以控制SSL网络流量的主要方法是配置客户机或服务器的SSL Profile。***Client Profile*** 是一种流量 Profile，允许 LTM 系统接受和终止任何通过全 SSL 封装的协议发送的客户机请求。您也可以选择使用 ***Server Profile*** 来配置 SSL Profile，以发起指向目标 Web 服务器的安全连接。

管理 SSL 流量需要完成以下这些任务：
- 在LTM系统上安装密钥/证书对，以便终止客户机端的安全连接。
- 配置一个Profile，然后将该Profile与一个Real Server进行关联。您可以使用Configuration工具对Profile进行配置。
- 将Profile与Real Server进行关联。

您也可以选择编写 iRule，它使您能够以特定的方式管理各个 SSL 连接。有关详细信息，请参阅第 13 章“编写 iRule”。

管理客户机端和服务器端的流量

通过 LTM 系统，您可以启用客户机端流量或服务器端流量的 SSL 流量管理。***客户机端流量***指客户机系统和 LTM 系统间的连接。***服务器端流量***指 LTM 系统和目标服务器系统间的连接。

- **管理客户机端SSL流量**
  启用LTM系统来管理客户机端SSL流量时，LTM系统通过解密客户机请求来终止流入的SSL连接。随后，LTM系统以明文方式将请求发送到目标服务器。接着，LTM系统检索明文响应（例如网页）并加密请求，然后将网页发送回客户机。终止SSL连接的流程中，可以选择让LTM系统执行所有的SSL证书验证功能，这些功能通常由目标Web服务器执行。有关配置客户机端SSL Profile的信息，请参阅第7-12页上的“了解SSL Profile”。

- **管理服务器端SSL流量**
  启用LTM系统来管理服务器端SSL流量时，LTM系统通过在将已解密的请求发送到目标服务器之前，重新加密该请求来增强网络安全性。除了此重新加密之外，还可以选择让LTM系统执行验证服务器证书的功能，这些功能与LTM系统验证客户机证书的功能相同。有关配置服务器端SSL Profile的信息，请参阅第7-12页上的“了解SSL Profile”。

SSL流量控制特性小结

LTM 系统包括若干与控制 SSL 流量相关的重要特性。这些特性中最为重要的是 SSL 认证（即证书验证和撤销）以及加密和解密。这些特性中的大多数都可以通过配置客户机或服务器的 SSL Profile 获得，其余特性则是通过诸如 iRules™这样的特性提供的。表 7.1 汇总了与 SSL 流量管理相关的特性；表格后的小节介绍了这些特性。

特性	说明	配置工具
证书验证	在终止和启动SSL连接时，LTM系统可以执行完整范围的证书验证任务，其中既包括客户机证书验证，也包括服务器证书验证。例如，可以如下定义系统对客户机证书的验证范围：您可以将系统配置为请求客户机证书（全部要求或全部忽略）。您还可以指定诸如证书链遍历深度这样的设置。	客户机和服务器的SSL Profile iRule
证书撤销	客户机或服务器向LTM系统出示证书时，系统可以检查证书的撤销状态，这是证书验证流程的一部分。	客户机和服务器的SSL Profile OCSP Profile
加密和解密	LTM系统对流入的客户机请求进行解密，这是从目标Web服务器卸载工作的一种途径。您可以将Profile配置为在将请求转发到服务器之前，对其进行重新加密，这个选项提供了额外的安全性。请求和响应的加密与解密基于您指定的特殊密码，这些密码是SSL Profile配置的一部分。	客户机和服务器的SSL Profile
授权	通过以特定方式配置LTM系统，您可以控制对系统资源的访问权限。例如，您可以创建一个iRule，将客户机证书信息插入客户机请求，然后根据该信息授予访问权限。此外，对于包含LDAP数据库服务器的环境，LTM系统可以使用客户机证书的认证信息来查询LDAP服务器，从而授予对资源的访问权限。您还可以限制并发TCP连接的数量。	SSL客户机证书LDAP Profile iRule
SSL会话持续性	LTM系统一个功能强大的特性是它能启用SSL会话的持续性。根据是否已将LTM系统配置为终止SSL连接，可用的SSL持续性有两类。	客户机和服务器的SSL Profile SSL Persistence Profile iRule
其它SSL特性	除了以上列出的特性，LTM系统还允许您配置其它一些选项，例如无效协议版本、SSL会话缓存的大小和超时值以及SSL关闭行为。	客户机和服务器的SSL Profile

表7.1 *与SSL流量控制相关的LTM系统特性小节*

了解证书验证

证书验证是确定客户机或服务器是否能够信任对端（即客户机或服务器）出示的证书的流程。从客户机接收到请求或从服务器接收到响应时，LTM 系统尝试验证客户机或服务器出示的证书是可信。

签发的证书

处理 SSL 连接时，对客户机和服务器在安全性方面的一项基本要求是：

任何时候与对端通信时，它们中的每一个都需出示由可信证书授权机构（CA）签发的证书。您也可以选择将 LTM 系统配置为执行客户机证书的验证任务。

在 LTM 系统上配置证书验证时，LTM 系统必须持有能够在处理 SSL 请求时向客户机出示的证书。

此外，您还可以将 LTM 系统配置为验证服务器响应。在此情形中，如果服务器对来自 LTM 系统的证书发出明确请求，那么 LTM 系统需要持有第二张证书。

如果将 LTM 系统配置为验证客户机和服务器的证书，那么必须在 LTM 系统上生成并安装密钥和证书，之后系统才能管理 SSL 流量。您可以通过 Configuration 工具执行此操作。您也可以导入现有的密钥/证书对，以代替生成新密钥/证书对的操作。有关导入现有密钥/证书对的详细信息，请参阅第 7-10 页上的“导入密钥、证书和档案”。

客户机端证书验证

客户机发出 HTTP 请求时，LTM 系统可以执行客户机证书验证任务，该任务通常由目标服务器执行。

客户机向 LTM 系统出示证书时，LTM 系统使用***客户机可信 CA*** 文件来确定自己可以信任的证书授权机构。使用此文件是 LTM 系统尝试验证客户机证书的主要方式。创建客户机端 Profile 时，LTM 系统自动创建缺省的客户机可信 CA 文件。您可以使用 Profile 中指定的缺省文件名，也可以指定其它文件名。有关详细信息，请参阅第 7-16 页上的“指定可信客户机 CA”。

客户机证书验证中的第二个要素是***客户机证书CA***文件，LTM系统使用该文件向客户机提供Profile信任的CA列表。请注意，此列表可以与LTM系统*实际*相信的CA的列表不同。如同可信CA文件一样，LTM系统自动创建此文件的缺省版本。

此外还有一个客户机链文件，LTM 系统将该文件发送至客户机，作为客户机证书验证流程的一部分。缺省的客户机链文件是客户机可信 CA 文件。有关详细信息，请参阅第 7-16 页上的“指定可信客户机 CA”。

服务器端证书验证

启用服务器 SSL Profile 并将出示服务器证书设置为 **Require** 时，便会进行服务器端验证。

服务器向 LTM 系统出示证书时，LTM 系统使用***服务器可信 CA*** 文件来确定自己可以信任的证书授权机构。使用此文件是 LTM 系统尝试验证服务器证书的主要方式。配置服务器端 Profile 时，LTM 系统自动创建缺省的服务器可信 CA 文件。您可以使用 Profile 中指定的缺省文件名，也可以指定其它文件名。

此外还有一个服务器链文件，LTM 系统将该文件发送至服务器，作为整个服务器证书验证流程的一部分。缺省的服务器链文件是服务器可信 CA 文件。

了解证书撤销

LTM 系统可以检查客户机或服务器正在出示的证书是否已被撤销。已撤销的客户机证书指示 LTM 系统，应使系统对客户机的认证失败。

对于检查证书撤销状态，LTM 系统支持两种业界标准方法。这两种方法是：

- **证书撤销列表（CRL）。**
  LTM系统可以使用CRL方法来检查正向LTM系统出示的证书是否已被撤销。这种CRL支持是以CRL文件加CRL路径的形式实现的。LTM系统允许您为客户机端Profile和服务器端Profile分别配置一个CRL文件和路径。对CRL的使用通过SSL Profile进行配置。有关详细信息，请参阅第7-25页上的"配置客户机或服务器的认证设置"。

- **在线证书状态协议（OCSP）**
  与使用CRL不同，OCSP确保证书的撤销状态始终是最新的。对OCSP的配置通过认证Profile进行。有关详细信息，请参阅第8章"认证应用流量"。

了解加密/解密

LTM 系统的另一个特性是能够处理加密和解密任务，这些任务通常由目标服务器执行，是处理客户机请求的一部分。LTM 系统使用客户机端 SSL Profile，在以纯文本形式将流入的请求发送到目标服务器之前，对这些请求进行解密。LTM 系统使用服务器端 Profile，在将请求发送到目标服务器之前对其进行重新加密，以提供更高的安全性级别。

与加密相关的一个 LTM 系统特性是它能够将客户机用来加密自己的请求的密码插入流入的 HTTP 请求中。然后，您可以根据该密码规范来引导流量。有关指定密码，以控制客户机请求目的地的详细信息，请参阅第 13 章"编写 iRule"。

了解客户机授权

与认证不同，***授权***与信任标识无关，它用于控制对系统资源的访问权限。一旦 SSL Profile 证实客户机或服务器可以信任，LTM 系统便可随即控制连接的级别和对目的地内容的访问权限类型。

支持针对 SSL 连接的访问权限控制的 LTM 系统特性包括：

- 将客户机证书字段插入HTTP请求中
- 限制并发客户机TCP连接的数量
- 通过LDAP数据库服务器进行客户机授权

要控制客户机对系统资源的访问权限，最有用的方法之一是创建将客户机证书字段以标头形式插入客户机请求的 iRule。例如，iRule 可以将客户机证书的状态以标头形式插入请求中，然后使用 **HTTP::header** 命令，基于该状态选择目标服务器。

有关使用此标头插入特性来控制客户机请求的目的地的详细信息，请参阅第 13 章"编写 iRule"。

了解SSL会话持续性

可供实施的 SSL 持续性有两类。第一类是标准的 SSL 持续性模式，此模式为不涉及 SSL 请求的解密和 SSL 响应的重新加密的 SSL 会话启用持续性。此 SSL 持续性模式可以通过配置 SSL 持续性 Profile 来启用。有关详细信息，请参阅第 9 章“启用会话持续性”。

第二类 SSL 持续性为涉及请求的解密和响应的重新加密的 SSL 会话启用持续性。在此情形中，通过将 SSL 会话 ID 以标头形式插入 HTTP 请求中来实施 SSL 持续性。插入会话 ID 标头可通过编写 iRule 实现。有关 iRule 的详细信息，请参阅第 13 章“编写 iRule”。

了解其它SSL特性

除了使用上述特性，您还可以执行其它一些任务，例如指定无效协议版本、配置 SSL 会话缓存的大小和超时值以及配置 SSL 关闭行为。您还可以将 SSL Profile 配置为基于超时值和数据传输量重新协商 SSL 会话。

管理密钥和证书

能够加密和解密 SSL 连接之前，必须在 LTM 系统上安装一个或多个 SSL 证书。第 7-3 页上的“了解证书验证”一节中介绍了这些证书的用途。

为使生成证书请求并将它们发送至证书授权机构的任务变得轻松，LTM 系统在 Configuration 工具中提供了一组密钥管理屏幕。这些证书管理屏幕可从 Main 选项卡的 **Local Traffic** 部分进行访问。管理密钥时，您可以执行以下操作：

- 显示有关全部现有密钥对和证书的信息。
- 为新密钥对和证书生成请求，然后将这些请求提交至证书授权机构。
- 更新证书请求。
- 显示密钥和证书的属性。
- 导入和导出PEM格式的密钥和证书。

显示有关现有密钥和证书的信息

通过Configuration工具可以获得有关现有密钥对和证书的汇总信息。“SSL证书”屏幕显示以下信息：

- 证书的状态（有效、即将过期或已过期）
- 生成请求时为证书分配的唯一名称
- 证书签发者
- 有效日期

显示有关现有证书和密钥的信息的步骤

1 在Main选项卡上，展开**Local Traffic**。
2 点击**SSL Certificates**。
此操作将打开SSL Certificates屏幕，其中列有LTM系统上已安装的所有证书。

3 点击证书名称。
此操作将显示该证书的属性。
4 如果要查看与该证书关联的密钥的有关信息，请点击菜单栏上的**Key**。
此操作将显示密钥的类型和大小。

为新证书和密钥生成请求

使用Configuration工具可以生成自签发的证书（通常仅供内部测试之用），也可以生成证书/密钥对的请求，以便发送到证书授权机构。将请求发送到证书授权机构时，该机构将返回已签发的证书。

通过以下两种方式中的任意一种，您都可以将证书请求发送到证书授权机构：

- 您可以使用剪切和粘贴，从Configuration工具屏幕中将新生成的请求的文本复制下来，然后提交给证书授权机构。
- 您可以将新生成的请求下载到文件，然后将该文件传送给证书授权机构。

将请求传送给证书授权机构（通过粘贴文本或通过文件附件）的方法是访问证书授权机构的网站。用于提交请求，以便证书授权机构签发的Configuration工具屏幕包含指向各大证书授权机构网站的链路。

请求自签发证书的步骤

1. 在Main选项卡上，展开**Local Traffic**。
2. 点击**SSL Certificates**。
   此操作将显示SSL Certificates屏幕。
3. 在屏幕的右上方，点击**Create**。
4. 为证书键入一个唯一的名称。
5. 对于**Issuer**设置，选择**Self**。
6. 配置**Common Name**设置和其它任何想修改的设置。
7. 在Key Properties部分中，选择密钥尺寸。
8. 点击**Finished**。

向证书授权机构请求证书的步骤

1. 在Main选项卡上，展开**Local Traffic**。
2. 点击**SSL Certificates**。
   此操作将显示SSL Certificates屏幕。
3. 在屏幕的右上方，点击**Create**。
4. 为证书键入一个唯一的名称。
5. 在**Issuer**框中，选择**Certificate Authority**。
6. 配置**Commmon Name**设置和其它任何想修改的设置。
7. 点击**Finished**。
   此操作将显示证书请求。
8. 通过以下任何方式之一，将请求下载到您系统上的文件中：
   - 从**Request Text**框中复制证书。
   - 点击**Request File**框中的按钮。
9. 在**Certificate Authorities**框中，点击一家证书授权机构的名称。
   此操作将显示该证书授权机构的网站。
10. 按照网站上的操作说明，粘贴复制的请求或附加生成的请求文件。

11. 点击**Finished**。

更新证书

所有的证书都具备有效日期。证书过期时，如果希望继续使用该证书，必须将其更新。

更新证书的步骤

1. 在Main选项卡上，展开**Local Traffic**。
2. 点击**SSL Certificates**。
   此操作将显示现有证书的列表。
3. 点击要更新的证书的名称。
   此操作将显示证书属性。
4. 在屏幕底部，点击**Renew**。
5. 修改或保留设置。
   请注意，**Common Name**设置的值是必需的。
6. 点击**Finished**。

删除证书/密钥对

您可以删除不再需要的证书和密钥。

删除证书的步骤

1. 在Main选项卡上，展开**Local Traffic**。
2. 点击**SSL Certificates**。
   此操作将显示现有证书的列表。
3. 对于要删除的证书，选中其名称左侧的Selective框。
4. 在屏幕底部，点击**Delete**。
   将会显示确认屏幕。
5. 点击**Delete**。
   此操作将删除证书。

导入密钥、证书和档案

如果已从其它系统将密钥/证书对、证书或密钥/证书档案传送到LTM系统中，且证书或档案的形式为文件或base-64编码的文本字符串，那么您可以将此证书或档案导入Configuration工具中。将证书或档案导入Configuration工具可以使证书或档案的管理任务变得轻松。仅当要导入的证书为增强型私人邮件（PEM）格式时，才可使用“导入SSL证书和密钥”屏幕。

导入密钥对、证书或档案的步骤

1 在Main选项卡上，展开**Local Traffic**。
2 点击**SSL Certificates**。
   此操作将显示现有证书的列表。
3 在屏幕的右上角，点击**Import**。
   选择导入类型（**Key**、**Certificate**或**Archive**）。
4 选择导入方法（文本或文件）。
5 键入密钥、证书或档案的名称。

6 点击**Import**。

创建档案

您可以为一个或多个密钥和证书创建档案。希望将多个密钥和证书导出至其它系统时，便可创建档案。

创建档案的步骤

1 在Main选项卡上，展开**Local Traffic**。
2 点击**SSL Certificates**。
此操作将显示现有证书的列表。
3 点击**Archive**。
4 为档案文件键入一个名称。
文件将拥有扩展名**.tgz**。
5 在Key List区域中，执行以下操作：
a) 选择要归档的密钥。
b) 使用移动按钮（**<<**）将密钥名称转移到**Enabled**框。
6 在Certificate List区域中，执行以下操作：
a) 选择要归档的证书。
b) 使用移动按钮（**<<**）将证书名称转移到**Enabled**框。
7 点击**locallb.sslcert.Generate&DownloadArchive**按钮。
8 点击**Finished**。

了解SSL Profile

如第5章“了解Profile”中所述，**Profile**是一组带有值的设置，用于确定LTM系统管理特定应用的网络流量的方式。Profile可以管理的流量类型之一是SSL流量。SSL Profile最基本的功能是从目标Web服务器卸载证书检验和验证任务，以及进行加密和解密。

SSL Profile的类型有以下两种：

- **客户机Profile**
客户机Profile允许LTM系统处理任何从客户机系统进行LTM系统的SSL连接的认证和加密任务。实施此类Profile的方法是使用缺省的**clientssl** Profile，或者基于该**clientssl** Profile创建定制Profile。

- **服务器Profile**
服务器Profile允许LTM系统处理任何从LTM系统发送到目标服务器的SSL连接的加密任务。要求LTM系统的认证时，通过向服务器出示证书的认证信息，服务器SSL Profile可以扮演客户机的角色。实施此类Profile的方法是使用缺省的**serverssl** Profile，或者基于该**serverssl** Profile创建定制Profile。

◆ 重要信息

启用SSL处理过程之前，首先必须通过可信证书授权机构生成有效的x509证书，或者生成临时证书，然后将其安装在LTM系统上。有关证书的详细信息，请参阅第7-3页上的“签发的证书”。有关如何在LTM系统上生成和安装证书的说明，请参阅第7-7页上的“管理密钥和证书”。

组成客户机或服务器SSL Profile的设置可分为以下三类：常规属性、配置和客户机认证/服务器认证。您可以在创建SSL Profile时配置这些设置，也可以在创建Profile之后，通过修改Profile的设置来进行配置。有关对Profile进行配置的具体流程，请参阅第5章“了解Profile”。

◆ **提示**

对于任何单独的SSL连接，您都可以覆盖SSL Profile设置的值。这是通过编写iRule，将那些与要覆盖的设置相对应的SSL iRule命令包括在内实现的。有关详细信息，请参阅第13章“编写iRule”。

配置SSL Profile的常规属性

本节介绍Client SSL Profile或Server SSL Profile屏幕的General Properties部分中显示的设置。有关其它SSL Profile设置的信息，请参阅第7-14页上的“对配置的设置进行配置”和第7-25页上的“配置客户机或服务器认证设置”。

有关创建或修改Profile的流程，请参阅第5章“了解Profile”。

表7.2显示了可以为Client或Server SSL Profile指定的常规属性。对于那些带有缺省值的设置，您可保留那些缺省设置，也可以进行修改。此表的下面是对这些常规属性的介绍。

常规属性	说明	缺省值
Name	指定用户提供的Profile名。	无缺省值
Parent Profile	指定系统提供的、从中衍生定制Profile的Profile。	**clientssl**或**serverssl**

***表7.2** SSL Profile的常规属性*

配置HTTP Profile的常规属性时，需为Profile指定一个唯一的名称，并选择一个上级Profile。

指定Profile名称

为了创建SSL Profile，必须为Profile指定一个唯一的名称。创建SSL Profile时，**Name**设置是唯一一个必须主动指定的设置；其它所有设置都具有缺省值。

选择上级Profile

您创建的每个Profile都是从上级Profile衍生而来的。使用**Parent Profile**设置，您可以将缺省SSL Profile配置成上级Profile，也可以配置其它已创建的SSL Profile。

对配置的设置进行配置

本节介绍Client SSL Profile或Server SSL Profile屏幕的Configuration部分中显示的设置。有关配置其它SSL Profile设置的信息，请参阅第7-13页

上的“配置SSL Profile的常规属性”和第7-25页上的“配置客户机或服务器认证设置”。

有关创建或修改SSL Profile的流程，请参阅第5章“了解Profile”。

表7.3显示了可以为Client SSL或Server SSL Profile进行配置的设置。对于那些带有缺省值的设置，您可保留那些缺省设置，也可以进行修改。此表的下面是对这些设置的介绍。

设置	说明	缺省值
Mode	启用或禁用SSL处理过程。	**Enabled**
Certificate	指定为终止或启动SSL连接，而在LTM系统上安装的证书的名称。	**default**
Key	指定为终止或启动SSL连接，而在LTM系统上安装的密钥的名称。	**default**
Pass Phrase	指定用于加密密钥的密码短语的名称。	无缺省值
Confirm Pass Phrase	确认用于加密密钥的密码短语的名称。	无缺省值
Chain	指定或建立证书链文件，客户机可以使用该文件来认证Profile。有关详细信息，请参阅第7-16页上的“配置证书链”。	无缺省值
Trusted Certificate Authorities	通过指定LTM系统信任的客户机或服务器CA列表，配置证书验证。有关详细信息，请参阅第7-16页上的“指定可信客户机CA”。	无缺省值
Ciphers	指定LTM系统支持的密码的列表。有关详细信息，请参阅第7-16页上的“指定SSL密码”。	**Default**
Options	指定值**All Bugfixes Enabled**，此值将启用一组与SSL处理过程有关的各种行业相关解决方案。有关详细信息，请参阅第7-17页上的“配置解决方案”。	**All Bugfixes Enabled**
ModSSL Methods	启用或禁用ModSSL方法模拟。	未选中
Cache Size	指定SSL会话缓存中的会话数。 **注意：**此设置仅适用于客户机端Profile。	**20000**
Cache Timeout	以秒为单位，指定SSL会话缓存条目的超时值。 **注意：**此设置仅适用于客户机端Profile。	300
Alert Timeout	以秒为单位，指定SSL会话缓存的超时持续时间。	**Indefinite**
Renegotiate Period	强制执行指定的SSL重新协商周期。	**Indefinite**
Renegotiate Size	强制执行指定的SSL重新协商的吞吐率大小（字节）。	**429496729**
Renegotiate Max Record Delay	强制执行SSL重新协商的最大记录延迟。 **注意：重新协商最大记录延迟**属性仅适用于客户机端Profile。	**Indefinited**
Unclean Shutdown	将LTM系统配置为启用或禁用非正常关机。	选中
Strict Resume	将LTM配置为启用或禁用在非正常关机之后恢复SSL会话。	未选中

表7.3 可配置的SSL Profile设置

在配置SSL Profile之前，先对可能要更改的特定设置进行规划描述将会很有帮助。

指定模式

Mode设置用于启用或禁用Profile。如果将其设置为**Enabled**，那么Real Server自动将Profile应用到任何SSL流量。如果该Profile是客户机端Profile，那么LTM系统将终止所有流入的SSL连接。如果该Profile是服务器端Profile，那么LTM系统将启动所有流出的SSL连接。

如果将其设置为**Disabled**，那么LTM系统既不会终止任何流入Real Server的SSL连接，也不会启动任何流出Real Server的SSL连接。

指定证书名称

Certificate设置的值是安装在LTM系统上，以便对客户机端或服务器端SSL连接进行认证的证书的名称。如果尚未在LTM系统上生成证书请求或安装证书，那么可以指定缺省证书的名称**default**。有关证书的详细信息，请参阅第7-3页上的“了解证书验证”。

指定密钥名称

Key设置的值是安装在LTM系统上，以便对客户机端或服务器端SSL连接进行认证的密钥的名称。如果尚未在LTM系统上生成密钥请求或安装密钥，那么可以指定缺省密钥的名称**default**。

有关密钥的详细信息，请参阅第7-3页上的“了解证书验证”。

配置证书链

在任何客户机验证流程中，不仅LTM系统需要对客户机进行认证，而且客户机可能需要对LTM系统进行认证。但有时，LTM系统用来让客户机对自己进行认证的证书是由该客户机不信任的中间CA签发的。在此情形中，LTM系统可能需要使用证书链。Profile允许您指定特定证书链文件的名称。请注意，构成链文件的证书文件必须为PEM格式。

指定可信的客户机CA

针对客户端SSL处理，您可以配置一个SSL Profile，以验证客户机或服务器出示的证书。使用**Trusted Certificate Authorities** 设置，您可以指定可信的客户机CA文件名，LTM系统随后会使用该文件验证客户机或服务器证书。如果您没有配置可信的CA文件，Profile将使用缺省的文件。

您指定用于验证证书的可信CA文件通常包含一个或多个证书，证书采用增强保密邮件（PEM）格式。手动建立文件时，该文件包括SSL Profile信任的客户机或服务器证书列表。如果您没有指定可信CA文件，或者所指定的可信CA文件无法访问LTM系统，那么系统将使用缺省的文件名。

指定SSL密码

您可以为每个SSL Profile指定可用于SSL连接的密码。在配置密码时，您必须确保为SSL Profile配置的密码与发送请求的客户机或发送响应的服务器的密码相匹配。

例如，客户机可能成功建立起与SSL Profile的连接；该Profile可以使用客户机和服务器端SSL。客户机发送额外数据（例如HTTP请求）之后，SSL Profile会尝试建立一条指向服务器的SSL连接。

但是，SSL Profile可能被配置为只能使用服务器端SSL的3DES密码，而服务器可能被配置为只接受RC4密码。此时，由于未启用通用密码，因此SSL Profile与服务器之间的SSL握手将会失败。结果客户机连接被关闭。如果客户机正在使用浏览器，那么用户很可能会收到提示网页加载失败的错误信息。您可以指定一个字符串来指明可用SSL密码的列表，或者也可以使用缺省的密码字符串 – **Default**。对于客户机SSL Profile，**Default**密码字符串的定义为**ALL:!SSLv2:@SPEED**。对于服务器SSL Profile，**Default**密码字符串的定义为**COMPAT+HW:@SPEED**。

LTM系统支持的密码为：

- SSLv2
- SSLv3
- TLSv1
- SGC/设置
- RFC 2246中描述的所有标准协议扩展和密码
- AES密码（在RFC 3268中进行了描述）

除非很有必要，否则我们不推荐使用SSLv2密码。因此，已连接的用户应该将密码字符串设置为**DEFAULT:-SSLv2**。

◆ 注

LTM系统支持版本0.9.7的OpenSSL密码列表格式。

◆ 提示

除了在SSL Profile中指定密码外，您也可以将密码规范插入到HTTP请求的标头中，然后根据这些密码引导流量。有关详细信息，请参阅第13章“编写iRule”。

配置解决方案

OpenSSL支持一系列故障解决方案和SSL选项。您在设置单独的客户机或服务器端SSL Profile时，可以启用这些解决方案和选项。**Options**设置的缺省值为**All Options Disabled**。**ALL_BUGFIXES**值可以启用设置中的所有解决方案。

表7.4列出并说明了您可以为SSL Profile配置的解决方案和选项。

SSL属性	说明
All Bugfixes Enabled	此选项可启用表中所描述的所有故障解决方案。当您希望与兼容存有故障的措施时，使用**启用所有Bugfixes**选项来启用故障解决方案选项将会非常安全。
Cipher server preference	当LTM系统选择一个密码时，此选项会使用服务器偏好代替客户机偏好。

	在未设置此选项时，SSL服务器会采用客户机的偏好。设置此选项之后，服务器会使用自己的偏好来选择SSLv3/TLSv1。由于存在不同的协议，因此SSLv2，服务器会向客户机发送其偏好列表，并由客户机自由选择密码。
Don't insert empty fragments	这一选项会针对容易影响CBC密码的SSL 3.0/TLS 1.0协议，禁用可能实施的对策。这些密码不能由某种存在故障的SSL措施进行处理。此选项不会对使用其他密码的连接造成影响。
Ephemeral RSA	这一选项可在实施RSA操作时使用短暂（临时）的RSA密钥。根据规范，仅当RSA密钥用于签名操作时（即导出具有严格RSA密钥长度的密码）才会用到此选项。设置这一选项后，LTM系统总会使用短暂的RSA密钥。它会破坏与SSL/TLS规范的兼容性，从而导致与客户之间的互操作出现问题。因此不推荐启用此选项，您应该使用EDH（短暂的Diffie-Hellman）密钥来进行代替。服务器端SSL会忽略这一选项。
Netscape CA DN bug workaround	此选项可处理与系统稳定性有关的故障。如果系统接受了要求提供客户机证书的Netscape浏览器连接，并且系统具有非自签发的CA（而在Netscape中没有CA），而且浏览器也拥有一个证书，那么系统会崩溃或挂起。
Netscape demo cipher change bug workaround	此选项将特意操纵SSL服务器会话恢复，以模拟某些Netscape服务器（参阅**Netscape重用密码变更bug解决方案**说明）。我们不推荐在正常使用情况下设置此选项，并且服务器端SSL处理会忽略此选项。
Netscape reuse cipher change bug workaround	当通过SSLv2/v3连接，然后又通过SSLv3重新连接时，此选项只会处理Netscape-Enterprise/2.01（**https://merchant.neape.com**）中出现的故障。此时，密码列表会发生变化。 首先，根据RC4-MD5密码列表会建立起一个连接。如果随后需要恢复，那么连接将切换到使用DES-CBC3-SHA密码列表。但是，根据RFC 2246，（7.4.1.3节，密码套件），密码列表应该保留RC4-MD5。 作为解决方案，您可以尝试与DES-CBC-SHA:RC4-MD5等密码列表连接。由于一些原因，每个新连接会使用RC4-MD5密码列表，但是任何重新进行的连接都会使用DES-CBC-SHA密码列表。因此Netscape在重新连接时会使用密码列表中的第一个连接。
No SSLv2	不要使用SSLv2协议。
No SSLv3	不要使用SSLv3协议。
No session resumption on renegotiation	当LTM系统进行SSL服务器重新协商时，此选项会开始一个新的会话（即会话恢复请求只被最初的握手所接受）。系统在进行服务器端处理时会忽略此选项。
N0 TLSv1	不要使用SSLv1协议。
Microsoft big SSLV3 buffer	此选项会启用一个解决方案，用于同使用非标准SSL记录尺寸的早期微软应用进行通信。
Microsoft IE SSLV2 RSA padding	此选项会启用一个解决方案，用于同使用非标准RSA密钥填充的早期微软应用进行通信。 服务器端SSL会忽略此选项。
PKCS1 check 1	调试选项将特意操纵SSL客户机PKCS1填充，以便其能够检测特殊的SSL服务器隐患。正常情况下我们不建议使用该选项。系统在进行客户机端处理时会忽略此选项。
PKCS1 check 2	调试选项特意操纵SSL客户机PKCS1填充，以便其能够检测特殊的SSL服务器隐患。正常情况下我们不建议使用该选项。系统在进行客户机端处理时会忽略此选项。
Single DH use	当使用临时/短暂的DH参数时，此选项会创建新的密钥。在未使用“强”质数（例如，使用DSA参数时）生成DH参数时，如果您希望防止子群攻击，那么您必须使用此选项。如果使用了“强”质数，那么可以不必在每

	次握手时生成新的DH密钥，但是我们推荐这样做。无论何时使用临时/短暂DH参数，您都应该启用**Single DH use**。
SSLEAY 080 client DH bug workaround	此选项会采用一种解决方案，用于同早期的SSLeay应用进行通信，这些应用通常指定了错误的Diffie-Hellman公共值长度。服务器端SSL会忽略此选项。
TLS D5 bug workaround	此选项会采用一种解决方案，用于同早期的启用TLSv1的应用进行通信，这些应用通常指定了错误加密的RSA密钥长度。服务器端SSL会忽略此选项。
TLS block padding bug workaround	此选项会启用一种解决方案，用于同早期的启用TLSv1的应用进行通信，这些应用通常使用错误的块填充。
TLS rollback bug workaround	此选项会禁用版本回滚攻击检测。在客户机密钥交换期，当客户机发送第一个**hello信息**时必须发送有关可接受的SSL/TLS协议等级的相同信息。一些客户机会适应服务应答，从而违反了这一规则。例如，客户机发送SSLv2 **hello信息**，并且接受到SSLv3.1（TLSv1），但是服务器只能理解到SSLv3。此时，客户机必须使用相同的SSLv3.1（TLSv1）声明。一些客户机会将服务器应答降至SSLv3，从而违反了版本回滚保护。服务器端SSL会忽略此选项。

表7.4 *解决方案和其他SSL选项*

值得注意的是，当配置协议版本时，您必须确保为LTM系统配置的协议版本与系统的协议版本相匹配。即，客户机SSL Profile中指定的协议版本必须与客户机中的协议版本相匹配，服务器端SSL Profile中指定的协议版本必须与服务器端中的协议版本相匹配。因此，对于客户机和服务器端SSL连接，您可以指定不希望LTM系统允许的协议版本。

您可以声明3个协议版本中的2个版本无效：**SSLv2**、**SSLv3**和**TLSv1**。如果没有指定协议版本，LTM系统会允许使用所有的SSL协议版本。

◆ **注**

我们推荐您至少将协议版本SSLv2指定为无效。

要指定解决方案选项，应该从**Options**设置中选择**Options List**。此时系统会显示**Options List**设置。从**Options List**设置中选择您希望配置的选项，然后点击**Enable**按钮。

启用ModSSL方法模拟

此设置可启用或禁用ModSSL方法模拟。当OpenSSL方法不够用时，您可以启用此设置。

当启用**ModSSL Methods**设置时，您可以使用**HTTP::header insert_modssl_fields**命令编写iRule，此命令会将一些ModSSL选项作为标头插入HTTP请求。表7.5列出了您能够在HTTP请求中插入的选项。

标头类型	标头名称和格式	说明
证书状态	SSLClientCertStatus: [status]	客户机证书的状态。[status]值可以为**NoClientCert**、**OK**或**Error**。如果状态是**NoClientCert**，那么请求中只会插入标头。如果状态为**Error**，那么错误后面应该带有用数字表示的错误代码。

标头类型	标头名称和格式	说明
证书版本	SSLClientCertVersion: [version]	证书版本
证书序列号	SSLClientCertSerialNumber: [serial]	证书的序列号。
证书的签名算法	SSLClientCertSignatureAlgorithm: [alg]	证书的签名算法。
证书的签发人	SSLClientCertIssuer: [issuer]	证书的签发人。
证书的有效日期	SSLClientCertNotValidBefore: [before] SSLClientCertNotValidAfter: [after]	证书的有效日期。在[before]之前和[after]之后的证书都是无效的。
证书主题	SSLClientCertSubject: [subject]	证书的主题。
主题的公钥	SSLClientCertSubjectPublicKey: [key]	公钥类型。允许的公钥类型为**RSA ([size] bit)**、**DSA**或**Unknown public key**。
证书本身	SSLClientCert: [cert]	实际的客户机证书。
证书的MD5 hash校验	SSLClientCertHash: [hash]	客户机证书的MD5 hash校验。

***7.5** 使用iRule的ModSSL选项*

有关向HTTP请求中插入标头的详细信息，请参阅第13章“编写iRule”。

配置SSL会话缓存

只有针对客户端的Profile时，才可以对SSL会话缓存的超时和尺寸值进行配置。因为每个Profile都具有一个独立的SSL会话缓存，所以您可以在预Profile中配置相关的值。

设置SSL会话缓存尺寸

使用配置工具，您可以指定SSL会话缓存的最大尺寸。SSL会话缓存尺寸的缺省值为20,000个条目。值为**0**表示禁用会话缓存。注意，此设置只能应用于客户端Profile。

您可以在预Profile中将客户端的会话缓存尺寸配置为最大值。要指定SSL会话缓存尺寸，应该在**Cache Size**设置中保持缺省缓存尺寸值或输入新的值。

设置SSL会话缓存超时时间

您可以使用配置工具指定已协商的SSL会话ID的生命周期秒数。SSL会话缓存的缺省超时值为300秒。可接受的值为大于或等于5的整数值。

那些使用已过期的会话ID尝试恢复SSL会话的客户机，将被强制在新的会话中进行协商。

注意，此设置只能应用于客户机Profile。

您可以逐一针对Profile来配置客户机的会话缓存超时值。要指定SSL会话缓存超时值，应该在**Cache Size**设置中保持缺省缓存超时值或输入新的值。

♦ 警告

如果将客户机SSL会话缓存的超时值设置为0，那么SSL会话ID会与会话缓存中Profile客户机协商，直到缓存充满并开始清除条目为止。如果正在重新使用那些会话ID的客户机又利用的宝贵资源，那么将数值设置为0会带来极大的安全风险。因此，实践中SSL会话缓存的超时时间通常设置为不超过24小时，或更短的时间。

要指定SSL会话缓存的超时时间，应该在**Create Timeout**设置中保持缺省值或者从列表中选择**Specify**、**Immediate**或**Indefinite**。如果您选择了**Specify**，那么请输入一个值。

指定报警超时时间

Alert Timeout设置表示SSL会话缓存中条目超时的持续时间（以秒为单位）。

强制SSL会话重新协商

长时间的连接容易受到中间人的攻击。要防止这种攻击，您可以强制LTM系统根据时间或应用尺寸重新协商SSL会话。您也可以强制LTM系统在收到指定的记录数之后终止SSL会话。

根据时间段重新协商会话

Renegotiate Period设置会强制LTM系统在指定的秒数后重新协商SSL会话。

要指定重新协商时间段，应该在**Renegotiate Period**设置中保持不定值或选择**Specify**。如果您选择了**Specify**，那么请输入一个值。

根据应用数据尺寸重新协商会话

Renegotiate Size设置会强制LTM系统在指定通过安全信道传输的应用数据量（以MB为单位）之后重新协商SSL会话。

要指定重新协商尺寸，应该在**Renegotiate Size**设置中保持缺省值或输入新的值。

指定最大记录延迟

当LTM系统等候客户机启动重新协商时，**Renegotiate Max Record Delay**设置会强制LTM系统在接受所指定的最大数量的SSL记录后终止SSL会话。如果LTM系统收到的记录数超过SSL的最大记录，那么它将关闭连接。

要指定最大记录延迟，应该在**Renegotiate Max Record Delay**设置中保持**Indefinite**值或选择**Specify**。如果您选择了**Specify**，那么请输入一个值。

配置SSL关机

需要关闭SSL连接时，您可以配置LTM系统上的两个设置：**Unclean Shutdown**和**Strict Resume**。

禁用不完全SSL关机

在**Unclean Shutdown**中，无需交换所要求的SSL关机报警即可关闭TCP连接。但是，您可以禁用不完全关机，通过配置设置，强制SSL Profile对所有SSL连接执行完全关机。

此特性对于Internet Explorer浏览器特别有用。不同的浏览器版本或者同一版本浏览器的不同模块处理关机报警的方式各不相同。一些版本或模块会要求服务器的关机报警，而另一些版本或模块不会做出这样的要求，但是SSL Profile无法总是检测出是否需要关机报警。如果浏览器期望关机报警，但是SSL Profile没有交换报警（默认设置），那么浏览器会显示错误消息。

缺省情况下，LTM系统会对所有SSL连接执行不完全关机。要禁用不完全关机，应该在**Unclean Shutdown**设置中取消复选框选择。

中断SSL会话

您可以在不完全关机之后配置LTM系统，以便中断SSL会话。缺省情况下，此设置为禁用，这会使LTM系统在不完全关机后恢复SSL会话。如果您启用此设置，那么LTM系统不会在不完全关机后恢复SSL会话。

要在不完全关机后中断SSL会话，应该在**Strict Resume**设置中选中复选框。

配置客户机或服务器认证设置

这一节将介绍Client SSL Profile屏幕的Client Authentication部分或Server SSL Profile的Server Authentication屏幕的设置。有关对其他SSL Profile设置进行配置的详细信息，请参阅第7-13页“配置SSL Profile的常规属性”和第7-14页“对配置设置进行配置”。

有关创建或修改SSL Profile的程序，请参阅第5章“了解Profile”。

表7.6列出并说明了客户机或服务器SSL Profile的认证设置。对于那些含有缺省值的设置，您可保留或者修改这些设置。下表是对具体设置的描述。

设置	说明	缺省值
Client or Server Certificate	配置SSL Profile请求、要求或忽略客户机或服务器出示的证书。	**Ignore**
Frequency	指定Profile是否应该在每次会话中、或者在会话之后重新使用SSL会话时对客户机进行认证。有关详细信息，请参阅第*7-27*页“配置每次会话认证”。	**One**
Advertised Trusted Certificate Authorities	详细说明了您向客户机建议的受Profile信任的CA。有关详细信息，请参阅第7-27页的*“通告可信客户机CA列表”*。	无缺省值

设置	说明	缺省值
Certificate Chain Traversal Depth	注：此属性只能应用于客户机Profile。 指定可在客户机证书链中穿越的证书最大数量。有关详细信息，请参阅7-28页“配置认证深度”。	9
Authenticate Name	根据嵌入服务器证书中的公用名称（CN）对目标服务器进行认证。有关详细信息，请参阅第*7-28*页“根据名称配置认证”。	无缺省值
Certificate Revocation List (CRL)	注：此属性只能应用于服务器端Profile 通过维护已撤销证书列表来配置证书撤销。有关详细信息，请参阅7-28页“证书撤销”。	无缺省值

***表7.6** SSL Profile中的认证设置*

配置证书颁发

在配置**Client Certificate**或**Server Certificate**设置时，可以采用多种方法使LTM系统处理客户机或服务器认证。

对于客户机处理，**Client Certificate**的设置值为：

- **Request**
  请求并验证客户机证书。此时，SSL Profile通常会授予访问的权限，而不管是否具有证书或证书的状态如何。
- **Require**
  要求客户机在授予访问权之前出示有效可信的证书。
- **Ignore**
  忽略证书（或缺少证书），因此不会对客户机认证。**Ignore**设置是缺省设置，使用此设置会忽略任何每次会话认证设置。有关配置每次会话认证的信息，请参阅第7-27页“配置每次会话认证”。
- **Auto**
  在认证模块请求证书之前始终忽略客户机证书。与选项设置为**Request**时类似，此时LTM系统会启动中间会话SSL握手。我们建议仅对那些无需出示客户机证书的连接应用此设置。

♦ **警告**

*如果您正在使用LDAP客户机认证特性，那么使用**Request**或**Ignore**选项有时会造成连接终止。有关基于LDAP客户机授权的详细信息，请参阅第8章“认证应用流量”。*

♦ **提示**

***请求**选项与标头插入特性配合密切。配置SSL Profile，以便向HTTP客户机请求中插入客户机证书信息并且根据**Request**选项对客户机认证，从而使LTM系统或服务器进行诸如将请求重新定向到另一台服务器、将不同的内容发送回客户机或进行客户机认证或会话ID持续性。*

对于服务器端处理，**Server Certificate**的设置值为：

- **Require**
  要求服务器在授予访问权之前出示有效可信的证书。

- **Ignore**
  忽略一个证书（或缺少一个证书），因此不会对服务器进行认证。**Ignore**设置是一个缺省的设置项，使用此设置会忽略任何每次会话认证设置。有关配置每次会话认证的信息，请参阅第7-27页“配置每次会话认证”。

配置每次会话认证

通过**Frequency**设置，您可以配置SSL Profile，以要求对每个SSL会话都进行一次认证（**Once**），或者对之后每次重新使用SSL会话进行认证（**Always**）。此选项的缺省值为**Once**。

您可以根据应用将此选项设置为**Once**或**Always**。完善设计的网络应用只需对每次会话进行一次证书验证。我们出于性能的原因，推荐您尽可能使用缺省设置（**Once**）。

