服务响应监视器

用户指南

版本 5.8

本文档包括内嵌帮助系统和以电子形式分发的材料（以下简称“文档”），其仅供参考，CA 随时可对其进行更改或撤销。

未经 CA 事先书面同意，不得擅自复制、转让、翻印、透露、修改或转录本文档的全部或部分内容。本文档属于 CA 的机密和专有信息，不得擅自透露，或除以下协议中所允许的用途，不得用于其他任何用途：(i) 您与 CA 之间关于使用与本文档相关的 CA 软件的单独协议；或者 (ii) 您与 CA 之间单独的保密协议。

尽管有上述规定，但如果您为本文档中所指的软件产品的授权用户，则您可打印或提供合理数量的本文档副本，供您及您的雇员内部用于与该软件相关的用途，前提是所有 CA 版权声明和标识必须附在每一份副本上。

打印或提供本文档副本的权利仅限于此类软件所适用的许可协议的有效期内。如果该许可因任何原因而终止，您应负责向 CA 书面证明已将本文档的所有副本和部分副本已退还给 CA 或被销毁。

在所适用的法律允许的范围内，CA 按照“现状”提供本文档，不附带任何保证，包括但不限于商品适销性、适用于特定目的或不侵权的默示保证。CA 在任何情况下对您或其他第三方由于使用本文档所造成的直接或间接的损失或损害都不负任何责任，包括但不限于利润损失、投资受损、业务中断、信誉损失或数据丢失，即使 CA 已经被提前明确告知这种损失或损害的可能性。

本文档中涉及的任何软件产品的使用均应遵照有关许可协议的规定且根据本声明中的条款不得以任何方式修改此许可协议。

本文档由 CA 制作。

仅提供“有限权利”。美国政府使用、复制或透露本系统受 FAR Sections 12.212、52.227-14 和 52.227-19(c)(1) - (2) 以及 DFARS Section 252.227-7014(b)(3) 的相关条款或其后续条款的限制。

版权所有 © 2013 CA。保留所有权利。此处涉及的所有商标、商品名称、服务标识和徽标均归其各自公司所有。

CA Technologies 产品引用

本文档引用以下 CA Technologies 产品：

- CA eHealth®
- CA Embedded Entitlements Manager (CA EEM)
- CA IT Asset Manager (CA ITAM)
- CA IT Client Manager (CA ITCM)
- CA Network and Systems Management (CA NSM)
- CA Patch Manager
- CA Server Automation
- CA Service Desk Manager (CA SDM)
- CA Spectrum®
- CA SystemEDGE
- CA Systems Performance for Infrastructure Managers
- CA Virtual Assurance for Infrastructure Managers
- CA Software Delivery

联系技术支持

要获取在线技术帮助以及办公地址、主要服务时间和电话号码的完整列表，请联系技术支持：http://www.ca.com/worldwide。

目录

第 1 章： 简介 9

范围 9
读者 9
相关出版物 9
约定 10

第 2 章： 功能特征 13

概述 13
体系结构 15
测试表信息 16
文件加密 18
控制文件处理 18
在可用性表中保留行 19
性能度量标准 19
示例：向 SRM AIM 应用文件 I/O 测试 20
- 确定配置文件 I/O 测试的方法 21
- 通过 UI 创建文件 I/O 测试 22
- 通过 UI 应用文件 I/O 测试 30
- 通过 CLI 创建、运行和应用文件 I/O 测试 32
- 文件 I/O 测试错误代码 37

第 3 章： 配置 39

编辑控制文件 39
- 全局参数块 42
- 测试定义参数块 45
- 监视器模板定义参数块 50
- 抽样配置文件 53

第 4 章： 测试管理 57

创建测试 57
- 选项和参数 60
- Active Directory 测试 60
- 自定义测试 63
- DHCP 测试 65
- DNS 测试 66
- 文件 I/O 测试 68

FTP 测试 74
HTTP 测试 76
HTTPS 测试 81
IMAP 测试 84
LDAP 测试 86
MAPI 测试 89
NIS/NIS+ 测试 93
NNTP 测试 95
ping 测试 97
POP3 测试 98
往返电子邮件测试 100
SMTP 测试 103
SNMP 测试 107
SQL 查询测试 112
TCP 连接测试 117
TFTP 测试 119
虚拟用户测试 122
测试的关键字 126
使用自定义脚本创建测试 132

附录 A： 服务响应监视器 CLI 命令 135

svcwatch add adir 命令-添加 Active Directory 测试 136
svcwatch add custom 命令-添加自定义测试 141
svcwatch add dhcp 命令-添加 DHCP 测试 146
svcwatch add dns 命令-添加 DNS 测试 151
svcwatch add fileio 命令-添加文件 IO 测试 156
svcwatch add ftp 命令-添加 FTP 测试 161
svcwatch add http｜ https 命令-添加 HTTP 或 HTTPS 测试 166
svcwatch add imap 命令-添加 IMAP 测试 172
svcwatch add ldap 命令-添加 LDAP 测试 177
svcwatch add mapi 命令-添加 MAPI 测试 182
svcwatch add nis 命令-添加 NIS 测试 188
svcwatch add nntp 命令-添加 NNTP 测试 193
svcwatch add ping 命令-添加 PING 测试 198
svcwatch add pop3 命令-添加 POP3 测试 203
svcwatch add rtemail 命令-添加往返电子邮件测试 208
svcwatch add smtp 命令-添加 SMTP 测试 214
svcwatch add snmp 命令-添加 SNMP 测试 219
svcwatch add sql 命令-添加 SQL 测试 225
svcwatch add tcpconnect 命令-添加 TCP 连接测试 231
svcwatch add tftp 命令-添加 TFTP 测试 236
svcwatch add vuser 命令－添加虚拟用户测试 241

svcwatch delete 命令-删除测试 246
svcwatch list 命令-查看测试信息 249
svcwatch setstatus 命令-更改测试状态 252
svcwatch version 命令-查看 SRM 版本信息 255

附录 B： 安装 259

通过 CA Virtual Assurance 设置的安装 259
远程部署 259
单个安装 261
升级 262
从 Windows 上卸载 262
从 Linux 或 UNIX 上卸载 263

附录 C： 错误代码 265

错误代码概述 265
常规错误代码 267
A 至 H 错误代码 268
I 至 R 错误代码 274
S - Z 错误代码 282

索引 289

第 1 章： 简介

此部分包含以下主题：

范围 (p. 9)
读者 (p. 9)
相关出版物 (p. 9)
约定 (p. 10)

范围

该指南说明了如何安装、配置和使用 CA Virtual Assurance 服务响应监控 Application Insight Module (SRM AIM)。

该指南描述了 AIM 的逐步测试配置。

读者

本指南适用于安装、配置和使用 CA Virtual Assurance 来管理虚拟环境的管理员。本指南假定您熟悉环境中所使用的操作系统、虚拟化技术和 SNMP。

相关出版物

CA Virtual Assurance 文档包括以下交付成果：

管理指南

了解如何管理和使用 CA Virtual Assurance 以在您的环境中管理虚拟资源。

安装指南

包含简短的体系结构信息、各种安装方法、后继安装配置信息以及入门说明。

联机帮助

提供有关窗口详细信息和程序说明，以便使用 CA Virtual Assurance 用户界面。

参考指南

提供有关 AutoShell、CLI 命令、MIB 属性的详细信息。

性能度量标准参考

说明可用于监控支持的平台的系统性能的性能度量标准。

版本说明

提供有关操作系统支持、系统要求、已发布的修正、国际化支持、已知问题以及文档路线图。

服务响应监控用户指南

提供 SRM 的安装和配置详细信息。

SystemEDGE 用户指南

提供 SystemEDGE 的安装和配置详细信息。

SystemEDGE 版本说明

提供有关操作系统支持、系统要求和功能的信息。

约定

本指南使用以下约定：

区分大小写

在本指南中提到的所有类、命令、指令、环境参数、函数和属性的名称均区分大小写，您必须按显示的形式正确拼写它们。- 系统命令和环境变量名称 *可能*区分大小写，视操作系统的要求而定。-

交叉引用

对其他指南或本指南其他部分中信息的引用采用以下格式：

指南名称

指示其他指南的名称。

“章名称”

表示本指南或其他指南中的章节名称。

同义词

属性、对象和对象标识符 (OID) 等术语与本文档中的术语“变量”是同义的。

SystemEDGE 代理和 CA SystemEDGE 等术语与本文档中的 SystemEDGE 是同义的。

语法

语法和用户输入使用以下格式：

斜体

表示必须为其提供实际值的变量名或占位符。

{a|b}

表示选择强制性操作数（a 或 b）。

[ ] 或 [[ ]]

表示可选操作数。

语法示例

以下示例使用这些约定：

```
modify -t ZONE [-m zoneserver] -p psetname {-min mincpu|-max maxcpu} pset
-session ssh
```

操作数 -min 和 -max 是强制性的，但您可以只使用二者之一，具体视希望定义处理器集中 CPU 的最小数量还是最大数量而定。操作数 -m 不是该命令运行所必需的。该命令的所有其他部分必须按显示的形式进行输入。

默认目录

在路径语句中使用的 *CASYSEDGE* 表示在其中安装 SystemEDGE 的目录。**默认值：**C:\Program Files\CA\SystemEDGE。

安装路径

在路径语句中使用的 *Install_Path* 表示在其中安装 CA Virtual Assurance 或 CA Virtual Assurance 组件的目录。

默认值：

- Windows x86：C:\Program Files\CA
- Windows x64：C:\CA、C:\Program Files (x86)\CA 或 C:\Program Files\CA
- UNIX、Linux：/opt/CA

第 2 章： 功能特征

此部分包含以下主题：

概述 (p. 13)
体系结构 (p. 15)
测试表信息 (p. 16)
文件加密 (p. 18)
控制文件处理 (p. 18)
在可用性表中保留行 (p. 19)
性能度量标准 (p. 19)
示例：向 SRM AIM 应用文件 I/O 测试 (p. 20)

概述

以下列表提供了有关 SRM 功能特征的概述。

状态管理

SRM 全面支持 SystemEDGE 的状态对象模型。您可以在配置文件中为关联的度量标准配置阈值和重要级别。

基于文件的配置、策略配置

您可以通过 CA Virtual Assurance 中的“策略配置”配置 SRM。该“策略配置”基于文件并提供以下热启动功能：

- 支持交付新的 SRM 控制文件时 SystemEDGE 触发的热启动。
- 允许在交付新的配置文件时 SRM 即时挂起执行并重新配置自身。

注意：有关如何执行策略配置的详细信息，请参阅 CA Virtual Assurance 联机帮助。

远程部署

运行 SRM 所需的所有组件（SRM AIM、高级加密、SystemEDGE）均可从 CA Virtual Assurance 管理器进行远程部署和安装。另请参阅“附录安装”。

传统兼容性

SRM 接受并收集 SRM 2.0 或 2.1 版收集的所有数据度量标准。SRM 可以使用 2.x 版本的配置文件。另请参阅该指南中的“附录安装”。

日志文件自定义

通过 SRM，您可以配置日志文件的名称、大小和数目。

命名的测试

SRM 支持配置有可以用于标识的测试名称的测试。

性能优化

性能度量标准提供有关 SRM AIM 功能的实时性能信息。您可以手动监控 SRM AIM 运行状况，或通过 SystemEDGE 完成该操作。您可以调整配置信息以从 SRM 获取最佳响应。

运行一次

SRM 支持仅在要求时运行测试，而不是通过轮询间隔排定程序运行测试。

基于 SNMP 的配置

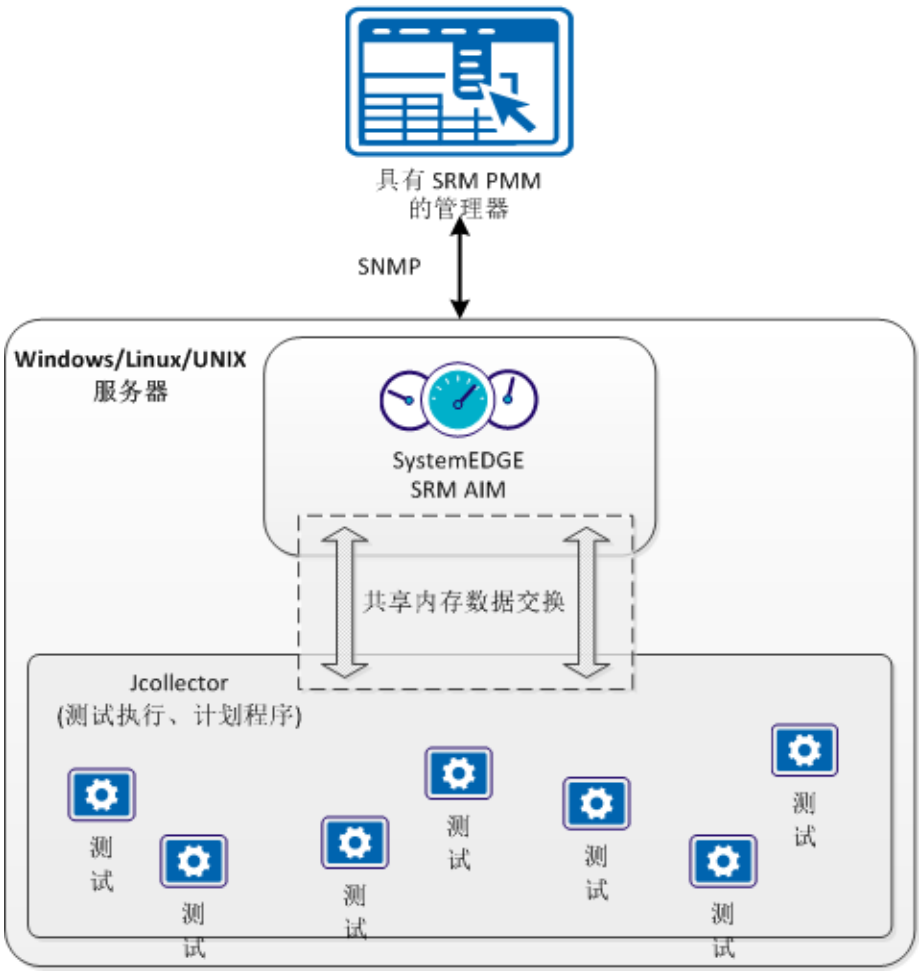
SRM 在其测试内支持 IPv6 和 SNMPv3。

体系结构

Service Response Monitoring Application Insight Module (SRM AIM) 是 SystemEDGE 版本 5.0 的功能扩展（插件）。SRM 检索运行在本地或远程系统上的逻辑或物理服务的响应。SRM 基于 Java，是多线程的，可处理跨多个服务器的多个测试配置。SRM 执行预配置或自定义的测试，以测量执行所需的时间和吞吐量。

下图说明了这些关系。

服务响应监控组件之间的交互



svcrsp.cf 配置文件包含测试规格。SRM AIM 将读取该配置文件，并使测试规格在共享内存段中可用。SRM Jcollector 组件从共享内存中读取每个测试配置。Jcollector 执行测试，收集此计时进程的结果，然后将结果传播到 SRM AIM。SystemEDGE 将这些结果和关联的状态信息发送到 CA Virtual Assurance。

测试表信息

需要具备监控特定度量标准和指定关联监视器重要级别的功能才能进行有效的 SRM 状态管理。

SRM 测试表存储以下信息：

测试实例名称

（可选）为测试指定测试实例名。该名称用于状态管理器对象信息、性能数据集合的资源实例信息，以及作为测试主键的随机整数*索引*（可能会根据所提供模板而变化）的备用内容。最优选择是使用一个非空测试名，但是仅对基于文件的配置（配置文件为 3.0 版或更高版本）是强制性的。SRM 保留传统支持。

注意：该值仅在创建测试时是可写的。测试创建完成后将无法修改，因为该值充当表的主键。

服务上下文信息

指定一个位置以存储管理员要存储的任何信息，如该测试对象的 UUID、标志、祖先项属性等。SRM 不直接将该信息用于任何功能，但会将这些信息作为任意管理员通知的一部分进行传递。但是，管理员可以使用该信息将测试结果发送到适当的受监控设备。例如，DNS 测试可以与实际的 DNS 设备关联，而不是与运行 DNS 测试的计算机关联。

测试类名称

（可选）为测试指定测试类名称。该名称用于状态管理器对象信息、性能数据集合的资源实例信息以及在测试时创建的监视器对象信息。

注意：该值仅在创建测试时是可写的。测试创建完成后将无法修改，因为该值充当表的主键。

日志级别

指定执行测试的代码的日志级别。如果该参数没有值或具有无效值，则会使用全局 SRM 日志级别。可能的值为：

-1－无记录

0－记录致命级别消息

1－同时记录严重级别消息

2－同时记录警告级别消息

3－同时记录信息级别消息

4－同时记录调试级别消息

5－同时记录 debug1 级别消息

6－同时记录 debug2 级别消息

7－同时记录 debug3 级别消息

注意：如果 HTTP 监视器启用了高级别记录功能，则 CPU 使用率会迅速上升。除极端情况外，建议将记录级别设置为低或中等。

标志

（可选）指定以下标志：

默认标志

指定“最佳实践”解决方案。

0x0001 [cube_collect]

表明该测试是否收集历史性能分析数据，以支持 Unicenter NSM 系统性能报告和分析。如果设置该标志，SRM 将添加启用多维收集的 emphistory 条目来监控固定的一组 SRM 度量标准，以用于测试。默认情况下不添加这些条目。有关 emphistory 的详细信息，请参阅 *《SystemEDGE 用户指南》*。

0x0100 [run_once]

表明该测试仅在要求时运行。不受轮询间隔排定程序控制。

SystemEDGE 监视器表包含用于 SRM 测试的监视器。SystemEDGE 监视器创建过程支持通过 SE-OID-helper 功能创建 SRM 监视器。该帮助程序要求“SE 类”、“实例”和“属性”分别填入 TestType、TestInstance 和 TestMetric，例如，Class=Http、Instance=MyHomePage、Attribute=Overall Response Time。该帮助程序检测对应的度量标准 OID，将其插入 SystemEDGE 监视器 OID 属性，并创建监视器。

注意：有关详细信息，请参阅 *《SystemEDGE 用户指南》*。

文件加密

SRM 可以将配置文件作为整体进行加密或仅加密个别敏感值。

只有当 SystemEDGE 处于受管模式时，才能将整个文件进行加密。如果在配置或重新配置时，svcrsp 接收到加密的输入配置文件，它也会加密修改后的配置文件。任何后续更改都会保持文件的加密状态。

部分加密总是存在的。当写入到 svcrsp.cf 文件时，测试密码参数始终是加密的。

SystemEDGE 对加密机制的详细信息进行处理。SRM 无权访问加密或解密密钥。SRM 始终使用 SystemEDGE 的解密功能访问配置文件，无论文件是否加密。

控制文件处理

当您将测试添加到配置文件时，请考虑以下步骤。

将测试添加到配置文件

1. 关闭 SystemEDGE 代理以编辑 svcrsp.cf 文件。
2. 将处于活动状态或 notInService 状态的测试添加到 svcrsp.cf 文件。
3. 存储文件并启动 SystemEDGE。

在该阶段，SystemEDGE 和 SRM 执行下列步骤：

1. SRM 解析 svcrsp.cf 文件并进行初始化。
2. 如果发生任何严重错误（如无效 java 路径），配置将会失败，SystemEDGE 将会禁用 AIM。
3. 如果任何测试配置无效或测试状态不是活动状态或 notInService 状态，SRM 将不会创建测试并将其从配置文件删除。
4. SRM 将测试移交给启动测试的 Jcollector 进程。
5. SRM 每 30 秒更新一次测试结果。

您可以在测试运行时通过 SNMP 更改大部分测试参数（名称、类等除外）。

在可用性表中保留行

使用该功能允许从本地添加的测试和 SNMP 管理器添加的测试共存。

SNMP 管理器或用户应按照这些步骤通过 SNMP 添加新的测试：

1. 获取第一个未使用的测试索引：来自 svcrsp.asn1 MIB 的 svcRspUnusedIndex SNMP 变量。
2. 使用该索引创建新的测试。

使用 reserved_range 全局参数确保 svcRspUnusedIndex 绝不会返回用于通过其他手段添加的测试的索引。

性能度量标准

性能度量标准组提供一个计数器，该计数器在排定测试未在分配时间内完成时递增。另外一个计数器记录测试运行的次数。随着时间的推移跟踪这些计数器将会发现 SRM 配置是否需要调整的有用迹象。性能度量标准提供有关 SRM AIM 功能的实时性能信息。您可以手动监控 SRM AIM 运行状况，或通过 SystemEDGE 完成该操作。您可以调整配置信息以从 SRM 获取最佳响应。

svcRspPrfReset

指定枚举的整数（1 = 确定，2 = 重置）允许最终用户为 AIM 重置所有性能计数器。设置重置 (2) 时，所有计数器设置为零 (0)，且该条目设置回“确定” (1)。

svcRspPrfRuns

表示 AIM 启动或计数器重置以来完成的执行间隔总数。

svcRspPrfLateRuns

表示 AIM 启动或计数器重置以来延迟的执行间隔总数。

svcRspPrfConsLate

表明已延迟的最后连续间隔的数目。应为 1 或 0，大于 1 的数字表示系统延迟。svcRspPrfConsLate 将以 late_exec_runs 当前值与先前 SystemEDGE 间隔的读数的差额（最大为 1）进行递增，并在首次更新（差额为 0）时重置为 0。

示例：向 SRM AIM 应用文件 I/O 测试

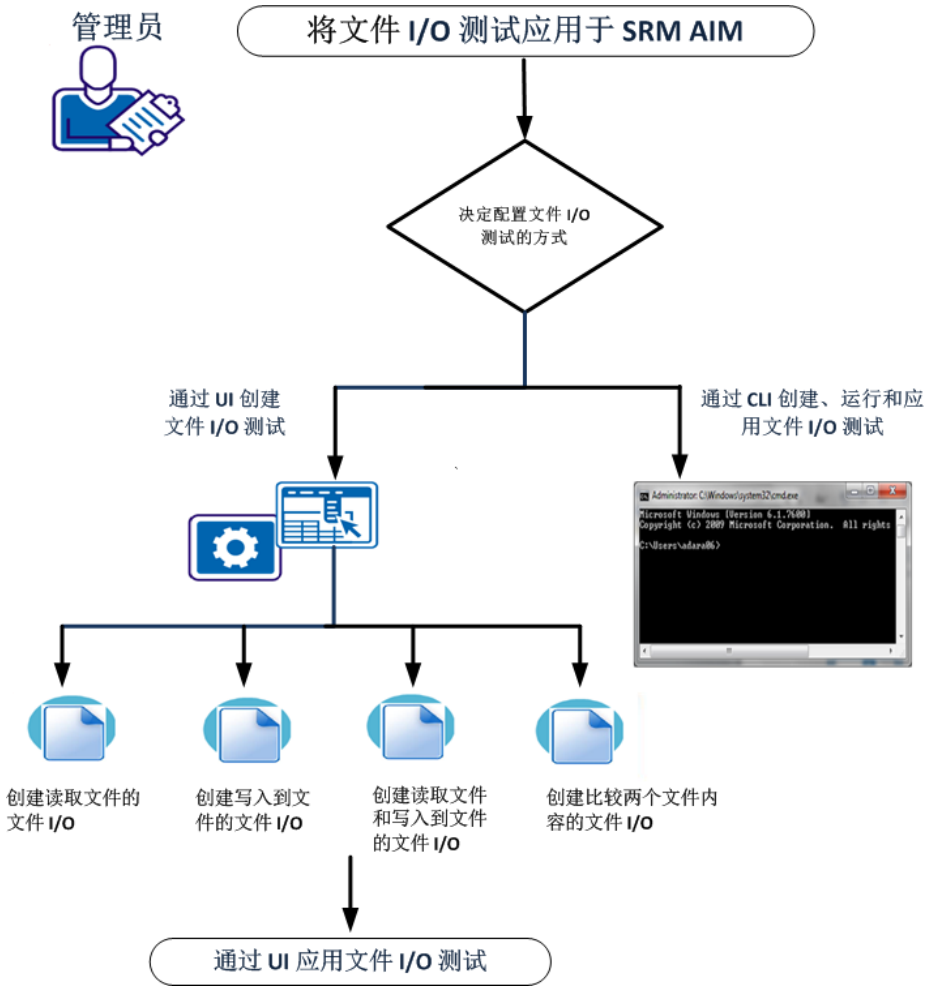
作为 CA Virtual Assurance 管理员，您的职责包括安装、维护、部署和配置服务响应监控应用程序审视模块 (SRM AIM)。SRM AIM 运行预配置或自定义的测试，以测量执行花费的时间和吞吐量。

CA Virtual Assurance 可以通过首先创建文件 I/O 测试然后将其应用到 SRM AIM 来帮助自动化这些活动。文件 I/O 测试监控在 NFS 或 SMB 文件系统上执行操作所需的时间长度。

对 SRM AIM 执行的文件 I/O 测试检索运行在本地或远程系统上的逻辑或物理服务的响应。每个示例测试每 30 秒运行一次，如果操作不成功，则在 10 秒之后超时。响应和可用性的统计信息每间隔 120 秒计算一次。管理员根据这些结果监控并管理虚拟网络的运行状况。

重要信息：SRM AIM 以 root 用户身份运行，所以文件 I/O 测试可能会写入 /etc/passwd 或 boot.ini 文件并使系统瘫痪。创建和启用这些测试时应十分谨慎。/sysedge/plugins/svcrsp 目录中存在示例测试文件。

该方案将指导您完成将文件 I/O 测试应用到 SRM AIM 的过程：



选择以下方法之一配置文件 I/O 测试：

- 通过 UI 创建文件 I/O 测试 (p. 22)
- 通过 CLI 创建、运行和应用文件 I/O 测试 (p. 32)

通过 UI 创建文件 I/O 测试时，您需要通过用户界面单独应用该测试。

- 通过 UI 应用文件 I/O 测试 (p. 30)

确定配置文件 I/O 测试的方法

创建文件 I/O 测试以定义一组监视器、配置首选项和控制代理如何运行及其监控内容的其他设置。

您可以通过用户界面或命令行接口 (CLI) 创建文件 I/O 测试。

- **用户界面**－帮助指定每个选项，提供简短说明，并显示默认值。
- **命令行接口**－允许您以无人值守和无提示模式配置和应用文件 I/O 测试。

通过 UI 创建文件 I/O 测试

您可以从“测试监视器”工具栏为文件 I/O 测试创建以下操作。文件 I/O 测试监视在 NFS 或 SMB 文件系统上执行以下操作之一所需的时间长度。

- 创建文件 I/O 测试以读取文件 (p. 22)
- 创建文件 I/O 测试以向文件执行写入 (p. 24)
- 创建文件 I/O 测试以对文件执行读写操作 (p. 26)
- 创建文件 I/O 测试以比较两个文件的内容 (p. 28)

创建文件 I/O 测试以读取文件

本示例创建监控读取位于 F:\Test\testfile.bin 的文件内容所需时间长度的测试。

遵循这些步骤:

1. 单击“测试”工具栏上的 +（新建）。

   此时将显示“新建测试”窗格。

2. 在以下字段中输入合适的值。

   测试名称

   指定有效的测试名称

   示例：Fileio Read Operation

   描述

   指定测试的说明

   示例：对 testfile.bin 执行读取操作。

   测试类

   （可选）指定有效的测试类

   示例：File IO R

   测试间隔

   指定测试的间隔周期

   默认：30

   测试超时

   指定测试的间隔周期

   默认：10

   测试类型

   指定测试类型

   示例：File I/O

   文件操作

   指定测试的可用操作

   示例：读取

   目标文件名

   指定目标文件名的路径

   示例：F:\Test\testFile.bin

   用户名

   指定用户名

   示例：FIOTestUser

3. 接受其他字段的默认值。
4. 单击“保存测试”。

   测试将保存并显示在“可用策略”页面中。

提交认更改时，SRM 将类似于以下内容的条目添加到 svcrsp.cf 文件中：

```
{
index=11
type=fileio
desc="Performing a read operation for testfile.bin."
destination=F:\Test\testFile.bin
args="op=r"
interval=30
samples=1
timeout=10
window=120
tos=0
limit=0
status=active
name="Fileio Read Operation"
class=""
context=""
flags="1"
loglevel=3
}
```

应用文件 I/O 测试时，将执行 svcrsp.cf 文件。

有关文件 I/O 测试返回的错误的信息，请参阅文件 I/O 测试错误代码。

创建文件 I/O 测试以向文件执行写入

该示例读取 C:\sysedge\bin\saFileIOTest.bin 文件，然后将内容写入 F:\Test\WTest.bin。

遵循这些步骤:

1. 在“测试监视器”工具栏上单击“+ (新建)”。

   此时将显示“新建测试”窗格。

2. 在以下字段中输入合适的值。

测试名称

指定有效的测试名称

示例：Fileio Write Operation

说明

指定测试的说明。

示例：对 WTest.bin 执行写入操作。

测试类

（可选）指定有效的测试类

示例：文件 IO W

测试间隔

指定测试的间隔周期

默认：30

测试超时

指定测试的间隔周期

默认：10

测试类型

指定测试类型

示例：文件 I/O

文件操作

指定测试的可用操作

示例：写入

源文件名

指定源文件名的路径

示例：C:\sysedge\bin\saFileIOTest.bin

目标文件名

指定目标文件名的路径

示例：F:\Test\WTest.bin

用户名

指定用户名

示例：FIOTestUser

3. 接受其他的默认值。
4. 单击“保存测试”。
   测试将保存并显示在“可用策略”页面中。

提交认更改时，SRM 将类似于以下内容的条目添加到 svcrsp.cf 文件中：

```
{
index=22
type=fileio
desc="Performing a write operation for WTest.bin."
destination=F:\Test\WTest.bin
args="op=w&local=C:\sysedge\bin\saFileIOTest.bin"
interval=30
samples=1
timeout=10
window=120
tos=0
status=active
name="Write Operation"
class=""
context=""
flags="1"
loglevel=3
}
```

应用文件 I/O 测试时，将执行 svcrsp.cf 文件。

有关文件 I/O 测试返回的错误的信息，请参阅文件 I/O 测试错误代码。

创建文件 I/O 测试以对文件执行读写操作

该示例读取 C:\sysedge\bin\saFileIOTest.bin 文件，将内容写入 F:\Test\RWTest.bin，然后读取 F:\Test\WTest.bin。

遵循这些步骤:

1. 在“测试监视器”工具栏上单击“+ (新建)”。
   此时将显示“新建测试”窗格。

2. 在以下字段中输入合适的值。

测试名称

指定有效的测试名称

示例：fileio

说明

指定测试的说明。

示例：对 RWTest.bin 执行读/写操作。

测试类

（可选）指定有效的测试类

示例：文件 IO RW

测试间隔

指定测试的间隔周期

默认：30

测试超时

指定测试的间隔周期

默认：10

测试类型

指定测试类型

示例：文件 I/O

文件操作

指定测试的可用操作

示例：读/写

源文件名

指定源文件名的路径

示例：C:\sysedge\bin\saFileIOTest.bin

目标文件名

指定目标文件名的路径

示例：F:\Test\RWTest.bin

用户名

指定用户名

示例：FIOTestUser

3. 接受其他的默认值。
4. 单击“保存测试”。
   测试将保存并显示在“可用策略”页面中。

提交认更改时，SRM 将类似于以下内容的条目添加到 svcrsp.cf 文件中：

```
{
index=33
type=fileio
desc="Performing a read/write operation for RWTest.bin."
destination=F:\Test\RWTest.bin
args="op=rw&local=C:\sysedge\bin\saFileIOTest.bin"
interval=30
samples=1
timeout=10
window=120
tos=0
status=active
name="Read-Write Operation"
class=""
context=""
flags="1"
loglevel=3
}
```

应用文件 I/O 测试时，将执行 svcrsp.cf 文件。

有关文件 I/O 测试返回的错误的信息，请参阅文件 I/O 测试错误代码。

创建文件 I/O 测试以比较两个文件的内容

该示例读取 C:\sysedge\bin\saFileIOTest.bin 文件和 F:\Test\CompTest.bin 文件，并比较两者的内容。

遵循这些步骤:

1. 在“测试监视器”工具栏上单击“+ (新建)”。
   此时将显示“新建测试”窗格。

2. 在以下字段中输入合适的值。

测试名称

指定有效的测试名称

示例：fileio

说明

指定测试的说明。

示例：比较文件

测试类

（可选）指定有效的测试类

示例：文件 IO 比较

测试间隔

指定测试的间隔周期

默认：30

测试超时

指定测试的间隔周期

默认：10

测试类型

指定测试类型

示例：文件 I/O

文件操作

指定测试的可用操作

示例：比较

源文件名

指定源文件名的路径

示例：C:\sysedge\bin\saFileIOTest.bin

目标文件名

指定目标文件名的路径

示例：F:\Test\CompTest.bin

用户名

指定用户名

示例：FIOTestUser

3. 接受其他的默认值。
4. 单击“保存测试”。
   测试将保存并显示在“可用策略”页面中。

提交认更改时，SRM 将类似于以下内容的条目添加到 svcrsp.cf 文件中：

```
{
index=44
type=fileio
desc="Comparing files."
destination=F:\Test\CompTest.bin
args="op=cmp&local=C:\sysedge\bin\saFileIOTest.bin"
interval=30
samples=1
timeout=10
window=120
tos=0
status=active
name="File Compare"
class=""
context=""
flags="1"
loglevel=3
}
```

应用文件 I/O 测试时，将执行 svcrsp.cf 文件。

有关文件 I/O 测试返回的错误的信息，请参阅文件 I/O 测试错误代码。

通过 UI 应用文件 I/O 测试

使用用户界面创建文件 I/O 测试之后，将它应用于企业内的计算机。CA Virtual Assurance 将包含所有设置的已编译配置文件应用于所有指定的代理计算机。新策略将在自动代理热启动之后实施。

遵循这些步骤:

1. 单击“策略”。
   此时将显示“策略”页面。
2. 打开“配置”窗格，展开“策略”，然后选择“服务响应”。
   此时将显示“可用策略”页面。
3. 在“可用策略”表中选择策略。
   将出现策略的“摘要”页面，其中包含策略的列表。
4. 选择文件 I/O 策略。
   文件 I/O 策略详细信息将显示在右侧窗格中。

5. 单击“操作”，然后选择“应用”。

   此时将出现用于选择要在其中应用策略的计算机的选项卡。使用“更新运行该策略的计算机”选项卡可以将策略应用于已经运行该策略的计算机。使用“应用于未运行该策略的计算机”选项卡，可以将策略应用于不使用任何策略或使用其他策略的计算机。

6. （可选）从“更新运行该策略的计算机”选项卡，执行以下操作之一：

   - 选择“使用该策略更新所有计算机”，在当前运行该策略的所有计算机上部署该策略。如果进行了希望全局应用的文件 I/O 测试更改，则该选项十分有用。
   - 选择“更新所选的计算机组”，仅更新满足以下任意条件的计算机：
     - 运行过期版本的策略
     - 使用有异常的策略
     - 运行当前版本的策略

     选择这些选项中的任意一个。当用户将点配置更改应用于不在应用的策略中表示的代理时，将发生策略异常。
   - 选择“高级”，然后在“选择计算机”窗格中手工选择要向其重新应用策略的计算机。

7. 单击“应用策略”。

   此时将启动策略应用程序。

8. （可选）选择“高级”，然后在“选择计算机”窗格中选择要向其重新应用策略的计算机。

如果发生以下情况之一，也可以将策略重新应用于系统：

- 已更新策略。
- 收到通知，告知代理计算机上的配置已更改。

应用测试后，每个示例测试将每 30 秒运行一次，如果操作不成功，则在 10 秒之后超时。响应和可用性的统计信息每间隔 120 秒计算一次。

管理员根据这些结果监控并管理虚拟网络的运行状况。

通过 CLI 创建、运行和应用文件 I/O 测试

可以使用 CLI 命令创建并自动执行 SRM AIM，然后根据结果运行操作。可以添加 svcwatch 命令以创建文件 I/O 测试，并将其应用于指定主机上的 SRM AIM。

此命令具有以下格式：

```
svcwatch [-h| -p| -v| -u| -n| -a| -A| -x| -X| -m| -t| -d| -f] -o add index descr fileio destination
username password args interval samples timeout winsiz tos limit flags name class contextInfo logLevel
```

svcwatch 命令使用以下参数：

-h *hostname* | **-h *ipAddr***

（可选）指定 CA SystemEDGE 主机。

默认值：localhost

-p *port*

（可选）指定 CA SystemEDGE SNMP 端口。

默认：161

-c *community*

（可选）指定 SNMP 版本 1 和 2c 的 SNMP 团体字符串。

默认值：public

-v *snmpVersion*

（可选）指定 SNMP 版本。可能的值为：

- 1
- 2c
- 3

默认：1

-u *secName*

（可选）指定 SNMPv3 安全用户的名称。

-u *secLevel*

（可选）指定 SNMPv3 的安全级别。可能的值为：

- 1－noAuthNoPriv
- 2－AuthNoPriv
- 3－AuthPriv

-n *contextName*

（可选）指定 MIBMuxed 代理的实例名称。

-a *authPassword*

（可选）标识针对 AuthNoPriv 或 AuthPriv 安全级别选择 SNMPv3 时所需的身份验证密码。

-A *authProtocol*

（可选）指定身份验证协议。可能的值为：

- MD5－身份验证协议 HMAC-MD5
- SHA－身份验证协议 HMAC-SHA

默认：MD5

-x *privPassword*

（可选）指定针对安全级别 3 (AuthPriv) 选择 SNMPv3 时所需的隐私（加密）密码。

-X *encryptProtocol*

（可选）指定针对隐私使用加密协议。可能的值为：

- DES-数据加密标准
- AES-使用 128 位加密密钥的高级加密标准 (AES128)
- 3DES－三重数据加密标准

-m *FIPSmode*

（可选）指定 FIPS 模式。可能的值为：

- 0－非 FIPS
- 1－FIPS 共存
- 2－仅 FIPS

默认：0

-t *timeout*

（可选）指定 SNMP 命令超时。

默认值：10 秒

-d *logLevel*

（可选）指定 SNMP 消息的日志级别。可能的值为：

- 0－记录致命消息
- 1－记录严重消息
- 2－记录警告消息
- 3－记录信息消息
- 4－记录所有消息
- 5－记录所有消息，包括调试消息

默认：0

-f *logFile*

（可选）指定日志文件的名称。

默认值：sysedge_utility.log

-o add *testparams*

将新测试添加到 SRM AIM 中。

testparams

为新测试指定参数。

index

指定 svcRspTable 索引。

descr

在引号中指定测试的说明。引号 ("") 中为空字符串将不指定说明。

fileio

指定文件 IO 服务类型。

destination

指定要测试的远程文件。

username

在引号中指定用于进行身份验证的用户名。引号 ("") 中为空字符串将不指定用户名。

password

在引号中指定用于进行身份验证的密码。引号 ("") 中为空字符串将不指定密码。

args

指定服务参数。每个参数都是一对关键字和值 (key=value)。与号 (&) 连接和分隔多个参数。完整参数字符串用引号括起来。

参数的常规语法："key1=value1[&key2=value2& ...]"

op=r－读取文件。

op=w－写入位于远程文件系统的测试文件，然后删除测试文件。

op=rw－写入远程文件系统上的测试文件，读取测试文件，然后删除测试文件。

op=cmp－先读取一个文件，再读取另一个文件，然后比较其内容。

local=*path*－用于写入、读取/写入以及比较操作的本地路径和文件名。

domain=*domain*－登录服务器的用户所属的域（仅 Windows）。

interval

指定测试间隔（秒）。

限制：30 秒的倍数

示例

指定每个间隔的抽样数。

超时

指定超时（秒）。

winsiz

指定统计时段大小（秒）。

tos

指定“服务类型”或“差分服务代码”IP。对于普通服务，使用 0（零）。另请参阅 RFC 1349。

limit

指定该测试总响应时间的可接受性能限制（或阈值）。在报告中使用该值。

flags

指定以下标志：

0x001 = 收集性能多维数据集

0x100 = 仅请求时执行（运行一次）

name

指定每种服务类型的唯一名称。引号 "" 中的空字符串不指定测试名称。

类

指定类名称。引号 "" 中的空字符串不指定类名称。

contextInfo

指定上下文信息。引号 "" 中的空字符串不指定上下文信息。

logLevel

指定测试执行码的日志级别。可能的值为：

-2 = 使用 SRM 全局日志级别（默认）

-1 = 不记录

0 = 致命（仅最重要的消息）

1 = 严重

...

