Unified Manager

SANtricity 11.8

NetApp
January 31, 2025

目录

使用Unified Manager 6进行多阵列管理

主接口

Unified Manager界面概述

Unified Manager是一个基于Web的界面、可用于在一个视图中管理多个存储阵列。

主页

登录到Unified Manager后、主页将打开*管理-全部*。在此页面中、您可以滚动浏览网络中发现的存储阵列列表、查看其状态、并对单个阵列或一组阵列执行操作。

导航边栏

您可以从导航边栏访问Unified Manager的特性和功能。

区域	说明
管理	发现网络中的存储阵列、为阵列启动SANtricity System Manager、将设置从一个阵列导入到多个阵列以及管理阵列组。选中阵列名称旁边的复选框以对其执行操作、例如导入设置和创建阵列组。每行末尾的省略号提供了一个在线菜单、用于对单个阵列执行操作、例如重命名该阵列。
操作	查看批处理操作的进度、例如将设置从一个阵列导入到另一个阵列。 当存储阵列处于非最佳状态时、某些操作不可用。
证书管理	管理证书以在浏览器和客户端之间进行身份验证。
访问管理	为Unified Manager界面建立用户身份验证。
支持	查看技术支持选项、资源和联系人。

接口设置和帮助

在界面的右上角、您可以访问帮助和其他文档。您还可以访问管理选项、这些选项可从您的登录名旁边的下拉列表中找到。

用户登录和密码

登录到系统的当前用户显示在界面的右上角。

有关用户和密码的详细信息、请参见：

- "设置管理员密码保护"

- "更改管理员密码"
- "更改本地用户配置文件的密码"

支持的浏览器

Unified Manager可从多种类型的浏览器进行访问。

支持以下浏览器和版本。

浏览器	最低版本
Google Chrome	89
Mozilla Firefox	80
Safari	14
Microsoft Edge	90

Web服务代理必须已安装并可供浏览器使用。

设置管理员密码保护

您必须为Unified Manager配置管理员密码、以防止其遭受未经授权的访问。

管理员密码和用户配置文件

首次启动Unified Manager时、系统会提示您设置管理员密码。具有管理员密码的任何用户都可以对存储阵列进行配置更改。

除了管理员密码之外、Unified Manager界面还包括预先配置的用户配置文件、其中包含一个或多个映射到这些配置文件的角色。有关详细信息，请参见 "访问管理的工作原理"。

无法更改用户和映射。只能修改密码。要更改密码、请参见：

- "更改管理员密码"
- "更改本地用户配置文件的密码"

会话超时

在单个管理会话期间、软件仅会提示您输入密码一次。默认情况下、会话在30分钟处于非活动状态后超时、此时您必须再次输入密码。如果另一个用户从另一个管理客户端访问软件并在会话期间更改了密码、则在下次尝试配置操作或查看操作时、系统会提示您输入密码。

出于安全原因、您只能在软件进入"锁定"状态之前尝试输入五次密码。在此状态下、软件将拒绝后续的密码尝试。您必须等待10分钟才能重置为"正常"状态、然后才能再次尝试输入密码。

您可以调整会话超时、也可以完全禁用会话超时。有关详细信息，请参见 "管理会话超时"。

更改管理员密码

您可以更改用于访问Unified Manager的管理员密码。

开始之前

- 您必须以本地管理员身份登录、其中包括root管理员权限。
- 您必须知道当前的管理员密码。

关于此任务

选择密码时、请记住以下准则：

- 密码区分大小写。
- 设置密码时、不会从密码中删除尾随空格。如果密码中包含空格、请小心操作。
- 为了提高安全性、请至少使用15个字母数字字符并频繁更改密码。

步骤

1. 选择菜单：设置[访问管理]。
2. 选择*本地用户角色*选项卡。
3. 从表中选择*管理员*用户。

   更改密码按钮将变为可用。

4. 选择 * 更改密码 * 。

   此时将打开更改密码对话框。

5. 如果未为本地用户密码设置最小密码长度、请选中此复选框以要求用户输入密码以访问系统。
6. 在两个字段中输入新密码。
7. 输入本地管理员密码以确认此操作、然后单击*更改*。

管理会话超时

您可以为Unified Manager配置超时、以便用户非活动会话在指定时间后断开连接。

关于此任务

默认情况下、Unified Manager的会话超时为30分钟。您可以调整该时间、也可以完全禁用会话超时。

如果使用阵列中嵌入的安全断言标记语言(SAML)功能配置访问管理、则当用户的SSO会话达到其最大限制时、可能会发生会话超时。可能会在System Manager会话超时之前发生这种情况。

步骤

1. 从菜单栏中、选择用户登录名旁边的下拉箭头。
2. 选择*启用/禁用会话超时*。

   此时将打开启用/禁用会话超时对话框。

3. 使用spinner控件以分钟为单位增加或减少时间。

   您可以设置的最小超时时间为15分钟。

   要禁用会话超时、请清除*设置时间长度…*复选框。

4. 单击 * 保存 * 。

存储阵列

发现概述

要管理存储资源、您必须先发现网络中的存储阵列。

如何发现阵列?

使用"添加/发现"页面查找并添加要在组织网络中管理的存储阵列。您可以发现多个阵列、也可以发现一个阵列。为此、您需要输入网络IP地址、然后Unified Manager将尝试单独连接到该范围中的每个IP地址。

了解更多信息。

- "发现阵列的注意事项"
- "发现多个存储阵列"
- "发现单个阵列"

如何管理阵列?

发现阵列后、转到*管理-全部*页面。在此页面中、您可以滚动浏览网络中发现的存储阵列列表、查看其状态、并对单个阵列或一组阵列执行操作。

如果要管理单个阵列、可以将其选中并打开System Manager。

了解更多信息。

- "访问System Manager的注意事项"
- "管理单个存储阵列"
- "查看存储阵列状态"

概念

发现阵列的注意事项

Unified Manager必须先发现要在组织网络中管理的存储阵列、然后才能显示和管理存储资源。您可以发现多个阵列、也可以发现一个阵列。

发现多个存储阵列

如果您选择发现多个阵列、请输入一个网络IP地址范围、然后Unified Manager将尝试单独连接到该范围中的每个IP地址。任何已成功访问的存储阵列都会显示在"Discover "页面上、并且可能会添加到您的管理域中。

发现单个存储阵列

如果您选择发现单个阵列、则输入存储阵列中一个控制器的单个IP地址、然后添加单个存储阵列。

Unified Manager只会发现并显示分配给控制器的范围内的单个IP地址或IP地址。如果为这些控制器分配的备用控制器或IP地址不在此单个IP地址或IP地址范围内、则Unified Manager将不会发现或显示它们。但是、添加存储阵列后、所有关联的IP地址都将被发现并显示在管理视图中。

用户凭据

在发现过程中、您必须为要添加的每个存储阵列提供管理员密码。

Web服务证书

在发现过程中、Unified Manager会验证发现的存储阵列是否正在使用受信任源的证书。Unified Manager对与浏览器建立的所有连接使用两种基于证书的身份验证：

- 可信证书

  对于Unified Manager发现的阵列、您可能需要安装证书颁发机构提供的其他受信任证书。

  使用*导入*按钮导入这些证书。如果您之前已连接到此阵列、则一个或两个控制器证书要么已过期、已撤销、要么在其证书链中缺少根证书或中间证书。在管理存储阵列之前、您必须替换已过期或已撤销的证书、或者添加缺少的根证书或中间证书。

- 自签名证书

  也可以使用自签名证书。如果管理员尝试在未导入签名证书的情况下发现阵列、则Unified Manager将显示一个错误对话框、允许管理员接受自签名证书。存储阵列的自签名证书将标记为可信、存储阵列将添加到Unified Manager中。

  如果您不相信与存储阵列的连接、请选择*取消*并验证存储阵列的安全证书策略、然后再将存储阵列添加到Unified Manager。

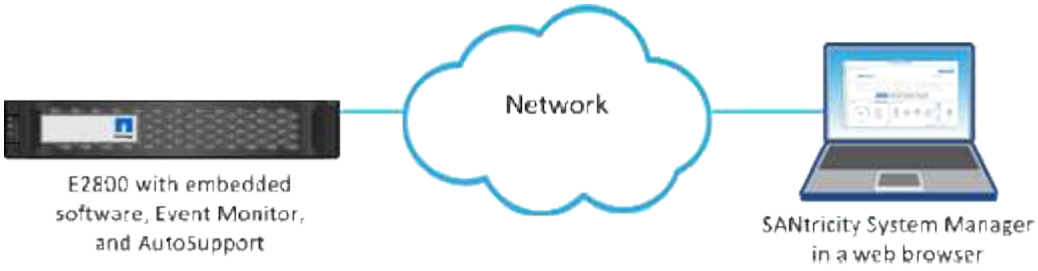
访问**System Manager**的注意事项

如果要配置和管理存储阵列、请选择一个或多个存储阵列并使用Launch选项打开System Manager。

System Manager是控制器上的嵌入式应用程序、它通过以太网管理端口连接到网络。它包括所有基于阵列的功能。

要访问System Manager、您必须具备：

- 此处列出的阵列型号之一："E 系列硬件概述"
- 使用Web浏览器与网络管理客户端的带外连接。



发现阵列

发现多个存储阵列

您可以发现多个阵列、以检测管理服务器所在子网中的所有存储阵列、并自动将发现的阵列添加到管理域中。

开始之前

- 您必须使用具有安全管理员权限的用户配置文件登录。
- 必须正确设置和配置存储阵列。
- 存储阵列密码必须使用System Manager的"访问管理"图块进行设置。
- 要解析不可信的证书、您必须拥有证书颁发机构(CA)提供的可信证书文件、并且证书文件可在本地系统上使用。

发现阵列是一种多步骤操作步骤。

第1步：输入网络地址

您可以输入一个网络地址范围、以便在本地子网络中搜索。任何已成功访问的存储阵列都会显示在"Discover "页面上、并且可能会添加到您的管理域中。

如果出于任何原因需要停止发现操作、请单击*停止发现*。

步骤

1. 在 Manage 页面中，选择 * 添加 / 发现 * 。

   此时将显示添加/发现对话框。

2. 选择*发现网络范围内的所有存储阵列*单选按钮。
3. 输入起始网络地址和结束网络地址以在本地子网络中搜索、然后单击*开始发现*。

   发现过程将启动。完成此发现过程可能需要几分钟时间。发现存储阵列时、会填充"发现"页面上的表。

   如果未发现任何可管理的阵列，请验证这些存储阵列是否已正确连接到您的网络，以及其分配的地址是否在范围内。单击 * 新发现参数 * 以返回到 " 添加 / 发现 " 页面。

4. 查看已发现的存储阵列列表。
5. 选中要添加到管理域的任何存储阵列旁边的复选框、然后单击*下一步*。

   Unified Manager会对要添加到管理域的每个阵列执行凭据检查。您可能需要解析与该阵列关联的任何自签名

证书和不可信证书。

6. 单击 * 下一步 * 继续执行向导中的下一步。

第2步：在发现期间解析自签名证书

在发现过程中、系统会验证存储阵列是否正在使用受信任源的证书。

步骤

1. 执行以下操作之一：
   - 如果您信任与发现的存储阵列的连接、请继续访问向导中的下一个卡。自签名证书将标记为可信证书、存储阵列将添加到Unified Manager中。
   - 如果您不相信与存储阵列的连接、请选择*取消*并验证每个存储阵列的安全证书策略、然后再将其中任何一个添加到Unified Manager。
2. 单击 * 下一步 * 继续执行向导中的下一步。

第3步：在发现期间解析不可信的证书

如果存储阵列尝试建立与Unified Manager的安全连接、但此连接无法确认为安全连接、则会发生不可信证书。在阵列发现过程中、您可以通过导入可信第三方颁发的证书颁发机构(CA)证书(或CA签名证书)来解析不可信的证书。

如果满足以下任一条件、您可能需要安装其他受信任的CA证书：

- 您最近添加了一个存储阵列。
- 一个或两个证书均已过期。
- 一个或两个证书均已撤销。
- 一个或两个证书缺少根证书或中间证书。

步骤

1. 选中要为其解析不可信证书的任何存储阵列旁边的复选框、然后选择"*导入"*按钮。

   此时将打开一个对话框、用于导入可信证书文件。

2. 单击*浏览*以选择存储阵列的证书文件。

   文件名显示在对话框中。

3. 单击 * 导入 * 。

   这些文件将上传并进行验证。

   如果任何存储阵列存在未解决的不可信证书问题、则不会添加到Unified Manager中。

4. 单击 * 下一步 * 继续执行向导中的下一步。

第4步：提供密码

您必须输入要添加到管理域的存储阵列的密码。

步骤

1. 输入要添加到Unified Manager的每个存储阵列的密码。
2. *可选：*将存储阵列与组关联：从下拉列表中、选择要与选定存储阵列关联的所需组。
3. 单击 * 完成 * 。

完成后

存储阵列将添加到管理域中并与选定组(如果指定)关联。

Unified Manager连接到指定存储阵列可能需要几分钟的时间。

发现单个阵列

使用添加/发现单个存储阵列选项手动发现单个存储阵列并将其添加到组织的网络中。

开始之前

- 必须正确设置和配置存储阵列。
- 存储阵列密码必须使用System Manager的"访问管理"图块进行设置。

步骤

1. 在 Manage 页面中，选择 * 添加 / 发现 * 。

   此时将显示添加/发现对话框。

2. 选择*发现单个存储阵列*单选按钮。
3. 输入存储阵列中某个控制器的IP地址、然后单击*启动发现*。

   Unified Manager连接到指定存储阵列可能需要几分钟的时间。

   如果无法连接到指定控制器的IP地址、则会显示"Storage Array not accessible"消息。

4. 如果出现提示、请解析任何自签名证书。

   在发现过程中、系统会验证发现的存储阵列是否正在使用受信任源的证书。如果找不到存储阵列的数字证书、则会提示您通过添加安全异常来解析未由可识别证书颁发机构(CA)签名的证书。

5. 如果出现提示、请解析任何不可信的证书。

   如果存储阵列尝试建立与Unified Manager的安全连接、但此连接无法确认为安全连接、则会发生不可信证书。通过导入可信第三方颁发的证书颁发机构(CA)证书来解析不可信证书。

6. 单击 * 下一步 * 。
7. *可选：*将发现的存储阵列与组相关联：从下拉列表中、选择要与该存储阵列关联的所需组。

   默认情况下、系统会选择"all"组。

8. 输入要添加到管理域的存储阵列的管理员密码、然后单击*确定*。

完成后

存储阵列将添加到Unified Manager中、如果指定此阵列、则还会添加到选定的组中。

如果启用了自动支持数据收集、则会自动收集您添加的存储阵列的支持数据。

管理阵列

查看存储阵列状态

Unified Manager将显示已发现的每个存储阵列的状态。

转到*管理-全部*页面。在此页面中、您可以查看Web服务代理与该存储阵列之间的连接状态。

下表介绍了状态指示灯。

状态	表示
最佳	存储阵列处于最佳状态。没有证书问题、密码有效。
密码无效	提供的存储阵列密码无效。
不可信证书	与存储阵列的一个或多个连接不可信、因为HTTPS证书是自签名的、尚未导入、或者证书是CA签名的、并且根和中间CA证书尚未导入。
需要关注	存储阵列存在问题、需要您进行干预才能进行更正。
锁定	存储阵列处于已锁定状态。
未知	从未联系过存储阵列。如果Web服务代理正在启动且尚未与存储阵列进行联系、或者存储阵列处于脱机状态且自Web服务代理启动以来从未进行过联系、则可能会发生这种情况。
脱机	Web服务代理先前已与存储阵列联系、但现在已断开与该存储阵列的所有连接。

管理单个存储阵列

如果要执行管理操作、您可以使用Launch选项为一个或多个存储阵列打开基于浏览器的System Manager。

步骤

1. 从管理页面中、选择要管理的一个或多个存储阵列。
2. 单击 * 启动 * 。

   系统将打开一个新窗口并显示System Manager登录页面。

3. 输入用户名和密码、然后单击*登录*。

更改存储阵列密码

您可以在Unified Manager中更新用于查看和访问存储阵列的密码。

开始之前

- 您必须使用包含存储管理员权限的用户配置文件登录。
- 您必须知道在System Manager中设置的存储阵列的当前密码。

关于此任务

在此任务中、您可以输入存储阵列的当前密码、以便在Unified Manager中访问该密码。如果在System Manager中更改了阵列密码、并且现在还必须在Unified Manager中更改该密码、则可能需要执行此操作。

步骤

1. 从管理页面中、选择一个或多个存储阵列。
2. 选择菜单：不常见任务(提供存储阵列密码)。
3. 输入每个存储阵列的密码、然后单击*保存*。

从**SANtricity** 统一管理器中删除存储阵列

如果您不想再从Unified Manager管理一个或多个存储阵列、可以将其删除。

关于此任务

您无法访问所删除的任何存储阵列。但是、您可以通过将浏览器直接指向已删除的任何存储阵列的IP地址或主机名来建立与此阵列的连接。

删除存储阵列不会以任何方式影响存储阵列或其数据。如果意外删除了存储阵列、则可以重新添加该存储阵列。

步骤

1. 选择*管理*页面。
2. 选择要删除的一个或多个存储阵列。
3. 选择菜单：不常见任务[删除存储阵列]。

   存储阵列将从SANtricity Unified Manager的所有视图中删除。

设置导入

设置导入概述

通过导入设置功能、您可以执行批量操作、将设置从一个阵列导入到多个阵列。当您需要在网络中配置多个阵列时、此功能可以节省时间。

可以导入哪些设置?

