Sun Identity Manager 概述

Sun Microsystems, Inc.
4150 Network Circle
Santa Clara, CA 95054
U.S.A.

文件号码 821–0061
2009 年 2 月

090729@22510

目录

前言

Sun Identity Manager 8.1 Overview对**什么是** *Sun™ Identity Manager* **和它是如何工作的？**问题进行了回答。本书将描述 Identity Manager 产品体系结构，以及有关如何规划高可用性部署的信息。

目标读者

本指南面向那些正寻求更好地理解 Sun Identity Manager 8.1 及其相关软件的 IT 专业人员。它对于那些正在评估 Identity Manager 或者刚开始规划 Identity Manager 部署的 IT 专业人员特别有用。

本书的结构

本指南包含以下章节：

第 1 章，产品概述描述 Identity Manager 的用途并重点介绍该应用程序的主要功能。

第 2 章，产品体系结构描述 Identity Manager 体系结构、Service Provider 体系结构和 Web 服务体系结构，还包括系统分隔和物理接近性准则。

第 3 章，群集和高可用性提供有关如何实施高可用性/容错 (high availability/fault tolerant, HA/FT) Identity Manager 环境的指导，还将帮助您评估 Identity Manager 部署所需的可用性程度。

相关文档

Sun Identity Manager 8.1 文档集包括以下文档。

主要读者	标题	描述
所有读者	《Sun Identity Manager 概述》	概述 Identity Manager 的特性和功能。提供产品体系结构信息，并描述 Identity Manager 如何与其他 Sun 产品（如 Sun Open SSO Enterprise 和 Sun Role Manager）集成。
	《Sun Identity Manager 8.1 发行说明》	描述已知问题、已解决的问题以及 Identity Manager 文档集内未提供的最新信息。
系统管理员	《安装指南》	描述如何安装 Identity Manager 和可选组件（如 Sun Identity Manager Gateway 和 PasswordSync）。
	《升级指南》	提供有关如何将 Identity Manager 从早期版本升级到较新版本的说明。
	《系统管理员指南》	其中包含的信息和说明可帮助系统管理员管理和调整其 Identity Manager 安装并对该安装进行故障排除。
业务管理员	《业务管理员指南》	描述如何使用 Identity Manager 置备和审计功能。包含有关用户界面、用户与帐户管理以及报告等功能的信息。
系统集成商	《部署指南》	描述如何在复杂的 IT 环境中部署 Identity Manager。所涵盖的主题包括处理身份属性、装入和同步数据、配置用户操作、应用自定义标记等。
	《部署参考资料》	包含有关工作流、表单、视图、规则和 XPRESS 语言的信息。
	《资源参考资料》	提供有关安装、配置和使用资源适配器的信息。
	《Service Provider 8.1 部署》	描述如何部署 Sun Identity Manager Service Provider，以及它在视图、表单和资源方面与标准 Identity Manager 产品的区别。
	《Web 服务指南》	描述如何配置 SPML 支持、受支持的 SPML 功能（以及受支持的原因）以及如何在现场扩展该支持。

文档更新

对本文档以及其他 Sun Identity Manager 出版物的更正和更新将发布到 Identity Manager 文档更新 Web 站点：

http://blogs.sun.com/idmdocupdates/

可以使用 RSS 订阅源读取器定期检查该网站，并在发布更新后通知您。要进行订阅，请下载订阅源读取器，并单击页面右侧“订阅源”下面的链接。从 8.0 版开始，将为每个主要发行版提供单独的订阅源。

相关的第三方 Web 站点引用

本文档引用了第三方 URL 以提供其他相关信息。

注 – Sun 对本文档中提到的第三方 Web 站点的可用性不承担任何责任。对于此类站点或资源中的（或通过它们获得的）任何内容、广告、产品或其他资料，Sun 并不表示认可，也不承担任何责任。对于因使用或依靠此类站点或资源中的（或通过它们获得的）任何内容、产品或服务而造成的、名义上造成的或连带产生的实际或名义损坏或损失，Sun 概不负责，也不承担任何责任。

文档、支持和培训

Sun Web 站点提供了有关以下附加资源的信息：

- 文档 (http://www.sun.com/documentation/)
- 支持 (http://www.sun.com/support/)
- 培训 (http://www.sun.com/training/)

Sun 欢迎您提出意见

Sun 致力于提高其文档的质量，并十分乐意收到您的意见和建议。要共享您的意见，请转至 http://docs.sun.com 并单击 "Feedback"（反馈）。

印刷约定

下表介绍了本文档中使用的印刷约定。

表 P–1 印刷约定

字样	含义	示例
`AaBbCc123`	命令、文件和目录的名称，以及计算机屏幕输出	编辑 `.login` 文件。 使用 `ls -a` 列出所有文件。 `machine_name% you have mail.`
`AaBbCc123`	您键入的内容，与计算机屏幕输出的显示不同	`machine_name%` **`su`** `Password:`
aabbcc123	占位符：将用实际名称或值替换	用于删除文件的命令为 `rm` *filename*。
AaBbCc123	书名、新术语和要强调的术语	请阅读用户指南中的第 6 章。 **高速缓存**是指在本地存储的副本。 请**勿**保存文件。 **注意**：某些强调项在联机查看时显示为粗体。

命令中的 Shell 提示符示例

下表显示了 C shell、Bourne shell 和 Korn shell 的默认 UNIX® 系统提示符和超级用户提示符。

表 P–2 Shell 提示符

Shell	提示符
C shell	`machine_name%`
用于超级用户的 C shell	`machine_name#`
Bourne shell 和 Korn shell	`$`
用于超级用户的 Bourne shell 和 Korn shell	`#`

◆ ◆ ◆ 第 1 章

1 产品概述

本章描述 Sun™ Identity Manager 的用途并重点介绍该应用程序的主要功能。本章还简要介绍了 Sun 提供的其他身份管理产品。

本章包含以下主题：

什么是 Identity Manager？

Sun Identity Manager 能够自动执行跨多个 IT 系统创建、更新和删除用户帐户的过程。此过程统称为**置备**（即创建和更新帐户）和**解除置备**（即删除用户帐户）。

例如，当员工加入公司时，Identity Manager 会运行一个工作流来检索必需的批准以授予其访问权限。当 Identity Manager 获取这些批准后，会在公司的人力资源系统 (PeopleSoft)、电子邮件系统 (Microsoft Exchange) 和企业应用程序 (SAP) 中为员工创建帐户。如果员工在公司中的角色发生变化，Identity Manager 会更新其用户帐户，并扩展他/她对于新角色所需的必要资源的访问权限。而且，当员工离开公司时，Identity Manager 会自动删除其用户帐户以防其继续访问相关资源。

Identity Manager 还可以实时强制实施审计策略。**审计策略**指定用户可以或不可以拥有的访问权限类型。例如，在美国，如果同一个用户既能够访问应付帐款系统又能够访问应收帐款系统，则会违反 Sarbanes-Oxley (SOX) 法案。这就是所谓的违反职责分离规则。Identity Manager 可以执行审计扫描以检查是否存在各种类型的违反情况，并根据所使用的配置，在检测到违反情况时，自动删除相关访问权限或者向管理员发送通知。此过程称为**纠正**。

