HP Server Automation

Ultimate 版

软件版本：10.10

用户指南：审核与符合性

文档发布日期：2014 年 6 月 30 日
软件发布日期：2014 年 6 月 30 日

法律声明

担保

HP 产品和服务的唯一担保已在此类产品和服务随附的明示担保声明中提出。此处的任何内容均不构成额外担保。 HP 不会为此处出现的技术或编辑错误或遗漏承担任何责任。

此处所含信息如有更改，恕不另行通知。

受限权利声明

机密计算机软件。必须拥有 HP 授予的有效许可证，方可拥有、使用或复制本软件。按照 FAR 12.211 和 12.212，并根据供应商的标准商业许可的规定，商业计算机软件、计算机软件文档与商品技术数据授权给美国政府使用。

版权声明

商标声明

Adobe® 是 Adobe Systems Incorporated 的商标。

Intel® 和 Itanium® 是 Intel Corporation 在美国和其他国家 / 地区的商标。

Microsoft®、 Windows®、 Windows® XP 是 Microsoft Corporation 在美国的注册商标。

Oracle 和 Java 是 Oracle 和 / 或其附属公司的注册商标。

UNIX® 是 The Open Group 的注册商标。

支持

请访问 HP 软件联机支持网站：

http://www.hp.com/go/hpsoftwaresupport

此网站提供了联系信息，以及有关 HP 软件提供的产品、服务和支持的详细信息。

HP 软件联机支持提供客户自助解决功能。通过该联机支持，可快速高效地访问用于管理业务的各种交互式技术支持工具。作为尊贵的支持客户，您可以通过该支持网站获得下列支持：

- 搜索感兴趣的知识文档
- 提交并跟踪支持案例和改进请求
- 下载软件修补程序
- 管理支持合同
- 查找 HP 支持联系人
- 查看有关可用服务的信息
- 参与其他软件客户的讨论
- 研究和注册软件培训

大多数提供支持的区域都要求您注册为 HP Passport 用户再登录，很多区域还要求用户提供支持合同。要注册 HP Passport ID，请访问：

http://h20229.www2.hp.com/passport-registration.html

要查找有关访问级别的详细信息，请访问：

http://h20230.www2.hp.com/new_access_levels.jsp

支持列表

有关完整的支持和兼容性信息，请参见相关产品发布的支持列表。可在 HP 软件联机支持网站上查找所有支持列表和产品手册，地址为：

http://h20230.www2.hp.com/sc/support_matrices.jsp

您还可以从 HP 软件联机支持产品手册网站下载此发布的 《HP Server Automation Support and Compatibility Matrix》，地址为：

http://h20230.www2.hp.com/selfsolve/manuals

文档更新

适用于此发布的所有最新 Server Automation 产品文档都位于以下 SA 文档库中：

http://support.openview.hp.com/selfsolve/document/KM00417675/binary/SA_10_docLibrary.html

使用 SA 文档库可以访问与此发布相关的任何指南、发行说明、支持列表和白皮书，还能够以捆绑包的形式下载整个文档集。SA 文档库按每次发布进行更新，并且每当更新了发行说明或引入了新白皮书时，也会更新 SA 文档库。

如何查找信息资源

使用下列任一方法，可以访问 Server Automation 的信息资源：

方法 1：在新 SA 文档库中按标题和版本访问最新的各个文档

方法 2：在下载了所有手册的本地目录中，使用完整的文档集

方法 3：在 HP 软件文档门户中搜索任何受支持发布的任何 HP 产品文档

访问各个文档：

1. 访问 SA 10.x 文档库：

   http://support.openview.hp.com/selfsolve/document/KM00417675/binary/SA_10_docLibrary.html

2. 使用您的 HP Passport 凭据登录。
3. 找到所需的文档标题和版本，然后单击 “go”。

在本地目录中使用完整的文档集：

1 要将完整的文档集下载到本地目录，请执行以下操作：

a 访问 SA 文档库：

http://support.openview.hp.com/selfsolve/document/KM00417675/binary/SA_10_docLibrary.html

b 使用您的 HP Passport 凭据登录。

c 找到对应于 SA 10.1 版本的所有手册下载标题。

d 单击 “go” 链接，将 ZIP 文件下载到本地目录。

e 解压缩该文件。

2 要在本地目录中查找文档，请使用文档目录 (docCatalog.html)，它提供了一个指向本地目录中已下载文档的索引门户。

3 要在文档集的所有文档中搜索关键字，请执行以下操作：

a 打开本地目录中的任何 PDF 文档。

b 选择 “Edit” > “Advanced Search”（或按 Shift+Ctrl_F）。

c 选择 “All PDF Documents” 选项，并浏览本地目录。

d 输入关键字，然后单击 “Search”。

在 HP 软件文档门户中查找更多文档：

访问 HP 软件文档门户：

http://h20230.www2.hp.com/selfsolve/manuals

需要注册 HP Passport 才能登录此站点。要注册 HP Passport ID，请单击 “HP Passport” 登录页面上的 **“New users - please register”** 链接。

此外，如果订阅了相应的产品支持服务，则还会收到更新的版本或新版本。有关详细信息，请与您的 HP 销售代表联系。有关任何版本的列表，请参见 “文档变更说明”。

产品版本

Server Automation 有两种版本：

- Server Automation (SA) 是 Server Automation Ultimate 版。有关 Server Automation 的信息，请参见 《SA Release Notes》、《SA 用户指南：Server Automation》。
- Server Automation Virtual Appliance (SAVA) 是 Server Automation Premium 版。有关 SAVA 所包括内容的详细信息，请参见 《SAVA Release Notes》和 《SAVA 概览》指南。

目录

1 审核和修正概述

在 HP Server Automation (SA) 中，使用审核和修正可识别在 IT 环境中要检查的对象、检查这些对象的位置和检查时间。

- *审核策略* 定义要检查的内容 - 例如文件、目录、配置值等。
- *审核* 定义要检查的位置 - 例如服务器或多个服务器。
- *审核 计划* 定义何时检查 - 例如一次性作业或重复作业。

这些功能将帮助您了解如何使托管服务器环境以及服务器符合要求。在 SA 中，可以定义服务器配置策略，以便确保设施中的服务器符合这些策略标准。如果发现服务器 *不符合要求*（未按所需的方式配置），可以对其进行修正以符合组织标准。

通过使用 SA 客户端，可以基于自定义值或预配置的审核策略来审核基于活动服务器或服务器快照的服务器配置值。此外，还可以创建服务器配置快照，以捕获系统的当前状态，以便将其他服务器与已知基线进行比较。

通过使用审核策略，可定义公司或行业范围内的符合性标准，然后可将这些标准用于审核、快照规范和其他审核策略中。引用审核或快照规范中的审核策略可帮助您更新组织中的最新符合性定义。

最佳实践：如果已订阅 BSA Essentials 订阅服务，则可以根据数据中心需求，及时了解最新的行业符合性标准。例如，通过订阅服务可获取定期更新的最佳安全实践，如 Internet 安全中心 (CIS)、支付卡行业 (PCI) 等。也可获取其他免费的非订阅内容，例如适用于 Server Automation 的 Microsoft Patch Supplement。通过 BSA Essentials 订阅服务，可获取最新的管理符合性策略，如联邦信息安全管理法案 (FISMA)、萨班斯 - 奥克斯利法案以及每日漏洞警报。可加入 HP Live Network (HPLN) 门户上的内容开发者社区，分享和访问自定义创建的审核策略和规则。有关订阅 BSA Essentials 订阅服务的信息，请与您的销售代表联系。

有关审核和修正所支持的操作系统的详细信息，请参见 《SA Support and Compatibility Matrix》。

术语

以下列表定义了在 HP Server Automation 审核和修正中使用的重要术语和概念：

- **存档的审核结果 / 快照**：通过存档审核结果和快照，可以将其从审核结果或快照列表中移出并使其可用作历史记录。
- **审核**：表达托管服务器配置对象 （如服务器的文件系统目录结构或文件、服务器的 Windows 注册表、应用程序配置等）所需状态的规则集 （可能含有单个*检查*）。审核还包含*源* （服务器、快照或快照规范）、*目标* （服务器或快照）、*规则异常* 和计划。

  审核规则可链接到审核策略，这意味着审核中的规则将替代审核策略中的规则。运行审核可将服务器配置对象值与*黄金服务器*、服务器快照或用户定义值进行基线比较，从而确定值的差异程度。当审核报告服务器或用户输入值之间存在差异时，可通过安装软件和服务器对象修正这些差异，以使服务器符合审核规则。
- **审核作业**：运行审核时发生的进程。审核作业可立即一次性运行或通过计划作业而重复运行。审核作业完成后，将生成报告差异的审核结果。
- **审核规则类型**：审核可包含以下规则类型：
  - **比较**：将服务器配置或快照的服务器配置与其他托管服务器或快照进行比较的规则。
  - **基于值 (用户定义)**：比较一个或多个用户定义的值集的规则。此审核类型包括链接到审核策略的审核。
  - **不存在：**检查对象是否不存在，以确定该对象是否在目标服务器上不存在。如果该对象在目标服务器上存在，则该规则不符合要求。请注意，在运行时不会查询源服务器 （如果有）。此外，如果选择了通配符规则对象，则将仅应用于目标服务器。
- **审核策略**：定义服务器所需配置的规则集合。审核可通过以下方式使用策略：
  - **链接**：链接的策略可在审核和策略之间保持持久连接。这意味着审核中的规则正是审核策略中的规则，如果对策略进行任何更新，则最新更改也会反映到策略所链接的审核中。当审核策略链接到审核或快照规范时，规则将在审核或快照规范内显示为只读。审核策略内的规则仍旧可编辑。
  - **导入 (替换、无链接)**：将策略导入到审核时，审核和审核策略之间的链接将不复存在。因此，可在不影响策略的情况下更改审核。相反，对策略进行的任何更改或更新都不会在审核中有所反映。
  - **导入 (合并)**：将审核策略导入审核并与审核合并时，审核策略的规则将添加到审核中当前已存在的规则。在审核与审核策略间将不再具有持久链接。合并过程中，如果发现有冲突的规则，则从审核策略中新导入的规则将替换审核中的规则。
- **审核结果**：运行审核的结果。审核结果的信息将显示目标服务器或服务器组的配置对象值与审核中定义的值是如何匹配或不匹配的。

- **异常**：已排除或禁用的服务器和特定规则，这样当审核运行时，将不针对规则异常对选定服务器进行检查。确定审核符合性时，将此服务器排除在外。
- **符合性**：服务器配置对某检查或测试的符合程度。该检查或测试在审核、快照规范或审核策略中定义的规则集中创建。审核和修正中的符合性由指定目标服务器期望值的审核规则或快照规则定义。如果目标服务器上的值与审核规则中指定的值不同，则该服务器认定为 “不符合”。
- **策略设置员**：负责定义组织的服务器配置符合性标准（服务器应配置的方式）和审核策略的用户。
- **规则**：一项在特定服务器配置对象上进行且包含所需值和可选修正值的*检查*。

  以下是两种规则类型：

  — **基于服务器的规则**：直接派生自源服务器

  — **用户定义的规则**：由用户创建

  如果已订阅 BSA Essentials 订阅服务，则可以获取用于定义各种行业符合性标准的预定义规则，例如 Microsoft Windows 的最新修补程序补充、当前管理符合性策略 （例如 FISMA、萨班斯 - 奥克斯利法案）、来自 EP 开发者社区的用户创建规则、每日漏洞内容更新等。
- **服务器对象**：要应用审核或快照规范的服务器的对象。该对象可以是值（如最小密码长度），也可以是对象 （如文件或目录、注册表条目、 Windows 服务硬件配置等）。
- **快照**：在特定日期、特定时间捕获托管服务器信息时，托管服务器配置状态的一种表现形式。快照由快照规范作业的运行而产生。
- **快照规范**：审核的源。通常将其称之为*反射审核*。当从快照规范运行审核时，审核将使用在该规范中定义的所有信息，然后应用已定义的任意筛选器。
- **快照规范作业**：运行快照规范时发生的进程。快照作业可一次性运行或通过计划作业而重复运行。快照规范作业完成时，将产生快照。
- **目标**：对其运行审核或获取快照的服务器。审核的目标可以是一个服务器、多个服务器、服务器组或快照。快照的目标也可以是其他服务器。

服务器配置

以下最佳实践和示例阐明了 SA 帮助您管理设施中服务器配置的方式：

- 强制实施安全标准
- 捕获和复制黄金服务器

强制实施安全标准

IT 组织通常具有必须实施的安全策略。这些策略验证服务器的配置是否正确且是否得到免受安全性攻击的保护。策略设置员可创建审核策略，强制实施这些安全标准。预定义审核策略可链接到多个审核或快照规范。管理活动服务器的管理员可通过引用正确的审核策略来确保这些服务器按正确的方式进行审核。

示例：您的公司具有 Solaris 10 服务器，其必须具有由通用漏洞与披露 (CVE) 指定的最新已知安全漏洞。公司希望确保这些服务器不易受到针对 Solaris 10 的已知威胁的攻击，例如 CVE-2009-0168 (CVSS 4.9)，其在 Sun Solaris 10 和 OpenSolaris snv_61 至 snv_106 中检查在 PPD 文件管理器 (ppdmgr) 中未指明的漏洞。通过订阅 BSA Essentials 订阅服务，可在线访问符合性检查集合。可使用这些检查审核您的 Solaris 10 服务器并验证它们是否存在这种安全漏洞风险。负责定义组织符合性标准的系统管理员可创建包含 CVE-2009-0168 符合性检查的审核策略。

最佳实践：负责管理 Solaris 服务器的系统管理员可为其服务器创建审核，然后将其审核规则链接到此审核策略。当审核链接到审核策略时，对该策略进行的任何更改都会立即在该审核中反映出来。因此，在服务器上运行审核的人员会知道这些审核规则始终是最新的。例如，如果有适用于 Solaris 10 服务器的新 CVE 更新，则策略设置员将更新此策略，所有链接到此策略的审核都将具有最新的符合性检查。在知道其审核会始终包含最新漏洞检查的情况下，策略设置员可将审核计划为定期运行，以检查其管理的所有 Solaris 10 服务器。如果审核结果显示任何目标服务器不包含新 CVE 安全检查，则将对这些服务器进行修正以解决该问题。

捕获和复制黄金服务器

有时会按以下方式配置服务器：该配置在您的设施中表示针对特定目的的服务器配置的理想状态。例如，如果要设置处理 Web 流量的服务器集合，则可以为 Web 服务器组配置表示理想配置（*黄金服务器*配置）的单个服务器。配置黄金服务器后，可将其配置复制到整个 SA 托管服务器组中。

示例：您有一个 Red Hat Linux 服务器，其具有 Apache Web 服务器的唯一配置。您要将此精确配置复制到其他几个托管服务器。使用审核和修正，您可以创建一个将黄金服务器用作源配置的审核。在此审核中，您选择要用于审核其他服务器的配置，如应用程序策略和特定的应用程序配置规则。将这些服务器选作该审核的目标，以按照黄金服务器进行配置。在审核运行后，可以对与黄金服务器不匹配的任何目标服务器配置进行修正。可以将此审核计划为定期运行。如果任何服务器不符合要求，则在其与黄金服务器不匹配时对其进行修正。

2 审核、审核策略和审核结果

审核

*审核*定义了一组规则或配置值，用于确定托管服务器或托管服务器组的配置是否符合您组织的符合性标准。审核规则可以临时配置，也可以引用专门定义 HP Server Automation 中托管服务器所需配置的预定义审核策略，进行更有效地配置。

审核可以：

- 将服务器配置与审核策略中定义的规则进行比较。
- 检查配置值是否满足审核规则中指定的条件。
- 进行检查以确保特定值存在或不存在。

使用某些审核规则，还可运行脚本捕获更详细的配置信息。

最佳实践：可将审核策略定义为：

- 识别 IIS 元数据库值是否存在，尤其当不希望该值存在时。
- 确保特定 Linux 服务设置为始终运行，尤其当出于安全考虑，服务必须作为关键服务始终运行时。
- 确定某特定文件系统目录是否未超出特定的大小限制。
- 确保未超出用户密码最大长度设置。

可以定义审核应查找的内容、期望在服务器上找到的值以及在发现差异时用于修正差异的替换值。

配置后，审核可运行一次、可按计划在将来运行或计划为定期运行。审核运行后，其结果将指示这些服务器对审核规则中定义集的符合程度。发现差异时，可通过修正这些服务器使之符合要求。

审核策略

*审核策略*是用于定义服务器配置所需状态的可重用规则集合，其基于行业标准和组织设定的符合性目标。审核策略可链接到审核、快照规范和其他审核策略。更改审核策略时，所有对该审核策略的引用也会随之更新。

审核策略通常由策略设置员创建，策略设置员了解公司为要求服务器满足特定配置域和操作系统而制定的合规性标准。通过将预定义审核策略链接到审核或快照规范，管理服务器的管理员可使用这些策略。如果对审核策略进行了任何更改，则链接到该策略的审核也将包含更新的规则。审核 SA 托管服务器的管理员可确保他们的审核将始终反映组织中最新的策略标准。

快照

*快照*是在特定日期、特定时间捕获托管服务器信息时，托管服务器配置状态的一种表现形式。快照对于捕获*黄金服务器*（即与设施中其他服务器比较时用作基准的服务器）的配置非常有用。可将快照用作审核的源。如果服务器与快照中捕获的配置不匹配，则可在运行审核后修正这些服务器。

符合性和修正

使用 SA 客户端中的 “符合性”视图，可查看设施中 SA 托管服务器的总体符合性级别。“符合性”视图也称为*符合性图表板*。在符合性图表板上，可以识别符合性问题，并随后对其进行修正。

审核管理

*审核*是可用于定义服务器配置中应存在或不应存在的内容的规则集合。审核包括规则、源、目标服务器和用于定义审核运行时间和运行方式的计划。

使用审核规则，可定义和检查托管服务器上各种配置或对象以及文件的状态，如服务器文件系统的状态、注册表设置、安装和注册的软件 （修补程序和程序包）、事件、软件、应用程序配置、操作系统设置等。

注意：如果目标服务器上的配置或对象与审核规则中定义的状态不同，或源服务器中存在的对象或规则在目标服务器中不存在，则认为该规则 “不符合”。

例如，如果只将组或用户添加到了源服务器，而没有添加到目标服务器，则将无法成功运行审核或修正。如果只在源服务器中更改注册表设置，而不在目标服务器中更改，也会出现错误。

查看审核结果时，可以修正对象配置以确保目标服务器的配置符合所需配置的要求。

可以为单个服务器、多个服务器或其他服务器快照审核服务器配置值。可以计划审核立即运行或按重复计划运行，并在审核完成后发送电子邮件通知。还可以取消正在运行的审核作业。

审核比较类型

通常情况下，根据审核的源，审核可包含以下几种比较类型：

- **比较**：基于源服务器的配置值或创建该审核时指定的源快照的配置值的审核。该源服务器或服务器快照也称为*黄金服务器*。例如，您可能想在托管服务器之间比较文件目录或文件内容、注册表结构、 IIS 元数据库条目或用户组设置。通过将快照用作审核的源，可以将此快照与设施中的其他服务器进行比较。

“比较”审核可执行以下几种比较类型：

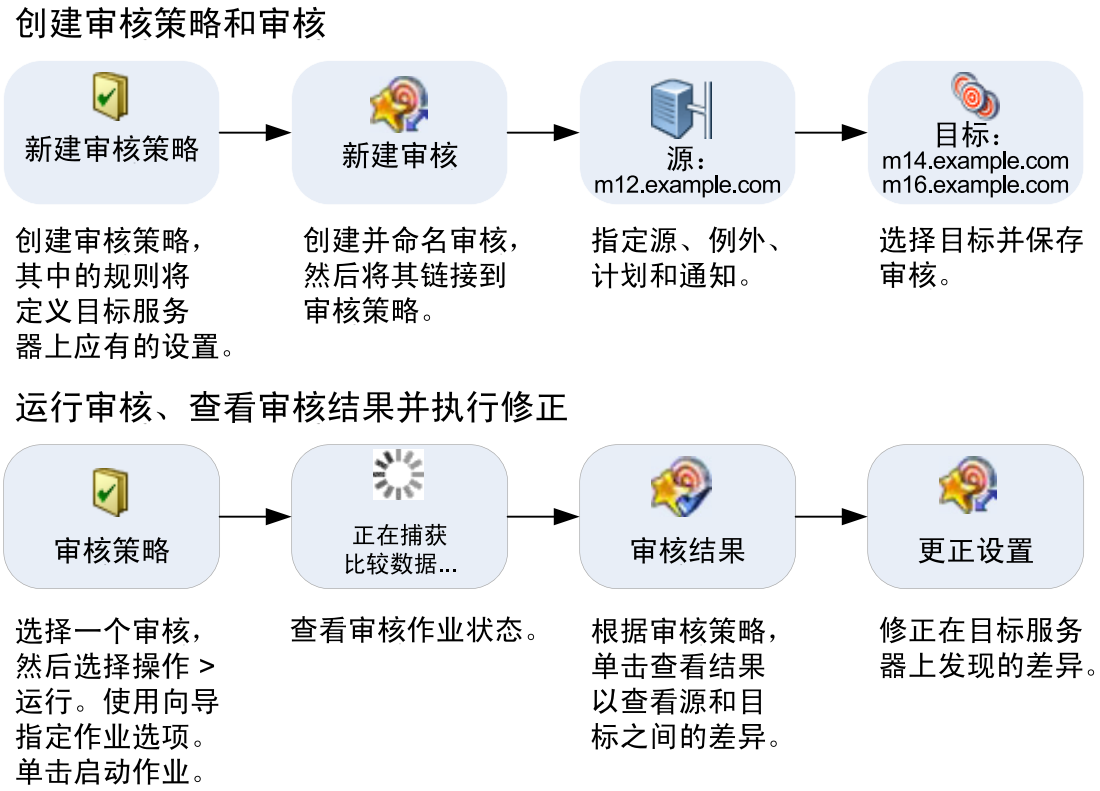
- **属性**：检查选定对象或对象配置的属性。例如，可以在目标服务器或多个务器上检查修补程序的发布版本，以确保它即是您要在目标上安装的修补程序。可以根据源服务器或快照选择版本号或添加您自己的值。
- **等价性**：进行检查以确定目标服务器与审核的源服务器或快照的配置相同。例如，可以进行检查以查看审核目标的用户组是否与从源服务器选择的组相同。
- **不存在**：检查对象是否不存在，以确定该对象是否在目标服务器上不存在。如果该对象在目标服务器上存在，则该规则不符合要求。例如，可以检查服务器以确保该服务器不包含特定 COM+ 对象。请注意，在运行时不会查询源服务器 （如果有）。此外，如果选择了通配符规则对象，则将仅应用于目标服务器。

- **基于值 (用户定义)**：基于每个服务器对象 （文件系统、 Windows 服务、 ISS 元数据库、用户和组等）的自定义、用户定义值的审核。这些值可派生自源服务器、 SA 特性或自定义特性。这种审核根据审核策略选择是否包含这些值。在审核策略中，策略设置员根据公司或行业符合性标准预定义每个配置对象的值。

审核进程

图 1 显示了审核的进程，包括每一步的描述。

图 1　　审核进程



审核元素

审核包括以下元素：

- **属性**：审核的名称和描述。
- **源**：审核的源可以是服务器、快照或根本没有源。但是，有些规则需要源。
  - 通过将服务器选为审核源，可以从该服务器中选择服务器对象作为审核基础。
  - 通过将快照选为审核源，可以使用快照的配置值。
  - 通过将快照规范选为源，可以随着时间审核服务器自身。

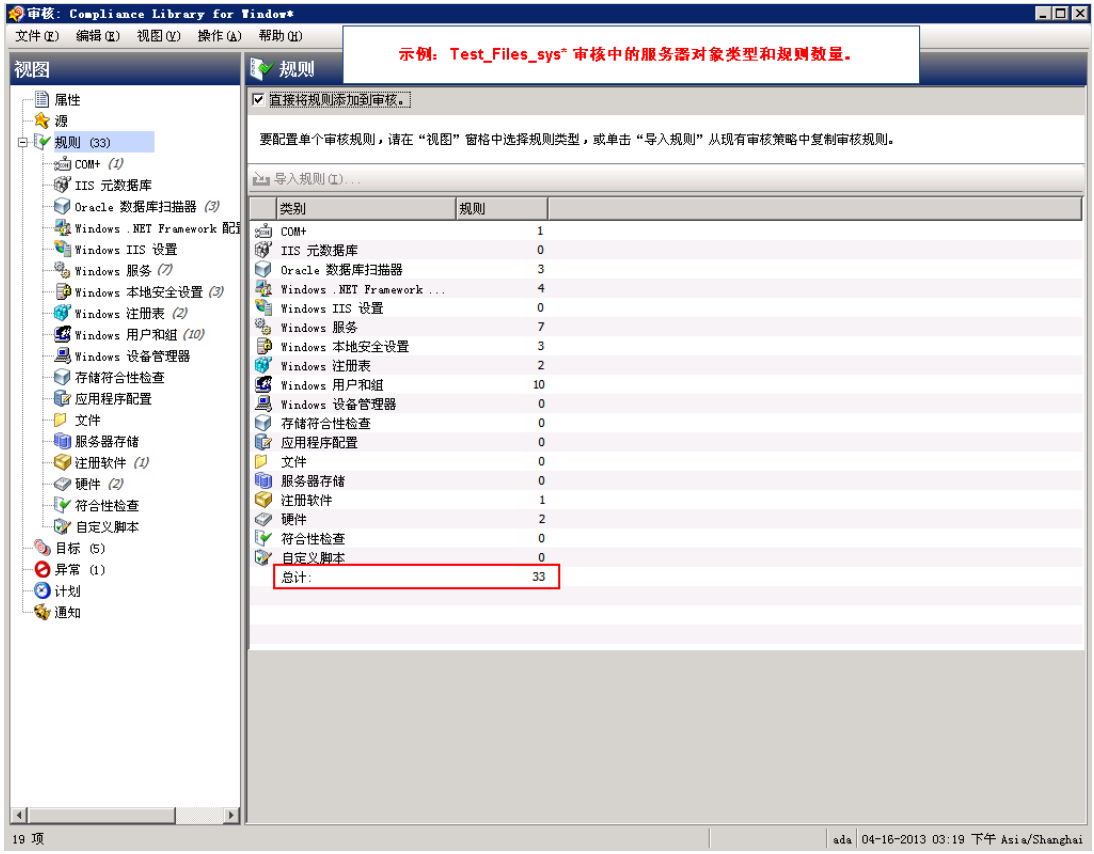
  例如，如果创建了一个服务器快照，然后将此快照规范用作审核的源，则每次运行审核时，都可以通过使用重复审核计划，将服务器的原始状态与其一段时间后的实际配置进行比较。如果选择无源，则仅可以定义审核或快照的自定义值。
- **规则**：一项使用所需值和可选修正值在特定服务器对象上进行的检查。例如，您可能要查看此服务器是否含有特定 Windows 服务，如果找到，则确定该服务是否已关闭。请参见服务器对象（第 33 页）。
- **目标**：审核将检查符合性的服务器。可以根据需要为审核或快照选择多个服务器或服务器组。

VMware ESXi 服务器不能作为审核或快照的目标。

- **异常**：审核运行时将不进行符合性检查的服务器和特定规则。
- **计划**：可以运行审核一次，或按重复计划运行审核。按重复计划运行的审核会在符合性图表板中作为单个符合性列显示。
- **通知**：可在审核完成运行时发送电子邮件，通知的内容有审核作业的成功、失败或完成。

要配置审核，请选择服务器配置对象，然后将规则应用到这些对象，以便定义它们所需的配置状态。例如，图 2 显示了一个含有 33 个定义规则的审核。这些规则用于确定目标服务器配置是否与审核中的规则匹配。

图 2　　审核浏览器显示审核中的对象



创建审核

在 SA 客户端中，可使用几种方法创建审核。

您可以：

- 选择托管服务器作为审核源，以便在单个服务器上运行此审核。

  请参见从服务器创建审核 （第 20 页）。
- 选择托管服务器组作为审核源，以便在该组中的所有服务器上运行此审核。

  请参见从服务器组创建审核 （第 20 页）。
- 从 SA 库创建新审核。

  请参见从 SA 库创建审核 （第 20 页）。
- 根据快照中捕获的服务器配置创建审核。

  请参见从快照创建审核 （第 21 页）。
- 根据审核策略创建审核。

  请参见从审核策略创建审核 （第 21 页）。

从服务器创建审核

当从托管服务器创建新审核时，该审核会将选定服务器用作审核源。可以选择其他服务器或快照作为审核源，或者根本不进行选择而是定义自己的自定义规则。

要审核托管服务器，该服务器必须是可访问的且您必须具有该服务器的访问权限。

要从服务器创建审核，请执行以下操作：

1. 在导航窗格中，选择 “设备” > “服务器” > “所有托管服务器”。
2. 选择服务器。
3. 从 “操作” 菜单，选择 “创建” > “审核” 打开 “审核” 窗口。

   请参见审核配置 （第 29 页）。

从服务器组创建审核

从服务器组创建审核时，审核将评估该组中所有可访问的服务器。但是，审核将仅评估用户有权访问的组中的服务器。

要审核服务器组，请执行以下操作：

1. 在导航窗格中，选择 “设备” > “设备组”。
2. 在内容窗格中，选择 “Public” 或 “专用”。
3. 选择要审核的服务器组。
4. 在内容窗格中选择一组服务器。
5. 从 “操作” 菜单，选择 “创建” > “审核” 打开 “审核” 窗口。

   当通过选择服务器组执行审核时，该服务器组将成为目标。如果审核规则需要源，则必须指定一个源。请参见审核配置 （第 29 页）。

从 SA 库创建审核

要从 SA 库创建审核，请执行以下操作：

1. 在导航窗格中，选择 “库” > “按类型” > “审核和修正”。
2. 在导航窗格中，展开 “审核”。
3. 选择操作系统：Windows 或 Unix。
4. 从 “操作” 菜单中，选择 “新建” 打开 “审核” 窗口。

   请参见审核配置 （第 29 页）。

从快照创建审核

可以在 SA 库中选择任何快照，然后根据此快照中捕获的服务器配置创建审核。此快照将充当审核源；但是从快照创建新审核后，也可以选择其他快照或服务器作为源。

要从快照创建审核，请执行以下操作：

1. 在导航窗格中，选择 “库” > “按类型” > “审核和修正”。
2. 在导航窗格中，展开 “快照规范”。
3. 选择操作系统：Windows 或 Unix。
4. 从 “操作”菜单中，选择 “新建”打开 “快照规范”窗口。

   请参见审核配置 （第 29 页）。

从审核策略创建审核

审核策略设计用于审核。从审核策略创建审核时，审核策略会链接到该审核。当对此审核策略进行更新时，所有更改都会反映到该审核中。

要从审核策略创建审核，请执行以下操作：

1. 在导航窗格中，选择 “库” > “按类型” > “审核和修正”。
2. 在导航窗格中，展开 “审核策略”。
3. 选择操作系统：Windows 或 Unix。
4. 从 “操作”菜单中，选择 “新建”打开 “审核策略”窗口。

   请参见审核配置 （第 29 页）。

运行审核

运行审核将在审核的目标服务器、服务器或快照中执行选定审核。审核将根据审核中定义的规则评估目标。可以从 SA 客户端中的以下位置运行审核：

- 从 SA 库 （第 21 页）
- 从所有托管服务器 （第 22 页）
- 从审核结果 （第 23 页）

从 SA 库

SA 库含有所有可运行的可用审核，这些审核按操作系统组织：Windows 或 Unix。库中的审核列表可通过任意列 （如名称、上次修改日期等）进行排序。搜索工具也可通过输入名称、 ID、审核创建人等用于搜索审核列表。

要从 SA 库运行审核，请执行以下操作：

1. 在导航窗格中，选择 “库” > “按类型” > “审核和修正”。
2. 选择 “审核”，然后选择 “Windows”或 “Unix”。
3. 选择要运行的审核，右键单击并选择 “运行审核”。

4 在 “运行” 窗口，步骤一显示了此审核的名称、源服务器、或审核中使用的快照、此审核中定义的规则总数以及此审核的所有目标 （服务器和快照）。单击 “查看规则详细信息” 可查看规则定义。

（*可选*）如果要立即运行审核，请在进程中的任意点单击 “启动作业”。

5 单击 “下一步”。

6 在 “计划” 页面，选择是否要立即运行或在以后的时间和日期运行该审核。要在以后运行该审核，请选择 “在该时间运行任务” 然后选择日期和时间。

7 单击 “下一步”。

8 在 “通知” 窗口，默认情况下，无论审核作业是否成功，用户都会收到审核完成时发送的通知电子邮件。要添加电子邮件通知者，请单击 “添加通知者”，并输入电子邮件地址。

9 （*可选*）可以指定是否要在审核作业成功或失败时发送该电子邮件。

10 （*可选*）可以在 “工单 ID” 字段中指定凭据跟踪 ID。仅当 SA Professional Services 将 SA 与您的变更控制系统集成时，才能使用 “工单 ID” 字段。否则，应将其留空。

11 单击 “下一步”。

12 在 “作业状态” 页中，单击 “启动作业” 运行审核。如果审核已运行，单击 “查看结果” 可查看审核的结果。

从所有托管服务器

如果服务器正用作审核的目标，则可以从此位置运行审核。

要从 “所有托管服务器” 列表运行审核，请执行以下操作：

1 在导航窗格中，选择 “设备” > “服务器” > “所有托管服务器”。

2 选择服务器。

3 从 “视图” 下拉列表中，选择 “审核和修正”。详细信息窗格将在内容窗格下方显示。

4 在详细信息窗格的 “显示” 下拉列表中，选择 “审核 - 服务器是目标”。

5 从列表中选择一个审核，右键单击并选择 “运行审核”。

6 在 “运行” 窗口，步骤一显示了此审核的名称、源服务器、或审核中使用的快照、此审核中定义的规则总数以及此审核的所有目标 （服务器和快照）。单击 “查看规则详细信息” 可查看规则定义。

（*可选*）如果要立即运行审核，请在进程中的任意点单击 “启动作业”。

7 单击 “下一步”。

8 在 “计划” 页面，选择是否要立即运行或在以后的时间和日期运行该审核。要在以后运行该审核，请选择 “在该时间运行任务” 然后选择日期和时间。

9 单击 “下一步”。

10 在 “通知” 窗口，默认情况下，无论审核作业是否成功，用户都会收到审核完成时发送的通知电子邮件。要添加电子邮件通知者，请单击 “添加通知者”，并输入电子邮件地址。

11 （*可选*）可以指定是否要在审核作业成功或失败时发送该电子邮件。

12 （*可选*）可以在 “工单 ID”字段中指定凭据跟踪 ID。仅当 SA Professional Services 将 SA 与您的变更控制系统集成时，才能使用 “工单 ID”字段。否则，应将其留空。

13 单击 “下一步”。

14 在 “作业状态”页中，单击 “启动作业”运行审核。如果审核已运行，单击 “查看结果”可查看审核的结果。

从审核结果

如果希望再次运行同一个审核，则可以从审核结果重新运行该审核。

当查看审核或快照结果，并从这些结果重新运行审核时，原始审核中的规则可能已在捕获结果后更改。可能运行的是已更新的审核，而不一定是产生这些结果的原始审核。

要重新运行审核，请执行以下操作：

1 在导航窗格中，选择 “库” > “按类型” > “审核和修正”。

2 选择 “审核”，然后选择 “Windows”或 “Unix”。

3 选择一个审核，然后在详细信息窗格中，选择该审核的审核结果。每次运行该审核时，其结果都会在详细信息窗格中进行累计。

4 双击审核结果可将其打开。

5 从 “操作”菜单中，选择 “重新运行审核”。

6 在 “运行”窗口，步骤一显示了此审核的名称、源服务器、或审核中使用的快照、此审核中定义的规则总数以及此审核的所有目标 （服务器和快照）。单击 “查看规则详细信息”可查看规则定义。

（*可选*）如果要立即运行审核，请在进程中的任意点单击 “启动作业”。

7 单击 “下一步”。

8 在 “计划”页面，选择是否要立即运行或在以后的时间和日期运行该审核。要在以后运行该审核，请选择 “在该时间运行任务”然后选择日期和时间。

9 单击 “下一步”。

10 在 “通知”窗口，默认情况下，无论审核作业是否成功，用户都会收到审核完成时发送的通知电子邮件。要添加电子邮件通知者，请单击 “添加通知者”，并输入电子邮件地址。

11 （*可选*）可以指定是否要在审核作业成功或失败时发送该电子邮件。

12 （*可选*）可以在 “工单 ID”字段中指定凭据跟踪 ID。仅当 SA Professional Services 将 SA 与您的变更控制系统集成时，才能使用 “工单 ID”字段。否则，应将其留空。

13 单击 “下一步”。

14 在 “作业状态”页中，单击 “启动作业”运行审核。如果审核已运行，单击 “查看结果”可查看审核的结果。

当查看审核或快照结果，并从这些结果重新运行审核时，试想一下，原始审核中的规则可能已在捕获和查看结果后更改。当重新运行审核时，可能运行的是已更新的审核，而不一定是产生这些结果的原始审核。

清除审核或快照结果

一旦在某个服务器上运行审核或快照并查看其结果后，必须关闭此审核或快照窗口以清除结果，然后才能在其他服务器上运行审核或快照。如果没有关闭此窗口，则所查看的任何结果和规则都将属于初始服务器。

计划审核

计划审核需要指定审核运行的时间 （运行一次或作为重复作业运行）以及要接收有关该作业状态的电子邮件通知的人员。也可以查看、编辑和删除或取消现有的已计划审核。当删除已计划审核时，所有与此审核关联的已创建计划也会被删除。还可以取消正在运行的审核作业。请参见取消活动的审核作业 （第 26 页）。

必须具有创建、查看、编辑和删除审核计划的权限。要获取这些权限，请与 SA 管理员联系。有关权限的详细信息，请参见 《SA 管理指南》。

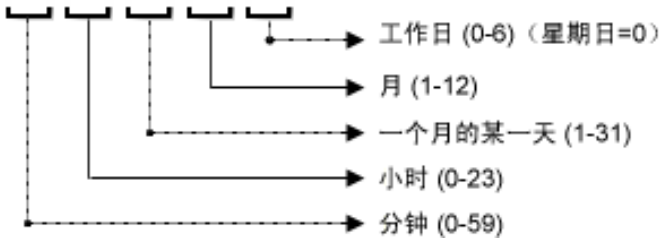
计划重复审核

在创建、配置和保存审核后，可以设置一个计划来指定希望该审核重复运行的时间。在指定重复计划时，必须允许审核作业在结束日期至少运行一次。计划设置后，可以根据需要编辑计划。

要计划重复审核，请执行以下操作：

1. 在导航窗格中，选择 “库” > “按类型” > “审核和修正”，然后选择审核。
2. 选择 OS （Windows 或 UNIX），然后双击打开审核。
3. 在 “审核”窗口的 “视图”窗格中，选择 “计划”。
4. 在 “计划”部分中，选择运行审核的频率是一次、每天一次、每周一次、每月一次，还是按自定义计划。参数包括：
   - **无**：不会设置任何计划。要运行审核，请选择该审核，右键单击并选择 “运行审核”。
   - **每日**：选择此选项将每天运行审核一次。
   - **每周**：选择要在一周的一天或几天运行审核。
   - **每月**：选择要运行审核的月份以及每月的日期。
   - **自定义**：在 “自定义 Crontab 字符串”字段中，输入表示时间计划的字符串。

     crontab 文件有五个字段用于指定周日期、月份、月日期、小时和分钟。以下图表显示了 crontab 文件中的各个位置，位置所对应的内容以及所允许的值：



crontab 字符串可包含连续值 (1,2,3,4) 和范围 (1-5) 值。只有一部分操作系统支持分钟格式 /2 或 /10，这种分钟格式用于每隔 2 分钟或 10 分钟运行一次审核。星号 (*) 表示该字段的所有值，如一年的所有月份。日可在两种字段中进行指定：月日期和周日期。如果两个日期都被指定，则这两个值都将执行。所有操作系统每个字段内都支持逗号隔离值。

例如：

5,10 0 10 * 1 意思是每个月或每个月 10 号和每个周一的上午 12:05 和 12:10 运行审核。

有关 crontab 输入格式的详细信息，请参考 Unix 手册页。

5 在 “时间和持续时间” 部分，为每个类型的计划指定启动每日计划的小时和分钟。除非指定结束时间，否则审核将无限期运行下去。

要选择审核计划的结束日期，请选择 “结束”，然后选择一个日期。*（可选）*如果希望审核计划无限期地运行下去，则 “时区” 设置为取消选择 “结束” 选项。

6 要保存审核计划，请从 “文件” 菜单中，选择 “保存”。这样审核将会根据定义的计划运行。

编辑审核计划

创建 （或编辑）并保存审核后，可以对其计划进行编辑。

要编辑已计划审核，请执行以下操作：

1 在导航窗格中，选择 “作业和会话”。

2 选择 “重复计划”。

3 在内容窗格顶部的下拉列表中，选择 “审核服务器”。

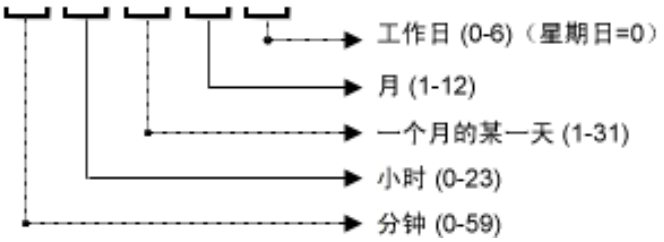
4 选择一个已计划审核作业，右键单击并选择 “打开”。

5 在 “审核” 窗口中，选择 “视图” 窗格中的 “计划” 查看审核计划。

6 要编辑审核计划，请修改以下参数：

- **无**：不会设置任何计划。要运行审核，请选择该审核，右键单击并选择 “运行审核”。
- **每日**：选择此选项将每天运行审核一次。
- **每周**：选择要在一周的一天或几天运行审核。
- **每月**：选择要运行审核的月份以及每月的日期。
- **自定义**：在 “自定义 Crontab 字符串” 字段中，输入表示时间计划的字符串。

  crontab 文件有五个字段用于指定周日期、月份、月日期、小时和分钟。以下图表显示了 crontab 文件中的各个位置，位置所对应的内容以及所允许的值：



crontab 字符串可包含连续值 (1,2,3,4) 和范围 (1-5) 值。只有一部分操作系统支持分钟格式 /2 或 /10，这种分钟格式用于每隔 2 分钟或 10 分钟运行一次审核。星号 (*) 表示该字段的所有值，如一年的所有月份。日可在两种字段中进行指定：月日期和周日期。如果两个日期都被指定，则这两个值都将执行。所有操作系统每个字段内都支持逗号隔离值。

例如：

5,10 0 10 * 1 意思是在每个月的 10 号和每个周一的上午 12：05 和 12：10 运行审核。

有关 crontab 输入格式的详细信息，请参考 Unix 手册页。

7 在 “时间和持续时间” 部分，为每个类型的计划指定启动每日计划的小时和分钟。除非指定结束时间，否则审核将无限期运行下去。要选择审核计划的结束日期，请选择 “结束”，然后选择一个日期。“时区” 将根据您的用户配置文件中设置的时区进行设置。

8 *（可选）*如果希望审核计划无限期运行下去，则取消选择 “结束” 选项。

9 要保存审核计划，请从 “文件” 菜单中，选择 “保存”。这样审核将会根据定义的计划运行。

如果您在之前发布 （SA 10.0 之前）中设置了审核计划，并且使用的是 “系统” 时区 （如 SystemV/PST8 或 System V/PST8PDT），则您必须使用所支持的时区重新设置该审核计划，否则将在运行审核时出错。

查看已完成的审核作业

要查看有关已完成的审核作业的信息，请执行以下操作：

1 在导航窗格中，选择 “作业和会话”。

2 选择 “作业日志”。

3 内容窗格会显示在此 SA 核心中运行的所有作业。要仅显示审核作业，请从内容窗格顶部的下拉列表中，选择 “运行审核” 任务。如果要仅查看已计划审核，请在内容窗格顶部的 “用户 ID” 字段中输入用户 ID。

4 打开审核作业查看审核结果，然后单击 “查看结果”。

导出 / 导入审核

使用审核筛选器告知 DET 要从 SA 核心 / 网状网络导出的审核，以便之后可以将其导入到另一个 SA 核心 / 网状网络。请参见 《SA 内容实用程序指南》。

取消活动的审核作业

在 SA 客户端中，可以终止*活动的审核作业*。活动审核作业是指已经启动且正在运行的作业。

对活动的审核作业执行的终止操作称为*软取消*。软取消是这样一种活动：作业正在部分运行，然后在您单击 “审核服务器” 向导中的 “作业状态” 步骤的 “结束作业” 时停止。软取消仅适用于要停止的活动的审核作业。

必须具有取消正在运行的审核的权限。通常情况下，如果有权启动审核作业，也将可以停止正在运行的审核作业。另外，如果具有 “编辑或取消任何作业” 权限，也将可以软取消正在运行的审核作业。请参见《SA 管理指南》中有关终止活动作业和权限参考章节的部分。要获取这些权限，请与 SA 管理员联系。

