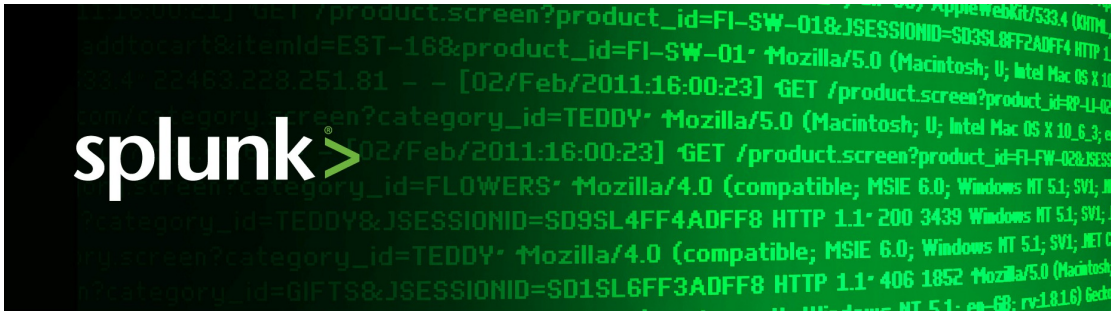


Splunk® Enterprise 6.5.0

确保 Splunk Enterprise 安全

生成时间：2016 年 9 月 26 日，下午 10:27

Table of Contents

关于确保 Splunk Enterprise 安全

关于确保 Splunk 软件安全

在 Splunk 安装期间和安装之后，您必须采取措施以确保您的配置和数据安全。遵循适当的步骤以确保 Splunk 安装减少攻击面并缓解大多数漏洞的风险和影响。有些步骤很简单，例如确保物理服务器安全，且密码管理正确。其他的步骤（如配置加密）有点复杂，但对数据的完整性很重要。

本手册介绍了应该包含在配置中的所有安全区域：

- 安全安装 Splunk 软件
- 使用您选择的验证形式管理用户和基于角色的访问控制
- 使用证书来确保数据最易受攻击的索引器、转发器和 Splunk Web 安全
- 使用加密确保您的配置信息安全
- 使用审计来跟踪系统中的活动。

使用“如何保护和强化 Splunk 软件安装”作为检查表和路线图，以确保您的配置和数据尽可能安全。

保护和强化您安装的 Splunk 软件安全的方式

将本主题作为本手册的检查表和路线图，以帮助您采取所有必要措施来确保 Splunk 软件配置安全并保护您的数据。

设置经过验证的用户并管理用户访问权限

- 确保您的管理员密码安全，并仅将其用于管理任务。
- 使用访问控制列表限制用户访问。
- 设置用户并配置角色和功能以控制用户访问。
- 使用下列任意方法配置用户验证：
  - Splunk 自己的内置系统，如设置使用 Splunk 的内置系统进行的用户验证所述。
  - LDAP，如设置使用 LDAP 进行的用户验证所述。
  - 通过外部验证系统进行脚本式验证 API，例如，PAM 或 RADIUS，如设置使用外部系统进行的用户验证所述。
- 使用使用 SAML 进行单点登录来为用户创建安全的单步登录。

使用证书和加密确保 Splunk 软件配置的通信安全

Splunk 软件提供了一组默认的证书和演示加密的密钥。Splunk 建议部署您自己的证书并将其配置为确保通信安全。请参阅本手册中的关于使用 SSL 确保 Splunk 安全。

强化 Splunk 软件实例，以减少漏洞和风险

- 确保索引器群集和搜索头群集安全。
- 在多个服务器上设置密码以确保一致的验证。
- 确保您服务帐户的安全。
- 强化您的 KV 存储端口。

定期审计您的系统

审计事件中含 Splunk 配置所作更改的相关信息。它为您提供更改的位置、时间以及进行更改的参与者的身份。使用审计事件可以提升安全性，并且还有其他优势：

- 定期审计您的系统以监视用户和管理员访问，以及其他可能导致不安全操作或安全漏洞的活动。
- 留意 Splunk 中的活动（例如搜索或配置更改）。您可以在事件响应期间使用此信息进行合规性报告，故障排除和归因。
- 审计事件在分布式 Splunk 配置中对于检测多个 Splunk 服务器上的配置和访问控制更改特别有用。
  要了解更多信息，请参阅本手册中的审计 Splunk Enterprise 活动。
- 在大多数支持 Splunk 的操作系统上，请使用开箱即用的基于文件系统的监视。
  有关监视的更多信息，请参阅*《数据导入手册》*中的“监视文件和目录”。]

安全安装 Splunk

安全安装 Splunk Enterprise

下载并安装 Splunk Enterprise 时采取以下步骤。

验证完整性

通过使用诸如 Message Digest 5 (MD5) 和 Secure Hash Algorithm-512 (SHA-512) 等哈希函数比较哈希来验证 Splunk Enterprise 下载。使用受信任版本的 OpenSSL。

MD5

1. https://www.splunk.com/en_us/download/splunk-enterprise/thank-you-for-downloading.html

2.点击 MD5 下载链接里面的栏

3.比较结果

SHA512

1.复制下载的链接名称

2.附加 SHA512

3. https://download.splunk.com/products/splunk/releases/6.4.3/windows/splunk-6.4.3-b03109c2bad4-x64-release.msi.sha512

验证签名

您可以按下列步骤使用 Splunk GnuPG 公共密钥验证下载的 RPM 软件包的真实性

1.下载 GnuPG 公共密钥文件（是的，此链接高于 TLS）。

2.使用以下安装密钥：

```
rpm --import <filename>
```

3.使用下列方法验证软件包签名：

```
rpm -K <filename>
```

确保 Splunk Enterprise 在您网络上的安全

在某些情况下，Splunk Enterprise 端口可能变得容易受到攻击。从 Internet 屏蔽 Splunk Enterprise 配置来阻止访问。

如可行，使用基于主机的防火墙限制对 Splunkweb、管理端口和数据端口的访问。保持 Splunk Enterprise 位于基于主机的防火墙内。让远程用户通过虚拟专用网络访问 Splunk Enterprise。

您也可以通过以下方式保护 Splunk Enterprise 免受攻击：

- 通过将此端口仅限定于从主机防火墙后面进行的本地调用，限制 CLI 安全。
- 除非必要，不允许通过任何端口访问转发器。
- 将 Splunk Enterprise 安装到仅可信任计算机可以访问的隔离网段中。
- 将端口可访问性限制为只有必需的连接才可访问。必需的连接为：
    - 最终用户和管理员必须访问 Splunkweb（默认情况下，TCP 端口 8000）。
    - 搜索头必须通过管理端口（默认情况下，TCP 端口 8089）访问搜索节点。
    - 部署客户端必须通过管理端口（默认情况下，TCP 端口 8089）访问部署服务器。
    - 转发器必须访问索引服务器数据端口（默认情况下，TCP 端口 9997）。
    - 远程 CLI 调用使用管理端口。
- 强化您的 KV 存储端口。通过限制 KVstore 访问您的端口来确保您的环境安全。默认情况下，端口 8191 对网络打开。对于搜索头群集，您应该只将端口打开给群集的其他成员，以便其他成员可以复制 KV 存储数据。（KVStore 端口只需能够被搜索头群集的其他成员访问，并且可以完全限制其他角色。）

确保您的管理员帐户安全

使用 Enterprise 许可证的 Splunk 具有默认的管理帐户和密码，admin/changeme。Splunk 强烈建议您更改默认值，以确保系统安全。您的密码应该很复杂，并遵循一般密码的最佳做法：

- 使用单词、数字、符号及大小写字母组合。

- 虽然复杂性很重要，但长度却至关重要。我们建议密码长度至少为 10 个字符。
- 不要将您的生日、社会保险号、电话号码或家人姓名等用作密码，因为可能不是很可靠。
- 不要使用字典中可以找到的单词。
- 不要使用您在其他地方使用或之前使用过的密码。

使用 Splunk Web

要更改管理员默认密码：

1.以管理员用户身份登录 Splunk Web。

2.单击界面右上方的**设置**。

3.在屏幕的“用户和验证”部分中单击**访问控制**。

4.单击**用户**。

5.单击 **admin** 用户。

6.更新密码，并单击**保存**。

使用 Splunk CLI

Splunk CLI 命令为：

```
splunk edit user
```

重要提示：您必须首先使用现有密码进行验证，然后才能更改密码。通过 CLI 或使用 `-auth` 参数登录 Splunk。例如，该命令将管理员密码从 *changeme* 更改为 *foo*：

```
splunk edit user admin -password foo -role admin -auth admin:changeme
```

注意：在 *nix 操作系统上，shell 会将某些特殊字符解释为命令指令。您必须对这些字符进行转义，方法是分别在各字符之前加上 \ 或者将密码用单引号 (') 括起。例如：

```
splunk edit user admin -password 'FFL14io!23ur$' -role admin -auth admin:changeme
```

或

```
splunk edit user admin -password FFL14io!23ur\$ -role admin -auth admin:changeme
```

在 Windows 上，使用脱字符 (^) 对保留的 shell 字符进行转义或者将密码用双引号 (") 括起。例如：

```
splunk edit user admin -password "FFL14io!23ur>" -role admin -auth admin:changeme
```

或

```
splunk edit user admin -password FFL14io!23ur^> -role admin -auth admin:changeme
```

注意：您还可以跨服务器一次重置所有密码。有关过程，请参阅“跨多个服务器部署密码”。

禁用多余的 Splunk Enterprise 组件

对于单服务器 Splunk Enterprise 部署：

- 转发器不应运行 Splunkweb，也不应配置为通过 TCP 或 UDP 端口接收数据，或从其他 Splunk Enterprise 实例接收数据。

对于多服务器 Splunk Enterprise 部署：

- 搜索头不应通过 TCP 或 UDP 端口接收数据，或者从其他 Splunk Enterprise 实例接收数据。
- 在分布式环境中，如果用户不在索引器上登录 Splunkweb，应在索引器上禁用 Splunkweb。
- 转发器不应运行 Splunkweb，也不应配置为通过 TCP 或 UDP 端口接收数据，或从其他 Splunk 实例接收数据。

确保您服务帐户的安全

应以非特权用户身份运行 Splunk 软件来实施最小权限的原则，而不要使用诸如 root 或管理员等的特权帐户。

- 在 Unix 或 Linux 中，使用通过 PKG 或 RPM 软件包创建的 "splunk" 用户，或创建只在 `$SPLUNK_HOME` 上具有特权和所有权的您自己的用户。
- 在 Windows 上，通常最好使用本地系统上下文。但是，如果您需要使用 windows 通信通道（如 WMI）进行通信，应使用受限制的访问帐户。

跨多个服务器部署安全密码

Splunk Enterprise 在初始启动阶段创建 `$SPLUNK_HOME/etc/auth/splunk.secret` 文件。此文件包含用于加密配置文件中的一些验证信息的密钥：

- `web.conf`：每个实例中的 SSL 密码。
- `authentication.conf`：您的 LDAP 密码（若有）。
- `inputs.conf`：使用 `splunktcp-ssl` 时的 SSL 密码。
- `outputs.conf:`：使用 `splunktcp-ssl` 时的 SSL 密码。
- `server.conf`: pass4symmkey，如果您有其中之一。

Splunk 软件启动后，如果在这些设置中检测到明文密码，它将创建或用加密密码覆盖等效的本地文件夹中的配置。

注意：如果 pass4symmkey 或 SSLPassword 在默认应用文件中指定，则当重新启动时，在文件的本地版本中将混淆密码。文件的默认版本为纯文本格式。然而，如果使用 `curl` 或 splunkd 端点列出文件，则密码将显示为加密。

在多个服务器上部署 Splunk 软件时，可以执行以下步骤来加密这些密码并确保密码在整个您的部署中保持一致。应在原始部署以及您需要为实例部署新密码时执行这些步骤：

1.配置一个 Splunk 实例并根据需要修改任何密码。（如果这是新配置，请勿启动任何其他实例。）

2.重新启动配置的实例以对文件中的密码进行加密。密码信息会继续以纯文本形式存储，直到其在重新启动时获得加密。

3.将加密文件 `splunk.secret` 从配置的示例复制到所有的其他示例。

4.启动已将此文件复制到的所有新实例，或者如果您要在部署之后分布修改后的文件，重新启动现有实例。

注意：该过程与搜索头群集无关。在群集的初始部署阶段，位于搜索头群集的管理员复制其 `splunk.secret` 文件至所有其他群集成员，所以您不必手动复制。作为其正常操作的一部分，群集也会自动复制由自己使用的应用所存储的任何凭据。

强化您的 KV 存储端口

我们建议您通过限制 KVstore 访问您的端口来确保您的环境安全。默认情况下，端口 8191 对网络打开。我们建议您尽可能限制此端口。

对于搜索头群集，您应该只将端口打开给群集的其他成员，以便其他成员可以复制 KV 存储数据。

有关使用 KV 存储的更多信息，请参阅“关于应用键值存储”。

强化您的配置

考虑利用以下机会确保您的配置安全：

- 使用配置管理工具（如 subversion）为 Splunk 配置提供版本控制。
- 将 Splunk 配置更改集成到您的现有更改管理框架中。
- 将 Splunk Enterprise 配置为监视其自己的配置文件并在发生更改时告警。
- 使用版本控制。Git 是一个有用的版本控制示例。
- 不要将您的配置作为公共职责发布。

服务器和操作系统的一些最佳做法

操作系统

要最大程度地提高安全性，请在运行 Splunk 软件的所有计算机上强化操作系统。

- 如果贵组织没有内部强化标准，请参阅 CIS 强化基准。
- 至少限制对 Splunk 服务器的 shell/命令行访问。

Splunk

- 配置冗余 Splunk 实例（两者均为相同数据的副本建立索引）。
- 定期备份 Splunk 数据和配置。
- 尝试从备份恢复 Splunk Enterprise 以定期执行恢复测试。

- 通过使用诸如 MD5 的哈希函数比较哈希来验证 Splunk 下载。例如：

```
./openssl dgst md5 <filename-splunk-downloaded.zip>
```

客户端浏览器

- 使用受支持浏览器（如 Firefox 或 Internet Explorer）的当前版本。
- 使用客户端 JavaScript 阻止程序（如 Firefox 或 Internet Explorer 8 过滤器上的 noscript）帮助防止 XSS、XSRF 及类似的漏洞。
- 确保用户安装最新的 Flash 版本。

物理安全性

- 确保对所有 Splunk 服务器的物理访问安全。
- 确保 Splunk 最终用户实施合理的物理和端点安全性。
    - 为 Splunk Web 用户会话设置较短的超时时间。有关更多信息，请参阅“配置超时”。

更多确保您配置安全的机会

- 使用配置管理工具（如 subversion）为 Splunk 配置提供版本控制。
- 将 Splunk 配置更改集成到您的现有更改管理框架中。
- 将 Splunk Enterprise 配置为监视其自己的配置文件并在发生更改时告警。

用户和基于角色的访问控制

使用访问控制确保 Splunk 数据安全

基于角色的访问控制提供了灵活高效的工具，可供您用于保护 Splunk 数据。

Splunk Enterprise 以类似关系数据库管理基于角色的访问控制的方式通过掩码向用户显示数据。在某些情况下，可能需要数据的总分段。在其他情况下，在显示层控制搜索和结果（可以在许多 Splunk 应用中实现）可能会符合您的安全需要。

决定如何设置您的配置以及基于角色的访问是否符合您的需要时，请考虑您的使用案例。例如：

- 对于极其敏感的数据，如果即使允许访问可能具有敏感数据的系统也会产生法律风险，请考虑安装和配置 Splunk Enterprise 的多个实例，然后对每个实例配置适合相应受众的数据。
- 有意或无意向错误的用户披露敏感数据可能会导致法律后果时，考虑针对特权帐户和非特权帐户专门创建索引，然后将它们分配给为每个访问级别创建的角色。
- 在存在安全问题但没有太大法律风险时，您可以使用“应用”限制访问。例如，您可以创建具有静态仪表板的应用，并将具有较低许可的角色分配给这些仪表板，限制分配有该角色的用户可以访问的信息类型。
- 字段加密、搜索排除和对已编辑数据设置字段别名也是加强限制搜索的好方法。

关于用户验证

Splunk Enterprise 验证允许添加用户、为用户分配**角色**以及根据组织的需要为这些角色提供自定义权限。

验证系统的选项如下：

- Splunk 验证：默认情况下提供**管理员**、**高级用户**和**普通用户**，您可以使用**功能**列表定义自己的角色。如果您有 Enterprise 许可证，则默认情况下启用 Splunk 验证。有关更多信息，请参阅设置使用 Splunk 的内置系统进行的用户验证。
- LDAP：Splunk Enterprise 支持使用其内部验证服务或您的现有 LDAP 服务器进行验证。有关更多信息，请参阅设置使用 LDAP 进行的用户验证。
- 脚本式验证 API：使用脚本式验证将 Splunk 验证与外部验证系统（如 RADIUS 或 PAM）集成起来。有关更多信息，请参阅设置使用外部系统进行的用户验证。

注意：验证包括本机验证、LDAP 和脚本式验证，但在 Splunk Free 中却无法使用。

您可以在 Splunk Web 中，或者通过编辑 authorize.conf 创建用户，并为用户分配灵活的角色。有关角色和功能的更多信息，请参阅关于基于角色的用户访问权限。

重要提示：Splunk 验证优先于任何外部系统。按以下顺序验证用户：

1.Splunk 验证

2.LDAP 或脚本式验证（如启用）

关于配置基于角色的用户访问权限

如果您运行 Splunk Enterprise，您可以创建具有密码的用户，然后将这些用户分配给**角色**。角色决定访问权限和分配到该角色的任何用户**权限**。

关于用户的更多信息，请参阅关于用户验证。

预定义角色：

- 管理员：此角色专门用于管理所有或大部分用户、对象和配置的管理员，并预定义了分配最多的**功能**。
- 高级用户：该角色可以编辑所有共享对象（保存的搜索等），以及告警、标记事件或其他类似任务。
- 普通用户：该角色可以创建并编辑自己的已保存搜索、运行搜索、编辑其首选项、创建并编辑事件类型和其他类似任务。
- can_delete：此角色允许用户按关键字删除。在使用删除搜索运算符时，才需要此功能。
- sc_admin（仅适用于云）：此角色允许用户创建用户和角色，但不会授予任何其他管理员功能。

您还可以创建自定义角色，并为您的用户分配这些角色。创建自定义角色时，您会确定以下内容：

- 允许的搜索：您可以定义分配给角色的用户允许执行的搜索。
- 角色继承：您可以让您的角色继承一个或多个现有角色的特定属性。本主题中稍后会讨论角色继承。
- 分配功能：您可以指定分配给角色的用户可以执行的操作（更改其密码，更改转发器设置等）。有关更多信息，请参阅关于使用功能定义角色。
- 设置允许的索引和默认索引：您可以限制对特定索引的访问，并设置默认搜索的索引。

要在 Splunk Web 中创建角色，请参阅通过 Splunk Web 添加和编辑角色。要通过编辑 `authorize.conf` 创建角色，请参阅使用 authorize.conf 添加和编辑角色。

继承

作为规则，多个角色的成员会从具有最广泛权限的角色继承属性。

用户如何继承搜索过滤器限制

您可以创建继承其他角色特性的角色。分配给多个角色的用户会从已分配的角色继承属性。

如果是搜索过滤器，将用户分配给具有不同搜索过滤器的角色时，会合并所有过滤器，从而应用每个角色的限制。

例如，默认情况下，高级用户和普通用户角色没有定义为限制搜索的搜索过滤器。如果用户具有这些角色和定义了过滤器（例如，`srchFilter=x`）的其他角色，则用户将继承该角色的限制（虽然与没有过滤器的角色关联）。

用户如何继承允许的索引

如果是允许的索引，则为用户提供已授予为其分配的角色的最高级别访问权限。

例如，如果将用户同时分配给“简单用户”角色（此角色只能访问一个特定的索引）和“高级用户”角色（此角色具有更多的功能，并允许访问所有索引），则该用户将具有所有索引的访问权限。如果您要授予“高级用户”的功能，但继续将其索引访问限制为针对“简单用户”定义的单个索引，则应专门为该用户创建一个新角色。

用户如何继承功能

如果是功能，为用户提供已授予为其分配的角色的最高级别权限。

例如，如果为用户同时分配具有最多功能的“管理员”角色和具有一组不同功能的“高级用户”角色，则该用户将具有这两个角色的功能。

关于使用功能定义角色

在 Splunk Web 中创建用户时，为该用户分配一个角色。有关更多信息，请参阅“关于基于角色的用户访问权限”。

每个角色都包含一组**功能**。您可以为新角色、现有角色和默认角色添加或编辑功能。例如，您可以授予角色添加输入或编辑保存的搜索的功能。

要在 Splunk Web 中添加或更改某个角色的功能，请参阅“通过 Splunk Web 添加和编辑角色”。要通过编辑 authorize.conf 创建角色，请参阅“使用 authorize.conf 添加和编辑角色”。

可用功能列表

此列表显示您可以添加到任何角色的功能。在 authorize.conf 中查找此列表的最新版本。管理员角色具有此列表中的所有功能，"delete_by_keyword" 功能除外。

功能名称	可执行的操作
accelerate_datamodel	启用或禁用数据模型加速。
accelerate_search	启用或禁用报表加速。为使某个角色能够使用此功能，该角色还必须具有 schedule_search 功能。
admin_all_objects	访问和修改系统中的任何对象（用户对象、搜索任务等）。（覆盖对象中设置的限制。）
change_authentication	更改验证设置和重新加载验证。
change_own_password	用户可以更改其密码。
delete_by_keyword	在搜索中使用 "delete" 运算符。
edit_deployment_client	更改部署客户端设置。
edit_deployment_server	更改部署服务器设置。
edit_dist_peer	添加和编辑分布式搜索的对等节点。
edit_forwarders	更改转发器设置。
edit_httpauths	编辑和结束用户会话。
edit_indexer_cluster	编辑索引器群集。
edit_input_defaults	更改输入数据的默认主机名。
edit_modinput_perfmon	在 perfmon.conf 中编辑模块化输入。
edit_modinput_admon	在 admon.conf 中编辑模块化输入。
edit_monitor	为监视文件添加输入和编辑设置。
edit_roles	编辑角色，并更改用户/角色映射。
edit_roles_grantable	编辑角色并更改有限组角色的用户/角色映射。可以为其他用户分配任何角色。要限制此功能，请在 authorize.conf 中配置 grantableRoles。例如：grantableRoles = role1;role2;role3
edit_scripted	创建和编辑脚本式输入。
edit_search_head_clustering	编辑搜索头群集设置。
edit_search_server	编辑诸如超时、检测信号和黑名单等一般分布式搜索设置。
edit_search_scheduler	编辑搜索计划程序。
edit_server	编辑诸如服务器名称、日志级别等一般服务器设置。
edit_server_crl	编辑服务器控件。
edit_splunktcp	更改从其他 Splunk 实例接收 TCP 输入的设置。
edit_splunktcp_ssl	可以列出或编辑 Splunk TCP 输入的特定于 SSL 的设置。
edit_splunktcp_token	编辑 Splunktcp 令牌。
edit_sourcetypes>	编辑 sourcetypes。
edit_tcp	更改接收一般 TCP 输入的设置。
edit_tcp_token	更改 TCP 令牌。这是管理员功能，应该只能分配给系统管理员。
edit_telemetry_settings	选择启用或退出产品工具。请参阅*《管理员手册》*中的“共享性能数据”。
edit_token_http	编辑 http 令牌
edit_udp	更改 UDP 输入的设置。
edit_user	创建、编辑或删除用户。具有 edit_user 功能的角色可以将任何角色分配给其他用户。要限制此功能，请在 authorize.conf 中配置 grantableRoles。例如：grantableRoles = role1;role2;role3
edit_view_html	创建、编辑或修改基于 HTML 的视图。
edit_web_settings	更改 web.conf 的设置。
embed_report	嵌入报表并禁用所嵌报表的嵌入操作。
export_results_is_visible	显示或隐藏 Splunk Web 中的**导出结果**按钮。默认值为显示按钮。
extra_x509_validation	添加附加 x509 验证。
get_diag	使用 /streams/diag 端点从 Splunk 实例获取远程诊断。

get_metadata	使用 "metadata" 搜索处理器。
get_typeahead	使用键盘缓冲。
indexes_edit	更改诸如文件大小和内存限制等索引设置。
input_file	添加文件作为输入。
license_tab	访问和更改许可证。
license_edit	编辑许可证。
license_view_warnings	查看许可证警告。
list_deployment_client	查看部署客户端设置。
list_deployment_server	查看部署服务器设置。
list_forwarders	查看转发器设置。
list_httpauths	查看用户会话。
list_inputs	查看不同输入的列表，其中包括文件、TCP、UDP、脚本等输入。
list_introspection	查看自检文件。
list_indexer_cluster	查看索引器群集列表
list_search_scheduler	查看搜索计划程序任务列表。
list_settings	查看所有配置设置。
list_storage_passwords	查看存储密码列表。
output_file	添加文件作为输出。
pattern_detect	在“搜索”视图中查看和使用“模式”选项卡的控制能力。
request_remote_tok	获取远程验证令牌。
rest_apps_management	编辑 python 远程应用处理程序中的设置。
rest_apps_view	列出 python 远程应用处理程序中的属性。
rest_properties_get	可以从服务/属性端点获取信息。
rest_properties_set	编辑服务/属性端点。
restart_splunkd	通过服务器控制处理程序重新启动 Splunk Enterprise。
rtsearch	运行实时搜索。
run_debug_commands	运行调试命令。
schedule_search	计划已保存搜索、创建并更新告警、查看触发的告警信息。
schedule_rtsearch	计划实时保存的搜索。为使用户能够使用此功能，该角色还必须具有 schedule_search 功能。
search	运行搜索。
srchFilter	让用户管理搜索筛选器。
srchIndexesAllowed	允许用户搜索索引。
srchJobsQuota	设置搜索任务配额。
srchMaxTime	设置搜索的最大时间。
use_file_operator	使用 "file" 搜索运算符。
srchIndexesDefault	设置默认的搜索索引。
web_debug	调试 Web 文件。

Windows 特定功能

如果您在 Windows 上运行 Splunk Enterprise，则将提供其他功能以便于监视。

功能名称	可执行的操作
edit_win_eventlogs	编辑 windows eventlogs。
edit_win_wmiconf	编辑 wmi.conf。

edit_win_regmon	（已弃用）
edit_win_admon	（已弃用）
edit_win_perfmon	（已弃用）
list_win_localavailablelogs	列出所有本地 Windows 事件日志。
list_pdfserver	查看 PDF 服务器文件
write_pdfserver	写入 PDF 服务器文件。
srchTimeWin	设置搜索时间限制。

通过 Splunk Web 添加和编辑角色

在创建用户时，您为用户分配决定 Splunk Enterprise 访问级别的角色，以及用户可以执行的任务。Splunk Enterprise 提供一组您可以使用的默认角色。您也可以创建自己的角色。