Identity Manager 如何与其他 IT 系统交互？

在 Identity Manager 中，受管应用程序和其他 IT 系统称为**资源**。Identity Manager 使用**适配器**或**连接器**与资源进行交互。

适配器和连接器安装在 Identity Manager 服务器上。（Identity Manager 不需要在目标资源上安装称为**代理**的特殊软件。）Sun 提供了许多 Identity Manager 适配器和连接器，可以创建新的适配器和连接器，以便通过标准协议或已知的应用程序编程接口 (application programming interface, API) 来与几乎所有的资源进行通信。Identity Manager 附带了各种能够与许多最常见的资源进行通信的适配器和连接器。另外，模板和框架代码可用于帮助程序员创建其他适配器和连接器。

对于某些资源，不能直接与之通信，需要使用 Sun Identity Manager Gateway 才能与之通信。需要 Gateway 的资源示例包括 Microsoft 产品（如 Exchange 和 Windows Active Directory）、Novell 产品（如 eDirectory，以前称为 Netware Directory Services）等。在这种情况下，Identity Manager 直接与 Gateway 通信，Gateway 再与这些资源进行交互。

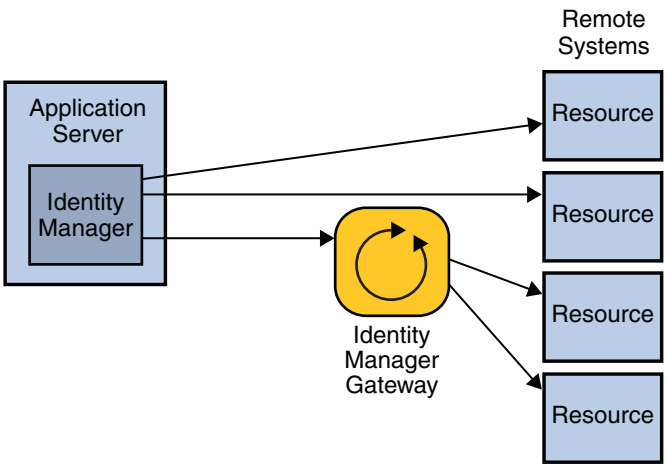

图 1–1 Identity Manager 直接与一些资源交互，而与另一些资源交互则需要使用 Identity Manager Gateway

有关 Identity Manager 所支持的资源的列表，请参见《Sun Identity Manager 8.1 发行说明》中的“支持的资源”。

用户如何连接到 Identity Manager？

Identity Manager 有一个面向管理员的用户界面 (user interface, UI)，还有一个面向最终用户的独立界面。要使用 Identity Manager，管理员和最终用户需要使用 Web 浏览器登录到 Identity Manager。

- 管理员使用**管理员界面**来管理用户、设置和分配资源、定义权限和访问级别、制定审计策略、管理遵循性，以及执行其他业务管理员和系统管理员功能。
- 最终用户使用**最终用户界面**执行大量自服务任务，如更改密码、设置对身份验证问题的答案、请求对 IT 系统的访问权限以及管理委托的分配。

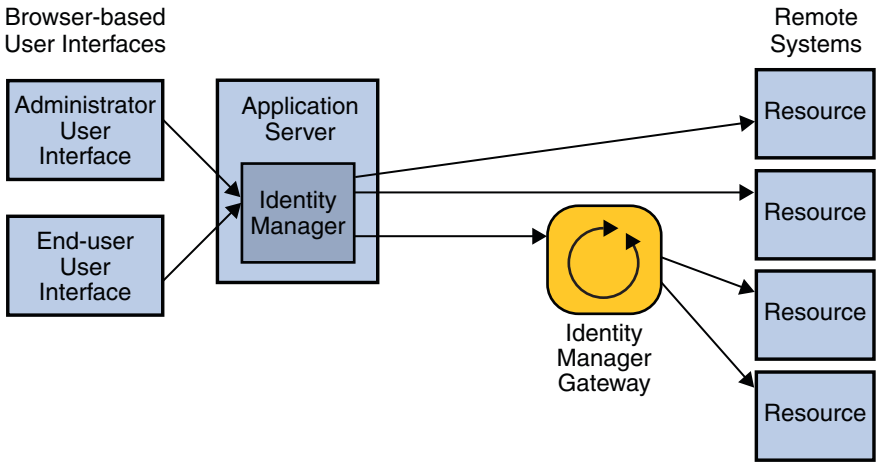

图 1–2 用户可以使用管理员界面和最终用户界面连接到 Identity Manager

公司还可以使用 SPML（Service Provisioning Markup Language，服务置备标记语言）创建其自己的用户界面，或者将现有的前端系统与 Identity Manager 集成。

其他 Identity Manager 界面包括：

- IVR（Interactive Voice Response，互动式语音应答）电话界面 — 允许最终用户使用电话执行 Identity Manager 功能
- Identity Manager IDE（Integrated Development Environment，集成开发环境）— 由软件开发者用来自定义 Identity Manager
- Identity Manager 控制台 — 可供管理员使用的命令行界面

什么是 Identity Manager Service Provider？

Identity Manager Service Provider 是可高度伸缩的、专注于外联网的身份管理功能，通过它可以置备和维护数百万个存储在 LDAP 目录服务器上的最终用户帐户。通过 Service Provider 功能还可以管理数千个管理员帐户并将 LDAP 帐户数据与其他资源同步。

Service Provider 功能使用 Identity Manager 中提供的部分特性和功能。例如，没有提供审计功能，因为它在外联网环境中用处不太大。

有关标准 Identity Manager 和 Service Provider 功能之间区别的详细说明，请参见《Sun Identity Manager Service Provider 8.1 Deployment》中的“Service Provider Features”。

Service Provider 以前作为一个单独的附加产品提供，现在是 Identity Manager 的一部分。但是，利用 Service Provider 功能需要进行特殊的规划。

- 有关 Identity Manager Service Provider 系统体系结构的信息，请参见第 19 页中的“了解 Identity Manager Service Provider 系统体系结构”。
- 有关规划高可用性 Identity Manager Service Provider 体系结构的信息，请参见第 27 页中的“了解所建议的 Service Provider HA 体系结构”。
- 有关部署 Identity Manager 以利用 Service Provider 功能的信息，请参见《Sun Identity Manager Service Provider 8.1 Deployment》。

了解 Sun 的其他身份管理产品

除了 Identity Manager，Sun 的其他身份管理解决方案包括 Sun Java™ System Directory Server Enterprise Edition、Sun OpenSSO Enterprise 和 Sun Role Manager。这些产品对 Identity Manager 进行了补充，Role Manager 可以对 Identity Manager 的功能进行扩展。

什么是 Sun Java System Directory Server Enterprise Edition？

Sun Java System Directory Server Enterprise Edition 是可伸缩的高性能 LDAP 数据存储，用来存储身份信息。Directory Server Enterprise Edition 提供核心目录服务以及其他补充数据服务。竞争的目录服务产品包括 Microsoft 的 Active Directory 和 Novell 的 eDirectory。