您可以导入警报方法、AutoSupport 配置、目录服务配置、存储配置(例如卷组和池)和系统设置(例如自动负载平衡)。

了解更多信息。

- "导入设置的工作原理"
- "复制存储配置的要求"

如何执行批量导入?

在要用作源的存储阵列上、打开System Manager并配置所需的设置。然后从Unified Manager中、转到"管理"页面并将设置导入到一个或多个阵列。

了解更多信息。

- "导入警报设置"
- "导入AutoSupport 设置"
- "导入目录服务设置"
- "导入存储配置设置"
- "导入系统设置"

概念

导入设置的工作原理

您可以使用Unified Manager将设置从一个存储阵列导入到多个存储阵列。导入设置功能是一个批处理操作、当您需要在网络中配置多个阵列时、可以节省时间。

可用于导入的设置

可以将以下配置导入到多个阵列：

- 警报-使用电子邮件、系统日志服务器或SNMP服务器向管理员发送重要事件的警报方法。
- * AutoSupport *—一种用于监控存储阵列运行状况并向技术支持发送自动派单的功能。
- 目录服务—一种通过LDAP (轻型目录访问协议)服务器和目录服务(例如Microsoft的Active Directory)管理的用户身份验证方法。
- 存储配置—与以下内容相关的配置：
  - 卷(仅限厚存储库卷和非存储库卷)
  - 卷组和池
  - 热备用驱动器分配
- 系统设置-与以下内容相关的配置：
  - 卷的介质扫描设置

- SSD 设置
- 自动负载平衡(不包括主机连接报告)

配置工作流

要导入设置、请按照以下工作流进行操作：

1. 在要用作源的存储阵列上、使用System Manager配置设置。
2. 在要用作目标的存储阵列上、使用System Manager备份其配置。
3. 在Unified Manager中、转到*管理*页面并导入设置。
4. 在*操作*页面中、查看导入设置操作的结果。

复制存储配置的要求

在将存储配置从一个存储阵列导入到另一个存储阵列之前、请查看相关要求和准则。

磁盘架

- 源阵列和目标阵列上控制器所在的磁盘架必须相同。
- 源阵列和目标阵列上的磁盘架ID必须相同。
- 扩展架必须使用相同驱动器类型填充到相同插槽中(如果在配置中使用驱动器、则未使用驱动器的位置无关紧要)。

控制器

- 源阵列和目标阵列的控制器类型可以不同(例如、从E2800导入到E5700)、但RVOD机箱类型必须相同。
- 源阵列和目标阵列之间的HIC (包括主机的DA功能)必须相同。
- 不支持从双工导入到单工配置；但是、允许从单工导入到双工。
- FDE设置不包括在导入过程中。

状态

- 目标阵列必须处于最佳状态。
- 源阵列无需处于最佳状态。

存储

- 只要目标阵列上的卷容量大于源阵列、驱动器容量可能会因源阵列和目标阵列而异。(目标阵列可能具有容量更大的较新驱动器、这些驱动器无法通过复制操作完全配置到卷中。)
- 源阵列上64 TB或更大的磁盘池卷将阻止目标上的导入过程。
- 导入过程不包括精简卷。

使用批量导入

导入警报设置

您可以将警报配置从一个存储阵列导入到其他存储阵列。当您需要在网络中配置多个阵列时、此批处理操作可以节省时间。

开始之前

- 系统会在System Manager中为要用作源的存储阵列配置警报(菜单：设置[警报])。
- 目标存储阵列的现有配置会在System Manager中进行备份(菜单：设置[系统>保存存储阵列配置])。

关于此任务

您可以为导入操作选择电子邮件、SNMP或系统日志警报。导入的设置包括：

- 电子邮件警报-邮件服务器地址和警报收件人的电子邮件地址。
- 系统日志警报—系统日志服务器地址和UDP端口。
- * SNMP警报*- SNMP服务器的社区名称和IP地址。

步骤

1. 在管理页面中、单击*导入设置*。

   此时将打开导入设置向导。

2. 在选择设置对话框中、选择*电子邮件警报*、* SNMP警报*或*系统日志警报*、然后单击*下一步*。

   此时将打开一个对话框、用于选择源阵列。

3. 在选择源对话框中、选择包含要导入的设置的阵列、然后单击*下一步*。
4. 在选择目标对话框中、选择一个或多个阵列以接收新设置。

   固件低于8.50的存储阵列不可供选择。此外、如果Unified Manager无法与该阵列进行通信(例如、阵列处于脱机状态或存在证书、密码或网络问题)、则该阵列不会显示在此对话框中。

5. 单击 * 完成 * 。

   操作页面将显示导入操作的结果。如果操作失败、您可以单击其行以查看更多信息。

结果

现在、目标存储阵列已配置为通过电子邮件、SNMP或系统日志向管理员发送警报。

导入**AutoSupport** 设置

您可以将AutoSupport 配置从一个存储阵列导入到其他存储阵列。当您需要在网络中配置多个阵列时、此批处理操作可以节省时间。

开始之前

- 已在System Manager中为要用作源的存储阵列配置AutoSupport (菜单：Support[支持中心])。
- 目标存储阵列的现有配置会在System Manager中进行备份(菜单：设置[系统>保存存储阵列配置])。

关于此任务

导入的设置包括不同的功能(基本AutoSupport 、AutoSupport OnDemand和远程诊断)、维护窗口、交付方法、和派单计划。

步骤

1. 在管理页面中、单击*导入设置*。

   此时将打开导入设置向导。

2. 在选择设置对话框中、选择* AutoSupport 、然后单击*下一步。

   此时将打开一个对话框、用于选择源阵列。

3. 在选择源对话框中、选择包含要导入的设置的阵列、然后单击*下一步*。
4. 在选择目标对话框中、选择一个或多个阵列以接收新设置。

   固件低于8.50的存储阵列不可供选择。此外、如果Unified Manager无法与该阵列进行通信(例如、阵列处于脱机状态或存在证书、密码或网络问题)、则该阵列不会显示在此对话框中。

5. 单击 * 完成 * 。

   操作页面将显示导入操作的结果。如果操作失败、您可以单击其行以查看更多信息。

结果

现在、目标存储阵列配置了与源阵列相同的AutoSupport 设置。

导入目录服务设置

您可以将目录服务配置从一个存储阵列导入到其他存储阵列。当您需要在网络中配置多个阵列时、此批处理操作可以节省时间。

开始之前

- 在System Manager中为要用作源的存储阵列配置了目录服务(菜单：设置[访问管理])。
- 目标存储阵列的现有配置会在System Manager中进行备份(菜单：设置[系统>保存存储阵列配置])。

关于此任务

导入的设置包括LDAP (轻型目录访问协议)服务器的域名和URL、以及LDAP服务器用户组与存储阵列预定义角色的映射。

步骤

1. 在管理页面中、单击*导入设置*。

   此时将打开导入设置向导。

2. 在选择设置对话框中、选择*目录服务*、然后单击*下一步*。

   此时将打开一个对话框、用于选择源阵列。

3. 在选择源对话框中、选择包含要导入的设置的阵列、然后单击*下一步*。
4. 在选择目标对话框中、选择一个或多个阵列以接收新设置。

   固件低于8.50的存储阵列不可供选择。此外、如果Unified Manager无法与该阵列进行通信(例如、阵列处于脱机状态或存在证书、密码或网络问题)、则该阵列不会显示在此对话框中。

5. 单击 * 完成 * 。

   操作页面将显示导入操作的结果。如果操作失败、您可以单击其行以查看更多信息。

结果

现在、目标存储阵列配置了与源阵列相同的目录服务。

导入系统设置

您可以将系统配置从一个存储阵列导入到其他存储阵列。当您需要在网络中配置多个阵列时、此批处理操作可以节省时间。

开始之前

- 系统设置在System Manager中为要用作源的存储阵列配置。
- 目标存储阵列的现有配置会在System Manager中进行备份(菜单：设置[系统>保存存储阵列配置])。

关于此任务

导入的设置包括卷的介质扫描设置、控制器的SSD设置和自动负载平衡(不包括主机连接报告)。

步骤

1. 在管理页面中、单击*导入设置*。

   此时将打开导入设置向导。

2. 在选择设置对话框中、选择*系统*、然后单击*下一步*。

   此时将打开一个对话框、用于选择源阵列。

3. 在选择源对话框中、选择包含要导入的设置的阵列、然后单击*下一步*。
4. 在选择目标对话框中、选择一个或多个阵列以接收新设置。

   固件低于8.50的存储阵列不可供选择。此外、如果Unified Manager无法与该阵列进行通信(例如、阵列处于脱机状态或存在证书、密码或网络问题)、则该阵列不会显示在此对话框中。

5. 单击 * 完成 * 。

   操作页面将显示导入操作的结果。如果操作失败、您可以单击其行以查看更多信息。

结果

现在、目标存储阵列配置了与源阵列相同的系统设置。

导入存储配置设置

您可以将存储配置从一个存储阵列导入到其他存储阵列。当您需要在网络中配置多个阵列时、此批处理操作可以节省时间。

开始之前

- 已在SANtricity 系统管理器中为要用作源的存储阵列配置存储。
- 目标存储阵列的现有配置会在System Manager中进行备份(菜单：设置[系统>保存存储阵列配置])。
- 源阵列和目标阵列必须满足以下要求：
  - 控制器所在的磁盘架必须相同。
  - 磁盘架ID必须相同。
  - 扩展架必须使用相同类型的驱动器填充到相同的插槽中。
  - RVOD机箱类型必须相同。
  - HIC (包括主机的数据保证功能)必须相同。
  - 目标阵列必须处于最佳状态。
  - 目标阵列上的卷容量大于源阵列的容量。
- 您了解以下限制：
  - 不支持从双工导入到单工配置；但是、允许从单工导入到双工。
  - 源阵列上64 TB或更大的磁盘池卷将阻止目标上的导入过程。
  - 导入过程不包括精简卷。

关于此任务

导入的设置包括已配置的卷(仅限厚存储库卷和非存储库卷)、卷组、池和热备用驱动器分配。

步骤

1. 在管理页面中、单击*导入设置*。

   此时将打开导入设置向导。

2. 在选择设置对话框中、选择*存储配置*、然后单击*下一步*。

   此时将打开一个对话框、用于选择源阵列。

3. 在选择源对话框中、选择包含要导入的设置的阵列、然后单击*下一步*。
4. 在选择目标对话框中、选择一个或多个阵列以接收新设置。

   固件低于8.50的存储阵列不可供选择。此外、如果Unified Manager无法与该阵列进行通信(例如、阵列处于脱机状态或存在证书、密码或网络问题)、则该阵列不会显示在此对话框中。

5. 单击 * 完成 * 。

   操作页面将显示导入操作的结果。如果操作失败、您可以单击其行以查看更多信息。

结果

现在、目标存储阵列配置了与源阵列相同的存储配置。

常见问题解答

将导入哪些设置?

导入设置功能是一个批处理操作、可将配置从一个存储阵列加载到多个存储阵列。在此操作期间导入的设置取决于源存储阵列在System Manager中的配置方式。

可以将以下设置导入到多个存储阵列：

- 电子邮件警报-设置包括邮件服务器地址和警报收件人的电子邮件地址。
- 系统日志警报-设置包括系统日志服务器地址和UDP端口。
- * SNMP警报*-设置包括SNMP服务器的社区名称和IP地址。
- * AutoSupport *—设置包括不同的功能(基本AutoSupport 、AutoSupport OnDemand和远程诊断)、维护窗口、交付方法、 和派单计划。
- 目录服务—配置包括LDAP (轻型目录访问协议)服务器的域名和URL、以及LDAP服务器用户组与存储阵列预定义角色的映射。
- 存储配置—配置包括卷(仅厚卷和非存储库卷)、卷组、池和热备用驱动器分配。
- 系统设置-配置包括卷的介质扫描设置、控制器的SSD缓存以及自动负载平衡(不包括主机连接报告)。

为什么我看不到所有存储阵列?

在导入设置操作期间、某些存储阵列可能在目标选择对话框中不可用。

存储阵列可能不会显示、原因如下：

- 固件版本低于8.50。
- 存储阵列已脱机。
- 系统无法与该阵列进行通信(例如、该阵列存在证书、密码或网络问题)。

阵列组

组概述

在管理组页面中、您可以创建一组存储阵列组、以便于管理。

什么是阵列组?

您可以通过对一组存储阵列进行分组来管理物理和虚拟化基础架构。您可能希望对存储阵列进行分组、以便更轻松地运行监控或报告作业。

组类型有两种：

- 所有组-所有组是默认组、其中包括在您的组织中发现的所有存储阵列。可以从主视图访问所有组。
- 用户创建的组-用户创建的组包含您手动选择添加到该组的存储阵列。可以从主视图访问用户创建的组。

如何配置组?

在管理组页面中、您可以创建一个组、然后向该组添加阵列。

了解更多信息。

- "配置存储阵列组"

配置存储阵列组

您可以创建存储组、然后将存储阵列添加到这些组中。

配置组是一个两步操作步骤。

第**1**步：创建组

首先创建组。存储组定义了哪些驱动器提供构成卷的存储。

步骤

1. 从管理页面中、选择菜单：管理组[创建存储阵列组]。
2. 在*名称*字段中、键入新组的名称。
3. 选择要添加到新组的存储阵列。
4. 单击 * 创建 * 。

第**2**步：将存储阵列添加到组

您可以将一个或多个存储阵列添加到用户创建的组中。

步骤

1. 在主视图中、选择*管理*、然后选择要将存储阵列添加到的组。
2. 选择菜单：管理组[将存储阵列添加到组]。
3. 选择要添加到组中的存储阵列。
4. 单击 * 添加。 *

从组中删除存储阵列

如果不再需要从特定存储组管理一个或多个受管存储阵列、则可以从组中删除该存储阵列。

关于此任务

从组中删除存储阵列不会以任何方式影响存储阵列或其数据。如果您的存储阵列由System Manager管理、则仍可使用浏览器对其进行管理。如果意外从组中删除了存储阵列、则可以重新添加该存储阵列。

步骤

1. 从管理页面中、选择菜单：管理组[从组中删除存储阵列]。
2. 从下拉列表中、选择包含要删除的存储阵列的组、然后单击要从组中删除的每个存储阵列旁边的复选框。
3. 单击 * 删除 * 。

删除存储阵列组

您可以删除不再需要的一个或多个存储阵列组。

关于此任务

此操作仅删除存储阵列组。与已删除组关联的存储阵列仍可通过全部管理视图或与其关联的任何其他组进行访问。

步骤

1. 从管理页面中、选择菜单：管理组[删除存储阵列组]。
2. 选择要删除的一个或多个存储阵列组。
3. 单击 * 删除 * 。

重命名存储阵列组

如果当前名称不再有意义或适用、您可以更改存储阵列组的名称。

关于此任务

请牢记这些准则。

- 名称可以由字母、数字和特殊字符下划线(_)、连字符(-)和井号(#)组成。如果选择任何其他字符、则会显示一条错误消息。系统将提示您选择其他名称。
- 名称限制为30个字符。名称中的任何前导空格和尾随空格将被删除。
- 请使用一个易于理解和记住的唯一有意义的名称。
- 避免将来会很快失去意义的任意名称或名称。

步骤

1. 在主视图中、选择*管理*、然后选择要重命名的存储阵列组。
2. 选择菜单：Manage Groups[重命名存储阵列组]。
3. 在*组名称*字段中、键入组的新名称。
4. 单击*重命名。*

升级

升级中心概述

从升级中心、您可以管理多个存储阵列的SANtricity OS软件和NVSRAM升级。

升级如何工作?

