Contents

故障排除

参考

- Azure PowerShell
- 用于 .NET 的 Azure SDK
- REST
- PSGallery（Az.Blueprint 模块）
- PSGallery（社区模块）
- 蓝图函数

资源

- GitHub - Azure 蓝图示例
- Azure 路线图
- 定价计算器
- UserVoice
- 治理 YouTube 频道
- Azure Friday - Azure 蓝图概述

Azure 蓝图服务概述

2019/8/26 • • Edit Online

正如工程师或建筑师使用蓝图勾勒出项目的设计参数一样，通过 Azure 蓝图，云架构师和中心信息技术组同样可以定义一组可重复的 Azure 资源，这些资源实现并遵守组织的标准、模式和要求。通过 Azure 蓝图，开发团队可以快速生成和构建新环境，并确信这些生成的环境符合组织规定，还可以使用一组有助于加快开发和交付过程的内置组件（如网络）。

蓝图是一种声明性方法，用于协调各个资源模板和其他项目的部署，例如：

- 角色分配
- 策略分配
- Azure 资源管理器模板
- 资源组

Azure 蓝图服务由全球分布的 Azure Cosmos DB 提供支持。蓝图对象将复制到多个 Azure 区域。无论蓝图将资源部署到哪个区域，此复制都可提供对蓝图对象的低延迟、高可用性和一致访问。

与资源管理器模板的不同之处

此服务旨在帮助进行 环境设置。此设置通常包括一组资源组、策略、角色分配和资源管理器模板部署。蓝图是将每个项目类型组合在一起的包，通过蓝图可编写和版本化该包 - 包括通过 CI/CD 管道 。最终可在一个可审计和跟踪的操作中将每个蓝图分配给订阅。

几乎所有要包含在蓝图中部署的内容都可以使用资源管理器模板完成。但是，资源管理器模板是 Azure 中不以本机方式存在的文档 – 每个模板均存储在本地或源代码管理中。该模板用于部署一个或多个 Azure 资源，但部署了这些资源后，资源与模板之间就不再存在有效的连接或关系。

使用蓝图，蓝图定义（应该部署的内容）和蓝图分配（已部署的内容）之间的关系仍然存在 。此连接支持改进部署的跟踪和审核。蓝图也能一次性升级由同一蓝图管理的多个订阅。

无需在资源管理器模板和蓝图之间进行选择。每个蓝图可以包含零个或多个资源管理器模板项目 。此支持意味着可以在蓝图中重复使用以前的资源管理器模板库开发和维护工作。

与 Azure Policy 的不同之处

蓝图是一个包或容器，用于组合与 Azure 云服务、安全性和设计的实现相关的一组针对目标的标准、模式和要求，这些标准、模式和要求可以重复使用以确保一致性和符合性。

策略是默认允许和显式拒绝系统，侧重于部署期间的资源属性，用于现有资源。它会验证订阅中的资源是否符合要求和标准，以此为云治理提供支持。

在蓝图中包含策略可以在分配蓝图期间创建正确的模式或设计。包含策略可确保只对环境进行批准或预期的更改，以确保持续符合蓝图意向。

策略可作为众多项目中的一项包含在蓝图定义中 。蓝图还支持在策略和计划中使用参数。

蓝图定义

蓝图由项目组成 。蓝图目前支持以下资源作为项目：

资源	层次结构选项	DESCRIPTION
资源组	订阅	创建新资源组以供蓝图中的其他项目使用。通过这些占位符资源组，可以按照所需方式组织资源，并为包含的策略和角色分配项目以及 Azure 资源管理器模板提供范围限制。
Azure 资源管理器模板	订阅、资源组	模板用于组合复杂的环境。示例环境：SharePoint 场、Azure 自动化状态配置或 Log Analytics 工作区。
策略分配	订阅、资源组	将蓝图分配到订阅后，允许将策略或计划分配给该订阅。该策略或计划必须位于蓝图定义位置的范围内。若策略或计划具有参数，则在创建蓝图时或在蓝图分配期间分配这些参数。
角色分配	订阅、资源组	将现有用户或组添加到内置角色，以确保始终为正确的人员提供正确的资源访问权限。可为整个订阅定义角色分配，也可将其嵌套到蓝图所包含的特定资源组。

蓝图定义位置

创建蓝图定义时，将定义蓝图的保存位置。蓝图可以保存到你有参与者访问权限的管理组或订阅。如果位置是一个管理组，则蓝图可以分配给该管理组的任何子级订阅。

蓝图参数

蓝图可以将参数传递给策略/计划或 Azure 资源管理器模板。将任意项目添加到蓝图时，由创建者决定为每个蓝图分配提供定义的值，或者让每个蓝图分配在分配时提供一个值 。这种灵活性让创建者可以为蓝图的所有使用定义预定值或者在分配时做出该决定。

> **NOTE**
> 蓝图可以有自己的参数，但目前只能为从 REST API 而不是从门户生成的蓝图创建这些参数。

有关更多信息，请参阅蓝图参数。

蓝图发布

首次创建蓝图时，将视其为处于“草稿”模式 。准备分配蓝图时，它必须处于“已发布”模式 。发布需要定义“版本”字符串（字母、数字和连字符，最大长度为 20 个字符）以及可选的“更改注释” 。该版本将其与针对同一蓝图的未来更改进行区别，并允许分配每个版本 。此版本控制也意味着可将同一蓝图的不同版本分配给同一订阅 。对蓝图进行其他更改时，除未发布的更改外，已发布版本仍然存在 。更改完成后，更新的蓝图是使用新的唯一版本发布的，现也可进行分配 。

蓝图分配

可将蓝图的每个已发布版本（最大名称长度为 90 个字符）分配给现有订阅 。在门户中，该蓝图默认使用最新发布的版本 。若存在项目参数（或蓝图参数），则在分配过程中定义参数。

Azure 蓝图中的权限

若要使用蓝图，必须通过基于角色的访问控制 (RBAC) 获得授权。要创建蓝图，帐户需要以下权限：

- `Microsoft.Blueprint/blueprints/write` - 创建蓝图定义
- `Microsoft.Blueprint/blueprints/artifacts/write` - 在蓝图定义上创建项目
- `Microsoft.Blueprint/blueprints/versions/write` - 发布蓝图

要删除蓝图，帐户需要以下权限：

- `Microsoft.Blueprint/blueprints/delete`
- `Microsoft.Blueprint/blueprints/artifacts/delete`
- `Microsoft.Blueprint/blueprints/versions/delete`

> **NOTE**
> 必须在保存蓝图定义的管理组或订阅范围上授予或继承蓝图定义权限。

要分配或取消分配蓝图，帐户需要以下权限：

- `Microsoft.Blueprint/blueprintAssignments/write` - 分配蓝图
- `Microsoft.Blueprint/blueprintAssignments/delete` - 取消分配蓝图

> **NOTE**
> 由于在订阅上创建了蓝图分配，因此必须在订阅范围授予蓝图分配和取消分配权限，或者将其继承到订阅范围。

上述所有权限都包含在"所有者"角色中 。"参与者"角色创建了蓝图并删除了蓝图权限，但并没有蓝图分配权限 。若这些内置角色不适合安全需求，请考虑创建自定义角色。

> **NOTE**
> 如果使用系统分配的托管标识，则 Azure 蓝图的服务主体需要在分配的订阅上具有**所有者**角色才能启用部署。若使用门户，则会自动为部署授予和撤消此角色。若使用 REST API，则必须手动授予此角色，但在部署完成后仍会自动撤消此角色。如果使用用户分配的托管标识，则只有创建蓝图分配的用户才需要"所有者" 权限。

命名限制

下面是某些字段存在的限制列表：

OBJECT	字段	允许的字符	最大 LENGTH
蓝图	Name	字母、数字、连字符和句点	48
蓝图	版本	字母、数字、连字符和句点	20
蓝图分配	Name	字母、数字、连字符和句点	90
蓝图项目	Name	字母、数字、连字符和句点	48

视频概述

以下 Azure 蓝图概述来自 Azure Fridays。如需下载视频，请访问第 9 频道的 Azure Fridays - An overview of Azure Blueprints（Azure Fridays - Azure 蓝图概述）。

后续步骤

- 创建蓝图 - 门户
- 创建蓝图 - REST API

快速入门:在门户中定义和分配蓝图

2019/9/5 • • Edit Online

了解如何创建和分配蓝图时，可以定义常见的模式，以便根据 Azure 资源管理器模板、策略、安全性等方面的要求开发可重复使用和可快速部署的配置。本教程介绍如何使用 Azure 蓝图来执行某些与在组织中创建、发布和分配蓝图相关的常见任务。这些任务包括：

- 新建蓝图并添加各种受支持的项目
- 对仍处于“草稿”状态的现有蓝图进行更改
- 使用“已发布”将蓝图标记为分配就绪
- 向现有订阅分配蓝图
- 检查已分配蓝图的状态和进度
- 删除已向订阅分配的蓝图

如果没有 Azure 订阅，请在开始之前创建一个免费帐户。

创建蓝图

定义符合性的标准模式的第一步是根据可用资源构建蓝图。本示例将创建名为 **MyBlueprint** 的新蓝图，以配置订阅的角色和策略分配。然后，将添加新的资源组，并在该资源组中创建资源管理器模板和角色分配。

1. 在左侧窗格中，选择“所有服务”。搜索并选择“蓝图”。

2. 从左侧页面选择“蓝图定义”，然后选择页面顶部的“+ 创建蓝图”按钮。

   或者，选择“入门”页上的“创建”，直接创建一个蓝图。

3. 提供蓝图名称，例如 **MyBlueprint**。（最多使用 48 个字母和数字，但不要包含空格或特殊字符）。暂时将“蓝图说明”留空。

4. 在“定义位置”框中，选择右侧的省略号，选择要在其中保存蓝图的管理组或订阅，然后选择“选择”。

5. 确认信息是否正确。稍后无法更改“蓝图名称”和“定义位置”字段。然后选择页面底部的“下一步: 项目”或页面顶部的“项目”选项卡。

6. 添加订阅级别的角色分配：

   a. 在“订阅”下选择“+ 添加项目”行。随即会在浏览器右侧打开“添加项目”窗口。

   b. 为“项目类型”选择“角色分配”。

   c. 在“角色”下，选择“参与者”。保留选中“添加用户、应用或组”框，指示使用动态参数。

   d. 选择“添加”将此项目添加到蓝图中。

> **NOTE**
>
> 大多数项目支持参数。在蓝图创建期间为其分配值的参数是静态参数 。如果在蓝图分配期间分配参数，则该参数是动态参数 。有关更多信息，请参阅蓝图参数。

7. 添加订阅级别的策略分配：
   a. 选择角色分配项目下的"+ 添加项目"行 。
   b. 为"项目类型"选择"策略分配" 。
   c. 将"类型"更改为"内置" 。在"搜索"中输入 **tag**。
   d. 单击"搜索" 以进行筛选。选择"对资源组追加标记及其默认值" 。
   e. 选择"添加" 将此项目添加到蓝图中。
8. 选择策略分配行"对资源组追加标记及其默认值"。
9. 随即将打开作为蓝图定义一部分的向项目提供参数的窗口，并允许基于此蓝图而不是在分配期间（动态参数）设置所有分配的参数（静态参数）。此示例在蓝图分配期间使用动态参数，因此请保留默认值并选择"取消" 。
10. 添加订阅级别的资源组：
    a. 在"订阅"下选择"+ 添加项目"行 。
    b. 为"项目类型"选择"资源组" 。
    c. 将"项目显示名称"、"资源组名称"和"位置"框留空，但请确保在每个参数属性上选中该复选框，以使其成为动态参数 。
    d. 选择"添加" 将此项目添加到蓝图中。
11. 在资源组下添加模板：
    a. 在"ResourceGroup"条目下选择"+ 添加项目"行 。
    b. 为"项目类型"选择"Azure 资源管理器模板"，将"项目显示名称"设置为"StorageAccount"，并将"说明"保留为空 。
    c. 在编辑器框的"模板" 选项卡上，粘贴以下资源管理器模板。粘贴模板后，选择"参数"选项卡，并注意已检测到模板参数 storageAccountType 和 location 。将自动检测并填充每个参数，但将其配置为"动态参数"。

> **IMPORTANT**
> 如果导入模板，请确保该文件仅为 JSON 且不包含 HTML。当指向 GitHub 上的 URL 时，请确保已选择“RAW”以获取纯 JSON 文件，而不是用 HTML 包装在 GitHub 上显示的文件。如果导入的模板不是纯 JSON，则会出现错误。

```
{
    "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
    "contentVersion": "1.0.0.0",
    "parameters": {
        "storageAccountType": {
            "type": "string",
            "defaultValue": "Standard_LRS",
            "allowedValues": [
                "Standard_LRS",
                "Standard_GRS",
                "Standard_ZRS",
                "Premium_LRS"
            ],
            "metadata": {
                "description": "Storage Account type"
            }
        },
        "location": {
            "type": "string",
            "defaultValue": "[resourceGroup().location]",
            "metadata": {
                "description": "Location for all resources."
            }
        }
    },
    "variables": {
        "storageAccountName": "[concat('store', uniquestring(resourceGroup().id))]"
    },
    "resources": [{
        "type": "Microsoft.Storage/storageAccounts",
        "name": "[variables('storageAccountName')]",
        "location": "[parameters('location')]",
        "apiVersion": "2018-07-01",
        "sku": {
            "name": "[parameters('storageAccountType')]"
        },
        "kind": "StorageV2",
        "properties": {}
    }],
    "outputs": {
        "storageAccountName": {
            "type": "string",
            "value": "[variables('storageAccountName')]"
        }
    }
}
```

d. 清除该 storageAccountType 复选框，并请注意，下拉列表仅包含 allowedValues 下的资源管理器模板中包含的值 。选中此框将其重新设置为动态参数。

e. 选择“添加” 将此项目添加到蓝图中。

12. 已完成的蓝图应如下所示：请注意，每个项目在“参数”列下都显示“已填充 y 个参数中的 x 个”。动态参数在每次分配蓝图期间设置。

13. 现在已添加所有计划项目，请选择页面底部的“保存草稿”。

编辑蓝图

在创建蓝图中，未提供说明，也未将角色分配添加到新资源组。二者都可按以下步骤修复：

1. 从左侧页面中选择“蓝图定义”。
2. 在蓝图列表中，右键单击之前创建的蓝图，然后选择“编辑蓝图”。
3. 在“蓝图说明”中，提供有关蓝图和组成它的项目的一些信息。在本示例中，输入如下内容：“此蓝图在订阅上设置标记策略和角色分配，创建 ResourceGroup，并将资源模板和角色分配部署到该 ResourceGroup。”
4. 选择“下一步：项目”或页面顶部的“项目”选项卡。
5. 在资源组下添加角色分配：
   a. 在“ResourceGroup”条目下选择“+ 添加项目”行。
   b. 为“项目类型”选择“角色分配”。
   c. 在“角色”下，选择“所有者”并清除“添加用户、应用或组”框下的复选框。
   d. 搜索并选择要添加的用户、应用或组。此项目使用每次分配此蓝图时以同样方式设置的静态参数。
   e. 选择“添加”将此项目添加到蓝图中。

6. 已完成的蓝图应如下所示：请注意，新添加的角色分配显示"已填充 1 个参数中的 1 个"。这意味着它是一个静态参数。

7. 草稿更新后，请单击"保存草稿"。

发布蓝图

现在，所有计划项目都已添加到蓝图中，可以将其发布了。发布后，即可将蓝图分配到订阅。

1. 从左侧页面中选择"蓝图定义"。
2. 在蓝图列表中，右键单击之前创建的蓝图，然后选择"发布蓝图"。
3. 在打开的窗格中，提供版本（字母、数字和连字符，最大长度为 20 个字符），例如"v1"。（可选）并提供更改注释，例如"首次发布"。
4. 选择页面底部的"发布"。

