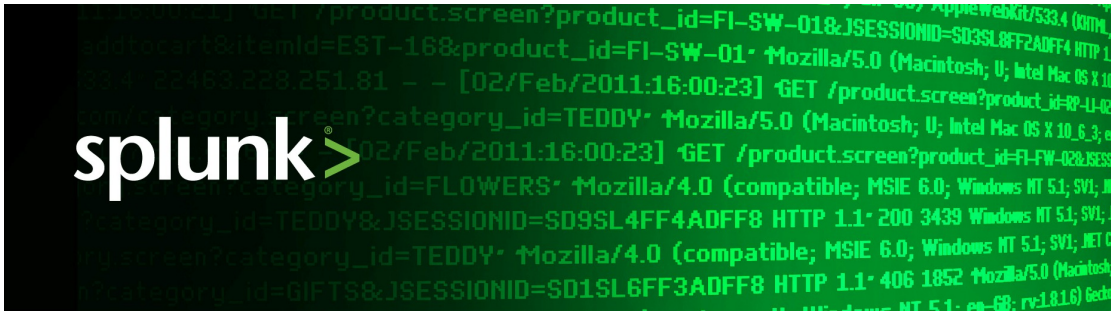

Splunk® Enterprise 7.2.0

添加 Microsoft Active Directory 数据：单实例

生成时间：2018 年 10 月 17 日，上午 11:19

Table of Contents

安装和配置

Microsoft Active Directory Guided Data Onboarding 手册：单实例

Guided Data Onboarding 文档假设您熟悉 Splunk 软件。如果您不知道如何使用 Splunk Enterprise 或不了解 Splunk Cloud，请参阅本手册中的*额外资源*主题。

以下为 Guided Data Onboarding 手册的前提条件。

- 已安装并正在运行的 Splunk Enterprise 单实例部署。
- Splunk Web 的访问权限。
- 允许应用安装的用户角色。

配置 Microsoft Active Directory 域以生成审计事件

配置 Microsoft Active Directory 设备以从作为支持的 Windows Server 版本的域控制器 (DC) 的 Windows 主机中收集 Active Directory 事件日志。

前提条件

在配置 Microsoft Active Directory 域之前，请先满足以下前提条件：

- 确认用户验证。要在您网络的远程 Windows 计算机上执行任何操作，Splunk Enterprise 必须以具有能够访问这些计算机凭据的用户身份运行。
- 确认磁盘带宽。确保带宽足以支持 Splunk Enterprise 索引器和数据。
- 请确保您配置所有安装的防毒软件，以避免监视 Splunk Enterprise 目录或进程，因为此类扫描将显著降低性能。
- 确认共享的主机。

配置 Active Directory 审计策略

配置 Active Directory 审计策略以允许 Active Directory 中的域控制器生成 Splunk 平台部署所需的事件。

默认情况下，Active Directory 不会自动审计某些安全事件。您必须启用事件审计，这样域控制器才会将这些事件记录在安全事件日志通道中。新建组策略对象 (GPO) 并为 AD 环境中的所有 DC 部署该 GPO。激活 GPO 之后，DC 会将这些安全事件记录到安全事件日志中。

然后，安装通用转发器作为 DC 的部署客户端，然后为这些客户端部署相应的 Active Directory 加载项。这些加载项会收集日志并将其转发到 Splunk 平台索引器中。

为两组设置新建单独的 GPO。您可将 PowerShell 和审计设置结合到一个单独的 GPO 中。独立于其他 GPO 新建并部署这些 GPO。

安全事件审计和索引量

启用 DC 上的安全事件日志审计之后，DC 会生成很多数据。这些事件会导致索引量明显增加，可能会造成索引许可证违规问题。您还可能会遇到域控制器性能下降问题，具体取决于服务器额外生成的数据量。

