管理 Web 服务

ONTAP 9

NetApp
April 24, 2024

目录

管理 Web 服务

管理 Web 服务概述

您可以为集群或 Storage Virtual Machine （ SVM ）启用或禁用 Web 服务，显示 Web 服务的设置以及控制某个角色的用户是否可以访问 Web 服务。

您可以通过以下方式管理集群或 SVM 的 Web 服务：

- 启用或禁用特定 Web 服务
- 指定对 Web 服务的访问是否仅限于加密 HTTP （ SSL ）
- 显示 Web 服务的可用性
- 允许或禁止某个角色的用户访问 Web 服务
- 显示允许访问 Web 服务的角色

要使用户能够访问 Web 服务，必须满足以下所有条件：

- 用户必须经过身份验证。

  例如， Web 服务可能会提示输入用户名和密码。用户的响应必须与有效帐户匹配。

- 必须为用户设置正确的访问方法。

  只有对给定 Web 服务使用正确访问方法的用户，身份验证才会成功。ONTAP API Web服务 `ontapi`)、则用户必须具有 `ontapi` 访问方法。对于所有其他Web服务、用户必须具有 `http` 访问方法。

  > 您可以使用 `security login` 用于管理用户访问方法和身份验证方法的命令。

- 必须将 Web 服务配置为允许用户的访问控制角色。

  > 您可以使用 `vserver services web access` 用于控制角色对Web服务的访问的命令。

如果启用了防火墙，则必须将用于 Web 服务的 LIF 的防火墙策略设置为允许 HTTP 或 HTTPS 。

如果使用 HTTPS 访问 Web 服务，则还必须为提供 Web 服务的集群或 SVM 启用 SSL ，并且必须为集群或 SVM 提供数字证书。

管理对 Web 服务的访问

Web 服务是用户可以使用 HTTP 或 HTTPS 访问的应用程序。集群管理员可以设置 Web 协议引擎，配置 SSL ，启用 Web 服务以及使某个角色的用户能够访问 Web 服务。

从 ONTAP 9.6 开始，支持以下 Web 服务：

- 服务处理器基础架构 (`spi`)

此服务使节点的日志，核心转储和 MIB 文件可通过集群管理 LIF 或节点管理 LIF 进行 HTTP 或 HTTPS 访问。默认设置为 `enabled`。

在请求访问节点的日志文件或核心转储文件时、 `spi` Web服务会自动创建从一个节点到文件所在的另一节点根卷的挂载点。您无需手动创建挂载点。`。

- ONTAP API (`ontapi`)

  通过此服务，您可以运行 ONTAP API ，以便使用远程程序执行管理功能。默认设置为 `enabled`。

  某些外部管理工具可能需要此服务。例如，如果您使用 System Manager ，则应保持此服务处于启用状态。

- Data ONTAP发现 (`disco`)

  通过此服务，机下管理应用程序可以发现网络中的集群。默认设置为 `enabled`。

- 支持诊断 (`supdiag`)

  此服务可控制对系统上特权环境的访问，以协助分析和解决问题。默认设置为 `disabled`。只有在技术支持的指导下，才应启用此服务。

- System Manager (`sysmgr`)

  此服务用于控制 ONTAP 附带的 System Manager 的可用性。默认设置为 `enabled`。此服务仅在集群上受支持。

- 固件基板管理控制器(BMC)更新 (`FW_BMC`)

  通过此服务，您可以下载 BMC 固件文件。默认设置为 `enabled`。

- ONTAP 文档 (`docs`)

  通过此服务可以访问 ONTAP 文档。默认设置为 `enabled`。

- ONTAP REST API (`docs_api`)

  通过此服务，您可以访问 ONTAP RESTful API 文档。默认设置为 `enabled`。

- 文件上传和下载 (`fud`)

  此服务提供文件上传和下载。默认设置为 `enabled`。

- ONTAP消息传送 (`ontapmsg`)

  此服务支持发布和订阅界面，允许您订阅事件。默认设置为 `enabled`。

- ONTAP门户 (`portal`)

  此服务将网关实施到虚拟服务器中。默认设置为 `enabled`。

- ONTAP restful界面 (`rest`)