什么是 OpenSSO Enterprise？

Sun OpenSSO Enterprise（以前称为 Sun Java System Access Manager 和 Sun Java System Federation Manager）为内部与外部应用程序和 Web 服务集中实施了一个全面的安全策略。它提供安全和集中的访问控制和单点登录 (single sign-on, SSO) 功能。使用它可以进

行联合身份管理，从而可以与拥有不同目录服务、安全和身份验证技术的公司共享应用程序。联合合作伙伴相互信任，能够验证其各自的用户，并保证用户对于访问服务的权限。

什么是 Sun Role Manager？

Sun Role Manager（以前称为 Vaau RBACx）通过基于用户在公司中的角色（而不是基于每个用户）来管理访问权限。公司基于使用情况和企业策略创建角色，从而获取对其访问权限更大的可见性，并以更高效、更安全和更符合要求的方式来管理访问权限。

◆ ◆ ◆ 第 2 章

2 产品体系结构

本章概述 Sun™ Identity Manager 产品体系结构。

本章包含以下主题：

了解 Identity Manager 组件

Identity Manager 是一种 Java 2 Platform, Enterprise Edition（J2EE™ 平台）Web 应用程序。J2EE 平台由一组符合行业标准的服务、API 和协议组成，提供用来开发基于 Web 的多层企业应用程序的功能。

Identity Manager 系统体系结构分布在以下四个逻辑层中：

- 用户层
- 应用层
- 数据库层
- 受管资源层

下面的几节将从应用层开始分别论述这四个层。

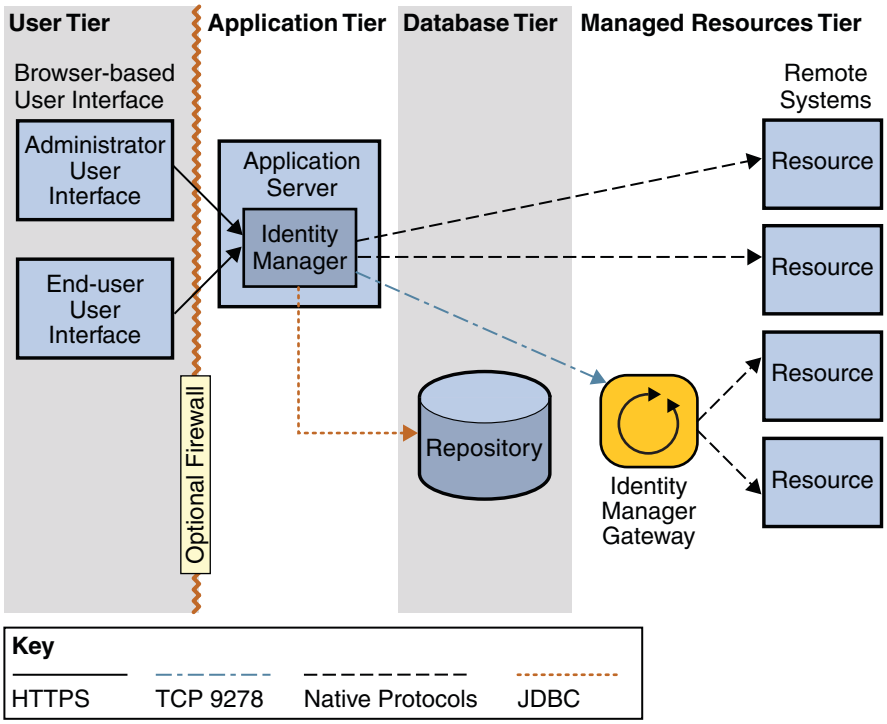

图 2–1 Identity Manager 系统体系结构

了解应用层

Identity Manager（又称为 Identity Manager 服务器）安装在应用服务器内部的 J2EE Web 容器中。Identity Manager 服务器由 JSP™ 文件、HTML、图像和 Java™ 类组成。与其他 IT 系统（又称为**资源**）交互的适配器和连接器也位于应用服务器上的 Identity Manager 中。

注 – 有关受支持的应用服务器的列表，请参见《Sun Identity Manager 8.1 发行说明》中的“应用服务器”。

由于 Identity Manager 是一种 Web 应用程序，因此用户界面驻留在应用服务器上，而且会根据每个请求向用户层提供页面。

在应用服务器上安装 Identity Manager 的过程非常简单：使用 Sun 提供的基于向导的图形安装程序和（在 UNIX® 系统上）命令行安装程序。应用服务器必须捆绑或安装了 Java Development Kit (JDK™) 才能运行可在 Identity Manager 中执行操作的 Java 类。

了解数据库层

Identity Manager 将其所有的置备和状态信息都存储在 Identity Manager **系统信息库**中。系统信息库由多个用来存储有关 Identity Manager 的所有配置数据的表组成。系统信息库是 Identity Manager 查找数据和锁定对象的单一点。系统信息库还包含一个审计日志，审计日志是在 Identity Manager 中所执行操作的历史记录。Identity Manager 数据以 XML 形式存储。尽管关系数据库在生产环境中是必需的，但是系统信息库可以驻留在本地文件中，也可以驻留在关系数据库中。

注 – 有关受支持的数据库服务器的列表，请参见《Sun Identity Manager 8.1 发行说明》中的“系统信息库数据库服务器”。

请注意，Identity Manager 中除了保留有关各个用户的最少数量的身份信息外，不保留其他用户数据。也就是说，系统信息库中仅保存为了确定和区分 Identity Manager 中的各个用户而必需的属性（例如，**名称**和**电子邮件地址**）。

Identity Manager 可以通过直接 JDBC 连接机制连接到系统信息库，也可以使用由应用服务器提供的数据源功能。

Identity Manager Service Provider 功能需要使用一个额外的 LDAP 系统信息库来存储用户信息。有关详细信息，请参见第 19 页中的 “了解 Identity Manager Service Provider 系统体系结构”。

了解受管资源层

受管资源层包括为其置备用户帐户和解除用户帐户置备的应用程序和 IT 系统。该层包括 Identity Manager Gateway，这是一个帮助应用程序，允许 Identity Manager 与某些资源交互。

适配器和连接器提供用户管理功能，其中包括创建、更新、删除和读取用户帐户，以及执行密码更改管理功能。适配器和连接器还可以从远程系统提取帐户信息。

注 – 在多数情况下，Identity Manager 管理远程系统上的用户数据，而不是将这些数据保留在其自己的数据存储中。

需要使用 Sun Identity Manager Gateway 的一些公共资源包括 Microsoft Exchange、Windows Active Directory、Novell eDirectory（以前称为 Netware Directory Services）、Lotus Domino 等等。（有关完整的列表，请参见《Sun Identity Manager 8.1 发行说明》中的“Sun Identity Manager Gateway”。）该 Gateway 在 Windows 中以服务形式安装，它使用 TCP 端口 9278 与 Identity Manager 通信。通信是使用专有的加密协议从 Identity Manager 启动的。Gateway 随后会使用资源的本机协议来与受管资源交互。

