使用选项自定义SMB服务器

ONTAP 9

NetApp
April 24, 2024

目录

使用选项自定义SMB服务器

可用的 SMB 服务器选项

在考虑如何自定义 SMB 服务器时，了解哪些选项可用非常有用。虽然某些选项在 SMB 服务器上通用，但也有一些选项用于启用和配置特定的 SMB 功能。SMB服务器选项可通过控制 `vserver cifs options modify` 选项

以下列表指定了在管理员权限级别可用的 SMB 服务器选项：

- * 配置 SMB 会话超时值 *

  通过配置此选项，您可以指定断开 SMB 会话之前空闲时间的秒数。空闲会话是指用户未在客户端上打开任何文件或目录的会话。默认值为900秒。

- * 配置默认 UNIX 用户 *

  通过配置此选项，您可以指定 SMB 服务器使用的默认 UNIX 用户。ONTAP 会自动创建一个名为 "`pcuser` " 的默认用户 （ UID 为 65534 ），创建一个名为 "`pcuser` " 的组 （ GID 为 65534 ），并将默认用户添加到 "`pcuser` " 组。创建 SMB 服务器时， ONTAP 会自动将 "`pcuser` " 配置为默认 UNIX 用户。

- * 配置子系统 UNIX 用户 *

  通过配置此选项，您可以指定从不可信域登录的用户映射到的 UNIX 用户的名称，从而允许来自不可信域的用户连接到 SMB 服务器。默认情况下，不会配置此选项（没有默认值）；因此，默认情况下不允许来自不可信域的用户连接到 SMB 服务器。

- * 启用或禁用模式位的读取授予执行 *

  通过启用或禁用此选项，您可以指定是否允许 SMB 客户端使用其具有读取访问权限的 UNIX 模式位运行可执行文件，即使未设置 UNIX 可执行位也是如此。默认情况下，此选项处于禁用状态。

- * 启用或禁用从 NFS 客户端删除只读文件的功能 *

  启用或禁用此选项将确定是否允许 NFS 客户端删除设置了只读属性的文件或文件夹。设置只读属性后，NTFS 删除语义不允许删除文件或文件夹。UNIX 删除语义将忽略只读位，而是使用父目录权限来确定是否可以删除文件或文件夹。默认设置为 `disabled`，这会导致NTFS删除义。

- * 配置 Windows Internet 名称服务服务器地址 *

  通过配置此选项，您可以将 Windows Internet 名称服务 （ WINS ）服务器地址列表指定为逗号分隔列表。您必须指定 IPv4 地址。不支持 IPv6 地址。没有默认值。

以下列表指定了在高级权限级别可用的 SMB 服务器选项：

- * 向 CIFS 用户授予 UNIX 组权限 *

  配置此选项可确定是否可以向不是文件所有者的传入 CIFS 用户授予组权限。如果CIFS用户不是UNIX安全模式文件的所有者、并且此参数设置为 `true`，则为该文件授予组权限。如果CIFS用户不是UNIX安全模式文件的所有者、并且此参数设置为 `false``则可以使用常规`UNIX`规则授予文件权限。此参数适用于权限设置为

的UNIX安全模式文件 `mode bits 和不适用于采用NTFS或NFSv4安全模式的文件。默认设置为 false。

- * 启用或禁用 SMB 1.0*

  默认情况下，在 ONTAP 9.3 中为其创建 SMB 服务器的 SVM 上禁用 SMB 1.0 。

  > 从 ONTAP 9.3 开始，默认情况下，对于在 ONTAP 9.3 中创建的新 SMB 服务器， SMB 1.0 处于禁用状态。您应尽快迁移到更高版本的 SMB ，以便为增强安全性和合规性做好准备。有关详细信息，请联系您的 NetApp 代表。

- * 启用或禁用 SMB 2.x *

  SMB 2.0 是支持 LIF 故障转移的最低 SMB 版本。如果禁用 SMB 2.x ，则 ONTAP 还会自动禁用 SMB 3.x

  SMB 2.0 仅在 SVM 上受支持。默认情况下，此选项在 SVM 上处于启用状态

- 启用或禁用**SMB 3.0**

  SMB 3.0 是支持持续可用共享的最低 SMB 版本。Windows Server 2012 和 Windows 8 是支持 SMB 3.0 的最低 Windows 版本。

