了解 NAS 文件访问

ONTAP 9

NetApp
September 12, 2024

目录

了解 NAS 文件访问

命名空间和接合点

命名空间和接合点概述

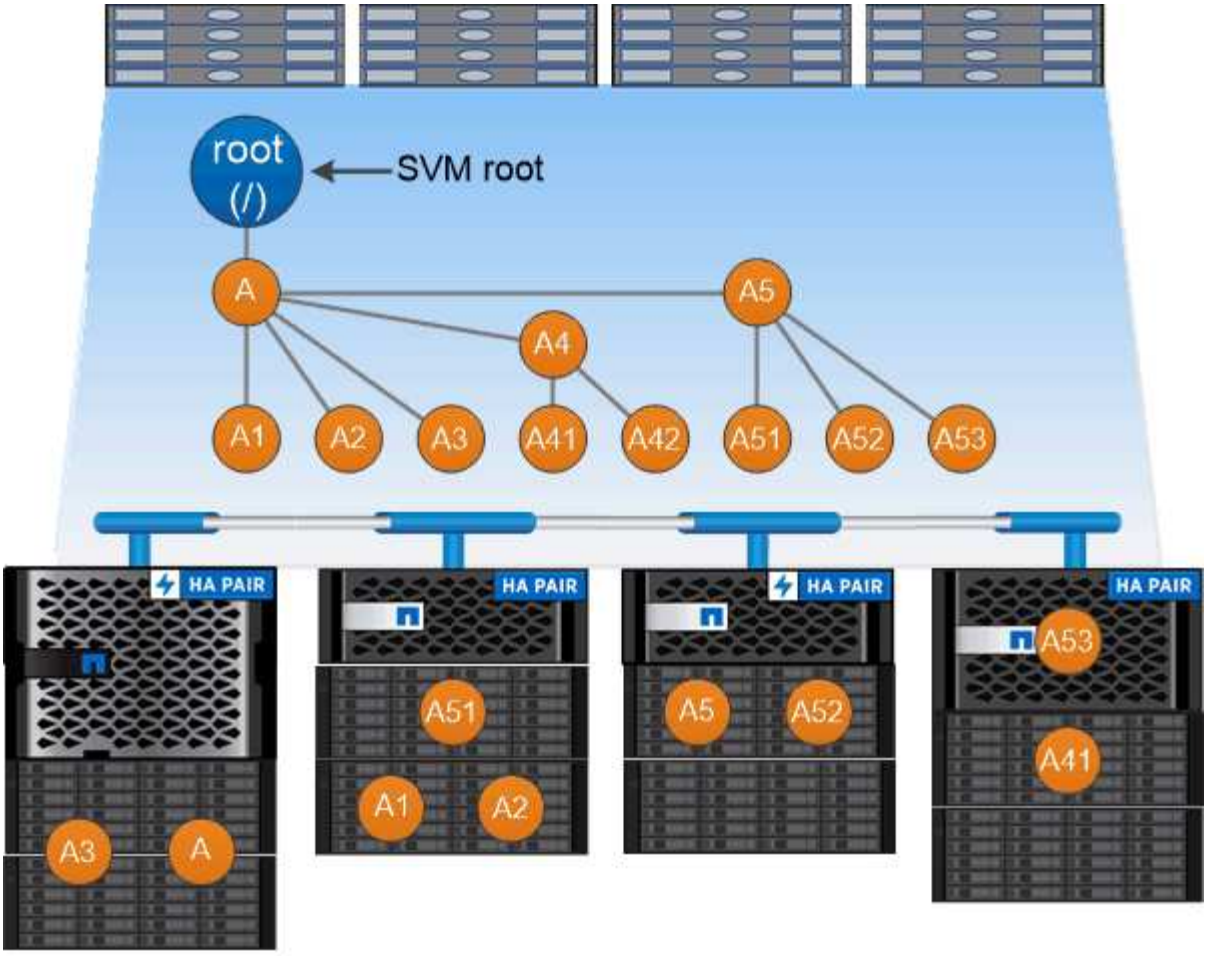
nas_namespaces_ 是指在 *junction points* 处联合在一起的卷的逻辑分组，用于创建单个文件系统层次结构。具有足够权限的客户端可以访问命名空间中的文件，而无需指定文件在存储中的位置。集群中的任何位置都可以驻留未分配的卷。