下载最新的操作系统软件、然后升级一个或多个阵列。

升级工作流

以下步骤提供了执行软件升级的高级工作流。

1. 您可以从支持站点下载最新的SANtricity OS软件文件(可从Unified Manager的"支持"页面中找到一个链接)。将此文件保存在管理主机系统(在浏览器中访问Unified Manager的主机)上、然后解压缩此文件。
2. 在Unified Manager中、您可以将SANtricity OS软件文件和NVSRAM文件加载到存储库(存储文件的Web服务代理服务器的一个区域)。您可以从菜单：升级中心[升级SANtricity 操作系统软件或从升级中心>管理软件存储库]添加文件。
3. 将文件加载到存储库中后、您可以选择要在升级中使用的文件。从升级SANtricity OS软件页面(菜单：升级中心[升级SANtricity OS软件])中、选择SANtricity OS软件文件和NVSRAM文件。选择软件文件后、此页面上将显示兼容存储阵列列表。然后、选择要使用新软件升级的存储阵列。(不能选择不兼容的阵列。)
4. 然后、您可以立即开始软件传输和激活、也可以选择稍后暂存文件以进行激活。在升级过程中、Unified Manager将执行以下任务：
   a. 对存储阵列执行运行状况检查、以确定是否存在任何可能阻止升级完成的条件。如果任何阵列未通过运行状况检查，您可以跳过该特定阵列并继续对其他阵列进行升级，也可以停止整个过程并对未通过的阵列进行故障排除。
   b. 将升级文件传输到每个控制器。
   c. 重新启动控制器并激活新的SANtricity OS软件、一次一个控制器。激活期间、现有SANtricity OS文件将替换为新文件。

   > 您还可以指定稍后激活此软件。

立即或分阶段升级

您可以立即激活升级，也可以稍后暂存升级。您可以选择稍后激活，原因如下：

- * 当前时间 * —激活软件可能需要很长时间，因此您可能需要等待 I/O 负载变轻。根据 I/O 负载和缓存大小，完成控制器升级通常需要 15 到 25 分钟。控制器会在激活期间重新启动并进行故障转移，因此在升级完成之前性能可能会比平常低。
- * 软件包类型 * —您可能需要先在一个存储阵列上测试新软件和固件，然后再升级其他存储阵列上的文件。

要激活暂存软件、请转到菜单：Support[升级中心]、然后单击标记为SANtricity OS控制器软件升级的区域中的*激活*。

运行状况检查

运行状况检查会在升级过程中运行、但您也可以在开始之前单独运行运行运行运行状况检查(转到菜单：升级中心[升级前运行状况检查])。

运行状况检查会评估所有存储系统组件、以确保升级可以继续进行。以下情况可能会阻止升级：

- 已分配的驱动器出现故障
- 正在使用热备件

- 卷组不完整
- 正在运行排他操作
- 缺少卷
- 控制器处于非最佳状态
- 事件日志事件数量过多
- 配置数据库验证失败
- 使用旧版 DAC 存储的驱动器

升级前需要了解哪些信息？

在升级多个存储阵列之前、请在规划过程中查看主要注意事项。

当前版本

您可以从Unified Manager的"管理"页面查看每个已发现存储阵列的当前SANtricity OS软件版本。此版本显示在SANtricity OS软件列中。单击每行中的 SANtricity OS 版本时，会在弹出对话框中显示控制器固件和 NVSRAM 信息。

其他需要升级的组件

在升级过程中、您可能还需要升级主机的多路径/故障转移驱动程序或HBA驱动程序、以便主机可以正确地与控制器进行交互。

有关兼容性信息，请参阅 "NetApp 互操作性表"。另请参见适用于您的操作系统的快速指南中的过程。快速指南可从获取 "E 系列和 SANtricity 文档"。

双控制器

如果存储阵列包含两个控制器，并且您安装了多路径驱动程序，则在升级期间，存储阵列可以继续处理 I/O 。在升级期间，将执行以下过程：

1. 控制器 A 将其所有 LUN 故障转移到控制器 B
2. 升级在控制器 A 上进行
3. 控制器 A 将收回其 LUN 以及控制器 B 的所有 LUN 。
4. 升级在控制器 B 上进行

升级完成后，您可能需要在控制器之间手动重新分布卷，以确保卷返回到正确的所属控制器。

升级软件和固件

执行升级前运行状况检查

运行状况检查会在升级过程中运行，但您也可以在开始之前单独运行运行运行运行状况检查。运行状况检查会评估存储阵列的组件，以确保升级可以继续进行。

步骤

1. 在主视图中，选择 * 管理 * ，然后选择菜单：升级中心 [升级前运行状况检查] 。

   此时将打开升级前运行状况检查对话框，其中列出了所有已发现的存储系统。

2. 如果需要，可对列表中的存储系统进行筛选或排序，以便您可以查看当前未处于最佳状态的所有系统。
3. 选中要通过运行状况检查运行的存储系统对应的复选框。
4. 单击 * 开始 * 。

   执行运行状况检查时，此进度将显示在对话框中。

5. 运行状况检查完成后，您可以单击每行右侧的省略号（ ... ）以查看更多信息并执行其他任务。

   如果任何阵列未通过运行状况检查，您可以跳过该特定阵列并继续对其他阵列进行升级，也可以停止整个过程并对未通过的阵列进行故障排除。

升级**SANtricity** 操作系统

使用最新软件和NVSRAM升级一个或多个存储阵列、以确保您拥有所有最新功能和错误修复。控制器NVSRAM是一个控制器文件、用于指定控制器的默认设置。

开始之前

- 运行SANtricity Web服务代理和Unified Manager的主机系统上提供了最新的SANtricity 操作系统文件。
- 您知道是要立即激活软件升级还是稍后激活。

  您可以选择稍后激活，原因如下：

  - * 当前时间 * —激活软件可能需要很长时间，因此您可能需要等待 I/O 负载变轻。控制器会在激活期间进行故障转移，因此，在升级完成之前，性能可能会比平常低。
  - * 软件包类型 * —您可能需要先在一个存储阵列上测试新的操作系统软件，然后再升级其他存储阵列上的文件。

系统必须运行SANtricity OS 11.70.5才能升级到11.80.x或更高版本。

关于此任务

```
[NOTE]
====
数据丢失风险或存储阵列损坏风险–升级期间，请勿更改存储阵列。为存储阵列供电。

====
.步骤
. 如果存储阵列仅包含一个控制器或未使用多路径驱动程序，请停止存储阵列的 I/O
活动，以防止出现应用程序错误。如果存储阵列有两个控制器，并且您安装了多路径驱动程序，则无
需停止 I/O 活动。
. 在主视图中、选择*管理*、然后选择要升级的一个或多个存储阵列。
. 选择菜单：升级中心 [ 升级 SANtricity 操作系统软件 ] 。
```

+
此时将显示升级 SANtricity OS 软件页面。

. 从 NetApp 支持站点将最新的 SANtricity OS 软件包下载到您的本地计算机。
+
.. 单击 * 将新文件添加到软件存储库 * 。
.. 单击链接以查找最新的 * SANtricity OS Downloads* 。
.. 单击 * 下载最新版本 * 链接。
.. 按照其余说明将 SANtricity 操作系统文件和 NVSRAM 文件下载到本地计算机。

+
[NOTE]
====
8.42
及更高版本需要使用数字签名固件。如果您尝试下载未签名的固件，则会显示一个错误，并中止下载。

====
. 选择要用于升级控制器的操作系统软件文件和 NVSRAM 文件：
+
.. 从 * 选择 SANtricity OS 软件文件 *
下拉列表中，选择下载到本地计算机的操作系统文件。
+
如果有多个可用文件，则这些文件将从最新日期到最旧日期进行排序。

+
[NOTE]
====
软件存储库列出了与 Web 服务代理关联的所有软件文件。如果未看到要使用的文件，可以单击链接 * 将新文件添加到软件存储库 * ，以浏览到要添加的操作系统文件所在的位置。

====
.. 从 * 选择 NVSRAM 文件 * 下拉列表中，选择要使用的控制器文件。
+
如果有多个文件，则这些文件将从最新日期到最旧日期进行排序。

. 在兼容存储阵列表中，查看与选定操作系统软件文件兼容的存储阵列，然后选择要升级的阵列。
+
** 默认情况下，您在 " 管理 " 视图中选择的存储阵列以及与选定固件文件兼容的存储阵列将在 " 兼容存储阵列 " 表中选择。
** 无法使用选定固件文件更新的存储阵列在兼容存储阵列表中不可选择，如状态 * 不兼容 * 所示。

. *可选：*要在不激活软件文件的情况下将其传输到存储阵列、请选中
*将操作系统软件传输到存储阵列、将其标记为暂存并稍后激活*复选框。
. 单击 * 开始 * 。
. 根据您选择现在激活还是稍后激活，执行以下操作之一：
+
** 键入 * 传输 * 确认要在选定升级的阵列上传输建议的操作系统软件版本，然后单击 * 传输 * 。
+
要激活已传输的软件，请选择菜单：升级中心 [激活暂存操作系统软件] 。

** 键入 * 升级 * 确认要在选定升级的阵列上传输并激活建议的操作系统软件版本，然后单击 * 升级 * 。
+
系统会将软件文件传输到您选择升级的每个存储阵列，然后通过启动重新启动来激活该文件。

+
升级操作期间会执行以下操作：

+
**
升级前运行状况检查会在升级过程中运行。升级前运行状况检查会评估所有存储阵列组件，以确保升级可以继续进行。
** 如果存储阵列的任何运行状况检查失败，升级将停止。您可以单击省略号（ ... ）并选择 * 保存日志 * 以查看错误。您还可以选择覆盖运行状况检查错误，然后单击 * 继续 * 继续升级。
** 您可以在升级前运行状况检查后取消升级操作。

. *可选：*升级完成后、您可以通过单击省略号(...)并选择*保存日志
*来查看为特定存储阵列升级的内容列表。
+
文件将保存在浏览器的"Downloads"文件夹中，名称为 `upgrade_log-<date>.json`。

[[IDa036aa524b91de83a487fe497d9370d9]]
= 激活暂存操作系统软件
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
您可以选择立即激活软件文件，也可以等到更方便的时间再激活。此操作步骤假定您稍后选择激活此软件文件。

.关于此任务
您可以传输固件文件、而无需激活这些文件。您可以选择稍后激活，原因如下：

* * 当前时间 * —激活软件可能需要很长时间，因此您可能需要等待 I/O
负载变轻。控制器会在激活期间重新启动并进行故障转移，因此在升级完成之前性能可能会比平常低。
* * 软件包类型 *
—您可能需要先在一个存储阵列上测试新软件和固件，然后再升级其他存储阵列上的文件。

[NOTE]
====
激活过程启动后，您无法停止它。

====
.步骤
. 在主视图中、选择*管理*。如有必要、单击页面顶部的状态列对状态为"OS Upgrade (waiting activation)"的所有存储阵列进行排序。
. 选择要为其激活软件的一个或多个存储阵列，然后选择菜单：升级中心 [激活暂存操作系统软件] 。
+
升级操作期间会执行以下操作：

+
**
在激活过程中会运行升级前运行状况检查。升级前运行状况检查会评估所有存储阵列组件，以确保激活可以继续进行。
** 如果存储阵列的任何运行状况检查失败，则激活将停止。您可以单击省略号（ ... ）并选择 * 保存日志 * 以查看错误。您也可以选择覆盖运行状况检查错误，然后单击 * 继续 *
继续进行激活。
**
您可以在升级前运行状况检查后取消激活操作。成功完成升级前运行状况检查后，将激活。激活所需的时间取决于您的存储阵列配置以及要激活的组件。

. *可选：*激活完成后、您可以通过单击省略号(...)并选择*保存日志
*来查看为特定存储阵列激活的内容列表。
+
文件将保存在浏览器的"Downloads"文件夹中，名称为 `activate_log-<date>.json`。

```
[[ID8cdea40c31c7671e3f8882459e6f36f4]]
= 管理软件存储库
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
软件存储库列出了与 Web 服务代理关联的所有软件文件。

如果您看不到要使用的文件、可以使用管理软件存储库选项将一个或多个SANtricity
操作系统文件导入到运行Web服务代理和Unified
Manager的主机系统中。您还可以选择删除软件存储库中的一个或多个SANtricity OS文件。

.开始之前
如果要添加SANtricity 操作系统文件、请确保操作系统文件在本地系统上可用。

.步骤
. 在主视图中、选择*管理*、然后选择菜单：升级中心[管理软件存储库]。
+
此时将显示管理软件存储库对话框。

. 执行以下操作之一：
+
[cols="25h,~"]
|===
| 选项 | 执行此操作


 a|
导入
 a|
.. 单击*导入。*
.. 单击*浏览*、然后导航到要添加的操作系统文件所在的位置。
+
操作系统文件的文件名类似于 `N2800-830000-000.dlp`。

.. 选择要添加的一个或多个操作系统文件、然后单击*导入*。




 a|
删除
```

```
 a|
.. 选择要从软件存储库中删除的一个或多个操作系统文件。
.. 单击 * 删除 * 。


|===


.结果
如果选择导入、则会上传并验证文件。如果选择了delete、则这些文件将从软件存储库中删除。



[[ID055734b805fd7027bf428f791eec06af]]
= 清除暂存操作系统软件
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
您可以删除暂存操作系统软件、以确保稍后不会无意中激活待定版本。删除暂存操作系统软件不会影响存储阵列上运行的当前版本。

.步骤
. 在主视图中、选择*管理*、然后选择菜单：升级中心[清除暂存操作系统软件]。
+
此时将打开清除暂存操作系统软件对话框、并列出所有已发现的具有待定软件或NVSRAM的存储系统。

. 如果需要、可对列表中的存储系统进行筛选或排序、以便您可以查看具有暂存软件的所有系统。
. 选中要清除的待定软件存储系统对应的复选框。
. 单击*清除*。
+
此操作的状态将显示在对话框中。




:leveloffset: -1


:leveloffset: -1
```

```
= 镜像

:leveloffset: +1


[[ID28273f63c6eda11f964a787ab32ebc7e]]
= 镜像概述
:allow-uri-read:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
使用镜像功能可以异步或同步在本地存储阵列和远程存储阵列之间复制数据。

[NOTE]
====
EF600或EF300存储系统不支持同步镜像。

====


== 什么是镜像?

SANtricity
应用程序包括两种类型的镜像：异步和同步。异步镜像可按需或按计划复制数据卷、从而最大限度地减少或避免因数据损坏或丢失而导致的停机时间。同步镜像可实时复制数据卷、以确保持续可用性。

了解更多信息。

* xref:{relative_path}mirroring-overview.html["镜像的工作原理"]
* xref:{relative_path}mirroring-terminology.html["镜像术语"]




== 如何配置镜像?

您可以在Unified Manager中配置异步或同步镜像、然后使用System Manager管理同步。

了解更多信息。

* xref:{relative_path}mirroring-configuration-workflow.html["镜像配置工作流"]
* xref:{relative_path}requirements-for-using-mirroring.html["使用镜像的要求"]
* xref:{relative_path}create-asynchronous-mirrored-pair-
um.html["创建异步镜像对"]
```

```
* xref:{relative_path}create-synchronous-mirrored-pair-
um.html["创建同步镜像对"]




= 概念

:leveloffset: +1


[[ID80394952a9388e7a770f976ecb9e21da]]
= 镜像的工作原理
:allow-uri-read:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
Unified Manager提供了SANtricity
镜像功能的配置选项、可使管理员在两个存储阵列之间复制数据以实现数据保护。

[NOTE]
====
EF600或EF300存储系统不支持同步镜像。

====


== 镜像类型

SANtricity 应用程序包括两种类型的镜像：异步和同步。

异步镜像可按需或按计划复制数据卷、从而最大限度地减少或避免因数据损坏或丢失而导致的停机时间。异步镜像可捕获主卷在特定时间点的状态、并仅复制自上次映像捕获以来发生更改的数据。可以立即更新主站点、并在带宽允许的情况下更新二级站点。此信息将在网络资源可用时进行缓存并稍后发送。这种类型的镜像非常适合备份和归档等定期过程。

同步镜像可实时复制数据卷、以确保持续可用性。其目的是、在两个存储阵列之一发生灾难时、提供一份重要数据副本、从而实现零丢失数据的恢复点目标(RPO)。副本与生产数据在每一刻都是相同的、因为每次对主卷执行写入时、都会对二级卷执行写入。在使用主卷上所做的更改更新二级卷之前、主机不会收到写入成功的确认消息。这种类型的镜像非常适合用于灾难恢复等业务连续性目的。



== 镜像类型之间的差异
```

下表介绍了这两种镜像类型之间的主要区别。

```
[cols="1a,1a,1a"]
|===
| 属性 | 异步 | 同步


 a|
复制方法
 a|
时间点–镜像是按需执行的、也可以根据用户定义的计划自动执行。
 a|
持续–镜像会自动持续执行、每次写入主机时都会复制数据。



 a|
距离
 a|
支持阵列之间的长距离。通常、距离仅受网络功能和通道扩展技术的限制。
 a|
限制为阵列之间的距离较短。通常、距离必须在本地存储阵列10公里(6.2英里)以内、才能满足延迟和应用程序性能要求。



 a|
通信方法
 a|
标准IP或光纤通道网络。
 a|
仅限光纤通道网络。



 a|
卷类型
 a|
标准或精简。
 a|
仅限标准配置。

|===



[[ID3b29399a6180f8ca22202aaade727a37]]
```

= 镜像配置工作流
:allow-uri-read:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
您可以在Unified Manager中配置异步或同步镜像、然后使用System Manager管理同步。

== 异步镜像工作流

异步镜像涉及以下工作流：

. 在Unified Manager中执行初始配置：
+
.. 选择本地存储阵列作为数据传输的源。
..
创建或选择现有镜像一致性组、该组是本地阵列上主卷和远程阵列上二级卷的容器。主卷和二级卷称为"镜像对"。如果您是首次创建镜像一致性组、请指定是要执行手动同步还是按计划同步。
.. 从本地存储阵列中选择主卷、然后确定其预留容量。预留容量是为复制操作分配的物理容量。
.. 选择一个远程存储阵列作为传输的目标、一个二级卷、然后确定其预留容量。
.. 开始从主卷到二级卷的初始数据传输。根据卷大小、此初始传输可能需要几小时的时间。

