CDO 中的VPN 监控和故障排除

监控远程访问 VPN 会话

CDO 远程访问监控控制面板可用于查看有关 RA VPN 用户的整合信息，包括用户当前状态、设备类型、客户端应用、用户地理位置信息和连接持续时间。您还可以根据需要断开 RA VPN 会话。

执行以下操作以查看 VPN 会话：

1. 在云交付的防火墙管理中心页面中，点击**返回主页 (Return Home)**。
2. 在 CDO 导航窗格中，点击 **VPN** > **远程访问 VPN 监控 (Remote Access VPN Monitoring)**。

有关详细信息，请参阅监控远程访问虚拟专用网络会话。

系统消息

邮件中心是开始进行故障排除的地方。通过此功能，可以查看持续生成的有关系统活动和状态的消息。要打开消息中心，请点击位于主菜单中**部署 (Deploy)** 按钮正右侧的**系统状态 (System Status)**。

VPN 系统日志

您可以为 威胁防御设备启用系统日志记录（系统日志）。日志记录信息可以帮助您发现并隔离网络或设备配置问题。启用 VPN 日志记录时，这些系统日志将从威胁防御设备发送到Cisco Secure Firewall Management Center进行分析和存档。

所有出现的 VPN 系统日志都具有默认严重性级别“错误”(ERROR) 或更高（除非已更改）。您可以通过威胁防御平台设置来管理VPN日志记录。您可以通过编辑目标设备的威胁防御平台设置策略

中的 **VPN 日志记录设置 (VPN Logging Settings)** 来调整消息严重性级别（**平台设置 (Platform Settings)** > **系统日志 (Syslog)** > **日志记录设置 (Logging Setup)**）。有关启用 VPN 日志记录、配置系统日志服务器以及查看系统日志的详细信息，请参阅配置系统日志。

注释 只要您配置了具有站点间或远程访问 VPN 的设备，它就会默认自动启用将 VPN 系统日志发送至 管理中心。

查看 VPN 系统日志

系统捕获事件信息，以帮助您收集有关 VPN 问题源的其他信息。显示的任何 VPN 系统日志都具有默认严重性级别“ERROR”或更高（除非已更改）。默认情况下，行按**时间**列排序。

您必须是枝叶域中的管理员用户才能执行此任务。

开始之前

通过选中 威胁防御平台设备中的**使记录至 FMC** 复选框，启用 VPN 日志记录（**设备** > **平台设置** > **系统日志** > **日志记录设置**）。有关启用 VPN 日志记录、配置系统日志服务器以及查看系统性记录的详细信息，请参阅配置系统日志。

过程

步骤 1 选择**设备** > **VPN** > **故障排除**。

步骤 2 您有以下选择：

- 搜索 - 要过滤当前消息信息，请点击**编辑搜索 (Edit Search)**。
- 查看 - 要查看与视图中所选消息关联的 VPN 详细信息，请点击**查看 (View)**。
- 查看全部 - 要查看视图中所有消息的事件详细信息，请点击**查看全部 (View All)**。
- 删除 - 要从数据库中删除选定的消息，请点击**删除 (Delete)** 或点击**全部删除 (Delete All)** 以删除所有消息。

调试命令

本节介绍如何使用调试命令来帮助您诊断和解决与 VPN 相关的问题。此处介绍的命令并非详尽无遗，本节将根据命令的作用来帮助您诊断 VPN 相关问题。

使用指南

由于调试输出在CPU进程中享有高优先级，因此可导致系统不可用。为此，应仅在对特定问题进行故障排除或与思科 Technical Assistance Center (TAC) 进行故障排除会话时使用 **debug** 命令。此外，最好在网络流量较低和用户较少时使用 **debug** 命令。在这些时段进行调试会减少因 **debug** 命令处理开销增加而影响系统使用的可能性。

您只能在 CLI 会话中查看调试输出。在连接到控制台端口的情况下，或者在诊断 CLI 中，您可以直接查看输出结果（输入 **system support diagnostic-cli**）。此外，您也可以在常规 Firepower Threat Defense CLI 中使用 **show console-output** 命令查看输出结果。

要显示给定功能的调试消息，请使用 **debug** 命令。要禁用调试消息的显示，请使用此命令的 **no** 形式。使用 **no debug all** 关闭所有调试命令。

debug *feature* [*subfeature*] [*level*]
no debug *feature* [*subfeature*]