如果您担心启用安全事件审计可能会影响索引量，您可更新策略设置以仅生成对您来说重要的数据。

在 Windows Server 2008、Server 2008 R2、Server 2012 和 Server 2012 R2 上启用审计

执行以下任务以在服务器上启用审计。

新建组策略对象

1. 从“启动 Windows”菜单中，单击**启动** > **管理工具** > **组策略管理**。
2. 在左侧窗格中，在**组策略管理**下，展开您想要设置组策略的林和域。
3. 右击**组策略对象**，然后选择**新建**。
4. 在打开的对话窗口中，在**名称**字段中输入您可以记住的新的组策略对象 GPO 的唯一名称，然后针对**来源启动器 GPO** 字段，勾选**无**。

编辑 GPO 以更改审计策略

如果您使用的是 2008 R1 之前的版本，请使用以下步骤：

1. 打开 GPO，通过右击“组策略对象”窗口中新建的 GPO 并选择**编辑**进行编辑。
2. 在 GPO 编辑器中，选择**计算机配置 > 策略 > Windows 设置 > 安全设置 > 本地策略 > 审计策略**。
3. 为以下策略设置启用**成功**和**失败**审计：
    - 审计帐户登录事件
    - 审计帐户管理
    - 审计目录服务访问权限
    - 审计登录事件
    - 审计对象访问权限
    - 审计策略更改
    - 审计权限使用
    - 审计系统事件
4. 关闭“组策略对象”编辑器窗口以保存更改。

如果您使用的是 2008 R2 或更新版本，请使用以下步骤：

1. 打开 GPO，通过右击“组策略对象”窗口中新建的 GPO 并选择**编辑**进行编辑。
2. 在 GPO 编辑器中，选择**计算机配置** > **策略** > **Windows 设置** > **安全设置** > **高级审计策略配置** > **审计策略**。
3. 为以下策略设置启用**成功**和**失败**审计：
    - 审计帐户登录事件
    - 审计帐户管理
    - 审计目录服务访问权限
    - 审计登录事件
    - 审计对象访问权限
    - 审计策略更改
    - 审计权限使用
    - 审计系统事件
4. 关闭“组策略对象”编辑器以保存更改。

如果您决定启用哪些策略时需要帮助，请参阅 Microsoft 文档获取审计策略意见。或者，遵循组织的安全要求。

部署 GPO

1. 在组策略管理中，右击窗口左窗格中的**域控制器**项目，然后单击**链接现有 GPO...**"
2. 选择您新建的 GPO。
3. 单击**确定**。GPMC 会重新刷新以显示 GPO 是否链接到**域控制器**组织单元。

在 Active Directory 中配置 PowerShell 执行策略

配置 DC 以允许本地执行 PowerShell 脚本，这样这些脚本可在 AD 环境中的 Active Directory 主机上运行。

Splunk App for Windows Infrastructure 安装包中包含的加载项包含 PowerShell 脚本，这些脚本必须在 AD 环境中的 AD（DC 和 DNS）主机上运行。您必须配置 DC 以允许本地执行 PowerShell 脚本，这样这些脚本才可以运行。

要在 DC 上启用本地执行 PowerShell 脚本：

1. 必要时从 Microsoft 支持网站下载并安装 Windows 管理框架。

   所有版本的 Windows Server 2008 SP2（Core 除外）和 Windows Server 2008 R2 均已默认安装 PowerShell。所有版本的 Windows Server 2012 均已默认安装 PowerShell 3.0。您可能需要在 Windows Server 2003 系列计算机上安装 Windows 管理框架。

2. 必要时从 Microsoft 下载并安装适用于 Microsoft PowerShell 的管理模板。

   所有版本的 Windows Server 2008（Core 除外）以及更高版本均已安装适用于 PowerShell 的所需模板。

3. 新建 Active Directory GPO。
4. 打开 GPO 进行编辑。
5. 在 GPO 编辑器中，选择**计算机配置** > **策略** > **管理模板** > **Windows 组件** > **Windows PowerShell**。
6. 右击**打开脚本执行**，然后选择**编辑**。
7. 单击**启用**单选按钮。
8. 在**执行策略**下拉菜单中，选择**允许执行本地脚本和远程签名脚本**。
9. 单击**确定**接受更改。
10. 关闭“组策略对象”编辑器以保存更改。
11. 部署 GPO。