分配蓝图

发布蓝图后，可将其分配到订阅。将创建的蓝图分配到管理组层次结构下的一个订阅。如果蓝图保存到某个订阅，则只能将其分配给该订阅。

1. 从左侧页面中选择"蓝图定义"。
2. 在蓝图列表中，右键单击之前创建的蓝图（或选择省略号），然后选择"分配蓝图"。
3. 在"分配蓝图"页面上，从"订阅"下拉列表中选择要将此蓝图部署到的订阅。

如果 Azure 计费中提供了受支持的企业产品/服务，则会在“订阅”框下激活“新建”链接 。执行以下步骤:

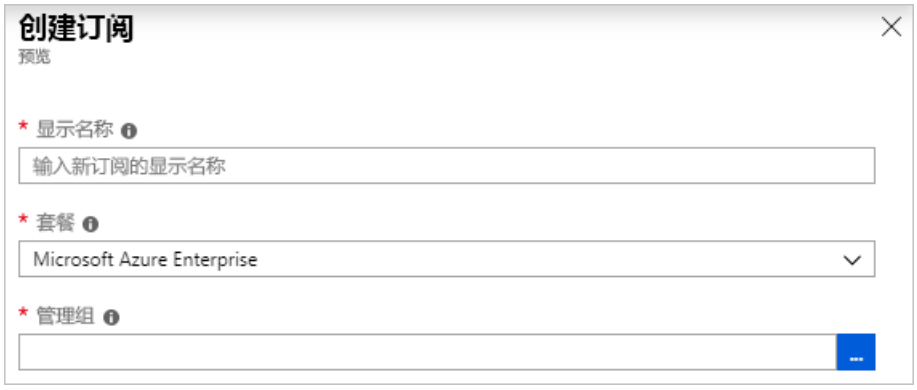
a. 选择“新建”链接以创建新订阅，而不是选择现有订阅 。

b. 提供新订阅的“显示名称” 。

c. 从下拉列表中选择可用“产品/服务” 。

d. 使用省略号选择管理组，订阅将是其子级。

e. 在页面底部选择“创建” 。



> **IMPORTANT**
> 选择“创建”后，将立即创建新订阅 。

> **NOTE**
> 将为选择每个订阅创建一个分配。可以在以后对单个订阅分配进行更改，而不强制对所选订阅的其余部分进行更改。

4. 对于“分配名称”，请为此分配提供唯一名称 。
5. 在“位置” 中，选择要在其中创建托管标识和订阅部署对象的区域。Azure 蓝图使用此托管标识在分配的蓝图中部署所有项目。若要了解详细信息，请参阅 Azure 资源的托管标识。
6. 在“v1” 条目上保留已发布 版本的“蓝图定义版本” 下拉列表。（默认为最近的已发布版本。）
7. 对于“锁定分配”，保留默认值“不锁定” 。有关详细信息，请参阅蓝图资源锁定。

8. 在托管标识下，保留默认值“系统已分配” 。
9. 对于订阅级别的角色分配“[用户组或应用程序名称]: 参与者”，搜索并选择用户、应用或组。
10. 对于订阅级别策略分配，请将“标记名称” 设置为“CostCenter”，并将“标记值” 设置为“ContosoIT” 。
11. 对于“ResourceGroup”，从下拉列表中提供“StorageAccount”的名称 和“East US 2”的位置 。

> **NOTE**
> 对于在蓝图定义期间在资源组下添加的每个项目，该项目将缩进以与将部署的资源组或对象对齐。只有在上下文信息中才会列出无法获取参数或者在分配时没有要定义的参数的项目。

12. 在 Azure 资源管理器模板“StorageAccount”上，为 storageAccountType 参数选择“Standard_GRS”。
13. 阅读页面底部的信息框，然后选择“分配”。

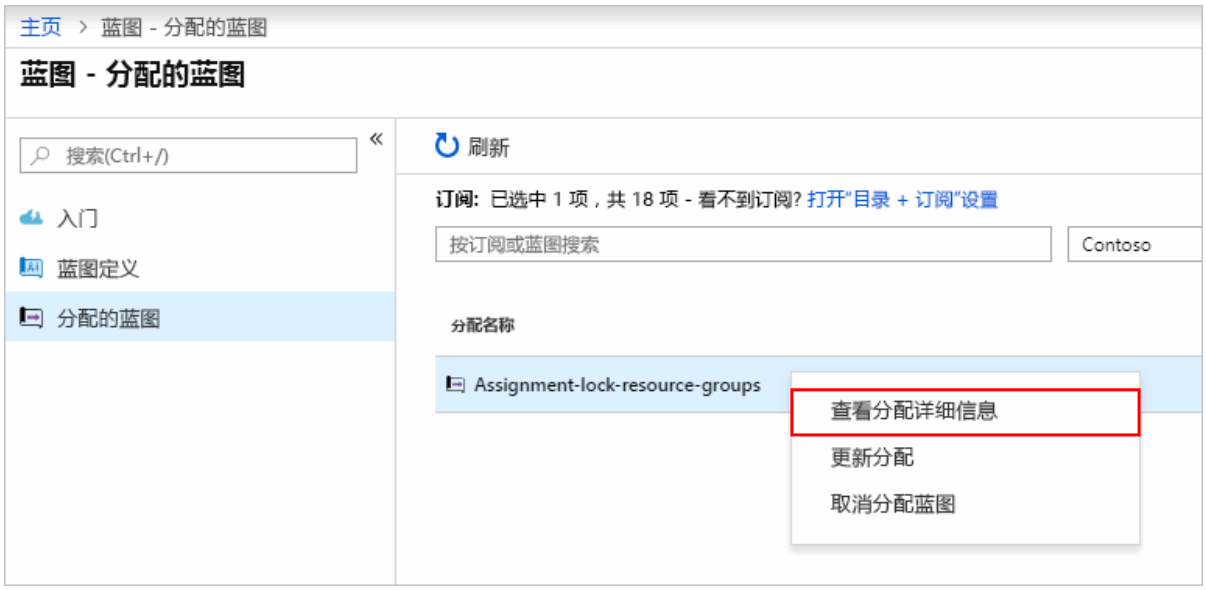
跟踪蓝图的部署

将蓝图分配给一个或多个订阅时，会发生以下两种情况：

- 蓝图将添加到每个订阅的“分配的蓝图”页
- 开始部署蓝图定义的所有项目的过程。

现在已将蓝图分配给订阅，请验证部署的进度：

1. 从左侧页面选择“分配的蓝图”。
2. 在蓝图列表中，右键单击之前分配的一个蓝图，然后选择“查看分配详细信息”。



3. 在“蓝图分配”页面上，验证是否已成功部署所有项目，以及在部署期间是否未出现任何错误。如果发生错误，请参阅蓝图故障排除，了解确定错误原因的操作步骤。

取消分配蓝图

如果不再需要蓝图，请从订阅中删除蓝图分配。蓝图可能已被替换为更新的蓝图，后者具有更新的模式、策略和设计。删除蓝图时，作为该蓝图的一部分分配的项目将保留。若要删除蓝图分配，请按照下列步骤操作：

1. 从左侧页面选择“分配的蓝图”。
2. 在蓝图列表中，选择要取消分配的蓝图。然后选择页面顶部的“取消分配蓝图”按钮。
3. 阅读确认消息，然后选择“确定”。

删除蓝图

1. 从左侧页面中选择“蓝图定义”。
2. 右键单击要删除的蓝图，然后选择“删除蓝图”。在确认对话框中选择“是”。

> **NOTE**
>
> 删除此方法中的蓝图还会删除所选蓝图的所有已发布版本。若要删除单个版本，请打开蓝图，选择“已发布版本”选项卡，选择要删除的版本，然后选择“删除此版本”。另外，只有在删除蓝图定义的所有蓝图分配之后，才能删除该蓝图。

后续步骤

- 了解蓝图生命周期。
- 了解如何使用静态和动态参数。
- 了解如何自定义蓝图排序顺序。
- 了解如何利用蓝图资源锁定。
- 了解如何更新现有分配。
- 使用一般故障排除在蓝图的分配期间解决问题。

快速入门：使用 PowerShell 定义和分配 Azure 蓝图

2019/9/5 • • Edit Online

了解如何创建和分配蓝图以后即可定义常见的模式，以便根据资源管理器模板、策略、安全性等方面的要求开发可重复使用和可快速部署的配置。本教程介绍如何使用 Azure 蓝图来执行某些与在组织中创建、发布和分配蓝图相关的常见任务，例如：

- 新建蓝图并添加各种受支持的项目
- 对仍处于“草稿”状态的现有蓝图进行更改
- 使用“已发布”将蓝图标记为分配就绪
- 向现有订阅分配蓝图
- 检查已分配蓝图的状态和进度
- 删除已向订阅分配的蓝图

如果没有 Azure 订阅，请在开始之前创建一个免费帐户。

创建蓝图

定义符合性的标准模式的第一步是根据可用资源构建蓝图。我们将创建名为“MyBlueprint”的蓝图，以配置订阅的角色和策略分配。然后，我们将添加资源组、资源管理器模板，然后在资源组上添加角色分配。

> **NOTE**
> 使用 PowerShell 时，首先创建 blueprint 对象 。对于每个要添加的具有参数的项目，需要在初始蓝图上提前定义该参数 。

1. 创建初始 blueprint 对象 。**BlueprintFile** 参数接受一个 JSON 文件，该文件包含有关蓝图、要创建的任何资源组和所有蓝图级别参数的属性。参数在分配过程中设置并由在后续步骤中添加的项目使用。

   - JSON 文件 - blueprint.json

```
{
    "properties": {
        "description": "This blueprint sets tag policy and role assignment on the subscription,
creates a ResourceGroup, and deploys a resource template and role assignment to that
ResourceGroup.",
        "targetScope": "subscription",
        "parameters": {
            "storageAccountType": {
                "type": "string",
                "defaultValue": "Standard_LRS",
                "allowedValues": [
                    "Standard_LRS",
                    "Standard_GRS",
                    "Standard_ZRS",
                    "Premium_LRS"
                ],
                "metadata": {
                    "displayName": "storage account type.",
                    "description": null
                }
            },
            "tagName": {
                "type": "string",
                "metadata": {
                    "displayName": "The name of the tag to provide the policy assignment.",
                    "description": null
                }
            },
            "tagValue": {
                "type": "string",
                "metadata": {
                    "displayName": "The value of the tag to provide the policy assignment.",
                    "description": null
                }
            },
            "contributors": {
                "type": "array",
                "metadata": {
                    "description": "List of AAD object IDs that is assigned Contributor role at
the subscription",
                    "strongType": "PrincipalId"
                }
            },
            "owners": {
                "type": "array",
                "metadata": {
                    "description": "List of AAD object IDs that is assigned Owner role at the
resource group",
                    "strongType": "PrincipalId"
                }
            }
        },
        "resourceGroups": {
            "storageRG": {
                "description": "Contains the resource template deployment and a role assignment."
            }
        }
    }
}
```

- PowerShell 命令

```
# Login first with Connect-AzAccount if not using Cloud Shell

# Get a reference to the new blueprint object, we'll use it in subsequent steps
$blueprint = New-AzBlueprint -Name 'MyBlueprint' -BlueprintFile .\blueprint.json
```

> **NOTE**
> 以编程方式创建蓝图定义时，请使用文件名 *blueprint.json*。调用 Import-AzBlueprintWithArtifact 时使用此文件名。

默认情况下，会在默认订阅中创建蓝图对象。若要指定管理组，请使用参数 **ManagementGroupId**。若要指定订阅，请使用参数 **SubscriptionId**。

2. 在订阅中添加角色分配。**ArtifactFile** 定义项目的种类、与角色定义标识符一致的属性以及以值的数组形式传递的主体标识 。在下面的示例中，主体标识被授予指定的角色，配置为蓝图分配过程中所设置的参数。此示例使用 GUID 为 `b24988ac-6180-42a0-ab88-20f7382dd24c` 的"参与者" 内置角色。

   - JSON 文件 - \artifacts\roleContributor.json

   ```
   {
       "kind": "roleAssignment",
       "properties": {
           "roleDefinitionId": "/providers/Microsoft.Authorization/roleDefinitions/b24988ac-6180-
   42a0-ab88-20f7382dd24c",
           "principalIds": "[parameters('contributors')]"
       }
   }
   ```

   - PowerShell 命令

   ```
   # Use the reference to the new blueprint object from the previous steps
   New-AzBlueprintArtifact -Blueprint $blueprint -Name 'roleContributor' -ArtifactFile
   .\artifacts\roleContributor.json
   ```

3. 在订阅中添加策略分配。**ArtifactFile** 定义项目的种类、与策略或计划定义一致的属性，并配置策略分配，以使用要在蓝图分配过程中配置的已定义蓝图参数 。此示例使用 GUID 为 `49c88fc8-6fd1-46fd-a676-f12d1d3a4c71` 的"将标记及其默认值应用于资源组"内置策略。

   - JSON 文件 - \artifacts\policyTags.json

   ```
   {
       "kind": "policyAssignment",
       "properties": {
           "displayName": "Apply tag and its default value to resource groups",
           "description": "Apply tag and its default value to resource groups",
           "policyDefinitionId": "/providers/Microsoft.Authorization/policyDefinitions/49c88fc8-
   6fd1-46fd-a676-f12d1d3a4c71",
           "parameters": {
               "tagName": {
                   "value": "[parameters('tagName')]"
               },
               "tagValue": {
                   "value": "[parameters('tagValue')]"
               }
           }
       }
   }
   ```

- PowerShell 命令

```
# Use the reference to the new blueprint object from the previous steps
New-AzBlueprintArtifact -Blueprint $blueprint -Name 'policyTags' -ArtifactFile
.\artifacts\policyTags.json
```

4. 在订阅中为存储标记(重复使用 storageAccountType 参数)添加其他策略分配 。此附加的策略分配项目演示了蓝图上定义的参数可由多个项目使用。在示例中，storageAccountType 用于在资源组上设置一个标记 。此值提供有关下一步骤中创建的存储帐户的信息。此示例使用 GUID 为 `49c88fc8-6fd1-46fd-a676-f12d1d3a4c71` 的"将标记及其默认值应用于资源组"内置策略。

   - JSON 文件 - \artifacts\policyStorageTags.json

```
{
    "kind": "policyAssignment",
    "properties": {
        "displayName": "Apply storage tag to resource group",
        "description": "Apply storage tag and the parameter also used by the template to resource
groups",
        "policyDefinitionId": "/providers/Microsoft.Authorization/policyDefinitions/49c88fc8-
6fd1-46fd-a676-f12d1d3a4c71",
        "parameters": {
            "tagName": {
                "value": "StorageType"
            },
            "tagValue": {
                "value": "[parameters('storageAccountType')]"
            }
        }
    }
}
```

   - PowerShell 命令

```
# Use the reference to the new blueprint object from the previous steps
New-AzBlueprintArtifact -Blueprint $blueprint -Name 'policyStorageTags' -ArtifactFile
.\artifacts\policyStorageTags.json
```

5. 在资源组下添加模板。资源管理器模板的 **TemplateFile** 包含模板的标准 JSON 组件。系统会向模板一一传递 **storageAccountType**、**tagName** 和 **tagValue** 蓝图参数，让模板重复使用这些参数。通过使用参数 **TemplateParameterFile** 和在使用键-值对的模板 JSON 中来注入值，模板可以使用蓝图参数。蓝图和模板参数名称可以相同。