此服务支持 RESTful 接口，用于远程管理集群基础架构的所有要素。默认设置为 `enabled`。

- 安全断言标记语言(SAML)服务提供程序支持 (`saml`)

  此服务可提供支持 SAML 服务提供程序的资源。默认设置为 `enabled`。

- SAML服务提供程序 (`saml-sp`)

  此服务可为服务提供商提供 SP 元数据和断言使用者服务等服务。默认设置为 `enabled`。

从 ONTAP 9.7 开始，支持以下附加服务：

- 配置备份文件 (`backups`)

  使用此服务可以下载配置备份文件。默认设置为 `enabled`。

- ONTAP安全性 (`security`)

  此服务支持 CSRF 令牌管理以增强身份验证。默认设置为 `enabled`。

管理 Web 协议引擎

您可以在集群上配置 Web 协议引擎，以控制是否允许 Web 访问以及可以使用哪些 SSL 版本。您还可以显示 Web 协议引擎的配置设置。

您可以通过以下方式在集群级别管理 Web 协议引擎：

- 您可以使用指定远程客户端是否可以使用HTTP或HTTPS访问Web服务内容 `system services web modify` 命令 `-external` 参数。
- 您可以使用指定是否应使用SSLv3进行安全Web访问 `security config modify` 命令 `-supported -protocol` 参数。
  默认情况下， SSLv3 处于禁用状态。传输层安全 1.0 （ TLSv1.0 ）已启用，可以根据需要将其禁用。
- 您可以为集群范围控制平面 Web 服务接口启用联邦信息处理标准（ Federal Information Processing Standard ， FIPS ） 140-2 合规模式。

  > 默认情况下， FIPS 140-2 合规模式处于禁用状态。

  - * 禁用 FIPS 140-2 合规模式 *
    您可以通过设置来启用FIPS 140-2合规模式 `is-fips-enabled` 参数设置为 `true` 。 `security config modify` 命令、然后使用 `security config show` 命令以确认联机状态。
  - * 启用 FIPS 140-2 合规模式 *
    - 从ONTAP 9.11.1开始、TLSv1、TLSv1.1和SSLv3将被禁用、只有TSLv1.2和TSLv1.3保持启用状态。它会影响ONTAP 9内部和外部的其他系统和通信。如果启用FIPS 140-2合规模式、然后再禁用、TLSv1、TLSv1.1和SSLv3将保持禁用状态。TLSv.1或TLSv1.3将保持启用状态、具体取决于先前的配置。
    - 对于9.11.1之前的ONTAP 版本、TLSv1和SSLv3均已禁用、只有TLSv1.1和TLSv1.2保持启用状态。启用 FIPS 140-2 合规模式后， ONTAP 会阻止您同时启用 TLSv1 和 SSLv3 。如果启用 FIPS 140-2

合规模式，然后将其禁用， TLSv1 和 SSLv3 将保持禁用状态，但 TLSv1.2 或 TLSv1.1 和 TLSv1.2 均已启用，具体取决于先前的配置。

- 您可以使用显示集群范围安全性的配置 `system security config show` 命令：

如果启用了防火墙，则必须将用于 Web 服务的逻辑接口（ LIF ）的防火墙策略设置为允许 HTTP 或 HTTPS 访问。

如果使用 HTTPS 访问 Web 服务，则还必须为提供 Web 服务的集群或 Storage Virtual Machine （ SVM ）启用 SSL ，并且必须为集群或 SVM 提供数字证书。

在 MetroCluster 配置中，您对集群上的 Web 协议引擎所做的设置更改不会复制到配对集群上。

用于管理 Web 协议引擎的命令

您可以使用 `system services web` 用于管理Web协议引擎的命令。您可以使用 `system services firewall policy create` 和 `network interface modify` 允许Web访问请求通过防火墙的命令。

