# Ansible Tower 自动化实践（4）- 管理项目和启动 Ansible 作业

第一节：为Ansible Playbook创建项目
项目：project

- Ansible项目至少代表了一个playbook及其相关playbook和角色的关联集合。
- 无论是否使用Ansible Tower，在版本控制系统中管理项目playbook代码是推荐做法。
- Ansible Tower的设计假定大多数Ansible项目都在版本控制系统中进行管理，并且可以从

  多个常用版本控制系统中自动检索项目的更新playbook代码。

- 在Ansible Tower Web界面中，每个Ansible项目都由一个项目资源来表示。
- 该项目配置为从版本控制系统检索这些playbook代码。
- Ansible Tower支持使用 *Git*、*Subversion* 或 *Mercurial* 从 SCM 下载和自动获取项目

  资料更新的功能。

  * 注意：
    1. Ansible Tower的项目基础路径：*/var/lib/awx/projects/*
    2. 可手动将项目复制到该目录中被Ansible Tower服务器所查询，可用于测试。
    3. 该目录由 */etc/tower/settings.py* 配置

```
# !!! DO NOT EDIT THIS FILE !!!
# Default AWX settings

################################################################################
# MISC PROJECT SETTINGS
################################################################################

ADMINS = (
    #('Joe Admin', 'joeadmin@example.com'),
)

STATIC_ROOT = '/var/lib/awx/public/static'

PROJECTS_ROOT = '/var/lib/awx/projects'  # Ansible Tower节点默认的项目目录

JOBOUTPUT_ROOT = '/var/lib/awx/job_status'

SECRET_KEY = open('/etc/tower/SECRET_KEY', 'rb').read().strip()

ALLOWED_HOSTS = ['*']

INTERNAL_API_URL = 'http://127.0.0.1:80'

```

    4. 推荐做法：更新此类项目需在Ansible Tower界面外进行手动干预（Manual）。
    5. 它还要求项目管理员具有直接访问权限以在Ansible Tower上的操作系统环境中进行