要停止活动的审核作业，请执行以下操作：

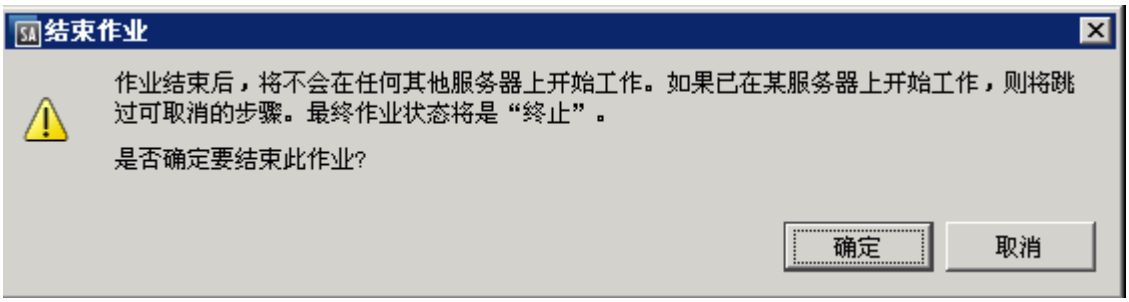
1 在 “作业状态” 窗格中，单击 “结束作业”。

此按钮仅在作业正在运行时可用。

2 此时将显示 “结束作业” 对话框。此对话框简短地描述了作业是如何终止的：

- 作业将不会在任何其他服务器上启动作业。
- 如果作业已在某服务器上运行，则该作业将取消所有可跳过的步骤。
- “作业状态” 将指示这些步骤是已完成还是已跳过。

3 如果作业成功结束，则最终作业状态将显示为 “已终止”。



4 单击 “确定” 确认要终止该作业。“作业状态” 窗口将显示终止操作过程的进度。

作业状态将为 “已终止”。服务器状态将为 “已取消”。任务状态将为 “成功” 或 “已跳过”。

5 当终止完成后，您还可以在 SA 客户端的 “作业日志” 中查看作业。

在 SA 客户端导航窗格中，选择 “作业和会话”。“作业日志” 视图将显示处于 “已终止” 状态的作业。

查看审核和快照使用情况

创建并运行审核后，可以从 “所有托管服务器” 列表或从 “设备资源管理器” 中查看该审核，并可以查看与特定服务器关联的所有审核。

从所有托管服务器

要从 “所有托管服务器” 列表查看服务器审核的使用情况，请执行以下操作：

1 在导航窗格中，选择 “设备” > “服务器” > “所有托管服务器”。

2 在内容窗格中选择一个服务器。

3 从 “视图” 下拉列表中，选择 “审核” 或 “快照规范”。详细信息窗格将显示有关审核和快照使用情况的信息。

4 如果选择 “审核”，则可在详细信息窗格中选择以下选项之一：

- **审核 - 服务器是目标**：显示以选定服务器为审核目标的所有审核。
- **审核 - 服务器是源**：显示将选定服务器用作审核源的所有审核。

或

5 如果选择 “快照规范”，则详细信息窗格将显示所有以选定服务器为目标的快照规范。

6 *（可选）*在这些视图的任意一个中，均可选择审核或审核结果，并从 “操作” 菜单执行操作。例如，可以打开审核、创建审核、重新运行审核或删除审核。

从设备资源管理器

要从 “设备资源管理器” 查看服务器审核的使用情况，请执行以下操作：

1 在导航窗格中，选择 “设备” > “所有托管服务器”。

2 在内容窗格中，选择服务器，右键单击并选择 “打开”。

3 在 “设备资源管理器” 中，从 “视图” 窗格，选择 “管理策略” > “审核”。

4 在内容窗格中，从 “显示” 下拉列表，选择以下选项之一：

- **审核 - 服务器是目标**：显示以选定服务器为审核目标的所有审核。
- **审核 - 服务器是源**：显示将选定服务器用作审核源的所有审核。

5 *（可选）* 在此视图中，可选择审核并从 “操作” 菜单执行操作。例如，可以打开审核、创建审核、重新运行审核或删除审核。

6 然后，可从 “视图” 窗格中选择 “存档的审核结果”，查看所有与此存档服务器关联的审核结果。

审核配置

配置审核或审核策略需要进行以下任务：

- 命名和描述审核或审核策略
- 为审核或审核策略选择一个源：服务器、快照、快照规范或无源。
- 配置审核规则 — 可以链接到审核策略。这指定要在审核中使用审核策略的规则。这也将禁用配置单个规则的功能。还可以将审核策略的所有规则导入到该审核中。
- 选择审核的目标服务器、服务器组或快照
- 添加审核规则异常 （可选）
- 计划审核
- 设置电子邮件通知 （*可选*）
- 保存审核

VMware ESXi 服务器不能作为审核或快照的源或目标。

要配置审核，请执行以下操作：

1 使用创建审核 （第 19 页）中所述的一种方法创建新审核。此时将打开 “审核”窗口。

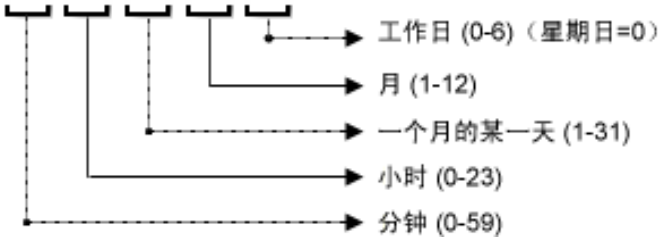
2 输入以下审核信息：

- **属性**：输入审核的名称和描述。
- **源**：任何审核都可以将服务器、快照或快照规范用作源。（或者也可以选择无源，然后定义自己的规则。）如果将服务器用作源，则可以通过浏览服务器的值定义审核规则。如果将快照选作源，则定义的审核规则将仅限于快照和快照结果中的规则。如果选择快照规范，则审核将比较为快照规范目标创建的快照，并将其与审核目标相比较。当将快照规范选作源时，快照中的规则不可编辑。如果选择无源，则必须定义自己的规则，或选择链接到规则部分的某个审核策略。但是一些规则在定义时需要源。
- **规则**：从列表中选择规则类型开始配置审核规则。每个审核规则都是唯一的，要求有自己的说明。有关如何配置单个审核规则的信息，请参见审核和修正规则 （第 35 页）。

  如果要使用审核策略来定义审核规则，则单击 “链接策略”或 “导入策略” 。当链接审核策略时，审核将保持与此审核策略的直接连接，并禁用创建规则的功能。链接策略后，审核将仅使用在该审核策略中配置的规则。所以，如果该策略有任何更改，审核将根据新更改做相应更新。如果导入审核策略，审核将使用在该策略中定义的所有规则，但不会保持与审核策略的链接。有关审核策略的信息，请参见审核策略管理 （第 79 页）。
- **目标**：选择审核的 “目标”。审核的目标是您希望配置的审核规则评估和比较的服务器、服务器组或快照。要添加服务器或服务器组，请单击 “添加” 。要添加快照目标，请在 “快照目标”部分单击 “添加”。

- **异常**：单击 “添加”将异常添加到审核的规则上。在 “添加异常”窗口中，选择一个或多个服务器（或设备组），然后选择希望将其从所选服务器中排除的一个或多个规则。可从任何目标服务器或快照中排除审核中的任何规则。可选择性地添加说明、工单 ID 以及此异常的到期日期。
- **计划** *（可选）*：选择运行审核的频率是一次、每天一次、每周一次、每月一次，还是按自定义计划。参数包括：
  - **无**：不会设置任何计划。如果希望立即运行审核或运行一次，则必须选择审核，右键单击并选择 “运行审核”。
  - **每日**：选择此选项将每天运行审核一次。
  - **每周**：选择一周的某天运行审核。
  - **每月**：选择要运行审核的月份。
  - **自定义**：在 “自定义 Crontab 字符串”字段中，输入表示时间计划的字符串。

    crontab 文件有五个字段用于指定周日期、月份、月日期、小时和分钟。以下图表显示了 crontab 文件中的各个位置，位置所对应的内容以及所允许的值：

    crontab 字符串可包含连续值 (1,2,3,4) 和范围 (1-5) 值。只有一部分操作系统支持分钟格式 /2 或 /10，这种分钟格式用于每隔 2 分钟或 10 分钟运行一次审核。星号 (*) 表示该字段的所有值，如一年的所有月份。日可在两种字段中进行指定：月日期和周日期。如果两个日期都被指定，则这两个值都将执行。所有操作系统每个字段内都支持逗号隔离值。例如：

    5,10 0 10 * 1 意思是每个月或每个月 10 号和每个周一的上午 12:05 和 12:10 运行审核。

    有关 crontab 输入格式的详细信息，请参考 Unix 手册页。
  - **时间和持续时间**：针对各种类型的计划，指定计划开始的小时、分钟、周日期和月份。除非指定结束时间，否则审核将无限期运行下去。要选择结束日期，请选择 “结束”。在日历选择器中，选择结束日期。“时区”将根据您的用户配置文件中设置的时区进行设置。
  - **通知**：输入电子邮件地址，以便在审核作业完成运行时通知用户。可以选择审核作业成功和失败时（而不是审核规则成功时）都发送电子邮件。要添加电子邮件地址，请单击 “添加通知”规则。（仅当审核设置为按重复计划运行时，此操作才适用）。

3 当完成配置审核时，从 “文件”菜单中，选择 “保存”。

审核与快照源

可以使用以下几个选项为审核或快照规范选择源：

- 源：服务器 （第 31 页）
- 源：快照 （第 32 页）
- 源：快照规范 （第 32 页）
- 源：规则 （第 33 页）

审核源确定了可以在审核或快照规范中选择和配置的规则。请根据审核或快照规范的目的选择源。

源：服务器

托管服务器可作为审核或快照规范的源。

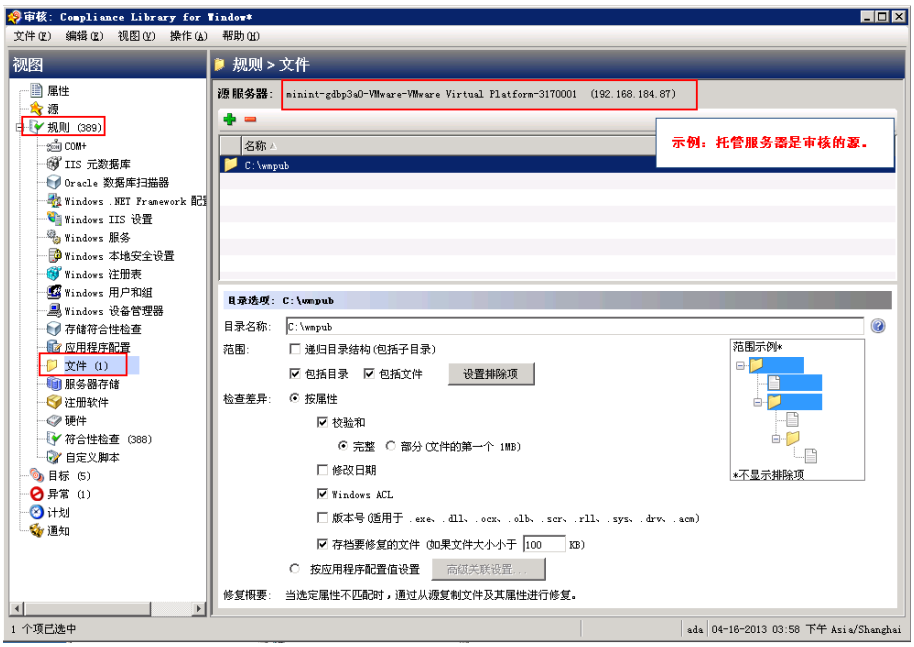
如果知道特定服务器包含要添加到审核或快照规范中的服务器对象，则可以将该服务器选作审核的源。例如，如果要审核特定目标服务器上 Apache Web 服务器的应用程序配置文件 （如 httpd.conf）或为其创建快照，则选择已知装有 Apache 且配置正确的服务器作为审核的源。

当创建审核或快照规范规则时，可选择几个不同的源服务器。也可以为每个服务器对象规则选择不同的源。

VMware ESXi 服务器不能作为审核或快照的源。

图 3 显示了当选择服务器作为审核的源时，在 “审核” 窗口或 “快照规范” 窗口将显示内容窗格。

图 3　　服务器作为审核的源：创建审核规则



有关目录选项的详细信息，请参见带图表的常见范围用例 （第 47 页）。

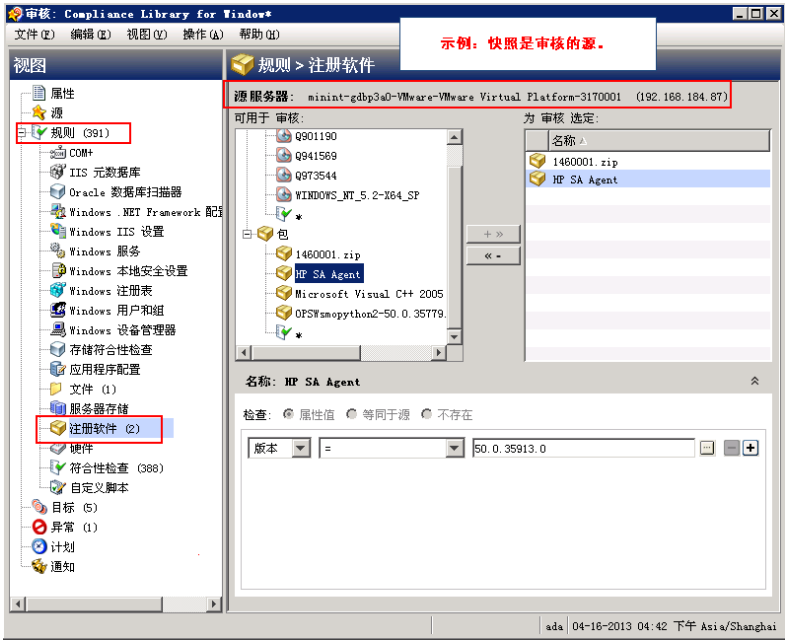
源：快照

快照可作为审核或快照规范的源。

如果有已知状态良好（*黄金服务器*配置）的托管服务器的快照，并打算将此快照与审核中的其他服务器进行比较，则将此快照选为审核或快照规范的源。或者，也可以选择此选项以使用捕获的服务器值创建其他服务器的快照。通过使用快照作为审核和快照规范的源，可选择快照所基于的原始快照规范的结果和规则。

图 4 显示了在使用快照为源时创建审核或快照规范规则所用的选项。可从快照结果和快照规则中选择。

图 4　　快照作为审核的源：创建审核规则可用的服务器对象



源：快照规范

快照规范可作为审核的源。通常将其称之为*反射审核*。当从快照规范运行审核时，审核将使用在该规范中定义的所有信息，然后应用已定义的任意筛选器。

如果要随着时间变化跟踪服务器配置并监控所发生的任何更改，则选择此选项。例如，您可能要跟踪某应用程序，以确保随着时间推移其配置依旧正确。如果此应用程序在多个服务器上运行，则可以创建用于定义服务器配置所需状态的快照规范，然后运行此快照。

接下来，可以创建一个审核，然后将快照规范用作此审核的源。被快照用作目标的每个服务器现在也作为审核的目标包含在内。当根据需要或按照计划运行此审核时，系统会将每个服务器的当前配置与最初在快照中捕获的状态进行比较。如果用作审核源的快照规范设置为重复运行，则审核将与最近运行的快照进行比较。所有更改都会显示在审核结果窗口中。

源：规则

使用源服务器的源值的规则可用作审核的源。

除了以下规则外，大部分规则都需要源才能进行定义：

- 任何未将值设为派生自源 （服务器、快照或快照规范）的预配置规则
- 未将比较值设为派生自源 （服务器、快照或快照规范）的自定义脚本规则

如果审核中含有需要源却未指定源的规则，则该审核无法保存。必须为所有比较检查和与源值相比较的规则选择源。

服务器对象

表 1 列出了可为其在审核中或快照规范中创建规则的所有服务器对象。一些服务器对象值被实时捕获和审核，一些对象则从模型库中捕获。

表 1　　用于审核和快照的服务器对象

服务器对象	描述	实时捕获和 / 或从模型库中捕获
应用程序配置	应用程序配置文件的内容及其值。	实时
Windows COM+ （请参见表下方的注释。）	COM+ 对象和组件类别。	实时
自定义脚本	编写您自己的自定义脚本，用于从服务器获取信息和比较内容。例如，可运行脚本从自定义应用程序收集输出，以及针对审核中设置的值评估已返回的输出。（Python 仅适用于 Python 脚本。）	实时
发现的软件	“发现的软件”提供了适用于 Windows 和 UNIX 托管服务器的基于签名的软件发现机制，可帮助您管理不受 SA 管理的应用程序和软件。	实时
文件	文件和目录（以及子目录）的内容、用户和组访问权限、文件校验和、文件修改日期以及 Windows ACL （仅限 Windows）。	实时
硬件	CPU、存储设备和内存。	模型库
IIS 元数据库	要创建快照或进行审核的 Microsoft IIS 元数据库对象和配置值。	实时
IIS 7.0	Microsoft IIS 7.0	实时

表 1　用于审核和快照的服务器对象 （续）

服务器对象	描述	实时捕获和 / 或从模型库中捕获
Internet 信息服务器	有关 Windows 服务器的 IIS 实时信息，如服务器名称、服务器类型、服务器状态、日志文件路径、文档文件路径等。	实时
本地安全设置	有关安全设置的实时信息，包括诸如密码策略、审核策略、用户权限和安全选项的安全设置。	实时
已注册软件	所有已安装的程序包或修补程序都实际安装在源服务器上，无论它们是否已由模型库注册。	实时
存储	与存储设备和 SAN 设备相关的信息以及数据中心中的连接 （如果核心已启用存储）。 要审核 SAN 对象并为其创建快照，需要 Storage Essentials (SE) 6.1.1 版或更高版本，且必须在 SA 核心上安装和配置 Server Automation SE Connector 组件。	实时
BSA Essentials 订阅服务“符合性检查”	如果已订阅 BSA Essentials 订阅服务，则有权访问许多不同类型的审核规则及其构成组件（也称为 “符合性检查”）。具体可访问的检查类型取决于用户订阅，但可以包含特定规则，如 Microsoft Windows 的最新修补程序补充、当前管理符合性策略 （例如 FISMA、萨班斯 - 奥克斯利法案）、 BSA Essentials 订阅服务开发者社区的用户创建规则、每日更新的漏洞内容等。	实时
用户和组	比较服务器上的用户和组的信息，如上次登录的用户名、是否启用 CTRL + ALT + DELETE 等。	实时
Windows .NET Framework 配置	有关配置集缓存和已配置的配置集列表的实时信息，如配置集名称、版本、区域设置、公共密钥标记、缓存文件 （GAC 或 ZAP）、处理器体系结构、自定义和文件名称。 对于每个已配置的配置集列表，可使用配置集名称、公共密钥标记、代码库、绑定策略、文件名、文件数据等信息。	实时

表 1　　用于审核和快照的服务器对象 （续）

服务器对象	描述	实时捕获和 / 或从模型库中捕获
Windows 注册表 （请参见表下方的警告。）	选择 Windows 注册表目录或注册表项值进行捕获和比较。	实时
Windows 服务	选择 Windows 服务。	实时
Windows 用户和组	Windows 服务器上的用户和组信息。	实时

即使 SA 将在设备资源管理器中显示空的 COM+ 文件夹，快照或审核也将不包含不具有任何对象的 Windows COM+ 类别 （文件夹）。

SA 客户端无法创建整个 Windows 注册表的快照或所有系统键的快照。此数据量超过当前设计允许的范围。

SA 审核和修正不支持设备文件或套接字。

审核和修正规则

当创建审核或快照规范时，必须配置审核和修正规则。这些规则定义了：

- 要创建快照或进行审核和比较的服务器对象类型。这些对象包括服务器文件系统、硬件信息、应用程序配置、已安装的修补程序或软件、用户和用户组等。
- 有关要进行审核或创建快照的对象的信息。例如，对于服务器的文件系统，可以捕获 Windows NT 文件的访问控制级别。对于应用程序，可以捕获要创建快照或进行审核的应用程序配置值，以及指定是否在规则和目标服务器的实际值之间发现差异的任何修正值。

规则可以包含用于确定所有存储在文件中的密码是否与特定字符长度匹配的自定义脚本。规则还可以包含用于确定特定 Windows 服务在服务器上是运行还是禁用的检查。对于某些规则，在审核运行之后，如果审核或快照中定义的值与服务器的值不匹配，则也可以为服务器对象指定修正值。例如，如果 Windows 服务已禁用，则可以指定修正值应重新启动服务。在审核运行之后，可从 “审核结果” 窗口手动实施修正值

配置规则

某些规则在配置和定义时非常简单，除了选择要创建快照或进行审核的服务器对象之外，不需要任何其他操作。某些规则可能需要通过检查来确定在服务器配置文件中是否存在值或属性，而不需要设置任何高级参数。

示例: “发现的软件” 规则检查在目标服务器上安装或部署的所有已注册和未注册的软件。

示例：通过使用“硬件”规则，可以检查 CPU、内存或目标服务器上存在的存储值。在这种情况下，不需要额外的规则参数。

其他规则要更复杂且需要更高级的配置，如指定用于查找值范围的表达式和指定修正替换不想要的值。

在审核和审核策略中，也可以定义希望对象具有什么修正值 （如果有）。修正值仅在发现服务器对象与所需状态不同 （即目标服务器上的配置与审核中的规则不符合）时使用。在审核运行之后，可从 “审核结果”窗口手动实施修正值

审核规则包括以下组件：

- **服务器对象**：审核可评估的特定服务器配置，如服务器文件系统、应用程序配置值、硬件信息、已安装的软件 （修补程序和程序包）、 Windows 注册表条目等。服务器对象通常由几个您也可以检查的其他对象组成。

  示例：在 Windows 服务器上，希望知道在目标服务器上是否存在特定 Windows 服务以及它是否启用。

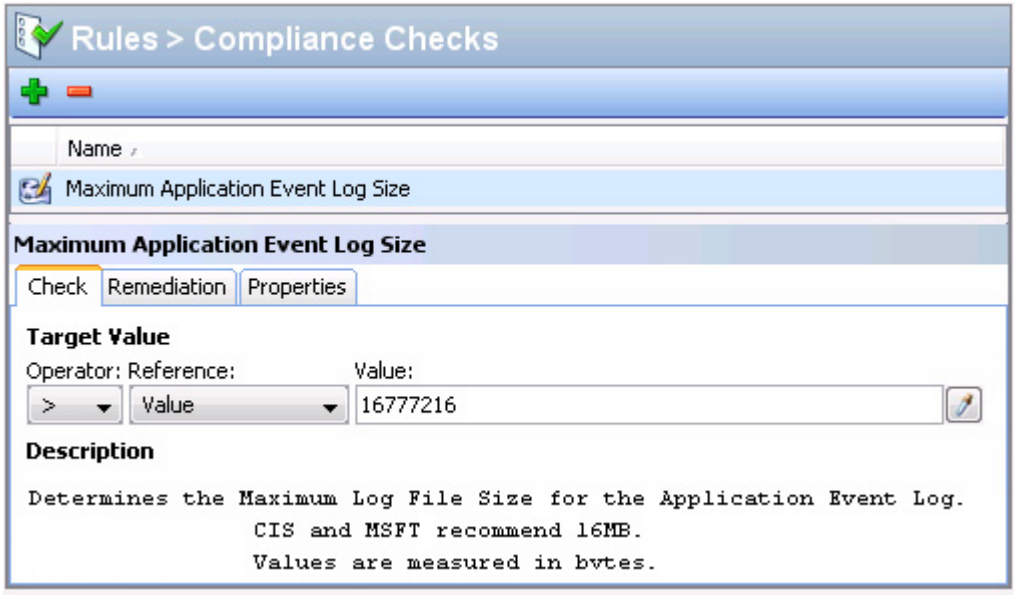
- **目标值**：要在目标服务器上检查的值或设置。

  示例：例如，要确定在服务器上是否存在某特定目录、应用程序是否配置正确、特定服务是否已启用等。

- **修正值**：当在目标服务器上未发现目标值时，要在修正期间更改的服务器对象的值。修正值无法自动实施。必须在审核运行之后进行修正更改。

图 5 展示了为名为 “文件复制”的 Windows 服务定义的审核规则。

图 5　　使用修正值配置的自定义审核规则



在图 5 中，审核规则已按以下方式配置：

- **规则 > 符合性检查**：列出从 BSA Essentials 订阅服务选择的规则（应用程序事件日志最大大小）。
- **规则详细信息检查**
  - **目标值**：与作为审核目标的服务器上的值相比较的所需值。在此示例中，该规则的配置目的是确定目标服务器的 “应用程序事件日志”文件大小是否未超过 16777216 字节。例如，“目标值”参数已设为：`> Value 16777216`。

— **描述**：描述了在目标服务器上正在检查的值。在此示例中，审核将检查以确认 “应用程序事件日志”文件大小是否未超过 CIS 和 MSFT 建议的大小限制 16MB （16777216 字节）。

此信息指示审核评估目标服务器的 “应用程序事件日志”文件大小并确定其是否超过 16MB。

- **修正**：修正值确定了当目标服务器上的值与审核中定义的值（目标值）不匹配时应采取的操作。在此示例中，修正值设为 CIS 和 MSFT 建议的大小限制 16MB （16777216 字节）。可在审核运行后，从 “审核结果”窗口修正此值，且仅当目标服务器值不符合规则条件时才可进行修正。

审核和快照规则

必须具有创建和配置审核和修正规则的权限。要获取这些权限，请与 SA 管理员联系。有关权限的详细信息，请参见 《SA 管理指南》。

有关可为每个服务器对象类型设置的规则的信息，请参见以下有关要配置规则的特定服务器对象的章节之一：

- 配置应用程序配置规则
- 配置 COM+ 规则
- 配置自定义脚本规则
- 配置发现的软件规则
- 配置文件规则
- 配置硬件规则
- 配置 IIS 元数据库规则
- 配置 IIS 规则
- 配置 IIS 7.0 规则
- 配置本地安全设置规则
- 配置注册软件规则
- 配置存储规则
- 配置 Windows .NET Framework 配置规则
- 配置 Windows 注册表规则
- 配置 Windows 服务规则
- 配置 Windows/UNIX 用户和组规则
- 配置符合性检查

某些 SA 核心可能包含法律内容，如带有符合性检查的事件日志记录、操作系统以及用户和用户组规则。这些检查已集成到可从 EP 获得的 CIS 策略。

配置应用程序配置规则

通过使用应用程序配置审核规则，可以审核托管服务器上的配置文件值，检查这些文件是否按所需方式配置。

可从预定义应用程序配置模板列表中选择，这些模板用作要审核的目标配置文件的比较基础。也可从由组织中的用户创建并可用于审核、快照规范或审核策略的自定义应用程序配置中选择。

审核中的应用程序配置构建应用程序配置文件的值和结构的模型。这样可以设置用于检查托管服务器上现有配置文件中值的规则。

选择审核、快照规范或审核策略中的应用程序配置，并单击 “查看”，将看到审核源的配置文件内容。将显示所有可添加到审核规则中的 “键 - 值”对。

“审核”窗口显示的信息取决于审核或审核策略的源 （或快照规范的目标）：

- 如果选择服务器作为审核或审核策略的源，则在审核规则中显示的应用程序配置值将是源服务器上的那些配置文件，这些配置文件通过应用程序配置模板进行了筛选。
- 如果选择快照作为审核或审核策略的源，则将仅可以修改该快照创建时捕获的值。
- 如果未选择任何源，则将无法配置应用程序配置文件的规则。
- 如果选择配置快照规范中的应用程序配置，则配置的值将派生自目标服务器。

在审核的应用程序配置规则中，将仅可以查看已在应用程序配置中建模的源配置文件的值。如果应用程序配置是自定义的，但未定义自定义特性 （但该值在源配置文件中存在），则将无法在审核或审核策略中看到该配置。

查看源应用程序配置文件内容之后，可以定义自己的规则，方法是从源文件中选择值并构建用于针对目标配置进行检查的规则。在审核发现规则和目标配置文件值之间存在差异时，也可以定义修正值。

创建应用程序配置规则

以下示例对理解如何配置应用程序配置规则非常有帮助。

示例：目标是为 UNIX 主机文件 (`/etc/hosts`) 创建审核规则，然后审核一组服务器的 `/etc/hosts` 文件以确保它们包含正确的值。特定*黄金服务器* 上的 UNIX 主机文件代表主机文件配置的理想状态，该状态是您希望其他服务器所遵从的状态。可以将该黄金服务器选作审核的源，然后使用该文件中的值构建审核规则。创建规则并保存审核后，可针对服务器组运行审核，以查看它们的 `/etc/hosts` 文件是否配置正确 （根据审核规则）。

在此示例中，使用了等号 (=) 运算符。应用程序配置规则的有效运算符有：=（等于）、<>（不等于）、<（小于）、<=（小于等于）、>（大于）、>=（大于等于）、包含、不包含、匹配 RE 以及不匹配 RE。

要创建应用程序配置规则，请执行以下操作：

1 使用创建审核（第 19 页）中描述的其中一种审核创建方法创建审核。如果要为快照规范创建此规则，请参见创建快照规范（第 115 页）。

2 选择审核源：服务器、快照、快照规范或无源。为审核选择的源将决定规则的类型，如果有，则可为应用程序配置创建规则。必须选择源，否则无法配置应用程序配置规则。

3 在“审核”窗口的“视图”窗格中，选择“规则”>“应用程序配置”。

4 在内容窗格中，单击 可访问所有可用的配置模板。

5 在“选择配置模板”窗口中，选择一个或多个要添加到审核规则的模板，然后单击“确定”。

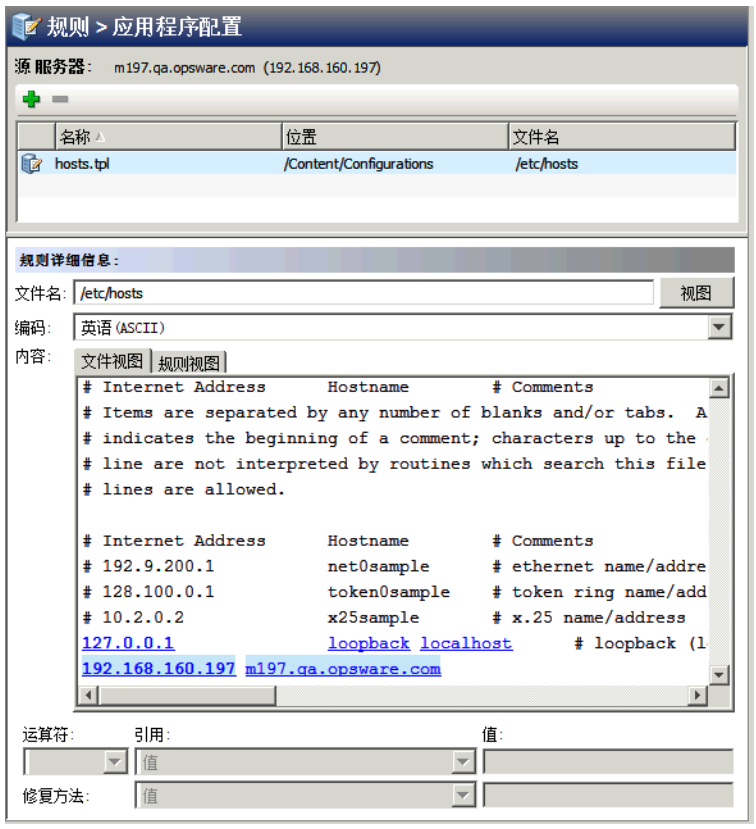
6 选择要配置的模板。模板内容将出现在模板编辑器中。

7 单击“查看”可在“文件视图”选项卡中查看该配置文件的内容。

如果看不到配置文件的内容，请在“文件名”部分中输入正确的路径。

示例: 如果查看 UNIX 主机文件，则可能会看到类似图 6 示例中的信息。可以查看源主机文件（突出显示的蓝色文本）的内容和 IP 地址 / 主机名对。

图 6 主机文件的应用程序配置审核规则



8 要为此配置文件创建审核规则，请从源服务器（选作审核源的服务器）的主机文件中选择“键 - 值”对。

9 要创建此规则，请在“文件视图”选项卡区域中选择 IP 地址。这将显示从源服务器获取的文件内容。在图 6 的示例中，可选择 IP 地址，如 127.0.0.1。选择 IP 地址后，元素便会以蓝色文本突出显示。蓝色文本表示已可以从该元素创建规则。

有关配置应用程序配置审核规则时使用的颜色方案的详细信息，请参见表 2。

在内容区域选择 IP 地址后，“运算符”字段中的值为空。这意味着运算符尚未添加到规则中。要将值添加到规则中，可以双击规则或在内容下方的规则表达式区域输入以下参数：

- **运算符**：选择 =（等于）。当将运算符改为 = 后，等于运算符便会立即添加到规则中。如果将运算符改回未选择，则该运算符便会立即从规则中移除。
- **引用**：选择“值”。
- **值**：输入 127.0.0.1。
- **修正方法**：输入 127.0.0.1。

这表示要查找值为 127.0.0.1 的 IP 地址。如果未找到该 IP 地址，则修正应为 127.0.0.1，所以可以将此修正添加到任何未含有此 IP 地址的目标服务器的主机文件中。

10 在“文件视图”选项卡区域中选择主机名。在上一步选定的初始 IP 地址将变为绿色。绿色文本表示所设置的下一个规则参数将与之前选定的 IP 地址进行配对。

11 在“规则”部分中，设置以下参数：

- **运算符**：选择 =（等于）。
- **引用**：选择“值”。如果为规则定义选择了自定义特性，则此自定义特定也必须在目标服务器上存在，否则此规则的审核将失败。
- **值**：选择主机。
- **修正方法**：选择主机。这将添加最后一部分规则，该规则将检查目标服务器关于 IP 地址 127.0.0.1 的“键 - 值”对是否与主机匹配。

12 选择“规则视图”选项卡。该规则将表述为：

“检查是否存在以下条目：IP 地址等于值 127.0.0.1 且主机名含有等于值 host 的条目。”

此规则将用于审核位于目标服务器或快照规范上的主机文件。

注意：IP 地址和主机名是“键 - 值”对，因此必须始终同时提供 IP 地址和主机名。

13 要配置更多的应用程序配置规则，请从“可用于审核”部分选择更多应用程序配置。

14 要完成审核配置，则定义其他规则并设置该审核的目标服务器、计划和通知。

15 保存审核。

16 要运行审核，请从“操作”菜单中，选择“运行审核”。有关详细信息，请参见运行审核（第 21 页）。

应用程序配置审核规则颜色方案

首次查看应用程序配置时，所有可用于构建审核规则的元素都显示为蓝色带下划线的文本。开始选择和构建规则后，颜色会发生更改。表 2 说明了用于配置应用程序配置审核规则的颜色方案。

表 2　　应用程序配置审核规则颜色方案

文本颜色	描述
蓝色带下划线	源配置文件中所有可用于规则的元素。
深蓝色突出显示	未关联规则的选定元素。
浅蓝色突出显示	已添加到规则的元素。
中蓝色突出显示	已关联规则的选定元素。
绿色	为主键的元素，与当前选定元素相关且用于与当前选定元素相同的规则中。 如果为当前选定元素提供比较值 （=、包含、匹配 ...），则也将为其他绿色文本的元素提供 = 比较值，如： `127.0.0.1  localhost` 如果选择本地主机，则 `127.0.0.1` 将为绿色。如果为本地主机提供比较值，则也将为 `127.0.0.1` 提供自动比较值，从而提供如下规则： 存在 IP 等于 `127.0.0.1` 且 `hostname` 等于 `localhost` 的条目。
粗体	主键。
斜体	自定义特性或 SA 特性。

配置 COM+ 规则

要配置 Windows COM+ 规则，请选择要在目标服务器上进行审核或创建快照的源 COM+ 对象。 COM+ 规则还会检查选定对象的访问控制级别 (ACL)，包括继承的 ACL。

COM+ 对象根据对象的特性进行分类，其中 COM+ 对象指定零个或多个类别。审核或快照窗口显示 COM+ 对象树 “规则” 部分的一个节点中的所有 COM+ 对象。要将 COM+ 规则添加到审核或快照，选择该规则，然后单击向右箭头按钮。

如果希望能够在审核或快照结果中修正 COM+ 规则，则在选择 COM+ 对象或类别时选择 “存档所有关联的文件” 选项。此选项也包含与审核或快照规则中 COM+ 对象关联的所有 “访问权限” 和 “启动权限”，包括那些继承的父 COM+ 对象。

➤ 无法审核 COM+ root 文件夹。但是可以审核 COM+ 单个对象或子类别。

要配置 COM+ 规则，请执行以下操作：

1. 使用创建审核（第 19 页）中描述的其中一种审核创建方法创建新审核。如果要为快照规范创建此规则，请参见创建快照规范 （第 115 页）。
2. 选择审核源：服务器、快照、快照规范或无源。应用程序配置和 Windows 用户和组等一些审核规则必须具有源。
3. 在 “审核” 窗口的 “视图” 窗格中，选择 “规则” > “COM+”。
4. 在 “审核” 窗口的内容窗格中，展开 “可用于审核” 部分的顶级节点，然后选择 COM+ 对象或对象类别。
5. 单击向右箭头按钮将 COM+ 对象或对象类别移动到 “为审核选定” 部分。所有选定 COM+ 对象或对象类别都将在目标服务器或快照规范上进行审核。可以为该规则选择单个和 COM+ 类别。无法选择将 root 文件夹添加到审核规则中。
6. 从规则窗口底部选择一个选项：
   - 如果希望能够在审核或快照结果中修正 COM+ 规则，则选择 “存档所有关联的文件” 选项。
   - 如果希望 COM+ 规则仅检查选定文件名而不检查完整路径，则选择 “仅比较文件名，不比较完全路径名称”。
7. 要完成审核配置，则定义所需的任何其他 COM+ 对象或对象类别规则并设置该审核的目标服务器、计划和通知。
8. 要保存审核，请从 “文件” 菜单中，选择 “保存”。也可将 “审核” 保存为策略。有关详细信息，请参见将审核或快照规范保存为审核策略 （第 85 页）。
9. 要运行审核，请从 “操作” 菜单中，选择 “运行审核”。有关运行审核的详细信息，请参见创建审核策略 （第 81 页）。

配置自定义脚本规则

通过使用自定义脚本规则，可以定义自己的脚本（批处理、Python 或 Visual Basic）以检索和比较审核、审核策略或快照规范中使用的值。也可以编写自己的修正脚本。

在配置自定义脚本规则时，指定目标值，即希望该脚本返回的期望值。审核可根据以下方法收集此信息：

- **基于比较的审核**：在源服务器上执行脚本。脚本的返回值 （退出码或标准输出）与脚本在目标服务器上运行后的输出相比较。此选项名为 *源*。
- **基于值的审核**：指定自己的值。此值与脚本在目标服务器上运行后的输出相比较。如果知道脚本的期望结果，则可手动输入此值；或者可在源服务器上执行脚本并使用返回的值。运行审核时，此值与脚本在目标服务器上执行后的返回结果相比较。此选项名为 *值*。

对于审核，还可配置修正脚本；如果规则与脚本在目标服务器上运行后返回的值之间存在差异，则可以使用此修正脚本。

对于快照，脚本结果将通过以下方法生成：在目标服务器上运行脚本（如规则详细信息中的定义），然后在快照中捕获。设置快照规范时，也可添加修正脚本。这种类型的脚本可用于在目标服务器上进行强制修正。通过 “快照”窗口，可分别在每个目标服务器上执行快照的修正脚本。

要配置自定义脚本规则，请执行以下操作：

1 使用创建审核 （第 19 页）中的其中一种审核创建方法创建新审核。（如果要为快照规范创建此规则，请参见创建快照规范 （第 115 页）。）

2 选择审核源：服务器、快照、快照规范或无源。（应用程序配置和 Windows 用户和组等一些审核规则必须具有源。）

3 要构建脚本并定义审核规则，可选择以下选项：

源

— **规则**：单击 “添加规则”添加新的自定义脚本规则。

— **上移**：单击 “上移”将选定审核规则向上移动，以便为自定义脚本审核规则指定执行顺序。审核规则按照指定的顺序进行保存。当打开审核或审核策略时，将显示此顺序。

— **下移**：单击 “下移”将选定审核规则向下移动，以便为自定义脚本审核规则指定执行顺序。审核规则按照指定的顺序进行保存。当打开审核或审核策略时，将显示此顺序。

规则详细信息

— **名称**：输入脚本的名称。

— **脚本类型**：从批处理、 Python、 PowerShell 或 Visual Basic (VBS) 中选择。

— **脚本**：在此处键入或复制粘贴脚本内容。或单击 “导入脚本”从本地磁盘导入脚本。

成功条件

— **输出**：为 “退出码”或 “标准输出”。

— **运算符**：选择运算符，如等于 (=)、不等于 (<>)、小于 (<)、大于 (>) 等。

— **引用**：选择脚本输出的源。

— **源**：如果希望规则在审核运行并获得脚本请求的值时在源上执行脚本，则选择此选项。此选项会将该值与从目标服务器上运行的脚本检索到的值进行比较。

如果为快照规范选择此选项，则脚本将在目标上运行，且脚本执行的结果将在快照（结果）中捕获。

如果审核的源是快照，则自定义脚本规则将使用快照规范中配置的自定义脚本定义。

— **值**：输入自己的值。此选项使用输入的值并将其与脚本在目标服务器上运行后返回的值进行比较。此选项表示在审核运行时，该脚本不会在源服务器上运行。如果要立即从源服务器获取脚本输出，请单击  图标。返回的值将显示在文本框中，可接受该值或根据需要编辑该值。

如果审核的源是快照，则自定义脚本规则将使用快照规范中配置的自定义脚本定义。

- **服务器特性**：选择此选项可将源服务器上发现的服务器特性与目标服务器上运行的脚本的输出进行比较。
- **自定义特性**：选择此选项可将目标服务器上发现的自定义特性与目标服务器上运行的脚本的输出进行比较。此选项的自定义特性派生自此审核的选定源服务器。

  如果在此为规则定义选择了自定义特性，则此自定义特定也必须在目标服务器上存在，否则此规则的审核将失败。

  如果不选择审核的源，则此列表为空。

修正

- **脚本类型**：从批处理、 Python、 PowerShell 或 Visual Basic (VB) 中选择。
- **脚本**：在此处键入或复制粘贴脚本内容。或单击 “导入脚本” 从本地磁盘导入脚本。

4 （**可选**）如果审核比较失败，则可以添加修正脚本来运行。此修正不会自动应用，仅可以从审核运行后的审核结果运行修正脚本。

对于快照，在此定义的修正脚本可分别在每个目标服务器上执行。修正执行的顺序不是单独指定的。相反，选定不符合规则的修正均按照审核或审核策略中定义的顺序执行。例如，如果审核策略有 10 个规则且规则 2、4、6 和 8 为不符合规则，并选择对规则 4 和 8 进行修正，则将首先运行规则 4 的修正脚本，然后运行规则 8 的修正脚本。

5 要完成审核配置，则设置该审核的目标服务器、计划和通知。

6 要保存审核，请从 “文件” 菜单中，选择 “保存”。也可将 “审核” 保存为策略。有关详细信息，请参见将审核或快照规范保存为审核策略 （第 85 页）。

7 要运行审核，请从 “操作” 菜单中，选择 “运行审核”。有关运行审核的详细信息，请参见创建审核策略 （第 81 页）。

自定义脚本示例

以下是自定义 VB 脚本规则的示例，该脚本规则设计用于启用 Windows 用户帐户和设置用户密码。此脚本仅适用于 Windows NT 4.0 以上版本的 Windows OS。如果要在 Windows NT 4.0 上启用用户帐户和设置密码，必须手动执行所需操作。

```
strComputer = "."
strAccountName = "red2"
Set objUser = GetObject("WinNT://"& strComputer & "/" & strAccountName )
objUser.AccountDisabled = False
objUser.SetPassword "AiH345^hjq"
objUser.SetInfo
```

配置发现的软件规则

“发现的软件” 规则提供了适用于 Windows 和 UNIX 托管服务器的基于签名的软件发现机制，可帮助您针对不受 SA 管理的应用程序和软件进行审核和快照创建。“发现的软件” 规则可以：

- 发现当前不受 SA 管理的未注册软件。
- 创建未作为 OS 注册的应用程序一部分安装或自定义构建的软件的库存。
- 使您能够创建在服务器上发现的软件的快照，然后定期根据快照对其执行审核。
- 使您能够跟踪内部或自定义构建软件。