  SMB 3.0仅在SVM上受支持。默认情况下，此选项在 SVM 上处于启用状态

- 启用或禁用**SMB 3.1**

  Windows 10 是唯一支持 SMB 3.1 的 Windows 版本。

  SMB 3.1仅在SVM上受支持。默认情况下，此选项在 SVM 上处于启用状态

- * 启用或禁用 ODX 副本卸载 *

  ODX 副本卸载由支持它的 Windows 客户端自动使用。默认情况下，此选项处于启用状态。

- * 启用或禁用 ODX 副本卸载的直接复制机制 *

  如果 Windows 客户端尝试以防止在复制过程中更改文件的模式打开副本的源文件，则直接复制机制可以提高副本卸载操作的性能。默认情况下，直接复制机制处于启用状态。

- * 启用或禁用自动节点转介 *

  对于自动节点转介， SMB 服务器会自动将客户端转介到托管通过请求的共享访问的数据的节点的本地数据 LIF 。

- * 启用或禁用 SMB 的导出策略 *

  默认情况下，此选项处于禁用状态。

- * 启用或禁用使用接合点作为重新解析点 *

  如果启用此选项，则 SMB 服务器会将接合点作为重新解析点公开给 SMB 客户端。此选项仅适用于 SMB 2.x 或 SMB 3.0 连接。默认情况下，此选项处于启用状态。

  此选项仅在 SVM 上受支持。默认情况下，此选项在 SVM 上处于启用状态

- * 配置每个 TCP 连接的最大并发操作数 *

  默认值为255。

- * 启用或禁用本地 Windows 用户和组功能 *

  默认情况下，此选项处于启用状态。

- * 启用或禁用本地 Windows 用户身份验证 *

  默认情况下，此选项处于启用状态。

- * 启用或禁用 VSS 卷影复制功能 *

  ONTAP 使用卷影复制功能对使用 Hyper-V over SMB 解决方案存储的数据执行远程备份。

  此选项仅在 SVM 上受支持，并且仅适用于基于 SMB 的 Hyper-V 配置。默认情况下，此选项在 SVM 上处于启用状态

- * 配置卷影复制目录深度 *

  通过配置此选项，您可以定义在使用卷影复制功能时要创建卷影副本的目录的最大深度。

  此选项仅在 SVM 上受支持，并且仅适用于基于 SMB 的 Hyper-V 配置。默认情况下，此选项在 SVM 上处于启用状态

- * 启用或禁用名称映射的多域搜索功能 *

  如果启用了此选项，则在使用 Windows 用户名的域部分（例如， *\joe ）中的通配符（ * ）将 UNIX 用户映射到 Windows 域用户时， ONTAP 将在对主域具有双向信任的所有域中搜索指定用户。主域是包含 SMB 服务器计算机帐户的域。

  除了搜索所有双向受信任域之外，您还可以配置首选受信任域的列表。如果启用了此选项并配置了首选列表，则会使用首选列表执行多域名称映射搜索。

  默认情况下，启用多域名称映射搜索。

- * 配置文件系统扇区大小 *

  通过配置此选项，您可以配置 ONTAP 向 SMB 客户端报告的文件系统扇区大小（以字节为单位）。此选项有两个有效值： `4096` 和 `512`。默认值为 `4096`。您可能需要将此值设置为 `512` 如果Windows应用程序仅支持512字节的扇区大小。

- * 启用或禁用动态访问控制 *

  启用此选项后，您可以使用动态访问控制（ DAC ）来保护 SMB 服务器上的对象，包括使用审核暂存中央访问策略以及使用组策略对象实施中央访问策略。默认情况下，此选项处于禁用状态。