有关角色，以及如何继承功能和权限的信息，请参阅关于基于角色的用户访问权限。

注意：从“管理员”或“高级”用户继承的自定义角色不会自动继承管理访问权限。有关授予自定义角色管理访问权限的信息，请参阅为自定义角色添加访问控制。

添加或编辑角色

在 Splunk Web 中创建或编辑角色：

1. 单击**设置 > 访问控制**。
2. 单击**访问控制**页面，单击**角色**。
3. 单击**新建**或选择并编辑现有角色。角色名称只能使用小写字符，不得包含空格、冒号或正斜线。
4. 为此角色指定**搜索限制**。通过指定搜索限制来创建和限制数据访问控制和搜索功能。
   - **限制搜索术语：**您可以创建搜索字符串，使其能够确定对于分配至角色的用户来说，将显示（或不显示）哪些数据。请参阅本主题的搜索过滤器格式。
   - **限制搜索时间范围**：指定此角色可以搜索的时间窗的范围。
   - **用户级并发搜索任务限制：**指定一次可以为此角色运行的最大搜索任务数。
   - **用户级并发实时搜索任务限制：**指定可以同时为此角色的用户运行的实时搜索任务数。
   - **角色级并发搜索任务限制：**指定一次可以为此角色运行的最大搜索任务数。
   - **角色级并发实时搜索任务限制：**指定可以同时为此角色运行的实时搜索任务数。
   - **限制任务总数磁盘配额：**指定您要专用于分配给角色的每个用户的搜索任务的总磁盘空间。
5. 在**继承**部分中，选择您要新角色从中继承功能和属性的角色。分配给多个角色的用户会从具有最广泛权限的角色继承属性。有关更多信息，请参阅关于基于角色的用户访问权限主题中的角色继承。
6. 在**功能**部分中，选择您要为此角色提供的各项功能。有关更多信息，请参阅关于使用功能定义角色。
7. 在**默认搜索的索引**中，指定在搜索中未指定索引时此角色将自动搜索的索引。
8. 在**索引**中，选择允许用户搜索的索引。如果您添加至少一个索引，则具有此角色的用户将只能在选定的一个或多个索引上执行搜索。如果您未指定任何索引，则分配给此角色的用户可以搜索所有索引。
9. 单击**保存**。

搜索过滤器格式

“搜索过滤器”字段中可以包括以下任一搜索术语：

- `source=`
- `host=`
- `index=`
- `eventtype=`
- `sourcetype=`
- 搜索字段
- 通配符
- 通过 `OR` 可使用多个术语，或通过 `AND` 可使搜索的限制性更高

搜索术语不能包括：

- 保存的搜索
- 时间运算符
- 正则表达式

- Splunk Web 可以覆盖的任何字段或修饰符

使用 authorize.conf 添加和编辑角色

您可以通过编辑 authorize.conf 添加或修改角色。用户会被分配给角色，这些角色决定了用户的访问级别以及可以执行的任务。有关角色和功能的更多信息，请参阅关于基于角色的用户访问权限。

警告：不要在 `$SPLUNK_HOME/etc/system/default/authorize.conf` 中编辑或删除任何角色。这可能破坏您的管理员功能。在 `$SPLUNK_HOME/etc/system/local/` 或您自己的自定义应用程序目录（在 `$SPLUNK_HOME/etc/apps/` 中）中编辑此文件。更多有关配置文件的一般信息，请参阅《管理员手册》中的"关于配置文件"。

注意：分布式搜索配置的授权需求稍有不同。您使用搜索头合并时，必须确保搜索头和搜索节点全部使用同一组 `authorize.conf` 文件。要确保为搜索合并正确设置了授权，请参阅"授权如何在分布式搜索中工作"。

添加角色

以下是通过 `$SPLUNK_HOME/etc/system/local/authorize.conf` 添加角色的语法：

```
[role_<roleName>]
<attribute> = <value>
<attribute> = <value>
...
```

段落标题中的 `<roleName>` 是您要为角色提供的名称。例如：`security`、`compliance`、`ninja`。

角色名称只能使用小写字符，不得包含空格、冒号、分号或正斜线。

您可以在角色段落中包括以下属性：

- `<capability> = enabled`
  - 您可以将任意多个功能添加到角色。有关更多信息，请参阅关于使用功能定义角色。
  - 默认情况下禁用功能。要将功能添加到角色，仅将其设置为 "enabled" 即可。
- `importRoles = <role>;<role>;...`
  - 设置完成后，当前角色将从 `<role>` 继承所有功能。分配给多个角色的成员会从具有最广泛权限的角色继承属性。有关更多信息，请参阅"关于用户和角色"主题中的角色继承。
  - 如果有多个角色，用分号分隔。
- `srchFilter = <search_string>`
  - 使用此字段对访问权限进行精细粒度的控制。对此角色的搜索将由此表达式过滤。有关更多信息，请参阅本主题的搜索过滤器格式。
- `srchTimeWin = <string>`
  - 通过此角色执行的搜索的最大时间跨度（单位为秒）。
- `srchDiskQuota = <int>`
  - 属于此角色的用户的搜索任务可以占用的最大磁盘空间量 (MB)。
- `cumulativeSrchJobsQuota = <number>`
  - 此角色的所有成员可以拥有的最多并发运行的历史搜索数量。
  - **注意：**某用户属于多个角色时，此用户首先使用具有最大累计搜索配额的角色的搜索。在该角色的搜索配额全部用完时，再使用具有较低配额的角色。
- `cumulativeRTSrchJobsQuota = <number>`
  - 此角色的所有成员可以拥有的最多并发运行的实时搜索数量。
  - **注意：**某用户属于多个角色时，此用户首先使用具有最大累计搜索配额的角色的搜索。在该角色的搜索配额全部用完时，再使用具有较低配额的角色。
- `srchJobsQuota = <int>`
  - 此角色的成员可以拥有的最多并发运行的搜索数量。
- `rtSrchJobsQuota = <number>`
  - 此角色的成员可以同时运行的实时搜索最大数目。
- `srchIndexesDefault = <string>`
  - 未指定索引时要搜索的以分号分隔的索引列表。
  - 这些索引可以使用通配符，但 '*' 不匹配内部索引。
  - 要匹配内部索引，以 '_' 开头。所有内部索引均由 '_*' 表示。
- `srchIndexesAllowed = <string>`
  - 允许此角色搜索的分号分隔的索引列表。
  - 遵守与 `srchIndexesDefault` 相同的通配符语义。

注意：对 `authorize.conf` 进行更改后，必须重新加载验证或重新启动 Splunk。否则，您的新角色将不会出现在**角色**列表中。要重新加载验证，转到 Splunk Web 的**管理器 > 验证**部分。此操作刷新验证缓存，但不会启动当前用户。

搜索过滤器格式

`srchFilter`/ 字段中可以包括以下任一搜索术语：

- source=
- host= 和主机标记
- index= 和索引名称
- eventtype= 和事件类型标记
- sourcetype=
- 搜索字段
- 通配符
- 通过 OR 可使用多个术语，或通过 AND 可使搜索的限制性更高。

搜索术语不能包括：

- 保存的搜索
- 时间运算符
- 正则表达式
- Splunk Web 可以覆盖的任何字段或修饰符

在 authorize.conf 中创建角色的示例

本示例创建 "ninja" 角色，该角色继承默认“用户”角色的功能。ninja 具有与默认“高级用户”角色几乎相同的功能，但此角色不能计划搜索。另外：

- 搜索过滤条件限制 ninja 在 host=foo 搜索。
- 如果未在搜索中指定索引，则 ninja 可以搜索所有公共索引（不以下划线开头），并将搜索索引 mail 和 main。
- ninja 可以同时运行 8 个搜索任务和 8 个实时搜索任务。（这些计数互不相关。）
- ninja 最多可以占用总计 500MB 的磁盘空间用于其所有任务。

```
[role_ninja]
rtsearch = enabled
importRoles = user
srchFilter = host=foo
srchIndexesAllowed = *
srchIndexesDefault = mail;main
srchJobsQuota   = 8
rtSrchJobsQuota = 8
srchDiskQuota   = 500
```

设置管理器控制台和应用的访问权限

利用 local.meta 文件可以方便地授予和限制对 Splunk 实例特定部分的访问权限。例如，您可以：

- 限制自定义角色中的用户只能访问特定应用
- 批准自定义角色中的用户访问管理员级别功能

将管理员角色授予用户

属于“管理员”角色的一些管理功能是该特定标签特有的功能。当您在 Splunk Web 或 authorize.conf 中配置角色时，这些功能不会从管理员角色中自动继承。

例如，假设您要创建一个自定义角色，该角色继承所有“管理员”功能但对您的搜索任务具有有限访问权限。为此，可以创建名为 "SpecialAdmin" 的新角色，并按关于使用功能定义角色中所述将其设置为继承管理员的所有功能，然后按关于配置基于角色的用户访问权限所述设置搜索限制。

限制对特定应用的访问

local.meta 文件也可用来限制访问权限。

例如，假设您要允许用户只访问一个仪表板视图。要达到此目的，可以为此视图创建一个应用，然后将用户的角色分配给此应用。您应使用 meta.local 允许角色查看此应用。

如何通过 local.meta 文件添加和删除访问权限

通过编辑 local.meta 文件在您需要的位置添加新角色可以授予或限制访问权限。

1. 找到 local.meta 文件。如果您正在编辑主搜索页面（如管理器控件）的访问权限，请查看 $SPLUNK_HOME/etc/system/metadata/。如果想要编辑特定应用的访问权限，则查看 $SPLUNK_HOME/etc/apps/<app_name>/metadata/。如果所需位置的目录未包含该文件，则您可以复制默认版本 default.meta 并对其进行重命名。

注意：请**不要**直接编辑 default.meta 文件，因为您在未来可能需要用到该文件中的默认值。

2.在 `local.meta` 文件中，将新角色的名称添加至与所需访问权限相对应的段落。

默认段落	用途
`[manager/accesscontrols]` `access = read : [ * ], write : [ admin, power ]`	允许所有用户根据所处的目录读取此应用的内容，或访问“Splunk 管理器”页面中的功能。除非由其他元数据所覆盖，只允许管理员和高级用户将对象共享到此应用。
`[views] [manager/accesscontrols]` `access = read : [ * ], write : [ admin ]`	决定管理器页面访问权限的访问控制。

3.完成所有更改后，重新启动 Splunk Enterprise。

示例

示例 1：名为 "usermanager" 的新角色只继承用户的功能，不继承搜索或索引。目的是使创建的角色没有数据访问权限，仅用于创建和管理用户帐户。

要创建此角色，您应编辑以下段落：

```
[manager/accesscontrols]
access = read : [ admin ], write : [ admin ]
```

包括以下内容：

```
[manager/accesscontrols]
access = read : [ admin, usermanager ], write : [ admin, usermanager ]
```

您刚刚为 "usermanager" 提供了查看和编辑管理器中“访问控制”页面内容的能力。

示例 2：要允许 "userview" 角色访问页面但不能编辑，只将角色添加到读取值即可：

```
[manager/accesscontrols]
access = read : [ admin, userview, usermanager ], write : [ admin, usermanager ]
```

您还可以使用通配符向“每个”角色授予读取管理器页面的访问权限：

```
[manager/accesscontrols]
access = read : [ * ], write : [ admin ]
```

示例 3：您要拥有只能读取您指定的销售数据的部分用户。要达到此目的，可以为仪表板创建一个应用，然后创建新角色 "salesusers"。

然后您可以在应用目录的 `local.meta` 文件中编辑以下段落（记得您可以从 `default.meta` 文件中创建一个）：

```
[viewstates]
access = read : [ * ], write : [ * ]

to read:

[viewstates]
access = read : [ salesusers ], write : [ admin ]
```

查找现有用户和角色

要在 Splunk Web 中查找现有用户或角色：

1.在主菜单中，单击**系统** > **访问控制**。

2.单击**用户**或**角色**，选择您要搜索的实体。

2.默认情况下，搜索指定字符串的所有字段。要搜索特定字段，请指定字段的名称。请注意，Splunk 搜索支持通配符。例如：

- 如需仅搜索电子邮件地址：

"email=<*电子邮件地址或地址片段*>:

- 如需仅搜索“全名”字段：

"realname=<*姓名或姓名片段*>.

- 如需仅搜索给定角色中的用户：

"roles="。

删除所有用户帐户

键入 `./splunk clean`，然后键入 `userdata` 参数，可以从 Splunk 安装中移除所有用户数据（用户帐户）。这会删除除默认用户帐户（管理员、高级用户、普通用户）以外的所有用户帐户。

警告：删除用户数据是不可撤消的操作；如果您意外删除了用户数据，则必须手动重新添加帐户。

删除系统中的所有用户帐户：

```
./splunk clean userdata
```

要删除系统中的用户帐户，并跳过确认提示：

```
./splunk clean userdata -f
```

Splunk 知识对象的安全访问

您使用 Splunk Enterprise 时，创建各种**知识对象**，例如，**事件类型、标记、查找、字段提取、工作流动作**和**保存的搜索**。利用 Splunk Web 可以限制和扩展对 Splunk 实现中知识对象的访问权限。您可以使用它来达到下述目的：

- 使对象可供所有应用的用户使用。
- 使对象可供特定应用的用户使用。
- 通过用户角色限制对象访问权限。
- 禁用或删除对象。
- 允许用户共享或删除他们未拥有的对象。

有关确保知识对象安全的更多信息，请参阅《知识管理器手册》中的“管理知识对象权限”和“禁用或删除知识对象”。

使用访问控制列表

要帮助确保 Splunk 配置的安全，使用 Splunk Enterprise 访问控制列表 (ACL) 限制可访问各个网络部分的 IP 地址。

要配置 ACL，请编辑 `server.conf` 和 `inputs.conf` 以指定不同的通信接受或拒绝的 IP 地址。

如何设置 ACL

用逗号或空格分隔各地址。可以使用下列格式提供地址：

- 单个 IPv4 或 IPv6 地址。例如：`10.1.2.3, fe80::4a3`。
- CIDR 地址块。例如：`10/8, fe80:1234/32`。
- DNS 名称，可能使用 * 作为通配符，例如：`myhost.example.com, *.splunk.com`。
- 匹配任何内容（这是默认值）的单个 `*`。

要添加希望包含的地址，使用如下所述的格式之一添加相应地址。要排除某个地址，应在该地址前面添加 '!' 前缀。

按顺序应用规则，并使用第一个匹配项。例如，`!10.1/16, *` 将允许来自除 10.1.*.* 网络以外其他任何地方的连接。

设置 ACL 的位置

您可以通过编辑 `[Accept from]` 值确保以下链接的 IP 地址的安全：

- 要指示节点只接受从带有特定 IP 的其他节点中复制的数据，请编辑 `httpServer` 段落（位于 `server.conf`）。如果设置此属性，必须确保包括群集中所有其他对等节点的 IP 地址。有关群集的更多信息，请参阅“关于群集和索引复制”。有关编辑 server.conf 的更多信息，请参阅 server.conf。
- 要限制对特定 IP 地址的 TCP 通信，请编辑 `tcp` 段落（位于 `inputs.conf`）。请谨慎操作，因为如有信息冲突，这将覆盖 `server.conf` 中的输出值。
- 要限制使用 SSL 对特定 IP 地址的 TCP 通信，请编辑 `tcp-ssl` 段落（位于 `inputs.conf`）。
- 要限制索引器只接受来自带有特定 IP 地址的转发器的数据，请编辑 `splunktcp` 段落（位于 `inputs.conf`）。这可防止某人欺骗您的转发器，进而可能破坏您的数据。
- 如果索引器通信的转发器通过 SSL 确保安全，则编辑 `splunktcp-ssl` 段落（位于 `inputs.conf`）以限制索引器只

接受来自带有特定 IP 地址转发器的数据。

- 要限制对特定 IP 地址的 UDP 通信，请编辑 `UDP` 段落（位于 `inputs.conf`）。

有关编辑 `inputs.conf` 的更多信息，请参阅 inputs.conf

Splunk Enterprise 本机验证

设置 Splunk 验证

通过 Splunk **验证**可轻松地在系统中设置用户。Splunk 验证总是优先于任何外部验证系统。以下是验证用户的顺序：

1.Splunk 验证。

2.LDAP 或脚本式验证（如启用）。有关更多信息，请参阅"设置使用 LDAP 进行的用户验证"和"设置使用外部系统进行的用户验证"。

注意：不能同时使用 LDAP 和脚本式验证。

您可以通过以下两种方法使用基于角色的访问控制系统创建新用户，并将这些用户分配给**角色**：

- 使用 Splunk Web 创建用户和分配角色。有关更多信息，请参阅"使用 Splunk Web 配置用户"。
- 使用 CLI 创建用户，然后使用 Splunk Web 将它们分配给角色。有关更多信息，请参阅"使用 CLI 配置用户"。

创建用户和角色时的重要命名指导原则

在本机验证中存储的用户名不得包含空格、冒号或正斜线。名称不区分大小写，例如："Jacque"、"jacque"、"JacQue" 对 Splunk 验证来说都相同。

角色名称只能使用小写字符，不得包含空格、冒号或正斜线。

使用 Splunk Web 配置用户

在 Splunk Web 中配置用户和角色：

1. 导航至**设置 > 用户和验证 > 访问控制**。
2. 单击**用户**。
3. 单击**新建**，或选择现有用户来编辑。
4. 指定或更改用户的信息。您可以指定用户的：
    - 全名。
    - 电子邮件地址。
    - 时区。这允许用户按他们自己的时区查看事件和其他信息。
    - 默认应用。这会覆盖从用户角色继承的默认应用。
    - 密码。
5. 将用户分配给现有的一个或多个角色，然后单击**保存**。

您还可以专为某个用户创建一个角色，准确地定义该用户对 Splunk Enterprise 具有哪些访问权限。然后，可以将用户分配给此角色。有关角色的信息，请参阅"关于基于角色的用户访问权限"。

有关管理用户设置的信息，请参阅 Splunk Enterprise 管理指南。

使用 CLI 配置用户

在 CLI 中使用 `add user` 命令。以下是一些示例：

- 添加密码为 "changeme2" 的新管理员用户：

```
./splunk add user admin2 -password changeme2 -role admin -auth admin:changeme
```

- 将现有用户的密码更改为 "fflanda"：

```
./splunk edit user admin -password fflanda -role admin -auth admin:changeme
```

重要提示：如果密码包含会被 shell 解释为其他含义的特殊字符（例如 '$' 或 '!'），则必须使用转义符或单引号。例如：

```
./splunk edit user admin -password 'fflanda$' -role admin -auth admin:changeme
```

或

./splunk edit user admin -password fflanda\$ -role admin -auth admin:changeme

通过 Splunk Web 将用户添加到角色

您可以将用户添加到默认角色或您自己创建的自定义角色。有关更多信息，请参阅"关于基于角色的用户访问权限"。

通过 Splunk Web 将一个或多个用户添加到角色：

1. 单击主菜单中的**设置 > 访问控制 > 访问控制**。

2. 单击**用户**。

3. 编辑现有用户或创建新用户。

4. 从**角色**列表中选择要映射到哪个角色。此处将列出您在 `authorize.conf` 中创建的任何自定义角色。

使用 LDAP 进行验证

设置使用 LDAP 进行的用户验证

Splunk Enterprise 支持三种类型的**验证**系统：

- Splunk 验证，如"设置使用 Splunk 的内置系统进行的用户验证"所述。
- LDAP，如您正在阅读的主题所述。
- 通过外部验证系统进行脚本式验证 API，例如，PAM 或 RADIUS，如"设置使用外部系统进行的用户验证"所述。

关于为 Splunk Enterprise 配置 LDAP 验证

Splunk Enterprise 允许为 LDAP 用户和组进行用户和角色配置。您可以配置一个或多个 LDAP 服务器，并将用户和用户组从您的服务器映射到 Splunk 角色。

有关配置多个 LDAP 服务器的更多信息，请参阅"Splunk 如何使用多个 LDAP 服务器"。

在配置 LDAP 之前，请参阅"LDAP 必备条件和注意事项"。

如何配置 LDAP 验证

以下是配置 Splunk Enterprise 以使用 LDAP 的主要步骤：

1. 配置一个或多个 LDAP 策略（通常，为每个 LDAP 服务器配置一个策略）。

2. 将 LDAP 组映射到一个或多个 Splunk 角色。

3. 如果您有多个 LDAP 服务器，指定这些服务器的连接顺序。

您在 Splunk Web 或通过编辑配置文件，可以执行这些步骤。有关更多信息，请参阅"使用 Splunk Web 配置 LDAP"或"使用配置文件配置 LDAP"。

验证优先顺序

Splunk 验证优先于任何外部系统。以下是 Splunk Enterprise 验证用户的顺序：

1. Splunk 验证

2. LDAP 或脚本式验证（如已启用其中一种方法）。有关脚本式验证的更多信息，请参阅"设置使用外部系统进行的用户验证"。

问答

有什么问题吗？请访问 Splunk Answers，查看在 Splunk 社区中围绕 Splunk 的 LDAP 验证有哪些问题和解答。

使用 LDAP 管理 Splunk 用户角色

要配置 Splunk Enterprise 使用 LDAP 验证，首先为每个 LDAP 服务器创建一个 Splunk 策略，然后将 Splunk 角色映射到该服务器的组。用户尝试登录时，Splunk Enterprise 会查询服务器找到该用户。它基于与用户所属 LDAP 组相关的角色，授予用户权限。

更改用户的权限时，您有几个选项：

- 要更改一组用户的权限，可以将 LDAP 组重新映射到不同的 Splunk 角色。您还可以更新角色本身，以为角色

指定一组不同的权限。此操作在 Splunk Enterprise 上执行。
- 要更改单个用户的权限，您可以将该用户移动到映射到不同的 Splunk 角色的 LDAP 组。此操作在 LDAP 服务器上执行。

以下是一些其他用户管理活动：

- 将用户添加到 Splunk 角色：首先，在 Splunk Web 上，确保您已经将 Splunk 角色映射到 LDAP 组。然后，在 LDAP 服务器上，将用户添加到此 LDAP 组。
- 从 Splunk 角色删除用户：在 LDAP 服务器上，从相应的 LDAP 组删除用户。

一个用户可以具有多个角色的成员资格。在这种情况下，用户对这些角色的所有可用功能具有访问权限。如果用户是 docs 和 eng 组的成员，并且 docs 映射到“用户”，eng 映射到“管理员”，则用户会获取分配到“用户”或“管理员”角色的所有权限。

注意：当用户尝试登录时，Splunk Enterprise 会检查 LDAP 成员信息。在添加或删除用户时，无需重新加载验证配置。

LDAP 必备条件和注意事项

在使用 Splunk 为验证配置 LDAP 之前，请按本主题中的说明进行准备。

确定用户和组基本 DN

在将 LDAP 设置映射到 Splunk 设置之前，确定您的用户和组基本 DN（可分辨名称）。DN 是目录中存储验证信息的位置。

如果用户的组成员信息保留在单独的条目中，请输入单独的 DN（识别为目录中存储组信息的子树）。在此 DN 下方的所有子节点上递归搜索用户和组。如果您的 LDAP 树没有组条目，则可以将组基本 DN 设置为与用户基本 DN 相同，以将用户视为其自己的组。这需要进一步配置，稍后介绍。

如果您无法获取此信息，请联系 LDAP 管理员寻求帮助。

注意：为了在将 Splunk Enterprise 与 Active Directory 集成在一起时获得最佳结果，请将组基本 DN 放在用户基本 DN 以外的单独层次结构中。

其他注意事项

配置 Splunk Enterprise 使用 LDAP 时，请注意以下事项：

- Splunk Web 和 `authentication.conf` 中的条目区分大小写。
- 通过 Splunk 本机验证本地创建的任何用户都优先于同名的 LDAP 用户。例如，如果 LDAP 服务器具有用户名属性为“管理员”（例如，cn 或 uid）的用户，并存在同名的默认 Splunk 用户，则 Splunk 用户将优先。只接受本地密码，在登录时，映射到本地用户的角色将生效。
- Splunk Web 可以为映射到角色显示的 LDAP 组的数目限制为 LDAP 服务器可以通过查询返回的数目。您可以使用**搜索请求大小限制**和**搜索请求时间限制**设置来配置此项。
  - 如要阻止 Splunk 列出不必要的组，请使用 `groupBaseFilter`。例如：`groupBaseFilter = (|(cn=SplunkAdmins)(cn=SplunkPowerUsers)(cn=Help Desk))`
  - 如果您要映射的角色必须超过组的最大数量，则可以直接编辑 `authentication.conf`。在本示例中，"roleMap_AD" 指定 Splunk 策略的名称。每个属性/值对将一个 Splunk 角色映射到一个或多个 LDAP 组：

```
[roleMap_AD]
admin = SplunkAdmins1;SplunkAdmins2
power = SplunkPowerUsers
user = SplunkUsers
```

- Splunk 始终使用 LDAP 协议版本 3（也称为 v3）。

使用 TLS 证书确保 LDAP 安全

Splunk 使用 OpenLDAP 和 OpenSSL。您可以利用这两种工具来使用证书确保 LDAP 验证安全。有关创建和管理证书的更多信息，请参阅 OpenSSL 文档

以下示例为 LDAP 的证书配置。有关在 LDAP 中配置证书的方法的详细信息，请参阅 OpenLDAP 文档，网址为：http://www.openldap.org/doc/admin24/tls.html:

LDAP 服务器配置

```
TLSCACertificateFile <filename>: the PEM-format file containing certificates for the CA's that slapd will trust,
including the certificate for the CA that signed the server certificate. Multiple certificates can be appended to
```

the file in no particular order.

TLSCertificateKeyFile <filename></code>: the file that contains the private key that matches the certificate stored in the
TLSCertificateFile file.

TLSCipherSuite <cipher-suite-spec>: ciphers will be accepted and the preference order. <cipher-suite-spec> should be a cipher specification for OpenSSL. Use "openssl ciphers -v ALL" for a list of available cipher specifications.

TLSRandFile <filename>: the file to obtain random bits from when /dev/urandom is not available. If the system provides /dev/urandom then this option is not needed, otherwise a source of random data must be configured.

TLSEphemeralDHParamFile <filename>: the file that contains parameters for Diffie-Hellman ephemeral key exchange.

TLSVerifyClient { never | allow | try | demand }: specifies what checks to perform on client certificates in an incoming TLS session, if any. This option is set to never by default, in which case the server never asks the client for a certificate.

LDAP 客户端配置

此指令指定包含客户端证书的文件。这是一个仅用户指令，只能在用户的 .ldaprc 文件中指定。

TLS_KEY <filename> specifies the file that contains the private key that matches the certificate stored in the TLS_CERT file. The same constraints mentioned for TLSCertificateKeyFile apply here. This is also a user-only directive.

TLS_RANDFILE <filename> the same as the server's TLSRandFile option.