要配置发现的软件规则，请执行以下操作：

1 使用创建审核 （第 19 页）中的一种方法创建新审核。（如果要为快照规范创建此规则，请参见创建快照规范 （第 115 页）。）

2 选择审核源：服务器、快照、快照规范或无源。

3 在 “审核” 窗口的 “视图” 窗格中，选择 “规则” > “发现的软件”。

4 在 “审核” 窗口的内容窗格中，展开 “可用于审核” 部分的 “软件” 图标。如果这是首次加载此规则且已选定审核或快照的源，则加载会花一些时间。

5 从列表中选择一个元素，然后单击向右箭头按钮将规则对象移到 “为审核选定” 部分，这样可创建此元素的规则。

6 对于要在规则中配置的每个检查，可在 “审核” 窗口的下半部分中选择以下规则条件类型之一：

   - **属性值**：用于检查目标对象的单个属性的基于值的检查。对于此类型的检查，每个对象都需要您使用规则窗口底部的下拉列表构建表达式，用于定义与此对象相关的属性。可指定唯一的运算符，运算符可以是字符串、数字 （整数或浮点数）、布尔值 （“true” 和 “false” 比较值）、日期 （日期比较而非时间比较）或数组，具体取决于对象类型。
   - **等同于源**：对位于源服务器和目标服务器上的对象执行一对一比较的比较检查。在这种类型的检查中，从源服务器和目标服务器选择的每个属性值必须与要符合的对象完全匹配。
   - **不存在**：检查对象是否不存在以确定该对象是否在目标服务器上存在的规则。如果该对象在目标服务器上存在，则该用户或组的规则不符合要求。请注意，在运行时不会查询源服务器（如果有）。此外，如果选择了通配符规则对象，则将仅应用于目标服务器。

7 也可以通过选择通配符规则对象  ，基于通配符搜索配置规则。选择此对象后，在窗口底部的规则配置部分会显示 “名称” 字段，可在其中键入用于在目标服务器上进行搜索的名称（主键）。

   例如，可通过简单输入 * 匹配目标服务器上的所有对象，输入 P* 将匹配所有以大写 P 开头的对象，而输入 *P 将匹配所有以大写字母 “P” 结尾的元素。

   输入名称或通配符字符串后，可按照步骤 6 中的相应操作配置规则参数。

   非常值得注意的是，使用通配符时，所有匹配的对象都受规则配置的限制。如果所有找到的对象均匹配规则参数，则此类型的审核规则视为符合。

8 要完成审核配置，则设置该审核的目标服务器、任何规则异常、计划和通知。

9 要保存审核，请从 “文件” 菜单中，选择 “保存”。也可将 “审核” 保存为策略，这样可允许其他用户访问在此审核中创建的规则集。有关详细信息，请参见将审核或快照规范保存为审核策略 （第 85 页）。

10 要运行审核，请从 “操作” 菜单中，选择 “运行审核”。有关运行审核的详细信息，请参见运行审核 （第 21 页）。

配置文件规则

通过使用文件规则，可以通过指定以下选项来审核和比较目标服务器上的文件和目录：

- **目录名称**：选定文件或目录的绝对路径。

  
  （*可选*）可将引用添加到环境变量 (`${varName}`) 或自定义特性 (`@varName@`) 中。请参见参数化 SA/ 自定义特性的文件名 （第 75 页）和路径名中的环境变量 （第 77 页）。

- **范围**：默认范围是目录和文件。“目录选项” 窗格中的 “范围示例” 图表显示了基于选定选项的范围用例层次结构。此图表未显示排除项。单击 “查看排除项” 查看 “设置包含项 / 排除项” 窗口中的排除项。

  递归目录结构 — 包括此审核选定文件系统文件夹中所有子目录的内容，如目录和文件 （递归）、仅文件 （递归）及仅目录 （递归）。

  包括目录 — 指定文件系统中要包含在审核内和排除在审核外的目录。请参见文件包含项和排除项规则 （第 71 页）。

  包括文件 — 指定文件系统中要包含在审核内和排除在审核外的文件。请参见文件包含项和排除项规则 （第 71 页）。

  以下列表按优先级顺序列出了 8 种常见用例。请参见以下带图表的常见范围用例：

  范围用例 1：目录和文件 （递归）（第 48 页）

  范围用例 2：目录和文件 （默认）（第 48 页）

  范围用例 3：仅文件 （第 48 页）

  范围用例 4：文件 （递归）（第 49 页）

  范围用例 5：目录 （递归）（第 49 页）

  范围用例 6：仅目录 （第 49 页）

  范围用例 7：仅目录 （第 50 页）

  范围用例 8：仅递归 （第 50 页）

- **检查差异**：

  按属性

  校验和：对目录中选定文件的内容执行校验和。可选择审核整个文件内容 （完整）或仅文件的第一个 1MB 的内容 （部分）。

  修改日期：审核用于文件或文件夹比较的文件修改日期。

  用户和组访问权 *（仅适用于 Unix）*：审核与文件和目录相关的用户和组访问权限。

Windows ACL *（仅适用于 Windows）*：审核文件和目录的 Windows 访问控制列表 (ACL)。

注意：如果正在检查文件规则的 ACL，而用户和组的 ACL 在目标上不存在，则在审核和修正进程完成后，将创建一个临时用户和组并为其指定一个未知名称。下次运行审核时，用户和组将显示为未知。有关修正的详细信息，请参见审核结果 （第 86 页）。

版本号：对于特定的 Windows 文件类型（.exe、.dll、.ocx、.olb、.scr、.rll、.sys、.drv、.acm），文件创建者可以设置文件版本和产品版本。此选项将对这些版本号进行比较。如果它们不同，则规则视为不符合，目标文件上的实际值可在审核结果中查看。

注意：并不是所有带有这些扩展的文件都有产品版本或文件版本特性。

存档要修正的文件：存档整个文件。此选项可使审核根据在规则中指定的差异检查指定文件的差异。如果要修正和查看所找到的规则和目标文件间的文件差异，则可使用此选项。如果找到差异，则修正差异会将源文件复制到目标服务器并使用源替换目标文件。

注意：此选项可能会根据所比较的文件的大小和数量，在 SA 核心数据库上创建磁盘空间需求。

按应用程序配置值设置：使用应用程序配置评估目标服务器上的配置文件。通过此选项（包括“高级关联设置”），可以使用配置模板比较源配置文件和目标服务器配置文件之间的任意值差异。请参见比较审核中的文件和配置模板 **（第 52 页）**。

- **修正概要**：当选定属性不匹配时，通过从源复制文件及其属性进行修正。

带图表的常见范围用例

以下示例展示了每种范围用例的 Windows 目录选项以及相关的文件系统图表。对于 Windows，“Windows ACL”选项可用。对于 Unix，“用户和组访问权”选项可用。

- 范围用例 1：目录和文件 （递归）（第 48 页）
- 范围用例 2：目录和文件 （默认）（第 48 页）
- 范围用例 3：仅文件 （第 48 页）
- 范围用例 4：文件 （递归）（第 49 页）
- 范围用例 5：目录 （递归）（第 49 页）
- 范围用例 6：仅目录 （第 49 页）
- 范围用例 7：仅目录 （第 50 页）
- 范围用例 8：仅递归 （第 50 页）

图 7 是目录和文件 （递归）所需的选项示例。

图 7　　范围用例 1：目录和文件 （递归）

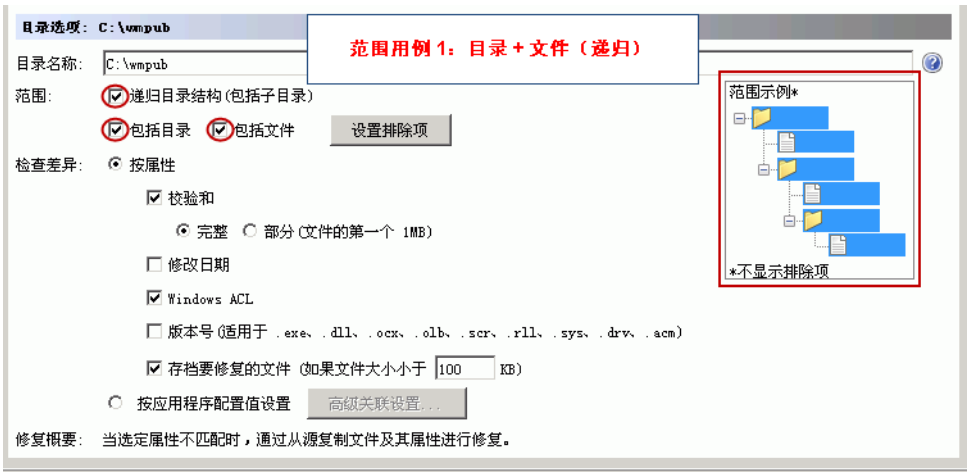


图 8 是目录和文件所需的选项示例。这些是默认选项。

图 8　　范围用例 2：目录和文件 （默认）

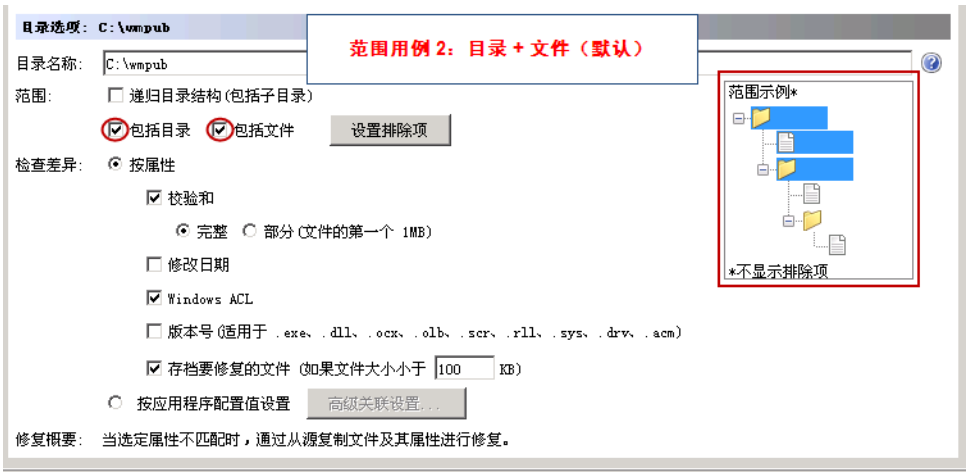


图 9 是仅文件所需的选项示例。

图 9　　范围用例 3：仅文件

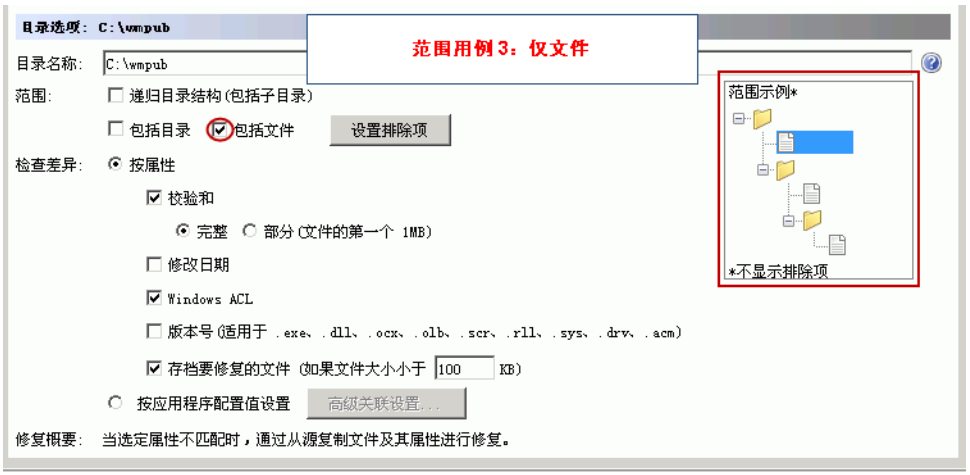


图 10 是文件 （递归）所需的选项示例。

图 10　　范围用例 4：文件 （递归）

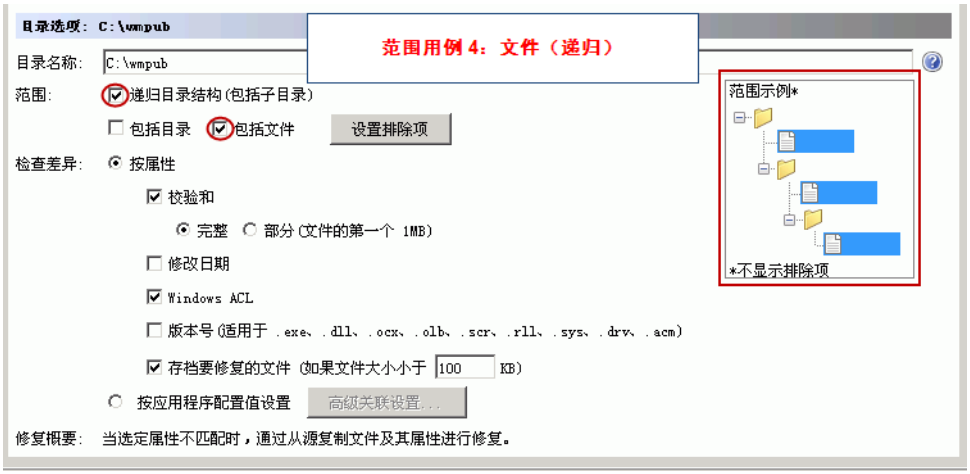


图 11 是目录 （递归）所需的选项示例。

图 11　　范围用例 5：目录 （递归）

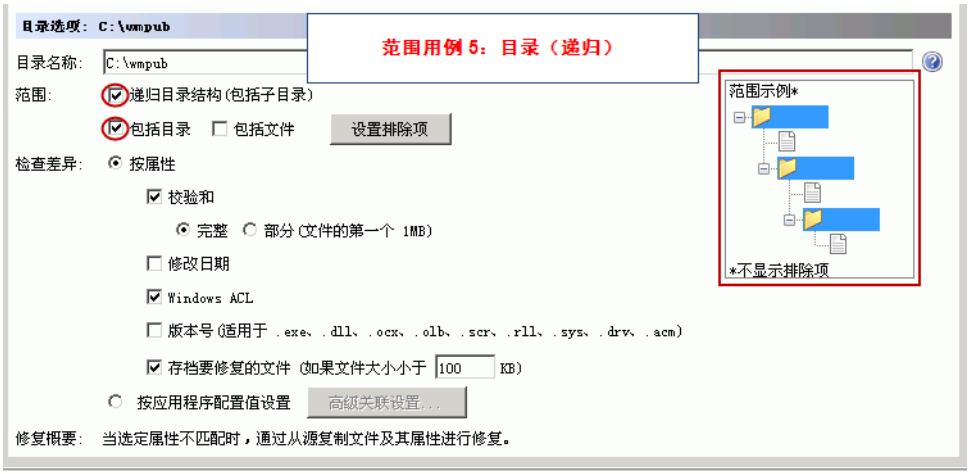


图 12 是仅目录所需的选项示例。

图 12　　范围用例 6：仅目录

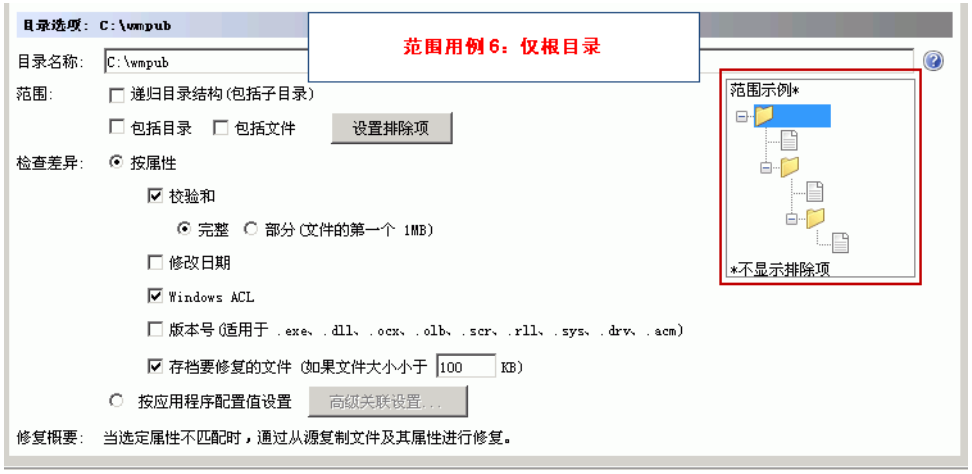


图 13 是仅目录所需的选项示例。

图 13　　范围用例 7：仅目录

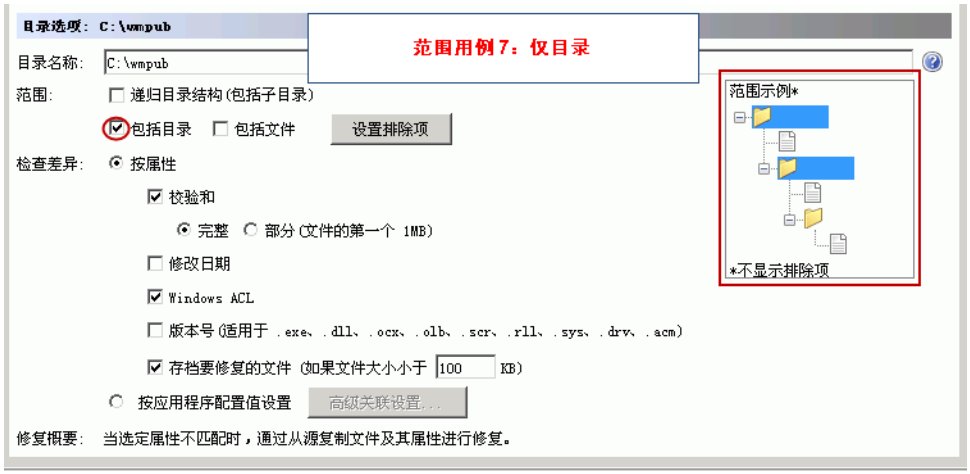
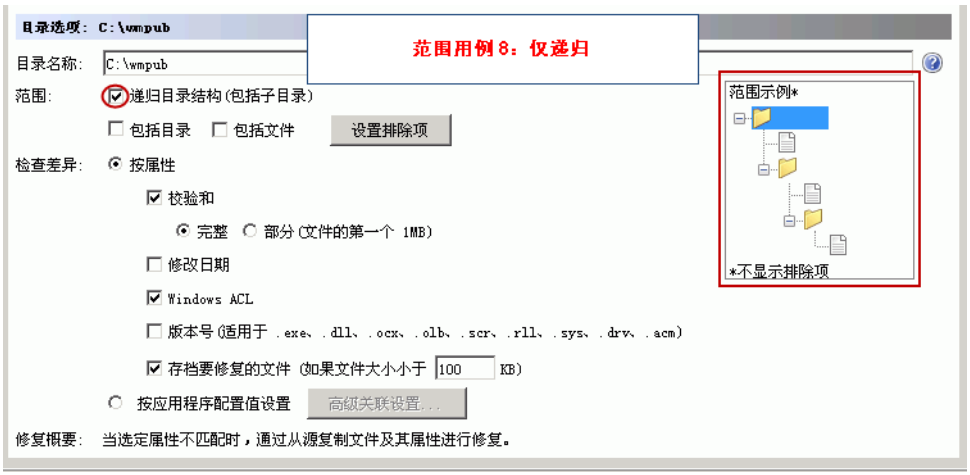


图 14 是仅递归所需的选项示例。

图 14　　范围用例 8：仅递归



将规则添加到审核的方法

有几种方法可将规则添加到审核。

您可以：

- （**推荐**）链接到现有审核策略。请参见将审核策略链接到审核或快照规范 （第 82 页）和将审核策略链接到主审核策略 （第 83 页）。
- 导入审核策略。请参见导入审核策略规则 （第 84 页）。
- 选择审核内的规则。

要配置文件规则，请执行以下操作：

1. 使用创建审核（第 19 页）中的一种方法创建新审核。如果要为快照规范创建此规则，请参见创建快照规范 （第 115 页）。
2. 指定将与目标值比较的参考数据源。

最佳实践：该源应代表此服务器或其应用程序的理想配置。

a 在 “审核” 窗口的 “视图” 窗格中，选择 “源”。

b 在 “源” 窗格中，指定将与目标值比较的引用数据的源，如 “无源”、“服务器”、“快照 - 所有目标针对同一快照” 或 “快照规范 - 每个目标针对最新快照”。如果选择快照，则仅可以比较快照中捕获的那些文件。应用程序配置和 Windows 用户和组等一些审核规则必须具有源。

基于所选的 “源”，将显示以下窗口之一：

如果选择 “服务器”，则显示 “选择服务器” 窗口。

如果选择 “快照 - 所有目标针对同一快照”，则显示 “选择快照” 窗口。

如果选择 “快照规范 - 每个目标针对最新快照”，则显示 “选择快照规范” 窗口。

c 进行选择，然后单击 “确定” 保存设置并关闭选择窗口。

3 选择文件规则：

a 在 “审核” 窗口的 “视图” 窗格中，选择 “规则” > “文件”。

（*推荐*）在 “规则” 内容窗格中，单击  打开 “选择审核策略” 窗口。选择一个策略，然后单击 “确定”。

最佳实践：此选择可允许创建*链接的规则*，即指向现有审核规则的链接。这意味着对该策略做出的所有更改都将在此审核规则中反映出来。

或

b （*可选*）如果要创建*未链接的规则*，则选中 “启用未链接的规则 (防止链接到预定义的审核策略)”。

在 “规则” 内容窗格中，单击 “导入规则” 打开 “选择审核策略” 窗口。选择一个策略，然后单击 “确定”。

或

c （*可选*）在审核或审核策略中，选中 “启用未链接的规则 (防止链接到预定义的审核策略)”。

单击  打开 “选择文件” 窗口。展开文件系统并选择文件或目录。单击 “确定” 将选定规则添加到审核。

4 选择要审核的文件和目录：

a 在 “审核” 窗口的 “视图” 窗格中，选择 “规则” > “文件”。

在 “源服务器” 内容窗格中，单击  打开 “选择文件” 窗口。

b 在 “可用于审核” 部分中，展开顶级节点并选择要在其中应用规则的文件夹或文件。

c 进行选择，然后单击 “选择” 保存设置并关闭 “选择文件” 窗口。

或

a 在 “审核” 窗口的 “视图” 窗格中，选择 “规则” > “文件”。

在 “源服务器” 内容窗格中，选择文件或目录以修改详细信息窗格中的 “文件选项” 或 “目录选项”。

b （*可选*）对于文件夹，可选择 “文件 / 目录通配符” 选项指定要包含在审核内或从审核中排除的文件和目录。

c 单击  添加新规则或单击 删除规则。有关如何输入文件和目录以及此操作如何影响审核的详细信息，请参见文件包含项和排除项规则 （第 71 页）。

5 （*可选*）如果要使用应用程序配置来比较配置文件，请选择 “按应用程序配置值设置”，然后单击 “高级关联设置”。

在 “AppConfig 文件比较关联” 窗口中，从 “AppConfig 模板” 列表，选择要用于比较源配置文件和目标配置文件的模板。在 “关联的文件” 部分中，使用源配置文件的默认路径或对该路径进行编辑。单击  为要与目标配置文件进行比较的源配置文件添加其他路径。

完成后，单击 “确定”。

6 要完成审核配置，则设置该审核的目标服务器、计划和通知。

7 要保存审核，请从 “文件” 菜单中，选择 “保存”。也可将 “审核” 保存为策略。有关详细信息，请参见将审核或快照规范保存为审核策略 （第 85 页）。

8 要运行审核，请从 “操作” 菜单中，选择 “运行审核”。有关运行审核的详细信息，请参见创建审核策略 （第 81 页）。

注意：使用 “刷新” 按钮刷新 “选择文件” 屏幕。

比较审核中的文件和配置模板

在目标服务器上审核文件的另一种方式是，以应用程序配置 (AppConfig) 模板为基础，将文件与源服务器文件进行比较。

配置模板将构建配置文件架构的模型并确定其内容和组织。当在审核的文件规则中使用配置模板以比较文件时，审核使用配置模板筛选要比较的源文件和目标文件的内容。这将确保在运行审核并比较文件时，仅比较模板中定义的值设置。

例如，可能要比较几个目标服务器上的 `/etc/passwd` 文件，以确保它们仅包含*黄金服务器*（即已知含有可接受值的服务器）的 `/etc/passwd` 文件中定义的值。使用配置文件比较功能，选择构建 `/etc/passwd` 文件 (`passwd.tpl`) 模型的配置模板，然后将该配置模板与在黄金源服务器和审核的目标服务器上的实际 `passwd` 文件相关联。

通过选择模板然后输入文件在目标服务器上的文件路径名来创建关联。还可使用此功能比较多个文件。例如，可选择已知含有几个配置文件的目录进行比较，并且可将配置模板与已知含有要比较的文件的目录相关联。

要在审核中使用配置文件比较功能，请执行以下操作：

1 使用创建审核 （第 19 页）中的一种方法创建新审核。

2 指定将与目标值比较的参考数据源。

最佳实践：该源应代表此服务器或其应用程序的理想配置。

a 在 “审核” 窗口的 “视图” 窗格中，选择 “源”。

b 在 “源” 窗格中，指定将与目标值比较的引用数据的源，如 “无源”、“服务器”、“快照 - 所有目标针对同一快照” 或 “快照规范 - 每个目标针对最新快照”。如果选择快照，则仅可以比较快照中捕获的那些文件。应用程序配置和 Windows 用户和组等一些审核规则必须具有源。

基于所选的 “源”，将显示以下窗口之一：

如果选择 “服务器”，则显示 “选择服务器” 窗口。

如果选择 “快照 - 所有目标针对同一快照”，则显示 “选择快照” 窗口。

如果选择 “快照规范 - 每个目标针对最新快照”，则显示 “选择快照规范” 窗口。

c 进行选择，然后单击 “确定” 保存设置并关闭选择窗口。

3 在 “审核” 窗口的 “视图” 窗格中，选择 “规则” > “文件”。

4 在 “审核” 窗口的详细信息窗格中，选择 “按应用程序配置值设置” ，然后单击 “高级关联设置”。

5 在 “AppConfig 文件比较关联” 窗口中，从 “AppConfig 模板” 列表，选择要用于比较源配置文件和目标配置文件的模板。在 “关联的文件” 部分中，使用源配置文件的默认路径或对该路径进行编辑。单击  为要与目标配置文件进行比较的源配置文件添加其他路径。

6 在 “关联的文件” 部分中，输入实际源和目标配置文件在源和目标服务器上的路径名。

注意：要使用配置模板进行比较的文件必须位于相同的路径中。

7 （*可选*）如果要为模板制作多个关联，请单击  添加其他目录。每个添加的目录都会应用到在 “AppConfig 模板” 部分中选择的任何模板。可在此窗口中根据需要制作多个关联。

8 完成后，单击 “确定”。

9 要完成审核配置，则设置该审核的目标服务器、计划和通知。

10 要保存审核，请从 “文件” 菜单中，选择 “保存”。也可将 “审核” 保存为策略。有关详细信息，请参见将审核保存为审核策略 （第 82 页）。

11 要运行审核，请从 “操作” 菜单中，选择 “运行审核”。有关运行审核的详细信息，请参见创建审核策略 （第 81 页）。

配置硬件规则

通过配置硬件规则，可以审核有关服务器硬件的以下信息：

- **接口**：比较服务器上的双工不匹配和所有网络接口。
- **CPU**：比较目标服务器的 CPU 类型和规格。
- **内存**：比较目标服务器的内存。
- **存储**：比较目标服务器上的存储容量。
- **接口**：比较附加到设备的所有网络接口。

如果在最近刚安装 SA 代理的服务器上对 “硬件” 规则进行审核或快照创建，则硬件可能尚未完全在模型库中注册，将无法针对准确的硬件信息进行审核或快照创建。（SA 代理通常在代理安装后的 24 小时内注册硬件。）如果不确定，请与 SA 管理员或在服务器上安装 SA 代理的人员联系。有关如何手动注册服务器硬件的说明，请参见 《SA 用户指南：Server Automation》。

要配置硬件规则，请执行以下操作：

1. 使用创建审核 （第 19 页）中所列的其中一种审核创建方法创建新审核。（如果要为快照规范创建此规则，请参见创建快照规范 （第 115 页）。）
2. 选择审核源：服务器、快照、快照规范或无源。（应用程序配置和 Windows 用户和组等一些审核规则必须具有源。）
3. 在 “审核” 窗口的 “视图” 窗格中，选择 “规则” > “硬件”。
4. 在 “审核” 窗口的内容窗格中，展开 “可用于审核” 部分的顶级节点，然后选择要为其创建规则的硬件类别。
5. 单击向右箭头按钮将硬件项移动到 “为审核选定” 部分。所有选定项将用于对目标服务器进行审核或快照创建。
6. 要完成审核配置，则设置该审核的目标服务器、计划和通知。
7. 要保存审核，请从 “文件” 菜单中，选择 “保存”。也可将 “审核” 保存为策略。有关详细信息，请参见将审核或快照规范保存为审核策略 （第 85 页）。
8. 要运行审核，请从 “操作” 菜单中，选择 “运行审核”。有关运行审核的详细信息，请参见创建审核策略 （第 81 页）。

配置 IIS 元数据库规则

通过使用 IIS 元数据库审核规则，可以选择要在审核中进行比较的 IIS 元数据库对象和对象文件夹。此审核将捕获 IIS 元数据库对象属性信息，如 ID、名称、路径、特性等。

如果要检查元数据库规则的 ACL，但用户和组 ACL 不存在，则在运行审核并进行修正后，如果用户和组在目标上不存在，则会创建未知名称的临时用户和组。下次运行该审核时，它将显示为未知，将显示名称而非源用户。

另外，如果从源服务器创建 IIS 元数据库规则，且为规则选定的元数据库对象从父元数据库对象继承了其值，则在审核运行后将显示差异。例如，修正一次后重新运行审核，如果源键在目标服务器上创建时未进行继承且特性具有 IED，则对象将根据父键的继承进行创建。当重新运行此审核时，结果会将 IED 显示为对象特性的差异。

有关修正的详细信息，请参见审核结果 （第 86 页）。

如果要在 Windows Server 2008 服务器上审核 Microsoft IIS 7.0，请在审核中创建和配置 IIS 7.0 规则。请参见配置 IIS 7.0 规则 （第 56 页）。

要配置 IIS 元数据库规则，请执行以下操作：

1. 使用创建审核 （第 19 页）中所列的其中一种审核创建方法创建新审核。（如果要为快照规范创建此规则，请参见创建快照规范 （第 115 页）。）
2. 选择审核源：服务器、快照、快照规范或无源。（应用程序配置和 Windows 用户和组等一些审核规则必须具有源。）
3. 在 “审核”窗口的 “视图”窗格中，选择 “规则” > “IIS 元数据库”。
4. 在 “审核”窗口的内容窗格中，展开 “可用于审核”部分的顶级节点，然后选择要为其创建规则的 IIS 元数据库文件夹或对象。（可为规则选择任意元数据库文件夹或对象，但不能将 root 文件夹选作规则。）
5. 单击向右箭头按钮将 IIS 元数据库文件夹或对象移动到 “为审核选定”部分。所有选定项将用于对目标服务器进行审核或快照创建。
6. 要完成审核配置，则设置该审核的目标服务器、计划和通知。
7. 要保存审核，请从 “文件”菜单中，选择 “保存”。也可将 “审核”保存为策略。有关详细信息，请参见将审核或快照规范保存为审核策略 （第 85 页）。
8. 要运行审核，请从 “操作”菜单中，选择 “运行审核”。有关运行审核的详细信息，请参见创建审核策略 （第 81 页）。

配置 IIS 规则

通过使用 Microsoft Internet Information Server 规则，可以将有关 IIS 的实时信息用于审核，如 Windows 服务器、服务器名称、服务器类型、服务器状态、日志文件路径、文档文件路径等。

要配置 Internet Information Server 规则，请执行以下操作：

1. 使用创建审核 （第 19 页）中的一种方法创建新审核。（如果要为快照规范创建此规则，请参见创建快照规范 （第 115 页）。）
2. 选择审核源：服务器、快照、快照规范或无源。（应用程序配置和 Windows 用户和组等一些审核规则必须具有源。）
3. 在 “审核”窗口的 “视图”窗格中，选择 “规则” > “Internet Information Server”。
4. 在 “审核”窗口的内容窗格中，展开 “可用于审核”部分的顶级节点，然后选择要从中创建规则的 Internet Information Server 规则。
5. 单击向右箭头按钮将规则对象移动到 “为审核选定”部分。配置的所有 Internet Information Server 规则都将在目标服务器或快照规范上进行审核。
6. 针对每个规则，选择以下检查类型之一：
   - **属性值**：用于检查目标对象的单个属性的基于值的检查。对于此类型的检查，每个对象都需要您使用规则窗口底部的下拉列表构建表达式，用于定义与此对象相关的属性。可指定唯一的运算符，运算符可以是字符串、数字 （整数或浮点数）、布尔值 （“true”和 “false”比较值）、日期 （日期比较而非时间比较）或数组，具体取决于对象类型。

- **等同于源**：对位于源服务器和目标服务器上的对象执行一对一比较的比较检查。在这种类型的检查中，从源服务器和目标服务器选择的每个属性值必须与要符合的对象完全匹配。
- **不存在**：检查对象是否不存在以确定该对象是否在目标服务器上存在的规则。如果该对象在目标服务器上存在，则该用户或组的规则不符合要求。请注意，在运行时不会查询源服务器（如果有）。此外，如果选择了通配符规则对象，则将仅应用于目标服务器。

7 也可以通过选择通配符规则对象  ，基于通配符搜索配置规则。选择此对象后，在窗口底部的规则配置部分会显示 “名称” 字段，可在其中键入用于在目标服务器上进行搜索的名称（主键）。

例如，可通过简单输入 * 匹配目标服务器上的所有对象，输入 P* 将匹配所有以大写 P 开头的对象，而输入 *P 将匹配所有以大写字母 “P” 结尾的元素。

输入名称或通配符字符串后，可按照步骤 6 中的相应操作配置规则参数。

非常值得注意的是，使用通配符时，所有匹配的对象都受规则配置的限制。如果所有找到的对象均匹配规则参数，则此类型的审核规则视为符合。

8 要完成审核配置，则设置该审核的目标服务器、任何规则异常、计划和通知。

9 要保存审核，请从 “文件” 菜单中，选择 “保存”。也可将 “审核” 保存为策略。请参见将审核或快照规范保存为审核策略 （第 85 页）。

10 要运行审核，请从 “操作” 菜单中，选择 “运行审核”。请参见创建审核策略 （第 81 页）。

配置 IIS 7.0 规则

在 SA 9.10 中，可为在 Windows Server 2008 上运行的 Microsoft IIS 7.0 创建审核和快照规范。可展开并搜索 IIS 7.0 应用程序池、网站和功能，然后将它们添加到审核或快照规范，以确定它们是否符合组织的符合性标准。审核或快照运行后，可以查看结果并修正找到的所有差异 （存在一些例外情况）。

例如，您可能要审核运行 IIS 7.0 的 Windows Server 2008 服务器，以确保每个服务器上均已启用 “匿名身份验证”。

要执行此符合性检查，请将已启用 “匿名身份验证” 的 Windows Server 2008 服务器选为审核的*源*服务器。然后，配置审核规则以检查审核的所有目标服务器上是否已启用 “匿名身份验证”。

运行审核时 （可计划重复运行），规则将检查目标服务器并找出任何未启用 “匿名身份验证” 的服务器。如果审核发现任何差异，则可以通过修正这些服务器来启用它们的 IIS 7.0 匿名身份验证。

➤ 无法在此发布中修正 IIS 7.0 审核规则的 ISAPI 过滤器。

要配置 IIS 7.0 规则，请执行以下操作：

1 使用创建审核 （第 19 页）中的一种方法创建新审核。（如果要为快照规范创建此规则，请参见创建快照规范 （第 115 页）。）

2 选择审核源：服务器、快照、快照规范或无源。

应用程序配置和 Windows 用户和组等一些审核规则类型必须具有作为规则基础的源服务器。检查 IIS 7.0 匿名身份验证等一些特定规则和条件也需要选择源服务器。如果未选择源服务器，则将局限于规则的特定性。

3 在 “审核”窗口的 “视图”窗格中，选择 “规则” > “IIS 7.0”。

4 在 “审核”窗口的内容窗格中，从 “可用于审核”部分展开要为其创建规则的其中一个 IIS 7.0 元素，如应用程序池、站点或功能。如果这是首次加载元素，则可能会花一些时间。

5 从列表中选择一个元素，然后单击向右箭头按钮将规则对象移到 “为审核选定”部分，这样可创建此元素的规则。例如，可以展开 “身份验证”文件夹并选择 “匿名身份验证”，然后单击向右箭头按钮将选择添加到审核中。

6 对于每个规则，可在 “审核”窗口的下半部分选择以下规则条件类型之一：

- **属性值**：用于检查目标对象的单个属性的基于值的检查。对于此类型的检查，每个对象都需要您使用规则窗口底部的下拉列表构建表达式，用于定义与此对象相关的属性。可指定唯一的运算符，运算符可以是字符串、数字 （整数或浮点数）、布尔值 （“true”和 “false”比较值）、日期 （日期比较而非时间比较）或数组，具体取决于对象类型。
- **等同于源**：对位于源服务器和目标服务器上的对象执行一对一比较的比较检查。在这种类型的检查中，从源服务器和目标服务器选择的每个属性值必须与要符合的对象完全匹配。

  IIS 7.0 规则的修正仅在使用等同于源的检查设置审核时才可实现。
- **不存在**：检查对象是否不存在以确定该对象是否在目标服务器上存在的规则。如果该对象在目标服务器上存在，则该用户或组的规则不符合要求。请注意，在运行时不会查询源服务器（如果有）。此外，如果选择了通配符规则对象，则将仅应用于目标服务器。

例如，如果您要检查运行 IIS 7.0 的目标服务器 （或多个服务器）是否启用 “匿名验证”，则可在 “审核”窗口底部选择：

- 属性值
- 状态
- =
- 已启用

这指示审核查看每个目标服务器的 IIS 7.0 匿名身份验证是否已启用。

7 也可以通过选择通配符规则对象  ，基于通配符搜索配置规则。选择此对象后，在窗口底部的规则配置部分会显示 “名称”字段，可在其中键入用于在目标服务器上进行搜索的名称（主键）。

例如，可输入星号 (*)，匹配目标上的一切。P* 将匹配所有以大写 P 开头的对象，而 *P 则将匹配所有以大写字母 P 结尾的元素。

输入名称或通配符字符串后，可按照步骤 6 中的相应操作配置规则参数。

非常值得注意的是，使用通配符时，所有匹配的对象都受规则配置的限制。如果所有找到的对象均匹配规则参数，则此类型的审核规则视为符合。

8 要完成审核配置，则设置该审核的目标服务器、任何规则异常、计划和通知。

9 要保存审核，请从 “文件” 菜单中，选择 “保存” 。也可将 “审核” 保存为策略，这样可允许其他用户访问在此审核中创建的规则集。请参见将审核或快照规范保存为审核策略（第 85 页）。

10 要运行审核，请从 “操作” 菜单中，选择 “运行审核”。请参见运行审核 （第 21 页）。

配置本地安全设置规则

通过使用 “本地安全设置” 规则，可以使用有关安全设置的实时信息，如密码策略、审核策略、用户权限和规则中的安全选项。

要配置 “本地安全设置” 规则，请执行以下操作：

1 使用创建审核 （第 19 页）中的一种方法创建新审核。（如果要为快照规范创建此规则，请参见创建快照规范 （第 115 页）。）

2 选择审核源：服务器、快照、快照规范或无源。（应用程序配置和 Windows 用户和组等一些审核规则必须具有源。）

3 在 “审核” 窗口的 “视图” 窗格中，选择 “规则” > “本地安全设置”。

4 在 “审核” 窗口的内容窗格中，展开 “可用于审核” 部分的顶级节点，然后选择要从中创建规则的 Internet Information Server 规则。

5 单击向右箭头按钮将规则对象移动到 “为审核选定” 部分。配置的所有 Internet Information Server 规则都将在目标服务器或快照规范上进行审核。

6 针对每个规则，选择以下检查类型之一：

- **属性值**：用于检查目标对象的单个属性的基于值的检查。对于此类型的检查，每个对象都需要您使用规则窗口底部的下拉列表构建表达式，用于定义与此对象相关的属性。可指定唯一的运算符，运算符可以是字符串、数字 （整数或浮点数）、布尔值 （“true” 和 “false” 比较值）、日期 （日期比较而非时间比较）或数组，具体取决于对象类型。
- **等同于源**：对位于源服务器和目标服务器上的对象执行一对一比较的比较检查。在这种类型的检查中，从源服务器和目标服务器选择的每个属性值必须与要符合的对象完全匹配。
- **不存在**：检查对象是否不存在，以确定该对象是否在目标服务器上不存在。如果该对象在目标服务器上存在，则该规则不符合要求。例如，可以检查服务器以确保该服务器不包含特定 COM+ 对象。请注意，在运行时不会查询源服务器 （如果有）。此外，如果选择了通配符规则对象，则将仅应用于目标服务器。

7 也可以通过选择通配符规则对象  ，基于通配符搜索配置规则。选择此对象时，“名称”字段会显示在窗口底部的规则配置部分中。输入将在目标服务器上进行搜索的名称 （主键）。

例如，可通过简单输入 * 匹配目标服务器上的所有对象，输入 P* 将匹配所有以大写 P 开头的对象，而输入 *P 将匹配所有以大写字母 “P”结尾的元素。

输入名称或通配符字符串后，可按照步骤 6 中的相应操作配置规则参数。

非常值得注意的是，使用通配符时，所有匹配的对象都受规则配置的限制。如果所有找到的对象均匹配规则参数，则此类型的审核规则视为符合。

8 要完成审核配置，则设置该审核的目标服务器、任何规则异常、计划和通知。

9 要保存审核，请从 “文件”菜单中，选择 “保存”。也可将 “审核”保存为策略。请参见将审核或快照规范保存为审核策略 （第 85 页）。

10 要运行审核，请从 “操作”菜单中，选择 “运行审核”。请参见运行审核 （第 21 页）。

配置注册软件规则

通过使用 “注册软件”规则，可使用实际安装在源服务器上的所有已安装程序包或修补程序来构建规则，而无论修补程序或程序包是否已由 SA 模型库注册。

要配置 “注册软件”规则，请执行以下操作：

1 使用创建审核 （第 19 页）中的一种方法创建新审核。（如果要为快照规范创建此规则，请参见创建快照规范 （第 115 页）。）

2 选择审核源：服务器、快照、快照规范或无源。（应用程序配置和 Windows 用户和组等一些审核规则必须具有源。）

3 在 “审核”窗口的 “视图”窗格中，选择 “规则” > “已注册软件”。

4 在 “审核”窗口的内容窗格中，展开 “可用于审核”部分的顶级节点，然后选择要从中创建规则的修补程序或程序包。

5 单击向右箭头按钮将规则对象移动到 “为审核选定”部分。配置的所有规则都将在目标服务器或快照规范上进行审核。

6 针对每个规则，选择以下检查类型之一：

- **属性值**：用于检查目标对象的单个属性的基于值的检查。对于此类型的检查，每个对象都需要您使用规则窗口底部的下拉列表构建表达式，用于定义与此对象相关的属性。可指定唯一的运算符，运算符可以是字符串、数字 （整数或浮点数）、布尔值 （“true”和 “false”比较值）、日期 （日期比较而非时间比较）或数组，具体取决于对象类型。
- **等同于源**：对位于源服务器和目标服务器上的对象执行一对一比较的比较检查。在这种类型的检查中，从源服务器和目标服务器选择的每个属性值必须与要符合的对象完全匹配。

- **不存在**：检查对象是否不存在以确定该对象是否在目标服务器上存在的规则。如果该对象在目标服务器上存在，则该用户或组的规则不符合要求。请注意，在运行时不会查询源服务器（如果有）。此外，如果选择了通配符规则对象，则将仅应用于目标服务器。

7 也可以通过选择通配符规则对象  ，基于通配符搜索配置规则。选择此对象时，“名称”字段会显示在窗口底部的规则配置部分中。输入将在目标服务器上进行搜索的名称 （主键）。

例如，可输入星号 (*)，匹配目标上的一切。P* 将匹配所有以大写 P 开头的对象，而 *P 则将匹配所有以大写字母 P 结尾的元素。

输入名称或通配符字符串后，可按照步骤 6 中的相应操作配置规则参数。

非常值得注意的是，使用通配符时，所有匹配的对象都受规则配置的限制。如果所有找到的对象均匹配规则参数，则此类型的审核规则视为符合。

8 要完成审核配置，则设置该审核的目标服务器、任何规则异常、计划和通知。

9 要保存审核，请从 “文件”菜单中，选择 “保存”。也可将 “审核”保存为策略。请参见将审核或快照规范保存为审核策略 （第 85 页）。

10 要运行审核，请从 “操作”菜单中，选择 “运行审核”。请参见运行审核 （第 21 页）。

配置存储规则

通过使用 “存储”规则，可以审核服务器的存储设备、 SAN 设备和数据中心中的连接，前提是您的核心已配置为连接到 SE。

要审核 SAN 对象并为其创建快照，需要 Storage Essentials (SE) 6.1.1 版或更高版本，且必须在 SA 核心上安装和配置 Server Automation SE Connector 组件。有关详细信息，请联系 SA 管理员或参见存储可见性与自动化文档。