您可以修改SSL Profile，以要求对每次会话认证一次以及对之后每次重新使用SSL会话进行认证。

通告可信客户机CA列表

此功能仅限于客户机Profile，如果您打算配置SSL Profile，以要求或请求对客户机证书认证，那么需要将Profile发送到服务器可能信任的客户机CA列表。可以通过配置**Advertised Tursted Certificate Authorities**设置来实现上述目的。

此列表也称作客户机证书CA文件，它与客户机可信CA文件不同。原因是在一些情况下，您的客户机可能不会处理有效的客户机证书，此时您可能不希望展示Profile信任的实际CA列表。客户机证书CA文件允许Profile通告与证书验证过程中配置的实际客户机可信CA文件不同的CA列表，从而解决这一问题。

◆ 提示

虽然客户机证书CA文件的内容与客户机可信CA文件的内容不同，但是由于兼容性的原因，您最好对客户机证书CA选项进行设置，使其与实际的客户机可信CA文件相匹配。这是因为，如果对等体请求证书客户机没有提供可信的CA列表，那么现在的浏览器可能不会允许通过SSL会话进行协商。

要配置Profile发送此列表，您可以指定PEM格式的证书文件，该文件包含至少一个客户机认证受服务器信任的CA。如果没有指定Client Certificate CA文件，那么没有可信的CA列表回发送到客户机。

配置认证深度

通过**Certificate Chain Traversal Depth**设置，您可以配置能够在证书链中穿越的最大证书数。此数量的缺省值为**9**。如果证书链较长，并且在此穿越数中，没有客户机被认证，那么客户机或服务器证书验证将会失败。如果将认证深度值设置为0，那么只会检测客户机或服务器证书以及其中的一个证书链文件。

根据名称配置认证

此功能仅限于服务器Profile，LTM系统支持根据名称认证，此特性能够防止中间人攻击。当您为服务器端Profile配置**Authenticate Name**设置时，LTM系统会参照目标服务器向LTM系统出示的证书中列出的公用名称（CN）来检查此名称。如果您所指定的名称属性与服务器证书中的CN不匹配，那么LTM系统会关闭连接。CN的示例之一是**www.f5.com**。

证书撤销

Certificate Revocation List（CRL）设置允许LTM系统在对客户机或服务器认证之前，使用CRL检查证书的撤销状态。

要为SSL Profile配置CRL，您必须配置CRL文件，该文件包括已撤销的客户机或服务器证书列表。当指定已撤销证书列表时，您所指定的文件必须为PEM格式。

♦ **重要信息**

*CRL文件可能会过期，需要每天进行更新，最长更新时间间隔不得超过30天。如果您的CRL文件已过期，那么LTM系统会拒绝**所有**有效或无效的证书。因此，保持最新的CRL文件至关重要。您可以从**/config/ssl/ssl.crl**目录中发出以下命令进行证书更新：**openssl crl -in <crlname> -text –noout**。*

另一种使用CRL的方法是利用在线证书状态协议（OCSP）特性，此特性可确保证书撤销状态为最新信息。有关详细信息，请参阅第8章“认证应用流量”。

管理SSL Profile

您可以使用配置工具查看SSL文件，删除您所创建的任何定制Profile。注意，您不能删除缺省的Profile **clientssl**和**serverssl**。

关于创建和修改SSL Profile的程序，请参阅第5章“Profile简介”。

查看或删除SSL Profile的步骤

1. 在Main选项卡上，展开**Local Traffic**。
2. 点击**Profiles**。
   将打开Profiles屏幕。
3. 从SSL菜单中选择Client或Server。
   这样可以显示任何客户机端或服务器端Profile的列表。
4. 删除Profile的步骤：
   a) 点击您希望删除的定制Profile左边的Selective框。
   b) 点击**Delete。**
      将会显示确认屏幕。
5. 点击**Delete。**
   此操作将删除Profile。
6. 查看SSL Profile的详细信息时，需要在名称栏中点击您希望查看的Profile名称。

随后会显示出Profile的详细信息。

8

认证应用流量

- 简介
- 实施**LDAP**认证模块
- 实施**RADIUS**认证模块
- 实施**TACACS+**认证模块
- 实施**SSL**客户机证书**LDAP**认证模块
- 实施**SSL OCSP**认证模块

简介

BIG-IP®本地流量管理（LTM）系统的重要特性是能够支持可插拔认证模块（PAM）技术。PAM技术使您能够从许多不同的认证和授权方案中进行选择，以便对网络流量进行认证或授权。

PAM技术的目标是将应用（如LTM系统）从其底层认证技术中分离出来。这意味着您可以采用您希望LTM系统使用的特定认证/授权技术，对进入BIG-IP系统的应用流量进行认证。

为此，LTM系统提供了多种称为认证模块的认证方案。这些***认证模块***使您能够使用远程系统对通过LTM系统的应用请求进行认证或授权。

要实施认证模块，可以使用Configuration工具来访问该工具的**Local Traffic**部分的Profile屏幕。通过这些屏幕，可以配置需要实施的认证模块的设置。

LTM认证模块

可以为远程认证实施的LTM模块包括：

- **小型目录访问协议（LDAP）**
  LTM系统可以使用存储在远程LDAP服务器或Microsoft® Windows Active Directory服务器上的数据对网络流量进行认证或授权。客户机证书基于基本的HTTP认证（用户名和密码）。

- **远程认证拨入用户服务（RADIUS）**
  LTM系统可以使用存储在远程RADIUS服务器上的数据对网络流量进行认证。客户机证书基于基本的HTTP认证（用户名和密码）。

- **TACACS+**
  LTM系统可以使用存储在远程TACACS+服务器上的数据对网络流量进行认证。客户机证书基于基本的HTTP认证（用户名和密码）。

- **SSL客户机证书LDAP**
  LTM系统可以使用存储在远程LDAP服务器上的数据对网络流量进行授权。客户机证书基于SSL证书以及定义的用户群和角色。

- **在线证书状态协议（OCSP）**
  LTM系统可以使用存储在远程OCSP服务器上的数据检查客户机证书的撤销状态。客户机证书基于SSL证书。

实施认证模块

使用LTM系统，可以实施前一部分列出的任何可用的认证模块。实施认证模块需要创建或配置以下对象：

- **RADIUS服务器或SSL OCSP响应器对象**
  该对象只对RADIUS和SSL OCSP认证模块是必需的。***服务器对象***和***响应器对象***由关于远程RADIUS服务器或OCSP响应器的设置组成。

- **配置对象**

这是通过一组可配置的设置控制认证模块的***配置对象***。配置对象设置的实例包括**Host**、**Service Port**和**Search Time Limit**等。

- **认证Profile**
  认证Profile是一种对象，它指定：您希望实施的认证模块的类型、上级Profile和配置对象（参见上一个步骤）。您既可以使用LTM系统为每种认证模块提供的缺省Profile，也可以创建定制Profile。有关Profile的背景信息，请参阅第5章“了解Profile”。

- **认证iRule**
  对于您希望实施的任何一种PAM模块，LTM系统都提供了必须与您的Profile和Real Server关联的相应缺省认证iRule。***认证iRule***是一种基于TCL的脚本，它根据相应Profile和配置对象的设置执行认证/授权行为。

在大多数情况下，您可以使用缺省的iRule，而不是创建定制的iRule。当需要实施多个相同类型的认证模块（如多个LDAP认证模块，每一个都有不同的配置对象和Profile设置）时，必需创建定制的iRules™。有关创建定制iRules的详细信息，请参阅第13章“编写iRules”。

实施认证模块的过程很简单。例如，要实施LDAP认证模块（这种模块通过用户名和密码认证，使用远程LDAP服务器对客户机流量进行认证），需要执行以下工作。请注意，该实例创建了一个定制Profile，并使用LTM系统提供的缺省iRule。

实施认证模块的步骤

1. 创建名为**my_ldap_config**的认证配置对象。有关创建LDAP认证配置对象的详细信息，请参阅第8-4页上的“创建LDAP配置对象”。

2. 创建名为**my_ldap_profile**的定制认证Profile，在该Profile中将认证模块类型指定为**LDAP**，指定上级Profile（缺省**LDAP Profile**或您创建的另一个定制Profile），并参考配置对象**my_ldap_config**。有关创建LDAP Profile的详细信息，请参阅第8-6页上的“创建LDAP Profile”。

3. 配置Real Server，以参考定制Profile**my_ldap_profile**和缺省认证iRule **auth_ldap**。有关如何配置Real Server设置的详细信息，请参阅第2章“配置Real Server”。

实施LDAP认证模块

LDAP认证模块是一种对通过LTM系统的客户机连接进行认证或授权的机制。当认证或授权数据存储在远程LDAP服务器或Microsoft® Windows“活动目录”服务器上，并且希望客户机证书基于基本的HTTP认证（也就是用户名和密码）时，该模块非常有用。

要实施LDAP认证模块，必须配置LTM系统来访问远程LDAP服务器上的数据。为此，必须创建：

- LDAP配置对象
- LDAP Profile

创建这些对象后，必须：
- 将LDAP Profile分配到Real Server。
- 将LDAP iRule分配到Real Server。

创建LDAP配置对象

创建LDAP配置对象时，需要配置各种设置。表8.1显示了为LDAP配置对象配置的设置和值。请注意，此表按照您在“新建认证配置”屏幕中看到的类别对设置进行分组。有关如何创建该对象的详细流程，请参阅第8-6页上的“创建LDAP配置对象的步骤”。

设置	说明	缺省值
常规属性		
Name	为配置对象指定一个唯一的名称。此设置是必需的。	无缺省值
Type	指定您希望实施的认证模块的类型。必须将该值设置为**LDAP**	无缺省值
配置		
Remote LDAP Tree	指定搜索库识别名	无缺省值
Hosts	列出LTM系统用来获取认证数据的LDAP服务器的地址	无缺省值
Service Port	指定用于LDAP服务的端口号	**389** (non-SSL) **636** (SSL-enabled)
LDAP Version	指定LDAP应用的版本号	**3**
Bind DN	指定要与其进行绑定的账户的识别名，以便执行搜索。这个搜索账户是用来进行搜索的只读账户。管理账户可以用作搜索账户。如果未指定管理识别名，那么就不进行绑定。只有当站点不允许匿名搜索时，该设置才是必需的。 如果远程服务器是Microsoft® Windows“活动目录”服务器，那么必须以电子邮件地址的形式显示识别名。	无缺省值
Bind Password	指定在LDAP服务器上创建的*搜索*账户的密码。如果使用**bind**识别名，那么该设置是必需的。	无缺省值
Confirm Bind Password	确认**bind**识别名的密码。该设置是可选的。	无缺省值
Search Time Limit	指定搜索的时限。	**30**
Bind Time Limit	指定绑定时限。	**30**
Filter	指定过滤器。该设置用于授权客户机流量。	无缺省值
Login Attribute	指定登录属性。通常，该设置的值是**uid**；但如果服务器是Microsoft Windows“活动目录”服务器，那么该值必须是账户名**SAMACCOUNTNAME**（不区分大小写）。	无缺省值
Group DN	指定群识别名。该设置用于授权客户机流量。	无缺省值
Group Member Attribute	指定群成员属性。该设置用于授	无缺省值

设置	说明	缺省值
	权客户机流量。	
SSL	允许的值包括：**Enabled**、**Disabled**和**Start TLS**。请注意，当启用时，LTM系统将服务端口号从**389**改为**636**。	**Disabled**
Check SSL Peer	当启用时，检查SSL对等体。	**Disabled**
SSL CA Certificate	指定SSL CA证书的名称。允许的值包括：**None**、**Default**和**Specify Full Path**。	**None**
SSL Client Key	指定SSL客户机密钥的名称。允许的值包括：**None**、**Default**和**Specify Full Path**。	**None**
SSL Client Certificate	指定SSL客户机证书的名称。允许的值包括：**None**、**Default**和**Specify Full Path**。	**None**
SSL Ciphers	指定SSL密码	无缺省值
Ignore Unknown User	当启用时，让LTM系统忽略未知用户。	**Disabled**
Warning Logging	启用或禁用警告消息。	**Enabled**
Debug Logging	启用或禁用LOG_DEBUG级别的调试信息。正常情况下不建议使用。	**Disabled**

***表8.1** LDAP配置对象的设置*

创建LDAP配置对象的步骤

1. 在Main选项卡上，展开**Local Traffic**。
2. 点击**Profiles**。
   将打开Profiles屏幕。
3. 从Authentication菜单中，选择Configurations。
4. 在屏幕的右上角，点击**Create**。
   此操作将显示New Configuration屏幕。
5. 对于**Name**设置，为配置对象输入一个唯一的名称，例如**my_ldap_config**。
6. 对于**Type**设置，选择**LDAP**。
   屏幕将扩展，显示若干设置。
7. 修改或保留所有显示的设置的值。
   （要配置高级设置，请定位至**Configuration**标题，然后选择**Advanced**。）
8. 点击**Finished**。

创建LDAP Profile+

创建LDAP配置对象之后，必须创建或配置LDAP Profile。此操作可以通过修改缺省的**LDAP** Profile来进行，也可以通过创建继承缺省Profile设置的定制Profile来进行。认证Profile的一项重要功能是参考已创建的现有配置对象。

在大多数情况下，缺省Profile应能满足您的需求。但是，即使您使用缺省Profile，也必须对其进行修改，指定您创建的相应配置对象。

如果选择创建定制Profile，那么必须指定符合以下条件的上级Profile（定制Profile或缺省Profile）：即该上级Profile包含希望新Profile继承的值。

创建LDAP Profile时，需要配置一些设置。表8.2显示了组成LDAP Profile的设置和值。有关创建LDAP Profile的详细流程，请参阅第8-7页上的“修改缺省LDAP Profile的步骤”，或参阅第8-7页上的“创建定制LDAP Profile的步骤”。

设置	说明	缺省值
Name	为Profile指定一个唯一的名称。此设置是必需的。	无缺省值
Type	指定您希望实施的认证模块的类型。必须将该值设置为**LDAP**。	无缺省值
Parent Profile	指定希望从中继承值的Profile。	**ldap**
Mode	指定是启用还是禁用Profile。可能的设置包括**Auto**、**Enabled**和**Disabled**。	**Enabled**
Configuration	指定一个现有的LDAP配置对象。此设置是必需的。	无缺省值
Rule	指定现有认证iRule的名称。如果不指定iRule，LTM系统将使用相应的缺省iRule。	**auth_ldap**
Idle Timeout	以秒为单位，指定认证或授权请求在超时前的空闲持续时间。您可以使用缺省值，指定一个不同的值，还可以选择**Indefinite**。	**300**

***表8.2** LDAP Profile的设置*

修改缺省LDAP Profile的步骤

1. 在Main选项卡上，展开**Local Traffic**。
2. 点击**Profiles**。
   将打开Profiles屏幕。
3. 从Authentication菜单中，选择Profiles。
   此操作将显示缺省认证Profile的列表。
4. 在Name栏中，点击**ldap**。
5. 对于**Mode**设置，选择**Enabled**或**Auto**。
6. 对于**Configuration**设置，从列表中选择配置对象。请注意，不允许选择值**None**。
7. 对于**Rule**设置，指定认证iRule：
   - 如果希望使用缺省iRule **auth_ldap**，请将设置保留为原状。
   - 如果不想使用缺省iRule **auth_ldap**，请选择已创建的现有iRule的名称。
8. 点击**Finished**。

创建定制LDAP Profile的步骤

1. 在Main选项卡上，展开**Local Traffic**。
2. 点击**Profiles**。
   将打开Profiles屏幕。
3. 从Authentication菜单中，选择Profiles。
4. 在屏幕的右上角，点击**Create**。
   此操作将显示New Profiles屏幕。
5. 对于**Name**设置，为Profile输入一个唯一的名称，例如**my_ldap_profile**。
6. 对于**Type**设置，选择**LDAP**。
   屏幕将扩展，显示其它设置。
7. 对于**Parent Profile**设置，执行以下操作：

- 如果要将缺省Profile **ldap**用于上级Profile，请将设置保留为原状。
- 如果要将定制Profile用于上级Profile，请从列表中选择定制Profile的名称。

8. 对于**Mode**设置，选择**Enabled**或**Auto**。
9. 对于**Configuration**设置，从列表中选择配置对象。
10. 对于**Rule**设置，指定认证iRule：
    - 如果希望使用缺省iRule **auth_ldap**，请将设置保留为原状。
    - 如果不想使用缺省iRule **auth_ldap**，请选择已创建的现有iRule的名称。
11. 点击**Finished**。

创建LDAP配置对象和LDAP Profile后，必须执行以下操作：

- 通过配置Real Server的**Authentication Profile**设置，将Profile分配到Real Server。
- 通过配置Real Server的**Rule**设置，将缺省**auth_ldap** iRule分配到Real Server。

有关如何配置Real Server设置的信息，请参阅第2章“配置Real Server”。

实施RADIUS认证模块

RADIUS认证模块是一种认证通过LTM系统进行客户机连接的机制。认证数据存储在远程RADIUS服务器时使用该模块。在这种情况下，客户机证书基于基本的HTTP认证（也就是，用户名和口令）。

为实施RADIUS认证模块，必须配置LTM系统来访问远程RADIUS服务器的数据。为此，必须创建：

- 一个或多个高级RADIUS服务器对象
- RADIUS配置对象
- RADIUSProfile

创建这些对象后，必须：

- 将RADIUSProfile分配到Real Server。
- 将RADIUS iRule分配到Real Server。

创建RADIUS服务器对象

创建RADIUS服务器对象时，需要配置一些设置。表8.3显示了组成缺省RADIUS服务器对象的设置和值。有关创建服务器对象的详细流程，请参阅第8-10页上的“创建RADIUS服务器对象的步骤”。

设置	说明	缺省值
Name	为RADIUS服务器对象指定一个唯一的名称，例如**my_radius_object**。此设置是必需的。	无缺省值
Host	指定RADIUS服务器的主机名称或IP地址。此设置是必需的。	无缺省值
Service Port	指定RADIUS认证流量的端口。	**1812**
Secret	设置用于加密或解密从服务器发送或接收的数据包的密钥。此	无缺省值

设置	说明	缺省值
Confirm Secret	设置是必需的。 确认为**密钥**设置提供的密钥。此设置是必需的。	无缺省值
Timeout	指定超时值	**3**

表8.3 *RADIUS服务器定义的设置*

创建RADIUS服务器对象的步骤

1. 在Main选项卡上，展开**Local Traffic**。
2. 点击**Profiles**。
   将打开Profiles屏幕。
3. 从Authentication菜单中，选择RADIUS Servers。
   此操作将显示RADIUS Server List屏幕。
4. 在屏幕的右上角，点击**Create**。
5. 对于**Name**设置，为RADIUS服务器对象输入一个唯一的名称，例如**my_radius_server**。
6. 对于**Server**设置，为远程RADIUS服务器输入一个主机名或IP地址。
7. 对于**Secret**和**Confirm Secret**设置，输入RADIUS密钥。
8. 保留或修改所有其它设置。
9. 点击**Finished**。
10. 对于冗余RADIUS服务器，重复这些步骤以创建其它服务器对象。

创建RADIUS配置对象

创建RADIUS配置对象时，需要配置各种设置。表8.5显示了组成RADIUS配置对象的设置和值。请注意，此表按照您在“新建认证配置”屏幕中看到的类别对设置进行分组。有关如何创建该配置对象的详细流程，请参阅第8-11页上的“创建RADIUS配置对象的步骤”。

设置	说明	缺省值
Name	为配置对象指定一个唯一的名称。此设置是必需的。	无缺省值
Type	指定您希望实施的认证模块的类型。必须将该值设置为**RADIUS**。	无缺省值
RADIUS Servers	列出LTM用来获取认证数据的RADUIS服务器的IP地址。 请注意，对于列出的每一个服务器，必须创建相应的RADIUS服务器定义。RADIUS服务器定义指定服务器名称、端口号、RADIUS密钥和超时值。有关详细信息，请参阅表8.3。	无缺省值
Client ID	通过字符串栏发送NAS标识符RADIUS属性。如果不指定**Client ID**设置的值，就使用PAM服务类型代替。通过指定空客户机ID,可以禁用该特性。	无缺省值
Debug Logging	启用LOG_DEBUG级别的SYSLOG调试信息。正常情况下我们不建议使用该选项。	**Disable**
Accounting Bug	禁止确认账户管理的响应矢量。该选项应该仅适用于较早的服	**Disable**

设置	说明	缺省值
Retries	务器。 指定在认证失败前LTM系统允许的认证重试次数。	**3**

表8.4 RADIUS配置对象的设置

创建RADIUS配置对象的步骤

1. 在Main选项卡上，展开**Local Traffic**。
2. 点击**Profiles**。
   将打开Profiles屏幕。
3. 从Authentication菜单中，选择Configuration。
4. 在屏幕的右上角，点击**Create**。
   此操作将显示New Confugurations屏幕。
5. 对于**Name**设置，为配置对象指定一个唯一的名称，例如**my_radius_config**。
6. 对于**Type**设置，选择**RADIUS**。
   屏幕将扩展，显示若干设置。
7. 修改或保留所有显示的设置的值。
   （要配置高级设置，请定位至**Configuration**标题，然后选择**Advanced**。）
8. 点击**Finished**。

创建RADIUS Profile

创建RADIUS配置对象之后，必须创建或配置RADIUSProfile。此操作可以通过修改缺省的**radius** Profile来进行，也可以通过创建继承缺省Profile设置的定制Profile来进行。认证Profile的一项重要功能是参考现有的配置对象。

在大多数情况下，缺省Profile应能满足您的需求。但是，即使您使用缺省Profile，也必须对其进行修改，指定您创建的相应配置对象。

如果选择创建定制Profile，那么必须指定符合以下条件的上级Profile（定制Profile或缺省Profile）：即该上级Profile包含希望新Profile继承的值。

创建RADIUSProfile时，需要配置各种设置。表8.5显示了组成RADIUSProfile的设置和值。有关创建RADIUSProfile的详细流程，请参阅第8-12页上的“修改缺省RADIUSProfile的步骤”，或参阅第8-13页上的“创建定制RADIUSProfile的步骤”。

设置	说明	缺省值
Name	为Profile指定一个唯一的名称。此设置是必需的。	无缺省值
Type	指定您希望实施的认证模块的类型。必须将该值设置为**RADIUS**。	无缺省值
Parent Profile	指定希望从中继承值的Profile。	**radius**
Mode	指定启用还是禁用Profile。可能的设置包括**Auto**、**Enabled**和**Disabled**	**Enabled**
Configuration	指定一个现有的RADIUS配置对象。	无缺省值
Rule	指定现有认证规则的名称。如果不指定iRule，LTM系统将使用	**auth_radius**

设置	说明	缺省值
Timeout	相应的缺省iRule。 以秒为单位，指定认证或授权请求在超时前的空闲持续时间。您可以使用缺省值，指定一个不同的值，还可以选择**Indefinite**。	**300**

表8.5 RADIUS Profile设置

修改缺省RADIUSProfile的步骤

1. 在Main选项卡上，展开**Local Traffic**。
2. 点击**Profiles**。
   将打开Profiles屏幕。
3. 从Authentication菜单中，选择Profiles。
   此操作将显示缺省认证Profile的列表。
4. 在Name栏中，点击**radius**。
5. 对于**Mode**设置，选择**Enabled**或**Auto**。
6. 对于**Configuration**设置，从列表中选择配置对象。请注意，不允许选择设置**None**。
7. 对于**Rule**设置，指定认证iRule：
   - 如果希望使用缺省iRule **auth_radius**，请将设置保留为原状。
   - 如果不想使用缺省iRule **auth_radius**，请选择已创建的现有iRule的名称。
8. 点击**Finished**。

创建定制RADIUSProfile的步骤

1. 在Main选项卡上，展开**Local Traffic**。
2. 点击**Profiles**。
   将打开Profiles屏幕。
3. 从Authentication菜单中，选择Profiles。
4. 在屏幕的右上角，点击**Create**。
   此操作将显示New Profiles屏幕。
5. 在**Name**设置中，为RADIUSProfile输入一个唯一的名称，例如**my_radius_profile**。
6. 在**Type**设置中，选择**RADIUS**。
   屏幕将扩展，显示其它设置。
7. 对于**Parent Profile**设置，执行以下操作：
   - 如果要将缺省Profile **radius**用于上级Profile，请将设置保留为原状。
   - 如果要将定制Profile用于上级Profile，请从列表中选择定制Profile的名称。
8. 在**Mode**设置中，选择**Enabled**或**Auto**。
9. 在**Configuration**设置中，从列表中选择配置对象。
10. 对于**Rule**设置，指定认证iRule：
    - 如果希望使用缺省iRule **auth_radius**，请将设置保留为原状。
    - 如果不想使用缺省iRule **auth_radius**，请选择已创建的现有iRule的名称。
11. 点击**Finished**。

创建RADIUS服务器对象、RADIUS配置对象和RADIUSProfile后，必须执行以下操作：

- 通过配置Real Server的**Autentication Profile**设置，将Profile分配到Real Server。
- 通过配置Real Server的**Rule**设置，将缺省**auth_radius** iRule分

配到Real Server。

有关如何配置Real Server设置的信息，请参阅第2章“配置Real Server”。

实施TACACS+认证模块

TACACS+认证模块是用来对通过LTM系统的客户机连接进行认证的机制。当认证数据存储在远程TACACS+服务器上时使用该模块。在这种情况下，客户机证书基于基本的HTTP认证（也就是用户名和密码）。

要实施TACACS+认证模块，必须配置LTM系统来访问远程TACACS+服务器上的数据。为此，必须创建：

- TACACS+配置对象
- TACACS+ Profile

创建这些对象后，必须：

- 将TACACS+ Profile分配到Real Server。
- 将TACACS+ iRule分配到Real Server。

创建TACACS+配置对象

创建TACACS+配置对象时，需要配置各种设置。表8.6显示了组成缺省TACACS+配置对象的设置和值。请注意，此表按照您在“新建认证设置”屏幕中看到的类别对设置进行分组。有关如何创建该对象的详细流程，请参阅第8-15页上的“创建TACACS+配置对象的步骤”。

设置	说明	缺省值
Name	为配置对象指定一个唯一的名称。此设置是必需的。	无缺省值
Type	指定要实施的认证模块的类型。必须将此值设置为**TACACS+**。	无缺省值
Servers	指定TACACS+服务器的主机名称或IP地址。此设置是必需的。	无缺省值
Secret	设置用于加密和解密发送到或接收自服务器的数据包的密钥。此设置是必需的。	无缺省值
Confirm Secret	确认为**Secret**设置提供的密钥。此设置是必需的。	无缺省值
Encryption	启用或禁用TACACS+数据包的加密。建议在正常情况下使用。	**Enabled**
Service Name	指定TACACS+服务器的接听设备，例如**PPP**。	无缺省值
Protocol Name	指定TACACS+服务器的接听设备，例如**lcp**。	无缺省值
Authentication	指定认证选项。可能的值包括**Authenticate to first server**和**Authenticate to each server until success**。	**Authenticate to first server**
Accounting Information	如果定义了多个TACACS+服务器并启用了PAM会话账户，那么将账户的开始和结束数据包发送到第一个可用的服务器或发送到所有服务器。可能的值包括**Send to first available serve** 和 **Send to all servers**。	**Send to first available server**

设置	说明	缺省值
Debug Logging	启用LOG_DEBUG级别的SYSLOG调试信息。不建议在正常情况下使用。	**Disable**

表8.6 TACACS+*配置对象的设置*

创建TACACS+配置对象的步骤

1. 在Main选项卡上，展开**Local Traffic**。
2. 点击**Profiles**。
   将打开Profiles屏幕。
3. 从Authentication菜单中，选择Configurations。
4. 在屏幕的右上角，点击**Create**。
   此操作将显示New Configuration屏幕。
5. 对于**Name**设置，为配置对象指定一个唯一的名称，例如**my_tacacs_config**。
6. 对于**Type**设置，选择**TACACS+**。
   屏幕将扩展，显示若干设置。
7. 修改或保留所有显示的设置的值。
   （要配置高级设置，请定位至**Configuration**标题，然后选择**Advanced**。）
8. 点击**Finished**。

创建TACACS+ Profile

创建TACACS+配置对象之后，必须创建或配置TACACS+ Profile。此操作可以通过修改缺省的**tacacs+ Profile**来进行，也可以通过创建继承缺省Profile设置的定制Profile来进行。认证Profile的一项重要功能是参考现有的配置对象。

在大多数情况下，缺省Profile应能满足您的需求。但是，即使您使用缺省Profile，仍必须对其进行修改，指定您创建的相应配置对象。

如果选择创建定制Profile，那么必须指定符合以下条件的上级Profile（定制Profile或缺省Profile）：即该上级Profile包含希望新Profile继承的值。

创建TACACS+ Profile时，将配置各种设置。表8.7显示了组成TACACS+ Profile的设置和值。有关创建TACACS+ Profile的详细流程，请参阅第8-16页上的“修改缺省TACACS+ Profile的步骤”，或参阅第8-17页上的“创建定制TACACS+ Profile的步骤”。

设置	说明	缺省值
Name	为Profile指定一个唯一的名称。此设置是必需的。	无缺省值
Type	指定要实施的认证模块的类型。必须将此值设置为**TACACS+**。	无缺省值
Parent Profile	指定希望从中继承值的Profile。	**tacacs+**
Mode	指定是启用还是禁用Profile。可能的设置包括**Auto**、**Enabled**和**Disabled**。	**Enabled**
Configuration	指定一个现有的TACACS+配置对象。	无缺省值
Rule	指定现有认证规则的名称。如果不指定iRule，LTM系统将使用相应的缺省iRule。	**auth_tacacs+**
Idle Timeout	以秒为单位，指定认证或授权请求在超时前的空闲持续时间。您可以使用缺省值，指定一个不同的值，还可以选择**Indefinite**。	**300**

表8.7 TACACS+ Profile的设置

修改缺省TACACS+ Profile的步骤

1. 在Main选项卡上，展开**Local Traffic**。
2. 点击**Profiles**。
   将打开Profiles屏幕。
3. 从Authentication菜单中，选择Profiles。
   此操作将显示缺省认证Profile的列表。
4. 在Name栏中，点击**tacacs+**。
5. 对于**Mode**设置，选择**Enabled**或**Auto**。
6. 对于**Configuration**设置，从列表中选择配置对象。请注意，不允许选择设置**None**。
7. 对于**Rule**设置，指定认证iRule：
   - 如果希望使用缺省iRule **auth_tacacs**，请将设置保留为原状。
   - 如果不想使用缺省iRule **auth_tacacs**，请选择已创建的现有iRule的名称。
8. 点击**Finished**。

创建定制TACACS+ Profile的步骤

1. 在Main选项卡上，展开**Local Traffic**。
2. 点击**Profiles**。
   将打开Profiles屏幕。
3. 从Authentication菜单中，选择Profiles。
4. 在屏幕的右上角，点击**Create**。
   此操作将显示New Profile屏幕。
5. 对于**Name**设置，为Profile指定一个唯一的名称。
6. 对于**Type**设置，选择**TACACS+**。
7. 对于**Parent Profile**设置，执行以下操作：
   - 如果要将缺省Profile **tacacs**用作上级Profile，请将设置保留为原状。
   - 如果要将定制Profile用作上级Profile，请从列表中选择定制Profile的名称。
8. 对于**Mode**设置，选择**Enabled**或**Auto**。
9. 对于**Configuration**设置，从列表中选择配置对象。
10. 对于**Rule**设置，指定认证iRule：
    - 如果希望使用缺省iRule **auth_tacacs**，请将设置保留为原状。
    - 如果不想使用缺省iRule **auth_tacacs**，请选择已创建的现有iRule的名称。
11. 点击**Finished**。

创建TACACS+配置对象和TACACS+ Profile后，必须执行以下操作：

- 通过配置Real Server的**Authentication Profile**设置，将Profile分配到Real Server。
- 通过配置Real Server的**Rules**设置，将缺省的**auth_tacacs** iRule分配到Real Server。

有关如何配置Real Server设置的信息，请参阅第2章“配置Real Server”。

实施SSL客户机证书LDAP认证模块

SSL客户机证书LDAP认证模块是用来对通过LTM系统的客户机连接进行认证或授权的机制。在此情形中，客户机认证信息基于SSL证书认证信息，而不是基于用户名和密码；LDAP客户机授权不仅基于SSL证书，而且基于您定义的用户群和角色。

◆ **重要信息**

*实施SSL客户机证书LDAP认证模块之前，必须配置并实施**Client SSL Profile**。在该Profile中，**Mode**配置设置的值必须设置为**Auto**或**Enabled**。*

了解SSL客户机证书授权

使用SSL客户机证书LDAP授权，LTM系统可以基于可信CA签发的签名客户机证书对客户机进行授权。然后，要进一步增强系统对客户机请求进行授权的能力，您还可以指定群和角色。使授权基于证书以及群和角色进行，这提供了控制客户机对系统资源的访问时所需的灵活性。

能够实施SSL客户机证书LDAP模块之前，必须了解两种不同类型的认证信息，LTM系统使用它们来对使用远程LDAP服务器上数据的应用流量进行授权。这两类认证信息是：

- SSL证书
- 群和角色

使用SSL证书进行LDAP授权

对客户机进行授权的过程中，LTM系统必须搜索LDAP数据库。使用基于证书的授权时，系统可以三种方式搜索LDAP数据库：

- **用户**
  很多LDAP服务器环境已将证书集成到存储在LDAP数据库中的用户信息中。在LDAP服务器环境中，配置授权的方法之一是将系统配置为比较入站证书和存储在LDAP数据库中且与客户机请求关联的用户证书。如果在用户的LDAP Profile中找到证书，则授予用户访问权限并批准请求。
- **证书映射**
  如果创建用于将证书映射到LDAP数据库中的用户的对象和类，那么可以将系统配置为在映射中搜索证书以及从该映射中检索用户。然后，系统将进行检查，确保LDAP数据库中的用户是有效的用户。
- **证书**
  如果证书未存储在LDAP数据库中，那么可以将系统配置为从作为入站客户机请求的一部分而出示的证书中提取用户名。然后，系统将检查LDAP数据库中是否存在用户条目。对于自己担当证书授权机构的公司，此方案是一个不错的选择。通过该方案公司可以确定证书是否经过验证，然后对用户进行授权。

不论执行何种类型的基于证书的授权，该过程都将产生表8.8中所示的结果。

搜索的结果	授权状态
无匹配记录	授权失败
一个匹配记录	授权成功，且服从群和角色的限制
两个或多个匹配记录	授权失败，原因是数据库条目无效

***表8.8** 搜索结果和相应的授权状态*

使用群和角色进行LDAP授权

除了启用基于证书的授权，还可以基于群和角色来配置授权。

- **群**
  因为LDAP服务器中已经建立了群的概念和结构，所以LTM系统可以在其授权特性中包括群。要使群能够用于授权，必须指明基础和范围，系统将按照这些条件在LDAP数据库中搜索群。此外，还必须指定群名称和成员名称的设置值。完成这些任务后，系统便可在有效群的列表中进行搜索，直至找到当前用户是其成员的群。
- **角色**
  与群不同，角色是直接与用户关联的设置。LTM系统执行的任何基于角色的授权都依赖内建有角色概念的LDAP数据库。为了确定是否应授予用户对资源的访问权限，LTM系统在分配给该用户的角色中进行搜索，并尝试将该角色与管理员定义的有效角色进行匹配。

要实施SSL客户机证书LDAP授权，必须将LTM系统配置为访问远程LDAP服务器上的数据。为此，必须创建：

- SSL客户机证书LDAP配置对象
- SSL客户机证书LDAP Profile

创建这些对象后，必须：

- 将SSL客户机证书LDAP Profile分配给Real Server。
- 将SSL客户机证书LDAP iRule分配给Real Server。

创建SSL客户机证书LDAP配置对象

SSL客户机证书LDAP配置对象由一组数据和指令组成。相应的外部LDAP服务器在处理来自LTM系统的授权请求时，需要这组数据和指令。

创建SSL客户机证书LDAP配置对象时，您将配置各种设置。表8.9列出并介绍了可在此配置对象中指定的设置。请注意，此表按照您在“新建认证配置”屏幕中看到的类别对设置进行分组。有关如何配置此对象的详细流程，请参阅第8-22页上的“创建SSL客户机证书LDAP配置对象的步骤”。

设置	说明	缺省值
Name	为配置对象指定一个唯一的名称。此设置是必需的。	无缺省值
Type	指定要实施的认证模块的类型。必须将此值设置为**SSL Client Certificate LDAP**。	无缺省值
Hosts	列出LTM系统将用来获取授权数据的LDAP服务器的IP地址，包括端口号。	无缺省值
Search Type	指定系统搜索LDAP数据库时，所使用的基于证书的授权方法（第8-18页上的“使用SSL证书进行LDAP授权”中进行了介绍）。可能的值包括**User**、**Certificate Map**和**Certificate**。	**User**
User Base DN	指定**User**和**Certificate**这两种搜索类型使用的子树的搜索基础。典型的搜索基础是：**ou=people,dc=company,dc=com**。有关详细信息，请参阅**Search Type**设置。	无缺省值

设置	说明	缺省值
User Key	指定LDAP数据库中，指定用户ID的属性的名称。此设置供**User**搜索类型使用。用户密钥值的典型实例是**uid**。有关详细信息，请参阅**Search Type**设置。	无缺省值
Cache Size	指定允许SSL会话缓存使用的最大容量。将此值设置为**0**表示不允许SSL会话缓存。	**20000**
Cache Timeout	以秒为单位，指定可协商的SSL会话ID的可用寿命。如果超过此时间，客户机必须协商新会话。	**300**
Secure	指示LTM系统在系统和LDAP服务器之间使用安全通信（即SSL/TLS）。	**Disabled**
Admin DN	指定要与其进行绑定的账户的识别名，以便执行搜索。这个*搜索*帐户是用来进行搜索的只读帐户。**Admin**账户可以用作*搜索*账户。如果未指定管理DN，将不尝试绑定。仅当站点不允许匿名搜索时才需要此设置。	无缺省值
Admin Password	为LDAP服务器上创建的*搜索*账户指定密码。	无缺省值
Confirm Admin Password	确认为LDAP服务器上创建的*搜索*账户指定的密码。	无缺省值
Group Base DN	指定群搜索使用的子树的搜索基础。仅当指定了有效群时才使用此参数。典型的搜索基础类似于：**ou=people,dc=company,dc=com**。	无缺省值
Group Key	指明LDAP数据库中，指定群子树中的群名称的属性的名称。	无缺省值
Group Member Key	指明LDAP数据库中，指定群成员（DN）的属性的名称。	无缺省值
Valid Groups	指定用户要获得授权，就必须属于其中的群的列表。此选项可以指定多次。要获得授权，客户机仅需是字符串中指定的某个群的成员。	无缺省值
Role Key	指明LDAP数据库中，指定用户授权角色的属性的名称。仅当使用有效角色（如下一条中所述）时才使用此密钥。	无缺省值
Valid Roles	指定角色列表。要获得授权，用户必须分配为这些角色之一。此列表中的有效角色以空格进行分隔。此选项可以指定多次。要获得授权，客户机仅需是字符串中指定的某个角色的成员。	无缺省值

***表8.9** SSL客户机证书LDAP配置对象的设置*

创建SSL客户机证书LDAP配置对象的步骤

1. 在Main选项卡上，展开**Local Traffic**。
2. 点击**Profiles**。
   将打开Profiles屏幕。
3. 从Authentication菜单中，选择Configuration。
4. 在屏幕的右上角，点击**Create**。
   此操作将显示New Configuration屏幕。
5. 对于**Name**设置，为配置对象指定一个唯一的名称。
6. 对于**Type**设置，选择**SSL Client Certificate LDAP**。
7. 修改或保留所有其它设置的值。
   （要配置高级设置，请定位至**Configuration**标题，然后选择**Advanced**。）
8. 点击**Finished**。

创建SSL客户机证书LDAP授权Profile

创建SSL客户机证书LDAP配置对象之后，必须创建或配置相应的Profile。此操作可以通过修改缺省的**ssl_cc_LDAP Profile**来进行，也可以通过创建继承缺省Profile设置的定制Profile来进行。认证Profile的一项重要功能是参考现有的配置对象。

在大多数情况下，缺省Profile应能满足您的需求。但是，即使您使用缺省Profile，仍必须对其进行修改，指定您创建的相应配置对象。

如果选择创建定制Profile，那么必须指定符合以下条件的上级Profile（定制Profile或缺省Profile）：即该上级Profile包含希望新Profile继承的值。

创建SSL客户机证书LDAP Profile时，您将配置各种设置。表8.10显示了组成SSL客户机证书LDAP Profile的设置和值。有关创建此类Profile的详细流程，请参阅第8-23页上的“修改缺省SSL客户机证书LDAP Profile的步骤”，或参阅第8-24页上的“创建定制SSL客户机证书LDAP Profile的步骤”。

设置	说明	缺省值
Name	为Profile指定一个唯一的名称。此设置是必需的。	无缺省值
Type	指定要实施的认证模块的类型。必须将此值设置为**LDAP（SSL Client Certificate）**。	无缺省值
Parent Profile	指定希望从中继承值的Profile。	**ssl_cc_ldap**
Mode	指定是启用还是禁用Profile。可能的设置包括**Auto**、**Enabled**和**disabled**。	**Enabled**
Configuration	指定现有的SSL客户机证书LDAP配置对象。	无缺省值
Rule	指定现有认证iRule的名称。如果不指定iRule，LTM系统将使用相应的缺省iRule。	**auth_ssl_cc_ldap**
Idle Timeout	以秒为单位，指定授权请求在超时前的空闲持续时间。您可以使用缺省值，指定一个不同的值，还可以选择**Indefinite**。	**300**

***表8.10** SSL客户机证书LDAP Profile的设置*

修改缺省SSL客户机证书LDAP Profile的步骤

1. 在Main选项卡上，展开**Local Traffic**。
2. 点击**Profiles**。
   将打开Profiles屏幕。
3. 从Authentication菜单中，选择Profiles。
   此操作将显示缺省认证Profile的列表。
4. 在Name栏中，点击**ssl_cc_ldap**。
5. 对于**Mode**设置，选择**Enabled**或**Auto**。
6. 对于**Configuration**设置，从列表中选择配置对象。请注意，不允许选择设置**None**。
7. 对于**Rule**设置，指定认证iRule：
   - 如果希望使用缺省iRule **auth_ssl_cc_ldap**，请将设置保留为原状。
   - 如果不想使用缺省iRule **auth_ssl_cc_ldap**，请选择已创建的现有iRule的名称。
8. 点击**Finished**。

创建定制SSL客户机证书LDAP Profile的步骤

1. 在Main选项卡上，展开**Local Traffic**。
2. 点击**Profiles**。
   将打开Profiles屏幕。

3. 从Authentication菜单中，选择Profiles。
4. 在屏幕的右上角，点击**Create**。
   此操作将显示New Profile屏幕。
5. 对于**Name**设置，为Profile指定一个唯一的名称。
6. 对于**Type**设置，选择SSL客户机证书LDAP。
7. 对于**Parent Profile**设置，执行以下操作：
   - 如果要将缺省Profile**ssl_cc_ldap**用作上级Profile，请将设置保留为原状。
   - 如果要将定制Profile用作上级Profile，请从列表中选择定制Profile的名称。
8. 对于**Mode**设置，点击屏幕右侧的“定制”框，然后选择**Enabled**或**Auto**。
9. 对于**Configuration**设置，点击屏幕右侧的Custom框，然后从列表中选择一个配置对象。
10. 对于**Rule**设置，点击屏幕右侧的“定制”框，然后指定一个认证iRule：
    - 如果希望使用缺省iRule **auth_ssl_cc_ldap**，请将设置保留为原状。
    - 如果不想使用缺省iRule **auth_ssl_cc_ldap**，请选择已创建的现有iRule的名称。
11. 点击**Finished**。

创建SSL客户机证书LDAP配置对象和SSL客户机证书LDAP Profile之后，必须执行以下操作：

- 通过配置Real Server的**Authentication**、**Profile**设置，将Profile分配到Real Server。
- 通过配置Real Server的**Rule**设置，将缺省的**auth_ssl_cc_ldap** iRule分配到Real Server。