7 = debug3（记录所有消息）

示例：比较两个文件的内容

该示例创建并应用文件 I/O 测试，以比较两个文件的内容：

```
svcwatch -h localhost -p 161 -c topsecret -o add 1360744 "FILEIO-TEST" fileio
"F:\Test\CompTest.bin" "" "" "op=cmp&local=C:\sysedge\bin\saFileIOTest.bin" 30
1 10 120 0 0 0x100 "FILEIO-TEST" "" ""
```

有关文件 I/O 测试返回的错误的信息，请参阅文件 I/O 测试错误代码。

应用测试后，每个示例测试将每 30 秒运行一次，如果操作不成功，则在 10 秒之后超时。响应和可用性的统计信息每间隔 120 秒计算一次。

管理员根据这些结果监控并管理虚拟网络的运行状况。

文件 I/O 测试错误代码

下表定义了由文件 I/O 测试返回的文件 I/O 错误代码。错误将显示在“测试监视器”和“测试配置文件监视器”页面上的“错误代码”列中。

错误代码	说明
1	常规错误。有关详细信息，请参阅以下任何错误日志： ■ *%SystemRoot%\windows\system32\sysedge.log*（Windows 系统）或系统日志文件 (UNIX) ■ *SystemEDGE-install-directory*\sysedge\plugins\svcrsp\jcollector.log (Windows) 或 *SystemEDGE-install-directory*/plugins/svcrsp/jcollector.log (UNIX)
2	访问本地文件被拒绝。该错误表示您正在使用的用户名和密码没有正确的权限。您可以在“修改测试”页面上指定其他用户名和密码。
3	访问远程文件被拒绝。该错误表示您正在使用的用户名和密码没有正确的权限。您可以在“修改测试”页面上指定其他用户名和密码。
4	找不到本地文件。
5	找不到远程文件。
6	路径参数指向本地目录中的文件。源文件应位于本地目录中，目标文件应位于远程文件系统上。您可以在“修改测试”页面上更改源文件名和目标文件名。
7	读取本地文件失败。当且仅当该抽象路径名指定的文件存在并且可由应用程序读取时，源文件为 true；否则为 false。
8	读取远程文件失败。
9	创建远程文件失败。
10	写入到远程文件失败。
11	外部命令的输出无效或没有输出。
12	删除远程文件失败。

错误代码	说明
13	文件比较失败。
14	无法执行 file_io_helper.jar。
15	无法写入日志 msg。

第 3 章： 配置

此部分包含以下主题：

编辑控制文件 (p. 39)

编辑控制文件

您可以通过在 SRM 配置文件 (svcrsp.cf) 中添加、删除或修改条目来配置 SRM 选项。例如，您可能需要更改某个时间点的活动线程数，可以通过编辑 svcrsp.cf 轻松完成该操作。请务必在编辑配置文件之前停止 SystemEDGE，然后重新启动。

当 SystemEDGE 启动（并且 SRM AIM 已配置为加载）时，代理会读取 svcrsp.cf 文件以确定配置。如果您是高级用户，而且非常熟悉 SystemEDGE 和 SRM，则可以使用 svcrsp.cf 文件来指定想要代理度量的服务。如果要配置几个系统以在整个企业内度量服务，可以创建单个 svcrsp.cf 文件，并将该文件部署到所有系统。

作为手工编辑 svcrsp.cf 的替代方法，您可以使用 svcwatch 实用工具来动态更新 svcrsp.cf 文件。有关详细信息，请参阅“SRM CLI 命令”。

手工编辑 svcrsp.cf

1. 在想要编辑文件的系统上停止 SystemEDGE：
   - 对于 UNIX 系统，以 root 身份登录，并根据您的系统在命令行中输入以下内容：

     Solaris 和 Linux：
     ```
     /etc/init.d/sysedge stop
     ```

     HP-UX：
     ```
     /sbin/init.d/sysedge stop
     ```

     AIX：
     ```
     /etc/rc.d/sysedge stop
     ```
   - 对于 Windows 系统，请使用 SystemEDGE 控制面板来停止 SystemEDGE。

     注意：有关操作系统 SystemEDGE 启动脚本的名称和位置的信息，请参阅*《SystemEDGE 用户指南》*。
2. 打开 svcrsp.cf 文件进行编辑。svcrsp.cf 的默认位置如下所示：
   - Solaris、HP-UX、AIX、Linux：/opt/CA/SystemEDGE/plugins/svcrsp
   - Windows：drive:\Program Files\CA\SystemEDGE\plugins\svcrsp
3. 重新启动 SystemEDGE 代理，如下所示：
   - 对于 UNIX 系统，根据您的系统在命令行中输入以下内容：

     Solaris 和 Linux：
     ```
     /etc/init.d/sysedge start
     ```

     HP-UX：
     ```
     /sbin/init.d/sysedge start
     ```

     AIX：
     ```
     /etc/rc.d/sysedge start
     ```
   - 对于 Windows 系统，请使用 SystemEDGE 控制面板来启动 SystemEDGE。

配置文件格式

SRM 配置文件包含一系列由大括号 ({ }) 分隔的条目。条目中的每个字段依赖于关键字（但*不*依赖于顺序）。可以忽略可选字段。条目的格式如下所示：

```
{
index=
type=
desc=" "
dest=" "
args=" "
username=" "
encoded=yes
password=" "
interval=
samples=
timeout=
window=
tos=
limit=
status=
name=
class=
context=
flags=
loglevel=
}
```

注意：如果想要手工编辑密码字段，必须首先指定 encoded=no，然后可以以明文形式键入密码。更改密码之后，将已编码字段重置为“yes”，然后重新启动 SystemEDGE。SRM 将对密码进行编码以将其遮蔽，但是密码既未加密也不安全。

样本条目

有关每个测试类型的样本 svcrsp.cf 条目，请参阅以下服务的示例部分：

- Active Directory 用户
- 自定义
- DHCP
- DNS
- FILE I/O
- FTP
- HTTP
- HTTPS
- IMAP

- LDAP
- MAPI
- NIS
- NNTP
- PING
- POP3
- 往返电子邮件
- SMTP
- SNMP
- SQL 查询
- TCP Connect
- TFTP
- 虚拟用户（仅 Windows）

有关每个测试的关键字列表，请参阅测试关键字 (p. 126)。

全局参数块

配置文件中的全局参数块提供以下参数：

type=global

在配置文件中指定全局段。

loglevel={-1 | 0 | 1 | 2 | ... | 7}

指定 SRM AIM 的日志级别。

-1：不记录消息

0：记录致命级别的消息

1：还记录重要级别的消息

2：还记录警告级别的消息

3：还记录信息级别的消息

4：还记录调试级别的消息

5：还记录调试 1 级别的消息

6：还记录调试 2 级别的消息

7：还记录调试 3 级别的消息

默认：2

logfile=*filename*

在 svcrsp 数据路径中指定日志文件名。

默认：jcollector

lognum=*number*

指定日志文件的数目。如果日志文件数等于 1（默认），则日志文件名为 jcollector.log。如果日志文件数大于 1，则日志文件为 jcollector0.log、jcollector1.log，依次类推。

默认：1

logsize=*size*

指定日志文件的最大大小（以 KB 为单位）。值 0 表示不限大小。

默认：1024

maxthreads=*number*

指定 Jcollector 用来执行测试的线程的最大数目（每个线程一个测试）。

默认：10

javabin=*path*

指定 java 可执行文件相对于 SystemEDGE 安装目录的位置。

默认：./jre/bin/java

javaclasspath=*classpath*

指定要加载的额外类。如果设置了 classpath，此参数将覆盖 CLASSPATH 环境变量。

默认：""

no_collector

SystemEDGE 不启动 Jcollector。要启用此参数，请删除注释符号 (#)。

重要信息！仅将 no_collector 用于调试。该参数可有效地禁用 SRM 执行。

默认：disabled

allow_scripts

允许执行外部脚本。要启用此参数，请删除注释符号 (#)。

默认：disabled

allow_fileio

允许执行文件 IO 测试。要启用此参数，请删除注释符号 (#)。

默认：disabled

allow_untrusted_ssl_certificates

允许在没有受信任 SSL 证书的站点上进行 SSL 测试。要启用此参数，请删除注释符号 (#)。

默认：disabled

disable_dns_cache

阻止 JRE 缓存 DNS 名称。要启用此参数，请删除注释符号 (#)。

默认：disabled

allow_snmp_pwd

允许 SRM 通过 SNMP get 请求以明码文本提供密码。要启用此参数，请删除注释符号 (#)。

默认：disabled

hide_security_flags

阻止 svcRspSecurityFlags OID 泄露安全设置。要启用此参数，请删除注释符号 (#)。

默认：disabled

preferIPV6_NoTOS（仅限 HP-UX Java）

当使用 IPV6 堆栈时，不支持 socket.setTrafficClass()。因此，默认情况下使用 IPV4 堆栈以保持标准 TOS 功能。要启用 IPV6 堆栈（从而在所有测试中禁用 TOS 功能），请将该参数取消注释。

注意：对于其他所有平台，此行仍应注释掉。

默认：disabled

shmkey=*integer*

指定共享内存访问键。

重要信息！除非与现已安装的程序冲突，否则请不要使用此参数。

默认：3131

reserved_range *start_index end_index*

指定测试索引的保留范围。

默认：无

示例

```
{
  type=global
  loglevel=4
  maxthreads=100
  #javabin=<Java executable path>
  javaclasspath=
  #no_collector
  #allow_scripts
  #allow_fileio
  #allow_untrusted_ssl_certificates
  #disable_dns_cache
  #allow_snmp_pwd
  #hide_security_flags
  #preferIPV6_NoTOS
  #shmkey=<integer>
  #reserved_range <start_index> <end_index>
}
```

测试定义参数块

配置文件中的测试定义参数块提供了以下参数：

type=*testtype*

指定测试类型。例如 HTTP、FTP、LDAP 等。有关测试类型的完整列表，请参阅本指南中的“测试管理”一章。

index=*integer*

指定一个唯一的数字来标识测试。该数字是相应的服务响应时间表项目的索引。

name=*string*

（可选）指定测试的测试实例名称，用于状态管理器对象信息，性能数据集合的资源实例信息，以及作为测试主键的随机整数索引的备用内容（可能会基于所提供的模板而有所变化）。仅在创建测试期间编写该值。

class=*string*

（可选）指定测试的类名称，用于状态管理器对象信息，性能数据集合的资源实例信息，以及作为测试主键的随机整数索引的备用内容（可能会基于所提供的模板而有所变化）。仅在创建测试期间编写该值。

context=*string*

（可选）指定一个占位符，用于放置配置该测试的管理员想要指定的任何内容。该字段可以视为一个位置，用于存储给定管理员要存储的任何信息，如该测试对象的 UUID、标志、祖先项等。SRM 不直接将该信息用于任何功能，但会将这些信息作为任意管理员通知的一部分进行传递。

desc=*string*

（可选）为测试指定有意义的描述。

限制：4096 个字符

dest=*string*

指定测试的目标。例如，URL、服务器名称、脚本等。

user=*string*

指定用户名（如果测试需要登录才可运行）。

pass=*string*

指定密码（如果测试需要登录才可运行）。默认情况下，密码是加密的。在这种情况下，svcRspSecurityFlags 的第 4 位设置为 1。如果密码未加密，svcRspSecurityFlags 的第 4 位设置为 0。

args=*string*

（可选）指定用于测量用途的特定于服务的参数。

限制：256 个字符

服务参数示例有：

dns：*dns-server hostname*

http：*URL* [*proxy-server*] [*username:user password:pass*]

https：*URL* [*proxy-server*] [*username:user password:pass*]

ftp：*ftp-server username passwd*

pop3：*pop3-server username passwd*

nntp：*nntp-server*

smtp：*smtp-server*

ping：*system-name packetsize*

tcpconnect：*system-name port*

custom：*not used*

encoded={yes | no}

指定密码加密。如果设置为“no”，SRM 将对密码进行加密并将该值更改为“yes”。

interval=*integer*

（可选）指定查询服务的时间间隔。

默认：60

samples=*integer*

（可选）指定在每个查询间隔获取的样本数目。###例如，如果将该值设为“3”、间隔为“60”，则 SRM 在每 60 秒间隔之后将执行 3 个抽样事务。

默认：1

timeout=*integer*

（可选）指定该值（以秒为单位），在该值之后特定服务度量的服务响应时间度量将超时。

默认：10

window=*integer*

（可选）指定该时段（以秒为单位），在该时段内将计算特定服务的响应时间统计（平均值、可用性等）。

默认：300

tos=*integer*

（可选）为每个测试在 IP 标头中指定 8 位 TOS 标头（IP 服务类型或差分服务代码）。该参数不会针对该字段的值强制任何具体的 RFC 标准。由您来决定一个合适的值。

默认：0

limit=*integer*

（选项）指定响应限制，用作引发异常的上下限。

默认：0

monitor=*monName, mon_index*

（可选）为测试指定关联的监控模板（阈值）。

monName 变量等于该监控模板的 monName 参数值。monIndex 变量是 SystemEDGE 的监视器表的表条目和索引的唯一值。

status={active | notInService}

（可选）指定该条目的状态。该变量在语义上相当于 SNMPv2 SMI RowStatus 约定(请参见 RFC 1443)。

active(1)：可以使用。

notInService(2)：禁用此行。

默认： notInService

flags=*hex_value*

（可选）测试配置标志：

0x0001 [cube_collect]：支持收集该测试的测试度量标准。

0x0100 [run_once]：指定该测试仅在要求时运行，而不是通过轮询间隔排定程序运行测试。

默认： 0x0

loglevel={-1 | 0 | 1 | 2 | ... | 7}

（可选）指定 SRM AIM 的日志级别。另请参见“全局参数块”。

-1：不记录消息

0：记录致命级别消息

1：还记录严重级别消息

2：还记录警告级别消息

3：还记录信息级别消息

4：还记录调试级别消息

5：还记录 debug1 级别消息

6：还记录 debug2 级别消息

7：还记录 debug3 级别消息

默认：全局日志级别

示例

```
{
  index=25
  type=http
  desc="www.ca.com Http"
  dest="http://www.ca.com"
  encoded="yes"
  password=""
  args="max_depth=3&content_dl=yes&content_err=no"
  interval=30
  samples=1
  timeout=20
  window=300
  tos=0
  limit=0
  status=active
  name="www.ca.com-http"
  class=""
  context=""
  loglevel=1
  flags="1"
  monitor=TotalMeanCritical9000,2511
  monitor=TotalMeanWarning5000,2510
}
{
  type=monitor
  monName="TotalMeanCritical9000"
  monSeverity=critical
  monAttribute=svcRspTableTotalMean
  monThreshold=9000
  monOperator=gt
}
```

```
{
  type=monitor
  monName="TotalMeanWarning5000"
  monSeverity=warning
  monAttribute=svcRspTableTotalMean
  monThreshold=5000
  monOperator=gt
}
```

监视器模板定义参数块

配置模板中的监视器模板定义参数块提供了以下参数：

type=monitor

指定参数块的监视器类型。

monName=*string*

指定监视器的名称。

monSeverity=*string*

（可选）指定要用于 SystemEDGE 对象状态模型的重要级别。值“无”会将该监视器条目排除在该对象状态模型之外。可能的值为：

无

正常

警告

轻微

重大

严重

致命

默认值：无

monAttribute=*string*

指定监控的属性。可能的属性为：

svcRspTableNumSamples－显示自该行初始化以来的采样总数。

svcRspTableTotalLastSample－最后采样的总响应时间（毫秒）。

svcRspTableTotalMin－显示统计窗口中的最小总响应时间采样值。

svcRspTableTotalMax－显示统计窗口中的最大总响应时间抽样值。

svcRspTableTotalMean－显示统计窗口中的平均总响应时间抽样值。

svcRspTableTotalVariance－统计窗口中总响应时间值差异 * 1000。对于差异值 1.337，SA 将返回 1337。该差异基于秒计算。

svcRspTableTotalAvailability－指示服务的可用性。该值等于统计窗口中的成功服务查询数目除以服务查询数目。如果某个服务条目在针对其指定的超时值内成功，则表示该条目成功。

svcRspTableNameLastSample－显示最后抽样的名称查找 (DNS) 时间（毫秒）。

svcRspTableNameMin－显示统计窗口中的最小名称查找时间抽样值。

svcRspTableNameMax－显示统计窗口中的最大名称查找时间抽样值。

svcRspTableNameMean－显示统计窗口中的平均名称查找时间抽样值。

svcRspTableNameVariance－显示统计窗口中名称查找时间值的差异。

svcRspTableConnLastSample－显示最后抽样的连接时间（毫秒）。

svcRspTableConnMin－显示统计窗口中的最小连接时间抽样值。

svcRspTableConnMax－显示统计窗口中的最大连接时间抽样值。

svcRspTableConnMean－显示统计窗口中的平均连接时间抽样值。

svcRspTableConnVariance－显示统计窗口中连接时间值的差异。

svcRspTableTranLastSample－显示最后抽样的事务处理时间（毫秒）。

svcRspTableTranMin－显示统计窗口中的最小事务处理时间抽样值。

svcRspTableTranMax－显示统计窗口中的最大事务处理时间抽样值。

svcRspTableTranMean－显示统计窗口中的平均事务处理时间抽样值。

svcRspTableTranVariance－显示统计窗口中事务处理时间值的差异。

svcRspTableBytesInLastSample－显示最后抽样中接收的字节数。

svcRspTableBytesOutLastSample－显示最后抽样中发送的字节数。

svcRspTableTotalBytesIn－显示 SA 启动以来接收的字节总数。该计数器最终会封装。

svcRspTableTotalBytesOut－显示 SA 启动以来发送的字节总数。该计数器最终会封装。

svcRspTableThroughput－显示统计窗口内计算的吞吐量（字节/秒）。每个抽样的 BytesInLastSample 和 BytesOutLastSample 将进行合计。每个抽样的该数字相加，然后除以该抽样的秒数。

monThreshold=*integer*

指定 SystemEDGE 用于比较受监控属性的当前值的阈值。

monOperator={nop | gt | lt | ge | le | eq | ne}

比较当前属性值和阈值 运算符 nop 只跟踪当前值，不将其与阈值进行比较。可能的值为：

nop（无运算）

gt（大于）

lt（小于）

ge（大于或等于）

le（小于或等于）

eq（等于）

ne（不等于）

默认：无运算

示例

本示例为统计窗口中的平均总响应时间抽样值指定了一个警告阈值和一个严重阈值，分别为 500 毫秒和 900 毫秒。

```
{
  type=monitor
  monName="TotalMeanCritical900"
  monSeverity=critical
  monAttribute=svcRspTableTotalMean
  monThreshold=900
  monOperator=gt
}
{
  type=monitor
  monName="TotalMeanWarning500"
  monSeverity=warning
  monAttribute=svcRspTableTotalMean
  monThreshold=500
  monOperator=gt
}
```

抽样配置文件

配置文件示例：

```
{
  type=global

 # SRM/SA AIM 和无特定日志级别的任何测试的日志级别（默认为 2）
 # -1—关闭、0—致命、1—严重、2—警告、3—信息、4—debug……7—debug3
   loglevel=2

 # 日志文件名（默认为 jcollector.log）
   logfile="jcollector.log"

# 日志文件号（默认为 1，只有一个日志文件，更大的数字将在 #<number> 日志文件中循环使用）
# 这些文件将命名为 <name><id>，例如，如果使用默认名称 jcollector0.log，则为
#jcollector1.log，以此类推。)
   lognum=1

# 日志文件大小限制（以千字节计，默认为 1024，0 表示无限制）
   logsize=10240

# 用于执行测试的线程数
   maxthreads=10

# Java 可执行文件的位置
 #javabin=<Java 可执行文件名包含 路径，相对于 SystemEDGE 实例。dir.>

# 要加载的额外的类；如果已定义则覆盖环境中的 CLASSPATH
   #javaclasspath=<a non-standard classpath>

# 取消注释，以使 sysedge 不启动 jcollector
   #no_collector

# 取消注释，以允许执行外部脚本
    #allow_scripts

# 取消注释以允许执行 fileIO 测试。
    #allow_fileio

# 如果希望以明文形式将测试密码提供给 SNMP Get     # 请求，则取消注释
    #allow_snmp_pwd
```

```
# 取消注释，以允许 SSL 测试与没有
# 可信 SSL 证书的站点协作。
    #allow_untrusted_ssl_certificates

# 取消注释，以阻止 JRE 永久缓存 DNS 名称
    #disable_dns_cache

# 取消注释，以阻止 svcRspSecurityFlags OID 显示
# 安全设置
    #hide_security_flags

# 对于当前 HP/UX Java，不支持 socket.setTrafficClass()
# 当使用 IPV6 堆栈时 默认情况下，IPV4 堆栈将
# 用于保留标准 TOS 功能（在之前的 SA
# 版本中）。要启用 IPV6 堆栈（并因此禁用所有 SA 测试的 TOS
# 功能），请取消注释以下行。
# （对于所有其他平台，该行应仍是被注释掉的。）
#
    #preferIPV6_NoTOS

# 共享的内存访问密钥，默认值为 3131
    #shmkey=<an integer number>

# 测试索引的保留范围，默认情况下为无
    reserved_range 20 2000
}

{
  index=22
  type=dns
  desc="Test DNS Lookup for http://ca.com_dns"
  dest="130.119.24.108"
  encoded="yes"
  password="gJnvpNczJKjubcMzOJ/h+tvbBnX="
  args="hostname=abc.ca.com"
  interval=300
  samples=1
  timeout=10
  window=86400
  tos=0
  limit=0
  status=notInService
  name="192.168.24.108 Dns"
  class=""
  context="context"
  loglevel=1
  flags="0x100"
  monitor=TotalMeanCritical9,1011
  monitor=TotalMeanWarning5,1010
}
```

```
{
  index=25
  type=http
  desc="www.ca.com Http"
  dest="http://www.ca.com"
  encoded="yes"
  password=""
  args="max_depth=3&content_dl=yes&content_err=no"
  interval=30
  samples=1
  timeout=20
  window=300
  tos=0
  limit=0
  status=active
  name="www.ca.com-http"
  class=""
  context=""
  loglevel=1
  flags="0x1"
  monitor=TotalMeanCritical9000,2511
  monitor=TotalMeanWarning5000,2510
}

{
  type=monitor
  monName="TotalMeanCritical9000"
  monSeverity=critical
  monAttribute=svcRspTableTotalMean
  monThreshold=9000
  monOperator=gt
}

{
  type=monitor
  monName="TotalMeanWarning5000"
  monSeverity=warning
  monAttribute=svcRspTableTotalMean
  monThreshold=5000
  monOperator=gt
}

{
  type=monitor
  monName="TotalMeanCritical900"
  monSeverity=critical
  monAttribute=svcRspTableTotalMean
  monThreshold=900
  monOperator=gt
}
```

```
{
  type=monitor
  monName="TotalMeanWarning500"
  monSeverity=warning
  monAttribute=svcRspTableTotalMean
  monThreshold=500
  monOperator=gt
}

{
  type=monitor
  monName="TotalMeanFatal10"
  monSeverity=fatal
  monAttribute=svcRspTableTotalMean
  monThreshold=10
  monOperator=gt
}

{
  type=monitor
  monName="TotalMeanCritical9"
  monSeverity=critical
  monAttribute=svcRspTableTotalMean
  monThreshold=9
  monOperator=gt
}

{
  type=monitor
  monName="TotalMeanWarning5"
  monSeverity=warning
  monAttribute=(null)
  monThreshold=5
  monOperator=gt
}
```

第 4 章： 测试管理

此部分包含以下主题：

创建测试 (p. 57)
测试的关键字 (p. 126)
使用自定义脚本创建测试 (p. 132)

创建测试

您可以创建 SystemEDGE 策略，以定义一组监视器、配置首选项和控制代理如何运行及其监视内容的其他设置。创建 SRM 测试后，可以将测试分组并将配置文件与代理和代理集相关联。

另请参阅 *《联机帮助》*和 *《管理指南》*中的“策略配置”。

遵循这些步骤:

1. 单击“资源”。
2. 打开“配置”窗格，展开“策略”，然后单击“服务响应”。

   将显示“服务响应”页面。可以创建新策略，或使用现有的默认策略（如果合适）。
3. 在“可用策略”工具栏上单击 +（新建）。

   将显示“新建服务响应监控策略”对话框。
4. 输入相应值并单击“确定”。

   CA Virtual Assurance 加载新策略。
5. 单击“测试”选项卡。

   此时将打开“测试监视器”窗格。
6. 在“测试监视器”工具栏上单击“+ (新建)”。

   这时将显示用于指定测试的字段。
7. 在“测试名称”字段中，指定测试的唯一名称。名称必须小于等于 64 个字符。测试名称区分大小写。
8. （可选）在“说明”字段中指定测试的说明和类别。说明为用户指定测试。必须小于等于 4096 个字符。
9. 在“测试间隔”字段中指定测试间的间隔（以秒为单位）。间隔必须是 30 秒的倍数。使用该选项来调整测试的性能。

10. 在“测试超时”字段中，指定经过多长时间后测试超时（以秒为单位）。选择一个小于间隔但是大于执行测试所需时间的数字。
11. 通过从“轮询间隔”列表中选择以下内容之一，设置轮询间隔：
    - 正常
    - 关
    - 慢放
12. 从“测试类型”列表中选择要创建的测试的类型：
    - Active Directory（仅限 Windows）
    - 自定义
    - DHCP
    - DNS
    - 文件 I/O
    - FTP
    - HTTP
    - HTTPS
    - IMAP
    - LDAP
    - MAPI（仅适用于 Windows）
    - NIS
    - NNTP
    - PING
    - POP3
    - 往返电子邮件
    - SMTP
    - SNMP
    - SQL 查询
    - TCP Connect
    - TFTP
    - 虚拟用户（仅 Windows）

13. 在“测试选项”字段中设置测试的选项。选项因测试类型而异。有关各个测试的设置选项的详细信息，请参阅该测试类型的特定页面。

    注意：您在本页上设置的选项适用于 SRM 为该测试创建的所有路径。在修改这些选项时，更改会影响每个路径。如果想修改仅一个路径的选项或仅选择路径（但并非所有使用该测试的路径），必须创建该测试的副本，修改要更改的选项，然后将新测试与要应用更改的代理相关联。

14. 要设置高级选项，请在“常用选项”区域中选择“高级”。

15. 使用“测试索引覆盖”字段控制测试的运行顺序，或对多个计算机上运行的同一个测试进行索引标准化。

    SystemEDGE 代理通常在多线程环境中运行测试，因此几个测试同时运行。如果您要依次运行测试并控制测试运行的顺序，请将线程计数设置为 1 以确保一次仅运行一个测试。然后将索引值分配给要排序的各个测试。索引覆盖值的范围为 1000000 到 1009999。最小的索引号优先级最高。

    注意：使用该选项时，最好在测试之间保留一些未分配的索引。这可轻松修改测试的顺序，或将新的测试添加到现有序列中，而无需对所有测试的索引进行更改。

16. 在“每间隔抽样数”字段中，指定每个间隔要执行的测试事务的数目。

在“统计窗口”字段中，指定 SRM 用来计算该测试的响应时间和可用性统计信息的时间（以秒为单位）。该值应当是 30 的倍数。确保“统计窗口”的设置大于“测试间隔”，最好为该值的倍数。例如，“测试间隔”为 60，“统计窗口”设置为 300。

1. 在“总响应限制”字段中，指定该测试总响应时间的可接受性能限制（或阈值）。在报告中使用该值。

2. 在“TOS/DSCP”字段中，指定“服务类型”(TOS) 或“差分服务代码点”(DSCP) IP 值（如果您的路由器配置成使用其中之一的话）。如果指定 TOS 或 DSCP 值，第一个测试会设置该值，从而在后续操作中将使用已设置的值。另请参阅：RFC 1349。

3. 完成所需输入项，然后单击“保存模板”。

   将保存新测试。

注意：指定路径名时，请确保针对将运行测试的操作系统使用正确类型的斜杠。也就是说，为 UNIX 系统指定目录时使用正斜杠 (/)，为 Windows 系统指定目录时使用反斜杠 (\)。

选项和参数

选项是所有测试所共有的属性。相比之下，参数是某一特定测试所特有的属性。

Options

选项是所有测试的共有属性。它们表示可以应用于所有测试的通用功能。

参数

参数是某些测试特有的属性。但是，部分测试使用相似/相同的参数；例如，http、https、POP3、往返电子邮件。它们表示可以应用于特定测试的功能。

Active Directory 测试

Active Directory 测试监视连接到 Windows 系统上的 Active Directory 服务，执行一次标准的用户名/密码身份验证，然后执行一个用户定义查询所需的时间长度。

选项和参数

Active Directory 测试需要以下特定选项和参数：

- **Active Directory 服务器**－您正在测试的 Active Directory 服务器的名称。

  注意：从 Service Availability r2.1 开始，可以使用 IPv6 地址，但是必须将其括在方括号内，例如 [0aff::230:6eff:fe4b:51db]:8080。此处的 0aff::230:6eff:fe4b:51db 表示 IPv6 地址，8080 表示端口号。
- **Active Directory 域**－Active Directory 服务器所在的域。
- **用户名**－Active Directory 服务器的有效用户名。
- **密码**－上面指定的用户名的密码。SRM 以加密格式存储密码。
- **查询**－将使用 LDAP 查询语言执行的查询。
- **筛选**－（可选）据其对查询结果进行筛选的条件。

在创建或修改测试时指定这些选项和参数。

示例

本节包括监视连接到本地和远程 Active Directory 服务器的时间长度的示例。

示例 1：测试本地 Active Directory 服务器

使用该示例来创建监视连接到名为 ADTest 的本地 Active Directory 服务器的时间长度的测试，验证用户名 adUser 和编码的密码，然后在 mylab.com 站点上查询条件“注册的用户”。

在策略中创建新的测试

1. 在“测试监视器”工具栏上单击“+ (新建)”。

   此时将显示“新建测试”窗格。
2. 从“测试类型”列表中选择 Active Directory。
3. 在“说明”字段中指定 ad_local。
4. 在“测试名称”字段中指定“本地 Active Directory 测试”。
5. 在“测试间隔”字段中指定 30。
6. 在“测试超时”字段中指定 10。
7. 在“每间隔抽样数”字段中指定 1。
8. 在“统计窗口”字段中指定 120。
9. 在“Active Directory 服务器”字段中指定 ADTEST。
10. 在“Active Directory 域”字段中指定 mylab.com。
11. 在“用户名”字段中指定 ADUser。
12. 在“密码”字段中指定 ADPass。
13. 在“查询”字段中指定 cn=Registered,cn=Users,dc=mylab,dc=com。
14. 在“筛选”字段中指定 cn=*。
15. 接受其他所有字段的默认值。
16. 单击“保存测试”。

提交更改时，SRM 将类似于以下内容的条目添加到 svcrsp.cf 文件中：

```
{
index=23
type=adir
desc="ad_local"
dest="ADTEST"
username="ADUser"
encoded=yes
password="bXVyaWM="
args="domain=mylab.com&query=cn=Registered,cn=Users,dc=mylab,dc=com&filter=cn
=*"
interval=30
samples=1
timeout=10
window=120
tos=0
limit=0
status=active
name="Local Active Directory Test"
class=""
context=""
flags="1"
loglevel=1
}
```

示例 2：测试远程 Active Directory 服务器

使用该示例来创建监视连接到位于 10.0.0.234 的远程 Active Directory 服务器的时间长度的测试，验证用户名 RemoteUser 和编码的密码，然后在 testlab.com 站点上查询条件来宾用户。

在策略中创建新的测试

1. 在“测试监视器”工具栏上单击“+ (新建)”。

   此时将显示“新建测试”窗格。

2. 从“测试类型”列表中选择 Active Directory。
3. 在“说明”字段中指定 ad_remote。
4. 在“测试名称”字段中指定“远程 Active Directory 测试”。
5. 在“测试间隔”字段中指定 30。
6. 在“测试超时”字段中指定 10。
7. 在“每间隔抽样数”字段中指定 1。
8. 在“统计窗口”字段中指定 120。
9. 在“Active Directory 服务器”字段中指定 10.0.0.234。
10. 在“Active Directory 域”字段中指定 Test.com。

11. 在“用户名”字段中指定 RemoteUser。
12. 在“密码”字段中指定 ADPass。
13. 在“查询”字段中指定 cn=Guest,cn=Users,dc=testlab,dc=com。
14. 在“筛选”字段中指定 cn=*。
15. 单击“保存测试”。

提交更改时，SRM 将类似于以下内容的条目添加到 svcrsp.cf 文件中：

```
{
index=24
type=adir
desc="ad_remote"
dest="10.0.0.234"
username="RemoteUser"
encoded=yes
password="bXVyaWMe"
args="domain=test.com&query=cn=Guest,cn=Users,dc=testlab,dc=com&filter=cn=*"
interval=30
samples=1
timeout=10
window=120
tos=0
status=active
name="Remote Active Directory Test"
class=""
context=""
flags="1"
loglevel=2
}
```

有关您在运行 Active Directory 测试时可能遇到的错误的信息，请参阅Active Directory 测试错误代码 (p. 268)。

自定义测试

自定义测试提供使用脚本或程序来执行自定义测试的功能。

选项和参数

自定义测试需要下列特定的选项或参数：

- **脚本路径 (dest)**—要用来执行自定义测试的脚本或程序的名称。该字段包含完整的脚本路径和参数。SRM 预期脚本或程序驻留在本地或已安装的文件系统上。

在创建或修改测试时指定此选项或参数。

示例

使用该示例来创建通过脚本或程序监视自定义服务的测试。该条目指示代理每 30 秒测试一次自定义服务，并等待最多 20 秒以接收成功响应。代理计算过去 3600 秒钟（1 小时）内的统计信息。

在策略中创建新的测试

1. 在“测试监视器”工具栏上单击“+ (新建)”。

   此时将显示“新建测试”窗格。

2. 从“测试类型”列表中选择“自定义”。
3. 在“测试名称”字段中指定 Custom_test。
4. 在“说明”字段中指定“测试自定义服务”。
5. 在“脚本路径”字段中指定 c:\@work\projects\shortcuts\custom_test.exe。
6. 在“测试间隔”字段中指定 30。
7. 在“测试超时”字段中指定 20。
8. 在“每间隔抽样数”字段中指定 1。
9. 在“统计窗口”字段中指定 3600。
10. 单击“保存测试”。

提交认更改时，SRM 将类似于以下内容的条目添加到 svcrsp.cf 文件中：

```
{
index=123
type=CUSTOM
desc="Test custom service"
dest="c:\@work\projects\shortcuts\custom_test.exe"
interval=30
samples=1
timeout=20
window=3600
tos=0
limit=0
status=active
name="Custom_test"
class="Custom_class"
context="Custom_context"
flags="0x0"
loglevel=3
}
```

DHCP 测试

DHCP 测试监控发送 DHCP 请求并接收响应所需的时间长度。

注意：仅对静态配置并且未运行 DHCP 客户端的系统运行 DHCP 测试。这些测试需要在端口 68 上具有开放的套接字来侦听请求。如果其他进程（如 DHCP 客户端）已经正在端口 68 上侦听，测试将失败。

选项和参数

DHCP 测试仅需要下列选项和参数：

DHCP 服务器－要测试的 DHCP 服务器的主机名或 IP 地址。在创建或修改测试时指定该参数。

注意：可以使用 IPv6 地址，但是必须将其括在方括号中，例如 [0:0:0:0:0:0:10.0.00.0]。

示例

使用该示例来创建监视将 DHCP 请求发送到 DHCP 服务器并接收响应所需的时间长度的测试。

在策略中创建新的测试

1. 在“测试监视器”工具栏上单击“+ (新建)”。

   此时将显示“新建测试”窗格。
2. 从“测试类型”列表中选择 DHCP。
3. 在“说明”字段中指定 dhcp_resp。
4. 在“测试名称”字段中指定“测试 DHCP 服务”。
5. 在“测试间隔”字段中指定 300。
6. 在“测试超时”字段中指定 10。
7. 在“每间隔抽样数”字段中指定 1。
8. 在“统计窗口”字段中指定 86400。
9. 在“DHCP 服务器”字段中，指定 192.174.12.89。
10. 接受其他所有字段的默认值。
11. 单击“保存测试”。

提交认更改时，SRM 将类似于以下内容的条目添加到 svcrsp.cf 文件中：

```
{
index=31
type=dhcp
desc="dhcp_resp"
dest="192.174.12.89"
args=""
interval=120
samples=1
timeout=100
window=300
tos=0
limit=0
status=active
name="Test DHCP Service"
class=""
context=""
flags="1"
loglevel=2
}
```

有关您在运行 DHCP 测试时可能遇到的错误的信息，请参阅 DHCP 测试错误代码 (p. 268)。

DNS 测试

DNS 测试监视解析指定服务器的 IP 地址所需的时间长度。

选项和参数

DNS 测试需要以下特定选项和参数：

- **DNS 服务器**－您正在测试的本地 DNS 服务器的名称。
- **要解析的主机名**－您要针对 DNS 服务器解析的主机名。

在创建或修改测试时指定这些选项和参数。

示例

使用该示例来创建监视使用位于 192.168.0.0 的名称服务器解析 http://www.ca.com 的 IP 地址所需的时间长度的测试。（在您的环境中，使用您的本地 DNS 服务器的 IP 地址。）该条目指示代理每 300 秒（5 分钟）测试一次服务，并等待最多 10 秒以接收成功响应。代理计算过去 86,400 秒钟（1 天）内的统计信息。

在策略中创建新的测试

1. 在“测试监视器”工具栏上单击“+ (新建)”。

   此时将显示“新建测试”窗格。

2. 从“测试类型”列表中选择 DNS。
3. 在“说明”字段中指定 ca.com_dns。
4. 在“测试名称”字段中指定“测试 DHCP 查找”。
5. 在“测试间隔”字段中指定 300。
6. 在“测试超时”字段中指定 10。
7. 在“每间隔抽样数”字段中指定 1。
8. 在“统计窗口”字段中指定 86400。
9. 在“DNS 服务器”字段中指定您的本地 DNS 服务器的 IP 地址（如 192.168.0.0）。
10. 在“要解析的主机名”字段中指定 http：//jimp.ca.com。
11. 单击“保存测试”。

提交认更改时，SRM 将类似于以下内容的条目添加到 svcrsp.cf 文件中：

```
{
index=10
type=dns
desc="Test DNS Lookup for http://ca.com_dns"
dest="192.168.0.0"
args="hostname=jimp.ca.com"
interval=300
samples=1
timeout=10
window=86400
tos=0
limit=0
status=active
name="Test DNS Lookup"
class=""
context=""
flags="1"
loglevel=2
}
```

有关您在运行 DNS 测试时可能遇到的错误的信息，请参阅 DNS 测试错误代码 (p. 268)。

文件 I/O 测试

文件 I/O 测试监视在 NFS 或 SMB 文件系统上执行以下操作之一所需的时间长度。

- 读取文件
- 写入文件
- 写入文件，然后读取该文件
- 比较两个文件

默认情况下关闭文件 I/O 测试。使 SRM 能够通过编辑 svcrsp.cf 文件以删除“allow_fileio”行开头的井号 (#) 来取消注释该行，从而运行文件 I/O 测试。有关编辑 svcrsp.cf 文件的说明，请参阅“手动编辑 svcrsp.cf 文件”。

在修改 svcrsp.cf 文件以启用它们之前，您可以创建文件 I/O 测试并且将其与代理关联在一起。然而，在按上述方法启用文件 I/O 测试之前，代理上创建的测试均处于“未就绪”状态，且无法变成活动（可以运行）状态。该配置文件指令“allow_fileio”是一种安全措施。因为 SRM 以 root 用户的身份运行，所以文件 I/O 测试可能会写入 /etc/passwd 或 boot.ini 文件并使系统瘫痪。启用和创建这些测试时应十分谨慎。

您正在测试的文件的大小可能会影响测试的性能。
drive:/sysedge/plugins/svcrsp 目录中存在示例测试文件。

选项和参数

文件 I/O 测试需要以下特定于测试的选项和参数：

- **文件操作**－要执行的操作类型；为以下类型之一：
  - **读取**－读取测试文件。文件必须存在于本地或远程安装的文件系统上。在“目标文件名”字段中指定要读取的文件的路径。
  - **写入**－将本地文件的内容写入远程文件系统上的测试文件，然后删除该测试文件。在“源文件名”字段中指定源文件的路径，并在“目标文件名”字段中指定测试文件的路径。源文件必须存在，目标文件不得存在。
  - **读取/写入**－将本地文件的内容写入远程文件系统上的测试文件，读取测试文件，将测试文件与原始文件进行比较，然后删除测试文件。在“源文件名”字段中指定源文件的路径，并在“目标文件名”字段中指定测试文件的路径。源文件必须存在，目标文件不得存在。
  - **比较**－先读取一个文件，然后读取另一个文件，并比较两者的内容。如果内容不匹配，则测试失败。在“源文件名”和“目标文件名”字段中指定源文件和目标文件。两个文件必须都存在。

  注意：如果您正在测试*本地*文件操作（如从 c:\ 和到 c:\），则不必指定主机/登录信息。仅在连接到远程计算机时需要主机/登录信息。
- **目标文件名**－本地或远程测试文件的完整路径和文件名。对于写入和读取/写入操作，在测试创建该文件之前，该文件不得存在。对于读取和比较操作，该文件在测试运行之前必须存在。

  注意：指定路径名时，请确保针对将运行测试的操作系统使用正确类型的斜杠。也就是说，为打算在 UNIX 系统上运行的测试指定目录时使用正斜杠 (/)，为打算在 Windows 上运行的测试指定目录时使用反斜杠 (\)。

  此外，您指定的文件必须在*已安装的*文件系统上存在。SystemEDGE 代理和 SRM 不安装文件系统。
- **用户名（仅 Windows）**－该 FTP 服务器的有效用户名。
- **密码（仅 Windows）**－指定的用户名的密码。SRM 以加密格式存储密码。

  注意：在“验证密码”字段中重新键入密码，以验证您是否正确输入密码。
- **域（仅 Windows）**－登录到服务器的用户的域。

在创建或修改测试时指定这些选项和参数。

示例

本节包括读取、写入、读取/写入和比较操作的示例。每个示例测试每 30 秒运行一次，如果操作不成功，则在 10 秒之后超时。响应和可用性的统计信息每间隔 120 秒计算一次。

示例 1：读取文件

该示例创建监视读取位于 F:\Test\testfile.bin 的文件的时间长度的测试。

在策略中创建新的测试

1. 在“测试监视器”工具栏上单击“+ (新建)”。

   此时将显示“新建测试”窗格。
2. 从“测试类型”列表中选择“文件 I/O”。
3. 在“说明”字段中指定 testfile.bin。
4. 在“测试名称”字段中指定“读取操作”。
5. 在“测试间隔”字段中指定 30。
6. 在“测试超时”字段中指定 10。
7. 在“每间隔抽样数”字段中指定 1。
8. 在“统计窗口”字段中指定 120。
9. 在“文件操作”字段中选择“读取”。
10. 在“目标文件名”字段中指定 F:\Test\testfile.bin。
11. 接受其他的默认值。
12. 单击“保存测试”。

提交认更改时，SRM 将类似于以下内容的条目添加到 svcrsp.cf 文件中：

```
{
index=11
type=fileio
desc="Performing a read operation for testfile.bin."
destination=F:\Test\testFile.bin
args="op=r"
interval=30
samples=1
timeout=10
window=120
tos=0
limit=0
status=active
name="Read Operation"
class=""
context=""
flags="1"
loglevel=3
}
```

示例 2：写入文件

该示例读取 C:\sysedge\bin\saFileIOTest.bin 文件，然后将内容写入 F:\Test\WTest.bin。

在策略中创建新的测试

1. 在“测试监视器”工具栏上单击“+ (新建)”。

   此时将显示“新建测试”窗格。

2. 从“测试类型”列表中选择“文件 I/O”。
3. 在“说明”字段中指定 WTest.bin。
4. 在“测试名称”字段中指定“写入操作”。
5. 在“测试间隔”字段中指定 30。
6. 在“测试超时”字段中指定 10。
7. 在“每间隔抽样数”字段中指定 1。
8. 在“统计窗口”字段中指定 120。
9. 在“文件操作”字段中选择“写入”。
10. 在“目标文件名”字段中指定 F:\Test\WTest.bin。
11. 在“源文件名”字段中指定 C:\sysedge\bin\saFileIOTest.bin。
12. 接受其他的默认值。
13. 单击“保存测试”。

提交认更改时，SRM 将类似于以下内容的条目添加到 svcrsp.cf 文件中：

```
{
index=22
type=fileio
desc="Performing a write operation for WTest.bin."
destination=F:\Test\WTest.bin
args="op=w&local=C:\sysedge\bin\saFileIOTest.bin"
interval=30
samples=1
timeout=10
window=120
tos=0
status=active
name="Write Operation"
class=""
context=""
flags="1"
loglevel=3
}
```

示例 3：写入和读取文件

该示例读取 C:\sysedge\bin\saFileIOTest.bin 文件，将内容写入 F:\Test\RWTest.bin，然后读取 F:\Test\WTest.bin。

在策略中创建新的测试

1. 在“测试监视器”工具栏上单击“+ (新建)”。

   此时将显示“新建测试”窗格。
2. 从“测试类型”列表中选择“文件 I/O”。
3. 在“说明”字段中指定 RWTest.bin。
4. 在“测试名称”字段中指定“读取-写入操作”。
5. 在“测试间隔”字段中指定 30。
6. 在“测试超时”字段中指定 10。
7. 在“每间隔抽样数”字段中指定 1。
8. 在“统计窗口”字段中指定 120。
9. 在“文件操作”字段中选择“读取/写入”。
10. 在“目标文件名”字段中指定 F:\Test\RWTest.bin。
11. 在“源文件名”字段中指定 C:\sysedge\bin\saFileIOTest.bin。
12. 接受其他的默认值。
13. 单击“保存测试”。

提交认更改时，SRM 将类似于以下内容的条目添加到 svcrsp.cf 文件中：

```
{
index=33
type=fileio
desc="Performing a read/write operation for RWTest.bin."
destination=F:\Test\RWTest.bin
args="op=rw&local=C:\sysedge\bin\saFileIOTest.bin"
interval=30
samples=1
timeout=10
window=120
tos=0
status=active
name="Read-Write Operation"
class=""
context=""
flags="1"
loglevel=3
}
```

示例 4：比较两个文件

该示例读取 C:\sysedge\bin\saFileIOTest.bin 文件和 F:\Test\CompTest.bin 文件，并比较两者的内容。

在策略中创建新的测试

1. 在“测试监视器”工具栏上单击“+ (新建)”。

   此时将显示“新建测试”窗格。

2. 从“测试类型”列表中选择“文件 I/O”。
3. 在“说明”字段中指定 CompTest。
4. 在“测试名称”字段中指定“文件比较”。
5. 在“测试间隔”字段中指定 30。
6. 在“测试超时”字段中指定 10。
7. 在“每间隔抽样数”字段中指定 1。
8. 在“统计窗口”字段中指定 120。
9. 在“文件操作”字段中选择“比较”。
10. 在“目标文件名”字段中指定 F:\Test\CompTest.bin。
11. 在“源文件名”字段中指定 C:\sysedge\bin\saFileIOTest.bin。
12. 接受其他的默认值。
13. 单击“保存测试”。

提交认更改时，SRM 将类似于以下内容的条目添加到 svcrsp.cf 文件中：

```
{
index=44
type=fileio
desc="Comparing files."
destination=F:\Test\CompTest.bin
args="op=cmp&local=C:\sysedge\bin\saFileIOTest.bin"
interval=30
samples=1
timeout=10
window=120
tos=0
status=active
name="File Compare"
class=""
context=""
flags="1"
loglevel=3
}
```

有关您在运行文件 I/O 测试时可能遇到的错误的信息，请参阅文件 I/O 测试错误代码 (p. 268)。

FTP 测试

FTP 测试监视登录并测试指定 FTP 服务器所需的时间长度。

选项和参数

FTP 测试需要以下特定选项和参数：

- **FTP 操作**。要测试的 FTP 操作的类型。选择“仅登录”、“获取”或“放入”。如果选择“仅登录”，则指定 FTP 服务器的名称、有效的端口号（默认是 21）、用户名和密码。该测试会使用指定的用户名和密码登录，然后注销。

  如果选择“获取”，则指定 FTP 服务器的名称、有效的端口号（默认是 21）、用户名、密码和远程文件名（要读取的文件的路径）。该测试会登录并读取指定的文件(但是不执行写入操作)，然后注销。如果选择“放入”，则指定 FTP 服务器的名称、有效的端口号（默认是 21）、用户名、密码和要写入 FTP 服务器的本地文件的名称。该测试会登录并将指定的文件写入到 FTP 服务器，然后注销。如果远程目录没有写入权限，测试将失败。