从安装的角度看，共有两种类型的适配器和连接器：*Identity Manager* **适配器和连接器**和**自定义的适配器和连接器**。Identity Manager 适配器和连接器预先安装在 Identity Manager 中。但是，自定义的适配器和连接器需要复制到应用服务器上 Identity Manager 安装目录中的指定目录下。

使用 Identity Manager **资源扩充工具** *(Resource Extension Facility, REF)* 工具包，可以非常方便地创建自定义适配器。REF 工具包提供了一个 API 和许多模板适配器，公司可以使用它们来启动开发过程。简单的资源功能可以通过仅实施八种 Java 方法来实现。

了解用户层

用户层由那些通过某个用户界面与 Identity Manager 交互的管理员和最终用户组成。本产品的主要用户界面是一个 Web 浏览器，该浏览器通过 HTTPS 与 Identity Manager 通信。即使某些功能可能会使用 Java applet，两个基于浏览器的用户界面（**管理员用户界面**和**最终用户界面**）也是主要由 HTML 页面组成。

为简单起见，图 2–1 中仅显示了管理员用户界面和最终用户界面。但是，用户层中还包括其他用户界面：IVR 电话界面、Identity Manager IDE、SPML Web 服务界面和 Identity Manager 控制台。

了解系统分隔和物理接近性准则

本节包含有关哪些 Identity Manager 组件应当在什么服务器上运行的基本准则，还包含有关为了尽可能减少因延迟和网络拥塞所造成的性能问题，而应当使哪些组件相邻放置的建议。

注 – 本节仅提供了基本准则。有关设计高可用性 Identity Manager 体系结构的信息，请参见第 3 章，群集和高可用性。

在开发环境中，应用服务器和数据库可以驻留在同一台计算机上。但是，在测试环境和生产环境中，每个 Identity Manager 实例都应当安装在其自己的专用服务器上。关系数据库也需要一台专用服务器。

必须在一台或多台 Windows 计算机上安装 Identity Manager Gateway（如果需要的话）。Gateway 是一种轻量组件，不需要安装在专用服务器上。由 网关 管理的所有 Windows 域必须属于同一个林。不支持跨林边界管理域。如果您有多个林，请在每个林中至少安装一个 网关。在生产环境中，必须使 Gateway 具有高可用性。有关详细信息，请参见第 25 页中的 “使网关具有高可用性”。

在生产环境中，数据库服务器与应用服务器之间发生的网络通信流量最多。这两台服务器必须位于同一个 LAN 中，而且网络跃点之间的距离应当尽可能最短。Gateway 实例以及受管资源不需要与 Identity Manager 位于同一个网络上。

如果 Identity Manager 将用于 Service Provider 配置中的外部用户，则应当在 DMZ 中设置一组 Web 服务器。有关详细信息，请参见第 27 页中的 “了解所建议的 Service Provider HA 体系结构”。

了解 SPML 和 Web 服务系统体系结构

服务置备标记语言 (Service Provisioning Markup Language, SPML) 和 Identity Manager Web 服务可用于为 Identity Manager 实施自定义的前端。Identity Manager 使用 HTTPS 协议收发 SPML 消息和响应。

有关 SPML 和 Web 服务的详细信息，请参见《Sun Identity Manager 8.1 Web Services》。

了解 Identity Manager Service Provider 系统体系结构

如果实施了 Identity Manager Service Provider 功能，则需要实施第五层。第五层称为 Web 层，由一台或多台位于 DMZ 中的 Web 服务器组成。Web 层中不安装任何 Identity Manager 组件。DMZ 中的 Web 服务器通过响应 Web 页请求为应用层中的一台或多台应用服务器提供支持。在 Web 层中添加一台或多台 Web 服务器可提供增强的可伸缩性，在 DMZ 中放置 Web 服务器可提供更好的网络安全性。

Service Provider 功能还需要使用一个 LDAP 系统信息库。此系统信息库驻留在数据库层中。由于 LDAP 系统信息库可以是受管资源，因此也可以理解为 LDAP 服务器驻留在受管资源层中。

注 – 在仅包含 Service Provider 的实施中，除了 LDAP 系统信息库外，还建议部署一个 Identity Manager 系统信息库，但这不是必需的。如果未部署 Identity Manager 系统信息库，某些功能（如某些报告功能）将不可用。