TLS_REQCERT { never | allow | try | demand }

请注意，由于每个客户端都必须配置为使用每个证书，因此如果托管两个或两个以上的 LDAP 服务器，则您可能不想使用自签名证书。在这种情况下，创建证书授权来签署服务器证书会更容易。

Splunk Enterprise 如何使用多个 LDAP 服务器

Splunk Enterprise 在验证用户时可以对多个 LDAP 服务器执行搜索。要配置多个 LDAP 服务器，可以设置多个 LDAP“策略”，每个 LDAP 服务器对应一个策略。

创建策略后，即可指定在搜索 LDAP 用户时希望 Splunk 查询这些策略的顺序。如果未指定搜索顺序，则 Splunk Enterprise 基于创建策略的顺序分配默认的“连接顺序”。

有关 LDAP 策略配置步骤的更多信息，请参阅“使用 Splunk Web 配置 LDAP”或“使用配置文件配置 LDAP”获取更多信息。

在搜索期间连接顺序如何工作

在验证期间，Splunk Enterprise 按指定的连接顺序基于为服务器创建的策略进行搜索。Splunk Enterprise 在服务器上找到用户后，就会退出搜索，并采用这些凭据。如果用户在稍后按搜索顺序找到的服务器上也有凭据时，则会忽略这些凭据。

例如，假定您按以下顺序配置和启用三个策略：A、B、C。Splunk Enterprise 将按同一顺序搜索其服务器：A、B、C。如果它在 A 上找到用户，则会停止查找。用户是否也存在于 B 和 C 上并不重要；Splunk Enterprise 将只为该用户使用 A 凭据。如果 Splunk 未在 A 上找到用户，则它将继续搜索剩余的服务器：首先搜索 B，然后搜索 C。

如果您以后禁用策略 A，则 Splunk Enterprise 将按以下顺序搜索剩余的策略：B，C。

您可以根据 Authentication.conf 规范文件中的说明随时编辑 Splunk Web 的策略属性或更改 `authSettings` 属性中的策略顺序来更改连接顺序。有关编辑用于 LDAP 的该文件的更多信息，请参阅编辑 authentication.conf。

重要提示：通过 Splunk 验证本地创建的任何用户都优先于同名的 LDAP 用户。有关详细信息，请参阅“关于用户验证”。

使用 Splunk Web 配置 LDAP

本部分介绍了如何通过 Splunk Web 配置 LDAP。如果想要直接通过编辑 `authentication.conf` 配置 LDAP，请参阅“使用配置文件配置 LDAP”。

使用 Splunk Web 配置 LDAP 有三个主要步骤：

1.创建 LDAP 策略。

2.将 LDAP 组映射到 Splunk 角色。

3.指定连接顺序（仅适用于多个 LDAP 服务器）

创建 LDAP 策略

创建 LDAP 策略：

1.单击**设置 > 用户和验证 > 访问控制**。

2.单击**验证方法**。

3.选中 **LDAP**。

4.单击**将 Splunk 配置为使用 LDAP 和映射组**。这将带您前往 **LDAP 策略**页面。

5.单击**新建**。这将带您前往**新增**页面。

6.为您的配置输入 **LDAP 策略名称**。

7.输入 LDAP 服务器的**主机**名称。确保 Splunk 服务器可以解析主机名称。**注意：此时，不支持 Windows 的 IPv6 地址格式。**

8.输入 Splunk Enterprise 连接到 LDAP 服务器时应使用的**端口**。

- 默认情况下，LDAP 服务器侦听 TCP 端口 389。
- LDAPS（具有 SSL 的 LDAP）默认为端口 636。

9.要打开 SSL，选中**已启用 SSL**。

- 为安全起见，建议进行此设置。
- 您还必须在 LDAP 服务器上启用 SSL。

10.输入**绑定 DN**。

- 这是用于绑定到 LDAP 服务器的可区分的名称。
- 这通常（但不一定）是管理员。该用户需要具有您要检索的所有 LDAP 用户和组条目的读取权限。
- 匿名绑定即可时，保留为空白。

11.为绑定用户输入并确认**绑定 DN 密码**。

12.指定**用户基本 DN**。可以用分号分隔来指定多个用户基本 DN 条目。

- Splunk Enterprise 使用此属性找到用户信息。
- 您必须设置此属性验证才能生效。

13.为筛选用户要依据的对象类别，输入**用户基本过滤器**。

- 建议输入该值的目的是仅返回适用的用户。例如：(department=IT)。
- 默认值为空白，表示无用户条目过滤。

14.输入包含用户名的**用户名属性**。

- 用户名属性不得包含空格。
- 在 Active Directory 中，这是典型的 `sAMAccountName`，但您还可以在其他属性，如 `cn` 中进行验证。
- 数值 `uid` 应该适用于其他大多数配置。

15.输入用户的**真实姓名属性**（常用名）。

- 典型值为 `displayName` 或 `cn`（通用名称）。

16.输入**电子邮件属性**。

17.输入**组映射属性**。

- 这是组条目定义其成员所使用的用户属性。
- 对于活跃的目录来说，默认为 `dn`；只有使用除用户 DN 以外的其他属性来映射组时才能设置此属性。
- 例如，用于将用户映射到组的典型属性为 `dn`。

18.输入**组基本 DN**。可以用分号分隔来指定多个组基本 DN 条目。

- 这是用户组在 LDAP 中的位置。
- 如果 LDAP 环境没有组条目，则可以将每个用户视为其自己的组：
  - 将 groupBaseDN 设置为与 userBaseDN 相同的值。这表示您将在与用户相同的位置中搜索组。
  - 接下来，将 groupMemberAttribute 和 groupMappingAttribute 设置为与 userNameAttribute 相同的属性。这表示条目（被视为组时）将用户名值用作其唯一的成员。

    - 为简明起见，您或许还应该将 groupNameAttribute 设置为与 userNameAttribute 相同的值。

注意：为了在集成 Active Directory 时获得最佳结果，请将组基本 DN 放在用户基本 DN 以外的单独层次结构中。

19.为您要筛选静态组所依据的对象类别，输入**静态组搜索过滤器**。

- 建议输入该值的目的是仅返回适用的用户组。例如：`(|(objectclass=groupofNames)(objectclass=groupofUniqueNames))`
- 默认值为空白，表示无静态组条目筛选。

20.输入**组名称属性**。

- 该组条目属性的值存储组名称。
- 这通常是 `cn`。

21.输入**静态成员属性**。

- 该组属性的值为组成员。
- 这通常是 `member`、`uniqueMember` 或 `memberUid`。

22.要扩展嵌套组，选中**嵌套组**。

- 这会控制 Splunk Enterprise 是否将使用 'memberof' 属性扩展嵌套组。只有在您具有利用 'memberof' 属性来解析其成员的嵌套组时，才选中此项。在 OpenLDAP 上，需要明确启用 'memberof' 叠加。

23.输入**动态组搜索过滤器**以检索动态组（如果有）。

- 此项必须与您的动态组定义的对象类别匹配，以确保这些组返回到 Splunk。例如：`(objectclass=groupOfURLs)`
- 默认值为空白，表示 Splunk Enterprise 在验证和授权期间不查找动态组条目。

24.输入**动态成员属性**。

- 这种组属性一般使用 LDAP 搜索 URL（比如 `ldap:///o=Acme, c=US??sub?(objectclass=person)`）的格式来定义其成员。
- 这通常是 `memberURL`。

25.如果选中**高级设置**，还会显示可以设置的多个其他选项：

- **启用只有匿名绑定的参照**。
    - 默认情况下，此设置处于打开状态。如果您不需要参照，请关闭此项。
    - Splunk 可以查找只有匿名绑定的参照。您还必须在 LDAP 服务器上启用匿名搜索。
    - 如果您看到较长的 LDAP 搜索超时（可能位于 Active Directory）和 ScopedLDAPConnection 的 `splunkd.log` 中的“操作错误”(Operations error)，则这些问题可能与参照相关。
- **搜索请求大小限制**
    - 为避免与性能相关的问题，可以设置搜索请求大小限制。然后，在响应搜索请求时，Splunk Enterprise 将请求 LDAP 服务器返回指定的最大条目数。在具有数百万用户的大规模部署中，根据 LDAP 策略配置中的搜索过滤器设置的不同，将此限制设置为高值可能导致响应时间较长。如果达到此限制，则 `splunkd.log` 应该包含一条 `size limit exceeded` 消息。
    - 您应当根据“配置用户会话超时”中的说明设置**搜索请求时间限制**和**搜索请求大小限制**值（与 `splunkweb` 超时属性结合使用）。如果您有在 Splunk 控制台中未显示的组，则由于以下限制之一可能已将其排除。根据需要调整这些属性。
    - 如要将请求大小限制设置为超过 1000，则必须同时编辑 `max_users_to_precache`（位于 `limits.conf`）以容纳为请求大小限制设置的用户数量。
- **搜索请求时间限制**
    - 为避免与性能相关的问题，可以设置搜索请求时间限制。然后，Splunk Enterprise 将请求 LDAP 服务器在指定的秒数内完成其搜索。在具有数百万用户的大规模部署中，将此限制设置为高值可能导致 Splunk Web 超时。如果达到此限制，则 `splunkd.log` 应该包含一条 `time limit exceeded` 消息。
    - 您应当根据“配置用户会话超时”中的说明设置**搜索请求时间限制**和**搜索请求大小限制**值（与 `splunkweb` 超时属性结合使用）。如果您有在 Splunk 控制台中未显示的组，则由于以下限制之一可能已将其排除。根据需要调整这些属性。
- **网络套接字超时**
    - 由于网络拥挤多个策略配置中的一个 LDAP 服务器无法访问，或者响应时间过长时，此属性用于断开验证链中的循环。在等待指定的秒数之后，验证进程将继续下一个可用的策略（如果有）。
    - 在先创建 LDAP 策略时，Splunk Enterprise 会验证 LDAP 服务器/端口和其他参数。如果 LDAP 服务器发生故障，或者在此时无法验证其中的一个参数，则不能创建 LDAP 策略。

26.单击**保存**。

将新的 LDAP 组映射到 Splunk 角色

在已将 Splunk Enterprise 配置为通过 LDAP 服务器验证后，将 LDAP 组映射到 Splunk 角色。如果您未使用组，则可以单独映射用户。

注意：您可以映射用户或组，但不能同时映射两者。如果您使用的是组，所有用户都必须是相应组的成员。组从它们所属的最高级别角色继承功能。

所有用户都显示在 Splunk 管理器的**用户**页面中。若要在 Splunk Web 中将角色分配给组：

1. 从主菜单中选择**系统 > 用户和验证 > 访问控制**。
2. 在**访问控制**页面中，单击**验证方法**。
3. 选择 **LDAP** 单选按钮，然后单击**将 Splunk 配置为使用 LDAP 和映射组**。这将带您前往 **LDAP 策略**页面。
4. 单击特定策略的“操作”列中的**映射组**。这将带您前往 **LDAP 组**页面。您可以使用页面右上角的搜索字段来满足组列表的条件；例如，搜索包含特定用户的组。
5. 单击组名称。这将带您前往映射页面，其中包括可用角色的列表，以及该组的 LDAP 用户的列表。
6. 要将角色映射到组，单击“可用角色”列表中的某个角色左侧的箭头。这会将组移动到“所选的角色”列表。可以将多个角色映射到组。
7. 单击**保存**。这将您带回 **LDAP 组**页面。
8. 针对您希望将 Splunk 角色分配到的每个组重复此过程。

指定服务器连接顺序

如果您启用了多个 LDAP 策略，则可以指定 Splunk Enterprise 搜索其服务器来查找用户的顺序，如“Splunk 如何使用多个 LDAP 服务器”中所述。

默认情况下，Splunk Enterprise 按启用服务器的顺序对其进行搜索。要更改连接（搜索）顺序，需要单独编辑每个策略的属性：

1. 从主菜单中选择**系统 > 用户和验证 > 访问控制**。
2. 单击**验证方法**。
3. 选中 **LDAP** 单选按钮。
4. 单击**将 Splunk 配置为使用 LDAP 和映射组**。这将带您前往 **LDAP 策略**页面。
5. 单击您要指定其连接顺序的策略。这将带您前往该策略的属性页面。
6. 编辑页面顶部的**连接顺序**字段。只有在启用多个策略时才显示此字段。

注意：最初创建策略时，不显示**连接顺序**字段。只有以后编辑其属性时才显示此字段。另外，如果策略已被禁用，则该字段将显示为灰色。

7. 单击**保存**。
8. 针对您要更改连接顺序的任何其他已启用策略，请重复此过程。

在 Splunk Web 中将 LDAP 组映射到 Splunk 角色

如果已将 Splunk Enterprise 配置为通过 LDAP 服务器验证，可以将 LDAP 组映射到 Splunk 角色。如果您未使用组，则也可以单独映射各个 LDAP 用户。

有关在 Splunk Web 中设置 LDAP 组的信息，请参阅本手册的“使用 Splunk Web 配置 LDAP”。

注意：您可以映射用户或组，但不能同时映射两者。如果您使用的是组，您希望访问 Splunk Enterprise 的所有用户都必须是相应组的成员。组从它们所属的最高级别角色继承功能。

所有用户都显示在 Splunk 管理器的**用户**页面中。若要在 Splunk Web 中将角色分配给组：

1. 单击 Splunk Web 中的**设置**。
2. 在**用户和验证**部分中，单击**访问控制**。
3. 单击**验证方法**。
4. 选中 **LDAP** 单选按钮。
5. 单击**将 Splunk 配置为使用 LDAP 和映射组**。这将带您前往 **LDAP 策略**页面。
6. 单击特定策略的“操作”列中的**映射组**。这将带您前往 **LDAP 组**页面。您可以使用页面右上角的搜索字段来满足组列表的条件；例如，搜索包含特定用户的组。
7. 单击组名称。这将带您前往映射页面，其中包括可用角色的列表，以及该组的 LDAP 用户的列表。

8. 要将角色映射到组，单击“可用角色”列表中的某个角色左侧的箭头。这会将组移动到“所选的角色”列表。可以将多个角色映射到组。

9. 单击**保存**。这将您带回 **LDAP 组**页面。

10. 针对您希望将 Splunk 角色分配到的每个组重复此过程。

使用配置文件配置 LDAP

使用 Splunk Web 配置 LDAP 时，还可以直接编辑 authentication.conf 文件。

在接下来的案例中，将带您浏览设置 `authentication.conf` 的过程。如果您倾向于使用 Splunk Web 配置 LDAP，请参阅使用 Splunk Web 配置 LDAP。

注意：如果您配置 LDAP 验证并稍后确定返回以使用默认 Splunk 验证，则最简便的方法是将现有的 `authentication.conf` 文件移除（比如通过将其重命名为 `authentication.conf.disabled`）并重新启动 Splunk Enterprise。

您可以在 authentication.conf 规范文件的末尾看到更多示例。

编辑 `authentication.conf`（位于 `$SPLUNK_HOME/etc/system/local/`）。有关配置文件的一般信息，请参阅*《管理员手册》*中的“关于配置文件”。

设置验证类型和策略名称

默认情况下，Splunk Enterprise 使用 Splunk 验证。在 `[authentication]` 段落中将类型更改为 LDAP：

```
[authentication]
authType = LDAP
authSettings = ldaphost1,ldaphost2
```

请注意以下事项：

- 通过设置 `authType = LDAP` 打开 LDAP。
- `authSettings` 属性确定一个或多个 LDAP 策略。每个策略都有自己的段落。

配置 LDAP 策略段落

每个 LDAP 策略都需要自己的段落。将 LDAP 值映射到策略段落中的属性/值对。

注意：Splunk Enterprise 对 Windows 不支持 IPv6 地址格式。

以下是之前在 `authSettings` 属性中指定的 "ldaphost1" 策略的示例段落：

```
[ldaphost1]
host = ldaphost1.domain.com
port = 389
SSLEnabled = 0
bindDN = cn=bind_user
bindDNpassword = bind_user_password
groupBaseDN = ou=Groups,dc=splunk,dc=com
groupBaseFilter = (objectclass=*)
groupMappingAttribute = dn
groupMemberAttribute = uniqueMember
groupNameAttribute = cn
realNameAttribute = displayName
userBaseDN = ou=People,dc=splunk,dc=com
userBaseFilter = (objectclass=*)
userNameAttribute = uid
```

注意：为了在集成 Active Directory 时获得最佳结果，请将组基本 DN 放在用户基本 DN 以外的单独层次结构中。

SSL

如果您为 LDAP 策略启用了 SSL，请确保 `ldap.conf` 中存在以下最低设置。

```
TLS_REQCERT= demand
TLS_CACERT= <path to cert, for example: /opt/splunk/etc/auth/LDAProotcert.crt>
TLS_CIPHER_SUITE= <your cipher suite>
```

配置多个 LDAP 策略

Splunk Enterprise 可以跨多个 LDAP 服务器搜索，如 Splunk 如何使用多个 LDAP 服务器中所述。如要将其配置，请根据想要 Splunk Enterprise 查询策略的顺序，设置 `authSettings` 属性为逗号分隔的所有策略的列表。然后，为每个策略指定单独的段落。

将组映射到角色

要映射 Splunk 角色至策略的 LDAP 组，您需要为该策略设置 `roleMap` 段落。每个策略都需要自己的 `roleMap` 段落。本示例将映射 "ldaphost1" 策略中的各组的角色。语法为 <Splunk RoleName> = <LDAP group string>：

```
[roleMap_ldaphost1]
admin = SplunkAdmins
itusers = ITAdmins
```

将用户直接映射到角色

如果您需要将用户直接映射到 Splunk 角色，则可以通过设置 `groupBaseDN` 为 `userBaseDN` 的值来完成。同样，设置 `groupMappingAttribute`、`groupMemberAttribute` 和 `groupNameAttribute` 的属性，以与 `userNameAttribute` 的属性相同。例如：

```
[supportLDAP]
SSLEnabled = 0
bindDN = cn=Directory Manager
bindDNpassword = #########
groupBaseDN = ou=People,dc=splunksupport,dc=com
groupBaseFilter = (objectclass=*)
groupMappingAttribute = uid
groupMemberAttribute = uid
groupNameAttribute = uid
host = supportldap.splunksupport.com
port = 389
realNameAttribute = cn
userBaseDN = ou=People,dc=splunksupport,dc=com
userBaseFilter = (objectclass=*)
userNameAttribute = uid

[roleMap_supportLDAP]
admin = rlee;bsmith
```

在配置文件中将 LDAP 组和用户映射到 Splunk 角色

设置了 LDAP 验证和用户后，即可在 Splunk Web 中将 LDAP 组和用户映射到角色。要为 Splunk Enterprise 设置 LDAP，请参阅本手册的“使用配置文件配置 LDAP”。

将组映射到角色

要映射 Splunk 角色至策略的 LDAP 组，您需要为该策略设置 `roleMap` 段落。每个策略都需要自己的 `roleMap` 段落。本示例将映射 "ldaphost1" 策略中的各组的角色：

```
[roleMap_ldaphost1]
admin = SplunkAdmins
itusers = ITAdmins
```

将用户直接映射到角色

如果您需要将用户直接映射到 Splunk 角色，则可以通过设置 `groupBaseDN` 为 `userBaseDN` 的值来完成。同样，设置 `groupMappingAttribute`、`groupMemberAttribute` 和 `groupNameAttribute` 的属性，以与 `userNameAttribute` 的属性相同。例如：

```
[supportLDAP]
SSLEnabled = 0
bindDN = cn=Directory Manager
bindDNpassword = #########
groupBaseDN = ou=People,dc=splunksupport,dc=com
groupBaseFilter = (objectclass=*)
groupMappingAttribute = uid
```

```
groupMemberAttribute = uid
groupNameAttribute = uid
host = supportldap.splunksupport.com
port = 389
realNameAttribute = cn
userBaseDN = ou=People,dc=splunksupport,dc=com
userBaseFilter = (objectclass=*)
userNameAttribute = uid

[roleMap_supportLDAP]
admin = rlee;bsmith
```

测试 LDAP 配置

如果您发现 Splunk Enterprise 无法连接到 LDAP 服务器，请尝试以下故障排除步骤：

1.有关任何验证错误，请查看 `$SPLUNK_HOME/var/log/splunk/splunkd.log`。在此为 AuthenticationManagerLDAP 打开 DEBUG 级别日志，以获取更多信息。可以从 Splunk Web UI - 服务器设置/服务器日志完成。

2.删除您已经为 **userBaseFilter** 和 **groupBaseFilter** 添加的任何自定义值。

3.使用 `ldapsearch` 以确定您正在指定的变量将返回预期的条目：

ldapsearch -x -h <ldap_host> -p <ldap_port> -D "bind_dn" -w "bind_passwd" -b "user_basedn" "userNameAttribute=*"

ldapsearch -x -h <ldap_host> -p <ldap_port> -D "bind_dn" -w "bind_passwd" -b "group_basedn" "groupNameAttribute=*"

如果这些命令返回匹配条目，则后端 LDAP 系统配置正确。请继续解决 Splunk LDAP 策略配置的问题。

从 Splunk 验证转换为 LDAP

如果您从 Splunk 验证移至 LDAP，请注意 Splunk 帐户不会自动被禁用并且优先于 LDAP 帐户，这一点非常重要。

如果您已经从 Splunk 验证系统转换为 LDAP，您可能需要删除 Splunk 用户，以确保使用的是 LDAP 凭据。只有在两个系统中的用户名相同时上述操作才是必需的。

确保本地 Splunk 帐户的安全

如果已将 Splunk Enterprise 配置为使用 LDAP 验证，则请注意使用 Splunk 验证的所有本地帐户都仍然存在并处于活动状态（其中包括“管理员”帐户），这一点非常重要。您需要考虑此情况的安全隐患。

在启用 LDAP 验证时删除所有当前的本地帐户：

- 移动 `$SPLUNK_HOME/etc/passwd` 文件至 `passwd.bak`。
- 创建一个空白的 `$SPLUNK_HOME/etc/passwd` 文件。
- 重新启动 Splunk Enterprise。

记住，在 Splunk Enterprise 处于 LDAP 验证模式时仍然可以创建本地 Splunk 帐户。另外，必须保留以用于备份或灾难恢复的任何本地 Splunk 帐户都应使用非常强的密码。

使用 LDAP 时，请确保 LDAP 实现强制执行：

- 对长度和复杂性有高要求的强密码。
- 较低的错误尝试密码锁定阈值。

保存的搜索

如果 LDAP 用户名与您在内置系统中先前使用的名称（但随后已删除）相同，保存的搜索应可以正常工作，而无需转换。

如果您在系统使用 Splunk 验证时创建了现有保存的搜索，并且要将这些搜索转给其他名称的 LDAP 用户，请编辑元数据：

1.修改 `$SPLUNK_HOME/etc/apps/<app_name>/metadata/local.meta` 并将 `owner = <username>` 字段（在每个 `savedsearch` 权限段落下方）换成相应的 LDAP 用户名并保存更改。

2.重新启动 Splunk Enterprise 使更改生效。

删除 LDAP 用户的最佳做法

如果您从 LDAP 目录删除用户，Splunk Enterprise 不会自动删除对应的 Splunk 用户。通常，这样没有问题，但如果用户具有任何形式的全局权限，则 LDAP 可能产生错误。

有关在 Splunk Enterprise 中使用 LDAP 用户的更多信息，请参阅本手册的"设置使用 LDAP 进行的用户验证"。

执行以下步骤，安全地删除 Splunk 用户：

1. 首先，备份 `$HOME/splunk/etc/users/$userid` 文件夹。

2. 针对用户 ID 字符串在 `$HOME/splunk/etc/apps/` 下方搜索文件，以查看用户是否拥有具备全局权限的任何搜索或对象。

3. 针对用户拥有的任何搜索或对象，更改所有者。将其更改为管理员用户或维护帐户，或者您喜欢的任何用户。

4. 在搜索头上查看 `splunkd.log` 以确保没有更多的 LDAP 验证错误。

5. 一旦重定向任意对象所有权，您可以安全移除 `$HOME/splunk/etc/users/$userid` 文件夹。

多因子验证

有关使用双重安全的双因子验证

Splunk 当前支持用于登录到 Splunk 平台的双重安全双因子验证。

注意：如果先前已将 Splunk 配置为通过 https://duo.com/docs/splunk 使用双重验证，则先前的配置不再有效。您必须使用以下任务来通过双重安全重新配置双因子登录。

启用双重安全双因子验证后，用户：

1. 使用其登录凭据登录到常规 Splunk 主页。（这被称为主要登录。）

2. 遇到第二个"双重验证"页面。（这被称为辅助登录。）

3. 用户第一次登录时，他们按照双重安全登录页面上的说明设置其登录。他们选择他们首选的方法访问其辅助凭据，如下所示：

- 使用通过您智能手机上的推送通知发送的凭据登录（需要双重安全移动应用）。
- 使用通过短信发送到您手机上的凭据登录。
- 使用您手机所接到的电话中提供的凭据登录。
- 通过输入由双重安全移动应用生成的一次性代码进行登录。

4. 用户使用上述任意选项设置其辅助凭据传输方法后，其随后的辅助登录凭据按先前配置的方式发送。

双因子验证如何与其他形式的验证配合使用

请注意，您不能使用具有 SSO 或 SAML 验证的任何形式的多因子验证。具有多因子验证的 Splunk 适用于以下验证来源：

- Splunk 本机认证
- LDAP
- 脚本式验证

在 Splunk 中设置双重安全双因子验证

1. 在双重安全网站上为您的 Splunk 配置创建一个帐户。更多信息请参阅 https://duo.com。

2. 向 Splunk 提供来自您"双重安全帐户"的以下信息。有关更多信息，请参阅配置 Splunk 以使用双重安全双因子验证。

配置 Splunk 以使用双重安全双因子验证

注意：如果先前已将 Splunk 配置为通过 https://duo.com/docs/splunk 使用双重验证，则先前的配置不再有效。您必须使用以下任务来通过双重安全重新配置双因子登录。

要配置双重安全的双因子验证以使用 Splunk：

1. 使用双重安全网站为 Splunk 创建一个双重安全帐户。更多信息请参阅 https://duo.com。

2. 通过向 Splunk 提供以下信息，将 Splunk 配置为使用双重安全：

- 您的集成密钥（例如，DIXXXXXXXXXXXXXXXXXX）
- 您的密钥

- 您的 API 主机名称（例如，api-XXXXXXXX.duosecurity.com）

3.随后用户登录 Splunk，然后按照双重安全登录页面上的说明获取辅助登录凭据。

这些是双重安全配置页面上的前三个项目，也可以在**应用程序** > **详细信息**下的双重安全中找到。如果您还未配置您的双重安全凭据，请参阅 https://duo.com。

1.在**菜单**上，选择**设置** > **用户和验证** > **访问角色**。

2.单击**验证方法**。

3.在**多因子验证**下，选择**双重安全**。

4.单击**配置双重安全**链接。

5.提供双重安全配置中的**集成密钥**。您可以在您的双重安全配置页面或**配置** > **详细信息**下查找此密钥。

6.提供双重安全配置或详细信息中的**密钥**。您可以在您的双重配置页面或**配置** > **详细信息**下查找此密钥。

7.从您的双重配置中提供 **API 主机名称**。您可以在您的双重配置页面或**配置** > **详细信息**下查找此密钥。

8.确定双重安全不可用时的"验证"行为：

- **允许用户登录**即使双重验证（即辅助验证）失败，已成功登录 Splunk 主页的用户（即主要验证）也可以访问 Splunk。
- **不允许用户登录**如果双重验证（即辅助验证）失败，已成功登录 Splunk 主页的用户（即主要验证）不可以访问 Splunk。

9.提供在连接超时之前尝试多长时间的验证的时间限制（以秒为单位）。

10.保存更改。您不需要重新加载验证以使多因子验证生效。

11.一旦用户登录 Splunk，将显示双重登录页面，指示用户选择访问其辅助登录凭据的方法。

使用配置文件配置双重双因子验证

在 `authentication.conf` 中，编辑 `[2FA stanza name]` 段落，如下所示：

```
externalTwoFactorVendor = Duo(as of now)
externalTwoFactorSettings = <2FA stanza name>
integrationKey = <Integration Key as provided by Duo>
secretKey = <Secret Key as provided by Duo>
applicationKey =<Manually generated secret key> apiHostname = <API Hostname as provided by Duo>
failOpen = True|False (Default : False)
timeout = <in seconds>
```

使用具有 SAML 的单点登录进行验证

使用 SAML 配置单点登录

通过使用您受支持的身份提供程序 (IdP) 提供的信息，您可以配置 Splunk 软件使用单点登录 (SSO) 的 SAML 验证。

警告：在尝试在 Splunk Cloud 中配置 SSO 之前，请与 Splunk 支持人员联系并打开票据，请求他们针对 SSO 准备您的云部署。当他们配置您的部署后，将通知您并提供所需的证书。

前提条件

- 可以是：
  - Splunk 软件的运行版本,或
  - Splunk Cloud 受管理部署。Splunk Cloud 的自助部署通过 Splunk 客户门户登录，且无法独立配置 SAML SSO。
- 配置身份提供程序以提供 `role`、`realName` 和 `mail` 属性。受支持的身份提供程序为：
  - Ping Identity
  - Okta
  - Azure AD
  - AD FS
  - OneLogin
  - Optimal
  - CA siteminder
- 具有 `change_authentication` 功能的管理员角色。该权限级别允许您启用 SAML 并在 Splunk 搜索头上编辑验证设置。

1.配置 SAML SSO，使用：

- Ping Identity
- Okta
- Azure AD 或 AD FS
- OneLogin
- Optimal
- CA siteminder

2.将 SAML 组映射到 Splunk Enterprise 角色。

使用 PingIdentity 作为您的身份提供程序配置 SSO

如果您已将 PingIdentity 配置为身份提供程序 (IdP)，则此任务将介绍如何为 Splunk Enterprise 设置 SSO。有关将 PingIdentity 配置为 IdP 的信息，请参阅 Ping Federate 文档。