GPO 更新

部署 GPO 之后，Active Directory 要将 GPO 应用于域之前最多可能需要 120 分钟时间。如果您想要更快地部署 GPO，必须在您想要更新 GPO 的每个计算机上运行 `GPUPDATE /force` 命令。

在 Splunk Enterprise 实例上启用接收器

要将数据来源中的数据导入 Splunk Enterprise 实例，您必须同时配置**接收器**和**转发器**。接收器是一个 Splunk Enterprise 实例。您可在数据主机上安装转发器以将数据发送到接收器。

使用 Splunk Web 启用接收器

1. 以管理员身份登录接收器。
2. 单击**设置 > 转发和接收**。
3. 在**配置接收**处，单击**新增**。
4. 您可以使用 `netstat` 工具确定系统上可用的端口。确保 Splunk Web 或 Splunkd 没有使用您选择的端口。
5. 指定您想要用作**接收端口**的 TCP 端口。您可以指定任何未使用端口。
6. 单击**保存**。Splunk 软件开始在您指定的端口处接收传入的数据。
7. 重新启动 Splunk 软件。

在每个 Microsoft Active Directory 主机上安装通用转发器

在 Windows 上安装通用转发器

在 Windows 上安装通用转发器，如下所示：

- 在系统驱动器（启动您 Windows 主机的驱动器）上的 `\Program Files\SplunkUniversalForwarder` 中安装通用转发器。
- 使用 TCP/8089 的默认管理端口安装通用转发器。
- 以“本地系统”用户身份配置通用转发器。
- 新建 Splunk 管理员密码。
- 启用“应用程序、系统和 Windows 安全事件日志”数据导入。

以默认选项在 Window 上安装转发器

1. 从 splunk.com 下载通用转发器。
2. 双击 MSI 文件开始安装。
3. 要查看许可协议，单击**查看许可协议**按钮。
4. 勾选**勾选此框以接受许可协议**复选框。
5. 要更改任何默认安装设置，单击“自定义选项”按钮。或者，单击**安装**按钮进行软件的默认安装。

   以下有两个步骤，至少执行其中一个步骤。否则，通用转发器无法将数据发送到任何地方：

6. （可选）在**部署服务器**窗格中，输入通用转发器应连接的部署服务器的主机名称或 IP 地址和管理端口，并单击**下一步**。
7. （可选）在**接收索引器**窗格中，输入通用转发器应将数据发送至的接收索引器的主机名称或 IP 地址和接收端口，并单击**下一步**。
8. 单击**安装**以继续。

   安装程序将运行并显示**安装完成**对话框。通用转发器自动启动。

9. 在控制面板中，确认 `SplunkForwarder` 服务正在运行。

用自定义选项安装

如果您在通用转发器设置对话框中选择了自定义选项，安装程序会显示以下选项：

1. （可选）单击**更改**指定其他安装目录。
2. （可选）选择 SSL 证书以验证本计算机的身份。根据证书要求不同，您可能需要指定密码和根证书颁发机构 (CA) 证书，以验证证书身份。或者，将这些字段留空。
3. 勾选**本地系统**或**域帐户**复选框，并单击**下一步**。如果指定的是本地系统，安装程序会显示**启用 Windows 输入**对话框。如果指定的是域帐户，安装程序会显示第二个对话框供您输入域和用户信息。
4. 如果勾选的是“域帐户”，安装程序会显示一个对话框让您输入用户名和密码凭据。在**用户名**和**密码**字段输入用户名和密码。仅以 `domain\username` 格式指定用户名。
5. 在**确认密码**字段再次输入密码。
6. 要将您指定的域用户添加到本地管理员组中，勾选**将用户添加为本地管理员**，并单击**下一步**。随后，安装程序会将您指定的域用户添加到本地管理员组。
7. （可选）从列表选择一个或多个 Windows 输入，并单击**下一步**。
8. 为 Splunk `admin` 用户新建密码，然后单击**下一步**。
9. （可选）输入您的部署服务器的主机名称或 IP 地址和管理端口，并单击**下一步**。
10. （可选）输入主机名称或 IP 地址和**接收端口**，并单击**下一步**。
11. 单击**安装**。