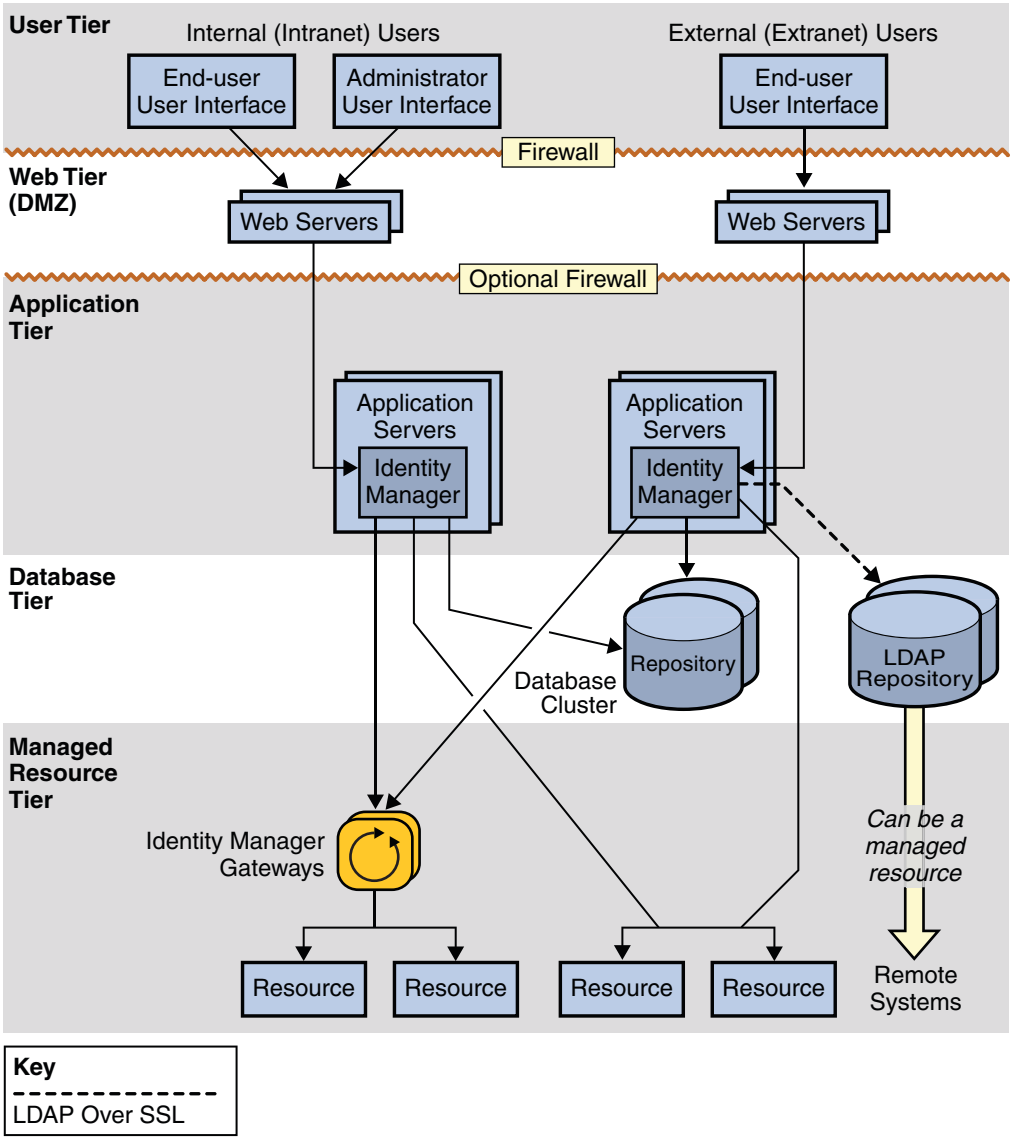

图 2–2 Identity Manager Service Provider 系统体系结构

◆ ◆ ◆ 第 3 章

3 群集和高可用性

本章提供有关如何实施高可用性/容错 (HA/FT) Identity Manager 环境的指南。

注 – 有关确保针对每种技术实现高可用部署的最佳做法，请查阅 Web 服务器、应用服务器和数据库提供商的文档。本指南不能替代供应商特定的 Web 服务器建议。

评估可用性需求

本节介绍如何评估特定部署所需的可用性程度。

评估停机时间成本

由于普通用户在处理他们已经能够访问的系统和应用程序时不需要 Identity Manager，因此 Identity Manager 停机时间不像您想象的那样可怕。如果 Identity Manager 不可用，最终用户仍能够通过为他们置备的帐户来访问资源。

Identity Manager 停机时间的主要成本是工作效率降低。如果 Identity Manager 关闭，最终用户将无法使用 Identity Manager 访问已对他们锁定或者未向他们置备的系统。

要计算停机时间的成本，需要的第一个数值就是由于最终用户无法访问企业内的计算资源而导致工作效率下降所带来的平均成本。在我们的评估中，此数值称为**每个工时的工作效率**。

需要确定的另一个主要数值就是用户群中需要在任何给定时间使用 Identity Manager 的用户所占的百分比。这些用户通常包括需要为其置备系统的新雇员，以及忘了密码的最终用户（如果密码管理是部署的一部分）。

请考虑下面的虚拟场景：

员工总数	20,000
一天内重置密码的次数	130
一天内新雇员的数量	30
一个工作日内的小时数	8

对于这个特定场景，可以按如下公式计算：

- 在任何给定小时内需要 Identity Manager 的员工数 = (130 + 30)/8 = 20
- 在任何给定小时内需要 Identity Manager 的员工所占的百分比 = 20/20,000 = 0.1% 或 1/1000

然后可以使用这些数值估计 Identity Manager 中断所带来的成本：

每个工时的工作效率	$100	
工作效率下降比例	0.5	（由于无法访问系统而导致工作效率下降 50%）
受影响的人数	20	
小计	$1,000	

中断时间间隔	2 个小时
总直接损失	$2,000

此示例说明即使由 Identity Manager 管理的用户很多，在任何给定时间内需要通过 Identity Manager 访问系统的用户通常很少。

需要考虑的另一点就是，将系统（如 Identity Manager）重新联机所需的时间通常少于手工执行正由 Identity Manager 自动完成的置备过程所需的时间。因此，尽管 Identity Manager 停机时间会带来成本，但该成本通常低于使用手动过程来让用户访问资源所带来的成本。

了解停机时间的原因

在规划 Identity Manager 高可用部署时，有必要考虑停机时间的原因。

这些原因包括：

- 操作员错误
- 硬件故障
- 软件故障
- 计划的停机时间（软硬件升级）
- 较差的性能（观察到的停机时间）

计算投资回报率

Identity Manager 自动执行相关过程并避免工作效率降低。在高可用性 Identity Manager 体系结构方面的投资回报率可通过尽可能缩短停机时间和避免工作效率降低来实现。

您可以使用停机时间所带来的成本来确定 Identity Manager 最终需要的可用性程度。通常，为使 Identity Manager 具有高可用性而进行适度投资是值得的。

在计算投资成本时，请记住，购买 HA/FT 硬件和软件只是实施可用解决方案的一部分。让知识渊博的人员启动并运行它也会带来成本。

了解 Identity Manager 高可用性功能集

Identity Manager 在设计上能够利用可用的 HA 基础结构。例如，Identity Manager 不需要通过应用服务器群集来实现高可用性，但是它可以利用现有的群集。

下图显示了在非冗余体系结构中部署的主要 Identity Manager 组件。随后的几节将描述如何使 Identity Manager 系统信息库、应用服务器和网关具有高可用性。

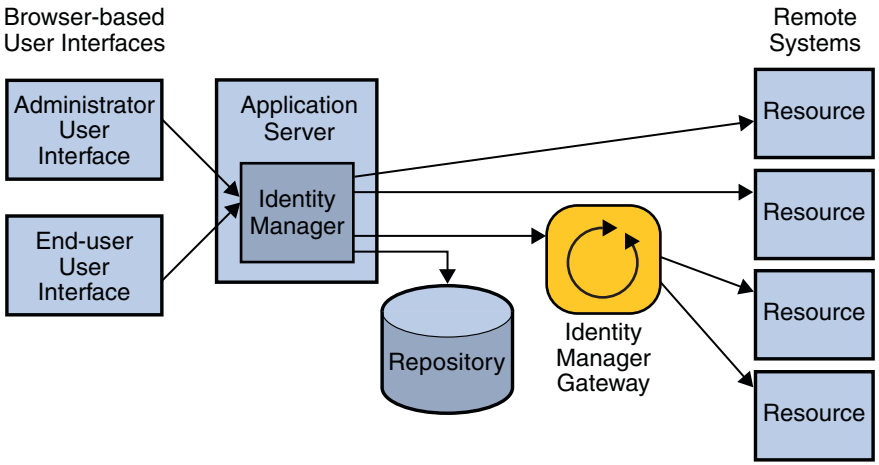

图 3–1 标准的 Identity Manager 系统体系结构

注 – 有关为了尽可能减少因延迟和网络拥塞所造成的性能问题，而应当使哪些组件相邻放置的信息，请参见第 18 页中的“了解系统分隔和物理接近性准则”。

使系统信息库具有高可用性

Identity Manager 将其所有的置备和状态信息都存储在 Identity Manager 系统信息库中。

用来存储 Identity Manager 系统信息库的数据库实例的可用性是实现高可用性 Identity Manager 部署的最关键部分。系统信息库代表整个 Identity Manager 安装，其中的数据必须与其他重要数据库应用程序一起进行保护。至少，必须定期执行备份。

注 – 不要将 Identity Manager 系统信息库放在虚拟平台（如 VMware 虚拟机）上，因为性能（每秒的事务数）将会受到显著影响。

系统信息库只能有一个映像。对于 Identity Manager 不可能有两个不同的数据库，而且不要尝试在夜间同步它们。Sun 建议使用数据库的群集或镜像功能来提供容错。