  此选项仅在 SVM 上受支持。

- * 设置非身份验证会话的访问限制（限制匿名） *

  设置此选项可确定非身份验证会话的访问限制。这些限制将应用于匿名用户。默认情况下，匿名用户没有访

问限制。

- * 启用或禁用在具有 UNIX 有效安全性的卷（ UNIX 安全模式卷或具有 UNIX 有效安全性的混合安全模式卷）上呈现 NTFS ACL *

  启用或禁用此选项可确定如何向 SMB 客户端提供具有 UNIX 安全性的文件和文件夹的文件安全性。如果启用，则 ONTAP 会将具有 UNIX 安全性的卷中的文件和文件夹呈现给 SMB 客户端，并将其视为具有 NTFS ACL 的 NTFS 文件安全性。如果禁用，则 ONTAP 会将具有 UNIX 安全性的卷显示为 FAT 卷，而不会提供文件安全性。默认情况下，卷显示为具有 NTFS ACL 的 NTFS 文件安全性。

- * 启用或禁用 SMB 虚假打开功能 *

  启用此功能可优化 ONTAP 在查询文件和目录上的属性信息时发出打开和关闭请求的方式，从而提高 SMB 2.x 和 SMB 3.0 的性能。默认情况下， SMB fake open 功能处于启用状态。此选项仅适用于使用 SMB 2.x 或更高版本建立的连接。

- * 启用或禁用 UNIX 扩展 *

  启用此选项可在 SMB 服务器上启用 UNIX 扩展。UNIX 扩展允许通过 SMB 协议显示 POSIX/UNIX 模式的安全性。默认情况下，此选项处于禁用状态。

  如果您的环境中有基于 UNIX 的 SMB 客户端，例如 Mac OSX 客户端，则应启用 UNIX 扩展。启用 UNIX 扩展后， SMB 服务器可以通过 SMB 将 POSIX/UNIX 安全信息传输到基于 UNIX 的客户端，然后将安全信息转换为 POSIX/UNIX 安全。

- * 启用或禁用对短名称搜索的支持 *

  启用此选项可使 SMB 服务器对短名称执行搜索。启用了此选项的搜索查询会尝试匹配 8.3 文件名和长文件名。此参数的默认值为 `false`。

- * 启用或禁用对自动公布 DFS 功能的支持 *

  启用或禁用此选项可确定 SMB 服务器是否自动向连接到共享的 SMB 2.x 和 SMB 3.0 客户端公布 DFS 功能。ONTAP 在实施用于 SMB 访问的符号链接时使用 DFS 转介。如果启用，则无论是否启用符号链接访问， SMB 服务器都会始终公布 DFS 功能。如果禁用，则只有当客户端连接到启用了符号链接访问的共享时，SMB 服务器才会公布 DFS 功能。

- * 配置最大 SMB 信用数 *

  从ONTAP 9.4开始、配置 `-max-credits` 选项允许您限制在客户端和服务器运行SMB版本2或更高版本时在SMB连接上授予的信用值数量。默认值为128。

- * 启用或禁用对 SMB 多通道的支持 *

  启用 `-is-multichannel-enabled` 如果在集群及其客户端上部署了适当的NIC、则ONTAP 9.4及更高版本中的选项允许SMB服务器为单个SMB会话建立多个连接。这样可以提高吞吐量和容错能力。此参数的默认值为 `false`。

  启用 SMB 多通道后，您还可以指定以下参数：

  - 每个多通道会话允许的最大连接数。此参数的默认值为 32 。
  - 每个多通道会话公布的最大网络接口数。此参数的默认值为256。

配置SMB服务器选项

在Storage Virtual Machine (SVM)上创建SMB服务器后、您可以随时配置SMB服务器选项。

步骤

1. 执行所需的操作：

要配置SMB服务器选项的项	输入命令 ...
处于管理权限级别	`vserver cifs options modify -vserver` *`vserver_name options`*
在高级权限级别	a. `set -privilege advanced` b. `vserver cifs options modify -vserver` *`vserver_name options`* c. `set -privilege admin`