实施SSL OCSP认证模块

SSL OCSP认证模块是用来对通过LTM系统的客户机连接进行认证的机制。更确切地说，SSL OCSP认证模块检查SSL证书的撤销状态，这是对该证书进行认证的一部分。

在线证书状态协议（OCSP）是一种第三方软件应用和业界标准协议，它提供了使用公匙技术时的证书撤销列表（CRL）的替代方案。***CRL***是已撤销的客户机证书的列表，服务器系统可以在验证客户机证书的流程中检查该列表。

希望使用OCSP代替CRL作为检查SSL证书撤销状态的机制时，便可实施SSL OCSP认证模块。

LTM系统既支持CRL协议，也支持OCSP协议。如果希望使用CRL代替OCSP，请配置SSL Profile。有关CRL的详细信息，请参阅第7章“管理SSL流量”。

有关OCSP的详细信息，请参阅***http://www.ietf.org***上的RFC 2560。

了解OCSP

与使用CRL相比，使用OCSP来检查客户机证书的撤销状态有着截然不同的优势。以下各小节介绍了CRL和OCSP之间的差异，以及OCSP的工作方式。

CRL的局限性

随客户机证书一起出示时，LTM系统有时需要在接受证书，然后将连接转发至目标服务器之前，评估该证书的撤销状态。评估撤销状态的标准方法是CRL，CRL存储在配置中的各台计算机上的独立CRL文件中。尽管CRL被视为检查SSL证书撤销状态的标准方法，但CRL仅以固定的时间间隔更新，这将导致检查状态时，CRL中的信息已过时的风险。

此外，必须在每台计算机上存储独立的CRL文件也会导致其它一些局限性：

- 所有CRL文件都必须保持同步。
- 在每台计算机上存储独立的CRL文件会引起安全性方面的风险。
- 无法从一个中心位置管理多个CRL文件。

OCSP的优势

OCSP确保LTM系统在证书验证流程中，始终能够获得实时撤销状态。

OCSP基于客户机/服务器模型。在此模型中，客户机系统请求证书的撤销状态，服务器系统发送响应。因此，实施SSL OCSP认证模块时，LTM系统充当OCSP客户机，称为OCSP响应器的外部系统充当OCSP服务器。所以，***OCSP响应器***是根据请求将证书撤销状态发送到LTM系统的外部服务器。

OCSP的工作方式

通常，接收到来自客户机应用的SSL证书后，LTM系统（充当OCSP客户机）向OCSP响应器请求证书撤销状态，然后阻止连接，直至接收到来从该响应器的状态。如果来自响应器的状态显示证书已撤销，LTM系统将拒绝证书和连接。如果来自响应器的状态显示证书仍有效，LTM将继续其正常证书验证流程，对客户机应用进行认证。

更确切地说，应用客户机发送用于认证的证书时，LTM系统将按照以下流程进行操作：

- 首先，LTM系统检查证书的签发者是否列在可信CA文件中。
- 如果证书列在其中，LTM系统接下去将检查证书是否已撤销。没有OCSP时，如果LTM系统上配置了CRL选项，LTM系统将通过读取证书撤销列表（CRL）来检查撤销状态。但有OCSP时，LTM系统将绕过CRL，准备将撤销状态请求发送到相应的OCSP响应器。
- 然后，LTM系统检查原始客户机证书的Issuer字段中指定的CA，并据此选择OCSP响应器。
- 下一步，LTM系统尝试将该CA与SSL OCSP Profile中列出的CA进行匹配。
- 如果存在匹配，LTM系统将检查客户机证书的**AuthorityInfoAcces***LDAPProfile*字段（如果该字段存在）中的目标URL，并使用该URL将证书撤销状态请求发送到OCSP响应器。
- 如果在SSL OCSP Profile中启用了**Ignore AIA**参数，LTM系统将转为使用相匹配的SSL OCSP Profile的url参数中指定的URL，发送证书撤销状态请求。
- 如果不存在匹配，LTM系统将检查系统中定义的另一个SSL OCSP Profile的**calist**设置。如果检查了所有的SSL OCSP Profile，没有找到任何匹配，证书验证将失败，LTM系统将拒绝

原始客户机请求。

- 如果进行了相应的配置，LTM系统会在接收到来自响应器的证书撤销状态后，将证书状态标头插入原始客户机请求中。证书状态标头的名称是SSLClientCertificateStatus。有关此标头的详细信息，请参阅下面的“先决LTMProfile”。

要实施SSL OCSP认证模块，必须将LTM系统配置为访问远程OCSP服务器上的数据。为此，必须创建：

- OCSP配置对象
- OCSP Profile

创建这些对象后，必须：

- 将OCSP Profile分配给Real Server。
- 将OCSP iRule分配给Real Server。

单个SSL OCSP Profile可以分配给特定的响应器；多个SSL OCSP Profile可以分配给同一个响应器。每个响应器都与一个证书授权机构（CA）关联，多个响应器可以与同一个CA关联。

♦ 注意

LTM系统允许您同时启用CRL选项和OCSP选项。大多数用户需要启用其中之一，而不是两个同时启用。然而，在极少数希望同时启用两个选项的情形中，请注意：CRL文件的搜索和指向响应器的连接都必须成功。否则，LTM系统无法获取状态。

先决LTMProfile

配置SSL OCSP认证模块不仅需要创建OCSP响应器对象和SSL OCSP Profile，而且还需要创建两个其它的Profile：HTTP和客户机SSL。

创建客户机SSL Profile时，我们建议您对该Profile进行配置来请求（而不是要求）证书。这样会优化LTM系统使用**SSLClientCertificateStatus**标头。请注意，只有预先配置将标头插入到客户机请求时（通过HTTP Profile或通过iRule），LTM系统才会插入该标头。

以下几部分描述了如何创建OCSP响应器对象、SSL OCSP配置对象以及SSL OCSP Profile。

创建OCSP响应器对象

OCSP响应器对象是一种用户创建的对象，它包括一个用于外部OCSP响应器的URL。您必须为每一个外部OCSP响应器创建单独的OCSP响应器对象。

随后创建OCSP配置对象时，该配置对象参考了已创建的任何OCSP响应器对象。

创建OCSP响应器对象时，需要配置一些设置。表8.11显示了组成SSL OCSP响应器对象的设置和值。有关如何创建该对象的详细流程，请参阅第8-29页上的“创建OCSP响应器对象的步骤”。

设置	说明	缺省值

设置	说明	缺省值
Name	为配置对象指定一个唯一的名称。此设置是必需的。	无缺省值
URL	指定用来联系有关响应器的OCSP服务的URL。	无缺省值
Certificate Authority File	指定包含可信CA证书的文件的名称，这些证书用来检验关于OCSP响应的签名。	无缺省值
Certificate Authority Path	指定包含可信CA证书的路径的名称，这些证书用来检验关于OCSP响应的签名。	无缺省值
Verify Other	当证书没有得到响应时，指定用来搜索OCSP响应签名证书的文件的名称。	无缺省值
Trust Other	通过**检验其它项**设置，指示LTM系统信任指定的证书。	**Disabled**
VA File	指定包含明确可信的响应器证书的文件名。如果已经加载到响应器的CA库的证书不包含该响应器，那么就需要此参数。	无缺省值
Signer	指定用来签署OCSP请求的证书。特殊含义： 如果指定了证书但未指定密钥，那么就会从与证书的作用一样的文件中读取私匙。 如果既未指定证书也未指定密钥，那么就不签署该请求。 如果未指定证书但指定了密钥，那么该配置被视为无效。	无缺省值
Signing Key	指定用来签署OCSP请求的密钥。	无缺省值
Sign Other	列出其它证书，添加到OCSP请求中。	无缺省值
Sign Digest	通过签署证书和密钥指定签署该请求的算法。 特殊含义： 如果请求签署无效（也就是，**Request Signing Certificate**和**Request Signing Key**参数为空），那么该参数没有任何意义。 只有请求签署有效时才需要该参数。	**Sha1**
Validity Period	指定LTM系统用来指定一个可接受错误范围的秒数。当OCSP响应器时钟和客户机时钟不同步时（这种情况会导致证书状态检查失败），使用该设置。该值必须是正数。该参数是必需的。	**300**
Status Age	以秒为单位指定一个时间，与**notBefore**字段进行比较。当状态响应不包括**notAfter**字段时使用。	**0**
Ignore AIA	指示LTM系统忽略包含在证书的**AIA**字段中的URL，并且始终使用响应器指定的URL代替。	Disabled
Trust Other	指定证书应该明确可信，无需再进行任何其它检查。	Disabled
Allow Certificates	允许证书添加到OCSP请求。	Enabled
Verify	让LTM系统检验OCSP响应签名或当前时间值。仅用于调试。	Enabled
Intern	当搜索签署者的证书时，让LTM系统忽略包含在OCSP响应中的证书。要使用该设置，必须通过**Verify Other**或**VA File**设置指定签署者的证书。	Enabled
Verify Signature	让LTM系统检查有关OCSP响应的签名。仅用于测试。	Enabled
Verify Certificate	让LTM系统检验有关OCSP响应的签名。	Enabled
Certificate Chain	让LTM系统构建有关OCSP响应的证书链。	Enabled
Check Certificates	让LTM系统进行其它检查，以查看是否授权签署者的证书来提供必需的状态信息。仅用于测试。	Enabled
Explicit OCSP	让LTM系统完全信任为签署OCSP响应而授权的OCSP响应签署者的证书。如果签署者的证书不包含**OCSP signing**扩展，那么该设置的规范会导致LTM系统不信任响应。	Enabled

表8.11 OCSP响应器的设置

创建OCSP响应器对象的步骤

1. 在Main选项卡上，展开**Local Traffic**。
2. 点击**Profiles**。
3. 从Authentication菜单中，选择OCSP Responders。
4. 在屏幕的右上角，点击**Create**。
5. 对于**name**设置，为配置对象输入一个唯一的名称，例如**my_ocsp_responder**。
6. 对于**URL**设置，输入用于外部响应器的URL。
7. 修改或保留所有其它设置的值。（要配置高级设置，请定位至**Configuration**标题，然后选择**Advanced**）。
8. 点击**Finished**。

创建SSL OCSP配置对象

SSL OCSP配置对象是一种参考一个或多个OCSP响应器对象的对象。

创建OCSP配置对象时，需要配置各种设置。表8.12列出并介绍了可在SSL OCSP配置对象中指定的设置。有关如何配置该对象的详细流程，请参阅下面的“创建SSL OCSP配置对象的步骤”部分。

设置	说明	缺省值
Name	为配置对象指定一个唯一的名称。此设置是必需的。	无缺省值
Type	指定您希望实施的认证模块的类型。必须将该值设置为**SSL OCSP**。	无缺省值
Responders	指定您希望用来检查SSL证书撤销状态的OCSP响应器。	无缺省值

表8.12 SSL OCSP配置对象的设置

创建SSL OCSP配置对象的步骤

1. 在Main选项卡中，展开**Local Traffic**。
2. 点击**Profiles**。
   将打开Profiles屏幕。
3. 从Authentication菜单中，选择Configurations。
4. 在屏幕的右上角，点击**Create**。
   此操作将显示New Configuration屏幕。
5. 对于**Name**设置，为配置对象指定一个唯一的名称，例如**my_ocsp_config**。
6. 对于**Type**设置，选择**SSL OCSP**。
7. 对于**Responders**设置，指定所有响应器对象。
8. 点击**Finished**。

创建SSL OCSP Profile

创建SSL OCSP配置对象之后，必须创建或配置SSL OCSP Profile。此操作可以通过修改缺省的**ssl_ocsp** Profile来进行，也可以通过创建继承缺省Profile设置的定制Profile来进行。认证Profile的一项重要功能是参考现有的配置对象。

在大多数情况下，缺省Profile应能满足您的需求。但是，即使您使用缺省Profile，也必须对其进行修改，指定您创建的相应配置对象。

如果选择创建定制Profile，那么必须指定上级Profile（定制Profile或缺

省Profile），该上级Profile包含要新Profile继承的值。

创建OCSP Profile时，需要配置各种设置。表8.13显示了组成SSL OCSP Profile的设置和值。有关创建OCSP Profile的详细流程，请参阅第8-31页上的“修改缺省SSL OCSP Profile的步骤”，或参阅第8-32页上的“创建定制SSL OCSP Profile的步骤”。

设置	说明	缺省值
Name	为Profile指定一个唯一的名称。此设置是必需的。	无缺省值
Type	指定您希望实施的认证模块的类型。必须将该值设置为**OCSP**。	无缺省值
Parent Profile	指定希望从继承值的Profile。	**ssl_ocsp**
Mode	指定启用还是禁用该Profile。可能的设置包括**Auto**、**Enabled**和**Disabled**。	**Enabled**
Configuration	指定现有OCSP配置对象的名称。此设置是必需的。	无缺省值
Rule	指定现有认证iRule的名称。如果不指定iRule，LTM系统将使用相应的缺省iRule。	**auth_ssl_ocsp**
Idle Timeout	以秒为单位，指定认证请求的空闲持续时间。您可以使用缺省值，指定一个不同的值，还可以选择**Indefinite**。	**300**

表8.13 *SSL OCSP Profile的设置*

修改缺省SSL OCSP Profile的步骤

1. 在Main选项卡上，展开**Local Traffic**。
2. 点击**Profiles**。
   将打开Profiles屏幕。
3. 从Authentication菜单中，选择Profiles。
   此操作将显示缺省认证Profile的列表。
4. 在Name栏中，点击**ssl_ocsp**。
5. 对于**Mode**设置，选择**Enabled**或**Auto**。
6. 对于**Configuration**设置，从列表中选择配置对象。请注意，不允许选择设置**None**。
7. 对于**Rule**设置，指定认证iRule：
   - 如果希望使用缺省iRule **auth_ocsp**，请将设置保留为原状。
   - 如果不想使用缺省iRule **auth_ocsp**，请选择已创建的现有iRule的名称。
8. 点击**Finished**。

创建定制SSL OCSP Profile的步骤

1. 在Main选项卡上，展开**Local Traffic**。
2. 点击**Profiles**。
   将打开Profiles屏幕。
3. 从Authentication菜单中，选择Profiles。
4. 在屏幕的右上角，点击**Create**。
   此操作将显示New Profile屏幕。
5. 对于**Name**设置，为Profile指定一个唯一的名称。
6. 对于**Type**设置，选择**SSL OCSP**。
7. 对于**Parent Profile**设置，执行以下操作：
   - 如果要将缺省Profile **ssl_ocsp**用于上级Profile，请将设置保留为原状。
   - 如果要将定制Profile用于上级Profile，请从列表中选择定制Profile的名称。
8. 对于**Mode**设置，点击屏幕右侧的Custom框，然后选择**Enabled**

或**Auto**。

9. 对于**Configuration**设置，点击屏幕右侧的Custom框，然后从列表中选择一个配置对象。
10. 对于**Rule**设置，指定认证iRule：
    - 如果希望使用缺省iRule **auth_ocsp**，请将设置保留为原状。
    - 如果不想使用缺省iRule **auth_ocsp**，请选择已创建的现有iRule的名称。
11. 点击**Finished**。

创建SSL OCSP响应器对象、SSL OCSP配置对象和SSL OCSP Profile之后，必须执行以下操作：

- 通过配置Real Server的**Authentication Profile**设置，将Profile分配到Real Server。
- 通过配置Real Server的**Rule**设置，将缺省**auth_ssl_ocsp** iRule分配到Real Server。

有关如何配置Real Server设置的信息，请参阅第2章“配置Real Server”。

9

启用会话持续性

- 会话持续性简介
- 持续性的类型及其**Profile**

会话持续性简介

您可以使用BIG-IP®本地流量管理（LTM）系统来配置会话持续性。配置***session Persistence***时，LTM系统会跟踪并存储会话数据，例如为客户机请求提供服务的特定Pool成员。跟踪并存储会话数据主要是为了确保在整个会话过程中或者在后续会话期间，将客户机请求定向至同一个Pool成员。此外，会话持续性还能跟踪并存储其它类型的信息，例如用户首选项或者用户名和密码。

LTM系统提供若干种类型的会话持续性，每一类都可满足一种特定类型的会话数据存储要求。具体实施哪一类持续性取决于您希望将客户机特有的信息（例如购物车内的物品或航空机票预订）存储在何处，以及用何种方式存储。

例如，您可以将航空机票预订信息存储在所有服务器都可访问的后台数据库中，存储在客户机最初连接的特定服务器上，或者存储在客户端计算机的cookie中。启用持续性时，返回的客户机可以绕过负载平衡，转为连接上次连接的服务器，以访问它们保存的信息。

LTM系统保存会话数据的时间由您指定。配置会话持续性的主要途径是配置一个持续性Profile，然后将其分配给Real Server。如果希望仅为特定类型的流量，而不是流经Real Server的所有流量启用持续性，那么可以编写iRule。

配置持续性Profile

持续性Profile是一种预配置的对象，可以在您将其分配给Real Server时，自动启用持续性。使用持续性Profile可以省去编写程序来实施某类持续性的过程。

LTM系统提供的每一类持续性都包括相应的缺省持续性Profile。这些持续性Profile中的每一个都包含一些设置及其值，这些设置和值定义了LTM系统对该类持续性的处理方式。您可以使用缺省Profile，也可以在该缺省文件的基础上创建定制Profile。

有关详细信息，请参阅本指南的以下章节：

- 要配置持续性Profile，请参阅第9-3页上的“持续性的类型及其Profile”。
- 要全面了解Profile，请参阅第5章“了解Profile”。

通过iRule启用会话持续性

除了配置用来为流经Real Server的所有会话启用某类持续性的持续性Profile之外，还可以编写用来为特定请求（例如：仅包括特定cookie版本的HTTP流量）启用某类持续性的iRule。

您也可以使用iRule为SSL终止的请求启用持续性，即LTM系统通过执行解密与重新加密和通过处理SSL证书认证来终止的请求。在此类iRule中，您可以使用“HTTP标头插入”这个iRule命令将SSL会话ID以标头形式插入HTTP请求。

本章的剩余部分着重讨论使用持续性Profile来启用持续性。有关通过编写iRule来启用持续性的信息，请参阅第13章“编写iRule”。

持续性的类型及其Profile

您可以配置持续性Profile的设置，以设置LTM系统的会话持续性。对这些设置的配置可以在创建Profile时进行，也可以在创建Profile之后，通过修改该Profile的设置进行。有关对Profile进行配置的具体流程，请参阅第5章“了解Profile”。

持续性的类型

使用持续性Profile可以启用的持续性类型包括：

- **cookie持续性**
  cookie持续性使用存储在客户端计算机上的HTTP cookie，从而允许客户机重新连接到之前在网站访问的那台服务器。

- **目的地地址相关性持续性**
  也称为粘着持续性，目的地地址相关性持续性支持TCP和UDP协议，完全根据数据包的目的地IP地址，将会话请求定向至同一台服务器。

- **散列持续性**
  散列持续性允许您基于现有的iRule创建持续性散列。

- **微软远程桌面协议持续性**
  微软远程桌面协议（MSRDP）持续性跟踪那些运行Microsoft®远程桌面协议（RDP）服务的客户机和服务器之间的会话。

- **SIP持续性**
  SIP持续性是用于以下这些服务器的持续性类型：它们接收通过UDP发送的会话启动协议（SIP）消息。SIP是一种支持实时消息传递、语音、数据和视频的协议。

- **源地址相关性持续性**
  也称为简单持续性，源地址相关性持续性支持TCP和UDP协议，完全根据数据包的源IP地址，将会话请求定向至同一台服务器。

- **SSL持续性**
  SSL持续性是使用SSL会话ID来跟踪未中断的SSL会话的持续性类型。即使客户机的IP地址发生了变化，LTM系统仍根据会话ID将连接识别为持续连接。请注意，术语***non-terminated SSL sessions***是指LTM系统未在其中执行SSL证书认证任务和加密/重新加密任务的会话。要为已中断的SSL会话启用持续性，请参阅第7章“管理SSL流量”和第13章“编写iRule”。

- **通用持续性**
  通用持续性允许您编写表达式，定义数据包中要持续的内容。此表达式以iRules™中使用的表达式语法编写而成，定义用作会话标识符的字节序列。

了解用于会话持续性的条件

无论实施何种类型的持续性，都可以指定LTM系统用来将源自给定客户机的所有请求发送至同一个Pool成员的条件。这些条件基于接纳客户机连接的Real Server或服务器。要指定这些条件，请使用**Match Across Services**和**Match Across Real Servers**这两个Profile设置。配置持续

性Profile之前，了解这些设置很有帮助。

指定Match Across Services设置

如果启用了**Match Across Services**这个Profile设置，那么仅当接纳连接的Real Server与接纳原始持续性连接的Real Server具有相同的虚拟地址时，LTM系统才尝试在持续性时限内，将接收自同一台客户机的所有持续性连接请求发送至同一个Pool成员。对于流向具有不同虚拟地址的其它Real Server的客户机连接请求，或是那些未使用持续性的连接请求，将根据为该pool定义的负载平衡方法进行负载平衡。

举例来说，假设配置了Real Server映射，其中Real Server**v1:http**启用了持续性并参考pool **http_pool**（包括节点**n1:http**和**n2:http**），Real Server**v1:ssl**启用了持续性并参考pool **ssl_pool**（包括节点**n1:ssl**和**n2:ssl**）。

如果客户机随后连接到**v1:ssl**，那么LTM系统将使用与首个连接建立的持续性会话来确定应接收该连接请求的Pool成员，而不是应用负载平衡方法。LTM系统应将第三个连接请求发送至**n1:ssl**，其使用的节点地址与**n1:http**节点的相同，**n1:http**节点目前接纳客户机的首个连接，通过此连接该节点共享持续性会话。

例如，客户机发起与**v1:http**的原始连接，分配给pool **http_pool**的负载平衡机制选择**n1:http**作为节点。如果同一台客户机随后连接至**v2:ssl**，那么LTM系统将开始跟踪新的持续性会话，并使用负载平衡方法确定哪个节点应接收此连接请求，因为请求的Real Server使用的虚拟地址（**v2**）与接纳首个持续性连接请求的Real Server使用的虚拟地址（**v1**）不同。要使此设置生效，使用相同虚拟地址的Real Server包括的节点地址应与Real Server映射中的节点地址相同，对于使用TCP或SSL持续性的Real Server也有同样的要求。

指定Match Across Real Servers设置

您可以将LTM系统设置成针对同一台客户机请求的所有会话维护持续性，而无需考虑由哪个Real Server接纳客户机发起的各个单独连接。启用**Match** Across **Real Servers**这一设置时，LTM系统尝试在持续性时限内，将接收自同一台客户机的所有持续性连接请求发送至同一个Pool成员。对于未使用持续性的客户机连接请求，将根据当前选定的负载平衡方法进行负载平衡。

♦ **警告**

要使此设置生效，使用具有TCP或SSL持续性的pool的Real Server所包括的成员地址应与Real Server映射中的成员地址相同。

cookie持续性

您可以将LTM系统设置为使用HTTP cookie持续性。***cookie持续性***使用存储在客户端计算机上的HTTP cookie，从而允许客户机重新连接到之前在网站访问的那个Pool成员。可用的cookie持续性方法有如下四种：

- HTTP cookie插入法
- HTTP cookie重写法
- HTTP cookie被动法
- Cookie Hash法

选用的方法影响着将cookie返回给客户机时，LTM系统对该cookie的处理方式。

Cookie Profile

要实施cookie持续性，可以使用缺省**Cookie Profile**，也可以创建定制Profile。表9.1显示了组成缺省**Cookie Profile**的设置和值。

设置	说明	缺省值
Name	为Profile指定一个唯一的名称。此设置是必需的。	无缺省值
Persistence Type	指定持续性的类型。此设置是必需的。	**cookie**
Match Across Services	指定：如果来自某个客户机IP地址的所有持续性连接都流向同一个虚拟IP地址，那么这些连接也将流向同一个节点。	禁用
Match Across Virtual Servers	指定：来自同一个客户机IP地址的所有持续性连接都将流向同一个节点。	禁用
Match Across Pools	指定：LTM系统可以使用包含此持续性条目的任何pool。	禁用
Cookie Method	指定LTM系统将要使用的cookie处理方法的类型。有关详细信息，请参阅下面的“指定‘cookie方法’设置”一节。	**HTTP Cookie Insert**
Cookie Name	指定LTM系统应查找或插入的cookie的名称。	此值根据pool名自动生成。
Expiration	设置cookie的有效时间。	**永不过期**

***表9.1** cookie持续性Profile的设置*

指定Cookie Method设置

您可以将Cookie Profile中的**Cookie Method**设置配置为四个值之一。

HTTP Cookie Insert法

如果在Profile中指定**HTTP Cookie Insert**法，那么有关客户机连接到其上的那台服务器的信息将以cookie形式，插入到来自该服务器的HTTP响应的的标头中。cookie将命名为**BIGipServer<pool_name>**，其中包括处理连接的那台服务器的地址和端口。cookie的有效日期根据LTM系统上配置的超时值来设置。**HTTP Cookie Insert**是**Cookie Method**设置的缺省值。

HTTP Cookie Rewrite法

如果指定**HTTP Cookie Rewrite**法，LTM系统将截听名为**BIGipcookie**、从服务器发送至客户机的**Set-Cookie**标头，然后改写该cookie的名称和值。新cookie将命名为**BIGipServer<pool_name>**，其中包括处理连接的那台服务器的地址和端口。

♦ **重要信息**

*我们建议，只要有可能便使用此方法，而不是**HTTP Cookie Passive**法。*

HTTP Cookie Rewrite法要求您设置服务器创建的cookie。要使**HTTP**

Cookie Rewrite法成功，需要有来自Web服务器的空白cookie，供LTM系统进行重写。借助Apache变量，可以将cookie添加到每个网页标头，方法是在**httpd.conf**文件中加入以下条目：

Header add Set-Cookie BIGipCookie=00000000000000000000000000...

（cookie总共必须包括120个零。）

♦ **注意**

要实现向后兼容性，空白cookie只能包含75个零。但是，这种大小的cookie不允许同时使用iRule和持续性。

HTTP Cooike Passive法

如果指定HTTP Cookie Passive法，LTM系统将不在来自服务器的响应中插入或搜索空白的**Set-Cookie**标头。此方法不会尝试设置cookie。使用此方法，服务器可以提供按照正确的服务器信息和超时值进行格式化的cookie。

♦ **重要信息**

我们建议，只要有可能便使用HTTP Cookie Rewrite法，而不是HTTP Cookie Passive法。

要使HTTP Cookie Passive法成功，需要有来自Web服务器且带有正确的服务器信息的cookie。使用Configuration工具，您可以生成自动添加编码的cookie字符串模板，然后对模板进行编辑，创建实际的cookie。

例如，以下字符串便是一个生成的cookie模板，并自动添加了编码，其中**[poolname]**是包含服务器的pool的名称，**336268299**是经过编码的服务器地址，**20480**是经过编码的端口：

Set-Cookie:BIGipServer[poolname]=336268299.20480.0000; expires=Sat, 01-Jan-2002 00:00:00 GMT; path=/

要从此模板中创建您自己的cookie，请键入实际的pool名称以及有效日期和时间。

或者，也可以使用以下方程式对地址（a.b.c.d）执行编码：

d*(256^3) + c*(256^2) + b*256 + a

对端口进行编码的方式是取表示端口的两个字节，然后反转。这样，端口**80**变成80*256 + 0 = 20480。端口**1433**（而不是5*256 + 153）变成153*256 + 5 = 39173。

借助Apache变量，可以将cookie添加到每个网页标头，方法是在**httpd.conf**文件中加入以下条目：

Header add Set-Cookie:"BIGipServer my_pool=184658624.20480.000; expires=Sat, 19-Aug-200219:35:45 GMT; path=/"

Cookie Hash法

如果指定Cookie Hash法，那么散列法会持续将cookie值映射到特定的节点。客户机返回站点时，LTM系统利用cookie信息将客户机返回到指

定的节点。在此模式中，Web服务器必须生成cookie；LTM系统不会像使用HTTP cookie插入法时那样自动创建cookie。

目的地地址相关性持续性

使用目的地地址相关性持续性可以优化服务器阵列。***目的地地址相关性持续性***也称为粘着持续性，用于将针对特定目的地IP地址的请求定向至同一台服务器，而不考虑生成请求的客户机。

对缓存服务器进行负载平衡时，此类持续性具有最佳用途。缓存服务器截听Web请求，然后返回缓存的网页（如果存在这样的网页）。为了提高这些服务器上缓存的效率，有必要将类似的请求重复发送至同一台服务器。使用目的地地址相关性持续性类型可以在一台服务器上缓存给定的网页，而无需在阵列中的每台服务器上进行缓存。这使其它服务器不必将网页复制到自己的缓存中，这种复制是对资金的浪费。

目的地地址相关性**Profile**

要实施目的地地址相关性持续性，可以使用缺省**dest_addr** Profile，也可以创建定制Profile。表9.2显示了组成缺省**dest_addr** Profile的设置及其值。

设置	说明	缺省值
Name	为Profile指定一个唯一的名称。此设置是必需的。	无缺省值
Persistence Type	指定持续性Profile的类型。此设置是必需的。	**Destination Address Affinity**
Match Across Services	指定：如果来自某个客户机IP地址的所有持续性连接都流向同一个虚拟IP地址，那么这些连接也将流向同一个节点。	Disabled
Match Across Virtual Servers	指定：来自同一个客户机IP地址的所有持续性连接都将流向同一个节点。	Disabled
Match Across Pools	指定：LTM系统可以使用包含此持续性条目的任何pool。	Disabled
Mask	指定在与现有持续性条目进行匹配之前，LTM系统应使用的掩码。	**255.255.255.255**

表9.2 *目的地地址相关性持续性Profile的设置*

散列持续性

散列持续性允许您基于现有的iRule创建持续性散列。

散列**Profile**

要实施散列持续性，可以使用缺省**hash** Profile，也可以创建定制Profile。表9.3显示了组成缺省**hash** Profile的设置及其值。

设置	说明	缺省值
Name	为Profile指定一个唯一的名称。此设置是必需的。	无缺省值
Persistence Type	指定持续性Profile的类型。此设置是必需的。	**Hash**
Match Across Services	指定：如果来自某个客户机IP地址的所有持续性连接都流向同一个虚拟IP地址，那么这些连接也将流向同一个节点。	禁用
Match Across	指定：来自同一个客户机IP地址的所有持续性连接都	禁用

设置	说明	缺省值
Virtual Servers Match Across Pools iRule Timeout	将流向同一个节点。 指定：LTM系统可以使用包含此持续性条目的任何pool。 指定要运行哪个确定此持续性条目的iRule。 以秒为单位，指定超时值。此设置另一个可能的值是**不确定**。	禁用 **_sys_auth_ldap** **180**

表9.3 *散列持续性Profile的设置*

微软远程桌面协议持续性

MSRDP持续性提供了一种在运行Microsoft®远程桌面协议（RDP）服务的Windows®客户机和服务器之间负载平衡流量并保持持续性会话的有效方式。建议用于启用MSRDP持续性特性的方法是创建一个由运行Windows.NET Server 2003（企业版或更高版本）的成员组成的负载平衡Pool，其中所有成员都属于某个Windows群集，并加入Windows会话目录。

MSRDP持续性的优势

如果没有MSRDP持续性，Windows服务器会在加入会话目录时，将客户机映射到各自的相关服务器，必要时使用重定向。如果客户机连接的群集服务器不正确，目标服务器将检查自己的客户机-服务器映射，然后执行指向正确服务器的重定向。

但启用MSRDP持续性时，加入了会话目录的Windows服务器会将连接始终重定向至同一台Real Server，而不是直接重定向至其它服务器。随后，LTM系统将连接发送至正确的Windows服务器。此外，当LTM系统上启用了MSRDP持续性且pool中的服务器加入了会话目录时，LTM系统将根据用户为LTM系统配置的负载平衡方式，对RDP连接进行负载平衡。因此，综合使用Windows服务器、会话目录服务和MSRDP持续性特性可以提供更高级的负载平衡，还可以在服务器断开连接时提供更可靠的重新连接。

服务器平台的有关问题

缺省情况下，启用了MSRDP持续性的LTM系统会根据用户为LTM系统配置的负载平衡方式，对连接进行负载平衡，只要pool中的每台服务器上都配置了会话目录。会话目录是仅在Windows.NET Server 2003（企业版或更高版本）平台上可用的特性，所以如果希望在缺省模式中使用MSRDP持续性，那么pool中的每台服务器都必须运行Windows.NET Server 2003企业版。此外，每个客户机系统都必须正在运行远程桌面客户机软件，任何.NET企业版服务器或Windows XP系统都带有该软件。

然而，如果希望启用MSRDP持续性，但服务器平台正在运行较早版本的Windows（会话目录在这些平台上不可用），那么可以在非缺省模式中启用MSRDP持续性。这会使LTM系统根据客户机提供的用户名，将该客户机连接到相同的Windows服务器。请注意，在非缺省模式中启用MSRDP持续性（即会话目录在服务器上不可用）不如在缺省模式中理想，因为前者提供的负载平衡和重定向功能有限。

在有会话目录的情况下配置MSRDP持续性

要在缺省模式中启用MSRDP持续性，必须在负载平衡Pool中的每一台Windows服务器上配置会话目录。除了配置会话目录之外，还必须在那些服务器上执行其它Windows配置任务。但是，配置Windows服务器之前，必须执行诸如创建负载平衡Pool，然后将Windows服务器指定为该pool的成员这样的任务，对LTM系统进行配置。

以下两节中介绍了对于使用RDP的Windows客户机-服务器配置，在缺省模式中启用MSRDP持续性所需的LTM配置任务。

在无会话目录的情况下配置MSRDP持续性

如果某个服务器没有会话目录，它便无法与其它服务器共享会话，进而无法在指向服务器的连接断开时执行任何重定向操作。在此情形中，Windows客户机向LTM系统提供用户名形式的数据来代替会话共享，这允许LTM系统将该客户机持续连接到同一台服务器上。让MSRDP持续性以这种方式发挥作用便是非缺省模式。

MSRDP Profile

要实施MSRDP持续性，可以使用缺省**msrdp** Profile，也可以创建定制Profile。表9.4显示了组成缺省**msrdp** Profile的设置及其值。

设置	说明	缺省值
Name	为Profile指定一个唯一的名称。此设置是必需的。	无缺省值
Persistence Type	指定持续性Profile的类型。此设置是必需的。	**Microsoft Remote Desktop**
Match Across Services	指定：如果来自某个客户机IP地址的所有持续性连接都流向同一个虚拟IP地址，那么这些连接也将流向同一个节点。	Disabled
Match Across Virtual Servers	指定：来自同一个客户机IP地址的所有持续性连接都将流向同一个节点。	Disabled
Match Across Pools	指定：LTM系统可以使用包含此持续性条目的任何pool。	Disabled
Timeout	指定持续性条目超时前可以存在的秒数。	**0**
Has Session Directory	指定服务器是否运行会话目录。	**Enabled**

***表9.4** MSRDP持续性Profile的设置*

SIP持续性

会话启动协议（SIP）是一个应用层协议，用于管理由多名参与者组成，因而启用实时消息传递、语音、数据和视频的会话。使用SIP，应用之间可以通过TCP或UDP交换消息，从而进行通信。这类应用的实例包括互联网会议和电话，或多媒体发行。

SIP持续性是为服务器pool提供的一类新型持续性。您可以为以下这类代理服务器配置SIP持续性：它们接收通过UDP发送的会话启动协议（SIP）消息。

SIPProfile

要实施SIP持续性，可以使用缺省**sip** Profile，也可以创建定制Profile。表9.5显示了缺省**sip** Profile的设置及其值。

设置	说明	缺省值
Name	为Profile指定一个唯一的名称。此设置是必需的。	无缺省值

设置	说明	缺省值
Persistence Type	指定持续性Profile的类型。此设置是必需的。	**SIP**
Match Across Services	指定：如果来自某个客户机IP地址的所有持续性连接都流向同一个虚拟IP地址，那么这些连接也将流向同一个节点。	Disabled
Match Across Virtual Servers	指定：来自同一个客户机IP地址的所有持续性连接都将流向同一个节点。	Disabled
Match Across Pools	指定：LTM系统可以使用包含此持续性条目的任何pool。	Disabled
Timeout	指定持续性条目超时前可以存在的秒数。	**180**

表9.5 *SIP持续性Profile的设置*

◆ **注意**

LTM系统目前仅支持用于通过UDP发送的SIP消息的持续性。

您指定的超时值允许LTM系统释放与旧的SIP持续性条目相关联的资源，而无需为每种不同类型的SIP最终消息测试每个入站数据包。现有的缺省超时值为180秒。如果改变该值，建议不要低于缺省值。

源地址相关性持续性

源地址相关性持续性也称为简单持续性，它仅根据源IP地址跟踪会话。客户机请求与支持源地址相关性持续性的Real Server进行连接时，LTM系统将检查该客户机之前是否连接过，如果是，便将该客户机返回至同一个Pool成员。

您可能希望将源地址相关性持续性与SSL持续性一起使用。在SSL会话ID超时，或者返回的客户机未提供会话ID的情形中，您可能希望LTM系统根据客户机的IP地址，将该客户机定向至原始Pool成员。只要客户机的源地址相关性持续性记录没有超时，LTM系统便能成功地将该客户机返回至适当的Pool成员。

这类持续性设置适用于所有协议。将持续性计时器设置为大于**0**的值时，该持续性便处于**on**的状态。而将持续性计时器设置为**0**时，该持续性便处于**off**状态。

持续性掩码特性仅对实施了源地址相关性持续性的Real Server有效。通过添加持续性掩码，您可以在连接到pool时，将一系列源IP地址标记成一个单一源地址相关性持续性连接进行管理。

源地址相关性Profile

要实施源地址相关性持续性，可以使用缺省**source_addr** Profile，也可以创建定制Profile。表9.6显示了组成缺省**source_addr** Profile的设置和值。

设置	说明	缺省值
Name	为Profile指定一个唯一的名称。此设置是必需的。	无缺省值
Persistence Type	指定持续性Profile的类型。此设置是必需的。	**Source Address Affinity**
Match Across Services	指定：如果来自某个客户机IP地址的所有持续性连接都流向同一个虚拟IP地址，那么这些连接也将流向同一个节点。	Disabled
Match Across	指定：来自同一个客户机IP地址的所有持续性连接都将	Disabled

设置	说明	缺省值
Virtual Servers	流向同一个节点。	
Match Across Pools	指定：LTM系统可以使用包含此持续性条目的任何pool。	Disabled
Timeout	指定持续性条目超时前可以存在的秒数。	**180**
Mask	指定在与现有持续性条目进行匹配之前，LTM系统应使用的掩码。	**0.0.0.0**
Map Proxies	启用或禁用代理映射。	**Enabled**

表9.6 *源地址相关性持续性Profile的设置*

SSL持续性

SSL持续性是一种持续性类型，它使用SSL会话ID来跟踪SSL会话，它是每个独立pool都具有的属性。如果客户机通常具有经过转换的IP地址或动态IP地址（例如互联网服务提供商通常分配的那些IP地址），那么使用SSL持续性特别重要。即使客户机的IP地址发生了变化，LTM系统仍根据会话ID将会话识别为持续连接。

您可能希望将SSL持续性与源地址相关性持续性一起使用。在SSL会话ID超时，或者返回的客户机未提供会话ID的情形中，您可能希望LTM系统根据客户机的IP地址，将该客户机定向至原始节点。只要客户机的简单持续性记录没有超时，LTM系统便能成功地将该客户机返回至适当的节点。

◆ **注意**

*SSL持续性类型仅对以下这类系统有效：它们不执行基于SSL证书的客户机请求认证或服务器响应认证。如果使用客户机SSL或服务器SSL Profile来配置基于证书的认证，您不应配置SSL持续性Profile，而应参阅第13章“**编写iRule**”。*

SSL Profile

要实施MSRDP持续性，可以使用缺省**SSL Profile**，也可以创建定制Profile。表9.7显示了组成缺省SSL持续性Profile的设置及其值。

设置	说明	缺省值
Name	为Profile指定一个唯一的名称。此设置是必需的。	无缺省值
Persistence Type	指定持续性Profile的类型。此设置是必需的。	**SSL**
Match Across Services	指定：如果来自某个客户机IP地址的所有持续性连接都流向同一个虚拟IP地址，那么这些连接也将流向同一个节点。	Disabled
Match Across Virtual Servers	指定：来自同一个客户机IP地址的所有持续性连接都将流向同一个节点。	Disabled
Match Across Pools	指定：LTM系统可以使用包含此持续性条目的任何pool。	Disabled
Timeout	指定持续性条目超时前可以存在的秒数。具体地说，此设置对SSL会话ID超时值进行设置，该值确定LTM系统将给定的SSL会话ID从系统中删除之前，存储该ID的时间长度。	**300**

表9.7 *SSL持续性Profile的设置*

通用持续性

LTM系统的通用检查引擎（UIE）中包括一组功能，您可以在LTM iRule

中指定这些功能以更精确的方式对流量进行定向。使用这些iRule功能，您可以编写表达式，根据内容数据对流量进行定向，或者将流量定向至特定Pool成员。

通用持续性进一步加强了这种iRule特性，允许您基于内容数据，或者基于与特定Pool成员的连接来实施会话持续性。通用持续性通过定义用作会话标识符的一些字节序列来实现这个目的。

为了使用针对持续性的iRule表达式，通用持续性Profile带有这样一个设置：它指定包含表达式的iRule的名称。

创建iRule并在通用Profile中指定iRule名称之后，必须将该iRule和该Profile作为资源一起分配给适当的Real Server。

有关iRule表达式和功能的完整介绍，请参阅第13章“编写iRule”。

通用持续性Profile

要实施通用持续性，可以使用缺省**universal** Profile，也可以创建定制Profile。表9.8显示了组成缺省通用持续性Profile的设置和值。

设置	说明	缺省值
Name	为Profile指定一个唯一的名称。此设置是必需的。	无缺省值
Persistence Type	指定持续性的类型。此设置是必需的。	**Universal**
Match Across Services	指定：如果来自某个客户机IP地址的所有持续性连接都流向同一个虚拟IP地址，那么这些连接也将流向同一个节点。	Disabled
Match Across Virtual Servers	指定：来自同一个客户机IP地址的所有持续性连接都将流向同一个节点。	Disabled
Match Across Pools	指定：LTM系统可以使用包含此持续性条目的任何pool。	Disabled
iRule	指定为了确定持续性条目，LTM应该运行的现有iRule的名称。	**_sys_auth_ldap**
Timeout	指定持续性条目超时前可以存在的秒数。	**180**

表9.8 *通用持续性Profile的设置*

10

配置 Monitor

- Monitor 简介
- 创建定制 Monitor
- 配置 Monitor 设置
- 特殊配置考虑因素
- 将 Monitor 与 pool 和节点关联
- 管理 Monitor

Monitor简介

BIG-IP®本地流量管理（LTM）系统的一个重要特性是称为 Monitor 的负载平衡工具。***Monitor*** 验证 Pool 成员和节点的连接。Monitor 可以是状态 Monitor 或性能 Monitor，设计用于以一定的时间间隔持续检查 pool、Pool 成员或节点的状态。如果正在检查的 Pool 成员或节点在特定的时限内未做出响应，或者 Pool 成员或节点的状态表明性能下降，那么 LTM 系统可以将流量重新引导到另一个 Pool 成员或节点。

一些 Monitor 是 LTM 系统的一部分，而其它 Monitor 是用户创建的。LTM 系统提供的 Monitor 称为*预配置 Monitor*。用户创建的 Monitor 称为*定制 Monitor*。有关预配置和定制 Monitor 的详细信息，请参阅第 10-7 页上的“了解预配置和定制的 Monitor”。