使应用服务器具有高可用性

Identity Manager 可以在一个应用服务器群集内运行，而且可以利用群集所提供的附加可用性和负载平衡。但是，Identity Manager 不使用任何需要群集的 J2EE 功能。

Identity Manager 使用可通过 Servlet API 访问的 HTTP Session 对象。此会话对象在用户登录和执行操作时跟踪用户的访问情况。在群集内，可以选择在给定会话期间让多个节点处理用户请求。但通常不建议这样做，因为多数安装都配置为将用户针对给定会话的整个请求发送到同一台服务器。

可以为运行 Identity Manager 的应用服务器额外增加可用性和容量，即使您未设置群集也是如此。可通过以下方法来增加可用性和容量：安装多台带有 Identity Manager 的应用服务器，将这些服务器连接到同一个系统信息库，并在所有的应用服务器前面放置一个具有**会话关联**的负载平衡器。

注 – 有关会话关联的详细信息，请参见第 34 页中的 “与会话关联和会话持久性有关的常见问题解答”。

Identity Manager 在后台运行某些任务（例如，预定的协调任务）。这些任务存储在数据库中，而且可以由任何 Identity Manager 服务器选取运行。Identity Manager 使用数据库来确保这些任务始终完成运行，即使数据库必须故障切换到另一个节点也是如此。

在应用服务器节点上配置 Active Sync 群集

`Waveset.properties` 文件中的 `sources.hosts` 设置控制多实例环境中的哪些主机可用于执行 Active Sync 请求。此设置提供有关可在其上运行源适配器的主机的列表。将该设置配置为 *localhost* 或 *null* 将允许源适配器在 Web 群中的任何主机上执行。（这是默认行为。）通过列出一个或多个主机，可以只允许该列表中的主机执行。如果存在来自另一个系统且进入某个主机的入站更新，请使用 `sources.hosts` 设置记录主机名。

另外，可以定义一个名为 `sources.` *resourceName* `.hosts` 的属性来控制将在何处运行资源的 Active Sync 任务。将 *resourceName* 替换为要指定的资源对象的名称。

使网关具有高可用性

Identity Manager 要求用轻量网关来管理不能直接从服务器访问的资源。这些资源包括需要执行特定于平台的客户端 API 调用的系统。例如，如果 Identity Manager 在基于 UNIX 的应用服务器上运行，则不可能对所管理的 NT 或 Active Directory 域进行 NTLM 或 ADSI 调用。由于 Identity Manager 需要用网关来管理这些资源，因此一定要确保使 Identity Manager Gateway 具有高可用性。

为了防止 Gateway 成为单个故障点，Sun 建议在多台计算机上运行 Gateway 实例。网络路由设备应当配置为在主 Gateway 实例终止时提供故障转移。应当针对粘性会话设置故障转移设备，并让故障转移设备使用一个简单的循环方案。请不要将 Gateway 放在负载平衡设备后面！因为该配置不受支持，而且将导致某些 Identity Manager 功能失败。

由 网关 管理的所有 Windows 域必须属于同一个林。不支持跨林边界管理域。如果您有多个林，请在每个林中至少安装一个 网关。

Win32 监视工具可以配置为在 Win32 主机上监视 gateway.exe 进程。如果 gateway.exe 失败，该进程会自动重新启动。

了解所建议的 HA 体系结构

下图显示在没有 Web 应用程序基础结构时，Sun 建议使用的 Identity Manager 体系结构。

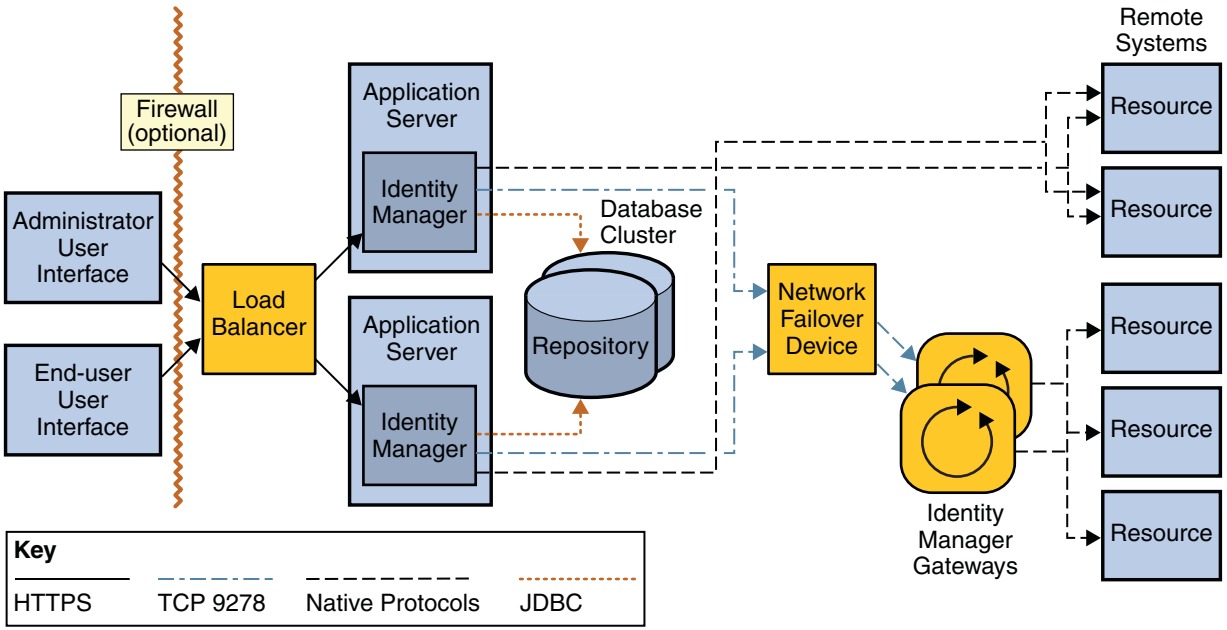

图 3–2 Identity Manager 高可用性体系结构

在实际部署中，应当尽可能充分利用现有的冗余应用服务器基础结构。此体系结构的价值在于它仅使用负载平衡器即可在应用服务器上实现冗余。具有会话关联的负载平衡器会检测失败的应用服务器实例并将其故障切换到活动实例。在 Web 环境中，负载平衡器还可以在服务器群集内分布用户请求，从而提供水平伸缩。

尽管这是一种简单的体系结构，但其运行时间特征能够与更复杂的部署媲美。由于该体系结构比较简单，因此需要维护和监视的软件更少，有可能失败的软件也会更少。由于人为错误是导致停机时间的首要原因，因此与更为复杂的解决方案相比，相对简单的解决方案可以实现更佳的运行时间特征。没有通用的正确答案。要点在于，了解导致停机时间的所有原因，并为您的投资选择将实现最佳可用性的体系结构。

注 – 不可能像对 Web 应用程序（如 Identity Manager）那样，描述所有不同的 HA 体系结构。

由于 Identity Manager 可以部署在各种可能的组合中，因此最经济的方法就是在部署 Identity Manager 时，确定现有的基础结构并尽可能充分利用它。