要配置 “存储”规则，请执行以下操作：

1 使用创建审核 （第 19 页）中的一种方法创建新审核。（如果要为快照规范创建此规则，请参见创建快照规范 （第 115 页）。）

2 选择审核源：服务器、快照、快照规范或无源。（应用程序配置和 Windows 用户和组等一些审核规则必须具有源。）

3 在 “审核”窗口的 “视图”窗格中，选择 “规则” > “存储”。

4 在 “审核”窗口的内容窗格中，展开 “可用于审核”部分的顶级节点，然后选择要从中创建规则的“存储”规则。每个存储审核规则检查每个类别的可接受值。可配置该规则以检查最小值、最大值或确切数字。

- **未装载的卷容量**：可接受的未装载卷总容量 （以字节为单位）。
- **未装载的卷计数**：可接受的未装载卷数。
- **网络结构**：可接受的网络结构数。
- **FCA**：可接受的光纤通道适配器 (FCA) 数。
- **发起程序端口**：可接受的发起程序端口数
- **交换机**：可接受的 SAN 交换机数。

- **目标端口**：可接受的目标端口数。
- **RAID 类型**：目标存储阵列上可接受的 RAID 类型。（**注意**：如果规则已选定但未指定 RAID 类型，则审核将失败。）

涉及端口、交换机或网络结构的符合性规则仅检查活动端口。这些类型的符合性规则不检查物理端口连接性。

5 单击向右箭头按钮将规则对象移动到 “为审核选定” 部分。配置的所有 “存储” 规则都将在目标服务器或快照规范上进行审核。

6 针对每个规则，选择以下检查属性之一：

- 运算符，如等于 (=)、小于 (<)、小于等于 (<=) 等。
- 基于规则类型的值，如数字。

7 要完成审核配置，则设置该审核的目标服务器、任何规则异常、计划和通知。

8 要保存审核，请从 “文件” 菜单中，选择 “保存”。也可将 “审核” 保存为策略。请参见将审核或快照规范保存为审核策略 （第 85 页）。

9 要运行审核，请从 “操作” 菜单中，选择 “运行审核”。请参见运行审核 （第 21 页）。

配置 Windows .NET Framework 配置规则

通过使用 “Windows .NET Framework 配置” 规则，可以使用有关配置集缓存和已配置的配置集列表的实时信息，如审核中的配置集名称、版本、区域设置、公共密钥标记、缓存文件 （GAC 或 ZAP）、处理器体系结构、自定义和文件名称。

要配置 “Windows .NET Framework 配置” 规则，请执行以下操作：

1 使用创建审核 （第 19 页）中的一种方法创建新审核。（如果要为快照规范创建此规则，请参见创建快照规范 （第 115 页）。）

2 选择审核源：服务器、快照、快照规范或无源。（应用程序配置和 Windows 用户和组等一些审核规则必须具有源。）

3 在 “审核” 窗口的 “视图” 窗格中，选择 “规则” > “Windows .NET Framework 配置”。

4 在 “审核” 窗口的内容窗格中，展开 “可用于审核” 部分的顶级节点，然后选择要从中创建规则的 “Windows .NET Framework 配置” 规则。

5 单击向右箭头按钮将规则对象移动到 “为审核选定” 部分。配置的所有 “Windows .NET Framework 配置” 规则都将在目标服务器或快照规范上进行审核。

6 针对每个规则，选择以下检查类型之一：

- **属性值**：用于检查目标对象的单个属性的基于值的检查。对于此类型的检查，每个对象都需要您使用规则窗口底部的下拉列表构建表达式，用于定义与此对象相关的属性。可指定唯一的运算符，运算符可以是字符串、数字 （整数或浮点数）、布尔值 （“true” 和 “false” 比较值）、日期 （日期比较而非时间比较）或数组，具体取决于对象类型。
- **等同于源**：对位于源服务器和目标服务器上的对象执行一对一比较的比较检查。在这种类型的检查中，从源服务器和目标服务器选择的每个属性值必须与要符合的对象完全匹配。

- **不存在**：检查对象是否不存在以确定该对象是否在目标服务器上存在的规则。如果该对象在目标服务器上存在，则该用户或组的规则不符合要求。请注意，在运行时不会查询源服务器（如果有）。此外，如果选择了通配符规则对象，则将仅应用于目标服务器。

7 也可以通过选择通配符规则对象  ，基于通配符搜索配置规则。选择此对象后，在窗口底部的规则配置部分会显示“名称”字段，可在其中键入用于在目标服务器上进行搜索的名称（主键）。

例如，可输入星号 (*)，匹配目标上的一切。P* 将匹配所有以大写 P 开头的对象，而 *P 则将匹配所有以大写字母 P 结尾的元素。

输入名称或通配符字符串后，可按照步骤 6 中的相应操作配置规则参数。

非常值得注意的是，使用通配符时，所有匹配的对象都受规则配置的限制。如果所有找到的对象均匹配规则参数，则此类型的审核规则视为符合。

8 要完成审核配置，则设置该审核的目标服务器、任何规则异常、计划和通知。

9 要保存审核，请从“文件”菜单中，选择“保存”。也可将“审核”保存为策略。请参见将审核或快照规范保存为审核策略（第 85 页）。

10 要运行审核，请从“操作”菜单中，选择“运行审核”。请参见运行审核（第 21 页）。

配置 Windows 注册表规则

“Windows 注册表”规则是基于比较的规则，使用此规则可从审核或快照规范的源选择 Windows 注册表项或文件夹，然后将其与目标服务器进行比较。审核对选定注册表文件夹和项进行比较，然后确定这些项和文件夹是否在目标服务器上存在。无法在此规则中设置目标或修正值。

Windows 注册表对象

通过使用 Windows 注册表对象，可以捕获注册表项、注册表值和子键。注册表项是含有注册表值的目录，其中注册表值类似于目录中的文件。子键类似于子目录。SA 客户端支持以下 Windows 注册表项：HKEY_CLASSES_ROOT、 HKEY_CURRENT_CONFIG、 HKEY_LOCAL_MACHINE 和 HKEY_USERS。

为项条目（数据）的内容审核和捕获的有效控制字符包括：#x9、 #xA、 [#xD, #x20-#xD7FF]、[#xE000-#xFFFD] 和 [#x10000-#x10FFFF]。无效控制字符不能由 SA 客户端存储，并且将转换成将显示为 &#; 的 XML 实体。例如，如果数据值是 00 00（以字节为单位），则 &#x00; 将在审核或快照规范结果中显示。

访问控制级别 (ACL)

还可以选择比较“Windows 注册表”规则的访问控制级别 (ACL)。如果要检查“Windows 注册表”规则的 ACL，但其中不存在用户和组 ACL，则在运行审核并进行修正后，如果用户和组在目标上不存在，则会使用未知名称创建临时用户和组。下次运行该审核时，它将显示为未知，这并非是源用户的名称。有关详细信息，请参见审核结果（第 86 页）。

要配置 “Windows 注册表”审核规则，请执行以下操作：

1 创建新审核。有关创建审核的方法，请参见创建审核 （第 19 页）。

*（可选）*如果要为快照规范创建此规则，请参见创建快照规范 （第 115 页）。

2 选择审核源：服务器、快照、快照规范或无源。

应用程序配置和 Windows 用户和组等一些审核规则必须具有源。

3 在 “审核”窗口的 “视图”窗格中，选择 “规则” > “Windows 注册表”。

4 在 “审核”窗口的内容窗格中，展开 “可用于审核”部分的顶级节点，然后选择要为其创建规则的 Windows 注册表文件夹或项。

5 单击向右箭头按钮将 Windows 注册表文件夹或项移动到 “为审核选定”部分。所有选定项将用于对目标服务器进行审核或快照创建。

6 对于创建的每个注册表条目项规则，可在审核检查目标时设置包含以下选项：

- **同时比较子键的内容** — 评估属于选定注册表项的所有子键。
- **同时比较 ACL** — 比较选定注册表项的 ACL。
- **对键值使用不区分大小写比较** — 如果名称存在大小写区别，则不在审核结果中显示键值差异。

7 要完成审核配置，则设置该审核的目标服务器、计划和通知。

8 在 “文件”菜单中，选择 “保存”以保存审核。

*（可选）*也可将 “审核”保存为策略。请参见将审核或快照规范保存为审核策略 （第 85 页）。

9 要运行审核，请从 “操作”菜单中，选择 “运行审核”。请参见运行审核 （第 21 页）。

注意：在 “审核策略”窗口，如果选择一个服务器查看其注册表信息，然后希望查看其他服务器的注册表信息，则必须关闭 “审核策略”窗口，然后将其重新打开以刷新注册表内容字段。

配置 Windows 服务规则

“Windows 服务”规则是基于比较的规则，使用此规则可从审核或快照规范的源选择 Windows 服务，然后将其与目标服务器进行比较。审核或快照规范将选定服务与目标服务器上的服务进行比较，以确定这些服务是否存在以及是否已开始、停止或禁用。无法使用此类型规则设置目标或修正值。

要配置 “Windows 服务”审核规则，请执行以下操作：

1 创建新审核。有关创建审核的方法，请参见创建审核 （第 19 页）。

*（可选）*如果要为快照规范创建此规则，请参见创建快照规范 （第 115 页）。

2 选择审核源：服务器、快照、快照规范或无源。

应用程序配置和 Windows 用户和组等一些审核规则必须具有源。

3 在 “审核”窗口的 “视图”窗格中，选择 “规则” > “Windows 服务”。

4 在 “审核”窗口的内容窗格中，展开 “可用于审核”部分的顶级节点，然后选择要为其创建规则的 Windows 服务。可为此规则选择任何可用的服务，但不能选择所有 Windows 服务的 root 文件夹。

5 单击向右箭头按钮将选定的 Windows 服务移动到 “为审核选定”部分。所有选定项将用于在目标服务器上进行审核或快照创建。

6 要完成审核配置，则设置该审核的目标服务器、计划和通知。

7 保存审核。

8 要运行审核，请从 “操作”菜单中，选择 “运行审核”。请参见运行审核 （第 21 页）。

配置 Windows/UNIX 用户和组规则

通过使用 Windows 或 Unix 用户和组规则，可以从 Windows 和 Unix 服务器访问本地用户和组的信息。

要配置 “用户和组”规则，请执行以下操作：

1 使用创建审核 （第 19 页）中的一种方法创建新审核。（如果要为快照规范创建此规则，请参见创建快照规范 （第 115 页）。）

2 选择审核源：服务器、快照、快照规范或无源。（应用程序配置和 Windows 用户和组等一些审核规则必须具有源。）

3 在 “审核”窗口的 “视图”窗格中，选择 “规则” > “Windows/Unix 用户和组”。

4 在 “审核”窗口的内容窗格中，展开 “可用于审核”部分的顶级节点，然后选择要从中创建规则的 “用户和组”规则。

5 单击向右箭头按钮将规则对象移动到 “为审核选定”部分。配置的所有 “用户和组”规则都将在目标服务器或快照规范上进行审核。

6 针对每个规则，选择以下检查类型之一：

- **属性值**：用于检查目标对象的单个属性的基于值的检查。对于此类型的检查，每个对象都需要您使用规则窗口底部的下拉列表构建表达式，用于定义与此对象相关的属性。可指定唯一的运算符，运算符可以是字符串、数字 （整数或浮点数）、布尔值 （“true”和 “false”比较值） 、日期 （日期比较而非时间比较）或数组，具体取决于对象类型。对于一些属性类型，可从 “值选择器框”中选择值。
- **等同于源**：对位于源服务器和目标服务器上的对象执行一对一比较的比较检查。在这种类型的检查中，从源服务器和目标服务器选择的每个属性值必须与要符合的对象完全匹配。
- **不存在**：检查对象是否不存在，以确定该对象是否在目标服务器上不存在。如果该对象在目标服务器上存在，则该规则不符合要求。请注意，在运行时不会查询源服务器 （如果有）。此外，如果选择了通配符规则对象，则将仅应用于目标服务器。

7 也可以通过选择通配符规则对象  ，基于通配符搜索配置规则。选择此对象时，“名称”字段会显示在窗口底部的规则配置部分中。输入将在目标服务器上进行搜索的名称 （主键）。

例如，可输入星号 (*)，匹配目标上的一切。P* 将匹配所有以大写 P 开头的对象，而 *P 则将匹配所有名称以大写字母 P 结尾的用户。

输入名称或通配符字符串后，可按照步骤 6 中的相应操作配置规则参数。

非常值得注意的是，使用通配符时，所有匹配的对象都受规则配置的限制。如果所有找到的对象均匹配规则参数，则此类型的审核规则视为符合。

8 要完成审核配置，则设置该审核的目标服务器、任何规则异常、计划和通知。

9 要保存审核，请从 “文件” 菜单中，选择 “保存”。也可将 “审核” 保存为策略。请参见将审核或快照规范保存为审核策略 （第 85 页）。

10 要运行审核，请从 “操作” 菜单中，选择 “运行审核”。请参见运行审核 （第 21 页）。

配置符合性检查

如果订阅了 BSA Essentials 订阅服务，则可以访问多个符合性规则及其组件，内容开发者将这些称为 *符合性检查*。

可访问的检查类型取决于用户内容订阅，但可以包含特定规则，如 Microsoft Windows 的最新修补程序补充、当前管理符合性策略（例如 FISMA、萨班斯 - 奥克斯利法案）、内容开发者社区分发的用户创建检查、每日更新的漏洞内容等。

如果未订阅 BSA Essentials 订阅服务，则在审核、审核策略、快照或符合性检查编辑器中将看不到任何符合性检查。如果要查看有关内容订阅和获取符合性检查的详细信息，请与 BSA Essentials 订阅服务销售代表联系。

因为每个符合性检查都略有不同且需要有自己的配置值，所以每个检查的基本参数都需要定义目标值 （即要在服务器上查找的期望值）以及可选的修正值。

有关管理核心符合性检查 （如编辑检查属性数据或创建符合性检查分组）的详细信息，请参见符合性检查 （第 68 页）。

要在审核或快照规范中配置符合性检查，请执行以下操作：

1 使用创建审核（第 19 页）中所述的一种方法创建审核或快照。（如果要为快照规范创建此规则，请参见创建快照规范 （第 115 页）。）

2 选择审核源：服务器、快照、快照规范或无源。

3 在 “审核” 窗口中，从 “视图” 窗格展开 “规则” 对象。

4 选择 “符合性检查”  规则。

5 在 “审核” 窗口的内容窗格中，单击 “添加”  按钮。

6 在“选择检查”窗口中，通过“浏览”选项卡，可浏览符合性检查类别并为审核或快照选择检查。

或者，可选择 “搜索”选项卡，然后通过名称搜索检查。检查搜索工具将搜索检查名称和检查描述中的任何字词。例如，如果要查找所有检查最大密码长度的规则，则可在 “关键字”字段中输入 `max password`。

通过使用 “高级搜索”选项，可以为查找检查设置更具体的参数。

7 选择一个检查 （或使用 CTRL 或 SHIFT + 单击选择多个检查）后，单击 “确定”将检查添加到审核中。

8 选择检查，然后定义或设置以下参数：

输入值

一些自定义检查需要一个输入值作为目标值配置的一部分。对于这些检查，需要通过设置 true 或 false 来指定成功或失败。审核规则的 “描述”部分对建议值进行了说明。

目标值

指定审核目标服务器上的期望值，或要在快照中捕获的值。可更改以下参数：

- **运算符**：要从脚本的输出构建表达式，请选择一个运算符，如等于 (=)、不等于 (<>)、小于 (<)、大于 (>) 等。
- **引用**：选择脚本输出的源。
- **源**：将使用源服务器上的值，并将该值与在目标服务器上找到的值进行比较。
- **值**：输入自己的值。此选项使用输入的值并将其与目标服务器上返回的值进行比较。单击  图标从源服务器获取值。返回的值将显示在文本框中，可接受该值或根据需要编辑该值。
- **服务器特性**：选择比较源服务器上的服务器特性。
- **自定义特性**：选择比较目标服务器上的自定义特性。

修正值

每个修正值的设置将因规则类型的不同而不同，所以请进行相应选择。

9 要完成审核配置，则设置该审核的目标服务器、计划和通知。

10 要保存审核，请从 “文件”菜单中，选择 “保存”。也可将 “审核”保存为策略。请参见将审核或快照规范保存为审核策略 （第 85 页）。

11 要运行审核，请从 “操作”菜单中，选择 “运行审核”。请参见运行审核 （第 21 页）。

重命名符合性检查

通过右键单击菜单，可轻松地重命名审核、审核策略或快照规范中的符合性检查实例。

有关重命名符合性检查和编辑其属性的信息，请参见符合性检查 （第 68 页）。

要重命名符合性检查的名称，请执行以下操作：

1. 在导航窗格，选择 “库” > “按类型” > “审核和修正” 然后打开审核、审核策略或快照规范。
2. 在 “审核”（或 “审核策略” 或 “快照规范”）窗口的 “视图” 窗格中，选择包含自定义检查的特定规则，如 “用户和组”。
3. 在内容窗格的 “可用于审核” 部分中，选择一个自定义检查，右键单击并选择 “重命名规则” 来重命名此规则。

如果审核或快照规范链接到审核策略，则无法重命名规则检查。

从审核 / 快照规范窗口搜索符合性检查

因为 SA 核心可能包含几十个到几百个符合性检查，所以可以在 “审核” 或 “快照规范” 窗口内使用搜索工具查找所需检查。

要在审核或快照规范内搜索符合性检查，请执行以下操作：

1. 在 “审核” 或 “快照规范” 窗口中，从 “视图” 窗格展开 “规则” 对象。
2. 选择 “符合性检查” 规则。
3. 在内容窗格中，单击 “添加”。
4. 在“选择检查”窗口中，通过“浏览”选项卡，可浏览符合性检查类别并为审核或快照选择检查。
5. 选择 “搜索” 选项卡通过名称搜索检查。检查搜索工具将搜索检查名称和检查描述中的任何字词。例如，如果要查找所有检查最大密码长度的规则，则可在 “关键字” 字段中输入 `max password`。
6. 单击 “高级搜索” 链接构建更具体的搜索条件。通过使用高级搜索，可以查找文本字符串并可在检查的属性中对查询值进行限制，如安全级别、外部 ID、平台和测试 ID。单击 添加其他高级搜索参数。

   有关如何将测试 ID、安全级别或外部 ID 添加到符合性检查属性的详细信息，请参见编辑符合性检查属性 （第 68 页）。
7. 要执行搜索，请单击 “搜索”。
8. 在搜索结果中，可选择要添加到审核或快照规范的检查，然后单击 “确定”。

符合性检查

必须具有访问符合性检查编辑器的权限。要获取这些权限，请联系 SA 管理员，或者参见 《SA 管理指南》获取详细信息。

通过使用符合性检查编辑器，可以对核心的 BSA Essentials 订阅服务符合性检查的相关属性信息（元数据）进行浏览、重新分组和编辑。

例如，您的组织可能需要一个外部编码系统，该系统与针对数据中心服务器运行的所有符合性检查相关联。使用符合性检查编辑器，可以将外部 ID 添加到这些检查中。也可以为使用此外部 ID 修改的检查创建自定义分组，这样当需要访问这些检查时，便可以轻松地在自定义文件夹中找到它们。也可以将此外部 ID 用作搜索条件，查找带有此 ID 号或字符串的所有检查。

还可以编辑有关自定义检查的信息，如更改检查名称、添加自定义安全级别或修改有关检查的描述信息。例如，可添加检查的修正描述，以说明修正期间所发生的情况。这将为要使用此检查的其他人提供了有关其行为的宝贵信息。

编辑符合性检查属性

通过使用符合性检查编辑器，可以修改符合性检查的属性，如为其重命名、添加描述、修改其属性信息、为其添加外部 ID 等。

要编辑符合性检查属性的信息，请执行以下操作：

1. 在 SA 客户端的 “工具”菜单中，选择 “符合性检查编辑器” 。如果未看到此菜单项，请与 SA 管理员联系，获取访问权限。
2. 在 “符合性检查编辑器”窗口的 “浏览”选项卡中，展开不同的 “自定义检查”类别查找要编辑的检查。通过在 “平台”筛选器下拉列表中选择操作系统可缩小此列表。
3. 如果要通过名称或名称和描述字段中的关键字来搜索检查，则选择 “搜索”选项卡。

   例如，如果要查找检查安全日志的所有规则，则需要在 “关键字”字段中输入 `security log`。如果要进一步缩小搜索范围，则添加关键字 `size` 查找审核安全日志文件大小的所有检查。

   通过使用 “高级搜索”选项，可以为查找检查设置更具体的参数。使用高级搜索，可通过其他属性 （如安全级别、外部 ID、平台或测试 ID）进行筛选。

   要添加其他搜索参数，请单击  。
4. 要编辑检查的属性信息，请从 “浏览”选项卡或 “搜索”选项卡结果中选择该检查。
5. 在符合性检查编辑器右侧的 “属性”选项卡中，编辑以下检查信息：
   - **名称**：在 “名称”值字段内双击可修改检查名称。
   - **类别**：单击 “单击以编辑”链接可将检查添加到自定义文件夹。例如，单击此链接，进入 “类别”窗口，按键盘上的 ENTER，然后键入名称以创建一个新的符合性检查类别。单击 “应用” 。要创建自定义分组文件夹，请单击 “符合性检查编辑器”窗口底部的 “应用更改”。有关创建检查自定义分组的信息，请参见创建自定义符合性检查类别 （第 69 页）。

- **外部 ID**：在该值字段内双击可添加或修改 “外部 ID”。
- **安全级别**：在该值字段内双击可输入或修改检查的安全级别。

6 单击 “符合性检查编辑器”窗口底部的 “应用更改”可将修改应用到检查。

7 要编辑检查的描述，请选择 “描述” 、“修正描述”或 “技术描述”选项卡，编辑每个描述的描述性文本。

8 要访问描述的 HTML 编辑器，请单击编辑图标  。

9 在 HTML 编辑器中，单击描述窗口左侧底部的 HTML 编辑图标。

10 编辑 HTML 描述。

11 单击 “应用”。如果要撤消任何更改，请从 “文件”菜单中，选择 “还原”。

12 单击 “符合性检查编辑器”窗口底部的 “应用更改”可将描述修改应用到检查。

创建自定义符合性检查类别

通过使用符合性检查编辑器，可以创建自己的自定义类别，其中包含安装在核心上的符合性检查。例如，可以创建一个自定义类别，其中包含审核 Windows 服务器中的用户和组设置的所有检查。或者，如果仅想访问与 Linux 服务相关的特定检查，则可以创建包含这些检查的类别。

要创建自定义符合性检查类别，请执行以下操作：

1 在 SA 客户端的 “工具”菜单中，选择 “符合性检查编辑器” 。如果未看到此菜单项，请与 SA 管理员联系，获取访问权限。

2 在 “符合性检查编辑器”窗口的 “浏览”选项卡中，展开不同的 “自定义检查”类别查找要编辑的检查。通过在 “平台”筛选器下拉列表中选择操作系统可缩小此列表。

3 选择符合性检查。

4 在 “符合性检查编辑器”窗口右上方 “属性”选项卡的 “类别”行中，单击 “单击以编辑”链接。

5 在 “类别”窗口中，将光标放置在主检查类别名称的后面，然后按键盘上的 ENTER。

6 键入名称以创建一个新的符合性检查类别。这将在符合性检查编辑器中创建一个新的符合性检查类别。要添加更多类别，可再次按 ENTER 建立新行并键入类别名称。选定检查将添加到每个新类别中。

7 单击 “应用”。

8 要创建自定义分组文件夹，请单击 “符合性检查编辑器”窗口底部的 “应用更改”。

9 要删除自定义类别，请重复此过程并在 “类别”窗口中删除此类别的名称。

将符合性检查恢复为默认值

如果要将所有符合性检查恢复为默认状态（即它们首次从 BSA Essentials 订阅服务门户下载时的原始状态），则使用恢复默认值操作。恢复默认值将删除对符合性检查所做的任何自定义，然后将其还原到原始的发布状态。

要将符合性检查恢复为默认状态，请执行以下操作：

1. 在 SA 客户端的 “工具”菜单中，选择 “符合性检查编辑器”。如果未看到此菜单项，请与 SA 管理员联系，获取访问权限。
2. 在 “符合性检查编辑器”窗口的 “编辑”菜单中，选择 “恢复默认值”。

   恢复默认值操作仅适用于选定的符合性检查。

显示弃用的检查

可以选择在符合性检查编辑器中显示已弃用的符合性检查。

要在符合性检查编辑器中显示弃用的检查，请执行以下操作：

1. 在 SA 客户端的 “工具”菜单中，选择 “符合性检查编辑器”。如果未看到此菜单项，请与 SA 管理员联系，获取访问权限。
2. 从 “视图”菜单中，选择 “显示弃用的检查”。
3. 展开任何选中的类别可查看任何弃用的检查。

   弃用的检查以灰色、斜体显示。

设置检查的包含项和排除项

可以指定要在符合性检查中包括或排除的文件或目录。

要指定要包括或排除的文件或目录，请执行以下操作：

1. 在 “审核”浏览器的 “视图”窗格中，展开 “规则”，然后选择 “文件”。
2. 在 “规则” > “文件”内容窗格，在 “目录选项”中，单击 “设置排除项”。
3. 在 “设置包含项 / 排除项”窗口中，请从每个下拉列表中指定 “包括”或 “排除”的内容。
4. 单击 “浏览”从源服务器选择文件或目录或输入文件路径。

   有效的通配符包括星号 (*) 和百分比符号 (%)。例如，如果要从符合性检查中排除所有 .exe 文件，请在 “排除”字段中输入 “*.exe”，不包括引号。

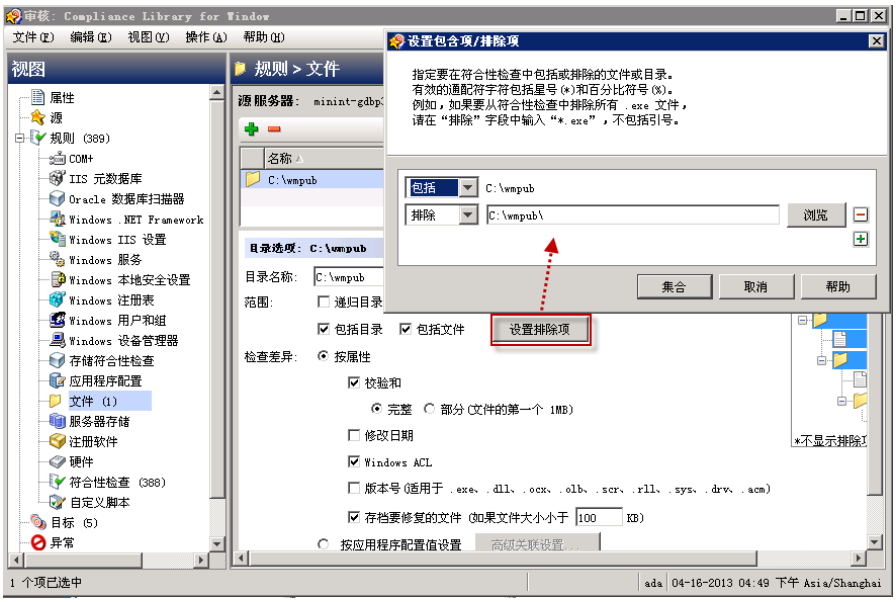
   当您选择某个目录时，可采用递归方式浏览该目录下的文件和子目录。无需从 c: 目录或 root 目录开始浏览。
5. 单击  添加其他行或单击 删除行。
6. 在 “浏览”窗口中，单击 “选择”保存选择。
7. 在 “设置包含项 / 排除项”窗口中，单击 “集合”保存设置。

文件包含项和排除项规则

当在审核、审核策略或快照规范中配置文件规则时，可以指定要在审核或快照中包含和排除的目录和文件。本节将说明包含项和排除项规则的内容以及如何将这些规则应用到文件绝对路径的相对子集中。

审核文件规则内的包含项和排除项规则位于审核或快照规范窗口的底部，如图 15 所示。

图 15　　文件系统文件 / 目录通配符包含项和排除项规则



当在审核或快照规范中配置文件规则时，可在“文件 / 目录通配符”字段中输入包含项 / 排除项规则。输入规则后，可从下拉列表中选择“包括”或“排除”。要添加新的包含项或排除项规则，请单击  。

有关如何创建和配置审核或快照规范的文件系统规则的信息，请参见配置文件规则 （第 46 页）。

包含项和排除项规则类型

审核和修正提供了以下类型的包含项和排除项规则，用于配置文件规则：

- 适用于文件名称路径且包含“/”或“\”的文件类型规则。
- 适用于相对路径且可在 Unix 中包含“/”以及在 Windows 中包含“\”且不是完全限定的相对类型规则。

- 适用于绝对路径的绝对类型规则。在 Unix 中，绝对路径以 “/” 为开头。在 Windows 中，绝对路径以卷号为开头，后跟 “:\”，绝对路径是完全限定的，如 “C:\”、“d:\”、“f:\” 等。如果在 Windows 路径中使用 “/”（正斜杠），则审核和修正会将其转换为 “\”（反斜杠）以作为有效路径使用。
- 文件名和路径的环境变量和自定义特性参数化。有关详细信息，请参见参数化 SA/ 自定义特性的文件名 （第 75 页）。

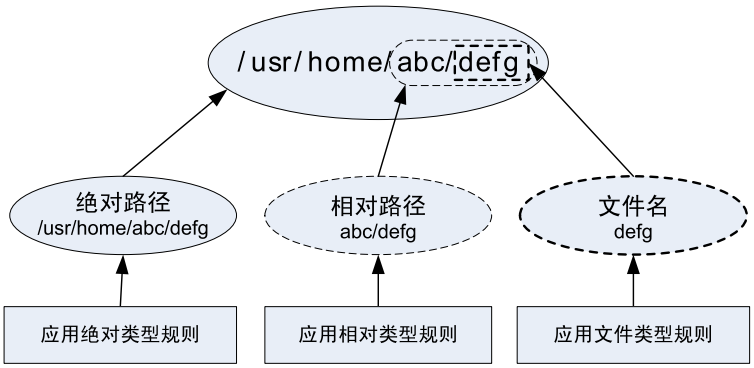
审核和修正首先处理所有排除项规则。排除项规则应用后才应用包含项规则。包含的默认设置是包含文件系统中的所有对象。在许多情况下，可能甚至不会处理包含项规则，因为包含项规则与排除项规则 （首先执行）可能没有有效交集。

在包含项和排除项规则中还可使用星号 (*) 和问号 (?) 作为有效通配符。通配符字符是一个与路径匹配的占位符，或一个或多个字母。

根据包含项和排除项规则的类型，该规则仅适用于文件绝对路径的相关子集。在审核和修正中，每个快照或审核都有一个顶级。用于针对包含项和排除项规则进行比较的每个文件都有绝对路径。在图 16 中，绝对路径是 /usr/home/abc/defg。快照或审核向下查看 /usr/home/abc/defg 绝对路径，并将 abc/defg 视为相对路径，将 defg 视为文件名。在此示例中，包含项和排除项规则将按以下方式进行应用：

- 文件类型规则适用于文件名称路径 defg。
- 相对类型规则适用于相对路径 abc/defg。
- 绝对类型规则适用于绝对路径 /usr/home/abc/defg。有关审核和修正如何将包含项和排除项规则应用到文件路径相关子集中的图解，请参见图 16。

图 16　　如何应用包含项和排除项规则



为了更好地说明这些规则是如何应用的，提供了以下示例。

示例：在快照或审核中包含所有 .txt 文件 （第 73 页）和示例：包含最后一个 temp.txt 文件并排除所有其他文件 （第 74 页）中使用的示例文件系统结构如下所示：

```
/dir1/dir2/a
/dir1/dir2/b
/dir1/dir2/names.txt
/dir1/dir2/temp.txt
/dir1/dir2/version1.exe
/dir1/dir2/subdir/version2.exe
```

示例：在快照或审核中包含所有 .txt 文件

如果要在快照或审核中包含所有带有 .txt 扩展的文件，则包含项和排除项规则应为：

- /dir1/dir2
- 包括 *.txt （此为文件类型规则。）
- 排除 * （此为文件类型规则。）

以下步骤说明了审核和修正如何通过文件结构进行迭代，以及如何应用任何相应的包含项和排除项规则：

a. * 将 /dir1/dir2/a 排除在外。然后将 *.txt 应用到 /dir1/dir2/a(a) 的文件部分，不存在匹配。文件将不包含在内。

b. * 将 /dir1/dir2/b 排除在外。然后将 *.txt 应用到 /dir1/dir2/b (b) 的文件部分，不存在匹配。文件将不包含在内。

c. * 匹配 names.txt，但 *.txt 也匹配 names.txt，这导致此文件排除在外。

d. 与步骤 3 相同。

e. 比较 a 和 *，存在匹配；比较 a 和 a，存在匹配。文件将包含在内。

f. 比较 b 和 *，存在匹配；比较 b 和 a，不存在匹配。文件将被排除在外。

这些步骤编号与示例文件结构中的路径相对应，编号从顶级路径开始。

示例：在快照或审核中仅包含文件 a

如果要在快照或审核中仅包含该文件，则包含项和排除项规则应为：

- /dir1/dir2
- 排除 * （此为文件类型规则。）
- 包括 a （此为文件类型规则。）

以下步骤说明了审核和修正如何通过文件结构进行迭代，以及如何应用任何相应的包含项和排除项规则：

a. * 将 /dir1/dir2/a 排除在外。然后将 *.txt 应用到 /dir1/dir2/a(a) 的文件部分，不存在匹配。文件将不包含在内。

b. * 将 /dir1/dir2/b 排除在外。然后将 *.txt 应用到 /dir1/dir2/b (b) 的文件部分，不存在匹配。文件将不包含在内。

c. * 匹配 names.txt，但 *.txt 也匹配 names.txt，这导致此文件包含在内。

d. 与步骤 3 相同。

e. 比较 a 和 *，存在匹配；比较 a 和 a，存在匹配。文件将包含在内。

f. 比较 b 和 *，存在匹配；比较 b 和 a，不存在匹配。文件将被排除在外。

这些步骤编号与示例文件结构中的路径相对应，编号从顶级路径开始。

示例：包含最后一个 temp.txt 文件并排除所有其他文件

如果要在快照或审核中包含最后一个 temp.txt 文件且排除所有其他文件，则包含项和排除项规则应为：

- /dir1/dir2
- 排除 *（此为文件类型规则。）
- 包括 dir3/temp.txt （此为相对类型规则。）

以下步骤说明了审核和修正如何通过文件结构进行迭代，以及如何应用任何相应的包含项和排除项规则：

a. * 将 /dir1/dir2/a 排除在外。然后将 *.txt 应用到 /dir1/dir2/a(a) 的文件部分，不存在匹配。文件将不包含在内。

b. * 将 /dir1/dir2/b 排除在外。然后将 *.txt 应用到 /dir1/dir2/b (b) 的文件部分，不存在匹配。文件将不包含在内。

c. * 匹配 names.txt，但 *.txt 也匹配 names.txt，这导致此文件包含在内。

d. 与步骤 3 相同。

e. dir3/temp.txt 与 /dir1/dir2/dir3/temp.txt 的相对部分进行比较，存在匹配。

f. 比较 a 和 *，存在匹配；比较 a 和 subdir/version2.exe，不存在匹配。文件将被排除在外。

这些步骤编号与示例文件结构中的路径相对应，编号从顶级路径开始。

文件规则重叠

当在规则中包含父目录 （以及选项）且子目录 （以及其他选项）作为附加参数时，父目录快照和子目录快照将相互重叠为一个快照。该逻辑也适用于 Windows NT ACL 集合和内容集合选项以及 Windows 注册表内容集合选项。以下示例说明了父目录和子目录的审核规则是如何重叠的。

请考虑以下文件系统，其中末尾的斜杠 (/) 代表了目录：

```
/cust/app/bin/
/cust/app/bin/file1
/cust/app/bin/conf/
/cust/app/bin/conf/conf1
/cust/app/bin/conf/conf2
/cust/app/bin/conf/dev/
/cust/app/bin/conf/dev/conf3
```

示例 A

如果使用以下两种规则创建快照：

目录 /cust/app/bin （递归，无校验和）

目录 /cust/app/bin/conf （不递归，检验和）

快照将记录以下文件系统信息：

```
/cust/app/bin/ (directory)
/cust/app/bin/file1 (no checksum)
/cust/app/bin/conf/ (directory)
/cust/app/bin/conf/conf1 (*checksum*)
/cust/app/bin/conf/conf2 (*checksum*)
/cust/app/bin/conf/dev/ (directory)
/cust/app/bin/conf/dev/conf3 (no checksum)
```

正如所看到的那样，即使 /cust/app/bin 是递归且无校验和， /cust/app/bin/conf 目录也会将其覆盖，并且该目录中的所有文件都为其记录了校验和。

示例 B

如果使用以下两种审核规则 （通过切换示例 A 中使用的选项）创建快照：

目录 /cust/app/bin （递归，校验和）
目录 /cust/app/bin/conf （不递归，无校验和）

快照将记录以下文件系统信息：

```
/cust/app/bin/ (directory)
/cust/app/bin/file1 (checksum)
/cust/app/bin/conf/ (directory)
/cust/app/bin/conf/conf1 (*no checksum*)
/cust/app/bin/conf/conf2 (*no checksum*)
/cust/app/bin/conf/dev/ (directory)
/cust/app/bin/conf/dev/conf3 (checksum)
```

示例 C

如果使用以下三种审核规则 （通过添加文件选项）创建快照：

目录 /cust/app/bin （递归，校验和）

目录 /cust/app/bin/conf （不递归，无校验和）

文件 /cust/app/bin/conf/conf1 （校验和）

快照将记录以下文件系统信息：

```
/cust/app/bin/ (directory)
/cust/app/bin/file1 (checksum)
/cust/app/bin/conf/ (directory)
/cust/app/bin/conf/conf1 (*checksum*)
/cust/app/bin/conf/conf2 (no checksum)
/cust/app/bin/conf/dev/ (directory)
/cust/app/bin/conf/dev/conf3 (checksum)
```

在此示例中， conf1 非常详细的审核规则覆盖了 /cust/app/bin/conf 审核规则。

参数化 SA/ 自定义特性的文件名

当在审核或快照规范中创建文件规则时，还可以在文件名中引用环境变量和自定义特性。在规则窗口的 “文件 / 目录通配符”区域中，可通过编辑文件名来添加这些引用。

要将引用添加到 Windows 环境变量，请使用语法 %envVarName%，在 Unix 中则使用语法 ${varName}。

指定自定义特性的语法是 @varName@。例如：

```
@/customattribute/custAttrbuteNAME@\rest\of\the\path
@/customattribute/FacilityCustomAttrbuteNAME@\rest\of\the\path
@/customattribute/CustomerCustomAttributeNAME@\rest\of\the\path
@/customattribute/ServerAttrbuteNAME@\rest\of\the\path
@/customattribute/GrpAttrbuteNAME@\rest\of\the\path
```

这允许通过在文件名中使用参数化的环境变量或自定义特性，审核源服务器和目标服务器上的相对路径。

参数化文件名示例

例如，在要审核的服务器上，已知到某应用程序的相对路径，但不一定知道对所有服务器的绝对路径。可以在审核的 “文件” 规则中参数化该路径，以便消除相对路径名，并且审核审核检查目标服务器上该应用程序所有位置的相对路径。

例如，要相对黄金源服务器审核目标服务器，其中在黄金源服务器中， %ProgramFiles% 为 :\Program Files，而在目标服务器中， %ProgramFiles% 为 D:\Program Files。

在 “文件” 规则的 “文件 / 目录通配符” 部分中，可在审核中将目录规则的 root 目录指定为 %ProgramFiles%\Company\MyApp。当运行审核时，审核会将 %ProgramFiles% 从其目标服务器的路径中删除。也就是说，源服务器上的 C:\Program Files\Company\MyApp\file1.txt 将与目标服务器上的 D:\Program Files\Company\MyApp\file1.txt 相比较。

再举一个例子，您可能要审核一个应用程序，该应用程序已安装到两个不同服务器的两个完全不同的子目录中。

例如，您在审核中从黄金源服务器配置中选择以下安装路径：

```
/usr/local/app-version-1232/prog
```

并且，目标服务器将应用程序安装在以下路径的任意位置：

```
/usr/local/app
```

为了审核目标服务器，可定义自定义特性 APP_INSTALL_LOC，其中黄金服务器的值为 /usr/local/app-version-1232/prog，而生产服务器的值为 /usr/local/app。审核中的 “文件” 规则将会如下所示：

```
@/customattribute/APP_INSTALL_LOC@/prog
```

这会导致审核将 @/opsware/customattribute/APP_INSTALL_LOC@ 视为目标服务器上的环境变量进行处理并执行路径替换。

如果要引用服务器特性，则输入如下路径：

```
@/server/APP_INSTALL_LOC@/prog
```

路径名中的环境变量

最佳实践：如果要在 Unix 上的文件名 PATH 中使用环境变量 （通常称之为*参数化检查*），则最好在以下文件和目录中定义这些环境变量：`etc/opt/opsware/snapshot/env`。请确保在 Unix 上不要将 `/etc/profile` 用作源环境变量。

要定义可用作 “文件” 规则配置的源的环境变量，可以在要进行审核或快照创建的托管服务器上创建带有变量的文件。

例如：

1. 要进行审核或快照创建的托管服务器的 SSH。
2. 在以下位置创建新目录：

   ```
   mkdir /etc/opt/opsware/snapshot
   ```

3. 创建一个新的空文件，如：

   ```
   touch /etc/opt/opsware/snapshot/env
   ```

4. 通过在新文件中输入相应变量，可定义要作为文件规则的源的环境变量。***示例：***

   ```
   TEST1='/tmp/test1'
   TEST2='/home/test2'
   export TEST1 TEST2
   ```

5. 完成编辑后，保存文件。

审核规则异常

对于大部分审核规则，可以在审核中的选定目标服务器 （或服务器组）上创建临时或永久的规则异常。这意味着在审核运行时，可从审核的选定目标上排除特定的规则。

例如，在审核几个服务器的审核中，您可能要暂停该审核的目标服务器子集的一个或多个规则。您可能有一个 Windows 服务器集合，该集合定期进行审核以确保 IIS 服务已禁用，例如，为了符合公司安全标准。审核已配置为对其中的每个服务器进行检查，以确保 IIS 已禁用。如果任何服务器上启用了 IIS，则审核将失败。

但是，您可能要短时间地运行某个需要启用 IIS 服务的业务应用程序，以便在审核的某些目标服务器上运行。可以为此管理 IIS 服务的规则创建一个规则异常，并将此异常与需要运行该应用程序的服务器关联。这确保了在遇到启用了 IIS 服务的服务器时审核可以继续运行而不会失败。

可以为此规则异常设置过期日期，以确保在不再需要此规则异常或不再允许其存在时，将此规则应用到审核中的所有服务器。还可以编写此异常的原因并将其与工单 ID 关联。在一个审核中创建的异常不会影响任何其他审核中的规则。

无法具有异常的规则

可以为大多数审核规则创建异常。但是，包含全部规则集合的规则类别无法具有异常。

将异常应用到设备组时的注意事项

当为设备组设置审核规则异常时，该异常将应用到组中的所有服务器。存在这样的可能性：具有此异常的组中的某个服务器同时也属于另一个设备组，而此设备组也恰好是某个未应用任何异常的审核的目标。

在这种情况下，即使此服务器也属于不具有异常的设备组，该规则异常也始终适用于此服务器。一般来说，请牢记，属于应用了规则异常的设备组的任何服务器均会排除审核规则，而不论该服务器是否属于作为某个审核的目标且在无异常的情况下应用了相同规则的另一设备组。

将规则异常添加到审核

要创建审核规则异常，请选择审核中配置的任何规则，然后使用 “添加规则异常”窗口将其与审核中的目标服务器关联。运行审核时，选定规则和与此规则关联的目标服务器或快照将不会应用。

还可以将规则异常应用到设备组。可以将此规则异常设置为无限期运行，或在将来的某个时间点到期。可以添加注释说明创建此异常的原因，并将此异常与工单 ID 关联。

某些审核规则和审核规则集合无法成为例外。有关详细信息，请参见无法具有异常的规则 （第 78 页）。

要将规则异常添加到审核，请执行以下操作：

1. 首先，创建一个审核。有关信息，请参见创建审核 （第 19 页）。
2. 配置此审核的审核规则。有关配置审核规则的信息，请参见审核和修正规则 （第 35 页）。
3. 在左侧的审核视图窗格中，选择 “异常” 图标。
4. 接下来，在内容窗格中，单击 “添加”。

也可以在 “审核”窗口中选择任何规则。右键单击并选择 “添加异常”。但是，如果审核正引用一个链接的审核策略，则无法通过右键单击规则添加异常。

5. 在 “添加异常”窗口的 “选择目标服务器”部分中，选择要应用此规则异常的服务器、多个服务器或设备组。
6. 接下来，从 “选择规则”部分中，选择要与上一步中选定的服务器关联的一个或多个规则。
7. （*可选*）在 “异常原因”部分中，添加说明。
8. （*可选*）在 “工单 ID”部分中，添加与此异常关联的工单 ID。
9. 在 “到期”部分中，输入日期指示该异常到期的时间或从下拉列表中选择一个日期。