. 检查初始同步的进度：
+
.. 在Unified Manager中、为本地阵列启动System Manager。
.. 在System Manager中、查看镜像操作的状态。镜像完成后、镜像对的状态为"最佳"。

. 您也可以在System
Manager中重新计划或手动执行后续数据传输。只有新的块和更改的块才会从主卷传输到二级卷。
+
[NOTE]
====
由于异步复制是定期进行的、因此系统可以整合更改的块并节省网络带宽。对写入吞吐量和写入延迟的影响最小。

====

== 同步镜像工作流

同步镜像涉及以下工作流：

. 在Unified Manager中执行初始配置：
+
.. 选择一个本地存储阵列作为数据传输的源。
.. 从本地存储阵列中选择主卷。
.. 选择一个远程存储阵列作为数据传输的目标、然后选择一个二级卷。
.. 选择同步和重新同步优先级。
.. 开始从主卷到二级卷的初始数据传输。根据卷大小、此初始传输可能需要几小时的时间。

. 检查初始同步的进度：
+
.. 在Unified Manager中、为本地阵列启动System Manager。
.. 在System Manager中、查看镜像操作的状态。镜像完成后、镜像对的状态为"最佳
"。这两个阵列会尝试通过正常操作保持同步。只有新的块和更改的块才会从主卷传输到二级卷。

. 您也可以在System Manager中更改同步设置。
+
[NOTE]
====
由于同步复制是持续的、因此两个站点之间的复制链路必须提供足够的带宽功能。

====

[[ID54ce5f069e45c7242b537f9077c8b423]]
= 镜像术语
:allow-uri-read:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
了解镜像术语如何应用于存储阵列。

[cols="25h,~"]
|===
| 期限 | 说明

a|

本地存储阵列

a|
本地存储阵列是您要对其执行操作的存储阵列。

a|
镜像一致性组

a|
镜像一致性组是一个或多个镜像对的容器。对于异步镜像操作、必须创建镜像一致性组。组中的所有镜像对会同时重新同步、从而保留一致的恢复点。

同步镜像不使用镜像一致性组。

a|
镜像对

a|
镜像对由两个卷组成、一个是主卷、一个是二级卷。

在异步镜像中、镜像对始终属于镜像一致性组。首先对主卷执行写入操作、然后将其复制到二级卷。镜像一致性组中的每个镜像对共享相同的同步设置。

a|
主卷

a|
镜像对的主卷是要镜像的源卷。

a|
远程存储阵列

a|
远程存储阵列通常指定为二级站点、该站点通常在镜像配置中保存数据的副本。

a|
预留容量

a|
预留容量是指用于任何复制服务操作和存储对象的物理分配容量。主机不能直接读取它。

需要这些卷、以便控制器能够持久保存必要的信息、以使镜像保持运行状态。它们包含增量日志和写入时复制数据等信息。

```
 a|
二级卷
 a|
镜像对的二级卷通常位于二级站点、并保存数据的副本。



 a|
同步
 a|
在本地存储阵列与远程存储阵列之间进行初始同步时进行同步。如果在通信中断后主卷和二级卷未同步、则也会发生同步。当通信链路重新工作时、任何未复制的数据都会同步到二级卷的存储阵列。

|===



[[ID56fb257b887fb786f749702713ad1b81]]
= 使用镜像的要求
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
如果您计划配置镜像、请记住以下要求。



== Unified Manager

* Web服务代理服务必须正在运行。
* Unified Manager必须通过HTTPS连接在本地主机上运行。
* Unified Manager必须显示存储阵列的有效SSL证书。您可以使用Unified
Manager接受自签名证书或安装自己的安全证书、并导航到菜单：Certificate[证书管理]。




== 存储阵列

[NOTE]
====
```

EF600或EF300存储阵列不支持同步镜像。

====
* 您必须有两个存储阵列。
* 每个存储阵列必须具有两个控制器。
* 必须在Unified Manager中发现这两个存储阵列。
* 主阵列和二级阵列中的每个控制器都必须配置一个以太网管理端口、并且必须连接到您的网络。
* 存储阵列的最低固件版本为7.84。(它们可以分别运行不同的操作系统版本。)
* 您必须知道本地和远程存储阵列的密码。
* 您必须在远程存储阵列上具有足够的可用容量、才能创建一个等于或大于要镜像的主卷的二级卷。
* 具有光纤通道(FC)或iSCSI主机端口的控制器支持异步镜像、而只有具有
FC主机端口的控制器才支持同步镜像。

== 连接要求

通过FC接口(异步或同步)进行镜像需要满足以下要求：

* 存储阵列的每个控制器都将其编号最高的FC主机端口专用于镜像操作。
* 如果控制器同时具有基本FC端口和主机接口卡(HIC) FC端口、则编号最高的端口位于
HIC上。登录到专用端口的任何主机都将注销、并且不接受任何主机登录请求。只有参与镜像操作的控制器才会接受此端口上的I/O请求。
* 专用镜像端口必须连接到支持目录服务和名称服务接口的FC网络结构环境。特别是、不支持将FC-AL和点对点作为参与镜像关系的控制器之间的连接选项。

通过iSCSI接口(仅限异步)进行镜像需要满足以下要求：

* 与FC不同、iSCSI不需要专用端口。在iSCSI
环境中使用异步镜像时、无需将存储阵列的任何前端iSCSI端口专用于异步镜像；这些端口可用于异步镜像流量和主机到阵列I/O连接。
* 控制器会维护一个远程存储系统列表、iSCSI
启动程序会尝试与这些系统建立会话。成功建立iSCSI连接的第一个端口将用于此后与该远程存储阵列进行的所有通信。如果通信失败、则会尝试使用所有可用端口进行新会话。
*
iSCSI端口在阵列级别逐个端口进行配置。用于配置消息传送和数据传输的控制器间通信使用全局设置、包括以下设置：
+
** VLAN：本地系统和远程系统必须具有相同的VLAN设置才能进行通信
** iSCSI侦听端口
** 巨型帧
** 以太网优先级

[NOTE]
====
iSCSI控制器间通信必须使用主机连接端口、而不是管理以太网端口。

====

== 镜像卷候选项

* 镜像对的主卷和二级卷上的RAID级别、缓存参数和区块大小可能不同。
+

NOTE: 对于EF600和
EF300控制器、异步镜像对中的主卷和二级卷必须匹配相同的协议、托盘级别、区块大小、安全类型和RAID级别。不符合条件的异步镜像对不会显示在可用卷列表中。

* 二级卷必须至少与主卷大小相同。
* 一个卷只能参与一个镜像关系。
* 对于同步镜像对、主卷和二级卷必须是标准卷。它们不能是精简卷或快照卷。
*
对于同步镜像、给定存储阵列上支持的卷数量存在限制。确保存储阵列上已配置的卷数小于支持的限制。当同步镜像处于活动状态时、创建的两个预留容量卷将计入卷限制。
* 对于异步镜像、主卷和二级卷必须具有相同的驱动器安全功能。
+
** 如果主卷支持FIPS,则二级卷必须支持FIPS.
** 如果主卷支持FDE,则二级卷必须支持FDE.
** 如果主卷未使用驱动器安全、则二级卷不得使用驱动器安全。

== 预留容量

异步镜像：

*
主卷和镜像对中的二级卷需要预留容量卷、以便记录写入信息、以便从控制器重置和其他临时中断中恢复。
*
由于镜像对中的主卷和二级卷都需要额外的预留容量、因此您必须确保镜像关系中的两个存储阵列都具有可用容量。

同步镜像：

* 主卷和二级卷需要预留容量、以便记录写入信息、以便从控制器重置和其他临时中断中恢复。
*
激活同步镜像后、系统会自动创建预留容量的卷。由于镜像对中的主卷和二级卷都需要预留容量、因此您必须确保参与同步镜像关系的两个存储阵列上都有足够的可用容量。

== 驱动器安全功能

*
如果您使用的是支持安全的驱动器、则主卷和二级卷必须具有兼容的安全设置。此限制不会强制实施；因此、您必须自行验证。
*
如果使用的是支持安全的驱动器、则主卷和二级卷应使用相同的驱动器类型。此限制不会强制实施；因此、您必须自行验证。
* 如果您使用的是数据保证(Data Assurance、DA)、则主卷和二级卷必须具有相同的DA设置。

:leveloffset: -1

= 配置镜像

:leveloffset: +1

[[ID2bd8f21abbe5d820f1b168b1d2e4d698]]
= 创建异步镜像对
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
要配置异步镜像、请创建一个镜像对、其中包括本地阵列上的主卷和远程阵列上的二级卷。

.开始之前
在创建镜像对之前、请满足Unified Manager的以下要求：

* Web服务代理服务必须正在运行。
* Unified Manager必须通过HTTPS连接在本地主机上运行。

* Unified Manager必须显示存储阵列的有效SSL证书。您可以使用Unified Manager接受自签名证书或安装自己的安全证书、并导航到菜单：Certificate[证书管理]。

此外、对于存储阵列和卷、请确保满足以下要求：

* 每个存储阵列必须具有两个控制器。
* 必须在Unified Manager中发现这两个存储阵列。
* 主阵列和二级阵列中的每个控制器都必须配置一个以太网管理端口、并且必须连接到您的网络。
* 存储阵列的最低固件版本为7.84。(它们可以分别运行不同的操作系统版本。)
* 您必须知道本地和远程存储阵列的密码。
* 您必须在远程存储阵列上具有足够的可用容量、才能创建一个等于或大于要镜像的主卷的二级卷。
* 本地和远程存储阵列通过光纤通道网络结构或iSCSI接口进行连接。
* 您已创建要在异步镜像关系中使用的主卷和二级卷。
* 二级卷必须至少与主卷大小相同。

.关于此任务
创建异步镜像对的过程包括多步操作步骤。

== 第1步：创建或选择镜像一致性组

在此步骤中、您可以创建一个新的镜像一致性组或选择一个现有镜像一致性组。镜像一致性组是主卷和二级卷(镜像对)的容器、并为组中的所有对指定所需的重新同步方法(手动或自动)。

.步骤
. 从*管理*页面中、选择要用于源的本地存储阵列。
. 选择菜单：操作[创建异步镜像对]。
+
此时将打开创建异步镜像对向导。

. 选择现有镜像一致性组或创建新的镜像一致性组。
+
要选择现有组、请确保已选择*现有镜像一致性组*、然后从表中选择该组。一个一致性组可以包含多个镜像对。

+
要创建新组、请执行以下操作：

+
.. 选择*新的镜像一致性组*、然后单击*下一步*。
..
输入最能描述要在两个存储阵列之间镜像的卷上的数据的唯一名称。名称只能由字母、数字和特殊字符下划线(_)、短划线(-)和哈希符号(#)组成。名称不能超过30个字符、并且不能包含空格。
.. 选择要与本地存储阵列建立镜像关系的远程存储阵列。

+
[NOTE]
====
如果远程存储阵列受密码保护、则系统会提示输入密码。

====
.. 选择是要手动还是自动同步镜像对：
+
*** *手动*-
选择此选项可手动为此组中的所有镜像对启动同步。请注意、如果稍后要执行重新同步、则必须启动主存储阵列的System Manager、然后转到菜单：存储(异步镜像)、从*镜像一致性组*选项卡中选择组、然后选择菜单：更多(手动重新同步)。
*** *自动*—从上次更新开始到下次更新开始、选择所需的间隔、以*分钟*、*小时*或*天*为单位。例如、如果将同步间隔设置为30分钟、而同步进程从下午4：00开始、则下一个进程从下午4：30开始

.. 选择所需的警报设置：
+
*** 对于手动同步、请指定接收警报时的阈值(由剩余容量百分比定义)。
*** 对于自动同步、您可以设置三种警报方法：
如果同步未在特定时间长度内完成、远程阵列上的恢复点数据早于特定时间限制、并且预留容量接近特定阈值(由剩余容量百分比定义)。

. 选择*下一步*并转到<<第2步：选择主卷>>。
+
如果定义了新的镜像一致性组、则Unified Manager会首先在本地存储阵列上创建镜像一致性组、然后在远程存储阵列上创建镜像一致性组。您可以通过为每个阵列启动System Manager来查看和管理镜像一致性组。

+
[NOTE]
====
如果Unified Manager在本地存储阵列上成功创建镜像一致性组、但无法在远程存储阵列上创建该一致性组、则它会自动从本地存储阵列中删除镜像一致性组。如果在Unified Manager尝试删除镜像一致性组时发生错误、您必须手动将其删除。

====

== 第2步：选择主卷

在此步骤中、您可以选择要在镜像关系中使用的主卷并分配其预留容量。在本地存储阵列上选择主卷时、系统会显示一个列表、其中列出了该镜像对符合条件的所有卷。不符合使用条件的任何卷不会显示在该列表中。

添加到本地存储阵列上的镜像一致性组的任何卷都将在镜像关系中发挥主要作用。

.步骤
. 从符合条件的卷列表中、选择要用作主卷的卷、然后单击*下一步*以分配预留容量。
. 从符合条件的候选卷列表中、选择为主卷预留的容量。
+
请记住以下准则：

+
** 预留容量的默认设置为基础卷容量的20%、通常此容量已足够。如果更改百分比、请单击*刷新候选项*。
** 所需容量因向主卷写入I/O的频率和大小以及保留容量所需的时间而异。
** 通常、如果存在以下一种或两种情况、请为预留容量选择更大的容量：
+
*** 您打算将镜像对保留很长时间。
*** 由于I/O活动繁重、主卷上的数据块会发生很大一部分更改。使用历史性能数据或其他操作系统实用程序帮助您确定主卷的典型I/O活动。

. 选择*下一步*并转到<<第3步：选择二级卷>>。

== 第3步：选择二级卷

在此步骤中、您可以选择要在镜像关系中使用的二级卷并分配其预留容量。在远程存储阵列上选择二级卷时、系统会显示一个列表、其中列出了该镜像对符合条件的所有卷。不符合使用条件的任何卷不会显示在该列表中。

您添加到远程存储阵列上的镜像一致性组的任何卷都将在镜像关系中具有二级角色。

.步骤
. 从符合条件的卷列表中、选择要用作镜像对中二级卷的卷、然后单击*下一步*以分配预留容量。
. 从符合条件的候选卷列表中、选择为二级卷预留的容量。
+
请记住以下准则：

+

** 预留容量的默认设置为基础卷容量的20%、通常此容量已足够。如果更改百分比、请单击*刷新候选项*。
** 所需容量因向主卷写入I/O的频率和大小以及保留容量所需的时间而异。
** 通常、如果存在以下一种或两种情况、请为预留容量选择更大的容量：
+
*** 您打算将镜像对保留很长时间。
*** 由于I/O活动繁重、主卷上的数据块会发生很大一部分更改。使用历史性能数据或其他操作系统实用程序帮助您确定主卷的典型I/O活动。

. 选择*完成*以完成异步镜像序列。

.结果
Unified Manager将执行以下操作：

* 开始在本地存储阵列和远程存储阵列之间进行初始同步。
* 在本地存储阵列和远程存储阵列上为镜像对创建预留容量。

NOTE：如果要镜像的卷是精简卷、则在初始同步期间、只会将配置的块(已分配容量而不是报告的容量)传输到二级卷。这样可以减少完成初始同步所需传输的数据量。

[[ID5d40423a7283dce7873f8bce487ae1a1]]
= 创建同步镜像对
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
要配置同步镜像、请创建一个镜像对、其中包括本地阵列上的主卷和远程阵列上的二级卷。

[NOTE]
====
EF600或EF300存储系统不支持此功能。

====
.开始之前

在创建镜像对之前、请满足Unified Manager的以下要求：

* Web服务代理服务必须正在运行。
* Unified Manager必须通过HTTPS连接在本地主机上运行。
* Unified Manager必须显示存储阵列的有效SSL证书。您可以使用Unified Manager接受自签名证书或安装自己的安全证书、并导航到菜单：Certificate[证书管理]。

此外、对于存储阵列和卷、请确保满足以下要求：

* 您计划用于镜像的两个存储阵列会在Unified Manager中发现。
* 每个存储阵列必须具有两个控制器。
* 主阵列和二级阵列中的每个控制器都必须配置一个以太网管理端口、并且必须连接到您的网络。
* 存储阵列的最低固件版本为7.84。（它们可以分别运行不同的操作系统版本。）
* 您必须知道本地和远程存储阵列的密码。
* 本地和远程存储阵列通过光纤通道网络结构进行连接。
* 您已创建要在同步镜像关系中使用的主卷和二级卷。
* 主卷必须是标准卷。它不能是精简卷或快照卷。
* 二级卷必须是标准卷。它不能是精简卷或快照卷。
* 二级卷应至少与主卷大小相同。

.关于此任务
创建同步镜像对的过程包括多步操作步骤。

== 第1步：选择主卷

在此步骤中、您可以选择要在同步镜像关系中使用的主卷。在本地存储阵列上选择主卷时、系统会显示一个列表、其中列出了该镜像对符合条件的所有卷。不符合使用条件的任何卷不会显示在该列表中。您选择的卷在镜像关系中具有主要角色。