- **FTP 服务器**。正在测试的 FTP 服务器的主机名。

  注意：从 Service Availability r2.1 开始，可以使用 IPv6 地址，但是必须将其括在方括号内，例如 [0aff::230:6eff:fe4b:51db]:8080。此处的 0aff::230:6eff:fe4b:51db 表示 IPv6 地址，8080 表示端口号。

- **FTP 端口**。（可选）运行 FTP 服务的端口（如果未在默认端口 21 上运行的话）。
- **用户名**。该 FTP 服务器的有效用户名。
- **密码**。指定的用户名的密码。SRM 以加密格式存储密码。

  注意：在“验证密码”字段中重新键入密码，以验证您是否正确输入密码。

在创建或修改测试时指定这些选项和参数。

示例

使用该示例创建一个测试，用于监控登录 ftpstage.ca.com 并测试其 FTP 服务状态所需的时间。该示例每 3600 秒（1 小时）测试一次服务器，并等待最多 10 秒以接收成功响应。它计算过去 60.48 万秒钟（1 周）内的响应时间和可用性统计信息。

在策略中创建新的测试

1. 在“测试监视器”工具栏上单击“+ (新建)”。

   此时将显示“新建测试”窗格。
2. 在“测试名称”字段中指定“FTP 测试”。
3. 在“描述”字段中指定“ftptest”
4. 在“测试间隔”字段中指定 3600。
5. 在“测试超时”字段中指定 10。
6. 在“每间隔抽样数”字段中指定 1。
7. 在“统计窗口”字段中指定 604800。
8. 在“FTP 操作”字段中指定“仅登录”。
9. 在“FTP 服务器”字段中指定“ftpstage.mydomain.com”。
10. 接受“FTP 端口”字段中的默认值。
11. 在“用户名”字段中指定“ftpuser”。
12. 在“密码”字段中指定“ftp123”。
13. 接受其他所有字段的默认值。
14. 单击“保存测试”。

提交认更改时，SRM 将类似于以下内容的条目添加到 svcrsp.cf 文件中：

```
{
index=289
type=ftp
desc="ftptest"
dest=ftpstage.mydomain.com:21
username="ftpuser"
encoded=yes
password="bmh12cy"
args="op=login"
interval=3600
samples=1
timeout=10
window=604800
tos=0
limit=0
status=active
name="FTP-Test"
class=""
context=""
flags="1"
loglevel=1
}
```

有关在运行 FTP 测试时可能遇到的错误的信息，请参阅《FTP 测试错误代码》 (p. 268)。

HTTP 测试

HTTP 测试用于监控登录和测试某个网站所需的时间。您可以直接测试站点，也可以使用代理。该测试支持在网页上搜索正则表达式，以及指定想要 HTTP 测试在测试期间遍历的嵌套层数的功能。

默认情况下，SRM 为所有 HTTP 请求使用 HTTP 1.1。它可以处理 HTTP 1.0 响应。

选项和参数

HTTP 测试需要以下特定选项和参数：

- **要测试的 URL**。要测试的系统的主机名。

  注意：从 Service Availability r2.1 开始，可以使用 IPv6 地址，但是必须将其括在方括号内，例如 [0aff::230:6eff:fe4b:51db]:8080。此处的 0aff::230:6eff:fe4b:51db 表示 IPv6 地址，8080 表示端口号。

- **URL 用户名**。(可选)尝试用于访问站点的用户名(如果站点需要 Web 身份验证的话）。

- **URL 密码**。（可选）指定的用户名的密码（如果站点需要 Web 身份验证的话）。SRM 以加密格式存储密码。
- **框架深度**。（可选）下载嵌套框架时测试应遍历的层数。（HTTP 测试在页面下载期间下载所有框架、图像、外部脚本和小程序，以便度量可以反映用户在下载网页时的体验。）默认值为 3。
- **文本匹配**。（可选）您希望 SRM 在测试的页面上匹配的正则表达式或文本字符串。匹配数目显示在代理的“监控”页面上的“结果字段”列中。
- **最小匹配数**。（可选）SRM 必须找到搜索表达式的最小次数（默认为 1）。如果找到搜索表达式的次数少于在该字段中指定的次数，测试将失败（可用性=0）。如果该字段设为零，并且代理找不到搜索表达式，则可用性度量不受影响。
- **下载内容**。选中该框将从代理站点下载所有图像、框架、脚本、小程序以及核心 HTML 代码。
- **遇到内容错误时失败**。选中该框将指定，下载图像、框架、脚本和小程序时遇到任何错误都将导致测试失败。
- **使用代理**。选中该框可对要测试的网站使用代理服务器。如果取消选中该框，则不会显示下列代理选项。
- **代理服务器**。要使用的代理服务器的主机名或 IP 地址（如果您要从中进行测试的系统不能直接访问 Internet 的话）。
- **代理端口**。（可选）要在代理服务器上使用的端口。默认值为 80。
- **代理用户名**。（可选）要在指定代理服务器上验证的有效用户名。
- **代理密码**。（可选）指定的用户名的密码。SRM 以加密格式存储密码。

在创建或修改测试时指定这些选项和参数。

注意：

- 在“验证代理密码”字段中重新键入密码，以验证您是否已正确地输入密码。
- HTTP 测试支持 HTTP 基本身份验证方案和 NTLM 身份验证。有关详细信息，请参考 Web 服务器上的文档。

示例

本节包括用于测试 Web 服务器响应的示例。

示例 1：测试 Web 服务器响应

使用该示例创建一个测试，用于监控访问主页 http://www.ca.com 所需的时间。该示例每 60 秒测试一次服务器，并等待最多 20 秒以接收成功响应。它计算过去 300 秒（5 分钟）内的响应时间和可用性统计信息。

在策略中创建新的测试

1. 在“测试监视器”工具栏上单击“+ (新建)”。

   此时将显示“新建测试”窗格。
2. 从“测试类型”列表中选择“HTTP”。
3. 在“描述”字段中指定“ca_web”。
4. 在“测试名称”字段中指定“ca.com 测试”。
5. 在“测试间隔”字段中指定 60。
6. 在“测试超时”字段中指定 20。
7. 在“每间隔抽样数”字段中指定 1。
8. 在“统计窗口”字段中指定 300。
9. 在“要测试的 URL”字段中指定“http://www.ca.com”。需指定完整的 Web 地址，包括 http://。
10. 接受其他所有字段的默认值。
11. 单击“保存测试”。

提交认更改时，SRM 将类似于以下内容的条目添加到 svcrsp.cf 文件中：

```
{
index=25
type=http
desc="ca-web"
dest="http://www.ca.com"
args="max_depth=3&content_dl=true&content_err=false"
interval=60
samples=1
timeout=20
window=300
tos=0
limit=0
status=active
name="ca.com test"
class=""
context=""
flags="100"
loglevel=3
}
```

示例 2：通过代理测试 Web 服务器响应

使用该示例创建一个测试，用于监控访问主页 http://www.weather.com 所需的时间。在该示例中，测试通过正在端口 8080 上运行的代理服务器 (myproxy) 访问 weather.com 网站。该示例每 60 秒测试一次服务器，并等待最多 20 秒以接收成功响应。它计算过去 300 秒（5 分钟）内的响应时间和可用性统计信息。

在策略中创建新的测试

1. 在“测试监视器”工具栏上单击“+ (新建)”。

   此时将显示“新建测试”窗格。

2. 从“测试类型”列表中选择“HTTP”。
3. 在“描述”字段中指定“weather.com_proxy”。
4. 在“测试名称”字段中指定“代理测试”。
5. 在“测试间隔”字段中指定 60。
6. 在“测试超时”字段中指定 20。
7. 在“每间隔抽样数”字段中指定 1。
8. 在“统计窗口”字段中指定 300。
9. 在“要测试的 URL”字段中指定“http://www.weather.com”。需指定完整的 Web 地址，包括 http://。
10. 在“代理服务器”字段中指定“myproxy”。
11. 在“代理端口”字段中指定“8080”。

12. 接受其他所有字段的默认值。
13. 单击“保存测试”。

提交认更改时，SRM 将类似于以下内容的条目添加到 svcrsp.cf 文件中：

```
{
index=26
type=http
desc="weather.com_proxy"
dest="http://www.weather.com"
args="max_depth=3&content_dl=true&content_err=false&proxy=myproxy:8080"
interval=60
samples=1
timeout=20
window=300
tos=0
status=active
name="Proxy test"
class=""
context=""
flags="100"
loglevel=3
}
```

示例 3：匹配 Web 服务器内容

使用该示例创建一个测试，用于从 http://www.weather.com 下载网页并在内容中搜索正则表达式，"cumulus." SRM 记录该表达式在测试的“结果”字段中出现的次数。该示例每 60 秒测试一次服务器，并等待最多 20 秒以接收成功响应。它计算过去 300 秒（5 分钟）内的响应时间和可用性统计信息。您可以使用类似的示例，通过指定 HTTPS 测试类型和安全 Web 服务器来测试 HTTPS 测试的内容。

在策略中创建新的测试

1. 在“测试监视器”工具栏上单击“+ (新建)”。

   此时将显示“新建测试”窗格。
2. 从“测试类型”列表中选择“HTTP”。
3. 在“描述”字段中指定“weather.com_content”。
4. 在“测试名称”字段中指定“测试 http://www.weather.com 上的 Web 内容”。
5. 在“测试间隔”字段中指定 60。
6. 在“测试超时”字段中指定 20。
7. 在“每间隔抽样数”字段中指定 1。
8. 在“统计窗口”字段中指定 300。

9. 在“要测试的 URL”字段中指定“http://www.weather.com”。需指定完整的 Web 地址，包括 http://。
10. 在“框架深度”字段中，接受默认值 3，搜索站点的 3 个层次以查找搜索文本。
11. 在“文本匹配”字段中输入“cumulus”。
12. 接受其他所有字段的默认值。
13. 单击“保存测试”。

在您确认对测试的更改时，SRM 会将类似以下内容的条目添加到 svcrsp.cf 文件中：

```
{
index=27
type=http
desc="weather.com."
dest="http://www.weather.com_content"
args="max_depth=3&search=cumulus&minmatch=1&content_dl=true&content_err=false
"
interval=60
samples=1
timeout=20
window=300
tos=0
limit=0
status=active
name="Web server content"
class=""
context=""
flags="1"
loglevel=1
}
```

有关在运行 HTTP 测试时可能遇到的错误的信息，请参阅《HTTP 测试错误代码》 (p. 268)。

HTTPS 测试

HTTPS 测试用于监控登录和测试某个安全网站所需的时间。您可以直接测试站点，也可以使用代理。您还可以在网页上搜索正则表达式，并可以指定想要 HTTPS 测试在测试期间遍历的嵌套层数。

默认情况下，SRM 为所有 HTTP 请求使用 HTTP 1.1。它可以处理 HTTP 1.0 响应。

选项和参数

HTTPS 测试需要以下特定选项和参数：

- **要测试的 URL**。要测试的安全网站的主机名。

  注意：可以使用 IPv6 地址，但是必须将其括在括号内，例如 [0aff::230:6eff:fe4b:51db]:8080。例如，0aff::230:6eff:fe4b:51db 表示 IPv6 地址，8080 表示端口号。

- **用户名**。（可选）正在测试的站点的用户名（如果站点需要 Web 身份验证的话）。
- **密码**。（可选）指定的用户名的密码（如果站点需要 Web 身份验证的话）。SRM 以加密格式存储密码。
- **框架深度**。（可选）下载嵌套框架时测试应遍历的层数。（HTTPS 测试在页面下载期间下载所有框架、图像、外部脚本和小程序，以便度量可以反映用户在下载网页时的体验。）默认值为 3。
- **文本匹配**。（可选）您希望 SRM 在测试的页面上匹配的正则表达式或文本字符串。匹配数目显示在代理的“监控”页面上的“结果字段”列中。
- **最小匹配数**。（可选）SRM 必须找到搜索表达式的最小次数（默认为 1）。如果找到搜索表达式的次数少于在该字段中指定的次数，测试将失败（可用性=0）。如果该字段设为零，并且代理找不到搜索表达式，则可用性度量不受影响。
- **下载内容**。选中该框将从代理站点下载所有图像、框架、脚本、小程序以及核心 HTML 代码。
- **遇到内容错误时失败**。选中该框将指定，下载图像、框架、脚本和小程序时遇到任何错误都将导致测试失败。
- **使用代理**。选中该框可对要测试的网站使用代理服务器。如果不选中该框，则下列代理选项不会出现在屏幕上。
- **代理服务器**。要使用的代理服务器的主机名或 IP 地址（如果您要从中进行测试的系统不能直接访问 Internet 的话）
- **代理端口**。（可选）要在代理服务器上使用的端口。默认值为 80。
- **代理用户名**。（可选）要在指定代理服务器上验证的有效用户名。
- **代理密码**。（可选）指定的用户名的密码。SRM 以加密格式存储密码。

在创建或修改测试时指定这些选项和参数。

注意：

- 在“验证代理密码”字段中重新键入密码，以验证您是否已正确地输入密码。
- HTTP 测试仅支持 HTTP 基本身份验证方案。有关详细信息，请参考 Web 服务器上的文档。

不受信任的 SSL 证书

如果证书无效（不受信任）或访问的网站地址与 SSL 证书不匹配，HTTPS 网站会显示一个 SSL 证书。

要允许不受信任的 SSL 证书，必须取消注释（即删除“#”）svcrsp.cf 配置文件中的“allow_untrusted_ssl_certificates”。

示例

使用该示例创建一个测试，用于监控访问安全网站 https://chargeMycredit.com 的主页所需的时间。该示例每 60 秒测试一次服务器，并等待最多 20 秒以接收成功响应。它计算过去 300 秒钟（5 分钟）内的响应时间和可用性统计信息。

在策略中创建新的测试

1. 在“测试监视器”工具栏上单击“+ (新建)”。

   此时将显示“新建测试”窗格。
2. 从“测试类型”列表中选择“HTTPS”。
3. 在“描述”字段中指定“chargeMycredit web”。
4. 在“测试名称”字段中指定“HTTPS 测试”。
5. 在“测试间隔”字段中指定 60。
6. 在“测试超时”字段中指定 20。
7. 在“每间隔抽样数”字段中指定 1。
8. 在“统计窗口”字段中指定 300。
9. 在“要测试的 URL”字段中指定“https://chargeMycredit.com”。需指定完整的 Web 地址，包括 https://。
10. 在“用户名”字段中指定“creditAcct”。
11. 在“密码”字段中指定“secret”。

12. 接受其他所有字段的默认值。
13. 单击“保存测试”。

提交认更改时，SRM 将类似于以下内容的条目添加到 svcrsp.cf 文件中：

```
{
index=27
type=https
desc="Test secure Web response at https://chargeMycredit.com"
dest="https://chargeMycredit.com"
username="creditAcct"
encoded=yes
password="ibwc3m"
args="max_depth=3&minmatch=1&content_dl=true&content_err=false"
interval=60
samples=1
timeout=20
window=300
tos=0
limit=0
status=active
name="HTTPS-Test"
class=""
context=""
flags="1"
loglevel=1
}
```

有关在运行 HTTPS 测试时可能遇到的错误的信息，请参阅《HTTPS 测试错误代码》 (p. 268)。

IMAP 测试

IMAP 测试用于监控登录到某个用户帐户并从 IMAP 服务器下载邮件所需的时间。IMAP 协议支持使用 SEARCH 命令对邮箱进行选择性筛选和搜索的功能。

选项和参数

IMAP 测试需要以下特定选项和参数：

- **IMAP 服务器**。IMAP 邮件服务器的主机名。

  注意：从 Service Availability r2.1 开始，可以使用 IPv6 地址，但是必须将其括在方括号内，例如 [0aff::230:6eff:fe4b:51db]:8080。此处的 0aff::230:6eff:fe4b:51db 表示 IPv6 地址，8080 表示端口号。

- **IMAP 端口**。（可选）运行 IMAP 服务的端口。默认值为 143。
- **用户名**。该服务器上的测试 IMAP 帐户的有效用户名。*不要*使用活动的邮箱，请创建一个测试帐户。

- **密码**。用户帐户的有效密码。SRM 以加密格式存储密码。
- **下载**。请从下列选项中选择一个：
  - **下载第一个邮件**－该选项仅下载该用户帐户的第一个邮件。
  - **下载所有邮件**－该选项下载该用户帐户的所有邮件。
- **删除下载的邮件**。（可选）选中该复选框可删除在测试期间下载的邮件，将其留空则可将邮件保留在测试系统中。

  注意：如果您使用“下载所有邮件”选项，并且如果下载失败，将删除测试邮箱中的部分邮件并重试测试。

在创建或修改测试时指定这些选项和参数。

示例

使用该示例创建一个测试，用于每 300 秒从 imapserver.yourdomain 下载一次 IMAPuser 帐户的所有邮件，并在下载之后删除这些邮件。测试等待最多 10 秒以接收成功响应，并计算过去 7200 秒钟（2 小时）内的响应时间和可用性统计信息。

在策略中创建新的测试

1. 在“测试监视器”工具栏上单击“+ (新建)”。

   此时将显示“新建测试”窗格。
2. 从“测试类型”列表中选择“IMAP”。
3. 在“描述”字段中指定“IMAP_Test”。
4. 在“测试名称”字段中指定“测试 IMAP 服务”。
5. 在“测试间隔”字段中指定 300。
6. 在“测试超时”字段中指定 10。
7. 在“每间隔抽样数”字段中指定 1。
8. 在“统计窗口”字段中指定 7200。
9. 在“IMAP 服务器”字段中输入“imapserver.yourdomain”。
10. 在“IMAP 端口”字段中，接受默认值 143。
11. 在“用户名”字段中指定“IMAPuser@server.domain”。
12. 在“密码”字段中指定“IMAP123”。
13. 在“下载”字段中选择“下载所有邮件”。
14. 选择“删除下载的邮件”。

15. 接受其他所有字段的默认值。
16. 单击“保存测试”。

提交认更改时，SRM 将类似于以下内容的条目添加到 svcrsp.cf 文件中：

```
{
index=60
type=imap
desc="IMAP_Test."
dest="imapserver.yourdomain.com:143"
args="download=Download All Messages&delete=true"
username="IMAPuser@server.domain"
encoded=yes
password="c4nrxzw"
interval=300
samples=1
timeout=10
window=7200
tos=0
limit=0
status=active
name="Test IMAP Service"
class=""
context=""
flags="1"
loglevel=1
}
```

有关在运行 IMAP 测试时可能遇到的错误的信息，请参阅《IMAP 测试错误代码》 (p. 274)。

LDAP 测试

LDAP 测试用于监控连接到 Windows 系统上的 LDAP 服务，执行一次标准的用户名/密码身份验证，然后执行一次用户定义的查询所需的时间。

选项和参数

LDAP 测试需要以下特定选项和参数：

- **LDAP 服务器所在的域**。正在测试的 LDAP 服务器的主机名或 IP 地址。

  注意：可以使用 IPv6 地址，但是必须将其括在括号内，例如 [0aff::230:6eff:fe4b:51db]:8080。此处的 0aff::230:6eff:fe4b:51db 表示 IPv6 地址，8080 表示端口号。
- **LDAP 域**。（可选）LDAP 服务器所在的域。
- **LDAP 端口**。（可选）运行 LDAP 服务的端口。默认值为端口 389。

- **用户名**。（可选）LDAP 服务器的有效用户名。
- **密码**。（可选）指定的用户名的密码。SRM 以加密格式存储密码。
- **查询**。要执行的 LDAP 查询。有关 LDAP 查询语言的信息，请参阅 LDAP 文档。
- **筛选器**。（可选）用于根据其筛选查询结果的参数。

在创建或修改测试时指定这些选项和参数。

示例

本节包括用于监控连接到本地 LDAP 服务器和远程 LDAP 服务器的时间的示例。

示例 1：测试本地 LDAP 服务器

使用该示例创建一个测试，用于监控连接到名为 arch 的本地 LDAP 服务器，验证用户名 ldapUser 和编码的密码，然后查询术语 annuity 的时间。

在策略中创建新的测试

1. 在“测试监视器”工具栏上单击“+ (新建)”。

   此时将显示“新建测试”窗格。
2. 从“测试类型”列表中选择“LDAP”。
3. 在“描述”字段中指定“ldap_arch”。
4. 在“测试名称”字段中指定“本地 LDAP 测试”。
5. 在“测试间隔”字段中指定 30。
6. 在“测试超时”字段中指定 10。
7. 在“每间隔抽样数”字段中指定 1。
8. 在“统计窗口”字段中指定 120。
9. 在“LDAP 服务器”字段中指定“arch”。
10. 在“LDAP 域”字段中指定“TEST”。
11. 在“用户名”字段中指定“ldapUser”。
12. 在“密码”字段中指定“ldapPassword”。
13. 在“查询”字段中指定“cn=annuity,ou=Boston,dc=fleet,dc=com”。
14. 在“筛选”字段中指定 cn=*。
15. 单击“保存测试”。

提交认更改时，SRM 将类似于以下内容的条目添加到 svcrsp.cf 文件中：

```
{
index=11
type=ldap
desc="LDAP-TEST"
dest="arch"
username="ldapUser"
encoded=yes
password="Z28ySGVsbA"
args="query=cn=annuity,ou=Boston,dc=fleet,dc=com&domain=Test&filter=cn=*"
interval=30
samples=1
timeout=10
window=120
tos=0
limit=0
status=active
name="Local LDAP Test"
class=""
context=""
flags="1"
loglevel=1
}
```

示例 2：测试远程 LDAP 服务器

使用该示例创建一个测试，用于监控连接到位于 10.0.0.123 的远程 LDAP 服务器，验证用户名 ldapRUser 和编码的密码，然后查询条件来宾用户的时间。

在策略中创建新的测试

1. 在“测试监视器”工具栏上单击“+ (新建)”。

   此时将显示“新建测试”窗格。

2. 从“测试类型”列表中选择“LDAP”。
3. 在“描述”字段中指定“ldap_remote”。
4. 在“测试名称”字段中指定“远程 LDAP 测试”。
5. 在“测试间隔”字段中指定 30。
6. 在“测试超时”字段中指定 10。
7. 在“每间隔抽样数”字段中指定 1。
8. 在“统计窗口”字段中指定 120。
9. 在“LDAP 服务器”字段中指定“10.0.0.123”。
10. 在“LDAP 域”字段中指定“Test”。
11. 在“用户名”字段中指定“ldapRUser”。

12. 在“密码”字段中指定“ldapRPass”。
13. 在“查询”字段中指定 cn=Guest,cn=Users,dc=testlab,dc=com。
14. 在“筛选”字段中指定 cn=*。
15. 单击“保存测试”。

提交认更改时，SRM 将类似于以下内容的条目添加到 svcrsp.cf 文件中：

```
{
index=23
type=ldap
desc="ldap_remote"
dest="10.0.0.123:389"
username="ldapRUser"
encoded=yes
password="bXVyaWM"
args="query=cn=guest,cd=users,dc=testlab,dc=com&domain=Test&filter=cn=*"
interval=30
samples=1
timeout=10
window=120
tos=0
limit=0
status=active
name="Remote LDAP Test"
class=""
context=""
flags="1"
loglevel=1
}
```

有关在运行 LDAP 测试时可能遇到的错误的信息，请参阅《LDAP 测试错误代码》 (p. 274)。

MAPI 测试

MAPI 测试用于监控登录到用户帐户并从 MAPI 服务器*发送*或*检索*邮件所需的时间。

注意：MAPI 是专有的 Microsoft 协议。MAPI 测试使用 Microsoft Extended MAPI 协议。鉴于此，MAPI 测试必须起源于当前运行 Microsoft Exchange 或 Microsoft Outlook 的 Windows 服务器 （Outlook Express 不符合要求，因为其未安装正确的 API。）MAPI 测试需要 MAPI 服务器来指定默认邮件存储和通讯簿提供商。

选项和参数

MAPI 测试需要以下特定选项和参数：

- **操作**。选择要执行的邮件测试的类型：“发送”还是“检索”。
- **MAPI 服务器**。MAPI 邮件服务器的主机名。该系统必须与您在“用户名”字段中指定的用户位于相同域中。您从其运行 SRM 测试的系统也必须位于同一域中。

  注意：可以使用 IPv6 地址，但是必须将其括在括号内，例如 [0aff::230:6eff:fe4b:51db]:8080。此处的 0aff::230:6eff:fe4b:51db 表示 IPv6 地址，8080 表示端口号。
- **用户名**。Exchange 服务器上的测试 MAPI 帐户的有效用户名。该用户必须在安装 SRM 的系统上具有“作为服务登录”的权限，以便验证收件人的身份。不要使用活动用户帐户进行该测试；请在与要测试的 MAPI 服务器相同的域中创建一个测试帐户，并确保该帐户具有“作为服务登录”的权限。
- **密码**。用户帐户的有效密码。密码已加密。

  注意：必须在“验证密码”字段中重新键入密码，以验证您是否已正确地输入密码。
- **用户域**。MAPI 用户帐户所在的 Windows 域。您正在测试的系统和用户必须位于相同域中。
- **邮件收件人**。（仅发送）邮件服务器所知道的有效邮件收件人的电子邮件地址。
- **邮件正文大小**。（仅发送）要发送的测试邮件的大小。默认值为 4096 字节。
- **下载**。（仅检索）选择以下内容之一：
  - **下载第一个邮件**。该选项仅下载该用户帐户的第一个邮件。
  - **下载所有邮件**。该选项下载该用户帐户的所有邮件。
- **删除下载的邮件**。（仅检索－可选）选中该复选框可删除在测试期间下载的邮件，将其留空则可将邮件保留在测试系统中。

在创建或修改测试时指定这些选项和参数。

指定“作为服务登录”权限

1. 打开“管理工具”控制面板。
2. 双击“本地安全策略 -> 本地策略 -> 用户权限分配”。

   将在右侧窗格中显示策略列表。

3. 双击“作为服务登录”。

   此时会显示“作为服务登录”对话框。

4. 单击“添加”。

   即会出现“选择用户或组”对话框。

5. 选择您想要添加到该策略的名称，单击“添加”，然后单击“确定”。

   注意：必须在用户所属的同一个域上运行该测试。

示例 1

使用该示例创建一个测试，用于每 120 秒在 mapiserver.yourdomain 上的 MAPI 用户帐户中下载一次第一封邮件，并在下载之后将其删除。测试等待最多 10 秒以接收成功响应，并计算过去 3600 秒钟（2 小时）内的响应时间和可用性统计信息。

在策略中创建新的测试

1. 在“测试监视器”工具栏上单击“+ (新建)”。

   此时将显示“新建测试”窗格。

2. 在“操作”字段中选择“发送”。
3. 从“测试类型”列表中选择“MAPI”。
4. 在“描述”字段中指定“MAPI-Test”。
5. 在“测试名称”字段中指定“MAPI-Test”。
6. 在“测试间隔”字段中指定 120。
7. 在“测试超时”字段中指定 10。
8. 在“每间隔抽样数”字段中指定 1。
9. 在“统计窗口”字段中指定 3600。
10. 在“MAPI 服务器”字段中输入“mapiserver.yourdomain.com”。
11. 在“用户名”字段中指定“MAPIuser”。
12. 在“密码”字段中，指定 MAPI123。
13. 在“验证密码”字段中指定“MAPI123”。
14. 在“用户域”字段中指定“myDomain”。
15. 在“邮件收件人”字段中指定“congo@yourdomain.com”。
16. 接受默认邮件正文大小（256 字节）。
17. 接受其他所有字段的默认值。
18. 单击“保存测试”。

提交认更改时，SRM 将类似于以下内容的条目添加到 svcrsp.cf 文件中：

```
{
index=71
type=mapi
desc="MAPI-Test"
dest="mapiserver.yourdomain.com"
username="MAPIuser"
encoded=yes
password="xlrpm6v"
args="domain=myDomain&op=send&to=congo@yourdomain.com&size=256"
interval=120
samples=1
timeout=10
window=3600
tos=0
limit=0
status=active
name="MAPI-Test"
class=""
context=""
flags="1"
loglevel=1
}
```

示例 2

使用该示例创建一个测试，用于每 120 秒在 mapiserver.yourdomain.com 上的已知 MAPI 用户帐户检索一次第一封邮件，并在下载之后将其删除。测试等待最多 10 秒以接收成功响应，并计算过去 3600 秒钟（2 小时）内的响应时间和可用性统计信息。

在策略中创建新的测试

1. 在“测试监视器”工具栏上单击“+ (新建)”。

   此时将显示“新建测试”窗格。

2. 在“操作”字段中选择“检索”。
3. 从“测试类型”列表中选择“MAPI”。
4. 在“描述”字段中指定“MAPI_Retrieve_Test”。
5. 在“测试名称”字段中指定“MAPI 检索测试”。
6. 在“测试间隔”字段中指定 120。
7. 在“测试超时”字段中指定 10。
8. 在“每间隔抽样数”字段中指定 1。
9. 在“统计窗口”字段中指定 3600。
10. 在“MAPI 服务器”字段中输入“mapiserver.yourdomain.com”。

11. 在“用户名”字段中指定“MAPIuser”。
12. 在“密码”字段中，指定 MAPI123。
13. 在“验证密码”字段中指定“MAPI123”。
14. 在“用户域”字段中指定“myDomain”。
15. 选择“删除下载的邮件”。
16. 单击“保存测试”。

提交认更改时，SRM 将类似于以下内容的条目添加到 svcrsp.cf 文件中：

```
{
index=31
type=mapi
desc="MAPI_Retrieve_Test"
dest="mapiserver.yourdomain.com"
username="MAPIuser"
encoded=yes
password="bufwate2"
args="domain=myDomain&op=recv&download=first&delete=yes"
interval=60
samples=1
timeout=30
window=300
tos=0
limit=0
status=active
name="MAPI Retrieve Test"
class=""
context=""
flags="1"
loglevel=1
}
```

有关在运行 MAPI 测试时可能遇到的错误的信息，请参阅《MAPI 测试错误代码》 (p. 274)。

NIS/NIS+ 测试

NIS/NIS+ 测试监控登录到指定 NIS 或 NIS+ 服务器并请求一个特定映射文件所需的时间。您也可以选择下载该映射文件。

选项和参数

NIS/NIS+ 测试需要以下特定选项和参数：

- **NIS 服务器**。NIS 服务器的主机名。

  注意：可以使用 IPv6 地址，但是必须将其括在括号内，例如 [0aff::230:6eff:fe4b:51db]:8080。此处的 0aff::230:6eff:fe4b:51db 表示 IPv6 地址，8080 表示端口号。

- **NIS 域**。映射文件所在的域。
- **NIS 映射**。要测试的映射文件。默认为主机文件。
- **下载 NIS 映射？**选择以下选项之一：
  - **是**。该选项可下载映射文件。
  - **否(仅验证)**。该选项验证映射文件是否存在，但不下载。

在创建或修改测试时指定这些选项和参数。

示例

使用该示例创建一个测试，用于每 300 秒从 nisserver.yourdomain 上的测试域下载一次主机映射文件。测试等待最多 20 秒以接收成功响应，并计算过去 7200 秒钟（2 小时）内的响应时间和可用性统计信息。

在策略中创建新的测试

1. 在“测试监视器”工具栏上单击“+ (新建)”。

   此时将显示“新建测试”窗格。

2. 从“测试类型”列表中选择“NIS”。
3. 在“描述”字段中指定“NIS_Test”。
4. 在“测试名称”字段中指定“NIS-Test”。
5. 在“测试间隔”字段中指定 300。
6. 在“测试超时”字段中指定 20。
7. 在“每间隔抽样数”字段中指定 1。
8. 在“统计窗口”字段中指定 7200。
9. 在“NIS 域”字段中输入“Test.com”。
10. 在“NIS 服务器”字段中输入“nisserver.yourdomain.com”。
11. 在“NIS 映射”字段中，接受默认主机。
12. 在“下载 NIS 映射?” 字段中选择“是”。

13. 接受其他所有字段的默认值。
14. 单击“保存测试”。

提交认更改时，SRM 将类似于以下内容的条目添加到 svcrsp.cf 文件中：

```
{
index=63
type=nis
desc="NIS-Test"
dest="nisserver.yourdomain"
args="domain=Test.com&map=hosts&download=true"
interval=300
samples=1
timeout=20
window=7200
tos=0
limit=0
status=active
name="NIS-Test"
class=""
context=""
flags="1"
loglevel=1
}
```

有关在运行 NIS 或 NIS+ 测试时可能遇到的错误的信息，请参阅《NIS 测试错误代码》 (p. 274)。

NNTP 测试

NNTP 测试监控连接到 NNTP 服务器并执行一次简单事务所需的时间。

选项和参数

NNTP 测试需要以下特定选项和参数：

- **NNTP 服务器**。要测试的新闻服务器的主机名。

  注意：可以使用 IPv6 地址，但是必须将其括在括号内，例如 [0aff::230:6eff:fe4b:51db]:8080。此处的 0aff::230:6eff:fe4b:51db 表示 IPv6 地址，8080 表示端口号。

- **NNTP 端口**。（可选）运行 NNTP 服务的端口。默认值为端口 119。

在创建或修改测试时指定这些选项和参数。

示例

使用该示例创建一个测试，用于监控连接到 new.yourdomain 上的 NNTP 服务并执行一次简单事务所需的时间。该示例每 3600 秒（1 小时）测试一次服务器，并等待最多 10 秒以接收成功响应。它计算过去 86400 秒钟（1 天）内的响应时间和可用性统计信息。

在策略中创建新的测试

1. 在“测试监视器”工具栏上单击“+ (新建)”。

   此时将显示“新建测试”窗格。

2. 从“测试类型”列表中选择“NNTP”。
3. 在“描述”字段中指定“新闻测试”。
4. 在“测试名称”字段中指定“新闻测试”。
5. 在“测试间隔”字段中指定 3600。
6. 在“测试超时”字段中指定 10。
7. 在“每间隔抽样数”字段中指定 1。
8. 在“统计窗口”字段中指定 86400。
9. 在“NNTP 服务器”字段中指定“news.yourdomain.com”。
10. 在“NNTP 端口”字段中，接受默认端口 119。
11. 接受其他所有字段的默认值。
12. 单击“保存测试”。

提交认更改时，SRM 将类似于以下内容的条目添加到 svcrsp.cf 文件中：

```
{
index=41
type=nntp
desc="NewsTest"
dest="news.yourdomain.com"
args=" "
interval=3600
samples=1
timeout=10
window=86400
tos=0
limit=0
status=active
name="News Test"
class=""
context=""
flags="1"
loglevel=1
}
```

有关在运行 NNTP 测试时可能遇到的错误的信息，请参阅《NNTP 测试错误代码》 (p. 274)。

ping 测试

ping 测试用于监控执行服务器的网络层 ping 操作所需的时间。通过该测试，可以确定系统是否正在运行以及网络连接是否存在。

选项和参数

ping 测试需要以下特定选项和参数：

- **目标**。要对其执行 ping 操作的系统的主机名。

  注意：可以使用 IPv6 地址，但是必须将其括在括号内，例如 [0aff::230:6eff:fe4b:51db]:8080。此处的 0aff::230:6eff:fe4b:51db 表示 IPv6 地址，8080 表示端口号。
- **负载**。（可选）在 ping 操作中发送的软件包的大小。默认数据包大小是 64 字节。

在创建或修改测试时指定这些选项和参数。

示例

使用该示例创建一个测试，用于每 60 秒在 server.yourdomain 上测试系统三次，并等待最多 5 秒以接收成功响应。它计算过去 3600 秒钟（1 小时）内的响应时间和可用性统计信息。

在策略中创建新的测试

1. 在“测试监视器”工具栏上单击“+ (新建)”。

   此时将显示“新建测试”窗格。
2. 从“测试类型”列表中选择“Ping”。
3. 在“描述”字段中指定“server.yourdomain_ping”。
4. 在“测试名称”字段中指定“ping 测试”。
5. 在“测试间隔”字段中指定 60。
6. 在“测试超时”字段中指定 5。
7. 在“每间隔抽样数”字段中指定 3。
8. 在“统计窗口”字段中指定 3600。
9. 在“目标”字段中指定“server.yourdomain.com”。
10. 在“负载”字段中，接受 64 字节的默认软件包大小。

11. 接受其他所有字段的默认值。
12. 单击“保存测试”。

提交认更改时，SRM 将类似于以下内容的条目添加到 svcrsp.cf 文件中：

```
{
index=45
type=ping
desc="server.yourdomain_Ping"
dest="server.yourdomain.com"
args="payload=64"
interval=60
samples=3
timeout=5
window=3600
tos=0
limit=0
status=active
name="Ping Test"
class=""
context=""
flags="100"
loglevel=2
}
```

有关在运行 ping 测试时可能遇到的错误的信息，请参阅《ping 测试错误代码》 (p. 274)。

POP3 测试

POP3 测试用于监控登录到某个用户帐户并从 POP3 服务器下载邮件所需的时间。

选项和参数

POP3 测试需要以下特定选项和参数：

- **POP3 服务器**。POP3 邮件服务器的主机名。

  注意：可以使用 IPv6 地址，但是必须将其括在括号内，例如 [0aff::230:6eff:fe4b:51db]:8080。此处的 0aff::230:6eff:fe4b:51db 表示 IPv6 地址，8080 表示端口号。

- **POP3 端口**。（可选）运行 POP3 服务的端口。默认值为 110。
- **用户名**。该服务器上的测试 POP3 帐户的有效用户名。*不要*使用活动的邮箱，请创建一个测试帐户。

- **密码**。用户帐户的有效密码。SRM 以加密格式存储密码。
- **下载**。选择以下选项之一：
  - **下载第一个邮件**。该选项仅下载该用户帐户的第一个邮件。
  - **下载所有邮件**。该选项下载该用户帐户的所有邮件。
- **删除下载的邮件**。（可选）选中该复选框可删除在测试期间下载的邮件，将其留空则可将邮件保留在测试系统中。

在创建或修改测试时指定这些选项和参数。

示例

使用该示例创建一个测试，用于每 300 秒从 popserver.yourdomain.com 下载一次 POPuser 帐户的所有邮件，并在下载之后删除这些邮件。测试等待最多 10 秒以接收成功响应，并计算过去 21600 秒钟（6 小时）内的响应时间和可用性统计信息。

在策略中创建新的测试

1. 在“测试监视器”工具栏上单击“+ (新建)”。

   此时将显示“新建测试”窗格。
2. 从“测试类型”列表中选择“POP3”。
3. 在“描述”字段中指定“popserver.yourdomain_test”。
4. 在“测试名称”字段中指定“POP3 测试”。
5. 在“测试间隔”字段中指定 300。
6. 在“测试超时”字段中指定 10。
7. 在“每间隔抽样数”字段中指定 1。
8. 在“统计窗口”字段中指定 21600。
9. 在“POP3 服务器”字段中输入“popserver.yourdomain”。
10. 在“POP3 端口”字段中指定“8080”。
11. 在“用户名”字段中指定“POPuser@yourdomain.com”。
12. 在“密码”字段中指定“POP123”。
13. 在“下载”字段中选择“下载所有邮件”。
14. 选择“删除下载的邮件”。
15. 接受其他所有字段的默认值。
16. 单击“保存测试”。

提交认更改时，SRM 将类似于以下内容的条目添加到 svcrsp.cf 文件中：

```
{
index=51
type=pop3
desc="popserver.yourdomain_test"
dest="popserver.yourdomain.com:8080"
username="POPuser"
encoded=yes
password="ijl3r2kr"
args="download=all&delete=yes"
interval=300
samples=1
timeout=10
window=21600
tos=0
limit=0
status=active
name="POP3 Test"
class=""
context=""
flags="1"
loglevel=1
}
```

有关在运行 POP 测试时可能遇到的错误的信息，请参阅《POP 测试错误代码》 (p. 274)。

往返电子邮件测试

往返电子邮件测试用于监控通过 SMTP 或 MAPI 将电子邮件发送到 POP3、IMAP 或 MAPI 电子邮件系统并从该服务器下载该邮件所需的时间。

选项和参数

往返电子邮件测试需要以下特定选项和参数：

- **邮件发送类型**。往返电子邮件测试支持 **SMTP** 和 **MAPI** 协议。选择一个。显示在该选项下方的字段将反映您选择的协议的类型。
- **SMTP|MAPI 服务器**。SMTP 或 MAPI 邮件服务器的主机名（发起电子邮件的服务器）。

  注意：可以使用 IPv6 地址，但是必须将其括在括号内，例如 [0aff::230:6eff:fe4b:51db]:8080。此处的 0aff::230:6eff:fe4b:51db 表示 IPv6 地址，8080 表示端口号。
- **SMTP 端口**。（可选）。运行 SMTP 服务的端口。默认值为 25。
- **SMTP|MAPI 邮件收件人**。测试将电子邮件发送到的帐户的名称。

- **SMTP|MAPI 邮件正文大小**。（可选）要发送的测试邮件的大小。默认值为 4096 字节。
- **发件人主机名**。（仅适用于 SMTP，可选）指定发件人的主机名（例如，*service_availability@hostname*）。默认为代理主机名。

  注意：从 Service Availability r2.1 开始，可以使用 IPv6 地址，但是必须将其括在方括号内，例如 [0aff::230:6eff:fe4b:51db]:8080。此处的 0aff::230:6eff:fe4b:51db 表示 IPv6 地址，8080 表示端口号。
- **SNMP|MAPI 用户名**。（对 SMTP 为可选）发送电子邮件的测试邮件帐户的有效用户名。不要使用活动邮箱；请创建一个测试帐户，确保在删除测试电子邮件时不会删除有效的电子邮件。
- **SNMP|MAPI 密码**。测试用户帐户的有效密码。SRM 以加密格式存储密码。（对 SMTP 为可选）
- **用户域**。（仅适用于 MAPI 测试）发送电子邮件的用户帐户所在的域。
- **使用 SSL/TLS**。（仅适用于 SMTP）如果 SMTP 服务器需要 SSL/TLS 身份验证，选中该复选框选项可启用安全套接字层 (SSL)/传输层安全性。
- **邮件检索类型**。用来检索电子邮件的邮件服务的类型。选择以下选项之一：
  - **POP3**。
  - **IMAP**。
  - **MAPI**。

    注意：MAPI 测试需要 Extended MAPI API。因此，MAPI 测试必须从运行 Microsoft Exchange 或 Microsoft Outlook *（不是* Outlook Express。Outlook Express 不包括适用于该测试的正确 API）的 Windows 服务器发起。
- **POP3|IMAP|MAPI 服务器**。邮件发送到的服务器的主机名。

  注意：可以使用 IPv6 地址，但是必须将其括在括号内，例如 [0aff::230:6eff:fe4b:51db]:8080。此处的 0aff::230:6eff:fe4b:51db 表示 IPv6 地址，8080 表示端口号。
- **POP3|IMAP 端口**。（可选）。运行邮件服务的端口。POP3 默认为 110，IMAP 默认为 143。
- **用户名**。接收电子邮件的测试邮件帐户的有效用户名。不要使用活动的邮箱，请创建一个测试帐户。
- **密码**。测试用户帐户的有效密码。SRM 以加密格式存储密码。
- **用户域**。（仅适用于 MAPI 测试）接收电子邮件的用户帐户所在的域。
- **轮询间隔**。检查收件人电子邮件帐户是否收到邮件的时间间隔。默认为 500 毫秒。

注意：每个间隔使用一个样本至少运行往返电子邮件测试 5 分钟。

在创建或修改测试时指定这些选项和参数。

该测试按电子邮件的标题和时间戳/日期戳进行匹配。它在每次运行时均会创建然后删除用户配置文件，并始终在测试结束时删除电子邮件然后注销。

示例

使用该示例创建一个测试，用于监控将 2000 字节的测试电子邮件从 server.mydomain 上的邮件服务器发送到邮件服务器 server.yourdomain 上的帐户 (you@yourdomain.com) 所需的时间。测试等待最多 5 秒以接收成功响应，使用 POP3 下载邮件并计算过去 86400 秒钟（1 天）内的响应时间和可用性统计信息。

在策略中创建新的测试

1. 在“测试监视器”工具栏上单击“+ (新建)”。

   此时将显示“新建测试”窗格。
2. 从“测试类型”列表中选择“往返电子邮件”。
3. 在“描述”字段中指定“RTE_SMTP_POP_Test”。
4. 在“测试名称”字段中指定“往返测试”。
5. 在“测试间隔”字段中指定 300。
6. 在“测试超时”字段中指定 5。
7. 在“每间隔抽样数”字段中指定 1。
8. 在“统计窗口”字段中指定 86400。
9. 在“发送邮件类型 = SMTP”字段中，指定“SMTP”。
10. 在“SMTP 服务器”字段中输入“server.mydomain.com”。
11. 在“SMTP 端口”字段中，接受默认值 25。
12. 在“邮件收件人”字段中指定“you@yourdomain.com”。
13. 在“发件人主机名”字段中指定“金级”。
14. 在“用户名”字段中指定“SMTPuser”。
15. 在“密码”字段中指定“SMTPpassword”。
16. 在“使用 SSL/TLS 字段”中，单击复选框。
17. 在“邮件正文大小”字段中指定“2000”。
18. 在“邮件检索类型”字段中选择“POP3”。