10 当完成配置异常时，单击 “添加”。

11 现在您将可以看到将在运行审核时应用的规则异常列表。

编辑或删除规则异常

可通过以下两种方式之一对异常进行编辑：

- 双击异常修改异常的原因、工单 ID 以及异常过期日期
- 单击 “添加”编辑规则 （覆盖现有规则）。

要编辑异常，请执行以下操作：

1 打开 “审核”窗口。

2 在 “视图”窗格中，选择 “异常”  图标。

3 在内容窗格中，双击某个异常。

4 在 “编辑异常”窗口中，可编辑任何异常以及所分配至的服务器或设备组。编辑异常之后，单击 “添加”。

5 如果要完全更改此规则，则单击 “添加”，然后在 “添加异常”窗口中，通过选择目标服务器和一个或多个规则来更改规则。完成后，单击 “添加”更改异常。

要删除异常，请执行以下操作：

1 打开 “审核”窗口。

2 在左侧的审核视图窗格中，选择 “异常”  图标。

3 在内容窗格中，选择要删除的异常，然后单击 “删除”。

审核策略管理 

通过使用审核策略，可以定义和存储可重用的集中服务器配置符合性规则集合。可以将审核策略链接到审核、快照规范和其他审核策略。

审核策略通常由策略设置员创建，策略设置员了解公司要求服务器满足的合规性标准。负责管理和审核实际服务器的其他用户可以使用预定义审核策略，方法是将审核策略链接到其审核或快照规范。如果对审核策略进行了更改，则链接到其的审核或快照规范将引用审核策略的更新规则。审核服务器的用户可确保他们的审核将始终反映组织中最新的符合性标准。

审核策略可链接到其他审核策略。例如，可将多个不同的单独审核策略组合成一个用于定义 Windows 服务配置方式的主策略。运行审核后，如果发现任何差异，则可以从审核结果对其进行修正。

可以从头开始创建审核策略或将审核、快照规范 （或其他审核策略）的规则保存为审核策略。所有审核策略都存储在 SA 客户端库中。

还可以查看附加到特定审核策略的托管服务器 （目标）的状态。

链接和导入审核策略

审核策略可通过*链接*在审核和快照规范或其他审核策略内使用。审核和快照规范也可通过*导入*使用审核策略。

链接审核策略

最佳实践：通过将审核策略*链接*到审核或快照规范，可以使审核或快照规范使用与审核策略中完全相同的规则集。如果审核策略中的任何规则发生更改，则审核和快照规范的规则将在下一次运行时反映相同的更改，因为它们已链接到审核策略中定义的规则集。

可通过选择**启用未链接的规则 (防止链接到预定义的审核策略)** 选项断开这种链接。请参见配置文件规则 （第 46 页）。

审核策略也可以链接到其他审核策略，您还可以将任意多个审核策略链接到同一个审核策略。将一个或多个审核策略链接到某个审核策略时，链接的一个或多个审核策略将成为该父审核策略的子级。如果创建了一个链接到父审核策略的审核，则当您在目标服务器上运行该审核时，系统将针对目标服务器运行所有链接策略中的规则。

导入审核策略

将审核策略*导入*到审核或快照规范会导入审核策略的所有规则。导入之后，可对规则进行编辑。将审核策略导入到审核中时，可选择替换审核中的任何当前值或将审核策略中的规则与审核或快照规范中的规则进行合并。审核策略无法从其他审核策略导入规则；但是可以链接到其他审核策略。

多个链接审核策略的规则重叠

由于可将审核或快照规范链接到可能引用其他审核策略的审核策略，因此某些链接的策略可能含有具有不同配置选项的相同规则。

规则在标识规则的相同对象时会在审核结果中进行合并，并且规则只能通过设置选项进行自定义。这些选项不管相同还是不同，在运行之前都会合并成一个规则，且仅会有一种结果。如果选项不同，这些选项将合并成单个规则。例如文件规则、注册表规则、元数据库规则 （旧版比较类型） 、Windows 服务规则等。

带有参数或指定符合性条件的规则当且仅当这些参数和条件完全相同时才进行合并。否则，它们将作为单独的规则执行。例如符合性 （可插入）规则、自定义脚本规则和基于服务器模块的规则。

创建审核策略

创建审核策略时，通过创建自定义规则或链接到其他审核策略的规则，可将活动服务器作为规则的选取源创建审核策略规则。

使用源服务器构建审核策略规则，可以使用托管服务器的实际配置作为审核策略规则的基础。在审核策略链接到审核或快照规范后，不再使用用于构建规则的源服务器。

所有审核策略都必须保存在 SA 客户端库的文件夹中。文件夹内每个审核策略的名称都必须是唯一的。要将审核策略保存到文件夹，必须具有写入该文件夹的权限。有关文件夹权限的详细信息，请参见 《SA 管理指南》。

要创建审核策略，请执行以下操作：

1. 在导航窗格中，选择 “库” > “按类型” > “审核和修正” > “审核策略”。
2. 选择操作系统：Windows 或 Unix。
3. 在 “操作” 菜单中，选择 “新建”。
4. （*可选*）在 “属性” 内容窗格中，输入名称和描述。名称中可包含下划线。
5. 单击 “选择” 在 SA 库中指定保存审核策略的位置。
6. 在“选择文件夹”窗口中，为此位置选择一个文件夹。您必须对保存策略的文件夹具有写入权限。
7. 选择位置后，单击 “选择”。
8. 如果希望将托管服务器用作审核策略规则的基础，则在 “审核策略” 窗口的 “视图” 窗格中，选择 “源”。
9. 在 “源” 内容窗格中，单击 “选择” 为审核策略选择一个源服务器。
10. 在 “选择服务器” 窗口中，选择一个服务器，然后单击 “确定”。
11. 在 “审核策略” 窗口的 “视图” 窗格中，选择 “规则”。

    如果要将其他审核策略链接到此审核，则单击 选择审核策略。

    如果要编辑任何链接的审核策略，请从 “规则” 列表中选择审核策略，然后单击 打开 “审核策略” 窗口。
12. 在 “选择审核策略” 窗口中，选择一个或多个审核策略链接到此审核策略，然后单击 “确定” 保存选择。

    将一个或多个审核策略链接到某审核策略时，仍旧可以在审核策略中配置单个规则。来自外部引用审核策略的所有规则都将与您创建的任何规则进行组合，以构建单个规则集。
13. 在 “视图” 窗格的 “规则” 列表中，创建要包含在此审核策略内的任何其他规则。请参见第 37 页第 2 章中的审核和快照规则，了解如何配置特定审核和修正规则。
14. 当完成配置审核时，从 “文件” 菜单中，选择 “保存”。保存后，审核策略便可以链接到审核、快照规范或其他审核策略。

注意：在“审核策略”窗口，如果选择一个服务器查看其注册表信息，然后希望查看其他服务器的注册表信息，则必须关闭“审核策略”窗口，然后将其重新打开以刷新注册表内容字段。

将审核保存为审核策略

可以将审核保存为审核策略。此操作仅保存该审核的规则，然后创建一个新的审核策略。如果审核规则要求目标服务器上安装最新代理，则 SA 客户端将显示消息提醒您更新代理，或在审核中创建异常以避免出现运行时错误。

创建的所有审核策略都必须保存在 SA 库的文件夹中。文件夹内每个审核策略的名称都必须是唯一的。必须对要保存审核策略的文件夹具有写入权限。有关文件夹权限的详细信息，请参见《SA 用户指南：Server Automation》或与 SA 管理员联系。

要保存审核以使用其创建审核策略，请执行以下操作：

1. 在“审核”或“快照规范”窗口的“文件”菜单中，选择“另存为”。
2. 在“另存为”窗口中，输入名称。如果要重命名审核或快照规范，则必须使用唯一名称。
3. *（可选）*输入描述。
4. 从“类型”下拉列表中，选择“审核”或“审核策略”。
5. 如果选择了“审核策略”，则从“位置”部分，单击“选择”。
6. 从 SA 库中选择一个文件夹保存此审核策略。必须对保存审核策略的文件夹具有写入权限。
7. 单击“确定”。

链接和导入审核策略的方式

可将审核策略导入或保存到审核、快照规范或其他审核策略：

- 将审核或快照规范保存为审核策略 （第 85 页）
- 将审核策略链接到主审核策略
- 导入审核策略规则（替换或合并）
- 将审核或快照规范保存为审核策略 （第 85 页）

将审核策略链接到审核或快照规范

将审核策略链接到审核或快照规范将创建一个链接，通过此链接可将审核策略的规则用于审核或快照规范。

最佳实践：如果策略设置员要为服务器定义服务器配置策略，然后让其他用户将其审核和快照规范链接到同一个审核策略，则链接到审核策略非常有用。如果策略设置员对此审核策略进行了任何更改，则更改将会在链接到该策略的审核或快照规范中有所反映。

当审核策略链接到审核或快照规范时，无法在审核或快照规范的上下文中修改规则。但是，如果具有所需的用户权限，则可以访问审核策略并编辑其规则。

如果要链接审核策略的审核或快照规范已定义规则，则在链接到外部审核策略时，审核或快照规范中的所有现有规则都将被*覆盖*。

要将审核策略链接到审核或快照规范，请执行以下操作：

1 从 SA 库中打开现有审核或快照规范：

a 在导航窗格中，选择“库”>“审核和修正”>“审核”。选择操作系统：Windows 或 Unix。从内容窗格中，打开一个审核。

b 在导航窗格中，通过选择 “库” >“审核和修正” >“快照规范”，打开现有的快照规范。从内容窗格中，打开一个快照规范。

2 从 “操作”菜单中，选择 “链接到策略”。

3 在 “选择审核策略”窗口中，选择一个审核策略，将其链接到审核或快照规范。对于每个审核或快照规范，仅可链接到一个审核策略。但是，可将*多个*审核策略链接到*一个*审核策略。请参见创建审核策略 （第 81 页）或将审核策略链接到主审核策略 （第 83 页）。

4 选定审核策略后，单击 “确定”。

如果将审核策略链接到已定义规则的审核或快照规范，则系统将显示一条消息，提示是否要*覆盖*任何现有规则定义。单击 “是”导入审核策略并覆盖现有规则。

5 从 “文件”菜单中，选择 “保存”保存审核或快照规范。

将审核策略链接到主审核策略

通过将审核策略链接到其他审核策略，可将多个审核策略组合成单个*主审核策略*。因为可根据需要将多个审核策略链接到一个审核策略，所以可将现有审核策略构建为满足特定审核需求的单个审核策略并进行重用。

将一个或多个审核策略链接到某个审核策略时，链接的一个或多个审核策略将成为该父 （或主）审核策略的子级。如果创建了一个链接到父审核策略的审核，则当您在目标服务器上运行该审核时，系统将针对目标服务器运行所有链接策略中的规则。

示例：SA 库包含几个单独的审核策略，这些审核策略定义了 HP-UX 服务器组的符合性标准。一个策略包含用于检查确保 FTP 服务已启用的规则。另一个策略包含用于检查确保 cron 日志记录始终启用的规则。在此示例中，您可以创建链接到这两种策略的单个*主审核策略*。这个*主审核策略*随后可被其他审核引用。

要将审核策略链接到主审核策略，请执行以下操作：

1 在导航窗格中，选择 “库” >“按类型” >“审核和修正” >“审核策略”。

2 选择操作系统：Windows 或 Unix。

3 选择一个现有审核策略或创建一个新的审核策略。请参见创建审核策略 （第 81 页）。

4 如果希望将托管服务器用作审核策略规则的基础，则在 “审核策略”窗口的 “视图”窗格中，选择 “源”。

a 单击 “选择”为审核策略选择一个源服务器。

b 在 “选择服务器”窗口中，选择一个服务器，然后单击 “确定”。

5 在 “审核策略”窗口的 “视图”窗格中，选择 “规则”。

a 如果要将其他审核策略链接到此审核，则单击  选择审核策略。

b 如果要编辑任何链接的审核策略，请从 “规则”列表中选择审核策略，然后单击  打开 “审核策略”窗口。

6 在 “选择审核策略”窗口中，选择一个或多个审核策略链接到此审核策略，然后单击 “确定”保存选择。

将一个或多个审核策略链接到某审核策略时，仍旧可以在审核策略中配置单个规则。来自外部引用审核策略的所有规则都将与您在审核策略中创建的任何规则进行组合。

7 在 “视图”窗格的 “规则”列表中，创建要包含在此审核策略内的任何其他规则。请参见审核和快照规则 （第 37 页）。

如果要编辑任何链接的审核策略，请从 “规则”列表中选择审核策略，然后单击  。

8 当完成配置审核策略时，从 “文件”菜单中，选择 “保存”。保存后，审核策略便可以链接到其他审核策略。

导入审核策略规则

通过将审核策略导入审核或快照规范，可以将审核策略的规则导入 （还可选择合并）到审核或快照规范中，而不保留与该审核策略的链接。

导入审核策略后，将不再存在与该审核策略的连接。对源审核策略进行的任何更改都将不会在该审核策略导入的位置中反映出来。

要将审核策略导入审核，请执行以下操作：

1 从 SA 库中打开现有审核或快照规范：

a 在导航窗格中，选择 “库” > “审核和修正” > “审核”。选择操作系统：Windows 或 Unix。从内容窗格中，打开一个审核。

b 在导航窗格中，通过选择 “库” > “审核和修正” > “快照规范”，打开现有的快照规范。从内容窗格中，打开一个快照规范。

2 从 “操作”菜单中，选择 “链接到策略”。

3 如果审核或快照规范已定义规则，请选择覆盖现有规则或将审核策略规则与现有规则合并。

最佳实践：根据规则类型，合并规则会产生不同的结果。最佳实践是检查所有产生的规则以确定合并的审核策略规则是符合要求还是需要修改。

如果单击 “是”，则审核策略会*覆盖*审核或快照规范中的任何现有规则。

如果单击 “否”，则审核策略会将审核策略规则与任何现有规则合并。如果出现任何冲突，则审核策略规则将*覆盖*任何现有规则。

4 从 “文件”菜单中，选择 “保存”保存审核或快照规范。

将审核或快照规范保存为审核策略

可将审核或快照规范的规则保存为审核策略。然后，可将此审核策略用于其他审核或快照规范。如果审核规则要求目标服务器上安装最新代理，则 SA 客户端将显示消息提醒您更新代理，或在审核中创建异常以避免出现运行时错误。

创建的所有审核策略都必须保存在 SA 库的文件夹中。文件夹内每个审核策略的名称都必须是唯一的。要将审核策略保存到文件夹，必须具有写入该文件夹的权限。有关文件夹权限的详细信息，请参见 《SA 用户指南：Server Automation》或与 SA 管理员联系。

要将审核或快照规范保存为审核策略，请执行以下操作：

1. 从 SA 库中打开现有审核或快照规范：
   a. 在导航窗格中，选择“库”>“审核和修正”>“审核”。选择操作系统：Windows 或 Unix。从内容窗格中，打开一个审核。
   b. 在导航窗格中，通过选择 “库”>“审核和修正”>“快照规范”，打开现有的快照规范。从内容窗格中，打开一个快照规范。
2. 配置审核或快照规范的规则后，从 “文件”菜单中，选择 “另存为”。
3. 在 “另存为”窗口中，输入名称和描述。
4. 在 “类型”列表中，选择 “审核策略”。
5. 单击 “选择”。
6. 在 “选择文件夹”窗口中，选择要保存审核策略的文件夹，然后单击 “确定”。则审核策略已保存，且可通过下列路径进行访问，“库”>“审核和修正”>“审核策略”。

在文件夹库中查找审核策略

创建审核策略并保存到文件夹库中后，可使用 “在文件夹中查找”功能在 SA 库中轻松查找该审核策略。

要在文件夹中查找审核策略，请执行以下操作：

1. 在导航窗格中，选择 “库”>“按类型”>“审核和修正”>“审核策略”，然后选择 Windows 或 Unix。
2. 选择一个审核，右键单击并选择 “在文件夹中查找”。此时将显示保存此审核策略的位置。

导出审核策略

如果要获取审核策略中包含和配置的所有规则的列表，请将策略导出到 CSV 和 HTML 中。

要导出审核策略，请执行以下操作：

1. 在导航窗格中，选择 “库”>“按类型”>“审核和修正”>“审核策略”。
2. 选择 Windows 或 Unix。

3 打开审核策略：

a 选择一个审核，然后双击。

或

b 选择一个审核，右键单击并选择 “打开”。

4 从 “操作” 菜单，选择 “导出”，然后选择其中一种格式 （“CSV”、“HTML”）。

5 为文件选择路径和文件名，然后单击 “导出”。

6 打开文件可查看导出的信息。

注意：要正确地查看导出的信息，请用文本编辑器打开 .csv 文件，关闭自动换行，然后水平地展开文本窗口。

查看审核策略的符合性

在 “审核策略” 浏览器中，可以查看附加到特定审核策略的托管服务器 （目标）的状态。

当您创建审核策略和引用它的目标时，必须运行审核以便在此浏览器中显示其符合性信息。至少要有一次审核运行或一个将审核策略链接到目标的现有审核结果，才能显示目标服务器的符合性状态。

最佳实践：选择对于保持数据中心符合性至关重要的审核策略。您还可以查看哪些托管服务器不符合要求。符合性状态以最新审核结果和 / 或任何审核策略更改为依据。

要查看审核策略的符合性，请执行以下操作：

1 在导航窗格中，选择 “库” > “按类型” > “审核和修正” > “审核策略”。

2 选择操作系统：Windows 或 Unix。

3 选择一个现有审核策略。

4 在 “审核策略” 窗口的 “视图” 窗格中，选择 “符合性”。

内容窗格将列出审核策略中引用的所有托管服务器及其符合性状态。

5 （*可选*）要查看列表中有关服务器的详细信息，请选择服务器，然后单击 “查看”，以显示 “服务器” 浏览器。

审核结果

审核定义了要在服务器上根据审核规则进行检查的服务器配置。审核结果通过运行审核产生。这些结果显示了审核规则和每个目标服务器或目标快照的实际服务器配置值之间的差异。

是否可以修正某规则取决于规则类型。规则必须支持修正，且服务器的审核规则源必须包含支持修正的数据。

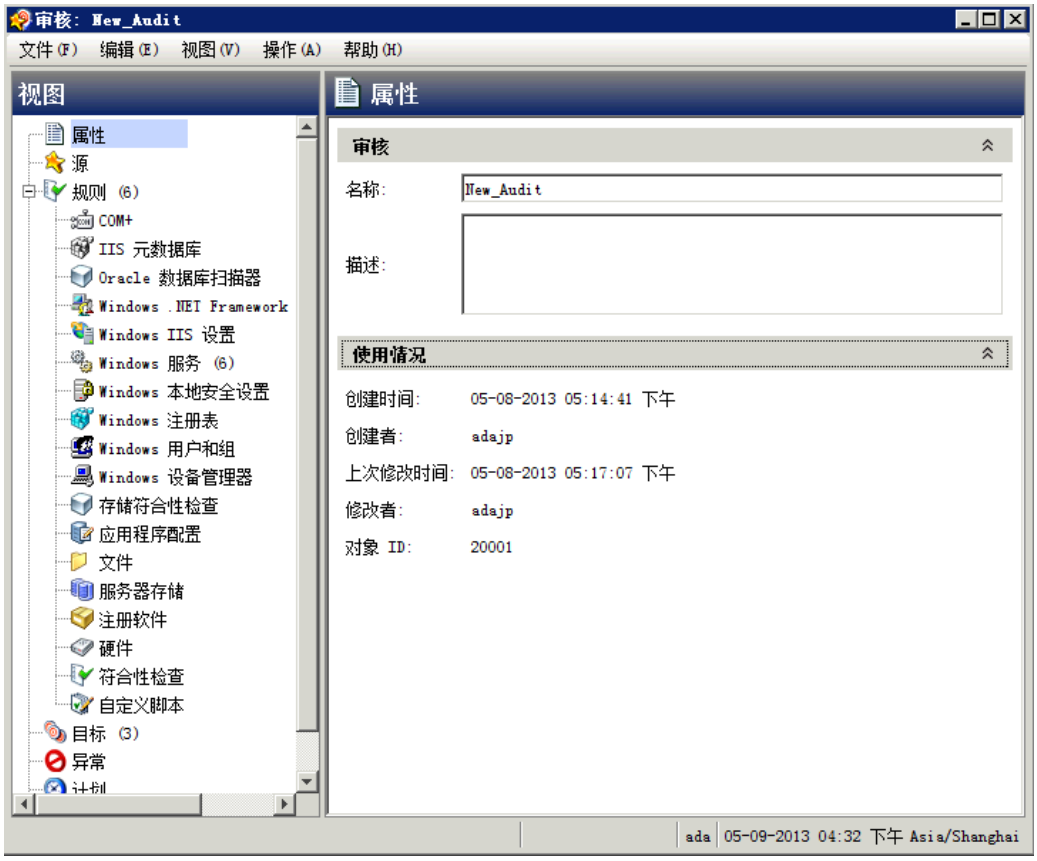
示例：一些规则不支持修正，如“硬件”规则。无法对服务器的物理内存或硬件进行修正。另外，如果审核将快照用作源且此快照无法从规则收集足够的信息，则该规则将无法进行修正。

对于链接到审核策略的审核，结果将显示审核中的所有规则。但是，结果并不显示最初在其中定义这些规则的一个或多个审核策略。

查看审核结果

在 SA 客户端中，可以查看任何审核的审核结果列表，如图 17 所示。当在“库”中选择一个审核时，与该审核关联的所有结果都将在底部的详细信息窗格中列出。

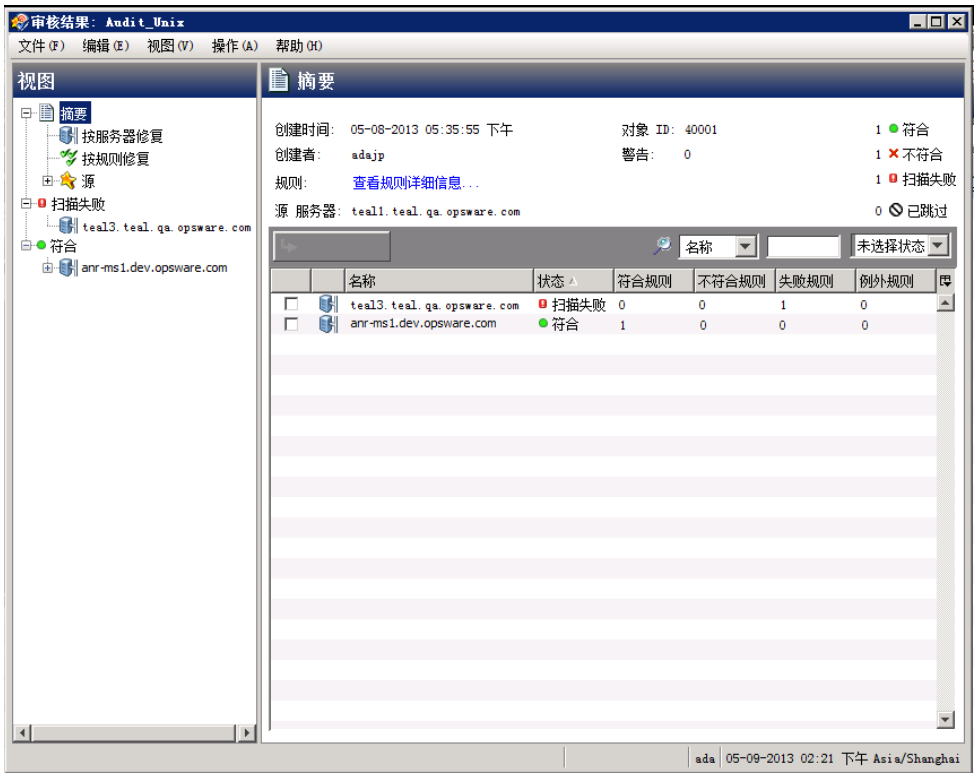
图 17　　审核结果



审核结果窗口

“审核结果”窗口提供有关审核作业 （如审核目标服务器与审核中定义的规则之间的差异）的详细信息，如图 18 所示。此信息有助于查看已审核的服务器是否与数据中心设置的标准相符合。

图 18　　审核结果窗口



SA 不会假定程序包 （“注册软件”规则）仅由名称唯一标识，这是一种已知的局限性。

示例：如果某个规则是检查服务器上安装的具有某个版本号的某个程序包（“注册软件”规则），而审核找到了具有相同程序包名称但版本号不同的程序包， SA 不会指示它是您所查找的程序包。相反， SA 将指示此规则未找到该程序包。

视图

“视图”窗格显示审核结果的概述，包括修正选项和按符合性状态分组的服务器 （目标）。

- **摘要**：可用于按服务器、按规则进行修正或修正所有服务器上的所有规则的修正选项。修正仅适用于目标服务器配置与审核中的规则定义不匹配的实例。“摘要”视图也显示了结果所依据的审核中使用的源服务器。审核的源可以是服务器、快照或根本没有源。但是，有些规则需要源。请参见审核元素 （第 18 页）。
- **符合**：● 与审核中所有规则均匹配的服务器。
- **不符合**：✕ 未与审核中所有规则均匹配的服务器。
- **扫描失败**：  审核无法为其确定目标服务器配置的服务器，例如无法与 SA 核心通信的服务器。
- **已跳过**：⃠ 已跳过的服务器。

摘要

“摘要”窗格显示有关审核作业的以下信息：

- **创建时间**、**创建者**：审核创建的时间以及创建者名称。
- **源**：结果所依据的审核中使用的源服务器。审核的源可以是服务器、快照或根本没有源。但是，有些规则需要源。请参见审核元素 （第 18 页）。
- **规则**：**查看规则详细信息 ...** 此链接可打开 “规则”窗口，以供您查看审核的规则。
- **警告**：审核过程中发现的警告数。
- **对象 ID**：SA 客户端使用的内部标识号。
- **符合**：● 与审核中所有规则均匹配的服务器数。
- **不符合**：✖ 并未与审核中所有规则均匹配的服务器数。
- **扫描失败**：审核无法为其确定目标服务器配置的服务器数，例如无法与 SA 核心通信的服务器。
- **已跳过**：⦸ 已跳过的服务器。
- **运行部分审核**：使用此链接，可选择服务器，然后仅在符合性状态为“不符合”或“扫描失败”的规则上重新运行该审核。

详细信息

“详细信息”窗格列出了运行该审核的所有服务器、每个服务器的符合性状态以及对审核中符合、不符合和扫描失败的规则的分别计数。还会显示对例外规则和失败规则的计数。

使用列选择器工具 更改显示首选项。要对列进行重新排序，请单击列标头，然后将其拖动到左边或右边来更改显示首选项。

- **符合**：● 目标服务器配置与审核中的规则匹配的规则数。
- **不符合**：✖ 与审核中的规则不匹配的服务器数。
- **扫描失败**：审核无法为其确定目标服务器配置的规则数，例如无法与 SA 核心通信的服务器。
- **已跳过**：⦸ 已跳过的服务器。

修正方法：全部、按服务器或按规则

在 “审核结果”窗口中，有几种修正审核结果中不符合规则的方法：

- 全部修正：在 “审核结果”窗口的 “操作”菜单中，选择 “全部修正”以修正审核结果中找到的差异。
- 按服务器修正：按审核结果的目标服务器进行修正。
- 按规则修正：修正特定的单个审核规则。

- 在 “安全选项”下，由于 Windows 本地安全设置规则， SA 不支持在 Windows Server 2000 服务器上修正以下两个值：重命名管理员帐户和重命名来宾帐户。
- 在此发布中，无法修正 IIS 7.0 审核规则的 ISAPI 过滤器。

全部修正

可选择修正审核结果中找到的所有可修正规则的所有差异。此选项修正所有审核目标服务器上的所有可修正规则。当审核运行时，无法修正具有 “符合” 状态的规则。

要修正审核结果中找到的所有差异，请执行以下操作：

1. 在导航窗格中，选择 “库” > “按类型” > “审核和修正” > “审核”。
2. 选择一个审核。在审核列表下方的详细信息窗格中，将显示所有与此审核关联的审核结果。
3. 选择一个审核结果，右键单击并选择 “打开”。
4. 在 “审核结果”窗口的 “操作”菜单中，选择 “全部修正”
5. 在 “修正审核”窗口中，步骤 1 显示了审核名称、审核目标和审核中定义的规则总数。如果您想要绕过所有审核任务步骤，请单击 “启动作业”立即运行审核作业。
6. 单击 “下一步”。
7. 在 “计划”页中，指定是要立即运行审核还是在以后的时间和日期运行审核。要在以后运行审核，请选择 “在该时间运行任务”，然后指定日期和时间。
8. 单击 “下一步”。
9. 在 “通知”页中，默认情况下，无论审核作业是否成功，用户都会收到在审核完成时发送的通知电子邮件。要添加电子邮件通知者，请单击 “添加通知者”，并输入电子邮件地址。
10. *（可选）*可以指定在审核作业成功或失败时是否发送电子邮件。
11. *（可选）*可以在 “工单 ID”字段中指定工单跟踪 ID。仅当 HP Professional Services 将 SA 与您的变更控制系统集成时，才能使用 “工单 ID”字段。否则，请将此字段保留为空。
12. 单击 “下一步”。
13. 在 “作业状态”页中，单击 “启动作业”运行审核。如果审核已运行，单击 “查看结果”可查看审核的结果。

按规则修正

可通过选择不符合要求的各个规则，修正在审核结果的规则中找到的特定差异，然后重新运行审核，以便仅修正选择的规则。可选择按所有审核目标服务器的单个规则修正，或选择仅修正选定服务器的规则。

要修正审核结果中找到的特定差异，请执行以下操作：

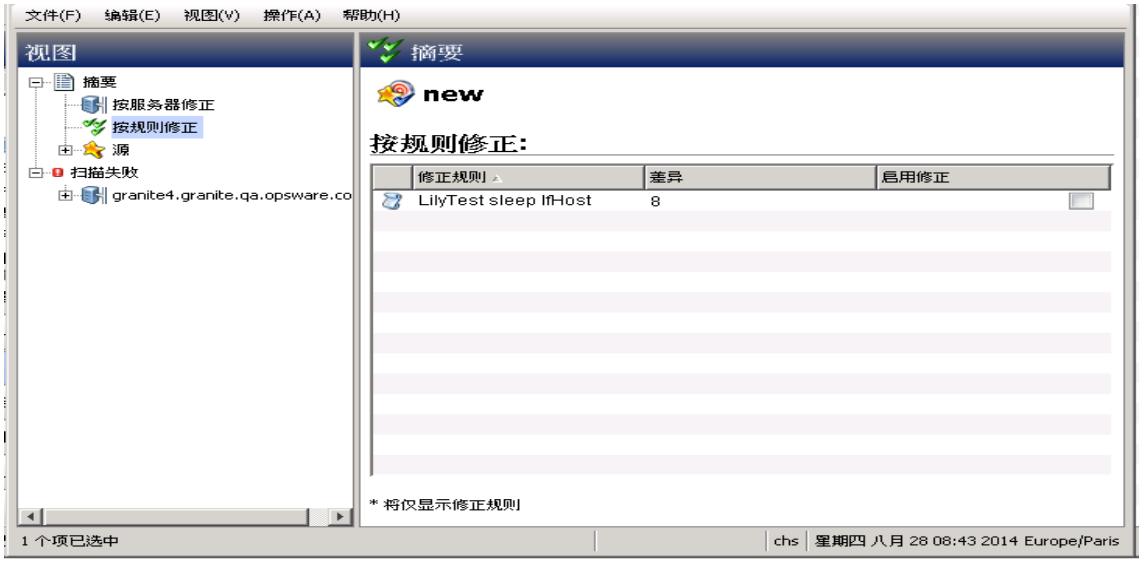
1 在导航窗格中，选择 “库” > “按类型” > “审核和修正” > “审核”。

2 选择一个审核。

3 在审核列表下方的详细信息窗格中，将显示所有与此审核关联的审核结果。

4 选择一个审核结果，右键单击并选择 “打开”。

5 在 “审核结果” 窗口中，展开 “摘要” 列表，然后选择 “按规则修正”。此时将显示审核结果中按规则发现的所有差异。



6 对于要修正的每个规则，在 “启用修正” 列的列表中选中复选标记。这意味着在修正审核结果时，也会修正应用该规则的所有审核目标服务器上的相应规则。

如果要全局选择所有规则，右键单击并选择 “全选” 。要取消选择所有规则，右键单击并选择 “取消全选”。

7 选定要修正的规则后，从 “操作” 菜单中选择 “修正”。

8 在 “修正审核” 窗口中，步骤 1 显示了审核名称、审核目标和审核中定义的规则总数。如果您想要绕过所有审核任务步骤，请单击 “启动作业” 立即运行审核作业。

9 单击 “下一步”。

10 在 “计划” 页中，指定是要立即运行审核还是在以后的时间和日期运行审核。要在以后运行审核，请选择 “在该时间运行任务”，然后指定日期和时间。

11 单击 “下一步”。

12 在 “通知” 页中，默认情况下，无论审核作业是否成功，用户都会收到在审核完成时发送的通知电子邮件。要添加电子邮件通知者，请单击 “添加通知者”，并输入电子邮件地址。

13 *（可选）*可以指定在审核作业成功或失败时是否发送电子邮件。

14 *（可选）*可以在 “工单 ID”字段中指定工单跟踪 ID。仅当 HP Professional Services 将 SA 与您的变更控制系统集成时，才能使用 “工单 ID”字段。否则，请将此字段保留为空。

15 单击 “下一步”。

16 在 “作业状态”页中，单击 “启动作业”运行审核。如果审核已运行，单击 “查看结果”可查看审核的结果。

按服务器修正

可按审核目标服务器修正在审核结果的规则中找到的特定差异。可选择修正所有服务器上的所有规则，或修正选定服务器上的所有规则。

要按服务器修正审核结果中找到的特定差异，请执行以下操作：

1 在导航窗格中，选择 “库” > “按类型” > “审核和修正” > “审核”。

2 选择一个审核。

3 在审核列表下方的详细信息窗格中，将显示所有与此审核关联的审核结果。

4 选择一个审核结果，右键单击并选择 “打开”。

5 在 “审核结果”窗口中，展开 “摘要”列表。

6 内容窗格列出了审核的目标服务器。对于要审核的每个服务器，选中 “启用修正”列的列表中服务器旁边的复选框，然后单击 “运行部分审核”。

或

可展开 “视图”窗格中的服务器列表；对于每个服务器，您将看到在所有审核目标服务器上找到的所有差异。

对要修正的每个服务器，在 “启用修正”列的列表中选中复选标记。这意味着在修正审核结果时，也会修正选中服务器上的所有规则。

或

如果要全局选择审核结果中的所有服务器，右键单击并选择 “全选”。要取消选择所有服务器，右键单击并选择 “取消全选”。

7 选定要修正的服务器后，从 “操作”菜单中选择 “修正”。

8 在“修正审核”窗口中，步骤 1 显示了审核名称、审核目标和审核中定义的规则总数。如果您想要绕过所有审核任务步骤，请单击“启动作业”立即运行审核作业。

9 单击“下一步”。

10 在“计划”页中，指定是要立即运行审核还是在以后的时间和日期运行审核。要在以后运行审核，请选择“在该时间运行任务”，然后指定日期和时间。

11 单击“下一步”。

12 在“通知”页中，默认情况下，无论审核作业是否成功，用户都会收到在审核完成时发送的通知电子邮件。要添加电子邮件通知者，请单击“添加通知者”，并输入电子邮件地址。

13 *（可选）*可以指定在审核作业成功或失败时是否发送电子邮件。

14 *（可选）*可以在“工单 ID”字段中指定工单跟踪 ID。仅当 HP Professional Services 将 SA 与您的变更控制系统集成时，才能使用“工单 ID”字段。否则，请将此字段保留为空。

15 单击“下一步”。

16 在“作业状态”页中，单击“启动作业”运行审核。如果审核已运行，单击“查看结果”可查看审核的结果。

修正基于比较的审核结果

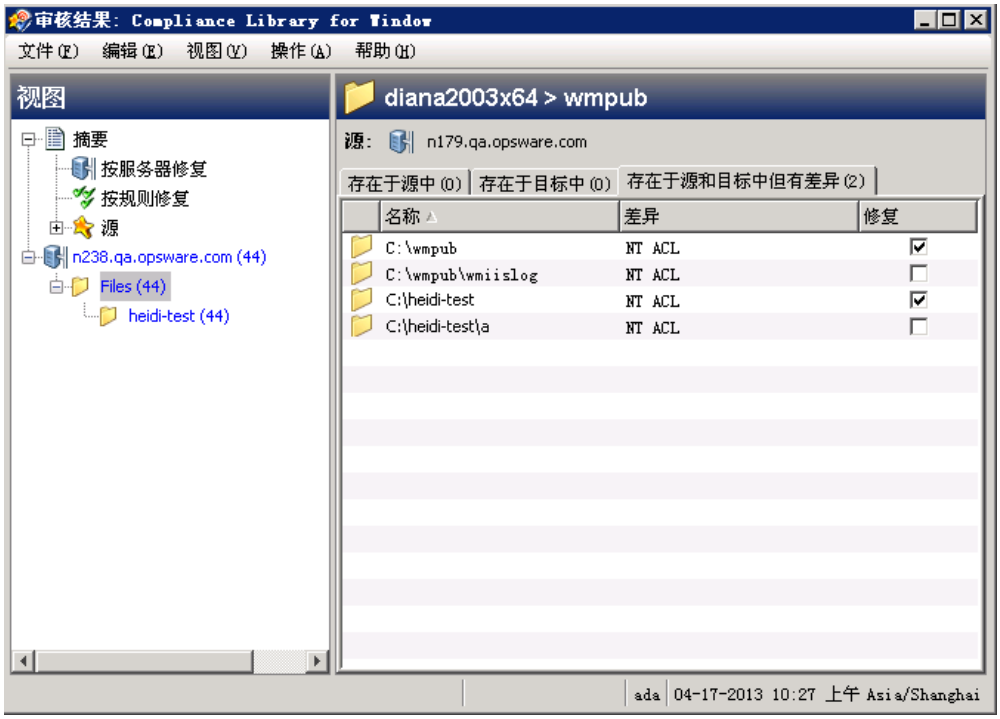
通过使用以基于比较的审核为基础的审核结果，可以查看源服务器或快照和目标服务器或快照之间的差异。如果审核结果失败（即发现源和目标间之间存在差异），则可修正这些差异（对于大部分规则类型而言）。可修正审核中源对象的规则值以及覆盖目标上的值（或添加存在于源但不存在于目标的值。）

“审核结果”窗口在“视图”窗格中显示审核中定义的所有对象。也会以浅蓝色字体突出显示失败的审核结果、在审核和目标服务器之间发现的差异。

例如，图 19 显示了 Windows 文件系统规则的审核结果，其中选定的文件和路径同时存在于源（审核规则源服务器）和目标中，但有差异，它们位于“审核结果”窗口的“存在于源和目标中但有差异”选项卡下。

在 “审核结果”窗口中，可选择 “文件”规则，然后从 “操作”菜单中选择 “修正”。

图 19　　基于比较的审核规则的审核结果



在此示例中，在源和目标之间找到了文件差异，可双击该规则，在单独的窗口中查看这些差异。查看这些差异信息，以确保是否要执行修正。然后，可从 “操作”菜单中选择 “修正”来修正不符合要求的规则或计划稍后运行的审核。修正时，审核的值（派生自源）将替换目标服务器上的相应值。

当修正快照或审核结果中的 COM+ 对象时， SA 客户端不会检查 COM+ 对象的版本。不管它们之间是否存在差异， SA 都将始终修正此对象。

修正带有继承的值的规则

如果基于从父对象集成属性的对象创建审核规则，则请注意，如果修正负责，目标服务器对象将不会继承父对象的属性。

示例：如果为从父级继承了某些值的注册表条目创建规则，则当修正目标服务器上的规则时，将不会修正从父级继承的任何值，且此规则将在审核结果中显示为规则。

另外，如果审核检查文件、注册表或 IIS 元数据库规则的 ACL，但用户和组 ACL 不存在，则在运行审核并进行修正后，如果用户和组在目标上不存在，则会创建未知名称的临时用户和组。下次运行该审核时，它将显示为未知，而不识别源用户。

另外，如果从源服务器创建 IIS 元数据库规则，且为规则选定的元数据库对象从父元数据库对象继承了其值，则在审核运行后将显示差异。

示例：修正一次后重新运行审核，如果源键在目标服务器上创建时未进行继承且特性具有 IED，则对象将根据父键的继承进行创建。当重新运行此审核时，结果会将 IED 显示为对象特性的差异。

如果审核结果中存在 SA 5.1 创建的审核的差异，而您已升级到 SA 6.x 或更高版本，则在 SA 客户端升级版本中查看这些审核结果时，审核结果列表中的“差异”列将错误地显示 -1 值差异。要查看实际的结果数，请打开 “审核结果”窗口查看结果中的所有差异。

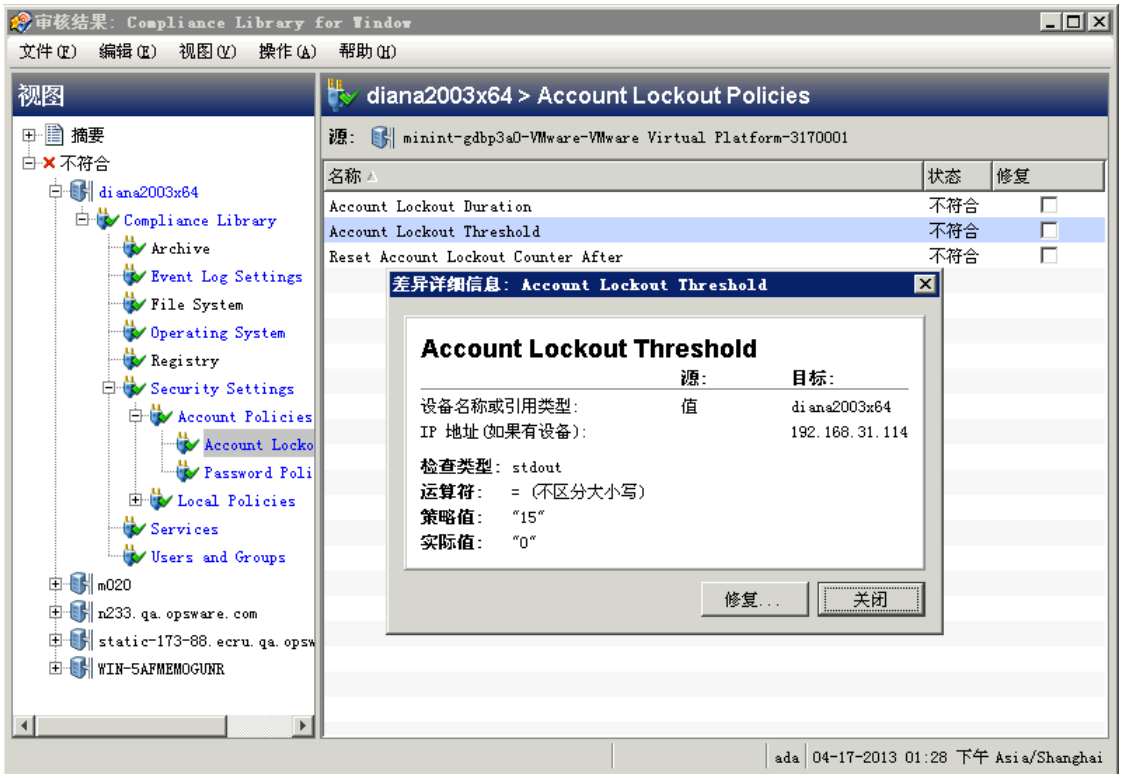
查看基于值的审核结果 — 审核规则修正

基于值的审核结果指示服务器配置是否与审核规则中定义的值匹配。可查看规则定义的期望值与目标服务器中找到的实际值之间的差异。根据规则，可以通过使用规则中指定的值进行替换来修正目标服务器上找到的差异。

一些基于值的规则不可修正。例如， Windows/Unix 用户和组、“属性”值检查不可修正。

图 20 显示了以自定义脚本形式存在的基于值的审核规则，其中该脚本的输出与源服务器上运行的相同脚本的结果不同。规则的 “状态”列标识为 “不符合”，表示脚本规则在源和目标上的输出不同。要解决这种差异，选择 “修正”选项，然后从 “操作”菜单中选择 “修正”。或者双击规则，然后单击 “修正”。

图 20　基于值的审核规则的审核结果



修正带有继承的值的规则

如果基于从父对象集成属性的对象创建审核规则，则请注意，如果修正负责，目标服务器对象将不会继承父对象的属性。

示例：如果为从父级继承了某些值的注册表条目创建规则，则当修正目标服务器上的规则时，将不会修正从父级继承的任何值，且此规则将在审核结果中显示为规则。

另外，如果审核检查文件、注册表或 IIS 元数据库规则的 ACL，但用户和组 ACL 不存在，则在运行审核并进行修正后，如果用户和组在目标上不存在，则会创建未知名称的临时用户和组。下次运行该审核时，它将显示为未知，而不识别源用户。

另外，如果从源服务器创建 IIS 元数据库规则，且为规则选定的元数据库对象从父元数据库对象继承了其值，则在审核运行后将显示差异。

示例：修正一次后重新运行审核，如果源键在目标服务器上创建时未进行继承且特性具有 IED，则对象将根据父键的继承进行创建。当重新运行此审核时，结果会将 IED 显示为对象特性的差异。