如果您要 ...	使用此命令 ...
在集群级别配置 Web 协议引擎： • 为集群启用或禁用 Web 协议引擎 • 为集群启用或禁用 SSLv3 • 为安全 Web 服务（ HTTPS ）启用或禁用 FIPS 140-2 合规性	`system services web modify`
显示集群级别的 Web 协议引擎配置，确定 Web 协议是否在整个集群中正常运行，并显示 FIPS 140-2 合规性是否已启用并联机	`system services web show`
显示节点级别的 Web 协议引擎配置以及集群中节点的 Web 服务处理活动	`system services web node show`
创建防火墙策略或将 HTTP 或 HTTPS 协议服务添加到现有防火墙策略中，以允许 Web 访问请求通过防火墙	`system services firewall policy create` 设置 `-service` 参数设置为 `http` 或 `https` 允许Web访问请求通过防火墙。
将防火墙策略与 LIF 关联	`network interface modify` 您可以使用 `-firewall-policy` 用于修改LIF的防火墙策略的参数。

配置对 Web 服务的访问

通过配置对 Web 服务的访问，授权用户可以使用 HTTP 或 HTTPS 访问集群或 Storage Virtual Machine （ SVM ） 上的服务内容。

步骤

1. 如果启用了防火墙，请确保已在防火墙策略中为用于 Web 服务的 LIF 设置 HTTP 或 HTTPS 访问：

   > 您可以使用检查是否已启用防火墙 `system services firewall show` 命令：

   a. 要验证是否已在防火墙策略中设置HTTP或HTTPS、请使用 `system services firewall policy show` 命令：

      您可以设置 `-service` 的参数 `system services firewall policy create` 命令 `http` 或 `https` 以启用支持Web访问的策略。

   b. 要验证支持HTTP或HTTPS的防火墙策略是否与提供Web服务的LIF关联、请使用 `network interface show` 命令 `-firewall-policy` 参数。

      您可以使用 `network interface modify` 命令 `-firewall-policy` 用于使LIF的防火墙策略生效的参数。

2. 要配置集群级别的Web协议引擎并使Web服务内容可访问、请使用 `system services web modify` 命令：
3. 如果您计划使用安全Web服务(HTTPS)、请使用为集群或SVM启用SSL并提供数字证书信息 `security ssl modify` 命令：
4. 要为集群或SVM启用Web服务、请使用 `vserver services web modify` 命令：

   必须对要为集群或 SVM 启用的每个服务重复此步骤。

5. 要授权某个角色访问集群或SVM上的Web服务、请使用 `vserver services web access create` 命令：

   您授予访问权限的角色必须已存在。您可以使用显示现有角色 `security login role show` 命令或使用创建新角色 `security login role create` 命令：

6. 对于已授权访问Web服务的角色、请检查的输出、确保为其用户配置了正确的访问方法 `security login show` 命令：

   以访问ONTAP API Web服务 `ontapi`)、则必须为用户配置 `ontapi` 访问方法。要访问所有其他Web服务、必须为用户配置 `http` 访问方法。

   > 您可以使用 `security login create` 用于为用户添加访问方法的命令。

用于管理 Web 服务的命令

您可以使用 `vserver services web` 用于管理集群或Storage Virtual Machine (SVM)

的Web服务可用性的命令。您可以使用 `vserver services web access` 用于控制角色对Web服务的访问的命令。

如果您要 ...	使用此命令 ...
为集群或 SVM 配置 Web 服务： • 启用或禁用 Web 服务 • 指定是否只能使用 HTTPS 访问 Web 服务	`vserver services web modify`
显示集群或 SVM 的 Web 服务的配置和可用性	`vserver services web show`
授权角色访问集群或 SVM 上的 Web 服务	`vserver services web access create`
显示有权访问集群或 SVM 上的 Web 服务的角色	`vserver services web access show`
阻止角色访问集群或 SVM 上的 Web 服务	`vserver services web access delete`

相关信息

"ONTAP 9命令"

用于管理节点上挂载点的命令

。 `spi` 在请求访问节点的日志文件或核心文件时、Web服务会自动创建从一个节点到另一节点根卷的挂载点。尽管您不需要手动管理挂载点、但也可以使用进行管理 `system node root-mount` 命令

如果您要 ...	使用此命令 ...
手动创建从一个节点到另一节点根卷的挂载点	`system node root-mount create` 从一个节点到另一个节点只能存在一个挂载点。
显示集群中节点上的现有挂载点，包括创建挂载点的时间及其当前状态	`system node root-mount show`
删除从一个节点到另一节点根卷的挂载点，并强制关闭与挂载点的连接	`system node root-mount delete`