更改，这会降低Ansible Tower服务器的安全性。

6. 最好让 Ansible Tower 从 SCM 系统获取项目playbook代码。

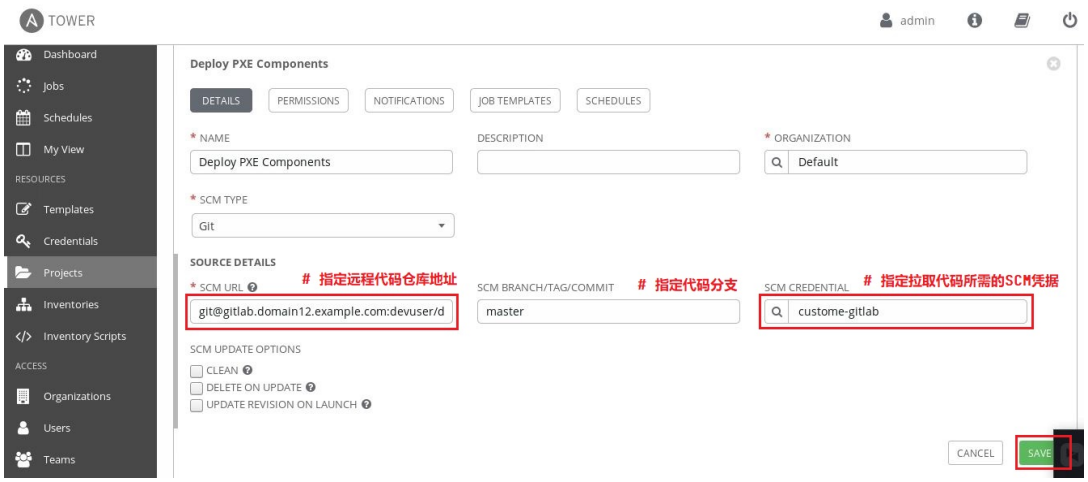
创建项目：

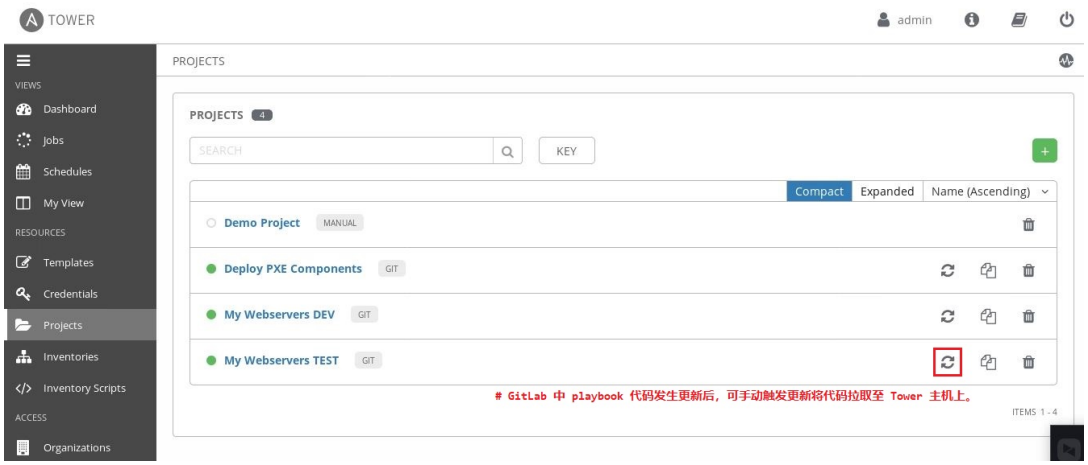
- 创建项目的过程，参看P327引导练习（略）。

  * 注意：

    1. 需先创建SCM凭据用于拉取远程代码仓库中指定用户的代码，再创建项目！
    2. 创建项目点击SAVE按钮时，Ansible Tower将自动从代码仓库中拉取代码至本地的

       /var/lib/awx/projects目录中。




项目角色：

- 通过项目资源的分配角色，向用户授予项目资源的权限。
- 可以直接为用户分配角色，也可以将角色分配至其所在的团队以继承角色。
- 若要让用户获得特定项目的权限，用户必须被分配或继承该项目的角色。

- 项目角色列表：

  1. Admin：
     a. Admin 角色授予用户对项目的完全访问权限。
     b. 被授予项目的此角色时，用户可以删除项目并修改其属性，包括权限。
     c. 此角色还授予用户 Use、Update 和 Read 角色。

  2. Use：

a. Use 角色授予用户在模板资源中使用项目的权限。
b. 此角色还授予用户与项目 Read 角色相关联的权限。

3. Update：
   a. Update 角色授予用户从其 SCM 来源手动更新或计划项目资料更新的权限。
   b. 此角色还授予用户与项目 Read 角色相关联的权限。

4. Read：
   a. Read 角色授予用户查看与项目关联的详细信息、权限和通知的权限。

管理项目访问权限：

- 首次创建项目时，用户必须拥有该项目的组织的 Admin 或 *Auditor* 角色才能访问它。
- 用户的其他访问权限必须经过特别配置。
- 创建项目时无法分配角色，而是必须通过编辑项目进行添加。
- 角色在项目编辑器屏幕的 PERMISSIONS 部分中分配。