如果审核结果中存在 SA 5.1 创建的审核的差异，而您已升级到 SA 6.x 或更高版本，则在 SA 客户端升级版本中查看这些审核结果时，审核结果列表中的“差异”列将错误地显示 -1 值差异。要查看实际的结果数，请打开 “审核结果”窗口查看结果中的所有差异。

查看和修正审核结果差异

对于审核结果中的一些对象，可查看存在于目标和源上的对象与存在差异的对象之间的差异。还可以查看它们之间差异的内容并可以修正差异 （如有需要）。

对于一些审核规则，可查看常规差异，如服务状态、修补程序的发布号、注册表项的值等。对于其他服务器对象 （如文件），可查看文件内容的差异。

查看和修正文件差异

对于一些规则 （如文件系统），可以并排或一行一行地查看文件之间的差异。可以查看已添加、已删除或已修改的行。

要查看和修正审核中两个不同文件的内容，请执行以下操作：

1. 在导航窗格中，选择 “库” > “按类型” > “审核和修正” > “审核”。
2. 选择一个审核。
3. 在审核列表下方的详细信息窗格中，将显示所有与选定审核关联的审核结果。
4. 选择一个审核结果，右键单击并选择 “打开”。
5. 在 “审核结果”窗口的 “视图”窗格中，展开其中一个目标服务器并选择一个结果。
6. 在内容窗格中，展开一个目标服务器并选择其中一个结果。
7. 接下来，在内容窗格中，选择 “存在于源和目标中但有差异”选项卡。
8. 选择一个文件，右键单击并选择 “查看差异”。
9. 在 “比较”窗口中，从 “编码”下拉列表中选择项，以指定所显示数据的字符编码。

如果所选文件的大小超过 2MB，审核和修正则无法显示文件的差异。

10 单击箭头查找已添加、已删除或已修改的第一行、下一行、上一行或最后一行。差异将根据以下颜色方案突出显示：

- **绿色**：此内容已添加。
- **蓝色**：此内容已修改。
- **红色**：此内容已删除。
- **黑色**：此内容未更改。

11 单击 “关闭” 可关闭此窗口。

12 要修正文件差异，从 “审核结果” 窗口内，选择 “存在于源中” 选项卡或 “存在于源和目标中但有差异” 选项卡，选择文件，然后右键单击并选择 “修正”。

13 在 “选择服务器” 窗口中，选择要将文件从源复制到其中的服务器，然后单击 “确定”。

取消活动的修正审核结果作业

在 SA 客户端中，可以终止*活动的修正审核结果作业*。活动的修正审核结果作业是已经开始且正在运行的作业。

对活动的修正审核结果作业执行的终止操作称为*软取消*。软取消是这样一种活动：作业正在部分运行，然后在您单击 “修正审核结果” 向导中的 “作业状态” 步骤的 “结束作业” 时停止。软取消仅适用于要停止的活动的修正审核结果作业。

必须具有取消正在运行的修正审核结果作业的权限。通常情况下，如果有权启动修正审核结果作业，也将可以停止正在运行的修正审核结果作业。另外，如果具有 “编辑或取消任何作业” 权限，也将可以软取消正在运行的修正审核结果作业。有关与审核相关的权限的详细信息，请参见《SA 管理指南》。要获取这些权限，请与 SA 管理员联系。

要停止活动的修正审核结果作业，请执行以下操作：

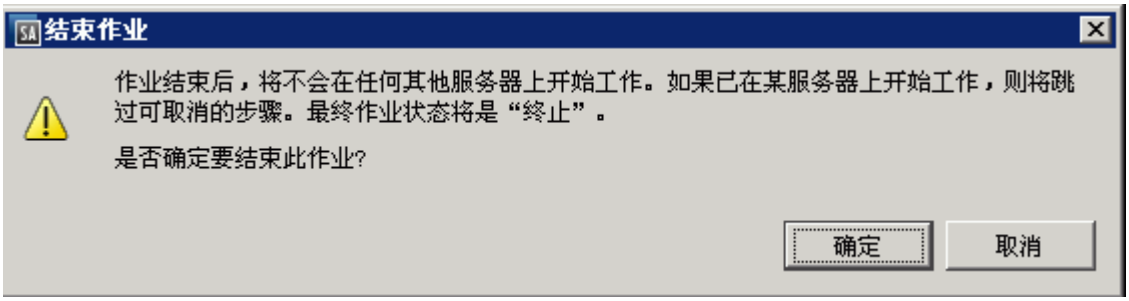
1 在 “作业状态” 窗格中，单击 “结束作业”。

此按钮仅在作业正在运行时可用。

2 此时将显示 “结束作业” 对话框。此对话框简短地描述了作业是如何终止的：

- 作业将不会在任何其他服务器上启动作业。
- 如果作业已在某服务器上运行，则该作业将取消所有可跳过的步骤。
- “作业状态” 将指示这些步骤是已完成还是已跳过。

3 如果作业成功结束，则最终作业状态将显示为 “已终止”。



4 单击 “确定”确认要终止该作业。“作业状态”窗口将显示终止操作过程的进度。

作业状态将为 “已终止”。服务器状态将为 “已取消”。任务状态将为 “成功”或 “已跳过”。

5 当终止完成后，您还可以在 SA 客户端的 “作业日志”中查看作业。

在 SA 客户端导航窗格中，选择 “作业和会话”。“作业日志”视图将显示处于 “已终止”状态的作业。

查看和修正对象差异

对于许多服务器对象（如用户和组、IIS 元数据库、Windows 注册表等），当源对象和目标对象存在差异时，可并排查看对象属性的差异。每个服务器对象将显示不同的窗口，具体取决于该对象以及该审核规则集是基于比较（源和目标之间的比较）还是基于值（用户定义的审核规则和目标之间的比较）。

对于一些基于值的审核规则，可在目标服务器上修正值。

要查看两个不同对象的内容，请执行以下操作：

1 在导航窗格中，选择 “库” > “按类型” > “审核和修正” > “审核”。

2 选择一个审核。

3 在审核列表下方的详细信息窗格中，将显示所有与选定审核关联的审核结果。

4 选择一个审核结果，右键单击并选择 “打开”。

5 在 “视图”窗格中，展开其中一个目标服务器并选择一个结果。

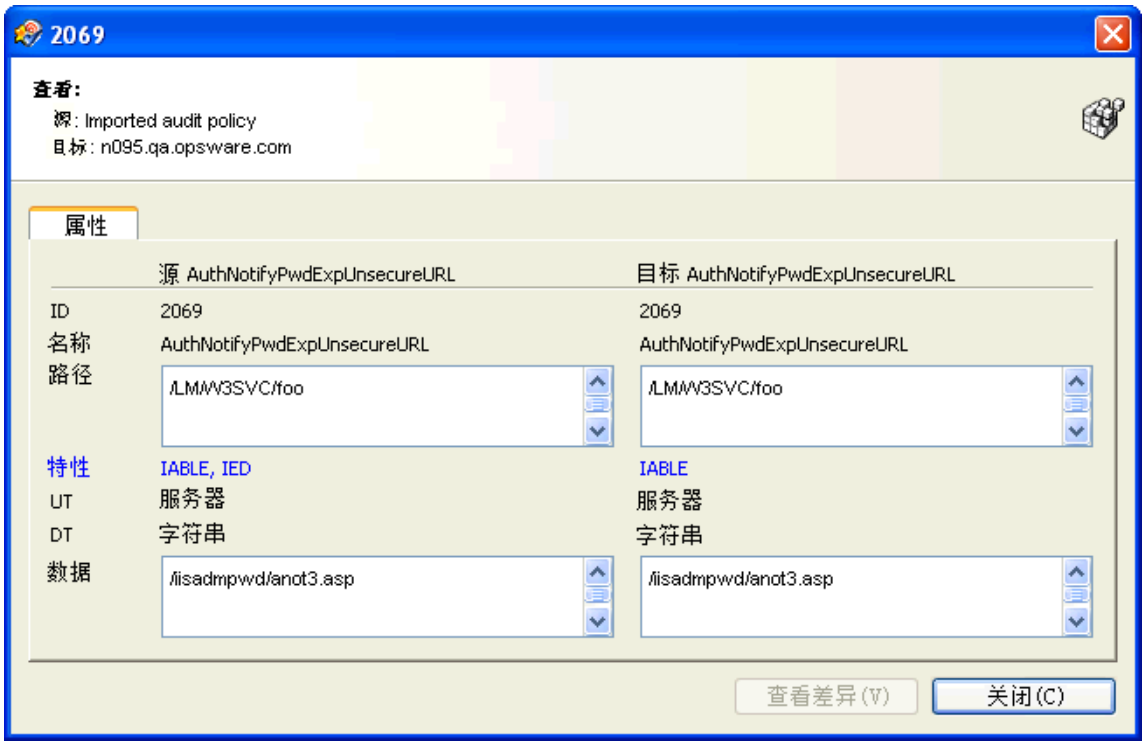
6 在 “视图”窗格中，选择一个对象。

7 在内容窗格中，选择 “存在于源和目标中但有差异”选项卡。

8 在内容窗格中，选择一个对象，右键单击并选择 “打开” 。您将看到一个窗口，其中显示了审核中定义的对象与目标服务器上的对象之间的差异。

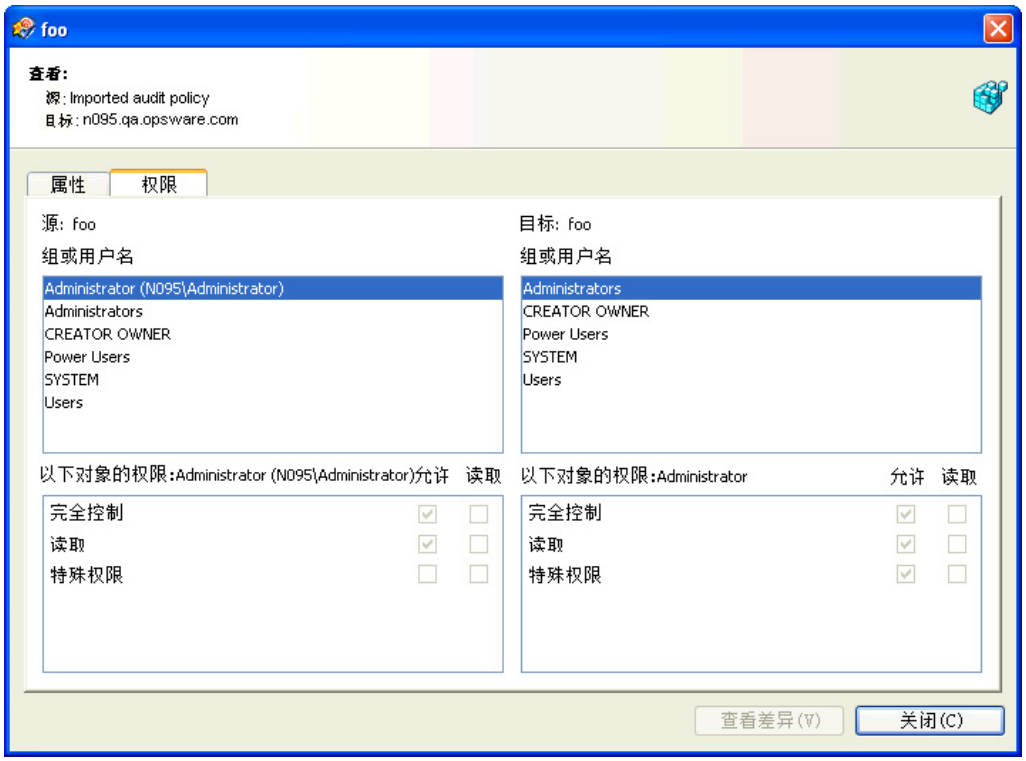
图 21 中的示例以蓝色字体显示了两个 IIS 元数据库对象之间的审核结果差异，显示了存在于服务器但不存在于目标服务器的对象的特性。

图 21　基于比较的审核结果差异：IIS 元数据库对象



对于基于值的规则，差异窗口略有不同，也将包含 “修正” 选项 （如果可修正）。此差异窗口显示审核规则，包括策略值和目标服务器上找到的实际值。图 22 中的示例显示了基于值的 “Windows 注册表” 规则的权限差异。

图 22　基于规则的审核结果差异：Windows 注册表权限差异



9　要修正差异，请选中每条规则旁边的 “修正” 复选标记。

10　从 “操作” 菜单中，选择 “修正”。

11　在 “修正” 窗口中，按照以下步骤运行或计划修正。有关修正审核结果的的详细信息，请参见 查看和修正审核结果差异 （第 96 页）。

查看带有异常的审核结果

如果审核包含规则异常，则审核运行时将不在目标服务器上检查这些例外规则。但是，审核结果将显示审核中的哪些规则是异常，包括有关这些规则异常的详细信息。

规则异常在审核结果中显示的方式取决于已被排除在外的规则的类型：

- 自定义脚本和自定义或可插入检查规则异常 （如由开发者创建或由 EP 内容订阅提供的相应内容）出现在 “审核结果” 窗口的内容窗格中。您可双击规则异常以查看该异常的详细信息。
- 对于所有其他规则异常 （如文件系统、注册表设置、服务、IIS 元数据库和 COM+ 规则），“审核结果” 窗口的 “视图” 窗格会显示一个 “异常” 图标 ，可通过选择该图标在内容窗格中查看该异常的详细信息。

搜索审核

可使用 SA 客户端搜索工具在设施中查找审核。可按名称、操作系统和许多其他条件搜索审核。

要搜索审核，请执行以下操作：

1. 在 SA 客户端 中，请确保搜索窗格已通过选择 “视图” > “搜索” 窗格激活。
2. 从顶部下拉列表中，选择 “审核”。
3. 单击绿色箭头按钮或 ENTER 执行搜索。
4. 结果将显示在内容窗格中。

如果要扩展搜索条件，可在内容窗格顶部的搜索参数部分中添加新条件。也可通过单击 “保存” 保存搜索，或导出搜索结果。请参见导出审核结果 （第 102 页）。

注意：要正确地查看搜索结果，请用文本编辑器打开 .csv 文件，关闭自动换行，然后水平地展开文本窗口。

删除审核

要节省磁盘空间，可删除不再需要的审核。如果要保留结果的记录，可选择存档审核生成的所有审核结果。

当删除审核时，所有与审核关联的计划也会删除。

要删除审核，请执行以下操作：

1. 在导航窗格中，选择 “库” > “按类型” > “审核和修正” > “审核”。
2. 选择 Windows 或 Unix。
3. 选择一个或多个审核，然后选择 “操作” > “删除”。
4. 在确认对话框中，单击 “是” 删除此审核，如果不想删除，则单击 “否”。也可选择 “存档审核” 选项，该选项将存档该审核生成的所有审核结果。如果不选择 “存档” 选项，则选定审核生成的所有审核结果都将被删除。

删除审核结果

最佳实践：删除确定不再需要的审核结果。

必须具有此快照的读取权限才能删除此快照。要获取这些权限，请与 SA 管理员联系。有关详细信息，请参见 《SA 管理指南》。

要删除审核结果，请执行以下操作：

1. 选择一个快照或选择多个快照，然后选择 “操作” > “删除”。
2. 在确认对话框中，单击 “是” 删除此快照，如果不想删除，则单击 “否”。
3. 如果要存档此快照，而不是将其删除，则选择此快照，右键单击并选择 “存档”。

删除快照时，并没有删除创建此快照的快照规范。请参见删除快照规范 （第 115 页）。

存档审核结果

最佳实践：一些审核会产生大量结果，尤其是计划重复运行的审核。存档所有审核结果可保留运行审核产生的所有审核结果的记录。存档审核结果时，SA 会删除其与原始审核的连接，但是审核的结果和目标将保持原样。

要存档审核结果，请执行以下操作：

1. 在导航窗格中，选择 “库” > “按类型” > “审核和修正” > “审核”。
2. 选择操作系统：Windows 或 Unix。
3. 选择一个审核。
4. 在审核列表下方的详细信息窗格中，将显示所有与选定审核关联的审核结果。
5. 要存档审核结果，请选择存档，右键单击并选择 “存档”。
6. 在 “继续存档审核结果”窗口中，系统会询问是否确定要存档审核结果并删除对审核的引用。单击 “是”存档审核结果并删除结果和审核之间的链接。
7. 要查看所有存档的审核结果，在导航窗格中，选择 “库” > “按类型” > “审核和修正” > “存档的审核结果”。

导出审核结果

可将审核结果导出为 CSV 和 HTML 格式。

要导出审核结果，请执行以下操作：

1. 在导航窗格中，选择 “库” > “按类型” > “审核”。
2. 选择 Windows 或 Unix。
3. 选择一个审核。审核结果显示在审核列表下方的面板中。
4. 右键单击审核结果
5. 选择 “打开”。
6. 在 “审核结果”窗口，选择 “操作” > “导出”。
7. 选择其中一种格式 （“CSV”、“HTML”、“XML”、“JSON”）。
8. 在 “导出”窗口，为导出内容选择文件夹、文件名称、编码类型以及文件类型。
9. 单击 “导出”。

   此时将显示导出进度栏。在 SA 与服务器连接之前，状态栏处于不确定模式并显示消息：“正在提取数据 ...”。一旦建立连接，状态栏将按已完成的导出任务数显示导出进度状态。
10. 单击 “停止”将停止导出过程
11. 单击 “后台运行”将关闭进度窗口，并继续在后台运行导出过程。

    单击 “后台运行”时，右下角将出现一个临时窗口，持续几秒钟。单击此临时窗口中的链接可重新激活进度栏的显示。

12 对于非 HTML 导出类型，当导出过程完成时，单击 “关闭” 可关闭进度栏显示。

如果审核导出类型是 HTML，进度窗口会在导出过程完成时自动关闭，审核结果将显示在浏览器中。

13 打开文件可查看导出的信息。

注意：要正确查看导出的 CVS 信息，请用文本编辑器打开 .csv 文件，关闭自动换行，然后水平展开文本窗口。

3 快照、快照规范和快照作业

快照

*快照*在特定时间点捕获托管服务器的配置，并提供已知工作（或已知不工作）的服务器当前状态的捕获方式。快照对于捕获代表所需配置状态的服务器配置非常有用。

最佳实践：还可以通过在审核中使用快照来比较快照和设施中的其他服务器。

快照也是一种备份托管服务器的有效方式，尤其是当计划更改服务器并要在进行任何更改之前对其进行记录时。

除了记录有关托管服务器上对象的信息外，快照还可以包含一些对象的内容。服务器快照也会识别特定类型操作系统上其他对象的特性，如 Windows 注册表和 Windows 服务、应用程序配置、 COM+ 对象、硬件信息、已安装的修补程序等。甚至还可以创建从目标托管服务器收集数据的自定义脚本。

SA 客户端无法创建整个 Windows 注册表的快照或所有系统键的快照。此数据量超过当前设计允许的范围。

VMware ESXi 服务器不能作为快照的源或目标。

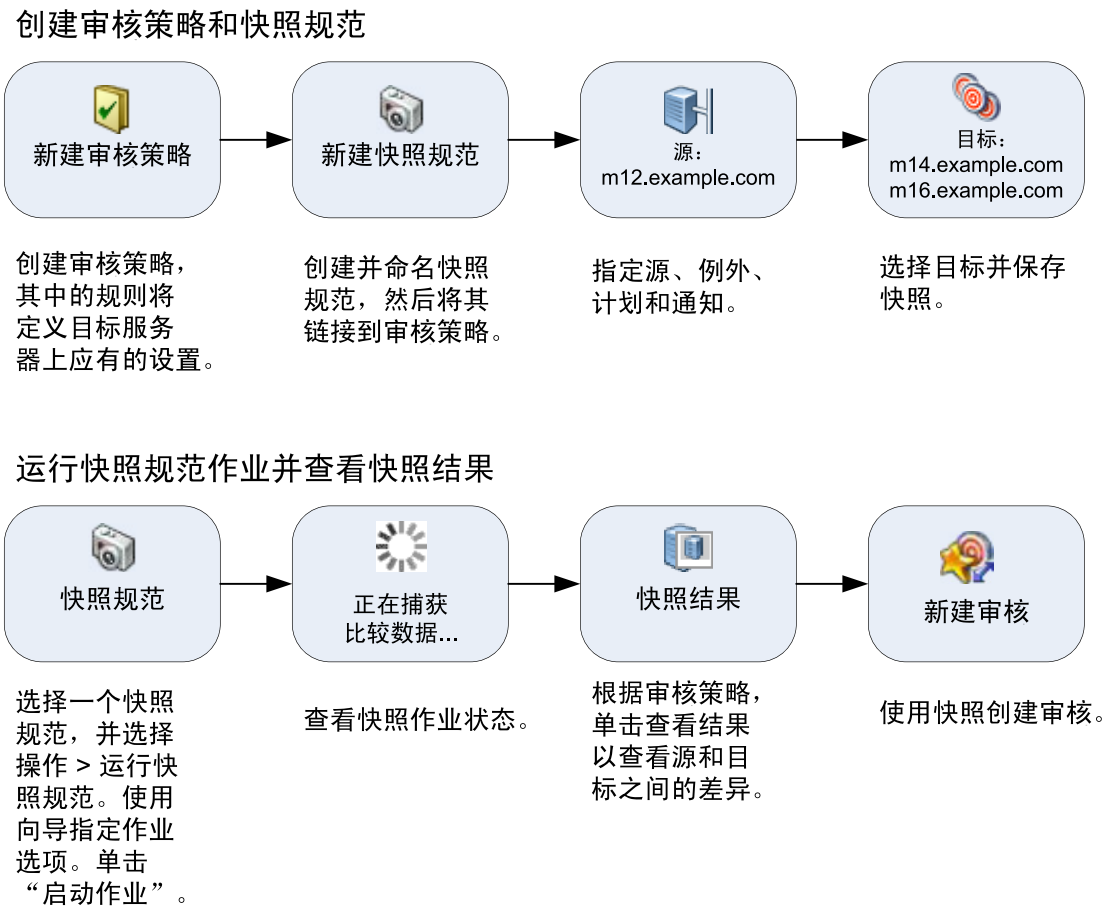
快照进程

要创建服务器配置的快照，需要完成以下任务：

- 创建快照规范，其可作为定义在目标服务器上捕获的配置参数的模板。
- 运行在快照中产生的快照规范作业。

图 23 显示了快照进程，包括分步描述。

图 23　　快照进程



快照和快照规范

快照的配置方式类似于审核的配置方式。首先，创建一个*快照规范*，用作定义要捕获服务器配置的精确内容的模板。接着，配置快照规范的规则，然后运行此快照规范。运行后会生成快照 — 服务器配置的照片。快照和审核之间主要的不同差异为：快照创建服务器配置的照片，而审核将服务器配置与定义的规则值进行比较。

可以计划创建快照的时间 （一次性或重复作业）以及要接收有关作业状态的电子邮件通知的人员。

审核中使用的快照

在审核中使用快照可比较托管服务器、服务器组和快照。通过在审核中使用快照，可以将存在问题的服务器（审核的目标）与已知工作的服务器（作为审核源的快照）进行比较。要进一步扩展审核定义，也可以为服务器对象定义规则。

将快照用作审核的源时，所有在快照结果中捕获的服务器配置值均可用作审核的规则。有关在审核中使用快照的详细信息，请参见审核配置 （第 29 页）。

审核中使用的快照规范

如果要随时间变化跟踪服务器配置并监控所发生的任何更改，则可以将快照规范用作审核的源。例如，您可能要跟踪特定应用程序，以确保随着时间推移其配置依旧正确。如果此应用程序在多个服务器上运行，则可以创建用于定义服务器配置所需状态的快照规范，然后运行此快照。

接下来，可以创建一个审核，然后将原始快照规范用作此审核的源。被快照用作目标的每个服务器现在也作为审核的目标包含在内。然后，当运行此审核时（根据需要或按照计划），系统会将每个服务器的当前配置与最初在原始快照中捕获的状态进行比较。所有更改都会显示在审核结果窗口中。请参见审核配置 （第 29 页）。

快照规范元素

快照规范包括以下元素：

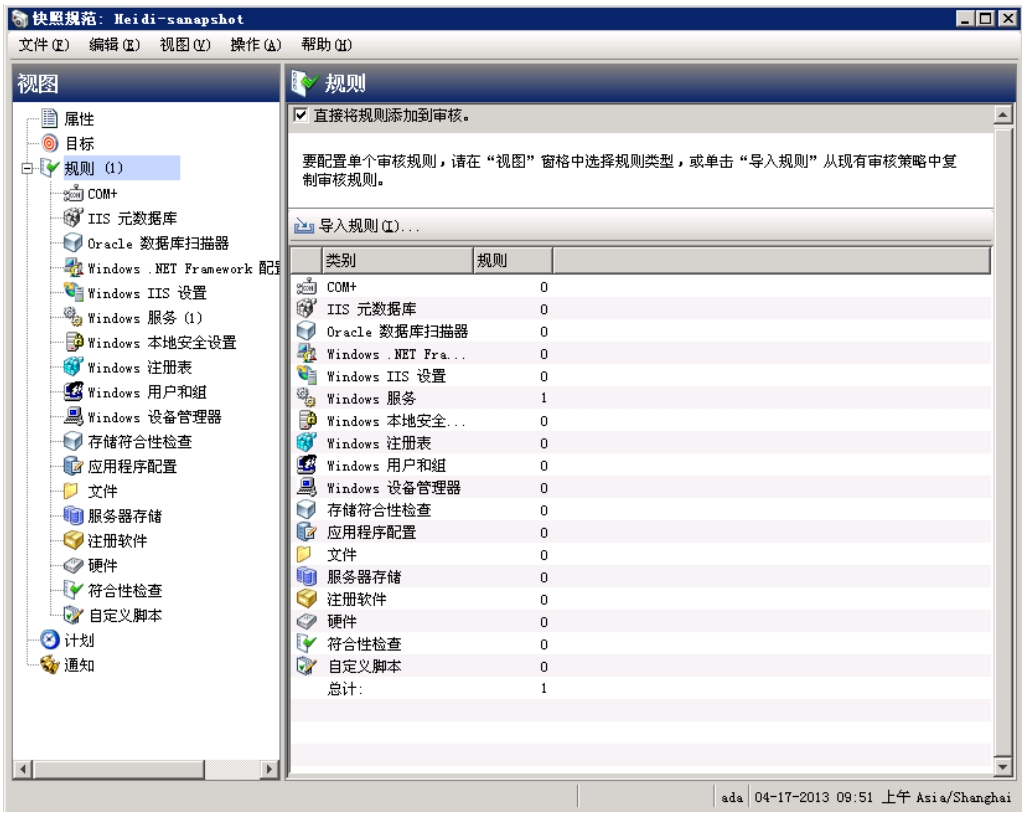
- **属性**：快照规范的名称和描述。如果要创建某些快照规范规则的库存，可以选择“执行库存”，快照结果将从目标服务器收集有关这些特定规则的所有信息。此选项适用于以下规则：“发现的软件”、“Internet Information Server”、“本地安全设置”、“注册软件”、“Windows 用户和组”和 “UNIX 用户和组”。
- **目标**：需要为其创建快照（即捕获快照规范规则中定义的特定服务器配置）的服务器。可以根据需要选择多个服务器或服务器组。
- **源**：快照规范的源。如果选择了服务器，则接下来便可以从该服务器选择服务器对象作为快照的基础。快照规范的源可以是服务器或根本没有源。（但是，有些规则需要源服务器。其他规则可通过自定义值定义为无源。）
- 请注意，在创建快照时不使用源参数的值。它仅在定义快照规范时才有意义。
- **规则**：一项使用所需值和可选修正值在特定服务器对象上进行的检查。例如，您可能要查看此服务器是否含有特定 Windows 服务，如果找到，则确定该服务是否已关闭。有关可在快照规范中为其定义规则的服务器对象的描述，请参见审核和修正规则 （第 35 页）。

- **计划**：快照将运行的时间。可以将快照规范作为作业按一次性计划或重复计划运行。
- **通知**：快照运行后所发送的电子邮件通知。可以在通知内容中包含快照规范作业的成功、失败或完成。

当设置快照规范时，在目标服务器上选择要检查的对象。也可将规则应用到定义它们所需配置状态的对象。对于某些规则，可在生成的快照用作审核源的情况下定义修正值。

图 24 显示了一个具有三个规则的快照规范，这三个规则将捕获有关目标服务器事件日志记录、操作系统和 Windows 服务的配置信息。

图 24　　快照规范服务器对象



查看快照

创建快照后，可在 SA 客户端的几个位置中进行查看。

在 SA 库中

要查看关联到特定服务器的快照，请执行以下操作：

1. 在导航窗格中，选择 “库” > “按类型” > “审核和修正” > “快照规范”。
2. 选择操作系统：Windows 或 Unix。
3. 在列表中，选择一个快照规范。详细信息窗格将显示所有从选定快照规范运行的快照。

在设备资源管理器中

要查看关联到特定服务器的快照，请执行以下操作：

1. 在导航窗格中，选择 “设备” > “服务器” > “所有托管服务器”。
2. 从列表中选择服务器，右键单击并选择 “打开”。
3. 在 “设备资源管理器” 窗口，选择 “库存” > “快照规范”。
4. 在内容窗格中，选择一个快照规范。详细信息窗格将显示所有关联的快照。
5. 要查看快照，请选择该快照，然后双击打开。

搜索快照

可使用 SA 客户端搜索工具在设施中查找快照。可按名称、操作系统和许多其他条件搜索快照。

要搜索快照，请执行以下操作：

1. 在 SA 客户端，选择 “视图” > “搜索窗格”。
2. 从下拉列表中，选择 “快照”。
3. 单击绿色箭头或 ENTER 启动搜索。结果将显示在内容窗格中。

   要展开搜索条件，可在内容窗格顶部的搜索参数部分中添加其他条件。也可以保存搜索或将搜索结果导出到 .html 或 .csv 文件。

注意：要正确地查看结果，请用文本编辑器打开 .csv 文件，关闭自动换行，然后水平地展开文本窗口。

查看快照结果

可以查看快照的内容，还可以查看有关记录的服务器配置的详细信息。

有关修正快照结果的信息，请参见复制对象 （第 113 页）。

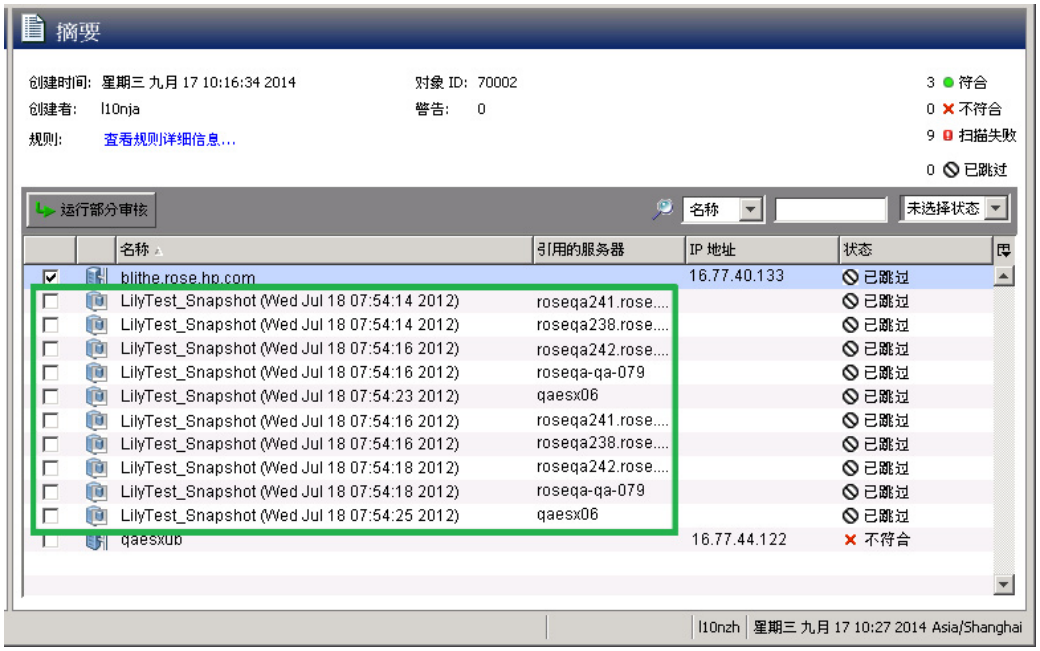
要查看快照的内容，请执行以下操作：

1 从查看快照 （第 109 页）中描述的其中一个起始点，打开快照。

图 25 Windows 服务器的快照

2 在 “快照”窗口中，可在 “Views 视图”窗格选择或展开以下服务器对象：

- **摘要**：显示有关快照的常规信息，如创建快照的日期和时间及用户、快照的源 （托管服务器的名称）、快照文件的大小，快照 ID 号、快照结果引用的服务器以及该服务器的 IP 地址。



还可以单击 “查看规则详细信息”查看此快照所基于的快照规范。

- **符合性库**：有关快照规范中配置的特定符合性检查的信息。有关可用的 BSA Essentials 订阅服务符合性检查类型及其配置方式的详细信息，请参见配置符合性检查 （第 65 页）
- **已安装的硬件**：有关快照中记录的 CPU 处理器类型和速度、缓存大小、SWAP 和 RAM 内存大小以及存储设备的信息。
- **已安装的修补程序**：显示有关快照中记录的已安装修补程序的信息，如修补程序类型。
- **已安装的程序包**：显示有关快照中记录的已安装程序包的信息，如程序包类型、程序包版本和发布号。
- 对于 .zip 程序包，快照不显示其版本号，而是显示该程序包在服务器上的安装路径。
- **事件日志记录**：显示快照中记录的安全、应用程序和系统日志文件。
- **文件系统**：显示快照中记录的目录、文件属性、特性和文件内容。

如果快照中的文件大小超过 2MB，审核和修正则无法显示此文件的内容。

- **Windows 服务**：显示有关快照中记录的运行服务的信息，如名称、描述、启动状态、启动类型和登录帐户。
- **Windows 注册表**：显示有关快照中的 Windows 注册表条目的信息，如注册表项、注册表值和子键。注册表项是含有注册表值的目录，其中注册表值类似于目录中的文件。子键类似于子目录。此窗口的内容区域不包含子键。审核和修正支持以下 Windows 注册表项：HKEY_CLASSES_ROOT、 HKEY_CURRENT_CONFIG、 HKEY_LOCAL_MACHINE 和 HKEY_USERS。
- **COM+**：显示有关快照中的 Windows COM （组件对象模型）对象的信息，如对象的名称和 GUID （全局唯一标识符）以及指向进程内服务器 DLL 的路径。
- SA 提供警告消息，说明如何处理 Windows COM 文件夹。适用于以下场景：
- 当创建快照并选择一个不包含任何对象的 Windows COM 文件夹时，快照窗口会显示摘要。SA 显示警告，说明此文件夹的 GUID （全局唯一标识符）无效，这意味着 Windows COM 文件夹未包含任何对象。
- 当创建快照规范并选择一个目标中不存在的 Windows COM+ 对象时，SA 显示警告，说明此文件夹无效。
- 当创建快照并选择一个不包含任何对象的 Windows COM+ 文件夹时，SA 显示警告，说明此文件夹为空。
- **IIS 元数据库**：显示有关快照中的 IIS 元数据库对象的信息，如对象的 ID、名称、路径、特性和数据。
- **自定义脚本**：显示有关快照中记录的自定义脚本规则的信息。
- **用户和组**：显示有关服务器上的用户和组的信息，如上次登录的用户名、是否启用 CTRL + ALT + DELETE 等。

3 单击 “关闭”以关闭对象浏览器。

存档快照

一些快照规范会产生大量快照，尤其是计划重复运行的快照规范。通过存档所有快照，可保存服务器或服务器组的所有快照运行的记录。

存档快照时，系统会将该快照与服务器分离，并删除其与原始快照规范之间的连接。

要存档快照，请执行以下操作：

1. 在导航窗格中，选择 “库” > “按类型” > “审核和修正” > “快照规范”。
2. 选择操作系统：Windows 或 Unix。
3. 选择快照规范 “详细信息”窗格将显示所有与选定快照规范关联的快照。
4. 要存档快照，将其选中，右键单击，然后选择 “存档”。
5. 单击 “是”确认要存档该快照，如果确认则快照和快照规范之间的链接将被删除。
6. 要查看所有存档的快照结果，在导航窗格中，选择 “库” > “按类型” > “审核和修正” > “存档的快照”。

删除快照

最佳实践：应仅在不再需要快照时，才从软件数据库中将其删除。这有助于节省磁盘空间。

必须具有此快照的读取权限才能删除此快照。要获取这些权限，请与 SA 管理员联系。有关详细信息，请参见 《SA 管理指南》。

要删除快照，请执行以下操作：

1. 选择一个快照或选择多个快照，然后选择 “操作” > “删除”。
2. 在确认对话框中，单击 “是”删除此快照，如果不想删除，则单击 “否”。
3. 如果要存档此快照，而不是将其删除，则选择此快照，右键单击并选择 “存档”。

删除快照时，并没有删除创建此快照的快照规范。请参见删除快照规范 （第 115 页）。

导出 / 导入快照

使用快照筛选器告知 DET 要从 SA 核心 / 网状网络导出的快照，以便之后可以将其导入到另一个 SA 核心 / 网状网络。有关快照筛选器的详细信息，请参见 《SA 内容实用程序指南》。

复制对象

从快照到服务器

查看快照内容后，可将特定对象复制到目标服务器。通过使用 SA，可将目录、文件、 Windows 服务（仅状态）、 IIS 元数据库对象、 COM+ 对象和类别以及 Windows 注册表项复制到托管服务器。

必须具有目标服务器的写入权限，才能将对象复制到该服务器。要获取这些权限，请与 SA 管理员联系。有关权限的详细信息，请参见 《SA 管理指南》。

要将 COM+ 规则快照结果从快照复制到服务器，必须在配置 COM+ 规则时选择 “存档所有关联的文件”选项。同时，为了能够复制到修正，正在复制的 COM+ 对象必须未用于任何应用程序。请参见配置 COM+ 规则 （第 41 页）。

在将这些对象复制到托管服务器之前，您需要了解复制到目标服务器或在其中创建的实际内容。

- 当选择目录时，则只会将该目录复制到目标服务器，而不包括该目录中的任何文件。例如，如果 dir1 包含 file1 和 file2，而您选择 dir1，那么审核和修正只会将 dir1 （而不是 file1 和 file2）复制到目标服务器。
- 当选择某个文件，而该文件的父目录在目标服务器上不存在时，审核和修正将在目标服务器上创建该目录并将文件复制到其中。例如，如果选择 file1 且 dir1 在目标服务器上不存在，那么审核和修正将在目标服务器上创建 dir1，并将 file1 复制到其中。
- 当复制 Windows 服务对象时，复制的是该服务的状态，如已启动、已停止、已暂停等。可一次选择一个或多个 Windows 服务对象进行复制。
- 当复制 Windows 注册表对象时，可一次选择一个或多个注册表项和子键进行复制。
- ACL 不会随 COM+ 对象或 Microsoft IIS 对象复制到目标服务器。
- 从快照结果使用 “复制到”修正 COM+ 对象时， SA 客户端不会对 COM+ 对象的版本进行检查，因此无论它们之间是否存在差异都会复制该对象。

要将对象从快照复制到托管服务器，请执行以下操作：

1 打开一个快照。请参见查看快照 （第 109 页）。

2 在 “视图” 窗格中，选择文件系统、 Windows 服务或 Windows 注册表对象。

3 在内容窗格中，选择要复制的一个或多个对象。

4 选择 “操作” > “复制到”。

5 在 “选择服务器” 窗口中，选择目标服务器。


使用搜索工具，可以通过输入服务器名称、 IP 地址或操作系统对此列表进行动态筛选。

6 单击 “选择” 将对象复制到该托管服务器，或单击 “取消” 不保存更改而关闭窗口。

注意：审核、审核结果修正和创建快照作业支持软取消。但是，快照修正作业、包括从快照 “复制到” 服务器，不支持软取消。

快照规范

通过 SA 客户端，可执行以下管理快照规范的任务：

- 快照规范和审核策略 （第 114 页）
- 创建快照规范 （第 115 页）
- 删除快照规范 （第 115 页）
- 配置快照规范 （第 116 页）
- 配置快照规范规则 （第 118 页）
- 将快照规范保存为审核策略 （第 118 页）
- 运行快照规范 （第 118 页）
- 计划重复快照作业 （第 119 页）

快照规范和审核策略

审核策略是定义服务器配置所需状态的规则集合。审核策略可在快照规范内使用，无论是通过链接还是导入。审核策略的有用性在于使策略设置员能够定义服务器配置符合性值，然后供其他人在自己的快照规范中使用。

由于审核策略可链接到审核或快照规范，因此无论何时对策略进行了更改，使用该策略的审核或快照规范都将会反映最新更改。或者在不保留指向源审核策略的链接的情况下，将审核策略导入到快照规范中。将审核策略导入到快照规范中时，可选择替换审核中的任何当前值或将审核策略中的值与快照规范中的值进行合并。

创建快照规范

可从 SA 客户端的以下位置创建快照规范：

- 从服务器 （第 115 页）
- 从 SA 库 （第 115 页）

必须具有创建和修改快照规范的权限集。要获取这些权限，请与 SA 管理员联系。有关权限的详细信息，请参见 《SA 管理指南》。

从服务器

当从托管服务器创建新的快照规范时，该快照规范将使用选定的服务器作为它的源。可在定义规则时为快照规范选择几个不同的服务器源，或者选择无源，然后定义自己的自定义规则。但是，有些规则需要源。

要创建托管服务器的快照，该服务器必须是可访问的且您必须具有该服务器的访问权限。

要从服务器创建快照规范，请执行以下操作：

1. 在导航窗格中，选择 “设备” > “服务器” > “所有托管服务器”。
2. 选择一个服务器然后选择 “操作” > “创建快照规范”。

从 SA 库

如果要创建一个新的快照规范并将所有规则设置为您自己的规则，则可通过执行以下步骤从 SA 客户端库创建审核：

1. 在导航窗格中，选择 “库” > “按类型” > “审核和修正”。
2. 在导航窗格中，选择快照规范，然后选择 Windows 或 Unix。

删除快照规范

要节省磁盘空间，可删除不再需要的快照规范。如果要保留结果的记录，可选择存档快照规范生成的所有快照。或者，可选择删除此快照规范以及与之关联的所有快照。

要删除快照规范，请执行以下操作：

1. 在导航窗格中，选择 “库” > “按类型” > “审核和修正” > “快照规范”。
2. 选择 Windows 或 Unix。
3. 选择一个或多个快照规范，然后选择 “操作” > “删除”。
4. 在确认对话框中，单击 “是” 删除此快照规范，如果不想删除，则单击 “否”。也可选择 “存档快照” 选项，该选项将存档该快照规范生成的所有快照。如果不选择 “存档” 选项，则选定快照规范生成的所有快照都将被删除。

删除快照规范时，所有与之关联的计划也将被删除。请参见快照作业 （第 119 页）。

配置快照规范

要配置快照规范，需要执行以下任务：

- 命名并描述快照规范，然后决定是否要执行库存。
- 选择要为其创建快照的目标服务器。可选择创建多个服务器或服务器组的快照。
- 配置自己的自定义规则，或选择源服务器的设置作为此快照规范规则的基础。
- 计划快照规范作业按一次性计划或重复计划运行。
- 设置电子邮件通知，以在快照规范作业成功完成时，或作业失败时，或这两种情况下通知用户。
- 保存快照规范。

如果为 32 位 Windows 服务器的 COM+ 对象创建快照，且尝试使用 “复制到” 将此结果修正到 Windows 64 位服务器中，此操作可能会失败。

VMware ESXi 服务器不能作为审核或快照的目标。

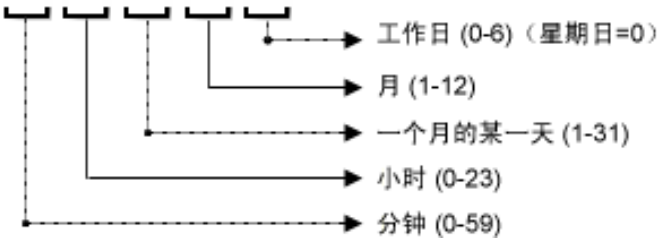
要配置快照规范，请执行以下操作：

1. 在导航窗格中，选择 “库” > “按类型” > “审核和修正”。
2. 在导航窗格中，选择 “快照规范”，然后选择 Windows 或 Unix。
3. 在 “操作” 菜单中，选择 “新建”。
4. 在 “快照规范” 窗口中，输入以下信息：
   - **属性**：输入快照规范的名称和描述。对于特定快照规范规则 （发现的软件、 Internet Information Server、本地安全设置、程序包和修补程序、 Windows 用户和组和 Unix 用户和组），还可以选择 “执行库存” 选项，此选项将捕获所有与此规则关联的资源。
   - **源**：为快照规范选择一个源。默认情况下，快照规范的源服务器将成为您选作快照规范的源的托管服务器。浏览源服务器的值以填充快照规范的规则。也可以为每个规则类别选择不同的源服务器作为快照规范的基础，或者选择无源。如果选择无源，则必须定义自己的规则，或选择链接到规则部分中的某个审核策略。
   - **规则**：从列表中选择规则类型，以开始配置快照规范的规则。由于每个规则都是唯一的，在配置时都有自己的说明，因此要配置特定规则，请参见审核和修正规则 （第 35 页）。