有关配置SMB服务器选项的详细信息、请参见的手册页 `vserver cifs options modify` 命令：

配置向SMB用户授予UNIX组权限

您可以将此选项配置为授予组访问文件或目录的权限、即使传入的SMB用户不是文件的所有者也是如此。

步骤

1. 将权限级别设置为高级： `set -privilege advanced`
2. 根据需要配置授予 UNIX 组权限：

如果您要 ...	输入命令 ...
启用对文件或目录的访问以获取组权限，即使用户不是文件的所有者也是如此	`vserver cifs options modify –grant-unix-group-perms-to-others true`
禁用对文件或目录的访问以获取组权限，即使用户不是文件的所有者也是如此	`vserver cifs options modify –grant-unix-group-perms-to-others false`

3. 验证此选项是否设置为所需值： `vserver cifs options show –fields grant-unix-group-perms-to-others`
4. 返回到管理权限级别： `set -privilege admin`

配置匿名用户的访问限制

默认情况下，未经身份验证的匿名用户（也称为 *null user*）可以访问网络上的某些信息。您可以使用SMB服务器选项为匿名用户配置访问限制。

关于此任务

。 `-restrict-anonymous` SMB服务器选项对应于 `RestrictAnonymous` Windows中的注册表项。

匿名用户可以列出或枚举网络上 Windows 主机中的某些类型的系统信息，包括用户名和详细信息，帐户策略和共享名称。您可以通过指定以下三种访问限制设置之一来控制匿名用户的访问：

价值	**Description**
`no-restriction` (默认)	不指定匿名用户的访问限制。
`no-enumeration`	指定仅限制匿名用户的枚举。
`no-access`	指定对匿名用户的访问进行限制。

步骤

1. 将权限级别设置为高级： `set -privilege advanced`
2. 配置限制匿名设置： `vserver cifs options modify -vserver` *`vserver_name`* `-restrict -anonymous {no-restriction|no-enumeration|no-access}`
3. 验证此选项是否设置为所需值： `vserver cifs options show -vserver` *`vserver_name`*
4. 返回到管理权限级别： `set -privilege admin`

相关信息

可用的 SMB 服务器选项

管理如何为 **UNIX** 安全模式数据的 **SMB** 客户端提供文件安全性

管理如何向 **SMB** 客户端提供文件安全性以了解 **UNIX** 安全模式数据概述

您可以通过启用或禁用向 SMB 客户端提供 NTFS ACL 来选择如何为 UNIX 安全模式数据的 SMB 客户端提供文件安全性。每个设置都有一些优势，您应了解这些优势，才能选择最适合您业务需求的设置。

默认情况下， ONTAP 会将 UNIX 安全模式卷上的 UNIX 权限作为 NTFS ACL 提供给 SMB 客户端。在某些情况下，这种做法是可取的，其中包括以下情形：

- 要查看和编辑 UNIX 权限，请使用 Windows 属性框中的 * 安全性 * 选项卡。

  如果 UNIX 系统不允许修改 Windows 客户端的权限，则不能修改此操作。例如，您不能更改不拥有的文件的所有权，因为 UNIX 系统不允许执行此操作。此限制可防止 SMB 客户端绕过对文件和文件夹设置的 UNIX 权限。

- 用户正在使用某些 Windows 应用程序编辑和保存 UNIX 安全模式卷上的文件，例如 Microsoft Office ，在这些应用程序中， ONTAP 必须在保存操作期间保留 UNIX 权限。
- 您的环境中有一些 Windows 应用程序希望对其使用的文件读取 NTFS ACL 。

在某些情况下，您可能需要禁用将 UNIX 权限作为 NTFS ACL 呈现。如果禁用此功能，则 ONTAP 会将 UNIX 安全模式卷作为 FAT 卷提供给 SMB 客户端。您可能希望将 UNIX 安全模式卷作为 FAT 卷提供给 SMB 客户端的具体原因如下：

- 您只能通过在 UNIX 客户端上使用挂载来更改 UNIX 权限。

  在 SMB 客户端上映射 UNIX 安全模式卷时， " 安全 " 选项卡不可用。映射的驱动器似乎已使用 FAT 文件系统进行格式化，该文件系统没有文件权限。

- 您正在通过 SMB 使用应用程序，这些应用程序会对访问的文件和文件夹设置 NTFS ACL ，如果数据驻留在 UNIX 安全模式卷上，则这些应用程序可能会失败。

