使用事件日志收集器和域配置ADC

目录

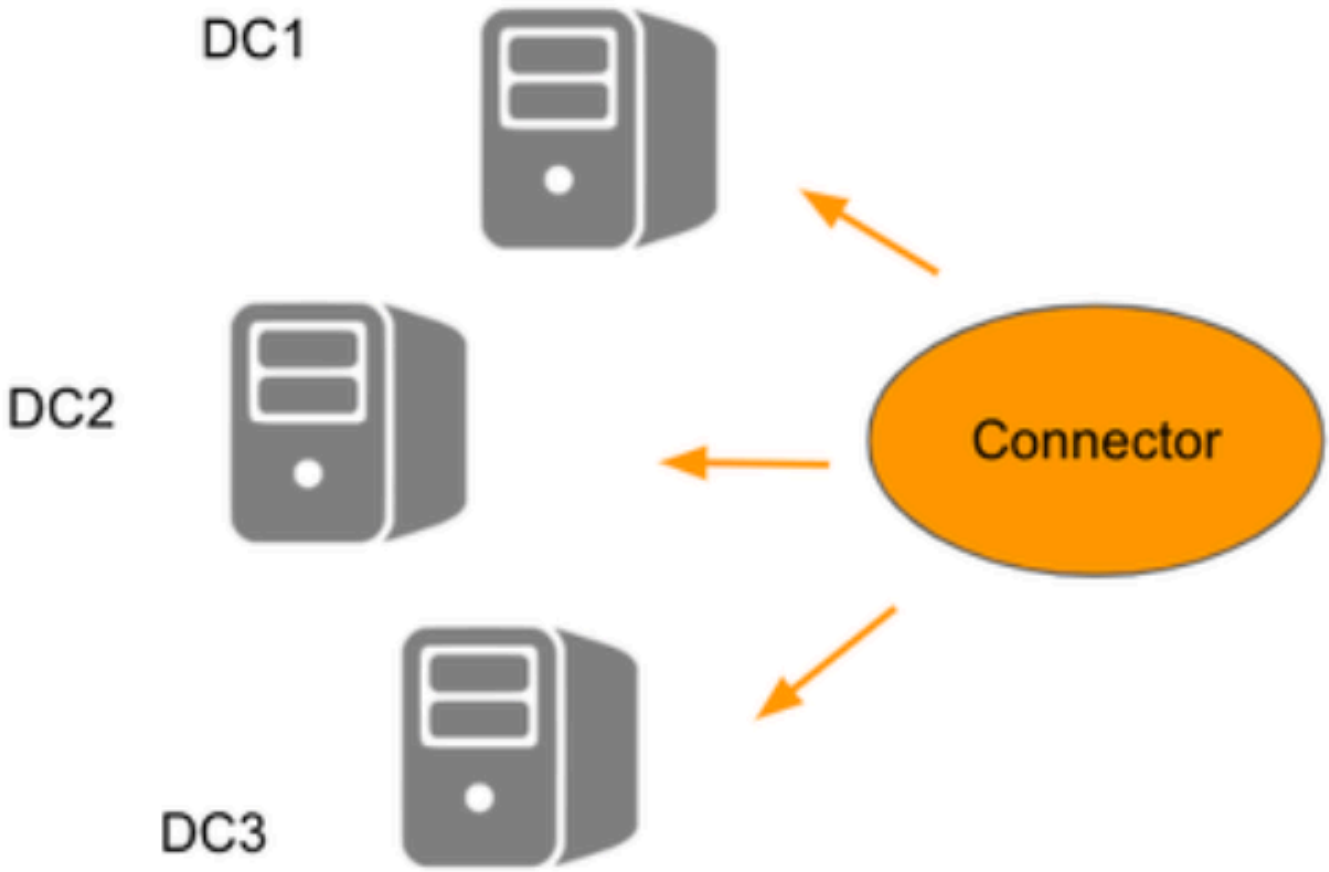
简介

本文档介绍如何使用事件日志收集器和域配置Active