     如果要使用审核策略来定义快照规范的规则，则单击 “链接策略” 或 “导入策略” 。当链接审核策略时，快照规范将保持与审核策略的直接连接，所以如果此策略进行了任何更改，快照规范也会更新这些更改。如果导入审核策略，快照规范将使用在该策略中定义的所有规则，但不会保持与审核策略的链接。有关如何导入或链接到快照规范的信息，请参见链接和导入审核策略的方式 （第 82 页）。

- **目标**：选择快照规范的目标。它们是要配置的快照规范规则捕获的服务器或服务器组。要添加服务器或服务器组，请单击“添加”。要选择用于创建快照规范规则的源服务器，请单击“选择”。
- **计划**：选择立即运行快照规范或按重复计划运行。选择运行的频率是一次、每天一次、每周一次、每月一次，还是按自定义计划。参数包括：
- **无**：不会设置任何计划。要运行快照规范，请选择快照规范，右键单击并选择 “运行快照规范”。
- **每日**：选择此选项将每天运行快照规范一次。
- **每周**：选择一周的某天运行快照规范。
- **每月**：选择运行快照规范的月份。
- **自定义**：在 “自定义 Crontab 字符串”字段中，输入表示时间计划的字符串。

  crontab 文件有五个字段用于指定周日期、月份、月日期、小时和分钟。以下图表显示了 crontab 文件中的各个位置，位置所对应的内容以及所允许的值：

  crontab 字符串可包含连续值 (1,2,3,4) 和范围 (1-5) 值。只有一部分操作系统支持分钟格式 /2 或 /10，这种分钟格式用于每隔 2 分钟或 10 分钟运行一次审核。星号 (*) 表示该字段的所有值，如一年的所有月份。日可在两种字段中进行指定：月日期和周日期。如果两个日期都被指定，则这两个值都将执行。所有操作系统每个字段内都支持逗号隔离值。例如：

  5,10 0 10 * 1 意思是每个月或每个月 10 号和每个周一的上午 12：05 和 12：10 运行审核。

  有关 crontab 输入格式的详细信息，请参考 Unix 手册页。
- **时间和持续时间**：针对各种类型的计划，指定启动每日计划的小时和分钟。除非指定结束时间，否则快照规范将无限期运行下去。要选择快照规范计划的结束日期，请选择 “结束”，然后从日历选择器中选择日期。“时区”将根据您的用户配置文件中设置的时区进行设置。
- **通知**：输入在快照规范作业结束运行时将收到电子邮件的电子邮件地址 （用逗号或空格分隔）。可以选择快照规范作业成功和失败时 （而不是审核规则成功时）都发送电子邮件。要添加电子邮件地址，请单击 “添加通知”规则。

5 当完成配置快照规范时，从 “文件”菜单中，选择 “保存”。

要防止进程出现失控，快照进程在其超过 60 分钟后超时或从托管服务器收集的数据超过 1 GB 时超时。如果指定要在选择的条件下收集文件的全部内容，则收集的数据很可能会超过可成功记录在快照中的最大大小。

配置快照规范规则

有关如何配置特定快照规范规则的信息，请参见审核和修正规则 （第 35 页）。

将快照规范保存为审核策略

可将快照中使用的选择条件保存为审核策略。这对于要将快照规范中配置的规则用于其他快照规范或审核非常有用。如果审核规则要求目标服务器上安装最新代理，则 SA 客户端将显示消息提醒您更新代理以避免出现运行时错误。

创建的所有审核策略都必须保存在 SA 库的文件夹中。必须对要保存审核策略的文件夹具有写入权限。有关文件夹权限的详细信息，请参见《SA 用户指南：Server Automation》或与 SA 管理员联系。

要将快照规范保存为审核策略，请执行以下操作：

1. 启动 SA 客户端。
2. 在导航窗格中，选择 “库” > “按类型” > “审核和修正”。
3. 选择 “快照规范”，然后双击要保存为审核策略的快照规范。
4. 在 “快照规范”窗口，选择 “文件” > “另存为”。
5. 在 “另存为”窗口中，输入名称和简短描述。
6. 从 “类型”下拉列表中，选择 “审核策略”。
7. 单击 “保存”。选定快照规范将保存为审核策略。
8. 要查看审核策略，在导航窗格，选择 “库” > “按类型” > “审核和修正” > “审核策略”。有关使用审核策略的详细信息，请参见审核策略管理 （第 79 页）。

运行快照规范

运行快照规范时，SA 将捕获（从目标服务器）规则中配置的所有配置参数。运行快照规范后，快照作业的结果将成为快照，并且可以从快照内部查看。

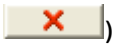
要运行快照规范，请执行以下操作：

1. 在导航窗格中，选择 “库” > “按类型” > “审核和修正”。
2. 在导航窗格中，选择 “快照规范”。
3. 选择 Windows 或 Unix。
4. 选择快照规范，右键单击并选择 “运行”。在 “运行快照规范”窗口中，步骤一将显示此快照的名称、所定义的规则总数以及所有目标。
5. 单击 “查看规则详细信息”可查看规则定义。
6. 单击 “下一步”。

7 在“计划”窗口中，选择是否要立即运行审核或在以后的时间和日期运行审核。要在以后运行审核，请选择第二个选项并指定日期和时间。

8 单击“下一步”。

9 在“通知”视图中，默认情况下，无论审核作业是否成功，用户都会收到在审核完成时发送的通知电子邮件。要添加电子邮件通知者，请单击“添加通知者”，并输入电子邮件地址。

10 *（可选）*可以指定在审核作业成功 () 或审核作业失败 () 时发送电子邮件。

11 *（可选）*可以在“工单 ID”字段中指定工单跟踪 ID。仅当 HP Professional Services 将 SA 与您的变更控制系统集成时，才能使用“工单 ID”字段。否则，请将此字段保留为空。

12 单击“下一步”。

13 在“作业状态”视图中，单击“启动作业”运行审核。如果审核已运行，单击“查看结果”可查看审核的结果。

快照作业

通过快照规范作业，可以指定希望 SA 客户端创建快照的时间 （创建一次或重复创建）以及有关作业状态的电子邮件通知的接收者。也可以查看、编辑和删除现有的快照规范计划。删除快照规范时，所有与此快照规范关联的计划都将被删除。

通过 SA 客户端，可执行以下管理快照作业的任务：

- 计划重复快照作业 （第 119 页）
- 查看和编辑快照作业计划 （第 120 页）
- 删除快照作业计划 （第 122 页）

计划重复快照作业

创建、配置和保存快照规范后，可以为快照规范计划重复快照作业。计划设置后，可以根据需要编辑计划。

要计划重复快照规范，请执行以下操作：

1 在导航窗格中，选择“库” > “按类型” > “审核和修正” > “快照规范”。

2 选择 Windows 或 Unix。

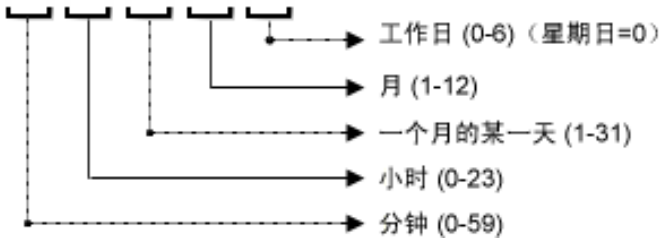
3 选择一个快照，然后双击将其打开。

4 在“快照规范”窗口的“视图”窗格中，选择“计划”。

5 在“计划”部分中，选择立即运行或按重复计划运行快照作业。选择运行的频率是一次、每天一次、每周一次、每月一次，还是按自定义计划。

- **无**：不会设置任何计划。要运行快照作业，请选择该快照规范，右键单击并选择 “运行审核”。
- **每日**：选择此选项将每天运行快照作业一次。
- **每周**：选择一周的某天运行快照规范作业。
- **每月**：选择运行快照规范作业的月份。
- **自定义**：在 “自定义 Crontab 字符串”字段中，输入表示时间计划的字符串。

  crontab 文件有五个字段用于指定周日期、月份、月日期、小时和分钟。以下图表显示了 crontab 文件中的各个位置，位置所对应的内容以及所允许的值：



  crontab 字符串可包含连续值 (1,2,3,4) 和范围 (1-5) 值。只有一部分操作系统支持分钟格式 /2 或 /10，这种分钟格式用于每隔 2 分钟或 10 分钟运行一次审核。星号 (*) 表示该字段的所有值，如一年的所有月份。日可在两种字段中进行指定：月日期和周日期。如果两个日期都被指定，则这两个值都将执行。所有操作系统每个字段内都支持逗号隔离值。例如：

  5,10 0 10 * 1 意思是每个月或每个月 10 号和每个周一的上午 12：05 和 12：10 运行审核。

  有关 crontab 输入格式的详细信息，请参考 Unix 手册页。

- 在 “时间和持续时间”部分，为每个类型的计划指定启动每日计划的小时和分钟。除非指定结束时间，否则快照规范作业将无限期运行下去。要选择审核计划的结束日期，请选择 “结束”，然后选择一个结束日期。“时区”将根据您的用户配置文件中设置的时区进行设置。
- *（可选）*如果希望快照规范作业无限期地运行下去，则取消选择 “结束”选项。

6 要保存快照规范作业计划，请从 “文件”菜单中，选择 “保存”。这样快照规范将会根据定义的计划运行。

查看和编辑快照作业计划

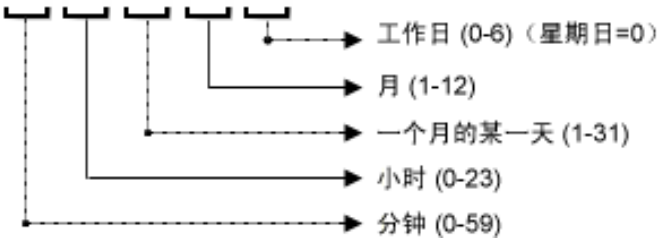
创建 （或编辑）并保存快照规范后，可以对其计划进行编辑。

要编辑已计划快照规范，请执行以下操作：

1 在导航窗格中，选择 “作业和会话”。
2 选择 “重复计划”。
3 从下拉列表中，选择 “创建快照”。列表将显示所有已计划的快照规范作业。
4 要查看某个已计划的快照规范，可对其双击。
5 在 “视图”窗格中，选择 “计划”对象。
6 要编辑快照规范作业计划，请修改以下参数：

- **计划**：选择立即运行快照规范或按重复计划运行。选择运行的频率是一次、每天一次、每周一次、每月一次，还是按自定义计划。参数包括：
- **无**：不会设置任何计划。要运行快照规范，请选择快照规范，右键单击并选择 “运行快照规范”。
- **每日**：选择此选项将每天运行快照作业一次。
- **每周**：选择一周的某天运行快照作业。
- **每月**：选择运行快照规范作业的月份。
- **自定义**：在 “自定义 Crontab 字符串”字段中，输入表示时间计划的字符串。

  crontab 文件有五个字段用于指定周日期、月份、月日期、小时和分钟。以下图表显示了 crontab 文件中的各个位置，位置所对应的内容以及所允许的值：

  crontab 字符串可包含连续值 (1,2,3,4) 和范围 (1-5) 值。只有一部分操作系统支持分钟格式 /2 或 /10，这种分钟格式用于每隔 2 分钟或 10 分钟运行一次审核。星号 (*) 表示该字段的所有值，如一年的所有月份。日可在两种字段中进行指定：月日期和周日期。如果两个日期都被指定，则这两个值都将执行。所有操作系统每个字段内都支持逗号隔离值。例如：

  5,10 0 10 * 1 意思是每个月或每个月 10 号和每个周一的上午 12：05 和 12：10 运行审核。

  有关 crontab 输入格式的详细信息，请参考 Unix 手册页。
- **时间和持续时间**：针对各种类型的计划，指定启动每日计划的小时、分钟、周日期 （和月份）。除非指定结束时间，否则快照规范作业将无限期运行下去。要选择快照规范作业的结束日期，请选择 “结束”，然后选择一个日期。“时区”将根据您的用户配置文件中设置的时区进行设置。
- *（可选）*如果希望快照规范计划无限期地运行下去，则取消选择 “结束”选项。

7 要保存快照规范计划，请从 “文件”菜单中，选择 “保存”。这样快照作业将会根据定义的计划运行。

删除快照作业计划

要删除快照作业计划，请执行以下操作：

1. 在导航窗格中，选择 “作业和会话”。
2. 选择 “重复计划”。
3. 从下拉列表中，选择 “创建快照”。
4. 内容窗格将显示所有在此 SA 核心上运行的快照规范作业。要仅显示快照规范作业，请从内容窗格顶部的下拉列表中，选择 “运行快照”任务。如果要仅查看已计划或运行的快照规范，请在顶部内容窗格的 “用户 ID”字段中输入用户 ID。
5. 要删除计划，请选择并右键单击该计划，然后选择 “删除计划”。

取消活动的快照作业

在 SA 客户端中，可以终止*活动的快照作业*。活动的快照作业是指已经启动且正在运行的作业。

对活动的快照作业的终止操作称为*软取消*。软取消是这样一种活动：作业正在部分运行，然后在您单击 “快照服务器”向导中的 “作业状态”步骤的 “结束作业”时停止。软取消仅适用于要停止的活动的快照作业。

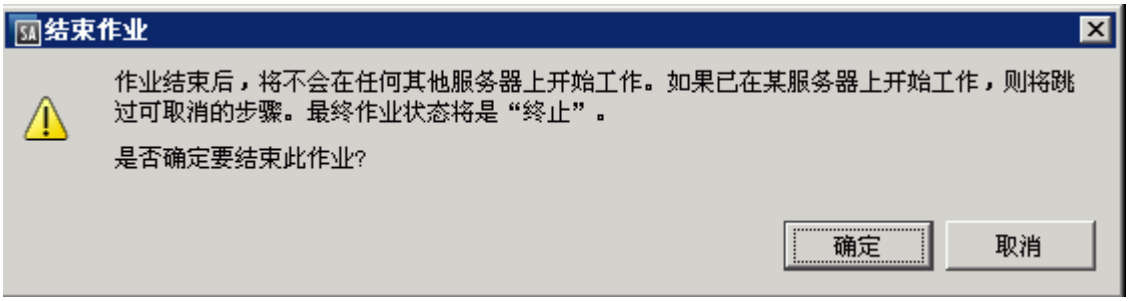
注意：审核、审核结果修正和创建快照作业支持软取消。但是，快照修正作业、包括从快照 “复制到”服务器，不支持软取消。

必须具有取消正在运行的快照的权限。通常情况下，如果有权启动快照作业，也将可以停止正在运行的快照作业。另外，如果具有 “编辑或取消任何作业”权限，也将可以软取消正在运行的快照作业。有关与审核相关的权限的详细信息，请参见 《SA 管理指南》。您还可以从 SA 管理员处获取这些权限。

要停止活动的快照作业，请执行以下操作：

1. 在 “作业状态”窗格中，单击 “结束作业”。

   此按钮仅在作业正在运行时可用。
2. 此时将显示 “结束作业”对话框。此对话框简短地描述了作业是如何终止的：
   - 作业将不会在任何其他服务器上启动作业。
   - 如果作业已在某服务器上运行，则该作业将取消所有可跳过的步骤。
   - “作业状态”将指示这些步骤是已完成还是已跳过。
3. 如果作业成功结束，则最终作业状态将显示为 “已终止”。



4 单击 “确定”确认要终止该作业。“作业状态”窗格将显示终止操作过程的进度。

作业状态将为 “已终止”。服务器状态将为 “已取消”。任务状态将为 “成功”或 “已跳过”。

5 当终止完成后，您还可以在 SA 客户端的 “作业日志”中查看作业。

在 SA 客户端导航窗格中，选择 “作业和会话”。“作业日志”视图将显示处于 “已终止”状态的作业。

4 SA 客户端中的符合性

概述

在 SA 客户端中，“符合性”视图可支持您查看设施中所有服务器和服务器组的整体符合性级别。从此视图（通常称为*符合性图表板*）中，您可以修正*不符合要求*的服务器。可以查看单个服务器、多个服务器、服务器组或受 SA 管理的所有服务器的符合性。

符合性图表板显示了针对审核、审核策略、软件策略、修补程序策略和应用程序配置的服务器或服务器组的所有符合性状态的结果。服务器的符合性状态基于*符合性策略*。符合性策略可定义唯一的服务器配置设置或值，用于确保将 IT 环境配置为所需的环境。

符合性策略通常由*策略设置员*创建和定义。在某些环境中，可能需要系统管理员创建临时的策略。策略设置员创建符合性策略，然后将其附加到服务器，以确保服务器符合组织的标准和策略。例如，策略设置员可以创建软件策略，用于定义服务器上必须安装的修补程序和程序包标准集。策略设置员还可定义必须采用何种方式在服务器上配置某些应用程序文件。如果服务器或服务器组的配置与策略设置员在符合性策略中定义的规则匹配，则会将它们视为*符合要求*。

通过符合性图表板，您可以确定服务器实际安装的软件、程序包、修补程序和配置文件设置是否与*软件策略*中定义的配置相匹配。“符合性”视图允许您查看服务器组的符合性，它显示了组的所有成员及子组成员的符合性状态汇总。在“符合性”视图中，可以发现*不符合要求*的服务器和服务器组，然后修正任何问题。请参见图 26 和图 30。

图 26　符合性视图 — 托管服务器

符合性图表板中显示的信息是 SA 客户端从核心请求的最新符合性信息。默认情况下，SA 客户端每 5 分钟检查是否有新的符合性信息。

有关如何更改此时间间隔的信息，请参见设置自动符合性检查频率 （第 141 页）。

按 **F5** 可以立即获取最新符合性信息，而不用等待经过默认设置的时间 （5 分钟）。

最佳实践：定期查看符合性图表板，以访问服务器符合性级别和执行任何必要操作解决问题。例如，使用 “符合性” 视图确定单独计划的审核的状态，这将确保诸如 Apache http.conf 文件的 Web 应用程序的配置符合组织设定的标准。希望确保没有人更改应用程序的配置。要验证是否没有进行不需要的更改，应定期检查此服务器 “设备资源管理器” 的 “符合性” 视图，查看此计划审核的符合性状态是否已更改为 “不符合”。如果状态已更改为 “不符合”，则查看审核结果并修正此问题。

最佳实践：使用符合性图表板有助于回答特定疑问或诊断特定问题。例如，创建一个计划审核，定义设施中服务器组的安全标准。此审核示例要求所有 Windows Server 2003 服务器均包含某个安全修补程序。当 Microsoft 发布新的安全修补程序时，需要标识含有和不含有新的修补程序的 Windows Server 2003 服务器。更新审核以包含新的安全修补程序，然后在设备组的 “符合性” 视图中浏览 Windows Server 2003 服务器。重新运行审核以查找需要此修补程序的服务器，然后通过安装新的必需安全修补程序对其进行修正。

术语

以下列表定义了 HP Server Automation 服务器符合性中使用的重要术语和概念：

- **符合性**：服务器配置对某检查或测试的符合程度。该检查或测试在审核、快照规范或审核策略中定义的规则集中创建。审核和修正中的符合性由指定目标服务器期望值的审核规则或快照规则定义。如果目标服务器上的值与审核规则中指定的值不同，则该服务器认定为 “不符合”。
- **符合性类别**：“符合性”视图显示以下符合性类别的符合性状态：审核、审核策略、软件、修补程序、修补程序策略和配置 （应用程序配置）。
- **符合性策略**：用户定义的配置，表达了服务器或设备配置或设置的所需状态。

  示例：

  修补程序策略 定义必须安装在计算机上的特定修补程序。

  审核策略 可定义必须始终禁用特定 Windows 服务。

  应用程序配置策略 定义对配置文件进行配置时必须使用的方式。
- **符合性规则**：定义服务器理想配置的策略内容或设置，如修补程序或程序包、文件配置、软件安装顺序、用户和组成员资格和权限等。
- **符合性状态**：指示符合性类别的符合性状态，报告期望内容 （符合性策略）和实际内容 （服务器配置）之间的差异。例如，如果策略中定义的所有配置均符合服务器配置，则 “符合性”视图中的软件符合性类别将显示状态 “符合”。组的符合性计算与单个服务器的计算稍有不同。
- **符合性扫描结果**：符合性扫描的结果。这些结果报告了符合性状态、详细信息，也可以包含修正选项。
- **符合性扫描**：检查符合性策略 （审核、软件、修补程序和应用程序配置）的目标服务器并将结果返回到 SA 客户端的机制。符合性扫描可以进行检查，以查看修补程序策略或软件策略的目标计算机上所安装的修补程序，并返回结果，或可以检查配置文件的内容，并确定该内容是否与应用程序配置中定义的规则相匹配。在“符合性”视图中，可以执行“软件”、“修补程序”和“配置”符合性类别的符合性扫描。审核不具有扫描功能；但是运行审核将实现相同的结果。运行审核可检查审核的目标服务器，以确定这些服务器是否与审核的规则定义相符合。
- **符合性视图**：显示设施中所有托管服务器或服务器组的总体和单个符合性级别。该视图也称为 *符合性图表板*。

符合性类别

服务器或服务器组的 “符合性”视图显示以下类别的符合性：

- **审核**：审核符合性代表所有按重复计划运行的审核的聚合，并表示计划审核中定义的规则是否符合目标服务器上安装和配置的内容。
- **审核策略**：审核策略通过审核与托管服务器关联。审核链接到符合性规则的审核策略，并定义要进行规则验证的多个服务器的列表。审核还可选择定义重复计划。审核策略可包含其他审核策略。
- **软件**：软件符合性由软件策略定义是否与服务器上安装的内容匹配来确定。软件策略定义修补程序、程序包、应用程序配置和脚本，包括其他服务器对象（如服务、Windows 注册表、COM+、IIS 元数据库等）的主机。软件策略也可以包含其他软件策略。有关详细信息，请参见 《SA 用户指南：软件管理》。
- **修补程序**：修补程序符合性由修补程序策略定义是否与服务器或服务器组上安装的修补程序匹配来确定。“符合性”视图仅显示 Windows 修补程序的符合性信息。有关详细信息，请参见《SA 用户指南：服务器修补程序》。
- **修补程序策略**：修补程序策略定义必须安装在计算机上的特定修补程序。
- **配置**：配置符合性由应用程序配置定义是否与服务器或服务器组上的配置匹配来确定。应用程序配置定义了应用程序配置文件的配置设置和值。配置符合性状态始终是附加到服务器的所有应用程序配置的聚合。不支持单个状态。有关详细信息，请参见 《SA 用户指南：应用程序配置》。另请参见以下小节：

符合性状态

通常情况下，服务器或服务器组可能为*符合*或*不符合*。此信息将在 “符合性”视图中显示。

符合 ：“符合性”视图在服务器符合附加到其的策略时显示此图标。如果策略中定义的规则与该策略附加到的服务器上的实际配置相匹配，则认定该服务器 “符合”。

不符合 ：“符合性”视图在服务器实际配置与策略中配置的规则不匹配时显示此图标。例如，可配置审核来确保 Windows Server 2003 服务器具有 Windows CIS 建议的最小密码长度，即至少 8 个字符。如果在运行该审核以检查服务器用户密码时发现用户密码仅具有 4 个字符，“符合性”视图会将此服务器的审核策略显示为 “不符合”。

最佳实践: 不要将*不符合的规则*与*对象差异*混淆。不符合的规则可显示多个对象差异。SA 会对不符合的规则进行计数，而不会对对象差异进行计数。例如，如果某个目录规则包括该目录中的许多文件（对象），而审核发现其中某些对象不同，SA 会将其计为一个差异。SA 不会将其计为*多个*差异。在 SA 客户端中，“审核结果”浏览器中的 “符合性”视图和摘要视图显示不符合的规则计数。这些视图不显示对象差异的计数。

当多个策略附加到服务器时，聚合列会组合 （汇总）所有策略的状态。如果此服务器属于多个服务器的设备组，则可以访问此组的“符合性”视图，以查看在此组的所有服务器 （包括任何子组中的服务器）上运行的所有审核的符合性状态级别。用于确定组的符合性状态的方法基于默认计算。如果该组中至少 95% 的服务器具有 “符合”状态，则认定该组服务器为 “符合” 。如果少于 95% 的服务器具有 “符合”状态，则该组的状态显示为 “部分符合”。

可以自定义服务器组的默认符合性状态阈值。请参见第 128 页的更改设备组的符合性设置。

实际服务器配置 （包括策略信息）可能会自上次查看 “符合性”视图中的服务器或服务器组的符合性后发生了更改。要从 SA 核心获取最新的符合性数据，请从 “视图”菜单中选择 “刷新”或按 “F5”。也可以通过在服务器或服务器组上运行符合性扫描来确定最新的符合性状态。

符合性状态定义

表 3 列出了策略、服务器和设备组的默认符合性状态。

表 3　　符合性状态图标

图标	符合性状态描述
	**符合** • **策略**：策略中定义的所有规则或项均与实际服务器配置相匹配。 • **服务器**：符合性扫描成功运行，且服务器配置与附加到该服务器的*所有* 策略中定义的*所有* 规则均匹配。 • **设备组**：符合性扫描成功运行，且符合的服务器的百分比大于在 “管理” 窗格的 “符合性设置” 选项中设置的最小阈值。默认情况下，“符合性” 状态的阈值是组中服务器的 95%。可以对 “符合” 的符合阈值定义进行修改。
	**部分符合性** • **策略**：由于向其中一个规则应用了异常，因此策略中定义的一个或多个规则或项与实际服务器配置不匹配。*仅适用于 Windows 修补程序策略。* • **服务器**：符合性扫描成功运行，且由于向其中一个规则应用了异常，服务器配置与附加到该服务器的任何策略中定义的至少一个规则不匹配。*仅适用于 Windows 修补程序策略。* • **设备组**：符合性扫描成功运行，且该组中有足够服务器满足在 “管理” 窗格的 “符合性设置” 中设置的 “不符合” 阈值条件，而组中剩余的服务器均为 “符合”。可以对 “部分符合性” 的符合阈值定义进行修改。
	**不符合** • **策略**：策略中定义的一个或多个规则或项与实际服务器配置不匹配。 • **服务器**：符合性扫描已运行，且实际服务器配置与该策略中定义的至少一个或多个规则不匹配。 • **设备组**：符合性扫描已运行，且该组中有足够服务器满足在 “管理” 窗格 “符合性设置” 选项中设置的 “不符合” 阈值条件。可以对 “不符合” 的符合阈值定义进行修改。
	**扫描失败** 符合性扫描无法运行。
	**已跳过** 已跳过的服务器。

表 3　　符合性状态图标 （续）

图标	符合性状态描述
	**需要扫描** 未定义结果。如果符合性扫描从未运行 （如新安装后）或服务器 （或设备组中的服务器）上的配置自上次向 SA 客户端报告信息后已更改，则会产生此种状态。
	**正在扫描**：当前正在运行符合性扫描。
—	**没有定义测试** 没有此种符合性策略附加到服务器或设备组中的所有服务器 （包括任何子组中的所有服务器）。

符合性状态阈值 — 策略、服务器和多个服务器

策略：策略的符合性状态基于该策略中的所有规则。如果策略中的某个规则为 “不符合”（不匹配托管服务器上的实际配置），则认定整个策略对服务器 “不符合”。

服务器和多个服务器：服务器的符合性状态基于附加到服务器的所有策略或将服务器定位为目标的所有策略。如果其中任一个符合性类别的符合性状态为 “不符合”，则服务器的整体符合性状态也将认定为 “不符合”。所有符合性类别中的所有策略都必须为 “符合”，服务器的整体符合性状态才会是 “符合”。

符合性状态阈值 — 设备组

当在 “符合性”视图中查看设备组符合性时，服务器是 “符合”还是 “不符合”非常重要。此状态基于可以配置和自定义的默认阈值计算。

不符合：在设备组的 “符合性”视图中，要让符合性类别 （审核、审核策略、软件、修补程序或配置）显示 “不符合”状态，*则对于此类别，组中必须有大于 5% 的服务器具有 “不符合”状态*。或者，也可以将设备组的 “不符合”理解为，*当组中有小于 95% 的服务器符合要求时*，将显示 “不符合”状态。

部分符合：在设备组的 “符合性”视图中，要让符合性类别 （审核、审核策略、软件、修补程序或配置）显示 “部分符合”状态，*则对于此类别，组中必须有大于 2% 且小于等于 5% 的服务器具有 “不符合”状态*。或者，也可以将设备组的 “部分符合”理解为，*当组中有小于 98% 且大于等于 95% 的服务器符合要求时*，将显示 “部分符合”状态。

符合：在设备组的 “符合性”视图中，要让符合性类别 （审核、软件、修补程序或配置）显示 “符合”状态，*则对于此类别，组中必须有小于 2% 的服务器具有 “不符合”状态*。或者，也可以将设备组的 “符合”理解为，*组中有至少有 98% 的服务器符合要求*。

根据附加到属于该组的所有服务器上的所有策略 （在所有符合性类别中）计算设备组状态。也包括所有子组 （即选定组的子级）中的服务器。

可更改用于计算符合性状态的默认阈值。例如，可将组的符合性状态配置为不递归计算，此类计算将从符合性计算中排除所有子组服务器成员。

更改设备组的符合性设置

默认情况下，使用 SA 客户端可配置确定设备组符合性的方式。

为了更改设备组符合性设置，您必须是分配有 SA 功能 “模型 :Opsware”权限的某个组的成员。有关已授予的权限类型的详细信息，请与 SA 管理员联系。

要更改设备组符合性设置，请执行以下操作：

1. 在导航窗格，选择 “管理” > “符合性设置”。
2. 在 “符合性设置”窗格的 “设备组符合性”部分中，单击 “编辑设置”。
3. 在 “设备组符合性设置”窗口中，配置以下设置：
   - **显示设备组汇总符合性**：此选项用于显示或隐藏每个符合性类别列顶部显示的图标，该图标指示父组的符合性状态。此图标指示选定组所有成员的符合性状态汇总。

     例如，如果选择此选项，则当您选择某个组，然后从 “视图”下拉列表中选择 “符合性”时，每个符合性类别列 （审核、软件、修补程序和配置）的顶部列标头会显示一个图标，指示选定组中所有服务器的符合性状态。将指针停放在此列标头上，即可查看此类别中所有设备的符合性状态。
   - **成员计算**：此选项用于选择在计算符合性类别的整体组符合性级别时是否包括子组的服务器。例如：
     - **考虑服务器和组成员**：这表示设备组的符合性状态将递归检查组中所有服务器和选定设备组所有子组中的所有服务器的符合性。
     - **仅考虑服务器成员**：这意味着选定设备组的符合性状态将只检查该组顶层服务器的符合性，不会包括任何子组成员的任何服务器。
   - **阈值**：允许您更改用于为所有符合性类别确定设备组符合性状态的符合阈值计算百分比 (%)。

     默认情况下，设备组将显示以下状态：

     不符合 — 如果组中大于 5% 的成员 “不符合”。

     部分符合 — 如果组中大于 2% 且小于等于 5% 的成员 “不符合”。

     符合 — 如果组中小于等于 2% 的成员 “不符合”。
   - **列类型**：用于更改可以发现并显示的符合性类别，如审核、审核策略、软件、修补程序和配置。
4. 单击 “确定”保存设置。

符合性图表板

在 SA 客户端中，可查看单个服务器、多个服务器或这两种类型服务器的符合性：

- 查看单个服务器的符合性
- 查看多个服务器的符合性
- 查看组符合性

查看多个服务器的符合性状态时，组中可能会存在该用户不具备查看权限的服务器。此外，用户帐户还可能不具备用于计算一组服务器的符合性状态的一些策略（审核、软件和修补程序）的查看权限。

在这些情况下，尽管不能查看某些服务器和策略，但仍可以查看用户有权查看的多个服务器的整体符合性状态。虽然有些策略可能已从视图中隐藏，但仍可以查看符合性类别汇总。

查看单个服务器的符合性

要查看单个服务器的符合性信息，请执行以下操作：

1. 在导航窗格中，选择 “设备” > “所有托管服务器”或 “虚拟服务器”。
2. 在内容窗格中选择一个服务器。
3. 右键单击并选择 “打开”，以显示 “服务器”浏览器。
4. 在 “信息”窗格中，选择 “管理策略”。
5. 在 “管理策略”窗格中，选择 “符合性”。

   内容窗格显示了每个符合性类别符合性状态的符合性摘要饼图，包括单个策略的详细状态信息。请参见图 27。
6. 要对其中一个符合性类别或类别中的单个策略执行操作，则在详细信息列表进行选择，然后单击 “运行审核”（仅适用于审核）、“修正”或 “扫描设备”。

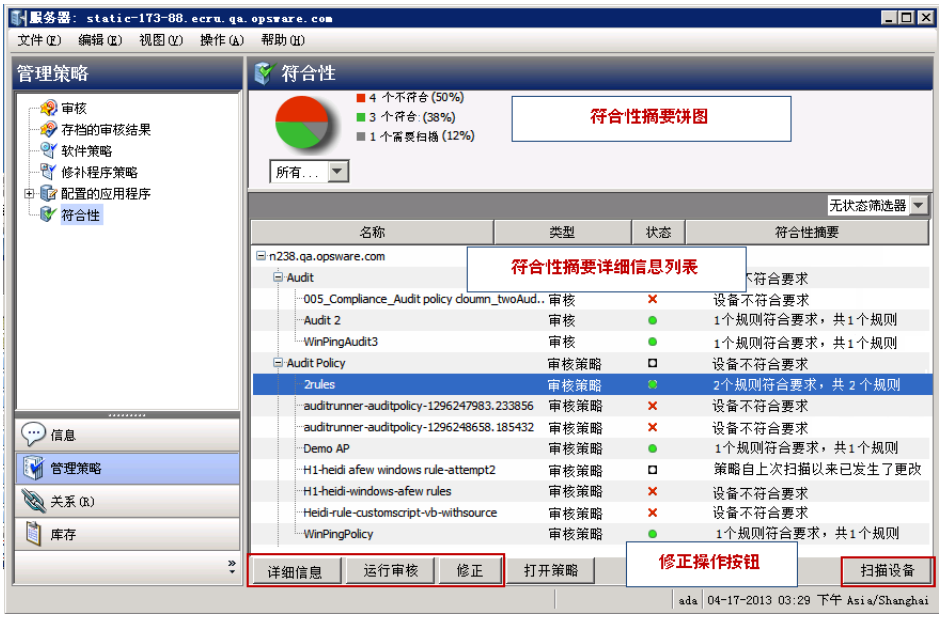
是否可以查看策略和对其执行修正操作取决于用户权限。如果无法查看策略或对其执行操作，则请与 SA 管理员联系。

符合性摘要饼图和详细信息

“符合性”视图包含以下主要部分：

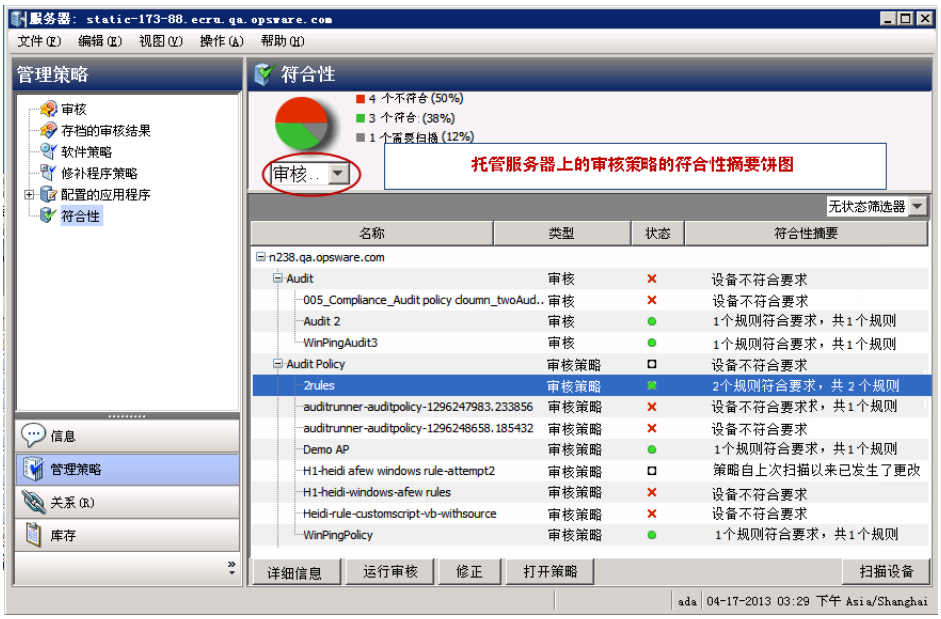
- *符合性摘要饼图* 以图形方式显示了附加到选定服务器上的所有策略的整体符合性状态。还可以对饼图进行筛选，仅显示特定符合性类别的状态。请参见图 27。
- *符合性摘要详细信息列表* 用于向下搜索每个符合性类别以查看整体符合性状态、每个类别中包含的策略、每个策略的符合性状态以及每个类别的摘要描述。根据选择，可启动操作以修正不符合要求的策略，如查看策略的详细信息、运行审核或扫描设备的符合性。请参见图 27。

图 27　　托管服务器的符合性摘要 — 所有策略



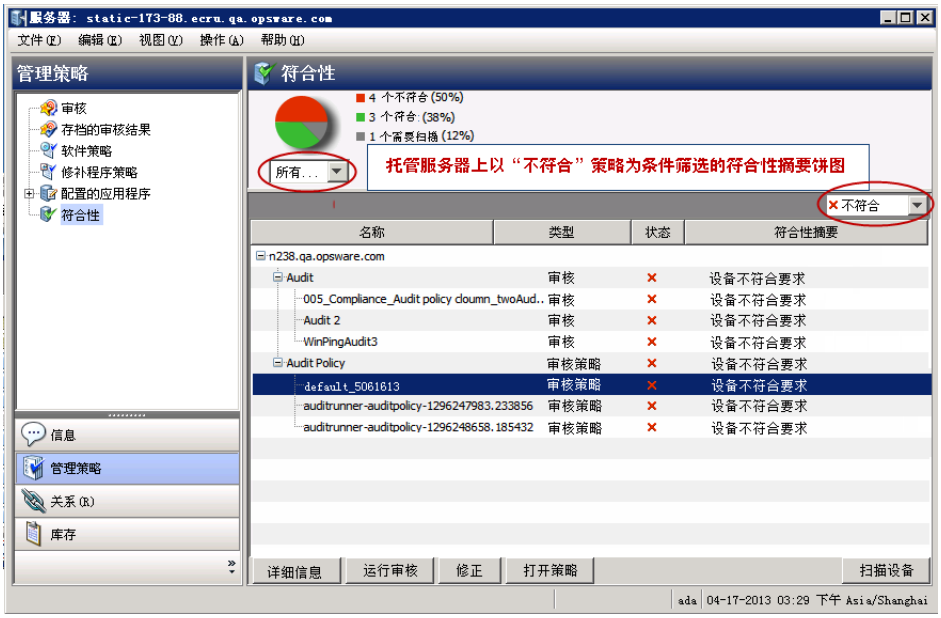
选择饼图下方的下拉列表，查看已按照每个符合性测试类别 （如审核策略）筛选过的饼图。请参见图 28。

图 28　　托管服务器的符合性摘要 — 审核策略



还可选择在饼图下方的详细信息窗格中筛选符合性策略详细信息，查看所有包含特定符合性状态的符合性策略。例如，在图 29 中，符合性视图经筛选后仅显示所有不符合的符合性策略。

图 29　　按不符合筛选的符合性摘要



在上一个示例中，“符合性”视图详细信息窗格显示了附加到服务器的所有 “不符合”策略。如果在策略中至少有一条配置的规则与服务器配置不匹配，则认定该策略为 “不符合”。

查看多个服务器的符合性

要查看多个服务器的符合性信息，请执行以下操作：

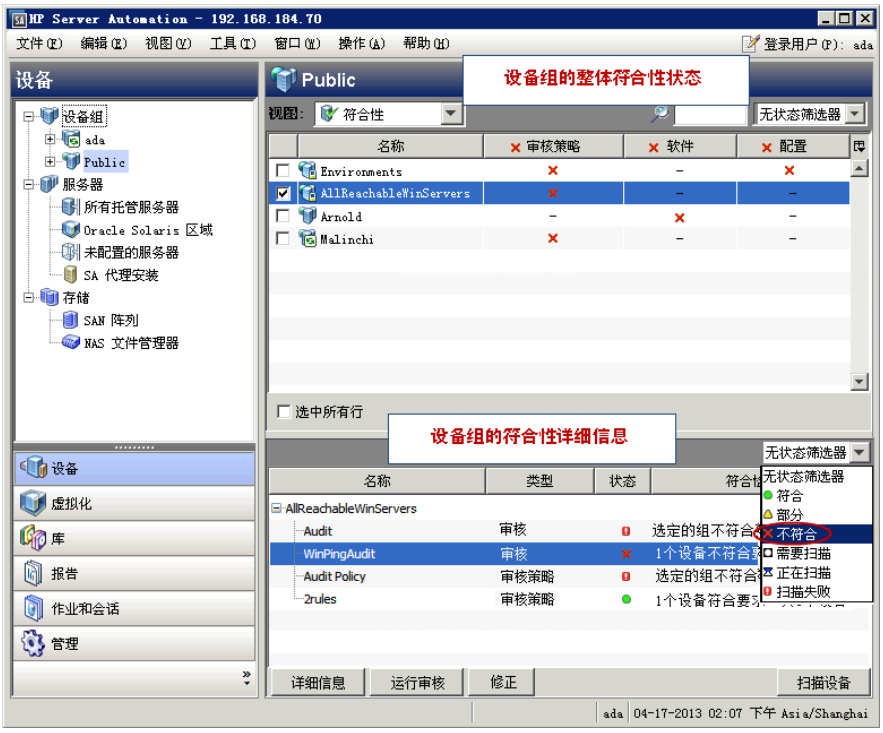
1 在导航窗格中，选择 “设备” > “设备组”。

2 在 “设备组”树中，选择 “Public”或选择自己的用户组列表。内容窗格将显示此列表中所有设备组的内容，所有公用组或所有用户创建的组。

3 从 “视图”下拉列表中，选择 “符合性”。

4 对于一个或多个设备组或列表中的任何服务器，选择其旁边的复选框，将其包含在 “符合性”视图详细信息窗格中。图 30 中的详细信息窗格显示选定组中所有服务器的符合性信息。

图 30 符合性视图 — 设备组



5 （*可选*）使用状态筛选器下拉列表按符合性状态筛选该视图。例如，可以选择仅查看具有 “不符合” ✘ 状态的设备组。

6 （*可选*）在详细信息窗格中，选择其中一个类别。根据类别和用户权限，单击窗格底部的某个操作按钮可获取详细信息，从而运行审核、修正软件策略或修补程序策略，或在所有组成员上运行符合性扫描。

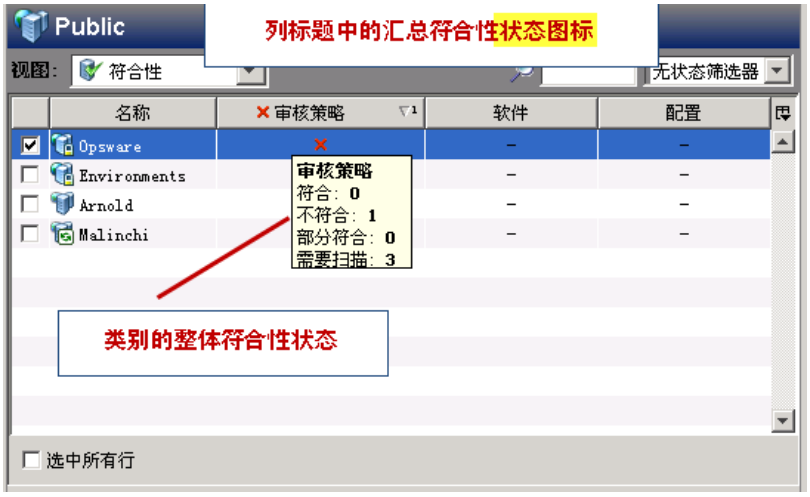
设备组符合性：状态汇总

设备组内容窗格显示在导航窗格（“设备” > “设备组”）选定的所有组成员和组内容的符合性状态汇总摘要。

列表顶部列标头中的符合性状态（符合、不符合、部分符合等）图标指示列表中所有组的汇总状态。要查看所有可见组的符合性类别的整体状态，可将指针停放在类别的列标头上。

在列表的每行中，此视图为列中的每个组显示所有符合性类别中每个组的符合性状态。这些类别包括审核、审核策略、软件、修补程序和配置，包括选择在此视图中显示的任何单独计划的审核。在图 31 中，每个符合性类别都显示了附加到该组服务器的每个类别的所有策略的符合性状态。

图 31　设备组的符合性汇总



设备组符合性：聚合汇总

当在内容窗格中选择一个或多个组 （或全部组）时，详细信息窗格将在内容窗格的每列中显示所有组成员的设备符合性聚合汇总。请参见图 32。

图 32　设备组的符合性聚合汇总

使用状态筛选器下拉列表按符合性状态筛选该视图。例如，可以选择仅查看具有 “不符合” ✖ 状态的设备组。

根据类别和用户权限，单击操作按钮可获取更多详细信息，从而运行审核、修正软件策略或修补程序策略，或在所有组成员上运行符合性扫描。

查看组符合性

在组资源管理器中，“符合性”视图针对作为整体的所有组成员的每个策略类型，显示了其符合性策略聚合的汇总，与单个服务器的符合性状态相反。这样，可以了解该组是否与每种策略类型以及组 （和任何子组）中的所有服务器相符合。

使用状态筛选器下拉列表按符合性状态筛选该视图。例如，可以选择仅查看具有 “不符合” ✖ 状态的设备组。

根据类别和用户权限，单击操作按钮可获取更多详细信息，从而运行审核、修正软件策略或修补程序策略，或在所有组成员上运行符合性扫描。

要在 “设备组资源管理器” 中查看服务器组，请执行以下操作：

1. 在导航窗格中，选择 “设备” > “设备组”。
2. 在 “设备组” 树中，选择 “Public” 或选择自己的用户组列表。内容窗格将显示此列表中所有设备组的内容，所有公用组或所有用户创建的组。
3. 选择一组服务器。
4. 右键单击并选择 “打开”。
5. 在组资源管理器的 “视图” 窗格中，选择 “符合性” 。“符合性” 视图显示组中所有服务器的摘要和汇总符合性状态信息。请参见图 33。

图 33　　组符合性视图

符合性摘要饼图以图形方式显示了组中所有关联服务器的所有策略聚合的整体符合性状态。饼图中的各部分按类别 （如符合、不符合、需要扫描、扫描失败等）显示符合性状态和每个状态级别的百分比。还可以对饼图进行筛选，仅显示特定符合性类别的状态。

详细信息窗格按符合性类别显示设备符合性聚合汇总。

根据类别和用户权限，单击操作按钮可获取更多详细信息，从而运行审核、修正软件策略或修补程序策略，或在所有组成员上运行符合性扫描。

添加和删除符合性视图列

在“符合性”视图中查看设备组时，默认情况下，以下符合性类别将在内容窗格中显示为列：审核、审核策略、软件、修补程序和配置。可显示或隐藏其中的任何类别、添加或删除每个类别中的单个策略。

要在 “符合性”视图中添加或删除设备组符合性类别，请执行以下操作：

1 在导航窗格中，选择 “设备” > “设备组”。

2 在 “设备组”中，展开设备组的列表或设备组的 “Public”列表。

3 在内容窗格中选择一个设备组。

4 在 “视图”下拉列表中，选择 “符合性”。

内容窗格将列出以下符合性类别：审核、审核策略、软件、修补程序和配置。内容窗格也指示设备组的每个成员的状态。

5 使用列选择器  可添加或删除类别。

6 在 “选择符合性视图列”窗口中，窗口左侧显示了每个符合性类别的选项卡，以及有权查看的类别中的所有符合性策略的选项卡。窗口右侧显了示在 “符合性”视图的每个类别中当前可见的策略。默认情况下，“符合性”视图显示类别中所有策略的聚合 （汇总）。

7 要在“符合性”视图中将单个策略添加为列，则在左侧选择符合性类别选项卡，然后选择策略，再单击加号 (+) 箭头按钮。

8 要从 “符合性”视图中删除单个策略或聚合列，在窗口右侧选择一个策略或聚合列，然后单击减号 (-) 箭头按钮。

9 单击 “确定”保存更改。

对符合性类别显示排序

最佳实践：升序或降序排列符合性类别对于自定义 “符合性”视图显示要求非常有用。

要在 “符合性”视图中对列进行排序，请执行以下操作：

1 在 “符合性”视图中，单击列标头内部。

数字 “1”将作为上标显示在符合性类别名称旁。这是此表的主要排序键。

2 单击标头内的向上或向下箭头，指示数据是按升序还是降序排列。

3 按 “Ctrl”键，然后在其他列标头内单击。

数字 “2”将作为上标显示在符合性类别名称旁。这是此表的次要排序键。

4 （*可选*）必要时重复步骤 3.