NAS 客户端不会挂载包含相关文件的每个卷，而是挂载 nfs *export* 或访问 SMB _share 。 _ 导出或共享表示整个命名空间或命名空间中的中间位置。客户端仅访问挂载在其访问点下方的卷。

您可以根据需要向命名空间添加卷。您可以直接在父卷接合下方或卷中的目录上创建接合点。名为"`vol3`"的卷的卷接合路径可能为 `/vol1/vol2/vol3`或 `/vol1/dir2/vol3`，甚至 `/dir1/dir2/vol3`。此路径称为 _junction path…

每个 SVM 都有一个唯一的命名空间。SVM 根卷是命名空间层次结构的入口点。

> 要确保在发生节点中断或故障转移时数据仍然可用，您应为 SVM 根卷创建一个 *load-sharing mirror* 副本。



A namespace is a logical grouping of volumes joined together at junction points to create a single file system hierarchy.

示例

以下示例将在` SVM VS1上创建一个具有接合路径的名为"`home"的卷 `/eng/home`：

```
cluster1::> volume create -vserver vs1 -volume home4 -aggregate aggr1
-size 1g -junction-path /eng/home
[Job 1642] Job succeeded: Successful
```

什么是典型的 **NAS** 命名空间架构

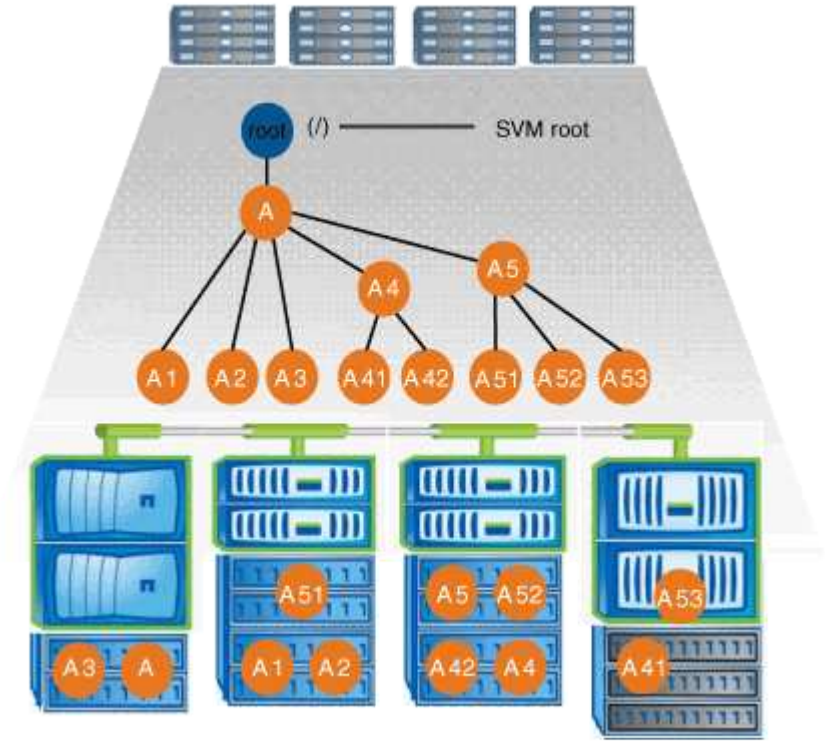
在创建 SVM 名称空间时，您可以使用几种典型的 NAS 命名空间架构。您可以选择符合业务和工作流需求的命名空间架构。