.步骤
. 从*管理*页面中、选择要用于源的本地存储阵列。
. 选择菜单：操作[创建同步镜像对]。
+
此时将打开创建同步镜像对向导。

. 从符合条件的卷列表中、选择要用作镜像中主卷的卷。
. 选择*下一步*并转到<<第2步：选择二级卷>>。

== 第2步：选择二级卷

在此步骤中、您可以选择要在镜像关系中使用的二级卷。在远程存储阵列上选择二级卷时、系统会显示一个列表、其中列出了该镜像对符合条件的所有卷。不符合使用条件的任何卷不会显示在该列表中。您选择的卷将在镜像关系中保留二级角色。

.步骤
. 选择要与本地存储阵列建立镜像关系的远程存储阵列。
+
[NOTE]
====
如果远程存储阵列受密码保护、则系统会提示输入密码。

====
+
** 存储阵列按其存储阵列名称列出。如果您尚未为存储阵列命名、则该存储阵列将列为"未命名"。
** 如果要使用的存储阵列不在列表中、请确保已在Unified Manager中发现它。

. 从符合条件的卷列表中、选择要用作镜像中二级卷的卷。
+
[NOTE]
====
如果选择的二级卷的容量大于主卷、则可用容量将限制为主卷的大小。

====
. 单击*Next*并转到<<第3步：选择同步设置>>。

== 第3步：选择同步设置

在此步骤中、您可以选择用于确定在通信中断后如何同步数据的设置。您可以设置在通信中断后主卷的控制器所有者与二级卷重新同步数据的优先级。您还必须选择手动或自动重新同步策略。

.步骤
. 使用滑块栏设置同步优先级。
+
同步优先级用于确定在通信中断后、与服务I/O请求相比、用于完成初始同步和重新同步操作的系统资源量。

+
此对话框中设置的优先级会同时对主卷和二级卷进行适用场景。您可以稍后转到System Manager并选择菜单：Storage[同步镜像>更多>编辑设置]来修改主卷上的速率。

+
同步优先级速率有五种：

+
** 最低
** 低
** 中
** 高
** 最高
+
如果将同步优先级设置为最低速率、则会优先处理I/O活动、并且重新同步操作所需时间会更长。如果将同步优先级设置为最高比率、则会优先执行重新同步操作、但存储阵列的I/O活动可能会受到影响。

. 选择是手动还是自动重新同步远程存储阵列上的镜像对。
+
** *手动*(建议选项
)—选择此选项可要求在恢复与镜像对的通信后手动恢复同步。此选项提供了恢复数据的最佳机会。
** *自动*—选择此选项可在与镜像对的通信恢复后自动开始重新同步。
+
要手动恢复同步、请转到System Manager并选择菜单：Storage[Synchronous Mirroring]、在表中突出显示镜像对、然后在*更多*下选择*恢复*。

. 单击*完成*以完成同步镜像序列。

.结果
激活镜像后、系统将执行以下操作：

* 开始在本地存储阵列和远程存储阵列之间进行初始同步。
* 设置同步优先级和重新同步策略。
* 保留控制器HIC编号最高的端口以进行镜像数据传输。
+
只有镜像对中二级卷的远程首选控制器所有者才会接受在此端口上收到的I/O请求。(允许在主卷上进行预留。)

*
创建两个预留容量卷、每个控制器一个、用于记录写入信息、以便从控制器重置和其他临时中断中恢复。
+
每个卷的容量为128 MiB。但是、如果将卷放置在池中、则会为每个卷预留4 GiB。

.完成后
转到System Manager并选择菜单：主页(查看正在执行的操作
)以查看同步镜像操作的进度。此操作可能会很长，并且可能会影响系统性能。

```
:leveloffset: -1


= 常见问题解答

:leveloffset: +1


[[IDe964732b986a543adb046967ecf3d8c9]]
= 在创建镜像一致性组之前、我需要了解哪些信息?
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
在创建镜像一致性组之前、请遵循以下准则。

满足以下Unified Manager要求：

* Web服务代理服务必须正在运行。
* Unified Manager必须通过HTTPS连接在本地主机上运行。
* Unified Manager必须显示存储阵列的有效SSL证书。您可以使用Unified
Manager接受自签名证书或安装自己的安全证书、并导航到菜单：Certificate[证书管理]。


此外、请确保满足以下存储阵列要求：

* 必须在Unified Manager中发现这两个存储阵列。
* 每个存储阵列必须具有两个控制器。
* 主阵列和二级阵列中的每个控制器都必须配置一个以太网管理端口、并且必须连接到您的网络。
* 存储阵列的最低固件版本为7.84。(它们可以分别运行不同的操作系统版本。)
* 您必须知道本地和远程存储阵列的密码。
* 本地和远程存储阵列通过光纤通道网络结构或iSCSI接口进行连接。


[NOTE]
====
EF600或EF300存储系统不支持同步镜像。

====
```

[[ID12f885d636b146dbcb1c88b746d5cb3b]]
= 在创建镜像对之前、我需要了解哪些信息?
:allow-uri-read:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
创建镜像对之前、请遵循以下准则。

* 您必须有两个存储阵列。
* 每个存储阵列必须具有两个控制器。
* 必须在Unified Manager中发现这两个存储阵列。
* 主阵列和二级阵列中的每个控制器都必须配置一个以太网管理端口、并且必须连接到您的网络。
* 存储阵列的最低固件版本为7.84。(它们可以分别运行不同的操作系统版本。)
* 您必须知道本地和远程存储阵列的密码。
* 您必须在远程存储阵列上具有足够的可用容量、才能创建一个等于或大于要镜像的主卷的二级卷。
* 具有光纤通道(FC)或iSCSI主机端口的控制器支持异步镜像、而只有具有FC主机端口的控制器才支持同步镜像。

[NOTE]
====
EF600或EF300存储系统不支持同步镜像。

====

[[ID28901bd96a2440c32e3ac44bab05aa9b]]
= 为什么要更改此百分比?
:allow-uri-read:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
对于异步镜像操作、预留容量通常为基础卷的20%。通常、此容量足以满足要求。

所需容量因向基础卷写入I/O的频率和大小以及要使用存储对象的副本服务操作的时间而异。通常、如果存在以下一种或两种情况、请选择较大的预留容量百分比:

* 如果特定存储对象的复制服务操作的生命周期很长。

* 如果由于
I/O活动繁重而导致基础卷上的大量数据块发生更改、使用历史性能数据或其他操作系统实用程序帮助您确定基础卷的典型I/O活动。

[[IDf9832f196b1cb33093f9e93464d23810]]
= 为什么我会看到多个预留容量候选项?
:allow-uri-read:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
如果一个池或卷组中有多个卷满足您为存储对象选择的容量百分比量、则您将看到多个候选卷。

您可以通过更改要在基础卷上为复制服务操作预留的物理驱动器空间百分比来刷新建议候选对象列表。根据您的选择显示最佳候选对象。

[[ID6d4fddc678bff84d509c5ea37cff7912]]
= 为什么我看不到所有卷?
:allow-uri-read:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
为镜像对选择主卷时、列表将显示所有符合条件的卷。

不符合使用条件的任何卷不会显示在该列表中。由于以下任一原因、卷可能不符合条件：

* 此卷不是最佳卷。
* 此卷已加入镜像关系。
* 对于同步镜像、镜像对中的主卷和二级卷必须是标准卷。它们不能是精简卷或快照卷。
* 对于异步镜像、精简卷必须启用自动扩展。

NOTE: 对于EF600和
EF300控制器、异步镜像对中的主卷和二级卷必须匹配相同的协议、托盘级别、区块大小、安全类型和RAID级别。不符合条件的异步镜像对不会显示在可用卷列表中。

[[IDc596b7c9f9b4843a20b25fd1b5e6da6b]]
= 为什么我看不到远程存储阵列上的所有卷?
:allow-uri-read:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
在远程存储阵列上选择二级卷时、列表将显示该镜像对的所有符合条件的卷。

不符合使用条件的任何卷不会显示在该列表中。由于以下任一原因、卷可能不符合条件:

* 此卷是一个非标准卷、例如Snapshot卷。
* 此卷不是最佳卷。
* 此卷已加入镜像关系。
* 对于异步镜像、主卷和二级卷之间的精简卷属性不匹配。
* 如果您使用的是数据保证(Data Assurance、DA)、则主卷和二级卷必须具有相同的DA设置。
+
** 如果主卷已启用DA、则二级卷必须已启用DA。
** 如果主卷未启用DA、则二级卷不能启用DA。

* 对于异步镜像、主卷和二级卷必须具有相同的驱动器安全功能。
+
** 如果主卷支持FIPS,则二级卷必须支持FIPS.
** 如果主卷支持FDE,则二级卷必须支持FDE.
** 如果主卷未使用驱动器安全、则二级卷不得使用驱动器安全。

[[ID1d4396f3d0427634cc9996cc5e612ce1]]
= 同步优先级对同步速率有何影响?
:allow-uri-read:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
同步优先级用于定义为同步活动分配的处理时间与系统性能相关。

主卷的控制器所有者在后台执行此操作。同时、控制器所有者会处理对主卷的本地I/O写入以及对二级卷的相关远程写入。由于重新同步会使控制器处理资源偏离I/O活动、因此重新同步可能会影响主机应用程序的性能。

请牢记以下准则、以帮助您确定同步优先级可能需要多长时间以及同步优先级如何影响系统性能。

可以使用以下优先级：

* 最低
* 低
* 中
* 高
* 最高

最低优先级速率支持系统性能、但重新同步所需时间较长。最高优先级速率支持重新同步、但系统性能可能会受到影响。

这些准则大致近似于优先级之间的差异。

[cols="45h,~"]
|===
| 完全同步的优先级速率 | 与最高同步速率相比所用时间

a|
最低
a|
约为最高优先级速率的八倍。

a|
低
a|
约为最高优先级速率的六倍。

a|
中
a|
大约是最高优先级速率的三倍半。

a|

高
 a|
大约是最高优先级速率时的两倍。

|===
卷大小和主机I/O速率负载会影响同步时间比较。

[[ID18973f421374869d60cea4ad6f1f0813]]
= 为什么建议使用手动同步策略?
:allow-uri-read:
:icons: font
:relative_path: ./um-manage/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
建议使用手动重新同步、因为它可以让您以最佳机会恢复数据的方式管理重新同步过程。

如果使用自动重新同步策略、并且在重新同步期间发生间歇性通信问题、则二级卷上的数据可能会暂时损坏。重新同步完成后、数据将得到更正。

:leveloffset: -1

:leveloffset: -1

= 证书

:leveloffset: +1

[[ID28183d03f82ce35808c89d19ca5733d5]]
= 证书概述
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
通过证书管理、您可以创建证书签名请求(CSR)、导入证书以及管理现有证书。

== 什么是证书?

_Certificates_是数字文件、用于标识网站和服务器等联机实体、以便在互联网上进行安全通信。证书有两种类型：_signed certificate"由证书颁发机构(CA)验证；_self-signed certificate"由实体所有者(而不是第三方)验证。

了解更多信息。

* xref:{relative_path}how-certificates-work-unified.html["证书的工作原理"]
* xref:{relative_path}certificate-terminology-unified.html["证书术语"]

== 如何配置证书?

在证书管理中、您可以为托管Unified Manager的管理工作站配置证书、也可以为阵列中的控制器导入证书。

了解更多信息。

* xref:{relative_path}use-ca-signed-certificate-um.html["对管理系统使用CA签名的证书"]
* xref:{relative_path}import-array-certificates-unified.html["导入阵列的证书"]

= 概念

:leveloffset: +1

[[IDd7214153f52ac1d61ee8b281ea25c7fd]]
= 证书的工作原理
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
证书是数字文件、用于标识网站和服务器等在线实体、以实现Internet上的安全通信。

== 签名证书

证书可确保Web通信仅在指定服务器和客户端之间以加密格式单独传输、不会被更改。使用Unified Manager、您可以管理主机管理系统上的浏览器证书以及发现的存储阵列中的控制器证书。

证书可以由可信的颁发机构签名、也可以是自签名证书。"签名"只是指有人验证了所有者的身份并确定其设备可以受信任。存储阵列会在每个控制器上随附一个自动生成的自签名证书。您可以继续使用自签名证书、也可以获取CA签名证书、以便在控制器和主机系统之间建立更安全的连接。

[NOTE]
====
虽然CA签名证书可提供更好的安全保护(例如、防止中间人攻击)、但如果您的网络较大、则还需要支付昂贵的费用。相比之下、自签名证书的安全性较低、但它们是免费的。因此、自签名证书最常用于内部测试环境、而不是生产环境。

====
签名证书由可信的第三方组织证书颁发机构(CA)进行验证。签名证书包括有关实体(通常是服务器或网站)所有者的详细信息、证书问题描述
和到期日期、实体的有效域以及由字母和数字组成的数字签名。

当您打开浏览器并输入Web地址时、系统会在后台执行证书检查过程、以确定您是否要连接到包含有效的CA签名证书的网站。通常、使用签名证书进行安全保护的站点会在地址中包含挂锁图标和https标志。如果您尝试连接到不包含CA签名证书的网站、浏览器将显示一条警告、指出此站点不安全。

CA会在应用程序过程中执行一些步骤来验证您的身份。他们可能会向您的注册业务发送电子邮件、验证您的业务地址以及执行HTTP或DNS验证。应用程序过程完成后、CA会向您发送数字文件、以便在主机管理系统上加载。通常、这些文件包括以下信任链：

* *根*-层次结构顶部是根证书、其中包含用于对其他证书进行签名的专用密钥。根标识特定的CA组织。如果对所有网络设备使用相同的CA、则只需要一个根证书。
* *中间证书*—从根分层是中间证书。
CA颁发一个或多个中间证书、充当受保护根证书和服务器证书之间的中间人。
* *服务器
*—链的底部是服务器证书、用于标识您的特定实体、例如网站或其他设备。存储阵列中的每个控制器都需要一个单独的服务器证书。

== 自签名证书

存储阵列中的每个控制器都包含一个预安装的自签名证书。自签名证书与CA签名证书类似、只是它由实体所有者而非第三方进行验证。与CA签名证书一样、自签名证书也包含自己的专用密钥、并确保数据经过加密并通过HTTPS连接在服务器和客户端之间发送。

自签名证书不受浏览器"`信任`"。每次尝试连接到仅包含自签名证书的网站时、浏览器都会显示一条警告消息。您必须单击警告消息中允许您继续访问网站的链接；这样、您实际上就是在接受自签名证书。

== Unified Manager的证书

Unified Manager界面随Web服务代理一起安装在主机系统上。打开浏览器并尝试连接到Unified Manager时、浏览器会尝试通过检查数字证书来验证主机是否为可信源。如果浏览器找不到服务器的CA签名证书、则会打开一条警告消息。从该站点、您可以继续访问该网站以接受该会话的自签名证书。或者、您也可以从CA获取签名的数字证书、以便不再显示警告消息。

== 控制器的证书

在Unified Manager会话期间、当您尝试访问没有
CA签名证书的控制器时、可能会看到其他安全消息。在这种情况下、您可以永久信任自签名证书、也可以为控制器导入CA签名证书、以便Web服务代理服务器可以对来自这些控制器的传入客户端请求进行身份验证。

[[ID4054be4fb9a601d2b6b5ca116a0106df]]
= 证书术语
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
以下术语适用于证书管理。