- 设置项目角色的过程，参看P327引导练习（略）。

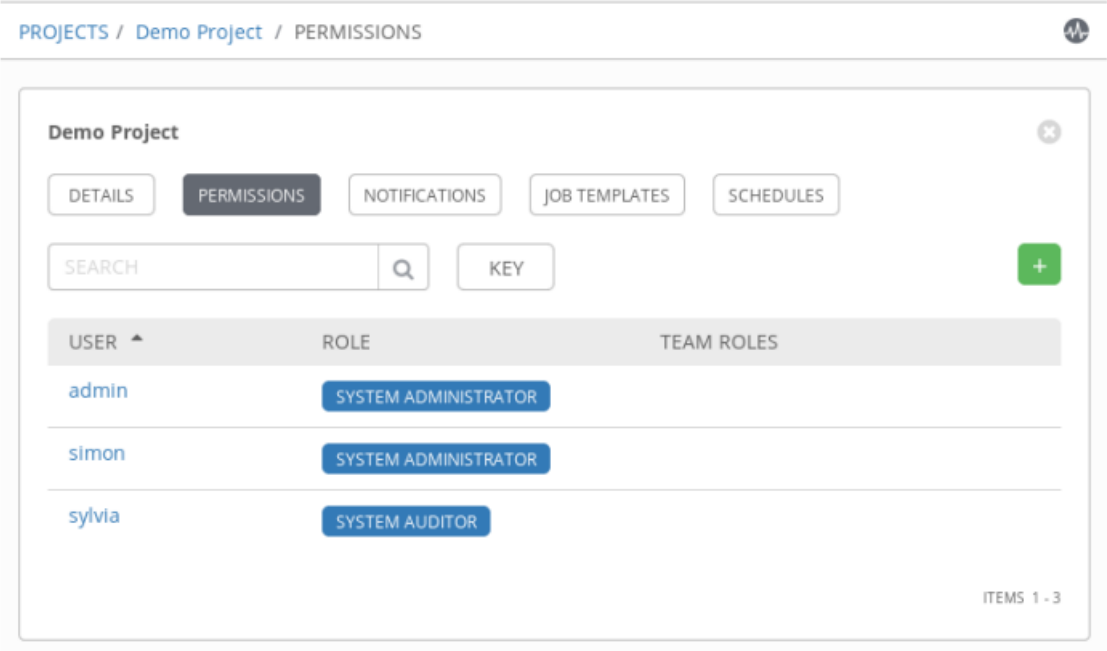
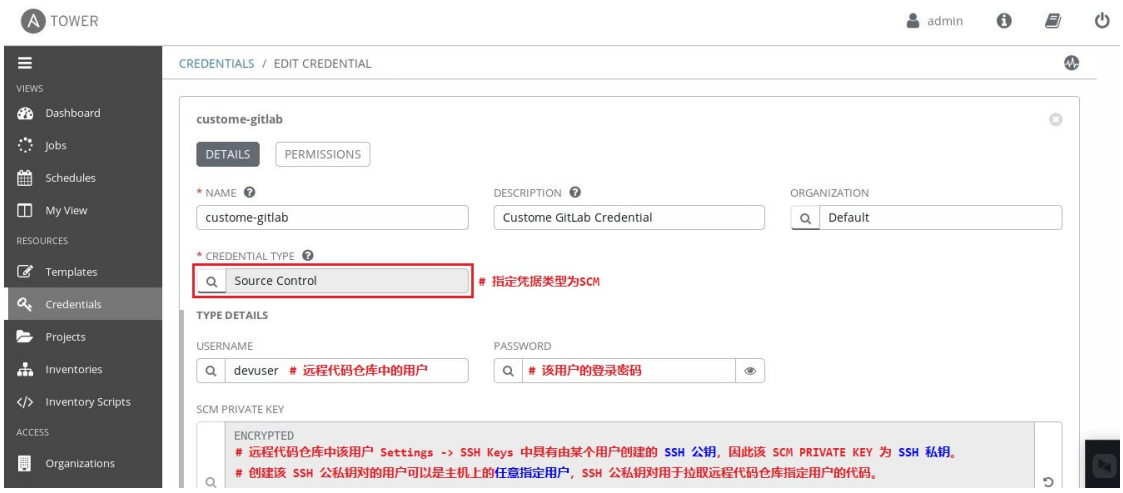



Figure 9.2: Assigning Project roles to a user

创建SCM凭据：

- 来源控制凭据（也称SCM凭据）存储身份验证信息，供Ansible Tower用来访问存储在像Git这样的版本控制系统中的项目playbook代码。
- SCM凭据存储对远程源代码库访问权限进行身份验证所需的用户名和密码或私钥。
- 创建SCM凭据的过程，参看P327引导练习（略）。