在配置和使用 Monitor 之前，了解一些关于 Monitor 类型、Monitor 设置和 Monitor 实施的基本概念是很有帮助的。

- **Monitor 类型**
  无论是预配置的还是定制的 Monitor，每一个 Monitor 的类型都是特定的。每种类型的 Monitor 都会检查特殊协议、服务或应用的状态。例如，一种类型的 Monitor 是 HTTP。HTTP 类型的 Monitor 使您能够监视 pool、Pool 成员或节点上 HTTP 服务的可用性。WMI 类型的 Monitor 使您能够监视正运行 Windows 管理构架（WMI）软件的 pool、Pool 成员或节点的性能。ICMP 类型的 Monitor 仅仅是确定节点的状态是 **Up** 还是 **Down**。有关 Monitor 类型的详细信息，请参阅第 10-2 页上的“Monitor 类型概述”和第 10-11 页上的“配置 Monitor 设置”。

- **Monitor 设置**
  每个 Monitor 都由设置和值组成。这些设置以及它们的值因 Monitor 类型的不同而不同。在有些情况下，LTM 系统指定缺省值。例如，图 10.1 表明 ICMP 类型的 Monitor 具有以下设置和缺省值。

```
Name my_icmp
Type ICMP
Interval 5
Timeout 16
Transparent No
Alias Address * All Addresses
```

*图**10.1** 具有缺省值的 Monitor 示例*

图 10.1 中的设置说明配置一个 ICMP 类型的 Monitor，每隔 5 秒检查一次 IP 地址的状态，每隔 16 秒超时一次。通过 **Alias Address** 设置和值 ***All Address** 指定 Monitor 检查的目的地 IP 地址。因此，在前面的示例中，与该 Monitor 关联的所有 IP 地址都得到了检查。有关 Monitor 设置的详细信息，请参阅第 10-3 页上的“Monitor 设置概述”和第 10-11 页上的“配置 Monitor 设置”。

- **Monitor 实施**
  实施 Monitor 的任务取决于是使用预配置 Monitor 还是创建定制 Monitor。如果要实施预配置 Monitor，那么只需要将 Monitor 与 pool、Pool 成员或节点关联。如果要实施定制 Monitor，那么必须首先创建定制 Monitor，然后将其与 pool、Pool 成员或节点关联。有关实施 Monitor 的详细信息，请参阅第 10-7 页上的“了解预配置和定制的 Monitor”和第 10-10 页上的“创建定制 Monitor”。

Monitor类型概述

LTM 系统包括很多不同类型的 Monitor，每种 Monitor 都设计用来执行特定类型的监视任务。表 10.1 列出了可以配置用于控制网络流量的 Monitor 类型。

Monitor 类型	说明
简单 Monitor	
ICMP	利用互联网控制信息协议（ICMP）检查节点的状态。
TCP Echo	利用传输控制协议（TCP）检查节点的状态。
扩展内容验证（ECV）Monitor	
TCP	通过尝试从节点接收特定内容来验证传输控制协议（TCP）服务。
HTTP	通过尝试从网页接收特定内容来验证超文本传输协议（HTTP）服务。
HTTPS	通过尝试从安全套接层（SSL）安全性保护的网页接收特定内容来验证安全超文本传输协议（HTTPS）服务。
扩展应用验证（EAV）Monitor	
External	使用户能够利用自己的程序来监视服务。
FTP	通过尝试将特定文件下载到 LTM 系统的**/var/tmp** 目录中来验证文件传输协议（FTP）服务。一旦下载成功，就不用保存该文件。
IMAP	通过尝试打开服务器上特定的邮件文件夹来验证互联网消息访问协议（IMAP）。该 Monitor 类似于 **pop3** Monitor。
LDAP	通过尝试对特定用户进行认证来验证小型目录访问协议（LDAP）服务。
MSSQL	验证基于 Microsoft® Windows SQL 的服务。
NNTP	通过尝试从服务器接收新闻组识别字符串来验证用户网新闻协议（NNTP）服务。
Oracle	通过尝试以 Oracle 身份登录到服务来验证基于 Oracle®的服务。
POP3	通过尝试连接到 pool、Pool 成员或节点，作为特定用户登录和注销来验证邮局协议（pop3）服务。
RADIUS	通过尝试对特定用户进行认证来验证远程访问拨号用户服务（RADIUS）。
Real Server	检查运行 RealServer 数据收集代理的 pool、Pool 成员或节点的性能，然后相应地动态平衡负载流量。
SIP	检查设备上会话启动协议（SIP）呼叫 ID 服务的状态。SIP 协议支持实时消息传递、话音、数据和视频。
SMTP	通过发布标准的简单邮件传输协议（SMTP）命令来检查 pool、Pool 成员或节点的状态。
SNMP DCA	检查运行 SNMP 数据收集代理的 pool、Pool 成员或节点的当前 CPU、内存和磁盘使用情况，然后相应地动态平衡负载流量。
SNMP DCA Base	检查运行 SNMP 数据收集代理的 pool、Pool 成员或节点的当前用户使用情况，然后相应地动态平衡负载流量。配置 Monitor 设置的方式决定了 LTM 系统收集的数据。
SOAP	基于简单对象访问协议（SOAP）来测试 Web 服务。
UDP	通过尝试将 UDP 数据包发送到 pool、Pool 成员或节点并接收回复来验证用户数据报协议（UDP）。
WMI	检查运行 Windows 管理基础设施（WMI）数据收集代理的 pool、Pool 成员或节点的性能，然后相应地动态平衡负载流量。

***表 10.1** 可用于 LTM 系统的 Monitor 类型*

Monitor设置概述

Monitor 包含设置和相应的值。这些设置以及它们的值会影响 Monitor 执行状态检查的方式。创建定制 Monitor 时，必须配置这些设置值。对于那些具有缺省值的设置，可以保留缺省值，也可以进行修改来满足您的需求。

表 10.2 包含一个所有可能的 Monitor 设置以及对这些设置的说明的完整列表。请注意，每个 Monitor 仅包含这些设置的子集。

设置	定义
Additional Accepted Status Codes	用于 SIP Monitor 的状态码。可接受的值包括 **Any**、**None** 或指定的状态码的列表。
Agent	代理规范仅用于 Real Server、SNMP 库和 WMI Monitor。
Agent Type	通过 SNMP DCAMonitor 监视在服务器上运行的代理的类型。
Alias Address	用于 ping 的目的地节点。通常包含值*，可检查所有节点。该设置促使 Monitor 实例 ping 通实例化的 IP 地址。指定各自的 IP 地址促使目的地指向该地址（也就是节点）。当 Monitor 包括 **Alias Address** 设置而不是 **Alias Service Port** 设置时，该 Monitorping 通节点地址而不是 Pool 成员地址。
Alias Service Port	用于 ping 的目的地 Pool 成员。通常包含值*:*，可检查所有 Pool 成员。该设置促使 Monitor 实例 ping 通实例化的 IP 地址和端口。指定各自的 IP 地址和端口促使目的地指向该地址和端口（也就是 Pool 成员）。
Arguments	所有需要的命令行参数。
Base	在 LDAP 层次结构中开始查询的起始位置，仅针对 LDAP Monitor。
Cipher List	仅供 HTTPS Monitor 使用的密码列表。
Command	与指标和指标值相关的命令。适用于 Real Server 和 WMI Monitor。
Community	仅适用于 SNMP DCAMonitor 的设置。缺省值是 **Public**。
CPU Coefficient	用于计算比率权重的 CPU 值。
CPU Threshold	允许的最高 CPU 阈值，用于计算比率权重。
Database	数据库名称，仅针对 Oracle 和 MSSQLMonitor。
Disk Coefficient	用于计算比率权重的磁盘值。
Disk Threshold	允许的最高磁盘阈值，用于计算比率权重。
Domain	仅针对 SMTP Monitor 的域名。
External Program	用户创建的 Monitor 类型。
Filter	将搜索的 LDAP 格式密钥，仅针对 LDAP Monitor。
Folder	仅针对 IMAP Monitor 的文件夹名。
Interval	以秒为单位检查 pool、Pool 成员或节点频率的时间间隔。
Memory Coefficient	用于计算比率权重的内存值。
Memory Threshold	允许的最高磁盘阈值，用于计算比率权重。
Method	方法规范，如 **GET** 或 **POST**。仅适用于 Real Server、SOAP 和 WMI Monitor。
Metrics	要监视的测量，如 CPU 百分比或内存使用情况。仅适用于 Real Server 和 WMI Monitor。
Mode	Monitor 的模式。
Newsgroup	仅针对 NNTP Monitor 的新闻组。
Password	具有密码安全性的密码。
Path/Filename	仅针对 FTP Monitor，该设置代替 **Send String** 设置。可以使用该设置指定文件的全路径。

设置	定义
Receive Row	在返回表中包含 **Receive String** 值的行。
Receive Column	在返回表中包含 **Receive String** 值的列。
Receive String	接收用于 ECV 检查的表达式。缺省 **Send String** 和 **Receive String** 值是空的（“”），可与任意字符串匹配。
Reverse	如果接收的内容与 **Receive String** 的字符串匹配，那么将 pool、Pool 成员或节点设置为 **Down** 状态的模式。
Secret	仅针对 RADIUS Monitor 的共享密钥。
Security	Monitor 应该使用的安全协议（**SSL**、**TLS** 或**无**）。仅适用于 LDAP Monitor。
Send Packets	使用 UDP Monitor 时要发送的数据包的数量。
Send String	发送用于 ECV 检查的字符串。缺省 **Send String** 和 **Receive String** 值是空的（“”），可与任意字符串匹配。
Timeout	以秒为单位检查 pool、Pool 成员或节点的超时。
Timeout Packets	以秒为单位接收 UDP 数据包的超时。
Transparent	促使通过 pool、Pool 成员或节点 ping 通 IP 地址和/或透明 Pool 成员和节点端口的模式，例如防火墙。
URL	针对 WMI Monitor，提供 URL。
URL Path User Name	针对 SOAP Monitor，提供 URL 路径。 具有密码安全性的服务用户名。只对 LDAP Monitor 来说，这是一个识别名，也就是 LDAP 格式用户名。

表 10.2 所有可能的 Monitor 设置的列表

了解预配置和定制的Monitor

要监视 Pool 成员或节点的状态或性能时，可以使用预配置 Monitor，或创建并配置定制 Monitor。

使用预配置 Monitor

对于 Monitor 类型的子集，LTM 系统包括一组预配置 Monitor。***预配置 Monitor*** 是 LTM 系统提供给用户的现有 Monitor，其设置是已经配置好的。不能修改预配置 Monitor 设置，因为您必须按原状使用这些设置。预配置 Monitor 的目的是消除显式创建一个 Monitor 的需要。当设置的值满足您当前的需要时，可以使用预配置 Monitor。

LTM 包括的预配置 Monitor 的名称是：

- **gateway_icmp**
- **http**
- **https**
- **https_443**
- **icmp**
- **real_server**
- **snmp_dca**

- **tcp**
- **tcp_echo**
- **tcp_half_open**

预配置 Monitor 的实例是 **icmp** Monitor。图 10.2 显示了 **icmp** Monitor 以及为其 **Interval**、**Timeout** 和 **Alias Address** 设置配置的值。请注意，**Interval** 值是 5，**Timeout** 值是 16，Transparent 值是 **No**，**Alias Address** 值是***All Address**。

```
Name icmp
Type ICMP
Interval 5
Timeout 16
Transparent No
Alias Address * All Addresses
```

图 10.2 I 图 10.2 cmp *预配置 Monitor*

如果 **Interval**、**Timeout**、**Transparent** 和 **Alias Address** 值能够满足您的需求，那么仅需使用 Configuration 工具中的 **Pools** 或 **Nodes** 屏幕将 **icmp** 预配置 Monitor 直接分配到 Pool、Pool 成员或节点。在这种情况下，不需要使用 Monitors 屏幕，除非只想查看这些预配置 Monitor 设置的值。

如果不想使用在预配置 Monitor 中配置的值，那么可以创建定制 Monitor。

使用定制 Monitor

定制 Monitor 是一种基于允许的 Monitor 类型创建的 Monitor。在预配置 Monitor 中定义的值不满足您的需求，或您所创建的 Monitor 类型不存在预配置 Monitor 时，就需要创建定制 Monitor。（有关 Monitor 类型的信息，请参阅第 10-2 页上的“Monitor 类型概述”。）

从预配置 Monitor 中导入设置

如果存在符合您创建的定制 Monitor 类型的预配置 Monitor，那么可以将该预配置 Monitor 的设置和值导入到定制 Monitor 中。然后，可以根据您的需要任意更改这些设置的值。例如，如果创建了一个称为 **my_icmp** 的定制 Monitor，那么该 Monitor 可以继承预配置 Monitor **icmp** 的设置和值。当希望保留新 Monitor 的一些设置值但不修改其它值的时候，这种导入现有设置值的能力是很有用的。

图 10.3 显示了称为 **my_icmp** 定制 ICMP 类型的 Monitor 的实例，该 Monitor 基于预配置 Monitor **icmp**。请注意，Interval 值已改为 **10**，而且 **Timeout** 值改为 **20**。其它设置保留在预配置 Monitor 中定义的值。

```
Name my_icmp
Type ICMP
Interval 10
Timeout 20
Transparent No
Alias Address * All Addresses
```

图 ***10.3*** *基于预配置 Monitor 的定制 Monitor*

从定制 Monitor 中导入设置

您可以从另一定制 Monitor 而不是从预配置 Monitor 导入设置。当使用在另一定制 Monitor 中定义的设置值，或创建的 Monitor 类型不存在预

配置 Monitor 时，这种能力是很有用的。例如，如果创建称为 **my_oracle_server2** 的定制 Monitor，那么可以从现有的 Oracle 类型的 Monitor（如 **my_oracle_server1**）导入设置。在这种情况下，由于 LTM 系统不提供预配置的 Oracle 类型的 Monitor，因此定制 Monitor 只是一种从中可以导入设置值的 Monitor。

选择 Monitor 的方法非常简单。和 **icmp** 一样，每个 Monitor 都包含基于它检查的服务类型的**类型**设置，例如，**http**、**https**、**ftp** 和 **pop3**，并将该类型作为其名称。（但不包括特定端口 Monitor，如调用用户提供的程序的 **External** Monitor。）

有关选择和配置 Monitor 的详细流程，请参阅第 10-10 页上的“创建定制 Monitor”。

从 Monitor 模板中导入设置

如果不存在符合正创建 Monitor 类型的预配置或定制 Monitor，那么 LTM 系统从 Monitor 模板中导入设置。***Monitor 模板***是一种看不见的实体，它存在于每一种 Monitor 的 LTM 系统中，并包含一组设置和缺省值。Monitor 模板仅用作 LTM 系统的工具，用于当不存在这种 Monitor 时将设置导入到定制 Monitor。

创建定制Monitor

当创建定制 Monitor 时，需要将 Configuration 工具用于：为 Monitor 提供唯一的名称，指定 Monitor 的类型，并且如果已经存在这种 Monitor，从现有的 Monitor 导入设置以及它们的值。然后，您可以更改任何导入的设置的值。

您必须根据 Monitor 类型创建每一个定制 Monitor。当创建 Monitor 时，Configuration 工具显示一个 Monitor 类型列表。要指定 Monitor 类型，仅选择符合需要检查的服务的类型。例如，如果要创建检查有关 pool 的 HTTP 服务运行状态的 Monitor，那么选择 **HTTP** 作为 Monitor 类型。

如果要检查有关 pool 或 Pool 成员的多种服务（例如 **HTTP** 和 **HTTPS**），那么可以将多个 Monitor 与该 pool 和 Pool 成员关联。有关详细信息，请参阅第 4 章“配置负载平衡 Pool”。

检查服务不是实施 Monitor 的唯一原因。如果想验证目的地 IP 地址是否有效，或通过透明节点的路径是否有效，那么使用其中一个简单 Monitor：**icmp** 或 **tcp_echo**。或者，如果仅想验证 TCP，那么使用 Monitor **tcp**。

♦ **注：**

在创建定制 Monitor 之前，必须确定 Monitor 的类型。有关 Monitor 类型的信息，请参阅第 10-11 页上的“配置 Monitor 设置”。

创建定制 Monitor 的步骤

1. 在 Main 选项卡上，展开 **Local Traffic**。
   将展开 **Local Traffic** 菜单。
2. 点击 **Monitors**。
   此操作将显示现有 Monitor 列表。
3. 在屏幕的右上角，点击 **Create**。
   将打开 New Monitor 屏幕。

4. 对于 **Type** 设置，选择要创建的 Monitor 的类型。
   如果这种 Monitor 已经存在，就会显示 **Import Settings**。
5. 根据其中一个设置来指定名称：
   - 如果显示 **Import Settings**，那么从列表中选择 Monitor 名称。
   - 如果所选的 Monitor 类型不存在，那么在 **Name** 框中，为定制 Monitor 输入一个唯一的名称。
6. 在屏幕的 Configuration 部分，选择 **Advanced**。此操作使您能够修改其它缺省设置。
7. 配置所有显示的设置。
8. 点击 **Finished**。

配置Monitor设置

在创建定制 Monitor 之前，必须选择 Monitor 的类型。Monitor 类型分为以下三类：

- **简单 Monitor**
  这些 Monitor 是状态 Monitor，可监视节点状态。
- **扩展内容验证（ECV）Monitor**
  这些 Monitor 是状态 Monitor，可通过从 Pool 成员或节点检索特定内容来验证服务状态。
- **外部应用验证（EAV）Monitor**
  这些 Monitor 是状态或性能 Monitor，可通过使用外部服务检查程序执行远程应用来验证服务状态。

简单Monitor

简单 Monitor 是那些只检查节点而不检查 Pool 成员的 Monitor。简单 Monitor 类型包括：

- ICMP
- 网关 ICMP
- TCP Echo
- TCP 半开

LTM 系统提供一组预配置的简单 Monitor：**icmp**、**gateway_icmp**、**tcp_echo** 和 **tcp_half_open**。您可以按原状使用这些预配置 Monitor，也可以创建这几种类型的定制 Monitor。

以下数节描述了每种类型的简单 Monitor，并介绍了该类型的预配置 Monitor。请注意，每个预配置 Monitor 均由设置及其值组成。每个预配置 Monitor 中的设置及其对应的值以粗体进行区分。

ICMP

通过 ICMP 类型的 Monitor，您可以使用互联网控制信息协议（ICMP）对节点进行简单的检查。如果 Monitor 收到对 ICMP_ECHO 数据报的响应，那么说明检查成功。图 10.4 显示了预配置 Monitor **icmp** 的设置和它们的值。

```
Name icmp
Type ICMP
Interval 5
Timeout 16
Transparent No
Alias Address * All Addresses
```

***图 10.4** icmp 预配置 Monitor*

Transparent 模式是 ICMP 类型的 Monitor 的一个选项。将将该模式设置为**是**时，Monitorping 通该 Monitor 与之关联的节点。有关 **Transparent** 模式的详细信息，请参阅第 10-34 页上的“使用透明模式和反向模式”。

网关 ICMP

网关 ICMP 类型的 Monitor 具有特殊目的。您可以将该 Monitor 用于执行网关安全保护以获得高可用性的 pool。

网关 ICMP Monitor 与 ICMP Monitor 的工作原理相同，但不可以将网关 ICMP Monitor 应用到 Pool 成员。（切记只可以将 ICMP Monitor 应用到节点而不能应用到 Pool 成员。）图 10.5 显示了预配置 **gateway_ICMP Monitor** 的设置和它们的值。

```
Name gateway_icmp
Type Gateway ICMP
Interval 5
Timeout 16
Alias Address * All Addresses
Alias Service Port * All Ports
```

***图 10.5 gateway_icmp** 预配置 Monitor*

TCP Echo

通过 TCP Echo 类型的 Monitor，可以验证传输控制协议（TCP）连接。如果 LTM 系统收到对 TCP Echo 消息的响应，那么说明该检查成功。TCP Echo 类型还支持 **Transparent** 模式。在这种模式下，与 Monitor 关联的节点被 ping 通到目的地节点。（有关 **Transparent** 模式的详细信息，请参阅第 10-34 页上的“使用透明模式和反向模式”）。

要使用 TCP Echo Monitor 类型，必须确保在监控的节点上启用 TCP Echo。图 10.6 显示了预配置 Monitor **tcp_echo** 的设置。

```
Name tcp_echo  {
Type TCP Echo
Interval 5
Timeout 16
Transparent No
Alias Address * All Addresses
```

***图 10.6 tcp_ech** 预配置 Monitor*

TCP 半开

TCP 半开类型的 Monitor 通过将 TCP SYN 数据包发送到相关服务，快速对该服务进行检查。Monitor 一旦收到来自该服务的 SYN-ACK 数据包，就会认为该服务处于开启的状态，并且将 RESET 发送到该服务，而不会完成三次握手。

图 10.7 显示了预配置 Monitor **tcp_half_open** 的设置。

```
Name tcp_half_open  {
Type TCP Half Open
Interval 5
Timeout 16
Transparent No
Alias Addresses * All Addresses
Alis Service Ports * All Ports
```

***图 10.7** tcp **_half**_open 预配置 Monitor*

扩展内容验证（ECV）Monitor

ECV Monitor 使用 **Send String** 和 **Receive String** 这两个设置尝试从 Pool 成员或节点中检索显式内容。LTM 系统为以下这些 ECVMonitor 类型提供预配置 Monitor **tcp**、**http**、**https** 和 **https_443**：

- TCP
- HTTP
- HTTPS

TCP、HTTP 和 HTTPS Monitor 仅能与 pool 和 Pool 成员进行关联，而无法与节点进行关联。您可以按原状使用预配置的 ECV Monitor，也可以根据这些 Monitor 类型创建定制 Monitor。

以下数节描述了每种类型的简单 Monitor，并介绍了该类型的预配置 Monitor。请注意，每个预配置 Monitor 均由设置及其值组成。每个预配置 Monitor 中的设置及其对应的值以粗体进行区分。

TCP

TCP 类型的 Monitor 尝试接收通过 TCP 发送的特定内容。这种检查在内容与 **Receive String** 值匹配时成功。TCP 类型的 Monitor 采用一个 **Send String** 值和一个 **Receive String** 值。如果 **Send String** 值为空且能够生成连接，则将服务视为已启用。空的 **Receive String** 值可以匹配任何响应。可用选项包括 **Transparent** 模式和 **Reverse** 模式。有关 **Transparent** 模式和 **Reverse** 模式的详细信息，请参阅第 10-34 页上的“使用透明模式和反向模式”。

图 10.8 显示了预配置 Monitor **tcp** 的设置。

```
Name tcp
Type TCP
Interval 5
Timeout 16
Send String ''
Receive String '"
Reverse No
Transparent No
Alias Address * All Addresses
Alias Service Port * All Ports
```

***图 10.8 tcp** 预配置 Monitor*

HTTP

使用 HTTP 类型的 Monitor 可以检查超文本传输协议（HTTP）流量的状态。HTTP Monitor 尝试接收网页的特定内容，这与 TCP Monitor 相同；与 TCP Monitor 不同的是，它可以发送用户名和密码。这种检查在内容与 **Receive String** 的值匹配时成功。HTTP Monitor 使用发送字符串、接收字符串、用户名、密码以及可选的 **Reverse** 模式和 **Transparent**

模式。（如果不具备密码安全性，必须为 **Username** 和 **Password** 设置使用空字符串**[""]**。）

有关 **Transparent** 模式和 **Reverse** 模式的详细信息，请参阅第 10-34 页上的“使用透明模式和反向模式”。

图 10.9 显示了预配置 Monitor **http** 的设置。

```
Name http
Type HTTP
Interval 5
Timeout 16
Send String GET /
Receive String ""
User Name ""
Password ""
Reverse No
Transparent No
Alias Address * All Addresses
Alias Service Port * All Ports
```

***图 10.9 http** 预配置 Monitor*

HTTPS

使用 HTTPS 类型的 Monitor 可以检查超文本传输协议安全（HTTPS）流量的状态。HTTPS 类型的 Monitor 尝试接收受到 SSL 安全性保护的特定网页内容。这种检查在内容与 **Receive String** 的值匹配时成功。

HTTPS 类型的 Monitor 使用发送字符串、接收字符串、用户名、密码以及可选的 **Reverse** 模式。（如果不具备密码安全性，必须为 **Username** 和 **Password** 设置使用空字符串**[""]**。）有关 **Reverse** 设置的详细信息，请参阅第 10-34 页上的“使用透明模式和反向模式”。

HTTPS 类型的 Monitor 还具有 **Cipher List**、**Compatibility** 和 **Client Certificate** 等设置。如果未指定密码列表，Monitor 将使用缺省密码列表 **DEFAULT:+SHA:+3DES:+kEDH**。将 **Compatibility** 设置为 **Enabled** 时，这会将 SSL 选项设置为“全部”。使用 **Client Certificate** 设置可以指定 Monitor 随后向服务器出示的证书文件。

LTM 系统提供两种预配置的 HTTPS Monitor：**https** 和 **https_443**。图 10.10 显示了预配置 Monitor **https** 的设置；图 10.11 显示了预配置 Monitor **https_443** 的设置。

```
Name https
Type HTTPS
Interval 5
Timeout 16
Send String GET /
Receive String ""
Cipher List ""
User Name ""
Password ""
Compatibility Enabled
Client Certificate ""
Reverse No
Alias Address * All Addresses
Alias Service Port * All Ports
```

***图 10.10** https 预配置 Monitor*

```
Name https_443
Type HTTPS_443
Interval 5
Timeout 16
Send String GET /
Receive String ""
Cipher List ""
User Name ""
Password ""
Compatibility Enabled
Client Certificate ""
Reverse No
Alias Address * All Addresses
Alias Service Port HTTPS
```

***图 10.11 https_443** 预配置 Monitor*

Reverse 模式是一个 Monitor 选项，用于导入 **https** 和 **https_443** Monitor 中的设置。有关 **Reverse** 模式的详细信息，请参阅第 10-34 页上的“使用透明模式和反向模式”。

外部应用验证（EAV）Monitor

EAV Monitor 使用位于目录**/user/bin/monitors** 中的外部服务检查器程序，通过远程运行服务器上的应用来验证这些应用。

可以创建的 EAV Monitor 类型包括：

- External
- FTP
- DVIAP
- LDAP
- MSSQL
- NNTP
- Oracle
- POP3
- RADIUS
- Real Server
- SIP
- SMTP
- SNMP DCA
- SNMP DCA Base
- SOAP
- UDP
- WMI

LTM 系统根据 Monitor 类型 SNMP DCA 和 Real Server，提供了两种对应的预配置 EAV Monitor：**snmp_dca** 和 **real_server**。对于要使用的任何其它 EAV Monitor 类型，请创建定制 Monitor。
以下数节描述了每种类型的简单 Monitor，并介绍了该类型的预配置 Monitor。请注意，每个预配置 Monitor 均由设置及其值组成。每个预配置 Monitor 中的设置及其对应的值以粗体进行区分。

External

使用外部类型的 Monitor 可以创建您自己的 Monitor 类型。要执行此操作，请创建一个定制的外部类型的 Monitor，然后在其中指定要运行的由用户提供的 Monitor。

对于用户提供的 Monitor 程序，用于指定其可执行名称的设置是 **External Program**。缺省情况下，外部类型的 Monitor 在目录

/user/bin/monitors 中搜索该 Monitor 名称。如果用户提供的 Monitor 驻留在其它位置，您必须输入完整有效的路径名。

Arguments 设置允许您指定所需的命令行参数。

图 10.12 显示了外部类型的 Monitor 的设置和缺省值。

```
Name my_external
Type External
Interval 5
Timeout 16
External Program ""
Arguments ""
Variables ""
Alias Address * All Addresses
Alias Service Port * All Ports
```

图 10.12 *使用缺省值的外部类型的定制 Monitor*

FTP

使用 FTP 类型的 Monitor 可以监视文件传输协议（FTP）流量。此类型的 Monitor 尝试将指定的文件下载到**/var/tmp** 目录中，检查在检索到该文件时成功。请注意，文件成功下载之后，LTM 系统并不保存该文件。

FTP Monitor 指定用户名、密码和指向要下载的文件的完整路径。

图 10.13 显示了 FTP 类型的 Monitor 的设置和缺省值。

```
Name my_ftp
Type FTP
Interval 10
Timeout 31
User Name ""
Password ""
Path/Filename ""
Mode Passive
Alias Address * All Addresses
Alias Service Port * All Ports
```

图 10.13 *使用缺省值的 FTP 类型的定制 Monitor*

IMAP

使用 IMAP 类型的 Monitor 可以检查互联网信息访问协议（IMAP）流量的状态。从本质上来讲，IMAP Monitor 也是 POP3 类型的 Monitor，只不过多了一个 **Folder** 设置。如果 Monitor 可以登录服务器并打开指定的邮件文件夹，则检查成功。

IMAP Monitor 需要您指定用户名和密码。图 10.14 显示了 IMAP 类型的 Monitor 的设置和缺省值。

```
Name my_imap
Type IMAP
Interval 5
Timeout 16
User Name ""
Password ""
Folder INBOX
Alias Address * All Addresses
Alias Service Port * All Ports
```

图 10.14 *使用缺省值的 IMAP 类型的定制 Monitor*

◆ 注意

将由 IMAP Monitor 检查的服务器通常需要特殊的配置，以维持高级别的安全性，同时还需要允许 Monitor 认证。

LDAP

LDAP 类型的 Monitor 检查小型目录访问协议（LDAP）服务器的状态。LDAP 协议实施电子邮件目录整合标准 X.500。如果返回指定的基位和过滤器的对应条目，则检查成功。LDAP Monitor 需要用户名、密码以及基位和过滤器字符串。图 10.15 显示了 LDAP 类型的 Monitor 的设置和缺省值。

```
Name my_ldap
Type LDAP
Interval 10
Timeout 31
User Name ""
Password ""
Base ""
Filter ""
Security None
Alias Address * All Addresses
Alias Service Port * All Ports
```

图 10.15 *使用缺省值的 LDAP 类型的定制 Monitor*

Username 设置用于指定识别名，即 LDAP 格式的用户名。

Base 设置用于指定 LDAP 层次结构的起始位置，查询从该位置开始。

Filter 设置用于指定 LDAP 格式的搜索项关键字。

Security 设置用于指定要使用的安全协议。可接受的值为 **SSL**、**TLS** 或 **None**。

MSSQL

使用 MSSQL 类型的 Monitor 可以对基于 Microsoft SQL Server（例如 Microsoft SQL Server 版本 6.5 和版本 7.0）的服务执行服务检查。LTM 系统要求在执行实际登录之前，安装 JDBC 驱动程序。有关详细信息，请参阅附录 A“其它 Monitor 注意事项”。

如果收到拒绝连接的消息，请验证 IP 地址和端口号或服务是否正确。如果仍存在登录问题，请参阅第 10-21 页上的“解决 MSSQL 登录故障”。

关于 MSSQLMonitor 的本节剩余部分介绍了先决任务、缺省 Monitor 设置和解决故障的提示。

MSSQL 的先决任务

使用 MSSQL 类型的 Monitor 之前，必须下载一组 JDBC Java™档案（JAR）文件，然后将其安装在 LTM 系统上。有关详细信息，请参阅附录 A“其它 Monitor 注意事项”。

MSSQLMonitor 的设置及其缺省值

图 10.16 显示了 MSSQL 类型的 Monitor 的设置和缺省值。

```
Name my_mssql
Type mssql
Interval 30
Timeout 91
Send String ''
Receive String '"
User Name '"
Password "'
Database "'
Receive Row ''
Receive Column '"
Alias Address * All Addresses
Alias Service Port * All Ports
```

图 10.16 使用缺省值的 MSSQL 类型的定制 Monitor

在 MSSQL 类型的 Monitor 中，**Database** 设置用于指定基于 Microsoft® SQL 的服务器上的数据源的名称。例如：**sales** 和 **hr**。

Send String 是可选设置，用于指定 LTM 系统应发送到服务器的 SQL 查询语句。例如：**SELECT * FROM sales** 和 **SELECT FirstName, LastName From Employees**。如果配置了“发送字符串”设置，那么还可以配置以下设置：

- **Receive String**
  Receive String 设置是可选参数，用于指定期望为**接收行**和**接收列**设置指定的行和列返回的值。以下是 **Receive String** 值的一个示例：**ALAN SMITH**。仅当配置了 **Send String** 设置时，才可配置此设置。
- **Receive Row**
  Receive Row 是可选设置，仅在指定了 **Receive String** 设置时有效。此设置用于指定包含 **Receive String** 值的返回表的行。仅当配置了 **Send String** 设置时，才可配置此设置。
- **Receive Column**
  Receive Column 是可选设置，仅在指定了 **Receive String** 设置时有效。此设置用于指定包含 **Receive String** 值的返回表的列。仅当配置了 **Send String** 设置时，才可配置此设置。

解决 MSSQL 登录故障

如果 MSSQL Monitor 无法登录到服务器，且已查明指定的 IP 地址和端口号或服务是正确的，请尝试以下方法：

- **验证能够其它工具登录。**
  例如，服务器程序 Microsoft NT SQL Server（版本 6.5）包括名为 ISQL/w 的**客户端**程序。此客户端程序可以执行到 SQL 服务器的简单登录。请使用此程序测试能否使用 ISQL/w 程序登录到服务器。

- **使用 Microsoft SQL Enterprise Manager 添加登录账户。**
  在 Microsoft SQL Server 上，您可以运行 SQL Enterprise Manager 来添加登录账户。首次进入 SQL Enterprise Manager 时，会提示您选择要**管理**的 SQL 服务器。

  您可以通过输入计算机名称、用户名和密码来注册服务器。如果这些名称都正确，服务器将变为已注册状态，您随后便可点击服务器图标。展开服务器的子树时，可看到登录账户的图标。

  在该子树之下可以找到 SQL 登录信息。在此，通过右键点击 **Logins** 图标可以更改密码或添加新的登录账户。首先，点击此图标访问 **Add Login** 选项。打开此选项后，键入新登录账户的用户

名、密码和允许该新账户访问的数据库。您必须授予 **test** 账户对 EAV 配置中指定的数据库的访问权限。

NNTP

使用 NNTP 类型的 Monitor 可以检查 Usenet 新闻流量的状态。如果 Monitor 从服务器检索到新闻组标识，则检查成功。NNTP Monitor 需要新闻组名称（例如：**alt.cars.mercedes**），必要时还要求输入用户名和密码。

图 10.17 显示了 NNTP 类型的 Monitor 的设置和缺省值。

```
Name my_nntp
Type NNTP
Interval 5
Timeout 16
User Name ""
Password ""
Newsgroup ""
Alias Address * All Addresses
Alias Service Port * All Ports
```

图 10.17 使用缺省值的 NNTP 类型的定制 Monitor

Oracle

使用 Oracle 类型的 Monitor 可以检查 Oracle 数据库服务器的状态。如果 Monitor 能够连接到服务器、以指定的用户身份登录，然后登出，则检查成功。

图 10.18 显示了 Oracle 类型的 Monitor 的设置和缺省值。

```
Name my_oracle
Type Oracle
Interval 30
Timeout 91
Send String GET /
Receive String ""
User Name ""
Password ""
Database ""
Receive Row ""
Receive Column ""
Alias Address * All Addresses
Alias Service Port * All Ports
```

图 10.18 使用缺省值的 Oracle 类型的定制 Monitor

Send String 设置用于指定 LTM 系统应发送到 Oracle 服务器的 SQL 语句。例如：**SELECT * FROM sales**。

Receive String 设置是可选参数，用于指定期望为 **Send String** 设置所检索的表的特定行和列返回的值。以下是 **Receive String** 值的一个示例：**SMITH**。

在 Oracle 类型的 Monitor 中，**Database** 设置用于指定 Oracle 服务器上的数据源的名称。例如：**sales** 和 **hr**。

Receive Row 是可选设置，仅在指定了 **Receive String** 设置时有效。此设置用于指定包含 **Receive String** 值的返回表的行。

Receive Column 是可选设置，仅在指定了 **Receive String** 设置时有

效。此设置用于指定包含 **Receive String** 值的返回表的列。

POP3

POP3 类型的 Monitor 用于检查邮局协议（POP）流量的状态。如果 Monitor 能够连接到服务器、以指定的用户身份登录，然后登出，则检查成功。POP3Monitor 需要用户名和密码。

图 10.19 显示了 POP3 类型的 Monitor 的设置和缺省值。

```
Name my_pop3
Type POP3
Interval 5
Timeout 16
User Name ""
Password ""
Alias Address * All Addresses
Alias Service Port * All Ports
```

图 10.19 *使用缺省值的 POP3 类型的定制 Monitor*

RADIUS

使用 RADIUS 类型的 Monitor 可以检查远程访问拨号用户服务（RADIUS）服务器的状态。如果服务器对发出请求的用户进行认证，则检查成功。RADIUS Monitor 需要用户名、密码和邮政编码的共享加密字符串。

注意
将由 RADIUS Monitor 检查的服务器通常需要特殊的配置，以维持高级别的安全性，同时还需要允许 Monitor 认证。

图 10.20 显示了 RADIUS 类型的 Monitor 的设置和缺省值。

```
Name my_radius
Type RADIUS
Interval 10
Timeout 31
User Name ""
Password ""
Secret ""
Alias Address * All Addresses
Alias Service Port * All Ports
```

图 10.20 *使用缺省值的 RADIUS 类型的定制 Monitor*

Real Server

Real Server 类型的 Monitor 用于检查运行 RealSystem Server 数据收集代理的 pool、Pool 成员或节点的性能。然后，Monitor 将相应地对流量进行动态负载平衡。性能 Monitor 通常与动态比率负载平衡共同使用。

有关性能 Monitor 和动态比率负载平衡的详细信息，请参阅第 4 章“配置负载平衡 Pool”和附录 A“其它 Monitor 注意事项”。

◆ **注意**

与状态 Monitor 不同，性能 Monitor 不报告 pool、Pool 成员或节点的状态。

LTM 系统提供名为 **real_server** 的预配置 Real Server Monitor。图 10.21 显示了 **real_server** Monitor 的设置和缺省值。

```
Name real_server
Type Real Server
Interval 5
Timeout 16
Method GET
Command GetServerStats
Metrics ServerBandwidth:1.5, CPUPercentUsage, MemoryUsage,
   TotalClientCount
Agent Mozilla/4.0 (compatible: MSIE 5.0; Windows NT)
Alias Address * All Addresses
Alias Service Port 12345
```

***图 10.21 real_server** 预配置 Monitor*

与所有预配置 Monitor 一样，用户无法修改 **real_server** Monitor。但如果希望修改 **Metrics** 设置，您可以创建一个定制 Real Server Monitor，然后向其添加指标并修改指标值。

♦ 注意

*创建定制 Real ServerMonitor 时，不可修改 **Method**、**Command** 和 **Agent** 这三个设置的值。*

表 10.3 显示了所有服务器专用的指标和适用于 **GetServerStats** 命令的指标设置缺省值。

指标	缺省系数	缺省阈值
ServerBandwidth（Kbps）	**1.0**	10,000
CPUPercentUsage	**1.0**	80
MemoryUsage（Kb）	**1.0**	100,000
TotalClientCount	**1.0**	1,000
RTSPClientCount	**1.0**	500
HTTPClientCount	**1.0**	500
PNAClientCount	**1.0**	500
UDPTransportCount	**1.0**	500
TCPTransportCount	**1.0**	500
MulticastTransportCount	**1.0**	500

***表 10.3** Real Server Monitor 的指标*

指标系数是用来确定指标值在整体比率权重计算中所占分量的因数。如果指标一定会具有一个权重，那么其阈值将是允许它具有的最大值。要了解如何使用这些值，有必要了解如何计算整体比率权重。整体比率权重是针对每个指标计算出的相对权重之和。而相对权重则基于以下三个因素：

- Monitor 返回的指标值
- 系数值
- 阈值

如果给定这些值，相对权重将按以下公式计算：

相对权重=((阈值-指标值)/阈值)*系数

不难看出，系数越大，针对该指标计算出的相对权重越大。同样，阈值越大，针对小于该阈值的任何指标值计算出的相对权重越大。（当指标值等于阈值时，权重为零。）

请注意，表 10.3 中显示的缺省系数值和缺省阈值是*指标*缺省值，而不是 *Monitor* 缺省值。Monitor 缺省值优先于指标缺省值，就像定制 **real_server**Monitor 中用户指定的值优先于 Monitor 缺省值一样。例如，所显示的 Monitor 为 **ServerBandwidth** 指定系数值 **1.5**，不指定其它指标的值。这表示，Monitor 使用 Monitor 缺省值 **1.5** 作为 **ServerBandwidth** 系数，使用指标缺省值 1 作为所有其它指标的系数。但是，如果对定制 Monitormy_real_server 进行配置，将 **ServerBandwidth** 系数指定为 **2.0**，那么这个用户指定的值将覆盖 Monitor 缺省值。

指标系数和阈值是仅有的非 Monitor 缺省值。如果要将不属于 Monitor 的指标添加到定制 Monitor，必须将该指标添加到 Metrics 设置的指标列表中。指定非缺省系数或阈值的语法为：

<metric>:<coefficient |<*>:<threshold>

SIP

使用 SIP 类型的 Monitor 可以检查 SIP 呼叫 ID 服务的状态。这类型的 Monitor 使用 UDP 向服务器设备发出请求。请求的目的是识别服务器设备支持的选项。如果返回相关请求，便将设备视为处于 **Update** 状态且正在响应命令。

图 10.22 显示了 SIP 类型的 Monitor 的设置和缺省值。

```
Name my_sip
Type SIP
Interval 5
Timeout 16
Mode UDP
Additional Accepted Status Codes None
Alias Address * All Addresses
Alias Service Port * All Ports
```

图 10.22 *使用缺省值的 SIP 类型的定制 Monitor*

Mode 设置可能的值包括 **TCP** 和 **UDP**。

Additional Accepted Status Codes 设置可能的值包括 **Any**、**None** 和 **Status Code List**。**Status Code List** 设置用于指定除状态代码 **200** 之外的一个或多个状态代码。为了指明 **Up** 状态，所有这些代码都是可接受的。多个状态代码应以空格分开。指定星号（*****）表明所有状态代码都可接受。

SMTP

SMTP 类型的 Monitor 检查简单邮件传输协议（SMTP）服务器的状态。此类 Monitor 是最基础的 Monitor，仅检查服务器的状态是否为 **Up** 且正在响应命令。如果邮件服务器响应标准的 SMTP 命令 **HELO** 和 **QUIT**，则检查成功。SMTP 类型的 Monitor 需要域名。

图 10.23 显示了 SMTP 类型的 Monitor 的设置和缺省值。

```
Name my_smtp
Type SMTP
Interval 5
Timeout 16
Domain '"
Alias Address * All Addresses
Alias Service Port * All Ports
```

图 10.23 *使用缺省值的 SMTP 类型的定制 Monitor*

SNMP DCA

使用 SNMP DCA 类型的 Monitor 可以检查运行 SNMP 代理（例如 UC Davis）的服务器的性能，以便对流向该服务器的流量进行负载平衡。通过此 Monitor 可以定义 CPU、内存和磁盘使用的比率权重。

性能 Monitor 通常与动态比率负载平衡共同使用。有关性能 Monitor 和动态比率负载平衡的详细信息，请参阅第 4 章“配置负载平衡 Pool”和附录 A“其它 Monitor 注意事项”。

◆ **注意**

与状态 Monitor 不同，性能 Monitor 不报告 pool、Pool 成员或节点的状态。

LTM 系统提供名为 **snmp_dca** 的预配置 SNMP DCA Monitor。图 10.24 显示了预配置 Monitor **snmp_dca** 的设置和值。

```
Name snmp_dca
Type SNMP DCA
Interval 10
Timeout 30
Community Public
Version v1
Agent Type UCD
CPU Coefficient 1.5
CPU Threshold 80
Memory coefficient 1.0
Memory Threshold 70
Disk Coefficient 2.0
Disk Threshold 90
Variables '"
Alias Address * All Addresses
Alias Service Port SNMP
```

图 10.24 snmp_dca *预配置 Monitor*

用户无法修改预配置 Monitor。因此，如果希望更改 SNMP DCAMonitor 设置的值，必须创建 SNMP DCA 类型的定制 Monitor。**Version** 设置可能的值包括 **v1**、**v2c** 和 **Other**。**Agent Type** 设置可能的值包括 **UCD**、**Win2000** 和 **Other**。