[cols="25h,~"]
|===
| 期限 | 说明

a|
CA
a|
证书颁发机构(Certificate Authority、
CA)是一个受信任的实体、负责颁发称为数字证书的电子文档以确保Internet安全。这些证书用于标识网站所有者、从而可以在客户端和服务器之间建立安全连接。

a|
CSR
a|
证书签名请求(CSR)是从申请人发送给证书颁发机构(CA)的一条消息。CSR会验证CA对证书进行问题描述 所需的信息。

a|
证书
a|
出于安全考虑、证书用于标识站点所有者、从而防止攻击者模拟站点。此证书包含有关站点所有者的信息以及对此信息进行认证(签名)的可信实体的身份。

a|
证书链
a|
一种文件层次结构、用于向证书添加一层安全保护。通常、此链包含一个位于层次结构顶部的根证书、一个或多个中间证书以及用于标识实体的服务器证书。

a|
中间证书
a|
一个或多个中间证书从证书链中的根分支。CA颁发一个或多个中间证书、充当受保护根证书和服务器证书之间的中间人。

a|
密钥库
a|
密钥库是主机管理系统上的存储库、其中包含私钥及其对应的公有
密钥和证书。这些密钥和证书用于标识您自己的实体、例如控制器。

a|
根证书
a|
根证书位于证书链中的层次结构顶部、其中包含用于对其他证书签名的专用密钥。根标识特定的CA组织。如果对所有网络设备使用相同的CA、则只需要一个根证书。

a|
签名证书
a|
由证书颁发机构(CA)验证的证书。此数据文件包含一个专用密钥、可确保通过HTTPS连接在服务器和客户端之间以加密形式发送数据。此外、签名证书还包括实体所有者的详细信息(通常为服务器或网站)以及由字母和数字组成的数字签名。签名证书使用信任链、因此最常用于生产环境。也称为"CA签名证书"或"管理证书"。

a|
自签名证书
a|
自签名证书由实体的所有者进行验证。此数据文件包含一个专用密钥、可确保通过HTTPS连接在服务器和客户端之间以加密形式发送数据。它还包括由字母和数字组成的数字签名。自签名证书与CA签名证书使用的信任链不同、因此最常用于测试环境。也称为"预安装"证书。

a|
服务器证书
a|
服务器证书位于证书链的底部。它标识您的特定实体、例如网站或其他设备。存储系统中的每个控制器都需要一个单独的服务器证书。

a|
信任存储库
a|
信任存储库是一个存储库、其中包含来自CA等可信第三方的证书。

|===

:leveloffset: -1

[[ID2daf93bed23a6c4751116f9d344666a8]]
= 对管理系统使用CA签名的证书
:allow-uri-read:
:experimental:
:icons: font

```
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
您可以获取并导入CA签名的证书、以安全访问托管Unified Manager的管理系统。

.开始之前
您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示证书功能。

.关于此任务
使用CA签名证书是一个三步操作步骤。



== 第1步：完成CSR文件

您必须先生成证书签名请求(CSR)文件、用于标识您的组织以及安装了Web服务代理和Unified Manager的主机系统。

[NOTE]
====
或者，也可以使用OpenSSL等工具生成CSR文件，然后跳至<<第2步：提交CSR文件>>。

====
.步骤
. 选择*证书管理*。
. 从管理选项卡中、选择*完成CSR*。
. 输入以下信息、然后单击*下一步*：
+
** *组织*—贵公司或组织的法定全名。包括后缀、例如Inc.或Corp.
** *组织单位(可选)*—组织中负责处理证书的部门。
** *城市/位置*-主机系统或业务所在的城市。
** *省/自治区/直辖市(可选)*—主机系统或业务所在的省/自治区/直辖市。
** *国家/地区ISO代码*—您所在国家/地区的两位数ISO (国际标准化组织)代码、例如美国。


. 输入有关安装了Web服务代理的主机系统的以下信息：
+
** *公用名*—安装了Web服务代理的主机系统的IP地址或
DNS名称。请确保此地址正确无误；它必须与您在浏览器中输入的地址完全匹配才能访问Unified Manager。请勿包含http：//或https://.DNS名称不能以通配符开头。
** *备用IP地址*-如果公用名称为IP地址、则可以选择为主机系统输入任何其他
IP地址或别名。对于多个条目、请使用逗号分隔格式。
** *备用DNS名称*-如果公用名称为DNS名称、请输入主机系统的任何其他
DNS名称。对于多个条目、请使用逗号分隔格式。如果没有备用DNS名称、但您在第一个字段中输入了DNS名称、请将此名称复制到此处。DNS名称不能以通配符开头。
```

. 确保主机信息正确无误。否则、从CA返回的证书将在您尝试导入时失败。
. 单击 * 完成 * 。
. 转到。 <<第2步：提交CSR文件>>

== 第2步：提交CSR文件

创建证书签名请求(CSR)文件后、您可以将其发送到证书颁发机构(CA)、以接收托管Unified Manager和Web服务代理的系统的已签名管理证书。

NOTE: E系列系统要求对签名证书使用PEM格式(Base64 ASCII编码)、其中包括以下文件类型：.pem、.crt、.cer或.key。

.步骤
. 找到已下载的CSR文件。
+
下载内容的文件夹位置取决于您的浏览器。

. 将CSR文件提交到CA （例如VeriSign或DigiCert)、并请求PEM格式的签名证书。
+
[CAUTION]
====
*将CSR文件提交给CA后，请勿重新生成其他CSR文件。*每当生成CSR时、系统都会创建一个专用密钥对和公有 密钥对。公有 密钥是CSR的一部分、而私钥则保留在系统的密钥库中。当您收到签名证书并将其导入时、系统会确保私钥和公有 密钥都是原始对。如果密钥不匹配、则签名证书将不起作用、您必须从CA请求新证书。

====
. 当CA返回签名证书时，请转到<<第3步：导入管理证书>>。

== 第3步：导入管理证书

从证书颁发机构(CA)收到签名证书后、请将这些证书导入到安装了Web服务代理和Unified Manager界面的主机系统中。

.开始之前
* 您已从CA收到签名证书。这些文件包括根证书、一个或多个中间证书以及服务器证书。
* 如果CA提供了一个链式证书文件(例如.p7b文件)、则必须将链式文件解压缩到各个文件中：根证书、一个或多个中间证书以及服务器证书。您可以使

用Windows `certmgr`实用程序解压缩文件(右键单击并选择菜单：所有任务[导出])。建议使用64位编码。导出完成后、系统将为链中的每个证书文件显示一个CER"文件。
* 您已将证书文件复制到运行Web服务代理的主机系统。

.步骤
. 选择*证书管理*。
. 从管理选项卡中、选择*导入*。
+
此时将打开一个对话框、用于导入证书文件。

. 单击*浏览*以首先选择根证书和中间证书文件、然后选择服务器证书。如果从外部工具生成CSR、则还必须导入随CSR一起创建的私钥文件。
+
文件名将显示在对话框中。

. 单击 * 导入 * 。

.结果
这些文件将上传并进行验证。证书信息将显示在证书管理页面上。

[[IDc4523685ccf1c7e2bb5bc0b0b0dd4dfe]]
= 重置管理证书
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
您可以将管理证书还原到原始出厂自签名状态。

.开始之前
您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示证书功能。

.关于此任务
此任务将从安装了Web服务代理和Unified Manager的主机系统中删除当前管理证书。重置证书后、主机系统将恢复为使用自签名证书。

.步骤
. 选择*设置>证书*。
. 选择*阵列管理*选项卡，然后选择*重置*。
+
此时将打开确认重置管理证书对话框。

. 在字段中键入 `reset`，然后单击*Reset （重置）*。
+
浏览器刷新后、浏览器可能会阻止对目标站点的访问并报告此站点正在使用HTTP严格传输安全性。切换回自签名证书时会出现此情况。要清除阻止访问目标的条件、您必须从浏览器中清除浏览数据。

.结果
系统将恢复为使用服务器中的自签名证书。因此、系统会提示用户为其会话手动接受自签名证书。

= 使用阵列证书

:leveloffset: +1

[[IDb0ce0ebc2bbaef122943f2f98c9fdf98]]
= 导入阵列的证书
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
如有必要、您可以导入存储阵列的证书、以便这些阵列可以在托管Unified Manager的系统中进行身份验证。证书可以由证书颁发机构(CA)签名、也可以是自签名证书。

.开始之前
* 您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示证书功能。
* 如果要导入可信证书、则必须使用System Manager为存储阵列控制器导入这些证书。

.步骤
. 选择*证书管理*。
. 选择*可信*选项卡。
+
此页面显示为存储阵列报告的所有证书。

. 选择菜单：Import[证书]以导入CA证书、选择菜单：Import[自签名存储阵列证书]以导入自签名证书。
+
要限制此视图、您可以使用*显示证书...*筛选字段、也可以单击列标题之一对证书行进行排序。

. 在对话框中、选择证书、然后单击*导入*。
+
已上传并验证此证书。

[[IDbdc0feba254b70ae1fc78ceb5077a01c]]
= 删除可信证书
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
您可以删除一个或多个不再需要的证书、例如已过期的证书。

.开始之前
请先导入新证书、然后再删除旧证书。

[CAUTION]
====
请注意、删除根证书或中间证书可能会影响多个存储阵列、因为这些阵列可以共享相同的证书文件。

====
.步骤
. 选择*证书管理*。
. 选择*可信*选项卡。
. 在表中选择一个或多个证书、然后单击*删除*。
+
[NOTE]
====
对于预安装的证书、*删除*功能不可用。

====
+
此时将打开确认删除可信证书对话框。

. 确认删除、然后单击*删除*。
+
此证书将从表中删除。

```
[[ID18f8747c02c80f69fd5afce20560668c]]
= 解析不可信的证书
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
```
如果存储阵列尝试建立与Unified Manager的安全连接、但此连接无法确认为安全连接、则会发生不可信证书。

在证书页面中、您可以通过从存储阵列导入自签名证书或导入可信第三方颁发的证书颁发机构(CA)证书来解析不可信的证书。

.开始之前
* 您必须使用具有安全管理员权限的用户配置文件登录。
* 如果您计划导入CA签名的证书：
+
** 您已为存储阵列中的每个控制器生成证书签名请求(.csr文件)、并将其发送给CA。
** CA返回了可信证书文件。
** 证书文件可在本地系统上使用。

.关于此任务
如果满足以下任一条件、您可能需要安装其他受信任的CA证书：

* 您最近添加了一个存储阵列。
* 一个或两个证书均已过期。
* 一个或两个证书均已撤销。
* 一个或两个证书缺少根证书或中间证书。

.步骤
. 选择*证书管理*。
. 选择*可信*选项卡。
+
此页面显示为存储阵列报告的所有证书。

. 选择菜单：Import[证书]以导入CA证书、选择菜单：Import[自签名存储阵列证书]以导入自签名证书。
+
要限制此视图、您可以使用*显示证书...*筛选字段、也可以单击列标题之一对证书行进行排序。

. 在对话框中、选择证书、然后单击*导入*。
+
已上传并验证此证书。

:leveloffset: -1

= 管理证书

:leveloffset: +1

[[ID8845a8bb8e7d1ce44d5b92267b43ccc2]]
= 查看证书
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
您可以查看证书的摘要信息、其中包括使用证书的组织、颁发证书的机构、有效期以及指纹(唯一标识符)。

.开始之前
您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示证书功能。

.步骤
. 选择*证书管理*。
. 选择以下选项卡之一：
+
** *管理*-显示托管Web服务代理的系统的证书。管理证书可以是自签名证书、也可以由证书颁发机构(CA)批准。它允许安全访问Unified Manager。
** *可信*-显示Unified Manager可访问的存储阵列和其他远程服务器(例如LDAP服务器)的证书。证书可以从证书颁发机构(CA)颁发、也可以是自签名证书。

. 要查看有关证书的详细信息、请选择其行、选择行末尾的省略号、然后单击*查看*或*导出*。

```
[[IDd5c5e0b44001fd79af0f2980fe0f93dc]]
= 导出证书
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
您可以导出证书以查看其完整详细信息。

.开始之前
要打开导出的文件、您必须具有证书查看器应用程序。

.步骤
. 选择*证书管理*。
. 选择以下选项卡之一：
+
** *管理*-显示托管Web服务代理的系统的证书。管理证书可以是自签名证书、也可以由证书颁发机构(CA)批准。它允许安全访问Unified Manager。
** *可信*-显示Unified Manager可访问的存储阵列和其他远程服务器(例如LDAP服务器)的证书。证书可以从证书颁发机构(CA)颁发、也可以是自签名证书。


. 从页面中选择一个证书、然后单击行末尾的省略号。
. 单击*导出*、然后保存证书文件。
. 在证书查看器应用程序中打开文件。




:leveloffset: -1


:leveloffset: -1


= 访问管理

:leveloffset: +1


[[IDd89bad6a2f6776c112e0cd93545fcc51]]
= 访问管理概述
:allow-uri-read:
```

```
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
访问管理是一种在Unified Manager中配置用户身份验证的方法。



== 有哪些身份验证方法可用?

可以使用以下身份验证方法：

* *本地用户角色*—身份验证通过RBAC （基于角色的访问控制
)功能进行管理。本地用户角色包括预定义的用户配置文件以及具有特定访问权限的角色。
* *目录服务*—身份验证通过LDAP （轻型目录访问协议)服务器和目录服务(例如Microsoft
的Active Directory)进行管理。
* * SAML *-身份验证通过使用SAML 2.0的身份提供程序(Identity Provider、
IdP)进行管理。


了解更多信息。

* xref:{relative_path}how-access-management-works-
unified.html["访问管理的工作原理"]
* xref:{relative_path}access-management-terminology-
unified.html["访问管理术语"]
* xref:{relative_path}permissions-for-mapped-roles-
unified.html["映射角色的权限"]
* xref:{relative_path}access-management-with-saml.html["SAML"]




== 如何配置访问管理?

SANtricity 软件已预先配置为使用本地用户角色。如果要使用
LDAP、可以在访问管理页面下对其进行配置。

了解更多信息。

* xref:{relative_path}access-management-with-local-user-roles-
unified.html["具有本地用户角色的访问管理"]
* xref:{relative_path}access-management-with-directory-services-
unified.html["使用目录服务进行访问管理"]
* xref:{relative_path}configure-saml.html["配置SAML"]
```

= 概念

:leveloffset: +1

[[IDcc54af36e5b1b5a973ad0657badb78b9]]
= 访问管理的工作原理
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
使用访问管理在Unified Manager中建立用户身份验证。

== 配置工作流

访问管理配置的工作原理如下：

. 管理员使用包含安全管理员权限的用户配置文件登录到Unified Manager。
+
[NOTE]
====
对于首次登录、系统会自动显示用户名 `admin`、并且无法更改。
`admin`用户可以完全访问系统中的所有功能。必须在首次登录时设置密码。

====
. 管理员可在用户界面中导航到访问管理、其中包括预配置的本地用户角色。这些角色是对RBAC（基于角色的访问控制）功能的实施。
. 管理员配置以下一种或多种身份验证方法：
+
** *本地用户角色*—身份验证通过RBAC功能进行管理。本地用户角色包括具有特定访问权限的预定义用户和角色。管理员可以使用这些本地用户角色作为单一身份验证方法、也可以将其与目录服务结合使用。除了为用户设置密码之外、无需进行任何配置。
** *目录服务*—身份验证通过LDAP （轻型目录访问协议）服务器和目录服务（例如Microsoft的Active Directory）进行管理。管理员连接到LDAP服务器、然后将LDAP用户映射到本地用户角色。
** * SAML *-身份验证通过使用安全断言标记语言（SAML） 2.0的身份提供程序（IdP）进行管理。管理员在IdP系统和存储阵列之间建立通信、然后将IdP用户映射到存储阵列中嵌入

的本地用户角色。

. 管理员为用户提供Unified Manager的登录凭据。
. 用户通过输入凭据登录到系统。登录期间、系统将执行以下后台任务：
+
** 根据用户帐户对用户名和密码进行身份验证。
** 根据分配的角色确定用户的权限。
** 使用户能够访问用户界面中的功能。
** 在顶部横幅中显示用户名。

== Unified Manager中提供的功能

对功能的访问权限取决于为用户分配的角色、这些角色包括：

* *存储管理*—对阵列上的存储对象具有完全读/写访问权限、但无法访问安全配置。
* *安全管理*—访问访问管理和证书管理中的安全配置。
* *支持管理*—访问存储阵列上的所有硬件资源、故障数据和
MEL事件。无法访问存储对象或安全配置。
* *监控*—对所有存储对象的只读访问、但无法访问安全配置。

不可用的功能将灰显或不显示在用户界面中。

[[IDc416fcbfe5cbb93404fa9c3dd66e2ca6]]
= 访问管理术语
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
了解访问管理术语如何应用于Unified Manager。

[cols="25h,~"]
|===
| 期限 | 说明

a|
Active Directory
a|
Active Directory (AD)是一种Microsoft目录服务、使用LDAP进行Windows域网络。

a|
绑定
a|
绑定操作用于向目录服务器对客户端进行身份验证。绑定通常需要帐户和密码凭据、但某些服务器允许匿名绑定操作。

a|
CA
a|
证书颁发机构(Certificate Authority、
CA)是一个受信任的实体、负责颁发称为数字证书的电子文档以确保Internet安全。这些证书用于标识网站所有者、从而可以在客户端和服务器之间建立安全连接。

a|
证书
a|
出于安全考虑、证书用于标识站点所有者、从而防止攻击者模拟站点。此证书包含有关站点所有者的信息以及对此信息进行认证(签名)的可信实体的身份。

a|
LDAP
a|
轻型目录访问协议(Lightweight Directory Access Protocol、
LDAP)是一种用于访问和维护分布式目录信息服务的应用程序协议。此协议允许许多不同的应用程序和服务连接到LDAP服务器以验证用户。

a|
RBAC
a|
基于角色的访问控制(Role-Based Access Control、
RBAC)是一种根据各个用户的角色来管理对计算机或网络资源的访问的方法。Unified Manager包含预定义角色。

```
 a|
SAML
 a|
安全断言标记语言(SAML)是一种基于XML的标准、用于在两个实体之间进行身份验证和授权。SAML支持多因素身份验证、在这种身份验证中、用户必须提供两个或更多项来证明其身份(例如密码和指纹)。存储阵列的嵌入式SAML功能在身份断言、身份验证和授权方面符合SAML2.0标准。



 a|
SSO
 a|
单点登录(SSO)是一种身份验证服务、允许一组登录凭据访问多个应用程序。



 a|
Web服务代理
 a|
Web服务代理可通过标准HTTPS机制提供访问、允许管理员为存储阵列配置管理服务。代理可以安装在Windows或Linux主机上。Unified Manager界面可用于Web服务代理。

|===



[[ID037df1fbf0f7261f4821a85174c3372a]]
= 映射角色的权限
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
RBAC （基于角色的访问控制）
功能包括已映射一个或多个角色的预定义用户。每个角色都具有访问Unified Manager中任务的权限。

这些角色可为用户提供对任务的访问权限、如下所示：

* *存储管理*—对阵列上的存储对象具有完全读/写访问权限、但无法访问安全配置。
* *安全管理*—访问访问管理和证书管理中的安全配置。
* *支持管理*—访问存储阵列上的所有硬件资源、故障数据和
```