19. 在“POP3 服务器”字段中指定“server.yourdomain.com”。
20. 在“POP3 端口”字段中，接受默认值 110。
21. 在“用户名”字段中输入“Mailuser”。
22. 在“密码”字段中输入“Mail123”。
23. 在“检查间隔”字段中，接受默认值 500 毫秒。
24. 接受其他所有字段的默认值。
25. 单击“保存测试”。

提交认更改时，SRM 将类似于以下内容的条目添加到 svcrsp.cf 文件中：

```
{
index=70
type=rtemail
desc="RTE_SMTP_POP_Test"
dest="server.mydomain.com:25"
username="RTUser"
encoded=yes
password="zrvr8tx"
args="send_Proto=SMTP&to=you@yourdomain.com&size=2000&shost=gold&
SMTP_SSL=yes&send_user=SMTPuser&send_pass=SMTPpassword&get_Proto=POP&
source=server.yourdomain.com:110&check=500"
interval=300
samples=1
timeout=5
window=86400
tos=0
limit=0
status=active
name="Roundtrip Test"
class=""
context=""
flags="1"
loglevel=1
}
```

有关在运行往返电子邮件测试时可能遇到的错误的信息，请参阅下列任一文档：

- IMAP、MAPI 和 POP3 测试错误代码 (p. 274)
- SMTP 测试错误代码 (p. 282)

SMTP 测试

SMTP 测试用于监控连接到邮件服务器上的 SMTP 服务并执行一次空事务所需的时间。该测试可提供发送电子邮件所需时间的基准。

选项和参数

注意：可以使用 IPv6 地址，但是必须将其括在括号内，例如 [0aff::230:6eff:fe4b:51db]:8080。此处的 0aff::230:6eff:fe4b:51db 表示 IPv6 地址，8080 表示端口号。

SMTP 测试需要以下特定选项和参数：

- **SMTP 服务器**。SMTP 邮件服务器的主机名（发起电子邮件的服务器）。
- **SMTP 端口**。（可选）运行 SMTP 服务的端口。默认值为 25。
- **邮件收件人**。测试将电子邮件发送到的电子邮件帐户。
- **邮件正文大小**。（可选）要发送的测试邮件的大小。默认值为 4096 字节。
- **发件人主机名**。发件人的主机名。默认为代理主机名。
- **用户名**。SMTP 授权的有效用户名。
- **密码**。SMTP 授权的有效密码。SRM 以加密形式存储密码（对 SMTP 为可选）。

  注意：必须在“验证密码”字段中重新键入密码，以验证您是否已正确地输入密码。
- **使用 SSL/TLS**。（仅适用于 SMTP）如果 SMTP 服务器需要 SSL/TLS 身份验证，选中该复选框选项可启用安全套接字层 (SSL)/传输层安全性。

在创建或修改测试时指定这些选项和参数。

示例

本节包括测试的示例，这些测试用于监控将测试电子邮件从 mailserver.yourdomain 上的邮件服务器发送到帐户 you@test.com 所需的时间。

示例 1：测试电子邮件发送时间

使用该示例创建一个测试，用于监控每 60 秒将 10,000 字节的测试电子邮件从 mailserver.yourdomain 上的邮件服务器发送到帐户 you@test.com 所需的时间。测试等待最多 10 秒以接收成功响应，并计算过去 300 秒钟（5 分钟）内的响应时间和可用性统计信息。

在策略中创建新的测试

1. 在“测试监视器”工具栏上单击“+ (新建)”。

   此时将显示“新建测试”窗格。
2. 从“测试类型”列表中选择“SMTP”。

3. 在“描述”字段中指定“smtp_test”。
4. 在“测试名称”字段中指定“SMTP 电子邮件发送测试”。
5. 在“测试间隔”字段中指定 60。
6. 在“测试超时”字段中指定 10。
7. 在“每间隔抽样数”字段中指定 1。
8. 在“统计窗口”字段中指定 300。
9. 在“SMTP 服务器”字段中指定“mailserver.yourdomain.com”。
10. 在“SMTP 端口”字段中，接受默认值 25。
11. 在“邮件收件人”字段中指定“you@test.com”。
12. 在“邮件正文大小”字段中指定“10000”。
13. 在“发件人主机名”字段中指定“银级”。
14. 在“用户名”字段中指定“SMTPuser”。
15. 在“密码”字段中指定“SMTPpassword”。
16. 在“使用 SSL/TLS”字段中，单击复选框。
17. 接受其他所有字段的默认值。
18. 单击“保存测试”。

提交认更改时，SRM 将类似于以下内容的条目添加到 svcrsp.cf 文件中：

```
{
index=80
type=smtp
desc="SMTP_Test"
dest="mailserver.yourdomain.com:25"
"username="SMTPuser"
encoded=yes
password:"c21o6BH12"
args="to=you@test.com&size=10000&shost=silver&SSL=yes"
interval=60
samples=1
timeout=10
window=300
tos=0
limit=0
status=active
name="SMTP Email Send Test"
class=""
context=""
flags="1"
loglevel=1
}
```

示例 2：当发件人主机为 IPv6 地址时测试电子邮件发送时间

使用该示例创建一个测试，用于监控每 60 秒将 10,000 字节的测试电子邮件从 mailserver.yourdomain 上的邮件服务器发送到帐户 you@test.com 所需的时间。

发件人主机为 IPv6 地址，SMTP 要求将 IPv6 地址放入括号内。“IPV6:”在 [IPV6:地址] 中不是必需的，但在运行时测试会加上。测试等待最多 10 秒以接收成功响应，并计算过去 300 秒（5 分钟）内的响应时间和可用性统计信息。

在策略中创建新的测试

1. 在“测试监视器”工具栏上单击“+ (新建)”。

   此时将显示“新建测试”窗格。
2. 从“测试类型”列表中选择“SMTP”。
3. 在“描述”字段中指定“smtp_test_ipv6”。
4. 在“测试名称”字段中指定“IPv6 SMTP 电子邮件发送测试”。
5. 在“测试间隔”字段中指定 60。
6. 在“测试超时”字段中指定 10。
7. 在“每间隔抽样数”字段中指定 1。
8. 在“统计窗口”字段中指定 300。
9. 在“SMTP 服务器”字段中指定“mailserver.yourdomain.com”。
10. 在“SMTP 端口”字段中，接受默认值 25。
11. 在“邮件收件人”字段中指定“you@test.com”。
12. 在“邮件正文大小”字段中指定“10000”。
13. 在“发件人主机名”字段中指定 [IPV6:2000::36:543:2111]。
14. 在“用户名”字段中指定“SMTPuser”。
15. 在“密码”字段中指定“SMTPpassword”。
16. 在“使用 SSL/TLS”字段中，单击复选框。
17. 接受其他所有字段的默认值。
18. 单击“保存测试”。

提交认更改时，SRM 将类似于以下内容的条目添加到 svcrsp.cf 文件中：

```
{
index=80
type=smtp
desc="SMTP_Test_ipv6"
dest="mailserver.yourdomain.com:25"
"username="SMTPuser"
encoded=yes
password:"c21o6BH12"
args="to=you@test.com&size=10000&shost=[IPV6:2000::36:543:2111]&SSL=yes"
interval=60
samples=1
timeout=10
window=300
tos=0
limit=0
status=active
name="IPv6 SMTP Email Send Test"
class=""
context=""
flags="1"
loglevel=1
}
```

有关在运行 SMTP 测试时可能遇到的错误的信息，请参阅《SMTP 测试错误代码》 (p. 282)。

SNMP 测试

SNMP 测试用于监控为特定代理中的 MIB 对象执行 SNMP GET 请求所需的时间。它仅支持 SNMPv1、SNMPv2c 和 SNMPv3 操作。

选项和参数

SNMP 测试需要以下特定选项和参数：

- **SNMP 代理**。SNMP 代理所驻留系统的主机名或 IP 地址。

  注意：可以使用 IPv6 地址，但是必须将其括在括号内，例如 [0aff::230:6eff:fe4b:51db]:8080。此处的 0aff::230:6eff:fe4b:51db 表示 IPv6 地址，8080 表示端口号。

- **SNMP 端口**。（可选）运行 SNMP 服务的端口。默认值为 161。
- **OID**。要查询的 MIB 对象的对象标识符。在您查询值为整数的 MIB 变量时，该值将显示在“监视器”页面的“结果字段”列中。默认情况下不显示该列。要将其设置为显示，请在“监视器”页面上选择“显示配置详细信息”，然后选择“结果字段”并单击“更新页面”。

SNMP 版本选项

选择您想要测试的 SNMP 版本。提供的选项包括 SNMPv1、SNMPv2c 和 SNMPv3。

SNMPv1 和 SNMPv2c 测试需要以下特定参数：

- **团体字符串**。用于联系代理的只读或可读写团体字符串。

SNMPv3 测试需要以下特定参数：

- **用户名**。SystemEDGE 中配置的 SNMPv3 用户名。
- **安全级别**。SNMPv3 安全模型中允许的安全级别。选择 NoAuthNoPriv、AuthNoPriv 或 AuthPriv：
  - **NoAuthNoPriv**。这表示 SNMPv3 用户将在没有任何身份验证和加密（隐私）的情况下进行配置。
  - **AuthNoPriv**。这表示 SNMPv3 用户将在具有身份验证但没有任何加密（隐私）的情况下进行配置。
  - **AuthPriv**。这表示 SNMPv3 用户将在具有身份验证和加密（隐私）的情况下进行配置。
- **MD5 或 SHA**。选择为 SNMPv3 用户配置的身份验证协议。仅适用于安全级别 AuthPriv 或 AuthNoPriv。
- **身份验证密码**。输入为 SNMPv3 用户配置的身份验证密码。仅适用于安全级别 AuthPriv 或 AuthNoPriv。
- **DES、AES 或 3DES**。选择为 SNMPv3 用户配置的隐私协议。仅适用于安全级别 AuthPriv。
- **身份验证隐私**。输入为 SNMPv3 用户配置的隐私密码。仅适用于安全级别 AuthPriv。

在创建或修改测试时指定这些选项和参数。

示例

本节包括 SNMP 版本测试的示例，这些测试监控检索 MIB 对象值所需的时间。

示例 1：SNMPv1 或 SNMPv2c 测试

使用该示例创建 SNMPv1 或 SNMPv2c 测试，用于监控系统（IP 地址为 172.32.6.93）端口 5000 上的代理检索 OID 为 1.3.6.1.4.1.546.1.1.1.8.0 的 MIB 对象值所需的时间。该测试每 30 秒为该对象执行一次 SNMP GET，等待最多 10 秒以接收成功响应，并计算过去 120 秒钟（2 分钟）内的响应时间和可用性统计信息。

在策略中创建新的测试

1. 在“测试监视器”工具栏上单击“+ (新建)”。

   此时将显示“新建测试”窗格。
2. 从“测试类型”列表中选择“SNMP”。
3. 对于“描述”，指定“snmpGet”。
4. 对于“测试名称”，指定“获取 OID 1.3.6.1.4.1.546.1.1.1.8.0 的值”。
5. 对于“测试间隔”，指定“30”。
6. 对于“测试超时”，指定“10”。
7. 对于“每间隔抽样数”，指定“1”。
8. 对于“统计窗口”，请指定“120”。
9. 对于“SNMP 代理”，请指定“172.32.6.93”。
10. 对于“SNMP 端口”，请指定“5000”。
11. 对于“团体字符串”，请指定“public”。
12. 对于“OID”，请指定“1.3.6.1.4.1.546.1.1.1.8.0”。
13. 接受其他所有字段的默认值。
14. 单击“保存测试”。

提交认更改时，SRM 将类似于以下内容的条目添加到 svcrsp.cf 文件中：

```
{
index=22
type=snmp
desc="snmpGet"
dest="172.32.6.93:5000"
encoded=yes
password="CHV1JB1"
args="oid=1.3.6.1.4.1.546.1.1.1.8.0"
interval=30
samples=1
timeout=10
window=120
tos=0
limit=0
status=active
name="Get value of OID 1.3.6.1.4.1.546.1.1.1.8.0"
class=""
context=""
flags="1"
loglevel=1
}
```

示例 2：SNMPv3 测试

使用该示例创建 SNMPv3 测试，用于监控系统（IP 地址为 172.32.6.93）端口 5000 上的代理检索 OID 为 1.3.6.1.4.1.546.1.1.1.8.0 的 MIB 对象值所需的时间。该测试每 30 秒为该对象执行一次 SNMP GET，等待最多 10 秒以接收成功响应，并计算过去 120 秒钟（2 分钟）内的响应时间和可用性统计信息。

在策略中创建新的测试

1. 在“测试监视器”工具栏上单击“+ (新建)”。

   此时将显示“新建测试”窗格。

2. 从“测试类型”列表中选择“SNMP”。
3. 对于“描述”，请指定“snmpv3Get”。
4. 对于“测试名称”，请指定“SNMPv3: Get value of OID+ 1.3.6.1.4.1.546.1.1.1.8.0”。
5. 对于“测试间隔”，指定“30”。
6. 对于“测试超时”，指定“10”。
7. 对于“每间隔抽样数”，指定“1”。
8. 对于“统计窗口”，请指定“120”。
9. 对于“SNMP 代理”，请指定“172.32.6.93”。

10. 对于“SNMP 端口”，请指定“5000”。
11. 对于“安全级别”，请选择“AuthPriv”。
12. 对于“用户名”，请选择“shades”。shades 应该是在 SystemEDGE 上配置的 SNMPv3 用户。
13. 对于 SNMPv3 用户 shades 使用的身份验证协议，请单击“SHA”。
14. 对于“身份验证密码”，请指定“shapassword”。
15. 对于“身份验证密码”下方的“验证密码”，请指定“shapassword”。
16. 对于 SNMPv3 用户 shades 使用的隐私协议，请单击“DES”。
17. 对于“隐私密码”，请指定“despassword”。
18. 对于“隐私密码”下方的“验证密码”，请指定“despassword”。
19. 对于“OID”，请指定“1.3.6.1.4.1.546.1.1.1.8.0”。
20. 接受其他所有字段的默认值。
21. 单击“保存测试”。

提交认更改时，SRM 将类似于以下内容的条目添加到 svcrsp.cf 文件中：

```
{
index=23
type=snmp
desc="snmpv3Get"
dest="172.32.6.93:5000"
encoded=yes
password="
c2VjbD0zJnNlY3U9bWQ1ZGVzMiZhdXRdcHI9TUQ1JmF1dGhwdz1wYXNzd29yZCZwcml7cHI6REVTJ
nByaXAwdy1wYXNzd29yZA=="
args="oid=1.3.6.1.4.1.546.1.1.1.8.0"
interval=30
samples=1
timeout=10
window=120
tos=0
limit=0
status=active
name="SNMPv3: Get value of OID 1.3.6.1.4.1.546.1.1.1.8.0"
class=""
context=""
flags="1"
loglevel=1
}
```

有关在运行 SNMP 测试时可能遇到的错误的信息，请参阅《SNMP 测试错误代码》 (p. 282)。

SQL 查询测试

SQL 查询测试用于监控连接到任何支持 JDBC 且可执行 SQL 查询的数据库所需的时间。它支持对 Oracle、Microsoft SQL Server 和其他数据库的查询。

在开始创建 SQL 查询测试之前，请验证相应的 JDBC 驱动程序可用。如有必要，请安装特定于您尝试测试的数据库的 JDBC 驱动程序文件。

- 适用于 SQL Server 的 sqljdbc.jar（JRE 1.5 版或更低版本）或 sqljdbc4.jar（JRE 1.6 版或更高版本）
- 适用于 Oracle 的 ojdbc<XYZ>.jar

将 JAR 文件复制到 SystemEDGE 安装目录下的 jre/lib/ext 目录中（例如，/opt/SystemEDGE/jre/lib/ext [UNIX] 或 *驱动器*:\sysedge\jre\lib\ext [Windows]）。要获取针对您的数据库的 JDBC 驱动程序 jar 文件，请访问分发该数据库的公司的企业网站。

验证 SQL JDBC 驱动程序可用性的示例

1. 更改为 *安装路径*/SystemEDGE/jre/lib/ext 目录。
2. 检查 sqljdbc.jar（JRE 1.5 版或更低版本）或 sqljdbc4.jar（JRE 1.6 版或更高版本）是否可用。

如果 SQL JDBC 不可用，请执行下列操作：

1. 从 microsoft.com/downloads 下载 SQL JDBC 驱动程序。
2. 解压缩下载的驱动程序包，并将 sqljdbc.jar（JRE 1.5 版或更低版本）或 sqljdbc4.jar（JRE 1.6 版或更高版本）复制到 *安装路径* /SystemEDGE/jre/lib/ext 目录。
3. 重新启动 SystemEDGE 以加载新的 Java 类。
4. 例如，通过 CA Virtual Assurance 中的“策略配置”设置新的 SQL 测试。如有必要，请参见解压缩的 JDBC 软件包中的帮助系统。

选项和参数

SQL 查询测试需要以下特定选项和参数：

- **数据库类型**：选择“Oracle”、“MSSQL”或“其他”。

  注意：对于 Oracle 和 MSSQL，SRM 会使用安装有 SRM 的默认 JDBC 驱动程序来创建动态 SQL 连接字符串。对于下载的任何其他 JDBC 驱动程序，不管数据库供应商是谁，都必须从供应商那获得驱动程序的 Java 类名和相应的 SQL 连接字符串，并且提供特定关键字（见下文）。

- **SQL 数据库服务器**：SQL 数据库服务器的主机名。

  注意：可以使用 IPv6 地址，但是必须将其括在括号内，例如 [0aff::230:6eff:fe4b:51db]:8080。此处的 0aff::230:6eff:fe4b:51db 表示 IPv6 地址，8080 表示端口号。

- **端口**：SQL 数据库正在其上运行的端口。选择 Oracle 或 MSSQL 时，将显示默认端口号。该字段为必填项。

- **用户名**：数据库的有效用户名。

- **密码**：指定的用户名的有效密码。SRM 以加密格式存储密码。

- **SQL 驱动程序**：连接到数据库所需的 JDBC 驱动程序。如果选择 Oracle 或 MSSQL 作为“数据库类型”，则 SQL 驱动程序名称默认为您在 SRM 安装期间指定的 Oracle 或 MSSQL 驱动程序（这种情况下不显示该字段）。要为 Oracle 或 MSSQL 指定其他 JDBC 驱动程序，请选择“其他”并填写必填字段。这包括识别要使用的 SQL 驱动程序的 Java 类名和相应的连接字符串。此外，连接字符串格式和所需信息因供应商而异。确保从供应商网站或供应商的驱动程序文档中获取该信息。

  示例:

  ```
  com.microsoft.sqlserver.jdbc.SQLServerDriver
  oracle.jdbc.OracleDriver
  com.mysql.jdbc.Driver
  ```

- **数据库名称**：指定数据库实例名程。该字段对于 Oracle 是必填项，对于 MSSQL 是可选项。驱动程序名称和连接字符串足以满足 MSSQL（数据库实例名称为空）。由于在显式 SQL 连接字符串中提供了该信息，因此如果选择“其他”，则不显示该字段。

- **查询**：要执行的 SQL 查询。有关 SQL 查询语言的信息，请参阅数据库文档。

- **连接字符串**：数据库所需的 SQL 连接字符串。仅当选择“其他”作为“数据库类型”时才会显示该字段，否则，SRM 会根据您在 SRM 用户界面的必填字段中提供的信息构建连接字符串。如果您的数据库驱动程序不是 Oracle 或 MSSQL 的默认驱动程序，则必须在该字段中指定显式连接字符串。

  注意：SQL 连接字符串的格式取决于特定供应商提供的数据库驱动程序。要获取 JDBC 驱动程序的适当连接字符串，请访问数据库供应商的网站或参阅 JDBC 驱动程序文档。

  数据库供应商提供的连接字符串包含一系列字段，其中一些字段可替换为显式*关键字*，如 unameValue、pwdValue、hostnameValue 和 portValue。在 GUI 中输入连接字符串时，请键入“unameValue”和“pwdValue”，并让代理进行代替。特定于供应商的连接字符串应规定在连接到中放置关键字的位置。（如果使用 Oracle 或 MSSQL 的默认 JDBC 驱动程序，则 SRM 会自动规定位置。）在 SRM 测试运行时，连接字符串中的下列 SRM 关键字将由您指定的值替代：

  - unameValue 关键字由指定用户名替代
  - pwdValue 关键字由指定密码替代
  - hostnameValue 关键字由指定主机名替代
  - portValue 键名称由指定端口替代

  示例:

  ```
  jdbc:oracle:thin:unameValue/pwdValue@hostnameValue:portValue:orcl
  (connects with orcl)
  jdbc:sqlserver://hostnameValue:portValue;databaseName=vasdb;user=unameVal
  ue;password=pwdValue (connects with vasdb)
  jdbc:sqlserver://hostnameValue:portValue;user=unameValue;password=pwdValu
  e (connects with default database)
  jdbc:mysql://hostnameValue:portValue/mydb?user=unameValue&password=pwdVal
  ue (connects with mydb)
  ```

在创建或修改测试时指定这些选项和参数。

示例 1：测试 Oracle 数据库

使用该示例创建一个测试，用于登录到 Oracle 数据库并执行查询，以便每 300 秒在用户表中检索一次表名称。测试等待最多 10 秒以接收成功响应，并计算过去 1800 秒钟（30 分钟）内的响应时间和可用性统计信息。

在策略中创建新的测试

1. 在“测试监视器”工具栏上单击“+ (新建)”。

   此时将显示“新建测试”窗格。

2. 从“测试类型”列表中选择“SQL 查询”。

3. 在“描述”字段中指定“SQLQuery_OracleTest”。

4. 在“测试名称”字段中指定“Oracle 测试”。
5. 在“测试间隔”字段中指定 300。
6. 在“测试超时”字段中指定 10。
7. 在“每间隔抽样数”字段中指定 1。
8. 在“统计窗口”字段中指定 1800。
9. 在“数据库类型”字段中选择“Oracle”。
10. 在“SQL 数据库服务器”字段中指定“OracleTest”。
11. 在“端口”字段中，接受默认值 1521。
12. 在“用户名”字段中指定“OracleUser”。
13. 在“密码”字段中指定“Oracle123”。
14. 在“数据库名称”字段中，指定要测试的数据库的名称，如 MYDB。
15. 在“查询”字段中，指定“select table_name from user_tables”。
16. 单击“保存测试”。

提交认更改时，SRM 将类似于以下内容的条目添加到 svcrsp.cf 文件中：

```
{
index=11
type=sql
desc="SQLQuery_OrcaleTest"
dest="OracleTest:1521"
username="OracleUser"
encoded=yes
password="aW1vdXJhdmlldg"
args="query=select table_name from user_tables&dbtype=oracle&dbname=MYDB"
interval=300
samples=1
timeout=10
window=1800
tos=0
limit=0
status=active
name="Oracle Test"
class=""
context=""
flags="1"
loglevel=2
}
```

示例 2：测试 Microsoft SQL Server 数据库

使用该示例创建一个测试，用于登录到 Microsoft SQL 数据库并执行查询，以便每 60 秒在用户表中检索一次表名称。测试等待最多 10 秒以接收成功响应，并计算过去 120 秒钟内的响应时间和可用性统计信息。

在策略中创建新的测试

1. 在“测试监视器”工具栏上单击“+ (新建)”。

   此时将显示“新建测试”窗格。
2. 从“测试类型”列表中选择“SQL 查询”。
3. 在“描述”字段中指定“SQLQuery_SQLServer”。
4. 在“测试名称”字段中指定“SQL 测试”。
5. 在“测试间隔”字段中指定 60。
6. 在“测试超时”字段中指定 10。
7. 在“每间隔抽样数”字段中指定 1。
8. 在“统计窗口”字段中指定 120。
9. 在“SQL 数据库服务器”字段中选择“MSSQL”。
10. 在“端口”字段中，接受默认值 1433。
11. 在“用户名”字段中指定“SQLUser”。
12. 在“密码”字段中指定“SQL123”。
13. 在“数据库名称”字段中，指定要测试的数据库的名称，如 Northwind。
14. 在“查询”字段中，指定“select * from categories”。
15. 单击“保存测试”。

提交认更改时，SRM 将类似于以下内容的条目添加到 svcrsp.cf 文件中：

```
{
index=11
type=sql
desc="SQLQuery.SQLServer"
dest="mySQLServer:1433"
username="SQLUser"
encoded=yes
password="bWnvTRPJhdmll"
args="query=select * from categories"&dbtype=mssql&dbname=Northwind"
interval=60
samples=1
timeout=10
window=120
tos=0
limit=0
status=active
name="SQL Test"
class=""
context=""
flags="1"
loglevel=1
}
```

有关在运行 SQL 查询测试时可能遇到的错误的信息，请参阅《SQL 查询测试错误代码》 (p. 282)。

TCP 连接测试

TCP 连接测试可监控通过 TCP 连接服务器上端口所需的时间。它可以帮助您确定 TCP 服务是否正在运行，以及网络连接是否存在。

选项和参数

TCP 连接测试需要以下特定选项和参数：

- **目标**。要连接的系统的主机名。

  注意：可以使用 IPv6 地址，但是必须将其括在括号内，例如 [0aff::230:6eff:fe4b:51db]:8080。此处的 0aff::230:6eff:fe4b:51db 表示 IPv6 地址，8080 表示端口号。

- **端口**。TCP 服务正在其上运行的端口。

在创建或修改测试时指定这些选项和参数。

示例

使用该示例创建一个测试，用于监控每 60 秒连接到系统 nfsserver.yourdomain 上的端口 2049 所需的时间。测试等待最多 5 秒以接收成功响应，并计算过去 600 秒钟（10 分钟）内的响应时间和可用性统计信息。

在策略中创建新的测试

1. 在“测试监视器”工具栏上单击“+ (新建)”。

   此时将显示“新建测试”窗格。

2. 从“测试类型”列表中选择“TCP 连接”。
3. 在“描述”字段中指定“nfsserver.yourdomain_tcp”。
4. 在“测试名称”字段中指定“TCP 连接测试”。
5. 在“测试间隔”字段中指定 60。
6. 在“测试超时”字段中指定 5。
7. 在“每间隔抽样数”字段中指定 1。
8. 在“统计窗口”字段中指定 600。
9. 在“目标”字段中输入“nfsserver.yourdomain.com”。
10. 在“端口”字段中指定“2049”。
11. 接受其他所有字段的默认值。
12. 单击“保存测试”。

提交认更改时，SRM 将类似于以下内容的条目添加到 svcrsp.cf 文件中：

```
{
index=90
type=tcpconnect
desc="nfsserver.yourdomain_tcp"
args=" "
dest="nfsserver.yourdomain:2049"
interval=60
samples=1
timeout=5
window=600
tos=0
limit=0
status=active
name="TCP Connection Test"
class=""
context=""
flags="1"
loglevel=1
}
```

有关在运行 TCP 连接测试时可能遇到的错误的信息，请参阅《常规错误代码》 (p. 267)。

TFTP 测试

TFTP 测试可监控使用 TFTP 协议读写文件所需的时间。

选项和参数

TFTP 测试需要以下特定选项和参数：

- **TFTP 服务器**。正在测试的 TFTP 服务器的主机名。在执行写入测试之前，某些 TFTP 服务器可能要求您在 TFTP 根目录中创建可写的种子文件（存根文件）。*存根文件*是与 TFTP 测试写入的文件同名的文件。如果存根文件不可写，测试将失败。

  注意：可以使用 IPv6 地址，但是必须将其括在括号内，例如 [0aff::230:6eff:fe4b:51db]:8080。此处的 0aff::230:6eff:fe4b:51db 表示 IPv6 地址，8080 表示端口号。

  注意：代理必须有权访问正在写入到 TFTP 服务器（不管是在本地写入还是加载到其中）的文件。

- **TFTP 端口**。（可选）运行 TFTP 服务的端口。默认值为 69。
- **操作**。要执行的操作的类型；以下类型之一：
  - **读取文件**—从服务器读取（尝试下载）文件。
  - **写入文件**—将文件写入到远程文件系统。TFTP 写入测试的输出将转到 TFTP 根目录。这是在 Windows 上安装（TFTP 服务器）之前或之后配置的目录。对于 UNIX 系统，它可能会显示在系统启动配置文件中（如 Solaris 上的 \etc\inetd.conf）。
- **文件名**。要 *写入*的文件的完整路径和文件名。如果要执行 *读取*操作，则必须提供完整路径或只提供文件名，具体取决于您正在联系的 TFTP 服务器的要求。必须以与特定服务器一致的方式指定 TFTP 服务器上的文件名或路径名。在大多数情况下，路径与 TFTP 目录的根目录有关。

  注意：指定路径名时，请确保针对将运行测试的操作系统使用正确类型的斜杠。也就是说，为要在 UNIX 系统上运行的测试指定目录时，请使用正斜杠 (/)；为要在 Windows 系统上运行的测试指定目录时，则使用反斜杠 (\)。

在创建或修改测试时指定这些选项和参数。

示例 1：使用 TFTP 读取文件

使用该示例创建一个测试，用于监控通过 tftpserver.yourdomain 上的 TFTP 服务读取文件所需的时间。该示例每 30 秒测试一次服务器，并等待最多 10 秒以接收成功响应。它计算过去 120 秒钟（2 分钟）内的响应时间和可用性统计信息。

在策略中创建新的测试

1. 在“测试监视器”工具栏上单击“+ (新建)”。

   此时将显示“新建测试”窗格。
2. 从“测试类型”列表中选择“TFTP”。
3. 在“描述”字段中指定“tftpserver_read”。
4. 在“测试名称”字段中指定“TFTP 读取文件测试”。
5. 在“测试间隔”字段中指定 30。
6. 在“测试超时”字段中指定 10。
7. 在“每间隔抽样数”字段中指定 1。
8. 在“统计窗口”字段中指定 120。
9. 在“TFTP 服务器”字段中指定“tftpserver.yourdomain”。
10. 在“TFTP 端口”字段中，接受默认值 69。
11. 在“操作”字段中选择“读取文件”。
12. 在“文件名”字段中指定“I:\SA\TFTP\get.txt”。
13. 接受其他所有字段的默认值。
14. 单击“保存测试”。

在您执行测试提交/同步时，SRM 会将类似于以下内容的条目添加到 svcrsp.cf 文件中：

```
{
index=11
type=tftp
desc="tftpserver.read"
dest="tftpserver@yourdomain.com:69"
args="op=r&path=I:\SA\TFTP\get.txt"
interval=30
samples=1
timeout=10
window=120
tos=0
limit=0
status=active
name="TFTP Reading File Test"
class=""
context=""
flags="1"
loglevel=1
}
```

示例 2：使用 TFTP 写入文件

使用该示例创建一个测试，用于监控通过 tftpserver.yourdomain 上的 TFTP 服务写入文件所需的时间。该示例每 30 秒测试一次服务器，并等待最多 10 秒以接收成功响应。它计算过去 120 秒钟（2 分钟）内的响应时间和可用性统计信息。

在策略中创建新的测试

1. 在“测试监视器”工具栏上单击“+ (新建)”。

   此时将显示“新建测试”窗格。

2. 从“测试类型”列表中选择“TFTP”。
3. 在“描述”字段中指定“tftpserver_write”。
4. 在“测试名称”字段中指定“TFTP 写入文件测试”。
5. 在“测试间隔”字段中指定 30。
6. 在“测试超时”字段中指定 10。
7. 在“每间隔抽样数”字段中指定 1。
8. 在“统计窗口”字段中指定 120。
9. 在“TFTP 服务器”字段中指定“tftpserver.yourdomain”。
10. 在“TFTP 端口”字段中，接受默认值 69。
11. 在“操作”字段中选择“写入文件”。

12. 在“文件名”字段中指定“I:\SA\TFTP\put.txt”。
13. 接受其他所有字段的默认值。
14. 单击“保存测试”。

提交认更改时，SRM 将类似于以下内容的条目添加到 svcrsp.cf 文件中：

```
{
index=22
type=tftp
desc="tftpserver_write"
dest="tftpserver.yourdomain.com:69"
args="op=w&path=I:\SA\TFTP\put.txt"
interval=30
samples=1
timeout=10
window=120
tos=0
status=active
name="TFTP Writing File Test"
class=""
context=""
flags="1"
loglevel=1
}
```

有关在运行 TFTP 测试时可能遇到的错误的信息，请参阅《TFTP 测试错误代码》 (p. 282)。

虚拟用户测试

虚拟用户测试将回放录制的 WinTask 脚本。通过该测试网站，可以获取实际用户事务的连续可用性和响应时间数据。

在创建虚拟用户测试之前，必须执行以下操作：

- 验证目标系统上的 SystemEDGE 能与桌面交互。
- 验证 svcrsp.cf 文件中存在 allow_scripts 指令，且未注释掉该指令。（如果该行前面有井号 (#)，请将其删除。）
- 安装 WinTask 运行时代理和要在将运行该测试的系统上运行的脚本。
- 确保打开了活动（未锁定）的桌面来运行脚本。

在运行虚拟用户测试时，请考虑以下各项：

- 只能在 Windows 系统上运行虚拟用户测试。
- 不得在 Citrix 环境中运行虚拟用户测试。

- 如果要为同一系统上的多个脚本设置测试，请编辑 svcrsp.cf 文件以设置 maxthreads=1。该设置排除了 SRM 尝试在同一系统上同时运行多个脚本的可能性。可以在 SRM 安装期间设置该变量，或通过手动编辑 svcrsp.cf 文件进行设置。
- 如果在“高级”选项中设置了测试间隔，请验证“统计窗口”的设置大于“测试间隔”，最好为该值的倍数。例如，“测试间隔”为 60，“统计窗口”设置为 300。

选项和参数

虚拟用户测试需要以下特定选项和参数：

- **脚本路径**。要运行的 WinTask 可执行文件和 WinTask 脚本的完整路径和文件名。首先输入 WinTask 可执行文件的路径，之后紧接着是空格字符，然后是脚本的路径。在指定完整路径时，请确保使用反斜杠 (\)。
- **目标主机**。（可选）运行该脚本的系统的主机名。

  注意：可以使用 IPv6 地址，但是必须将其括在括号内，例如 [0aff::230:6eff:fe4b:51db]:8080。此处的 0aff::230:6eff:fe4b:51db 表示 IPv6 地址，8080 表示端口号。
- **目标端口**。（可选）目标系统中可以运行脚本的端口。
- **运行用户**。（可选）运行脚本所需的用户名（如果脚本必须作为特定用户运行的话）。

  注意：用户必须是本地用户（无需登录域），并且必须能够作为服务登录。按如下方式在 Windows 中设置功能：“控制面板”>“管理工具”>“本地安全策略”>“本地策略”>“用户权限分配”>“作为服务登录”。
- **密码**。（可选）正在运行该脚本的用户的密码。SRM 以加密格式存储密码。

  注意：如果指定主机名和端口的值，则 SRM 会尝试通过 TCP 连接连接到系统和端口。如果连接成功，SRM 会尝试在指定系统和端口上执行脚本。如果不指定主机名和端口，则 SRM 不会提供 DNS 名称解析或连接次数。
- **域**。（可选）运行该脚本的用户的域。

在创建或修改测试时指定这些选项和参数。

示例

使用该示例创建一个测试，用于监控每 120 秒在 mySystem 的端口 8080 上运行脚本 (C:\myScripts\playback_script.rob) 所需的时间。该脚本必须以用户 myVUser（密码 VUser123）运行。测试等待最多 10 秒以接收成功响应，并计算过去 3600 秒钟（2 小时）内的响应时间和可用性统计信息。

在策略中创建新的测试

1. 在“测试监视器”工具栏上单击“+ (新建)”。

   此时将显示“新建测试”窗格。
2. 从“测试类型”列表中，选择“虚拟用户”。
3. 在“说明”字段中，指定 vuser_test。
4. 在“测试名称”字段中，指定“VUser 测试”。
5. 在“测试间隔”字段中指定 120。
6. 在“测试超时”字段中指定 10。
7. 在“每间隔抽样数”字段中指定 1。
8. 在“统计窗口”字段中指定 3600。
9. 在“脚本路径”字段中，指定 C:\wintask\bin\wintask.exe C:\myScripts\playback_script.rob。
10. 在“目标主机”字段中，指定 mySystem。
11. 在“目标端口”字段中，指定 8080。
12. 在“运行用户”字段中，指定 myVUser。
13. 在“密码”字段中，指定 VUser123。
14. 接受其他所有字段的默认值。
15. 单击“保存测试”。

提交认更改时，SRM 将类似于以下内容的条目添加到 svcrsp.cf 文件中：

```
{
index=21
type=vuser
desc="vuser_test"
dest="C:\WinTask\bin\taskexec.exe C:\WinTask\Scripts\notepad.rob"
args=""
interval=60
samples=1
timeout=15
window=300
tos=0
limit=0
status=active
name="VUserTest"
class=""
context=""
flags="1"
loglevel=1
}
```

错误和可用性度量

SRM 在“结果字段”和“错误代码”这两个字段中记录有关虚拟用户测试错误方面的信息，以帮助您区分 SRM 错误和 WinTask 应用程序所遇到的错误。

下表解释错误代码如何影响可用性度量。“结果字段”提供 WinTask 返回的值，“错误代码”字段提供服务可用性错误代码。

注意：“错误代码”列为 2 时，“结果字段”列将显示 taskexec.exe 应用程序返回的错误代码。

结果字段	错误代码	对可用性造成的影响	错误的说明
0	0	无影响	无错误。
在 300 到 400 范围内的任何数字	2	负面	SRM 无法以“运行用户”字段中指定的用户身份登录。
介于 600,000 和 700,000 之间的任何数字	61	无影响	正在运行的 WinTask 脚本可能会出现错误。
-1	2	负面	系统错误。
任何其他数字	2	负面	正在运行的 WinTask 脚本可能会出现错误。

有关运行虚拟用户测试时可能会遇到的错误的相关信息，请参见虚拟用户测试错误代码 (p. 282)。

测试的关键字

所有 SRM 测试都将 keyword=value 格式用于参数字段中显示的参数。关键字-值对由与号 (&) 分隔。例如，往返电子邮件测试的参数字段显示类似如下内容：

```
send_proto=smtp&to=recipient&size=256&shost=senderhost&smtp_ssl=true
&send_user=sender&send_pass=secret&get_proto=pop3&source=popserver
&source_port=110&check=600
```

当您使用 SRM 页面来添加或修改测试时，SRM 会自动使用正确的关键字。如果要手工或使用 svcwatch 来编辑 svcrsp.cf 文件以动态地更新文件，则必须使用以下关键字。

测试	关键字	描述
Active Directory 用户	域	Active Directory 服务器所在的域。
	查询	要发送给 Active Directory 服务器的查询。
	filter	服务器端结果筛选。
自定义	无附加参数	
DHCP	无附加参数	
DNS	主机名	要查找的主机名。
文件 I/O	local	要用于写入、读取/写入以及比较操作的本地路径和文件名。
	域	登录服务器的用户所在的域（仅 Windows）。
	op	可以为以下值之一： ■ r－读取文件。 ■ w－将本地参考文件的内容写入位于远程文件系统的测试文件，然后删除测试文件。 ■ rw－将本地参考文件的内容写入远程文件系统上的测试文件、读取测试文件，然后将其删除。 ■ cmp－先读取一个文件，再读取另一个文件，然后比较其内容。

测试	关键字	描述
FTP	local	指定要在 FTP 服务器上写入的文件的名称。
	remote	指定要读取的文件的路径。
	op	可以为以下值之一： ■ g－(get) 登录并读取指定的文件（但是不执行写入操作），然后注销。 ■ p－(put) 登录并将指定的文件写出到 FTP 服务器，然后注销。如果远程目录没有写入权限，测试将失败。 ■ login（无 remote 和 local 关键字）－使用指定的用户名和密码登录，然后注销。
HTTP 和 HTTPS	max_depth	下载嵌套框架时测试应遍历的层数（在页面下载期间 HTTP 和 HTTPS 测试会下载所有框架、图像、外部脚本以及小程序，以便度量可以反映用户在下载网页时的体验。）默认值为 3。
	proxy	在您要从中测试的系统没有直接 Internet 访问权限时要使用的代理服务器的主机名。
	proxyuser	该代理的用户名。
	proxypass	代理用户的密码。
	content_dl	■ true－下载内容，包括脚本、图像、小程序等。 ■ false－不下载内容。
	content_err	■ true－下载时出现的任何错误都会导致测试失败。 ■ false－下载期间不考虑出现的错误。
	minmatch	查找搜索模式的最小次数。
	搜索	要使 SRM 在您测试的页面上匹配的正则表达式。
IMAP	download	要下载的电子邮件；可以为以下值之一： ■ 下载第一封邮件－仅为该用户帐户下载第一封邮件。 ■ 下载所有邮件－为该用户帐户下载所有邮件。

测试	关键字	描述
	删除	是否删除下载的邮件；可以为以下值之一： ■ true－删除下载的邮件。 ■ false－不删除下载的邮件。
LDAP	查询	指定要发送到 LDAP 服务器的查询。
	域	指定 LDAP 域。
	filter	指定服务器端结果筛选。
MAPI	域	用户帐户所在的 Windows 域。
	op	■ send－发送测试邮件。 ■ recv－接收测试邮件。
	download	要下载的电子邮件；可以为以下值之一： ■ 下载第一封邮件－仅为该用户帐户下载第一封邮件。 ■ 下载所有邮件－为该用户帐户下载所有邮件。
	to	■ 指定测试邮件的电子邮件收件人。
	大小	■ 指定测试邮件的大小（字节）。默认值 256
	删除	是否删除下载的邮件；可以为以下值之一： ■ true－删除下载的邮件。 ■ false－不删除下载的邮件。
NIS	域	指定映射文件所在的域。
	map	指定要测试的映射文件。默认值：host
	download	■ true－下载指定的 NIS 映射。 ■ false－不下载指定的映射。
文件 I/O	local	要用于写入、读取/写入以及比较操作的本地路径和文件名。
	域	登录服务器的用户所在的域（仅 Windows）。
NNTP	无附加参数	
PING	payload	在 ping 操作中发送的数据包的大小。默认数据包大小是 64 字节。

测试	关键字	描述
POP3	download	要下载的电子邮件；可以为以下值之一： ■ 下载第一封邮件－仅为该用户帐户下载第一封邮件。 ■ 下载所有邮件－为该用户帐户下载所有邮件。
	删除	是否删除下载的邮件；可以为以下值之一： ■ true－删除下载的邮件。 ■ false－不删除下载的邮件。
往返电子邮件	to	接收邮件的用户帐户。
	大小	要发送的电子邮件的大小（字节）。默认值 256
	send_proto	要用于发送邮件的协议；可以为以下值之一： ■ smtp ■ mapi
	shost	指定发送邮件的主机名。
	smtp_ssl	■ true－启用 SMTP SSL 加密。 ■ false－禁用 SMTP SSL 加密。
	send_user	指定发件人帐户的名称。
	send_pass	指定发件人的密码。
	sdomain	（仅 MAPI 协议）用于使用 MAPI 协议发送邮件的用户域。
	get_proto	用于接收邮件的协议；可以为以下值之一： ■ pop ■ imap ■ mapi
	source	指定电子邮件所发送到的主机。
	source_port	指定 IMAP 或 POP3 的端口号。默认值：110 (POP3)、143 (IMAP)
	gdomain	（仅 MAPI 协议）用于使用 MAPI 协议检索邮件的用户域。
	check	指定轮询间隔（秒）。默认：600

测试	关键字	描述
	删除	是否删除下载的邮件；可以为以下值之一： ■ true－删除下载的邮件。 ■ false－不删除下载的邮件。
SMTP	to	接收电子邮件的用户帐户。
	大小	要发送的电子邮件的大小（字节）。默认：256
	shost	指定发送邮件的主机名。
	ssl	■ true－启用 SMTP SSL 加密。 ■ false－禁用 SMTP SSL 加密。
SNMP	snmpversion	■ snmp－指定 SNMPv1/2。 ■ snmp3－指定 SNMPv3。
	user	指定 SNMPv3 用户名。
	securitylevel	指定 SNMPv3 安全级别： ■ AuthPriv－身份验证和隐私 ■ NoAuthNoPriv－无身份验证，无隐私 ■ AuthNoPriv－身份验证，无隐私
	auth_protocol	指定 SNMPv3 身份验证协议： ■ MD5 ■ SHA
	auth_password	指定身份验证密码。
	priv_protocol	指定 SNMPv3 隐私协议： ■ DES ■ AES ■ 3DES
	priv_password	指定隐私密码。
	oid	要查询的变量的对象标识符。
	community	用于读取变量的团体字符串。
SQL 查询	查询	要发送给数据库的查询。