使用以下任务配置 Splunk 部署以识别和使用 PingIdentity 配置。然后，将 PingIdentity 用户组映射到 Splunk 用户角色，以便这些用户可以登录。

警告：在尝试在 Splunk Cloud 中配置 SSO 之前，请与 Splunk 支持人员联系并打开请求 SSO 的云部署的票据。支持人员将配置您的部署，并提供所需的证书。

前提条件

验证您的系统是否满足所有要求。参阅"使用 SAML 配置单点登录"。

1.在**设置**菜单中，选择**访问控制 > 验证方法**。

2.选择 **SAML** 作为您的验证类型。

3.单击**将 Splunk 配置为使用 SAML**。

4.在"SAML 组"页面，单击 **SAML 配置**。

5.浏览并选择元数据文件，或将元数据直接复制并粘贴到文本窗口中。如果您无法确定如何获取元数据文件，请参阅 IdP 文档。

6.在**常规设置**中，提供如下信息。

单点登录 URL。	此字段自动通过所选元数据文件填充。这是 Splunk 将向其发送验证请求的 IdP 上的受保护端点。如果您正在使用 Splunk Cloud，打开支持的提交问题以使 Splunk Cloud 运营小组打开端口，从而与 IdP 通信。 您的用户使用该 URL 进行 SSO 登录。如要在启用 SAML 后访问登录页面，请在整个登录 URL (`/account/login`) 后附加 `loginType=Splunk`。用户还可以通过直接导航到 `splunkweb:port/en-US/account/login/loginType=Splunk` 登录到其本地 Splunk 帐户。
单点注销 URL。	此字段通过元数据文件自动填充，并成为 IdP 协议端点。如果您不提供该 URL，则不会注销用户。
IdP 的证书路径	此值可以为目录或文件，具体取决于 IdP 要求。如果您提供了文件，则 Splunk 软件会用该文件验证 SAML 响应。如果提供目录，Splunk 软件将查找该目录下的所有证书，并尝试用其中的每个证书验证 SAML 响应。如果任何验证失败，则视响应为无效。
实体 ID。	此字段在您的 IdP 上配置在 SP 连接条目中的实体 ID。
签名 AuthRequest。	选择此选项。
签名 SAML 响应。	选择此选项。

7.在**属性查询**中，可选择提供以下信息，以便稍后可以创建计划的搜索。

属性查询 URL。	（可选）此为在 SOAP 上的查询应该发送到的 IdP 上的端点。格式如下： <urn:oasis:names:tc:SAML:2.0:attrname-format:uri>
签名属性查询请求	验证此字段是否已选。
签名属性查	

签名属性查询响应	验证此字段是否已选。

8. 仅在需要设置负载平衡或更改 SAML 绑定时填充高级部分。请参阅“配置负载平衡或 SAML 绑定”。

9. 单击**保存**。

后续步骤

将 SAML 组映射到 Splunk Enterprise 角色

使用 Okta 作为您的身份提供程序配置 SSO

如果您已将 Okta 配置为身份提供程序 (IdP)，则此任务将介绍如何为 Splunk Enterprise 设置 SSO。有关将 Okta 配置为 IdP 的信息，请参阅 Okta 文档。

使用以下任务配置 Splunk 部署以识别和使用 Okta 配置。然后，将 IdP 的组映射到 Splunk 用户角色，以便这些组可以登录。

警告：在尝试在 Splunk Cloud 中配置 SSO 之前，请与 Splunk 支持人员联系并打开票据，以请求他们为 SSO 准备您的云部署。当他们配置您的部署时，将通知您并提供所需的证书。

前提条件

验证您的系统是否满足所有要求。参阅“使用 SAML 配置单点登录”。

1. 在**设置**菜单中，选择**访问控制 > 验证方法**。

2. 选择 **SAML** 作为您的验证类型。

3. 单击**将 Splunk 配置为使用 SAML**。

4. 在“SAML 组”页面，单击 **SAML 配置**。

5. 浏览并选择元数据文件，或将元数据直接复制并粘贴到文本窗口中。如果您无法确定如何查找元数据文件，请参阅 Okta 文档。

6. 在**常规设置**中，提供如下信息：

单点登录 URL。	此字段自动通过所选元数据文件填充。这是 Splunk Enterprise 将向其发送验证请求的 IdP 上的受保护端点。如果您正在使用 Splunk Cloud，打开支持的提交问题以使 Splunk Cloud 运营小组打开端口，从而与 IdP 通信。 您的用户使用该 URL 进行 SSO 登录。 如要在启用 SAML 后访问登录页面，请在整个登录 URL (`/account/login`) 后附加 `loginType=Splunk`。用户还可以通过直接导航至 – splunkweb:port/en-US/account/login?loginType=Splunk 来登录其本地 Splunk 帐户
单点注销 URL。	此字段通过元数据文件自动填充，并成为 IdP 协议端点。如果您不提供该 URL，则不会注销用户。
IdP 的证书路径	此值可以为目录或单个文件，具体取决于 IdP 要求。如果您提供了文件，则 Splunk Enterprise 会用该文件验证 SAML 响应的真实性。如果提供目录，Splunk Enterprise 将查找该目录下的所有证书，并尝试用其中的每个证书验证 SAML 响应。如果任何验证失败，则整个验证都算是失败。
实体 ID。	此字段在您的 IdP 上配置在 SP 连接条目中的实体 ID。
签名 AuthRequest。	选择此选项。
签名 SAML 响应。	选择此选项。

7. 跳过**属性查询**并转到步骤 **8** 和 **9**。

8. 仅在需要设置负载平衡或更改 SAML 绑定时填充高级部分。请参阅“配置负载平衡或 SAML 绑定”

9. 单击**保存**。

后续步骤

将 SAML 组映射到 Splunk Enterprise 角色

使用 AzureAD 或 AD FS 作为您的身份提供程序配置 SSO

如果您已将 AzureAD 或 ADFS 配置为身份提供程序 (IdP)，则此任务将介绍如何为 Splunk 部署设置 SSO。配置 IdP 时，在 AzureAD 中配置组时，请注意以下建议：

- 回复 URL 可能最后需要 /SAML/acs。
- 您可能需要将 groupMembershipClaims 从空值更改为 SecurityGroup。

有关将 AzureAD 或 AD FS 配置为 IdP 的信息，请参阅您的 IdP 文档。

使用以下任务配置 Splunk 部署以识别和使用 AzureAD 或 AD FS 配置。然后，将 AzureAD 或 AD FS 用户组映射到 Splunk 用户角色，以便这些用户可以登录。

警告：在尝试在 Splunk Cloud 中配置 SSO 之前，请与 Splunk 支持人员联系并打开请求他们为 SSO 准备您的 Splunk Cloud 部署的票据。当他们配置您的部署后，将通知您并提供所需的证书。

前提条件

验证您的系统是否满足所有要求。参阅"使用 SAML 配置单点登录"。

1.在**设置**菜单中，选择**访问控制 > 验证方法**。

2.选择 **SAML** 作为您的验证类型。

3.单击**将 Splunk 配置为使用 SAML**。

4.在"SAML 组"页面，单击 **SAML 配置**。

5.浏览并选择元数据文件，或将元数据直接复制并粘贴到文本窗口中。如果您无法确定如何获取元数据文件，请参阅 IdP 文档。

6.在**常规设置**中，提供如下信息。

单点登录 URL。	此字段自动通过所选元数据文件填充。这是 Splunk Enterprise 将向其发送验证请求的 IdP 上的受保护端点。针对 Splunk Cloud，打开支持的提交问题以使 Splunk Cloud 运营小组打开端口，从而与您的 IdP 通信。 您的用户也会使用该 URL 进行 SSO 登录。如要在启用 SAML 后访问登录页面，请在整个登录 URL (`/account/login`) 后附加 `loginType=Splunk`。用户还可以通过直接导航到 `splunkweb:port/en-US/account/login/loginType=Splunk` 登录到其本地 Splunk 帐户。
单点注销 URL。	此字段通过元数据文件自动填充，并成为 IdP 协议端点。如果您不提供该 URL，则不会注销用户。
IdP 的证书路径	此值可以为目录或文件，具体取决于 IdP 要求。如果您提供了文件，则 Splunk 软件会用该文件验证 SAML 响应的真实性。如果提供目录，Splunk 将查找该目录下的所有证书，并尝试用其中的每个证书验证 SAML 响应。如果该验证失败，则整个验证都算是失败。
实体 ID。	此字段在您的 IdP 上配置在 SP 连接条目中的实体 ID。
签名 AuthRequest。	选择此选项。
签名 SAML 响应。	选择此选项。

7.跳过**属性查询**部分，并转到步骤 **8** 和 **9**。

8.仅在需要设置负载平衡或更改 SAML 绑定时填充高级部分。请参阅"配置负载平衡或 SAML 绑定"

9.单击**保存**。

后续步骤

将 SAML 组映射到 Splunk Enterprise 角色

使用 OneLogin 作为您的身份提供程序配置 SSO

如果您已将 OneLogin 配置为身份提供程序 (IdP)，则此任务将介绍如何为 Splunk 设置 SSO。有关将 OneLogin 配置为 IdP 的信息，请参阅 OneLogin 文档。

使用以下任务配置 Splunk 以识别和使用 OneLogin 配置。然后，将 OneLogin 用户组映射到 Splunk 用户角

色，以便这些用户可以登录 Splunk。

警告：在尝试在 Splunk Cloud 中配置 SSO 之前，请与 Splunk 支持人员联系并打开请求 SSO 的云部署的票据。支持人员将配置您的部署，并提供所需的证书。

前提条件

验证您的系统是否满足所有要求。参阅"使用 SAML 配置单点登录"。

1.在**设置**菜单中，选择**访问控制 > 验证方法**。

2.选择 **SAML** 作为您的验证类型。

3.单击**将 Splunk 配置为使用 SAML**。

4.在"SAML 组"页面，单击 **SAML 配置**。

5.浏览并选择元数据文件，或将元数据直接复制并粘贴到文本窗口中。如果您无法确定如何获取元数据文件，请参阅 IdP 文档。

6.在**常规设置**中，提供如下信息。

单点登录 URL。	此字段自动通过所选元数据文件填充。这是 Splunk 将向其发送验证请求的 IdP 上的受保护端点。如果您正在使用 Splunk Cloud，打开支持的提交问题以使 Splunk Cloud 运营小组打开端口，从而与 IdP 通信。 您的用户使用该 URL 进行 SSO 登录。 如要在启用 SAML 后访问登录页面，请在整个登录 URL (`/account/login`) 后附加 `loginType=Splunk`。用户还可以通过直接导航至 – splunkweb:port/en-US/account/login/loginType=Splunk 来登录其本地 Splunk 帐户
单点注销 URL。	OneLogin 支持单点注销的重定向绑定。将绑定设置为 'HTTPRedirect'。
IdP 的证书路径	此值可以为目录或文件，具体取决于 IdP 要求。如果您提供了文件，则 Splunk 会用该文件验证 SAML 响应的真实性。如果您提供了目录，则 Splunk 会查找所有以子目录呈现的证书并尝试验证每个 SAML 响应。如果 Splunk 无法验证所有的真实性，则响应将被视为不真实。
实体 ID。	此字段在您的 IdP 上配置在 SP 连接条目中的实体 ID。
签名 AuthRequest。	将此值设置为 false。
签名 SAML 响应。	将此值设为 False。

7.跳过**属性查询**部分，并转到步骤 **8** 和 **9**。

8.仅在需要设置负载平衡或更改 SAML 绑定时填充高级部分。请参阅"配置负载平衡或 SAML 绑定"

9.单击**保存**。

后续步骤

将 SAML 组映射到 Splunk Enterprise 角色

使用 Optimal 作为您的身份提供程序配置 SSO

如果您已将 Optimal 配置为身份提供程序 (IdP)，则此任务将介绍如何为 Splunk 设置 SSO。有关将 Optimal 配置为 IdP 的信息，请参阅 Optimal 文档。

使用以下任务配置 Splunk 以识别和使用 Optimal 配置。然后，将 Optimal 用户组映射到 Splunk 用户角色，以便这些用户可以登录 Splunk。

警告：在尝试在 Splunk Cloud 中配置 SSO 之前，请与 Splunk 支持人员联系并打开票据，请求 SSO 的云部署。支持人员将配置您的部署，并提供所需的证书。

前提条件

验证您的系统是否满足所有要求。参阅"使用 SAML 配置单点登录"。

1.在**设置**菜单中，选择**访问控制 > 验证方法**。

2.选择 **SAML** 作为您的验证类型。

3. 单击**将 Splunk 配置为使用 SAML**。

4. 在“SAML 组”页面，单击 **SAML 配置**。

5. 浏览并选择元数据文件，或将元数据直接复制并粘贴到文本窗口中。如果您无法确定如何获取元数据文件，请参阅 IdP 文档。

6. 在**常规设置**中，提供如下信息。

单点登录 URL。	此字段自动通过所选元数据文件填充。这是 Splunk 将向其发送验证请求的 IdP 上的受保护端点。如果您正在使用 Splunk Cloud，打开支持的提交问题以使 Splunk Cloud 运营小组打开端口，从而与 IdP 通信。 您的用户使用该 URL 进行 SSO 登录。 如要在启用 SAML 后访问登录页面，请在整个登录 URL (`/account/login`) 后附加 `loginType=Splunk`。用户还可以通过直接导航至 – splunkweb:port/en-US/account/login/loginType=Splunk 来登录其本地 Splunk 帐户
单点注销 URL。	此字段通过元数据文件自动填充，并成为 IdP 协议端点。如果您不提供该 URL，则不会注销用户。
IdP 的证书路径	此值可以为目录或文件，具体取决于 IdP 要求。如果您提供了文件，则 Splunk 会用该文件验证 SAML 响应的真实性。如果您提供了目录，则 Splunk 会查找所有以子目录呈现的证书并尝试验证每个 SAML 响应。如果 Splunk 无法验证所有的真实性，则响应将被视为不真实。
实体 ID。	此字段在您的 IdP 上配置在 SP 连接条目中的实体 ID。
签名 AuthRequest。	选择此选项。
签名 SAML 响应。	选择此选项。

7. 跳过**属性查询**部分，并转到步骤 **8** 和 **9**。

8. 仅在需要设置负载平衡或更改 SAML 绑定时填充高级部分。请参阅“配置负载平衡或 SAML 绑定”

9. 单击**保存**。

后续步骤

将 SAML 组映射到 Splunk Enterprise 角色

在 CA siteminder 中配置 SSO

如果您已将 CA 配置为身份提供程序 (IdP)，则此任务将介绍如何为 Splunk 设置 SSO。有关将 CA 配置为 IdP 的信息，请参阅 CA 文档。

使用以下任务配置 Splunk 以识别和使用 CA 配置。然后，将 CA 用户组映射到 Splunk 用户角色，以便这些用户可以登录 Splunk。

警告：在尝试在 Splunk Cloud 中配置 SSO 之前，请与 Splunk 支持人员联系并打开票据，请求 SSO 的云部署。支持人员将配置您的部署，并提供所需的证书。

前提条件

验证您的系统是否满足所有要求。参阅“使用 SAML 配置单点登录”。

1. 在**设置**菜单中，选择**访问控制 > 验证方法**。

2. 选择 **SAML** 作为您的验证类型。

3. 单击**将 Splunk 配置为使用 SAML**。

4. 在“SAML 组”页面，单击 **SAML 配置**。

5. 浏览并选择元数据文件，或将元数据直接复制并粘贴到文本窗口中。如果您无法确定如何获取元数据文件，请参阅 IdP 文档。

6. 在**常规设置**中，提供如下信息。

单点登录 URL。	此字段自动通过所选元数据文件填充。这是 Splunk 将向其发送验证请求的 IdP 上的受保护端点。如果您正在使用 Splunk Cloud，打开支持的提交问题以使 Splunk Cloud 运营小组打开端口，从而与 IdP 通信。 您的用户使用该 URL 进行 SSO 登录。 如要在启用 SAML 后访问登录页面，请在整个登录 URL (`/account/login`) 后附加 `loginType=Splunk`。用户还可以通过直接导航至 - splunkweb:port/en-US/account/login/loginType=Splunk 来登录其本地 Splunk 帐户
单点注销 URL。	此字段通过元数据文件自动填充，并成为 IdP 协议端点。如果您不提供该 URL，则不会注销用户。
IdP 的证书路径	此值可以为目录或文件，具体取决于 IdP 要求。如果您提供了文件，则 Splunk 会用该文件验证 SAML 响应的真实性。如果您提供了目录，则 Splunk 会查找所有以子目录呈现的证书并尝试验证每个 SAML 响应。如果 Splunk 无法验证所有的真实性，则响应将被视为不真实。
实体 ID。	此字段在您的 IdP 上配置在 SP 连接条目中的实体 ID。
签名 AuthRequest。	选择此选项。
签名 SAML 响应。	选择此选项。

7. 跳过**属性查询**，并转到步骤 **8** 和 **9**。

8. 仅在需要设置负载平衡或更改 SAML 绑定时填充高级部分。请参阅“配置负载平衡或 SAML 绑定”

9. 单击**保存**。

后续步骤

将 SAML 组映射到 Splunk Enterprise 角色

使用 TLS 证书确保 SSO 安全

配置以下 SSL 设置以使 Splunk Enterprise 能够在 Splunk 实例和提供 `AttributeQuery` 服务的 SOAP 实例之间执行 TLS 验证。

除非注明，否则未设置的值默认为 `server.conf` 中指定的设置。

```
[<saml-authSettings-key>]

sslVersions = <Comma-separated list of SSL versions to support>

sslCommonNameToCheck = <commonName> When populated, and sslVerifyServerCert is "true", splunkd limits most outbound
HTTPS connections to hosts which use a cert with this common name.

sslAltNameToCheck = <alternateName1>, <alternateName2>, ...If set, and sslVerifyServerCert' is "true",
splunkd can verify certificates with "Subject Alternate Name" that matches any of the alternate names in this list

ecdhCurveName = <ECDH curve to use for ECDH key negotiation>

sslKeysfile = <Server certificate file> Default certificates, "sever.pem" are auto-generated by splunkd upon
starting Splunk, you may replace the default cert with your own PEM format file

sslKeysfilePassword = <Server certificate password>

caCertFile = <Public key of the signing authority> The default value is cacert.pem

caPath = <Path where all these certs are stored>. Default value is $SPLUNK_HOME/etc/auth

sslVerifyServerCert = [ true | false ] If true, distributed search makes a search request to another
server in the search cluster.
```

配置 SAML SSO

当您将 Splunk 配置为使用 SAML 验证系统时，您可以通过将它们映射到 Splunk 用户角色来授权组登录 IdP。

警告：在尝试在 Splunk Cloud 中配置 SSO 之前，请与 Splunk 支持人员联系并打开票据，请求他们针对 SSO 准备您的云部署。当他们配置您的部署时，将通知您并提供所需的证书。

前提条件

验证您的系统是否满足所有要求。参阅"使用 SAML 配置单点登录"。

1.在**设置**菜单中，选择**访问控制 > 验证方法**。

2.选择 **SAML** 作为您的验证类型。

3.单击**将 Splunk 配置为使用 SAML**。

4.在"SAML 组"页面，单击 **SAML 配置**。

5.浏览并选择元数据文件，或将元数据直接复制并粘贴到文本窗口中。如果您无法确定如何获取元数据文件，请参阅 IdP 文档。

6.在**常规设置**中，提供如下信息。

单点登录 URL。	此字段自动通过所选元数据文件填充。这是 Splunk 将向其发送验证请求的 IdP 上的受保护端点。如果您正在使用 Splunk Cloud，打开支持的提交问题以使 Splunk Cloud 运营小组打开端口，从而与 IdP 通信。 您的用户使用该 URL 进行 SSO 登录。 如要在启用 SAML 后访问登录页面，请在整个登录 URL (`/account/login`) 后附加 `loginType=Splunk`。用户还可以通过直接导航至 – splunkweb:port/en-US/account/login/loginType=Splunk 来登录其本地 Splunk 帐户
单点注销 URL。	此字段通过元数据文件自动填充，并成为 IdP 协议端点。如果您不提供该 URL，则不会注销用户。
IdP 的证书路径	此值可以为目录或文件，具体取决于 IdP 要求。如果您提供了文件，则 Splunk 会用该文件验证 SAML 响应的真实性。如果您提供了目录，则 Splunk 会查找所有以子目录呈现的证书并尝试验证每个 SAML 响应。如果 Splunk 无法验证所有的真实性，则响应将被视为不真实。
实体 ID。	此字段在您的 IdP 上配置在 SP 连接条目中的实体 ID。
签名 AuthRequest。	选择此选项。
签名 SAML 响应。	选择此选项。

7.如果您将 PingIdentity 用作 IdP，则在**属性查询**中提供以下信息，这样您可以稍后创建计划的搜索。这些字段并非通过 Okta、Azure AD 或 AD FS 创建计划搜索的必填字段。

属性查询 URL。	此字段为在 SOAP 上的查询应该发送到的 IdP 上的端点。格式如下： <urn:oasis:names:tc:SAML:2.0:attrname-format:uri>
签名属性查询请求	验证此字段是否已选。
签名属性查询响应	验证此字段是否已选。

8.在**高级设置**中，提供如下信息。

属性别名角色	使用此字段指定任何 IdP 新属性名称，然后为 3 个属性中的任何一个在 Splunk 端配置别名。 如果您已配置 AD FS 内置"角色"属性为返回，并具备 AD 组信息，则指定 `http://schemas.microsoft.com/ws/2008/06/identity/claims/role`。此值会告诉 Splunk，包含 SAML 响应中角色信息的属性已返回。 如果您已配置 Azure AD，则指定 `http://schemas.microsoft.com/ws/2008/06/identity/claims/groups`。
属性别名邮件	如果您将 Azure AD 用作 IdP，则填充此字段。此值将别名映射到返回的 SAML 响应中的用户电子邮件地址。输入 `http://schemas.microsoft.com/identity/claims/displayname`。
属性别名真实	如果您将 Azure AD 用作 IdP，则填充此字段。此值会告诉 Splunk Enterprise 在返回

属性别名真实姓名	的 SAML 响应中映射真实姓名的位置。输入 `http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress`。
FQDN - 负载均衡器的主机名或 IP	设置为：https://sh1.STACKID.splunkcloud.com。此设置用于带有“单点搜索头设置”或“搜索头群集设置”的 Splunk 部署。如果您通过搜索头群集使用负载均衡，则必须提供一个地址。
（可选）**重定向端口**	根据之前字段的说明为负载均衡器提供一个重定向端口。为 Okta 将其设置为 "0"（零）。

9. 单击**保存**。

后续步骤

将 SAML 组映射到 Splunk Enterprise 角色

为 SSO 配置高级设置

如果他们希望您设置负载平衡或更改 SAML 绑定，则填充高级部分。

在**高级设置**中，提供如下信息。

属性别名角色	使用此字段指定任何 IdP 新属性名称，然后为三个属性中的任何一个在 Splunk 端配置别名。
属性别名真实姓名	您可以跳过此字段。对于 ADFS，您可以使用“属性别名真实姓名”的显示名称。
FQDN - 负载均衡器的主机名或 IP	设置为：https://sh1.STACKID.example.com。此设置用于带有“单点搜索头设置”或“搜索头群集设置”的 Splunk 部署。如果您通过搜索头群集使用负载均衡，则必须提供一个地址。
（可选）**重定向端口**	根据之前字段的说明为负载均衡器提供一个重定向端口。

将 SAML 组映射到角色

当您将 Splunk 部署配置为使用 SAML 验证系统时，您可以通过将它们映射到 Splunk 用户角色来授权组登录 SAML 服务器。您可以映射多个组到单点用户角色。

前提条件

有关 SAML SSO

1. 在**设置**菜单中，选择**访问控制 > 验证方法**。

2. 选择 **SAML** 作为您的验证类型。

3. 单击**将 Splunk 配置为使用 SAML**。

4. 在“SAML 组”页面，单击**新建组**或单击**编辑**您想要修改的组。

5. 为组提供名称。

6. 通过将所需的角色从左列移动到右列来确定您想要分配给该组的角色。

7. 单击**保存**。

配置 SAML SSO 并映射组到角色之后，您可以分发登录 URL 至您的用户。

修改或删除角色映射

当您将 Splunk 部署配置为使用 SAML 验证系统时，您可以通过将它们映射到 Splunk 用户角色来授权组登录 SAML 服务器。您可以映射多个组到单点用户角色。

本主题介绍了如何从现有组中删除角色或完全删除组。要从 SAML 组中删除个别用户，请参阅您的 IdP 文档。

前提条件

有关 SAML SSO

1.在**设置**菜单中，选择**访问控制 > 验证方法**。

2.选择 **SAML** 作为您的验证类型。

3.单击**将 Splunk 配置为使用 SAML**。

4.要删除整个组，请单击要移除的组中的**删除**。

5.在“SAML 组”页面，单击**编辑**以编辑您想要修改的组。

6.通过将所需的角色从右列移动到左列来指定您想要从该组删除的角色。

7.单击**保存**。

配置 SAML SSO 并映射组到角色之后，您可以分发登录 URL 至您的用户。

在配置文件中配置 SAML SSO

本主题将介绍如何使用配置文件为 SAML v2 设置 SSO：

- 在 Splunk Enterprise 中配置 `authentication.conf` 和 `web.conf`
- 配置您的身份提供程序
- 确保 SAML 配置安全

配置 `authentication.conf`

在`authentication.conf` 中配置以下段落

```
[authentication]
authSettings = saml_settings
authType = SAML
[roleMap_SAML]
admin = Super Admin;
power = Power Admin;
user = <list roles> Admin;Employee;
[saml_settings]
entityId = <entityid>
idpAttributeQueryUrl = <optional path to the Attribute query> https://your path/idp/attrsvc.ssaml2
idpCertPath = <path to the idp cert in Splunk> /home/user/splunk/saml-install/etc/auth/ping_idp.crt.>
idpSSOUrl = <path to the sso url> https://your path/idp/SSO.saml2.
idpSLOUrl = <Logout url. If not specified, this will be treated as a typical sso and the logout button will be
disabled.
https://your path/idp/SLO.saml2 #
redirectPort=443
attributeQueryTTL = 3600
signAuthnRequest = true
signedAssertion = true
attributeQueryRequestSigned = <Set to true if using optional idpAttributeQuerySSL>
attributeQueryResponseSigned = <Set to true if using optional idpAttributeQuerySSL>
attributeQuerySoapPassword = <your password>
attributeQuerySoapUsername = <your username>
```

要通过 Azure AD 或 ADFS 配置单点登录，请添加以下其他属性：

nameIDFormat = （可选）指定在 SAML 响应中返回的主题格式。AzureAD 返回一个字符串以确定主题，并且此属性允许您选择指定一个不同的格式（我们建议使用电子邮件地址）。它对于审计和已保存的搜索十分有用。要按此格式指定电子邮件地址，请使用：`urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress`

role = 如果您将 Azure AD 用作 SSO 或 ADFS，则填充此字段。此值会告诉 Splunk Enterprise，提供 SAML 响应中角色信息的属性已返回。对于 Azure AD，请使用：`http://schemas.microsoft.com/ws/2008/06/identity/claims/groups`

email = 此值将别名映射到返回的 SAML 响应的用户电子邮件地址中。对于 Azure AD，请使用：`http://schemas.microsoft.com/identity/claims/displayname`

realName = 此值告诉 Splunk Enterprise 在返回的 SAML 响应中的什么位置映射真实名称。对于 Azure AD，请使用：`http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress`。