  * 注意：
    创建SCM凭据时所使用的远程代码仓库的用户的SSH公私钥对需提前配置！




SCM凭据角色：

- SCM凭据仅供其创建者以及 System Administrator 和 *System Auditor* 用户使用。
- 分配给某一组织的SCM凭据可以与其他用户共享，方法是为用户或团队分配该凭据的相应角色。

- 为用户提供对SCM凭据的访问权限的角色列表：

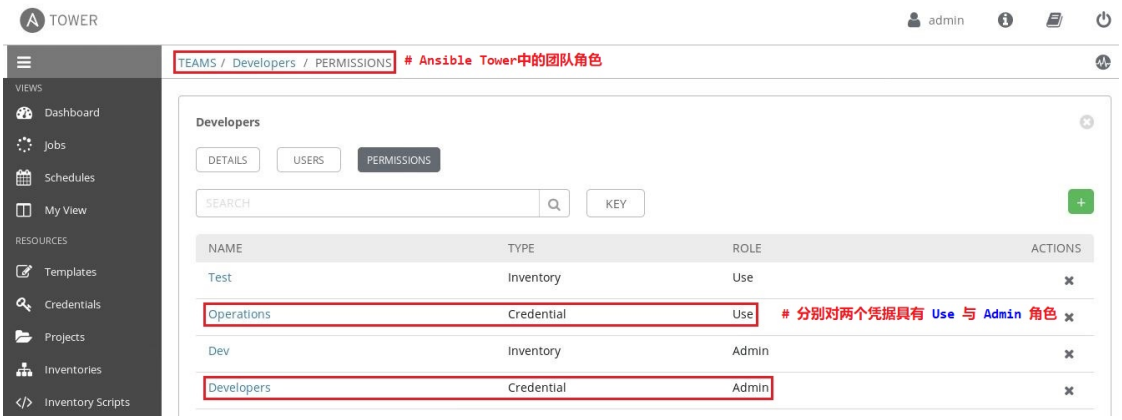
1. Admin：
   a. Admin 角色授予用户对SCM凭据的完全权限。
   b. 这些权限包括删除和修改SCM凭据。
   c. 此角色还授予用户与凭据 Use 与 Read 角色相关联的权限。

2. Use：
   a. Use 角色授予用户将SCM凭据与项目资源关联的权限。
   b. 此角色还授予用户与凭据 Read 角色相关联的权限。
   c. Use 角色不控制用户自己是否可以使用SCM凭据来更新项目，只控制他们是否可以分配该SCM凭据，以便它随后可由拥有该项目的 Update 角色的用户使用。
   d. 若SCM凭据与某一项目关联，则被分配了该项目的 Update 角色的任何用户都可以
      使用关联的SCM凭据，而无需被授予该凭据的 Use 角色。

3. Read：
   a. Read 角色授予用户查看SCM凭据详细信息的权限。

管理SCM凭据访问权限：

- 首次创建组织凭据时，只能由具有被分配了凭据的组织的 Admin 或 Auditor 角色进行访问。
- 其他用户的其他访问权限必须经过特别配置。
- 将SCM凭据角色分配给用户或团队将规定谁拥有属于某一组织的SCM凭据的权限。
- 这些权限不能在创建SCM凭据时分配，在创建后通过编辑凭据进行调整。
- 设置SCM凭据角色的访问权限过程，参看P327引导练习（略）。