配置 SNMP DCA 定制 Monitor 时，可以使用 Monitor 中指定的缺省 CPU、内存和磁盘系数与阈值，也可以更改这些缺省值。您也可以选择指定系数和阈值，以收集其它类型的数据。请注意，如果所配置的 Monitor 用于除 UC Davis 之外的 SNMP 代理类型，那么必须指定代理类型，例如 **Win2000**。

SNMP DCA Base

使用 SNMP DCA Base 类型的 Monitor 可以检查运行 SNMP 代理（例

如 UC Davis）的服务器的性能。但是，仅当希望负载平衡的目标完全基于用户数据，而不基于 CPU、内存或磁盘的使用时，才应使用此 Monitor。

图 10.25 显示了 SNMP DCA Base 类型的 Monitor 的设置和缺省值。

```
Name my_snmp_dca_base
Type snmp_dca_base
Interval 10
Timeout 30
Community Public
Version v1
Variables ""
Alias Address * All Addresses
Alias Service Port SNMP
```

图 10.25 *使用缺省值的 SNMP DCA Base 类型的定制 Monitor*

性能 Monitor 通常与动态比率负载平衡共同使用。有关性能 Monitor 和动态比率负载平衡的详细信息，请参阅第 4 章“配置负载平衡 Pool”和附录 A“其它 Monitor 注意事项”。

◆ **注意**

与状态 Monitor 不同，性能 Monitor 不报告 pool、Pool 成员或节点的状态。

SOAP

SOAP Monitor 用于测试基于简单对象访问协议（SOAP）的 Web 服务。更确切地说，Monitor 向基于 SOAP 的 Web 服务发出请求，然后（可选）验证返回值或故障。图 10.26 显示了 SOAP 类型的 Monitor 的设置和缺省值。

```
Name my_soap
Type soap
User Name ""
Password ""
Protocol" HTTP
URL Path ""
Namespace ""
Method ""
Parameter Name ""
Parameter Type bool
Parameter Value ""
Return Type bool
Return Value ""
Expect Fault No
Alias Address * All Addresses
Alias Service Port * All Ports
```

图 10.26 *使用缺省值的 SOAP 类型的定制 Monitor*

Protocol 设置可能的值包括 **HTTP** 和 **HTTPS**。

Parameter Type 设置可能的值包括：**bool**、**int**、**long** 和 **string**。

Return Type 设置可能的值包括：**bool**、**int**、**short**、**long**、**float**、**double** 和 **string**。

Expect Fault 设置可能的值包括 **No** 和 **Yes**。

UDP

您在系统发送用户数据报协议（UDP）数据包时，使用 UDP 类型的

Monitor。按照设计，UDP 类型的 Monitor 向目标 pool、Pool 成员或节点发送一个或多个 UDP 数据包，以检查 UDP 服务的状态。

图 10.27 显示了 UDP 类型的 Monitor 的设置和缺省值。如图中所示，**Timeout Packets** 设置的值（以秒为单位）应低于 **Interval** 设置的值。

```
Name my_udp
Type UDP
Interval 5
Timeout 16
Send String default send string
Send Packets 2
Timeout Packets 2
Alias Address * All Addresses
Alias Service Port * All Ports
```

图 10.27 *使用缺省值的 UDP 类型的定制 Monitor*

使用 UDP 类型的 Monitor 来监视 pool、Pool 成员或节点时，必须同时启用另一类 Monitor（例如 **ICMP**）来监视 pool、Pool 成员或节点。只有 UDP 类型的 Monitor 和另一类 Monitor 都报告 UDP 服务处于“启动”状态时，UDP 服务才会接收流量。详细信息请参阅表 10.4。

UDP Monitor 报告的状态	**另一个 Monitor 报告的状态**	**相应 UDP 服务的状态**
Up	Up	Up
Up	Down	Down
Down	Up	Down
Down	Down	Down

表 10.4 *确定 UDP 服务的状态*

WMI

WMI 类型的 Monitor 检查运行 Windows 管理基础架构（WMI）数据收集代理的 pool、Pool 成员或节点的性能，然后相应地对流量进行动态负载平衡。

通常将诸如 WMI Monitor 这样的性能 Monitor 与动态比率负载平衡一起使用。有关性能 Monitor 和动态比率负载平衡的详细信息，请参阅第 4 章 *“配置负载平衡 Pool”* 和附录 A *“其它 Monitor 注意事项”*。

◆ 注意

与状态 Monitor 不同，性能 Monitor 不报告 pool、Pool 成员或节点的状态。

图 10.28 显示了 WMI 类型的 Monitor 的设置和缺省值。

```
Name my_wmi
Type wmi
Interval 5
Timeout 16
User Name ""
Password ""
Method POST
URL /scripts/f5Isapi.dll
Command GetCPUInfo, GetDiskInfo, GetOSInfo
Metrics LoadPercentage, DiskUsage, PhysicalMemoryUsage:1.5,
   VirtualMemoryUsage:2.0
Agent Mozilla/4.0 (compatible: MSIE 5.0; Windows NT)
Post RespFormat=HTML
Alias Address * All Addresses
Alias Service Port HTTP
```

图 10.28 *使用缺省值的 WMI 类型的定制 Monitor*

请注意，创建定制 WMI Monitor 时，唯一需要更改的缺省值是用户名和密码的空值。还应注意，不可更改 **Method** 设置的值。

表 10.5 显示了可以使用 **Command** 和 **Metrics** 设置来指定的全部命令和指标，同时还显示了缺省指标值。

命令	指标	缺省系数	缺省阈值
GetCPUInfo	LoadPercentage（%）	1.0	80
GetOSInfo	PhysicalMemoryUsage（%）	1.0	80
	VirtualMemoryUsage（%）	1.0	80
	NumberRunningProcesses	1.0	100
GetDiskInfo	DiskUsage（%）	1.0	90
GetPerfCounters	TotalKBytesPerSec	1.0	10,000
	ConnectionAttemptsPerSec	1.0	500
	CurrentConnections	1.0	500
	GETRequestsPerSec	1.0	500
	PUTRequestsPerSec	1.0	500
	POSTRequestsPerSec	1.0	500
	AnonymousUsersPerSec	1.0	500
	CurrentAnonymousUsers	1.0	500
	NonAnonymousUsersPerSec	1.0	500
	CurrentNonAnonymousUser	1.0	500
	CGIRequestsPerSec	1.0	500
	CurrentCG I Requests	1.0	500

命令	指标	缺省系数	缺省阈值
	ISAPIRequestsPerSec	1.0	500
	CurrentISAPIRequests	1.0	500
GetWinMediaInfo	Agg regateRead Rate	1.0	10,000 Kbps
	Agg regateSend Rate	1.0	10,000 Kbps
	ActiveLiveUnicastStreams	1.0	1000
	ActiveStreams	1.0	1000
	ActiveTCPStreams	1.0	1000
	ActiveUDPStreams	1.0	1000
	Allocated Bandwidth	1.0	10,000 Kbps
	AuthenticationRequests	1.0	1000
	AuthenticationsDenied	1.0	100
	Authorization Requests	1.0	1000
	AuthorizationsRefused	1.0	100
	ConnectedClients	1.0	500
	ConnectionRate	1.0	500
	HTTPStreams	1.0	1000
	HTTPStreamsReadingHeader	1.0	500
	HTTPStreamsStreamingBody	1.0	500
	Late Reads	1.0	100
	PendingConnections	1.0	100
	PluginErrors	1.0	100
	PluginEvents	1.0	100
	SchedulingRate	1.0	100
	Stream Errors	1.0	100
	Stream Terminations	1.0	100
	UDPResendRequests	1.0	100
	UDPResendsSent	1.0	100

***表 10.5** WMI 类型的 Monitor 的命令和指标*

特殊配置考虑因素

每个预配置 Monitor 或定制 Monitor 都带有一些设置以及为它们分配的缺省值。以下数节介绍了更改这些缺省值时需要用到的信息。

设置目的地

缺省情况下，Monitor 中 **Alias Address** 的设置为*** Addresses**，**Alias Service Port** 的设置为*** Ports**，此处的*****是通配符。此值使针对 pool、Pool 成员或节点创建的 Monitor 实例采用该节点的地址或地址加端口作为自己的目的地。但您可以创建一个定制 Monitor，使用明确的目的地值代替这两个通配符或者其中之一。**Alias Address** 和/或 **Alias Service Port** 设置的确切值用于将实例目的地强行指定为一个特定的地址和/或端口（可以不是 pool、Pool 成员或节点的地址和/或端口）。

ECVMonitor 的 **http**、**https** 和 **tcp** 具有 **Send String** 和 **Receive String** 两个设置，分别用于发送字符串和接收表达式。

最常见的 **Send String** 值是 **GET /**，它检索网站的缺省 HTML 页面。要从网站检索特定的页面，可以输入 **Send String** 值，也就是一个完整有效的路径名称，例如：

"GET /www/support/customer_info_form.html"

Receive String 表达式是 Monitor 在返回的资源中查找的文本字符串。最常见的 **Receive String** 表达式包含包括在特殊站点 **HTML** 页面中的文本。文本字符串可以是规则文本、**HTML** 标签或图像名称。

以下的示例 **Get** 表达式用于搜索标准的 **HTML** 标签：

"<HEAD>"

您也可以使用缺省的空 **Receive String** 值[""]。在此情形中，接收的任何内容都视为匹配项。如果 **Send String** 和 **Receive String** 都保留为空，将仅执行简单连接检查。

对于 **HTTP** 和 **FTP Monitor**，可以使用特殊设置 **get** 或 **hurl** 来代替 **Send String** 和 **Receive String** 语句。（仅针对 **FTP Monitor**）**GET** 设置用于指定要检索的文件的完整路径。

使用透明模式和反向模式

Monitor 的正常缺省行为是通过一个未指定的路由器，对目的地的 pool、Pool 成员或节点进行试通（ping 命令），如果测试成功，则将节点的状态标记为 **Up**。但对于某些特定类型的 Monitor，可以指定路由器，供 Monitor 对目的地的服务器进行试通。这个配置可以通过指定定制 Monitor 中的 **Transparent** 或 **Reverse** 设置来实现。

- **Transparent 设置**
  有时，需要通过透明的 pool、Pool 成员或节点对具有别名的目的地进行试通。创建定制 Monitor 并将 **Transparent** 设置设定为 **Yes** 时，**LTM** 系统将强制 Monitor *通过*与其关联的 pool、Pool 成员或节点（通常是防火墙）对 pool、Pool 成员或节点进行试通。（换句话说，如果负载平衡 Pool 中有两个防火墙，则始终通过指定的 pool、Pool 成员或节点，而不是通过负载平衡方法选择的 pool、

Pool 成员或节点对目的地的 pool、Pool 成员或节点进行试通。）在这种方式中，将对透明的 pool、Pool 成员或节点进行测试：如果没有响应，则将透明的 pool、Pool 成员或节点标记为 **Down**。

常见示例包括通过防火墙检查路由器、邮件或 **FTP** 服务器。例如，您可能希望通过透明防火墙 **10.10.10.101:80** 来检查路由器地址 **10.10.10.53:80**。要实现此目的，请创建称为 **http_trans** 的 Monitor，并在其中指定 **10.10.10.53:80** 作为 Monitor 的目的地地址，同时将 **Transparent** 设置设定为 **Yes**。然后，将 Monitor **http_trans** 与透明的 pool、Pool 成员或节点进行关联。

这会使 Monitor 通过 **10.10.10.101:80** 检查地址 **10.10.10.53:80**。（换句话说，LTM 系统通过 **10.10.10.101:80** 来路由对 **10.10.10.53:80** 的检查。）如果没有从 **10.10.10.53:80** 接收到正确的响应，则将 **10.10.10.101:80** 标记为 **Down**。有关将 Monitor 与 Pool 成员或节点进行关联的详细信息，请参阅第 10-36 页上的*“将 Monitor 与 pool 和节点关联”*。

- **Reverse 设置**
  如果将 **Reverse** 设置设定为 **Yes**，Monitor 在测试成功时将 pool、Pool 成员或节点标记为**关闭**。例如，如果网站主页采用动态内容，经常变化，那么可能希望建立反向 **ECV** 服务检查，查找字符串“**Error**”。找到此字符串的匹配项意味着 Web 服务器已 **Down**。

表 10.6 显示了包含 **Transparent** 设置、**Reverse** 设置或这两个设置的 Monitor。

Monitor 类型	**设置**	
TCP	Transparent	Reverse
HTTP	Transparent	Reverse
HTTP	Transparent	Reverse
TCP Echo	Transparent	
ICMP	Transparent	

表 10.6 *包含* **Transparent** *设置或* **Reverse** *设置的 Monitor*

将Monitor与pool和节点关联

创建 Monitor 并配置其设置之后，最后一项任务是将 Monitor 与要监视的一个或多个服务器进行关联。此处所说的服务器可以是 pool、Pool 成员或节点，具体取决于 Monitor 的类型。

按照设计，一些 Monitor 类型仅与节点相关联，而不与 pool 或 Pool 成员相关联；而其它 Monitor 类型则仅与 pool 和 Pool 成员相关联，不与节点相关联。因此，使用 Configuration 工具将 Monitor 与 pool、Pool 成员或节点进行关联时，工具仅显示设计用来与该服务器进行关联的那些预配置 Monitor。例如，无法将 Monitor**icmp** 与 pool 或其成员进行关联，因为 **ICMP Monitor** 设计用于检查节点自身的状态，而不是检查运行在该节点上的任何服务的状态。

将 Monitor 与服务器进行关联时，**LTM** 系统自动为该服务器创建该 Monitor 的 ***instance***。进而，Monitor 关联将为您指定的每台服务器创建一个 Monitor 实例。因此，您可以在服务器上运行同一个 Monitor 的多个实例。

Configuration 工具允许您禁用正在服务器上运行的 Monitor 实例。这使您能够挂起状态或性能检查，而无需真地删除 Monitor 关联。准备再次

开始监视该服务器时，只需简单地重新启用该 Monitor 实例。

Monitor关联的类型

Monitor 关联有如下三种类型：

- **Monitor 与 pool 关联**
  此类关联将 Monitor 与整个负载平衡 Pool 进行关联。在此情形中，Monitor 检查该 pool 的所有成员。例如，您可以为 **my_pool** pool 的每个成员创建一个 **httP Monitor** 实例，从而确保该 pool 中的所有成员都受到检查。

- **Monitor 与 Pool 成员关联**
  此类关联将 Monitor 与单独的 Pool 成员（即 IP 地址和服务）进行关联。在此情形中，Monitor 仅检查该 Pool 成员，而不检查该 pool 的任何其它成员。例如，您可以为 **my_pool** 的 Pool 成员 **10.10.10.10:80** 创建一个 **httP Monitor** 实例。

- **Monitor 与节点关联**
  此类关联将 Monitor 与特定节点进行关联。在此情形中，Monitor 仅检查节点自身，而不检查节点上运行的任何服务。例如，您可以为节点 **10.10.10.10** 创建一个 **ICMP Monitor** 实例。在此情形中，Monitor 仅检查这个特定的节点，而不检查该节点上运行的任何服务。

有关将 Monitor 与 pool 和 Pool 成员进行关联的详细信息，请参阅第 4 章 *“配置负载平衡 Pool”*。有关将 Monitor 与节点进行关联的详细信息，请参阅第 3 章 *“配置节点”*。

管理Monitor

管理现有 Monitor 时，您可以显示或删除这些 Monitor，也可以启用和禁用 Monitor 实例。请注意，删除 Monitor 之前，必须删除全部现有的 Monitor 关联。

显示 Monitor 的步骤

1. 在 Main 选项卡上，展开 **Local Traffic**。
2. 点击 **Monitors**。
   将显示现有 Monitor 的列表。
3. 点击一个 Monitor 名称。
   此操作将显示 Monitor 的设置及其值。

删除 Monitor 的步骤

1. 在 Main 选项卡上，展开 **Local Traffic**。
2. 点击 **Monitors**。
   将显示现有 Monitor 的列表。
3. 点击要删除的 Monitor 对应的 Select 框。
4. 点击 **Delete**。
   将显示确认消息。
5. 点击 **Delete**。

启用或禁用 Monitor 实例的步骤

1. 在 Main 选项卡上，展开 **Local Traffic**。
2. 点击 **Monitors**。

此操作将显示定制 Monitor 列表。

3. 在列表中点击 Monitor 名称。
4. 在菜单栏中，点击 Instance。
   此操作将列出全部现有的 Monitor 实例。
5. 对于要管理的实例，点击相应的 Select 框。
6. 点击 **Enable** 或 **Disable**。
7. 点击 **Update**。

11

配置 SNAT 和 NAT

- 安全网络地址转换简介
- 创建 SANT pool
- 实施 SNAT
- 实施 NAT
- 管理 SNAT 和 NAT
- SNAT 示例

安全网络地址转换简介

在 BIG-IP®本地流量管理（LTM）系统上配置的 Real Server 可以将入站数据包的目的地 IP 地址转换为另一个目的地 IP 地址，以便对该数据包进行负载平衡。通常，源 IP 地址保持不变。

此外，也可以创建安全网络地址转换（SNAT）。*SNAT* 是一个将原始客户机 IP 地址（也就是源 IP 地址）映射到您所选择的转换地址的对象。因此，***SNAT*** 会让 LTM 系统将入站数据包的源 IP 地址转换为您指定的地址。SNAT 的目的非常简单，即：确保目标服务器通过 LTM 系统将其响应返回到指定的地址，而不是直接发送到原始客户机 IP 地址。

要创建 SNAT，可以使用 Configuration 工具或编写 iRule，这取决于您创建的 SNAT 类型。

◆ 注

这种转换类型对 Real Server 执行的目的地地址转换没有影响。

在以下情况下 SNAT 十分有用：

- 连接到需要可路由返回 IP 地址的外部设备；
- 通过与客户机相同的 IP 子网上的节点连接到 Real Server。

◆ 提示

*由于 SNAT 的目的只是改变入站数据包的源 IP 地址，因此术语**安全网络地址转换**有些用词不当。缩写词 SNAT 最好定义为**源网络地址转换**，或**源 NAT**。*

SNAT的工作原理

SNAT 的工作原理如下：

1. LTM 系统接收从原始客户机 IP 地址发送的数据包，并检查 SNAT 中是否定义了此源地址。

2. 如果 SNAT 中定义了客户机的 IP 地址，那么 LTM 系统将源 IP 地址改变为 SNAT 中定义的转换地址。

3. 然后，LTM 系统将 SNAT 转换地址作为源地址，向目标服务器发送客户机请求。

此流程的最终结果是目标服务器为客户机提供了一个可路由的 IP 地址，服务器在响应时，可将此 IP 地址指定为目的地 IP 地址。

将原始IP地址映射到转换地址

根据您的需要，在创建 SNAT 时可以通过多种方法将原始 IP 地址映射到转换地址。例如，您可以显式地将原始 IP 地址映射到单一转换地址，或者创建一个转换地址的 pool，然后将原始 IP 地址映射到此地址 pool。

将特定原始 IP 地址映射到特定转换地址

创建 SNAT 的一种方法是将一个或多个原始 IP 地址直接映射到您所选

择的特定转换地址。采用这种方法创建的 SNAT 是标准型 SNAT。***标准 SNAT*** 是使用 Configuration 工具的“New SNAT”屏幕创建的 SNAT 对象。有关标准 SNAT 的详细信息，请参阅第 11-6 页上的*“实施 SNAT”*。

使用 SNAT 自动映射特性

创建 SNAT 的另一种方法是使用 LTM 系统的 SNAT 自动映射特性。***SNAT Automap*** 特性可自动将系统本身的 IP 地址映射到在创建 SNAT 过程中指定的原始 IP 地址。在使用该特性时，无需显式指定转换地址。

采用这种方法创建的 SNAT 是标准型 SNAT。有关标准 SNAT 的详细信息，请参阅第 11-6 页上的*“实施 SNAT”*。

将特定原始 IP 地址映射到转换地址 pool

您也可以通过创建转换地址 pool，然后将原始 IP 地址映射到整个转换 pool 来创建 SNAT。这个转换地址 pool 就是众所周知的 *SANT pool*。您可以使用 Configuration 工具的“New SANT Pool”屏幕来创建 SANT pool。有关创建 SANT pool 的详细信息，请参阅第 11-6 页上的*“实施 SNAT”*。

创建 SANT pool 并将其映射到原始 IP 地址之后，Real Server 就会接收从原始 IP 地址发送的数据包，而 LTM 系统会从 SANT pool 选择转换地址。然后，系统会将原始 IP 地址转换为所选地址。

您可以采用以下两种方法之一将原始 IP 地址映射到 SANT pool：

- **通过创建 SNAT 对象。**
  通过 Configuration 工具中的“New SNAT”屏幕，采用这种方法创建的 SNAT 是标准型 SNAT。有关标准 SNAT 的详细信息，请参阅第 11-6 页上的*“创建标准 SNAT”*。

- **通过编写 iRule。**
  采用这种方法，您无需创建 SNAT 对象。但是需要编写包括 **snat** 或 **snat pool** 命令的 iRule。通过编写 iRule 创建的 SNAT 类型称为智能 SNAT。***智能 SNAT*** 使用 iRule，将一个或多个原始客户机 IP 地址映射到转换地址。有关智能 SNAT 的详细信息，请参阅第 11-9 页上的*“创建智能 SNAT”*。

将所有原始 IP 地址映射到转换地址 pool

创建 SNAT 的另一种方法是创建 SANT pool（使用 Configuration 工具的“New SANT pool”屏幕），并且将其直接分配到 Real Server，作为 Real Server 的资源。在将 SANT pool 分配到 Real Server 之后，LTM 系统会自动将来自 Real Server 的所有原始 IP 地址映射到该 SANT pool。借助智能 SNAT，您无需使用 Configuration 工具的“New SNAT”屏幕创建 SNAT 对象。有关这种类型的 SNAT 的详细信息，请参阅第 11-10 页上的*“将 SANT pool 直接分配到 Real Server”*。

创建SANT pool

如果您决定使用 SANT pool 作为在 SNAT 中指定转换地址的方法，那么必须首先创建 SANT pool，指定一个或多个您所希望包括在 SANT pool 中的转换地址。您可以使用 Configuration 工具创建 SANT pool。有关

SANT pool 的背景信息，请参阅第 11-3 上页的*“将特定原始 IP 地址映射到转换地址 pool ”*。

创建 SANT pool 后，可以创建最符合您的需求的 SNAT 类型（Standard SNAT、Intelligent SNAT 或直接分配到 Real Server 的 SANT pool）。要了解您可以创建的不同 **SNAT** 类型，请参阅第 11-6 页上的*“实施 SNAT ”*。

在创建 SANT pool 时，必须对两个设置进行配置。表 11.1 列出并介绍了这些设置。

属性	说明	缺省值
Name	**SANT pool** 的唯一名称。	无缺省值
Member List	您希望包括在 **SANT pool** 中的 **IP** 地址列表。如果您添加的 **IP** 地址还没有被指定为转换地址，那么 **LTM** 系统会自动将其指定为转换地址，并且根据它们的缺省值，分配适当的属性。此设置是必需的。	无缺省值

表 11.1 *SANT pool 的属性*

您向 SANT pool 添加的每个转换地址都有多个设置，您可以在向 SANT pool 添加地址之后对这些设置进行配置。有关这些设置的详细信息，请参阅第 11-8 页上的*“指定转换地址 ”*。

创建了 SANT pool 后，您必须执行以下操作之一：

- 参考您创建的 SNAT 对象中的 SANT pool。在创建标准 SNAT 时执行此操作。有关详细信息，请参阅第 11-6 页上的*“创建标准 SNAT ”*。
- 参考 iRule 中的 SANT pool，然后将 iRule 作为一项资源分配到 Real Server。在创建智能 SNAT 时执行此操作。有关详细信息，请参阅第 11-9 页上的*“创建智能 SNAT ”*。
- 将 SANT pool 直接作为一项资源分配到 Real Server。有关详细信息，请参阅第 11-10 页上的*“将 SANT pool 直接分配到 Real Server ”*。

创建 SANT pool 的步骤

1. 在 Main 选项卡上，展开 **Local Traffic**。
2. 点击 **SNATs**。
   此操作将显示现有 SNAT 列表。
3. 在菜单栏中，点击 SNAT Pool List。
   此操作将显示现有 **SANT Pool 列表**。
4. 在屏幕的右上角，点击 **Create**。
5. 在 **Name** 设置中，输入 SANT pool 的唯一名称。
6. 在 **Member List** 设置中，输入 IP 地址。
7. 点击 **Add**。
8. 对希望添加的每个转换地址重复步骤 6 和步骤 7。
9. 点击 **Finished**。

实施SNAT

在实施安全网络地址转换前，应该决定要创建哪种类型的 SNAT。可以创建的 SNAT 类型包括：

- **标准 SNAT**
  标准 SNAT 是使用 Configuration 工具创建的对象，它指定将一个或多个原始客户机 IP 地址映射到转换地址。对于这种类型的 SNAT，LTM 系统用来决定何时应用转换地址的标准将严格基于原始 IP 地址。也就是说，如果数据包来自您在 SNAT 中指定的原始 IP 地址，那么 LTM 系统会将该地址转换为指定的转换地址。

  您可以创建的标准 SNAT 包括以下三种类型：

  - 在其中可以指定特定转换地址的 SNAT
  - 使用自动映射特性的 SNAT
  - 在其中可以指定 SANT pool 作为转换地址的 SNAT

- **智能 SNAT**
  与标准 SNAT 类似，***智能 SNAT*** 可将一个或多个原始客户机 IP 地址映射到转换地址。但是，您应该在 iRule 中而不是通过创建 SNAT 对象来实施这种类型的 SNAT 映射。对于这种类型的 SNAT，LTM 系统用来确定何时应用转换地址的标准基于在 iRule 中指定的任何数据片断（例如，HTTP cookie 或服务器端口）。

- **将 SANT pool 作为 Real Server 资源分配**
  这种类型的 SNAT 只包含直接作为一项资源分配到 Real Server 的 SANT pool。在实施这种类型的 SNAT 时，只需创建 SANT pool，而无需创建 SNAT 对象或 iRule。

有关将原始 IP 地址映射到转换地址的详细信息，请参阅第 11-2 页上的 *“将原始 IP 地址映射到转换地址”。*

创建标准SNAT

您可以使用 Configuration 工具创建标准 SNAT。转换地址或映射原始 IP 地址的地址可以是特定 IP 地址、现有 SANT pool 或自身 IP 地址（使用自动映射特性）。

在创建标准 SNAT 时，LTM 系统自动为 SNAT 分配一组属性。同时，您必须在创建 SNAT 时配置 **Name** 和 **Translation** 设置，您可以使用其它设置的缺省值，也可以在以后修改这些值。

创建标准 SNAT 的步骤

1. 在 Main 选项卡上，展开 **Local Traffic**。
2. 点击 **SNATs**。
   此操作将显示现有 SNAT 列表。
3. 在屏幕的右上角，点击 **Create**。
4. 在 **Name** 设置中，输入 SNAT 的唯一名称。
5. 在 **Translation** 设置中，选择 **IP Address**、**SANT Pool** 或 **Automap**。
6. 如果选择 **IP Address** 或 **SANT Pool**，那么输入 IP 地址或选择 SANT pool 名称。
7. 更改或保留所有其它值。
8. 点击 **Finished**。

表 11.2 显示了可以为 SNAT 配置的设置。表格的下面是每种设置的详细说明。

属性	说明	缺省值
Name	指定标准 SNAT 的唯一名称。此属性设置是必需的。	无缺省值

Translation	根据所选的值，指定单独的 IP 地址、SANT pool 名称或自动映射选项。可能的值包括：**IP Address**、**SANT Pool** 或 **Automap**。	**Automap**
Origin	指定您希望映射转换地址、转换 pool 或自身 IP 地址的原始客户机 IP 地址。可能的值包括 **All Address** 或 **Address List**。	**所有地址**
VLAN Traffic	希望应用 SNAT 的 VLAN。可能的值包括：**All VLANs**、**Enabled On** 和 **Disabled On**。	**所有 VLAN**

表 11.2 *标准 SNAT 的属性*

指定 SNAT 名称

您可以为标准 SNAT 配置的最基本设置是 SNAT 名称。SNAT 名称要区分大小写，并且只能包含字母、数字和下划线(_)。不允许使用保留的关键字。

您定义的每个 SNAT 都必须有唯一的名称。

指定转换地址

Translation 设置可指定您希望映射到原始客户机 IP 地址的转换地址。有关转换地址的背景信息，请参阅第 11-2 页上的 *"将原始 IP 地址映射到转换地址"*。

Translation 设置包括 3 个可能的值：

- **IP 地址**
  在创建 SNAT 时，可以指定一个您希望 SNAT 将其用作转换地址的特殊 IP 地址。有关指定特殊转换地址的详细流程，请参阅第 11-14 页上的 *"显式定义转换地址的步骤"*。

- **SANT pool**
  此值使您能够指定映射原始客户 IP 地址的现有 SANT pool。有关 SANT pool 以及如何创建 SANT pool 的信息，请参阅第 11-4 页上的 *"创建 SANT pool"*。有关使用 SANT pool 的标准 SNAT 的示例，请参阅第 11-16 页上的 *"示例 1——建立使用 SANT pool 的标准 SNAT"*。

- **自动映射**
  与 SANT pool 类似，SNAT 自动映射特性使您能够将一个或多个原始客户机 IP 地址映射到转换地址 pool。但是，使用 SNAT 自动映射特性，您无需创建 pool。LTM 系统会利用 LTM 系统的所有自身 IP 地址，作为 pool 的转换地址高效地为您创建 pool。

在指定转换地址或 SANT pool 时，LTM 系统会自动为该转换地址分配一组属性。您可以使用这些属性的缺省值，也可以根据您的需要更改这些值。表 11.3 列出并说明了转换地址的属性。

属性	说明	缺省值
IP address	指定为转换地址的 IP 地址。此设置是必需的。	无缺省值

State	转换地址的状态包括启用和禁用。如果设置为禁用，那么转换地址无法用于启动连接。	**Enabled**
ARP	决定 LTM 系统是否响应 ARP 请求或发送 ARP 欺骗的设置。	**Enabled**
Connection Limit	转换地址不再启动连接前所必须达到的连接数量限制。缺省值 0 表示设置是禁用的。	**0**
TCP Idle Timeout	定义了允许使用 SNAT 地址启动的 TCP 连接秒数的定时器，在连接自动断开之前保持空闲。可能的值为不确定或指定。	**Indefinite**
UDP Idle Timeout	定义了允许使用 SNAT 地址启动 UDP 连接的秒数的定时器，在连接自动断开之前保持空闲。可能的值为不确定或指定。	**Indefinite**
IP Idle Timeout	定义了允许使用 SNAT 地址启动 IP 连接的秒数的定时器，在连接自动断开之前保持空闲。可能的值为不确定或指定。	**Indefinite**

***表 11.3** SNAT 转换地址的属性*

指定原始 IP 地址

Origin 设置可指定希望映射到转换地址的原始客户机 IP 地址。您可以添加一个 IP 地址或多个 IP 地址作为此设置的值。

指定 VLAN 流量

VLAN Traffic 设置可指定您希望应用 SNAT 的 VLAN。可能的值包括：**ALL VLANS**、**Enabled On** 和 **Diabled On**。

创建智能SNAT

进行安全地址转换的一种方法是创建智能 SNAT。如前面所述，***智能 SNAT*** 不是 SNAT 对象，而是将一个或多个原始客户机 IP 地址映射到转换地址的 iRule。要创建智能 SNAT，必须完成以下任务：

- 如果您正在将原始 IP 地址映射到 SANT pool（与单个转换地址相反），那么可以使用 New SANT Pools 屏幕来创建一个或多个将那些转换地址作为成员的 SANT pool。有关详细信息，请参阅第 11-5 页上的 *“创建 SANT pool”*。
- 使用“新建规则”屏幕来创建包括 **snat** 或 **snatpool** 命令的 iRule。这些 iRule 命令可指定转换地址或转换地址 pool，LTM 系统会从该 pool 中选择转换地址。有关 iRules™的详细信息，请参阅第 13 章 *“编写 iRule”*。
- 从 Resources 屏幕选择适当的 Real Server，然后将 iRule 作为一项资源分配到该 Real Server。有关 Real Server 的详细信息，请参阅第 2 章 *“配置 Real Server”*。

◆ **注**

*有关智能 SNAT 的示例，请参阅第 11-17 上的 “**示例 2——建立智能 SNAT**”。*

将SANT pool直接分配到Real Server

除了使用 iRule 创建 SNAT 对象或智能 SNAT，您也可以选择只创建 SANT pool，然后直接将其作为一项资源分配到 Real Server。这样，您

就无需显式定义映射转换地址的原始 IP 地址。

实施NAT

网络转换地址（NAT）可提供别名 IP 地址，当建立或接收外部网络上到客户机的连接时,节点会将此别名 IP 地址用作其源 IP 地址。（这使其与只能启动而不能接收连接的 SNAT 区分开来。）

识别内部网络上节点的 IP 地址无需经外部网络路由。这不仅可以确保节点避免非法连接，而且也可防止节点（和内部网络上的其它主机）接收直接管理连接或启动到外部服务器（如邮件服务器或数据库）的连接。

使用 NAT 可以解决这个问题。NAT 会向特殊节点分配可路由的 IP 地址，在连接到外部服务器时，该节点可以用作其源 IP 地址。您可以使用 NAT IP 地址，通过 LTM 系统直接连接到节点，而不是让 LTM 系统根据指定的负载平衡方法向随机节点发送流量。

◆ **注**

请注意，NAT 不支持端口转换，不适用于在数据包中嵌入 IP 地址的协议如 FTP、NT 域或 CORBA IIOP。

您必须使用 Configuration 工具为每个节点创建单独的 NAT。建 NAT 时，需要配置一组属性。同时，您必须在创建 NAT 时配置 **NAT Address** 和 **Origin Address** 设置，您可以使用其它设置的缺省值，也可以在以后修改这些值。

创建 NAT 的步骤

1. 在 Main 选项卡上，展开 **Local Traffic**。
2. 点击 **SNATs**。
   将打开 SNAT 屏幕。
3. 点击 NAT List 菜单。
4. 在屏幕的右上角，点击 **Create**。
   将打开 New NAT 屏幕。
5. 在 **NAT Address** 框中，输入您希望用作转换地址的 IP 地址。
6. 在 **Origin Address** 框中，输入要转换的原始客户机 IP 地址。
7. 在必要时保留或修改所有其它值。
8. 点击 **Finished**。

表 11.4 列出了您可以为 NAT 配置的设置及每项设置的说明。

NAT 属性	说明	缺省值
NAT Address	在 LTM 系统的外部网络上可路由的 IP 地址。	无缺省值
Origin Address	原始地址是您希望通过 NAT 连接的主机节点 IP 地址。	无缺省值
State	NAT 的状态，即 NAT 启用或禁用。	**Enabled**
ARP	指示 LTM 系统响应来自指定 NAT 地址的 ARP 请求、并发送用于路由器表更新的 ARP 欺骗请求的设置。	**Enabled**
VLAN Traffic	在存在多个内部 VLAN 时,可以显式禁用 NAT 不会映射的 VLAN。	**All VLANS**

***表 11.4** NAT 配置设置*

除了这些选项，您也可以设置转换型 Real Server，有选择性地将流量

转发到特定地址。

其它限制

使用 NAT 时，应该了解以下限制：

- **Origin Address** 框中定义的 IP 地址必须可路由到系统后面的特定服务器。
- 必须在重新定义一个 NAT 前删除原来的 NAT。

管理SNAT和NAT

使用 Configuration 工具，您可以以多种方式管理现有 SNAT。例如，您可能在创建新的 SANT pool 之前查看现有 SANT pool 的列表。或者，您可能希望修改标准 SNAT 将源 IP 地址映射到转换地址的方式。

在管理 SNAT 时，必须执行以下任务：

- 查看或修改 SNAT、SNAT 或 SANT pool。
- 定义或查看转换地址。
- 删除 SNAT 或 NAT、SANT pool 和转换地址。
- 启用或禁用负载平衡 Pool 的 SNAT 或 NAT。
- 启用或禁用 SNAT 或 NAT 转换地址。

查看或修改SNAT、NAT和SANT pool

您可以查看或修改以前创建的任何 SNAT、NAT 或 SNAT。

查看或修改 SNAT 或 NAT 的步骤

1. 在 Main 选项卡上，展开 **Local Traffic**。
2. 点击 **SNATs**。
   此操作将显示现有 SNAT 列表。
3. 选择要查看的项目类型：
   - 如果要查看或修改 SNAT，点击 SNAT 名称。
   - 如果要查看或修改 NAT，找到 NAT List 菜单，然后点击 NAT 地址。
4. 查看或修改显示的设置。
5. 如果修改了任何设置，点击 **Update**。

查看或修改 SANT pool 的步骤

1. 在 Main 选项卡上，展开 **Local Traffic**。
2. 点击 **SNATs**。
   此操作将显示现有 SNAT 列表。
3. 在菜单栏上，点击 SANT Pool List 菜单。
   此操作将显示现有 SNAT 列表。
4. 点击 SANT pool 名称。
5. 查看或修改显示的设置。
6. 如果修改了任何设置，点击 **Update**。

定义并查看转换地址

您可以定义转换地址或查看以前定义的任何现有转换地址。

显式定义转换地址的步骤

1. 在 Main 选项卡上，展开 **Local Traffic**。
2. 点击 **SNATs**。
3. 在菜单栏上，点击 SNAT Translation List 菜单。
   此操作将显示任何现有转换地址。
4. 在屏幕的右上角，点击 **Create**。
5. 保留或更改所有属性设置。
6. 点击 **Finished**。

查看转换地址的步骤

1. 在 Main 选项卡上，展开 **Local Traffic**。
2. 点击 **SNATs**。
   此操作将显示现有 SNAT 列表。
3. 在菜单栏上，点击 SNAT Translation List 菜单。
   此操作将显示现有转换地址列表。
4. 点击一个转换地址。
5. 查看或修改显示的设置。
6. 如果修改了任何设置，点击 **Update**。

删除SNAT、NAT、SANT pool和转换地址

您可以删除以前创建的任何现有 SNAT、NAT、SANT pool 或转换地址。

删除 SNAT 或 NAT 的步骤

1. 在 Main 选项卡上，展开 **Local Traffic**。
2. 点击 **SNATs**。
   此操作将显示现有 SNAT 列表。
3. 选择要删除的项目类型：
   - 如果要删除 SNAT，首先找到要删除的 SNAT，然后选中左边的 Select 框。
   - 如果要删除 NAT，点击 NAT List 菜单，找到要删除的 NAT，然后选中左边的 Select 框。
4. 在屏幕底部，点击 **Delete**。

删除 SANT pool 的步骤

1. 在 Main 选项卡上，展开 **Local Traffic**。
2. 点击 **SNATs**。
   此操作将显示现有 SNAT 列表。
3. 在菜单栏上，点击 SANT Pool List 菜单。
   此操作将显示现有 SANT Pool 列表。
4. 找到要删除的 SANT pool，选中左边的 Select 框。
5. 在屏幕底部，点击 **Delete**。

删除转换地址的步骤

1. 在 Main 选项卡上，展开 **Local Traffic**。
2. 点击 **SNATs**。
   此操作将显示现有 SNAT 列表。
3. 在菜单栏上，点击 SNAT Translation List 菜单。
   此操作将显示现有转换地址列表。
4. 找到要删除的转换地址，选中左边的 Select 框。
5. 在屏幕底部，点击 **Delete**。

启用或禁用负载平衡Pool的SNAT或NAT

配置负载平衡 Pool 时，可以明确禁止在使用该 pool 的任何连接上进行 SNAT 或 NAT 转换。在缺省模式下，可以启用此设置。有关详细信息，请参阅第 4 章*“配置负载平衡 Pool”*。

启用或禁用SNAT转换地址

使用 Configuration 工具，可以启用或禁用单独的 SNAT 转换地址。

启用或禁用 SNAT 转换地址的步骤

1. 在 Main 选项卡上，展开 **Local Traffic**。
2. 点击 **SNATs**。
3. 在菜单栏上，点击 SNAT Translation List 菜单。
4. 找到要启用或禁用的转换地址，选中左边的 Select 框。
5. 在屏幕底部，点击 **Enable** 或 **Disable**。

SNAT示例

下面的示例展示了实施使用 SANT pool 的 SNAT 的方法。这些示例说明了您如何：

- 建立使用 SANT pool 的标准 SNAT。
- 建立智能 SNAT。

◆ **注**

为了更好地说明使用 SANT pool 的 SNAT，下面的示例展示了 LTM 系统的 ***bigip.conf*** *文件中的示例条目。****bigip.conf*** *文件中的条目代表了使用 Configuration 工具配置 LTM 系统的结果。*

示例1——建立使用SANT pool的标准SNAT

在某些情况下，您可能需要创建将原始 IP 地址映射到 SANT pool 而非单独的转换地址的 SNAT。为了阐明这种类型的 SNAT，假设 ISP 为两个客户分别提供了可路由的 IP 地址，用于链接到互联网。客户需要将这些可路由的 IP 地址用作虚拟 IP 地址和转换地址，以便流量流入自己的服务器和从自己的服务器流出。

在这种情况下，SNAT 提供了解决方案。为了实施 SNAT，ISP 采取了以下三个步骤。

首先，ISP 创建图 11.1 所示的负载平衡 Pool **isp_pool**。

```
pool isp_pool {
lb_method rr
member 199.5.6.254:0
member 207.8.9.254:0
}
```

图 11.1 *基本负载平衡 Pool 的 bigip.conf 条目*

接下来，ISP 创建 3 个 SANT pool：**customer1_snatpool**、**customer2_snatpool** 和 **other_snatpool**。如图 11.2 所示。请注意，LTM 系统自动指定 SANT Pool 成员作为转换地址。

```
snatpool customer1_snatpool {
member 199.5.6.10
member 207.8.9.10
}
snatpool customer2_snatpool {
member 199.5.6.20
member 207.8.9.20
}
snatpool other_snatpool {
member 199.5.6.30
member 207.8.9.30
}
```

***图 11.2** 3 个 SANT pool 的 bigip.conf 条目*

最后，ISP 使用 Configuration 工具创建可将每个原始 IP 地址直接映射到适当 SANT pool 的 SNAT。图 11.3 所示为在 **bigip.conf** 文件中显示的映射。

```
snat map {
192.1.1.10 192.1.1.11 to snatpool customer1_snatpool
}

snat map {
192.1.1.20 192.1.1.21 to snatpool customer2_snatpool
}

snat map default to snatpool other_snatpool
```

图 11.3 将原始地址映射到 SANT pool 的 bigip.conf 条目

示例2——建立智能SNAT

如果要使 SNAT 映射基于除原始客户机 IP 地址之外的标准（如服务器端口），那么可以编写 iRule 并在 iRule 中指定 SANT pool。在这种情况下，可以使用 Configuration 工具中的 SNAT 屏幕只创建 SANT pool，而不创建实际的 SNAT 对象。

例如，假设用户（如 ISP）有两个冗余互联网连接。此外，ISP 需要处理许多同时进行的 CHAT 连接（使用端口 **531**），并且希望避免消耗服务器端客户机端口资源。最后，ISP 希望分别收集 CHAT、SMTP 和所有其它流量的统计数据。在这种情况下，配置智能 SNAT 是选择转换地址的最佳方法。

为了实施 SNAT，ISP 采取了以下步骤。

首先，ISP 创建称为 **out_pool** 的负载平衡 Pool。**在 bigip.conf** 文件中，pool 与图 11.4 中的示例类似。

```
pool out_pool {
lb_method round_robin
member 199.5.6.254:0
member 207.8.9.254:0
}
```

***图 11.4** 用于智能 SNAT 的 pool 的 bigip.conf 条目*

接下来，如图 11.5 所示，ISP 使用 Configuration 工具来创建称为 **chat_snatpool** 的 SANT pool，该 pool 包含 4 个 IP 地址：**199.5.6.10**、**199.5.6.11**、**207.8.9.10** 和 **207.8.9.11**。LTM 系统会在创建 SANT pool 的过程中自动将这些 IP 地址指定为转换地址。这些地址对应两个用于 CHAT 流量的下一跳网络。**在 bigip.conf** 文件中，SANT pool 与图 11.5 中的示例类似。

```
snatpool chat_snatpool {
member 199.5.6.10
member 199.5.6.11
member 207.8.9.10
member 207.8.9.11
}
```