命名空间的顶部始终为根卷，以斜杠（/）表示。根下的命名空间架构分为三个基本类别：

- 一个分支树，与命名空间根只有一个接合点
- 多个分支树，多个接合点指向命名空间的根
- 多个独立卷，每个卷都有一个指向名称空间根的单独接合点

包含单个分支树的命名空间

包含单个分支树的架构在 SVM 命名空间的根上具有一个插入点。单个插入点可以是接合卷，也可以是根下的目录。所有其他卷都挂载在单个插入点（可以是卷或目录）下的接合点处。

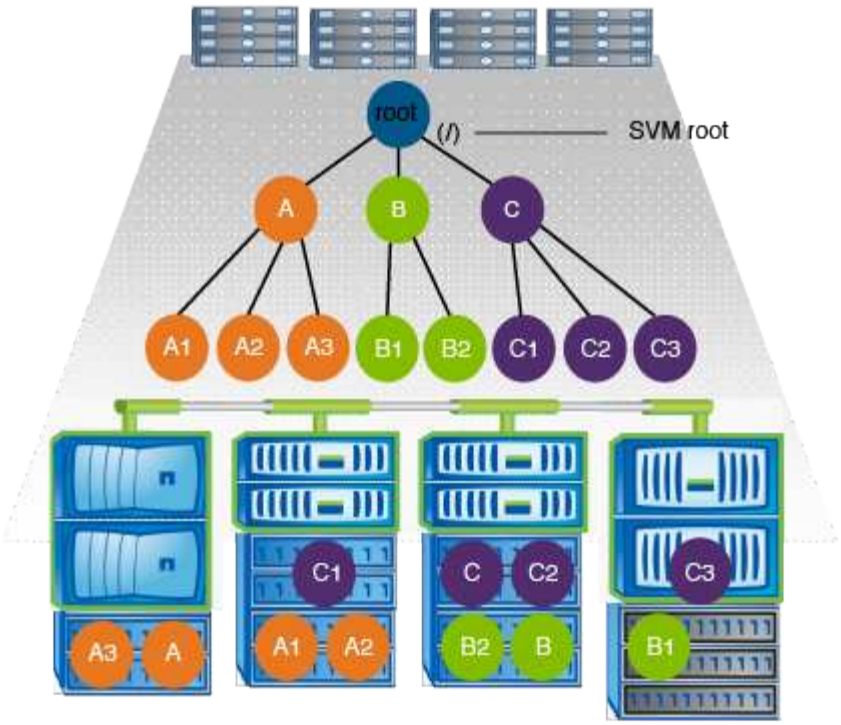


例如，具有上述命名空间架构的典型卷接合配置可能类似于以下配置，其中所有卷都在单个插入点（即名为 `data` 的目录）下接合：

```
                      Junction                          Junction
Vserver Volume        Active   Junction Path            Path Source
------- ------------ -------- -------------------      -----------
vs1     corp1        true     /data/dir1/corp1         RW_volume
vs1     corp2        true     /data/dir1/corp2         RW_volume
vs1     data1        true     /data/data1              RW_volume
vs1     eng1         true     /data/data1/eng1         RW_volume
vs1     eng2         true     /data/data1/eng2         RW_volume
vs1     sales        true     /data/data1/sales        RW_volume
vs1     vol1         true     /data/vol1               RW_volume
vs1     vol2         true     /data/vol2               RW_volume
vs1     vol3         true     /data/vol3               RW_volume
vs1     vs1_root     -        /                        -
```

包含多个分支树的命名空间

包含多个分支树的架构在 SVM 命名空间的根目录中具有多个插入点。插入点可以是接合卷，也可以是根下的目录。所有其他卷都挂载在插入点下方的接合点（可以是卷或目录）。