更新项目：

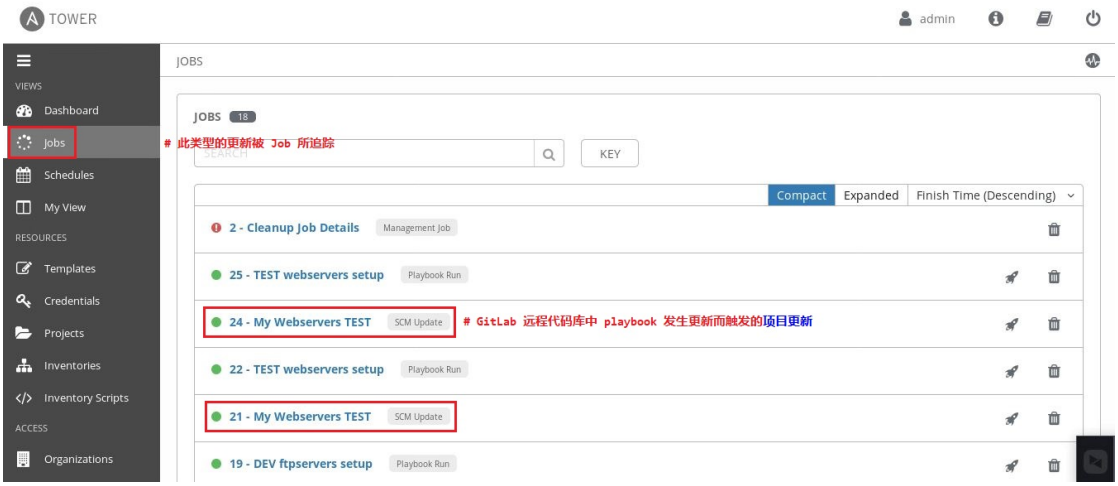
- Ansible Tower中的SCM项目资源代表从SCM来源获得的playbook和角色的副本。
- 由于对这些playbook和角色的内容的修改来自外部SCM系统，因此在Ansible Tower项目中，

  其相应的对等项必须定期从SCM来源更新，以反映新的更改。

- 可通过多种方式在Ansible Tower中更新SCM项目资源。

- 可将项目配置为从其SCM来源进行更新，方法是在项目信息中选择三个 SCM 更新选项之一：

1. Clean：
   a. 在从源代码控制存储库获取最新版本之前删除本地修改。
2. Delete on Update：
   b. 在从源代码控制存储库获取最新版本之前完全删除 Ansible Tower 上的本地项目存储库。
   c. 对于大型存储库要花费比 Clean 更长的时间。
3. Update on Launch：
   a. 在每次使用项目启动作业时，从源代码控制存储库更新项目。
   b. 更新本身作为单独的作业由 Ansible Tower 进行跟踪。




* 注意：
  1. 用户根据项目的 SCM 更新而手动触发项目更新时，必须赋予对项目的 Update 角色。

3. 若项目已配置 Update on Launch 更新选项，没有被授予项目的 Update 角色的用户
使用该项目，该项目仍会执行更新。

对Ansible角色的支持：

- 项目可指定外部 Ansible 角色，它们作为依赖项存储在 Ansible Galaxy 或其他源代码

  管理存储库中。

- 在项目更新结束时，若项目的存储库包括一个包含有效 *requirements.yml* 文件的 roles

  目录，则Ansible Tower将自动运行 ansible-galaxy 命令以安装角色。

- 如下所示：

```
$ ansible-galaxy install -r roles/requirements.yml -p ./roles/ --force
```

* 注意：
1. 若在Ansible Tower主机的/var/lib/awx/projects/目录中对应的项目中已存在相应的
角色，Ansible Tower将直接使用该角色。
2. 若使用 Ansible Galaxy 中的角色可先拉取至本地 SCM 中，再由Ansible Tower主机
创建项目时使用，可加速 playbook 的执行。

第二节：创建作业模板与启动作业
作业模板、项目与清单：

- 在Ansible Tower中，作业模板是可用来启动运行playbook的作业的模板。
- 作业模板关联的资源：

  1. 项目中的 playbook，项目中也包含 SCM 凭据。
  2. 主机清单
  3. 用于身份验证的主机凭据
  4. 在启动作业以运行该 playbook 时使用的其他参数