   - JSON Azure 资源管理器模板文件 - \artifacts\templateStorage.json

```
{
    "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
    "contentVersion": "1.0.0.0",
    "parameters": {
        "storageAccountTypeFromBP": {
            "type": "string",
            "metadata": {
                "description": "Storage Account type"
            }
        },
        "tagNameFromBP": {
            "type": "string",
            "defaultValue": "NotSet",
            "metadata": {
                "description": "Tag name from blueprint"
            }
        },
        "tagValueFromBP": {
            "type": "string",
            "defaultValue": "NotSet",
            "metadata": {
                "description": "Tag value from blueprint"
            }
        }
    },
    "variables": {
        "storageAccountName": "[concat(uniquestring(resourceGroup().id), 'standardsa')]"
    },
    "resources": [{
        "type": "Microsoft.Storage/storageAccounts",
        "name": "[variables('storageAccountName')]",
        "apiVersion": "2016-01-01",
        "tags": {
            "[parameters('tagNameFromBP')]": "[parameters('tagValueFromBP')]"
        },
        "location": "[resourceGroup().location]",
        "sku": {
            "name": "[parameters('storageAccountTypeFromBP')]"
        },
        "kind": "Storage",
        "properties": {}
    }],
    "outputs": {
        "storageAccountSku": {
            "type": "string",
            "value": "[variables('storageAccountName')]"
        }
    }
}
```

- JSON Azure 资源管理器模板参数文件 - \artifacts\templateStorageParams.json

```
{
    "$schema": "https://schema.management.azure.com/schemas/2015-01-
01/deploymentParameters.json#",
    "contentVersion": "1.0.0.0",
    "parameters": {
        "storageAccountTypeFromBP": {
            "value": "[parameters('storageAccountType')]"
        },
        "tagNameFromBP": {
            "value": "[parameters('tagName')]"
        },
        "tagValueFromBP": {
            "value": "[parameters('tagValue')]"
        }
    }
}
```

- PowerShell 命令

```
# Use the reference to the new blueprint object from the previous steps
New-AzBlueprintArtifact -Blueprint $blueprint -Type TemplateArtifact -Name 'templateStorage' -
TemplateFile .\artifacts\templateStorage.json -TemplateParameterFile
.\artifacts\templateStorageParams.json -ResourceGroupName storageRG
```

6. 在资源组下添加角色分配。与上一角色分配项类似，以下示例对“所有者”角色使用定义标识符，并向其提供不同于蓝图参数的另一参数 。此示例使用 GUID 为 `8e3af657-a8ff-443c-a75c-2fe8c4bcb635` 的“所有者” 内置角色。

   - JSON 文件 - \artifacts\roleOwner.json

```
{
    "kind": "roleAssignment",
    "properties": {
        "resourceGroup": "storageRG",
        "roleDefinitionId": "/providers/Microsoft.Authorization/roleDefinitions/8e3af657-a8ff-
443c-a75c-2fe8c4bcb635",
        "principalIds": "[parameters('owners')]"
    }
}
```

   - PowerShell 命令

```
# Use the reference to the new blueprint object from the previous steps
New-AzBlueprintArtifact -Blueprint $blueprint -Name 'roleOwner' -ArtifactFile
.\artifacts\roleOwner.json
```

发布蓝图

现在，项目已添加到蓝图，可以将其发布了。发布后，即可将其分配到订阅。

```
# Use the reference to the new blueprint object from the previous steps
Publish-AzBlueprint -Blueprint $blueprint -Version '{BlueprintVersion}'
```

`{BlueprintVersion}` 的值为最大长度为 20 个字符的字母、数字和连字符（不含空格或其他特殊字符）字符串。使用唯一且具有信息性的内容，如 v20180622-135541 。

分配蓝图

使用 PowerShell 发布蓝图后，即可将其分配给订阅。将你创建的蓝图分配给管理组层次结构下的一个订阅。如果蓝图保存到某个订阅，则只能将其分配给该订阅。**Blueprint** 参数指定要分配的蓝图。若要提供名称、位置、标识、锁定和蓝图参数，请在 `New-AzBlueprintAssignment` cmdlet 上使用匹配的 PowerShell 参数，或在 **AssignmentFile** 参数 JSON 文件中提供这些参数。

1. 通过将蓝图部署分配到订阅，运行它。由于“参与者”和“所有者”参数需要主体的 objectId 数组才能授予角色分配，因此请使用 Azure Active Directory Graph API 来收集 objectId，以供自己的用户、组或服务主体在 **AssignmentFile** 中使用 。

   - JSON 文件 - blueprintAssignment.json

```
{
    "properties": {
        "blueprintId":
"/providers/Microsoft.Management/managementGroups/{YourMG}/providers/Microsoft.Blueprint/blueprin
ts/MyBlueprint",
        "resourceGroups": {
            "storageRG": {
                "name": "StorageAccount",
                "location": "eastus2"
            }
        },
        "parameters": {
            "storageAccountType": {
                "value": "Standard_GRS"
            },
            "tagName": {
                "value": "CostCenter"
            },
            "tagValue": {
                "value": "ContosoIT"
            },
            "contributors": {
                "value": [
                    "7be2f100-3af5-4c15-bcb7-27ee43784a1f",
                    "38833b56-194d-420b-90ce-cff578296714"
                ]
            },
            "owners": {
                "value": [
                    "44254d2b-a0c7-405f-959c-f829ee31c2e7",
                    "316deb5f-7187-4512-9dd4-21e7798b0ef9"
                ]
            }
        }
    },
    "identity": {
        "type": "systemAssigned"
    },
    "location": "westus"
}
```

   - PowerShell 命令

```
# Use the reference to the new blueprint object from the previous steps
New-AzBlueprintAssignment -Blueprint $blueprint -Name 'assignMyBlueprint' -AssignmentFile
.\blueprintAssignment.json
```

   - 用户分配的托管标识

蓝图分配也可使用用户分配的托管标识。在此示例中，JSON 分配文件的 **identity** 部分更改如下。将 `{tenantId}`、`{subscriptionId}`、`{yourRG}` 和 `{userIdentity}` 分别替换为你的 tenantId、subscriptionId、资源组名称和用户分配的托管标识的名称。

```
"identity": {
    "type": "userAssigned",
    "tenantId": "{tenantId}",
    "userAssignedIdentities": {

"/subscriptions/{subscriptionId}/resourceGroups/{yourRG}/providers/Microsoft.ManagedIdentity/user
AssignedIdentities/{userIdentity}": {}
    }
},
```

用户分配的托管标识可以位于任何订阅和资源组中，只要分配蓝图的用户有权访问它即可。

> **IMPORTANT**
>
> 蓝图不管理用户分配的托管标识。用户负责分配足够的角色和权限，否则蓝图分配会失败。

取消分配蓝图

可以从订阅中删除蓝图。通常会在不再需要项目资源时将其删除。删除蓝图时，作为该蓝图的一部分分配的项目将保留。若要删除蓝图分配，请使用 `Remove-AzBlueprintAssignment` cmdlet：

assignMyBlueprint

```
Remove-AzBlueprintAssignment -Name 'assignMyBlueprint'
```

后续步骤

- 了解蓝图生命周期。
- 了解如何使用静态和动态参数。
- 了解如何自定义蓝图排序顺序。
- 了解如何利用蓝图资源锁定。
- 了解如何更新现有分配。
- 使用一般故障排除在蓝图的分配期间解决问题。

快速入门：使用 REST API 定义和分配 Azure 蓝图

2019/9/5 • • Edit Online

了解如何创建和分配蓝图以后即可定义常见的模式，以便根据资源管理器模板、策略、安全性等方面的要求开发可重复使用和可快速部署的配置。本教程介绍如何使用 Azure 蓝图来执行某些与在组织中创建、发布和分配蓝图相关的常见任务，例如：

- 新建蓝图并添加各种受支持的项目
- 对仍处于“草稿”状态的现有蓝图进行更改
- 使用“已发布”将蓝图标记为分配就绪
- 向现有订阅分配蓝图
- 检查已分配蓝图的状态和进度
- 删除已向订阅分配的蓝图

如果没有 Azure 订阅，请在开始之前创建一个免费帐户。

REST API 入门

如果不熟悉 REST API，请首先查看 Azure REST API 参考，大致了解 REST API，尤其是请求 URI 和请求正文。本文使用这些概念来提供有关如何使用 Azure 蓝图的说明，并假定具有相关的实践经验。ARMClient 和其他工具可自动处理授权，建议初学者使用。

有关蓝图规范，请参阅 Azure 蓝图 REST API。

REST API 和 PowerShell

如果尚无用于进行 REST API 调用的工具，请考虑使用 PowerShell 获取说明。下面是使用 Azure 进行身份验证的示例标头。生成身份验证标头，有时称为持有者令牌，然后向要连接到的 REST API URI 提供任何参数或请求正文：

```
# Log in first with Connect-AzAccount if not using Cloud Shell

$azContext = Get-AzContext
$azProfile =
[Microsoft.Azure.Commands.Common.Authentication.Abstractions.AzureRmProfileProvider]::Instance.Profile
$profileClient = New-Object -TypeName Microsoft.Azure.Commands.ResourceManager.Common.RMProfileClient -
ArgumentList ($azProfile)
$token = $profileClient.AcquireAccessToken($azContext.Subscription.TenantId)
$authHeader = @{
    'Content-Type'='application/json'
    'Authorization'='Bearer ' + $token.AccessToken
}

# Invoke the REST API
$restUri = 'https://management.azure.com/subscriptions/{subscriptionId}?api-version=2016-06-01'
$response = Invoke-RestMethod -Uri $restUri -Method Get -Headers $authHeader
```

替换上面 $restUri 变量中的 `{subscriptionId}`，以获取订阅的相关信息 。$Response 变量可保留 `Invoke-RestMethod` cmdlet 的结果，后者可使用 ConvertFrom-Json 之类的 cmdlet 进行分析。如果 REST API 服务终结点需要请求正文，请向 `Invoke-RestMethod` 的 `-Body` 参数提供 JSON 格式的变量 。

创建蓝图

定义符合性的标准模式的第一步是根据可用资源构建蓝图。我们将创建名为“MyBlueprint”的蓝图，以配置订阅的

角色和策略分配。然后，我们将添加资源组、资源管理器模板，然后在资源组上添加角色分配。

> **NOTE**
> 使用 REST API 时，首先创建 blueprint 对象 。对于每个要添加的具有参数的项目，需要在初始蓝图上提前定义该参数 。

在每个 REST API URI 中，包含替换为自己的值所使用的变量：

- `{YourMG}` - 替换为管理组的 ID
- `{subscriptionId}` - 替换为订阅 ID

> **NOTE**
> 也可以在订阅级别创建蓝图。要查看示例，请参阅在订阅示例级别创建蓝图。

1. 创建初始 blueprint 对象 。请求正文包括有关蓝图的属性、要创建的任何资源组，以及所有蓝图级别参数 。参数在分配过程中设置并由在后续步骤中添加的项目使用。

   - REST API URI

     ```
     PUT
     https://management.azure.com/providers/Microsoft.Management/managementGroups/{YourMG}/providers/Microsoft.Blueprint/blueprints/MyBlueprint?api-version=2018-11-01-preview
     ```

   - 请求正文

```
{
    "properties": {
        "description": "This blueprint sets tag policy and role assignment on the subscription,
creates a ResourceGroup, and deploys a resource template and role assignment to that
ResourceGroup.",
        "targetScope": "subscription",
        "parameters": {
            "storageAccountType": {
                "type": "string",
                "metadata": {
                    "displayName": "storage account type.",
                    "description": null
                }
            },
            "tagName": {
                "type": "string",
                "metadata": {
                    "displayName": "The name of the tag to provide the policy assignment.",
                    "description": null
                }
            },
            "tagValue": {
                "type": "string",
                "metadata": {
                    "displayName": "The value of the tag to provide the policy assignment.",
                    "description": null
                }
            },
            "contributors": {
                "type": "array",
                "metadata": {
                    "description": "List of AAD object IDs that is assigned Contributor role at
the subscription"
                }
            },
            "owners": {
                "type": "array",
                "metadata": {
                    "description": "List of AAD object IDs that is assigned Owner role at the
resource group"
                }
            }
        },
        "resourceGroups": {
            "storageRG": {
                "description": "Contains the resource template deployment and a role assignment."
            }
        }
    }
}
```

2. 在订阅中添加角色分配。请求正文可定义项目的种类、与角色定义标识符一致的属性以及以值的数组形式传递的主体标识 。在下面的示例中，主体标识被授予指定的角色，配置为蓝图分配过程中所设置的参数。此示例使用 GUID 为 `b24988ac-6180-42a0-ab88-20f7382dd24c` 的“参与者” 内置角色。

   - REST API URI

   ```
   PUT
   https://management.azure.com/providers/Microsoft.Management/managementGroups/{YourMG}/providers/M
   icrosoft.Blueprint/blueprints/MyBlueprint/artifacts/roleContributor?api-version=2018-11-01-
   preview
   ```

   - 请求正文

```
{
    "kind": "roleAssignment",
    "properties": {
        "roleDefinitionId": "/providers/Microsoft.Authorization/roleDefinitions/b24988ac-6180-
42a0-ab88-20f7382dd24c",
        "principalIds": "[parameters('contributors')]"
    }
}
```

3. 在订阅中添加策略分配。请求正文可定义项目的种类、与策略或计划定义一致的属性，并配置策略分配，以使用要在蓝图分配过程中配置的已定义蓝图参数 。此示例使用 GUID 为 `49c88fc8-6fd1-46fd-a676-f12d1d3a4c71` 的"将标记及其默认值应用于资源组"内置策略。

   - REST API URI

   ```
   PUT
   https://management.azure.com/providers/Microsoft.Management/managementGroups/{YourMG}/providers/M
   icrosoft.Blueprint/blueprints/MyBlueprint/artifacts/policyTags?api-version=2018-11-01-preview
   ```

   - 请求正文

   ```
   {
       "kind": "policyAssignment",
       "properties": {
           "description": "Apply tag and its default value to resource groups",
           "policyDefinitionId": "/providers/Microsoft.Authorization/policyDefinitions/49c88fc8-
   6fd1-46fd-a676-f12d1d3a4c71",
           "parameters": {
               "tagName": {
                   "value": "[parameters('tagName')]"
               },
               "tagValue": {
                   "value": "[parameters('tagValue')]"
               }
           }
       }
   }
   ```

4. 在订阅中为存储标记（重复使用 storageAccountType 参数）添加其他策略分配 。此附加的策略分配项目演示了蓝图上定义的参数可由多个项目使用。在示例中，storageAccountType 用于在资源组上设置一个标记 。此值提供有关下一步骤中创建的存储帐户的信息。此示例使用 GUID 为 `49c88fc8-6fd1-46fd-a676-f12d1d3a4c71` 的"将标记及其默认值应用于资源组"内置策略。

   - REST API URI

   ```
   PUT
   https://management.azure.com/providers/Microsoft.Management/managementGroups/{YourMG}/providers/M
   icrosoft.Blueprint/blueprints/MyBlueprint/artifacts/policyStorageTags?api-version=2018-11-01-
   preview
   ```

   - 请求正文

```
{
    "kind": "policyAssignment",
    "properties": {
        "description": "Apply storage tag and the parameter also used by the template to resource
groups",
        "policyDefinitionId": "/providers/Microsoft.Authorization/policyDefinitions/49c88fc8-
6fd1-46fd-a676-f12d1d3a4c71",
        "parameters": {
            "tagName": {
                "value": "StorageType"
            },
            "tagValue": {
                "value": "[parameters('storageAccountType')]"
            }
        }
    }
}
```

5. 在资源组下添加模板。资源管理器模板的请求正文包括模板的常规 JSON 组件，并使用 properties.resourceGroup 定义目标资源组 。系统会向模板一一传递 **storageAccountType**、**tagName** 和 **tagValue** 蓝图参数，让模板重复使用这些参数。通过定义 properties.parameters 并置于键/值对用于插入值的模板 JSON 内，蓝图参数可供模板使用 。蓝图和模板参数名称可以相同，但对于如何分别从蓝图项目传入模板项目的说明有所区别。

   - REST API URI

   ```
   PUT
   https://management.azure.com/providers/Microsoft.Management/managementGroups/{YourMG}/providers/M
   icrosoft.Blueprint/blueprints/MyBlueprint/artifacts/templateStorage?api-version=2018-11-01-
   preview
   ```