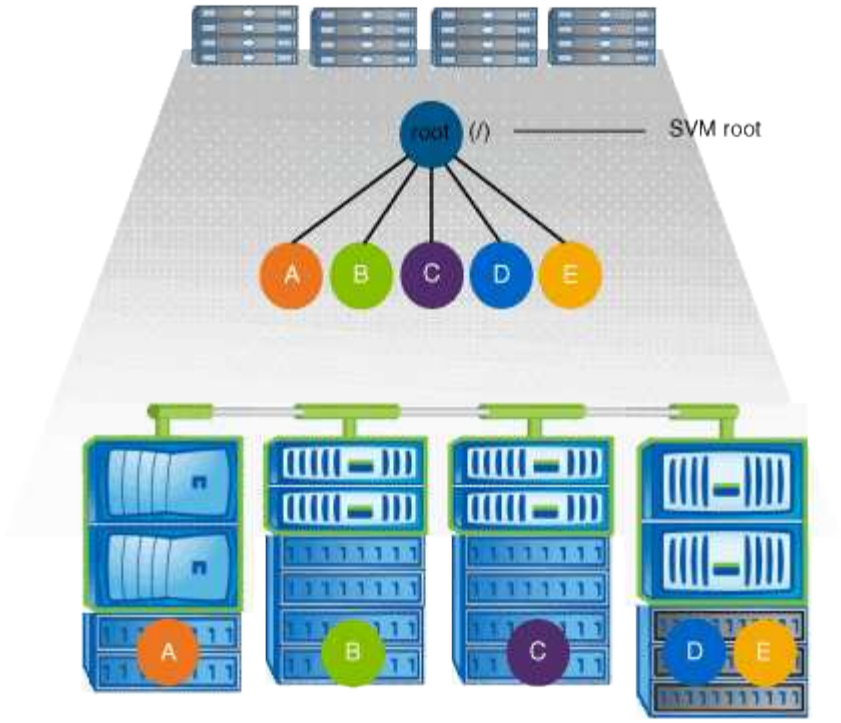


例如，具有上述命名空间架构的典型卷接合配置可能类似于以下配置，其中有三个插入点指向 SVM 的根卷。两个插入点是名为 `data` 和 "`projects` " 的目录。一个插入点是名为 "`audit` " 的接合卷：

```
                      Junction                          Junction
Vserver Volume        Active   Junction Path            Path Source
------- ------------ -------- --------------------     -----------
vs1     audit        true     /audit                   RW_volume
vs1     audit_logs1  true     /audit/logs1             RW_volume
vs1     audit_logs2  true     /audit/logs2             RW_volume
vs1     audit_logs3  true     /audit/logs3             RW_volume
vs1     eng          true     /data/eng                RW_volume
vs1     mktg1        true     /data/mktg1              RW_volume
vs1     mktg2        true     /data/mktg2              RW_volume
vs1     project1     true     /projects/project1       RW_volume
vs1     project2     true     /projects/project2       RW_volume
vs1     vs1_root     -        /                        -
```

包含多个独立卷的命名空间

在具有独立卷的架构中，每个卷都有一个插入点指向 SVM 命名空间的根；但是，卷不会接合到另一个卷下。每个卷都有一个唯一的路径，可以直接在根下接合，也可以在根下的目录下接合。



例如，具有上述命名空间架构的典型卷接合配置可能类似于以下配置，其中有五个插入点指向 SVM 的根卷，每个插入点表示一个卷的路径。

```
                      Junction                          Junction
Vserver Volume        Active   Junction Path            Path Source
------- ------------ -------- --------------------     -----------
vs1     eng           true     /eng                     RW_volume
vs1     mktg          true     /vol/mktg                RW_volume
vs1     project1      true     /project1                RW_volume
vs1     project2      true     /project2                RW_volume
vs1     sales         true     /sales                   RW_volume
vs1     vs1_root      -        /                        -
```

ONTAP 如何控制对文件的访问

ONTAP 如何控制对文件的访问概述

ONTAP 会根据您指定的基于身份验证和基于文件的限制来控制对文件的访问。

当客户端连接到存储系统以访问文件时， ONTAP 必须执行两项任务：

- 身份验证

  ONTAP 必须通过使用可信源验证身份来对客户端进行身份验证。此外，客户端的身份验证类型是一种可用于确定客户端在配置导出策略时是否可以访问数据的方法（对于 CIFS 为可选）。