图 11.5 CHAT 流量的 SANT pool 定义

接下来，对于每个转换地址，ISP 使用 Configuration 工具将 TCP 连接的超时值改为 **600**。

然后，ISP 创建第二个 SANT pool**smtp_snatpool**，该 pool 包括两个转换地址：**199.5.6.20** 和 **207.8.9.20**。每个地址分别对应两个用于 SMTP 流量的下一跳网络中的一个。在 **bigip.conf** 文件中，SANT pool 与图 11.6 中的示例类似。

```
snatpool smtp_snatpool {
member 199.5.6.20
member 207.8.9.20
}
```

图 11.6 SMTP 流量的 SANT pool 定义

接下来，ISP 创建面向所有其它流量（即非 CHAT 和非 SMTP 流量）的 SANT pool**other_snatpool**，在该 pool 中，每个 IP 地址分别对应所有其它流量将使用的两个下一跳网络中的一个。如图 11.7 所示。

```
snatpool other_snatpool { \SNAT pool definition
member 199.5.6.30
member 207.8.9.30
}
```

图 11.7 所有其它流量的 SANT pool 定义

然后，ISP 编写 iRule，根据初始数据包的服务器端口选择 SANT pool 和负载平衡 Pool **out_pool**。第 11-19 页的图 11.9 显示了 iRule 如何指定命令 **TCP::local_port** 来说明可用作选择转换地址基础的数据包数据的类型。iRule 还显示了命令 **snatpool**（图 11.8 所示）来指定 SANT pool，LTM 系统将从该 pool 选择转换地址。

```
rule my_iRule {
when SERVER_CONNECTED
if { TCP::local_port equals 531 } {
use snatpool chat_snatpool
}
else if { TCP::local_port equals 25 } {
use snatpool smtp_snatpool
}
else {
use snatpool other_snatpool
}
use pool out_pool
}
```

图 11.8 参考智能 SNAT 的 iRule 示例

iRule 中的 if 语句指示 LTM 系统测试在客户机请求的标头中指定的服务器端口值。LTM 系统根据结果选择 SANT pool 和负载平衡 Pool。

最后，ISP 将 iRule 作为一项资源分配到通配符 Real Server，如图 11.9 所示。

```
virtual 0.0.0.0:0 use rule my_iRule
```

图 11.9 将 iRule 分配到通配符 Real Server

12

配置速率调整

- 速率调整简介
- 创建并实施速率等级
- 配置速率等级设置
- 管理速率等级

速率调整简介

BIG-IP®本地流量管理（LTM）系统具有称为速率调整的特性。***速率调整***使您能够对入站流量执行吞吐率政策。吞吐率政策有助于优化和限制选定流量模式的带宽。

速率调整对于拥有首选客户机的电子商务站点很有帮助。例如，该站点可以对首选客户提供较高的吞吐率，而对其它站点流量提供较低的吞吐率。

速率调整特性发挥作用的途径是：首先按照速率等级对选定的数据包进行排队，然后以显示的速率和按速率等级指定的显示顺序对数据包执行出队操作。***速率等级***是一种定义吞吐率限制的速率调整政策，也是一种应用于由速率等级处理的所有流量的数据包调度方法。

通过创建一个或多个速率等级然后将其分配到数据包过滤器或 Real Server，可以对速率调整进行配置。也可以使用 iRules™特性来指导 LTM 系统将速率等级应用到特殊连接。

此外，可以明确将速率等级应用到从服务器到客户机或从客户机到服务器的流量。如果为流入客户机的流量配置速率等级，那么 LTM 系统不会将吞吐率政策应用到流向服务器的流量。相反，如果为流入服务器的流量配置速率等级，那么 LTM 系统不会将吞吐率政策应用到流向客户机的流量。

要配置速率调整，可以使用 Configuration 工具的 **Local Traffic** 部分中 Rate Shaping 屏幕。

创建并实施速率等级

速率等级定义吞吐率限制和数据包调度方法，LTM 系统可将其应用到速率等级处理的所有流量。将速率等级分配到 Real Server 和数据包过滤器规则以及 iRule。

如果相同的流量属于从多个位置分配的速率等级，那么 LTM 系统只使用最新分配的速率等级。LTM 系统按照以下顺序应用速率等级：

- LTM 系统分配的第一个速率等级来自与流量匹配并指定速率等级的最新数据包过滤器规则。
- LTM 系统分配的下一个速率等级来自 Real Server。如果 Real Server 指定了一个速率等级，那么该速率等级会覆盖数据包过滤器选择的所有速率等级。
- 分配的最新速率等级来自 iRule。如果 iRule 指定了一个速率等级，那么该速率等级会覆盖所有以前选择的速率等级。

创建速率等级的步骤

1. 在 Main 选项卡上，展开 **Local Traffic**。
2. 点击 **Rate Shaping**。
   此操作将显示现有速率等级列表。
3. 在屏幕的右上角，点击 **Create**。
   此操作将显示 New Rate Class 屏幕。

4. 指定是否希望使速率等级能够从上一速率等级借用带宽：
   - 如果不希望速率等级从上一级借用带宽，那么选择 **Basic**。有关详细信息，请参阅第 12-7 页上的*“借用带宽”*。
   - 如果希望使速率等级能够从上一速率等级借用带宽，那么选择 **Advanced**。有关详细信息，请参阅第 12-7 页上的*“指定上一速率等级”*。
5. 按需配置所有设置。
   有关设置的详细信息，请参阅第 12-3 页上的*“配置速率等级设置”*或查看在线帮助。
6. 点击 **Finished**。

创建速率等级后，必须将其分配到 Real Server 或数据包过滤器规则，或者必须在 iRule 中指定速率等级。

- 有关 Real Server 的详细信息，请参阅第 2 章*“配置 Real Server”*。
- 有关数据包过滤器规则的详细信息，请访问 Configuration 工具中的“数据包过滤器”屏幕并显示在线帮助。
- 有关 iRule 的详细信息，请参阅第 13 章*“编写 iRule”*。

配置速率等级设置

创建速率等级时，LTM 系统将一些缺省设置分配到速率等级。您可以保留这些缺省设置，也可以根据需要对它们进行修改。表 12.1 描述了可以对速率等级进行配置的设置。

设置	说明	缺省值
Name	为速率等级指定一个唯一的名称。每一个速率等级都需要一个名称。	无缺省值
Base Rate	指定速率等级处理的流量所允许的基础吞吐率。通常不允许数据包超过指定的速率。此设置是必需的。	无缺省值
Ceiling Rate	与基础速率相似，但指定了一个严格且绝对的限制。这一数字指定了对速率的绝对限制，在猝发或借用时允许流量以该速率流动。有关带宽猝发和借用的信息，请参阅第 12-4 页上的*“指定猝发长度”*。	与基础速率相同
Burst Size	指定在需要借用带宽前，允许流量超过基础速率猝发的最大字节数。该值设置为 0 时，不允许猝发。有关带宽猝发和借用的信息，请参阅第 12-4 页上的*“指定猝发长度”*。	**0**
Direction	指定应用速率等级的流量的方向。可能的值包括 **Any**、**Clent** 和 **Server**。	**Any**
Parent Class	指定下一速率等级可以从中借用带宽的速率等级。下一速率等级可以从上一速率等级中借用未使用的带宽，从而补充下一速率等级的猝发长度。此设置是 **Advanced**。有关带宽猝发和借用的信息，请参阅第 12-4 页上的*“指定猝发长度”*。	**无**
Queue Discipline	指定速率等级用来对流量进行排队和执行出队操作的方法。允许的设置包括 **Stochastic Fair Queue** 和 **Priority FIFO**。	如果指定了上一速率等级，那么就与上一速率等级相同；否则，是 **Stochastic Fair Queue**。

表 12.1 *用于配置速率等级的设置*

配置速率等级的设置前，对这些设置进行描述是很有帮助的。

指定名称

为速率等级配置的第一个设置是速率等级名称。速率等级名称要区分大小写，并且只能包含字母、数字和下划线(_)。不允许使用保留的关键字。

定义的每个速率等级都必须有唯一的名称。此设置是必需的。

要指定速率等级的名称，在 New Rate Class 屏幕上找到 **Name** 框，然后为速率等级输入唯一的名称。

指定基础速率

Base Rate 设置指定速率等级处理的流量所允许的基础吞吐率。通常不允许数据包超过指定的速率。您可以以比特/秒（bps）、千比特/秒（Kbps）、兆比特/秒（Mbps）或吉比特/秒（Gbps）为单位指定基础速率。缺省单位是比特/秒。此设置是必需的。

可以配置的最小基础速率是 296bps。

◆ 注

这些数字是以比特数的 10 次幂而非 2 次幂增长。

指定最高速率

Ceiling Rate 设置指定了对速率的绝对限制，在猝发或借用时允许流量以该速率流动。您可以以比特/秒（bps）、千比特/秒（Kbps）、兆比特/秒（Mbps）或吉比特/秒（Gbps）为单位指定最高速率。缺省单位是比特/秒。

如果指定了最高速率，那么该速率必须等于或大于基础速率。如果忽略了最高速率或将最高速率设置为等于基础速率，那么流量吞吐率就永远不能超过基础速率。

指定猝发长度

要使速率等级控制的流量速率超过基础速率，可以使用 **Burst Size** 设置。超过基础速率称为*猝发*。配置允许猝发的速率等级（通过指定一个除 0 以外的值）时，LTM 系统保存未使用的带宽，稍后使用这个带宽让流量的速率暂时超过基础速率。指定猝发长度有助于消除可能导致波动或超过基础速率的流量模式，如 HTTP 流量。

Burst Size 设置的值定义允许猝发的最大字节数。因此，如果将猝发长度设置为 5,000 个字节，并且流量速率每秒超过基础速率 1,000 个字节，那么 LTM 系统允许流量的猝发时间最多为 5 秒。

指定猝发长度时，LTM 系统创建这种长度的猝发流量 pool。*猝发库*保存 LTM 用于以后猝发的带宽。当流量速率超过基础速率时，就会耗尽该猝发流量 pool；当流量速率低于基础速率时，就要对该猝发流量 pool 进行补充。因此，按速率等级配置的 **Burst Size** 值表示：

- 当流量速率超过基础速率时，允许速率等级传输的最大字节数。
- LTM 可以向猝发流量 pool 补充的最大字节数。

- 最初可用于超过基础速率猝发的带宽总数。

以字节测量猝发长度。例如，**10000** 或 **10K** 的值等于 10,000 个字节。缺省值为 0。

耗尽猝发流量 pool

当流量速率超过基础速率时，LTM 系统会以每秒流量超过基础速率的字节数确定的速率，自动耗尽猝发流量 pool。

继续来看前面流量每秒超过基础速率 1,000 个字节的例子，如果流量速率仅超过基础速率两秒，那么会从猝发长度中消耗 2,000 个字节，而且可用于猝发的最大字节数减少到 3,000。

补充猝发流量 pool

当流量速率低于基础速率时，LTM 系统将存储猝发流量 pool 中未使用的带宽（也就是基础速率和实际流量速率间的差异）。随后，当流量超过基础速率时，LTM 系统使用该带宽。因此，无论何时由于流量超过基础速率而耗尽猝发流量 pool，LTM 系统都会进行补充。

猝发流量 pool 的长度不能超过指定的猝发长度。因此，LTM 系统仅用未使用的带宽来补充流量 pool，直到流量 pool 达到 **Burst Size** 设置指定的数量。当流量速率超过基础速率时，如果猝发长度设置为 **5,000**，那么 LTM 系统仅可以存储未使用带宽的 5,000 个字节供以后使用。

♦ 注

指定猝发长度不允许速率等级超过最高速率。

指定非零的猝发长度

以下示例说明将 **Burst Size** 设置设为除 0 之外的任意值（不包括 0）时，LTM 系统的行为。

该示例表明以字节/秒而不是缺省的比特/秒为单位的吞吐率。这只会使示例变得简单。通过将比特/秒的总数除以 8，可以从位/秒换算到字节/秒。

假设用这些值来配置速率等级设置：

- 基础速率：1,000 字节/秒
- 最高速率：4,000 字节/秒
- 猝发长度：5,000 个字节

考虑一下以下情况：

- **如果当前的流量速度是每秒 800 个字节**

  不需要猝发，因为流量的速率低于在速率等级中定义的基础速率。

  由于每秒 200 个字节的流量速率低于基础速率，因此 LTM 系统可以将未使用带宽的 200 个字节添加到猝发流量 pool 中。但是，由于还未发生猝发，流量 pool 的流量在达到指定的 5,000 个字节时

就已经满了，因此要防止 LTM 系统存储流量 pool 中 200 个字节的未使用带宽。在这种情况下，LTM 系统只需放弃未使用的带宽。

- **如果流量上升到每秒 1,000 个字节（等于基础速率）**

  仍不发生猝发，并且没有未使用的带宽。

- **如果流量突升至每秒 2,500 个字节**

  为了使流量保持每秒 2,500 个字节，LTM 系统需要从猝发流量 pool 清空 1,500 个字节（流量速率和基础速率间的差异）。在耗尽 5,000 个字节的猝发流量 pool 之前，仅允许三秒以上的猝发。一旦耗尽该流量 pool，LTM 系统就会将流量速率降低到每秒 1,000 个字节的基础速率，而且不允许猝发。

- **如果流量降回至每秒 800 个字节**

  不需要猝发，但是现在 LTM 系统可以将未使用带宽的每秒 200 个字节添加回猝发流量 pool，因为该流量 pool 是空的。如果流量继续以每秒 800 个字节的速度流动，那么猝发流量 pool 在 25 秒内将得到全面补充，从 0 变为 5,000 个字节（以每秒 200 个字节的速率）。如果流量完全停止流动，停止创建每秒 1,000 个字节的未使用带宽，那么 LTM 系统会将每秒 1,000 个字节添加到猝发流量 pool，从而仅用 5 秒钟就将流量 pool 从 0 补充到 5,000 个字节。

借用带宽

某些情况下，速率等级可以从上一速率等级的猝发流量 pool 借用带宽。有关详细信息，请参阅下面的*“指定上一速率等级”*。

指定方向

使用 **Direction** 设置，可以将速率等级应用到客户机或服务器流量。因此，可以将速率等级应用到流入客户机、服务器或既流入客户机又流入服务器的流量。可能的值包括 **Any**、**Client** 和 **Server**。缺省值为 **Any**。

在流量具有方向偏离特性的情况下，指定方向是很有用的。例如，如果向外部客户机提供 FTP 服务，那么与从站点下载文件的客户机的吞吐率相比，您可能更关注限制将文件上传到站点的客户机的吞吐率。在这种情况下，可以选择 **Server** 作为 FTP 速率等级的方向，因为 **Server** 值仅将吞吐率限制应用到从客户机到服务器的流量。

指定上一速率等级

创建速率等级时，可以使用 **Parent Class** 设置来指定包含上一速率等级的速率等级。这使速率等级能够从上一速率等级借用未使用的带宽。下一速率等级可以从其上一速率等级借用未使用的带宽，但上一速率等级不能从下一速率等级借用。相同上一速率等级的两个下一速率等级之间或两个无关的速率等级之间不能彼此借用。

通过显示 New Rate Class 屏幕并选择 **Advanced**，然后在 **Parent Class** 设置中选择速率等级名称来指定上一速率等级。

如果不建立循环依赖关系，那么上一速率等级本身也可以有上一速率等级。***循环依赖***是一种速率等级本身直接或间接是下一速率等级的关系。

如果速率等级具有上一速率等级，那么下一速率等级可以从上一速率等级那里获取未使用的带宽。过程如下：

- 如果下一速率等级的流量速率超过基础速率，那么下一速率等级就会按前面所述开始消耗其猝发流量 pool。
- 如果流量 pool 是空的（或未定速率等级的猝发长度），那么 LTM 系统从上一速率等级那里获取未使用的基础速率带宽，并将其提供给下一速率等级。
- 如果耗尽了上一速率等级未使用的带宽，那么下一速率等级开始使用上一速率等级的流量 pool。
- 如果上一速率等级的流量 pool 是空的（或未定义上一速率等级的猝发长度），而且如果上一速率等级本身也具有上一速率等级，那么下一速率等级会尝试从上一速率等级那里借用带宽。
- 继续该过程，直到没有可借用的带宽或没有可借用的上一速率等级为止。

借用仅允许下一速率等级延长其猝发持续时间，在任何情况下下一速率等级都不能超过最高速率。

◆ 注

尽管以上描述使用了术语“借用”，但下一速率等级借用的带宽此后并未偿还给上一速率等级，而且下一速率等级未使用的带宽也未返还给上一速率等级。

指定队列规则

Queue Displine 设置确定了 LTM 系统对数据包排队和执行出队操作的方法和顺序。

速率等级支持两种队列规则：

- **随机平等队列**
  随机平等队列（SFQ）是一种通过一系列列表对流量进行排队的排队方法，它根据定期变化的连接信息来选择特定的列表。这导致了来自相同连接的流量总是在同一个列表中排队。然后，SFQ 以伦循方式将流量从一系列列表中除去。这样做的整体效果是可实现出队的公平性，因为一个高速连接不能在损害速度较慢连接的情况下独占队列空间。
- **优先级 FIFO**
  优先级 FIFO（PFIFO）排队方法基于流量的“服务类型”（ToS）字段对五个列表下的所有流量进行排队。其中四个列表对应四个可能的 ToS 值（**Minimum Delay**、**Maximum Throughput**、**Maximum Reliability** 和 **Minimum cost**）。第五个列表表示无 ToS 值的流量。然后，PFIFO 方法对这五个列表进行处理，并且尽可能保留 ToS 字段的含义。例如，ToS 字段设置为 **Minimum Cost** 的数据包会让 ToS 字段设置为 **Minimum Delay** 的数据包出队。

管理速率等级

创建速率等级后，可以使用 Configuration 工具列出现有的速率等级，查

看或修改速率等级的设置，或删除速率等级。

列出现有速率等级的步骤

1. 在 Main 选项卡上，展开 **Local Traffic**。
2. 点击 **Rate Shaping**。
   此操作将显示现有速率等级及其设置值列表。
3. 查看速率等级列表。

查看或修改速率等级的步骤

1. 在 Main 选项卡上，展开 **Local Traffic**。
2. 点击 **Rate Shaping**。
   此操作将显示现有速率等级列表。
3. 点击列表中的速率等级名称。
   此操作将显示该速率等级的设置。
4. 保留或修改任何设置值。有关速率等级设置的信息，请参阅第 12-3 页上的*“配置速率等级设置”*。
5. 点击 **Update**。

删除速率等级的步骤

1. 在 Main 选项卡上，展开 **Local Traffic**。
2. 点击 **Rate Shaping**。
   此操作将显示现有速率等级列表。
3. 在列表中找到速率等级名称，并在名称的左边，选中 Select 框。
4. 在屏幕底部，点击 **Delete**。
   此操作将显示确认删除的屏幕。
5. 点击 **Delete**。
   此操作将删除速率等级。

13

编写 iRule

- iRule 简介
- 创建 iRule
- 控制对 iRule 的选择运用
- 指定工具命令
- 指定流量目的地和地址转换
- 查询标头或内容数据
- 处理标头或内容数据
- 使用 UIE 函数命令
- 使用 Profile
- 通过 iRule 启用会话持续性
- 创建、管理和使用数据组
- 覆盖 Profile 设置

iRule简介

iRule 是 BIG-IP®本地流量管理（LTM）系统中提供的一个功能强大的灵活特性，可以用于管理网络流量。使用 iRules™特性，不仅可以基于标头数据来选择 pool，而且可以通过搜索您定义的任何内容数据类型来对引导流量。因此，iRule 特性可以显著增强对内容交换的定制能力，以准确满足您的需求。

什么是iRule？

iRule 是一种脚本。如果希望各个连接不要指向为 Real Server 定义的缺省 pool，而是指向其它 pool，就可以编写 iRule。iRule 允许您更直接地指定希望将流量引导至哪些 pool。使用 iRule 不仅可以将流量发送至 pool，而且可以发送至各个 Pool 成员、端口或 URI。

根据您对内容交换的需要，可以创建简单 iRule，也可以创建复杂 iRule。图 13.1 显示了一个简单 iRule 的示例。

```
iRule my_iRule
  when CLIENTSSL_HANDSHAKE
  if { [IP::local_addr] eq 10.10.10.10 } {
        pool my_pool
     }
  }
```

图 13.1 *iRule 示例*

此 iRule 在完成客户机端 SSL 握手时触发，使 LTM 系统将数据包发送至 pool**my_pool**。

使用称为***通用检查引擎（UIE）***的特性，可以编写搜索数据包标头或数据包实际内容的 iRule，然后基于该搜索结果来引导数据包。iRule 还可以基于尝试进行客户机认证的结果来引导数据包。

iRule 不仅可以将流量引导至特定的 pool，还可以引导至各个 Pool 成员（包括端口号和 URI 路径），以实施持续性或满足特定的负载平衡要求。

用来编写 iRule 的语法基于工具命令语言（Tcl）编程标准。因此，您可以使用众多标准 Tcl 命令，外加 LTM 系统提供的一组健壮的扩展命令来帮助进一步提高负载平衡的效率。

有关标准 Tcl 语法的信息，请参阅以下网址：**http://tmml.sourceforge.net/doc/tcl/index.html**。有关已在 LTM 系统中禁用，因此编写 iRule 时无法使用的 Tcl 命令列表，请参阅附录 B *“禁用的 Tcl 命令”*。

iRule基本元素

iRule 由以下这些基本元素组成：

- 事件声明
- 运算符
- iRule 命令

事件声明

iRule 是事件驱动的，这表示 LTM 系统基于您在 iRule 中指定的事件来触发 iRule。***事件声明***是 iRule 中的事件规范，它使 LTM 系统在该事件发生时触发该 iRule。以下是可以触发 iRule 的事件声明示例：系统从 HTTP 请求中接收内容数据时触发 iRule 的 **HTTP_REQUEST_DATA**，以及客户机已建立连接时触发 iRule 的 **CLIENT_ACCCEPTED**。

有关 iRule 事件的详细信息，请参阅第 13-5 页上的*“指定事件”*。

运算符

iRule 运算符用于比较表达式中的两个运算对象。例如，您可以使用 **equals** 运算符将可变运算对象与常量进行比较。您可以创建表示以下含义的 **if** 语句：“如果远程客户机的地址是 **10.10.10.10**，便发送至 **my_pool**。”

表 13.1 列出了可以在 iRule 中使用的有效运算符。

运算符	语法
关系运算符	contains matches equals starts_with ends_with matches_regex
逻辑运算符	not and or

***表 13.1** iRule 运算符*

iRule 命令

iRule *命令*是 iRule 中的命令规范，它使 LTM 系统执行某些操作。可以包括在 iRule 中的命令类型有：

- **查询命令**
  这些命令用于搜索标头和内容数据。**IP::remote_addr** 便是查询命令的一个示例，它搜索并返回连接的远程 IP 地址。有关查询命令的详细信息，请参阅第 13-16 页上的*“查询标头或内容数据”*。

- **操作/修改命令**
  这些命令执行各种操作，例如将标头插入 HTTP 请求中。**HTTP::header remove<name>**便是操作命令的一个示例，它从请求或响应中删除最后一个命名标头实例。有关操作/修改命令的详细信息，请参阅第 13-24 页上的*“处理标头或内容数据”*。

- **语句命令**
  这些命令用于指定流量的目的地，例如 pool 或 URL（用于重写 HTTP 重定向）。**pool <name>**便是语句命令的一个示例，它将流量引导至命名负载平衡 Pool。有关详细信息，请参阅第 13-12 页上的*“指定流量目的地和地址转换”*与第 13-31 页上的*“使用 UIE 函数命令”*。

- **UIE 命令**
  这些命令用于执行深层数据包检查功能，以便直接选择 pool 中的 Pool 成员，或者根据对命令中指定的任何数据的搜索结果来选择 pool。**decode_uri <string>**便是 UIE 命令的一个示例，它对使用

HTTP URI 编码的命名字符串进行解码，然后返回结果。有关使用 UIE 函数命令的详细信息，请参阅第 13-31 页上的“使用 UIE 函数命令”。

创建iRule

您可以使用 Configuration 工具来创建 iRule。

创建 iRule 的步骤

1. 在 Main 选项卡上，展开 **Local Traffic**。
2. 点击 **iRules**。
   将显示 iRules 屏幕。
3. 在屏幕的右上角，点击 **Create**。
4. 在 **Name** 框中，键入名称（1 到 31 个字符）。
5. 在 **Definition** 框中，键入 iRule 的语法。
6. 点击 **Finished**。

有关编写 iRule 的详细语法信息，请参阅本章剩余部分。

♦ **重要信息**

*创建 iRule 之后，需要配置 Real Server 来参考 iRule。有关配置 Real Server 来参考 iRule 的信息，请参阅第 2 章“**配置 Real Server**”。*

控制对iRule的选择运用

在没有 iRule 的基本系统配置中，LTM 系统将入站流量引导至为接收该流量的 Real Server 分配的缺省 pool。但您可能希望 LTM 系统将特定类型的连接引导至其它目的地。实现这一点的方式是编写随着特定事件类型的发生，将流量引导至其它目的地的 iRule。如果未发生该类事件，流量将继续流入分配给 Real Server 的缺省 pool。

只要发生您在 iRule 中指定的事件，便会选择运用规则。例如，如果 iRule 包括事件声明 CLIENT_ACCEPTED，那么只要 LTM 系统接受客户机请求，便触发 iRule。然后，LTM 系统将按照 iRule 中剩余部分指示的方向，确定数据包的目的地。

配置前提条件

LTM 系统能够选择运用所编写的 iRule 前，必须执行以下操作：

- **将 iRule 分配给 Real Server。**
  将 iRule 分配给 Real Server 时，表示该 Real Server *参考*该 iRule，这类似于 Real Server 参考 pool 或 Profile。

- 确保 **Real Server 参考正确的 Profile**。
  例如，如果 iRule 包括事件声明 **HTTP_REQUEST**，那么仅当 Real Server 参考 **HTTP Profile** 类型时，LTM 系统才选择运用 iRule。

有关将 iRule 和 Profile 分配给 Real Server 的信息，请参阅第 2 章*“配置 Real Server”*。

指定事件

iRule 特性包括数类可在 iRule 中指定的事件声明。指定事件声明用于确定 LTM 系统选择运用 iRule 的时机。以下小节列出并介绍了这些事件类型，同时还介绍了 iRule 的环境概念和关键字 **when** 的用法。

事件类型

iRule 命令语法包括以下数类可在 iRule 中指定的事件声明：

- 全局事件
- HTTP 事件
- SSL 事件
- 认证事件

表 13.2 列出并介绍了可在 iRule 中声明的每种事件类型的事件。

iRule 事件	**说明**
全局事件	
CLIENT_ACCEPTED	客户机建立连接时触发。
CLIENT_DATA	连接处于 **Collect** 状态时，如果客户机收到新数据，便触发此事件。
SERVER_SELECTED	LTM 系统选定目标节点时触发。
SERVER_CONNECTED	系统与目标节点建立连接时触发。
SERVER_DATA	连接处于 **Hold** 状态时，如果客户机接收到来自目标节点的新数据，便触发此事件。
RULE_INIT	添加或修改 iRule 时触发。此事件用于初始化 iRule 中使用的全局变量。
HTTP 事件	
HTTP_REQUEST	系统完全解析整个客户机请求标头时触发。此处所说标头是指方法、URI、版本和所有标头，不包括请求正文。
HTTP_REQUEST_DATA	请求接收到新的 HTTP 内容数据时触发。
HTTP_RESPONSE	系统解析服务器响应中的所有响应状态和标头行时触发。
HTTP_RESPONSE_DATA	系统从响应中接收到新的 HTTP 内容数据时触发。
HTTP_RESPONSE_CONTINUE	系统从服务器接收到 **100 Continue** 响应时触发。
SSL 事件	
CLIENTSSL_HANDSHAKE	完成客户机端 SSL 握手时触发。
CLIENTSSL_CLIENTCERT	系统将 SSL 客户机证书添加到客户机证书链时触发。LTM 系统可以使用 **SSL::cert** 和 **SSL::cert issuer** 命令来检索 X509 证书及其 X509 签发者。
SERVERSSL_HANDSHAKE	完成服务器端 SSL 握手时触发。
认证事件	

iRule 事件	说明
AUTH_FAILURE	未成功的授权操作结束时触发。此事件的缺省处理程序与每个认证 Profile 都相关联，可使系统关闭连接。
AUTH_ERROR	授权过程出错时触发。此事件的缺省处理程序与每个认证 Profile 都相关联，可使系统关闭连接。收到此事件表示相关认证会话 ID 失效，用户应立即丢弃该会话 ID。
AUTH_WANTCREDENTIAL	授权操作需要其它证书时触发。另请参阅第 13-23 页上 *"查询认证数据"*一节中对 **AUTH::wantcredential_prompt** 命令的描述。此事件的缺省处理程序与每个认证 Profile 都相关联，可使系统关闭连接，除非能够获得所需证书。通常，这意味着因为系统未启用所需的认证协议，所以提供证书的协议层也尚未获得证书。每个认证 Profile 都包含用于其各自协议的适当缺省处理程序。
AUTH_SUCCESS	授权成功完成全部所需的认证服务时触发。

***表 13.2** iRule 的事件声明*

iRule 的环境

对于在 iRule 中指定的每个事件，您还可以指定环境，由关键字 **clientside** 或 **serverside** 指明。因为每个事件都带有与其关联的缺省环境，所以仅当希望更改缺省环境时，才需要声明环境。

例如，图 13.2 显示了 **my_iRule1**，其中包括事件声明 **CLIENT_ACCEPTED**，以及 iRule 命令 **IP::remote_addr**。在此情形中，iRule 命令返回的 IP 地址是客户机的 IP 地址，因为事件声明 **CLIENT_ACCEPTED** 的缺省环境是 **clientside**。

```
iRule my_iRule1 {
   when CLIENT_ACCEPTED
   if { [IP::remote_addr] eq 10.1.1.80 } {
       pool my_pool1
 }
```

***图 13.2** 使用缺省 **clientside** 环境的 iRule*

与之类似，图 13.3 显示了 **my_iRule2**，其中包括事件声明 **SERVER_CONNECTED**，以及 iRule 命令 **IP::remote_addr**。在此情形中，iRule 命令返回的 IP 地址是服务器的 IP 地址，因为事件声明 **SERVER CONNECTED** 的缺省环境是 **serverside**。

```
iRule my_iRule2 {
   when SERVER_CONNECTED
   if { [IP::remote_addr] eq 10.1.1.80 } {
       pool my_pool2
 }
```

***图 13.3** 使用缺省 **serverside** 环境的 iRule*

以上两个示例显示了如果所编写的 iRule 使用缺省环境来处理 iRule 命令，将产生的结果。但您可以明确指定关键字 **clientside** 和 **serverside**，以改变 iRule 命令的行为。

继续上一个示例，图 13.4 显示了 **my_iRule3**，其中包括事件声明 **SERVER_ACCEPTED**，并为 iRule 命令 **IP::remote_addr** 明确指定关

键字 **clientside**。

在此情形中，iRule 命令返回的 IP 地址是客户机的 IP 地址，尽管事件声明的缺省环境是服务器端。

```
iRule my_iRule3 {
   when SERVER_CONNECTED
   if { clientside [IP::remote_addr] eq 10.1.1.80 } {
       pool my_pool2
 }
```

图 13.4 *明确指定 iRule 环境的 iRule*

使用关键字“when”

在 iRule 中，使用后接事件名称的关键字 **when** 来进行事件声明。上图显示了 iRule 中的一个事件声明示例。

Real Server 上列出的 iRule

为 Real Server 分配多个 iRule 作为资源时，有必要考虑它们在 Real Server 上列出的顺序。这是因为 LTM 系统按照可用 iRule 列出的顺序来处理重复的 iRule 事件。因此，iRule 事件可以终止事件的触发，从而阻止 LTM 系统触发后续事件。

◆ **注意**

如果 iRule 参考 Profile，那么 LTM 系统将最后处理此类 iRule，而不考虑它在分配给 Real Server 的 iRules 列表中的顺序如何。

指定语句命令

有些可在 iRule 中使用的命令称为语句命令。***语句命令***用于使 LTM 系统以某种方式执行直接操作。例如，这些命令中的一些用于指定希望 LTM 系统将流量引导至其中的 pool 或服务器。其它命令则用于指定将流量重定向至其中的 URI 或端口号，以及用于实施 SNAT 连接的转换地址。

表 13.3 列出并介绍了可以在 iRule 中使用的语句命令。

语句命令	说明
cache <expression> { origin_pool <pool_name> cache_pool <pool_name> [hot_pool <pool_name>] [hot_threshold <hit_rate>] [cool_threshold <hit_rate>] [hit_period <seconds>] [content_hash_size <sets>] [persist <value>]}	动态选择要用于负载平衡的 pool（请参阅 **pool** 命令）。如果<表达式>的值为假，那么使用原始 pool。如果值为真，使用高速缓存 pool，除非符合常用标准，此时将使用 hot_pool。此语句可以按照一定的条件与 if 语句进行关联。
clientside {<iRule commands>}	用于使指定的 iRule 命令在客户机端环境下得到选择运用。如果 iRule 已在客户机端环境下得到选择运用，此命令不会产生任何效果。
detach	停止对此连接选择运用此 iRule 事件。但 iRule 继续运行。
discard	此命令将导致当前数据包或连接（具体取决于事件的环境）被丢弃。此语句必须按照一定的条件与 if 语句进行关联。

语句命令	说明
drop	与 **discard** 命令相同。
forward	将连接设置为转发 IP 数据包。

if { <expression> } {
<statement command>
}
elseif { <expression> } {
<statement command>
}
	询问一个判断真假的问题，然后根据答案（真或假）执行一些操作。
	请注意：在 iRule 中，if 语句可以嵌套的最大层数是 100 层。

log [<facility> <level>} <message>	生成指定的消息，然后记录到系统日志工具。语句通过在为 HTTP Profile 的 **Header Insert** 属性定义的消息基础上，执行可变扩充来实现这些操作。 如果使用不当，**log** 语句会生成大量输出。
matchclass <data-group name>	指定数据组。通常在 if 语句中与 **contains** 运算符一起使用。
[use] node <addr> [<port>]	此命令导致对标识的服务器节点的直接使用，从而绕过任何负载平衡。
peer { <iRule commands> }	用于使指定的 iRule 命令在对等（相反）环境下得到选择运用。
persist <persistence_profile_name>	用于使 LTM 系统利用命名持续性 Profile 来实现连接的持续性。有关使用 iRule 启用持续性的详细信息，请参阅第 13-35 页上的 *“使用 Profile”*。
[use] pool <pool_name> [member <addr> [<port>]]	用于使 LTM 系统将流量负载平衡至命名的 pool。此语句必须按照一定的条件与 if 语句进行关联。您也可以选择指定要将流量引导至其中的特定 Pool 成员。
[use] rateclass <rate_class>	用于使 LTM 系统选择指定的速率等级，以便传输数据包时使用。
reject	此命令导致连接被拒，返回适合于该协议的重置结果。
return [<expression>]	终止执行 iRule 事件，然后（可选）返回对**<expression>**选择运用的结果。
serverside { <iRule commands> }	用于使指定的 iRule 命令在服务器端环境下得到选择运用。如果 iRule 已在服务器端环境下得到选择运用，此命令不会产生任何效果。
[use] snat <addr> [<port>]	用于使 LTM 系统将指定的转换地址分配给 iRule 中指定的一个或多个源 IP 地址。
[use] snatpool <snatpool_name>	此命令导致使用由**<snatpool_name>**标识的 pool 的地址作为转换地址，来创建 SNAT。

***表 13.3** iRule 语句命令*

指定工具命令

有些可在 iRule 中使用的命令称为工具命令。这些命令中的大多数用于确保数据的完整性。表 13.4 列出并介绍了可以在 iRule 中使用的语句命令。

工具命令	说明
b64encode <string>	返回 base-64 编码的字符串，如果发生错误，则返回空字符串。
b64decode <string>	返回 base-64 解码的字符串，如果发生错误，则返回空字符串。
crc32 <string>	返回所提供字符串的 **crc32** 校验和，如果发生错误，则返回空字符串。用于确保数据的完整性。
md5 <string>	返回运用 RSA Data Security 公司 MD5 消息摘要算法（**md5**）得到的所提供字段串的消息摘要；或者如果发生错误，则返回空字符串。用于确保数据的完整性。
sha1 <string>	返回运用 1.0 版安全散列算法（**SHA1**）得到的所提供字段串的消息摘要；或者如果发生错误，则返回空字符串。用于确保数据的完整性。

***表 13.4** iRule 工具命令*

指定流量目的地和地址转换

第 13-8 页上“指定语句命令”一节中描述的 iRule 命令用于指示 LTM 系统以某种方式执行直接操作。以下数节介绍语句命令的一个子集，这些命令或者将流量引导至特定目的地，或者分配用于 SNAT 实施的转换地址。

有关语句命令的完整列表，请参阅第 13-8 页上的*“指定语句命令”*。

选择负载平衡Pool

在 iRule 中指定查询后，可以使用 **pool** 命令来选择希望 LTM 系统将数据包发送至其中的负载平衡 Pool。图 13.5 显示了此命令的一个示例。

```
iRule my_iRule1 {
   when HTTP_REQUEST
   if { [IP::remote_addr] ends_with ".gif" } {
       pool my_pool
      } elseif { [HTTP::uri] ends_with ".jpg" } {
       pool your_pool
      }
}
```

***图 13.5** iRule 中的 **pool** 命令的示例*

选择特定服务器

您也可以编写将流量引导至 pool 中特定服务器的 iRule，以代替 **pool** 命令。要编写此 iRule，请使用 **node** 命令。图 13.6 显示了此命令的一个示例。

```
iRule my_iRule1 {
   when HTTP_REQUEST
   if { [IP::remote_addr] ends_with ".gif" } {
       node my_pool
      }
}
```

***图 13.6** iRule 中的 **node** 命令的示例*

选择高速缓存pool

iRule 可以包含基于 HTTP 标头数据来选择 pool 的 **cache** 命令。**cache** 命令返回原始 pool、常用 pool 或高速缓存 pool。选择高速缓存 pool 时，还包括指明的节点地址和端口。iRule 返回 pool 和 Pool 成员时，LTM 系统不会进行任何额外的负载平衡或持续性处理。

图 13.7 显示了一个包含 **cache** 命令的 iRule 示例。

```
iRule my_iRule
    when HTTP_REQUEST{
    if { [HTTP::host] starts_with "abc" } {
        cache { [HTTP::uri] ends_with "html" or [HTTP::uri] ends_with "gif" } {
          origin_pool origin_server
          cache_pool cache_servers
          hot_pool cache_servers
          hot_threshold 100
          cool_threshold 10
          hit_period 60
          content_hash_size 1024
        } else {
         pool host named_servers
       }
}
```

图 13.7 *包含* ***cache*** *命令的 iRule 示例*

表 13.5 介绍了 **cache** 命令的属性及其语法。

属性	说明	必需属性？
origin_pool <pool_name>	指定包含以下所有内容的服务器的 pool：无法高速缓存所请求内容时；所有高速缓存服务器都不可用时；或者使用 LTM 系统来重定向高速缓存中已丢失的请求时，将请求负载平衡至这些内容。	是
cache_pool <pool_name>	指定以下这类高速缓存服务器的 pool：将请求引导至这些服务器，以优化高速缓存性能。	是
hot_pool <pool_name>	指定包含以下内容的服务器的 pool：所请求内容经常被请求（常用）时，将请求负载平衡至该内容。如果指定此表中以下属性的任何一个，**hot_pool** 属性便是必需的。	否
persist <expr>	指定将被选择运用，并用于持续连接至高速缓存 pool 中同一节点的表达式。	否
cool_threshold <hit_rate>	指定对所指定内容的最大请求次数，此最大值将使内容在周期结束时由常用内容变为罕用内容。	否
hit_period <seconds>	以秒为单位指定一个周期，将按照该周期来计算对特定内容的请求，然后确定是否将该内容的状态变为常用或罕用。	否
content_hash_size <sets_in_content_hash>	指定计算内容处于常用还是罕用状态时，将该内容分成多少个子集。将对同一子集中所有内容的请求加在一起，然后据此为每个子集分配一个常用状态或罕用状态。此属性的值不应超过可能的实际请求数。例如，如果整个站点由 500,000 条内容组成，那么 **content_hash_size** 通常为 100,000。	否

表 13.5 cache *命令语法介绍*

重定向HTTP请求

除了将 iRule 配置为选择特定 pool 之外，还可以使用 iRule 命令 **HTTP::redirect** 对 iRule 进行配置，将 HTTP 请求重定向至特定位置。该位置可以是主机名称，也可以是 URI。

例如，字符串 **https://www.siterequest.com** 指定将 HTTP 请求重定向至一个不同的协议（**https**，而不是标准的 **http**）。

图 13.8 显示了配置用于重定向 HTTP 请求的 iRule。

```
iRule my_iRule
    when HTTP_REQUEST{
    if { [HTTP::status] ends_with "404"} {
        [HTTP::redirect "http://www.siterequest.com"]
       } else {
         pool web_pool
       }
}
```

图 13.8 *基于 HTTP 重定向的 iRule*

为SNAT连接分配转换地址

iRule 特性带有 **snat** 和 **snatpool** 这两个语句命令。

使用 **snat** 命令可以将特定转换地址分配给 iRule 中的源 IP 地址，而无需再使用 Configuration 工具中的 SNAT 屏幕。

尽管与 **snat** 命令不同，但 **snatpool** 命令也可以用于将转换地址分配给源 IP 地址，它使 LTM 系统从指定的以前创建的 SANT pool 中选择转换地址。

有关实施 SNAT 的详细信息，请参阅第 11 章 *“配置 SNAT 和 NAT”*。

查询标头或内容数据

iRule 特性包含若干命令，专门设计用于允许您对以下内容运行查询：

- 链路层标头
- IP 标头
- TCP 标头和内容
- UDP 标头和内容
- HTTP 请求中的 SSL 标头
- 认证数据

查询链路层标头

您可以通过指定链路层标头信息来选择 pool，表 13.6 列出并介绍了这些命令。

iRule 命令	**说明**
LINK::vlan_id	返回数据包的 VLAN 标记。
LINK::vlan_qos	返回数据包的 VLAN 服务质量（QoS）值。

表 13.6 *用于查询链路层标头的 iRule 命令*

服务质量（QoS）级别

网络设备通过***服务质量（QoS）***标准来根据标识符确认和区别对待流量。流量进入站点时，LTM 系统可以应用根据数据包中的 QoS 级别将流量发送至不同服务器 pool 的 iRule。

要将 iRule 配置为根据数据包的 QoS 级别来选择 pool，可以使用 iRule 命令 **LINK::vlan_qos**，如图 13.9 中的示例所示。

```
iRule my_iRule
  when CLIENT_ACCEPTED{
  if { [LINK::vlan_qos] > 2 } {
    pool fast_pool
    } else {
    pool slow_pool
    }
}
```

图 13.9 *基于服务质量（QoS）级别的 iRule*

有关针对数据包设置 QoS 值的详细信息，请参阅第 13-24 页上的*“处理链路层数据”*和第 4 章*“配置负载平衡 Pool”*。

查询IP数据包标头

您可以通过查询 IP 数据包标头信息来选择 pool，表 13.7 列出并介绍了这些命令。

iRule 命令	**说明**
IP::remote_addr	返回连接的远程 IP 地址。
IP::local_addr	返回连接的本地 IP 地址。
IP::client_addr	返回连接的客户机 IP 地址。此命令与命令 **clientside { IP::remote_addr }**等效。
IP::server_addr	返回服务器的 IP 地址。此命令与命令 **serverside { IP::remote_addr }** 等效。
IP::protocol	返回 IP 协议值。
IP::tos	返回 IP 协议的服务类型（ToS）字段的值。
IP::idle_timeout	返回或设置空闲超时值。