测试	关键字	描述
	qtype	（可选）查询的类型。有效值是: ■ query－（默认值）查询参数表示普通的查询，例如，SELECT。 ■ stored－查询参数表示 EXECUTE 查询的参数；存储程序和参数。 ■ update－查询参数包含更新查询，例如，INSERT。该查询类型返回整数值：-1、0、正整数
	dbtype	指定数据库的类型。 ■ oracle ■ mssql ■ other
	driver	（对于“other”数据库）用于查询的 JDBC 驱动程序。
	url	（对于“other”数据库）数据库连接字符串；因数据库类型而异。有关连接字符串的信息，请参阅数据库文档。
	dbname	要查询的数据库的名称 使用“other”作为数据库类型时，该字段不显示在用户界面中。改为在连接字符串中指定数据库名称。
TCP Connect	无附加参数	
TFTP	路径	要读取或写入的文件的路径和文件名。
	op	可以为以下值之一： ■ r－从服务器读取文件。 ■ w－将文件写入远程文件系统。
虚拟用户	域	正在运行脚本的用户所在的域。
	port	脚本在其上运行的端口。
	主机名	目标系统的主机名；该值用于 DNS 查找和连接计时。

使用自定义脚本创建测试

您可以创建自定义脚本来指示 SRM 对本地系统执行自定义测试。

创建自定义测试的准则

在创建自定义测试时请考虑以下内容：

- 如果自定义测试返回的名称解析时间、连接时间或事务处理时间的值 <= 0，则测试可用性将设置为 0。
- 由自定义脚本所报告的时间的单位是毫秒。
- 成功的自定义脚本需要只返回整数值。
- 成功的脚本返回 0 作为其退出代码。除 0 之外的任何值均表示失败的自定义脚本。
- 结果代码放置在该测试的 MIB 的结果字段中。

编写脚本的准则

您可以将脚本作为二进制可执行文件或采用脚本编写语言（如 UNIX shell 或 Perl）来编写脚本。自定义响应模块的工作方式与 SystemEDGE 代理扩展对象的工作方式极其类似。有关 SystemEDGE 扩展对象的详细信息，请参阅 *《SystemEDGE 用户指南》*。SRM 预期自定义脚本提供单行输出，*至少*有三个值（最多六个值），后跟换行符。

您创建的脚本必须按如下顺序返回以下信息：

1. DNS 解析时间（必需）
2. 连接时间（必需）
3. 事务处理时间（必需）
4. 结果代码（可选）
5. 输入字节数（可选）
6. 输出字节数（可选）

SRM 基于该脚本返回的输入字节数和输出字节数数据计算吞吐量。因此，如果脚本提供输入字节数，它还必须提供输出字节数（反之亦然）。正确的脚本输出必须是下列三个选项之一：

选项 A：

1. DNS 解析时间
2. 连接时间
3. 事务处理时间

选项 B：

1. DNS 解析时间
2. 连接时间
3. 事务处理时间
4. 结果代码

选项 C：

1. DNS 解析时间
2. 连接时间
3. 事务处理时间
4. 结果代码
5. 输入字节数
6. 输出字节数

选项和参数

自定义测试需要下列特定的选项或参数：

脚本路径－要运行的自定义脚本的完整路径和文件名。

注意：指定路径名时，确保使用适用于运行测试的操作系统的正确斜线类型，即，对于打算在 UNIX 系统上运行的测试，请在指定目录时使用正斜线 (/)；对于打算在 Windows 系统上运行的测试，请在指定目录时使用反斜线 (\)。

当您为自定义测试指定超时值时，确保它提供允许脚本执行的足够时间。如果脚本没有足够的时间执行，SRM 将终止它，并且如果脚本不清除自己的子进程，这些进程会继续运行，最终可能会导致系统挂起。

在创建或修改测试时指定此选项或参数。

示例

使用该示例来创建用于监控运行位于 /local/bin/custom_Test.pl 的脚本所需的时间量的测试。条目会指示代理每 120 秒（2 分钟）测试服务一次，并最多等待 20 秒以获得成功响应。代理将计算过去 3600 秒（6 小时）内的统计数据。

在“新建测试”页面上执行以下操作

1. 选择“常用选项”旁边的“高级”。
2. 从“测试类型”列表中选择“自定义”。
3. 在“测试名称”字段中，指定 custom_Test.pl。
4. 在“说明”字段中，指定“测试自定义服务”。
5. 在“测试间隔”字段中指定 120。
6. 在“测试超时”字段中指定 20。
7. 在“每间隔抽样数”字段中指定 1。
8. 在“统计窗口”字段中指定 3600。
9. 在“脚本路径”字段中，指定 /local/bin/custom_Test.pl。
10. 单击“保存测试”。

提交认更改时，SRM 将类似于以下内容的条目添加到 svcrsp.cf 文件中：

```
{
index=99
type=custom
desc="Test custom service"
dest="/local/bin/custom_Test.pl"
interval=120
samples=1
timeout=20
window=3600
tos=0
limit=0
status=active
name="Custom Service Test"
class=""
context=""
flags="1"
loglevel=1
}
```

有关运行自定义测试时可能会遇到的错误的相关信息，请参阅自定义测试错误代码。

附录 A： 服务响应监视器 CLI 命令

您可以使用 CLI 命令为 CA 服务响应监视器编写脚本并使其自动化，并基于命令结果执行操作。

此部分包含以下主题：

svcwatch add adir 命令-添加 Active Directory 测试 (p. 136)
svcwatch add custom 命令-添加自定义测试 (p. 141)
svcwatch add dhcp 命令-添加 DHCP 测试 (p. 146)
svcwatch add dns 命令-添加 DNS 测试 (p. 151)
svcwatch add fileio 命令-添加文件 IO 测试 (p. 156)
svcwatch add ftp 命令-添加 FTP 测试 (p. 161)
svcwatch add http | https 命令-添加 HTTP 或 HTTPS 测试 (p. 166)
svcwatch add imap 命令-添加 IMAP 测试 (p. 172)
svcwatch add ldap 命令-添加 LDAP 测试 (p. 177)
svcwatch add mapi 命令-添加 MAPI 测试 (p. 182)
svcwatch add nis 命令-添加 NIS 测试 (p. 188)
svcwatch add nntp 命令-添加 NNTP 测试 (p. 193)
svcwatch add ping 命令-添加 PING 测试 (p. 198)
svcwatch add pop3 命令-添加 POP3 测试 (p. 203)
svcwatch add rtemail 命令-添加往返电子邮件测试 (p. 208)
svcwatch add smtp 命令-添加 SMTP 测试 (p. 214)
svcwatch add snmp 命令-添加 SNMP 测试 (p. 219)
svcwatch add sql 命令-添加 SQL 测试 (p. 225)
svcwatch add tcpconnect 命令-添加 TCP 连接测试 (p. 231)
svcwatch add tftp 命令-添加 TFTP 测试 (p. 236)
svcwatch add vuser 命令—添加虚拟用户测试 (p. 241)
svcwatch delete 命令-删除测试 (p. 246)
svcwatch list 命令-查看测试信息 (p. 249)
svcwatch setstatus 命令-更改测试状态 (p. 252)
svcwatch version 命令-查看 SRM 版本信息 (p. 255)

svcwatch add adir 命令-添加 Active Directory 测试

svcwatch add adir 命令用于向指定主机上的 SRM 添加 Active Directory 测试。

此命令具有以下格式：

```
svcwatch [options] -o add index descr adir destination
username password args interval samples timeout winsiz tos
limit flags name class contextInfo logLevel
```

该 add 命令使用以下参数：

选项

指定该命令的可能选项。

-h *hostname* | **-h *ipAddr***

（可选）指定 SystemEDGE 主机。

默认值：localhost

-p *port*

（可选）指定 SystemEDGE SNMP 端口。

默认：161

-c *community*

（可选）指定 SNMP 版本 1 和 2c 的 SNMP 团体字符串。

默认值：public

-v *snmpVersion*

（可选）指定 SNMP 版本。可能的值为：

- 1
- 2c
- 3

默认：1

-u *secName*

（可选）指定 SNMPv3 安全用户的名称。

-u *secLevel*

（可选）指定 SNMPv3 的安全级别。可能的值为：

- 1－noAuthNoPriv
- 2－AuthNoPriv
- 3－AuthPriv

-n *contextName*

（可选）指定 MIBMuxed 代理的实例名称。

-a *authPassword*

（可选）标识针对 AuthNoPriv 或 AuthPriv 安全级别选择 SNMPv3 时所需的身份验证密码。

-A *authProtocol*

（可选）指定身份验证协议。可能的值为：

- MD5－身份验证协议 HMAC-MD5
- SHA－身份验证协议 HMAC-SHA

默认：MD5

-x *privPassword*

（可选）指定针对安全级别 3 (AuthPriv) 选择 SNMPv3 时所需的隐私（加密）密码。

-X *encryptProtocol*

（可选）指定针对隐私使用加密协议。可能的值为：

- DES-数据加密标准
- AES-使用 128 位加密密钥的高级加密标准 (AES128)
- 3DES－三重数据加密标准

-m *FIPSmode*

（可选）指定 FIPS 模式。可能的值为：

- 0－非 FIPS
- 1－FIPS 共存
- 2－仅 FIPS

默认：0

-t *timeout*

（可选）指定 SNMP 命令超时。

默认值：10 秒

-d *logLevel*

（可选）指定 SNMP 消息的日志级别。可能的值为：

- 0－记录致命消息
- 1－记录严重消息
- 2－记录警告消息
- 3－记录信息消息
- 4－记录所有消息
- 5－记录所有消息，包括调试消息

默认：0

-f *logFile*

（可选）指定日志文件的名称。

默认值：sysedge_utility.log

-L

（可选）检测控制台和语言目录的当前区域设置（如果可用）。如果未找到语言目录，实用工具将重新使用英语作为默认语言。

-o add *testparams*

向 SRM 添加新测试。

testparams

指定新测试的参数。

index

指定 svcRspTable 索引。

descr

在引号中指定测试说明。如果引号 "" 中为空字符串，则表示未指定说明。

adir

指定 Active Directory 服务类型。

destination

指定用于测试的域控制器。

用户名

在引号中指定用于进行身份验证的用户名。如果引号 "" 中为空字符串，则表示未指定用户名。

password

在引号中指定用于进行身份验证的密码。如果引号 "" 中为空字符串，则表示未指定密码。

args

指定服务参数。每个参数都是一对关键字和值 (key=value)。通过与号 (&) 连接和分隔多个参数。完整参数字符串用引号括起来。

参数的常规语法："key1=value1[&key2=value2& ...]"

domain=*domain*-Active Directory 服务器所在的域。

query=*query*-要发送给 Active Directory 服务器的查询。

filter=*filter*-服务器端结果筛选。

注意：有关每种服务类型的特定参数的详细信息，请参阅测试关键字 (p. 126)。

interval

指定测试间隔（秒）。

限制：30 秒的倍数

示例

指定每个间隔的抽样数。

超时

指定超时（秒）。

winsiz

指定统计时段大小（秒）。

tos

指定“服务类型”或“差分服务代码”IP。对于普通服务，使用 0（零）。另请参阅 RFC 1349。

limit

指定该测试总响应时间的可接受性能限制（或阈值）。在报告中使用该值。

flags

指定以下标志：

0x001 = 收集性能多维数据集

0x100 = 仅请求时执行（运行一次）

name

指定每种服务类型的唯一名称。引号 "" 中的空字符串不指定测试名称。

类

指定类名称。引号 "" 中的空字符串不指定类名称。

contextInfo

指定上下文信息。引号 "" 中的空字符串不指定上下文信息。

logLevel

指定测试执行码的日志级别。可能的值为：

-2 = 使用 SRM 全局日志级别（默认）

-1 = 不记录

0 = 致命（仅最重要的消息）

1 = 严重

...

7 = debug3（记录所有消息）

示例

添加 Active Directory 测试：

```
svcwatch -p 161 -c admin -o add 1360740 "AD-TEST" adir "DC.com" "ADUser"
"bXVyaWM=" "domain=mylab.com&query=cn=Registered,cn=Users,dc=mylab,
dc=com&filter=cn=*" 30 3 30 60 0 0 0x100 "AD-TEST" "ClassName"
"ContextName" 7
```

详细信息

测试的关键字 (p. 126)

svcwatch add custom 命令-添加自定义测试

svcwatch add custom 命令用于向指定主机上的 SRM 添加自定义测试。

此命令具有以下格式：

```
svcwatch [options] -o add index descr custom destination
username password args interval samples timeout winsiz tos
limit flags name class contextInfo logLevel
```

该 add 命令使用以下参数：

选项

指定该命令的可能选项。

-h *hostname* | **-h *ipAddr***

（可选）指定 SystemEDGE 主机。

默认值：localhost

-p *port*

（可选）指定 SystemEDGE SNMP 端口。

默认：161

-c *community*

（可选）指定 SNMP 版本 1 和 2c 的 SNMP 团体字符串。

默认值：public

-v *snmpVersion*

（可选）指定 SNMP 版本。可能的值为：

- 1
- 2c
- 3

默认：1

-u *secName*

（可选）指定 SNMPv3 安全用户的名称。

-u *secLevel*

（可选）指定 SNMPv3 的安全级别。可能的值为：

- 1－noAuthNoPriv
- 2－AuthNoPriv
- 3－AuthPriv

-n *contextName*

（可选）指定 MIBMuxed 代理的实例名称。

-a *authPassword*

（可选）标识针对 AuthNoPriv 或 AuthPriv 安全级别选择 SNMPv3 时所需的身份验证密码。

-A *authProtocol*

（可选）指定身份验证协议。可能的值为：

- MD5－身份验证协议 HMAC-MD5
- SHA－身份验证协议 HMAC-SHA

默认：MD5

-x *privPassword*

（可选）指定针对安全级别 3 (AuthPriv) 选择 SNMPv3 时所需的隐私（加密）密码。

-X *encryptProtocol*

（可选）指定针对隐私使用加密协议。可能的值为：

- DES-数据加密标准
- AES-使用 128 位加密密钥的高级加密标准 (AES128)
- 3DES－三重数据加密标准

-m *FIPSmode*

（可选）指定 FIPS 模式。可能的值为：

- 0－非 FIPS
- 1－FIPS 共存
- 2－仅 FIPS

默认：0

-t *timeout*

（可选）指定 SNMP 命令超时。

默认值：10 秒

-d *logLevel*

（可选）指定 SNMP 消息的日志级别。可能的值为：

- 0－记录致命消息
- 1－记录严重消息
- 2－记录警告消息
- 3－记录信息消息
- 4－记录所有消息
- 5－记录所有消息，包括调试消息

默认：0

-f *logFile*

（可选）指定日志文件的名称。

默认值：sysedge_utility.log

-L

（可选）检测控制台和语言目录的当前区域设置（如果可用）。如果未找到语言目录，实用工具将重新使用英语作为默认语言。

-o add *testparams*

向 SRM 添加新测试。

testparams

指定新测试的参数。

index

指定 svcRspTable 索引。

descr

在引号中指定测试说明。如果引号 "" 中为空字符串，则表示未指定说明。

custom

指定自定义服务类型。

destination

指定脚本路径。

用户名

在引号中指定用于进行身份验证的用户名。如果引号 "" 中为空字符串，则表示未指定用户名。

password

在引号中指定用于进行身份验证的密码。如果引号 "" 中为空字符串，则表示未指定密码。

args

没有自定义服务类型可用的参数。如果引号 "" 中为空字符串，则表示未指定参数。

注意：有关每种服务类型的特定参数的详细信息，请参阅测试关键字 (p. 126)。

interval

指定测试间隔（秒）。

限制：30 秒的倍数

示例

指定每个间隔的抽样数。

超时

指定超时（秒）。

winsiz

指定统计时段大小（秒）。

tos

指定“服务类型”或“差分服务代码”IP。对于普通服务，使用 0（零）。另请参阅 RFC 1349。

limit

指定该测试总响应时间的可接受性能限制（或阈值）。在报告中使用该值。

flags

指定以下标志：

0x001 = 收集性能多维数据集

0x100 = 仅请求时执行（运行一次）

name

指定每种服务类型的唯一名称。引号 "" 中的空字符串不指定测试名称。

类

指定类名称。引号 "" 中的空字符串不指定类名称。

contextInfo

指定上下文信息。引号 "" 中的空字符串不指定上下文信息。

logLevel

指定测试执行码的日志级别。可能的值为：

-2 = 使用 SRM 全局日志级别（默认）

-1 = 不记录

0 = 致命（仅最重要的消息）

1 = 严重

...

7 = debug3（记录所有消息）

示例

添加自定义测试：

```
svcwatch -h localhost -p 161 -c topsecret -o add 1360741 "CUSTOM-TEST" custom
"c:\scripts\custom-test.bat" "" "" "" 30 3 30 60 0 0 0x100 "Custom-TEST"
"ClassName" "ContextName" 7
```

详细信息

测试的关键字 (p. 126)

svcwatch add dhcp 命令-添加 DHCP 测试

svcwatch add dhcp 命令用于向指定主机上的 SRM 添加 DHCP 测试。

此命令具有以下格式：

```
svcwatch [options] -o add index descr dhcp destination
username password args interval samples timeout winsiz tos
limit flags name class contextInfo logLevel
```

该 add 命令使用以下参数：

选项

指定该命令的可能选项。

-h *hostname* | **-h *ipAddr***

（可选）指定 SystemEDGE 主机。

默认值：localhost

-p *port*

（可选）指定 SystemEDGE SNMP 端口。

默认：161

-c *community*

（可选）指定 SNMP 版本 1 和 2c 的 SNMP 团体字符串。

默认值：public

-v *snmpVersion*

（可选）指定 SNMP 版本。可能的值为：

- 1
- 2c
- 3

默认：1

-u *secName*

（可选）指定 SNMPv3 安全用户的名称。

-u *secLevel*

（可选）指定 SNMPv3 的安全级别。可能的值为：

- 1－noAuthNoPriv
- 2－AuthNoPriv
- 3－AuthPriv

-n *contextName*

（可选）指定 MIBMuxed 代理的实例名称。

-a *authPassword*

（可选）标识针对 AuthNoPriv 或 AuthPriv 安全级别选择 SNMPv3 时所需的身份验证密码。

-A *authProtocol*

（可选）指定身份验证协议。可能的值为：

- MD5－身份验证协议 HMAC-MD5
- SHA－身份验证协议 HMAC-SHA

默认：MD5

-x *privPassword*

（可选）指定针对安全级别 3 (AuthPriv) 选择 SNMPv3 时所需的隐私（加密）密码。

-X *encryptProtocol*

（可选）指定针对隐私使用加密协议。可能的值为：

- DES-数据加密标准
- AES-使用 128 位加密密钥的高级加密标准 (AES128)
- 3DES－三重数据加密标准

-m *FIPSmode*

（可选）指定 FIPS 模式。可能的值为：

- 0－非 FIPS
- 1－FIPS 共存
- 2－仅 FIPS

默认：0

-t *timeout*

（可选）指定 SNMP 命令超时。

默认值：10 秒

-d *logLevel*

（可选）指定 SNMP 消息的日志级别。可能的值为：

- 0－记录致命消息
- 1－记录严重消息
- 2－记录警告消息
- 3－记录信息消息
- 4－记录所有消息
- 5－记录所有消息，包括调试消息

默认：0

-f *logFile*

（可选）指定日志文件的名称。

默认值：sysedge_utility.log

-L

（可选）检测控制台和语言目录的当前区域设置（如果可用）。如果未找到语言目录，实用工具将重新使用英语作为默认语言。

-o add *testparams*

向 SRM 添加新测试。

testparams

指定新测试的参数。

index

指定 svcRspTable 索引。

descr

在引号中指定测试说明。如果引号 "" 中为空字符串，则表示未指定说明。

dhcp

指定 DHCP 服务类型。

destination

指定要测试的 DHCP 服务器的主机名或 IP 地址。

用户名

在引号中指定用于进行身份验证的用户名。如果引号 "" 中为空字符串，则表示未指定用户名。

password

在引号中指定用于进行身份验证的密码。如果引号 "" 中为空字符串，则表示未指定密码。

args

没有 DHCP 服务类型可用的参数。如果引号 "" 中为空字符串，则表示未指定参数。

注意：有关每种服务类型的特定参数的详细信息，请参阅测试关键字 (p. 126)。

interval

指定测试间隔（秒）。

限制：30 秒的倍数

示例

指定每个间隔的抽样数。

超时

指定超时（秒）。

winsiz

指定统计时段大小（秒）。

tos

指定“服务类型”或“差分服务代码”IP。对于普通服务，使用 0（零）。另请参阅 RFC 1349。

limit

指定该测试总响应时间的可接受性能限制（或阈值）。在报告中使用该值。

flags

指定以下标志：

0x001 = 收集性能多维数据集

0x100 = 仅请求时执行（运行一次）

name

指定每种服务类型的唯一名称。引号 "" 中的空字符串不指定测试名称。

类

指定类名称。引号 "" 中的空字符串不指定类名称。

contextInfo

指定上下文信息。引号 "" 中的空字符串不指定上下文信息。

logLevel

指定测试执行码的日志级别。可能的值为：

-2 = 使用 SRM 全局日志级别（默认）

-1 = 不记录

0 = 致命（仅最重要的消息）

1 = 严重

...

7 = debug3（记录所有消息）

示例

添加 DHCP 测试：

```
svcwatch -h localhost -p 161 -c topsecret -o add 1360742 "DHCP-TEST" dhcp
"dhcpservername" "" "" "" 30 3 30 60 0 0 0x100 "DHCP-TEST" "ClassName"
"ContextName" 7
```

详细信息

测试的关键字 (p. 126)

svcwatch add dns 命令-添加 DNS 测试

svcwatch add dns 命令用于向指定主机上的 SRM 添加 DNS 测试。

此命令具有以下格式：

```
svcwatch [options] -o add index descr dns destination
username password args interval samples timeout winsiz tos
limit flags name class contextInfo logLevel
```

该 add 命令使用以下参数：

选项

指定该命令的可能选项。

-h *hostname* | **-h *ipAddr***

（可选）指定 SystemEDGE 主机。

默认值：localhost

-p *port*

（可选）指定 SystemEDGE SNMP 端口。

默认：161

-c *community*

（可选）指定 SNMP 版本 1 和 2c 的 SNMP 团体字符串。

默认值：public

-v *snmpVersion*

（可选）指定 SNMP 版本。可能的值为：

- 1
- 2c
- 3

默认：1

-u *secName*

（可选）指定 SNMPv3 安全用户的名称。

-u *secLevel*

（可选）指定 SNMPv3 的安全级别。可能的值为：

- 1－noAuthNoPriv
- 2－AuthNoPriv
- 3－AuthPriv

-n *contextName*

（可选）指定 MIBMuxed 代理的实例名称。

-a *authPassword*

（可选）标识针对 AuthNoPriv 或 AuthPriv 安全级别选择 SNMPv3 时所需的身份验证密码。

-A *authProtocol*

（可选）指定身份验证协议。可能的值为：

- MD5－身份验证协议 HMAC-MD5
- SHA－身份验证协议 HMAC-SHA

默认：MD5

-x *privPassword*

（可选）指定针对安全级别 3 (AuthPriv) 选择 SNMPv3 时所需的隐私（加密）密码。

-X *encryptProtocol*

（可选）指定针对隐私使用加密协议。可能的值为：

- DES-数据加密标准
- AES-使用 128 位加密密钥的高级加密标准 (AES128)
- 3DES－三重数据加密标准

-m *FIPSmode*

（可选）指定 FIPS 模式。可能的值为：

- 0－非 FIPS
- 1－FIPS 共存
- 2－仅 FIPS

默认：0

-t *timeout*

（可选）指定 SNMP 命令超时。

默认值：10 秒

-d *logLevel*

（可选）指定 SNMP 消息的日志级别。可能的值为：

- 0－记录致命消息
- 1－记录严重消息
- 2－记录警告消息
- 3－记录信息消息
- 4－记录所有消息
- 5－记录所有消息，包括调试消息

默认：0

-f *logFile*

（可选）指定日志文件的名称。

默认值：sysedge_utility.log

-L

（可选）检测控制台和语言目录的当前区域设置（如果可用）。如果未找到语言目录，实用工具将重新使用英语作为默认语言。

-o add *testparams*

向 SRM 添加新测试。

testparams

指定新测试的参数。

index

指定 svcRspTable 索引。

descr

在引号中指定测试说明。如果引号 "" 中为空字符串，则表示未指定说明。

dns

指定 DNS 服务类型。

destination

指定用于测试的 DNS 服务器。

用户名

在引号中指定用于进行身份验证的用户名。如果引号 "" 中为空字符串，则表示未指定用户名。

password

在引号中指定用于进行身份验证的密码。如果引号 "" 中为空字符串，则表示未指定密码。

args

指定服务参数。参数是一对用引号括起的参数和值 (hostname=*host*)。

hostname=*host*-要查询的主机名。

注意：有关每种服务类型的特定参数的详细信息，请参阅测试关键字 (p. 126)。

interval

指定测试间隔（秒）。

限制：30 秒的倍数

示例

指定每个间隔的抽样数。

超时

指定超时（秒）。

winsiz

指定统计时段大小（秒）。

tos

指定“服务类型”或“差分服务代码”IP。对于普通服务，使用 0（零）。另请参阅 RFC 1349。

limit

指定该测试总响应时间的可接受性能限制（或阈值）。在报告中使用该值。

flags

指定以下标志：

0x001 = 收集性能多维数据集

0x100 = 仅请求时执行（运行一次）

name

指定每种服务类型的唯一名称。引号 "" 中的空字符串不指定测试名称。

类

指定类名称。引号 "" 中的空字符串不指定类名称。

contextInfo

指定上下文信息。引号 "" 中的空字符串不指定上下文信息。

logLevel

指定测试执行码的日志级别。可能的值为：

-2 = 使用 SRM 全局日志级别（默认）

-1 = 不记录

0 = 致命（仅最重要的消息）

1 = 严重

...

7 = debug3（记录所有消息）

示例

添加 DNS 测试：

```
svcwatch -h localhost -p 161 -c topsecret -o add 1360743 "DNS-TEST"
dns "mydnsserver" "" "" "hostname=testhost" 30 3 30 60 0 0 0x100
"DNS-Test" "ClassName" "ContextName" 7
```

详细信息

测试的关键字 (p. 126)

svcwatch add fileio 命令-添加文件 IO 测试

svcwatch add fileio 命令用于向指定主机上的 SRM 添加文件 IO 测试。

此命令具有以下格式：

svcwatch [-h| -p| -v| -u| -n| -a| -A| -x| -X| -m| -t| -d| -f] -o add *index descr* fileio *destination username password args interval samples timeout winsiz tos limit flags name class contextInfo logLevel*

add 命令使用以下参数：

选项

指定该命令的可能选项。

-h *hostname*｜ -h *ipAddr*

（可选）指定 SystemEDGE 主机。

默认值：localhost

-p *port*

（可选）指定 SystemEDGE SNMP 端口。

默认：161

-c *community*

（可选）指定 SNMP 版本 1 和 2c 的 SNMP 团体字符串。

默认值：public

-v *snmpVersion*

（可选）指定 SNMP 版本。可能的值为：

- 1
- 2c
- 3

默认：1

-u *secName*

（可选）指定 SNMPv3 安全用户的名称。

-u *secLevel*

（可选）指定 SNMPv3 的安全级别。可能的值为：

- 1－noAuthNoPriv
- 2－AuthNoPriv
- 3－AuthPriv

-n *contextName*

（可选）指定 MIBMuxed 代理的实例名称。

-a *authPassword*

（可选）标识针对 AuthNoPriv 或 AuthPriv 安全级别选择 SNMPv3 时所需的身份验证密码。

-A *authProtocol*

（可选）指定身份验证协议。可能的值为：

- MD5－身份验证协议 HMAC-MD5
- SHA－身份验证协议 HMAC-SHA

默认：MD5

-x *privPassword*

（可选）指定针对安全级别 3 (AuthPriv) 选择 SNMPv3 时所需的隐私（加密）密码。

-X *encryptProtocol*

（可选）指定针对隐私使用加密协议。可能的值为：

- DES-数据加密标准
- AES-使用 128 位加密密钥的高级加密标准 (AES128)
- 3DES－三重数据加密标准

-m *FIPSmode*

（可选）指定 FIPS 模式。可能的值为：

- 0－非 FIPS
- 1－FIPS 共存
- 2－仅 FIPS

默认：0

-t *timeout*

（可选）指定 SNMP 命令超时。

默认值：10 秒

-d *logLevel*

（可选）指定 SNMP 消息的日志级别。可能的值为：

- 0－记录致命消息
- 1－记录严重消息
- 2－记录警告消息
- 3－记录信息消息
- 4－记录所有消息
- 5－记录所有消息，包括调试消息

默认：0

-f *logFile*

（可选）指定日志文件的名称。

默认值：sysedge_utility.log

-L

（可选）检测控制台和语言目录的当前区域设置（如果可用）。如果未找到语言目录，实用工具将重新使用英语作为默认语言。

-o add *testparams*

将新测试添加到 SRM 中。

testparams

为新测试指定参数。

index

指定 svcRspTable 索引。

descr

在引号中指定测试的说明。引号 ("") 中为空字符串将不指定说明。

fileio

指定文件 IO 服务类型。

destination

指定要测试的远程文件。

username

在引号中指定用于进行身份验证的用户名。引号 ("") 中为空字符串将不指定用户名。

password

在引号中指定用于进行身份验证的密码。引号 ("") 中为空字符串将不指定密码。

args

指定服务参数。每个参数都是一对关键字和值 (key=value)。通过与号 (&) 连接和分隔多个参数。完整参数字符串用引号括起来。

参数的常规语法："key1=value1[&key2=value2& ...]"

op=r-读取文件。

op=w-将本地参考文件的内容写入远程文件系统上的测试文件，然后删除测试文件。

op=rw-将本地参考文件的内容写入远程文件系统上的测试文件，读取测试文件，然后删除测试文件。

op=cmp-逐个读取文件，并比较文件内容。

local=*path*-用于写入、读取/写入以及比较操作的本地路径和文件名。

domain=*domain*-登录服务器的用户所属的域（仅 Windows）。

注意：有关每个服务类型的特定参数的详细信息，请参阅测试的关键字 (p. 126)。

interval

指定测试间隔（秒）。

限制：30 秒的倍数

示例

指定每个间隔的抽样数。

超时

指定超时（秒）。

winsiz

指定统计时段大小（秒）。

tos

指定“服务类型”或“差分服务代码”IP。对于普通服务，使用 0（零）。另请参阅 RFC 1349。

limit

指定该测试总响应时间的可接受性能限制（或阈值）。在报告中使用该值。

flags

指定以下标志：

0x001 = 收集性能多维数据集

0x100 = 仅请求时执行（运行一次）

name

指定每种服务类型的唯一名称。引号 "" 中的空字符串不指定测试名称。

类

指定类名称。引号 "" 中的空字符串不指定类名称。

contextInfo

指定上下文信息。引号 "" 中的空字符串不指定上下文信息。

logLevel

指定测试执行码的日志级别。可能的值为：

-2 = 使用 SRM 全局日志级别（默认）

-1 = 不记录

0 = 致命（仅最重要的消息）

1 = 严重

...

7 = debug3（记录所有消息）

示例

添加文件 I/O 测试：

```
svcwatch -h localhost -p 161 -c topsecret -o add 1360744 "FILEIO-TEST"
fileio "F:\Test\CompTest.bin" "" ""
"op=cmp&local=C:\sysedge\bin\saFileIOTest.bin"
30 1 10 120 0 0 0x100 "FILEIO-TEST" "" ""
```

详细信息

测试的关键字 (p. 126)

svcwatch add ftp 命令-添加 FTP 测试

svcwatch add ftp 命令用于向指定主机上的 SRM 添加 FTP 测试。

此命令具有以下格式：

```
svcwatch [options] -o add index descr ftp destination
username password args interval samples timeout winsiz tos
limit flags name class contextInfo logLevel
```

该 add 命令使用以下参数：

选项

指定该命令的可能选项。

-h *hostname* | **-h *ipAddr***

（可选）指定 SystemEDGE 主机。

默认值：localhost

-p *port*

（可选）指定 SystemEDGE SNMP 端口。

默认：161

-c *community*

（可选）指定 SNMP 版本 1 和 2c 的 SNMP 团体字符串。

默认值：public

-v *snmpVersion*

（可选）指定 SNMP 版本。可能的值为：

- 1
- 2c
- 3

默认：1

-u *secName*

（可选）指定 SNMPv3 安全用户的名称。

-u *secLevel*

（可选）指定 SNMPv3 的安全级别。可能的值为：

- 1－noAuthNoPriv
- 2－AuthNoPriv
- 3－AuthPriv

-n *contextName*

（可选）指定 MIBMuxed 代理的实例名称。

-a *authPassword*

（可选）标识针对 AuthNoPriv 或 AuthPriv 安全级别选择 SNMPv3 时所需的身份验证密码。

-A *authProtocol*

（可选）指定身份验证协议。可能的值为：

- MD5－身份验证协议 HMAC-MD5
- SHA－身份验证协议 HMAC-SHA

默认：MD5

-x *privPassword*

（可选）指定针对安全级别 3 (AuthPriv) 选择 SNMPv3 时所需的隐私（加密）密码。

-X *encryptProtocol*

（可选）指定针对隐私使用加密协议。可能的值为：

- DES-数据加密标准
- AES-使用 128 位加密密钥的高级加密标准 (AES128)
- 3DES－三重数据加密标准

-m *FIPSmode*

（可选）指定 FIPS 模式。可能的值为：

- 0－非 FIPS
- 1－FIPS 共存
- 2－仅 FIPS

默认：0

-t *timeout*

（可选）指定 SNMP 命令超时。

默认值：10 秒

-d *logLevel*

（可选）指定 SNMP 消息的日志级别。可能的值为：

- 0－记录致命消息
- 1－记录严重消息
- 2－记录警告消息
- 3－记录信息消息
- 4－记录所有消息
- 5－记录所有消息，包括调试消息

默认：0

-f *logFile*

（可选）指定日志文件的名称。

默认值：sysedge_utility.log

-L

（可选）检测控制台和语言目录的当前区域设置（如果可用）。如果未找到语言目录，实用工具将重新使用英语作为默认语言。

-o add *testparams*

向 SRM 添加新测试。

testparams

指定新测试的参数。

index

指定 svcRspTable 索引。

descr

在引号中指定测试说明。如果引号 "" 中为空字符串，则表示未指定说明。

ftp

指定 FTP 服务类型。

destination

指定用于测试的 FTP 服务器。

用户名

在引号中指定用于进行身份验证的用户名。如果引号 "" 中为空字符串，则表示未指定用户名。

password

在引号中指定用于进行身份验证的密码。如果引号 "" 中为空字符串，则表示未指定密码。

args

指定服务参数。每个参数都是一对关键字和值 (key=value)。通过与号 (&) 连接和分隔多个参数。完整参数字符串用引号括起来。

参数的常规语法："key1=value1[&key2=value2& ...]"

op=g (get)-登录并读取指定文件（但不执行写入操作），然后注销。

op=p (put)-登录 FTP 服务器并在其中写入指定文件，然后注销。如果远程目录没有写入权限，测试将失败。

op=login-使用指定用户名和密码登录，然后注销。

remote=*path*-指定要读取的文件的路径。

local=*path*-指定 FTP 服务器上要写入的文件的名称。

注意：有关每种服务类型的特定参数的详细信息，请参阅测试关键字 (p. 126)。

interval

指定测试间隔（秒）。

限制：30 秒的倍数

示例

指定每个间隔的抽样数。

超时

指定超时（秒）。

winsiz

指定统计时段大小（秒）。

tos

指定“服务类型”或“差分服务代码”IP。对于普通服务，使用 0（零）。另请参阅 RFC 1349。

limit

指定该测试总响应时间的可接受性能限制（或阈值）。在报告中使用该值。

flags

指定以下标志：

0x001 = 收集性能多维数据集

0x100 = 仅请求时执行（运行一次）

name

指定每种服务类型的唯一名称。引号 "" 中的空字符串不指定测试名称。

类

指定类名称。引号 "" 中的空字符串不指定类名称。

contextInfo

指定上下文信息。引号 "" 中的空字符串不指定上下文信息。

logLevel

指定测试执行码的日志级别。可能的值为：

-2 = 使用 SRM 全局日志级别（默认）

-1 = 不记录

0 = 致命（仅最重要的消息）

1 = 严重

...

7 = debug3（记录所有消息）

示例

添加 ftp 测试：

```
svcwatch -h localhost -p 161 -c topsecret -o add 1360745 "FTP-TEST"
ftp "ftpstage.mydomain.com:21" "ftpuser" "ftp123" "op=login" 3600 1
10 604800 0 0 0x100 "FTP-TEST" "" "" 1
```

详细信息

测试的关键字 (p. 126)

svcwatch add http | https 命令-添加 HTTP 或 HTTPS 测试

svcwatch add http | https 命令用于向指定主机上的 SRM 添加 HTTP 或 HTTPS 测试。

此命令具有以下格式：

```
svcwatch [options] -o add index descr {http|https} destination
username password args interval samples timeout winsiz tos
limit flags name class contextInfo logLevel
```

该 add 命令使用以下参数：

选项

指定该命令的可能选项。

-h *hostname* | -h *ipAddr*

（可选）指定 SystemEDGE 主机。

默认值：localhost

-p *port*

（可选）指定 SystemEDGE SNMP 端口。

默认：161

-c *community*

（可选）指定 SNMP 版本 1 和 2c 的 SNMP 团体字符串。

默认值：public

-v *snmpVersion*

（可选）指定 SNMP 版本。可能的值为：

- 1
- 2c
- 3

默认：1

-u *secName*

（可选）指定 SNMPv3 安全用户的名称。

-u *secLevel*

（可选）指定 SNMPv3 的安全级别。可能的值为：

- 1－noAuthNoPriv
- 2－AuthNoPriv
- 3－AuthPriv

-n *contextName*

（可选）指定 MIBMuxed 代理的实例名称。

-a *authPassword*

（可选）标识针对 AuthNoPriv 或 AuthPriv 安全级别选择 SNMPv3 时所需的身份验证密码。

-A *authProtocol*

（可选）指定身份验证协议。可能的值为：

- MD5－身份验证协议 HMAC-MD5
- SHA－身份验证协议 HMAC-SHA

默认：MD5

-x *privPassword*

（可选）指定针对安全级别 3 (AuthPriv) 选择 SNMPv3 时所需的隐私（加密）密码。

-X *encryptProtocol*

（可选）指定针对隐私使用加密协议。可能的值为：

- DES-数据加密标准
- AES-使用 128 位加密密钥的高级加密标准 (AES128)
- 3DES－三重数据加密标准

-m *FIPSmode*

（可选）指定 FIPS 模式。可能的值为：

- 0－非 FIPS
- 1－FIPS 共存
- 2－仅 FIPS

默认：0

-t *timeout*

（可选）指定 SNMP 命令超时。

默认值：10 秒

-d *logLevel*

（可选）指定 SNMP 消息的日志级别。可能的值为：

- 0－记录致命消息
- 1－记录严重消息
- 2－记录警告消息
- 3－记录信息消息
- 4－记录所有消息
- 5－记录所有消息，包括调试消息

默认：0

-f *logFile*

（可选）指定日志文件的名称。

默认值：sysedge_utility.log

-L

（可选）检测控制台和语言目录的当前区域设置（如果可用）。如果未找到语言目录，实用工具将重新使用英语作为默认语言。

-o add *testparams*

向 SRM 添加新测试。

testparams

指定新测试的参数。

index

指定 svcRspTable 索引。

descr

在引号中指定测试说明。如果引号 "" 中为空字符串，则表示未指定说明。

http | https

指定 HTTP 或 HTTPS 服务类型。

destination

指定用于测试的 Web 服务器。

用户名

在引号中指定用于进行身份验证的用户名。如果引号 "" 中为空字符串，则表示未指定用户名。

password

在引号中指定用于进行身份验证的密码。如果引号 "" 中为空字符串，则表示未指定密码。

args

指定服务参数。每个参数都是一对关键字和值 (key=value)。通过与号 (&) 连接和分隔多个参数。完整参数字符串用引号括起来。

参数的常规语法："key1=value1[&key2=value2& ...]"

max_depth=*number*-下载嵌套框架时测试应遍历的层数（HTTP 和 HTTPS 测试在页面下载期间下载所有框架、图像、外部脚本以及小程序，从而使度量可以反映下载页面时的用户体验）。

默认：3

search=*pattern*-希望 SRM 在测试页面上匹配的正则表达式。

minmatch=*number*-查找搜索模式的最少次数。

content_dl=true|false-包括脚本、图像、小程序等的下载内容。

content_err=true|false-下载时出现的任何错误都会导致测试失败。

proxy=*proxy*-要使用的代理服务器的主机名（如果从中测试的系统没有直接 Internet 访问）。

proxyuser=*puser*-该代理的用户名。

proxypass=*ppass*-代理用户的密码。

注意：有关每种服务类型的特定参数的详细信息，请参阅测试关键字 (p. 126)。

interval

指定测试间隔（秒）。

限制：30 秒的倍数

示例

指定每个间隔的抽样数。

超时

指定超时（秒）。

winsiz

指定统计时段大小（秒）。

tos

指定“服务类型”或“差分服务代码”IP。对于普通服务，使用 0（零）。另请参阅 RFC 1349。

limit

指定该测试总响应时间的可接受性能限制（或阈值）。在报告中使用该值。

flags

指定以下标志：

0x001 = 收集性能多维数据集

0x100 = 仅请求时执行（运行一次）

name

指定每种服务类型的唯一名称。引号 "" 中的空字符串不指定测试名称。

类

指定类名称。引号 "" 中的空字符串不指定类名称。

contextInfo

指定上下文信息。引号 "" 中的空字符串不指定上下文信息。

logLevel

指定测试执行码的日志级别。可能的值为：

-2 = 使用 SRM 全局日志级别（默认）

-1 = 不记录

0 = 致命（仅最重要的消息）

1 = 严重

...