</pre>

配置 `web.conf` 并选择添加一个失败的重定向地址

将以下值添加到 `web.conf` 中的设置段落

```
[settings]
appServerPorts = 7065 <make sure this attribute is enabled>
ssoAuthFailureRedirect = http://10.140.31.19:7000/ui/en-us/account/sso_error <this is your custom user redirect for failed logins>
```

配置您的身份提供程序

现在您必须配置 IdP 来导入 Splunk 软件的元数据。要在 IdP 中导入 Splunk 软件元数据，请确保 `AuthnRequest` 签名和 `AttributeQuery` 请求签名设置在 Splunk 软件和 IdP 中兼容：

1.将 IdP 证书导出到您的 Splunk 软件实例中的一个文件里。

2.确保 `authentication.conf` 指向 SAML 配置段落中的此证书。

3.将 Splunk 软件服务器证书 (`server.pem`) 导入 IdP 以进行签名确认。

请注意，您可以使用 Splunk Web 上的 `/saml/spmetadata` 端点导出 Splunk 软件元数据。您还可以访问 `SAML-sp-metadata` 端点（位于 `splunkd`）。

确保 SAML 配置安全

SAML attributequery 服务支持 Splunk Enterprise 的所有标准 SSL 设置，以在 Splunk 实例和提供 AttributeQuery 服务的 SOAP 实例之间执行 TLS 验证。

一般来说，以下设置仅适用于支持属性查询的 IdP。但是，`sslKeysFile` 和 `sslKeysFilePassword` 属性适用于任何 IdP。

编辑 `server.conf` 以配置证书验证：

```
[<saml-authSettings-key>]
sslVersions = <recommended settings tls1.1 and tls1.2>
sslCommonNameToCheck = <commonName> If this value is set, and 'sslVerifyServerCert' is set to true, splunkd will limit most outbound HTTPS connections to hosts which use a cert with this common name. If not set, Splunk uses the setting specified in server.conf.
sslAltNameToCheck = <alternateName1>, <alternateName2> If this value is set, and 'sslVerifyServerCert' is set to true, splunkd will also be willing to verify certificates which have a so-called "Subject Alternate Name" that matches any of the alternate names in this list. If not set, Splunk uses the setting specified in server.conf.
ecdhCurveName = <string> ECDH curve to use for ECDH key negotiation. If not set, Splunk uses the setting specified in server.conf.
sslKeysfile = <server certificate file>. Certificates are auto-generated by splunkd upon starting Splunk but you can replace the default cert with your own PEM format file. Default is server.pem. If not set, Splunk uses the setting specified in server.conf. This setting is valid for all IdPs.
sslKeysfilePassword = <server certificate password> This setting is valid for all IdPs.
caCertFile = <fPublic key of the signing authority, default is cacert.pem> If not set, Splunk uses the setting specified in server.conf.
caPath = <path where all these certs are stored, the default is $SPLUNK_HOME/etc/auth>
sslVerifyServerCert = [ true | false ] Used by distributed search: when making a search request to another server in the search cluster. If not set, Splunk uses the setting specified in server.conf.
```

SAML SSO 故障排除

下面是一些常见问题以及如何解决。

问题

您收到了如下消息：

```
ERROR AuthenticationManagerSAML - Requesting user info from ID returned an error Error in Attribute query request, AttributeQueryTransaction err=Cannot resolve hostname, AttributeQueryTransaction descr=Error resolving: Name or service not known, AttributeQueryTransaction statusCode=502
```

要缓解该问题

- 确保 `cipherSuite` 在 SAML 段落中正确指定。例如：
  - `cipherSuite = TLSv1+MEDIUM:@STRENGTH`
  - `cipherSuite = ALL:!aNULL:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM`
- 确保满足所有 SOAP 密码要求。

- 确保 SAML 的 SSL 设置在 `authentication.conf` 中正确配置。

问题

您收到了如下消息：

```
ERROR UserManagerPro - user="samluser1" had no roles
```

要缓解该问题

- 确保 `rolemap_SAML` 包含正确的角色映射，且每个角色名称后都有 ";"。

问题

您收到了如下消息：

```
ERROR AuthenticationManagerSAML - Attribute query request failed. Status
code=urn:oasis:names:tc:SAML:2.0:status:UnknownPrincipal, Status msg=No attributes found for requested subject
```

要缓解该问题

- 确保 `role`、`mail` 和 `realName` 属性将映射，以作为 `AuthnRequest` 和“属性查询请求”的一部分返回。

问题

用户在成功断言验证后无法登录。在本地映射或断言中无法找到有效的 Splunk 角色。

要缓解该问题

- 确保 `rolemap_SAML` 段落包含从 IdP 返回的角色和相应 Splunk 角色之间的正确映射。
- 确保 `authentication.conf` 中定义的每个角色之间及其前后没有空格。例如：

```
user = User;Employee
```

问题

验证被配置为 SAML 并且设置显示是正确的，但是登录屏幕反而显示的是 Splunk 验证的页面。

要缓解该问题

- 确保在 `web.conf` 中 `appServerPorts` 设置为有效端口，而并非 '0'。

使用代理 SSO 进行验证

有关 ProxySSO

Spunk Enterprise 上的 ProxySSO 验证允许您通过反向代理服务器为 Splunk 实例配置单点登录。这意味着一旦用户登录到反向代理服务器，他们可以无缝访问 Splunk Web。

在许多情况下，ProxySSO 比现有的单点登录更简单，因为与用户身份一起，组信息也可以在 HTTP 标头中传递到 Splunk。Spunk 使用此信息对用户进行验证，并通过将组映射到相应的 Splunk 角色来对其进行授权。

ProxySSO 验证：

- 将认证和授权为用户合并成一个步骤，简化登录过程。
- 减少配置步骤。无需在 Splunk Enterprise 中配置复杂的 LDAP 策略。
- 减少 Splunk 和验证服务之间的来回信息，使您的验证效率更高。
- 只要代理服务器可以传递所需的信息，外部认证服务不限于 LDAP

请注意，当前无法通过 Splunk Web 配置 ProxySSO。相反，您必须使用 REST API 或修改配置文件配置

ProxySSO。

Splunk Cloud 目前不支持 ProxySSO。

前提条件

要设置 ProxySSO，您应已经配置了以下内容：

- 配置为发送所需 HTTP 标头的代理服务器。
- 有效的 Splunk Enterprise 配置。有关如何配置上述项目并设置 ProxySSO 的更多信息，请参阅配置 ProxySSO

Splunk 软件如何处理代理请求

ProxySSO 支持通过反向代理服务器进行验证和授权。代理服务器根据配置的验证服务进行验证并创建 HTTP 请求。Splunk 从受信任的反向代理服务器接收 HTTP 标头。`trustedIP` 在 `web.conf` 中配置，并在从代理接收请求时接受检查。

对于验证，Splunk Enterprise 会信任标头中传递的身份。除了用户验证，Splunk Enterprise 还会解析标头中的组信息。组对角色映射在 `authentication.conf`（位于 `[roleMap_proxySSO]` 段落中）指定。Splunk Enterprise 用它来确定用户的 Splunk 角色。如果组不能映射到任何角色，则用户将使用默认配置的角色登录。如果未找到任何角色，则用户将无法登录。

登录成功后，将为用户创建会话 cookie，并可以无缝访问 Splunk Web。

配置 ProxySSO

配置反向代理服务器

您可以配置代理服务器，使其充当 Splunk Web 的代理，提示用户输入凭据，并通过 HTTP 标头将用户身份和组传递到 Splunk Web。

下面的示例显示了如何为 ProxySSO 配置 Apache 服务器：

```
AuthType Basic
AuthBasicProvider ldap
....
ProxyPass / http://mysplunkhost:8000/
ProxyPassReverse / http://mysplunkhost:8000/
....
AuthLDAPURL "ldap://<ldap-server>:<ldap-port>/OU=IT Department,DC=com?sn,sAMAccountName?"
....
RequestHeader set Remote_User %{AUTHENTICATE_sn}e
RequestHeader set Remote_Groups %{AUTHENTICATE_sAMAccountName}e
....
```

此配置提示用户输入 LDAP 用户名和密码，并查询指定的 LDAP 服务器。然后，它使用 LDAP 属性值在 HTTP 标头 `Remote_User` 和 `Remote_Groups` 中设置用户和组信息。

配置 Splunk Enterprise

1.配置 `web.conf`

```
[settings]
SSOMode = strict
trustedIP = 10.1.1.2
remoteUser = Remote_User
remoteGroups = Remote_Groups
remoteGroupsQuoted = true
allowSsoWithoutChangingServerConf = 1
```

此配置将仅信任来自 IP 地址 `10.1.1.2` 的传入请求，因为我们已设置 `SSOMode = strict`。

它将从具有密钥的标头中提取值为 `Remote_User` 和 `Remote_Groups`。

您可以设置 `allowSsoWithoutChangingServerConf = 1` 或将 `trustedIP` 设置为 127.0.0.1（在 `server.conf` 中）

与 `Remote_Groups` 对应的值是以逗号分隔的组的列表，例如 `IT, Engineering, HR`。但是，组条目可以由逗号组成。要处理这种情况，可以通过启用 `remoteGroupsQuoted = true`.将组包含在引号内并由 Splunk 解析。例如组列表 `"IT, North America", "Engineering"` 将被解析为两个组（`IT, North Americas` 和 `Engineering`）。

重新启动 Splunk 实例使更改生效。

2.在 `authentication.conf` 中，配置 `[authentication]` 段落：

```
[authentication]
authType = ProxySSO
authSettings = my_proxy
```

3.在 `roleMap_proxySSO` 段落中，将组映射到 Splunk 角色。

```
[roleMap_proxySSO]
admin = IT operational admin
splunk-system-role = IT sub-admin
```

4.配置其他设置的 `[my_proxy]` 段落：

```
[my_proxy]
defaultRoleIfMissing = user
```

如果未找到组映射，则分配 `defaultRoleIfMissing` 中配置的角色。

配置完成后，重新加载验证以使更改生效。

代理 SSO 故障排除

您可以在设置 `settings` 段落下 `web.conf` 中的 `enableWebDebug=true` 后，查看代理服务器发送到以下端点上的 Splunk Web 的 HTTP 请求标头：

```
http://<ProxyServerIP>:<ProxyServerPort>/debug/sso
```

此端点将有助于验证一些常见的配置或设置错误：

- 传入请求 IP 与 `trustedIP` 的配置值匹配
- 确保代理服务器上设置的标头属性名称与 Splunk 上配置的标头属性名称相同
- 确保组条目发送和解析正确。特别是当设置 `remoteGroupsQuoted = true` 时。您可以通过添加 `splunkd` 段落下 `etc/log.cfg` 中的 `category.UiAuth=DEBUG` 来查看组的解析方式。

一旦验证，请检查以下配置：

- 在 `roleMap_proxySSO` 中具有映射的已解析的组
- 在某些情况下，用户无法登录，因为用户或其角色被列入黑名单。检查以 `authSettings` 的值命名的段落下的黑名单对象

这些类型的登录事件以及失败的原因记录在 `var/log/splunkd.log` 中。

验证使用反向代理的单点登录

关于使用反向代理进行单点登录

Splunk 单点登录 (SSO) 允许您使用反向代理处理 Splunk **验证**，这意味着用户登录到其代理后，就可以无缝访问 Splunk Web（可以是配置到您的代理的任何其他应用程序）。

Splunk Enterprise SSO 反向代理的实现支持仅通过 Splunk Web 登录 Splunk Enterprise。因为实现依赖 cookie 保存验证信息，所以 SSO 不能用于 Splunk Enterprise 的 CLI 验证。调用 `https://localhost:8089`（或已分配管理端口）仍旧需要独立的验证。

有关如何配置上述项目并设置 SSO 的更多信息，请参阅配置单点登录

如何工作

Splunk Enterprise 管理员和用户会通过使用 Splunk Web 部署的代理 URL 调用 Splunk Web。代理会依据您的验证系统验证传入请求。一旦成功验证，代理就会通过验证身份的属性设置请求头，并发送此信息到 Splunk Enterprise。

Splunk Enterprise 会接受代理的传入 HTTP 请求，如果 Splunk Enterprise 识别标头中包含的用户，则用户会

绕过登录页面，并且自动获得授权。

为了单点登录成功，从代理到 Splunk Web 的所有请求都必须包括这一经验证的标头。如果标头未包括在请求中，用户会返回到登录页面或错误页面，具体取决于您的配置。Splunk 软件在浏览器会话期间使用这个经过验证的标头。

Splunk 软件如何处理代理请求

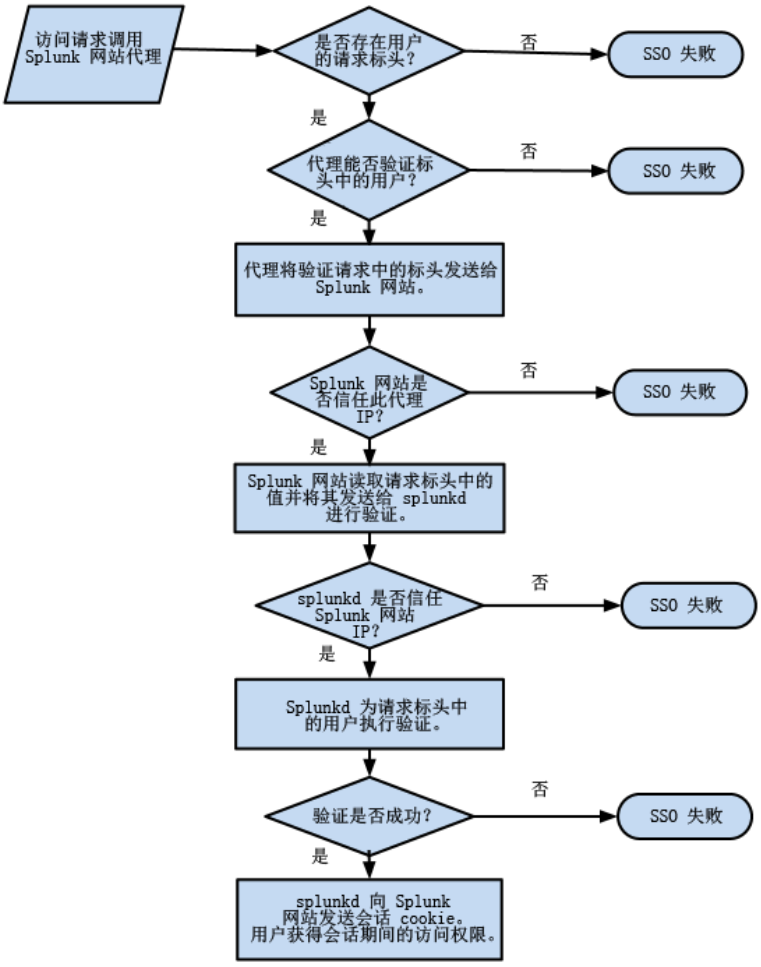
当代理服务器发送请求至 Splunk Web 时，Splunk Web 会查看 `trustedIP` 值（位于 `web.conf`）以验证代理 IP 在受信任的 IP 列表中。

如果 IP 不受信任，会拒绝该请求，并且登录尝试失败。如果 IP 地址受信任，则 Splunk Web 会查询请求头中的标记，并向 splunkd 发送包含标头信息的授权请求。

一旦从 Splunk Web 接收授权请求，splunkd 就会验证客户端（一般为 Splunk Web）的传入 IP 地址是否匹配 `server.conf` 文件的 `trustedIP` 属性的值。

如果 IP 地址并未出现在 `trustedIP` 列表中，则该请求会被拒绝，并且登录尝试失败。用户将要么返回至登录页面，要么显示一个错误页面，具体取决于 web.conf 中的 `SSOmode` 配置。有关此属性和其他配置信息的更多信息，请参阅配置 Splunk 单点登录。

如果 IP 受信任，则 splunkd 使用在请求头中包含的信息，并执行授权过程。



Splunk 软件如何授权用户

Splunk 软件首先检查指定的身份和角色是否与 Splunk 用户的任何身份和角色匹配。如果找不到匹配项，Splunk 软件会查看是否存在任何 LDAP 匹配。（有关 Splunk 软件如何验证用户的信息，请参阅本手册的设置使用 LDAP 进行的用户验证。）

如果未找到匹配项，并且无法为标头中的用户授权，则浏览器会重定向到错误页面。

如果找到匹配项，Splunk 软件会授权用户，并查看是否存在现有会话。如果会话已经存在，Splunk 软件会使用会话标记，并创建必需的 cookie 以允许用户访问 Splunk Web。如果会话不存在，则 Splunk 软件会为 Splunk

Web 授权创建一个新会话以及必需的 cookie。

创建 cookie 后，Splunk Web 会恢复其正常流。只要请求头中包含受信任的标记，并且在用户关闭浏览器会话之前，通过代理 URL 对 Splunk Enterprise 进行的任何后续访问都不要求重新授权。

配置使用反向代理的单点登录

在使用 Splunk Enterprise 配置基于反向代理的 SSO 之前，请确保您具有以下各项：

- 配置为反向代理用于验证到外部系统的代理服务器（Splunk Enterprise 支持 IIS 或 Apache）。
- LDAP 服务器或其他外部验证系统，配置有代理验证时所使用的相应组和用户。
- 有效的 Splunk Enterprise 配置，被配置为使用与您的代理（通常为 LDAP）相同的外部验证系统，或者具有与外部验证系统中包含的用户和组 ID 匹配的本机 Splunk Enterprise 用户。

配置使用反向代理的 SSO 需要以下步骤：

1.编辑代理服务器上的属性以使用外部验证系统进行验证。

2.编辑 Splunk Enterprise `server.conf` 文件。

3.编辑 Splunk Enterprise `web.conf` 文件。

注意：为了达到最佳安全，基于 HTTP 标头的解决方案应通过启用了 TLS/SSL 的部署实现。

配置 `server.conf`

编辑 `trustedIP`（位于 `general settings` 段落）以添加 IP 地址，该地址将确保验证请求安全发送到 splunkd。此地址通常为 Splunk Web，因而是 localhost。您只能为每个 splunkd 实例输入一个 IP 地址。

trustedIP=127.0.0.1

如果 `trustedIP` 列表中未提供 IP 地址，则 Splunk SSO 将默认为禁用。

配置 web.conf

要启用 SSO，请在 `[settings]` 段落中配置以下内容，该段落位于 `web.conf` (`SPLUNK_HOME/etc/system/local`) 中。

```
SSOMode = strict
trustedIP = 127.0.0.1,10.3.1.61,10.1.8.81
remoteUser = Remote-User
tools.proxy.on = False
```

属性	默认	值
`SSOMode`	no	`SSOMode` 属性确定 Splunk Web SSO 是否以 `strict` 或 `permissive` 模式运行。 严格模式限制对匹配 `trustedIP` 属性中罗列的 IP 地址身份的验证。如果尝试连接的 IP 地址未与任何 IP 地址匹配，则向用户显示错误页面。建议对 SSO 使用严格模式。 许可模式同样限制对来自 `trustedIP` 列表中 IP 请求的验证。在许可模式下，如果尝试连接的 IP 未与任何 IP 地址匹配，则会显示登录页面允许用户重新验证。
`trustedIP`	n/a	将此属性设置为验证一个或多个代理的 IP 地址。指定单个地址，或用逗号分隔的地址列表；不支持 IP 范围和网络掩码符号。
`remoteUser`	`REMOTE_USER`	`remoteUser` 属性确定验证的身份属性，该属性通过 HTTP 请求头由代理服务器传递。此值默认为 `REMOTE_USER`，但只要代理在验证后正确设置此属性，任何 LDAP 属性就可以在此请求头中传递。当您配置 `remoteUser` 属性时，您必须同样在代理配置中配置 `RequestHeader` 属性，以将身份属性传递给 Splunk 软件。此过程在"关于 Splunk 单点登录"中进行了介绍。 使用的默认 Splunk 标头为 `REMOTE_USER`，但如果您的代理使用不同的标头，则可以在此处更改标头名称。
`tools.proxy.on`	false	对于 apache 1.x 代理，此值应设置为 True。对于更新的版本 2.4，此值应设置为 False。

如果托管 Splunk Web 前面的代理未将 Splunk Web 置于代理根，则您可能还需配置 `root_endpoint` 设置（位于 `$SPLUNK_HOME/etc/system/local/web.conf`）。

比如说，如果您的代理在 "yourhost.com:9000/splunk" 托管 Splunk Web，则 `root_endpoint` 应该设置为 `/splunk`。

例如：

```
root_endpoint=/lzone
ProxyPass /lzone http://splunkweb.splunk.com:8000/lzone
ProxyPassReverse /lzone http://splunkweb.splunk.com:8000/lzone
```

在上例中，Splunk Web 通过 `http://splunk.example.com:8000/lzone` 而不是 `http://splunk.example.com:8000/` 进行访问。

接下来您将通过在 `httpd.conf` 中将其映射来显示给代理：

```
ProxyPass /lzone http://splunkweb.splunk.com:8000/lzone
ProxyPassReverse /lzone http://splunkweb.splunk.com:8000/lzone
```

会话管理

由于没有简单的会话注销，并且只要代理标头中包含正确的标头信息 Splunk Enterprise 就会保留会话，所以您应记得设置代理的会话超时值。

如果您需要在出现超时之前结束会话，则可以使用 REST 终点以及会话标记终止会话：

```
curl -s -uadmin:changeme  -k -X DELETE https://localhost:8089/services/authentication/httpauth-
tokens/990cb3e61414376554a39e390471fff0
```

反向代理 SSO 故障排除

Splunk Web 提供一个界面，通过此界面可分析环境和运行时数据来帮助您调试部署。可以通过代理或直接 URL 访问此页面。如果您未通过代理服务器访问此页面，则请求头不可用。

+Splunk 建议在故障排除完成后禁用此设置。

此 URL 位于：

```
http://YourSplunkServer:8000/debug/sso
```

重要提示：默认情况下，调试页面不可用。为了使页面可用，必须完成两个步骤。首先，正在访问此端点的角色必须具有 `web_debug` 功能，该功能默认情况下管理员角色已具备。第二，在 `web.conf` 中，必须配置 `enableWebDebug=true` 设置。在完成故障排除后，应立即禁用此设置。

使用故障排除页面分析您的部署时请注意以下问题：

- 将作为 **Splunk 受信任 IP** 提供的 IP 与**主机 IP**的 IP 进行比较。两个值必须相同（它们应是您代理的 IP）。如果它们在故障排除页面中互不相同，则必须编辑 `trustedIP` 值（位于 `server.conf`）。
- 在值中检查 **Splunkweb 收到的传入请求 IP**，确保它显示的是您客户端的 IP 地址。如果此 IP 与您客户端的 IP 不匹配，您必须：
  - 编辑 `web.conf` 以将其矫正。
  - 确保 `tools.proxy.on` 设置为 `true`。
- 确保您的代理提供标头。请检查**其他 HTTP 标头**下方的**授权**字段。如果没有值呈现，则在代理中检查 `http.conf` 文件，以确保远程标头属性值正确设置。Splunk 软件配置为接受 `REMOTE_USER` 的远程标头值，这在默认情况下用于大多数代理。如果您的代理远程标头有所不同，而您想要保留此值，则可以在 `web.conf` 中编辑远程标头值以更改 Splunk 软件可以接受的标头。有关更多信息，请参阅“配置 SSO”。
- 确保 Splunk Web 创建发送到 splunkd 的 cookie。检查**其他 HTTP 标头**下方的 **Cookie** 字段，确保设置了 cookie。如果 cookie 未设置，则可以查看 `web.conf` 文件以确保文件正确配置。有关更多信息，请参阅“配置 SSO”。

脚本式验证

设置使用外部系统进行的用户验证

您的用户验证选项有：

- Splunk 验证
- LDAP
- 单点登录
- 用于外部验证系统的脚本式验证 API，例如 PAM 或 RADIUS，如本节所述。

重要提示：Splunk 验证优先于任何外部系统。

以下是 Splunk 软件验证 LDAP 用户的顺序：

1.Splunk 验证或 SSO。

2.LDAP 或脚本式验证（如启用）。有关 LDAP 的更多信息，请参阅"设置使用 LDAP 进行的用户验证"。

脚本式验证如何工作

在脚本式验证中，用户生成的 Python 脚本充当 Splunk 服务器和诸如 PAM 或 RADIUS 等外部验证系统之间的中介。

API 由处理 Splunk 软件和验证系统之间通信的一些功能组成。您需要使用实现这些功能的处理程序创建脚本。

要将验证系统与 Splunk Enterprise 集成在一起，请确保验证系统正在运行，然后执行以下操作：

1.创建 Python 验证脚本。有关过程，请参阅"创建验证脚本"。

2.通过编辑 authentication.conf 启用脚本，指定脚本式验证和相关设置。有关过程，请参阅"编辑 authentication.conf"。

示例

Splunk 提供了多个示例验证脚本和相关的配置文件，其中一组用于 RADIUS，另一组用于 PAM。还有一个称为 `dumbScripted.py` 的简单脚本，一般专注于脚本和 Splunk 部署之间的交互。

您可以从示例脚本和配置文件开始创建您自己的脚本。您必须针对自己的环境修改它们。

您可以在 `$SPLUNK_HOME/share/splunk/authScriptSamples/` 中找到这些示例。该目录还包含具有示例信息的"自述"文件，以及有关在 Splunk Enterprise 和外部系统之间设置连接的其他信息。

重要提示：这些脚本用作您可以根据需要进行修改或扩展的示例。它们不受支持，并且不能保证它们将完全满足您的验证和安全需求。

创建验证脚本

要将验证系统与 Splunk 部署集成在一起，请确保验证系统正在运行，然后执行以下操作：

1.创建 Python 验证脚本。有关过程，请参阅本主题的"创建 Python 脚本"。

2.测试新脚本。有关过程，请参阅本主题的"测试脚本"。

3.通过编辑 authentication.conf 启用脚本，指定脚本式验证和相关设置。有关过程，请参阅"编辑 authentication.conf"。

创建 Python 脚本

您必须创建实现以下验证函数的 Python 脚本：

- userLogin
- getUserInfo
- getUsers

Splunk 服务器将根据需要调用这些函数，以验证用户登录或获取有关用户角色的信息。

脚本也可以选择包括此函数的处理程序：

- getSearchFilter

下表汇总了验证函数、其参数以及其返回值：

函数	描述	参数字符串	返回值字符串

`userLogin`	使用用户凭据登录。	`--username=<username>`
		`--password=<password>`
		（`stdin` 上方通过的值，一行占一个）
			失败
			（`stdout` 上方安全通过）

getUserInfo	返回用户信息，其中包括名称和角色。	--username=<username>	--status=success|fail -- userInfo=<userId>;<username>;<realname>;<roles> 请注意以下事项： • userInfo 必须指定一个分号分隔的列表。 • <userId> 已弃用，您应该只返回相关的分号。 • <username> 为必填。 • <realname> 为可选，但其分号为必填。 • <roles> 为必填。要返回多个角色，使用冒号分隔角色。 例如：admin:power • 本示例只返回名为 "docsplunk" 的用户的角色： --status=success -- userInfo=;docsplunk;;admin:power
getUsers	返回所有 Splunk 用户的信息。	无	--status=success|fail -- userInfo=<userId>;<username>;<realname>;<roles> -- userInfo=<userId>;<username>;<realname>;<roles> -- userInfo=<userId>;<username>;<realname>;<roles> ... 请注意以下事项： • 请查看有关语法的 getUserInfo 信息，以返回每个用户的信息。 • 使用空格分隔每个用户的信息。 • <roles> 为必填。要返回多个角色，使用冒号分隔角色。 例如：admin:power
getSearchFilter	可选。返回专门应用于此用户的过滤器，以及应用于用户角色的过滤器。过滤器以 OR 连接在一起。	--username=<username>	--status=success|fail --search_filter=<filter> --search_filter=<filter> ... **注意：**基于用户的搜索过滤器是可选的，并且不建议使用。更好的方法是将搜索过滤器分配给角色，然后将用户分配给相应的角色。 有关更多信息，请参阅"在搜索时使用 getSearchFilter 函数筛选"