MEL事件。无法访问存储对象或安全配置。
* *监控*—对所有存储对象的只读访问、但无法访问安全配置。

如果用户没有对某个功能的权限、则该功能不可供选择或不会显示在用户界面中。

[[IDc7be912c51fe841562a425b79706074c]]
= 具有本地用户角色的访问管理
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
管理员可以使用Unified Manager中强制实施的RBAC （基于角色的访问控制）功能。这些功能称为"本地用户角色"。

== 配置工作流

本地用户角色已在系统中预先配置。要使用本地用户角色进行身份验证、管理员可以执行以下操作：

. 管理员使用包含安全管理员权限的用户配置文件登录到Unified Manager。
+
[NOTE]
====
 `admin`用户可以完全访问系统中的所有功能。

====
. 管理员会查看用户配置文件、这些配置文件是预定义的、无法修改。
. 管理员也可以为每个用户配置文件分配新密码。
. 用户使用分配的凭据登录到系统。

== 管理

如果仅使用本地用户角色进行身份验证、则管理员可以执行以下管理任务：

* 更改密码。
* 设置密码的最小长度。
* 允许用户在不使用密码的情况下登录。

[[ID343e8e95488d8723012aa17620fbdf0f]]
= 使用目录服务进行访问管理
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
管理员可以使用LDAP (轻型目录访问协议)服务器和目录服务、例如Microsoft的Active Directory。

== 配置工作流

如果在网络中使用LDAP服务器和目录服务、则配置的工作原理如下：

. 管理员使用包含安全管理员权限的用户配置文件登录到Unified Manager。
+
[NOTE]
====
 `admin`用户可以完全访问系统中的所有功能。

====
. 管理员输入LDAP服务器的配置设置。设置包括域名、URL和绑定帐户信息。
. 如果LDAP服务器使用安全协议(LDAPS)、则管理员将上传证书颁发机构(CA)证书链、以便在LDAP服务器与安装了Web服务代理的主机系统之间进行身份验证。
. 建立服务器连接后、管理员会将用户组映射到本地用户角色。这些角色是预定义的、无法修改。
. 管理员测试LDAP服务器与Web服务代理之间的连接。
. 用户使用其分配的LDAP/Directory服务凭据登录到系统。

== 管理

使用目录服务进行身份验证时、管理员可以执行以下管理任务：

* 添加目录服务器。
* 编辑目录服务器设置。
* 将LDAP用户映射到本地用户角色。
* 删除目录服务器。

* 更改密码。
* 设置密码的最小长度。
* 允许用户在不使用密码的情况下登录。

[[IDd7dad19d8c9a5c3a8c5a292ad6af5361]]
= 使用SAML进行访问管理
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
对于访问管理、管理员可以使用阵列中嵌入的安全断言标记语言(Security Assertion Markup Language、SAML) 2.0功能。

== 配置工作流

SAML配置的工作原理如下：

. 管理员使用包含"安全管理员"权限的用户配置文件登录到Unified Manager。
+
[NOTE]
====
 `admin`用户对System Manager中的所有功能具有完全访问权限。

====
. 管理员转到访问管理下的* SAML *选项卡。
. 管理员配置与身份提供程序(Identity Provider、IdP)的通信。
IdP是一种外部系统、用于向用户请求凭据并确定用户是否已成功通过身份验证。要配置与存储阵列的通信、管理员需要从Idp系统下载Idp元数据文件、然后使用Unified Manager将该文件上传到存储阵列。
. 管理员在服务提供商和IdP之间建立信任关系。服务提供商负责控制用户授权；在这种情况下、存储阵列中的控制器充当服务提供商。要配置通信、管理员可使用Unified Manager导出控制器的服务提供商元数据文件。然后、管理员会从Idp系统将元数据文件导入到Idp中。
+
[NOTE]
====
管理员还应确保IdP支持在身份验证时返回名称ID。

====
. 管理员会将存储阵列的角色映射到IdP中定义的用户属性。为此、管理员使用Unified Manager创建映射。
. 管理员测试对IdP URL的SSO登录。此测试可确保存储阵列和IdP能够进行通信。
+
[CAUTION]
====
启用SAML后、您无法通过用户界面将其禁用、也无法编辑IdP设置。如果需要禁用或编辑SAML配置、请联系技术支持以获得帮助。

====
. 在Unified Manager中、管理员可为存储阵列启用SAML。
. 用户使用其SSO凭据登录到系统。

== 管理

使用SAML进行身份验证时、管理员可以执行以下管理任务：

* 修改或创建新角色映射
* 导出服务提供商文件

== 访问限制

启用SAML后、用户无法从原有Storage Manager界面发现或管理该阵列的存储。

此外、以下客户端无法访问存储阵列服务和资源：

* 企业管理窗口(EMW)
* 命令行界面(CLI)
* 软件开发人员套件(SDK)客户端
* 带内客户端
* HTTP基本身份验证REST API客户端
* 使用标准REST API端点登录

:leveloffset: -1

= 使用本地用户角色

```
:leveloffset: +1


[[ID7b7da9d75a30c5f2e03c8c9b82435323]]
= 查看本地用户角色
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
在本地用户角色选项卡中、您可以查看用户与默认角色的映射。这些映射是Unified Manager Web服务代理中强制实施的RBAC （基于角色的访问控制）的一部分。

.开始之前
您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示访问管理功能。

.关于此任务
无法更改用户和映射。只能修改密码。

.步骤
. 选择*访问管理*。
. 选择*本地用户角色*选项卡。
+
下表显示了这些用户：

+
** *管理员*—超级管理员、有权访问系统中的所有功能。此用户包括所有角色。
** *存储*—负责所有存储配置的管理员。此用户包括以下角色：存储管理员、支持管理员和监控。
** *安全性
*—负责安全性配置的用户、包括访问管理和证书管理。此用户包括以下角色：安全管理员和监控。
** *支持*—负责硬件资源、故障数据和固件升级的用户。此用户包括以下角色：支持管理员和监控。
** *监控*—对系统具有只读访问权限的用户。此用户仅包含监控角色。
** *读/写*—此用户包括以下角色：存储管理员、支持管理员和监控。
** * ro *(只读)—此用户仅包含监控角色。




[[ID8e3554414b50f0f8d0c17a586835ec0e]]
= 更改本地用户配置文件的密码
:allow-uri-read:
:icons: font
```

```
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
您可以在Access Management中更改每个用户的用户密码。

.开始之前
* 您必须以本地管理员身份登录、其中包括root管理员权限。
* 您必须知道本地管理员密码。


.关于此任务
选择密码时、请记住以下准则：

* 任何新的本地用户密码必须满足或超过当前最低密码设置(在"查看/编辑设置"中)。
* 密码区分大小写。
* 设置密码时、不会从密码中删除尾随空格。如果密码中包含空格、请小心操作。
* 为了提高安全性、请至少使用15个字母数字字符并频繁更改密码。


.步骤
. 选择*访问管理*。
. 选择*本地用户角色*选项卡。
. 从表中选择一个用户。
+
更改密码按钮将变为可用。

. 选择 * 更改密码 * 。
+
此时将打开更改密码对话框。

. 如果未为本地用户密码设置最小密码长度、则可以选中此复选框以要求用户输入密码以访问系统。
. 在两个字段中输入选定用户的新密码。
. 输入本地管理员密码以确认此操作、然后单击*更改*。


.结果
如果用户当前已登录、则更改密码会导致用户的活动会话终止。



[[IDe00857dcc386ca00bf878937729c195e]]
= 更改本地用户密码设置
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
```

```
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
```
您可以为所有新的或更新的本地用户密码设置所需的最小长度。您还可以允许本地用户访问系统而无需输入密码。

.开始之前
您必须以本地管理员身份登录、其中包括root管理员权限。

.关于此任务
设置本地用户密码的最小长度时、请记住以下准则：

* 设置更改不会影响现有本地用户密码。
* 本地用户密码的最小长度设置必须介于0到30个字符之间。
* 任何新的本地用户密码都必须满足或超过当前的最小长度设置。
* 如果希望本地用户在未输入密码的情况下访问系统、请勿设置密码的最小长度。

.步骤
. 选择*访问管理*。
. 选择*本地用户角色*选项卡。
. 选择*查看/编辑设置*。
+
此时将打开本地用户密码设置对话框。

. 执行以下操作之一：
+
** 要允许本地用户在不输入密码的情况下访问系统、请清除"至少需要所有本地用户密码"复选框。
** 要为所有本地用户密码设置最小密码长度、请选中"要求所有本地用户密码至少为"复选框、然后使用spinner框设置所有本地用户密码所需的最小长度。
+
任何新的本地用户密码都必须满足或超过当前设置。

. 单击 * 保存 * 。

```
:leveloffset: -1


= 使用目录服务

:leveloffset: +1
```

```
[[ID20c6ae3599ace3b5e26ce8b0c188b957]]
= 添加目录服务器
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
要为访问管理配置身份验证、请在LDAP服务器与运行适用于Unified Manager的
Web服务代理的主机之间建立通信。然后、将LDAP用户组映射到本地用户角色。

.开始之前
* 您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示访问管理功能。
* 必须在目录服务中定义用户组。
* LDAP服务器凭据必须可用、包括域名、服务器URL以及可选的绑定帐户用户名和密码。
* 对于使用安全协议的LDAPS服务器、必须在本地计算机上安装LDAP服务器的证书链。


.关于此任务
添加目录服务器分为两步。首先输入域名和URL。如果服务器使用安全协议、则如果CA证书由非标准
签名颁发机构签名、则还必须上传此CA证书以进行身份验证。如果您拥有绑定帐户的凭据、则还可以
输入您的用户帐户名称和密码。接下来、将LDAP服务器的用户组映射到本地用户角色。

.步骤
. 选择*访问管理*。
. 从*目录服务*选项卡中、选择*添加目录服务器*。
+
此时将打开添加目录服务器对话框。

. 在*服务器设置*选项卡中、输入LDAP服务器的凭据。
+
.字段详细信息
[%collapsible]
====
[cols="25h,~"]
|===
| 设置 | 说明


 a|
*配置设置*
```

a|
域
a|
输入LDAP服务器的域名。对于多个域、请在逗号分隔列表中输入域。域名用于登录(_username_@_domain_)以指定要对其进行身份验证的目录服务器。

a|
服务器URL
a|
以的形式输入用于访问LDAP服务器的URL `ldap[s]://*host*:*port*`。

a|
上传证书(可选)
a|

NOTE：只有在上述服务器URL字段中指定了LDAPS协议时、才会显示此字段。

单击*浏览*并选择要上传的CA证书。这是用于对LDAP服务器进行身份验证的可信证书或证书链。

a|
绑定帐户(可选)
a|
输入一个只读用户帐户、用于对LDAP服务器进行搜索查询以及在组中进行搜索。以LDAP类型格式输入帐户名称。例如，如果绑定用户名为"bindacct"，则可以输入一个值，例如`CN=bindacct,CN=Users,DC=cpoc,DC=local`。

a|
绑定密码(可选)
a|

NOTE：输入绑定帐户时会显示此字段。

输入绑定帐户的密码。

a|
添加前测试服务器连接
a|

如果要确保系统可以与您输入的LDAP服务器配置进行通信、请选中此复选框。单击对话框底部的*添加*后、将进行测试。

如果选中此复选框且测试失败、则不会添加配置。您必须解决此错误或取消选中此复选框、才能跳过测试并添加配置。

a|
权限设置

a|
搜索基础DN
a|
输入LDAP环境以搜索用户，通常以的形式 `CN=Users, DC=cpoc, DC=local`。

a|
username属性
a|
输入绑定到用户ID的属性以进行身份验证。例如： `sAMAccountName`。

a|
组属性
a|
输入用户上的组属性列表、用于组到角色映射。例如： `memberOf, managedObjects`。

|===
====
. 单击*角色映射*选项卡。
. 将LDAP组分配给预定义角色。一个组可以分配多个角色。
+
.字段详细信息
[%collapsible]
====
[cols="25h,~"]
|===
| 设置 | 说明

a|
映射

```
 a|
组DN
 a|
为要映射的LDAP用户组指定组可分辨名称(DN)。支持正则表达式。如果这些特殊正则表达式字符不属于正则表达式模式、则必须使用反斜杠(\)进行转义：\.[] {} ()<>*+-=！？^$\



 a|
角色
 a|
单击此字段、然后选择要映射到组DN的本地用户角色之一。您必须单独为此组选择要包含的每个角色。要登录到SANtricity Unified
Manager、需要将监控角色与其他角色结合使用。映射的角色包括以下权限：

** *存储管理*—对阵列上的存储对象具有完全读/写访问权限、但无法访问安全配置。
** *安全管理*—访问访问管理和证书管理中的安全配置。
** *支持管理*—访问存储阵列上的所有硬件资源、故障数据和
MEL事件。无法访问存储对象或安全配置。
** *监控*—对所有存储对象的只读访问、但无法访问安全配置。


|===
====
+

NOTE：包括管理员在内的所有用户都需要"监控"角色。

. 如果需要、请单击*添加另一个映射*以输入更多组到角色的映射。
. 完成映射后、单击*添加*。
+
系统将执行验证、以确保存储阵列和LDAP服务器可以进行通信。如果显示错误消息、请检查在对话框中输入的凭据、并根据需要重新输入信息。




[[IDd27aa93506e7a05bd42bc5b6399a0642]]
= 编辑目录服务器设置和角色映射
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/
```

[role="lead"]
如果您之前在Access Management中配置了目录服务器、则可以随时更改其设置。设置包括服务器连接信息和组到角色映射。

.开始之前
* 您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示访问管理功能。
* 必须定义目录服务器。

.步骤
. 选择*访问管理*。
. 选择*目录服务*选项卡。
. 如果定义了多个服务器、请从表中选择要编辑的服务器。
. 选择*查看/编辑设置*。
+
此时将打开目录服务器设置对话框。

. 在*服务器设置*选项卡中、更改所需设置。
+
.字段详细信息
[%collapsible]
====
[cols="25h,~"]
|===
| 设置 | 说明

a|
配置设置

a|
域
a|
LDAP服务器的域名。对于多个域、请在逗号分隔列表中输入域。域名用于登录(_username_@_domain_)以指定要对其进行身份验证的目录服务器。

a|
服务器URL
a|
用于访问LDAP服务器的URL，格式为 `ldap[s]://host:port`。

a|
绑定帐户（可选）
a|
用于对LDAP服务器进行搜索查询以及在组内进行搜索的只读用户帐户。

a|
绑定密码（可选）
a|
绑定帐户的密码。（输入绑定帐户时会显示此字段。）

a|
保存前测试服务器连接
a|
检查系统是否可以与LDAP服务器配置进行通信。单击*保存*后会进行测试。如果选中此复选框且测试失败、则不会更改配置。您必须解决此错误或清除此复选框、才能跳过测试并重新编辑配置。

a|
权限设置

a|
搜索基础DN
a|
用于搜索用户的LDAP环境，通常采用的形式 `CN=Users, DC=cpoc, DC=local`。

a|
username属性
a|
绑定到用户ID进行身份验证的属性。例如：
`sAMAccountName`。

a|
组属性

```
 a|
用户上的组属性列表、用于组到角色映射。例如：
`memberOf, managedObjects`。

|===
====
. 在*角色映射*选项卡中、更改所需的映射。
+
.字段详细信息
[%collapsible]
====
[cols="25h,~"]
|===
| 设置 | 说明


 a|
*映射*



 a|
组DN
 a|
要映射的LDAP用户组的域名。支持正则表达式。如果这些特殊正则表达式字符不属于正则表达式模式、则必须使用反斜杠(\)进行转义：

\.[] {} ()<>*+-=! ？ ^$|



 a|
角色
 a|
要映射到组DN的角色。您必须单独为此组选择要包含的每个角色。要登录到SANtricity Unified Manager、需要将监控角色与其他角色结合使用。这些角色包括：

** *存储管理*—对阵列上的存储对象具有完全读/写访问权限、但无法访问安全配置。
** *安全管理*—访问访问管理和证书管理中的安全配置。
** *支持管理*—访问存储阵列上的所有硬件资源、故障数据和
MEL事件。无法访问存储对象或安全配置。
** *监控*—对所有存储对象的只读访问、但无法访问安全配置。


|===
====
+
```

NOTE: 包括管理员在内的所有用户都需要"监控"角色。

. 如果需要、请单击*添加另一个映射*以输入更多组到角色的映射。
. 单击 * 保存 * 。

.结果
完成此任务后、所有活动用户会话都将终止。仅会保留当前用户会话。

[[ID134af0d7ea0e1b09a03be3748a713eb9]]
= 删除目录服务器
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
要中断目录服务器与Web服务代理之间的连接、您可以从"访问管理"页面中删除服务器信息。如果您配置了新服务器、然后要删除旧服务器、则可能需要执行此任务。