   - 请求正文

   ```
   {
       "kind": "template",
       "properties": {
           "template": {
               "$schema": "https://schema.management.azure.com/schemas/2015-01-
   01/deploymentTemplate.json#",
               "contentVersion": "1.0.0.0",
               "parameters": {
                   "storageAccountTypeFromBP": {
                       "type": "string",
                       "defaultValue": "Standard_LRS",
                       "allowedValues": [
                           "Standard_LRS",
                           "Standard_GRS",
                           "Standard_ZRS",
                           "Premium_LRS"
                       ],
                       "metadata": {
                           "description": "Storage Account type"
                       }
                   },
                   "tagNameFromBP": {
                       "type": "string",
                       "defaultValue": "NotSet",
                       "metadata": {
                           "description": "Tag name from blueprint"
                       }
                   },
                   "tagValueFromBP": {
                       "type": "string",
   ```

```
                    "defaultValue": "NotSet",
                    "metadata": {
                        "description": "Tag value from blueprint"
                    }
                }
            },
            "variables": {
                "storageAccountName": "[concat(uniquestring(resourceGroup().id), 'standardsa')]"
            },
            "resources": [{
                "type": "Microsoft.Storage/storageAccounts",
                "name": "[variables('storageAccountName')]",
                "apiVersion": "2016-01-01",
                "tags": {
                   "[parameters('tagNameFromBP')]": "[parameters('tagValueFromBP')]"
                },
                "location": "[resourceGroups('storageRG').location]",
                "sku": {
                    "name": "[parameters('storageAccountTypeFromBP')]"
                },
                "kind": "Storage",
                "properties": {}
            }],
            "outputs": {
                "storageAccountSku": {
                    "type": "string",
                    "value": "[variables('storageAccountName')]"
                }
            }
        },
        "resourceGroup": "storageRG",
        "parameters": {
            "storageAccountTypeFromBP": {
                "value": "[parameters('storageAccountType')]"
            },
            "tagNameFromBP": {
                "value": "[parameters('tagName')]"
            },
            "tagValueFromBP": {
                "value": "[parameters('tagValue')]"
            }
        }
    }
}
```

6. 在资源组下添加角色分配。与上一角色分配项类似，以下示例对“所有者”角色使用定义标识符，并向其提供不同于蓝图参数的另一参数 。此示例使用 GUID 为 `8e3af657-a8ff-443c-a75c-2fe8c4bcb635` 的“所有者” 内置角色。

   - REST API URI

     ```
     PUT
     https://management.azure.com/providers/Microsoft.Management/managementGroups/{YourMG}/providers/Microsoft.Blueprint/blueprints/MyBlueprint/artifacts/roleOwner?api-version=2018-11-01-preview
     ```

   - 请求正文

```
{
    "kind": "roleAssignment",
    "properties": {
        "resourceGroup": "storageRG",
        "roleDefinitionId": "/providers/Microsoft.Authorization/roleDefinitions/8e3af657-a8ff-
443c-a75c-2fe8c4bcb635",
        "principalIds": "[parameters('owners')]"
    }
}
```

发布蓝图

现在，项目已添加到蓝图，可以将其发布了。发布后，即可将其分配到订阅。

- REST API URI

```
PUT
https://management.azure.com/providers/Microsoft.Management/managementGroups/{YourMG}/providers/Microsof
t.Blueprint/blueprints/MyBlueprint/versions/{BlueprintVersion}?api-version=2018-11-01-preview
```

`{BlueprintVersion}` 的值为最大长度为 20 个字符的字母、数字和连字符（不含空格或其他特殊字符）字符串。使用唯一且具有信息性的内容，如 v20180622-135541 。

分配蓝图

使用 REST API 发布蓝图后，即可将其分配给订阅。将你创建的蓝图分配给管理组层次结构下的一个订阅。如果蓝图保存到某个订阅，则只能将其分配给该订阅。请求正文可指定要分配的蓝图、向蓝图定义中的任何资源组提供名称和位置，并且提供在蓝图上定义的所有参数并供一个或多个附加项目使用 。

在每个 REST API URI 中，包含替换为自己的值所使用的变量：

- `{tenantId}` - 替换为租户 ID
- `{YourMG}` - 替换为管理组的 ID
- `{subscriptionId}` - 替换为订阅 ID

1. 在目标订阅上，向 Azure 蓝图服务主体提供“所有者”角色 。AppId 是静态的 (`f71766dc-90d9-4b7d-bd9d-4499c4331c3f`)，但服务主体 ID 根据租户各有不同。可以使用以下 REST API 请求租户的详细信息。它可使用具有不同授权的 Azure Active Directory Graph API。

   - REST API URI

   ```
   GET https://graph.windows.net/{tenantId}/servicePrincipals?api-version=1.6&$filter=appId eq
   'f71766dc-90d9-4b7d-bd9d-4499c4331c3f'
   ```

2. 通过将蓝图部署分配到订阅，运行它。由于“参与者”和“所有者”参数要求主体的 objectId 数组被授予角色分配，使用 Azure Active Directory Graph API 来收集 objectId，以供自己的用户、组或服务主体用于请求正文中 。

   - REST API URI

   ```
   PUT
   https://management.azure.com/subscriptions/{subscriptionId}/providers/Microsoft.Blueprint/bluepri
   ntAssignments/assignMyBlueprint?api-version=2018-11-01-preview
   ```

   - 请求正文

```
{
    "properties": {
        "blueprintId":
"/providers/Microsoft.Management/managementGroups/{YourMG}/providers/Microsoft.Blueprint/blueprin
ts/MyBlueprint",
        "resourceGroups": {
            "storageRG": {
                "name": "StorageAccount",
                "location": "eastus2"
            }
        },
        "parameters": {
            "storageAccountType": {
                "value": "Standard_GRS"
            },
            "tagName": {
                "value": "CostCenter"
            },
            "tagValue": {
                "value": "ContosoIT"
            },
            "contributors": {
                "value": [
                    "7be2f100-3af5-4c15-bcb7-27ee43784a1f",
                    "38833b56-194d-420b-90ce-cff578296714"
                ]
            },
            "owners": {
                "value": [
                    "44254d2b-a0c7-405f-959c-f829ee31c2e7",
                    "316deb5f-7187-4512-9dd4-21e7798b0ef9"
                ]
            }
        }
    },
    "identity": {
        "type": "systemAssigned"
    },
    "location": "westus"
}
```

- 用户分配的托管标识

  蓝图分配也可使用用户分配的托管标识。在此示例中，请求正文的 **identity** 部分更改如下：将 `{yourRG}` 和 `{userIdentity}` 分别替换为资源组名称和用户分配托管标识的名称。

```
"identity": {
    "type": "userAssigned",
    "tenantId": "{tenantId}",
    "userAssignedIdentities": {

"/subscriptions/{subscriptionId}/resourceGroups/{yourRG}/providers/Microsoft.ManagedIdentity/user
AssignedIdentities/{userIdentity}": {}
    }
},
```

用户分配的托管标识可以位于任何订阅和资源组中，只要分配蓝图的用户有权访问它即可。

> **IMPORTANT**
>
> 蓝图不管理用户分配的托管标识。用户负责分配足够的角色和权限，否则蓝图分配会失败。

取消分配蓝图

可以从订阅中删除蓝图。通常会在不再需要项目资源时将其删除。删除蓝图时，作为该蓝图的一部分分配的项目将保留。若要删除蓝图分配，请使用以下 REST API 操作：

- REST API URI

```
DELETE
https://management.azure.com/subscriptions/{subscriptionId}/providers/Microsoft.Blueprint/blueprintAssignments/assignMyBlueprint?api-version=2018-11-01-preview
```

删除蓝图

若要删除蓝图本身，请使用以下 REST API 操作：

- REST API URI

```
DELETE
https://management.azure.com/providers/Microsoft.Management/managementGroups/{YourMG}/providers/Microsoft.Blueprint/blueprints/MyBlueprint?api-version=2018-11-01-preview
```

后续步骤

- 了解蓝图生命周期。
- 了解如何使用静态和动态参数。
- 了解如何自定义蓝图排序顺序。
- 了解如何利用蓝图资源锁定。
- 了解如何更新现有分配。
- 使用一般故障排除在蓝图的分配期间解决问题。

教程：基于蓝图示例创建环境

2019/8/26 • • Edit Online

示例蓝图示范了 Azure 蓝图的功能。每个示例蓝图附带具体的意图或目的，但其本身无法创建完整的环境。每个示例蓝图旨在用作探索 Azure 蓝图的起点，其中带有包含的项目、设计和参数的各种组合。

以下教程使用“采用 RBAC 的资源组”蓝图示例来展示蓝图服务的各个方面。本文包括以下步骤：

- 基于示例创建新的蓝图定义
- 将示例副本标记为“已发布”
- 将蓝图副本分配到现有的订阅
- 检查要分配的已部署资源
- 取消分配蓝图以删除锁

先决条件

若要完成本教程，需要一个 Azure 订阅。如果没有 Azure 订阅，请在开始之前创建一个免费帐户。

基于示例创建蓝图定义

首先实施蓝图示例。通过导入可以基于示例在环境中创建新的蓝图。

1. 在左侧窗格中，选择“所有服务”。搜索并选择“蓝图”。
2. 在左侧的“开始”页中，选择“创建蓝图”下的“创建”按钮。
3. 在“其他示例”下找到“采用 RBAC 的资源组”蓝图示例，然后选择“使用此示例”。
4. 输入该蓝图示例的“基本信息”：
   - **蓝图名称**：提供蓝图示例副本的名称。本教程使用名称 *two-rgs-with-role-assignments*。
   - **定义位置**：使用省略号并选择要将示例副本保存到的管理组或订阅。
5. 选择页面顶部的“项目”选项卡，或页面底部的“下一步:项目”。
6. 查看构成蓝图示例的项目列表。本示例定义两个资源组，其显示名称为 *ProdRG* 和 *PreProdRG*。在蓝图分配期间，将设置每个资源组的最终名称和位置。为 *ProdRG* 资源组分配“参与者”角色，为 *PreProdRG* 资源组分配“所有者”和“读取者”角色。定义中分配的角色是静态的，但分配有角色的用户、应用或组是在蓝图分配期间设置的。
7. 查看完蓝图示例后，选择“保存草稿”。

此步骤在选定的管理组或订阅中创建示例蓝图定义的副本。对已保存的蓝图定义的管理方式类似于从头开始创建的任何蓝图。可将示例保存到管理组或订阅任意次。但是，必须为每个副本提供唯一的名称。

“保存蓝图定义成功”门户通知出现后，转到下一步骤。

发布示例副本

现已在环境中创建蓝图示例的副本。该副本在创建后处于“草稿”模式，必须先将其发布，然后才能分配和部署它。可根据环境和需求自定义蓝图示例的副本。本教程不会对副本进行任何更改。

1. 在左侧窗格中，选择“所有服务”。搜索并选择“蓝图”。
2. 在左侧选择“蓝图定义”页。使用筛选器找到 *two-rgs-with-role-assignments* 蓝图定义，并将其选中。

3. 选择页面顶部的“发布蓝图”。在右侧的新窗格中，输入 *1.0* 作为蓝图示例副本的**版本**。以后做出修改时，此属性非常有用。提供**更改注释**，例如，“基于‘采用 RBAC 的资源组’蓝图示例发布的第一个版本”。然后选择页面底部的“发布”。

使用此步骤可将蓝图分配到订阅。发布后，仍可进行更改。若要进行其他更改，需要使用新的“版本”值发布，以跟踪同一蓝图定义的不同版本之间的差异。

“发布蓝图定义成功”门户通知出现后，转到下一步骤。

分配示例副本

成功发布蓝图示例的副本后，可将它分配到它所在的管理组中的某个订阅。在此步骤中，需提供参数来使蓝图示例副本的每个部署保持唯一。

1. 在左侧窗格中，选择“所有服务”。搜索并选择“蓝图”。
2. 在左侧选择“蓝图定义”页。使用筛选器找到 *two-rgs-with-role-assignments* 蓝图定义，并将其选中。
3. 选择蓝图定义页面顶部的“分配蓝图”。
4. 提供蓝图分配的参数值：

   - 基础
     - **订阅**：在蓝图示例副本所保存到的管理组中选择一个或多个订阅。如果选择多个订阅，将使用输入的参数为每个订阅创建一个分配。
     - **分配名称**：系统会根据蓝图定义的名称预先填充该名称。
     - **位置**：选择要在其中创建托管标识的区域。Azure 蓝图使用此托管标识在分配的蓝图中部署所有项目。若要了解详细信息，请参阅 Azure 资源的托管标识。本教程选择了“美国东部 2”。
     - **蓝图定义版本**：选择示例蓝图定义副本的“已发布”版本 *1.0*。
   - 锁分配

     选择“只读”蓝图锁定模式。有关更多信息，请参阅蓝图资源锁定。
   - 托管标识

     保留默认的“系统分配”选项。有关详细信息，请参阅托管标识。
   - 项目参数

     在本部分定义的参数将应用到定义了这些参数的项目。这些参数属于动态参数，因为它们是在分配蓝图期间定义的。对于每个项目，请将参数值设置为“值”列中定义的值。对于 `{Your ID}`，请选择你的 Azure 用户帐户。

项目名称	项目类型	参数名称	值	说明
ProdRG 资源组	资源组	名称	ProductionRG	定义第一个资源组的名称。
ProdRG 资源组	资源组	位置	美国西部 2	设置第一个资源组的位置。
参与者	角色分配	用户或组	{你的 ID}	定义要将“参与者”角色授予第一个资源组中的哪个用户或组。

项目名称	项目类型	参数名称	值	说明
PreProdRG 资源组	资源组	名称	PreProductionRG	定义第二个资源组的名称。
PreProdRG 资源组	资源组	位置	美国西部	设置第二个资源组的位置。
所有者	角色分配	用户或组	{你的 ID}	定义要将“所有者”角色授予第二个资源组中的哪个用户或组。
读取者	角色分配	用户或组	{你的 ID}	定义要将“读取者”角色授予第二个资源组中的哪个用户或组。

5. 输入所有参数后，选择页面底部的“分配”。

此步骤部署定义的资源，并配置选定的锁分配。应用蓝图锁最长可能需要花费 30 分钟。

“分配蓝图定义成功”门户通知出现后，转到下一步骤。

检查分配部署的资源

蓝图分配会创建并跟踪蓝图定义中定义的项目。可以在蓝图分配页中通过直接查看资源来检查资源的状态。

1. 在左侧窗格中，选择“所有服务”。搜索并选择“蓝图”。
2. 在左侧选择“分配的蓝图”页。使用筛选器找到 *Assignment-two-rgs-with-role-assignments* 蓝图分配，并将其选中。

   在此页中，可以看到分配成功消息、创建的资源列表及其蓝图锁定状态。如果更新了分配，“分配操作”下拉列表会显示有关每个定义版本的部署的详细信息。可以单击列出的每个已创建资源，打开该资源的属性页。
3. 选择“ProductionRG”资源组。

   可以看到，该资源组的名称是 **ProductionRG**，而不是项目显示名称 *ProdRG*。此名称与蓝图分配期间设置的值相匹配。
4. 在左侧选择“访问控制(IAM)”页，然后选择“角色分配”选项卡。

   在此处可以看到，为你的帐户授予了“此资源”范围的“参与者”角色。*Assignment-two-rgs-with-role-assignments* 蓝图分配具有“所有者”角色，因为资源组是使用该分配创建的。这些权限还用于管理配置有蓝图锁的资源。
5. 在 Azure 门户痕迹导航中，选择“Assignment-two-rgs-with-role-assignments”返回前一页面，然后选择“PreProductionRG”资源组。
6. 在左侧选择“访问控制(IAM)”页，然后选择“角色分配”选项卡。

   在此处可以看到，为你的帐户授予了“此资源”范围的“所有者”和“读取者”角色。与第一个资源组一样，该蓝图分配也具有“所有者”角色。
7. 选择“拒绝分配”选项卡。

   该蓝图分配在部署的资源组中创建了一个拒绝分配，以强制实施“只读”蓝图锁定模式。该拒绝分配会阻止“角色分配”选项卡中具有相应权限的某人执行特定的操作。拒绝分配会影响所有主体。