Syntax Description

feature	指定要为其启用调试的功能。若要查看可用功能，请使用 **debug ?** 命令获取 CLI 帮助。
subfeature	（可选）根据功能，您可以为一项或多项子功能启用调试消息。使用 ? 查看可用的子功能。
级别	（可选）指定调试级别。使用 ? 可查看可用的级别。

Command Default

默认调试级别为 1。

示例

在远程接入 VPN 上运行多个会话时，由于日志的大小，可能会很难进行故障排除。可以使用 **debug webvpn condition** 命令设置过滤器，以便更精确地定位调试进程。

debug webvpn condition { **group** *name* | **p-ipaddress** *ip_address* [{ **subnet** *subnet_mask* | **prefix** *length*}] | **reset** | **user** *name*}

其中：

- **group** *name* 对组策略进行过滤，而不是隧道组或连接配置文件。
- **p-ipaddress** *ip_address* [{**subnet** *subnet_mask* | **prefix** *length*}] 对客户端的公共 IP 地址进行过滤。子网掩码（用于 IPv4）或前缀（用于 IPv6）是可选的。
- **reset** 重置所有过滤器。可以使用 **no debug webvpn condition** 命令关闭特定的过滤器。
- **user** *Name* 按用户名过滤。

如果配置多个条件，则条件是合并的 (AND)，因此只有满足所有条件时才显示调试。

设置条件过滤器后，使用基本 **debug webvpn** 命令打开调试。只设置条件不会启用调试。使用 **show debug** 和 **show webvpn debug-condition** 命令查看调试的当前状态。

下文是在用户 jdoe 上启用条件调试的示例。

```
firepower# debug webvpn condition user jdoe

firepower# show webvpn debug-condition
INFO: Webvpn conditional debug is turned ON
INFO: User name filters:
INFO: jdoe
```

```
firepower# debug webvpn
INFO: debug webvpn  enabled at level 1.

firepower# show debug
debug webvpn  enabled at level 1
INFO: Webvpn conditional debug is turned ON
INFO: User name filters:
INFO: jdoe
```

Related Commands

命令	说明
show debug	显示当前活动的调试设置。
undebug	禁用功能调试。此命令与 **no debug** 的效果相同。

调试 aaa

请参阅以下命令以调试配置或身份验证、授权和记帐 (AAA) 设置。

debug *aaa* [*accounting* | *authentication* | *authorization* | *common* | *internal* | *shim* | *url-redirect*]

Syntax Description

aaa	启用对 AAA 的调试。使用 ? 查看可用的子功能。
accounting	（可选）启用 AAA 记帐调试。
authentication	（可选）启用 AAA 身份验证调试。
authorization	（可选）启用 AAA 授权调试。
common	（可选）指定 AAA 通用调试级别。使用 ? 查看可用的级别。
internal	（可选）启用 AAA 内部调试。
shim	（可选）指定 AAA shim 调试级别。使用 ? 查看可用的级别。
url-redirect	（可选）启用 AAA url-redirect 调试。

Command Default

默认调试级别为 1。

Related Commands

命令	说明
show debug aaa	显示 AAA 当前的活动调试设置。
undebug aaa	禁用 AAA 的调试。此命令与 **no debug aaa** 的效果相同。

debug crypto

请参阅以下用于调试与 crypto 相关联的配置或设置的命令。

debug *crypto* [*ca* | *condition* | *engine* | *ike-common* | *ikev1* | *ikev2* | *ipsec* | *ss-apic*]

Syntax Description

crypto	启用对 *crypto* 的调试。使用 ? 查看可用的子功能。
ca	（可选）指定 PKI 调试级别。可以使用 ? 查看可用子功能。
condition	（可选）指定 IPsec/ISAKMP 调试过滤器。可以使用 ? 查看可用过滤器。
engine	（可选）指定 crypto 引擎调试级别。可以使用 ? 查看可用级别。
ike-common	（可选）指定 IKE 常用调试级别。可以使用 ? 查看可用级别。
ikev1	（可选）指定 IKE 版本 1 调试级别。可以使用 ? 查看可用级别。
ikev2	（可选）指定 IKE 版本 2 调试级别。可以使用 ? 查看可用级别。
ipsec	（可选）指定 IPsec 调试级别。使用 ? 可查看可用的级别。
condition	（可选）指定 Crypto 安全套接字 API 调试级别。可以使用 ? 查看可用级别。
vpnclient	（可选）指定 EasyVPN 客户端调试级别。使用 ? 可查看可用的级别。