表 13.7 *用于查询 IP 数据包标头的 iRule 命令*

如上表所示，可以在 iRule 中查询的特定 IP 数据包标头数据类型包括：

- IP 地址
- 协议号
- ToS 级别
- 空闲超时值

指定 IP 地址

您可以在 iRule 中指定 **IP::remote_addr** 或 **IP::local_addr** 命令，以便

选择 pool。例如，您可以根据客户机的 IP 地址部分对流量进行负载平衡，也可以指定 **IP::client_addr** 和 **IP::server_addr** 命令。

图 13.10 显示了实施上述语句的 iRule。在此示例中，将源地址首字节等于 **206** 的所有客户机请求都引导至名为 **clients_from_206** 的 pool。而将所有其它请求引导至名为 **other_clients_pool** 的 pool。

```
iRule clients_from_206_iRule
    when CLIENT_ACCEPTED{
  if { [IP::local_addr] equals 206.0.0.0 netmask 255.0.0.0 }
{
     pool clients_from_206
     } else {
     pool other_clients_pool
     }
}
```

*图 **13.10** 基于 **IP::local_addr** 命令的 iRule*

指定 IP 协议号

LTM 系统包括 iRule 命令 **IP::protocol**，使用该命令可以根据 IP 协议号来选择 pool。

要将 iRule 配置为根据 IP 协议号来选择 pool，请使用如图 13.11 中的示例所示的语法。

```
iRule my_iRule
    when CLIENT_ACCEPTED{{
    if { [IP::protocol] == 6 } {
        pool tcp_pool
       } else {
         pool slow_pool
       }
}
```

*图 **13.11** 基于 IP 协议号的 iRule*

指定服务类型（ToS）级别

网络设备通过*服务类型（ToS）*标准来根据标识符确认和区别对待流量。流量进入站点时，LTM 系统可以应用根据数据包中的 ToS 级别将流量发送至不同服务器 pool 的 iRule。

用来针对数据包设置 ToS 级别的命令是 **IP::tos**。

要将 iRule 配置为根据数据包的 ToS 级别来选择 pool，可以使用 iRule 命令 **IP::tos**，如图 13.12 中的示例所示。

```
iRule my_iRule
  when CLIENT_ACCEPTED{{
  if { [IP::tos] == 16 } {
    pool telnet_pool
    } else {
    pool slow_pool
    }
}
```

***图 13.12** 基于服务类型（ToS）级别的 iRule*

有关针对数据包设置 ToS 值的详细信息，请参阅第 13-24 页上的“*处理 IP 标头*”和第 4 章“*配置负载平衡 Pool*”。

指定空闲超时值

通过 iRule 中的 **IP::idle_timeout** 命令，可以将空闲超时值指定为选择希望 LTM 系统将流量发送至其中的 pool 的标准。

查询UDP标头和内容

您可以通过指定 UDP 标头或内容信息来选择 pool。表 13.8 列出并介绍了这些命令。

iRule 命令	**说明**
UDP::remote_port	返回远程的 UDP 端口/服务号。
UDP::local_port	返回本地的 UDP 端口/服务号。
UDP::client_port	返回客户机的 UDP 端口/服务号。与命令 **clientside { UDP::remote_port }**等效。
UDP::server_port	返回服务器的 UDP 端口/服务号。与命令 **serverside { UDP::remote_port }**等效。
UDP::payload [<size>]	返回当前 UDP 有效负载内容。
UDP::payload length	返回 UDP 有效负载内容的大小（以字节为单位）。

表 13.8 *用于查询 UDP 标头或内容的 iRule 命令*

查询TCP标头和内容

您可以通过指定 TCP 标头或内容信息来选择 pool。表 13.9 列出并介绍了这些命令。

iRule 命令	**说明**
TCP::remote_port	返回远程的 TCP 端口/服务号。
TCP::local_port	返回本地的 TCP 端口/服务号。
TCP::client_port	返回客户机的 TCP 端口/服务号。与命令 **clientside { TCP::remote_port }**等效。
TCP::server_port	返回服务器的 TCP 端口/服务号。与命令 **serverside { TCP::remote_port }**等效。
TCP::payload [<size>]	返回累计的 TCP 数据内容。
TCP::payload_length	返回累积的 TCP 数据内容的大小（以字节为单位）。
TCP::rtt	返回为 TCP 连接估计的正常返回时间。
TCP::mss	返回 TCP 连接的连接最大字段大小（MSS）。
TCP::unused_port	返回指定 IP 元祖未使用的 TCP 端口，以<hint_port>的值作为起点。
TCP::offset	返回所收集的 TCP 数据在 TCP 数据流中的开始位置。

表 13.9 用于查询 TCP 标头或内容的 iRule 命令

例如，您可能希望 iRule 具有如下逻辑含义：“如果数据包的数据包含带有字符串 **XYZ** 的 TCP 请求，那么使用 pool **xyz_servers** 进行负载平衡。如果未找到该字符串，那么在指定的偏移处搜索字符串 **ABC**，然后使用 pool **abc_servers** 来进行负载平衡。如果未找到字符串 **ABC**，那么使用 pool **web_servers** 来进行负载平衡。”

要实现这一操作，您可以编写使用 **TCP::payload** 命令的 iRule。图 13.13 显示的 iRule 说明了此示例。

```
iRule my_iRule
     when CLIENT_DATA{{
     if { [TCP::payload [<size>]] contains "XYZ" } {
         pool xyz_servers
       } elseif { [substr[TCP::payload [<size>] [](100), 50,
3] == "ABC" {
         pool abc_servers
        } else {
         pool web_servers
     }
}
```

***图 13.13** 使用 TCP 请求字符串命令的示例 iRule*

查询HTTP标头和内容

您可以通过指定 HTTP 标头或内容信息来选择目的地。表 13.10 列出并介绍了这些命令。请注意，此列表未包括用于查询 HTTP 请求中的 SSL 相关标头的命令。有关查询 SSL 标头的信息，请参阅第 13-22 页上的*“查询 HTTP 请求的 SSL 标头”*。

iRule 命令	说明
HTTP::header [value] <name>	返回名称等于**<name>**值的 HTTP 标头的值。如果标头名称不与任何子命令冲突，那么可以省略**<value>**参数。
HTTP::header names	返回请求或响应中带有的所有标头的列表。
HTTP::header count	返回请求或响应中带有的 HTTP 标头数。
HTTP::header at <index>	返回系统在基于零的索引值处找到的 HTTP 标头。
HTTP::header exists <name>	如果请求或响应中带有此命名标头，那么返回“真”。
HTTP::method	返回 HTTP 请求方法的类型。
HTTP::status	返回响应状态代码。
HTTP::version ["0.9" | "1.0" | "1.1"]	返回请求或响应的 HTTP 版本。
HTTP::username	返回 HTTP 基本授权的用户名部分。
HTTP:: password	返回 HTTP 基本授权的密码部分。
HTTP::path [<string>]	返回 HTTP 请求的路径部分。
HTTP::uri [<string>]	返回请求的完整 URI。

iRule 命令	说明
HTTP::query [<string>]	返回 HTTP 请求的查询部分。
HTTP::is_redirect	如果响应是特定类型的重定向，那么返回**真**。
HTTP::is_keepalive	如果此连接是 **Keep-Alive** 连接，那么返回**真**。
HTTP::collect [<length>]	收集通过**[length]**参数指定的数据量。系统收集指定的数据量时，将调用 Tcl 事件 **HTTP_REQUEST_DATA** 或 **HTTP_RESPONSE_DATA**。省略内容长度值时应格外小心。虽然在特定情形中允许这样做，但省略内容长度值或是使用大于实际长度大小的值会使连接延迟。
HTTP:: release	释放收集的数据。没有必要在 **HTTP_REQUEST_DATA** 和 **HTTP_RESPONSE_DATA** 事件中使用 **HTTP::release** 命令，因为在这些事件下，数据是暗中释放的。
HTTP::payload [<size>]	返回 **HTTP::collect** 命令截至目前收集的内容。如果不指定大小，系统将返回收集的内容。
HTTP::payload length	返回命令截至目前收集的内容的大小，不包括 HTTP 标头。
HTTP::payload replace <offset> <length> <string>	用开始于**<string>**的**<offset>**处的**<length>**参数来代替指定的内容数量。
HTTP::close	插入 **Connection:Close** 标头，然后关闭 HTTP 连接。
URI::protocol <string>	从指定的 URI 字符串中提取协议部分。
URI::basename <string>	从指定的 URI 字符串中提取基础名称部分。
URI::path <string>	从指定的 URI 字符串中提取路径部分。
URI::query <string>	从指定的 URI 字符串中提取查询部分。
URI::host <string>	从指定的 URI 字符串中提取主机部分。
URI::compare <uri1> <uri2>	根据 RFC 2616 第 3.2.3 节的建议比较 URI。
URI::decode <string>	返回经过解码的 URI 字符串。
URI::encode <string>	返回经过编码的 URI 字符串。
URI::port <string>	从指定的 URI 字符串中提取端口部分。

表 13.10 *用于查询 IHTTP 标头和内容的 iRule 命令*

例如，您可能希望 iRule 具有如下逻辑含义：“如果数据包的数据包含 URI 以 **cgi** 结束的 HTTP 请求，那么使用 pool **cgi_pool** 进行负载平衡。无此类 HTTP 请求时，如果数据包的数据包含 URI 以**/foo** 开始的 HTTP 请求，那么使用 pool **foo_servers** 进行负载平衡。无此类 HTTP 请求时，使用 pool **default_pool** 进行负载平衡。”

图 13.14 显示的 iRule 说明了此示例。

```
iRule cgi_iRule
    when HTTP_REQUEST {
    if { [HTTP::uri] ends_with "cgi" } {
       pool cgi_pool
    }
    elseif { [HTTP::uri] starts_with "/foo" } {
       pool foo_servers
    }
}
```

***图 13.14** 使用 HTTP 请求字符串命令的示例 iRule*

查询 HTTP 请求的SSL标头

您可以根据 HTTP 请求的 SSL 标头中驻留的数据来选择目的地。表 13.11 列出并介绍了这些命令。

iRule 命令	说明
SSL::mode	在客户机端环境下，返回 **require**、**request**、**ignore** 或 **auto** 之一。在服务器端环境下，返回 **require** 或 **ignore** 之一。
SSL::cert <index>	返回索引值大于或等于零的对等证书链中的 X509 SSL 证书索引。值为零代表证书链中的第一个证书，值为一代表第二张证书，依此类推。此命令目前仅在客户机端环境下可用，在服务器端环境下将返回错误。
SSL::cert issuer <index>	返回索引值大于或等于零的对等证书链中的 X509 SSL 证书索引的签发者证书。值为零代表证书链中的第一个证书，值为一代表第二张证书，依此类推。此命令目前仅在客户机端环境下可用，在服务器端环境下将返回错误。
SSL::cert count	返回对端提供的证书总数。
SSL::verify_result	返回对等证书验证的结果代码，所用的值与 OpenSSL **SSL_get_verify_result()**函数相同。
SSL::cipher name	返回当前 SSL 加密版本，所用的格式与 OpenSSL **SSL_CIPHER_get_version()**函数相同。
SSL::cipher version	返回当前 SSL 加密版本，所用格式与 OpenSSL **SSL_CIPHER_get_version()**函数相同。
SSL::cipher bits	返回当前 SSL 加密使用的密码位数，所用的格式与 OpenSSL **SSL_CIPHER_get_bits()**函数相同。
SSL::SSL::current_sessionid	返回当前协商的 SSL 会话 ID；如果会话 ID 不存在，返回值-1。
SSL::modssl_sessionid_headers [<option>+]	返回系统将要添加到 HTTP 标头，以便模拟 **modssl** 行为的字段列表。返回类型是 Tcl 列表，系统随后将其以标头名称/标头值对的形式进行解释。使用此命令可以指定的选项包括 **initial** 和 **current**。有关 ModSSL 模拟的信息，请参阅第 7 章*“管理 SSL 流量”*。

***表 13.11** 用于查询 HTTP 请求中的 SSL 标头的 iRule 命令*

查询认证数据

您可以根据认证数据来选择目的地，表 13.12 列出并介绍了这些命令。

iRule 命令	说明

iRule 命令	说明
AUTH::wantcredential_prompt <authid>	返回系统最后一次请求（系统生成 AUTH_WANTCREDENTIAL 事件时）的授权会话授权 ID 的证书提示字符串，例如 **Username:**。向交互式协议（例如 **telnet** 和 **ftp**）提供认证服务时，此命令格外有用，此时实际文本提示和响应可能直接与远程用户通信。
AUTH::wantcredential_prompt_style <authid>	返回系统最后一次请求（系统生成 AUTH_WANTCREDENTIAL 事件时）的授权会话授权 ID 的证书提示样式。返回的值可以是 **echo_on**、**echo_off** 或 **unknown**。向交互式协议（例如 **telnet** 和 **ftp**）提供认证服务时，此命令格外有用，此时实际文本提示和响应可能直接与远程用户通信。
AUTH::wantcredential_type <authid>	返回系统最后一次请求（系统生成 AUTH_WANTCREDENTIAL 事件时）的授权会话授权 ID 的证书类型。返回的值可以是 **username**、**password**、**x509**、**x509_issuer** 或 **unknown**，具体取决于证书提示字符串和样式的系统评估。
AUTH::status <authid>	根据系统对授权会话授权 ID 执行的最近一次授权的结果，返回值 **success**、**failure**、**error** 或 **not-authed**。
AUTH::ssl_cc_ldap_username <authid>	返回系统最后一次对授权会话授权 ID 进行成功的基于客户机证书的 LDAP 查询时，从 LDAP 数据库中检索的用户名。如果最后一次的成功查询并未执行成功的基于客户机证书的 LDAP 查询，或者尚未执行查询，系统将返回空字符串。
AUTH::ssl_cc_ldap_status <authid>	返回最后一次对授权会话授权 ID 进行成功的基于客户机证书的 LDAP 查询时的状态。如果最后一次的成功查询并未执行基于客户机证书的 LDAP 查询，或者尚未执行查询，系统将返回空字符串。

***表 13.12** 用于查询认证数据的 iRule 命令*

处理标头或内容数据

iRule 特性包括若干专门设计用来处理特定数据类型的命令。此处的数据处理是指插入、替换和删除数据，以及对标头和 cookie 中的特定值进行设置。

可以使用 iRule 来处理的标头和内容包括以下数类：

- 链路层数据
- IP 标头
- TCP 标头
- HTTP 标头和 cookie
- SSL 标头

处理链路层数据

使用表 13.13 中介绍的命令可以设置用于发送数据包的 QoS 级别。

iRule 命令	说明
LINK::vlan_qos	设置希望系统在发送数据包时使用的 VLAN QoS 级别。

表 13.13 用于处理链路层数据的 iRule 命令

处理IP标头

使用表 13.14 中介绍的命令可以设置用于发送数据包的 ToS 级别。

iRule 命令	说明
IP::tos	设置希望系统在发送数据包时使用的 IP ToS 级别。

表 13.14 用于处理 IP 标头数据的 iRule 命令

处理TCP标头和内容

使用表 13.15 中介绍的命令可以处理 TCP 标头和内容数据。

iRule 命令	说明
TCP::collect <length>	使 TCP 开始收集指定数量的内容数据。
TCP:: release	使 TCP 恢复对连接的处理，并更新已收集的数据。
TCP::payload replace <offset> <length> <data>	用给定的数据替代已收集的有效负载。
TCP::respond <data>	将命名数据直接发送给对端。此命令用于通过 iRule 完成协议握手。
TCP::close	关闭连接。

表 13.15 用于处理 TCP 内容数据的 iRule 命令

处理HTTP标头和cookie

以下这几个可在 iRule 中使用的 iRule 命令用于处理 HTTP 标头数据、内容数据和 cookie。

处理HTTP标头和内容

表 13.16 列出的 iRule 命令可以用于处理 HTTP 请求和响应中的标头。

iRule 命令	说明
HTTP::header insert ["lws"] <name> <value>	将命名 HTTP 标头及其值插入 HTTP 请求和响应的结尾处。如果指定"lws"，系统将为长标头值添加直线型空白。
HTTP::header insert ["lws"] {n1, v1, n2, v2, n3, v3, ...}	传递要插入标头中的 Tcl 列表。在此情形中，系统将列表作为名称/值对的列表进行处理。如果指定"lws"，系统将为长标头值添加直线型空白。
HTTP::header [value] <name> <string>	设置命名标头的值。如果标头存在，此命令将替换标头；如果不存在，命令将添加标头。如果标头名称不与任何其它值冲突，那么可以省略**<value>**参数。
HTTP::header replace <name> [<string>]	使用**<string>**的值替换最后一个命名标头。如果标头不存在，此命令将执行标头插入的操作。
HTTP::header remove <name>	删除请求或响应中的最后一个命名标头。
HTTP::redirect <url>	将 HTTP 请求或响应重定向至指定的 URL。请注意，此命令将立即向客户机发送响应。因此，不能在一个 iRule 中多次指定此命令，也不能在指定此命令后，指定任何修

iRule 命令	说明
	改标头或内容的其它命令。

表 13.16 用于处理 HTTP 请求和响应中的标头的 iRule 命令

iRule 命令	说明
HTTP::respond <status code> [content <content Value>] [<Header name> <Header Value>]+	这是一个功能强大的 API，允许用户生成或重写客户机请求或服务器响应。在客户机端运行此命令时，系统不进行任何负载平衡便将响应发送给客户机。如果在服务器端运行此命令，系统将丢弃实际服务器中的内容，代之以为此 API 提供的信息。请注意，因为此 iRule 运行后，系统将立即发送响应数据，所以我们建议不要在此 API 之后运行任何额外的 iRule。
HTTP::header insert_modssl_fields {options}	插入复制 ModSSL 行为所需的 HTTP 标头字段。请注意，要使用此命令，必须在 SSL Profile 中启用 **ModSSL Methods** 设置。有关 ModSSL 选项的详细信息，请参阅第 7 章 *“管理 SSL 流量”*。
HTTP::header sanitize <header name>+	删除所有标头，指定的标头除外。此命令不会删除一些基本的 HTTP 标头。
HTTP::request_num	返回客户机针对此连接发出的 HTTP 请求数。
COMPRESS::enable	此命令启用对当前 HTTP 响应的压缩。请注意，使用此命令时，必须将 HTTP Profile 的 **Compression** 设置配置为 **Selective**。此命令仅可在 iRule 事件 HTTP_REQUEST、HTTP_REQUEST_DATA 和 HTTP_RESPONSE 的环境下使用。
COMPRESS::disable	此命令启用对当前 HTTP 响应的压缩。请注意，使用此命令时，必须将 HTTP Profile 的 **Compression** 设置配置为 **Selective**。此命令仅可在 iRule 事件 HTTP_REQUEST、HTTP_REQUEST_DATA 和 HTTP_RESPONSE 的环境下使用。
COMPRESS::buffer_size <value>	设置压缩缓冲区的大小，第 6 章“管理 HTTP 和 FTP 流量”中对此进行了详细介绍。此命令仅可在 iRule 事件 HTTP_REQUEST、HTTP_REQUEST_DATA 和 HTTP_RESPONSE 的环境下使用。
COMPRESS::gzip memory_level <level>	设置 **gzip** 内存级别，第 6 章“管理 HTTP 和 FTP 流量”中对此进行了详细介绍。此命令仅可在 iRule 事件 HTTP_REQUEST、HTTP_REQUEST_DATA 和 HTTP_RESPONSE 的环境下使用。
COMPRESS::gzip window_size <size>	设置 **gzip** 窗口的大小，第 6 章“管理 HTTP 和 FTP 流量”中对此进行了详细介绍。此命令仅可在 iRule 事件 HTTP_REQUEST、HTTP_REQUEST_DATA 和 HTTP_RESPONSE 的环境下使用。
COMPRESS::gzip level <level>	指定压缩的数量和速度。

表 13.16 用于处理 HTTP 请求和响应中的标头的 iRule 命令

您也可以选择使用插入 HTTP 请求中的标头的值作为 SSL 查询命令的结果。要实现这一点，请将 SSL 查询命令指定为 **HTTP::header insert** 命令的参数。有关 SSL 查询命令的信息，请参阅第 13-22 页上的 *“查询 HTTP 请求的 SSL 标头”*。

◆ **注意**

*在 iRule 中使用 **HTTP::header insert** 或 **HTTP::remove** 命令将覆盖相应 HTTP Profile 中的**标头插入**和**标头删除**设置。*

处理 HTTP cookie

表 13.17 列出的 iRule 命令可以用于处理 **HTTP** 请求和响应中的 cookie。

iRule 命令	说明
用于请求消息的命令	
HTTP::cookie names	返回 HTTP 标头中显示的所有 cookie 的名称。
HTTP::cookie count	返回 HTTP 标头中显示的 cookie 的数量。
HTTP::cookie [value] <name> [string]	设置或获取给定名称的 cookie 值。如果 cookie 名称不与任何其它命令冲突，那么可以省略此命令的值。
HTTP::cookie version <name> [version]	设置或获取 cookie 的版本。
HTTP::cookie path <name> [path]	设置或获取 cookie 的路径。
HTTP::cookie domain <name> [domain]	设置或获取 cookie 的域。
HTTP::cookie ports <name> [portlist]	设置或获取版本 1 cookie 的 cookie 端口列表。
HTTP::cookie insert <name> <value> [path <path>] [domain <domain>] [version <0 | 1 | 2>]	添加或替代 cookie。版本缺省值为 0。
HTTP::cookie remove <name>	删除 cookie。
HTTP::cookie sanitize [attribute]+	删除 cookie 中的所有属性，指定的属性除外。
HTTP::cookie exists <name>	如果 cookie 存在，返回“真”值。
Commands for response messages	
HTTP::cookie names	返回 HTTP 标头中显示的所有 cookie 的名称。
HTTP::cookie count	返回 HTTP 标头中显示的 cookie 的数量。
HTTP::cookie [value] <name> [string]	设置或获取给定名称的 cookie 值。如果 cookie 名称不与任何其它命令冲突，那么可以省略此命令的值。
HTTP::cookie version <name> [version]	设置或获取 cookie 的版本。
HTTP::cookie path <name> [path]	设置或获取 cookie 的路径。
HTTP::cookie domain <name> [domain]	设置或获取 cookie 的域。
HTTP::cookie ports <name> [portlist]	设置或获取版本 1 cookie 的 cookie 端口列表。
HTTP::cookie insert <name> <value> [path] [domain][version]	添加或替代 cookie。cookie 的版本缺省值为 0。
HTTP::cookie remove <name>	删除 cookie。
HTTP::cookie maxage <name> [seconds]	设置或获取最长生存时间。仅适用于版本 1 的 cookie。
HTTP::cookie expires <name> [seconds] [absolute | relative]	设置或获取过期属性。仅适用于版本 0 的 cookie。如果指定 **absolute** 参数，那么 **seconds** 值表示自 UNIX 发布（1970 年 1 月 1 日）以来的秒数。缺省秒数是 **relative**，表示自当前时间以来的秒数。
HTTP::cookie comment <name> [comment]	设置或获取 cookie 的注释。仅适用于版本 1 的 cookie。
HTTP::cookie secure <name> [enable|disable]	设置或获取安全属性。仅适用于版本 1 的 cookie。
HTTP::cookie commenturl <name> [commenturl]	设置或获取注释的 URL。仅适用于版本 1 的 cookie。
HTTP::cookie discard <name> [enable|disable]	设置或获取丢弃属性。仅适用于版本 1 的 cookie。
HTTP::cookie sanitize [attribute]	删除 cookie 中的所有属性，指定的属性除外。
HTTP::cookie exists <name>	如果 cookie 存在，返回“真”值。
HTTP::cookie encrypt <name> <pass phrase> <data> ["128" | "192" | "256"]	使用密码短语生成的密钥来加密给定 cookie 的值。缺省密钥长度为 **128**。
HTTP::cookie decrypt <name>	使用密码短语生成的密钥来解密给定 cookie 的值。缺省密钥长

iRule 命令	说明
<pass phrase> <data> ["128" | "192" | "256"]	度为 **128**。

表 13.17 *用于处理 HTTP 请求和响应中的 cookie 的 iRule 命令*

处理 SSL 标头和内容

可以在 iRule 中使用的 SSL 数据处理命令分为以下两类：

- 用于处理 SSL 查询结果的命令
- 用于更改设置或调用操作的命令

以下两节介绍了这些命令

处理 SSL 查询结果

iRule 特性包括用于处理 SSL 查询命令结果的 SSL 命令。表 13.18 显示了这些命令。有关 SSL 查询命令的详细信息，请参阅第 13-22 页上的*"查询 HTTP 请求的 SSL 标头"*。

iRule 命令	说明
X509::version <X509 certificate>	返回 X509 证书的版本号（一个整数）。
X509::serial_number <X509 certificate>	返回 X509 证书的序列号（一个整数）。
X509::signature_algorithm <X509 certificate>	返回 X509 证书的签名算法。
X509::issuer <X509 certificate>	返回 X509 证书的签发者。
X509::not_valid_before <X509 certificate>	返回 X509 证书的 **not-valid-before** 日期（生效日期）。
X509::not_valid_after <X509 certificate>	返回 X509 证书的 **not-valid-after** 日期（失效日期）。
X509::subject <X509 certificate>	返回 X509 证书的主题。
X509::subject_public_key_type <X509 certificate>	返回 X509 证书主题的公钥类型。值可以是 **RSA**、**DSA** 或 **unknown**。
X509::subject_public_key <X509 certificate>	返回 X509 证书主题的公钥。
X509::subject_public_key_RSA_bits <X509 certificate>	返回 X509 证书主题的公共 RSA 密钥的位数。仅当公钥类型为 **RSA** 时，此命令才适用，否则会生成错误。
X509::extensions <X509 certificate>	返回证书上的 X509 扩展集。
X509::whole <X509 certificate>	以 PEM 格式返回整个 X509 证书。
X509::hash <X509 certificate>	返回 X509 证书的 MD5 散列（指纹）。
X509::verify_cert_error_string <X509 verify error code>	与 OpenSSL 函数 **X509_verify_cert_error_string()**的返回结果相同。**<X509 verify error code >**参数使用的值与 **SSL::verify result** 命令返回的值相同。
X509::cert_fields <X509 certificate> <verify error code> {options}	返回将要添加到 HTTP 标头，以便模拟 ModSSL 行为的字段列表。返回类型是 Tcl 列表，系统随后将其以标头名称/标头值对的形式进行解释。有关 ModSSL 的详细信息，请参阅第 7 章*"管理 SSL 流量"*。

表 13.18 *用于处理 SSL 查询结果的 iRule 命令*

更改 SSL 设置或调用操作

表 13.19 列出并介绍了一组可用于更改 SSL 设置或调用操作的 SSL 命令。

iRule 命令	说明

iRule 命令	说明
SSL::renegotiate	根据 LTM 系统是在客户机端环境下还是在服务器端环境下选择运用此命令，命令的结果有所不同。 仅当针对连接启用了 SSL 时，命令才会成功；否则，命令将返回错误。 在客户机端环境下选择运用此命令时，系统将使用强制 SSL 重新协商的配置选项，立即重新协商关联客户机端连接的请求。重新协商会强制更改连接的任何 SSL 设置，包括客户机证书设置。在服务器端环境下选择运用此命令时，系统将使用强制 SSL 重新协商的配置选项，立即启动关联服务器端连接的重新协商。
SSL::cert mode <"request" | "require" | "ignore" | "auto">	根据系统是在客户机端环境下还是在服务器端环境下选择运用此命令，命令的结果有所不同。 系统在客户机端环境下选择运用此命令时，命令将覆盖客户机端 SSL 连接关于客户机证书的当前设置。 系统在服务器端环境下选择运用此命令时，命令将覆盖服务器端 SSL 连接关于服务器证书的当前设置。在此实例中，有效参数只有 **require** 或 **ignore**。
SSL::authenticate <"once" | "always">	此命令仅在客户机端环境下有效，它覆盖客户机端 SSL 连接关于认证频率的当前设置。
SSL::authenticate depth <number>	根据系统是在客户机端环境下还是在服务器端环境下选择运用此命令，命令的结果有所不同。 系统在客户机端环境下选择运用此命令时，命令将覆盖客户机端 SSL 连接关于最大证书链遍历深度的当前设置。 系统在服务器端环境下选择运用此命令时，命令将覆盖服务器端 SSL 连接关于最大证书链遍历深度的当前设置。
SSL::unclean shutdown <"enable" | "disable">	根据系统是在客户机端环境下还是在服务器端环境下选择运用此命令，命令的结果有所不同。系统在客户机端环境下选择运用此命令时，命令将覆盖客户机端 SSL 连接关于非正常关机的当前设置。系统在服务器端环境下选择运用此命令时，命令将覆盖服务器端 SSL 连接关于非正常关机的当前设置。
SSL::verify result <result_code>	设置对等证书验证的结果代码。**<result_code>**参数使用的值与 **SSL::verify result** 命令返回的值相同。
SSL::handshake hold	中止任何有关认证的 SSL 操作。
SSL::handshake resume	恢复系统之前使用 **SSL::handshake hold** 命令中止的任何 SSL 操作。

***表 13.19** 用于更改设置或调用操作的 iRule 命令*

使用UIE函数命令

LTM 系统包括若干可用作表达式一部分的特殊函数命令。这些 iRule 命令是通用检查引擎（UIE）的组成部分。

UIE 表达式的主要用途是返回持续性字符串，或者返回 pool 能够将流量直接发送到其中的节点。

◆ 注意

有关持续性的信息，参阅第 13-35 页上的“使用 Profile”。

可以在 UIE 表达式中使用的函数命令分为以下两类：用于返回字符串的命令和用于直接选择节点的命令。

用于返回字符串的命令

表 13.20 列出并介绍了用于返回指定字符串的命令，表后的数页中提供了命令的详细信息和示例。

命令	说明
findstr	在另一个字符串中查找字符串，然后从匹配项中指定的偏移处开始，返回字符串。
substr	在另一个字符串中查找字符串，然后从匹配项中指定的偏移处开始，返回字符串。
getfield	以字符为基础分割字符串，然后返回与特定字段相关的字符串。
findclass	查找包含指定表达式的结果的类成员，然后返回该类成员。
decode_uri	选择运用表达式，然后返回经过如下处理、带有任何%XX 换码序列的字符串：这些字符串按照 RFC2396 中定义的 HTTP 换码序列进行解码。
domain	解析并返回指定表达式中域名的后缀部分，直至达到指定的个数。
imid	用于解析 i-mode®标识符字符串的 **http_uri** 变量和 **user-agent** 标头字段，此字符串可用于持续进行 i-mode 会话。

***表 13.20** 用于返回字符串的 UIE 命令*

findstr

findstr 命令在**<string>**中查找字符串**<search string>**，任何根据匹配位置的**<skip_count>**和**<terminator>**返回子字符串。

请注意以下数点：

- **<terminator>**可以是字符，也可以是长度。
- 如果未指定**<skip_count>**，那么缺省为零。
- 如果未指定**<terminator>**，那么缺省为字符串的结尾。
- 此命令（不带有**<skip_count>**或**<terminator>**）与以下 Tcl 命令等效：“**string range <string> [string first <string> <search string>] end**”。

findstr()命令的语法如下：

findstr <string> <search string> [<skip_count> [<terminator>]

图 13.15 显示了一个使用 **findstr** 命令的 iRule 示例。

```
iRule my_iRule
  when CLIENT_ACCEPTED{{
  if { [findstr [http_uri] "?type=" 6 "&"] == "cgi" } {
     pool cgi_servers
  } else {
     pool web_servers
  }
}
```

图 13.15 使用 findstr 命令的 iRule

substr

substr 命令根据**<skip_count>**和**<terminator>**的值返回子字符串**<string>**。

请注意以下数点：

- **<skip_cunnt>**和**<terminator>**参数的用法与它们在 **findstr** 命令中的用法相同。
- 此命令与 Tcl 命令 **string range** 等效，区别在于此命令的**<terminator>**值可以是字符，也可以是数字。

substr 命令的语法如下：

substr <string> <skip_count> [<terminator>]

getfield

getfield 命令以字符为基础分割字符串，然后返回与特定字段相关的字符串。

getfield 命令的语法如下：

getfield <string> <split> <field_number>

findclass

findclass 命令从数据组列表中搜索以**<string>**开始的成员，然后返回数据组成员字符串。此命令与 **matchclass** 命令类似，区别在于此命令不要求成员相等，而只要求成员以该字符串开始，而且此命令返回的是整个成员值。

findclass 命令的语法如下：

findclass <string> <class>

decode_uri

decode_uri 命令使用根据 RFC2616 编码的 HTTP URI 来解码字符串**<string>**，然后返回结果。

decode_uri 命令的语法如下：

decode_uri <string>

domain

domain 命令将字符串**<string>**解析为以点分隔的域名，然后返回域名最后的**<count>**部分。

domain 命令的语法如下：

domain <string> <count>

imid

imid 函数专用于为特有的 i-mode 用户标识符字符串解析 **HTTP::uri** 和 **HTTP::header** 的“user-agent”值，该字符串可用于会话持续性。**imid** 命令没有任何参数，仅仅返回表示 i-mode 标识符的字符串；如果没有找到相关项，则返回空字符串。

imid 命令的语法如下：

imid

用于返回节点地址的命令

表 13.21 列出并介绍了用于返回节点地址，以便直接选择 Pool 成员的命令。

命令	说明
node	返回从地址加端口的字符串表示方法中转换而来的字符型节点地址。
mapclass2node	表示命令 **findclass**、**findstr** 和 **node** 的简单组合。
wlnode	返回从特定 BEA WebLogic™字符串格式转换成字符型节点地址的字符型节点地址，用于表示应用 IP 地址和服务。

表 13.21 *用于返回节点地址的 UIE 命令*

node

node 命令返回从地址加端口的字符串表示方法中转换而来的字符型节点地址。设计此函数的主要目的是与持续性表达式一起使用，以便直接选择要持续连接的节点。

node 命令的语法如下：

node <string>

mapclass2node

mapclass2node 命令在**<class>**中搜索以**<string>**开始的类成员，根据**<split>**分割成员字符串，然后将第二个字段转换为节点对象。如果未指定**<split>**，那么缺省为空格字符。此命令与以下汇聚命令等效：**node [getfield [findclass <string> <class>] <split> 2]**。**mapclass2node** 命令是 **findclass**、**findstr** 和 **node** 命令的简单组合。

wlnode

wlnode 函数返回从 BEA WebLogic™格式的字符串转换而来的字符型节点地址，以便标识连接应与其进行持续的应用节点。

设计 **wlnode** 函数的主要目的是与持续性表达式一起使用，以便直接选择要持续连接的节点。

使用Profile

编写 iRule 时，可能希望 iRule 获得特定 Profile 设置的值，以便能够制定更有针对性的流量管理决策。幸运的是，iRules 特性包括一个命令，专门设计用于读取 iRule 中指定的 Profile 设置的值。

iRule 不仅能够读取 Profile 设置的值，而且能够覆盖特定设置的值。这表示，您可以对单独的连接应用配置值，这些值与 LTM 系统应用到流经

Real Server 的大多数连接的值不同。

读取Profile设置

iRule 特性包括一个称为 **PROFILE** 的命令。在 iRule 中指定 **PROFILE** 命令并命名 Profile 类型和设置时，iRule 便会读取该特定 Profile 设置的值。为了实现此目的，iRule 查找分配给 Real Server 的命名 Profile 类型，然后读取 **PROFILE** 命令序列中指定的设置的值。随后，iRule 可以使用此信息来管理流量。

例如，可以在 iRule 中指定命令 **PROFILE::tcp idle_timeout**。然后，LTM 系统查找分配给 Real Server 的 TCPProfile（例如 **my_tcp**），并查询分配给 **Idle Timeout** 设置的值。

覆盖Profile设置

一些特定的 iRule 命令可以用于覆盖特定的 Profile 设置。例如，可以使用这些命令来覆盖 SSL 或 HTTP Profile 中的设置。

然后，为对其应用 iRule 的连接指定带有设置值的 iRule 命令时，LTM 系统将使用在 iRule 中指定的设置值，而不是相应 Profile 中的值。用于覆盖 Profile 设置的 iRule 命令包括：

- **SSL::renegotiate**
- **SSL::cert mode**
- **SSL::authenticate**
- **SSL::authenticate depth**
- **SSL::unclean shutdown**
- **COMPRESS::buffer_size**
- **COMPRES S::gzip memory_level**
- **COMPRESS::gzip window_size**
- **COMPRESS::gzip level**

通过iRule启用会话持续性

第 9 章“启用会话持续性”介绍了如何配置持续性 Profile，将其分配到 Real Server，从而启用会话持续性。如该章中所述，LTM 系统将这些持续性 Profile 的设置应用于流经 Real Server 的每个适用的会话。例如，如果将 **msrdp** Profile 分配给 Real Server，那么 LTM 系统将对每个入站的 Microsoft®远程桌面协议（RDP）连接应用那些设置。

但在有些情形中，您可能希望以更精确的方式启用持续性。例如，您可能希望根据插入 HTTP 请求标头的 SSL 证书状态来持续会话，而不是使用仅作用于非端接 SSL 流量的 **ssl** 持续性 Profile。要实现此目的，可以使用 **HTTP::header** 命令编写一个 iRule，然后将该 iRule 分配给 Real Server。这样，只要 LTM 系统终止了一个 SSL 请求，iRule 便会将证书状态以标头形式插入请求，然后根据该状态来持续会话。

LTM 系统包括一个特殊的 iRule 命令 **persist**，用于实施第 9 章“启用会话持续性”中介绍的会话持续性类型。您只需在 iRule 中键入 **persist** 命令，以便指定持续性类型。对于某些持续性类型，必须指定一些额外的参数。

- **persist cookie**
- **persist destaddr [mask <mask>] [<timeout>]**
- **persist hash**

- **persist msrdp**
- **persist sip**
- **persist srcaddr [mask <mask>] [<timeout>]**
- **persist ssl**
- **persist universal <string> [<timeout>]**
- **persist none**

persist none、**hash**、**srcaddr**、**destaddr** 和 **universal** 命令可在任何情形中使用，即使没有配置相应的持续性 Profile，然后将其分配给 Real Server。但 **persist ssl**、**cookie**、**msrdp** 和 **sip** 命令要求为 Real Server 分配相应的持续性 Profile。尝试在没有相应 Profile 的情况下使用这些命令将生成运行时 iRule 错误。

创建、管理和使用数据组

数据组在编写 iRule 时非常有用。简单地来说，***data group*** 是相关元素的编组，例如用于 AOL 客户机的一组 IP 地址。将数据组与 **matchclass** 命令或 **contains** 运算符一起指定时，便无需在 iRule 表达式中列出多个值作为参数。

要了解数据组的用途，有必要首先了解 **matchclass** 命令和 **contains** 运算符。

使用matchclass命令和contains运算符

LTM 系统包括一个称为 **matchclass** 的 iRule 命令，可以用于根据 iRule 中正在使用的命令是否代表特定数据组的成员来选择 pool。使用 **matchclass** 命令时，LTM 系统知道跟在标识符后面的字符串便是数据组的名称。

例如，如果 **IP::remote_addr** 命令的值是数据组 AOL 的成员，那么使用 **matchclass** 命令可以使 LTM 系统对所有指向 pool **aol_pool** 的入站 AOL 连接进行负载平衡。图 13.16 显示了此类 iRule。在此情形中，**matchclass** 命令清楚地指示名为 **aol** 的对象是一个数值集合（即数据组）。

```
iRule my_iRule
    when CLIENT_ACCEPTED{{
    if { [IP::remote_addr] eq matchclass aol } {
        pool aol_pool
     }
      else {
         pool all_pool
       }
}
```

图 13.16 基于 matchclass 命令的 iRule

请注意，如果表达式（例如 **IP::remote _addr eq matchclass aol**）确实具有至少一个数据组中的特定值，那么表达式为真。

您也可以使用 **contains** 运算符，它与 **matchclass** 命令类似。例如，可以编写如图 13.17 中所示的 iRule。

```
iRule my_iRule
    when CLIENT_ACCEPTED{{
    if { aol contains [IP::remote_addr] } {
        pool aol_pool
     }
      else {
         pool all_pool
       }
}
```

***图 13.17** 基于 **contains** 运算符的 iRule*

创建数据组

在 iRule 中使用 **matchclass** 命令时，可以指定以下三类数据组中的任何一组：

- 地址数据组－－IP 地址的集合
- 字符串数据组－－字符串的集合（例如***.jpg**）
- 整数数据组－－数值的集合

以下数节中介绍了这些数据组类型。

◆ 注意

数据组的大小仅受系统资源的限制。

地址数据组

IP 地址数据组有两类：网络 IP 地址和主机 IP 地址。

以下过程可用于创建网络或主机地址数据组：

创建地址数据组的步骤

1. 在 Main 选项卡上，展开 **Local Traffic**。
2. 点击 **iRules**。
   将显示 iRules 屏幕。
3. 在菜单栏上，点击 Data Group List。
4. 在屏幕的右上角，点击 **Create**。
5. 在 **Name** 框中，为数据组键入一个唯一的名称，例如 **my_address_group**。
6. 在 **Type** 框中，选择 **Address**。
   屏幕将扩展，显示更多设置。
7. 在 Records 部分中，选择所需 **Type**（**Host** 或 **Network**）。
8. 在 Address 框中，键入数据组的第一个 IP 地址。如果要创建网络数据组，请在 **Mask** 框中输入网络掩码。
9. 点击 **Add**。
   此条目将显示在 **Address Record** 框中。
10. 重复步骤 7 和 8，直到输入了所有 IP 地址。
11. 点击 **Finished**。

字符串数据组

字符串数据组包含一个字符串列表，例如***.jpg** 或***.gif**。以下过程可用于创建字符串数据组。

请注意，此示例使用引号和粗体字表示 UI。

创建字符串数据组的步骤

1. 在 Main 选项卡上，展开 **Local Traffic**。
2. 点击 **iRules**。
   将显示 iRules 屏幕。
3. 在菜单栏上，点击 Data Group List。
4. 在屏幕的右上角，点击 **Create**。
5. 在 **Name** 框中，为数据组键入一个唯一的名称，例如 **my_images**。
6. 在 **Type** 框中，选择 **String**。
   屏幕将扩展，显示字符串专用的设置。
7. 在 **String** 框中，键入数据组的第一个字符串。
8. 点击 **Add**。
   此条目将显示在 **String Record** 框中。
9. 重复步骤 6 和 7，直到输入了所有字符串。
10. 点击 **Finished**。

整数数据组

整数数据组包含一个整数列表。以下过程介绍了如何创建整数数据组。

创建整数数据组的步骤

1. 在 Main 选项卡上，展开 **Local Traffic**。
2. 点击 **iRules**。
   将显示 iRules 屏幕。
3. 在菜单栏上，点击 Data Group List。
4. 在屏幕的右上角，点击 **Create**。
5. 在 Name 框中，为数据组键入一个唯一的名称，例如 **my_integer_group**。
6. 在 **Type** 框中，选择 **Integer**。
   屏幕将扩展，显示 Records 部分。
7. 在 **Integer** 框中，键入数据组的第一个整数。
8. 点击 **Add**。
   此条目将显示在 **Integer Records** 框中。
9. 重复步骤 6 和 7，直到添加了所有整数。
10. 点击 **Finished**。

存储选项

LTM 系统允许您以两种方式存储数据组，即嵌入式存储和外部存储。

嵌入式存储

创建数据组时，LTM 系统自动将它们作为一个整体存储在 **bigip.conf** 文件中。这类存储称为*嵌入式存储*。

数据组中的任何数据需要更新时，必须重新加载整个数据组。通常，由于对大型数据组的广泛搜索要求，嵌入式存储会占用额外的系统资源。此外，嵌入式存储要求即使以增量方式更新数据，也需要重新加载整个数据组。考虑到这些因素，LTM 系统为您提供了以外部方式（即在 **bigip.conf** 文件之外）存储数据组的功能。