相关信息

"ONTAP 9命令"

管理SSL

SSL 协议可通过使用数字证书在 Web 服务器和浏览器之间建立加密连接来提高 Web 访问

的安全性。

您可以通过以下方式管理集群或 Storage Virtual Machine （ SVM ）的 SSL：

- 启用 SSL
- 生成并安装数字证书并将其与集群或 SVM 关联
- 显示 SSL 配置以查看是否已启用 SSL ，以及 SSL 证书名称（如果可用）
- 为集群或 SVM 设置防火墙策略，以便可以处理 Web 访问请求
- 定义可使用的 SSL 版本
- 限制对 Web 服务的 HTTPS 请求的访问

用于管理SSL的命令

您可以使用 `security ssl` 用于管理集群或Storage Virtual Machine (SVM)的SSL协议的命令。

如果您要 ...	使用此命令 ...
为集群或 SVM 启用 SSL ，并将数字证书与其关联	`security ssl modify`
显示集群或 SVM 的 SSL 配置和证书名称	`security ssl show`

对 Web 服务访问问题进行故障排除

配置错误发生发生原因 Web 服务访问问题。您可以通过确保 LIF ，防火墙策略， Web 协议引擎， Web 服务，数字证书， 和用户访问授权均已正确配置。

下表可帮助您确定并解决 Web 服务配置错误：

此访问问题 ...	由于此配置错误而发生 ...	要解决此错误 ...
您的Web浏览器将返回 `unable to connect` 或 `failure to establish a connection` 尝试访问Web服务时出错。	您的 LIF 可能配置不正确。	确保您可以对提供 Web 服务的 LIF 执行 ping 操作。 您可以使用 `network ping` 命令对LIF执行ping操作。有关网络配置的信息，请参见 *Network Management Guide* 。

此访问问题 ...	由于此配置错误而发生 ...	要解决此错误 ...
防火墙配置可能不正确。	确保防火墙策略已设置为支持 HTTP 或 HTTPS ，并且已将此策略分配给提供 Web 服务的 LIF 。 您可以使用 `system services firewall policy` 用于管理防火墙策略的命令。您可以使用 `network interface modify` 命令 `-firewall -policy` 用于将策略与LIF关联的参数。	您的 Web 协议引擎可能已禁用。
确保已启用 Web 协议引擎，以便可以访问 Web 服务。 您可以使用 `system services web` 用于管理集群的Web协议引擎的命令。	您的Web浏览器将返回 `not found` 尝试访问Web服务时出错。	此 Web 服务可能已禁用。
确保已分别启用要允许访问的每个 Web 服务。 您可以使用 `vserver services web modify` 命令以启用Web服务以进行访问。	Web 浏览器无法使用用户的帐户名称和密码登录到 Web 服务。	无法对用户进行身份验证，访问方法不正确或用户无权访问 Web 服务。

此访问问题 ...	由于此配置错误而发生 ...	要解决此错误 ...
确保用户帐户存在，并使用正确的访问方法和身份验证方法进行配置。此外，确保用户的角色已获得访问 Web 服务的授权。 您可以使用 `security login` 用于管理用户帐户及其访问方法和身份验证方法的命令。访问ONTAP API Web服务需要 `ontapi` 访问方法。访问所有其他Web服务需要 `http` 访问方法。您可以使用 `vserver services web access` 用于管理角色对Web服务的访问权限的命令。	您使用 HTTPS 连接到 Web 服务，而 Web 浏览器指示您的连接已中断。	您可能未在提供 Web 服务的集群或 Storage Virtual Machine （ SVM ）上启用 SSL 。
确保集群或 SVM 已启用 SSL ，并且数字证书有效。 您可以使用 `security ssl` 用于管理HTTP服务器和的SSL配置的命令 `security certificate show` 用于显示数字证书信息的命令。	您使用 HTTPS 连接到 Web 服务，并且 Web 浏览器指示此连接不可信。	您可能正在使用自签名数字证书。