有关如何实现以下函数的详细信息，请参阅示例脚本。

测试脚本

由于 Splunk 部署和脚本之间通过 stdin 和 stdout 通信，所以您可以使用命令 shell 通过交互方式测试脚本。一定要每行发送一个参数，并且用 EOF (Ctrl-D) 结束每个函数调用。

使用以下模式单独测试每个函数：

```
> python [script] [function name]
[pass arguments here, one per line]
[send eof, with Ctrl-D]
[output appears here, check that it's correct]
>
```

以下示例显示通过两个用户 "alice" 和 "bob" 对名为 "example.py" 的虚构脚本执行一些简单测试的调试会话。"alice" 是"管理员"和"高级用户"角色的成员，"bob" 是"普通用户"角色的成员。

```
> python example.py userLogin
--username=alice
--password=correctpassword
<send an EOF>
```

```
--status=success
> python example.py userLogin
--username=bob
--password=wrongpassword
<send an EOF>
--status=fail
> python example.py getUsers
<no arguments for this function, send an EOF>
--status=success --userInfo=bob;bob;bob;user --userInfo=alice;alice;alice;admin:super
> python example.py getUserInfo
--username=bob
<send an EOF>
--status=success --userInfo=bob;bob;bob;user
> python example.py getUserInfo
--username=userdoesnotexist
<send an EOF>
--status=fail
>
```

重要提示：本例只是有关如何测试脚本的示例，并不尝试执行任何真实脚本的详尽测试。

编辑 authentication.conf

要将验证系统与 Splunk 部署集成在一起，请确保验证系统正在运行，然后执行以下操作：

1.创建和测试 Python 验证脚本。有关过程，请参阅"创建验证脚本"。

2.编辑 authentication.conf 启用验证脚本。请参阅本主题的"启用您的脚本"。

3.编辑 authentication.conf 设置缓存持续时间。请参阅本主题的"设置缓存持续时间"。

启用您的脚本

一旦您创建 Python 脚本以执行验证，请更新 `authentication.conf`（位于 `$SPLUNK_HOME/etc/system/local/`）以启用您的脚本。您还可以复制和编辑一个示例 `authentication.conf`（来自 `$SPLUNK_HOME/share/splunk/authScriptSamples/`）。

指定 `Scripted` 为您的验证类型（在 `[authentication]` 段落头下方）：

```
[authentication]
authType = Scripted
authSettings = script
```

在 `[script]` 段落头下方设置脚本变量。例如：

```
[script]
scriptPath = $SPLUNK_HOME/bin/python $SPLUNK_HOME/bin/<scriptname.py>
```

设置缓存持续时间

要在使用脚本式验证时显著提高验证性能，请启用 Splunk 验证缓存。您可以通过添加可选的 `[cacheTiming]` 段落来完成。每个脚本功能（除了 `getSearchFilter`）都具有可设置的 `cacheTiming` 属性，它能够为该功能打开缓存，并指定其缓存持续时间。比如，要为 `getUserInfo` 功能指定缓存时间，请使用 `getUserInfoTTL` 属性。只有在指定其相关的属性时才缓存函数。

`cacheTiming` 设置指定 Splunk 软件调用脚本以与外部验证系统通信的频率。您可以按秒、分钟、小时、天等指定时间。通常，将缓存频率限制为秒或分钟。如果未指定单位，则值默认为秒。因此，值 "5" 相当于 "5s"。

本例所示为缓存的典型值：

```
[cacheTiming]
userLoginTTL    = 10s
getUserInfoTTL  = 1m
getUsersTTL     = 2m
```

您将设置 `userLoginTTL` 为较低值，因为这样能够决定用户登录/密码有效性缓存的时长。

要立刻刷新所有缓存，请使用 CLI 命令 `reload auth`：

```
./splunk reload auth
```

注意：此命令不会使当前用户从系统中注销。

还可以在 Splunk Web 中刷新缓存：

1.在**系统**菜单的**用户和验证**下方，选择**访问控制**。

2.单击**验证方法**。

3.单击**重新加载验证配置**刷新缓存。

每个指定的功能（除了 `getUsers`）对于每个用户都具有单独的缓存。所以，如果您有 10 个用户登录并指定 `getUserInfoTTL` 属性，则 `getUserInfo` 功能将具有 10 个基于用户的缓存。`getUsers` 功能包含所有用户，因此是单个的全局缓存。

使用 PAM 验证

您可以通过位于 `$SPLUNK_HOME/share/splunk/authScriptSamples/` 中示例目录的“自述”(README) 的如下步骤配置 Splunk Enterprise 以使用 PAM。

如果您仍旧无法验证，请编辑 `/etc/pam.d/pamauth` 并添加此行：

```
auth sufficient pam_unix.so
```

在搜索时使用 getSearchFilter 函数筛选

此函数是可选的，可用于在搜索时实现基于用户的筛选。启用 `getSearchFilter` 后，每次运行搜索，Splunk 软件就将其调用。基于用户的搜索过滤器可以补充为该用户角色指定的过滤器。返回的过滤器将应用于每个搜索，以及在角色级别配置的搜索。此函数没有过滤器缓存。

注意：基于用户的搜索过滤器是可选的，并且不建议使用。更好的方法是将搜索过滤器分配给角色，然后将用户分配给相应的角色。

要启用 `getSearchFilter` 功能，请设置 `scriptSearchFilters` 参数（位于 `authentication.conf`）：

```
[script]
scriptPath = $SPLUNK_HOME/bin/python $SPLUNK_HOME/bin/<scriptname.py>
scriptSearchFilters = 1
```

注意：在之前的版本中，`getSearchFilter` 也可以用于为通过 Splunk 软件验证的用户执行搜索过滤器职能。从 4.2 版本开始，Splunk 仅为通过脚本式验证的用户调用 `getSearchFilter`。

此外，如果调用 `getSearchFilter` 失败，Splunk Enterprise 将取消用户的搜索并返回一个错误消息，以确保用户无法查看未经授权的搜索结果。

使用 SSL 确保 Splunk Enterprise 通信安全

关于使用 SSL 确保 Splunk Enterprise 安全

本部分介绍您可能希望使用 SSL 来确保安全的 Splunk 配置类型。

关于默认证书

Splunk 软件随附了（并已配置为使用）一组默认证书。使用默认证书将阻止偶然遇到的窥探者，但您仍然容易受到攻击，因为每次 Splunk 下载的根证书都是相同的，任何拥有此相同根证书的人员都可以通过验证。

启动时生成和配置默认证书并位于 `$SPLUNK_HOME/etc/auth/`。它们设置为在生成三年后过期，并且那时必须创建和配置新证书。

- 有关 Splunk Web 默认证书的信息，请参阅“通过 Splunk Web 启用加密 (https)”或“使用 web.conf 启用加密 (https)”。
- 有关配置 SSL 使用默认证书进行转发的信息，请参阅“将 Splunk 转发配置为使用默认证书”。

确保 Splunk Enterprise 安全的方法

您可以使用自己的证书应用加密和/或验证：

- 浏览器与 **Splunk Web** 之间的通信
- Splunk **转发器**与**索引器**之间的通信
- 其他类型的通信，例如通过管理端口的 Splunk 实例之间的通信

下表描述了最常见方案和默认 SSL 设置：

交换类型	客户端功能	服务器功能	加密	证书验证	公用名检查	交换的数据类型
浏览器到 Splunk Web	浏览器	Splunk Web	默认情况下不启用	由客户端（浏览器）指定	由客户端（浏览器）指定	搜索术语结果
Splunk 间通信	Splunk Web	`splunkd`	默认情况下启用	默认情况下不启用	默认情况下不启用	搜索术语结果
转发	`splunkd` 用作转发器	`splunkd` 用作索引器	默认情况下不启用	默认情况下不启用	默认情况下不启用	要索引的数据
索引器的部署服务器	`splunkd` 用作转发器	`splunkd` 用作索引器	默认情况下不启用	默认情况下不启用	默认情况下不启用	不推荐。改用 Pass4SymmKey。

浏览器与 Splunk Web 之间的通信

浏览器与 Splunk Web 之间的数据通常包括搜索请求和返回的数据。

数据加密 (HTTPS) 可以轻松地使用 Splunk Web 或通过编辑**配置文件**启用。记住，使用默认证书的加密可防止偶然的侦听，但也并不绝对安全。

要获得更好的安全性，应将默认证书替换为由受信 CA 签名的证书。在这种情况下，我们强烈建议使用 CA 证书，而不是签署您自己的证书。如果您无法将您的 CA 添加到将访问 Splunk Web 的每个浏览器的证书库中，自签名证书将被用户的浏览器视为不可信。有关更多信息，请参阅"关于确保 Splunk Web 安全"。

Splunk 转发器到索引器

从转发器发送到索引器的数据将被索引器用于搜索和报表。根据贵组织、所传输数据的性质和格式以及 Splunk 配置，该数据可能是可读或敏感数据，也可能不是可读或敏感数据。

确保敏感的原始数据安全有助于避免窥探和中间人攻击。

您可以使用默认证书启用 SSL 加密并提供加密和压缩。但是，使用默认证书进行通信并不提供安全验证，因为证书密码随 Splunk 软件的每个安装一起提供。将默认证书设置为在原始启动后三年到期，届时转发器与索引器之间将无法通信。

为了提高安全性，需要使用自签名证书或 CA 签名证书进行证书验证。外部方认为由已知且相互信任的证书颁发机构签名的证书要比您自己签名的证书更为安全。有关对 Splunk 转发器和索引器使用证书的详细信息，请参阅"关于确保来自转发器的数据安全"。

其他 Splunk SSL 通信

其他 Splunk 通信是指不同的 Splunk 软件实例之间通过管理端口进行的通信，这种通信通常（但不总是）发生在分布式环境中。一个相关示例是由部署服务器发送到客户端的配置数据。

默认情况下，此方案中的 SSL 加密已启用。这足以适用于大部分配置；建议采用此安全类型。不过，如果您需要使用 SSL 验证确保通信安全，可参阅本手册"关于确保 Splunk 与 Splunk 间通信安全"中提供的一些指导原则以获得帮助。

获取您的证书

如果您对 SSL 证书很熟悉，可以照常创建这些证书，然后直接将您的 Splunk 实例配置为使用它们。

如果您需要帮助获取全部证书，可参考提供的几个非常简单的 OpenSSL 命令使用示例。（OpenSSL 随 Splunk 软件一起提供）

- 如何自签名证书
- 如何获取第三方证书
- 如何自签名 Splunk Web 的证书
- 如何获取 Splunk Web 的第三方证书

获得证书后的操作

有关在您获得证书后将 Splunk 软件配置为使用您的证书的更多信息，请参阅下列主题：

- 使用您自己的证书确保 Splunk Web 安全
- 将 Splunk 转发配置为使用您自己的证书
- 关于确保 splunk 间通信安全

关于在 Windows 和 Linux 上使用 SSL 工具

本手册介绍如何将 Splunk 部署配置为使用默认证书、自签名证书或证书颁发机构签名的证书。对于可能尚未获得证书的人员，我们还提供了有关使用命令行和与 Splunk 软件一起打包的 OpenSSL 版本生成证书和密钥的简单示例。

使用 OpenSSL 命令行示例

本手册提供了几个有关在命令行中使用 OpenSSL 的 Splunk 版本创建证书的基本示例。要执行这些任务，您必须具有 root 管理员权限。如果您是在远程或虚拟机上操作，可能需要执行额外步骤以确保能够执行所有任务：

- 在 Windows 平台上操作时，可能需要以管理员身份打开命令行：在“开始”菜单中，右键单击 .exe 应用程序并选择**以管理员身份运行**。
- 在 *nix 平台上操作时，您可能需要使用 sudo 以 root 管理员身份登录。

有关 Windows 与 *nix 之间区别的更多信息，请参阅《管理指南》。

关于 SSL 工具

Splunk 软件随附在 `$SPLUNK_HOME/splunk/lib` 中 OpenSSL 的最新版本。对于 6.0，Splunk 支持启用了 FIPS 140-2 的 OpenSSL。

可用于创建和设置证书的其他各种 SSL 工具需要购买和下载。如果您选择使用 OpenSSL 来配置证书，我们强烈建议您使用 Splunk 随附的版本，以避免兼容性问题。要确保您正在使用 Splunk 软件随附的版本，请将环境设置为 Windows `$SPLUNK_HOME/splunk/lib` 或 `$SPLUNK_HOME\splunk\bin` 中的版本。

以下是 *nix 中的库路径的示例：

```
export LD_LIBRARY_PATH=$SPLUNK_HOME/splunk/lib
```

以下是 Windows 中的库路径的示例：

```
set PATH = %PATH%;%SPLUNK_HOME%\bin
```

关于 FIPS

FIPS 使用某些算法的政府认证版本来符合法规指导原则。它本身不会被视为安全性的增强，因此可能会使您的系统变缓。确保在您的环境有相关法规要求时才启用 FIPS。

如果您在考虑是否启用 FIPS，应牢记以下几点：

- Splunk 仅在 Linux、Windows 和 Solaris 上支持启用 FIPS 140-2（64 位 x86) 的 OpenSSL。
- Splunk Enterprise 支持 OpenSSL Canister FIPS 证书编号 1747 和 2398。
- 虽然默认情况下禁用 FIPS，但您在内核处于 FIPS 模式下的 Linux 计算机上运行 Splunk 软件时会自动启用 FIPS。
- 在 Splunk 软件用于运行应用的 Python 的实例中，FIPS 模块会禁止使用一些加密算法（例如 md5 和 rc4）。请确保您要运行的 Splunk 应用经过认证可在 FIPS 模式下运行，并且与上述算法没有依存关系。

启用 FIPS：

在您首次启动 Splunk Enterprise 之前，请编辑 `$SPLUNK_HOME/etc/splunk-launch.conf` 以添加如下行：

```
SPLUNK_FIPS=1
```

注意：安装 Splunk 软件的非 FIPS 版本后，无法将其升级到 FIPS 版本。如果您需要 FIPS 合规性，请确保您的初始 Splunk 安装已启用 FIPS。

配置允许的和限制的 SSL 版本

Splunk Enterprise 6.2 提供 `sslVersions` 关键字来限制协议的旧版本。SSLv3 即可使用以支持简易的升级，但会在升级完成时禁用。默认情况下，Splunk Enterprise 允许 SSLv3 和所有后续版本上的通信。

当 Splunk Enterprise 在 FIPS 模式配置时，无论是否有任何其他配置，SSLv2 和 SSLv3 始终禁用。

警告：要避免 v3 "POODLE" 漏洞，请在将升级应用于您的环境时移除 SSLv3。

配置 `web.conf`

1.在 `web.conf` 中更新 `sslVersions` 属性以列出或限制想要允许的版本（用逗号隔开）。默认情况下此属性设置为 `*,-sslv2`，该版本比 SSLv2（不建议使用）新。对于 6.2，允许的 SSL 版本为：

- SSLv2（不建议使用）
- SSLv3（不建议使用）
- TLS1.0（不建议使用）
- TLS1.1
- TLS1.2

例如：

```
sslVersions = tls1.1, tls1.2
```

语法选项

要选择所有支持的版本，使用 "*"：

```
sslVersions = *
```

要包括所有版本 tls1.0 或更新版本，使用 "tls"：

```
sslVersions = tls
```

要限制特定版本，请使用 "-" 进行前缀：

```
sslVersions = *, -ssl3
```

注意：当 Splunk Enterprise 在 FIPS 模式配置时，无论是否有此配置，SSLv2 和 SSLv3 始终禁用。

2.在 `inputs.conf` 中更新 `sslVersions` 属性以列出或限制想要 Splunk Enterprise 支持的版本（用逗号隔开）。

```
sslVersions = ssl2, tls1.1, tls1.2
```

您可使用 "*" 选择所有支持的版本：

```
sslVersions = *
```

只需使用 "tls" 包括所有版本 tls1.1 或更新版本：

```
sslVersions = tls
```

使用 "-" 作为版本前缀，以限制某个特定版本：

```
sslVersions = *, -ssl3
```

3.配置转发器，使其与您的索引器兼容。更改或限制 SSL 版本（并限制 SSLv3）可能会出现与转发器兼容问题，尤其是那些运行较早版本的 Splunk Enterprise 的转发器。对于运行 6.2 的转发器，除了索引器外，您还可以通过更新每个转发器的 `inputs.conf` 和 `web.conf` 设置来解决兼容性问题。

更新任何转发器到 6.2，以与您的索引器和 SSL 设置一致（对于向后兼容性，6.0 可支持 tls1.1 之前的所有版本）。

配置 `server.conf`

配置 `server.conf` 文件以接受与客户端的连接（比如 `web.conf`），方法是编辑 `sslVersions` 属性使它与客户端相同。

例如：

```
[sslConfig]
sslVersions = tls1.1, tls1.2
```

确保浏览器和 Splunk Web 间的通信安全

关于确保 Splunk Web 安全

传输到 **Splunk Web** 的信息主要是由搜索请求和结果组成的。

请注意，浏览器与 Splunk Web 之间的传输并不总是需要进行保护。例如，如果用户只是从本地浏览器访问 Splunk Web，并且该本地浏览器与 Splunk Web 设置了相同防火墙，此时可能就不需要担心安全问题。在这种情况下，可能只需使用 Splunk 的默认证书进行加密就足够了。

- 有关 Splunk Web 默认证书的信息，请参阅通过 Splunk Web 启用加密 (https) 或使用 web.conf 启用加密 (https)
- 有关配置 SSL 使用默认证书进行转发的信息，请参阅将 Splunk 转发配置为使用默认证书。

要启用基本加密，请参阅通过 Splunk Web 启用加密 (https)。

另一方面，如果您的 Splunk 配置采用分布式环境（即，可以从各种不同位置的防火墙外部的浏览器访问 Splunk Web），应该使用签名证书实现更高的安全性。有关配置 Splunk Web 使用签名证书的信息，请参阅使用您自己的证书确保 Splunk Web 安全。

您可以通过多种方式使用签名证书来提高浏览器与 Splunk Web 间通信的安全性：

- **对于使用验证的安全加密，可将默认证书替换为签名证书。**
  将 Splunk 提供的默认证书替换为您从受信任证书颁发机构请求的证书。如果担心安全问题，这是建议使用的最安全的选择。
  有关更多获取 Splunk 部署 CA 证书的信息，请参阅“获取 Splunk Web 的第三方签名证书”。
  请注意，您还可以使用自签名证书确保验证的安全，然而，因为它们是由您而不是知名和受信任的证书颁发机构来签名，因此浏览器不会将您作为 CA 储存在证书库中，因而也不会信任您或您的证书。要使自签名证书生效，您需要能够将证书添加到将访问 Splunk Web 的每个单独浏览器的证书库中。
  有关更多创建 Splunk 部署自签名证书的信息，请参阅 Splunk Web 的自签名证书。

- **如果您使用签名证书，可以通过启用公用名检查进一步加强 SSL 配置。**
  公用名检查要求各通信实例证书中所提供的公用名必须匹配，因此又增加了一层安全性。设置证书时，您可以启用公用名检查并配置 Splunk Enterprise 在验证时检查该公用名。

有关配置 Splunk Enterprise 使用证书，以及有关公用名检查的更多信息，请参阅使用您自己的证书确保 Splunk Web 安全。

通过 Splunk Web 启用加密 (https)

本主题介绍如何使用 Splunk Web 为浏览器与 Splunk Web 间的通信启用 HTTPS。Splunk 软件可以侦听 HTTPS 或 HTTP，但不能同时侦听二者。

在 Splunk Web 上可以启用的简单加密使用“现成”安装中所提供的默认证书。由于每个安装所提供的默认证书都是相同的，因此该方法并不是很安全。如果安全性是首要考虑的重要问题，请更改默认证书并对验证进行配置，以实现更好的安全性。有关替换默认证书的信息，请参阅使用您自己的证书确保 Splunk Web 安全。

通过 Splunk Web 启用 HTTPS：

1. 在 Splunk Web 中，选择**设置 > 系统 > 服务器设置**，然后单击**常规设置**。

2. 在 **Splunk Web** 下，对于**在 Splunk Web 中启用 SSL (HTTPS)**，选择**是**单选按钮。

默认情况下，在启用加密时，Splunk 部署指向默认证书，因此无需其他操作。

3. 重新启动 Splunk Web。

现在，您必须将 "https://" 预加到用于访问 Splunk Web 的 URL。

使用 web.conf 启用加密 (https)

您可以通过 `web.conf` 配置文件启用 HTTPS。如果在您的本地目录中尚未显示，请将文件的默认版本从 `$SPLUNK_HOME/etc/system/default` 复制到本地目录 `$SPLUNK_HOME/etc/system/local/` 或 `$SPLUNK_HOME/etc/apps/` 中自定义应用程序目录。有关配置文件的一般信息，请参阅“关于配置文件”。

根据此处所述任务启用的加密并不安全。如果安全性是首要考虑的重要问题，请更改默认证书并对验证进行配置，以实现更好的安全性。有关替换默认证书的信息，请参阅使用您自己的证书确保 Splunk Web 安全。

要通过 `web.conf` 启用 HTTPS：

1. 设置 `enableSplunkWebSSL` 属性为 `true`：

```
[settings]
httpport = <https port number>
enableSplunkWebSSL = true
```

注意：默认情况下，在启用加密时，Splunk 软件会指向默认证书。

2. 重新启动 Splunk。

现在，您必须将 "https://" 预加到用于访问 Splunk Web 的 URL。

使用您自己的证书确保 Splunk Web 安全

本例假定您已经生成了自签名证书或已经购买了第三方证书。如果您还没有这样做，而且不确定如何继续操作，可参考我们提供的一些简单示例：

- 自签名 Splunk Web 的证书。
- 获取 Splunk Web 的第三方签名证书。

注意：Splunk Web 当前不支持带密码保护的专用密钥。在配置 Splunk Web 的证书之前，应先删除密钥中的密码。

开始之前：将证书复制到新文件夹

复制服务器证书至 `$SPLUNK_HOME/etc/auth/splunkweb` 或 `$SPLUNK_HOME/etc/auth` 中自身的证书存储库。

在下例中，我们的网络证书称为 `mySplunkWebCertificate.pem` 并且专用密钥称为 `mySplunkWebPrivateKey.key`：

*nix：

```
# cp $SPLUNK_HOME/etc/auth/mycerts/mySplunkWebCertificate.pem
$SPLUNK_HOME/etc/auth/mycerts/mySplunkWebPrivateKey.key
$SPLUNK_HOME/etc/auth/splunkweb
```

Windows：

```
copy $SPLUNK_HOME\etc\auth\mycerts\mySplunkWebCertificate.pem $SPLUNK_HOME\etc\auth\splunkweb\

copy $SPLUNK_HOME\etc\auth\mycerts\mySplunkWebPrivateKey.key $SPLUNK_HOME\etc\auth\splunkweb\
```

注意：请勿覆盖或删除 `$SPLUNK_HOME/etc/auth/splunkweb/` 中现有的证书。此位置中的证书是在启动时自动生成的，这意味着您所做的任何更改将在启动时被覆盖。在后续步骤中，我们将重写相关配置文件以使其指向新的证书位置。

将 Splunk Web 配置为使用密钥和证书文件

注意：Splunk Web 不支持专用密钥密码，因此您必须删除密钥中的密码才能使用此密钥来确保 Splunk Web 安全。

1.在 `$SPLUNK_HOME/etc/system/local/web.conf`（如果您正在使用的是部署服务器，则可能是其他适用性位置）中，确保对 `[settings]` 段落进行下列修改：

以下是已编辑 settings 段落的示例：

```
[settings]
enableSplunkWebSSL = true
privKeyPath = </home/user/certs/myprivatekey.pem> Absolute paths may be used. non-absolute paths are relative to
$SPLUNK_HOME
serverCert = </home/user/certs/mycacert.pem. Absolute paths may be used. non-absolute paths are relative to
$SPLUNK_HOME
```

2.重新启动 Splunk Web：

```
# $SPLUNK_HOME/bin/splunk restart splunkweb
```

Splunk Web 验证问题故障排除

如果您无法验证证书配置，则可以使用 `web_service.log`（位于 `$SPLUNK_HOME/var/log/splunk`）查看重启时出现的任何错误讯息并排除故障。

查找 SSL 配置警告。比如，如果您提供的 `serverCert` 中声明的服务器证书路径不正确，则 Splunk Web 将无法启动并会出现以下错误信息：

```
2010-12-21 16:25:02,804 ERROR [4d11455df3182e6710] root:442 - [Errno 2] No such file or
directory: '/opt/splunk/share/splunk/mycerts/mySplunkWebCertificate.pem'
```

注意：如果 `privKeyPath` 中提供的密钥带密码保护，则不会提供任何错误讯息，但您的浏览器也不会加载 Splunk Web。

有关删除密码的信息，请参阅自签名 Splunk Web 的证书或获取 Splunk Web 的第三方签名证书。

确保 Splunk 转发器与索引器之间的通信安全

关于确保来自转发器的数据安全

转发器会将原始数据发送到**索引器**。该数据容易遭到窥探和损坏。如果在封闭或共用网络外部转发数据，或者如果数据非常敏感，应使用 SSL 证书来确保数据安全。

使用默认证书将阻止临时窥探者，但您仍然容易受到攻击，因为每次下载的根证书都是 Splunk 软件随附的根证书，

任何拥有此根证书的人员都可以通过验证。启动时生成和配置默认证书并位于 `$SPLUNK_HOME/etc/auth/`。

重要提示：如果您使用默认证书，切记将这些证书设置为在生成后的三年后到期，届时您必须使用本手册中介绍的一种方法来创建和配置新的证书。

有关使用默认证书设置 SSL 的信息，请参阅将 Splunk 转发配置为使用默认证书。

为确保任何人都不会很容易窥探到您的流量或将数据发送到您的索引器，我们建议您使用新的签名证书（自签名证书或从第三方证书颁发机构购买的证书）。要将转发器和索引器配置为使用证书，请参阅将 Splunk 转发配置为使用您自己的证书。

您可以通过多种方式使用自签名证书或 CA 签名证书来提高转发器与索引器之间的安全性：

- **可将默认证书替换为您自己的根 CA 签名的证书。**
  将 Splunk 提供的默认证书替换为您自己生成并签名的证书。有关生成和自签名证书的信息，请参阅如何自签名证书。
- **可将默认证书替换为由受信任证书颁发机构签名的证书。**
  请参阅如何获取第三方签名的证书。
- **可通过配置公用名检查进一步加强安全性。**
  公用名检查要求每个索引器证书中所提供的公用名与转发器配置文件中指定的公用名匹配，进而又增加了一层安全性。还可以使用不同的公用名配置多个证书，并将其分发到索引器。应在设置证书时启用公用名检查。有关更多信息，请参阅将 Splunk 转发配置为使用您自己的证书。

将 Splunk 转发配置为使用默认证书

每次下载时的根证书都是 Splunk 软件随附的默认根证书。这意味着已下载 Splunk 软件的任何人的服务器证书都具有相同根证书的签名，他们都可以通过您证书的验证。为确保任何人都无法轻易窥探到您的流量或不当地将数据发送到您的索引器，我们建议您将这些证书替换为签名证书。

重要提示：将默认证书设置为在这些证书生成后三年到期，届时必须使用本手册中介绍的一种方法来创建和配置新的证书。

要将转发器配置为使用您自己的根 CA 或第三方 CA 签名的证书，请参阅将 Splunk 转发配置为使用您自己的证书。

在本主题中，我们介绍如何：

- 将索引器配置为使用 Splunk 软件随附的默认证书
- 将转发器配置为使用 Splunk 软件随附的默认证书

注意：配置多个转发器时，应分别将每个转发器都配置为使用默认证书。

将索引器设置为使用默认服务器证书

1.在 `$SPLUNK_HOME/etc/system/local/inputs.conf`（或您正在用于分发转发配置的任何应用的相应目录）中，设置以下段落：

在本例中，我们使用端口 9997 从转发器接收数据。

```
[SSL]
rootCA = $SPLUNK_HOME/etc/auth/cacert.pem
serverCert = $SPLUNK_HOME/etc/auth/server.pem
password = password
requireClientCert=false
[splunktcp-ssl:9997]
disabled=0
```