8. 选择该拒绝分配，然后在左侧选择“拒绝的权限”页。

   该拒绝分配正在阻止使用 * 和 **Action** 配置的所有操作，但允许通过 **NotActions** 排除 ***/read**，以此进行读取访问。

9. 在 Azure 门户痕迹导航中，选择“PreProductionRG - 访问控制(IAM)”。在左侧选择“概述”页，然后选择“删除资源组”按钮。输入名称 *PreProductionRG* 以确认删除，然后选择窗格底部的“删除”。

   此时会显示门户通知“删除资源组 PreProductionRG 失败”。错误中指出，尽管你的帐户有权删除资源组，但蓝图分配拒绝了访问。回顾前文，我们在蓝图分配期间选择了“只读”蓝图锁定模式。蓝图锁会阻止具有权限的帐户（甚至包括“所有者”）删除资源。有关更多信息，请参阅蓝图资源锁定。

这些步骤演示了我们的资源是根据定义创建的，蓝图锁会阻止意外的删除，甚至可以阻止具有权限的帐户执行删除。

取消分配蓝图

最后一步是删除蓝图分配及其部署的资源。删除分配不会删除已部署的项目。

1. 在左侧窗格中，选择“所有服务”。搜索并选择“蓝图”。
2. 在左侧选择“分配的蓝图”页。使用筛选器找到 *Assignment-two-rgs-with-role-assignments* 蓝图分配，并将其选中。
3. 选择页面顶部的“取消分配蓝图”按钮。阅读确认对话框中的警告，然后选择“确定”。

   删除蓝图分配时，蓝图锁也会一并删除。具有权限的帐户现在又可以删除创建的资源。

4. 在 Azure 菜单中选择“资源组”，然后选择“ProductionRG”。
5. 在左侧选择“访问控制(IAM)”页，然后选择“角色分配”选项卡。

每个资源组的安全性仍具有部署的角色分配，但蓝图分配不再具有“所有者”访问权限。

“删除蓝图分配成功”门户通知出现后，转到下一步骤。

清理资源

完成本教程后，请删除以下资源：

- 资源组 *ProductionRG*
- 资源组 *PreProductionRG*
- 蓝图定义 *two-rgs-with-role-assignments*

后续步骤

- 了解蓝图生命周期
- 了解如何使用静态和动态参数
- 了解如何使用蓝图资源锁定
- 了解如何自定义蓝图排序顺序
- 了解如何更新现有分配
- 使用常规疑难解答在蓝图分配期间解决问题

教程：使用 Azure 蓝图资源锁保护新资源

2019/8/26 • • Edit Online

使用 Azure 蓝图资源锁可以保护新部署的资源，防止其遭到篡改（即使使用拥有“所有者”角色的帐户，也无法篡改）。可在蓝图定义中将这种保护添加到资源管理器模板项目创建的资源。

在本教程中，你将完成以下步骤：

- 创建蓝图定义
- 将蓝图定义标记为“已发布”
- 将蓝图定义分配到现有的订阅
- 检查新资源组
- 取消分配蓝图以删除锁

先决条件

需要一个 Azure 订阅才能完成此教程。如果没有 Azure 订阅，请在开始之前创建一个免费帐户。

创建蓝图定义

首先创建蓝图定义。

1. 在左侧窗格中，选择“所有服务”。搜索并选择“蓝图”。
2. 在左侧的“开始”页中，选择“创建蓝图”下的“创建”。
3. 在页面顶部找到“空白蓝图”蓝图示例。选择“以空白蓝图开始”。
4. 在“基本信息”选项卡上输入此信息：
   - **蓝图名称**：提供蓝图示例副本的名称。本教程使用名称 **locked-storageaccount**。
   - **蓝图描述**：添加蓝图定义的说明。使用“用于测试已部署资源中的蓝图资源锁定”。
   - **定义位置**：选择省略号按钮 (...)，然后选择要将蓝图定义保存到的管理组或订阅。
5. 选择页面顶部的“项目”选项卡，或选择页面底部的“下一步: 项目”。
6. 添加订阅级别的资源组：
   a. 在“订阅”下选择“添加项目”行。
   b. 在“项目类型”下选择“资源组”。
   c. 将“项目显示名称”设置为 **RGtoLock**。
   d. 将“资源组名称”和“位置”框保留为空，但请确保在每个属性上选中该复选框，以使其成为动态参数。
   e. 选择“添加”将此项目添加到蓝图中。
7. 在资源组下添加模板：
   a. 在“RGtoLock”条目下选择“添加项目”行。
   b. 在“项目类型”下选择“Azure 资源管理器模板”，将“项目显示名称”设置为“StorageAccount”，并将“说明”保留为空。
   c. 在“模板”选项卡上，将以下资源管理器模板粘贴到编辑器框中。粘贴模板后，选择“添加”将此项目添加到蓝图。

```
{
    "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
    "contentVersion": "1.0.0.0",
    "parameters": {
        "storageAccountType": {
            "type": "string",
            "defaultValue": "Standard_LRS",
            "allowedValues": [
                "Standard_LRS",
                "Standard_GRS",
                "Standard_ZRS",
                "Premium_LRS"
            ],
            "metadata": {
                "description": "Storage Account type"
            }
        }
    },
    "variables": {
        "storageAccountName": "[concat('store', uniquestring(resourceGroup().id))]"
    },
    "resources": [{
        "type": "Microsoft.Storage/storageAccounts",
        "name": "[variables('storageAccountName')]",
        "location": "[resourceGroup().location]",
        "apiVersion": "2018-07-01",
        "sku": {
            "name": "[parameters('storageAccountType')]"
        },
        "kind": "StorageV2",
        "properties": {}
    }],
    "outputs": {
        "storageAccountName": {
            "type": "string",
            "value": "[variables('storageAccountName')]"
        }
    }
}
```

8. 选择页面底部的“保存草稿”。

此步骤在选定的管理组或订阅中创建蓝图定义。

“保存蓝图定义成功”门户通知出现后，转到下一步骤。

发布蓝图定义

现已在环境中创建蓝图定义。该副本在创建后处于“草稿”模式，必须先将其发布，然后才能分配和部署它。

1. 在左侧窗格中，选择“所有服务”。搜索并选择“蓝图”。

2. 在左侧选择“蓝图定义”页。使用筛选器找到 **locked-storageaccount** 蓝图定义，并将其选中。

3. 选择页面顶部的“发布蓝图”。在右侧的新窗格中，输入 **1.0** 作为版本。以后做出更改时，此属性非常有用。输入更改注释，例如，“为锁定蓝图部署的资源而发布的第一个版本”。然后选择页面底部的“发布”。

使用此步骤可将蓝图分配到订阅。发布蓝图定义后，仍可进行更改。如果进行了更改，则需要使用新的版本值发布定义，以跟踪同一蓝图定义的不同版本之间的差异。

“发布蓝图定义成功”门户通知出现后，转到下一步骤。

分配蓝图定义

发布蓝图定义后，可将它分配到它所在的管理组中的某个订阅。在此步骤中，请提供参数来使蓝图定义的每个部署保持唯一。

1. 在左侧窗格中，选择“所有服务”。搜索并选择“蓝图”。

2. 在左侧选择“蓝图定义”页。使用筛选器找到 **locked-storageaccount** 蓝图定义，并将其选中。

3. 选择蓝图定义页面顶部的“分配蓝图”。

4. 提供蓝图分配的参数值：

   - **基础知识**
     - **订阅**：在蓝图定义所保存到的管理组中选择一个或多个订阅。如果选择多个订阅，将使用输入的参数为每个订阅创建一个分配。
     - **分配名称**：系统会根据蓝图定义的名称预先填充该名称。我们希望此分配表示新资源组的锁定，因此请将分配名称更改为 **assignment-locked-storageaccount-TestingBPLocks**。
     - **位置**：选择要在其中创建托管标识的区域。Azure 蓝图使用此托管标识在分配的蓝图中部署所有项目。若要了解详细信息，请参阅 Azure 资源的托管标识。本教程选择了“美国东部 2”。
     - **蓝图定义版本**：选择蓝图定义的已发布版本 **1.0**。
   - **锁分配**

     选择“只读”蓝图锁定模式。有关更多信息，请参阅蓝图资源锁定。

   - **托管的标识**

     使用默认选项：“系统分配”。有关详细信息，请参阅托管标识。

   - **项目参数**

     在本部分定义的参数将应用到定义了这些参数的项目。这些参数属于动态参数，因为它们是在分配蓝图期间定义的。对于每个项目，请将参数值设置为“值”列中显示的值。

项目名称	项目类型	参数名称	值	说明
RGtoLock 资源组	资源组	名称	TestingBPLocks	定义要将蓝图锁应用到的新资源组的名称。
RGtoLock 资源组	资源组	位置	美国西部 2	定义要将蓝图锁应用到的新资源组的位置。
StorageAccount	资源管理器模板	storageAccountType (StorageAccount)	Standard_GRS	存储 SKU。默认值为 *Standard_LRS*。

5. 输入所有参数后，选择页面底部的“分配”。

此步骤部署定义的资源，并配置选定的锁分配。应用蓝图锁最长可能需要花费 30 分钟。

“分配蓝图定义成功”门户通知出现后，转到下一步骤。

检查分配部署的资源

该分配创建了资源组 *TestingBPLocks*，资源管理器模板项目部署了存储帐户。新资源组和选定的锁定状态显示在分配详细信息页上。

1. 在左侧窗格中，选择“所有服务”。搜索并选择“蓝图”。

2. 在左侧选择"分配的蓝图"页。使用筛选器找到 **assignment-locked-storageaccount-TestingBPLocks** 蓝图分配，并将其选中。

   在此页中，可以看到分配成功消息和已部署资源的消息，以及新的蓝图锁定状态。如果更新了分配，"分配操作"下拉列表会显示有关每个定义版本的部署的详细信息。可以选择资源组打开属性页。

3. 选择"TestingBPLocks"资源组。

4. 选择左侧的"访问控制(IAM)" 页。然后选择"角色分配"选项卡 。

   在此处可以看到，*assignment-locked-storageaccount-TestingBPLocks* 蓝图分配具有"所有者"角色。之所以具有此角色，是因为资源组是使用此角色部署和锁定的。

5. 选择"拒绝分配"选项卡。

   该蓝图分配在部署的资源组中创建了一个拒绝分配，以强制实施"只读"蓝图锁定模式。该拒绝分配会阻止"角色分配"选项卡中具有相应权限的某人执行特定的操作。拒绝分配会影响所有主体。

   若要了解如何从拒绝分配中排除主体，请参阅蓝图资源锁定。

6. 选择该拒绝分配，然后在左侧选择"拒绝的权限"页。

   该拒绝分配正在阻止使用 * 和 **Action** 配置的所有操作，但允许通过 **NotActions** 排除 ***/read**，以此进行读取访问。

7. 在 Azure 门户痕迹导航中，选择"TestingBPLocks - 访问控制(IAM)"。在左侧选择"概述"页，然后选择"删除资源组"按钮。输入名称 **TestingBPLocks** 以确认删除，然后选择窗格底部的"删除"。

   此时会显示门户通知"删除资源组 TestingBPLocks 失败"。错误中指出，尽管你的帐户有权删除资源组，但蓝图分配拒绝了访问。回顾前文，我们在蓝图分配期间选择了"只读"蓝图锁定模式。蓝图锁会阻止具有权限的帐户（甚至包括"所有者"）删除资源。有关更多信息，请参阅蓝图资源锁定。

这些步骤演示了部署的资源现在受到蓝图锁的保护，蓝图锁可以阻止意外的删除，甚至可以阻止具有权限的帐户删除资源。

取消分配蓝图

最后一步是删除蓝图定义的分配。删除分配不会删除关联的项目。

1. 在左侧窗格中，选择"所有服务" 。搜索并选择"蓝图" 。

2. 在左侧选择"分配的蓝图"页。使用筛选器找到 **assignment-locked-storageaccount-TestingBPLocks** 蓝图分配，并将其选中。

3. 选择页面顶部的"取消分配蓝图"。阅读确认对话框中的警告，然后选择"确定"。

   删除蓝图分配时，蓝图锁也会一并删除。具有相应权限的帐户现在又可以删除资源。

4. 在 Azure 菜单中选择"资源组"，然后选择"TestingBPLocks"。

5. 在左侧选择"访问控制(IAM)"页，然后选择"角色分配"选项卡。

资源组的安全性显示该蓝图分配不再拥有"所有者"访问权限。

"删除蓝图分配成功"门户通知出现后，转到下一步骤。

清理资源

完成本教程后，请删除以下资源：

- 资源组 *TestingBPLocks*

- 蓝图定义 *locked-storageaccount*

后续步骤

- 了解蓝图生命周期。
- 了解如何使用静态和动态参数。
- 了解如何使用蓝图资源锁定。
- 了解如何自定义蓝图排序顺序。
- 了解如何更新现有分配。
- 在分配蓝图期间排查问题。