.开始之前
您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示访问管理功能。

.关于此任务
完成此任务后、所有活动用户会话都将终止。仅会保留当前用户会话。

.步骤
. 选择*访问管理*。
. 选择*目录服务*选项卡。
. 从列表中、选择要删除的目录服务器。
. 单击 * 删除 * 。
+
此时将打开删除目录服务器对话框。

. 键入 `remove`字段，然后单击*Remove*。
+
此时将删除目录服务器配置设置、权限设置和角色映射。用户无法再使用此服务器的凭据登录。

:leveloffset: -1

```
= 使用SAML

:leveloffset: +1


[[ID7b0676e4c0539e10d5218614cc341a2f]]
= 配置SAML
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
要为访问管理配置身份验证、您可以使用存储阵列中嵌入的安全断言标记语言(SAML)功能。此配置将在身份提供程序和存储提供程序之间建立连接。

.开始之前
* 您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示访问管理功能。
* 您必须知道存储阵列中控制器的IP地址或域名。
* IdP管理员已配置IdP系统。
* IdP管理员已确保IdP支持在身份验证时返回名称ID。
* 管理员已确保IdP服务器和控制器时钟同步(通过NTP服务器或通过调整控制器时钟设置)。
* Idp元数据文件将从Idp系统下载、并可在用于访问Unified Manager的本地系统上使用。


.关于此任务
身份提供程序(IdP)是一种外部系统、用于向用户请求凭据并确定该用户是否已成功通过身份验证。可以将IdP配置为提供多因素身份验证并使用任何用户数据库、例如Active Directory。您的安全团队负责维护IdP。服务提供商(Service Provider、SP)是一个控制用户身份验证和访问的系统。使用SAML配置访问管理时、存储阵列充当服务提供商、向身份提供程序请求身份验证。要在IdP和存储阵列之间建立连接、您需要在这两个实体之间共享元数据文件。接下来、将IdP用户实体映射到存储阵列角色。最后、在启用SAML之前、您需要测试连接和SSO登录。

[NOTE]
====
* SAML和目录服务*。如果在将目录服务配置为身份验证方法时启用SAML、则SAML将取代Unified Manager中的目录服务。如果稍后禁用SAML、则目录服务配置将返回到其先前的配置。

====
[CAUTION]
====
*编辑和禁用。*启用SAML后、您无法通过用户界面将其禁用、也无法编辑IdP设置。如果需要禁用或
```

编辑SAML配置、请联系技术支持以获得帮助。

====
配置SAML身份验证是一个多步骤操作步骤。

== 第1步：上传IdP元数据文件

要为存储阵列提供Idp连接信息、请将Idp元数据导入到Unified Manager中。
IdP系统需要使用此元数据将身份验证请求重定向到正确的URL并验证收到的响应。

.步骤
. 选择菜单：设置[访问管理]。
. 选择*SAML*选项卡。
+
此页面将显示配置步骤的概述。

. 单击*导入身份提供程序(IdP)文件*链接。
+
此时将打开导入身份提供程序文件对话框。

. 单击*浏览*以选择您复制到本地系统的IdP元数据文件并将其上传。
+
选择文件后、将显示IdP实体ID。

. 单击 * 导入 * 。

== 第2步：导出服务提供商文件

要在IdP和存储阵列之间建立信任关系、请将服务提供商元数据导入到IdP中。Idp需要此元数据才能与控制器建立信任关系并处理授权请求。此文件包含控制器域名或IP地址等信息、以便IdP可以与服务提供商进行通信。

.步骤
. 单击*导出服务提供商文件*链接。
+
此时将打开导出服务提供商文件对话框。

. 在*控制器A*字段中输入控制器IP地址或DNS名称、然后单击*导出
*将元数据文件保存到本地系统。
+
单击*导出*后、服务提供商元数据将下载到本地系统。记下文件的存储位置。

. 从本地系统中、找到您导出的XML格式的服务提供商元数据文件。
. 从
Idp服务器中、导入服务提供商元数据文件以建立信任关系。您可以直接导入文件、也可以手动输入文件中的控制器信息。

== 第3步：映射角色

要为用户提供对Unified Manager的授权和访问权限、您必须将
Idp用户属性和组成员资格映射到存储阵列的预定义角色。

.开始之前
* IdP管理员已在IdP系统中配置用户属性和组成员资格。
* Idp元数据文件将导入到Unified Manager中。
* 将控制器的服务提供商元数据文件导入到Idp系统中以建立信任关系。

.步骤
. 单击*映射Unified Manager*角色的链接。
+
此时将打开角色映射对话框。

. 为预定义角色分配IdP用户属性和组。一个组可以分配多个角色。
+
.字段详细信息
[%collapsible]
====
[cols="25h,~"]
|===
| 设置 | 说明

a|
映射

a|
用户属性
a|
指定要映射的SAML组的属性(例如、"member for")。

a|

属性值

 a|
指定要映射的组的属性值。支持正则表达式。(`\`如果这些特殊正则表达式字符不属于正则表达式模式，则必须使用反斜杠转义：\.[] {} ()<>*+=!?^$|

 a|
角色

 a|
单击此字段、然后选择要映射到此属性的存储阵列角色之一。您必须单独选择要包括的每个角色。要登录到Unified Manager、需要将"监控
"角色与其他角色结合使用。至少一个组还需要安全管理员角色。

映射的角色包括以下权限：

** *存储管理*—对存储对象(例如卷和磁盘池)具有完全读/写访问权限、但无法访问安全配置。
** *安全管理
*—访问访问管理、证书管理、审核日志管理中的安全配置、以及打开或关闭原有管理界面(符号)的功能。
** *支持管理*—访问存储阵列上的所有硬件资源、故障数据、
MEL事件和控制器固件升级。无法访问存储对象或安全配置。
** *监控*—对所有存储对象的只读访问、但无法访问安全配置。

|===
====
+
[NOTE]
====
包括管理员在内的所有用户都需要"监控"角色。如果没有"监控"角色、则Unified
Manager将无法对任何用户正常运行。

====
. 如果需要、请单击*添加另一个映射*以输入更多组到角色的映射。
+
[NOTE]
====
启用SAML后、可以修改角色映射。

====
. 完成映射后、单击*保存*。

== 第4步：测试SSO登录

为了确保IdP系统和存储阵列可以进行通信、您可以选择测试SSO登录。在启用SAML的最后一步中、也会执行此测试。

.开始之前
* Idp元数据文件将导入到Unified Manager中。
* 将控制器的服务提供商元数据文件导入到Idp系统中以建立信任关系。

.步骤
. 选择*测试SSO登录*链接。
+
此时将打开一个对话框、用于输入SSO凭据。

. 输入具有安全管理员权限和监控权限的用户的登录凭据。
+
在系统测试登录时、将打开一个对话框。

. 查找Test Successful消息。如果测试成功完成、请转至下一步以启用SAML。
+
如果测试未成功完成、则会显示一条错误消息、其中包含更多信息。请确保：

+
** 该用户属于具有安全管理员和监控权限的组。
** 您为IdP服务器上传的元数据正确无误。
** SP元数据文件中的控制器地址正确。

== 第5步：启用SAML

最后一步是完成用户身份验证的SAML配置。在此过程中、系统还会提示您测试SSO登录。上一步介绍了SSO登录测试过程。

.开始之前
* Idp元数据文件将导入到Unified Manager中。
* 将控制器的服务提供商元数据文件导入到Idp系统中以建立信任关系。
* 至少配置了一个监控器和一个安全管理员角色映射。

[CAUTION]
====
*编辑和禁用。*启用SAML后、您无法通过用户界面将其禁用、也无法编辑IdP设置。如果需要禁用或编辑SAML配置、请联系技术支持以获得帮助。

====
.步骤
. 从* SAML *选项卡中、选择*启用SAML *链接。
+
此时将打开确认启用SAML对话框。

. 键入 `enable`，然后单击*Enable*。
. 输入用于SSO登录测试的用户凭据。

.结果
系统启用SAML后、它将终止所有活动会话并开始通过SAML对用户进行身份验证。

[[ID29f598141840bf9a9e007d8afa831c2a]]
= 更改SAML角色映射
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
如果先前已为访问管理配置SAML、则可以更改IdP组与存储阵列的预定义角色之间的角色映射。

.开始之前
* 您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示访问管理功能。
* IdP管理员已在IdP系统中配置用户属性和组成员资格。
* 已配置并启用SAML。

.步骤
. 选择菜单：设置[访问管理]。
. 选择*SAML*选项卡。
. 选择*角色映射*。
+
此时将打开角色映射对话框。

. 为预定义角色分配IdP用户属性和组。一个组可以分配多个角色。
+
[CAUTION]
====
请注意、在启用SAML的情况下、不要删除您的权限、否则您将无法访问Unified Manager。

```
====
+
.字段详细信息
[%collapsible]
====
[cols="25h,~"]
|===
| 设置 | 说明


 a|
*映射*


 a|
用户属性
 a|
指定要映射的SAML组的属性(例如、"member for")。


 a|
属性值
 a|
指定要映射的组的属性值。


 a|
角色
 a|
单击此字段、然后选择要映射到此属性的存储阵列角色之一。您必须单独为此组选择要包含的每个角色。要登录到Unified Manager、需要将"监控
"角色与其他角色结合使用。必须至少将安全管理员角色分配给一个组。映射的角色包括以下权限：

** *存储管理*—对存储对象(例如卷和磁盘池)具有完全读/写访问权限、但无法访问安全配置。
** *安全管理
*—访问访问管理、证书管理、审核日志管理中的安全配置、以及打开或关闭原有管理界面(符号)的功能。
** *支持管理*—访问存储阵列上的所有硬件资源、故障数据、
MEL事件和控制器固件升级。无法访问存储对象或安全配置。
** *监控*—对所有存储对象的只读访问、但无法访问安全配置。


|===
====
```

+

NOTE：包括管理员在内的所有用户都需要"监控"角色。如果没有"监控"角色、则Unified Manager将无法对任何用户正常运行。

. 或者、也可以单击*添加另一个映射*以输入更多组到角色的映射。
. 单击 * 保存 * 。

.结果
完成此任务后、所有活动用户会话都将终止。仅会保留当前用户会话。

[[ID8062a517f58cfec4e9df2c141547599a]]
= 导出SAML服务提供程序文件
:allow-uri-read:
:experimental:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
如有必要、您可以导出存储阵列的服务提供程序元数据、然后将该文件重新导入到身份提供程序(Identity Provider、Idp)系统中。

.开始之前
* 您必须使用包含安全管理员权限的用户配置文件登录。否则、不会显示访问管理功能。
* 已配置并启用SAML。

.关于此任务
在此任务中、您将从控制器导出元数据。Idp需要此元数据才能与控制器建立信任关系并处理身份验证请求。此文件包含IdP可用于发送请求的控制器域名或IP地址等信息。

.步骤
. 选择菜单：设置[访问管理]。
. 选择*SAML*选项卡。
. 选择*导出*。
+
此时将打开导出服务提供商文件对话框。

. 单击*Export*将元数据文件保存到本地系统。
+
[NOTE]
====

域名字段为只读。

====
+
记下文件的存储位置。

. 从本地系统中、找到您导出的XML格式的服务提供商元数据文件。
. 从
Idp服务器中、导入服务提供商元数据文件。您可以直接导入文件、也可以手动输入控制器信息。
. 单击 * 关闭 * 。

:leveloffset: -1

= 常见问题解答

:leveloffset: +1

[[ID7b8a63bb52ec66aeb26c640b829f2d60]]
= 为什么我无法登录?
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
如果在尝试登录时收到错误、请查看这些可能的原因。

出现登录错误的原因可能如下：

* 您输入的用户名或密码不正确。
* 您的权限不足。
* 您尝试多次登录失败、从而触发锁定模式。等待10分钟以重新登录。
* 已启用SAML身份验证。刷新浏览器以登录。

[[IDf8ac1260fa013754872f42bd541b518c]]
= 在添加目录服务器之前、我需要了解哪些信息?
:allow-uri-read:
:icons: font

```
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
在Access Management中添加目录服务器之前、您必须满足特定要求。

* 必须在目录服务中定义用户组。
* LDAP服务器凭据必须可用、包括域名、服务器URL以及可选的绑定帐户用户名和密码。
* 对于使用安全协议的LDAPS服务器、必须在本地计算机上安装LDAP服务器的证书链。




[[IDebe9cb8bb93503ff20647c824dcec14e]]
= 关于映射到存储阵列角色、我需要了解哪些信息?
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/


[role="lead"]
在将组映射到角色之前、请查看相关准则。

RBAC （基于角色的访问控制）功能包括以下角色：

* *存储管理*—对阵列上的存储对象具有完全读/写访问权限、但无法访问安全配置。
* *安全管理*—访问访问管理和证书管理中的安全配置。
* *支持管理*—访问存储阵列上的所有硬件资源、故障数据和
MEL事件。无法访问存储对象或安全配置。
* *监控*—对所有存储对象的只读访问、但无法访问安全配置。


[NOTE]
====
包括管理员在内的所有用户都需要"监控"角色。

====
如果您使用的是LDAP （轻型目录访问协议）服务器和目录服务、请确保：

* 管理员已在目录服务中定义用户组。
* 您知道LDAP用户组的组域名。
```

== SAML

如果您使用的是存储阵列中嵌入的安全断言标记语言(SAML)功能、请确保：

* 身份提供程序(Identity Provider、IdP)管理员已在IdP系统中配置用户属性和组成员资格。
* 您知道组成员资格名称。
* 您知道要映射的组的属性值。支持正则表达式。
(`\`如果这些特殊正则表达式字符不属于正则表达式模式，则必须使用反斜线转义：
+
[listing]

\.[]{}()<>*+-=!?^$|
----
* 包括管理员在内的所有用户都需要"监控"角色。如果没有"监控"角色、则Unified Manager将无法对任何用户正常运行。

[[ID7b73d9c8e69515eed4bf89461694a8e2]]
= 在配置和启用SAML之前、我需要了解哪些信息?
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
在配置和启用安全断言标记语言(SAML)身份验证功能之前、请确保满足以下要求并了解SAML限制。

== 要求

开始之前、请确保：

* 已在网络中配置身份提供程序(Identity Provider、IdP)。
IdP是一种外部系统、用于向用户请求凭据并确定用户是否已成功通过身份验证。您的安全团队负责维护IdP。
* IdP管理员已在IdP系统中配置用户属性和组。
* IdP管理员已确保IdP支持在身份验证时返回名称ID。
* 管理员已确保IdP服务器和控制器时钟同步(通过NTP服务器或通过调整控制器时钟设置)。
* Idp元数据文件将从Idp系统下载、并在用于访问Unified Manager的本地系统上可用。
* 您知道存储阵列中控制器的IP地址或域名。

== 限制

除了上述要求之外、请确保您了解以下限制：

* 启用SAML后、您无法通过用户界面将其禁用、也无法编辑IdP设置。如果需要禁用或编辑SAML配置、请联系技术支持以获得帮助。建议您先测试SSO登录、然后再在最终配置步骤中启用SAML。（系统还会在启用SAML之前执行SSO登录测试。）
* 如果您将来禁用SAML、则系统会自动还原先前的配置（本地用户角色和/或目录服务）。
* 如果当前已为用户身份验证配置目录服务、则SAML将覆盖此配置。
* 配置SAML后、以下客户端将无法访问存储阵列资源：
+
** 企业管理窗口（EMW）
** 命令行界面（CLI）
** 软件开发人员套件（SDK）客户端
** 带内客户端
** HTTP基本身份验证REST API客户端
** 使用标准REST API端点登录

[[ID8d1ce000fe00069224037ac3aee0cc21]]
= 本地用户有哪些?
:allow-uri-read:
:icons: font
:relative_path: ./um-certificates/
:imagesdir: {root_path}{relative_path}../media/

[role="lead"]
本地用户在系统中预定义、并包括特定权限。

本地用户包括：

* *管理员
*—超级管理员、有权访问系统中的所有功能。此用户包括所有角色。必须在首次登录时设置密码。
* *存储
*—负责所有存储配置的管理员。此用户包括以下角色：存储管理员、支持管理员和监控。在设置密码之前，此帐户将被禁用。
* *安全性
*—负责安全性配置的用户、包括访问管理和证书管理。此用户包括以下角色：安全管理员和监控。在设置密码之前，此帐户将被禁用。
* *支持
*—负责硬件资源、故障数据和固件升级的用户。此用户包括以下角色：支持管理员和监控。在设置密

码之前，此帐户将被禁用。
* *监控
*—对系统具有只读访问权限的用户。此用户仅包含监控角色。在设置密码之前，此帐户将被禁用。
* *读/写
*—此用户包括以下角色：存储管理员、支持管理员和监控。在设置密码之前，此帐户将被禁用。
* * ro *(只读)—此用户仅包含监控角色。在设置密码之前，此帐户将被禁用。

:leveloffset: -1

:leveloffset: -1

:leveloffset: -1

:leveloffset: -1

<<<
版权信息