7 = debug3（记录所有消息）

示例

添加 https 测试：

```
svcwatch -h localhost -p 161 -c topsecret -o add 1360746 "HTTPS-TEST"
https "https://chargeMycredit.com" "creditAcct" "secret"
"max_depth=3&minmatch=1&content_dl=true&content_err=false" 60 1 20
300 0 0 0x100 "HTTPS-TEST" "" ""
```

详细信息

测试的关键字 (p. 126)

svcwatch add imap 命令-添加 IMAP 测试

svcwatch add imap 命令用于向指定主机上的 SRM 添加 IMAP 测试。

此命令具有以下格式：

```
svcwatch [options] -o add index descr imap destination
username password args interval samples timeout winsiz tos
limit flags name class contextInfo logLevel
```

该 add 命令使用以下参数：

选项

指定该命令的可能选项。

-h *hostname* | **-h *ipAddr***

（可选）指定 SystemEDGE 主机。

默认值：localhost

-p *port*

（可选）指定 SystemEDGE SNMP 端口。

默认：161

-c *community*

（可选）指定 SNMP 版本 1 和 2c 的 SNMP 团体字符串。

默认值：public

-v *snmpVersion*

（可选）指定 SNMP 版本。可能的值为：

- 1
- 2c
- 3

默认：1

-u *secName*

（可选）指定 SNMPv3 安全用户的名称。

-u *secLevel*

（可选）指定 SNMPv3 的安全级别。可能的值为：

- 1－noAuthNoPriv
- 2－AuthNoPriv
- 3－AuthPriv

-n *contextName*

（可选）指定 MIBMuxed 代理的实例名称。

-a *authPassword*

（可选）标识针对 AuthNoPriv 或 AuthPriv 安全级别选择 SNMPv3 时所需的身份验证密码。

-A *authProtocol*

（可选）指定身份验证协议。可能的值为：

- MD5－身份验证协议 HMAC-MD5
- SHA－身份验证协议 HMAC-SHA

默认：MD5

-x *privPassword*

（可选）指定针对安全级别 3 (AuthPriv) 选择 SNMPv3 时所需的隐私（加密）密码。

-X *encryptProtocol*

（可选）指定针对隐私使用加密协议。可能的值为：

- DES-数据加密标准
- AES-使用 128 位加密密钥的高级加密标准 (AES128)
- 3DES－三重数据加密标准

-m *FIPSmode*

（可选）指定 FIPS 模式。可能的值为：

- 0－非 FIPS
- 1－FIPS 共存
- 2－仅 FIPS

默认：0

-t *timeout*

（可选）指定 SNMP 命令超时。

默认值：10 秒

-d *logLevel*

（可选）指定 SNMP 消息的日志级别。可能的值为：

- 0－记录致命消息
- 1－记录严重消息
- 2－记录警告消息
- 3－记录信息消息
- 4－记录所有消息
- 5－记录所有消息，包括调试消息

默认：0

-f *logFile*

（可选）指定日志文件的名称。

默认值：sysedge_utility.log

-L

（可选）检测控制台和语言目录的当前区域设置（如果可用）。如果未找到语言目录，实用工具将重新使用英语作为默认语言。

-o add *testparams*

向 SRM 添加新测试。

testparams

指定新测试的参数。

index

指定 svcRspTable 索引。

descr

在引号中指定测试说明。如果引号 "" 中为空字符串，则表示未指定说明。

imap

指定 IMAP 服务类型。

destination

指定用于测试的 IMAP 服务器和端口 (*server*:*port*)。默认端口：143

用户名

在引号中指定用于进行身份验证的用户名。如果引号 "" 中为空字符串，则表示未指定用户名。

password

在引号中指定用于进行身份验证的密码。如果引号 "" 中为空字符串，则表示未指定密码。

args

指定服务参数。每个参数都是一对关键字和值 (key=value)。通过与号 (&) 连接和分隔多个参数。完整参数字符串用引号括起来。

参数的常规语法："key1=value1[&key2=value2& ...]"

download=Download First Message-仅下载该用户帐户的第一条消息。

download=Download All Messages-下载该用户帐户的所有消息。

delete=true-删除下载的消息。

delete=false-不删除下载的消息。

注意：有关每种服务类型的特定参数的详细信息，请参阅测试关键字 (p. 126)。

interval

指定测试间隔（秒）。

限制：30 秒的倍数

示例

指定每个间隔的抽样数。

超时

指定超时（秒）。

winsiz

指定统计时段大小（秒）。

tos

指定“服务类型”或“差分服务代码”IP。对于普通服务，使用 0（零）。另请参阅 RFC 1349。

limit

指定该测试总响应时间的可接受性能限制（或阈值）。在报告中使用该值。

flags

指定以下标志：

0x001 = 收集性能多维数据集

0x100 = 仅请求时执行（运行一次）

name

指定每种服务类型的唯一名称。引号 "" 中的空字符串不指定测试名称。

类

指定类名称。引号 "" 中的空字符串不指定类名称。

contextInfo

指定上下文信息。引号 "" 中的空字符串不指定上下文信息。

logLevel

指定测试执行码的日志级别。可能的值为：

-2 = 使用 SRM 全局日志级别（默认）

-1 = 不记录

0 = 致命（仅最重要的消息）

1 = 严重

...

7 = debug3（记录所有消息）

示例

添加 IMAP 测试：

```
svcwatch -h localhost -p 161 -c topsecret -o add 1360747 "IMAP-TEST"
imap "imapserver.yourdomain.com:143" "IMAPuser@server.domain" "IMAP123"
"download=Download All Messages&delete=true" 300 1 10 7200 0 0 0x100
"IMAP-TEST" "" ""
```

详细信息

测试的关键字 (p. 126)

svcwatch add ldap 命令-添加 LDAP 测试

svcwatch add ldap 命令用于向指定主机上的 SRM 添加 LDAP 测试。

此命令具有以下格式：

```
svcwatch [options] -o add index descr ldap destination
username password args interval samples timeout winsiz tos
limit flags name class contextInfo logLevel
```

该 add 命令使用以下参数：

选项

指定该命令的可能选项。

-h *hostname* | **-h *ipAddr***

（可选）指定 SystemEDGE 主机。

默认值：localhost

-p *port*

（可选）指定 SystemEDGE SNMP 端口。

默认：161

-c *community*

（可选）指定 SNMP 版本 1 和 2c 的 SNMP 团体字符串。

默认值：public

-v *snmpVersion*

（可选）指定 SNMP 版本。可能的值为：

- 1
- 2c
- 3

默认：1

-u *secName*

（可选）指定 SNMPv3 安全用户的名称。

-u *secLevel*

（可选）指定 SNMPv3 的安全级别。可能的值为：

- 1－noAuthNoPriv
- 2－AuthNoPriv
- 3－AuthPriv

-n *contextName*

（可选）指定 MIBMuxed 代理的实例名称。

-a *authPassword*

（可选）标识针对 AuthNoPriv 或 AuthPriv 安全级别选择 SNMPv3 时所需的身份验证密码。

-A *authProtocol*

（可选）指定身份验证协议。可能的值为：

- MD5－身份验证协议 HMAC-MD5
- SHA－身份验证协议 HMAC-SHA

默认：MD5

-x *privPassword*

（可选）指定针对安全级别 3 (AuthPriv) 选择 SNMPv3 时所需的隐私（加密）密码。

-X *encryptProtocol*

（可选）指定针对隐私使用加密协议。可能的值为：

- DES-数据加密标准
- AES-使用 128 位加密密钥的高级加密标准 (AES128)
- 3DES－三重数据加密标准

-m *FIPSmode*

（可选）指定 FIPS 模式。可能的值为：

- 0－非 FIPS
- 1－FIPS 共存
- 2－仅 FIPS

默认：0

-t *timeout*

（可选）指定 SNMP 命令超时。

默认值：10 秒

-d *logLevel*

（可选）指定 SNMP 消息的日志级别。可能的值为：

- 0－记录致命消息
- 1－记录严重消息
- 2－记录警告消息
- 3－记录信息消息
- 4－记录所有消息
- 5－记录所有消息，包括调试消息

默认：0

-f *logFile*

（可选）指定日志文件的名称。

默认值：sysedge_utility.log

-L

（可选）检测控制台和语言目录的当前区域设置（如果可用）。如果未找到语言目录，实用工具将重新使用英语作为默认语言。

-o add *testparams*

向 SRM 添加新测试。

testparams

指定新测试的参数。

index

指定 svcRspTable 索引。

descr

在引号中指定测试说明。如果引号 "" 中为空字符串，则表示未指定说明。

ldap

指定 LDAP 服务类型。

destination

指定用于测试的 LDAP 服务器和端口 (*server*:*port*)。默认端口：389

用户名

在引号中指定用于进行身份验证的用户名。如果引号 "" 中为空字符串，则表示未指定用户名。

password

在引号中指定用于进行身份验证的密码。如果引号 "" 中为空字符串，则表示未指定密码。

args

指定服务参数。每个参数都是一对关键字和值 (key=value)。通过与号 (&) 连接和分隔多个参数。完整参数字符串用引号括起来。

参数的常规语法："key1=value1[&key2=value2& ...]"

query=*query*-指定要发送给 LDAP 服务器的查询。

domain=*domain*-指定 LDAP 域。

filter=*filter*-指定服务器端结果筛选。

注意：有关每种服务类型的特定参数的详细信息，请参阅测试关键字 (p. 126)。

interval

指定测试间隔（秒）。

限制：30 秒的倍数

示例

指定每个间隔的抽样数。

超时

指定超时（秒）。

winsiz

指定统计时段大小（秒）。

tos

指定“服务类型”或“差分服务代码”IP。对于普通服务，使用 0（零）。另请参阅 RFC 1349。

limit

指定该测试总响应时间的可接受性能限制（或阈值）。在报告中使用该值。

flags

指定以下标志：

0x001 = 收集性能多维数据集

0x100 = 仅请求时执行（运行一次）

name

指定每种服务类型的唯一名称。引号 "" 中的空字符串不指定测试名称。

类

指定类名称。引号 "" 中的空字符串不指定类名称。

contextInfo

指定上下文信息。引号 "" 中的空字符串不指定上下文信息。

logLevel

指定测试执行码的日志级别。可能的值为：

-2 = 使用 SRM 全局日志级别（默认）

-1 = 不记录

0 = 致命（仅最重要的消息）

1 = 严重

...

7 = debug3（记录所有消息）

示例

添加 LDAP 测试：

```
svcwatch -h localhost -p 161 -c topsecret -o add 1360748 "LDAP-TEST"
ldap "arch" "ldapUser" "ldapPassword" "query=cn=annuity,ou=Boston,
dc=fleet,dc=com&domain=Test&filter=cn=*" 30 1 10 120 0 0 0x100
"LDAP-TEST" "" ""
```

详细信息

测试的关键字 (p. 126)

svcwatch add mapi 命令-添加 MAPI 测试

svcwatch add mapi 命令用于向指定主机上的 SRM 添加 MAPI 测试。

此命令具有以下格式：

```
svcwatch [options] -o add index descr mapi destination
username password args interval samples timeout winsiz tos
limit flags name class contextInfo logLevel
```

该 add 命令使用以下参数：

选项

指定该命令的可能选项。

-h *hostname* | **-h *ipAddr***

（可选）指定 SystemEDGE 主机。

默认值：localhost

-p *port*

（可选）指定 SystemEDGE SNMP 端口。

默认：161

-c *community*

（可选）指定 SNMP 版本 1 和 2c 的 SNMP 团体字符串。

默认值：public

-v *snmpVersion*

（可选）指定 SNMP 版本。可能的值为：

- 1
- 2c
- 3

默认：1

-u *secName*

（可选）指定 SNMPv3 安全用户的名称。

-u *secLevel*

（可选）指定 SNMPv3 的安全级别。可能的值为：

- 1－noAuthNoPriv
- 2－AuthNoPriv
- 3－AuthPriv

-n *contextName*

（可选）指定 MIBMuxed 代理的实例名称。

-a *authPassword*

（可选）标识针对 AuthNoPriv 或 AuthPriv 安全级别选择 SNMPv3 时所需的身份验证密码。

-A *authProtocol*

（可选）指定身份验证协议。可能的值为：

- MD5－身份验证协议 HMAC-MD5
- SHA－身份验证协议 HMAC-SHA

默认：MD5

-x *privPassword*

（可选）指定针对安全级别 3 (AuthPriv) 选择 SNMPv3 时所需的隐私（加密）密码。

-X *encryptProtocol*

（可选）指定针对隐私使用加密协议。可能的值为：

- DES-数据加密标准
- AES-使用 128 位加密密钥的高级加密标准 (AES128)
- 3DES－三重数据加密标准

-m *FIPSmode*

（可选）指定 FIPS 模式。可能的值为：

- 0－非 FIPS
- 1－FIPS 共存
- 2－仅 FIPS

默认：0

-t *timeout*

（可选）指定 SNMP 命令超时。

默认值：10 秒

-d *logLevel*

（可选）指定 SNMP 消息的日志级别。可能的值为：

- 0－记录致命消息
- 1－记录严重消息
- 2－记录警告消息
- 3－记录信息消息
- 4－记录所有消息
- 5－记录所有消息，包括调试消息

默认：0

-f *logFile*

（可选）指定日志文件的名称。

默认值：sysedge_utility.log

-L

（可选）检测控制台和语言目录的当前区域设置（如果可用）。如果未找到语言目录，实用工具将重新使用英语作为默认语言。

-o add *testparams*

向 SRM 添加新测试。

testparams

指定新测试的参数。

index

指定 svcRspTable 索引。

descr

在引号中指定测试说明。如果引号 "" 中为空字符串，则表示未指定说明。

mapi

指定 MAPI 服务类型。

destination

指定用于测试的 MAPI 服务器。

用户名

在引号中指定用于进行身份验证的用户名。如果引号 "" 中为空字符串，则表示未指定用户名。

password

在引号中指定用于进行身份验证的密码。如果引号 "" 中为空字符串，则表示未指定密码。

args

指定服务参数。每个参数都是一对关键字和值 (key=value)。通过与号 (&) 连接和分隔多个参数。完整参数字符串用引号括起来。

参数的常规语法："key1=value1[&key2=value2& ...]"

domain=*domain*-用户帐户所属的 Windows 域。

op=send-发送测试消息。

op=recv-接收测试消息。

download=Download First Message-仅下载该用户帐户的第一条消息。

download=Download All Messages-下载该用户帐户的所有消息。

to=*recipient*-指定测试消息的电子邮件收件人。

size=*number of bytes*-指定测试消息的大小（字节）。默认值：256

delete=true-删除下载的消息。

delete=false-不删除下载的消息。

注意：有关每种服务类型的特定参数的详细信息，请参阅测试关键字 (p. 126)。

interval

指定测试间隔（秒）。

限制：30 秒的倍数

示例

指定每个间隔的抽样数。

超时

指定超时（秒）。

winsiz

指定统计时段大小（秒）。

tos

指定“服务类型”或“差分服务代码”IP。对于普通服务，使用 0（零）。另请参阅 RFC 1349。

limit

指定该测试总响应时间的可接受性能限制（或阈值）。在报告中使用该值。

flags

指定以下标志：

0x001 = 收集性能多维数据集

0x100 = 仅请求时执行（运行一次）

name

指定每种服务类型的唯一名称。引号 "" 中的空字符串不指定测试名称。

类

指定类名称。引号 "" 中的空字符串不指定类名称。

contextInfo

指定上下文信息。引号 "" 中的空字符串不指定上下文信息。

logLevel

指定测试执行码的日志级别。可能的值为：

-2 = 使用 SRM 全局日志级别（默认）

-1 = 不记录

0 = 致命（仅最重要的消息）

1 = 严重

...

7 = debug3（记录所有消息）

示例

添加 MAPI 测试：

```
svcwatch -h localhost -p 161 -c topsecret -o add 1360749"MAPI-TEST"
mapi "mapiserver.yourdomain.com" "MAPIuser" "MAPI123" "domain=myDomain
&op=send&to=congo@yourdomain.com&size=256" 120 1 10 3600 0 0 0x100
"MAPI-TEST" "" ""
```

详细信息

测试的关键字 (p. 126)

svcwatch add nis 命令-添加 NIS 测试

svcwatch add nis 命令用于向指定主机上的 SRM 添加 NIS 测试。

此命令具有以下格式：

```
svcwatch [options] -o add index descr nis destination
username password args interval samples timeout winsiz tos
limit flags name class contextInfo logLevel
```

该 add 命令使用以下参数：

选项

指定该命令的可能选项。

-h *hostname* | **-h *ipAddr***

（可选）指定 SystemEDGE 主机。

默认值：localhost

-p *port*

（可选）指定 SystemEDGE SNMP 端口。

默认：161

-c *community*

（可选）指定 SNMP 版本 1 和 2c 的 SNMP 团体字符串。

默认值：public

-v *snmpVersion*

（可选）指定 SNMP 版本。可能的值为：

- 1
- 2c
- 3

默认：1

-u *secName*

（可选）指定 SNMPv3 安全用户的名称。

-u *secLevel*

（可选）指定 SNMPv3 的安全级别。可能的值为：

- 1－noAuthNoPriv
- 2－AuthNoPriv
- 3－AuthPriv

-n *contextName*

（可选）指定 MIBMuxed 代理的实例名称。

-a *authPassword*

（可选）标识针对 AuthNoPriv 或 AuthPriv 安全级别选择 SNMPv3 时所需的身份验证密码。

-A *authProtocol*

（可选）指定身份验证协议。可能的值为：

- MD5－身份验证协议 HMAC-MD5
- SHA－身份验证协议 HMAC-SHA

默认：MD5

-x *privPassword*

（可选）指定针对安全级别 3 (AuthPriv) 选择 SNMPv3 时所需的隐私（加密）密码。

-X *encryptProtocol*

（可选）指定针对隐私使用加密协议。可能的值为：

- DES-数据加密标准
- AES-使用 128 位加密密钥的高级加密标准 (AES128)
- 3DES－三重数据加密标准

-m *FIPSmode*

（可选）指定 FIPS 模式。可能的值为：

- 0－非 FIPS
- 1－FIPS 共存
- 2－仅 FIPS

默认：0

-t *timeout*

（可选）指定 SNMP 命令超时。

默认值：10 秒

-d *logLevel*

（可选）指定 SNMP 消息的日志级别。可能的值为：

- 0－记录致命消息
- 1－记录严重消息
- 2－记录警告消息
- 3－记录信息消息
- 4－记录所有消息
- 5－记录所有消息，包括调试消息

默认：0

-f *logFile*

（可选）指定日志文件的名称。

默认值：sysedge_utility.log

-L

（可选）检测控制台和语言目录的当前区域设置（如果可用）。如果未找到语言目录，实用工具将重新使用英语作为默认语言。

-o add *testparams*

向 SRM 添加新测试。

testparams

指定新测试的参数。

index

指定 svcRspTable 索引。

descr

在引号中指定测试说明。如果引号 "" 中为空字符串，则表示未指定说明。

nis

指定 NIS 服务类型。

destination

指定用于测试的 NIS 服务器。

用户名

在引号中指定用于进行身份验证的用户名。如果引号 "" 中为空字符串，则表示未指定用户名。

password

在引号中指定用于进行身份验证的密码。如果引号 "" 中为空字符串，则表示未指定密码。

args

指定服务参数。每个参数都是一对关键字和值 (key=value)。通过与号 (&) 连接和分隔多个参数。完整参数字符串用引号括起来。

参数的常规语法："key1=value1[&key2=value2& ...]"

domain=domain-指定映射文件所在的域。

map=map-指定要测试的映射文件。默认值：主机

download=true|false-指定是否下载 NIS 映射。

注意：有关每种服务类型的特定参数的详细信息，请参阅测试关键字 (p. 126)。

interval

指定测试间隔（秒）。

限制：30 秒的倍数

示例

指定每个间隔的抽样数。

超时

指定超时（秒）。

winsiz

指定统计时段大小（秒）。

tos

指定“服务类型”或“差分服务代码”IP。对于普通服务，使用 0（零）。另请参阅 RFC 1349。

limit

指定该测试总响应时间的可接受性能限制（或阈值）。在报告中使用该值。

flags

指定以下标志：

0x001 = 收集性能多维数据集

0x100 = 仅请求时执行（运行一次）

name

指定每种服务类型的唯一名称。引号 "" 中的空字符串不指定测试名称。

类

指定类名称。引号 "" 中的空字符串不指定类名称。

contextInfo

指定上下文信息。引号 "" 中的空字符串不指定上下文信息。

logLevel

指定测试执行码的日志级别。可能的值为：

-2 = 使用 SRM 全局日志级别（默认）

-1 = 不记录

0 = 致命（仅最重要的消息）

1 = 严重

...

7 = debug3（记录所有消息）

示例

添加 NIS 测试：

```
svcwatch -h localhost -p 161 -c topsecret -o add 1360750 "NIS-TEST"
nis "nisserver.yourdomain" "" "" "domain=Test.com&map=hosts&download=true"
300 1 20 7200 0 0 0x100 "NIS-TEST" "" ""
```

详细信息

测试的关键字 (p. 126)

svcwatch add nntp 命令-添加 NNTP 测试

svcwatch add nntp 命令用于向指定主机上的 SRM 添加 NNTP 测试。

此命令具有以下格式：

```
svcwatch [options] -o add index descr nntp destination
username password args interval samples timeout winsiz tos
limit flags name class contextInfo logLevel
```

该 add 命令使用以下参数：

选项

指定该命令的可能选项。

-h *hostname* | **-h *ipAddr***

（可选）指定 SystemEDGE 主机。

默认值：localhost

-p *port*

（可选）指定 SystemEDGE SNMP 端口。

默认：161

-c *community*

（可选）指定 SNMP 版本 1 和 2c 的 SNMP 团体字符串。

默认值：public

-v *snmpVersion*

（可选）指定 SNMP 版本。可能的值为：

- 1
- 2c
- 3

默认：1

-u *secName*

（可选）指定 SNMPv3 安全用户的名称。

-u *secLevel*

（可选）指定 SNMPv3 的安全级别。可能的值为：

- 1－noAuthNoPriv
- 2－AuthNoPriv
- 3－AuthPriv

-n *contextName*

（可选）指定 MIBMuxed 代理的实例名称。

-a *authPassword*

（可选）标识针对 AuthNoPriv 或 AuthPriv 安全级别选择 SNMPv3 时所需的身份验证密码。

-A *authProtocol*

（可选）指定身份验证协议。可能的值为：

- MD5－身份验证协议 HMAC-MD5
- SHA－身份验证协议 HMAC-SHA

默认：MD5

-x *privPassword*

（可选）指定针对安全级别 3 (AuthPriv) 选择 SNMPv3 时所需的隐私（加密）密码。

-X *encryptProtocol*

（可选）指定针对隐私使用加密协议。可能的值为：

- DES-数据加密标准
- AES-使用 128 位加密密钥的高级加密标准 (AES128)
- 3DES－三重数据加密标准

-m *FIPSmode*

（可选）指定 FIPS 模式。可能的值为：

- 0－非 FIPS
- 1－FIPS 共存
- 2－仅 FIPS

默认：0

-t *timeout*

（可选）指定 SNMP 命令超时。

默认值：10 秒

-d *logLevel*

（可选）指定 SNMP 消息的日志级别。可能的值为：

- 0－记录致命消息
- 1－记录严重消息
- 2－记录警告消息
- 3－记录信息消息
- 4－记录所有消息
- 5－记录所有消息，包括调试消息

默认：0

-f *logFile*

（可选）指定日志文件的名称。

默认值：sysedge_utility.log

-L

（可选）检测控制台和语言目录的当前区域设置（如果可用）。如果未找到语言目录，实用工具将重新使用英语作为默认语言。

-o add *testparams*

向 SRM 添加新测试。

testparams

指定新测试的参数。

index

指定 svcRspTable 索引。

descr

在引号中指定测试说明。如果引号 "" 中为空字符串，则表示未指定说明。

nntp

指定 NNTP 服务类型。

destination

指定用于测试的 NNTP 服务器和端口 (*server*:*port*)。默认端口：119

用户名

在引号中指定用于进行身份验证的用户名。如果引号 "" 中为空字符串，则表示未指定用户名。

password

在引号中指定用于进行身份验证的密码。如果引号 "" 中为空字符串，则表示未指定密码。

args

没有 NNTP 服务类型可用的参数。如果引号 "" 中为空字符串，则表示未指定参数。

注意：有关每种服务类型的特定参数的详细信息，请参阅测试参数关键字 (p. 126)。

interval

指定测试间隔（秒）。

限制：30 秒的倍数

示例

指定每个间隔的抽样数。

超时

指定超时（秒）。

winsiz

指定统计时段大小（秒）。

tos

指定“服务类型”或“差分服务代码”IP。对于普通服务，使用 0（零）。另请参阅 RFC 1349。

limit

指定该测试总响应时间的可接受性能限制（或阈值）。在报告中使用该值。

flags

指定以下标志：

0x001 = 收集性能多维数据集

0x100 = 仅请求时执行（运行一次）

name

指定每种服务类型的唯一名称。引号 "" 中的空字符串不指定测试名称。

类

指定类名称。引号 "" 中的空字符串不指定类名称。

contextInfo

指定上下文信息。引号 "" 中的空字符串不指定上下文信息。

logLevel

指定测试执行码的日志级别。可能的值为：

-2 = 使用 SRM 全局日志级别（默认）

-1 = 不记录

0 = 致命（仅最重要的消息）

1 = 严重

...

7 = debug3（记录所有消息）

示例

添加 NNTP 测试：

```
svcwatch -h localhost -p 161 -c topsecret -o add 1360751 "NNTP-TEST" nntp
"nntpservername:119" "" "" "" 30 3 30 60 0 0 0x100 "TestNNTP" "ClassName"
"ContextName" 7
```

详细信息

测试的关键字 (p. 126)

svcwatch add ping 命令-添加 PING 测试

svcwatch add ping 命令用于向指定主机上的 SRM 添加 PING 测试。

此命令具有以下格式：

```
svcwatch [options] -o add index descr ping destination
username password args interval samples timeout winsiz tos
limit flags name class contextInfo logLevel
```

该 add 命令使用以下参数：

选项

指定该命令的可能选项。

-h *hostname* | **-h *ipAddr***

（可选）指定 SystemEDGE 主机。

默认值：localhost

-p *port*

（可选）指定 SystemEDGE SNMP 端口。

默认：161

-c *community*

（可选）指定 SNMP 版本 1 和 2c 的 SNMP 团体字符串。

默认值：public

-v *snmpVersion*

（可选）指定 SNMP 版本。可能的值为：

- 1
- 2c
- 3

默认：1

-u *secName*

（可选）指定 SNMPv3 安全用户的名称。

-u *secLevel*

（可选）指定 SNMPv3 的安全级别。可能的值为：

- 1－noAuthNoPriv
- 2－AuthNoPriv
- 3－AuthPriv

-n *contextName*

（可选）指定 MIBMuxed 代理的实例名称。

-a *authPassword*

（可选）标识针对 AuthNoPriv 或 AuthPriv 安全级别选择 SNMPv3 时所需的身份验证密码。

-A *authProtocol*

（可选）指定身份验证协议。可能的值为：

- MD5－身份验证协议 HMAC-MD5
- SHA－身份验证协议 HMAC-SHA

默认：MD5

-x *privPassword*

（可选）指定针对安全级别 3 (AuthPriv) 选择 SNMPv3 时所需的隐私（加密）密码。

-X *encryptProtocol*

（可选）指定针对隐私使用加密协议。可能的值为：

- DES-数据加密标准
- AES-使用 128 位加密密钥的高级加密标准 (AES128)
- 3DES－三重数据加密标准

-m *FIPSmode*

（可选）指定 FIPS 模式。可能的值为：

- 0－非 FIPS
- 1－FIPS 共存
- 2－仅 FIPS

默认：0

-t *timeout*

（可选）指定 SNMP 命令超时。

默认值：10 秒

-d *logLevel*

（可选）指定 SNMP 消息的日志级别。可能的值为：

- 0－记录致命消息
- 1－记录严重消息
- 2－记录警告消息
- 3－记录信息消息
- 4－记录所有消息
- 5－记录所有消息，包括调试消息

默认：0

-f *logFile*

（可选）指定日志文件的名称。

默认值：sysedge_utility.log

-L

（可选）检测控制台和语言目录的当前区域设置（如果可用）。如果未找到语言目录，实用工具将重新使用英语作为默认语言。

-o add *testparams*

向 SRM 添加新测试。

testparams

指定新测试的参数。

index

指定 svcRspTable 索引。

descr

在引号中指定测试说明。如果引号 "" 中为空字符串，则表示未指定说明。

ping

指定 PING 服务类型。

destination

指定用于测试的目标计算机。

用户名

在引号中指定用于进行身份验证的用户名。如果引号 "" 中为空字符串，则表示未指定用户名。

password

在引号中指定用于进行身份验证的密码。如果引号 "" 中为空字符串，则表示未指定密码。

args

指定服务参数。参数指用引号括起来的一对参数和值 (payload=*number of bytes*)。

payload=*number of bytes*-在 ping 中发送的数据包大小。默认数据包大小是 64 字节。

注意：有关每种服务类型的特定参数的详细信息，请参阅测试关键字 (p. 126)。

interval

指定测试间隔（秒）。

限制：30 秒的倍数

示例

指定每个间隔的抽样数。

超时

指定超时（秒）。

winsiz

指定统计时段大小（秒）。

tos

指定“服务类型”或“差分服务代码”IP。对于普通服务，使用 0（零）。另请参阅 RFC 1349。

limit

指定该测试总响应时间的可接受性能限制（或阈值）。在报告中使用该值。

flags

指定以下标志：

0x001 = 收集性能多维数据集

0x100 = 仅请求时执行（运行一次）

name

指定每种服务类型的唯一名称。引号 "" 中的空字符串不指定测试名称。

类

指定类名称。引号 "" 中的空字符串不指定类名称。

contextInfo

指定上下文信息。引号 "" 中的空字符串不指定上下文信息。

logLevel

指定测试执行码的日志级别。可能的值为：

-2 = 使用 SRM 全局日志级别（默认）

-1 = 不记录

0 = 致命（仅最重要的消息）

1 = 严重

...

7 = debug3（记录所有消息）

示例

添加 ping 测试：

```
svcwatch -h localhost -p 161 -c admin -o add 1360752 "TEST" ping "127.0.0.1"
"" "" "payload=1000" 30 3 30 60 0 0 0x100 "TestPING" "ClassName" "ContextName"
7
```

详细信息

测试的关键字 (p. 126)

svcwatch add pop3 命令-添加 POP3 测试

svcwatch add pop3 命令用于向指定主机上的 SRM 添加 POP3 测试。

此命令具有以下格式：

```
svcwatch [options] -o add index descr pop3 destination
username password args interval samples timeout winsiz tos
limit flags name class contextInfo logLevel
```

该 add 命令使用以下参数：

选项

指定该命令的可能选项。

-h *hostname* | **-h *ipAddr***

（可选）指定 SystemEDGE 主机。

默认值：localhost

-p *port*

（可选）指定 SystemEDGE SNMP 端口。

默认：161

-c *community*

（可选）指定 SNMP 版本 1 和 2c 的 SNMP 团体字符串。

默认值：public

-v *snmpVersion*

（可选）指定 SNMP 版本。可能的值为：

- 1
- 2c
- 3

默认：1

-u *secName*

（可选）指定 SNMPv3 安全用户的名称。

-u *secLevel*

（可选）指定 SNMPv3 的安全级别。可能的值为：

- 1－noAuthNoPriv
- 2－AuthNoPriv
- 3－AuthPriv

-n *contextName*

（可选）指定 MIBMuxed 代理的实例名称。

-a *authPassword*

（可选）标识针对 AuthNoPriv 或 AuthPriv 安全级别选择 SNMPv3 时所需的身份验证密码。

-A *authProtocol*

（可选）指定身份验证协议。可能的值为：

- MD5－身份验证协议 HMAC-MD5
- SHA－身份验证协议 HMAC-SHA

默认：MD5

-x *privPassword*

（可选）指定针对安全级别 3 (AuthPriv) 选择 SNMPv3 时所需的隐私（加密）密码。

-X *encryptProtocol*

（可选）指定针对隐私使用加密协议。可能的值为：

- DES-数据加密标准
- AES-使用 128 位加密密钥的高级加密标准 (AES128)
- 3DES－三重数据加密标准

-m *FIPSmode*

（可选）指定 FIPS 模式。可能的值为：

- 0－非 FIPS
- 1－FIPS 共存
- 2－仅 FIPS

默认：0

-t *timeout*

（可选）指定 SNMP 命令超时。

默认值：10 秒

-d *logLevel*

（可选）指定 SNMP 消息的日志级别。可能的值为：

- 0－记录致命消息
- 1－记录严重消息
- 2－记录警告消息
- 3－记录信息消息
- 4－记录所有消息
- 5－记录所有消息，包括调试消息

默认：0

-f *logFile*

（可选）指定日志文件的名称。

默认值：sysedge_utility.log

-L

（可选）检测控制台和语言目录的当前区域设置（如果可用）。如果未找到语言目录，实用工具将重新使用英语作为默认语言。

-o add *testparams*

向 SRM 添加新测试。

testparams

指定新测试的参数。

index

指定 svcRspTable 索引。

descr

在引号中指定测试说明。如果引号 "" 中为空字符串，则表示未指定说明。

pop3

指定 POP3 服务类型。

destination

指定用于测试的 POP3 服务器和端口 (*server*:*port*)。默认端口：110

用户名

在引号中指定用于进行身份验证的用户名。如果引号 "" 中为空字符串，则表示未指定用户名。

password

在引号中指定用于进行身份验证的密码。如果引号 "" 中为空字符串，则表示未指定密码。

args

指定服务参数。每个参数都是一对关键字和值 (key=value)。通过与号 (&) 连接和分隔多个参数。完整参数字符串用引号括起来。

参数的常规语法："key1=value1[&key2=value2& ...]"

download=Download First Message-仅下载该用户帐户的第一条消息。

download=Download All Messages-下载该用户帐户的所有消息。

delete=true-删除下载的消息。

delete=false-不删除下载的消息。

注意：有关每种服务类型的特定参数的详细信息，请参阅测试关键字 (p. 126)。

interval

指定测试间隔（秒）。

限制：30 秒的倍数

示例

指定每个间隔的抽样数。

超时

指定超时（秒）。

winsiz

指定统计时段大小（秒）。

tos

指定“服务类型”或“差分服务代码”IP。对于普通服务，使用 0（零）。另请参阅 RFC 1349。

limit

指定该测试总响应时间的可接受性能限制（或阈值）。在报告中使用该值。

flags

指定以下标志：

0x001 = 收集性能多维数据集

0x100 = 仅请求时执行（运行一次）

name

指定每种服务类型的唯一名称。引号 "" 中的空字符串不指定测试名称。

类

指定类名称。引号 "" 中的空字符串不指定类名称。

contextInfo

指定上下文信息。引号 "" 中的空字符串不指定上下文信息。

logLevel

指定测试执行码的日志级别。可能的值为：

-2 = 使用 SRM 全局日志级别（默认）

-1 = 不记录

0 = 致命（仅最重要的消息）

1 = 严重

...

7 = debug3（记录所有消息）

示例

添加 POP3 测试：

```
svcwatch -h localhost -p 161 -c doublesecret -o add 1360753 "POP3-TEST"
pop3 "mypop3server:110" "pop3user" "pop3pass" "download=Download First Message
&delete=true" 30 3 30 60 0 0 0x100 "TestPOP3" "ClassName" "ContextName" 7
```

详细信息

测试的关键字 (p. 126)

svcwatch add rtemail 命令-添加往返电子邮件测试

svcwatch add rtemail 命令用于向指定主机上的 SRM 添加往返电子邮件测试。

此命令具有以下格式：

```
svcwatch [options] -o add index descr rtemail destination
username password args interval samples timeout winsiz tos
limit flags name class contextInfo logLevel
```

该 add 命令使用以下参数：

选项

指定该命令的可能选项。

-h *hostname*｜ -h *ipAddr*

（可选）指定 SystemEDGE 主机。

默认值：localhost

-p *port*

（可选）指定 SystemEDGE SNMP 端口。

默认：161

-c *community*

（可选）指定 SNMP 版本 1 和 2c 的 SNMP 团体字符串。

默认值：public

-v *snmpVersion*

（可选）指定 SNMP 版本。可能的值为：

- 1
- 2c
- 3

默认：1

-u *secName*

（可选）指定 SNMPv3 安全用户的名称。

-u *secLevel*

（可选）指定 SNMPv3 的安全级别。可能的值为：

- 1－noAuthNoPriv
- 2－AuthNoPriv
- 3－AuthPriv

-n *contextName*

（可选）指定 MIBMuxed 代理的实例名称。

-a *authPassword*

（可选）标识针对 AuthNoPriv 或 AuthPriv 安全级别选择 SNMPv3 时所需的身份验证密码。

-A *authProtocol*

（可选）指定身份验证协议。可能的值为：

- MD5－身份验证协议 HMAC-MD5
- SHA－身份验证协议 HMAC-SHA

默认：MD5

-x *privPassword*

（可选）指定针对安全级别 3 (AuthPriv) 选择 SNMPv3 时所需的隐私（加密）密码。

-X *encryptProtocol*

（可选）指定针对隐私使用加密协议。可能的值为：

- DES-数据加密标准
- AES-使用 128 位加密密钥的高级加密标准 (AES128)
- 3DES－三重数据加密标准

-m *FIPSmode*

（可选）指定 FIPS 模式。可能的值为：

- 0－非 FIPS
- 1－FIPS 共存
- 2－仅 FIPS

默认：0

-t *timeout*

（可选）指定 SNMP 命令超时。

默认值：10 秒

-d *logLevel*

（可选）指定 SNMP 消息的日志级别。可能的值为：

- 0－记录致命消息
- 1－记录严重消息
- 2－记录警告消息
- 3－记录信息消息
- 4－记录所有消息
- 5－记录所有消息，包括调试消息

默认：0

-f *logFile*

（可选）指定日志文件的名称。

默认值：sysedge_utility.log

-L

（可选）检测控制台和语言目录的当前区域设置（如果可用）。如果未找到语言目录，实用工具将重新使用英语作为默认语言。

-o add *testparams*

向 SRM 添加新测试。

testparams

指定新测试的参数。

index

指定 svcRspTable 索引。

descr

在引号中指定测试说明。如果引号 "" 中为空字符串，则表示未指定说明。

rtemail

指定往返电子邮件服务类型。

destination

指定用于测试的 SMTP 或 MAPI 服务器 (*smtpserver*:*port*)。默认 SMTP 端口：25

用户名

在引号中指定用于进行身份验证的用户名。如果引号 "" 中为空字符串，则表示未指定用户名。

password

在引号中指定用于进行身份验证的密码。如果引号 "" 中为空字符串，则表示未指定密码。

args

指定服务参数。每个参数都是一对关键字和值 (key=value)。通过与号 (&) 连接和分隔多个参数。完整参数字符串用引号括起来。

参数的常规语法："key1=value1[&key2=value2& ...]"

send_proto=smtp|mapi-指定发送协议。

to=*recipient*-指定电子邮件收件人的姓名。

size=*number of bytes*-指定测试消息的大小（字节）。默认值：256

shost=*senderhost*-指定发送消息的主机名。

smtp_ssl=true|false-指定是否启用 SMTP SSL 加密。

send_user=*suser*-指定发件人帐户的名称。

send_pass=*spass*-指定发件人的密码。

sdomain=*domain*-（仅限 MAPI）指定发件人所属的域。

get_proto=pop3|imap|mapi-指定接收协议。

source=*targethost*-指定向其发送电子邮件的主机。

source_port=*port*-IMAP 或 POP3 的端口号。默认值：110 (POP3)、143 (IMAP)

gdomain=*domain*-（仅限 MAPI）指定收件人所属的域。

check=*poll interval*-指定轮询时间间隔（秒）。默认：600

注意：有关每种服务类型的特定参数的详细信息，请参阅测试关键字 (p. 126)。

interval

指定测试间隔（秒）。

限制：30 秒的倍数

示例

指定每个间隔的抽样数。

超时

指定超时（秒）。

winsiz

指定统计时段大小（秒）。

tos

指定“服务类型”或“差分服务代码”IP。对于普通服务，使用 0（零）。另请参阅 RFC 1349。

limit

指定该测试总响应时间的可接受性能限制（或阈值）。在报告中使用该值。

flags

指定以下标志：

0x001 = 收集性能多维数据集

0x100 = 仅请求时执行（运行一次）

name

指定每种服务类型的唯一名称。引号 "" 中的空字符串不指定测试名称。

类

指定类名称。引号 "" 中的空字符串不指定类名称。

contextInfo

指定上下文信息。引号 "" 中的空字符串不指定上下文信息。

logLevel

指定测试执行码的日志级别。可能的值为：

-2 = 使用 SRM 全局日志级别（默认）

-1 = 不记录

0 = 致命（仅最重要的消息）

1 = 严重

...

7 = debug3（记录所有消息）

示例

添加往返电子邮件测试：

```
svcwatch -p 161 -c admin -o add 1360754 "RT-EMAIL TEST" rtemail
"mysmtp.com:25" "smtpuser" "zrvr8tx" "send_proto=smtp&to=recipient
&size=256&shost=senderhost&smtp_ssl=true&send_user=sender&send_pass=secret
&get_proto=pop3&source=popserver&source_port=110&check=600"
30 3 30 60 0 0 0x100 "TestRTEMAIL" "ClassName" "ContextName" 7
```

详细信息

测试的关键字 (p. 126)

svcwatch add smtp 命令-添加 SMTP 测试

svcwatch add smtp 命令用于向指定主机上的 SRM 添加 SMTP 测试。

此命令具有以下格式：

```
svcwatch [options] -o add index descr smtp destination
username password args interval samples timeout winsiz tos
limit flags name class contextInfo logLevel
```

该 add 命令使用以下参数：

选项

指定该命令的可能选项。

-h *hostname* | **-h *ipAddr***

（可选）指定 SystemEDGE 主机。

默认值：localhost

-p *port*

（可选）指定 SystemEDGE SNMP 端口。

默认：161

-c *community*

（可选）指定 SNMP 版本 1 和 2c 的 SNMP 团体字符串。

默认值：public

-v *snmpVersion*

（可选）指定 SNMP 版本。可能的值为：

- 1
- 2c
- 3

默认：1

-u *secName*

（可选）指定 SNMPv3 安全用户的名称。

-u *secLevel*

（可选）指定 SNMPv3 的安全级别。可能的值为：

- 1－noAuthNoPriv
- 2－AuthNoPriv
- 3－AuthPriv

-n *contextName*

（可选）指定 MIBMuxed 代理的实例名称。

-a *authPassword*

（可选）标识针对 AuthNoPriv 或 AuthPriv 安全级别选择 SNMPv3 时所需的身份验证密码。

-A *authProtocol*

（可选）指定身份验证协议。可能的值为：

- MD5－身份验证协议 HMAC-MD5
- SHA－身份验证协议 HMAC-SHA

默认：MD5

-x *privPassword*

（可选）指定针对安全级别 3 (AuthPriv) 选择 SNMPv3 时所需的隐私（加密）密码。

-X *encryptProtocol*

（可选）指定针对隐私使用加密协议。可能的值为：

- DES-数据加密标准
- AES-使用 128 位加密密钥的高级加密标准 (AES128)
- 3DES－三重数据加密标准

-m *FIPSmode*

（可选）指定 FIPS 模式。可能的值为：

- 0－非 FIPS
- 1－FIPS 共存
- 2－仅 FIPS

默认：0

-t *timeout*

（可选）指定 SNMP 命令超时。

默认值：10 秒

-d *logLevel*

（可选）指定 SNMP 消息的日志级别。可能的值为：

- 0－记录致命消息
- 1－记录严重消息
- 2－记录警告消息
- 3－记录信息消息
- 4－记录所有消息
- 5－记录所有消息，包括调试消息

默认：0

-f *logFile*

（可选）指定日志文件的名称。

默认值：sysedge_utility.log

-L

（可选）检测控制台和语言目录的当前区域设置（如果可用）。如果未找到语言目录，实用工具将重新使用英语作为默认语言。

-o add *testparams*

向 SRM 添加新测试。

testparams

指定新测试的参数。

index

指定 svcRspTable 索引。

descr

在引号中指定测试说明。如果引号 "" 中为空字符串，则表示未指定说明。

smtp

指定 SMTP 服务类型。

destination

指定用于测试的 SMTP 服务器和端口 (*server*:*port*)。默认端口：25

用户名

在引号中指定用于进行身份验证的用户名。如果引号 "" 中为空字符串，则表示未指定用户名。

password

在引号中指定用于进行身份验证的密码。如果引号 "" 中为空字符串，则表示未指定密码。

args

指定服务参数。每个参数都是一对关键字和值 (key=value)。通过与号 (&) 连接和分隔多个参数。完整参数字符串用引号括起来。

参数的常规语法："key1=value1[&key2=value2& ...]"

to=*recipient*-指定电子邮件收件人的姓名。

size=*number of bytes*-指定测试消息的大小（字节）。默认值：256

shost=*senderhost*-指定发送消息的主机名。

ssl=true|false-指定是否启用 SMTP SSL 加密。

注意：有关每种服务类型的特定参数的详细信息，请参阅测试关键字 (p. 126)。

interval

指定测试间隔（秒）。

限制：30 秒的倍数

示例

指定每个间隔的抽样数。

超时

指定超时（秒）。

winsiz

指定统计时段大小（秒）。

tos

指定“服务类型”或“差分服务代码”IP。对于普通服务，使用 0（零）。另请参阅 RFC 1349。

limit

指定该测试总响应时间的可接受性能限制（或阈值）。在报告中使用该值。

flags

指定以下标志：

0x001 = 收集性能多维数据集

0x100 = 仅请求时执行（运行一次）

name

指定每种服务类型的唯一名称。引号 "" 中的空字符串不指定测试名称。

类

指定类名称。引号 "" 中的空字符串不指定类名称。

contextInfo

指定上下文信息。引号 "" 中的空字符串不指定上下文信息。

logLevel

指定测试执行码的日志级别。可能的值为：

-2 = 使用 SRM 全局日志级别（默认）

-1 = 不记录

0 = 致命（仅最重要的消息）

1 = 严重

...