Azure 蓝图示例

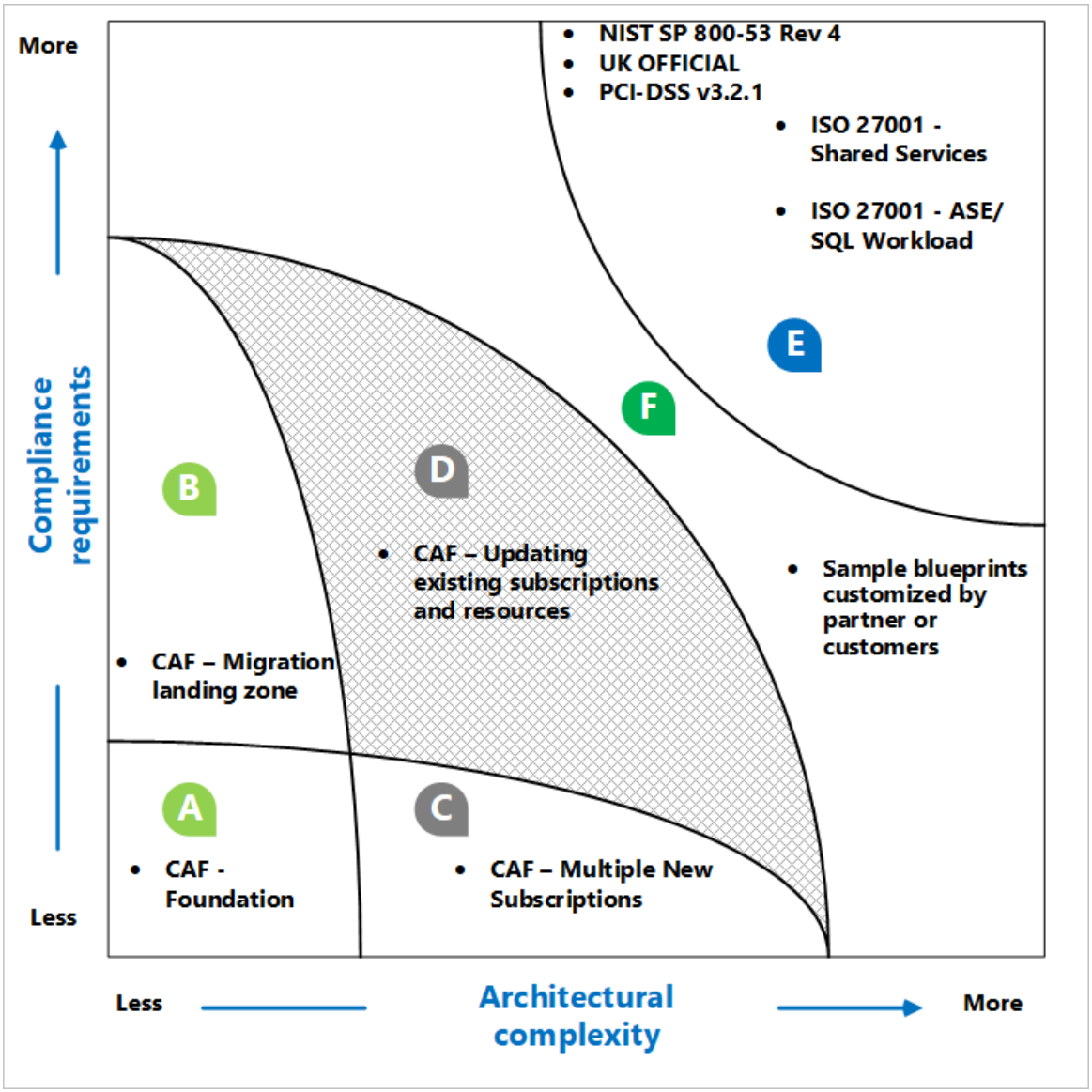
2019/9/4 • • Edit Online

下表包含 Azure 蓝图示例的链接。每个示例都可投入实际生产运行，并且现在已可供部署，以便帮助满足你的各种符合性需求。

基于标准的蓝图示例

加拿大联邦 PBMM	提供防护措施，以便符合加拿大联邦受保护的 B、中等完整性、中等可用性 (PBMM)。
CIS Microsoft Azure 基础基准	提供一组策略以帮助符合 CIS Microsoft Azure 基础基准建议。
IRS 1075	提供用于符合 IRS 1075 的规范措施。
ISO 27001	提供用于符合 ISO 27001 的规范措施。
ISO 27001 共享服务	提供了一组符合标准的基础结构模式和策略防护机制，以便帮助通过 ISO 27001 认证。
ISO 27001 应用服务环境/SQL 数据库工作负荷	为 ISO 27001 共享服务蓝图示例提供了其他基础结构。
NIST SP 800-53 R4	提供用于符合 NIST SP 800-53 R4 的规范措施。
PCI-DSS v3.2.1	提供一组策略以帮助用户符合 PCI-DSS v3.2.1。
英国官方和英国 NHS 监管	提供了一组符合标准的基础结构模式和策略防护措施，以便帮助用户通过英国官方和英国 NHS 认证。
CAF 基础	提供了一组控制措施，以便帮助你管理云资产，使其与适用于 Azure 的 Microsoft 云采用框架 (CAF) 相符合。
CAF 迁移登陆区域	提供了一组控制措施，以便帮助你安排迁移你的第一个工作负荷并管理你的云资产，使其与适用于 Azure 的 Microsoft 云采用框架 (CAF) 相符合。

示例策略



CAF 基础和 CAF 迁移登陆区域蓝图假定客户正在准备一个现有的干净单一订阅，以便将本地资产/工作负荷迁移到 Azure。（上图中的区域 A 和 B）。

可以基于示例蓝图进行迭代，并查找客户正在应用的自定义模式。此外，还可以主动处理特定于行业（如金融服务和电子商务）的蓝图（区域 B 的顶端）。同样，我们设想针对复杂的架构考虑因素（如多个订阅、高可用性、跨区域资源以及对现有订阅和资源实施控制的客户）构建蓝图（区域 C 和 D）。

有一些示例蓝图可满足符合性要求较高、体系结构复杂性较高的客户场景需求（上图中的区域 E）。上面的区域 F 表示将由客户和合作伙伴处理的一种示例蓝图，客户和合作伙伴利用这些示例蓝图并根据自己的独特需求对其进行自定义。

后续步骤

- 了解蓝图生命周期。
- 了解如何使用静态和动态参数。
- 了解如何自定义蓝图排序顺序。
- 了解如何利用蓝图资源锁定。
- 了解如何更新现有分配。
- 使用一般故障排除在蓝图的分配期间解决问题。

加拿大联邦 PBMM 蓝图示例的控制映射

2019/9/2 • • Edit Online

以下文章详细介绍了 Azure 蓝图加拿大联邦保护的 B、中等完整性、中等可用性 (PBMM) 蓝图示例如何映射到加拿大联邦 PBMM 控制。有关控制的详细信息，请参阅加拿大联邦 PBMM。

以下映射到**加拿大联邦 PBMM** 控制。使用右侧的导航栏可直接跳转到特定的控制映射。许多的映射控制措施都是使用 Azure Policy 计划实施的。若要查看完整计划，请在 Azure 门户中打开“策略”，并选择“定义”页。然后，找到并选择“[预览]: 审核加拿大联邦 PBMM 控制”内置策略计划。

位置约束

此蓝图通过分配以下 Azure Policy 定义，帮助你将所有资源和资源组的部署位置限制为“加拿大中部”和“加拿大东部”：

- 允许的位置（已硬编码为“加拿大中部”和“加拿大东部”）
- 允许的资源组位置（已硬编码为“加拿大中部”和“加拿大东部”）

AC-2 帐户管理

此蓝图可帮助你查看可能不符合你组织的帐户管理要求的帐户。此蓝图分配 Azure Policy 定义，这些定义用于审核对订阅和弃用帐户具有读、写和所有者权限的外部帐户。通过查看受到这些策略审核的帐户，可以采取适当的措施，确保满足帐户管理要求。

- 应从订阅中删除弃用的帐户
- 应从订阅中删除拥有所有者权限的已弃用帐户
- 应从订阅中删除拥有所有者权限的外部帐户
- 应从订阅中删除拥有读取权限的外部帐户
- 应从订阅中删除具有写入权限的外部帐户

AC-2 (7) 帐户管理 | 基于角色的方案

Azure 实施了基于角色的访问控制 (RBAC) 来帮助你管理谁有权访问 Azure 中的资源。使用 Azure 门户可以评审有权访问 Azure 资源的用户及其权限。此蓝图还分配 Azure Policy 定义，用于审核 Azure Active Directory 身份验证在 SQL 服务器和 Service Fabric 中的使用。使用 Azure Active Directory 身份验证可以简化权限管理，以及集中化数据库用户和其他 Microsoft 服务的标识管理。此外，此蓝图还分配一个 Azure Policy 定义用于审核自定义 RBAC 规则的使用。了解实施自定义 RBAC 规则的位置有助于验证需求以及实施是否适当，因为自定义 RBAC 规则容易出错。

- 应该为 SQL 服务器预配 Azure Active Directory 管理员
- Service Fabric 群集只应使用 Azure Active Directory 进行客户端身份验证

AC-4 信息流强制

跨域资源共享 (CORS) 支持从外部域请求应用服务资源。Microsoft 建议只允许必需的域与 API、函数和 web 应用程序进行交互。此蓝图分配了一个 Azure Policy 定义，有助于你监视 Azure 安全中心中的 CORS 资源访问限制。了解 CORS 实现有助于你验证信息流控制措施是否实现。

- CORS 不应允许所有资源都能访问你的 Web 应用程序

AC-5 职责分离

仅分配一个 Azure 订阅所有者并不能实现管理冗余。相反，分配过多的 Azure 订阅所有者会增大违规的可能性，因为会有更多的所有者帐户可能会泄密。此蓝图可帮助你通过分配用于审核 Azure 订阅所有者数目的 Azure Policy 定义，来保持适当的 Azure 订阅所有者数目。此蓝图还分配 Azure Policy 定义，有助于你控制 Windows 虚拟机上管理员组的成员身份。管理订阅所有者和虚拟机管理员权限有助于实现适当的职责分离。

- 只多只为订阅指定 3 个所有者
- 应该为你的订阅分配了多个所有者
- 审核在其管理员组中包含任何指定成员的 Windows VM
- 审核在其管理员组中不包含所有指定成员的 Windows VM
- 部署要求以审核在其管理员组中包含任何指定成员的 Windows VM
- 部署要求以审核在其管理员组中不包含所有指定成员的 Windows VM

AC-6 最小特权

Azure 实施了基于角色的访问控制 (RBAC) 来帮助你管理谁有权访问 Azure 中的资源。使用 Azure 门户可以评审有权访问 Azure 资源的用户及其权限。此蓝图分配 Azure Policy 定义，用于审核应优先评审的帐户。评审这些帐户指标可帮助确保实现最低特权控制措施。

- 只多只为订阅指定 3 个所有者
- 应该为你的订阅分配了多个所有者
- 审核在其管理员组中包含任何指定成员的 Windows VM
- 审核在其管理员组中不包含所有指定成员的 Windows VM
- 部署要求以审核在其管理员组中包含任何指定成员的 Windows VM
- 部署要求以审核在其管理员组中不包含所有指定成员的 Windows VM

AC-7 安全属性

Azure SQL 数据库高级数据安全性的数据发现和分类功能提供用于发现、分类、标记和保护数据库中敏感数据的功能。它可用于直观查看数据库分类状态，以及跟踪对数据库内和其边界外的敏感数据的访问。高级数据安全性有助于确保信息与组织的相应安全属性相关联。此蓝图分配 Azure Policy 定义用于在 SQL 服务器上监视和强制使用高级数据安全性。

- 应在 SQL 托管实例上启用高级数据安全性
- 应在 SQL 服务器上启用高级数据安全性
- 在 SQL 服务器上部署高级数据安全

AC-17 (1) 远程访问 | 自动监视/控制

此蓝图可帮助你监视和控制远程访问，因为它会分配 Azure Policy 定义用于监视 Azure 应用服务应用程序的远程调试处于关闭状态，此蓝图还会分配策略定义用于审核允许来自无密码帐户的远程连接的 Linux 虚拟机。此蓝图还将分配一个 Azure Policy 定义，用于帮助监视对存储帐户的无限制访问。监视这些指标可以帮助确保远程访问方法符合安全策略。

- [预览]: 审核允许通过没有密码的帐户进行远程连接的 Linux VM
- [预览]: 部署要求以审核允许通过没有密码的帐户进行远程连接的 Linux VM
- 审核对存储帐户的不受限的网络访问
- 应为 API 应用禁用远程调试
- 应对函数应用禁用远程调试
- 应禁用 Web 应用程序的远程调试

AU-3 (2) 审核记录的内容

Azure Monitor 收集的日志数据存储在支持集中配置和管理的 Log Analytics 工作区中。此蓝图通过分配 Azure Policy 定义来确保事件被记录下来，这些定义审核并强制在 Azure 虚拟机上部署 Log Analytics 代理。

- [预览]: 审核 Log Analytics 代理部署 - VM 映像 (OS) 未列出
- [预览]: 审核 VMSS 中的 Log Analytics 代理部署 - VM 映像 (OS) 未列出
- [预览]: 审核 VM 的 Log Analytics 工作区 — 报告不匹配
- [预览]: 为 Linux VM 部署 Log Analytics 代理
- [预览]: 为 Windows VM 部署 Log Analytics 代理

AU-5 对审核处理失败的响应

此蓝图分配 Azure Policy 定义用于监视审核和事件日志记录配置。监视这些配置可以提供审核系统故障或配置错误的指标，帮助你采取纠正措施。

- 审核诊断设置
- 审核 SQL 服务器级别审核设置
- 应在托管实例上启用高级数据安全性
- 应在 SQL 服务器上启用高级数据安全性

AU-6 (4) 审核评审、分析和报告 | 中心评审和分析

Azure Monitor 收集的日志数据存储在支持集中报告和分析的 Log Analytics 工作区中。此蓝图通过分配 Azure Policy 定义来确保事件被记录下来，这些定义审核并强制在 Azure 虚拟机上部署 Log Analytics 代理。

- [预览]: 审核 Log Analytics 代理部署 - VM 映像 (OS) 未列出
- [预览]: 审核 VMSS 中的 Log Analytics 代理部署 - VM 映像 (OS) 未列出
- [预览]: 审核 VM 的 Log Analytics 工作区 — 报告不匹配
- [预览]: 为 Linux VM 部署 Log Analytics 代理
- [预览]: 为 Windows VM 部署 Log Analytics 代理

AU-12 审核生成

此蓝图通过分配 Azure Policy 定义来帮助确保记录系统事件，这些定义用于审核在 Azure 资源上的日志设置。这些策略定义审核并强制部署 Azure 虚拟机上的 Log Analytics 代理并强制配置针对其他 Azure 资源类型的审核设置。这些策略定义还审核诊断日志配置，以提供对 Azure 资源内执行的操作的见解。此外，审核和高级数据安全在 SQL 服务器上配置。

- [预览]: 审核 Log Analytics 代理部署 - VM 映像 (OS) 未列出
- [预览]: 审核 VMSS 中的 Log Analytics 代理部署 - VM 映像 (OS) 未列出
- [预览]: 审核 VM 的 Log Analytics 工作区 — 报告不匹配
- [预览]: 为 Linux VM 部署 Log Analytics 代理
- [预览]: 为 Windows VM 部署 Log Analytics 代理
- 审核诊断设置
- 审核 SQL 服务器级别审核设置
- 应在托管实例上启用高级数据安全性
- 应在 SQL 服务器上启用高级数据安全性
- 在 SQL 服务器上部署高级数据安全
- 对 SQL 服务器部署审核
- 为网络安全组部署诊断设置

CM-7 (5) 最少的功能 | 授权软件/允许列表

Azure 安全中心中的自适应应用程序控制是一种智能、自动化端到端的应用程序允许列表解决方案，可以阻止或防止特定软件在虚拟机上运行。应用程序控制帮助你为虚拟机创建批准的应用程序列表。此蓝图分配了一个 Azure Policy 定义，用于帮助监视建议使用应用程序允许列表但尚未对其进行配置的虚拟机。

- 应在虚拟机上启用自适应应用程序控制

CM-11 用户安装的软件

Azure 安全中心中的自适应应用程序控制是一种智能、自动化端到端的应用程序允许列表解决方案，可以阻止或防止特定软件在虚拟机上运行。应用程序控制可以帮助你强制执行和监视软件限制策略的符合性。此蓝图分配了一个 Azure Policy 定义，用于帮助监视建议使用应用程序允许列表但尚未对其进行配置的虚拟机。

- 应在虚拟机上启用自适应应用程序控制

CP-7 备用处理站点

Azure Site Recovery 将在虚拟机上运行的工作负荷从主位置复制到辅助位置。如果在主站点发生故障，工作负荷将故障转移到辅助位置。此蓝图分配了一个 Azure Policy 定义，用于审核没有配置灾难恢复的虚拟机。监视此指标可以帮助确保必要的应变控制措施已到位。

- 审核没有配置灾难恢复的虚拟机

IA-2 (1) 标识和身份验证(组织用户)| 对特权帐户的网络访问

此蓝图分配 Azure Policy 定义用于审核拥有所有者和/或写入权限但未启用多重身份验证的帐户，从而帮助你限制和控制特权访问。即使某个身份验证信息片段已泄密，多重身份验证也有助于保护帐户的安全。通过监视未启用多重身份验证的帐户，可以识别出更有可能会泄密的帐户。

- 应在对订阅拥有所有者权限的帐户上启用 MFA
- 应在对订阅拥有写入权限的帐户上启用 MFA

IA-5 验证器管理

此蓝图分配 Azure Policy 定义，用于审核允许来自无密码帐户的远程连接并/或在密码文件中设置了不正确权限的 Linux 虚拟机。此蓝图还会分配一个策略定义用于审核 Windows 虚拟机密码加密类型的配置。监视这些指标有助于确保系统验证器符合组织的标识和身份验证策略。

- [预览]: 审核未将密码文件权限设为 0644 的 Linux VM
- [预览]: 审核具有不使用密码的帐户的 Linux VM
- [预览]: 部署要求以审核未将密码文件权限设置为 0644 的 Linux VM
- [预览]: 部署要求以审核具有不使用密码的帐户的 Linux VM

IA-5 (1) 验证器管理 |基于密码的身份验证

此蓝图通过分配 Azure Policy 定义用于审核不强制实施最低强度和其他密码要求的 Windows 虚拟机，来帮助你强制实施强密码。感知虚拟机是否违反密码强度策略有助于采取纠正措施，确保所有虚拟机用户帐户的密码与组织的密码策略相符。