在安装程序中启用数据导入的注意事项

如果在安装通用转发器时启用了**启用输入**对话框中的数据导入，安装程序也会安装适用于 Windows 的 Splunk 加载项。安装程序会将启用这些输入的配置保存到加载项中。此配置包括索引定义。

这表示此转发器发送数据至其中的接收索引器必须具有以下定义的索引：

- `perfmon` ，用于“性能监视”输入。
- `windows` ，用于一般的 Windows 输入。
- `wineventlog` ，用于“Windows 事件日志”输入。

默认情况下，索引器未定义这些索引。在安装通用转发器之前定义索引，或在索引器上安装适用于 Windows 的 Splunk 加载项。

有关通用转发器附带的 Windows 第三方二进制文件的相关信息

有关 Windows 版通用转发器提供的 Windows 第三方二进制文件的信息，请参阅 Splunk Enterprise *安装手册*中的*有关随 Splunk Enterprise 分布的 Windows 第三方二进制文件的信息*主题。

在 Splunk 平台上安装适用于 Microsoft Active Directory 的 Splunk 加载项

要安装适用于 Microsoft Active Directory 的 Splunk 加载项，请从 Splunkbase 下载。

然后，完成以下步骤：

1. 下载加载项。
2. 在 Splunk Web 主屏幕中，单击**应用**旁边的齿轮图标。
3. 单击**通过文件安装应用**。
4. 查找已下载的文件并单击**上载**。
5. 如收到重启提示，则重新启动 Splunk Enterprise。

您可通过在 `$SPLUNK_HOME/etc/apps/Splunk_TA_microsoft_ad` 中查找适用于 Microsoft AD 的 Splunk 加载项来确认安装是否成功。

在 Splunk Enterprise 部署上配置适用于 Microsoft Active Directory 的 Splunk 加载项

默认情况下，适用于 Microsoft Active Directory 的 Splunk 加载项不需要任何配置编辑。当您将加载项部署到 Active Directory 域控制器时，只要您配置了审计策略，加载项就会立即开始收集数据。

验证数据

运行 Splunk 软件的“搜索”字段中的以下搜索验证 Microsoft Active Directory 数据是否在 Splunk Enterprise 部署中显示：

```
index=* sourcetype=msad*
```

。

额外资源

额外资源

以下部分提供了额外信息和链接。

关于 Guided Data Onboarding

同时使用 Splunk Web 和 Splunk 文档，Guided Data Onboarding (GDO) 提供端对端指导，以便将特定数据来源导入特定的 Splunk 平台部署。如果您已启动 Splunk 部署并正在运行，并且您具有可以安装加载项的管理员角色或同等角色，您可使用这些指南将热门数据来源导入 Splunk。

查找 Guided Data Onboarding 的位置

从 Splunk Web 主页面中，可通过单击**添加数据**查找数据导入指南。然后，您可以搜索数据来源或浏览不同的数据来源类别。目前，分类有**网络**、**操作系统**和**安全**。

选择数据来源后，您必须选择部署方案。这样您可查看方案和高级步骤来设置和配置数据来源。

Splunk Web 链接到更详细说明如何设置和配置数据来源的文档。您可单击 Splunk Enterprise 文档站点上的**添加数据**选项卡查找所有 Guided Data Onboarding 手册。

支持的部署方案

对于每个数据来源，目前有三种 Splunk 部署方案支持 Guided Data Onboarding。请参阅下表查看每种方案的说明：

部署方案	描述
单实例 部署	Splunk Enterprise 单实例可处理**索引**和**搜索管理**。在此部署方案中，您通常还可以在生成数据的主机上安装**转发器**以向单实例提供主机数据。
分布式部署 索引器群集化	在分布式部署中，多个 Splunk Enterprise **实例**协同工作，以支持数据来自多台计算机的环境，或很多用户需要搜索数据的环境。索引器群集化是一种 Splunk Enterprise 功能，通过此功能**索引器群集**可复制数据以实现若干目标。包括数据可用性、数据保真度、灾难容错和改进的搜索性能。
Splunk Cloud	Splunk Cloud 作为基于云的托管式服务提供 Splunk Enterprise 优势。