其中 `rootCA` 是 CA 公共密钥的路径，而 `serverCert` 是默认服务器证书的路径。

默认证书位于 `$SPLUNK_HOME/etc/auth/server.pem`。

注意：使用默认证书时，无需设置 `requireClientCert = true`，这是因为我们无需检查默认服务器证书的有效性。

2.重新启动 splunkd：

$SPLUNK_HOME/bin/splunk restart splunkd

配置转发器

将转发器设置为使用与索引器相同的默认证书，并将转发器配置为将数据发送到配置的侦听端口。

在下例中，索引器 IP 地址为 10.1.12.112。

1.在 $SPLUNK_HOME/etc/system/local/outputs.conf（或您正在用于分发转发配置的任何应用的相应目录）中定义以下段落：

```
[tcpout]
server = 10.1.12.112:9997
sslVerifyServerCert = false
server.conf/[sslConfig]/sslRootCAPath
sslCertPath = $SPLUNK_HOME/etc/auth/server.pem
sslPassword = password
```

其中 rootCA 是 CA 公共密钥的路径，而 serverCert 是默认服务器证书的路径。

请确保 outputs.conf 中的 sslVerifyServerCert 属性与 </code>outputs.conf</code> 中的属性值相同。Splunk Enterprise 建议将此值设置为 false（默认值）。2.重新启动 splunkd：

$SPLUNK_HOME/bin/splunk restart splunkd

后续步骤

接下来，应检查连接以确保配置有效。有关更多信息，请参阅"验证配置"。

将 Splunk 转发配置为使用您自己的证书

本主题介绍如何使用您自己的 SSL 证书将来自转发器的数据发送到索引器。使用证书保护来自转发器的数据有助于确保安全地对正在网络中传输的数据进行加密。本主题介绍以下步骤：

- 按照本主题所述将索引器配置为使用新签名证书。
- 按照本主题所述将转发器配置为使用新签名证书。

开始之前，必须获得并准备好您的证书。确保您的证书是 x509 格式的 PEM 文件并且您的密钥采用 RSA 格式。如果需要帮助，我们提供了几个简单示例，以帮助您创建和准备您自己的证书。有关更多信息，请参阅"关于确保来自转发器的数据安全"和"关于确保 Splunk 间通信安全"。

为了增加安全性，您还可以使用不同的公用名来创建多个证书（由同一 CA 签名），并将这些证书分发给索引器。当给定 CA 的公共密钥时，转发器信任 CA 并验证 CA 的证书，并匹配 sslCommonNameToCheck 或 sslAltNameToCheck

将索引器配置为使用您的证书

1.将服务器证书和 CA 公共证书复制到要配置的索引器上的一个可访问文件夹中。例如：$SPLUNK_HOME/etc/auth/mycerts/

警告：如果在应用目录中配置 inputs.conf 或 outputs.conf，密码不会进行加密，并且纯文本值仍保留在文件中。因此，您可能希望创建不同的证书（由同一根 CA 签名），以便在应用目录中配置 SSL 时使用。

2.在索引器中配置 inputs.conf 以使用新服务器证书。在 $SPLUNK_HOME/etc/system/local/inputs.conf（或您正在用于分发转发配置的任何应用的相应目录）中，设置 [SSL] 段落：

```
[SSL]
rootCA = $SPLUNK_HOME/etc/auth/mycacert.pem <The public CA of the same CA that issued the forwarder's certificate>
serverCert = $SPLUNK_HOME/etc/auth/myservercert.pem <the certificate issued by customer-generated CA>
requireClientCert = false
compressed = false <this attribute must be the same value as the attribute on the forwarder>
[splunktcp-ssl:9996]
```

当您在 $SPLUNK_HOME/etc/system/local/inputs.conf 中编辑文件时，Splunk 软件会对密码进行加密，并覆盖重启 Splunk Enterprise 时所提供的明文服务器证书。

注意：我们不建议您禁用 tls 压缩，因为它可能会导致带宽问题。

3.重新启动 splunkd。

$SPLUNK_HOME/bin/splunk restart splunkd

将转发器配置为使用您的证书

1.生成一个新证书，并将该证书和 CA 公共证书 myCACertificate.pem 复制到计划要配置的转发器上一个可访问的文件夹中。对于本示例，我们将它们置于 $SPLUNK_HOME/etc/auth/mycerts/。

警告：如果在应用目录中配置 inputs.conf 或 outputs.conf，密码不会进行加密，并且纯文本值仍保留在文件中。因此，您可能希望创建不同的证书（由同一根 CA 签名），以便在应用目录中配置 SSL 时使用。

2.在 $SPLUNK_HOME/etc/system/local/outputs.conf（或您正在用于分发转发配置的任何应用的相应目录）中定义 [SSL] 段落：

```
[tcpout:splunkssl]
compressed = false
disabled = false
server = indexer:9997
sslCommonNameToCheck = indexercn.example.org
clientCert = $SPLUNK_HOME/etc/auth/client.pem
server.conf/[sslConfig]/sslRootCAPath <The public certificate of the same CA that issued the indexer's certificate>
sslVerifyServerCert = true
```

注意，当您在 $SPLUNK_HOME/etc/system/local/outputs.conf 中保存文件时，Splunk 会加密并覆盖重启 splunkd 时的明文服务器证书。

3.重新启动 splunkd。

$SPLUNK_HOME/bin/splunk restart splunkd

其他配置选项

将数据转发到多个索引器

要将转发器配置为通过多个索引器的验证，只需将其 HOST:PORT 地址以逗号分隔列表的形式添加到目标组定义段落的 "server" 配置参数中。

以下示例对索引器和转发器使用相同的证书：

```
[tcpout]
defaultGroup = splunkssl

[tcpout:splunkssl]
server = 10.1.12.112:9997,10.1.12.111:9999
compressed = false
disabled = false
server = indexer:9997
sslCommonNameToCheck = indexercn.example.org
sslCertPath = $SPLUNK_HOME/etc/auth/client.pem
sslRootCAPath = $SPLUNK_HOME/etc/auth/mycacert.pem <The public certificate of the same CA that issued the indexer's
certificate>
sslVerifyServerCert = true
```

使用具有不同公用名的证书将数据转发到多个索引器

您可以为每个索引器创建并配置一个服务器证书，方法是在转发器的 outputs.conf 中为每个索引器配置一个特定于服务器的 [SSLConfig] 段落。

如果您为每个索引器创建一个服务器证书，并在每个转发器要查看的索引器证书中设置一个唯一的 sslCommonNameToCheck 或 sslAltNameToCheck，则需要为 outputs.conf 中的每个索引器配置一个 [tcpout-server://HOST:PORT] 配置段落。这样您就可以指定要针对哪个索引器检查哪个名称。

后续步骤

接下来，应检查连接以确保配置有效。有关更多信息，请参阅“验证配置”。

验证配置

部署配置之前，您可以使用 splunkd.log 验证配置并排除故障。Splunkd.log 位于 $SPLUNK_HOME/var/log/splunk/splunkd.log 中的索引器和转发器。

在索引器上，按启动顺序查找以下或类似消息，以验证连接是否成功：

```
02-06-2011 19:19:01.552 INFO TcpInputProc - using queueSize 1000
02-06-2011 19:19:01.552 INFO TcpInputProc - SSL cipherSuite=ALL:!aNULL:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM
02-06-2011 19:19:01.552 INFO TcpInputProc - supporting SSL v2/v3
02-06-2011 19:19:01.555 INFO TcpInputProc - port 9997 is reserved for splunk 2 splunk (SSL)
02-06-2011 19:19:01.555 INFO TcpInputProc - Port 9997 is compressed
02-06-2011 19:19:01.556 INFO TcpInputProc - Registering metrics callback for: tcpin_connections
```

在转发器上，按启动顺序查找以下或类似消息，以验证连接是否成功：

```
02-06-2011 19:06:10.844 INFO TcpOutputProc - Retrieving configuration from properties
02-06-2011 19:06:10.848 INFO TcpOutputProc - found Whitelist forwardedindex.0.whitelist , RE :
forwardedindex.0.whitelist
02-06-2011 19:06:10.848 INFO TcpOutputProc - found Whitelist forwardedindex.1.blacklist , RE :
forwardedindex.1.blacklist
02-06-2011 19:06:10.848 INFO TcpOutputProc - found Whitelist forwardedindex.2.whitelist , RE :
forwardedindex.2.whitelist
02-06-2011 19:06:10.850 INFO TcpOutputProc - Will retry at max backoff sleep forever
02-06-2011 19:06:10.850 INFO TcpOutputProc - Using SSL for server 10.1.12.112:9997,
sslCertPath=/opt/splunk/etc/aut/server.pem
02-06-2011 19:06:10.854 INFO TcpOutputProc - ALL Connections will use SSL with sslCipher=
02-06-2011 19:06:10.859 INFO TcpOutputProc - initializing single connection with retry strategy for 10.1.12.112:9997
```

如需帮助解决配置问题，请参阅本手册中的"转发器与索引器之间配置的故障排除"。

转发器与索引器之间验证的故障排除

1.查看 `$SPLUNK_HOME/var/log/splunk/splunkd.log`（索引器和转发器）的错误讯息。在索引器中查看来自 TCP 输入处理器 `TcpInputProc` 的消息。在转发器中查看来自 TCP 输出处理器 `TcpOutputProc` 的消息。

2.提高 `$SPLUNK_HOME/etc/log.cfg` 中索引器和转发器相应处理器的日志级别。

在转发器中设置 `category.TcpOutputProc=DEBUG` 并在索引器中设置 `category.TcpInputProc=DEBUG`。

3.重新启动 Splunk Enterprise 以使设置生效，并观察相关组件的启动顺序。通过此方法可发现大多数配置问题。

4.使用 `btool` 检查 SSL 配置如下：

在索引器中：

$SPLUNK_HOME/bin/splunk cmd btool inputs list --debug

在转发器中：

$SPLUNK_HOME/bin/splunk cmd btool outputs list --debug

常见问题

- 服务器证书文件路径在 inputs.conf 中设置为 `serverCert` 值是错误的，或文件无法阅读。这样会生成如下错误 ：

12-16-2010 16:07:30.965 ERROR SSLCommon - Can't read certificate file /opt/splunk/etc/auth/server.pem errno=33558530 error:02001002:system library:fopen:No such file or directory

- 服务器证书文件中包含的 RSA 专用密钥的密码不正确。

12-07-2010 07:56:45.663 ERROR SSLCommon - Can't read key file /opt/splunk/etc/auth/server.pem

在 *nix 上，您可以使用以下命令手动测试文件中包含的 RSA 密钥的密码：

openssl rsa -in /opt/splunk/etc/auth/server.pem -text

在 Windows 上，您可以使用以下命令手动测试 RSA 密钥的密码：

>openssl.exe rsa -in "c:\Program Files\Splunk\etc\auth\server.pem" -text

确保分布式环境安全

关于确保 Splunk 间通信安全

本主题介绍下列"Splunk 到 Splunk"通信类型和确保通信类型安全的方法：

- 确保分布式搜索头和对等节点安全
- 确保部署服务器和客户端安全
- 关于确保群集安全

确保分布式搜索头和对等节点安全

分布式搜索配置通过管理端口共享搜索信息、知识对象以及应用和配置信息。

搜索头与对等节点之间的通信依赖于公共密钥加密。启动时，Splunk 软件会在您的 Splunk 安装中生成专用密钥和公共密钥。在搜索头上配置分布式搜索时，搜索头会将公共密钥分布到对等节点，以用于确保通信安全。此默认配置提供了内置加密以及数据压缩，因此可提高性能。

可以用您自己的密钥来换掉这些生成的密钥。但是，建议不要这样做，一般情况下不需要如此操作。要为分布式搜索设置配置公共密钥加密，应创建您自己的密钥并将其分布到搜索头和对等节点。要了解有关将密钥文件分布到分布式搜索节点的更多信息，请查看《分布式搜索手册》中关于配置分布式搜索的部分："分布密钥文件"。

使用证书验证确保部署服务器和客户端安全

不推荐在部署服务器和客户端之间使用签名证书进行认证，因为从部署服务器推送到客户端的配置数据通常不会提供可利用的信息。为部署服务器和客户端配置证书验证会影响其余配置：

- 如果未同时将 Splunk Web 配置为使用证书，Splunk Web 将无法进行验证。
- CLI 将无法与部署服务器进行通信。

不过，在某些分布式配置中，可能需要将极其敏感的服务器配置数据发送到防火墙外部的各种不同位置，此时您可能会发现有必要采用证书验证。您可以手动配置每个索引器以与"部署服务器"通信：

1. 使用相同根 CA 创建一个或多个证书。

2. 将这些证书分布到部署服务器和客户端。

3. 编辑 `server.conf` 以提供证书位置：

```
[sslConfig]
enableSplunkdSSL = true
serverCert = server.pem
sslPassword = password
sslRootCAPath = cacert.pem
absolute path to the cert file
```

4. 编辑 `server.conf` 以通过添加如下属性至之前步骤中的 [sslConfig] 段落来对证书进行验证：

```
requireClientCert = true
```

重要提示： 默认情况下，`requireClientCert` 设置为 "false"。如果将其更改为 true 以强制 Splunk 检查客户端证书，还将检查 Splunk Web 和 CLI 的证书。CLI 连接将不再有效，因为 CLI 无法以客户端身份显示证书。

5. 编辑 `web.conf` 以代表通过相同根 CA 签名的证书，这样 Splunk Web 就可以连接至服务器。

以下是已编辑 settings 段落的示例：

```
[settings]
enableSplunkWebSSL = true
privKeyPath = etc/auth/splunkweb/mySplunkWebPrivateKey.key
serverCert = etc/auth/splunkweb/mySplunkWebCertificate.pem
cipherSuite = <your chosen cipher suite (optional)>
```

注意： Splunk Web 不支持密码，因此必须删除专用密钥中的密码。有关更多信息，请参阅"获取 Splunk Web 的第三方签名证书"。

使用 Pass4SymmKey 确保群集安全

Splunk 提供了一个安全密钥，以允许搜索头或索引器群集节点相互进行验证。设置索引器群集或搜索头群集时，您可以为群集中的每个节点分配相同的密钥。此密钥直接或通过 Splunk Web 或 CLI 在 `pass4SymmKey` 属性（在 `server.conf` 中）中设置。

强烈建议设置此密钥：

请注意，`pass4SymmKey` 控制 intraSplunk 认证，并且不管理用户访问。

为搜索头群集配置 `pass4SymmKey`

部署搜索头群集时，配置 `pass4SymmKey`。请参阅"部署搜索头群集"。

有关在搜索头群集上配置 `pass4SymmKey`（包括如何在部署后将其设置）的详细信息，请参阅"为搜索头群集设置安全密钥"。

为索引器群集配置 `pass4SymmKey`

在部署索引器群集时配置 `pass4SymmKey`，同时启用主节点。请参阅"启用索引器群集主节点"。

有关在索引器群集中设置 pass4SymmKey 的更多详细信息，请参阅“配置安全密钥”。

pass4SymmKey 在应用程序中加密的方式

如果在应用中以明文形式指定 pass4SymmKey（例如 etc/apps/myapp/default/server.conf），则在重新启动时会将混淆版本写入本地文件（在本示例中为 system/local/server.conf）。

打算采用这种行为。通常默认目录中的配置文件为只读，并且信息也会写入可编辑的本地文件。

使用 curl 或 splunkd 端点列出配置时，pass4SymmKey 显示为加密。如果配置位置为只读，则 Splunk 软件同样写入本地。

审计 Splunk Enterprise 活动

使用 Splunk Enterprise 审计您的系统活动

了解系统中正在发生什么对确保其安全非常重要。要充分利用您的系统并确保其安全，我们建议以下最佳做法：

- 定期对 Splunk 访问和审计日志进行检查。
- 定期对 Splunk 服务器审计和安全日志进行检查。
- 定期对所有 Splunk 用户和角色进行检查。

使用审计事件确保 Splunk Enterprise 安全

使用 Splunk 搜索审计日志以查看和告警管理访问：

1.审计用户访问权限

index="_audit" action=log* action="login attempt"

2.查找用户访问 Splunk 的位置：

index="_internal" | eval timestamp=strftime(_time, "%Y-%m-%d %H:%M:%S.%Q") | table timestamp, user, clientip

3.考虑设置管理员用户访问的实时告警：

(index="_audit" action=log* action="login attempt") OR (index="_internal") user=admin

有关创建告警的更多信息，请参阅《告警手册》。

4.您还可以创建收集和显示所选搜索的仪表板，请参阅《仪表板和可视化手册》中的“在 Splunk Web 中构建仪表板”。

管理数据完整性

Splunk Enterprise 数据完整性控制功能提供了一种验证被索引数据完整性的方式。

当您为索引启用数据完整性控制时，Splunk Enterprise 计算每片数据的哈希值并存储这些哈希值（使用 SHA 256），以便稍后回来验证数据的完整性。

如何工作

当您启用数据完整性控制时，Splunk Enterprise 计算每片新索引原始数据的哈希值并写入到 l1Hashes 文件。当数据桶从热滚动到温时，Splunk Enterprise 计算 l1Hashes 内容的哈希值，并将计算的哈希值储存在 l2Hash 中。两个哈希值文件都储存在该数据桶的 rawdata 目录中。

注意，数据完整性控制对于新索引数据进行哈希处理，来自转发器的数据应该受保护并使用 SSL 加密。有关更多信息，请参阅关于使用 SSL 确保 Splunk 安全。

检查哈希值来验证您的数据

要检查 Splunk Enterprise 数据，运行下列 CLI 命令来验证索引或数据桶的完整性：

```
./splunk check-integrity -bucketPath [ bucket path ] [ verbose ]

./splunk check-integrity -index [ index name ] [ verbose ]
```

配置数据完整性控制

要配置数据完整性控制，请编辑 `indexes.conf` 以为每个索引启用 `enableDataIntegrityControl` 属性。所有索引的默认值为 `false`（关闭）。

```
enableDataIntegrityControl=true
```

群集环境中的数据完整性

在群集环境中，群集主节点和所有对等节点必须运行 Splunk Enterprise 6.3 来启用准确的索引复制。从群集主节点向对等节点推送带有数据完整性配置的软件包。

有关管理群集环境中配置的更多信息，请参阅“分布式部署手册”

可选择修改数据切片的大小

默认情况下，数据片大小设为 128kb，这意味着每 128KB 创建一个数据片并进行哈希处理。您可以选择编辑 `indexes.conf` 以指定每个扇区的大小。

```
rawChunkSizeBytes = 131072
```

存储并保护您数据的哈希值

为了达到最佳安全，您可选择在托管数据的系统外部存储您的哈希值，例如不同的服务器。为了避免命名冲突，将您要保护的哈希值存储在不同的目录中。

重新生成哈希值

如果您丢失了数据桶的哈希值，使用下列 CLI 命令来重新生成数据桶或索引的哈希文件。该命令提取嵌入在日志中的哈希值：

```
./splunk generate-hash-files -bucketPath [ bucket path ]  [ verbose ]

./splunk generate-hash-files -index [ index name ] [ verbose ]
```

Splunk Enterprise Security 的最佳实践

危险命令的防护

Splunk Enterprise 包含内置搜索处理语言 (SPL) 防护，当您在不知情的情况下，运行包含可能具有安全性风险命令的搜索时，它会给予警告。当单击的链接或键入的 URL 加载包含风险性命令的搜索时，此警告会出现。

而当您创建特殊搜索时，该警告不会出现。

该警告会提醒您某个恶意用户可能正在进行未授权操作。其他未授权操作包括：

- 复制或传输数据（数据渗透）
- 删除数据
- 覆盖数据

当有恶意人员创建包含渗透或损坏数据命令的搜索时，可能会出现这种情况。然后恶意人员向毫无防范的用户发送搜索链接。该 URL 包含一个查询字符串 (q) 和一个搜索标识符 (sid)，但该 sid 已过期。恶意人员希望此用户会使用该链接，并且搜索将运行。

触发警告的命令

此处列出触发该警告的命令：

- `collect`
- `crawl`
- `dump`
- `delete`
- `input`
- `outputcsv`
- `outputlookup`
- `runshellscript`
- `script`
- `sendalert`

- `sendemail`
- `tscollect`

警告对话框中的操作

Splunk Enterprise 分析风险性命令的搜索，而不立即运行搜索。如果识别出一个或多个风险性命令，则会出现警告对话框。您可以取消、运行或调查该搜索。

取消
: 关闭警告对话框。搜索将不会运行，并且搜索从“搜索”栏中移除。可以通过单击“关闭”按钮 (X) 关闭对话框，同样也可以单击**取消**。

运行
: 运行该搜索。

调查
: 在“搜索”栏中显示搜索，这样您可以查看 SPL。使用此选项复制搜索的语法。发送搜索副本，以及关于链接的数据来源的任何信息到您的系统管理员。

关闭警告

只有具备“写入”权限的用户才能编辑 `web.conf` 文件以关闭警告对话框。

您可以针对某特定命令或所有风险性命令关闭警告。

针对特定命令关闭警告

1. 复制 `commands.conf.spec` 文件（位于 `$SPLUNK_HOME/etc/system/default` 目录）。
2. 在 `$SPLUNK_HOME/etc/system/local` 目录中粘贴文件副本。
3. 搜寻命令，并将设置从 `is_risky = true` 更改为 `is_risky = false`。
4. 重新启动 Splunk Enterprise。

针对所有命令关闭警告

1. 打开 `web.conf` 文件。此文件位于 `$SPLUNK_HOME/etc/system/default/` 目录中。
2. 更改 `enable_risky_command_check` 参数为 `false`。
3. 重新启动 Splunk Enterprise。

另请参阅

在*《管理员手册》*中：

关于配置文件
commands.conf 文件
web.conf 文件

Splunk 服务器令牌

如果令牌已损坏或遭到拒绝，您将从通用转发器的日志中接收到错误消息。如果没有找到错误令牌，那么该转发器将继续尝试使用过期的通用转发器令牌。

要找到丢失的转发器令牌：按如下方式编辑 `SPLUNK_HOME/etc/log.cfg`：

```
category.TcpOutputProc=DEBUG
category.TcpInputConfig=DEBUG
category.TcpInputProc=DEBUG
```

当两个令牌（索引器和转发器的令牌）匹配时，则生成以下消息：

索引器：

```
09-15-2015 13:21:30.746 -0700 DEBUG TcpInputProc -  Forwarder token matched
```

通用转发器：

```
09-15-2015 13:24:00.343 -0700 DEBUG TcpOutputProc - Indexer can use tokens
```

当令牌不匹配时，会生成错误消息，例如：

```
09-15-2015 13:22:01.747 -0700 ERROR TcpInputProc - Exception:  Token not sent by forwarder src=10.140.126.58:51838!
for data received from src=10.140.126.58:51838

09-15-2015 13:52:14.803 -0700 ERROR TcpInputProc - Exception:  Token sent by forwarder does not match configured
```

tokens src=10.140.126.58:51990! for data received from src=10.140.126.58:51990

避免在搜索中使用恶意 CSV 文件

如果您将搜索结果导出为 CSV，然后在 Excel/OpenOffice 中打开，则将执行以 '=' 字符开头的任何字段。

例如：

1.用户运行 stats count | eval trick="=1+1"。

2.用户将结果导出为 CSV 文件。

3.用户在 Excel 中加载新的 CSV 文件。

4.当值应为 '=1+1 时，Excel 中的“字段”值为 2。

为了避免这种情况，您可以执行以下其中一个操作：

- 对于以以下字符开头的任何单元格，请向开头添加一个空格，并移除单元格中的任何制表符字符 (0x09)。
  - =
  - -
  - "
  - @
  - +
- 将以之前列出的字符开头的任何单元格附加撇号 (')。
- 确保用户没有 "export_results_is_visible" 功能（仅限于 6.4 及更高版本）。此功能显示导出结果按钮，如果没有此功能，则根本无法生成 CSV 文件。

附录 A：如何获取 SSL 证书

如何自签名证书

本主题介绍如何使用 OpenSSL 对证书进行自签名以确保转发器与索引器之间以及 Splunk 之间通信安全。

如果您已经拥有所需的证书，或者您知道如何生成所需的证书，可以跳过本主题，直接进入配置步骤（将在本手册的后文中介绍）：

- 如何为 Splunk 准备签名证书
- 将 Splunk 转发配置为使用您自己的证书
- 关于确保 Splunk 间通信安全

自签名证书最适用于组织内部或两个已知实体之间的数据通信。如果出于任何原因您要与未知实体进行通信，我们建议使用 CA 签名的证书来确保数据安全。

开始之前

在此次讨论中，`$SPLUNK_HOME` 指的是 Splunk 安装目录。在 Windows 中，默认情况下 Splunk 软件安装在 `C:\Program Files\splunk`。对于大多数 Unix 平台，默认安装目录为 `/opt/splunk`；对于 Mac OS 则为 `/Applications/splunk`。有关在 Windows 和 *nix 中运行的更多信息，请参阅《管理指南》。

将环境设置为 *nix 中 `$SPLUNK_HOME/lib` 的版本或 Windows 中 `$SPLUNK_HOME\bin` 的版本，以确保使用 Splunk 软件随附的 OpenSSL 版本。为此，您可以：

- 创建证书之前运行数据来源 `$SPLUNK_HOME/bin/setSplunkEnv`。

或

- 导航至 `$SPLUNK_HOME/bin/` 并使用 `./openssl` 以运行证书生成的命令。

为您的证书创建新目录

创建证书时，应创建一个新的工作目录。在我们的示例中，我们正在使用 `$SPLUNK_HOME/etc/auth/mycerts`：

```
# mkdir $SPLUNK_HOME/etc/auth/mycerts
# cd $SPLUNK_HOME/etc/auth/mycerts
```

要确保不会覆盖驻留在 `$SPLUNK_HOME/etc/auth` 中的 Splunk 提供的证书，请在不同的目录中工作。

创建根证书

首先创建一个根证书以用作您的根证书颁发机构。使用此根 CA 对生成的服务器证书进行签名并将其分布到 Splunk

实例。

为您的根证书生成专属密钥。

1.创建一个密钥以对证书进行签名。

在 *nix 中：

```
# openssl genrsa -des3 -out myCAPrivateKey.key 2048
```

在 Windows 中，您可能需要附加 `openssl.cnf` 文件的位置：

```
>openssl genrsa -des3 -out myCAPrivateKey.key 2048
```

2.出现提示时，为密钥创建密码。

完成此步骤时，密钥 `myCAPrivateKey.key` 将出现在您的目录中。

生成证书并签名

1.生成新的证书签名请求 (CSR)：

在 *nix 中：

```
# openssl req -new -key myCAPrivateKey.key -out myCACertificate.csr
```

在 Windows 中：

```
>openssl req -new -key myCAPrivateKey.key -out myCACertificate.csr -config $SPLUNK_HOME\openssl.cnf
```

2.出现提示时，请输入 `$SPLUNK_HOME/etc/auth/mycerts/myCAPrivateKey.key` 中针对密钥创建的密码。

3.提供请求的证书信息，包括公用名（如果您要在 Splunk 配置中使用公用名检查）。

新的 CSR `myCACertificate.csr` 将出现在您的目录中。

4.使用 CSR `myCACertificate.csr` 生成公用证书：

在 *nix 中：

```
# openssl x509 -req -in myCACertificate.csr -sha256 -signkey myCAPrivateKey.key -CAcreateserial -out
myCACertificate.pem -days 1095
```