- Authorization

  ONTAP 必须通过将用户凭据与文件或目录上配置的权限进行比较并确定要提供的访问类型（如果有）来授权用户。

要正确管理文件访问控制， ONTAP 必须与 NIS ， LDAP 和 Active Directory 服务器等外部服务进行通信。要使用 CIFS 或 NFS 配置存储系统以进行文件访问，需要根据您在 ONTAP 中的环境设置相应的服务。

基于身份验证的限制

通过基于身份验证的限制，您可以指定哪些客户端计算机以及哪些用户可以连接到 Storage Virtual Machine （ SVM ）。

ONTAP 支持从 UNIX 和 Windows 服务器进行 Kerberos 身份验证。

基于文件的限制

ONTAP 会评估三个安全级别，以确定实体是否有权对 SVM 上的文件和目录执行请求的操作。在评估三个安全级别后，访问权限由有效权限决定。

任何存储对象最多可包含三种类型的安全层：

- 导出（ NFS ）和共享（ SMB ）安全性

  导出并共享对给定 NFS 导出或 SMB 共享的安全适用场景客户端访问。具有管理权限的用户可以管理 SMB 和 NFS 客户端的导出和共享级别安全性。

- 存储级别访问防护文件和目录安全性

  存储级别访问防护安全性适用场景 SMB 和 NFS 客户端对 SVM 卷的访问。仅支持 NTFS 访问权限。要使 ONTAP 对 UNIX 用户执行安全检查，以访问应用了存储级别访问防护的卷上的数据， UNIX 用户必须映射到拥有该卷的 SVM 上的 Windows 用户。

  > 如果您从 NFS 或 SMB 客户端查看文件或目录的安全设置，则不会看到存储级别访问防护安全性。即使是系统（ Windows 或 UNIX ）管理员也无法从客户端撤消存储级别访问防护安全性。

- NTFS ， UNIX 和 NFSv4 原生文件级安全性

  表示存储对象的文件或目录具有原生文件级安全性。您可以从客户端设置文件级安全性。无论使用 SMB 还是 NFS 访问数据，文件权限都是有效的。

ONTAP如何处理NFS客户端身份验证

ONTAP 如何处理 NFS 客户端身份验证概述

NFS 客户端必须经过适当的身份验证，才能访问 SVM 上的数据。ONTAP 会根据您配置的名称服务检查客户端的 UNIX 凭据，从而对客户端进行身份验证。

当 NFS 客户端连接到 SVM 时， ONTAP 会根据 SVM 的名称服务配置检查不同的名称服务来获取用户的 UNIX 凭据。ONTAP 可以检查本地 UNIX 帐户， NIS 域和 LDAP 域的凭据。必须至少配置其中一个， ONTAP 才能成功对用户进行身份验证。您可以指定多个名称服务以及 ONTAP 搜索这些服务的顺序。

在采用 UNIX 卷安全模式的纯 NFS 环境中，此配置足以对从 NFS 客户端连接的用户进行身份验证并提供正确的文件访问权限。

如果您使用的是混合、NTFS或统一卷安全模式、则ONTAP必须获取UNIX用户的SMB用户名、以便通过Windows域控制器进行身份验证。这可以通过使用本地UNIX帐户或LDAP域映射单个用户来实现、也可以改用默认SMB用户来实现。您可以指定ONTAP搜索哪些名称服务的顺序、也可以指定默认SMB用户。

ONTAP 如何使用名称服务

ONTAP 使用名称服务获取有关用户和客户端的信息。ONTAP 使用此信息对访问存储系统上的数据或管理存储系统的用户进行身份验证，并在混合环境中映射用户凭据。

配置存储系统时，必须指定希望 ONTAP 用于获取用户凭据进行身份验证的名称服务。ONTAP 支持以下名称服务：

- 本地用户（文件）
- 外部 NIS 域（ NIS ）
- 外部 LDAP 域（ LDAP ）

您可以使用 `vserver services name-service ns-switch` 命令系列、用于为SVM配置源以搜索网络信息以及搜索顺序。这些命令提供与等效的功能 `/etc/nsswitch.conf` 文件。