Command Default

默认调试级别为 1。

Related Commands

命令	说明
show debug crypto	显示当前处于活动状态的适用于 crypto 的调试设置。
undebug crypto	禁用对 crypto 的调试。此命令与 **no debug crypto** 的效果相同。

debug crypto ca

请参阅以下用于调试与 crypto ca 相关联的配置或设置的命令。

debug *crypto ca* [*cluster* | *messages* | *periodic-authentication* | *scep-proxy* | *transactions* | *trustpool*] [*1-255*]

Syntax Description

crypto ca	启用对 *crypto ca* 的调试。使用 ? 查看可用的子功能。
cluster	（可选）指定 PKI 集群调试级别。可以使用 ? 查看可用级别。
cmp	（可选）指定 CMP 交易调试级别。可以使用 ? 查看可用级别。
messages	（可选）指定 PKI 输入/输出消息调试级别。可以使用 ? 查看可用级别。

periodic-authentication	（可选）指定 PKI 周期性身份验证调试级别。可以使用 ? 查看可用级别。
scep-proxy	（可选）指定 SCEP 代理调试级别。可以使用 ? 查看可用级别。
server	（可选）指定本地 CA 服务器调试级别。可以使用 ? 查看可用级别。
transactions	（可选）指定 PKI 交易调试级别。可以使用 ? 查看可用级别。
trustpool	（可选）指定信任池调试级别。使用 ? 查看可用的级别。
1-255	（可选）指定调试级别。

Command Default 默认调试级别为 1。

Related Commands

命令	说明
show debug crypto ca	显示当前处于活动状态的适用于 crypto ca 的调试设置。
undebug	禁用对 crypto ca 的调试。此命令与 **no debug crypto ca** 的效果相同。

debug crypto ikev1

有关与 Internet 密钥交换版本 1 (IKEv1) 相关联的调试配置或设置，请参阅以下命令。

debug *crypto ikev1* ［*timers*］［*1-255*］

Syntax Description

ikev1	启用 *ikev1* 调试。使用 ? 查看可用的子功能。
timers	（可选）启用 IKEv1 计时器调试。
1-255	（可选）指定调试级别。

Command Default 默认调试级别为 1。

Related Commands

命令	说明
show debug crypto ikev1	显示 IKEv1 的当前活动调试设置。
undebug crypto ikev1	禁用 IKEv1 调试。此命令与 **no debug crypto ikev1** 的效果相同。

debug crypto ikev2

有关与 Internet 密钥交换版本 2 (IKEv2) 相关联的调试配置或设置，请参见以下命令。

debug *crypto ikev2* ［*ha* | *platform* | *protocol* | *timers*］

Syntax Description

ikev2	启用调试 *ikev2*。使用 ? 查看可用的子功能。

ha	（可选）指定 IKEv2 HA 调试级别。使用 ? 查看可用的级别。
platform	（可选）指定 IKEv2 平台调试级别。使用 ? 查看可用的级别。
protocol	（可选）指定 IKEv2 协议调试级别。使用 ? 查看可用的级别。
timers	（可选）启用针对 IKEv2 计时器的调试。

Command Default 默认调试级别为 1。

Related Commands

命令	说明
show debug crypto ikev2	显示 IKEv2 的当前活动调试设置。
undebugcrypto ikev2	禁用针对 IKEv2 的调试。此命令与 **no debug crypto ikev2** 的效果相同。

debug crypto ipsec

有关调试与 IPsec 关联的配置或设置的信息，请参阅以下命令。

debug *crypto ipsec* ［*1-255*］

Syntax Description

ipsec	启用对 *ipsec* 的调试要使用 ? 请查看可用的子功能。
1-255	（可选）指定调试级别。

Command Default 默认调试级别为 1。

Related Commands

命令	说明
show debug crypto ipsec	显示 IPsec 的当前活动调试设置。
undebugcrypto ipsec	禁用对 IPsec 的调试。此命令与 **no debug crypto ipsec** 的效果相同。

debug ldap

有关调试与 LDAP 关联的配置或设置的信息（轻量级目录访问协议），请参阅以下命令。

debug *ldap* ［*1-255*］

Syntax Description

ldap	启用对 LDAP 的调试。要使用 ? 请查看可用的子功能。
1-255	（可选）指定调试级别。

Command Default 默认调试级别为 1。

Related Commands

命令	说明
show debug ldap	显示 LDAP 的当前活动调试设置。
undebugldap	禁用对 LDAP 的调试。此命令与 **no debug ldap** 的效果相同。