7 = debug3（记录所有消息）

示例

添加 SMTP 测试：

```
svcwatch -p 161 -c admin -o add 1360755 "SMTP TEST" smtp "mysmtp.com:25"
"smtpuser" "zrvr9tx" "to=recipient&size=256&shost=senderhost&smtp_ssl=true"
30 3 30 60 0 0 0x100 "TestSMTP" "ClassName" "ContextName" 7
```

详细信息

测试的关键字 (p. 126)

svcwatch add snmp 命令-添加 SNMP 测试

svcwatch add snmp 命令用于向指定主机上的 SRM 添加 SNMP 测试。

此命令具有以下格式：

```
svcwatch [options] -o add index descr snmp destination
username password args interval samples timeout winsiz tos
limit flags name class contextInfo logLevel
```

该 add 命令使用以下参数：

选项

指定该命令的可能选项。

-h *hostname* | **-h *ipAddr***

（可选）指定 SystemEDGE 主机。

默认值：localhost

-p *port*

（可选）指定 SystemEDGE SNMP 端口。

默认：161

-c *community*

（可选）指定 SNMP 版本 1 和 2c 的 SNMP 团体字符串。

默认值：public

-v *snmpVersion*

（可选）指定 SNMP 版本。可能的值为：

- 1
- 2c
- 3

默认：1

-u *secName*

（可选）指定 SNMPv3 安全用户的名称。

-u *secLevel*

（可选）指定 SNMPv3 的安全级别。可能的值为：

- 1－noAuthNoPriv
- 2－AuthNoPriv
- 3－AuthPriv

-n *contextName*

（可选）指定 MIBMuxed 代理的实例名称。

-a *authPassword*

（可选）标识针对 AuthNoPriv 或 AuthPriv 安全级别选择 SNMPv3 时所需的身份验证密码。

-A *authProtocol*

（可选）指定身份验证协议。可能的值为：

- MD5－身份验证协议 HMAC-MD5
- SHA－身份验证协议 HMAC-SHA

默认：MD5

-x *privPassword*

（可选）指定针对安全级别 3 (AuthPriv) 选择 SNMPv3 时所需的隐私（加密）密码。

-X *encryptProtocol*

（可选）指定针对隐私使用加密协议。可能的值为：

- DES-数据加密标准
- AES-使用 128 位加密密钥的高级加密标准 (AES128)
- 3DES－三重数据加密标准

-m *FIPSmode*

（可选）指定 FIPS 模式。可能的值为：

- 0－非 FIPS
- 1－FIPS 共存
- 2－仅 FIPS

默认：0

-t *timeout*

（可选）指定 SNMP 命令超时。

默认值：10 秒

-d *logLevel*

（可选）指定 SNMP 消息的日志级别。可能的值为：

- 0－记录致命消息
- 1－记录严重消息
- 2－记录警告消息
- 3－记录信息消息
- 4－记录所有消息
- 5－记录所有消息，包括调试消息

默认：0

-f *logFile*

（可选）指定日志文件的名称。

默认值：sysedge_utility.log

-L

（可选）检测控制台和语言目录的当前区域设置（如果可用）。如果未找到语言目录，实用工具将重新使用英语作为默认语言。

-o add *testparams*

向 SRM 添加新测试。

testparams

指定新测试的参数。

index

指定 svcRspTable 索引。

descr

在引号中指定测试说明。如果引号 "" 中为空字符串，则表示未指定说明。

snmp

指定 SNMP 服务类型。

destination

指定用于测试的 SNMP 代理主机和端口 (*server*:*port*)。默认 SNMP 端口：161

用户名

在引号中指定用于进行身份验证的用户名。如果引号 "" 中为空字符串，则表示未指定用户名。

password

在引号中指定用于进行身份验证的密码。如果引号 "" 中为空字符串，则表示未指定密码。

args

指定服务参数。每个参数都是一对关键字和值 (key=value)。通过与号 (&) 连接和分隔多个参数。完整参数字符串用引号括起来。

参数的常规语法："key1=value1[&key2=value2& ...]"

snmpversion=snmp|snmp3-指定 SNMPv1/2 或 SNMPv3。

user=*user name*-指定 SNMPv3 用户名。

securitylevel=AuthPriv|NoAuthNoPriv|AuthNoPriv-指定 SNMPv3 安全级别。

auth_protocol=MD5|SHA-指定 SNMPv3 身份验证协议。

auth_password=*password*-指定身份验证密码。

priv_protocol=DES|AES|3DES-指定 SNMPv3 隐私协议。

priv_password=*password*-指定隐私密码。

oid=*oid*-要查询的变量的对象标识符。

community=*string*-用于读取变量的团体字符串。

注意：有关每种服务类型的特定参数的详细信息，请参阅测试关键字 (p. 126)。

interval

指定测试间隔（秒）。

限制：30 秒的倍数

示例

指定每个间隔的抽样数。

超时

指定超时（秒）。

winsiz

指定统计时段大小（秒）。

tos

指定“服务类型”或“差分服务代码”IP。对于普通服务，使用 0（零）。另请参阅 RFC 1349。

limit

指定该测试总响应时间的可接受性能限制（或阈值）。在报告中使用该值。

flags

指定以下标志：

0x001 = 收集性能多维数据集

0x100 = 仅请求时执行（运行一次）

name

指定每种服务类型的唯一名称。引号 "" 中的空字符串不指定测试名称。

类

指定类名称。引号 "" 中的空字符串不指定类名称。

contextInfo

指定上下文信息。引号 "" 中的空字符串不指定上下文信息。

logLevel

指定测试执行码的日志级别。可能的值为：

-2 = 使用 SRM 全局日志级别（默认）

-1 = 不记录

0 = 致命（仅最重要的消息）

1 = 严重

...

7 = debug3（记录所有消息）

示例

添加 SNMPv1 测试：

```
svcwatch -p 161 -c admin -o add 1360757 "SNMP TEST" snmp "myhost:161" "" ""
"snmpversion=snmp&oid=1.3.6.1.4.1.546.1.1.7.8.27.0&community=admin" 30 3 30
60 0 0 0x100 "TestSNMP" "" "" 7
```

添加 SNMPv3 测试：

```
svcwatch -p 161 -c admin -o add 1360756 "SNMP3 TEST" snmp "myhost:161" "" ""
"snmpversion=snmp3&user=admin&securitylevel=AuthPriv&auth_protocol=MD5
&auth_password=XP1abcTZ&oid=1.3.6.1.4.1.546.1.1.7.8.27.0&community=topsecret"
30 3 30 60 0 0 0x100 "TestSNMP3" "" "" 7
```

详细信息

测试的关键字 (p. 126)

svcwatch add sql 命令-添加 SQL 测试

svcwatch add sql 命令用于向指定主机上的 SRM 添加 SQL 测试。有关详细信息和先决条件，请参阅本指南中的 SQL 查询测试 (p. 112)。

此命令具有以下格式：

```
svcwatch [options] -o add index descr sql destination
username password args interval samples timeout winsiz tos
limit flags name class contextInfo logLevel
```

该 add 命令使用以下参数：

选项

指定该命令的可能选项。

-h *hostname* | **-h *ipAddr***

（可选）指定 SystemEDGE 主机。

默认值：localhost

-p *port*

（可选）指定 SystemEDGE SNMP 端口。

默认：161

-c *community*

（可选）指定 SNMP 版本 1 和 2c 的 SNMP 团体字符串。

默认值：public

-v *snmpVersion*

（可选）指定 SNMP 版本。可能的值为：

- 1
- 2c
- 3

默认：1

-u *secName*

（可选）指定 SNMPv3 安全用户的名称。

-u *secLevel*

（可选）指定 SNMPv3 的安全级别。可能的值为：

- 1－noAuthNoPriv
- 2－AuthNoPriv
- 3－AuthPriv

-n *contextName*

（可选）指定 MIBMuxed 代理的实例名称。

-a *authPassword*

（可选）标识针对 AuthNoPriv 或 AuthPriv 安全级别选择 SNMPv3 时所需的身份验证密码。

-A *authProtocol*

（可选）指定身份验证协议。可能的值为：

- MD5－身份验证协议 HMAC-MD5
- SHA－身份验证协议 HMAC-SHA

默认：MD5

-x *privPassword*

（可选）指定针对安全级别 3 (AuthPriv) 选择 SNMPv3 时所需的隐私（加密）密码。

-X *encryptProtocol*

（可选）指定针对隐私使用加密协议。可能的值为：

- DES-数据加密标准
- AES-使用 128 位加密密钥的高级加密标准 (AES128)
- 3DES－三重数据加密标准

-m *FIPSmode*

（可选）指定 FIPS 模式。可能的值为：

- 0－非 FIPS
- 1－FIPS 共存
- 2－仅 FIPS

默认：0

-t *timeout*

（可选）指定 SNMP 命令超时。

默认值：10 秒

-d *logLevel*

（可选）指定 SNMP 消息的日志级别。可能的值为：

- 0－记录致命消息
- 1－记录严重消息
- 2－记录警告消息
- 3－记录信息消息
- 4－记录所有消息
- 5－记录所有消息，包括调试消息

默认：0

-f *logFile*

（可选）指定日志文件的名称。

默认值：sysedge_utility.log

-L

（可选）检测控制台和语言目录的当前区域设置（如果可用）。如果未找到语言目录，实用工具将重新使用英语作为默认语言。

-o add *testparams*

向 SRM 添加新测试。

testparams

指定新测试的参数。

index

指定 svcRspTable 索引。

descr

在引号中指定测试说明。如果引号 "" 中为空字符串，则表示未指定说明。

sql

指定 SQL 服务类型。

destination

指定用于测试的数据库服务器和端口 (*server*:*port*)。默认端口：1433 (SQL Server)、1521 (Oracle)

用户名

在引号中指定用于进行身份验证的用户名。如果引号 "" 中为空字符串，则表示未指定用户名。

password

在引号中指定用于进行身份验证的密码。如果引号 "" 中为空字符串，则表示未指定密码。

args

指定服务参数。每个参数都是一对关键字和值 (key=value)。通过与号 (&) 连接和分隔多个参数。完整参数字符串用引号括起来。

参数的常规语法："key1=value1[&key2=value2& ...]"

query=*query*-指定 SQL 查询。

qtype=query|stored|update-(可选）指定查询类型（默认值：query）。

dbtype=oracle|mssql|other-指定数据库类型。

dbname=*name*-（仅限 oracle 和 mssql）指定数据库名称。选择“other”时，请在连接字符串中指定数据库名称。

driver=driver-（仅限 other）用于查询的 JDBC 驱动程序。

url=*string*-（仅限 other）数据库连接字符串，因数据库类型而异。有关连接字符串的信息，请参阅数据库文档。

注意：有关每种服务类型的特定参数的详细信息，请参阅测试关键字 (p. 126)。

interval

指定测试间隔（秒）。

限制：30 秒的倍数

示例

指定每个间隔的抽样数。

超时

指定超时（秒）。

winsiz

指定统计时段大小（秒）。

tos

指定“服务类型”或“差分服务代码”IP。对于普通服务，使用 0（零）。另请参阅 RFC 1349。

limit

指定该测试总响应时间的可接受性能限制（或阈值）。在报告中使用该值。

flags

指定以下标志：

0x001 = 收集性能多维数据集

0x100 = 仅请求时执行（运行一次）

name

指定每种服务类型的唯一名称。引号 "" 中的空字符串不指定测试名称。

类

指定类名称。引号 "" 中的空字符串不指定类名称。

contextInfo

指定上下文信息。引号 "" 中的空字符串不指定上下文信息。

logLevel

指定测试执行码的日志级别。可能的值为：

-2 = 使用 SRM 全局日志级别（默认）

-1 = 不记录

0 = 致命（仅最重要的消息）

1 = 严重

...

7 = debug3（记录所有消息）

示例

添加 SQL Server 测试：

```
svcwatch -p 161 -c admin -o add 1360758 "TestSqlServer" sql
"192.168.100.100:1433" "sa" "AdminLvl1" "query=select * from
vas_system&dbtype=mssql&dbname=vasdb" 30 3 30 60 0 0 0x100
"TestSQL" "" ""
```

添加 SQL Server JDBC 驱动程序测试：

```
svcwatch -p 161 -c admin -o add 1360761 "TestSqlServerJDBCDriver"
sql "192.168.100.100:1433" "sa" "AdminLvl1" "query=select * from
my_system&dbtype=other&driver=com.microsoft.sqlserver.jdbc.SQLServerDriver
&url=jdbc:sqlserver://hostnameValue:portValue;databaseName=vasdb;
user=unameValue;password=pwdValue" 30 3 30 60 0 0 0x100
"TestSqlServerJDBCDriver" "" ""
```

添加 Oracle 测试：

```
svcwatch -p 161 -c admin -o add 1360759 "TestOracle" sql
"192.168.101.101:1521" "joe" "AdminLvl1" "query=select * from big_system
&dbtype=oracle&dbname=bigdb" 30 3 30 60 0 0 0x100 "TestOracle" "" ""
```

添加 Oracle JDBC 精简驱动程序测试：

```
svcwatch -p 161 -c admin -o add 1360762 "TestOracleJDBCThinDriver" sql
"192.168.101.101:1521" "joe" "AdminLvl1" "query=select table_name from
user_tables&dbtype=other&driver=oracle.jdbc.OracleDriver
&url=jdbc:oracle:thin:unameValue/pwdValue@hostnameValue:portValue:orcl"
30 3 30 60 0 0 0x100 "TestOracleThin" "" ""
```

详细信息

测试的关键字 (p. 126)
SQL 查询测试 (p. 112)

svcwatch add tcpconnect 命令-添加 TCP 连接测试

svcwatch add tcpconnect 命令用于向指定主机上的 SRM 添加 TCP 连接测试。

此命令具有以下格式：

```
svcwatch [options] -o add index descr tcpconnect destination
username password args interval samples timeout winsiz tos
limit flags name class contextInfo logLevel
```

该 add 命令使用以下参数：

选项

指定该命令的可能选项。

-h *hostname* | **-h *ipAddr***

（可选）指定 SystemEDGE 主机。

默认值：localhost

-p *port*

（可选）指定 SystemEDGE SNMP 端口。

默认：161

-c *community*

（可选）指定 SNMP 版本 1 和 2c 的 SNMP 团体字符串。

默认值：public

-v *snmpVersion*

（可选）指定 SNMP 版本。可能的值为：

- 1
- 2c
- 3

默认：1

-u *secName*

（可选）指定 SNMPv3 安全用户的名称。

-u *secLevel*

（可选）指定 SNMPv3 的安全级别。可能的值为：

- 1－noAuthNoPriv
- 2－AuthNoPriv
- 3－AuthPriv

-n *contextName*

（可选）指定 MIBMuxed 代理的实例名称。

-a *authPassword*

（可选）标识针对 AuthNoPriv 或 AuthPriv 安全级别选择 SNMPv3 时所需的身份验证密码。

-A *authProtocol*

（可选）指定身份验证协议。可能的值为：

- MD5－身份验证协议 HMAC-MD5
- SHA－身份验证协议 HMAC-SHA

默认：MD5

-x *privPassword*

（可选）指定针对安全级别 3 (AuthPriv) 选择 SNMPv3 时所需的隐私（加密）密码。

-X *encryptProtocol*

（可选）指定针对隐私使用加密协议。可能的值为：

- DES-数据加密标准
- AES-使用 128 位加密密钥的高级加密标准 (AES128)
- 3DES－三重数据加密标准

-m *FIPSmode*

（可选）指定 FIPS 模式。可能的值为：

- 0－非 FIPS
- 1－FIPS 共存
- 2－仅 FIPS

默认：0

-t *timeout*

（可选）指定 SNMP 命令超时。

默认值：10 秒

-d *logLevel*

（可选）指定 SNMP 消息的日志级别。可能的值为：

- 0－记录致命消息
- 1－记录严重消息
- 2－记录警告消息
- 3－记录信息消息
- 4－记录所有消息
- 5－记录所有消息，包括调试消息

默认：0

-f *logFile*

（可选）指定日志文件的名称。

默认值：sysedge_utility.log

-L

（可选）检测控制台和语言目录的当前区域设置（如果可用）。如果未找到语言目录，实用工具将重新使用英语作为默认语言。

-o add *testparams*

向 SRM 添加新测试。

testparams

指定新测试的参数。

index

指定 svcRspTable 索引。

descr

在引号中指定测试说明。如果引号 "" 中为空字符串，则表示未指定说明。

tcpconnect

指定 TCP 连接服务类型。

destination

指定用于测试的远程主机和端口 (*server*:*port*)。

用户名

在引号中指定用于进行身份验证的用户名。如果引号 "" 中为空字符串，则表示未指定用户名。

password

在引号中指定用于进行身份验证的密码。如果引号 "" 中为空字符串，则表示未指定密码。

args

没有 DHCP 服务类型可用的参数。如果引号 "" 中为空字符串，则表示未指定参数。

注意：有关每种服务类型的特定参数的详细信息，请参阅测试关键字 (p. 126)。

interval

指定测试间隔（秒）。

限制：30 秒的倍数

示例

指定每个间隔的抽样数。

超时

指定超时（秒）。

winsiz

指定统计时段大小（秒）。

tos

指定“服务类型”或“差分服务代码”IP。对于普通服务，使用 0（零）。另请参阅 RFC 1349。

limit

指定该测试总响应时间的可接受性能限制（或阈值）。在报告中使用该值。

flags

指定以下标志：

0x001 = 收集性能多维数据集

0x100 = 仅请求时执行（运行一次）

name

指定每种服务类型的唯一名称。引号 "" 中的空字符串不指定测试名称。

类

指定类名称。引号 "" 中的空字符串不指定类名称。

contextInfo

指定上下文信息。引号 "" 中的空字符串不指定上下文信息。

logLevel

指定测试执行码的日志级别。可能的值为：

-2 = 使用 SRM 全局日志级别（默认）

-1 = 不记录

0 = 致命（仅最重要的消息）

1 = 严重

...

7 = debug3（记录所有消息）

示例

添加 TCP 连接测试：

```
svcwatch -p 161 -c admin -o add 1360763 "Test" tcpconnect
"192.168.90.10:1433" "" "" "" 60 5 30 60 0 0 0X100
"Testtcpconnect" "" "" 1
```

由于此处未指定主机，因此使用默认值 localhost。端口号为 161。“add”向 SRM 中添加新测试。唯一的 svcRspTable 索引号是 2013。“Test”是该测试的说明。tcpconnect 指定 TCP 连接服务类型。测试的远程主机和端口的详细信息是 192.168.90.10:1433。

引号 ("") 中的两个空字符串表示不指定用于身份验证的用户名和密码。"" 指定没有可用于 tcpconnect 服务类型的参数。测试时间间隔指定为 60 秒。每个时间间隔内测试的采样数为 5。超时为 30 秒。统计信息窗口大小为 60 秒。0（零）指定正常服务（不是 IP 服务类型或差分服务）

0（零）指定该测试总响应时间的可接受性能限制（或阈值）。仅根据请求执行该测试（运行一次），并将标志设置为 0x100。将每个服务类型的唯一名称指定为 Testtcpconnect。不在 "" 中指定类名和上下文信息。以关键日志级别（“1”）执行该测试。

详细信息

测试的关键字 (p. 126)

svcwatch add tftp 命令-添加 TFTP 测试

svcwatch add tftp 命令用于向指定主机上的 SRM 添加 TFTP 测试。

此命令具有以下格式：

```
svcwatch [options] -o add index descr tftp destination
username password args interval samples timeout winsiz tos
limit flags name class contextInfo logLevel
```

该 add 命令使用以下参数：

选项

指定该命令的可能选项。

-h *hostname* | **-h *ipAddr***

（可选）指定 SystemEDGE 主机。

默认值：localhost

-p *port*

（可选）指定 SystemEDGE SNMP 端口。

默认：161

-c *community*

（可选）指定 SNMP 版本 1 和 2c 的 SNMP 团体字符串。

默认值：public

-v *snmpVersion*

（可选）指定 SNMP 版本。可能的值为：

- 1
- 2c
- 3

默认：1

-u *secName*

（可选）指定 SNMPv3 安全用户的名称。

-u *secLevel*

（可选）指定 SNMPv3 的安全级别。可能的值为：

- 1－noAuthNoPriv
- 2－AuthNoPriv
- 3－AuthPriv

-n *contextName*

（可选）指定 MIBMuxed 代理的实例名称。

-a *authPassword*

（可选）标识针对 AuthNoPriv 或 AuthPriv 安全级别选择 SNMPv3 时所需的身份验证密码。

-A *authProtocol*

（可选）指定身份验证协议。可能的值为：

- MD5－身份验证协议 HMAC-MD5
- SHA－身份验证协议 HMAC-SHA

默认：MD5

-x *privPassword*

（可选）指定针对安全级别 3 (AuthPriv) 选择 SNMPv3 时所需的隐私（加密）密码。

-X *encryptProtocol*

（可选）指定针对隐私使用加密协议。可能的值为：

- DES-数据加密标准
- AES-使用 128 位加密密钥的高级加密标准 (AES128)
- 3DES－三重数据加密标准

-m *FIPSmode*

（可选）指定 FIPS 模式。可能的值为：

- 0－非 FIPS
- 1－FIPS 共存
- 2－仅 FIPS

默认：0

-t *timeout*

（可选）指定 SNMP 命令超时。

默认值：10 秒

-d *logLevel*

（可选）指定 SNMP 消息的日志级别。可能的值为：

- 0－记录致命消息
- 1－记录严重消息
- 2－记录警告消息
- 3－记录信息消息
- 4－记录所有消息
- 5－记录所有消息，包括调试消息

默认：0

-f *logFile*

（可选）指定日志文件的名称。

默认值：sysedge_utility.log

-L

（可选）检测控制台和语言目录的当前区域设置（如果可用）。如果未找到语言目录，实用工具将重新使用英语作为默认语言。

-o add *testparams*

向 SRM 添加新测试。

testparams

指定新测试的参数。

index

指定 svcRspTable 索引。

descr

在引号中指定测试说明。如果引号 "" 中为空字符串，则表示未指定说明。

tftp

指定 TFTP 服务类型。

destination

指定用于测试的 TFTP 服务器和端口 (*server*:*port*)。默认端口：69

用户名

在引号中指定用于进行身份验证的用户名。如果引号 "" 中为空字符串，则表示未指定用户名。

password

在引号中指定用于进行身份验证的密码。如果引号 "" 中为空字符串，则表示未指定密码。

args

指定服务参数。每个参数都是一对关键字和值 (key=value)。通过与号 (&) 连接和分隔多个参数。完整参数字符串用引号括起来。

参数的常规语法："key1=value1[&key2=value2& ...]"

op=r-从服务器上读取文件。

op=w-将文件写入远程文件系统。

path=*path*-要读取或写入的文件的路径和文件名。

注意：有关每种服务类型的特定参数的详细信息，请参阅测试关键字 (p. 126)。

interval

指定测试间隔（秒）。

限制：30 秒的倍数

示例

指定每个间隔的抽样数。

超时

指定超时（秒）。

winsiz

指定统计时段大小（秒）。

tos

指定“服务类型”或“差分服务代码”IP。对于普通服务，使用 0（零）。另请参阅 RFC 1349。

limit

指定该测试总响应时间的可接受性能限制（或阈值）。在报告中使用该值。

flags

指定以下标志：

0x001 = 收集性能多维数据集

0x100 = 仅请求时执行（运行一次）

name

指定每种服务类型的唯一名称。引号 "" 中的空字符串不指定测试名称。

类

指定类名称。引号 "" 中的空字符串不指定类名称。

contextInfo

指定上下文信息。引号 "" 中的空字符串不指定上下文信息。

logLevel

指定测试执行码的日志级别。可能的值为：

-2 = 使用 SRM 全局日志级别（默认）

-1 = 不记录

0 = 致命（仅最重要的消息）

1 = 严重

...

7 = debug3（记录所有消息）

示例

添加 TFTP 测试：

```
svcwatch -p 161 -c admin -o add 1360764 "Test" tftp "192.168.120.10:69"
"" "" "op=r&path=I:\SA\TFTP\get.txt" 60 3 30 60 0 0 0X100 "Testtftp"
"" "" 0
```

详细信息

测试的关键字 (p. 126)

svcwatch add vuser 命令—添加虚拟用户测试

svcwatch add vuser 命令用于将虚拟用户测试添加到指定主机上的 SRM。

此命令具有以下格式：

```
svcwatch [options] -o add index descr vuser destination
username password args interval samples timeout winsiz tos
limit flags name class contextInfo logLevel
```

add 命令使用以下参数：

选项

指定该命令的可能选项。

-h *hostname* | **-h *ipAddr***

（可选）指定 SystemEDGE 主机。

默认值：localhost

-p *port*

（可选）指定 SystemEDGE SNMP 端口。

默认：161

-c *community*

（可选）指定 SNMP 版本 1 和 2c 的 SNMP 团体字符串。

默认值：public

-v *snmpVersion*

（可选）指定 SNMP 版本。可能的值为：

- 1
- 2c
- 3

默认：1

-u *secName*

（可选）指定 SNMPv3 安全用户的名称。

-u *secLevel*

（可选）指定 SNMPv3 的安全级别。可能的值为：

- 1－noAuthNoPriv
- 2－AuthNoPriv
- 3－AuthPriv

-n *contextName*

（可选）指定 MIBMuxed 代理的实例名称。

-a *authPassword*

（可选）标识针对 AuthNoPriv 或 AuthPriv 安全级别选择 SNMPv3 时所需的身份验证密码。

-A *authProtocol*

（可选）指定身份验证协议。可能的值为：

- MD5－身份验证协议 HMAC-MD5
- SHA－身份验证协议 HMAC-SHA

默认：MD5

-x *privPassword*

（可选）指定针对安全级别 3 (AuthPriv) 选择 SNMPv3 时所需的隐私（加密）密码。

-X *encryptProtocol*

（可选）指定针对隐私使用加密协议。可能的值为：

- DES-数据加密标准
- AES-使用 128 位加密密钥的高级加密标准 (AES128)
- 3DES－三重数据加密标准

-m *FIPSmode*

（可选）指定 FIPS 模式。可能的值为：

- 0－非 FIPS
- 1－FIPS 共存
- 2－仅 FIPS

默认：0

-t *timeout*

（可选）指定 SNMP 命令超时。

默认值：10 秒

-d *logLevel*

（可选）指定 SNMP 消息的日志级别。可能的值为：

- 0—记录致命消息
- 1—记录严重消息
- 2—记录警告消息
- 3—记录信息消息
- 4—记录所有消息
- 5—记录所有消息，包括调试消息

默认：0

-f *logFile*

（可选）指定日志文件的名称。

默认值：sysedge_utility.log

-L

（可选）检测控制台和语言目录的当前区域设置（如果可用）。如果未找到语言目录，实用工具将重新使用英语作为默认语言。

-o add *testparams*

将新测试添加到 SRM 中。

testparams

为新测试指定参数。

index

指定 svcRspTable 索引。

descr

在引号中指定测试的说明。引号 ("") 中为空字符串将不指定说明。

vuser

指定虚拟用户服务类型。

destination

为测试指定脚本的路径。

username

在引号中指定要运行脚本的用户名。引号 ("") 中为空字符串将不指定用户名。

password

在引号中指定用于进行身份验证的密码。引号 ("") 中为空字符串将不指定密码。

args

指定服务参数。每个参数都是一对关键字和值 (key=value)。通过与号 (&) 连接和分隔多个参数。完整参数字符串用引号括起来。

参数的常规语法："key1=value1[&key2=value2& ...]"

host=*hostname*:*port*—目标系统的主机名；此值用于 DNS 查找和连接计时。正在运行脚本的端口。

domain=*domain*—正在运行脚本的用户所在的域。

注意：有关每个服务类型的特定参数的详细信息，请参阅测试的关键字 (p. 126)。

interval

指定测试间隔（秒）。

限制：30 秒的倍数

示例

指定每个间隔的抽样数。

超时

指定超时（秒）。

winsiz

指定统计时段大小（秒）。

tos

指定“服务类型”或“差分服务代码”IP。对于普通服务，使用 0（零）。另请参阅 RFC 1349。

limit

指定该测试总响应时间的可接受性能限制（或阈值）。在报告中使用该值。

flags

指定以下标志：

0x001 = 收集性能多维数据集

0x100 = 仅请求时执行（运行一次）

name

指定每种服务类型的唯一名称。引号 "" 中的空字符串不指定测试名称。

类

指定类名称。引号 "" 中的空字符串不指定类名称。

contextInfo

指定上下文信息。引号 "" 中的空字符串不指定上下文信息。

logLevel

指定测试执行码的日志级别。可能的值为：

-2 = 使用 SRM 全局日志级别（默认）

-1 = 不记录

0 = 致命（仅最重要的消息）

1 = 严重

...

7 = debug3（记录所有消息）

示例

添加虚拟用户测试：

```
svcwatch -h localhost -p 161 -c snmp_admin -o add 1360765 "vUser Test"
vuser "C:\WinTask\bin\taskexec.exe C:\WinTask\Scripts\notepad.rob" ""
"" "" 30 1 10 120 0 0 0x001 "vUserTEST" "ClassName" "ContextName" 7
```

详细信息

测试的关键字 (p. 126)

svcwatch delete 命令-删除测试

svcwatch delete 命令用于删除指定主机上的测试。

此命令具有以下格式：

```
svcwatch [options] -o delete index
```

该 delete 命令使用以下参数：

选项

指定该命令的可能选项。

-h *hostname*｜ -h *ipAddr*

（可选）指定 SystemEDGE 主机。

默认值：localhost

-p *port*

（可选）指定 SystemEDGE SNMP 端口。

默认：161

-c *community*

（可选）指定 SNMP 版本 1 和 2c 的 SNMP 团体字符串。

默认值：public

-v *snmpVersion*

（可选）指定 SNMP 版本。可能的值为：

- 1
- 2c
- 3

默认：1

-u *secName*

（可选）指定 SNMPv3 安全用户的名称。

-u *secLevel*

（可选）指定 SNMPv3 的安全级别。可能的值为：

- 1－noAuthNoPriv
- 2－AuthNoPriv
- 3－AuthPriv

-n *contextName*

（可选）指定 MIBMuxed 代理的实例名称。

-a *authPassword*

（可选）标识针对 AuthNoPriv 或 AuthPriv 安全级别选择 SNMPv3 时所需的身份验证密码。

-A *authProtocol*

（可选）指定身份验证协议。可能的值为：

- MD5－身份验证协议 HMAC-MD5
- SHA－身份验证协议 HMAC-SHA

默认：MD5

-x *privPassword*

（可选）指定针对安全级别 3 (AuthPriv) 选择 SNMPv3 时所需的隐私（加密）密码。

-X *encryptProtocol*

（可选）指定针对隐私使用加密协议。可能的值为：

- DES-数据加密标准
- AES-使用 128 位加密密钥的高级加密标准 (AES128)
- 3DES－三重数据加密标准

-m *FIPSmode*

（可选）指定 FIPS 模式。可能的值为：

- 0－非 FIPS
- 1－FIPS 共存
- 2－仅 FIPS

默认：0

-t *timeout*

（可选）指定 SNMP 命令超时。

默认值：10 秒

-d *logLevel*

（可选）指定 SNMP 消息的日志级别。可能的值为：

- 0－记录致命消息
- 1－记录严重消息
- 2－记录警告消息
- 3－记录信息消息
- 4－记录所有消息
- 5－记录所有消息，包括调试消息

默认：0

-f *logFile*

（可选）指定日志文件的名称。

默认值：sysedge_utility.log

-L

（可选）检测控制台和语言目录的当前区域设置（如果可用）。如果未找到语言目录，实用工具将重新使用英语作为默认语言。

-o delete *index*

删除指定测试。

index

指定用于标识要删除的测试的 svcRspTable 索引。

示例

删除 myremote 主机上的测试：

```
svcwatch -h myremote -p 161 -c admin -o delete 1360739
```

svcwatch list 命令-查看测试信息

svcwatch list 命令用于列出指定主机上的可用测试。

此命令具有以下格式：

```
svcwatch [options] -o list
```

该 list 命令使用以下参数：

选项

指定该命令的可能选项。

-h *hostname*｜ -h *ipAddr*

（可选）指定 SystemEDGE 主机。

默认值：localhost

-p *port*

（可选）指定 SystemEDGE SNMP 端口。

默认：161

-c *community*

（可选）指定 SNMP 版本 1 和 2c 的 SNMP 团体字符串。

默认值：public

-v *snmpVersion*

（可选）指定 SNMP 版本。可能的值为：

- 1
- 2c
- 3

默认：1

-u *secName*

（可选）指定 SNMPv3 安全用户的名称。

-u *secLevel*

（可选）指定 SNMPv3 的安全级别。可能的值为：

- 1－noAuthNoPriv
- 2－AuthNoPriv
- 3－AuthPriv

-n *contextName*

（可选）指定 MIBMuxed 代理的实例名称。

-a *authPassword*

（可选）标识针对 AuthNoPriv 或 AuthPriv 安全级别选择 SNMPv3 时所需的身份验证密码。

-A *authProtocol*

（可选）指定身份验证协议。可能的值为：

- MD5－身份验证协议 HMAC-MD5
- SHA－身份验证协议 HMAC-SHA

默认：MD5

-x *privPassword*

（可选）指定针对安全级别 3 (AuthPriv) 选择 SNMPv3 时所需的隐私（加密）密码。

-X *encryptProtocol*

（可选）指定针对隐私使用加密协议。可能的值为：

- DES-数据加密标准
- AES-使用 128 位加密密钥的高级加密标准 (AES128)
- 3DES－三重数据加密标准

-m *FIPSmode*

（可选）指定 FIPS 模式。可能的值为：

- 0－非 FIPS
- 1－FIPS 共存
- 2－仅 FIPS

默认：0

-t *timeout*

（可选）指定 SNMP 命令超时。

默认值：10 秒

-d *logLevel*

（可选）指定 SNMP 消息的日志级别。可能的值为：

- 0－记录致命消息
- 1－记录严重消息
- 2－记录警告消息
- 3－记录信息消息
- 4－记录所有消息
- 5－记录所有消息，包括调试消息

默认：0

-f *logFile*

（可选）指定日志文件的名称。

默认值：sysedge_utility.log

-L

（可选）检测控制台和语言目录的当前区域设置（如果可用）。如果未找到语言目录，实用工具将重新使用英语作为默认语言。

-o list

列出可用测试。

示例

列出本地主机上的测试：

```
svcwatch -o list
```

svcwatch setstatus 命令-更改测试状态

svcwatch setstatus 命令用于更改指定主机上的测试状态。

此命令具有以下格式：

```
svcwatch [options] -o setstatus index status
```

该 setstatus 命令使用以下参数：

选项

指定该命令的可能选项。

-h *hostname*｜ -h *ipAddr*

（可选）指定 SystemEDGE 主机。

默认值：localhost

-p *port*

（可选）指定 SystemEDGE SNMP 端口。

默认：161

-c *community*

（可选）指定 SNMP 版本 1 和 2c 的 SNMP 团体字符串。

默认值：public

-v *snmpVersion*

（可选）指定 SNMP 版本。可能的值为：

- 1
- 2c
- 3

默认：1

-u *secName*

（可选）指定 SNMPv3 安全用户的名称。

-u *secLevel*

（可选）指定 SNMPv3 的安全级别。可能的值为：

- 1－noAuthNoPriv
- 2－AuthNoPriv
- 3－AuthPriv

-n *contextName*

（可选）指定 MIBMuxed 代理的实例名称。

-a *authPassword*

（可选）标识针对 AuthNoPriv 或 AuthPriv 安全级别选择 SNMPv3 时所需的身份验证密码。

-A *authProtocol*

（可选）指定身份验证协议。可能的值为：

- MD5－身份验证协议 HMAC-MD5
- SHA－身份验证协议 HMAC-SHA

默认：MD5

-x *privPassword*

（可选）指定针对安全级别 3 (AuthPriv) 选择 SNMPv3 时所需的隐私（加密）密码。

-X *encryptProtocol*

（可选）指定针对隐私使用加密协议。可能的值为：

- DES-数据加密标准
- AES-使用 128 位加密密钥的高级加密标准 (AES128)
- 3DES－三重数据加密标准

-m *FIPSmode*

（可选）指定 FIPS 模式。可能的值为：

- 0－非 FIPS
- 1－FIPS 共存
- 2－仅 FIPS

默认：0

-t *timeout*

（可选）指定 SNMP 命令超时。

默认值：10 秒

-d *logLevel*

（可选）指定 SNMP 消息的日志级别。可能的值为：

- 0－记录致命消息
- 1－记录严重消息
- 2－记录警告消息
- 3－记录信息消息
- 4－记录所有消息
- 5－记录所有消息，包括调试消息

默认：0

-f *logFile*

（可选）指定日志文件的名称。

默认值：sysedge_utility.log

-L

（可选）检测控制台和语言目录的当前区域设置（如果可用）。如果未找到语言目录，实用工具将重新使用英语作为默认语言。

-o setstatus *index status*

指定测试的新状态。

index

指定用作测试标识符的 svcRspTable 索引。

注意：将 add 命令与该测试的索引结合使用时，将用新测试覆盖现有测试。

状态

指定状态。可能的值为：

active (1)，

notInService (2)，

notReady (3)，

createAndGo (4)，

createAndWait (5)，

destroy (6)

示例

更改测试状态：

```
svcwatch -p 161 -c admin -o setstatus 1360739 2
```

svcwatch version 命令-查看 SRM 版本信息

svcwatch version 命令用于显示指定主机上的 SRM AIM 版本。

此命令具有以下格式：

```
svcwatch [options] -o version
```

该 version 命令使用以下参数：

选项

指定该命令的可能选项。

-h *hostname*｜ -h *ipAddr*

（可选）指定 SystemEDGE 主机。

默认值：localhost

-p *port*

（可选）指定 SystemEDGE SNMP 端口。

默认：161

-c *community*

（可选）指定 SNMP 版本 1 和 2c 的 SNMP 团体字符串。

默认值：public

-v *snmpVersion*

（可选）指定 SNMP 版本。可能的值为：

- 1
- 2c
- 3

默认：1

-u *secName*

（可选）指定 SNMPv3 安全用户的名称。

-u *secLevel*

（可选）指定 SNMPv3 的安全级别。可能的值为：

- 1－noAuthNoPriv
- 2－AuthNoPriv
- 3－AuthPriv

-n *contextName*

（可选）指定 MIBMuxed 代理的实例名称。

-a *authPassword*

（可选）标识针对 AuthNoPriv 或 AuthPriv 安全级别选择 SNMPv3 时所需的身份验证密码。

-A *authProtocol*

（可选）指定身份验证协议。可能的值为：

- MD5－身份验证协议 HMAC-MD5
- SHA－身份验证协议 HMAC-SHA

默认：MD5

-x *privPassword*

（可选）指定针对安全级别 3 (AuthPriv) 选择 SNMPv3 时所需的隐私（加密）密码。

-X *encryptProtocol*

（可选）指定针对隐私使用加密协议。可能的值为：

- DES-数据加密标准
- AES-使用 128 位加密密钥的高级加密标准 (AES128)
- 3DES－三重数据加密标准

-m *FIPSmode*

（可选）指定 FIPS 模式。可能的值为：

- 0－非 FIPS
- 1－FIPS 共存
- 2－仅 FIPS

默认：0

-t *timeout*

（可选）指定 SNMP 命令超时。

默认值：10 秒

-d *logLevel*

（可选）指定 SNMP 消息的日志级别。可能的值为：

- 0－记录致命消息
- 1－记录严重消息
- 2－记录警告消息
- 3－记录信息消息
- 4－记录所有消息
- 5－记录所有消息，包括调试消息

默认：0

-f *logFile*

（可选）指定日志文件的名称。

默认值：sysedge_utility.log

-L

（可选）检测控制台和语言目录的当前区域设置（如果可用）。如果未找到语言目录，实用工具将重新使用英语作为默认语言。

-o version

显示服务响应监控的 CA SystemEDGE AIM 的版本。

示例

在 myremote 主机上显示版本：

```
svcwatch -h myremote -o version
```

附录 B： 安装

此部分包含以下主题：

通过 CA Virtual Assurance 设置的安装 (p. 259)
远程部署 (p. 259)
单个安装 (p. 261)
升级 (p. 262)
从 Windows 上卸载 (p. 262)
从 Linux 或 UNIX 上卸载 (p. 263)

通过 CA Virtual Assurance 设置的安装

在运行 CA Virtual Assurance 自定义安装时，您可以选择您想安装的 AIM。自定义安装默认情况下在管理器系统上安装 SystemEDGE 和所有 AIM。

远程部署

您可以在 AIX、HP-UX、Linux、Solaris 或 Windows 系统上从 CA Virtual Assurance 管理器通过远程部署安装 SystemEDGE 和 AIM。

要将代理部署到系统，请创建部署作业。部署作业包含 CA Virtual Assurance 将部署软件包适时传送给相应系统所需的详细信息。

遵循这些步骤:

1. 依次选择“资源”、“部署”。

   “部署”窗格显示“软件包”、“模板”和“作业”。

2. 在“管理资源”窗格中右键单击“作业”文件夹，然后选择“创建新作业”。还可以选择“作业”文件夹，然后单击“作业状态”工具栏上的 +（新建）。

   此时将显示“作业设置”页面。

3. 在“作业名称”窗格中输入名称，可以选择使该作业基于现有的模板，然后单击“下一步”。

   此时将显示“软件包选择”页面。

4. 选择平台和希望部署的软件包。

5. （可选）单击“详细信息”选项卡。

   此时将显示“软件包打包程序详细信息”对话框，您可以使用该对话框以内联方式编辑软件包属性。如果软件包打包程序处于不完整或无效状态，可以通过内联编辑修改字段。

   a. 单击“编辑”并修改软件包打包程序属性。

   b. 单击“保存”，然后单击“确定”。

      软件包打包程序属性即已更新。

6. 单击向下箭头将软件包打包程序添加到作业中，然后单击“下一步”。

   此时将显示“计算机选择”页面。

7. 选择要部署到的系统，然后单击“下一步”。如果您的环境中有许多服务器，则需要多个包含一些条目的页面才能列出所有服务器。在页面上选择服务器并滚动到下一页时，在前一页上选择的所有服务器仍是有效的。

   此时将显示“已选择计算机”页面。

8. 单击“设置凭据”，设置建立连接所需的系统凭据，然后单击“下一步”。

   注意：使用域凭据部署到 Windows 目标系统必须采用“域\用户名”形式。

   此时将显示“高级”页。

9. （可选）设置分发服务器来管理部署。如果不设置，则将进行自动选择。

10. 为该作业选择排定选项：

    立即交付

    在创建新部署作业后立即启动作业。“立即交付”是默认选项。

    交错交付

    在特定时间段内交付软件包。

    排定交付

    排定未来特定时间的部署。

11. （可选）如果先前已使用该部署基础架构将某个软件包成功部署到系统，您可以强制是否再次运行。

12. 单击“下一步”。

    此时将显示“摘要”页面。

13. 检查作业的详细信息，然后单击“部署”。

    部署作业创建完成。

注意：在创建作业之后，您可以将该作业另存为模板。模板可以省去软件包和机器的选择，因此可以在后续作业中轻松复用。

单个安装

当您在安装完 SystemEDGE 之后安装 SRM AIM 时，请考虑 SRM AIM 依赖于高级加密和 SystemEDGE。

根据这些依存关系，安装顺序如下所示：

1. SystemEDGE 核心
2. 高级加密
3. SRM AIM

安装程序不允许采用其他任何顺序。例如，当您尝试在未安装高级加密的情况下安装 SRM 时，将显示错误消息，并且安装不会开始。

注意：有关安装 SystemEDGE 的详细信息，请参阅《CA Virtual Assurance 实施指南》或《SystemEDGE 用户指南》。

使用 ca-setup.exe 在 Windows 上安装 SRM AIM

1. 导航到 DVD1\Installers\Windows\Agent\SysMan 目录。通过考虑相应顺序在该目录中安装以下组件：
    1. CA_SystemEDGE_Core
    2. CA_SystemEDGE_AdvancedEncryption
    3. CA_SystemEDGE_SRM
2. 转到相应的目录，并运行以下命令：

    ```
    ca-setup
    ```

    按照屏幕说明进行操作并完成安装。

使用 ca-setup.sh 在 Linux 和 UNIX 上安装 SRM AIM

1. 打开终端控制台并转到 DVD2/Installers/*Platform*/Agent/SysMan 目录。通过考虑相应顺序在该目录中安装以下组件：
    1. CA_SystemEDGE_Core
    2. CA_SystemEDGE_AdvancedEncryption
    3. CA_SystemEDGE_SRM
2. 转到相应目录并运行以下命令：

    ```
    sh ca-setup.sh
    ```

    按照屏幕说明进行操作并完成安装。

在 SRM 安装期间，您可以指定以下参数：

允许运行脚本

指定是否允许运行自定义脚本。这些脚本使用超级用户权限运行。

默认值：否（典型安装）

允许文件 IO 测试

允许运行文件 IO 测试。由于测试使用超级用户权限运行，因此它们可以在启用该选项时访问系统上的任何文件。

默认值：否（典型安装）

允许不信任的 SSL 证书

允许 HTTPS 测试访问具有无效证书（不受信任的证书，或者网站与证书中的名称不匹配）的站点。

默认值：否（典型安装）

杂项

安装 SRM 文档组件。

默认值：Yes

升级

所有功能增强均被指定为*附加*功能。在配置文件中，它们的参数可以填充为默认信息，也允许为 NULL。SRM AIM 支持从 SRM 2.0 和 SRM 2.1 升级，且在适当的情况下接受版本为 2.x 的 svcrsp.cf 文件。