当 NFS 客户端连接到 SVM 时， ONTAP 会检查指定的名称服务以获取用户的 UNIX 凭据。如果名称服务配置正确，并且 ONTAP 可以获取 UNIX 凭据，则 ONTAP 将成功对用户进行身份验证。

在具有混合安全模式的环境中， ONTAP 可能必须映射用户凭据。您必须为您的环境正确配置名称服务，以使 ONTAP 能够正确映射用户凭据。

ONTAP 还使用名称服务对 SVM 管理员帐户进行身份验证。在配置或修改名称服务切换时，必须牢记这一点，以免意外禁用 SVM 管理员帐户的身份验证。有关SVM管理用户的详细信息、请参见 "管理员身份验证和 RBAC"。

ONTAP 如何从 NFS 客户端授予 SMB 文件访问权限

ONTAP 使用 Windows NT 文件系统（ NTFS ）安全语义来确定 NFS 客户端上的 UNIX 用户是否有权访问具有 NTFS 权限的文件。

为此， ONTAP 会将用户的 UNIX 用户 ID （ UID ）转换为 SMB 凭据，然后使用 SMB 凭据验证用户是否有权访问此文件。SMB 凭据由一个主安全标识符（ SID ）（通常是用户的 Windows 用户名）以及一个或多个与用户所属 Windows 组对应的组 SID 组成。

ONTAP 将 UNIX UID 转换为 SMB 凭据所需的时间可能从数十毫秒到数百毫秒不等，因为此过程涉及到与域控制器联系。ONTAP 会将 UID 映射到 SMB 凭据，并在凭据缓存中输入映射，以缩短转换所导致的验证时间。

NFS 凭据缓存的工作原理

当 NFS 用户请求访问存储系统上的 NFS 导出时， ONTAP 必须从外部名称服务器或本地文件检索用户凭据以对用户进行身份验证。然后， ONTAP 会将这些凭据存储在内部凭据缓存中，以供日后参考。了解 NFS 凭据缓存的工作原理有助于您处理潜在的性能和访问问题。

如果没有凭据缓存， ONTAP 将必须在 NFS 用户每次请求访问时查询名称服务。在许多用户访问的繁忙存储系统上，这可能会快速导致严重的性能问题，从而导致不必要的延迟，甚至拒绝 NFS 客户端访问。

通过凭据缓存， ONTAP 会检索用户凭据，然后将其存储一段预定的时间，以便在 NFS 客户端发送另一个请求时快速轻松地进行访问。此方法具有以下优势：

- 它可以减少对外部名称服务器（例如 NIS 或 LDAP ）的请求，从而减轻存储系统的负载。
- 它可以减少向外部名称服务器发送的请求，从而减轻这些服务器的负载。
- 它可以在用户进行身份验证之前，消除从外部源获取凭据的等待时间，从而加快用户访问速度。

ONTAP 会将肯定和否定凭据存储在凭据缓存中。肯定凭据表示用户已通过身份验证并获得访问权限。否定凭据表示用户未通过身份验证，并被拒绝访问。

默认情况下， ONTAP 会将肯定凭据存储 24 小时；也就是说，在对用户进行初始身份验证后， ONTAP 会对该用户 24 小时内的任何访问请求使用缓存的凭据。如果用户在 24 小时后请求访问，则此周期将重新开始： ONTAP 丢弃缓存的凭据，并从相应的名称服务源再次获取凭据。如果名称服务器上的凭据在过去 24 小时内发生更改，则 ONTAP 会缓存更新后的凭据，以供未来 24 小时使用。

默认情况下， ONTAP 会将否定凭据存储两个小时；也就是说，在最初拒绝用户访问后， ONTAP 会继续拒绝该用户的任何访问请求两个小时。如果用户在 2 小时后请求访问，则循环将重新开始： ONTAP 再次从相应的名称服务源获取凭据。如果名称服务器上的凭据在过去两小时内发生更改，则 ONTAP 会缓存更新后的凭据，以供未来两小时使用。