如果您确定部署时需要帮助，请参阅*继承 Splunk Enterprise 部署*手册。

支持的数据来源

目前以下几种数据来源支持 Guided Data Onboarding：

数据来源	描述
Cisco ASA	允许管理员将 Cisco ASA 设备、Cisco PIX 和 Cisco FWSM 事件映射到 Splunk **CIM**。 我们可为以下部署方案提供 Guided Data Onboarding： • 单实例 • 具有索引器群集化功能的分布式部署 • 托管式 Cloud 您还可参阅*适用于 Cisco ASA 的 Splunk 加载项*手册了解更多。
McAfee ePO	允许管理员收集防病毒信息和漏洞扫描报告。 我们可为以下部署方案提供 Guided Data Onboarding： • 单实例 • 具有索引器群集化功能的分布式部署 • Splunk Cloud 您还可参阅*适用于 McAfee 的 Splunk 加载项*手册了解更多。

Microsoft Active Directory	允许管理员从 Windows 主机收集 Active Directory 和域名服务器调试日志，这些主机用作受支持的 Windows 服务器版本的域控制器。 我们可为以下部署方案提供 Guided Data Onboarding： • 单实例 • 具有索引器群集化功能的分布式部署 • Splunk Cloud 您还可参阅*适用于 Microsoft Active Directory 的 Splunk 加载项*手册了解更多。
Microsoft Windows	允许管理员通过数据导入收集 CPU、磁盘、I/O、内存、日志、配置和用户数据。 我们可为以下部署方案提供 Guided Data Onboarding： • 单实例 • 具有索引器群集化功能的分布式部署 • Splunk Cloud 您还可参阅*适用于 Windows 的 Splunk 加载项*手册了解更多。
Palo Alto Networks	允许管理员收集 Palo Alto Networks Next-generation Security Platform 中每个产品的数据。 我们可为以下部署方案提供 Guided Data Onboarding： • 单实例 • 具有索引器群集化功能的分布式部署 • Splunk Cloud 您还可访问 splunk.paloaltonetworks.com 了解更多。
Symantec Endpoint Protection	允许管理员通过 dump 文件收集 Symantec Endpoint Protection Manager 中的日志。 我们可为以下部署方案提供 Guided Data Onboarding： • 单实例 • 具有索引器群集化功能的分布式部署 • Splunk Cloud 您还可参阅*适用于 Symantec Endpoint Protection 的 Splunk 加载项*手册了解更多。

关闭 Guided Data Onboarding

如果您不想要在 Splunk Web 中显示 Guided Data Onboarding 功能，请前往 `$SPLUNK_HOME/etc/apps/splunk_gdi/default/gdi_settings.conf` 文件将 `allowWebService` 变量设为 false。

Splunk 文档

Splunk 文档类型多样，包括教程、使用案例、管理员、开发人员和用户手册。

- 要获取 Splunk Enterprise 软件的深入介绍，请参阅 *Splunk Enterprise 概览*手册。
- 更多有关 Splunk Cloud 的更多信息，请参阅 *Splunk Enterprise 用户*手册。
- 如果您是一名继承了 Splunk Enterprise 部署的系统管理员，或者您不确定您拥有哪种类型的部署方案，请参阅*继承 Splunk Enterprise 部署*手册。
- 有关将数据的导入 Splunk 软件的更多信息，请参阅*数据导入*手册。
- 有关安装加载项的更多信息，请参阅 *Splunk 加载项*手册。

您可以在 Splunk 文档站点中找到其他信息。

Splunk 社区

通过 Splunk Answers、Slack、用户组和日志，您可以找到要聊天的其他用户。在社区门户上查找您和 Splunk 社区联系所需的所有内容。

Splunk Education

要了解更多 Splunk 功能和使用方法，请参阅 Splunk Education 视频和课程系列。