- [预览]: 审核允许重用之前的 24 个密码的 Windows VM
- [预览]: 审核未将最长密码期限设为 70 天的 Windows VM
- [预览]: 审核未将最短密码期限设为 1 天的 Windows VM
- [预览]: 审核未启用密码复杂性设置的 Windows VM
- [预览]: 审核未将最短密码长度限制为 14 个字符的 Windows VM

- [预览]: 部署要求以审核允许重用之前的 24 个密码的 Windows VM
- [预览]: 部署要求以审核未将最长密码期限设为 70 天的 Windows VM
- [预览]: 部署要求以审核未将最短密码期限设为 1 天的 Windows VM
- [预览]: 部署要求以审核未启用密码复杂性设置的 Windows VM
- [预览]: 部署要求以审核未将最短密码长度限制为 14 个字符的 Windows VM

IA-8 (100) 标识和身份验证(非组织用户) | 标识和凭据保证级别

此蓝图分配 Azure Policy 定义用于审核拥有所有者和/或写入权限但未启用多重身份验证的帐户，从而帮助你限制和控制特权访问。即使某个身份验证信息片段已泄密，多重身份验证也有助于保护帐户的安全。通过监视未启用多重身份验证的帐户，可以识别出更有可能会泄密的帐户。

- 应在对订阅拥有所有者权限的帐户上启用 MFA
- 应在对订阅拥有写入权限的帐户上启用 MFA

RA-5 漏洞扫描

此蓝图分配 Azure Policy 定义用于在 Azure 安全中心内监视操作系统漏洞、SQL 漏洞和虚拟机漏洞，来帮助你管理信息系统漏洞。Azure 安全中心提供报告功能，使你能够实时洞察已部署的 Azure 资源的安全状态。此蓝图还会分配策略定义用于审核和强制执行 SQL 服务器上的高级数据安全。高级数据安全包括漏洞评估和高级威胁防护功能，可帮助你了解已部署资源中的漏洞。

- 应在托管实例上启用高级数据安全性
- 应在 SQL 服务器上启用高级数据安全性
- 在 SQL 服务器上部署高级数据安全
- 应该修复虚拟机规模集上安全配置中的漏洞
- 应该修复虚拟机上安全配置中的漏洞
- 应该修复 SQL 数据库中的漏洞
- 应该通过漏洞评估解决方案修复漏洞

SC-5 拒绝服务保护

Azure 的分布式拒绝服务 (DDoS) 标准层通过基本服务层提供额外功能和缓解功能。这些额外功能包括 Azure Monitor 集成和查看攻击后的缓解报告的功能。此蓝图分配了一个 Azure Policy 定义，用于审核是否启用 DDoS 标准层。了解服务层之间的功能差异有助于为 Azure 环境选择最佳解决方案来解决拒绝服务保护问题。

- 应启用 DDoS 防护标准版

SC-7 边界保护

此蓝图通过分配一个 Azure Policy 定义用于根据 Azure 安全中心的网络安全组强化建议进行监视，以此帮助你管理和控制系统边界。Azure 安全中心分析面向 Internet 的虚拟机的流量模式，并提供网络安全组规则建议，以减少潜在的攻击面。此外，此蓝图还会分配策略定义用于监视不受保护的终结点、应用程序和存储帐户。不受防火墙保护的终结点和应用程序，以及具有无限制访问权限的存储帐户，可能会允许意外访问信息系统中包含的信息。

- 应该强化面向 Internet 的虚拟机的网络安全组规则
- 应该限制通过面向 Internet 的终结点进行访问
- 审核对存储帐户的不受限的网络访问
- 应该强化 IaaS 上 Web 应用程序的 NSG 规则

SC-7 (3) 边界保护 | 接入点

实时 (JIT) 虚拟机访问会锁定发往 Azure 虚拟机的入站流量，降低遭受攻击的可能性，同时在需要时还可轻松连接

到 VM。实时虚拟机访问有助于限制对 Azure 中资源的外部连接数。此蓝图分配了一个 Azure Policy 定义，有助于你监视能够支持实时访问但尚未配置的虚拟机。

- 应在虚拟机上应用实时网络访问控制

SC-7 (4) 边界保护 | 外部电信服务

实时 (JIT) 虚拟机访问会锁定发往 Azure 虚拟机的入站流量，降低遭受攻击的可能性，同时在需要时还可轻松连接到 VM。实时虚拟机访问有助于通过促进访问请求和审批流程来管理流量策略的例外情况。此蓝图分配了一个 Azure Policy 定义，有助于你监视能够支持实时访问但尚未配置的虚拟机。

- 应在虚拟机上应用实时网络访问控制

SC-8 (1) 传输保密性和完整性 | 加密或备用物理保护

此蓝图分配 Azure Policy 定义来帮助你监视针对通信协议实施的加密机制，以此帮助你保护传输信息的机密性和完整性。确保通信得到适当的加密可帮助你满足组织的要求，或者防范信息遭到未经授权的透漏和修改。

- 只能通过 HTTPS 访问 API 应用
- 审核未使用安全通信协议的 Windows Web 服务器
- 部署要求以审核未使用安全通信协议的 Windows Web 服务器
- 应该只能通过 HTTPS 访问函数应用
- 应该启用只能通过安全方式连接到 Redis 缓存
- 只能通过 HTTPS 访问 Web 应用程序
- 应该启用安全传输到存储帐户

SC-28 (1) 保护静态信息

此蓝图分配 Azure Policy 定义用于强制实施特定的加密控制措施并审核弱加密设置的使用，从而帮助你强制实施有关通过使用加密控制措施保护静态信息的策略。了解 Azure 资源中的哪些位置采用欠佳的加密配置有助于采取纠正措施，以确保根据信息安全策略配置资源。具体地说，该蓝图分配的策略定义要求对数据湖存储帐户进行加密；要求 SQL 数据库上的透明数据加密；审核 SQL 数据库、虚拟机磁盘和自动化帐户变量上缺少的加密。

- 应在托管实例上启用高级数据安全性
- 应在 SQL 服务器上启用高级数据安全性
- 在 SQL 服务器上部署高级数据安全
- 部署 SQL DB 透明数据加密
- 应在虚拟机上启用磁盘加密
- 要求对 Data Lake Store 帐户加密
- 应在 SQL 数据库上启用透明数据加密

SI-2 缺陷修正

此蓝图分配 Azure Policy 定义用于在 Azure 安全中心内监视缺少的系统更新、操作系统漏洞、SQL 漏洞和虚拟机漏洞，从而帮助你管理信息系统缺陷。Azure 安全中心提供报告功能，使你能够实时洞察已部署的 Azure 资源的安全状态。此蓝图还会分配一个策略定义用于确保虚拟机规模集的操作系统的修补。

- 要求自动在虚拟机规模集上执行 OS 映像修补
- 应在虚拟机规模集上安装系统更新
- 应在虚拟机上安装系统更新
- 应该修复虚拟机规模集上安全配置中的漏洞
- 应该修复虚拟机上安全配置中的漏洞
- 应该修复 SQL 数据库中的漏洞

- 应该通过漏洞评估解决方案修复漏洞

SI-3 恶意代码防护

此蓝图分配 Azure Policy 定义用于监视 Azure 安全中心中虚拟机上缺失的终结点防护并在 Windows 虚拟机上强制执行 Microsoft 反恶意软件解决方案，从而帮助管理终结点防护，包括恶意代码防护。

- 为 Windows Server 部署默认 Microsoft IaaSAntimalware 扩展
- 应在虚拟机规模集上安装 Endpoint Protection 解决方案
- 监视 Azure 安全中心 Endpoint Protection 的缺失情况

SI-3 (1) 恶意代码防护 | 集中管理

此蓝图分配 Azure Policy 定义用于监视 Azure 安全中心中虚拟机上缺失的终结点防护，从而帮助管理终结点防护，包括恶意代码防护。Azure 安全中心提供集中管理和报告功能，用于实时洞察已部署的 Azure 资源的安全状态。

- 应在虚拟机规模集上安装 Endpoint Protection 解决方案
- 监视 Azure 安全中心 Endpoint Protection 的缺失情况

SI-4 信息系统监视

此蓝图有助于通过审核和跨 Azure 资源强制执行日志记录和数据安全来监视系统。具体而言，分配的策略审核并强制执行 Log Analytics 代理的部署和 SQL 数据库、存储帐户和网络资源的强化安全设置。这些功能有助于检测异常行为和攻击指标，以便你采取相应措施。

- [预览]: 审核 Log Analytics 代理部署 - VM 映像 (OS) 未列出
- [预览]: 审核 VMSS 中的 Log Analytics 代理部署 - VM 映像 (OS) 未列出
- [预览]: 审核 VM 的 Log Analytics 工作区 — 报告不匹配
- [预览]: 为 Linux VM 部署 Log Analytics 代理
- [预览]: 为 Windows VM 部署 Log Analytics 代理
- 应在托管实例上启用高级数据安全性
- 应在 SQL 服务器上启用高级数据安全性
- 在 SQL 服务器上部署高级数据安全
- 在存储帐户上部署高级威胁防护
- 对 SQL 服务器部署审核
- 创建虚拟网络时部署网络观察程序
- 在 SQL 服务器上部署威胁检测

> **NOTE**
> 特定 Azure Policy 定义的可用性在 Azure 政府和其他国家云中可能会有所不同。

后续步骤

有关蓝图和如何使用这些蓝图的更多文章：

- 了解蓝图生命周期。
- 了解如何使用静态和动态参数。
- 了解如何自定义蓝图排序顺序。
- 了解如何利用蓝图资源锁定。
- 了解如何更新现有分配。

CIS Microsoft Azure 基础基准蓝图示例的概述

2019/9/4 • • Edit Online

CIS Microsoft Azure 基础基准蓝图示例使用 Azure Policy 提供监管防护措施，帮助你评估特定 CIS Microsoft Azure 基础基准建议。对于 Azure 部署的任何必须实施 CIS Microsoft Azure 基础基准建议的体系结构，此蓝图可帮助客户为其部署一组核心策略。

建议映射

“建议映射”部分提供了有关此蓝图中包含的策略的详细信息，以及这些策略如何处理 CIS Microsoft Azure 基础基准中的各种建议。分配给一个体系结构时，资源由 Azure Policy 评估是否不符合已分配的策略。有关详细信息，请参阅 Azure Policy。

后续步骤

你已查看了 CIS Microsoft Azure 基础基准蓝图示例的概述。接下来，请参阅以下文章，了解建议映射：

CIS Microsoft Azure 基础基准蓝图 - 建议映射

有关蓝图和如何使用这些蓝图的更多文章：

- 了解蓝图生命周期。
- 了解如何使用静态和动态参数。
- 了解如何自定义蓝图排序顺序。
- 了解如何利用蓝图资源锁定。
- 了解如何更新现有分配。

CIS Microsoft Azure Foundations Benchmark 蓝图示例的建议映射

2019/9/5 • • Edit Online

以下文章详细说明了 Azure 蓝图 CIS Microsoft Azure Foundations Benchmark 蓝图示例如何映射到 CIS Microsoft Azure Foundations Benchmark 建议。有关建议的详细信息，请参阅 CIS Microsoft Azure Foundations Benchmark。

以下映射适用于 **CIS Microsoft Azure Foundations Benchmark v1.1.0** 建议。使用右侧的导航栏可直接跳转到特定的建议映射。许多的映射建议都是使用 Azure Policy 计划实施的。若要查看完整计划，请在 Azure 门户中打开“策略”，并选择“定义”页。然后，找到并选择“[预览] 审核 CIS Microsoft Azure Foundations Benchmark v1.1.0 建议并部署特定 VM 扩展以支持审核要求”内置策略计划。

> **NOTE**
> 完整的蓝图示例即将推出。关联的 Azure Policy 计划现已推出。

1.1 确保为所有特权用户启用多重身份验证

此蓝图分配与此 CIS 建议相符的 Azure Policy 定义。

- 应在对订阅拥有所有者权限的帐户上启用 MFA
- 应在对订阅拥有写入权限的帐户上启用 MFA

1.2 确保为所有非特权用户启用多重身份验证

此蓝图分配与此 CIS 建议相符的 Azure Policy 定义。

- 应在对订阅拥有读取权限的帐户上启用 MFA

1.3 确保没有任何来宾用户

此蓝图分配与此 CIS 建议相符的 Azure Policy 定义。

- 应从订阅中删除拥有所有者权限的外部帐户
- 应从订阅中删除拥有读取权限的外部帐户
- 应从订阅中删除具有写入权限的外部帐户

2.3 确保 ASC 默认策略设置“监视系统更新”不是处于“已禁用”状态

此蓝图分配与此 CIS 建议相符的 Azure Policy 定义。

- 应在计算机上安装系统更新

2.4 确保 ASC 默认策略设置“监视 OS 漏洞”不是处于“已禁用”状态

此蓝图分配与此 CIS 建议相符的 Azure Policy 定义。

- 应该修复计算机上安全配置中的漏洞

2.5 确保 ASC 默认策略设置“监视终结点保护”不是处于“已禁用”状态

此蓝图分配与此 CIS 建议相符的 Azure Policy 定义。

- 监视 Azure 安全中心 Endpoint Protection 的缺失情况

2.6 确保 ASC 默认策略设置“监视磁盘加密”不是处于“已禁用”状态

此蓝图分配与此 CIS 建议相符的 Azure Policy 定义。

- 应在虚拟机上启用磁盘加密

2.8 确保 ASC 默认策略设置“监视 Web 应用程序防火墙”不是处于“已禁用”状态

此蓝图分配与此 CIS 建议相符的 Azure Policy 定义。

- 应该强化 IaaS 上 Web 应用程序的 NSG 规则

2.10 确保 ASC 默认策略设置“监视漏洞评估”不是处于“已禁用”状态

此蓝图分配与此 CIS 建议相符的 Azure Policy 定义。

- 应该通过漏洞评估解决方案修复漏洞

2.12 确保 ASC 默认策略设置“监视 JIT 网络访问”不是处于“已禁用”状态

此蓝图分配与此 CIS 建议相符的 Azure Policy 定义。

- 应在虚拟机上应用实时网络访问控制

2.15 确保 ASC 默认策略设置“监视 SQL 加密”不是处于“已禁用”状态

此蓝图分配与此 CIS 建议相符的 Azure Policy 定义。

- 应在 SQL 数据库上启用透明数据加密

3.1 确保“需要安全传输”设置为“已启用”

此蓝图分配与此 CIS 建议相符的 Azure Policy 定义。

- 应该启用安全传输到存储帐户

3.7 确保将针对存储帐户的默认网络访问规则设置为“拒绝”

此蓝图分配与此 CIS 建议相符的 Azure Policy 定义。

- 审核对存储帐户的不受限的网络访问

4.1 确保“审核”设置为“打开”

此蓝图分配与此 CIS 建议相符的 Azure Policy 定义。

- 应在 SQL Server 的高级数据安全设置上启用审核

4.2 确保在“审核”策略中为 SQL 服务器正确设置“AuditActionGroups”

此蓝图分配与此 CIS 建议相符的 Azure Policy 定义。

- SQL 审核设置中应包含配置为捕获关键活动的操作组

4.3 确保审核保留期“大于 90 天”

此蓝图分配与此 CIS 建议相符的 Azure Policy 定义。

- 应将 SQL 服务器的审核保留期配置为大于 90 天。

4.4 确保将 SQL 服务器上的“高级数据安全性”设置为“打开”

此蓝图分配与此 CIS 建议相符的 Azure Policy 定义。

- 应在 SQL 服务器上启用高级数据安全性

4.5 确保“威胁检测类型”设置为“所有”

此蓝图分配与此 CIS 建议相符的 Azure Policy 定义。

- 应在 SQL 服务器的“高级数据安全性”设置中将“高级威胁保护类型”设置为“所有”
- 应在 SQL 托管实例的“高级数据安全性”设置中将“高级威胁保护类型”设置为“所有”