调试 ssl

请参阅调试与 SSL 会话关联的配置或设置的以下命令。

debug *ssl* [*cipher* | *device*] [*1-255*]

Syntax Description

ssl	启用对 SSL 的调试。使用 ? 查看可用的子功能。
cipher	（可选）指定 SSL 密码调试级别。使用 ? 查看可用的级别。
device	（可选）指定 SSL 设备调试级别。使用 ? 查看可用的级别。
1-255	（可选）指定调试级别。

Command Default

默认调试级别为 1。

Related Commands

命令	说明
show debug ssl	显示 SSL 当前的活动调试设置。
undebug ssl	禁用对 SSL 的调试。此命令与 **no debug ssl** 的效果相同。

debug webvpn

请参阅以下调试与 WebVPN 关联的配置或设置的命令。

debug *webvpn* [*anyconnect* | *chunk* | *cifs* | *citrix* | *compression* | *condition* | *cstp-auth* | *customization* | *failover* | *html* | *javascript* | *kcd* | *listener* | *mus* | *nfs* | *request* | *response* | *saml* | *session* | *task* | *transformation* | *url* | *util* | *xml*]

Syntax Description

webvpn	启用 WebVPN 的调试。使用 ? 可查看可用的子功能。
anyconnect	（可选）指定 WebVPN AnyConnect 调试级别。使用 ? 可查看可用的级别。
chunk	（可选）指定 WebVPN 分块调试级别。使用 ? 可查看可用的级别。
cifs	（可选）指定 WebVPN CIFS 调试级别。使用 ? 可查看可用的级别。
citrix	（可选）指定 WebVPN Citrix 调试级别。使用 ? 可查看可用的级别。
compression	（可选）指定 WebVPN 压缩调试级别。使用 ? 可查看可用的级别。

condition	（可选）指定 WebVPN 过滤条件调试级别。使用 ? 可查看可用的级别。
cstp-auth	（可选）指定 WebVPN CSTP 身份验证调试级别。使用 ? 可查看可用的级别。
customization	（可选）指定 WebVPN 自定义调试级别。使用 ? 可查看可用的级别。
failover	（可选）指定 WebVPN 故障切换调试级别。使用 ? 可查看可用的级别。
html	（可选）指定 WebVPN HTML 调试级别。使用 ? 可查看可用的级别。
javascript	（可选）指定 WebVPN Javascript 调试级别。使用 ? 可查看可用的级别。
kcd	（可选）指定 WebVPN KCD 调试级别。使用 ? 可查看可用的级别。
listener	（可选）指定 WebVPN 侦听程序调试级别。使用 ? 可查看可用的级别。
mus	（可选）指定 WebVPN MUS 调试级别。使用 ? 可查看可用的级别。
nfs	（可选）指定 WebVPN NFS 调试级别。使用 ? 可查看可用的级别。
request	（可选）指定 WebVPN 请求调试级别。使用 ? 可查看可用的级别。
response	（可选）指定 WebVPN 响应调试级别。使用 ? 可查看可用的级别。
saml	（可选）指定 WebVPN SAML 调试级别。使用 ? 可查看可用的级别。
session	（可选）指定 WebVPN 会话调试级别。使用 ? 可查看可用的级别。
task	（可选）指定 WebVPN 任务调试级别。使用 ? 可查看可用的级别。
transformation	（可选）指定 WebVPN 转换调试级别。使用 ? 可查看可用的级别。
url	（可选）指定 WebVPN URL 调试级别。使用 ? 可查看可用的级别。
util	（可选）指定 WebVPN 实用程序调试级别。使用 ? 可查看可用的级别。
xml	（可选）指定 WebVPN XML 调试级别。使用 ? 可查看可用的级别。

Command Default

默认调试级别为 1。

Related Commands

命令	说明
show debug webvpn	显示 WebVPN 的当前活动调试设置。
undebug webvpn	禁用 WebVPN 的调试。此命令与 **no debug webvpn** 的效果相同。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。