在 Windows 中：

```
>openssl x509 -req -in myCACertificate.csr -sha256 -signkey myCAPrivateKey.key -CAcreateserial -out
myCACertificate.pem -days 1095
```

5.出现提示时，请输入针对密钥 `myCAPrivateKey.key` 的密码。

新的文件 `myCACertificate.pem` 将出现在您的目录中。这是将分布到 Splunk 实例的公共 CA 证书。

创建服务器证书

现在，您已经创建了一个根证书来充当 CA，必须创建服务器证书并对其进行签名。

重要提示：本例向您显示如何创建新的专用密钥和服务器证书。您可以将此服务器证书分布到所有转发器、索引器以及通过管理端口进行通信的 Splunk 实例。如果您希望对每个实例使用不同的公用名，只需重复此处所述的过程来为您的 Splunk 实例创建不同的证书（每个证书各有一个不同的公用名）。

例如，如果要配置多个转发器，您可以使用以下示例为您的索引器创建 `myServerCertificate.pem` 证书，然后使用相同根 CA 创建另一个证书 `myForwarderCertificate.pem`，并在您的转发器中安装该证书。请注意，索引器将仅从转发器接受正确生成并配置的且由相同根 CA 签名的证书。

有关配置转发器和索引器的更多信息，请参阅"将 Splunk 转发配置为使用您自己的证书"。

为您的服务器证书生成密钥。

1.为您的服务器证书生成新的 RSA 专用密钥。在本例中，我们同样使用的是 DES3 加密和 2048 位密钥长度：

在 *nix 中：

```
# openssl genrsa -des3 -out myServerPrivateKey.key 2048
```

在 Windows 中：

```
# openssl genrsa -des3 -out myServerPrivateKey.key 2048
```

2. 出现提示时，为密钥创建一个新密码。

新的密钥 `myServerPrivateKey.key` 已创建。此密钥将用于加密已将其作为服务器证书一部分安装的任何 Splunk 实例中的传出数据。

生成新服务器证书并对其进行签名

1. 使用新服务器密钥 `myServerPrivateKey.key` 为您的服务器证书生成 CSR。

在 *nix 中：

```
# openssl req -new -key myServerPrivateKey.key -out myServerCertificate.csr
```

在 Windows 中：

```
openssl req -new -key myServerPrivateKey.key -out myServerCertificate.csr -config $SPLUNK_HOME\openssl.cnf
```

2. 出现提示时，请提供密钥 `myServerPrivateKey.key` 的密码。

3. 为您的证书提供请求的信息，包括公用名（如果您要将 Splunk Enterprise 配置为通过公用名检查进行验证）。

新的 CSR `myServerCertificate.csr` 将出现在您的目录中。

4. 使用 CSR `myServerCertificate.csr` 和您的 CA 证书与密钥生成服务器证书。

在 *nix 中：

```
# openssl x509 -req -in myServerCertificate.csr -sha256 -CA myCACertificate.pem -CAkey myCAPrivateKey.key -
CAcreateserial -out myServerCertificate.pem -days 1095
```

在 Windows 中：

```
# openssl x509 -req -in myServerCertificate.csr -sha256 -CA myCACertificate.pem -CAkey myCAPrivateKey.key -
CAcreateserial -out myServerCertificate.pem -days 1095
```

5. 出现提示时，请提供证书授权密钥 `myCAPrivateKey.key` 的密码。务必使用您的专用密钥对此服务器证书进行签名，而不要使用刚刚创建的服务器密钥。

新的公用服务器证书 `myServerCertificate.pem` 将出现在您的目录中。

后续步骤

现在，您所创建的目录中应该包含以下文件，这些文件是配置索引器、转发器和通过管理端口通信的 Splunk 实例所需的所有信息。

- `myServerCertificate.pem`
- `myServerPrivateKey.key`
- `myCACertificate.pem`

现在，您已经拥有所需的证书，必须准备您的服务器证书（包括附加任何中间证书），然后将 Splunk 配置为查找并使用这些证书：

- 有关如何将您的证书设置为用于 Splunk 的信息，请参阅"如何为 Splunk 准备签名证书"。
- 有关为转发配置证书验证的更多信息，请参阅"将 Splunk 转发配置为使用您自己的证书"。
- 有关为 Splunk 间通信配置证书验证的更多信息，请参阅"关于确保 Splunk 间通信安全"。

如何获取第三方签名的证书

本主题介绍如何使用 Splunk Enterprise 随附的 OpenSSL 版本获取第三方证书，以便使用该证书来确保转发器与索引器之间以及 Splunk 之间通信的安全。

要获取可用于确保浏览器与 Splunk Web 之间通信安全的证书，请参阅"获取 Splunk Web 的第三方签名证书"。

如果您已经拥有这些证书，或者您知道如何生成这些证书，可以跳过本主题，直接进入配置步骤（将在本手册的后文中介绍）：

- 将 Splunk 转发配置为使用您自己的证书
- 关于确保 Splunk 间通信安全

注意： 如果您要在配置中使用多个公用名，可以重复此处所述的步骤使用相同根 CA 为每个实例创建不同的服务器证书（每个证书都有各自的公用名），然后将 Splunk 实例配置为使用这些证书。有关配置转发器和索引器的更多信息，请参阅"将 Splunk 转发配置为使用您自己的证书"。

开始之前

此次讨论中， `$SPLUNK_HOME` （位于 Windows 中的 `%SPLUNK_HOME%`）指的是 Splunk Enterprise 安装目录。在 Windows 中，您可能需要在“系统属性”对话的命令行或“环境”选项卡中设置此变量。

在 Windows 中，默认情况下 Splunk Enterprise 目录位于 `C:\Program Files\Splunk`。对于大多数 Unix 平台，默认安装目录为 `/opt/splunk`。对于 Mac Os，则为 `/Applications/splunk`。有关在 Windows 和 *nix 中运行的更多信息，请参阅《管理指南》。

将环境设置为 *nix 中 `$SPLUNK_HOME/splunk/lib` 的版本或 Windows 中 `%SPLUNK_HOME%/splunk/bin` 的版本，以确保使用随附 Splunk Enterprise 的 OpenSSL 版本。

为您的证书创建新目录

创建证书时，应创建一个新的工作目录。在我们的示例中，我们正在使用 `$SPLUNK_HOME/etc/auth/mycerts`：

```
# mkdir $SPLUNK_HOME/etc/auth/mycerts
# cd $SPLUNK_HOME/etc/auth/mycerts
```

Splunk 强烈建议您设立一个新文件夹，这样您就不会覆盖新证书和密钥的 `$SPLUNK_HOME/etc/auth` 中的现有证书。在新目录下工作可保护 Splunk 附带的证书，使您可以根据需要对其他 Splunk 组件使用这些证书。

请求您的服务器证书

创建证书签名请求 (CSR) 并进行签名以发送到您的证书颁发机构。

重要提示：本例向您显示如何创建新的专用密钥并请求服务器证书。您可以将此服务器证书分布到所有转发器、索引器以及通过管理端口进行通信的 Splunk 实例。如果您希望对每个实例使用不同的公用名，只需重复此处所述的过程来为您的 Splunk 实例创建不同的证书（每个证书各有一个不同的公用名）。

例如，如果要配置多个转发器，您可以使用以下示例为您的索引器创建 `myServerCertificate.pem` 证书，然后使用相同根 CA 创建另一个证书 `myForwarderCertificate.pem`，并在您的转发器中安装该证书。请注意，索引器将仅从转发器接受正确生成并配置的且由相同根 CA 签名的证书。

有关配置转发器和索引器的更多信息，请参阅“将 Splunk 转发配置为使用您自己的证书”。

为您的服务器证书生成专属密钥。

1. 创建新的专用密钥。以下示例使用 DES3 加密和 2048 位密钥长度，我们建议使用 2048 或更长的密钥。

在 *nix 中：

```
openssl genrsa -des3 -out myServerPrivateKey.key 2048
```

在 Windows 中：

```
openssl genrsa -des3 -out myServerPrivateKey.key 2048 -config $SPLUNK_HOME\openssl.cnf
```

2. 出现提示时，为密钥创建一个密码。

完成此操作时，将在目录中创建新密钥 `myServerPrivateKey.key`。此密钥将用于对证书签名请求 (CSR) 进行签名。

生成新的证书签名请求 (CSR)

1. 使用密钥 `myServerPrivateKey.key` 为您的服务器证书生成 CSR：

在 *nix 中：

```
openssl req -new -key myServerPrivateKey.key -out myServerCertificate.csr
```

在 Windows 中：

```
openssl req -new -key myServerPrivateKey.key -out myServerCertificate.csr -config $SPLUNK_HOME\openssl.cnf
```

2. 出现提示时，请为密钥 `myServerPrivateKey.key` 提供创建的密码。

3. 为您的证书提供请求的信息。要使用公用名检查，在输入证书详细信息时务必提供公用名。

完成此操作时，将在目录中出现新的 CSR `myServerCertificate.csr`。

下载并验证服务器证书和公共密钥

1. 将 CSR 发送到证书颁发机构 (CA) 以请求新的服务器证书。请求过程取决于所使用的证书颁发机构。

2. 准备好后，从证书颁发机构下载新的服务器证书。对于本手册中的示例，我们称之为 `myServerCertificate.pem`。

3. 还要下载证书颁发机构的公共 CA 证书。对于本手册中的示例，我们称之为 `myCACertificate.pem`。

如果您的证书颁发机构没有为您提供 PEM 格式的证书，您必须使用适合现有文件类型的 OpenSSL 命令对证书进行转换，有关转换不同文件类型的更多信息，请参阅 OpenSSL 文档。

4. 查看内容以确保其中包含您所需的所有信息：

- "Issuer" 条目应当指的是 CA 信息。
- 在之前创建 CSR 时，"Subject" 条目应当显示您输入的相关信息（国家名称、组织名称、公用名等）。

后续步骤

现在，您所创建的目录中应该包含以下文件，这些文件是配置索引器、转发器和通过管理端口通信的 Splunk 实例所需的所有信息。

- `myServerCertificate.pem`
- `myServerPrivateKey.key`
- `myCACertificate.pem`

现在，您已经拥有所需的证书，必须准备您的服务器证书（包括附加任何中间证书），然后将 Splunk 软件配置为查找并使用您的证书：

- 有关如何将您的证书设置为用于 Splunk 的信息，请参阅"如何为 Splunk 准备签名证书"。
- 有关为转发配置证书验证的更多信息，请参阅"将 Splunk 转发配置为使用您自己的证书"。
- 有关为 Splunk 间通信配置证书验证的更多信息，请参阅"关于确保 Splunk 间通信安全"。

如何为 Splunk 验证准备签名证书

有了证书之后，您必须将服务器证书和您的密钥合并为一个 Splunk 软件可以使用的文件。

如果您还没有证书，而且需要帮助您获得证书，我们在以下主题中提供了一些使用 OpenSSL 的基本示例：

- 如何自签名证书。
- 如何获取第三方签名的证书。

注意： 要为 Splunk 软件配置 SSL，应确保您的证书和公共密钥采用 x509 格式并且您的专用密钥采用 RSA 格式。

创建单个 PEM 文件

将您的服务器证书和公共证书按顺序合并为单个 PEM 文件。

在此处的示例中，我们使用的是"如何自签名证书"和"如何获取第三方签名的证书"中介绍的文件名。

以下是 *nix 的示例：

```
# cat myServerCertificate.pem myServerPrivateKey.key myCACertificate.pem > myNewServerCertificate.pem
```

以下是 Windows 的示例：

```
>type myServerCertificate.pem myServerPrivateKey.key myCACertificate.pem > myNewServerCertificate.pem
```

创建之后，应当包含文件 `myNewServerCertificate` 中的内容，以如下顺序排列：

- 服务器证书 (`myServerCertificate.pem`)
- 密钥 (`myServerPrivateKey.key`)
- 证书授权公共密钥 (`myCACertificate.pem`)

下面是正确连接的证书的示例：

```
-----BEGIN CERTIFICATE-----
MIICUTCCAboCCQCscBkn/xey1TANBgkqhkiG9w0BAQUFADBtMQswCQYDVQQGEwJV
...
<Server Certificate>
...
8/PZr3EuXYk1c+N5hgIQys5a/HIn
-----END CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,CFCECC7976725DE5

S+DPcQ0l2Z1bk71N3cBqr/nwEXPNDQ4uqtecCd3iGMV3B/WSOWAQxcWzhe9JnIsl
```

```
...
<Server Private Key - Passphrase protected>
...
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIICUTCCAboCCQCscBkn/xey1TANBgkqhkiG9w0BAQUFADBtMQswCQYDVQQGEwJV
...
<Certificate Authority Public Key>
...
8/PZr3EuXYk1c+N5hgIQys5a/HIn

-----END CERTIFICATE-----
```

如何配置证书链

要使用多个证书，应将中间证书附加到服务器证书文件的末尾。您可以按照层次结构的递减顺序添加所需数量的证书，一直到根目录。

连接证书时应遵循如下顺序：

```
[ server certificate]
[ intermediate certificate]
[ root certificate (if required) ]
```

例如，证书链可能类似如下所示：

```
-----BEGIN CERTIFICATE-----
... (certificate for your server)...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
... (the intermediate certificate)...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
... (the root certificate for the CA)...
-----END CERTIFICATE-----
```

后续步骤

现在您已经有了所需的证书，必须对 Splunk 软件进行配置以使其能够找到并使用这些证书：

- 有关为转发配置证书验证的更多信息，请参阅“将 Splunk 转发配置为使用您自己的证书”。
- 有关为 Splunk 间通信配置证书验证的更多信息，请参阅“关于确保 Splunk 间通信安全”。

自签名 Splunk Web 的证书

本主题提供使用 Splunk 软件随附的 OpenSSL 版本在命令行中创建自签名证书的基本示例。

您可以通过多种方式来创建签名证书，具体取决于组织策略、平台和所使用的工具。如果您已经生成了这些证书和密钥，或者如果您在生成证书方面已很有经验，可以跳过此任务直接转到本手册中的配置主题“使用您自己的证书确保 Splunk Web 安全”。

因为自签名证书是由贵组织签署，所以它们并不在浏览器证书库中。因此，Web 浏览器会将自签名证书视为“不受信任”。从而为用户生成一个警告页面，甚至可能会阻止该用户的访问。

对于发生在组织内部或两个已知实体之间的浏览器和 Splunk Web 间通信，如果您可以将自己的 CA 添加到将与 Splunk Web 联系的所有浏览器库中，此时最好使用自签名证书。对于任何其他情况，建议使用 CA 签名证书。有关更多信息，请参阅“获取 Splunk Web 的第三方签名证书”。

开始之前

在此次讨论中，`$SPLUNK_HOME` 指的是 Splunk 安装目录。在 Windows 中，默认情况下 Splunk 软件安装在 `C:\Program Files\splunk`。对于大多数 Unix 平台，默认安装目录为 `/opt/splunk`；对于 Mac OS 则为 `/Applications/splunk`。有关在 Windows 和 *nix 中运行的更多信息，请参阅《管理指南》。

将环境设置为 *nix 中 `$SPLUNK_HOME/splunk/lib` 的版本或 Windows 中 `$SPLUNK_HOME/splunk/bin` 的版本，以确保使用随附 Splunk 软件的 OpenSSL 版本。

生成新的根证书作为您的证书颁发机构

1. 创建用于托管您的证书和密钥的新目录。对于此示例，我们将使用 `$SPLUNK_HOME/etc/auth/mycerts`。

我们建议您将新证书置于其他目录，而不是 $SPLUNK_HOME/etc/auth/splunkweb 这样您就不会覆盖现有证书。这将确保您可以根据需要为其他 Splunk 组件在 $SPLUNK_HOME/etc/auth/splunkweb 中使用随附 Splunk 软件的证书。

注意：如果您按"如何自签名证书"中所述创建了自签名证书，可以将根证书复制到您的目录并跳到下一步："为 Splunk Web 创建新专用密钥"。

2. 生成新的 RSA 专用密钥。本例使用 2048 位长度：

```
# openssl genrsa -des3 -out myCAPrivateKey.key 2048
```

注意，在 Windows 中，您可能需要附加 openssl.cnf 文件的位置：

```
>openssl genrsa -des3 -out myCAPrivateKey.key 2048  -config $SPLUNK_HOME\openssl.cnf
```

在我们的示例中，密钥长度为 2048（建议的最小值），但是若浏览器支持的话，您可以指定长度大于 2048 的密钥。

3. 出现提示时，创建密码。

专用密钥 myCAPrivateKey.key 将出现在您的目录中。这是您的根证书专用密钥。

4. 使用根证书专用密钥 myCAPrivateKey.key 生成证书签名请求。

在 *nix 中：

```
# openssl req -new -key myCAPrivateKey.key -out myCACertificate.csr
```

在 Windows 中：

```
>openssl req -new -key myCAPrivateKey.key -out myCACertificate.csr  -config $SPLUNK_HOME\openssl.cnf
```

5. 提供密钥 myCAPrivateKey.key 的密码。

新的 CSR myCACertificate.csr 将出现在您的目录中。

6. 使用 CSR 生成新的根证书，并使用您的专用密钥对该证书进行签名：

在 *nix 中：

```
# openssl x509 -req -in myCACertificate.csr -signkey myCAPrivateKey.key -out myCACertificate.pem -days 3650
```

在 Windows 中：

```
>openssl x509 -req -in myCACertificate.csr -signkey myCAPrivateKey.key -out myCACertificate.pem -days 3650  -config
$SPLUNK_HOME\openssl.cnf
```

7. 出现提示时，请提供密钥 myCAPrivateKey.key 的密码。

新的证书 myCACertificate.pem 将出现在您的目录中。这是您的公共证书。

为 Splunk Web 创建新专用密钥

1. 生成新的专用密钥：

在 *nix 中：

```
# openssl genrsa -des3 -out mySplunkWebPrivateKey.key 2048
```

在 Windows 中：

```
>openssl genrsa -des3 -out mySplunkWebPrivateKey.key 2048 -config $SPLUNK_HOME\openssl.cnf
```

2. 出现提示时，创建密码。

新的密钥 mySplunkWebPrivateKey.key 将出现在您的目录中。

3. 从密钥中删除密码。（Splunk Web 当前不支持带密码保护的专用密钥。）

在 *nix 中：

```
# openssl rsa -in mySplunkWebPrivateKey.key -out mySplunkWebPrivateKey.key
```

在 Windows 中：

```
>openssl rsa -in mySplunkWebPrivateKey.key -out mySplunkWebPrivateKey.key -config $SPLUNK_HOME\openssl.cnf
```

您可以通过发出以下命令确保密码已经删除：

在 *nix 中：

```
# openssl rsa -in mySplunkWebPrivateKey.key -text
```

在 Windows 中：

```
>openssl rsa -in mySplunkWebPrivateKey.key -text -config $SPLUNK_HOME\openssl.cnf
```

您应该无需提供密码即可读取证书的内容。

创建服务器证书并对其进行签名

1.使用您的专用密钥 `mySplunkWebPrivateKey.key` 创建新的证书签名请求：

在 *nix 中：

```
# openssl req -new -key mySplunkWebPrivateKey.key -out mySplunkWebCert.csr
```

在 Windows 中：

```
>openssl req -new -key mySplunkWebPrivateKey.key -out mySplunkWebCert.csr -config $SPLUNK_HOME\openssl.cnf
```

CSR `mySplunkWebCert.csr` 将出现在您的目录中。

2.对带有根证书专用密钥 `myCAPrivateKey.key` 的 CSR 进行自签名：

在 *nix 中：

```
# openssl x509 -req -in mySplunkWebCert.csr -CA myCACertificate.pem -CAkey myCAPrivateKey.key -CAcreateserial -out
mySplunkWebCert.pem -days 1095
```

在 Windows 中：

```
>openssl x509 -req -in mySplunkWebCert.csr -CA myCACertificate.pem -CAkey myCAPrivateKey.key -CAcreateserial -out
mySplunkWebCert.pem -days 1095 -config $SPLUNK_HOME\openssl.cnf
```

3.出现提示时，请提供根证书专用密钥 `myCAPrivateKey.key` 的密码。

证书 `mySplunkWebCert.pem` 已添加至您的目录中。这是您的服务器证书。

创建单个 PEM 文件

将您的服务器证书和公共证书按顺序合并为单个 PEM 文件。

如下为在 Linux 中如何操作的示例：

```
# cat mySplunkWebCert.pem myCACertificate.pem > mySplunkWebCertificate.pem
```

如下为在 Windows 中的示例：

```
# type mySplunkWebCert.pem myCACertificate.pem > mySplunkWebCertificate.pem
```

设置证书链

要使用多个证书，应按以下顺序将中间证书附加到服务器证书文件的末尾：

```
[ server certificate]
[ intermediate certificate]
[ root certificate (if required) ]
```

例如，证书链可能类似如下所示：

```
-----BEGIN CERTIFICATE-----
... (certificate for your server)...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
... (the intermediate certificate)...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
... (the root certificate for the CA)...
-----END CERTIFICATE-----
```

后续步骤

现在，您已经有了证书，需要分发这些证书并将 Splunkd 和 Splunk Web 配置为可使用这些证书。有关更多信息，请参阅本手册中的"使用您自己的证书确保 Splunk Web 安全"。

获取 Splunk Web 的第三方签名证书

本主题提供创建第三方签名证书的基本示例，这些证书是配置 Splunk Web 使用 SSL 验证和加密所必需的。

可通过多种方式来创建这些证书，具体取决于贵组织的策略、您的网络结构以及所使用的工具。如果您已经生成了这些证书和密钥，或者如果您在生成第三方证书方面已很有经验，可能希望跳过此任务，直接转到本手册中的配置主题"使用您自己的证书确保 Splunk Web 安全"。

开始之前

在此次讨论中，`$SPLUNK_HOME` 指的是 Splunk 安装目录。在 Windows 中，默认情况下 Splunk 软件安装在 `C:\Program Files\splunk`。对于大多数 Unix 平台，默认安装目录为 `/opt/splunk`；对于 Mac OS 则为 `/Applications/splunk`。有关在 Windows 和 *nix 中运行的更多信息，请参阅《管理指南》。

将环境设置为 *nix 中 `$SPLUNK_HOME/lib` 的版本或 Windows 中 `$SPLUNK_HOME/bin` 的版本，以确保使用随附 Splunk 的 OpenSSL 版本。

为 Splunk Web 创建新专用密钥

1. 创建用于托管您自己的证书和密钥的新目录。在此示例中，我们将使用 `$SPLUNK_HOME/etc/auth/mycerts`。

我们建议您将新证书置于其他目录，而不是 `$SPLUNK_HOME/etc/auth/splunkweb` 这样您就不会覆盖现有证书。这将确保您可以根据需要对其他 Splunk 组件使用 Splunk 随附的证书。

2. 生成新的专用密钥。我们的示例使用的密钥长度为 2048。

```
# openssl genrsa -des3 -out mySplunkWebPrivateKey.key 2048
```

注意，在 Windows 中，您可能需要附加 `openssl.cnf` 文件的位置：

```
>openssl genrsa -des3 -out mySplunkWebPrivateKey.key 2048 -config $SPLUNK_HOME\openssl.cnf
```

3. 出现提示时，创建密码。

新专用密钥 `mySplunkWebPrivateKey.key` 已添加至您的目录中。您可以使用此密钥来对 CSR 进行签名。

4. 从专用密钥中删除密码（Splunk Web 不支持专用密钥密码）：

```
# openssl rsa -in mySplunkWebPrivateKey.key -out mySplunkWebPrivateKey.key
```

可以使用以下命令确保您的密码已成功删除：

```
# openssl rsa -in mySplunkWebPrivateKey.key -text
```

系统将提示您输入原始密钥的密码。（以授权从密钥删除密码）

如果密码已成功删除，您无需提供密码即可查看证书内容。

创建证书颁发机构 (CA) 请求并获取服务器证书

1. 使用您的专用密钥 `mySplunkWebPrivateKey.key` 创建新的证书签名请求：

在 *nix 中：

```
# openssl req -new -key mySplunkWebPrivateKey.key -out mySplunkWebCert.csr
```

在 Windows 中：

```
>openssl req -new -key mySplunkWebPrivateKey.key -out mySplunkWebCert.csr -config $SPLUNK_HOME\openssl.cnf
```

Windows 平台的注意事项：如果您看到类似以下内容的错误：

无法从 c:\\build-amd64-5.0.2-20130120-1800\\splunk/ssl/openssl.cnf 加载配置信息

尝试在命令提示中键入以下内容，然后再次运行 `openssl` 命令：

```
set OPENSSL_CONF=c:/Program Files/Splunk/openssl.cnf
```

2. 使用此 CSR `mySplunkWebCert.csr` 以便从证书授权 (CA) 请求新签名证书。请求签名证书的过程取决于证书颁发机构对证书签名请求的处理方式。请联系您的 CA 了解更多信息。

3. 下载证书颁发机构所返回的服务器证书。对于此示例，我们称之为 "`mySplunkWebCert.pem`"。

4. 下载证书颁发机构的公共 CA 证书。对于此示例，我们称之为 "`myCAcert.pem`"。

5. 确保服务器证书和公共 CA 证书均为 PEM 格式。如果这些证书并非 PEM 格式，则使用适用于您现有文件类型的 `openssl` 命令将它们转换。以下是可用于 DER 格式的命令的示例：

x509 -in input.crt -inform DER -out output.crt -outform PEM/x509 -in input.crt -inform DER -out output.crt -outform PEM

6. 对两个证书进行检查，以确保其中已包含必需的信息并且没有密码保护。

```
# openssl x509 -in myCACert.pem -text
# openssl x509 -in mySplunkWebCert.pem -text
>openssl x509 -in myCACert.pem -text -config $SPLUNK_HOME\openssl.cnf
>openssl x509 -in mySplunkWebCert.pem -text -config $SPLUNK_HOME\openssl.cnf
```

`mySplunkWebCert.pem` 的颁发者信息应当为 `myCACert.pem` 的主题信息（除非您正在使用中间证书）。

将您的证书和密钥合并为单个文件

将您的服务器证书和公共证书按顺序合并为单个 PEM 文件。

设置证书链

要使用多个证书，应按以下顺序将中间证书附加到服务器证书文件的末尾：

```
[ server certificate]
[ intermediate certificate]
[ root certificate (if required) ]
```

例如，证书链可能类似如下所示：

```
-----BEGIN CERTIFICATE-----
... (certificate for your server)...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
... (the intermediate certificate)...
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
... (the root certificate for the CA)...
-----END CERTIFICATE-----
```

请注意，用于签发中间证书以及所有中间证书的根 CA 必须位于浏览器证书库中。

后续步骤

配置 Splunk 的 Web.conf 文件以查找并使用您的证书进行验证。有关更多信息，请参阅"使用您自己的证书确保 Splunk Web 安全"。

确定密码套件

您可以选择并指定 Splunk 间、Splunk Web 以及 Splunk 转发器与索引器间通信的密码套件。可以通过在服务器 SSL 配置段落末尾附加一行来添加密码套件。

以下为当配置转发器至索引器证书验证时您将如何更新 `inputs.conf` 的示例：

```
[splunktcp-ssl:9998]
[SSL]
password = password
requireClientCert = false
rootCA = $SPLUNK_HOME/etc/auth/cacert.pem
serverCert = $SPLUNK_HOME/etc/auth/server.pem
cipherSuite = AES256-SHA256:DHE-RSA-AES256-SHA256
```

要查看可用的密码：

```
$SPLUNK_HOME/bin/splunk cmd openssl ciphers -v
```

```
$SPLUNK_HOME/bin/splunk cmd openssl ciphers -v "TLSv1.2"
$SPLUNK_HOME/bin/splunk cmd openssl ciphers -v "HIGH"
```

对您可用的密码套件取决于您的 OpenSSL 版本。要查看您正在运行的 OpenSSL 版本：

```
$SPLUNK_HOME/bin/splunk cmd openssl version
```