- 用户必须被授予 SCM 凭据、项目、主机清单、主机凭据、作业模板等资源的相应角色，否则

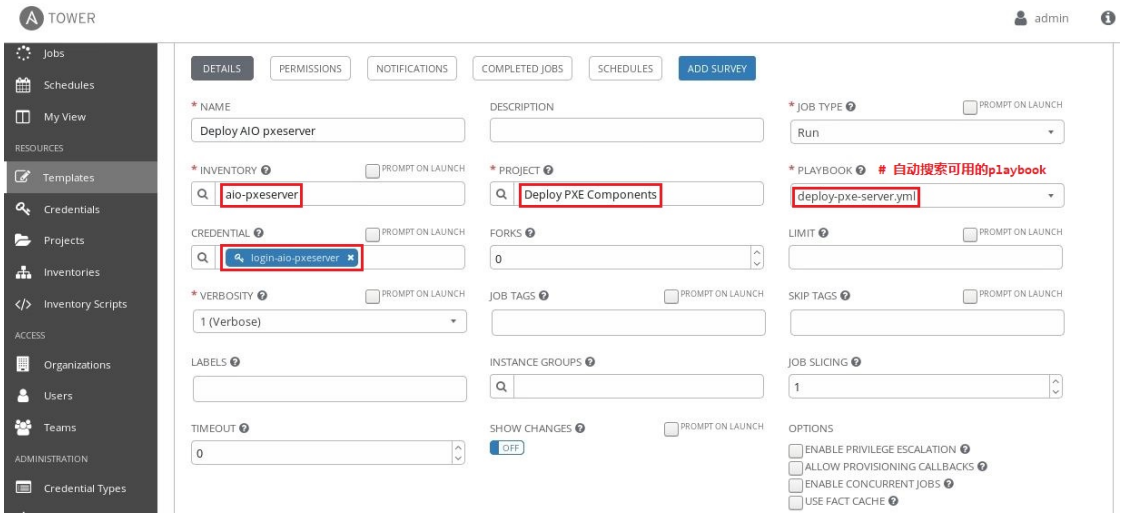
  将不能创建与管理作业模板！

- 作业模板定义了用于执行Ansible作业的参数。
- 作业模板必须定义项目的 playbook，以及包含受管主机列表的清单文件。
- 此外，作业模板还必须定义将用于对受管主机进行身份验证的主机凭据。
- 与项目和清单类似，必须将主机凭据的 Use 角色分配给用户，才能将主机凭据关联到作业模板。
- 在定义后，作业模板允许重复执行作业，因此适合日常执行任务。
- 由于项目、清单和主机凭据参数是作业模板定义的一部分，因此该作业每次都以相同的方式运行。

创建作业模板：job template

- 与其他Ansible Tower资源不同，作业模板不直接属于组织，而是由属于组织的项目使用。

- 作业模板与组织的关系由它所使用的项目决定。
- 因此，无需在组织中具有Admin角色即可创建作业模板。
- 只需要拥有分配到作业模板的项目的 *Use* 角色。
- 创建作业模板的过程，参看P338引导练习（略）。