Directory连接器(ADC)。

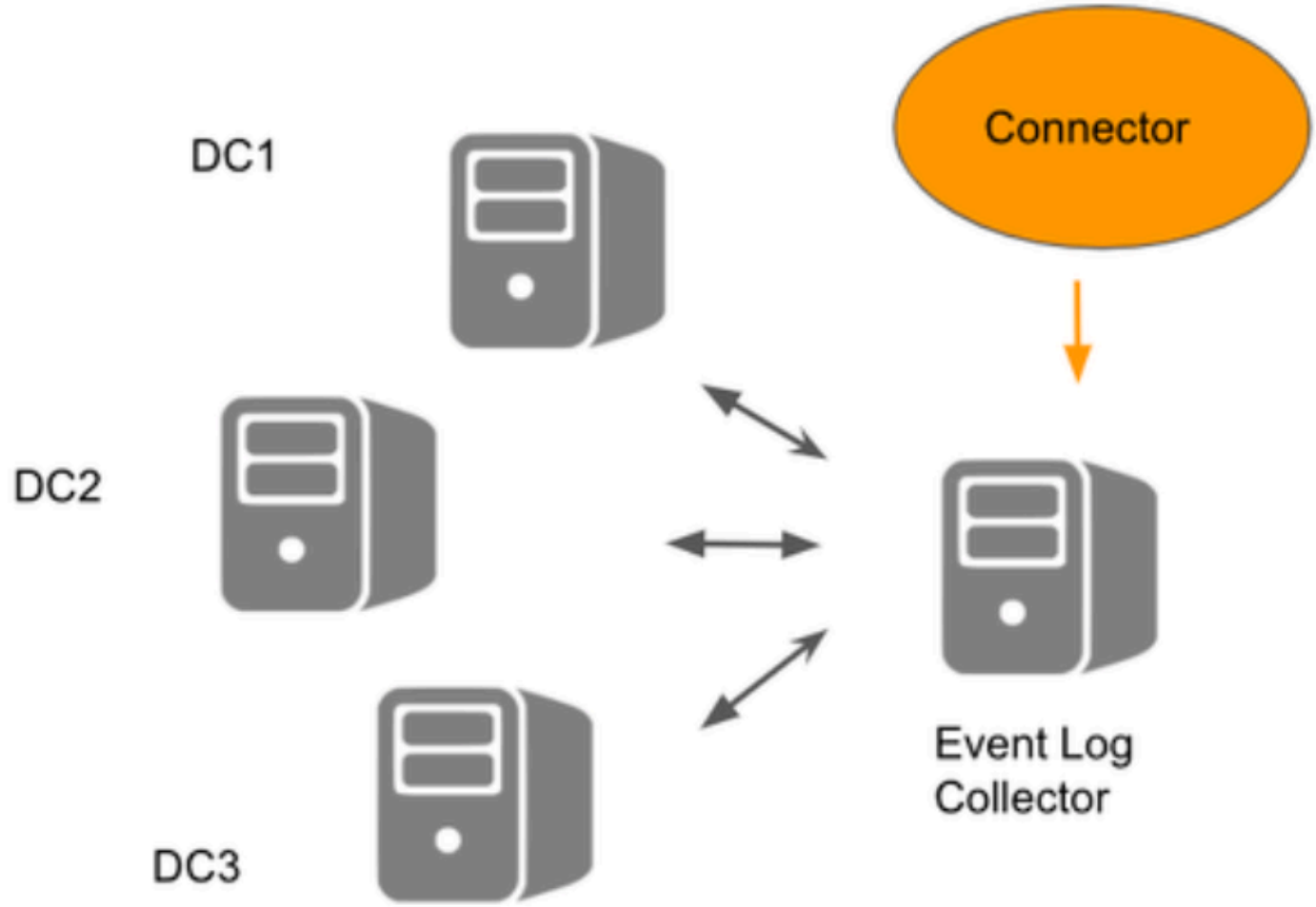
配置选项

有两个设置选项可用于使用Active Directory:

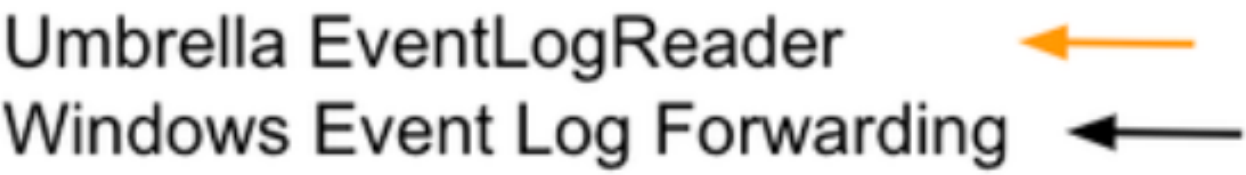
1. 注册域控制器：这涉及使用虚拟设备(VA)和AD连接器，AD连接器直接与所有已注册的域控制器(DC)通信。
2. **事件日志收集**器：此设置包括域、VA和AD连接器。在这种情况下，Windows事件日志转发将信息从DC发送到中央事件日志收集器服务器。然后，AD连接器仅与此中央服务器通信，而非DC



22062473499540

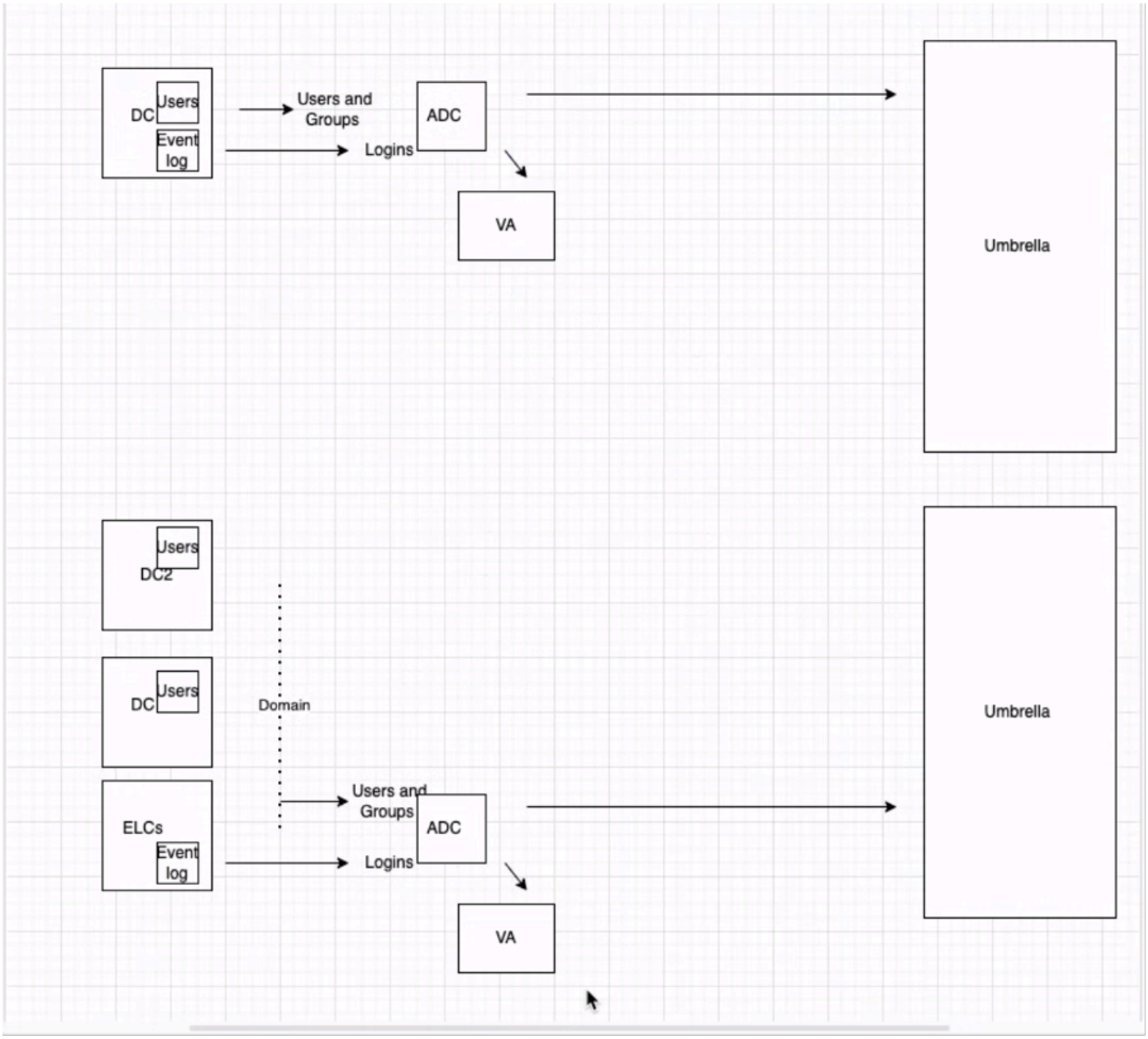


22062473502228



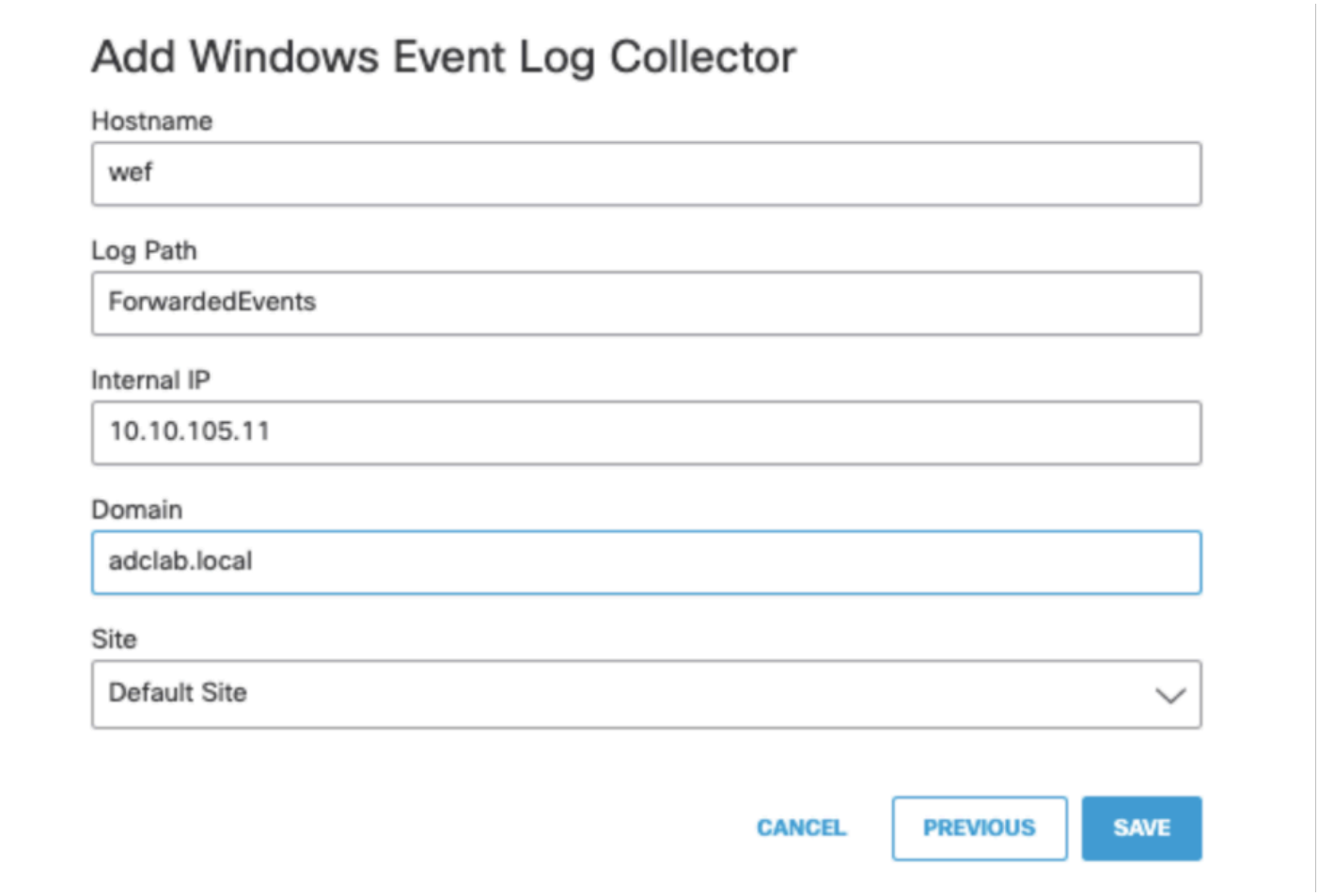