从 Windows 上卸载

您可以从控制面板或命令行卸载 SRM AIM。删除最初通过远程部署安装的组件时，不会卸载 Idprimer 和 CAM。

从 Windows 的“添加或删除程序”窗口卸载 SRM AIM

1. 选择“开始”、“设置”、“控制面板”、“添加或删除程序”。

   显示“添加或删除程序”窗口并列出以下组件：

   - CA SystemEDGE Core
   - CA SystemEDGE AdvancedEncryption
   - CA SystemEDGE SRM

2. 右键单击 CA SystemEDGE SRM 并选择“卸载”。

   对话框中会显示此卸载过程。卸载完成时，对话框将关闭。

从命令行卸载 SRM AIM

1. 打开命令提示符并转到 DVD1\Installers\Windows\Agent\SysMan\CA_SystemEDGE_SRM 目录。
2. 运行下列命令：

   ```
   ca-setup -x
   ```

   对话框中会显示此卸载过程。卸载完成时，对话框将关闭。

从 Linux 或 UNIX 上卸载

从命令行卸载 SRM AIM。删除最初通过远程部署安装的组件时，不会卸载 Idprimer 和 CAM。

使用 ca-setup.sh 在 UNIX 上卸载 SRM AIM

1. 打开终端控制台并以 root (su) 登录。
2. 转到 DVD2/Installers/<*Platform*>/Agent/SysMan/CA_SystemEDGE_SRM 目录并运行以下命令：

   ```
   sh ca-setup.sh -x
   ```

   对话框中会显示此卸载过程。卸载过程完成时，对话框将关闭。

使用 lsm 在 UNIX 上卸载 SRM AIm

1. 打开终端控制台并以 root (su) 登录。
2. 运行下列命令：

   ```
   lsm -e CA_SystemEDGE_SRM
   ```

   跟随卸载过程的进度，直到它完成。

附录 C： 错误代码

此部分包含以下主题：

错误代码概述 (p. 265)
常规错误代码 (p. 267)
A 至 H 错误代码 (p. 268)
I 至 R 错误代码 (p. 274)
S - Z 错误代码 (p. 282)

错误代码概述

本页定义您在使用 SRM 时可能会遇到的错误代码。错误将显示在“测试监视器”和“测试配置文件监视器”页面上的“错误代码”列中。有关某些测试的其他信息显示在“结果字段”列中。（要显示“错误代码”和“结果字段”列，请单击“测试监视器”页面上的“显示列配置”，选择“错误代码”和“结果字段”，然后单击“更新页面”。）

Windows 系统

在 Windows 系统上，SRM 在下列位置记录错误：

- *Install_Path*\SystemEDGE\data\port161\sysedge.log－代理端消息
- *Install_Path*\SystemEDGE\data\port161\plugins\svcrsp\jcollector.log－收集器消息，包括所有测试参数的初始化以及每个测试执行的结果
- *Install_Path*\SystemEDGE\data\port161\plugins\svcrsp\sarunas.log－虚拟用户作为用户运行的错误

注意：驱动器和安装目录取决于安装 SRM 的目录。

UNIX 系统

在 UNIX 系统上，SRM 在下列位置记录错误：

- 您平台的系统日志 (syslog) 文件－代理端错误
- *Install_Path*/SystemEDGE/data/port161/svcrsp/jcollector.log－收集器消息，包括所有测试参数的初始化以及每个测试执行的结果

jcollector.log 文件

所有测试特定错误代码都记录在 jcollector.log 文件中。

在该文件中设置调试级别

1. 停止 SystemEDGE。
2. 打开 svcrsp.cf 文件进行编辑。
3. 取消注释（删除前面的井号 (#)）#collector_debug 一行，并按如下所示设置记录级别指令：
   - 对于常规使用，请指定 loglevel=0。
   - 指定 loglevel=1 以查看每遍测试的开始和结束时间。
   - 指定 loglevel=2 以查看每个单独测试的开始和结束时间。
   - 指定 loglevel=3 以用于调试。

注意：使用 [#] 找到与失败的测试对应的调试日志部分。

CA 特定的错误代码通常优先于服务的标准数字代码，因为 CA 特定的代码通常指示程序中的错误。例如，如果 HTTP 测试开始下载页面，返回 404 错误，然后在事务处理结束之前遇到文件 I/O 错误，则 SRM 表中的“错误代码”字段将设置为 58（事务处理期间的 I/O 错误），而不是 404。

错误代码描述

SRM 会生成下列错误类型代码：

- 常规
- Active Directory 用户
- 自定义
- DHCP
- DNS
- 文件 I/O
- FTP
- HTTP/HTTPS
- IMAP
- LDAP
- MAPI
- NIS
- NNTP
- Ping
- POP3
- 重新配置和初始化

- SMTP
- SNMP
- SQL 查询
- TFTP
- 虚拟用户
- 结果字段

常规错误代码

常规错误代码

这些代码适用于所有测试类型。

错误代码	描述
50	不正确的或格式错误的测试参数。要修改这些参数，请转到“测试管理”页面，选择要修改的测试，然后单击“修改”。有关详细信息，请参阅您正在运行的测试类型的“帮助”页面（如“文件 I/O”帮助页面）。
51	未知主机。要修改该主机名，请转到“测试管理”页面，选择要修改的测试，然后单击“修改”。有关详细信息，请参阅您正在运行的测试类型的“帮助”页面。
52	端口无效。您正在测试的系统上可能正在使用选择的端口或该端口不可用。您可以在“修改测试”页面上修改测试的端口。有关详细信息，请参阅您正在运行的测试类型的“帮助”页面。
53	设置套接字选项（如 TOS）时出错。该错误可能是由于目标系统上注册表的无效权限而导致的。请检查系统配置设置。
54	测试超时。您可以在“修改测试”页面上为测试设置其他超时值。有关详细信息，请参阅您正在运行的测试类型的“帮助”页面。
55	创建套接字时出错。该错误可能是由于系统配置问题而导致的。请检查目标系统上的系统配置设置。
56	连接套接字时出错。该错误可能是由于系统配置问题而导致的。请检查目标系统上的系统配置设置。
57	关闭套接字时出错。该错误可能是由于系统配置问题而导致的。请检查目标系统上的系统配置设置。

错误代码	描述
58	事务处理期间发生 I/O 错误。该错误可能是由于系统配置问题而导致的。请检查目标系统上的系统配置设置。
59	WSAStartup 期间出现错误（仅 Windows）。WSAStartup 允许应用程序指定必需的 Windows Sockets API 的版本，以及检索特定 Windows Sockets 实施的详细信息。请检查目标系统上的系统配置设置。
60	套接字关闭过早。该错误表示目标系统意外终止连接。请检查目标系统上的系统配置设置。
61	抽样错误，拒绝结果。

A 至 H 错误代码

Active Directory 和 LDAP 测试错误代码

错误代码	描述
1	常规错误。有关详细信息，请参阅以下任何错误日志： ■ %SystemRoot%\windows\system32\sysedge.log（Windows 系统）或系统日志文件 (UNIX) ■ *SystemEDGE-install-directory*\sysedge\plugins\svcrsp\jcollector.log (Windows) 或 *SystemEDGE-install-directory*/plugins/svcrsp/jcollector.log (UNIX)
2	ldap.jar 文件可能安装错误。检查目标系统以确保 jre/lib/ext 目录中存在该文件。如果不存在，则将该文件复制到该目录。
3	域可能不正确。验证是否为正在测试的 LDAP 服务器指定了正确的域。您可以在“修改测试”页面上指定其他域。有关详细信息，请参阅“LDAP 测试”。
4	登录失败。验证是否为正在测试的 LDAP 服务器指定了有效的用户名和密码。您可以在“修改测试”页面上指定其他用户名和密码。有关详细信息，请参阅“LDAP 测试”。
5	查询未生成任何结果。如果输入了无效的查询，或者查询与 LDAP 服务器上的任何内容均不匹配，则可能会导致该错误。您可以在“修改测试”页面上指定其他查询。有关详细信息，请参阅“LDAP 测试”。

自定义测试错误代码

错误代码	描述
1	执行自定义脚本时出错。验证您在“修改测试”页面上指定的目录中是否存在该脚本。必要时，可以在该页面上更改脚本名称和目标。有关详细信息，请参阅“使用自定义脚本”。
2	自定义脚本返回了错误的退出代码。该错误可能表示该脚本不符合编写自定义脚本的准则。必要时，请更新脚本。
3	自定义脚本输出了格式错误的输出结果。该错误可能表示该脚本不符合编写自定义脚本的准则。必要时，请更新脚本。
4	自定义脚本未输出任何输出结果。该错误可能表示该脚本不符合编写自定义脚本的准则。必要时，请更新脚本。
5	从 I/O 数据流读取时出错。该错误可能是由于系统配置问题而导致的。请检查目标系统上的系统配置设置。

DHCP 测试错误代码

错误代码	描述
1	常规错误。有关详细信息，请参阅以下任何错误日志： ■ %SystemRoot%\windows\system32\sysedge.log（Windows 系统）或系统日志文件 (UNIX) ■ *SystemEDGE-install-directory*\sysedge\plugins\svcrsp\jcollector.log (Windows) 或 *SystemEDGE-install-directory*/plugins/svcrsp/jcollector.log (UNIX)
2	无法绑定到套接字。请检查目标系统上的系统配置设置。
3	套接字在接收时超时。请检查目标系统上的系统配置设置。

DNS 测试错误代码

错误代码	描述
1	发送查询时出错。检查目标系统的网络设置和可用性。
2	接收响应时出错。检查目标系统的网络设置和可用性。

错误代码	描述
3	服务器指示查询无效。
4	服务器指示服务器错误。该错误表示 SRM 可以与目标系统联系，但该系统出现错误。请检查目标系统上的系统配置设置。
5	服务器指示未找到主机。该错误表示 SRM 可以与目标系统联系，但该系统出现错误。请检查目标系统上的系统配置设置。

文件 I/O 测试错误代码

错误代码	描述
1	常规错误。有关详细信息，请参阅以下任何错误日志： ■ *%SystemRoot%\windows\system32\sysedge.log*（Windows 系统）或系统日志文件 (UNIX) ■ *SystemEDGE-install-directory*\sysedge\plugins\svcrsp\jcollector.log (Windows) 或 *SystemEDGE-install-directory*/plugins/svcrsp/jcollector.log (UNIX)
2	访问本地文件被拒绝。该错误表示您正在使用的用户名和密码可能没有正确的权限。您可以在“修改测试”页面上指定其他用户名和密码。有关详细信息，请参阅“文件 I/O 测试”。
3	访问远程文件被拒绝。该错误表示您正在使用的用户名和密码可能没有正确的权限。您可以在“修改测试”页面上指定其他用户名和密码。有关详细信息，请参阅“文件 I/O 测试”。
4	找不到本地文件。
5	找不到远程文件。
6	路径参数指向本地目录中的文件。源文件应位于本地目录中，目标文件应位于远程文件系统上。您可以在“修改测试”页面上更改源文件名和目标文件名。有关详细信息，请参阅“文件 I/O 测试”。
7	读取本地文件失败。当且仅当该抽象路径名指定的文件存在并且可由应用程序读取时，源文件为 true；否则为 false
8	读取远程文件失败。
9	创建远程文件失败。
10	写入到远程文件失败。

错误代码	描述
11	外部命令的输出无效或没有输出。
12	删除远程文件失败。
13	文件比较失败。
14	无法执行 file_io_helper.jar。
15	无法写入日志 msg。

FTP 测试错误代码

错误代码	描述
421	服务不可用；正在关闭控制连接。（如果服务知道必须关闭连接，则可能会通过关闭连接来响应任何命令。）该错误表示 SRM 可以与目标系统联系，但该系统出现错误。请检查目标系统上的系统配置设置。
425	无法打开数据连接。该错误表示 SRM 可以与目标系统联系，但该系统出现错误。请检查目标系统上的系统配置设置。
426	连接已关闭；传输已中止。该错误表示 SRM 可以与目标系统联系，但该系统出现错误。请检查目标系统上的系统配置设置。
450	请求的文件操作未执行。文件不可用。该错误可能表示该文件在使用中或不在预期的位置。验证您正在测试的文件是否存在且未在使用中。
451	请求的操作已中止。处理时发生本地错误。该错误表示 SRM 可以与目标系统联系，但该系统出现错误。请检查目标系统上的系统配置设置。
452	请求的操作未执行。系统中的存储空间不足。该错误表示您可能需要将更多的磁盘空间添加到 FTP 服务器。
500	语法错误。命令无法识别。如果命令行过长，或者正在运行不标准的 FTP 软件，则可能会收到该错误消息。
501	参数中存在语法错误。如果正在运行不标准的 FTP 软件，则可能会收到该错误消息。
502	命令未执行。如果正在运行不标准的 FTP 软件，则可能会收到该错误消息。
503	命令顺序错误。如果正在运行不标准的 FTP 软件，则可能会收到该错误消息。

错误代码	描述
504	未针对该参数执行命令。如果正在运行不标准的 FTP 软件，则可能会收到该错误消息。
530	用户未登录。验证您是否使用了有效的用户名和密码执行 FTP 操作。您可以在“修改测试”页面上指定其他用户名和密码。有关详细信息，请参阅“FTP 测试”。
532	存储文件需要帐户。验证您用于测试的用户帐户是否可以在 FTP 服务器上存储文件。
550	请求的操作未执行。文件不可用。如果未找到该文件，或者服务没有对该文件的访问权限，则可能会收到该错误消息。
552	请求的文件操作已中止。已超出存储空间分配。验证 FTP 服务器是否具有足够的存储空间用于您正尝试执行的操作。
553	请求的操作未执行。文件名非法。验证对于正在尝试执行的 FTP 操作，所使用文件的文件名是否正确。

HTTP/HTTPS 测试错误代码

错误代码	描述
1	指定的 URL 无效。您可以在“修改测试”页面上指定其他 URL。有关详细信息，请参阅“HTTP 测试”或“HTTPS 测试”。
2	URL 包含错误的协议：它使用 http://，而不是 https://。您可以在“修改测试”页面上指定其他 URL。有关详细信息，请参阅“HTTPS 测试”。
3	发送请求时出错。该错误可能表示您正在使用 SRM 不支持的非标准 HTTP 服务器。
4	读取 HTTP 状态代码时出错。该错误可能表示您正在使用 SRM 不支持的非标准 HTTP 服务器。
5	检索 HTTP 头时出错。该错误可能表示您正在使用 SRM 不支持的非标准 HTTP 服务器。
6	检索 HTTP 内容时出错。该错误可能表示您正在使用 SRM 不支持的非标准 HTTP 服务器。
7	解析文档时出错。该错误可能表示您正在使用 SRM 不支持的非标准 HTTP 服务器。
8	指定的最大深度无效。您可以在“修改测试”页面上指定其他深度。有关详细信息，请参阅“HTTP 测试”或“HTTPS 测试”。

错误代码	描述
20	跟踪链接时未找到主机。该错误表示您正在测试的站点上存在问题。
21	跟踪链接时的协议无效。该错误表示您正在测试的网页上存在问题。
400	请求错误。该错误表示您正在测试的 HTTP 页面上存在问题。
401	未经授权。该错误表示您正在测试的站点上存在问题。
402	需进行付款。该错误表示您正在测试的站点上存在问题。
403	已禁止。该错误表示您正在测试的站点上存在问题。
404	找不到。该错误表示您正在查找的位置中不存在请求的网页或内容。该错误可能是由于您正在测试网页出现的问题而导致的，也可能是由于错误的 URL 而导致的。您可以在“修改测试”页面上指定其他 URL。有关详细信息，请参阅“HTTP 测试”或“HTTPS 测试”。
405	方法不允许。该错误表示您正在测试的站点上存在问题。
406	不可接受。该错误表示您正在测试的站点上存在问题。
407	需进行代理身份验证。该错误可能表示您提供的代理用户名或密码错误。验证您使用的是否是有效的帐户。您可以在“修改测试”页面上为代理服务器指定其他用户名和密码。有关详细信息，请参阅“HTTP 测试”或“HTTPS 测试”。
408	请求超时。该错误表示您正在测试的站点上存在问题。
409	冲突。该错误表示您正在测试的站点上存在问题。
410	不再存在。该错误表示您正在测试的站点上存在问题。
411	必须提供长度。该错误表示您正在测试的站点上存在问题。
412	前提条件失败。该错误表示您正在测试的站点上存在问题。
413	请求实体太大。该错误表示您正在测试的站点上存在问题。
414	请求 URL 太大。该错误表示您正在测试的站点上存在问题。
415	不支持介质类型。该错误表示您正在测试的站点上存在问题。
500	服务器错误。该错误表示您正在测试的站点上存在问题。
501	未实施。该错误表示您正在测试的站点上存在问题。
502	网关错误。该错误表示您正在测试的站点上存在问题。
503	资源不足。该错误表示您正在测试的站点上存在问题。
504	网关超时。该错误表示您正在测试的站点上存在问题。

错误代码	描述
505	不支持 HTTP 版本。该错误表示您正在测试的站点上存在问题。

I 至 R 错误代码

IMAP 测试错误代码

错误代码	描述
10	常规错误。有关详细信息，请参阅以下任何错误日志： ■ %SystemRoot%\windows\system32\sysedge.log（Windows 系统）或系统日志文件 (UNIX) ■ *SystemEDGE-install-directory*\sysedge\plugins\svcrsp\jcollector.log (Windows) 或 *SystemEDGE-install-directory*/plugins/svcrsp/jcollector.log (UNIX)
11	无法绑定到套接字。该错误表示您正在测试的邮件服务器上的套接字不可用。
12	套接字在接收时超时。该错误表示您正在测试的邮件服务器上的套接字不可用。
13	登录失败。该错误可能表示 IMAP 邮件服务器出现问题，也可能表示您配置的用户名和密码不正确。您可以在“修改测试”页面上指定其他用户名和密码。有关详细信息，请参阅“IMAP 测试”。
14	选择收件箱失败。该错误可能表示 IMAP 邮件服务器出现问题，也可能表示您为正在测试的帐户配置的用户名和密码不正确。您可以在“修改测试”页面上指定其他用户名和密码。有关详细信息，请参阅“IMAP 测试”。
15	收件箱为空。该错误表示您尚未向测试帐户发送邮件，因此测试无法下载任何电子邮件。重新配置测试电子邮件帐户，以便其包含电子邮件。如果在配置测试时选择了“删除所有邮件”，则必须确保下次运行测试之前将更多的电子邮件发送到帐户。
16	从收件箱读取失败。该错误可能表示 IMAP 邮件服务器出现问题。
17	邮件标记更改失败。该错误表示该电子邮件未根据您执行的操作显示为已读或已删除。请检查 IMAP 邮件服务器的配置。

错误代码	描述
18	邮件删除失败。该错误表示即使您在“修改测试”页面上选择了“删除下载的邮件”，测试也无法删除邮件。请检查 IMAP 邮件服务器的配置。
19	无法通过主题找到邮件。该错误表示邮件服务器无法执行筛选，或者表示您搜索的主题的邮件不存在。请检查 IMAP 邮件服务器和用户帐户。
20	无法连接到服务器。

MAPI 测试错误代码

错误代码	描述
50	参数错误；内部 jcollector 错误。
200	主机名错误。DNS 查找失败。该错误可能表示您在创建测试时提供的 MAPI 服务器名称不正确。您可以在“修改测试”页面上修改名称。有关详细信息，请参阅“MAPI 测试”。
210	MAPI 登录失败。该错误可能表示您在创建测试时提供的用户名或密码不正确。您可以在“修改测试”页面上修改名称。有关详细信息，请参阅“MAPI 测试”。
211	MAPI 注销失败。该错误可能表示 MAPI 服务器出现问题。
220	初始化 MAPI 失败。该错误可能表示 MAPI 服务器出现问题。请检查服务器配置。
221	无法打开用户的邮件存储区。该错误可能表示 MAPI 服务器出现问题。请检查服务器配置。
222	无法打开用户的内容表。该错误可能表示 MAPI 服务器出现问题。请检查服务器配置。
223	无法打开全局邮件存储区表。该错误可能表示 MAPI 服务器出现问题。请检查服务器配置。
224	无法设置搜索列。该错误可能表示 MAPI 服务器出现问题。请检查服务器配置。
225	查询表列失败。该错误可能表示 MAPI 服务器出现问题。请检查服务器配置。
226	无法获取行数。该错误可能表示 MAPI 服务器出现问题。请检查服务器配置。

错误代码	描述
227	无法找到默认接收文件夹。该错误可能表示 MAPI 服务器出现问题。请检查服务器配置。
228	无法打开文件夹。该错误可能表示 MAPI 服务器出现问题。请检查服务器配置。
229	内存分配 (malloc) 失败。请检查服务器配置。
230	邮件存储区为空。该错误可能表示 MAPI 服务器出现问题。请检查服务器配置。
231	无法重置行位置。请检查服务器配置。
240	找不到用户的邮箱。该错误可能表示您在“修改测试”页面上提供的用户名或密码不正确。有关详细信息，请参阅“MAPI 测试”。
241	用户没有要读取的邮件。该错误可能表示您未为测试的帐户创建邮件，也可能表示在测试删除了帐户中所有的邮件后未发送新的邮件。验证测试是否可以下载您发送到该帐户的邮件。有关详细信息，请参阅“MAPI 测试”。
242	找不到邮件。SRM 不搜索特定邮件。该错误可能表示 MAPI 服务器出现问题。请检查服务器配置。
243	测试超时。您可以在“修改测试”页面上设置其他超时值。有关详细信息，请参阅“MAPI 测试”。
250	无法删除邮件。该错误可能表示 MAPI 服务器或用户帐户权限出现问题。请检查 MAPI 服务器设置和用户帐户管理。
260	MAPI 配置文件已存在。该错误可能表示 MAPI 服务器出现问题。请检查服务器配置。
261	无法创建动态配置文件。该错误可能表示 MAPI 服务器出现问题。请检查服务器配置。
262	无法删除动态配置文件。该错误可能表示 MAPI 服务器出现问题。请检查服务器配置。

NIS 测试错误代码

错误代码	描述
1	常规错误。有关详细信息，请参阅以下任何错误日志： ■ %SystemRoot%\windows\system32\sysedge.log（Windows 系统）或系统日志文件 (UNIX) ■ *SystemEDGE-install-directory*\sysedge\plugins\svcrsp\jcollector.log (Windows) 或 *SystemEDGE-install-directory*/plugins/svcrsp/jcollector.log (UNIX)
2	nis.jar 文件可能未安装在 jre/lib/ext 中。请检查 jre/lib/ext 目录。如果 nis.jar 文件不在该目录中，则将其复制到该目录。
3	域可能不正确。您可以在“修改测试”页面上指定其他域名。有关详细信息，请参阅“NIS 测试”。
4	无法找到主机。该错误可以表示您正在查询的 NIS 服务器不可用，也可以表示测试正在使用的服务器名称不正确。您可以在“修改测试”页面上修改 NIS 服务器名称。有关详细信息，请参阅“NIS 测试”。
5	映射文件名可能不正确。您可以在“修改测试”页面上指定其他映射文件。有关详细信息，请参阅“NIS 测试”。

NNTP 测试错误代码

错误代码	描述
400	服务停止。该错误表示该服务器上已停止 NNTP 服务。请检查服务器配置设置。
411	没有此类新闻组。SRM 不会查询特定新闻组，因此该错误表示出现的问题与 SRM 无关。
412	尚未选择新闻组。SRM 不会查询特定新闻组，因此该错误表示出现的问题与 SRM 无关。
420	尚未选择当前的文章。SRM 不会查询特定新闻组，因此该错误表示出现的问题与 SRM 无关。
421	该组中没有下一篇文章。SRM 不会查询特定新闻组，因此该错误表示出现的问题与 SRM 无关。
422	该组中没有上一篇文章。SRM 不会查询特定新闻组，因此该错误表示出现的问题与 SRM 无关。

错误代码	描述
423	该组中没有此文章编号。SRM 不会查询特定新闻组，因此该错误表示出现的问题与 SRM 无关。
430	找不到此类文章。SRM 不会查询特定新闻组，因此该错误表示出现的问题与 SRM 无关。
435	文章不需要；请不要发送。SRM 不会查询特定新闻组，因此该错误表示出现的问题与 SRM 无关。
436	传输失败；请稍后再试。SRM 不会传输 NNTP 测试的数据，因此该错误表示出现的问题与 SRM 无关。
437	文章被拒绝；请不要重试。SRM 不会查询特定新闻组，因此该错误表示出现的问题与 SRM 无关。
440	不允许发布。SRM 不会发布 NNTP 测试的信息，因此该错误表示出现的问题与 SRM 无关。
441	发布失败。SRM 不会发布 NNTP 测试的信息，因此该错误表示出现的问题与 SRM 无关。
500	命令无法识别。该错误可能表示您正在使用 SRM 不支持的非标准 NNTP 服务器。
501	命令语法错误。该错误可能表示您正在使用 SRM 不支持的非标准 NNTP 服务器。
502	访问限制或权限被拒绝。该错误可能表示 NNTP 服务未运行在您在“修改测试”页面上指定的端口上。有关详细信息，请参阅“NNTP 测试”。 该错误也可能表示 NNTP 服务器要求进行登录，而 SRM 测试不执行登录。请检查 NNTP 服务器上的系统设置。
503	程序错误；命令未执行。该错误可能表示您正在使用 SRM 不支持的非标准 NNTP 服务器。

Ping 测试错误代码

错误代码	描述
1	负载为负数。该错误表示您指定用于 ping 测试的负载为无效（负）数字。您可以在“修改测试”页面上修改此值。有关详细信息，请参阅“Ping 测试”。

POP3 测试错误代码

错误代码	描述
{0}	POP3 服务器返回了 +OK。此消息表示查询已运行。它仅起通知作用。
1	POP3 服务器返回了 -ERR。该错误表示查询未运行。有关详细信息，请参阅以下任何错误日志： ■ %SystemRoot%\windows\system32\sysedge.log（Windows 系统）或系统日志文件 (UNIX) ■ *SystemEDGE-install-directory*\sysedge\plugins\svcrsp\jcollector.log (Windows) 或 *SystemEDGE-install-directory*/plugins/svcrsp/jcollector.log (UNIX)
2	POP3 服务器返回了无效响应。该错误表示 SRM 无法识别服务器返回的响应（无论测试成功还是失败）。有关详细信息，请参阅以下任何错误日志： ■ %SystemRoot%\windows\system32\sysedge.log（Windows 系统）或系统日志文件 (UNIX) ■ *SystemEDGE-install-directory*\sysedge\plugins\svcrsp\jcollector.log (Windows) 或 *SystemEDGE-install-directory*/plugins/svcrsp/jcollector.log (UNIX)

重新配置和初始化错误代码

错误代码	描述
101	检测到配置文件中的结构错误。
102	插件的值不等于 svcrsp。
103	无法打开传递的配置文件进行读取。
104	路径的值为空。
105	配置文件解码失败。
106	处理文件时出现未指定的错误。
107	找到了不支持的参数。
108	模式参数的值不是预期的。
109	给定的配置文件不存在。

错误代码	描述
110	启动 Jcollector 失败。
111	给定的 Java 可执行文件缺失。
112	参数的值太长。处理期间将会截短该值。
113	配置文件中不存在版本指示。
114	不支持配置文件的版本。
201	找到了重复的监视器索引（在测试定义块中）。
202	找到了重复的监视器模板定义名称（在监视器模板定义块中）。
203 (1)	参数 monAttribute 的值无效。不是所有的属性都允许被监控。
205 (2)	参数 monOperator 的值无效。
206 (3)	参数 monSeverity 的值无效。
208	监视器模板名称 (monName) 缺失。
209	缺少监视器模板阈值 (monThreshold)。
210	缺少监视器模板运算符 (monOperator)。
211	缺少监视器模板属性 (monAttribute)。
301	找到重复测试索引。
302	测试间隔低于预定义的最小值。系统会将测试间隔调整为预定义的最小值。
303	测试引用了不存在的监视器模板。
304	测试定义中另一个参数的值无效。
305	参数“samples”不允许的值；必须是整数。
306	参数“status”不允许的值。
307	参数“timeout”不允许的值；必须是整数，小于或等于“interval”的值。
308	参数“window”不允许的值；必须是整数。
309	缺少目标属性。
310	缺少测试名称。
311	缺少测试类型。
312	缺少测试索引。
313	测试索引的保留范围无效。

错误代码	描述
314	测试索引无效。

(1) 有效值为以下值之一：

- svcRspTableNumSamples (11)
- svcRspTableTotalLastSample (12)
- svcRspTableTotalMin (13)
- svcRspTableTotalMax (14)
- svcRspTableTotalMean (15)
- svcRspTableTotalVariance (16)
- svcRspTableTotalAvailability (17)
- svcRspTableNameLastSample (18)
- svcRspTableNameMin (19)
- svcRspTableNameMax (20)
- svcRspTableNameMean (21)
- svcRspTableNameVariance (22)
- svcRspTableConnLastSample (23)
- svcRspTableConnMin (24)
- svcRspTableConnMax (25)
- svcRspTableConnMean (26)
- svcRspTableConnVariance (27)
- svcRspTableTranLastSample (28)
- svcRspTableTranMin (29)
- svcRspTableTranMax (30)
- svcRspTableTranMean (31)
- svcRspTableTranVariance (32)
- svcRspTableBytesInLastSample (33)
- svcRspTableBytesOutLastSample (34)
- svcRspTableTotalBytesIn (35)
- svcRspTableTotalBytesOut (36)
- svcRspTableThroughput (37)

(2) 有效值为以下值之一：

- NOP－nop，无操作 (1)
- GT－gt，大于 (2)
- LT－lt，小于 (3)
- GE－ge，大于或等于 (4)
- LE－le，小于或等于 (5)
- EQ－eq，等于 (6)
- NE－ne，不等于 (7)

(3) 有效值为以下值之一：

- NONE－无重要级别（默认值），不会创建监视器 (1)
- WARNING－创建重要级别为 warning 的监视器 (3)
- MINOR－创建重要级别为 minor 的监视器 (4)
- MAJOR－创建重要级别为 major 的监视器 (5)
- CRITICAL－创建重要级别为 critical 的监视器 (6)
- FATAL－创建重要级别为 fatal 的监视器 (7)

S - Z 错误代码

SMTP 测试错误代码

错误代码	描述
3	SMTP 服务器返回无效的响应。该错误表示 SRM 无法识别服务器返回的响应。有关详细信息，请参阅以下任何错误日志： ■ %SystemRoot%\windows\system32\sysedge.log（Windows 系统）或系统日志文件 (UNIX) ■ *SystemEDGE-install-directory*\sysedge\plugins\svcrsp\jcollector.log (Windows) 或 *SystemEDGE-install-directory*/plugins/svcrsp/jcollector.log (UNIX)
421	域服务不可用。关闭传输通道。该错误表示 SMTP 服务器未运行。
432	需要密码转换。该错误表示 SMTP 服务器发生问题。请检查配置设置。（SRM 不提供用于测试 SMTP 服务的密码或用户帐户。）

错误代码	描述
450	未采取请求的邮件操作：邮箱不可用；已拒绝 ATRN 请求。该错误表示您在“修改测试”页面上指定的邮件收件人无效。有关详细信息，请参阅“SMTP 测试”。
451	请求的操作已中止：处理时发生本地错误；无法立即处理 ATRN 请求。该错误表示 SMTP 服务器发生问题。请检查服务器配置设置。
452	未采取请求的操作：系统存储不足。该错误表示 SMTP 服务器没有的足够磁盘空间来存储测试发送的消息。检查可用空间，如有必要，添加更多的磁盘空间，或者将您的测试配置为使用另一台服务器。
453	您没有邮件。这是一则通知消息。SRM 不检查 SMTP 帐户中的邮件。
454	TLS 暂时不可用；请求的身份验证机制需要加密。该错误表示 SMTP 服务器配置发生问题。SRM 不对 SMTP 测试使用身份验证。
458	无法为节点排队消息。该错误表示 SMTP 服务器配置发生问题。
459	不允许“节点”节点：原因。该错误表示 SMTP 服务器配置发生问题。
500	无法识别命令：命令；语法错误。该错误表示您正在使用无法识别 SRM 命令的非标准 SMTP 服务器。
501	语法错误。未允许任何参数。该错误表示您正在使用无法识别 SRM 命令的非标准 SMTP 服务器。
502	命令未执行。该错误表示您正在使用无法识别 SRM 命令的非标准 SMTP 服务器。
503	命令顺序错误。该错误表示您正在使用无法识别 SRM 命令的非标准 SMTP 服务器。
504	未实施命令参数。该错误表示您正在使用无法识别 SRM 命令的非标准 SMTP 服务器。
521	计算机不接受邮件。该错误表示您在“修改测试”页面上指定的邮件收件人无效。有关详细信息，请参阅“SMTP 测试”。
530	必须先发出 STARTTLS 命令；请求的身份验证机制需要加密。该错误表示 SMTP 服务器配置发生问题。SRM 不对 SMTP 测试使用身份验证。
534	身份验证机制太弱。该错误表示 SMTP 服务器配置发生问题。SRM 不对 SMTP 测试使用身份验证。

错误代码	描述
538	请求的身份验证机制需要加密。该错误表示 SMTP 服务器配置发生问题。SRM 不对 SMTP 测试使用身份验证。
550	未采取请求的操作：邮箱不可用。该错误表示您在“修改测试”页面上指定的邮件收件人无效。有关详细信息，请参阅“SMTP 测试”。
551	不是本地用户；请尝试转发路径。该错误表示您在“修改测试”页面上指定的邮件收件人无效。有关详细信息，请参阅“SMTP 测试”。
552	请求的邮件操作已中止：超出存储空间分配。该错误表示需要从“修改测试”页面上指定的邮件收件人帐户中删除邮件。有关详细信息，请参阅“SMTP 测试”。
553	未采取请求的操作：邮箱名称不允许使用。该错误表示您在“修改测试”页面上指定的邮件收件人无效。有关详细信息，请参阅“SMTP 测试”。
554	事务失败。该错误表示您在“修改测试”页面上指定的邮件收件人无效，或者 SMTP 服务器遇到问题。有关详细信息，请参阅“SMTP 测试”并检查您的 SMTP 服务器配置。

SNMP 测试错误代码

错误代码	描述
1	太大。
2	没有此名称。该错误表示您在“修改测试”页面上指定的 OID 不正确。有关详细信息，请参阅“SNMP 测试”。
3	不正确值。该错误表示您正查询的对象返回无效值。这表示您正查询的对象发生问题。
4	只读。该错误表示您正查询的对象为只读型。该消息仅供参考。SRM 不会尝试为 MIB 对象设置值。
5	常规错误。有关详细信息，请参阅以下任何错误日志： ■ %SystemRoot%\windows\system32\sysedge.log (Windows) 或系统日志文件 (UNIX) ■ *SystemEDGE-install-directory*\sysedge\plugins\svcrsp\jcollector.log (Windows) 或 *SystemEDGE-install-directory*/plugins/svcrsp/jcollector.log (UNIX)

错误代码	描述
6	常规错误。有关详细信息，请参阅以下任何错误日志： ■ %SystemRoot%\windows\system32\sysedge.log (Windows) 或系统日志文件 (UNIX) ■ *SystemEDGE-install-directory*\sysedge\plugins\svcrsp\jcollector.log (Windows) 或 *SystemEDGE-install-directory*/plugins/svcrsp/jcollector.log (UNIX)
7	无法绑定到套接字。该错误可能是由于目标系统上注册表的无效权限而导致的。请检查系统配置设置。
8	套接字在接收时超时。该错误可能是由于目标系统上注册表的无效权限而导致的。请检查系统配置设置。
9	无法创建传出数据包。该错误表示 SRM 发生问题。有关详细信息，请参阅系统日志文件：%SystemRoot%\windows\system32\sysedge.log (Windows) 或系统日志文件 (UNIX)。
10	无法对传入数据包解码。该错误表示 SRM 发生问题。有关详细信息，请参阅系统日志文件：%SystemRoot%\windows\system32\sysedge.log (Windows) 或系统日志文件 (UNIX)。

SQL 查询测试错误代码

错误代码	描述
1	常规错误。有关详细信息，请参阅以下任何错误日志： ■ %SystemRoot%*windows**system32**sysedge.log* (Windows) 或系统日志文件 (UNIX) ■ *SystemEDGE-install-directory*\sysedge\plugins\svcrsp\jcollector.log (Windows) 或 *SystemEDGE-install-directory*/plugins/svcrsp/jcollector.log (UNIX)
2	JDBC 驱动程序可能未安装在 jre/lib/ext 中。验证您的数据库的 JDBC 驱动程序是否存在于 jre/lib/ext 目录中。如果不存在，则将其复制到该目录中。

错误代码	描述
3	发生 Java SLQ 异常。有关详细信息，请参阅 jcollector.log 文件，该文件位于 *SystemEDGE-install-directory*\sysedge\plugins\svcrsp (Windows) 或 *SystemEDGE-install-directory/*plugins/svcrsp 目录 (UNIX)

TFTP 测试错误代码

错误代码	描述
1	常规错误。有关详细信息，请参阅以下任何错误日志： ■ %SystemRoot%\windows\system32\sysedge.log (Windows) 或系统日志文件 (UNIX) ■ *SystemEDGE-install-directory*\sysedge\plugins\svcrsp\jcollector.log (Windows) 或 *SystemEDGE-install-directory/*plugins/svcrsp/jcollector.log (UNIX)
2	套接字在接收时超时。该错误可能是由于目标系统上注册表的无效权限而导致的。请检查系统配置设置。
3	TFTP 客户端上的操作失败。该错误表示在“修改测试”页面上指定的要读或写的文件的路径不正确，或者 TFTP 服务器上的配置不正确。有关详细信息，请参阅“TFTP 测试”，或检查 TFTP 服务器上的系统配置设置。

虚拟用户测试错误代码

错误代码	描述
300	无法获取进程内标识。该错误表示 SRM 无法与应运行测试的系统进行通信。可能是服务可用性发生问题，请尝试以其他用户身份登录。有关详细信息，请参阅以下任何错误日志： ■ %SystemRoot%\windows\system32\sysedge.log ■ *SystemEDGE-install-directory*\sysedge\plugins\svcrsp\sarunas.log ■ *SystemEDGE-install-directory*\sysedge\plugins\svcrsp\jcollector.log

错误代码	描述
301	无法调整内标识权限。该错误表示 SRM 无法与应运行测试的系统进行通信。有关详细信息，请参阅以下任何错误日志： ■ %SystemRoot%\windows\system32\sysedge.log ■ *SystemEDGE-install-directory*\sysedge\plugins\svcrsp\sarunas.log ■ *SystemEDGE-install-directory*\sysedge\plugins\svcrsp\jcollector.log
302	无法以用户身份登录。该错误表示 sarunas.exe 文件未安装在 *drive*:sysedge\plugins\svcrsp\sarunas.log 目录中，或者您在“修改测试”页面上指定的用户名或密码不正确。有关详细信息，请参阅“虚拟用户测试”和 *SystemEDGE-install-directory*\sysedge\plugins\svcrsp\sarunas.log 文件。
303	无法授予用户桌面访问权。该错误表示您没有启用 SNMP 与桌面进行交互。有关详细信息，请参阅“启用 SNMP 服务与桌面进行交互”。
304	进程创建失败。有关详细信息，请参阅以下任何错误日志： ■ %SystemRoot%*windows**system32**sysedge.log* ■ *SystemEDGE-install-directory*\sysedge\plugins\svcrsp\sarunas.log ■ *SystemEDGE-install-directory*\sysedge\plugins\svcrsp\jcollector.log

结果字段

“结果字段”显示不同类型的数据，具体取决于您正在运行的测试的类型和“错误代码”列的信息。下表描述使用“结果字段”的测试，以及在列中为每个测试显示的信息类型。

测试类型	在“结果字段列”中显示的信息
自定义	从自定义测试脚本返回的第四个参数。（前三个参数是 DNS 解析时间、连接时间和事务处理时间。）
HTTP 和 HTTPS	如果测试为“搜索表达式”指定值，则该字段提供该测试匹配目标页面上的搜索表达式的次数。
虚拟用户	如果“错误代码”字段的值是 2，则该字段表示 taskexec.exe 应用程序返回的退出代码。

索引

A

A 至 H 错误代码 - 268
Active Directory 测试 - 60

C

CA Technologies 产品引用 - 4

D

DHCP 测试 - 65
DNS 测试 - 66

F

FTP 测试 - 74

H

HTTP 测试 - 76
HTTPS 测试 - 81

I

I 至 R 错误代码 - 273
IMAP 测试 - 84

L

LDAP 测试 - 86

M

MAPI 测试 - 89

N

NIS/NIS+ 测试 - 93
NNTP 测试 - 95

P

ping 测试 - 97
POP3 测试 - 98

S

S - Z 错误代码 - 281
SMTP 测试 - 104
SNMP 测试 - 107
SQL 查询测试 - 112
svcwatch add adir 命令-添加 Active Directory 测试 - 136
svcwatch add custom 命令-添加自定义测试 - 141
svcwatch add dhcp 命令-添加 DHCP 测试 - 146
svcwatch add dns 命令-添加 DNS 测试 - 151
svcwatch add fileio 命令-添加文件 IO 测试 - 156
svcwatch add ftp 命令-添加 FTP 测试 - 161
svcwatch add http | https 命令-添加 HTTP 或 HTTPS 测试 - 166
svcwatch add imap 命令-添加 IMAP 测试 - 172
svcwatch add ldap 命令-添加 LDAP 测试 - 177
svcwatch add mapi 命令-添加 MAPI 测试 - 182
svcwatch add nis 命令-添加 NIS 测试 - 188
svcwatch add nntp 命令-添加 NNTP 测试 - 193
svcwatch add ping 命令-添加 PING 测试 - 198
svcwatch add pop3 命令-添加 POP3 测试 - 203
svcwatch add rtemail 命令-添加往返电子邮件测试 - 208
svcwatch add smtp 命令-添加 SMTP 测试 - 214
svcwatch add snmp 命令-添加 SNMP 测试 - 219
svcwatch add sql 命令-添加 SQL 测试 - 225
svcwatch add tcpconnect 命令-添加 TCP 连接测试 - 231
svcwatch add tftp 命令-添加 TFTP 测试 - 236
svcwatch add vuser 命令—添加虚拟用户测试 - 241
svcwatch delete 命令-删除测试 - 246
svcwatch list 命令-查看测试信息 - 249
svcwatch setstatus 命令-更改测试状态 - 252
svcwatch version 命令-查看 SRM 版本信息 - 255

T

TCP 连接测试 - 117
TFTP 测试 - 119

四划

从 Linux 或 UNIX 上卸载 - 263
从 Windows 上卸载 - 262
升级 - 262
文件 I/O 测试 - 68
文件 I/O 测试错误代码 - 37
文件加密 - 18

五划

功能特征 - 13
示例：向 SRM AIM 应用文件 I/O 测试 - 20

六划

全局参数块 - 42
创建文件 I/O 测试以比较两个文件的内容 - 28
创建文件 I/O 测试以对文件执行读写操作 - 26
创建文件 I/O 测试以向文件执行写入 - 24
创建文件 I/O 测试以读取文件 - 22
创建测试 - 57
在可用性表中保留行 - 19
安装 - 259
约定 - 10
自定义测试 - 63

七划

体系结构 - 15
远程部署 - 259

八划

使用自定义脚本创建测试 - 131
单个安装 - 261
往返电子邮件测试 - 100
性能度量标准 - 19
抽样配置文件 - 53
服务响应监视器 CLI 命令 - 135
范围 - 9

九划

测试定义参数块 - 45
测试的关键字 - 126
测试表信息 - 16
测试管理 - 57
相关出版物 - 9
选项和参数 - 60

十划

监视器模板定义参数块 - 50
读者 - 9
通过 CA Virtual Assurance 设置的安装 - 259
通过 CLI 创建、运行和应用文件 I/O 测试 - 32
通过 UI 创建文件 I/O 测试 - 22
通过 UI 应用文件 I/O 测试 - 30
配置 - 39

十一划

常规错误代码 - 267
控制文件处理 - 18
虚拟用户测试 - 122

十二划

确定配置文件 I/O 测试的方法 - 21
编辑控制文件 - 39
联系技术支持 - 4

十三划

概述 - 13
简介 - 9
错误代码 - 265
错误代码概述 - 265