修改作业执行：

- 作业模板的其他设置参数：

1. DESCRIPTION：
   a. 作业模板的可选描述
2. FORKS：
   a. 用于控制在playbook执行期间允许的并行进程数量的 forks 设置。
   b. 等同于 ansible-playbook 命令的 *-f* 或 *--forks* 选项。
   c. 若值为 0，则使用Ansible配置文件中的默认设置。
3. LIMIT：
   a. 限制由作业模板的清单提供的受管主机的列表。
   b. 通过提供主机模式作为此字段的值来完成过滤。
   c. 等同于 ansible-playbook 命令的 *-l* 或 *--limit* 选项。
4. JOB TAGS：
   a. 接受在playbook中存在的以逗号分隔的标记列表。
   b. 标记用于识别playbook的不同部分。
   c. 通过在此字段中指定标记列表，可选择性地仅执行playbook的特定部分。
   d. 等同于 ansible-playbook 命令的 *-t* 或 *--tags* 选项。
5. SKIP TAGS：
   a. 接受在playbook中存在的以逗号分隔的标记列表。
   b. 通过在此字段中指定标记列表，可选择性地在playbook执行期间跳过其中的特定部分。
   c. 等同于 ansible-playbook 命令的 *--skip-tags* 选项。
6. LABELS：
   a. 可附加到作业模板以帮助分组或过滤作业模板的名称。
7. Enable Privilege Escalation：
   a. 启用后，此复选框将导致playbook使用升级的特权来执行。
   b. 等同于 ansible-playbook 命令的 *--become* 选项。
8. Allow Provisioning Callbacks：
   a. 启用后，此复选框会导致在Ansible Tower上创建调配回调 URL，供主机用于使用
   作业模板请求配置更新。
9. Enable Concurrent Jobs：
   a. 启用后，此复选框将允许多次同时执行此作业模板。
10. Use Fact Cache：

a. 启用后，此复选框将导致使用缓存的事实，并将新发现的事实存储在Ansible Tower
上的事实缓存中。

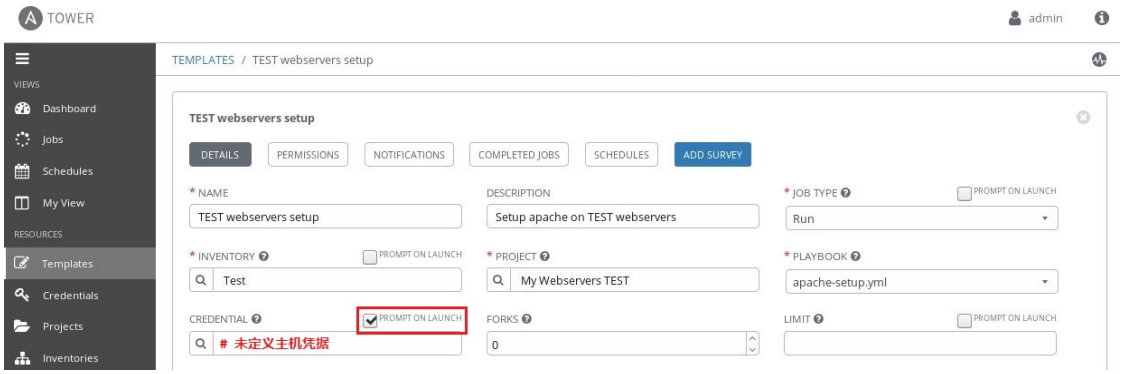
11. EXTRA VARIABLES：
    a. 此字段与 ansible-playbook 命令的 *-e* 或 *--extra-vars* 选项等效，可用于将
    额外的命令行变量传递到作业执行的playbook。
    b. 这些额外的变量定义为使用 YAML 或 JSON 的键/值对。