了解所建议的 Service Provider HA 体系结构

如果要利用 Identity Manager Service Provider 功能，Sun 建议您在用户层和应用层之间添加一个 Web 层。该 Web 层由一台或多台驻留在隔离区 (DMZ) 中的 Web 服务器组成，并由防火墙将其与应用层隔开。

如果要利用 Service Provider 功能，则需要使用 LDAP 系统信息库。如果 Identity Manager 仅支持外联网客户端，建议使用标准的 Identity Manager 系统信息库，但这不是必需的。否则，如果 Identity Manager 既支持内联网又支持外联网用户，则需要一个 LDAP 系统信息库和一个标准的 Identity Manager 系统信息库。

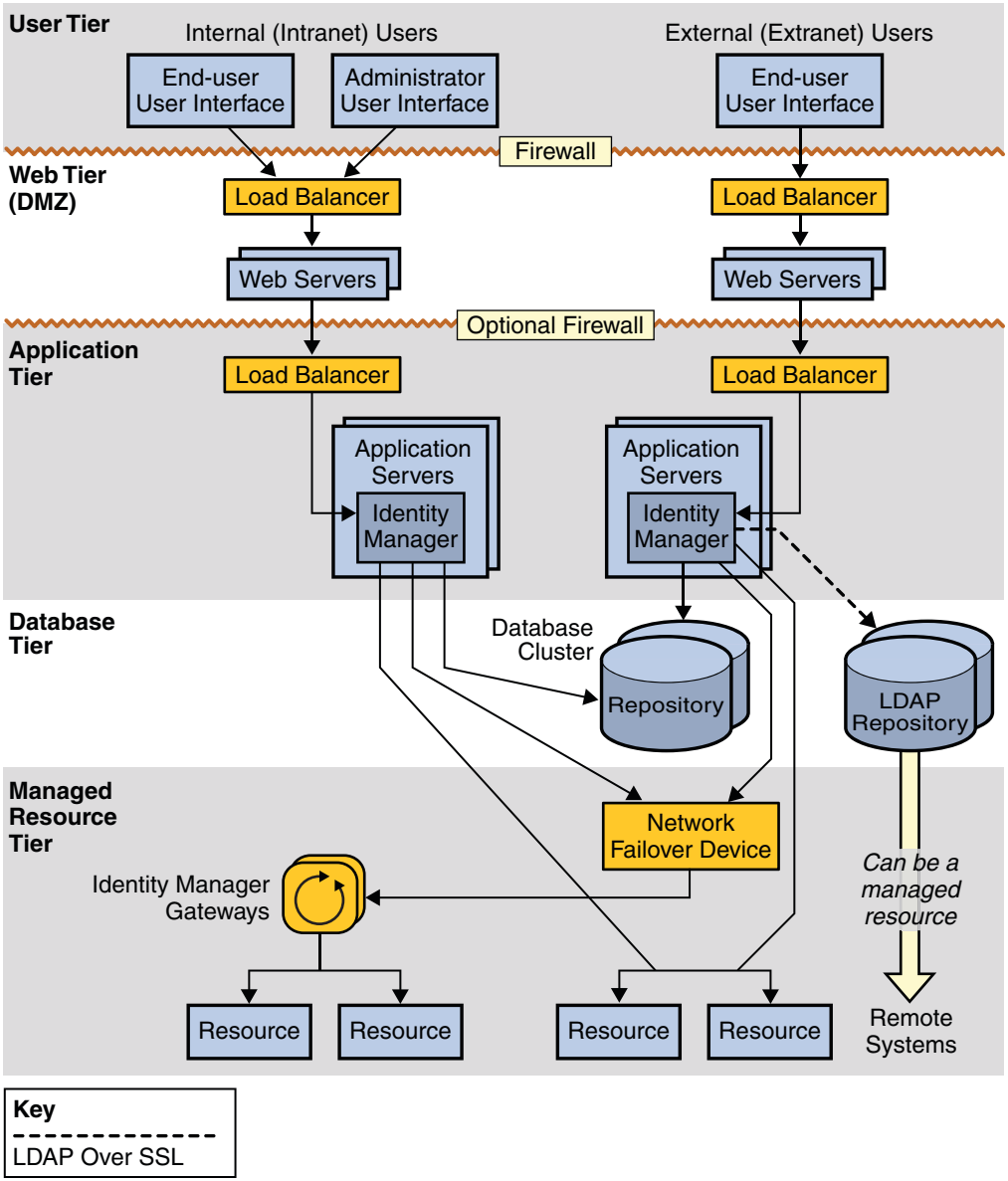

图 3–3 Identity Manager Service Provider 高可用性体系结构

了解故障方案

本节列出了八个故障方案，并对两个分别具有会话持久性和不具有会话持久性的部署进行了比较。

- **具有**会话持久性的部署跨负载平衡器具有会话关联。在该部署中，一个群集内有多个实例，在这些实例中打开了某种形式的会话持久性，以便将会话更改写入物理位置不同的系统信息库节点。
- **不具有**会话持久性的部署跨负载平衡器具有会话关联，它具有多个不属于一个群集的实例。

方案 1：无工作流的方案

方案描述

最终用户或管理员正在编辑不属于工作流的表单。最终用户已在其上建立会话的实例已关闭。

不具有会话持久性

用户体验：不透明的故障转移。在提交表单时，系统将用户返回到登录页面。

恢复步骤：用户重新输入其用户名和密码。Identity Manager 随后处理该表单并在用户登录之后立即将结果显示在下一页。

具有会话持久性

用户体验：用户无需注销和重新登录，即可提交表单并得到返回的结果。

恢复步骤：不需要用户执行任何操作。

该方案的其他示例

- 在实例关闭时，最终用户已经登录，而且已经检索为用户或其他系统信息库对象搜索的结果。
- 在实例关闭时，管理员将要使用管理员界面提交“重置密码”或“编辑用户”请求。

方案 2：工作流正在进行的方案

方案描述

最终用户或管理员提交了触发工作流的表单。正针对其执行工作流的实例通常就是存在用户会话的实例，但是在某些预定任务上，它们可能不是同一个。实例在工作流正在进行时关闭。

不具有会话持久性

用户体验：不透明的故障转移。在提交表单时，系统将用户返回到登录页面。正在执行的工作流任务实例应当位于系统信息库中，但是，由于执行节点已关闭，因此工作流状态将为“已终止”。

恢复步骤：必须再次提交工作流，方法是返回到同一表单，重新输入在节点失败之前用来触发工作流的信息。

在某些情况（但并非所有情况）下，提交同样的请求数据可能会起作用。如果在工作流执行期间将其置备给多个资源，而其中的一些资源在发生故障之前已经置备，则在用户重新提交工作流时将必须考虑“已经置备的”资源。请注意，已终止的工作流仍停留在系统信息库中，直到 `resultLimit` 在 `TaskInstance` 对象上过期为止。

具有会话持久性

用户体验：不透明的故障转移。不会将用户注销，因为用户的会话将得以保持并在新实例中重新建立。但是，在提交表单时可能会因工作流将被终止而导致错误。此故障转移是不透明的，因为需要执行恢复操作。