  如果 ONTAP 将卷报告为 FAT ，则应用程序不会尝试更改 ACL 。

相关信息

在 FlexVol 卷上配置安全模式

在 qtree 上配置安全模式

启用或禁用为 **UNIX** 安全模式数据提供 **NTFS ACL**

您可以为 UNIX 安全模式数据（ UNIX 安全模式卷和具有 UNIX 有效安全性的混合安全模式卷）启用或禁用向 SMB 客户端提供 NTFS ACL 。

关于此任务

如果启用此选项，则 ONTAP 会将具有有效 UNIX 安全模式的卷上的文件和文件夹作为具有 NTFS ACL 提供给 SMB 客户端。如果禁用此选项，这些卷将作为 FAT 卷呈现给 SMB 客户端。默认情况下，将 NTFS ACL 提供给 SMB 客户端。

步骤

1. 将权限级别设置为高级： `set -privilege advanced`
2. 配置UNIX NTFS ACL选项设置： `vserver cifs options modify -vserver` *`vserver_name`* `-is-unix-nt-acl-enabled {true|false}`
3. 验证此选项是否设置为所需值： `vserver cifs options show -vserver` *`vserver_name`*
4. 返回到管理权限级别： `set -privilege admin`

ONTAP 如何保留 **UNIX** 权限

当 Windows 应用程序编辑和保存 FlexVol 卷中当前具有 UNIX 权限的文件时， ONTAP 可以保留 UNIX 权限。

当 Windows 客户端上的应用程序编辑和保存文件时，它们会读取文件的安全属性，创建新的临时文件，将这些属性应用于临时文件，然后为临时文件提供原始文件名。

当 Windows 客户端对安全属性执行查询时，它们会收到一个构建的 ACL ，该 ACL 准确表示 UNIX 权限。此构建 ACL 的唯一目的是，在 Windows 应用程序更新文件时保留文件的 UNIX 权限，以确保生成的文件具有相同的 UNIX 权限。ONTAP 不会使用构建的 ACL 设置任何 NTFS ACL 。

使用 **Windows** 安全性选项卡管理 **UNIX** 权限

如果要在 SVM 上操作混合安全模式卷或 qtree 中的文件或文件夹的 UNIX 权限，可以使用 Windows 客户端上的安全性选项卡。或者，您也可以使用可以查询和设置 Windows ACL 的应用程序。

- 修改 UNIX 权限

  您可以使用 Windows 安全性选项卡查看和更改混合安全模式卷或 qtree 的 UNIX 权限。如果您使用 Windows 安全性主选项卡更改 UNIX 权限，则必须先删除要编辑的现有 ACE （此操作会将模式位设置为 0 ），然后再进行更改。或者，您也可以使用高级编辑器更改权限。

  如果使用模式权限，则可以直接更改列出的 UID ， GID 和其他（在计算机上具有帐户的其他所有人）的模式权限。例如，如果显示的 UID 具有 r-x 权限，则可以将 UID 权限更改为 rwx 。

- 将 UNIX 权限更改为 NTFS 权限

  您可以使用 Windows 安全性选项卡将 UNIX 安全对象替换为混合安全模式卷或 qtree 上的 Windows 安全对象，其中文件和文件夹采用 UNIX 有效安全模式。

  您必须先删除列出的所有 UNIX 权限条目，然后才能将其替换为所需的 Windows 用户和组对象。然后，您可以在 Windows 用户和组对象上配置基于 NTFS 的 ACL 。通过删除所有 UNIX 安全对象并仅将 Windows 用户和组添加到混合安全模式卷或 qtree 中的文件或文件夹，可以将文件或文件夹上的有效安全模式从 UNIX 更改为 NTFS 。

  更改文件夹的权限时，默认的 Windows 行为是将这些更改传播到所有子文件夹和文件。因此，如果您不想将安全模式的更改传播到所有子文件夹，子文件夹和文件，则必须将传播选项更改为所需设置。