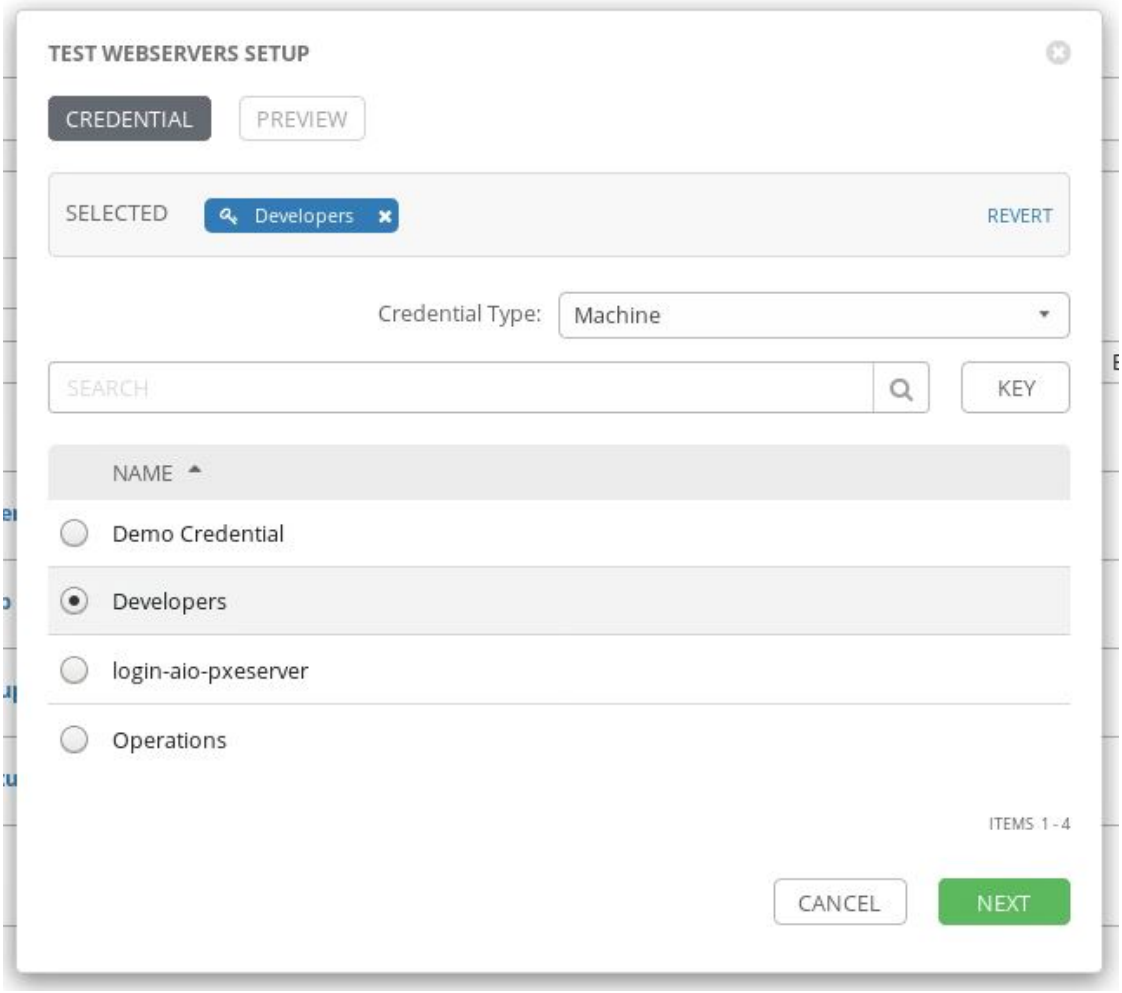
**提示输入作业参数：**

- Ansible Tower中若部分参数未定义，勾选 *Prompt on launch* 选项将在启动作业模板时

  提示用户选择参数以提高作业模板使用的灵活性，而无需创建不同参数值的作业模板。

- 如下所示：






作业模板角色：

- 用于控制用户对作业模板的访问权限的角色：

  1. Admin：
     a. 为用户提供删除作业模板或编辑其属性（包括其关联的权限）的权限。
     b. 此角色还授予与作业模板 Execute 和 Read 角色相关联的权限。
  2. Execute：
     a. 授予用户使用作业模板执行作业的权限。
     b. 它还授予用户使用作业模板计划作业的权限。
     c. 此角色还授予与作业模板 Read 角色相关联的权限。
  3. Read：
     a. 授予用户查看作业模板属性的只读访问权限。
     b. 它还授予访问权限以查看与作业模板相关的其他信息，如使用作业模板执行的作业列表，
        以及相关的权限和通知。

管理作业模板访问权限：

- 设置作业模板访问权限的过程，参看P338引导练习（略）。

启动作业：

- 设置启动作业的过程，参看P338引导练习（略）。

评估作业结果：

- 示例如下所示：

  使用作业模板将servera节点部署为 all-in-one PXE 服务器。