恢复步骤：与不具有会话持久性的模式相同。用户必须使用相同或经过修改的参数重新提交在先前的工作流中触发的请求。

该方案的其他示例

- 最终用户只要提交一个用来创建 Identity Manager 帐户的自行注册请求，该实例就关闭了。
- 管理员只要提交正在进行的“密码重置”请求，该实例就关闭了。

方案 3：工作流暂停或休眠方案

方案描述

此方案包括如下情况：工作流已启动，但是正在等待批准者手动执行操作。

不具有会话持久性

用户体验：故障转移相对于批准者是透明的，但前提是批准者尚未登录。在节点出现故障之后，当批准者登录时，批准者仍能够在其收件箱中看到批准请求，即使该请求是从已经关闭的节点触发也是如此。

恢复步骤：不需要用户执行任何操作。

具有会话持久性

用户体验：与不具有会话持久性的模式相同。

恢复步骤：与不具有会话持久性的模式相同。

该方案的其他示例

- 工作流处于休眠状态，例如，在员工授权生效或失效日期之前处于休眠状态的手动操作。
- 管理员提交了一个正在等待批准者登录和批准的用户创建请求。在批准者批准该请求之前，从中发送该请求的节点发生故障。

方案 4：工作项目编辑方案

方案描述

此方案包括如下情况：用户正在编辑一个工作项目，在提交该工作项目之前，用户在其中具有会话的节点关闭。

不具有会话持久性

用户体验：不透明的故障转移。在提交了工作项目编辑表单之后，系统将用户注销并返回到登录页面。

恢复步骤：在重新提交登录凭据时，用户的工作项目被标记为已完成，而且工作流能够从那时继续执行。该工作流应当由新模式拾取并从用户的手动操作被标记为已完成时开始执行。

具有会话持久性

用户体验：在提交了工作项目编辑表单之后，用户看到其提交操作的结果，例如，自定义工作流中的下一个表单（如果有的话）或者指示成功的消息。

恢复步骤：不需要用户执行任何操作。

该方案的其他示例

- 最终用户正在填写与自定义工作流中的手动操作（例如，请求对特定资源的访问权限）相关联的表单。在用户提交请求之前，用户在其中具有会话的节点已终止。
- 管理员已经登录 Identity Manager 并且已经打开了要编辑的批准请求。在提交请求之前，管理员在其中具有会话的节点已出现故障。

方案 5：预定任务正在进行的方案

方案描述

这些方案包括如下情况：在正在进行协调或者正在执行报告时，节点出现故障。

不具有会话持久性

用户体验：预定的任务正在被终止。

恢复步骤：必须重新启动正在进行的预定任务。该任务必须从头开始启动。（该任务将不会从出现故障的时间点重新启动。）这与创建和启动新任务相同。

具有会话持久性

用户体验：与不具有会话持久性的模式相同。

恢复步骤：与不具有会话持久性的模式相同。

该方案的其他示例

- Active Sync 适配器配置为在故障节点上运行。

方案 6：预定任务暂停方案

方案描述

这些方案包括如下情况：用户的自定义工作流已经预定了一个日后在特定节点上执行的任务。在到达预定日期之前，预定在其上运行该任务的节点出现故障。

不具有会话持久性

用户体验：故障转移对于确保此任务在其预定时间执行而必须采取的恢复操作是透明的。

恢复步骤：在到达预定的执行时间时，预定任务由任何活动节点拾取。

具有会话持久性

用户体验：与不具有会话持久性的模式相同。

恢复步骤：与不具有会话持久性的模式相同。

该方案的其他示例

- 在创建用户帐户的过程中，使用延迟任务扫描程序实施如下功能：针对生效日期启用该帐户，或者针对失效日期禁用该帐户。在到达生效日期或失效日期之前，预定在其上运行该任务的节点出现故障。
- 预定在将来的时间运行报告，或者预定在某个特定时间运行协调操作，但是，在该时间到达之前，预定运行该任务的节点出现故障。

方案 7：Web 服务工作流请求尚未由 Identity Manager 接收的方案

方案描述

这些方案包括如下情况：Identity Manager GUI 不用于启动置备功能。相反，该用户界面由使用 SPML 或其他自定义 Web 服务接口在内部调用 Identity Manager 的应用程序提供。在这里，与通过用户界面进入的用户有关的用户会话借助于调用应用程序来管理。对于 Identity Manager，请求均作为“soapadmin”主体来启动。

在类似的使用案例中，此故障方案包括如下情况：在经由 Identity Manager 端点的请求尚未接收时，目标节点出现故障。

不具有会话持久性

用户体验：透明的故障转移。对于每个 SOAP 请求来说，SOAP 管理员的凭据通过有线通信或者通过 `Waveset.properties` 设置在 Identity Manager 中传入。只要将要接收此 SOAP 请求的节点在关闭之前尚未收到请求，则无论具有或不具有会话持久性，故障转移都是透明的。

恢复步骤：不需要执行任何操作。SOAP 请求发送到执行它的实时节点。

具有会话持久性

用户体验：与不具有会话持久性的模式相同。

恢复步骤：与不具有会话持久性的模式相同。

方案 8：Web 服务工作流请求正在由 Identity Manager 进行的方案

方案描述

此方案与方案 7 类似。二者唯一的区别在于，在方案 8 中，当节点出现故障时，工作流正在进行；在方案 7 中，当节点出现故障时，节点尚未收到 SOAP 请求。

不具有会话持久性

用户体验：此方案与方案 2（工作流正在进行）相似。工作流被标记为已终止，用户看到一个因 SOAP 请求产生的错误。

恢复步骤：用户必须使用相似的或经过修改的参数（基于故障出现在工作流中的位置），通过第三方应用程序中的用户界面重新提交表单。

具有会话持久性

用户体验：与不具有会话持久性的模式相同。

恢复步骤：与不具有会话持久性的模式相同。

与会话关联和会话持久性有关的常见问题解答

在对应用服务器水平伸缩时，是否应当启用会话关联？

是。

在对应用服务器水平伸缩时，是否应当使用会话持久性？

除非您的业务要求特别强调在会话持久性会产生影响的有限情况下实施透明故障转移，否则 Sun 不建议使用会话持久性。会话持久性具有其自己的性能开销，除非您的业务要求确实需要透明的故障转移，否则请关闭会话持久性。

在研究第 29 页中的 “了解故障方案”中记录的八个故障方案后就会发现，在其中的六个方案中，无论是否启用了业务持久性，最终用户体验或所需的恢复操作没有任何区别。只有在方案 1 和方案 4 中，具有会话持久性的方案才会与没有会话持久性的方案有区别。

在这两个方案中，会话持久性可以提供故障转移透明性，但会话持久性会降低性能。根据会话对象的大小、用于会话持久性的系统信息库以及对于特定应用服务器的会话管理代码的优化，性能开销可能会从 10% 到 20% 或更高。

在水平伸缩时，一个群集内是否应当有多个应用服务器实例？

除非您需要会话持久性，否则并不是绝对需要多个应用服务器实例。即使所有的应用服务器节点都不在一个群集内，也可以实现不具有会话持久性的故障转移。