外部存储

您可以选择将数据组存储在 LTM 系统上的其它位置，即存储在 **bigip.conf** 文件之外。这些数据组称为***外部数据组***。外部数据组的缺省

存储位置是**/config** 目录下。因为数据组以外部方式存储在其它位置，所以 **bigip.conf** 文件仅包含数据组的元数据。对于以外部方式存储的数据组文件，其中的数据存储为逗号分割的数值列表（CSV 格式）的形式。

创建外部数据组非常有用，因为无需在加载数据时对它们进行排序。反之，数据存储在内核的散列表中。iRule 使用大型数据组将流量引导至 pool 时，这种存储方法可获得性能的提高。

以外部方式存储数据组的步骤

1. 在 Main 选项卡上，展开 **Local Traffic**。
2. 点击 **iRules**。
   将显示 iRules 屏幕。
3. 在菜单栏上，点击 Data Group List。
4. 在屏幕的右上角，点击 **Create**。
5. 在 **Type** 框中，键入希望存储在外部位置的现有数据组的名称。
6. 在 **Type** 框中，选择**(External File)**。
   屏幕将扩展，显示 Records 部分。
7. 指定存储位置：
   - 如果不希望将数据组存储在缺省外部位置（**/config**）中，请使用 **Path/Filename** 框指定外部位置的路径名和文件名，例如**/home/my_address_group**。
     此文件名应与分配给数据组自身的名称相匹配。
   - 如果希望将数据组存储在缺省外部位置（**/config**）中，请将 **Path/Filename** 框保留为空。
8. 在 **File Contents** 框中，选择适合于数据组的文件类型（**Address**、**String** 或 **Integer**）。
9. 点击 **Finished**。

将数据存储在外部数据组文件中时，LTM 系统将它们存储为逗号分割列表的形式；任何数据值（例如 IP 地址）的格式都与 **bigip.conf** 文件中使用的格式相匹配。图 13.18 显示了数据组文件**/home/ip2.data group** 的内容。

```
network 195.93.32.0 mask 255.255.255.0
,network 195.93.33.0 mask 255.255.255.0
,network 195.93.34.0 mask 255.255.255.0
,network 195.93.48.0 mask 255.255.255.0
,network 195.93.49.0 mask 255.255.255.0
,network  195.93.50.0 mask 255.255.255.0
```

图 13.18 外部数据组文件示例

显示数据组属性

使用 Configuration 工具可以显示现有数据组的属性。

显示数据组属性的步骤

1. 在 Main 选项卡上，展开 **Local Traffic**。
2. 点击 **iRules**。
   将显示 iRules 屏幕。
3. 在菜单栏上，点击 Data Group List。
4. 点击数据组的名称。
   此操作将显示该数据组的属性。

管理数据组成员

使用 Configuration 工具可以向现有数据组添加成员，也可以从现有数据组中删除成员。

向数据组添加成员的步骤

1. 在 Main 选项卡上，展开 **Local Traffic**。
2. 点击 **iRules**。
   将显示 iRules 屏幕。
3. 在菜单栏上，点击 Data Group List。
4. 点击数据组的名称。
   此操作将显示该数据组的属性。
5. 找到记录框，然后在合适的框中键入地址、字符串或整数。
6. 点击 **Add**。
7. 在屏幕底部，点击 **Update**。

从数据组中删除成员的步骤

1. 在 Main 选项卡上，展开 **Local Traffic**。
2. 点击 **iRules**。
   将显示 iRules 屏幕。
3. 在菜单栏上，点击 Data Group List。
4. 点击数据组的名称。
   此操作将显示该数据组的属性。
5. 选中要删除的成员对应的 **Select** 框。
6. 点击 **Delete** 按钮，显示确认信息时再次点击 **Delete**。

在同步配置时包括外部数据组

同步冗余系统的 BIG-IP 系统配置时，LTM 系统仅包括驻留在 **bigip.conf** 文件中的数据组，即以嵌入方式存储的数据组。如果希望同步过程包括以外部方式存储的数据组，必须为每个数据组添加一个关联条目到 **bigip.conf** 文件中。

覆盖Profile设置

对于一些用来查询和处理标头和内容数据的 iRule 命令，各种 Profile 中具有等效设置。在 iRule 中使用那些命令时，如果有事件触发了该 iRule，LTM 系统将覆盖那些 Profile 设置的值，改为使用 iRule 中指定的值。

例如，HTTP Profile 可以指定要使用的特定缓冲区大小，以便压缩 HTTP 数据，但您可能希望为特定类型的 HTTP 连接指定不同的缓冲区大小。在此情形中，您可以在 iRule 中包括命令 **HTTP::compress_buffer_size**，指定与 Profile 值不同的值。

A

其它 Monitor 注意事项

- 实施用于“动态比率”负载平衡的 Monitor
- 实施 MSSQL Monitor

实施用于“动态比率”负载平衡的Monitor

您可以为 pool 配置“动态比率”负载平衡，这些 pool 由 RealNetworks® RealServer 服务器、配备了 Windows 管理架构（WMI）的 Windows® 服务器、或配备了 SNMP 代理的任何服务器（如 UC Davis SNMP 代理或 Windows® 2000 Server SNMP 代理）组成。

为了对这几种服务器实施“动态比率”负载平衡，BIG-IP®本地流量管理（LTM）系统为每种服务器提供了特殊 Monitor 插件文件以及状态或性能 Monitor。例外情况是配备 SNMP 代理的服务器。在这种情况下，LTM 系统仅提供 Monitor，不需要用于运行 SNMP 代理的服务器的特殊插件文件。

必须在每一个要监视的服务器中安装 Monitor 插件，而且必须创建位于 LTM 系统中的性能 Monitor。创建了 Monitor 后，该 Monitor 就直接与服务器插件进行通信。对于每一种服务器，表 A.1 显示了所需的 Monitor 插件和相应的性能 Monitor 类型。

服务器类型	Monitor 插件	Monitor 类型
RealServer Windows server	**F5RealMon.dll**	Real Server
RealServer UNIX server	**f5realmon.so**	Real Server
Windows server with WMI	**F5Isapi.dll**	WMI
Windows 2000 Server server	SNMP agent	SNMP DCA 和 SNMP DCA Base
UNIX server	UC Davis SNMP agent	SNMP DCA 和 SNMP DCA Base

***表 A.1** Monitor 插件和相应的 Monitor 模板*

实施Real ServerMonitor

对于 RealSystem Server 系统，当在该系统中安装插件时，LTM 系统提供了收集所需指标的 Monitor 插件。配置用于“动态比率”负载平衡的 RealSystem Server 包括以下四项任务：

- 在 RealSystem 服务器中安装 Monitor 插件。
- 在 LTM 系统中配置 Real ServerMonitor。
- 将 Monitor 与服务器关联来收集指标。
- 创建或修改服务器 pool，以使用“动态比率”负载平衡。

在 RealSystem Server 系统中（Windows 版本）安装 Monitor 插件的步骤

1. 从 LTM 系统下载 Monitor 插件 **F5RealMon.dll**。
   该插件位于文件夹 **/usr/contrib/f5/isapi** 中。（URL 是 **https://<bigip_address>/doc/rsplug-in/f5realmon.dll**。）

2. 将 **f5realmon.dll** 复制到 RealServer **plug-ins** 目录。
   （例如，**C:\Program Files\RealServer\plug-ins**。）

3. 如果 RealSystem Server 程序正在运行，那么重启该程序。

在 RealSystem Server 系统（UNIX 版本）中安装 Monitor 插件的步骤

1. 从 RealSystem Server CD，复制目录 **downloads/rsplug-ins** 下的文件 **F5RealMonsrc.tgz。**

2. 从 <http://proforma.real.com/rnforms/resources/server/realsystemsdk/index.html>下载 RealSystem Server SDK。

3. 使用 UNIX 工具 **gunzip** 和 **tar，**按如下命令解压文件 **F5RealMonsrc.tgz：**

   gunzip F5ReaMonsrc.tgz

   tar -xpf F5RealMonsrc.tar

   显示一个文件列表，包括两个 makefile：**linux-2.0-libc6-i386.mak** 和 **sunos-5.7-sparc.mak**，分别用于 Linux 和 SunOS 系统。

4. 在这两个 makefile 中，更改指向 SDK 位置的路径。

5. 输入适用于操作系统的命令：

   - 对于 Linux 系统，输入：
   make -f linux-2.0-libc6-i386.mak

   - 对于 UNIX 系统，输入：
   make -f sunos-5.7-sparc.mak

   这会为 RealSystem Server 插件 **F5RealMon.so** 创建一个源文件。

6. 将 **F5RealMon.so** 插件转移到 RealSystem Server 主目录下的**插件/**目录。

7. 启动 RealSystem Server。

安装了插件后，必须配置 Real ServerMonitor，将已配置的 Monitor 与 Pool 成员相关联（RealSystem Server 服务器），并且将负载平衡设置为“动态比率”：

- 有关配置 Real ServerMonitor 的详细信息，请参阅第 10 章*“配置 Monitor”*。
- 有关将性能 Monitor 与 Pool 成员相关联的详细信息，请参阅第 4 章*“配置负载平衡 Pool”*。
- 有关将 pool 的负载平衡方法设置为“动态比率”方法的详细信息，请参阅第 4 章*“配置负载平衡 Pool”*。

实施WMI Monitor

对于运行 Windows 管理构架（WMI）的 Windows，LTM 系统为该服务器提供了一个 Data Gathering Agent **F5Isapi.dll。**配置用于“动态比率”负载平衡的 Windows 平台包括以下四项任务：

- 在服务器中安装 Data Gathering Agent **F5Isapi.dll。**
- 在 LTM 系统中配置 WMI Monitor。
- 将 Monitor 与服务器相关联来收集指标。

- 创建或修改服务器 pool，以使用“动态比率”负载平衡方法。

在服务器中安装 Data Gathering Agent（F5Isapi）的步骤

1. 从 LTM 系统下载 **Data Gathering Agent（F5Isapi.dll）。**
   该插件位于文件夹 **/usr/contrib/f5/isapi 中。**（URL 是 **https://<bigip_address>/doc/rsplug-in/f5realmon.dll。**）

2. 将 **f5isapi.dll** 复制到目录 **C:\Inetpub\scripts。**

3. 打开 Internet Services Manager。

4. 在 Internet Services Manage 的左侧面板，打开文件夹 **<machine_name>\Default Web Site\Script**，在该文件夹中，**<machine_name>**是配置的服务器的名称。
   在右侧面板中，打开 **Scripts** 文件夹的内容。

5. 在右侧面板中，右击 **F5Isapi.dll，**并选择 **Properties。**
   将打开 **F5Isapi.dll** 的 Properties 会话框。

6. 取消选定 **Logvisits。**
   （每次访问代理的快速日志记录将填充日志文件。）

7. 点击 **File Security** 选项卡。
   此操作将显示“文件安全性”选项。

8. 在 **Anonymous access and authentication control group** 框中，点击 **Edit。**
   将打开 Authentication Methods 会话框。

9. 在会话框中，清除所有复选框，然后选择 **Basic Authentication。**

10. 在 **Authentication Method** 会话框中，点击 **OK** 来接受更改。

11. 在 **Properties** 会话框中，点击 **Apply**。
    现在，可以使用 WMI Data Gathering Agent。

安装了插件后，必须配置 WMI Monitor，将已配置的 Monitor 与 Pool 成员相关联，并且将负载平衡设置为“动态比率”：

- 有关配置 WMI Monitor 的详细信息，请参阅第 10 章 *“配置 Monitor”*。

- 有关将定制 Monitor 与 Pool 成员相关联的详细信息，请参阅第 4 章 *“配置负载平衡 Pool”*。

- 有关将 pool 的负载平衡方法设置为“动态比率”方法的详细信息，请参阅第 4 章 *“配置负载平衡 Pool”*。

实施SNMP DCA或SNMP DCA BaseMonitor

LTM 系统包括一个 SNMP 数据收集代理，可以查询各种远程 SNMP 代理，其中包括 UC Davis 代理和 Windows 2000 Server 代理。

LTM 系统提供两种 Monitor，通过这两种 Monitor 可以为使用 SNMP 代理的服务器创建性能 Monitor。这两种 Monitor 类型是：

- **SNMP DCA**
  当希望使用缺省值或为 CPU、内存和磁盘指标指定新值时，使用该 Monitor。使用该模板时，也可以为其它希望收集的指标类型指定值。

- **SBMP DCA Base**
  当希望使用缺省值或为 CPU、内存和磁盘使用率以外的指标指定值时，使用该 Monitor。使用该 Monitor 时，省略 CPU、内存和磁盘指标的值。

配置将其 SNMP 代理用于“动态比率”负载平衡的服务器包括以下三项任务：配置 SNMP DCA 或 SNMP DCA BaseMonitor，将该 Monitor 与适用的 Pool 成员相关联，并将 pool 的负载平衡方法设置为“动态比率”方法。有关详细信息，请参阅该指南的以下章节或部分：

- 有关配置 SNMP DCA 或 SNMP DCA BaseMonitor 的详细信息，请参阅第 10 章 *“配置 Monitor ”*。

- 有关将 Monitor 与 pool 相关联的详细信息，请参阅第 4 章 *“配置负载平衡 Pool ”*。

- 有关将 pool 的负载平衡方法设置为“动态比率”方法的详细信息，请参阅第 4 章 *“配置负载平衡 Pool ”*。

实施MSSQLMonitor

使用 MSSQL 类型的 Monitor 之前，必须从微软网站下载一组 JDBC Java™ 档案（JAR）文件，然后将其安装在 BIG-IP 系统上。

下载并安装 Microsoft JDBC 文件的步骤

1. 从互联网浏览器访问 **www.microsoft.com**。
2. 在左侧面板的 Resources 下，点击 **Download**。
   此操作将显示一个列表。
3. 选择 **SQL Server**。
4. 在 **Keyword** 字段中，输入 **JDBC Driver**。
5. 点击 **Go**。
   此操作将显示选项列表。
6. 点击 **Microsoft SQL Server 2000 Driver for JDBC**。
7. 确认下载的是 UNIX **.tar** 文件，而不是 Windows 包。如果不是，返回到上一屏幕。
8. 在屏幕的右侧，点击 **Download**。
9. 查询时，选择 **Save the file to disk**。
10. 创建 Linux 目录，将**.tar** 文件转移到该目录，并使用此命令解压文件：
    tar -xvf mssqlserver.tar。
    此命令可提取四个文件：**EULA.txt**、**install.ksh**、**msjdbc.tar** 和 **read.me**。
11. 通过在命令行提示中输入 **install.ksh** 来安装这些文件。此操作将展开可创建多个子目录的 **msjdbc.tar** 文件。查找 **lib** 子目录。
12. 此目录包含三个前面列出的 JAR 文件。
13. 将这三个 JAR 文件复制到 BIG-IP 目录**/usr/bin/monitors/**。
    现在，可以逐步删除在第 10 步中创建的 LINUX 目录。

B

禁用的 Tcl 命令

- 禁用的 Tcl 命令

禁用的Tcl命令

使用 BIG-IP®本地流量管理（LTM）系统的 iRules™ 特性创建用于管理本地网络流量的脚本时，使用行业标准的工具命令语言（Tcl）。但是，在 LTM 系统上禁止使用 Tcl 命令的子集。因此，编写 iRule 时应避免使用这些命令。

在 LTM 系统上禁止使用的 Tcl 命令是：

- **after**
- **auto_execok**
- **auto_import**
- **auto_load**
- **auto_mkindex**
- **auto_mkindex_old**
- **auto_qualify**
- **auto_reset**
- **bgerror**
- **cd**
- **close**
- **eof**
- **exec**
- **exit**
- **fblocked**
- **fconfigure**
- **fcopy**
- **file**
- **fileevent**
- **filename**
- **flush**
- **gets**
- **glob**
- **http**
- **interp**
- **load**
- **memory**
- **namespace**
- **open**
- **package**
- **pid**
- **pkg::create**
- **pkg_mkIndex**
- **proc**
- **pwd**
- **rename**
- **seek**
- **socket**
- **source**
- **tcl_findLibrary**
- **tell**
- **unknown**
- **update**
- **uplevel**
- **upvar**
- **vwait**

术语表

active unit

在冗余系统中，活动设备是当前装载平衡连接的系统。如果冗余系统中的活动设备发生故障，那么备用设备可进行控制并开始装载平衡连接。请参阅 *“冗余系统”*。

authentication

认证是当用户试图登录到系统时，验证用户身份的过程。

authentication module

认证模块是一种为进行客户机流量的认证或授权而创建的 PAM 模块。请参阅 *“PAM ”*。

authentication profile

认证 Profile 是一种配置工具，使用它可以实施 PAM 认证模块。可以通过认证 Profile 实施的认证模块类型是：LDAP、RADIUS、TACACS+、SSL 客户机证书 LDAP 和 OCSP。请参阅 *“PAM ”*。

authentication iRule

认证 iRule 是系统提供的或用户创建的 iRule，它对在 LTM 系统上实施 PAM 认证模块是必不可少的。请参阅 *“iRule，PAM ”*。

authorization

授权是识别经授权可访问系统资源的登录用户访问级别的过程。

bigtop

bigtop 工具是一种安装在 BIG-IP 系统上的统计监视工具。该工具可提供实时统计信息。

BIND (Berkeley Internet Name Domain)

BIND 是一种最常见的实施域名系统（DNS）的方法。BIND 提供了一个用于将域名和 IP 地址匹配的系统。有关详细信息，请访问 **http://www.isc.org/products/BIND。**

bursting

猝发是指速率调整方面，在流量速率超过定义的基础速率时，就会发生猝发。

certificate

证书是一种由权威认证机构签发的在线证书，用作对 SSL 网络流量进行认证的方法。

certificate authority (CA)

证书授权机构是一个外部权威机构，它对请求计算机系统签发签名的数字证书，用作获取 SSL 网络流量认证的证书。

certificate revocation list (CRL)

证书撤销列表是一种认证系统检查的列表，用来查看是否已撤销请求系

统为获得认证而提供的 SSL 证书。

certificate verification

证书验证是 SSL 握手的一部分，可对权威认证机构已签发的客户机 SSL 证书进行验证。

chain

链是一系列用于限制访问 IP 地址的过滤标准。链中标准的顺序决定了如何应用过滤器，这一应用过程首先从一般性标准开始，一直到链的末端更详细的标准。

chunking

请参阅 *"HTTP 中继"*。

cipher

密码是一种加密/解密算法，当使用 SSL 协议传输数据时计算机系统会使用这种算法。

client-side SSL profile

客户端 SSL Profile 是一种 SSL Profile，可控制 SSL 流量从客户机系统流入 LTM 系统时的行为。

clone pool

该特性使 pool 能够复制所有入站流量，并将这些流量发送到一个复制的 pool。

configuration object

配置对象是用户创建的对象，LTM 系统使用该对象实施 PAM 认证模块。创建的每一种认证模块都有一种配置对象。请参阅 *"PAM 认证模块"*。

Configuration utility

Configuration 工具是用来配置 LTM 系统的基于浏览器的应用。

connection persistence

连接持续性是一种优化技术，凭借该技术，网络连接为减少握手操作而保持开放状态。

connection pooling

连接 Pool 是一种集中服务器端连接，以供其它客户机请求重复使用的优化特性。连接 Pool 可减少必须为服务器端客户机请求而保持开放的新连接的数量。

content switching

通过内容转换，可以基于数据包中的数据选择 pool。

.

cookie persistence

Cookie 持续性是一种持续模式，在这种模式下 LTM 系统将持续连接信息存储在 cookie 中。

custom profile

定制 Profile 就是您创建的 Profile。定制 Profile 可以从指定的上级 Profile 中继承缺省设置。请参阅 *“上级 Profile ”*。

default profile

缺省 Profile 是 LTM 系统提供缺省设置值的 Profile。可以按原状使用缺省 Profile，也可以对它进行修改。创建定制 Profile 时，也可以将其指定为上级 Profile。此外，不能创建或删除缺省 Profile。请参阅 *“Profile，定制 Profile ”*。

default VLAN

可以配置 LTM 系统具有两个缺省 VLAN，各支持一个接口。其中一个缺省 VLAN 命名为**内部**，另一个命名为**外部**。请参阅 *“VLAN ”*。

default wildcard virtual server

缺省通配符 Real Server 有一个 IP 地址和端口号 **0.0.0.0:0.**或***:***或**"any":"any"**。该 Real Server 接受与在配置中定义的任何其它 Real Server 都不匹配的所有流量。

destination address affinity persistence

也称为粘着持续性，目的地地址相关性持续性支持 TCP 和 UDP 协议，完全根据数据包的目的地 IP 地址，将会话请求定向至统一台服务器。

domain name

域名是与一个或多个 IP 地址相关联的唯一名称。域名用于 URL 中识别特殊网页。例如，在 URL **http://www.siterequest.com/index.html** 中，域名是 **siterequest.com**。

Dynamic Ratio load balancing method

“动态比率”模式与“比率”模式相似（参见“比率法”），只是前者的比率权重以持续监控服务器为基础，因此可持续改变。“动态比率”负载平衡可以在 RealNetworks® RealServer 平台、配备了 Windows 管理架构（WMI）的 Microsoft® Windows®平台、或者配备了 UC Davis SNMP 代理或 Windows 2000 Server SNMP 代理的服务器上实施。

EAV (Extended Application Verification)

EAV 是一种状态检查，可通过远程运行应用对节点上的应用进行验证。EAV 状态检查只是 LTM 系统上可用的三种状态检查类型之一。请参阅 *“状态检查，状态 Monitor”和“外部 Monitor”*。

ECV (Extended Content Verification)

ECV 是一种状态检查，它使您能够根据节点是否返回特定内容来确定节点是 **Up** 还是 **Down**。ECV 状态检查只是 LTM 系统上可用的三种状态检查类型之一。请参阅*“状态检查”*。

external authentication

外部认证是指使用远程服务器存储数据，以便对试图访问 LTM 系统的用户或应用进行认证的过程。

external monitor

外部 Monitor 是用户提供的状态 Monitor。请参阅“*状态检查，状态 Monitor*”。

external VLAN

在 BIG-IP 系统上，外部 VLAN 是的一个缺省 VLAN。在基本配置中，这种 VLAN 的管理端口为锁定状态。在标准配置中，这种 VLAN 通常用于外部客户机请求到服务器的连接。

fail-over

故障切换是指当在活动设备上检测到软件故障或硬件故障时，冗余系统中的备用设备接替工作的过程。

fail-over cable

故障切换电缆直接将冗余系统中的两个设备连接在一起。

Fastest method

“最快”模式是一种负载平衡法，可根据当前所有运行节点的最快响应速度传递新的连接。

FDDI (Fiber Distributed Data Interface)

FDDI 是一种以高达 100 Mbps 的速度在光纤电缆上传输数据的多模式协议。

floating self IP address

浮动本机 IP 地址是一种附加的 VLAN 本机 IP 地址，可作为 BIG-IP 冗余系统的两个设备的共享地址。

forwarding virtual server

转换型 Real Server 是一种没有 Pool 成员进行负载平衡的 Real Server。这种 Real Server 能够直接将数据包转发至客户机请求中指定的目的地 IP 地址。请参阅“*Real Server*”。

hash persistence

散列持续性使您能够根据现有 iRule 创建持续性散列。

health check

状态检查是 LTM 系统的一个特性，用于确定节点是**开启**还是**关闭**。状态检查是通过状态 Monitor 实施的。请参阅“*状态 Monitor，ECV，EAV*”和“*外部 Monitor*”。

health monitor

状态 Monitor 检查节点是否**开启**并提供给定的服务。如果节点未能通过检查，就会被标记为**关闭**。不同的 Monitor 用于检查不同的服务。请参阅“*状态检查，EAV，ECV*”和“*外部 Monitor*”。

host virtual server

主机 Real Server 是代表一个具体站点，比如一个互联网站点或一个 FTP 站点的 Real Server，它可以负载平衡以内容服务器（并属于 Pool 成员）为目的地的流量。

HTTP chunking

HTTP 中继是指称为中继编码的 HTTP/1.1 特性，它允许将 HTTP 信息分为几个部分。在发送响应时，服务器经常会使用中继。

HTTP redirect

HTTP 重定向可向客户机发送“找到 HTTP 302 对象”消息。您可以通过 HTTP 重定向配置一个 pool，如果 Pool 成员标记为 **Down**，那么可将客户机发送给另一个节点或 Real Server。

HTTP transformation

当 LTM 系统进行 HTTP 转换时，系统会处理服务器端 HTTP 请求的 **Connection** 标头，以确保连接保持打开状态。请参阅“*连接持续性*”。

ICMP (Internet Control Message Protocol)

ICMP 是一种互联网通信协议，用于确定路由到目的地地址的信息。

i-mode

i-mode®是 NTT DoCoMo 公司创建的一项业务，使移动电话用户能够访问互联网。

interface

接口是 BIG-IP 系统的物理端口。

internal VLAN

内部 VLAN 是 BIG-IP 系统的缺省 VLAN。在基本配置中，这种 VLAN 的管理端口为打开状态。在标准配置中，它可用作一个处理来自内部服务器的连接的网络接口。

IPSEC

IPSEC（互联网安全协议）是一种通信协议，可为互联网的网络层提供安全保护，而不用对运行在其上的应用提出要求。

iRule

iRule 是用户编写的脚本，可控制通过 LTM 系统的连接的行为。iRule 是 F5 Networks 产品的一个特性，经常用于将特定的连接引导至非缺省负载平衡 Pool。然而，iRule 也可执行其他任务，如实施安全网络地址转换和启用会话持续性。

iSNAT (intelligent SNAT)

iSNAT 是使用 iRule，将一个或多个原始客户机 IP 地址映射到转换地址的方法。在编写 iRule 创建 iSNAT 之前，必须首先创建 SANT pool。请参阅“*SANT pool*”。

JAR file

JAR 文件是一种 Java™ 档案（JAR）文件格式的文件，使您能够将多个文件捆绑为一个档案文件。通常，JAR 文件包含类文件及与 applet 和应用相关联的辅助资源。

JDBC

JDBC 是一种 Java™ 技术。它是一种应用编程接口，可提供跨各种 SQL 数据库的数据库管理系统（DBMS）连接，也可访问其它表格数据源，如电子数据表或平面文件。

Kilobytes/Second mode

“千字节/秒”模式是一种动态负载平衡模式，可将连接分配给当前每秒处理流量（千字节）最少的服务器。

last hop

最后中继是到 BIG-IP 系统的连接的最后一次中继。您可以让 BIG-IP 系统自动确定最后中继，以便将数据包发送回原始设备。也可通过使最后中继成为最后中继 pool 的成员来手动指定最后中继。

LDAP (Lightweight Directory Access Protocol)

LDAP 是一种互联网协议，电子邮件程序可以利用该协议从服务器查找联系信息。

LDAP authentication module

LDAP 认证模块是一种用户创建的模块，您可以在 LTM 系统上实施此模块，以便使用远程 LDAP 服务器对客户机流量进行认证。

LDAP client certificate SSL authentication module

LDAP 客户机证书 SSL 认证模块是一种用户创建的模块，您可以在 LTM 系统上实施此模块，以便使用 SSL 客户机证书和远程 LDAP 服务器对客户机流量进行授权。

Least Connections method

“最少连接”模式是一种动态负载平衡方法，可基于当前哪个服务器管理的开放连接最少来分配连接。

load balancing method

负载平衡法是一种决定如何在负载平衡 Pool 中分配连接的特殊方法。

load balancing pool

请参阅 *“pool ”*。

load balancing virtual server

负载平衡 Real Server 是一种可将客户机流量引导至负载平衡 Pool 的 Real Server。这是一种最基本的 Real Server 类型。请参阅*“Real Server”*。

local traffic management (LTM)

本地流量管理（LTM）是指管理流入或流出局域网（LAN，其中包括内联网）的网络流量的过程。

loopback adapter

回路适配器是一种与实际网卡无关的软件接口。nPath 路由配置要求您在服务器上配置回路适配器。

MAC (Media Access Control)

MAC 是一种定义了工作站访问传输媒体方式的协议，在局域网中使用最为广泛。对于 IEEE LAN，MAC 层是数据链路层协议的较低子层。

MAC address

MAC 地址用于表示以太网上的硬件设备。

member

成员是指特殊负载平衡 Pool 中的节点。这种 pool 通常包括多个成员节点。

MindTerm SSH

MindTerm SSH 是 3-DNS 控制器上的第三方应用，使用 SSH 进行安全的远程通信。SSH 可以对所有网络流量（包括密码）进行加密，从而有效地消除了窃听、连接劫持和其它网络攻击。SSH 还提供安全隧道功能和各种认证方法。

minimum active members

最小激活成员数量是指必须在优先组别中运行的成员的数量，以便 LTM 系统向该组别发送请求。如果激活成员的数量低于此数量，请求就会被发送到下一个最高的优先组别（下一个拥有相应最低优先成员数量的优先组别）。

Monitor

LTM 系统使用 Monitor 来确定节点是**开启**还是**关闭**。Monitor 包括几种不同的类型，它们使用不同方法来确定服务器或服务的状态。

monitor association

Monitor 关联是用户在状态或性能 Monitor 和 pool、Pool 成员或节点之间进行的关联。

monitor instance

当状态 Monitor 与 Pool 成员或节点关联时，可以创建 Monitor 实例。状态检查实际上是由 Monitor 实例而不是 Monitor 进行的。

monitor template

Monitor 模板是一种内部机制，当没有预配置 Monitor 时，LTM 系统可使用此机制为定制 Monitor 提供缺省值。

MSRDP persistence

MSRDP 持续性可跟踪那些运行 Microsoft®远程桌面协议（RDP）服务的客户机和服务器之间的会话。

name resolution

名称解析是名称服务器将域名请求和 IP 地址进行匹配，并向请求解析的客户机发送信息的过程。

NAT (Network Address Translation)

NAT 是一个别名 IP 地址，用以标识由 LTM 系统管理的到外部网络的具体节点。

network virtual server

网络 Real Server 是指 IP 地址的主机部分中没有位元（bits set）的 Real Server（即其 IP 地址的主机部分为 0）。网络 Real Server 有两种类型：根据一系列目的地 IP 地址引导客户机流量的服务器，以及根据 LTM 系统不能识别的具体目的地 IP 地址引导客户机流量的服务器。

node

节点地址是与一个或多个节点关联的 IP 地址。这个 IP 地址可以是网络服务器的真实 IP 地址，也可以是网络服务器的别名 IP 地址。

node alias

节点别名是 LTM 系统用于验证多个节点状态的节点地址。当 LTM 系统使用节点别名检查节点状态时，会 ping 通节点别名。如果 LTM 系统收到 ping 响应，就会将所有与节点别名关联的节点标记为 **Up**。如果 LTM 系统没有收到 ping 响应，就会将所有与节点别名关联的节点标记为 **Down**。

node port

节点端口是由特定节点托管的端口号或服务名称。

node status

节点状态是指节点处于可接收连接的 **Up** 状态，还是不可用的 **Down** 状态。LTM 系统使用节点 ping 和状态检查特性来确定节点的状态。

Observed method

“观察”模式是一种动态负载平衡法，可基于结合了以下两个因素的服务器来分配连接：当前托管的连接数量最少，而且响应速度最快。

OCSP (Online Certificate Status Protocol)

OCSP 是一种协议，认证系统可使用此协议来检查数字签名 SSL 证书的撤销状态。使用 OCSP 可替代使用证书撤销列表（CRL）。请参阅“*证书撤销列表（CRL）*”。

OCSP authentication module

OCSP 认证模块是一种用户创建的模块，您可以在 LTM 系统上实施此模块，以便使用远程 OCSP 响应器对客户机流量进行认证。OCSP 认证模块用于检查客户机 SSL 证书的撤销状态。

OCSP responder

OCSP 响应器是一种外部服务器，用于 SSL 证书撤销状态与认证服务器（如 LTM 系统）之间的通信。

OCSP responder object

响应器对象是一种 LTM 系统上的软件应用，可与 OCSP 响应器通信，以便检查客户机或服务器 SSL 证书的撤销状态。

OneConnect™

F5 Networks OneConnect™ 特性通过保持服务器端连接打开并将它们集中起来以便重新使用，可优化网络连接的使用。

packet rate

数据包速率是指服务器每秒处理数据包的数量。

PAM (Pluggable Authentication Module) module

PAM 模块是一种软件模块，服务器应用可使用该模块对客户机流量进行认证。PAM 模块的模块化设计使企业能够在基本不影响应用的情况下，添加、替换或从服务器应用删除该认证机制。PAM 模块的一个例子就是使用远程小型目录访问协议（LDAP）服务器对客户机流量进行认证。请参阅*"LDAP（小型目录访问协议）"*。

parent profile

上级 Profile 是可将其值传播到另一个 Profile 的 Profile。上级 Profile 既可以是缺省 Profile，也可以是定制 Profile。请参阅*"Profile"*。

performance monitor

性能 Monitor 可收集统计信息并检查目标设备的状态。

persistence

请参阅*"连接持续性"*或*"会话持续性"*。

persistence profile

持续性 Profile 是用于实施特定类型的会话持续性的配置工具。持续性 Profile 类型的例子是 cookie 持续性 Profile。

pipelining

流水线技术是 HTTP/1.0 的一个特性，允许客户机在还没有从服务器收到对之前请求的响应的情况下，再次发送请求。

pool

pool 由一组网络设备（又称为成员）构成。LTM 系统会根据创建 pool 或编辑其属性时选择的负载平衡方法和持续性方法，向 pool 中的节点发出负载平衡请求。

pool member

Pool 成员是一种属于负载平衡 Pool 成员的服务器。

port

端口可以用与主机支持的特定服务相关联的编号来表示。关于端口编号和相应服务，请参阅*"服务和端口索引"*。

port mirroring

端口镜像是一种使您能够从任意一个或一组端口将流量复制到窃听设备连接的一个独立端口的特性。

port-specific wildcard virtual server

指定端口的通配符 Real Server 是指使用 0 以外的端口号的 Real Server。请参阅*"通配符 Real Server"*。

pre-configured monitor

预配置 Monitor 是系统提供的状态或性能 Monitor。您可以按原状使用预配置 Monitor，但是不能对其进行修改或删除。请参阅*"Monitor"*。

Predictive method

"预测"法是一种动态负载平衡法，可基于结合了以下两个因素的服务器来分配连接：当前托管的连接数量最少，而且响应速度最快。采用"预测"法，还可以对随时间变化的服务器性能进行分级，并且将连接传递到显示性能提高而非下降的服务器。

Profile

Profile 是一种配置工具，其中包含了用于定义网络流量行为的设置。LTM 系统包含用于管理 FastL4、HTTP、TCP、FTP、SSL 和 RTSP 流量以及用于实施持续性和应用认证的 Profile。

profile setting

Profile 设置 Profile 内一种属性，该 Profile 具有与其关联的值。您可以对 Profile 设置进行配置，以定制 LTM 系统管理流量类型的方式。

profile type

Profile 类型是可用于特定目的的某类 Profile。Profile 类型的例子是 HTTP Profile，您可以对该 Profile 进行配置，以管理 HTTP 网络流量。

protocol profile

协议 Profile 是一种为控制 FastL4、TCP、UDP、OneConnect 和 RTSP 流量的行为而创建的 Profile。

Quality of Service (QoS) level

服务质量（QoS）级别是网络设备用来根据标识符确认和区别对待流量的一种方法。从根本上说，在数据包中指定的 QoS 级别加强了该数据包的吞吐率要求。

RADIUS (Remote Authentication Dial-in User Service)

RADIUS 是进行远程用户认证和账户管理的服务。虽然此服务也可用于任何需要对其工作站进行集中认证和/或提供账户管理服务的网络，但是

它的主要使用者是互联网服务提供商。

RADIUS authentication module

RADIUS 认证模块是一种用户创建的模块，您可以在 LTM 系统上实施此模块，以便使用远程 RADIUS 服务器对客户机流量进行认证。

rate class

可以使用 Configuration 工具或命令行工具创建速率过滤器。当将速率等级分配到速率过滤器时，速率等级会决定允许通过速率过滤器的流量大小。请参阅“*速率调整*”。

rate shaping

速率调整是一个扩展 IP 过滤器类型。速率调整使用同一种 IP 过滤方法，但只应用可决定允许的网络流量大小的速率等级。请参阅“*速率等级*”。

ratio

比率是一个为了实现负载平衡，向 Real Server 分配权重的参数。

Ratio method

“比率”负载平衡法按照分配到每个独立 Real Server 的比率权重对一组 Real Server 分配连接。

Real-Time Stream Protocol (RTSP)

请参阅“*RTSP*”。

receive expression

接收表达式是在扩展内容验证（ECV）状态检查期间，LTM 系统在 Web 服务器返回的网页中搜索的文本字符串。

redundant system

冗余系统指为故障切换而配置的一对设备。在冗余系统中，这两个设备中的一个作为活动设备运行，另一个作为备用设备运行。如果活动设备发生故障，备用设备就会接替工作并管理连接请求。

remote administrative IP address

远程管理 IP 地址是 BIG-IP 系统允许 shell 连接的 IP 地址，如 Telnet 或 SSH。

responder object

请参阅“*OCSP 响应器对象*”。

RFC 1918 addresses

RFC 1918 地址是 IETF RFC 1918 中描述的、在不可路由的地址范围之内的地址。

Round Robin mode

“Round Robin”模式是一种按照服务器顺序分配连接的静态负载平衡模式。“Round Robin”模式可将连接请求发送到序列中的下一个可用服务

器。

RTSP

RTSP（实时流协议）可建立和控制一个或多个连续媒介（如音频或视频）的时间同步流。

secure network address translation (SNAT)

请参阅 *“SNAT ”*。另请参阅*“iSNAT”*。

self IP address

本机 IP 地址是用于访问内部和外部 VLAN 的 BIG-IP 系统拥有的 IP 地址。

Send String

发送字符串是在扩展内容验证（ECV）状态检查期间，LTM 系统发送到 Web 服务器的请求。

server-side SSL profile

服务器端 SSL Profile 是控制 LTM 系统和目的地服务器系统之间 SSL 流量流动的 SSL Profile。

service

服务是指诸如 TCP、UDP、HTTP 和 FTP 等服务。

services profile

服务 Profile 是 LTM 系统上的配置工具，用于管理 HTTP 或 FTP 网络流量。

session persistence

会话持续性是指一系列从同一个客户机接收的相关连接，这些连接具有相同的会话 ID。当启用了持续性时，LTM 系统会将具有相同会话 ID 的连接发送到同一个节点，而不是对连接进行负载平衡。切记，不能将会话持续性与*连接持续性*混淆。

Setup utility

“设置”工具可指导您完成初始系统配置过程。您可以从 Configuration 工具的起始页运行“设置”工具。

simple persistence

请参阅“*源地址相关持续性*”。

SIP persistence

IP 持续性是用于服务器的持续性类型，这些服务器可接收通过 UDP 发送的会话启动协议（SIP）消息。SIP 是一种支持实时消息传递、话音、数据和视频的协议。

SNAT (Secure Network Address Translation)

SNAT 是一种可以在 LTM 系统上配置的协议。SNAT 定义了一个可路由

的别名 IP 地址。在连接到外网主机时，一个或多个节点可使用它作为源 IP 地址。请参阅“*标准 SNAT 和 iSNAT*”。

SANT pool

SANT pool 是一种转换地址 pool，可映射到一个或多个原始 IP 地址。SANT pool 中的转换地址不是本机 IP 地址。

SNMP (Simple Network Management Protocol)

SNMP 是 STD 15、RFC 1157 中定义的互联网标准协议，用于管理 IP 网络上的节点。

source address affinity persistence

也称为简单持续性，源地址相关持续性支持 TCP 和 UDP 协议，完全根据数据包的源 IP 地址，将会话请求引导到同一台服务器。

source processing

源处理表示接口对入站数据包的源进行重写。

spanning tree protocol (STP)

生成树协议是一种在配置中提供回路解析的协议。在这些配置中，一个或多个外部交换机与 BIG-IP 系统并行连接。

SSH

SSH 是一种支持安全远程登录和非安全网络上其它安全网络服务的协议。

SSL (Secure Sockets Layer)

SSL 是一种采用公钥技术安全地传输数据的网络通信协议。

SSL persistence

SSL 持续性是使用 SSL 会话 ID 来跟踪非端接 SSL 会话的持续性类型。

SSL Profile

SSL Profile 是一种配置工具，用于从客户机或服务器终止和启动 SSL 连接。

standard SNAT

标准 SNAT 是使用 Configuration 工具的 SNAT 屏幕实施的 SNAT。请参阅“*SNAT 和 iSNAT*”。

standby unit

冗余系统中的备用设备是指如果活动设备发生故障，随时准备成为活动设备的设备。

state mirroring

状态监视是 LTM 系统的一种特性，可保存冗余系统的连接和持续性信息。

sticky persistence

请参阅“*目的地地址相关持续性*”。

subdomain

子域是较高级别域的子部分。例如，**.com** 是高级别域，**F5.com** 是**.com** 域的子域。

TACACS (Terminal Access Controller Access Control System)

TACACS 是 UNIX 系统常用的早期认证协议。TACACS 允许远程访问服务器将用户的登录密码转发到认证服务器。

TACACS+

TACACS+是为取代早期 TACACS 协议而设计的认证机制。然而，这两个协议几乎没有相似之处，因而彼此并不兼容。

TACACS+ authentication module

TACACS+认证模块是一种用户创建的模块，您可以在 LTM 系统上实施此模块，以便使用远程 TACACS+服务器对客户机流量进行认证。

tagged VLAN

您可以将任何接口定义为标记 VLAN 的一个成员。您可以为每个标记接口创建一个 VLAN 标记或名称列表。请参阅“*VLAN*”。

Tcl

Tcl（工具命令语言）是一种行业标准的脚本语言。在 LTM 系统上，用户可以使用 Tcl 编写 iRules™。

transparent node

透明节点是路由到其他网络设备（包括 BIG-IP 系统）的路由器。

trunk

中继是配置为一个链路的两个或多个接口和线缆的组合。

trusted CA file

可信 CA 文件是包含当处理客户机认证请求时，认证系统可以信任的证书授权列表的文件。可信 CA 文件位于认证系统中，用于对 SSL 网络流量进行认证。

Type of Service (ToS) level

除了服务质量（QoS）级别外，服务类型（QoS）级别是另一种网络设备用来根据标识符确认和区别对待流量的方法。

Universal Inspection Engine (UIE)

通用检查引擎（UIE）是一种提供通用持续性和通用内容交换的特性，可以增强负载平衡能力。UIE 包含一组规则变量和函数，用于构建在 pool 定义和规则中指定的表达式。

universal persistence

通用持续性使您能够持续获得在数据包中找到的任何字符串。此外，您也可以直接选择希望持续存在的 Pool 成员。

virtual address

虚拟地址是与 LTM 系统管理的一个或多个 Real Server 相关联的 IP 地址。

virtual port

虚拟端口是与 LTM 系统管理的一个或多个 Real Server 相关联的端口号或服务名称。虚拟端口号应该与客户机程序连接的 TCP 或 UDP 端口号相同。

Real Server

Real Server 是虚拟地址和虚拟端口的特定组合，与由 LTM 系统或其他类型的主机服务器管理的内容站点相关联。

VLAN

VLAN 是指虚拟局域网。VLAN 是网络设备的逻辑分组。您可以使用 VLAN 对不同网段上的设备进行逻辑分组。

VLAN name

VLAN 名称是用于识别 VLAN 的符号名称。例如，可以将 VLAN 命名为市场部 VLAN 或开发部 VLAN。请参阅*"VLAN"*。

watchdog timer card

watchdog 计时卡是监控 BIG-IP 系统硬件故障的硬件设备。

wildcard virtual server

通配符 Real Server 是使用 IP 地址 **0.0.0.0**、*****或"**any**"的 Real Server。通配符 Real Server 接受本地网外部目的地的连接请求。只有在透明节点模式配置中包括通配符 Real Server。

WKS (well-known services)

常用服务是广泛用于特定数据类型的端口 0 到端口 1023 上的协议。常用服务及其相应端口的例子包括：HTTP（80 端口）、HTTPS（443 端口）和 FTP（20 端口）。

索引