5 （*可选*）将光标停放在列表头可显示特定类别的符合性状态汇总。

6 要重置排序键，可在未注释的列表头上单击。

按符合性状态筛选

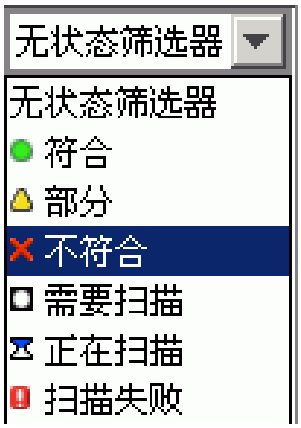
当在 “符合性”视图中查看单个托管服务器和服务器组的符合性时，可筛选视图，仅显示至少含有一个服务器与显示的任何符合性类别的特定符合性状态匹配的组和服务器。例如，当选择一个组，然后选择 “符合性”视图时，可使用状态筛选器仅显示符合以下条件的选定组成员（单个服务器和任何子组中的服务器）：每个符合性类别 （如审核、审核策略、修补程序、软件等）都具有 “不符合”状态。

要通过符合性状态筛选 “符合性”视图，请执行以下操作：

1. 在导航窗格中，选择 “设备” > “设备组”。
2. 在 “设备组”树中，导航并选择 “Public”或选择自己的用户组列表。
3. 在 “Public”窗格中，选择一个设备组。

   内容窗格显示选定组中所有成员的 “符合性”视图状态。
4. 要通过符合性状态筛选此视图，请从下拉列表中选择一个状态筛选器。请参见图 34。

图 34　　符合性状态筛选器



5. “符合性”视图仅显示状态为 “不符合” ✖ 的组中的成员（单个服务器和任何子组中的服务器）。
6. 选择组中所列的任何服务器或子组。

   详细信息窗格显示了这些服务器的符合性状态信息。可通过使用详细信息窗格中的状态筛选器筛选此窗格中的信息。

刷新符合性信息

最佳实践：刷新 “符合性”视图可用于确保当前查看的是核心中的最新符合性信息。要从核心获取最新的符合性信息，请从 “视图”菜单中，选择 “刷新”或按 “F5”。

当首次选择 “符合性”视图，显示的信息为 SA 核心为每个符合性类别报告的最新信息。服务器配置可能自您上次查看 “符合性”视图后已更改。策略也可能自您上次在 “符合性”视图中查看服务器和组后已更改。如果是这种情况，则可能要通过扫描符合性或重新运行审核生成新的 “符合性”视图显示数据。

设置自动符合性检查频率

默认情况下，SA 客户端每 5 分钟检查核心是否有新的或更改的符合性信息。可使用设置选项窗口更改此时间间隔。

如果希望 SA 客户端立即检查核心中的新符合性信息，则按 “F5”。

要更改自动符合性检查频率的设置，请执行以下操作：

1. 在 SA 客户端的 “工具”菜单中，选择 “选项”。
2. 在设置选项窗口的 “视图”窗格中，选择 “常规”。
3. 在 “缓存”部分的 “每隔 <xx> 分钟检查更新”字段中，输入时间间隔，即希望 SA 客户端检查核心以获取新符合性信息的频率。

   此检查适用于 SA 客户端可从核心访问的所有信息，而不仅是符合性信息。如果时间间隔较长，则会增大显示过时信息的可能性。如果时间间隔较短，则会增大核心的网络流量，这意味着您将查看到更新的信息。
4. （*可选*）单击 “更新缓存”可立即从核心检查新信息。
5. （*可选*）单击 “重新加载缓存”可立即重新加载 （刷新）缓存。
6. 单击 “保存”。

导出符合性视图信息

如果要以文件形式查看 “符合性”视图中显示的所有信息，可将此视图导出到 html 或 .csv。

要将 “符合性”视图信息导出到文件，请执行以下操作：

1. 在导航窗格中，选择 “设备” > “设备组”。
2. 选择要查看其符合性的组，然后从 “视图”菜单中，选择 “符合性”。
3. 在内容窗格中，选择组中的一个服务器。

4 右键单击并选择 “导出到”，然后选择 CSV 或 HTML。

5 在 “导出符合性视图” 窗口中：

a 输入文件的名称。

b （*可选*）如果希望所保存的文件使用特定的编码方案，则可更改编码。

c 单击 “保存”。

注意：要正确地查看符合性结果，请用文本编辑器打开 .csv 文件，关闭自动换行，然后水平地展开文本窗口。

符合性图表板修正

除了提供服务器和组的符合性状态信息，通过 “符合性” 视图，还可以修正不符合组织标准的服务器配置，这种修正可由审核、软件、修补程序和应用程序配置符合性策略定义。

通过定义，修正服务器或服务器组的操作意味着查找服务器或服务器组不符合要求 （不符合）的方式和位置，然后确保服务器的实际配置符合符合性策略。

从服务器或服务器组的 “符合性” 视图，可执行以下操作：

- 修正修补程序策略或软件策略。
- 运行、查看和修正审核结果。
- 将应用程序配置推送到服务器。
- 运行修补程序、软件或应用程序配置的符合性扫描，获取服务器的最新符合性信息。

当在 “符合性” 视图中选择服务器或服务器组，或在设备或设备组资源管理器中查看时，详细信息窗格为有助于发现和修正不符合要求策略的操作提供了操作按钮。可用的操作类型取决于策略的类型、选择的是单个托管服务器还是服务器组，以及是否在详细信息窗格中选择了单个策略、多个策略或符合性类别汇总。

符合性视图修正 — 服务器组

图 35 显示了 “符合性” 视图是如何启用服务器组的修正操作的。

图 35　　服务器组的修正

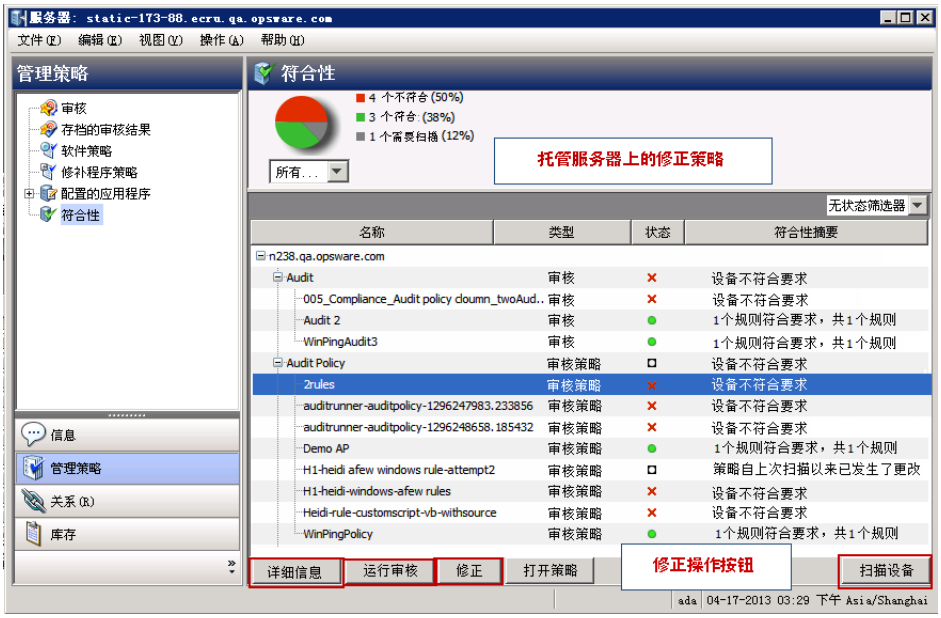
选定组的详细信息窗格显示了附加到组中所有服务器 （以及子组中的所有服务器）的所有策略的摘要，这些服务器按符合性类别 （审核、审核策略、软件、修补程序和配置）排列。选择组时，可仅修正某个类别的所有策略，如附加到不符合要求的组中所有服务器的所有软件策略或所有修补程序策略。如果在详细信息窗格中选择 “软件” 类别，则会启用 “修正” 按钮。单击 “修正” 时， SA 客户端将启动修正向导。完成向导中的步骤可修正组中所有服务器的任何不符合要求的策略配置。

通过选择组并从 “操作” 菜单中选择 “打开”，可查看相同信息和访问这些选项。此操作将启动组资源管理器，并显示相同的组详细信息窗格和详细信息窗格中的操作按钮。

符合性视图修正 — 服务器

图 36 显示了 “符合性” 视图如何启用单个服务器的修正操作。

图 36　　单个服务器的修正



对于服务器组，修正操作始终适用于组中的所有成员。对于单个托管服务器，可以修正附加到服务器的所有策略或选定策略。例如可启动一个服务器，然后从该服务器的设备资源管理器，选择 “管理策略” > “符合性” 查看附加到该服务器的所有符合性策略。

在详细信息窗格中，选择审核或软件策略来查看该审核。使用操作按钮运行审核，修正软件策略或扫描设备的符合性。

符合性扫描

在 “符合性” 视图中，可以执行 “审核”、“审核策略”、“软件”、“修补程序” 或 “配置” 符合性类别的符合性扫描。扫描符合性时，通过扫描符合性策略的目标服务器，确定目标服务器配置是否与策略规则定义匹配。例如，符合性扫描可查看计算机上安装的修补程序，并将其与修补程序或软件策略相比较，然后将结果返回到 “符合性” 视图中。或者，符合性扫描可检查服务器上的配置文件内容，以确定配置文件是否与应用程序配置中定义的规则相匹配。

审核不具有扫描功能；但是运行审核将产生相同的结果。对于审核，当运行审核时，SA 通过检查目标服务器配置确定其与审核规则定义匹配的程度。

扫描符合性类别时会产生以下操作：

- **软件符合性扫描**：比较服务器上的文件，确定这些文件是否与存储在附加到该服务器的软件策略中的文件匹配。

- **修补程序符合性扫描**：将安装在服务器上的修补程序与附加到该服务器的修补程序策略和修补程序策略异常相比较。此扫描的结果将显示符合要求 （已安装所有必要的修补程序）的服务器和不符合要求（未安装所有必要的修补程序）的服务器。扫描修补程序符合性仅适用于 Windows 修补程序管理。
- **配置符合性扫描**：将服务器上的配置文件与附加到该服务器的模板定义的应用程序配置相比较。此扫描的结果将显示符合要求 （配置文件定义与配置模板匹配）的服务器和不符合要求 （配置文件定义与配置模板不匹配）的服务器。请参见有关配置符合性的详细信息。

修补程序符合性

在 HP Server Automation 中，使用修补程序管理可在托管服务器和服务器组上识别、安装和删除修补程序。使用 Windows 修补程序管理，可识别和安装 Windows Server 2000 SP 4、 Windows Server 2003 和 Windows Server 2008 和操作系统的修补程序，包括 Service Pack、更新汇总和修复程序。

在 “符合性”视图中，可通过查看修补程序策略的符合性状态查看服务器是否已安装正确的修补程序。在修补程序符合性扫描期间， HP Server Automation 会检查托管服务器和公用设备组，确定是否已成功安装策略和策略异常中的所有修补程序。如果服务器上已安装 （或未安装）的修补程序与修补程序策略定义不匹配，则此服务器修补程序策略将在 “符合性”视图中显示为 “不符合” ✖ 。

符合性扫描可一次性运行，也可按计划重复运行。可修正服务器的修补程序策略以确保服务器或服务器组的修补程序符合要求。

有关详细信息，请参见 《SA 用户指南：服务器修补程序》。

修补程序符合性状态条件

修补程序符合性状态由以下条件决定：

- **修补程序符合性 — 单个服务器**：如果修补程序策略中至少有一个项与在该策略所附加的服务器上找到的内容不匹配，则该服务器的修补程序符合性状态为 “不符合” ✖ 。服务器的设备资源管理器窗口的详细信息窗格将显示 “修补程序”类别为 “不符合”，并且摘要列将指示全部规则中 “不符合”的规则 （修补程序策略项）数。

  例如，如果修补程序策略包含 10 个项，其中 6 个项为 “不符合”，则该修补程序策略的状态为 “不符合”，且摘要描述为：“6 个规则不符合要求，共 10 个规则”。

  如果多个修补程序策略将单个服务器作为目标，并且这些策略中至少有一个为 “不符合” ，则 “修补程序”的聚合符合性状态也将显示为 “不符合”。可展开详细信息窗格的 “修补程序”类别，查看不符合要求的策略，包括每个策略中有多少个规则符合或不符合要求的详细信息。
- **修补程序策略 — 规则异常**：如果规则异常应用到其中一个修补程序策略项，则服务器的修补程序符合性将显示 “部分符合” ⚠ 的符合性状态。*修补程序是唯一允许策略级别存在规则异常的符合性类别。*

修补程序符合性 — 设备组：*如果附加到策略的组中有大于 5% 的服务器具有 “不符合” ✖ 状态*，则认定附加到该服务器组的修补程序策略为 “不符合” 。如果是这种情况，则修补程序策略的聚合符合性将显示为 “不符合”。或者，也可以将设备组的 “不符合” 理解为，*当组中有小于 95% 的服务器符合要求时*，将显示 “不符合” 状态。

但是，*如果对于此类别，组中有大于 2% 且小于等于 5% 的服务器具有 “不符合” 状态*，则其状态为 “部分符合” ⚠。或者，也可以将设备组的 “部分符合” 理解为，*当组中有小于 98% 且大于等于 95% 的服务器符合要求时*，将显示 “部分符合” 状态。

如果对于此类别，组中有小于 2% 的服务器具有 “不符合” 修补程序策略状态，则整体状态为 “符合”。或者，也可以将设备组的 “符合” 理解为，*组中有至少有 98% 的服务器符合要求*。

在 “符合性” 视图中，服务器组的详细信息窗格将显示修补程序策略是否符合要求。此信息不展开显示单个服务器和策略的详细信息。

可修改用于决定服务器组符合性的阈值。

修正服务器的修补程序符合性

当修正单个服务器或多个服务器的修补程序符合性时，可选择修正附加到服务器的全部策略或选择修正单个策略。可通过查看服务器的设备资源管理器修正单个服务器的修补程序策略，或通过在 “设备组” 列表中选择策略修正多个服务器的修补程序策略。

要在单个服务器上修正修补程序策略，请执行以下操作：

1. 要在设备资源管理器中修正单个服务器的修补程序策略，在导航窗格中，选择 “设备” > “服务器” > “所有托管服务器”。
2. 在内容窗格中，选择一个服务器。
3. 右键单击并选择 “打开”，以打开 “服务器” 浏览器。
4. 在导航窗格，选择 “管理策略” > “符合性”。
5. 在 “符合性” 视图的详细信息窗格中，展开 “修补程序” 类别，然后选择单个策略或顶级 “修补程序” 类别。此选项可修正附加到服务器的所有修补程序策略。
6. 单击 “修正”，然后完成 “修正” 向导中的步骤。

要在多个服务器上修正修补程序策略，请执行以下操作：

1. 要修正多个服务器的修补程序策略，在导航窗格，选择 “设备” > “设备组” 然后选择一个组。
2. 从 “视图” 下拉列表中，选择 “符合性”。
3. 在 “符合性” 视图的详细信息窗格中，展开 “修补程序” 类别，然后选择附加到选定服务器的修补程序策略。或者，如果要修正附加到选定服务器的所有修补程序策略，则选择顶级 “修补程序” 类别。
4. 单击下列按钮之一，以修正修补程序策略：
   - **修正**：启动 “修正” 向导，该向导可修正选定服务器的选定修补程序策略。

- **扫描设备**：显示“扫描符合性”窗口，在其中可首先选择要扫描的策略类型，然后单击“扫描”启动作业。此过程扫描选定服务器中附加到服务器的所有审核、审核策略、软件、修补程序和配置策略，并且对以服务器为目标的审核没有任何影响。

  要监控扫描进度，请刷新 “符合性”窗口 （按 F5）。

注意：您还可以选择 “操作” > “扫描”来查看扫描进度。

修正组的修补程序符合性

当修正单个服务器组或多个服务器组的修补程序策略时，可修正附加到单个组或多个组中所有服务器上的所有策略。但是，当选择一个组或多个组时，仅可修正附加到该组及其任何子组中的*所有*服务器的*所有*修补程序策略。

要修正单个服务器组的修补程序策略，请执行以下操作：

1. 要在设备资源管理器中修正单个服务器的修补程序策略，在导航窗格中，选择 “设备” > “服务器” > “所有托管服务器”。
2. 在内容窗格中，选择一个服务器。
3. 右键单击并选择 “打开”，以打开 “服务器”浏览器。
4. 在导航窗格，选择 “管理策略” > “符合性”。
5. 在 “符合性”视图的详细信息窗格中，展开 “修补程序”类别，然后选择单个修补程序策略或顶级 “修补程序”类别。此选项可修正附加到服务器的所有修补程序策略。
6. 单击 “修正”，然后完成 “修正”向导中的步骤。

要修正多个服务器组的修补程序策略，请执行以下操作：

1. 要修正多个服务器的修补程序策略，从导航窗格，选择“设备”>“设备组”，然后选择一个组。
2. 从 “视图”下拉列表中，选择 “符合性”。
3. 在 “符合性”视图的详细信息窗格中，展开 “修补程序”类别，然后选择附加到选定服务器的策略。或者，如果要修正附加到选定服务器的所有策略，则选择顶级 “修补程序”类别。
4. 单击 “修正”，然后完成 “修正”向导中的步骤。

审核符合性

在 HP Server Automation 中，使用审核和修正，可定义*审核*中的服务器配置策略。*审核*有助于确保设施中的服务器符合审核策略的标准。审核由可定义用于为这些标准建模的规则集合组成。例如，审核可由 Windows COM+ 配置、注册表设置、服务、文件系统设置、硬件配置、用户和组密码设置、软件安装、程序包、存储设置等组成，这些定义了*理想服务器配置*。或者，审核可能代表*不良服务器配置*，该配置可决定配置服务器时*不*应该使用的方式。

*审核符合性*决定了在重复审核中定义的规则是否匹配所有审核目标服务器的实际服务器配置。通过“符合性”视图，可查看在服务器或服务器组上按重复计划运行的所有审核的聚合和单个符合性状态。如果任何审核为 “不符合”，则可修正在审核和审核目标服务器之间发现的任何差异。

“符合性”视图从定期计划的审核中派生审核符合性服务器和服务器组。

审核符合性状态条件

审核符合性状态由以下条件决定：

- **审核符合性 — 单个服务器**：如果审核中的单个规则与目标服务器配置不匹配，则服务器的审核符合性状态为 “不符合”。服务器的设备资源管理器的详细信息窗格将显示 “审核”类别为“不符合”，并且摘要列将指示全部规则中 “不符合”的规则数。

  例如，如果审核有 10 个规则，其中 4 个规则为 “不符合”，则审核状态会列为 “不符合”，且摘要描述显示为：“4 个规则不符合要求，共 10 个规则”。

  如果多个审核将服务器作为目标，并且这些审核中至少有一个为 “不符合”，则审核的聚合符合性状态也将显示为 “不符合”。可展开详细信息窗格的 “审核”类别，查看不符合要求的审核，包括每个审核中有多少个规则符合或不符合要求的详细信息。

- **审核符合性 — 设备组**：如果审核目标服务器组中至少有 95% 的服务器具有“符合”状态，则认定以该组服务器 （以及所有子组中的所有服务器）为目标的审核为 “符合”。

  如果审核目标服务器组中大于 5% 的服务器具有 “不符合”状态，则审核的聚合符合性将显示为 “不符合”。或者，也可以将设备组的 “不符合”理解为，*当组中有小于 95% 的服务器符合要求时*，将显示 “不符合”状态。

  但是，如果对于此类别，组中有大于 2% 且小于等于 5% 的服务器具有 “不符合”状态，则状态为 “部分符合”。或者，也可以将设备组的 “部分符合”理解为，*当组中有小于 98% 且大于等于 95% 的服务器符合要求时*，将显示 “部分符合”状态。

  如果对于此类别，组中有小于 2% 的服务器具有 “不符合”审核状态，则整体状态为 “符合”。或者，也可以将设备组的 “符合”理解为，*组中有至少有 98% 的服务器符合要求*。

  在 “符合性”视图中，服务器组的详细信息窗格将显示是否所有审核都符合要求。此信息不展开显示单个服务器和审核的详细信息。

审核符合性修正

通过使用 “符合性”视图，可查看所有以服务器或服务器组为目标的审核，并修正不符合要求的结果。这确保了服务器配置符合审核中定义的规则。

对于目标服务器上不符合要求的每个审核规则 （服务器配置不匹配规则定义或并不存在），修正会通过将该规则对象复制到目标服务器使其与规则匹配。或者，对于基于值的审核规则，修正会将目标服务器配置更改为与规则匹配。

示例：某个审核用于检查 Windows 服务器组，以确保它们包含特定注册表项和 ACL。此审核在 Windows 服务器上运行后，可能会有几个规则不符合要求。这意味着，在目标服务器上并未找到在审核规则中指定的注册表项。进行修正时，审核功能会将在审核规则中指定的注册表项复制到目标服务器中。这可确保服务器具有这些特定项和关联的 ACL。对于服务器组，修正具有相同的结果 — 仅修正操作可应用于组中的所有服务器，包括任何子组中包含的所有服务器。

修正附加到服务器的审核

可修正附加到单个服务器的审核，也可修正附加到多个服务器的审核。仅可修正单个审核。不能在顶级聚合审核。对于选定的任何组，组中的所有直接服务器子级均是修正的对象。

当“符合性”视图中的“修正”按钮未启用时，即使在详细信息窗格中选择了单个策略，并在摘要窗格中选择了一个或多个服务器，这通常也意味着对于该策略并没有任何要修正的审核结果。

无法通过“符合性”视图在服务器组上运行审核。但是，可以从“审核结果”窗口中创建在服务器组上运行的审核，并修正服务器组的审核结果。

要在单个服务器上修正单个审核，请执行以下操作：

1. 在导航窗格中，选择“设备” > “服务器” > “所有托管服务器”。
2. 在内容窗格中选择一个服务器。
3. 右键单击并选择“打开”，以打开服务器资源管理器。
4. 在导航窗格，选择“管理策略” > “符合性”。
5. 在“符合性”视图的详细信息窗格中，展开“审核”类别，然后选择单个策略。
6. 单击“修正”，然后完成“修正”向导中的步骤。

要在多个服务器上修正单个审核，请执行以下操作：

1. 在导航窗格，选择“设备” > “设备组”，然后选择一个组。
2. 从“视图”下拉列表中，选择“符合性”。
3. 通过选中每个服务器旁边的复选框选择多个服务器。
4. 在“符合性”视图的详细信息窗格中，展开“审核”类别，然后选择以所有选定服务器为目标的单个审核。
5. 单击下列按钮之一，在单个服务器或多个服务器上执行某种类型的审核修正：
   - **详细信息**：显示“审核结果”窗口，该窗口显示在审核和目标之间发现的所有差异，并可以通过规则或服务器修正这些差异。单击“查看规则详细信息”链接，打开“规则”窗口并查看审核规则。选择一个服务器，并单击“运行部分审核”启动“审核服务器”向导。
   - **运行审核**：启动“审核服务器”向导，并可以立即运行审核或稍后按计划运行审核。审核将在该审核的所有目标服务器上运行。

- **修正**：启动 “修正” 向导，通过该向导可修正不符合审核规则要求的目标服务器配置。可通过规则或服务器修正差异。如果任何选定服务器都不具有选定策略的修正结果，则将显示 “没有找到要修正的结果！” 消息。
- **扫描设备**：显示 “扫描符合性” 对话框，在其中可首先选择要扫描的策略类型，然后单击 “扫描” 启动作业。此过程扫描选定服务器中附加到服务器的所有审核、审核策略、软件、修补程序和配置策略，并且对以服务器为目标的审核没有任何影响。

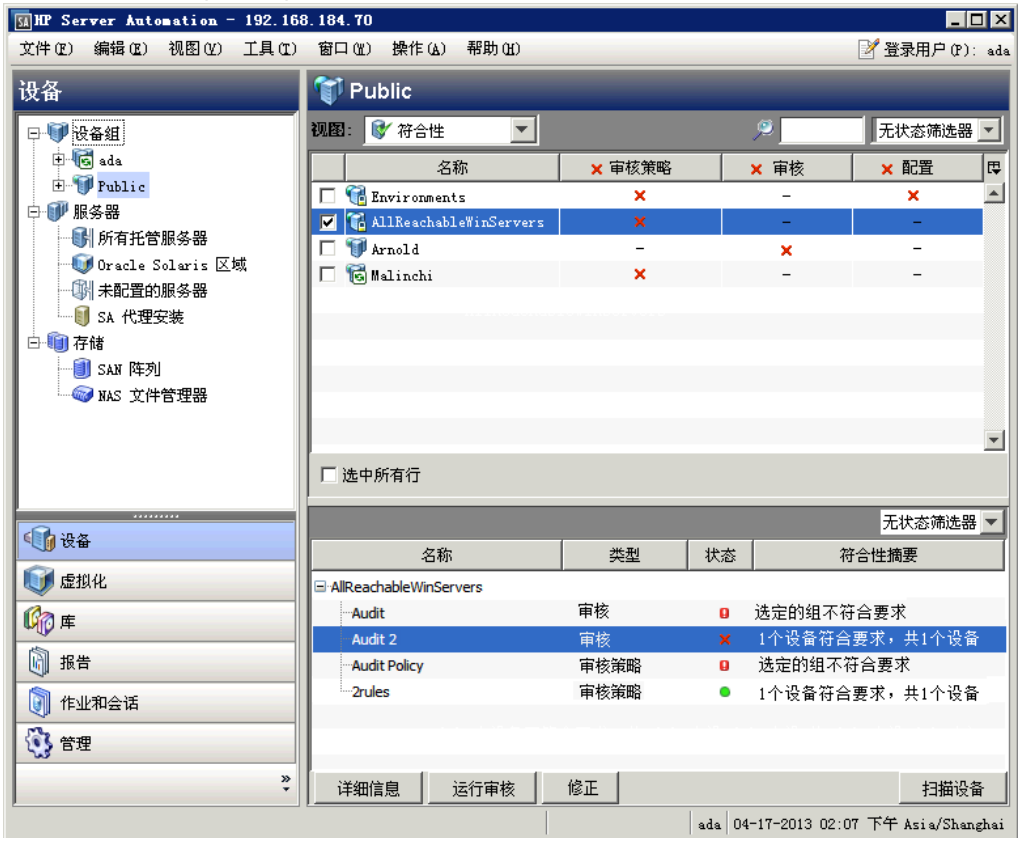
  要监控扫描进度，请刷新 “符合性” 窗口 （按 F5）。

注意：您还可以选择 “操作” > “扫描” 来查看扫描进度。

审核策略符合性

可将具有重复计划的审核添加到 “符合性” 视图中。“符合性” 视图将显示审核的最新运行结果。审核可直接包含审核规则，也可从源快照或源快照规范继承审核规则。在 “符合性” 视图中，应显示 “审核” 列以确认关联的审核规则。请参见图 37。

图 37　具有审核和审核策略的符合性视图。



最佳实践：应将审核链接到此审核规则的审核策略。这是常见且推荐的用例。通过此结构，可将几个审核链接到同一个审核策略。每个审核可包含一个不同的服务器集合或包含具有不同重复计划的多个服务器。在 “符合性” 视图的 “审核策略” 列中，将显示链接到策略的每个审核的所有符合性结果。

如果有多个审核具有重叠的服务器集，则 “审核策略” 列将显示每个服务器的最近结果的状态，而不考虑最后运行的是哪个审核。要查看给定操作的最近审核结果，则在 “符合性” 视图中选择审核，然后单击 “详细信息”、“运行审核” 或 “修正”。请参见图 37。

审核策略可分层。即，审核策略可链接到其他审核策略。

示例：

策略 A 链接到策略 B。策略 B 链接到策略 C。

- 当创建了一个审核并将其链接到策略 A 时，该审核将使用属于策略 A、策略 B 和策略 C 的符合性规则的平展列表运行。
- 如果在 “符合性”视图中为策略 A 添加 “审核策略”列，则符合性状态将显示具有策略 A、策略 B 和策略 C 的所有规则的审核结果。
- 如果没有直接链接到策略 B 和策略 C 的审核，则这些策略便没有可用的单独结果。如果在 “符合性”视图中为这些策略添加 “审核策略”列，则短划线 (-) 将指示没有结果可显示。

“符合性”视图中的“审核”和“审核策略”列之间的其他差异是仅具有重复计划的审核才可显示。但是，任何审核策略都可以作为列，正如其应用于软件和修补程序策略一样。

可为 “符合性”视图选择的符合性类别 （列）均可配置。

- 默认设置包括 “审核策略”、“软件”、“修补程序”和 “配置”。
- 对于新安装，“审核”类别不会列出。

软件符合性

在 HP Server Automation 中，使用软件管理可创建用于同时安装软件和配置应用程序的*软件策略*。*软件策略*可包含几个不同的项，如程序包、 RPM 程序包、修补程序、应用程序配置和其他软件策略。创建软件策略后，可将其附加到服务器或服务器组。

软件符合性将指示软件策略中的项是否符合实际服务器配置。如果实际的服务器配置与软件策略的定义不匹配，则服务器的软件策略为 “不符合” ✖ 。

当扫描服务器或服务器组以获取软件符合性时，“符合性”视图将派生软件策略的软件符合性信息。

有关详细信息，请参见 《SA 用户指南：软件管理》。

软件符合性状态条件

软件符合性状态由以下条件决定：

- **软件符合性 — 单个服务器**：如果软件策略中至少有一个项与在该策略所附加的服务器上找到的内容不匹配，则该服务器的软件符合性状态为 “不符合” ✖ 。服务器的设备资源管理器的详细信息窗格将显示 “软件”类别为 “不符合”，并且摘要列将指示全部规则中 “不符合”的规则（软件策略项）数。

  例如，如果软件策略包含 10 个项，其中 6 个项为 “不符合”，则该软件策略的状态会列为 “不符合”，且摘要描述为：“6 个规则不符合要求，共 10 个规则”。

如果多个软件策略将单个服务器作为目标，并且这些策略中至少有一个为 “不符合”，则 “软件”的聚合符合性状态也将显示为 “不符合”。可展开详细信息窗格的 “软件”类别，查看不符合要求的策略，包括每个策略中有多少个规则符合或不符合要求的详细信息。

- **软件符合性 — 设备组**：*如果附加到策略的组中有大于 5% 的服务器具有 “不符合” ✕ 状态*，则认定附加到该服务器组的软件策略为 “不符合” 。如果是这种情况，则软件策略的聚合符合性将显示为 “不符合”。或者，也可以将设备组的 “不符合”理解为，*当组中有小于 95% 的服务器符合要求时*，将显示 “不符合”状态。

  但是，如果对于此类别，组中有大于 2% 且小于等于 5% 的服务器具有 “不符合”状态，则其状态为 “部分符合” ⚠。或者，也可以将设备组的 “部分符合”理解为，*当组中有小于 98% 且大于等于 95% 的服务器符合要求时*，将显示 “部分符合”状态。

  如果对于此类别，组中有小于 2% 的服务器具有 “不符合”软件策略状态，则整体状态为 “符合”。或者，也可以将 “符合”理解为，*组中有至少有 98% 的服务器符合要求*。

  在 “符合性”视图中，服务器组的详细信息窗格将显示软件策略是否符合要求。此信息不展开显示单个服务器和策略的详细信息。

  可修改用于决定服务器组符合性的阈值。

软件符合性修正

通过使用 “符合性”视图，可查看所有附加到服务器或服务器组的软件策略，并修正不符合要求的服务器。这可确保服务器的软件配置符合软件策略定义。

对于每个软件策略项 （如软件、程序包、修补程序、脚本和应用程序配置），软件修正将在目标服务器上安装 （对于脚本，为执行）这些项。如果这些项在服务器上不存在，则进行安装。如果这些项已存在，但与策略不匹配，则使用正确版本进行升级。

例如，有一个由几个程序包、修补程序、脚本和一个应用程序配置组成的软件策略，均按照它们的安装和执行顺序进行组织。首先，在服务器上修正该软件策略，以确保服务器符合公司的软件安装标准。随着时间变化，软件策略中的某些项进行了更新 （如添加了新的程序包集），以及出于某种原因，卸载了服务器中的某个软件项。

执行软件符合性扫描时，扫描通过将此软件策略内容与服务器上安装的实际软件进行比较来确定该服务器的符合性状态。即使只有一个附加到其中一个服务器上的软件项不符合此策略，此服务器的软件符合性状态也将为 “不符合” ✕。

修正服务器或服务器组时，策略中指定的修补程序、程序包和应用程序配置将按照策略中指定的顺序进行安装和应用。对于服务器组，修正具有相同的结果，仅修正操作可应用于组中的所有服务器，包括任何子组中包含的所有服务器。

修正服务器的软件符合性

当修正单个服务器或多个服务器的软件符合性时，可选择修正附加到服务器的全部策略或选择修正单个策略。

可选择会修正所有选定服务器的所有软件策略的 “软件聚合” 策略。如果选定了组，则修正该组的所有直接服务器子级。如果在详细信息窗格中选择单个软件策略，则摘要窗格中选择的实体会修正该策略。

要在单个服务器上修正软件策略，请执行以下操作：

1. 在导航窗格中，选择 “设备” > “服务器” > “所有托管服务器”。
2. 在内容窗格中，选择一个服务器。
3. 右键单击并选择 “打开”，以打开 “服务器” 浏览器。
4. 在导航窗格，选择 “管理策略” > “符合性”。
5. 在 “符合性” 视图的详细信息窗格中，展开 “软件” 类别，然后选择单个软件策略或顶级 “软件” 类别。此选项可修正附加到服务器的策略。
6. 单击 “修正”，然后完成 “修正” 向导中的步骤。如果 SA 未找到要修正的设备，则将显示警告对话框。

要在多个服务器上修正软件策略，请执行以下操作：

1. 在导航窗格，选择 “设备” > “设备组”，然后选择一个组。
2. 从 “视图” 下拉列表中，选择 “符合性”。
3. 在内容窗格中，选择服务器。
4. 在 “符合性” 视图的详细信息窗格中，展开 “软件” 类别，然后选择附加到选定服务器的软件策略。或者，如果要修正附加到选定服务器的所有软件策略，则选择顶级 “软件” 类别。
5. 单击下列按钮之一，以修正软件策略：
   - **修正**：启动 “修正” 向导，该向导可修正选定服务器的选定软件策略。
   - **扫描设备**：显示 “扫描符合性” 窗口，在其中可首先选择要扫描的策略类型，然后单击 “扫描” 启动作业。此过程扫描选定服务器中附加到服务器的所有审核、审核策略、软件、修补程序和配置策略，并且对以服务器为目标的审核没有任何影响。

     要监控扫描进度，请刷新 “符合性” 窗口 （按 F5）。

注意：您还可以选择 “操作” > “扫描” 来查看扫描进度。

修正组的软件符合性

修正单个服务器组或多个服务器组的软件策略时，可修正附加到单个服务器组或多个服务器组中的所有服务器的所有策略。但是，当选择一个组或多个组时，仅可修正附加到该组及其任何子组中的**所有**服务器的**所有**软件策略。

要修正单个服务器组或多个服务器组的软件策略，请执行以下操作：

1. 要在设备资源管理器中修正单个服务器的软件策略，在导航窗格中，选择“设备”>“服务器”>“所有托管服务器”。
2. 在内容窗格中选择一个服务器。
3. 右键单击并选择 “打开”，以打开 “设备”浏览器。
4. 在导航窗格，选择 “管理策略” > “符合性”。
5. 在“符合性”视图的详细信息窗格中，展开 “软件”类别，然后选择单个软件策略或顶级 “软件”类别。此选项可修正附加到服务器的所有策略。
6. 单击 “修正”，然后完成 “修正”向导中的步骤。

   或

7. 在显示属于该组的服务器列表的内容窗格中，通过选中每个服务器旁边的复选框来选择多个服务器。（*可选*）选择 “选中所有行”以选择所有服务器。
8. 要修正多个服务器的软件策略，在导航窗格，选择 “设备” > “设备组”然后选择一个组。
9. 从 “视图”下拉列表中，选择 “符合性”。
10. 在 “符合性”视图的详细信息窗格中，展开 “软件”类别，然后选择附加到选定服务器的软件策略。或者，如果要修正附加到选定服务器的所有软件策略，则选择顶级 “软件”类别。
11. 单击下列按钮之一，以修正软件策略：
    - **修正**：启动 “修正”向导，该向导可修正选定服务器的选定软件策略。
    - **扫描设备**：显示“扫描符合性”窗口，在其中可首先选择要扫描的策略类型，然后单击“扫描”启动作业。此过程扫描选定服务器中附加到服务器的所有审核、审核策略、软件、修补程序和配置策略，并且对以服务器为目标的审核没有任何影响。

      要监控扫描进度，请刷新 “符合性”窗口 （按 F5）。

注意：您还可以选择 “操作” > “扫描”来查看扫描进度。

配置符合性

在 HP Server Automation 中，*应用程序配置* 管理托管服务器上的配置文件。应用程序配置可管理单个服务器或服务器组的一个或多个配置文件。每个应用程序配置包含一个或多个模板，用于构建字段理想配置状态的模型。这些模板有助于管理服务器上特定文件的配置值 （*“键 - 值”对*）。

例如，可创建一个应用程序配置，用于管理数据中心的服务器主机文件。可定义标准 Unix 主机文件的 “IP 地址 - 主机名”键 - 值对，然后将应用程序配置附加到包含此文件的几个服务器或一个服务器组。*应用程序配置* 用作 *有助于确保目标服务器上的主机文件具有正确 “IP 地址 - 主机名”定义的策略*。

应用程序配置符合性指示是否所有附加到服务器的应用程序配置 （策略）都符合托管服务器上的实际应用程序配置文件要求。在主机文件示例中，如果服务器配置中的主机文件内的信息与在应用程序配置中定义的值不匹配，则服务器的配置为 “不符合” ✖ 。如果有多个应用程序配置附加到服务器，且作为应用程序配置目标的其中任一个实际配置文件是不同的，则整个服务器在 “符合性” 视图中显示为 “不符合”。

相反，如果未在应用程序配置和服务器的文件之间找到差异，则 “配置” 符合性状态为 “符合” ● 。所有应用程序配置都必须 100% 符合，服务器的 “配置” 符合性状态才会在 “符合性” 视图中显示为 “符合”。

要检查应用程序配置的目标配置文件的最新状态，可通过执行应用程序配置符合性扫描确定应用程序配置和服务器的实际配置文件之间是否存在任何差异。

有关详细信息，请参见 《SA 用户指南：应用程序配置》。

配置符合性状态条件

配置符合性状态由以下条件决定：

- **配置符合性 — 单个服务器**：如果在应用程序配置和目标服务器的实际配置文件之间发现任何差异，则服务器的 “配置” 符合性状态为 “不符合” ✖ 。服务器的设备资源管理器的详细信息窗格将 “配置” 类别显示为 “不符合”。如果有多个应用程序配置附加到服务器，且作为应用程序配置目标的其中任一个实际配置文件与应用程序配置不同，则认定整个服务器在 “符合性” 视图中为 “不符合”。
- **配置符合性 — 设备组**：*如果附加到应用程序配置的组中有大于 5% 的服务器具有 “不符合” ✖ 状态*，则认定附加到该服务器组的应用程序配置策略为 “不符合” 。如果是这种情况，则配置的聚合符合性将显示为 “不符合”。或者，也可以将设备组的 “不符合” 理解为，*当组中有小于 95% 的服务器符合要求时*，将显示 “不符合” 状态。

  但是，*如果对于此类别，组中有大于 2% 且小于等于 5% 的服务器具有 “不符合” 状态*，则其状态为 “部分符合” ▲ 。或者，也可以将设备组的 “部分符合” 理解为，*当组中有小于 98% 且大于等于 95% 的服务器符合要求时*，将显示 “部分符合” 状态。

  如果对于此类别，组中有小于 2% 的服务器具有 “不符合” 配置状态，则整体状态为 “符合”。或者，也可以将 “符合” 理解为，*组中有至少有 98% 的服务器符合要求*。

  在 “符合性” 视图中，服务器组的详细信息窗格将显示应用程序配置是否符合要求。此信息不展开显示单个服务器和策略的详细信息。

  可修改用于决定服务器组符合性的阈值。

修正配置符合性 — 服务器和组

应用程序配置的修正与其他符合性类别类型的修正稍有不同。要修正应用程序配置，不是修正服务器上的策略 （如修正审核策略、软件或修补程序时），而是在设备资源管理器或组资源管理器上选择一个应用程序配置。然后使用*推送*功能，将在此应用程序中定义的值推送到服务器或服务器组上的实际配置文件。推送应用程序配置时，会将应用程序配置模板中定义的所有值添加到目标配置文件，或替换目标配置文件中的相应值。

应用程序配置中值的推送方式 （如列表和标量的序列）取决于这些值在应用程序配置继承层次结构中所设置的方式，以及在配置模板中所配置的序列合并模式。

要在服务器或服务器组上修正应用程序配置，请执行以下操作：

1. 要在设备资源管理器中修正单个服务器的应用程序配置，在导航窗格中，选择 “设备” > “服务器” > “所有托管服务器”，然后选择一个服务器。

   或

2. 要修正服务器组的应用程序配置，在导航窗格，选择 “设备” > “设备组”然后选择一个组。
3. 右键单击并选择 “打开”，以打开 “设备”浏览器。
4. 在 “信息”窗格，选择 “管理策略” > “配置的应用程序”。请参见 《SA 用户指南：应用程序配置》，以便继续操作。另请参见：

索引

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

W

X

Y

Z