22062518240276

请注意：注册域控制器和添加域是不同的过程。



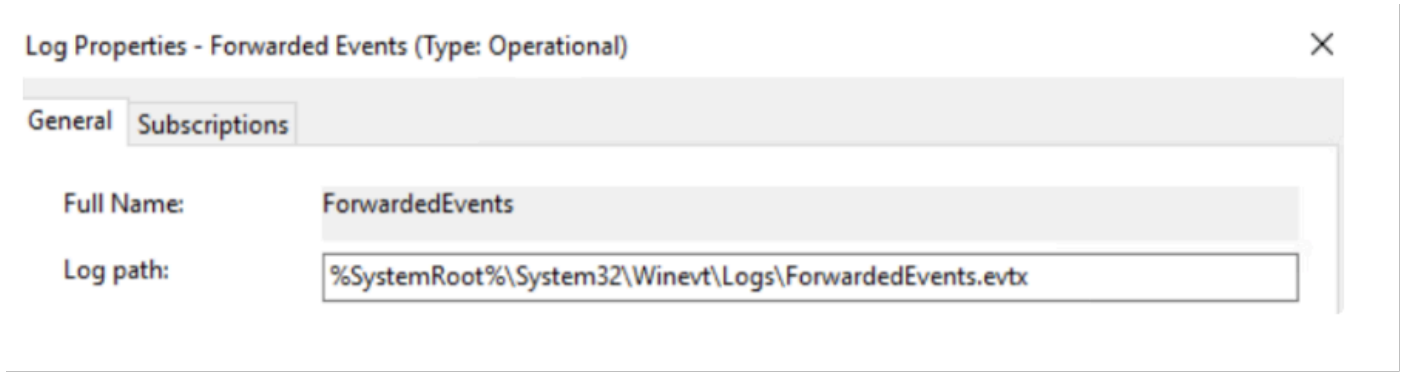
22062518241684

1. 要在Umbrella控制面板中启动配置，请导航到Deployments > Configuration > Sites and Active Directory，然后点击Add。选择Windows Event Log Collector，然后单击“下一步”。



22062473507220

2.客户可以检查日志文件属性（在Windows事件查看器中）以查找日志的名称。请注意，日志文件名必须不带.evtx扩展名或完整路径详细信息。



22062518244756

重要注意事项：

为了使连接器正常工作，有必要继续正常部署步骤：

1. 在“Sites and Active Directory”（站点和Active Directory）页面上注册“Domain”（域），以便进行用户调配。这是必要的，因为没有注册的DC来同步用户/组。
2. 部署“虚拟设备”。

此部署模式存在一些已知限制：

- 即使工作正常，连接器也可能出现错误状态。

要使AD连接器高效工作，需要某些权限。您可以在此处查看这些权限：OpenDNS_Connector用户所需的权限。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。