4.6 确保设置“将警报发送到”

此蓝图分配与此 CIS 建议相符的 Azure Policy 定义。

- SQL 服务器的“高级数据安全性”设置应包含用于接收安全警报的电子邮件地址

4.7 确保“电子邮件服务和协同管理员”设置为“已启用”

此蓝图分配与此 CIS 建议相符的 Azure Policy 定义。

- SQL 托管实例的“高级数据安全性”设置应包含用于接收安全警报的电子邮件地址

4.8 确保配置 Azure Active Directory 管理员

此蓝图分配与此 CIS 建议相符的 Azure Policy 定义。

- 应该为 SQL 服务器预配 Azure Active Directory 管理员

4.9 确保将 SQL 数据库上的“数据加密”设置为“打开”

此蓝图分配与此 CIS 建议相符的 Azure Policy 定义。

- 应在 SQL 数据库上启用透明数据加密

4.10 确保使用 BYOK(使用自己的密钥)加密 SQL 服务器的 TDE 保护器

此蓝图分配与此 CIS 建议相符的 Azure Policy 定义。

- 应使用自己的密钥加密 SQL 服务器的 TDE 保护器
- 应使用自己的密钥加密 SQL 托管实例的 TDE 保护器

5.1.7 确保 Azure KeyVault 日志记录设置为“已启用”

此蓝图分配与此 CIS 建议相符的 Azure Policy 定义。

- 应启用 Key Vault 中的诊断日志

7.1 确保“OS 磁盘”已加密

此蓝图分配与此 CIS 建议相符的 Azure Policy 定义。

- 应在虚拟机上启用磁盘加密

7.2 确保“数据磁盘”已加密

此蓝图分配与此 CIS 建议相符的 Azure Policy 定义。

- 应在虚拟机上启用磁盘加密

7.5 确保已应用适用于所有虚拟机的最新 OS 修补程序

此蓝图分配与此 CIS 建议相符的 Azure Policy 定义。

- 应在计算机上安装系统更新

7.6 确保已安装适用于所有虚拟机的终结点保护

此蓝图分配与此 CIS 建议相符的 Azure Policy 定义。

- 监视 Azure 安全中心 Endpoint Protection 的缺失情况

8.5 在 Azure Kubernetes 服务中启用基于角色的访问控制 (RBAC)

此蓝图分配与此 CIS 建议相符的 Azure Policy 定义。

- [预览]: 应在 Kubernetes 服务中使用基于角色的访问控制 (RBAC)

9.2 确保 Web 应用将所有 HTTP 流量重定向到 Azure 应用服务中的 HTTPS

此蓝图分配与此 CIS 建议相符的 Azure Policy 定义。

- 只能通过 HTTPS 访问 Web 应用程序

后续步骤

了解 CIS Microsoft Azure Foundations Benchmark 蓝图的控制映射后，接下来请阅读以下文章了解该蓝图，或者在 Azure 门户中访问 Azure Policy 以分配计划：

CIS Microsoft Azure Foundations Benchmark 蓝图 - 概述 Azure 门户

有关蓝图和如何使用这些蓝图的更多文章：

- 了解蓝图生命周期。
- 了解如何使用静态和动态参数。
- 了解如何自定义蓝图排序顺序。
- 了解如何利用蓝图资源锁定。
- 了解如何更新现有分配。

IRS 1075 蓝图示例概述

2019/9/4 • • Edit Online

IRS 1075 蓝图示例提供了监管防护措施，其中使用 Azure Policy 来帮助评估特定 IRS 1075 控制要求。对于 Azure 部署的任何必须实现 IRS 1075 控制要求的体系结构，此蓝图可帮助客户为其部署一组核心策略。

控制映射

控制映射部分提供了有关包含在此蓝图内的策略的详细信息，以及这些策略如何满足 IRS 1075 中的各种控制要求。分配给一个体系结构时，资源由 Azure Policy 评估是否不符合已分配的策略。有关详细信息，请参阅 Azure Policy。

后续步骤

你已查看了 IRS 1075 蓝图示例概述。接下来，请访问以下文章，了解控制映射以及如何部署此示例：

IRS 1075 蓝图 - 控制映射

有关蓝图和如何使用这些蓝图的更多文章：

- 了解蓝图生命周期。
- 了解如何使用静态和动态参数。
- 了解如何自定义蓝图排序顺序。
- 了解如何利用蓝图资源锁定。
- 了解如何更新现有分配。

IRS 1075 蓝图示例的控制映射

2019/9/2 • • Edit Online

以下文章详细说明了 Azure 蓝图 IRS 1075 蓝图示例如何映射到 IRS 1075 控制措施。有关控制措施的详细信息，请参阅 IRS 1075。

以下映射适用于 **IRS 1075** 控制措施。使用右侧的导航栏可直接跳转到特定的控制映射。许多的映射控制措施都是使用 Azure Policy 计划实施的。若要查看完整计划，请在 Azure 门户中打开“策略”，并选择“定义”页。然后，找到并选择“[预览]:审核 IRS 1075 控制措施并部署特定 VM 扩展以支持审核要求”内置策略计划 。

9.3.2.1 AC-2 帐户管理

此蓝图可帮助你查看可能不符合你组织的帐户管理要求的帐户。此蓝图分配 Azure Policy 定义，这些定义用于审核对订阅和弃用帐户具有读、写和所有者权限的外部帐户。通过查看受到这些策略审核的帐户，可以采取适当的措施，确保满足帐户管理要求。

- 应从订阅中删除弃用的帐户
- 应从订阅中删除拥有所有者权限的已弃用帐户
- 应从订阅中删除拥有所有者权限的外部帐户
- 应从订阅中删除拥有读取权限的外部帐户
- 应从订阅中删除具有写入权限的外部帐户

9.3.2.1 AC-2 (7) 帐户管理 | 基于角色的方案

Azure 实施了基于角色的访问控制 (RBAC) 来帮助你管理谁有权访问 Azure 中的资源。使用 Azure 门户可以评审有权访问 Azure 资源的用户及其权限。此蓝图还分配 Azure Policy 定义，用于审核 Azure Active Directory 身份验证在 SQL 服务器和 Service Fabric 中的使用。使用 Azure Active Directory 身份验证可以简化权限管理，以及集中化数据库用户和其他 Microsoft 服务的标识管理。此外，此蓝图还分配一个 Azure Policy 定义用于审核自定义 RBAC 规则的使用。了解实施自定义 RBAC 规则的位置有助于验证需求以及实施是否适当，因为自定义 RBAC 规则容易出错。

- 应该为 SQL 服务器预配 Azure Active Directory 管理员
- 审核自定义 RBAC 规则的使用
- Service Fabric 群集只应使用 Azure Active Directory 进行客户端身份验证

9.3.2.1 AC-2 (12) 帐户管理 | 帐户监视/异常使用

实时 (JIT) 虚拟机访问会锁定发往 Azure 虚拟机的入站流量，降低遭受攻击的可能性，同时在需要时还可轻松连接到 VM。所有访问虚拟机的 JIT 请求都记录在活动日志中，用于监视异常使用情况。此蓝图分配了一个 Azure Policy 定义，有助于你监视能够支持实时访问但尚未配置的虚拟机。

- 应在虚拟机上应用实时网络访问控制

9.3.1.4 AC-4 信息流强制

跨域资源共享 (CORS) 支持从外部域请求应用服务资源。Microsoft 建议只允许必需的域与 API、函数和 web 应用程序进行交互。此蓝图分配了一个 Azure Policy 定义，有助于你监视 Azure 安全中心中的 CORS 资源访问限制。了解 CORS 实现有助于你验证信息流控制措施是否实现。

- CORS 不应允许所有资源都能访问你的 Web 应用程序

9.3.1.5 AC-5 职责分离

仅分配一个 Azure 订阅所有者并不能实现管理冗余。相反，分配过多的 Azure 订阅所有者会增大违规的可能性，因为会有更多的所有者帐户可能会泄密。此蓝图可帮助你通过分配用于审核 Azure 订阅所有者数目的 Azure Policy 定义，来保持适当的 Azure 订阅所有者数目。此蓝图还分配 Azure Policy 定义，有助于你控制 Windows 虚拟机上管理员组的成员身份。管理订阅所有者和虚拟机管理员权限有助于实现适当的职责分离。

- 只多只为订阅指定 3 个所有者
- 审核在其管理员组中包含任何指定成员的 Windows VM
- 审核在其管理员组中不包含所有指定成员的 Windows VM
- 部署要求以审核在其管理员组中包含任何指定成员的 Windows VM
- 部署要求以审核在其管理员组中不包含所有指定成员的 Windows VM
- 应该为你的订阅分配了多个所有者

9.3.1.6 AC-6 (7) 最小特权 | 用户特权评审

Azure 实施了基于角色的访问控制 (RBAC) 来帮助你管理谁有权访问 Azure 中的资源。使用 Azure 门户可以评审有权访问 Azure 资源的用户及其权限。此蓝图分配 Azure Policy 定义，用于审核应优先评审的帐户。评审这些帐户指标可帮助确保实现最低特权控制措施。

- 只多只为订阅指定 3 个所有者
- 审核在其管理员组中包含任何指定成员的 Windows VM
- 审核在其管理员组中不包含所有指定成员的 Windows VM
- 部署要求以审核在其管理员组中包含任何指定成员的 Windows VM
- 部署要求以审核在其管理员组中不包含所有指定成员的 Windows VM
- 应该为你的订阅分配了多个所有者

9.3.1.12 AC-17 (1) 远程访问 | 自动监视/控制

此蓝图可帮助你监视和控制远程访问，因为它会分配 Azure Policy 定义用于监视 Azure 应用服务应用程序的远程调试处于关闭状态，此蓝图还会分配策略定义用于审核允许来自无密码帐户的远程连接的 Linux 虚拟机。此蓝图还将分配一个 Azure Policy 定义，用于帮助监视对存储帐户的无限制访问。监视这些指标可以帮助确保远程访问方法符合安全策略。

- [预览]: 审核允许通过没有密码的帐户进行远程连接的 Linux VM
- [预览]: 部署要求以审核允许通过没有密码的帐户进行远程连接的 Linux VM
- 审核对存储帐户的不受限的网络访问
- 应为 API 应用禁用远程调试
- 应对函数应用禁用远程调试
- 应禁用 Web 应用程序的远程调试

9.3.1.3 AU-3 (2) 审核记录的内容 | 计划的审核记录内容的集中管理

Azure Monitor 收集的日志数据存储在支持集中配置和管理的 Log Analytics 工作区中。此蓝图通过分配 Azure Policy 定义来确保事件被记录下来，这些定义审核并强制在 Azure 虚拟机上部署 Log Analytics 代理。

- [预览]: 审核 Log Analytics 代理部署 - VM 映像 (OS) 未列出
- [预览]: 审核 VMSS 中的 Log Analytics 代理部署 - VM 映像 (OS) 未列出
- [预览]: 审核 VM 的 Log Analytics 工作区 — 报告不匹配
- [预览]: 为 Linux VM 规模集(VMSS)部署 Log Analytics 代理
- [预览]: 为 Linux VM 部署 Log Analytics 代理
- [预览]: 为 Windows VM 规模集(VMSS)部署 Log Analytics 代理

- [预览]: 为 Windows VM 部署 Log Analytics 代理

9.3.3.5 AU-5 对审核处理失败的响应

此蓝图分配 Azure Policy 定义用于监视审核和事件日志记录配置。监视这些配置可以提供审核系统故障或配置错误的指标，帮助你采取纠正措施。

- 审核诊断设置
- 审核 SQL 服务器级别审核设置
- 应在托管实例上启用高级数据安全性
- 应在 SQL 服务器上启用高级数据安全性

9.3.3.6 AU-6 (4) 审核评审、分析和报告 | 中心评审和分析

Azure Monitor 收集的日志数据存储在支持集中报告和分析的 Log Analytics 工作区中。此蓝图通过分配 Azure Policy 定义来确保事件被记录下来，这些定义审核并强制在 Azure 虚拟机上部署 Log Analytics 代理。

- [预览]: 审核 Log Analytics 代理部署 - VM 映像 (OS) 未列出
- [预览]: 审核 VMSS 中的 Log Analytics 代理部署 - VM 映像 (OS) 未列出
- [预览]: 审核 VM 的 Log Analytics 工作区 — 报告不匹配
- [预览]: 为 Linux VM 规模集(VMSS)部署 Log Analytics 代理
- [预览]: 为 Linux VM 部署 Log Analytics 代理
- [预览]: 为 Windows VM 规模集(VMSS)部署 Log Analytics 代理
- [预览]: 为 Windows VM 部署 Log Analytics 代理

9.3.3.11 AU-12 审核生成

此蓝图通过分配 Azure Policy 定义来帮助确保记录系统事件，这些定义用于审核在 Azure 资源上的日志设置。这些策略定义审核并强制部署 Azure 虚拟机上的 Log Analytics 代理并强制配置针对其他 Azure 资源类型的审核设置。这些策略定义还审核诊断日志配置，以提供对 Azure 资源内执行的操作的见解。此外，审核和高级数据安全在 SQL 服务器上配置。

- [预览]: 审核 Log Analytics 代理部署 - VM 映像 (OS) 未列出
- [预览]: 审核 VMSS 中的 Log Analytics 代理部署 - VM 映像 (OS) 未列出
- [预览]: 审核 VM 的 Log Analytics 工作区 — 报告不匹配
- [预览]: 为 Linux VM 规模集(VMSS)部署 Log Analytics 代理
- [预览]: 为 Linux VM 部署 Log Analytics 代理
- [预览]: 为 Windows VM 规模集(VMSS)部署 Log Analytics 代理
- [预览]: 为 Windows VM 部署 Log Analytics 代理
- 审核诊断设置
- 审核 SQL 服务器级别审核设置
- 应在托管实例上启用高级数据安全性
- 应在 SQL 服务器上启用高级数据安全性
- 在 SQL 服务器上部署高级数据安全
- 对 SQL 服务器部署审核
- 为网络安全组部署诊断设置

9.3.5.7 CM-7 (2) 最少的功能 | 防止程序执行

Azure 安全中心中的自适应应用程序控制是一种智能、自动化端到端的应用程序允许列表解决方案，可以阻止或防止特定软件在虚拟机上运行。应用程序控制可以在强制模式下运行，从而禁止未批准的应用程序运行。此蓝图分配

了一个 Azure Policy 定义，用于帮助监视建议使用应用程序允许列表但尚未对其进行配置的虚拟机。

- 应在虚拟机上启用自适应应用程序控制

9.3.5.7 CM-7 (5) 最少的功能 | 授权软件/允许列表

Azure 安全中心中的自适应应用程序控制是一种智能、自动化端到端的应用程序允许列表解决方案，可以阻止或防止特定软件在虚拟机上运行。应用程序控制帮助你为虚拟机创建批准的应用程序列表。此蓝图分配了一个 Azure Policy 定义，用于帮助监视建议使用应用程序允许列表但尚未对其进行配置的虚拟机。

- 应在虚拟机上启用自适应应用程序控制

9.3.5.11 CM-11 用户安装的软件

Azure 安全中心中的自适应应用程序控制是一种智能、自动化端到端的应用程序允许列表解决方案，可以阻止或防止特定软件在虚拟机上运行。应用程序控制可以帮助你强制执行和监视软件限制策略的符合性。此蓝图分配了一个 Azure Policy 定义，用于帮助监视建议使用应用程序允许列表但尚未对其进行配置的虚拟机。

- 应在虚拟机上启用自适应应用程序控制

9.3.6.6 CP-7 备用处理站点

Azure Site Recovery 将在虚拟机上运行的工作负荷从主位置复制到辅助位置。如果在主站点发生故障，工作负荷将故障转移到辅助位置。此蓝图分配了一个 Azure Policy 定义，用于审核没有配置灾难恢复的虚拟机。监视此指标可以帮助确保必要的应变控制措施已到位。

- 审核没有配置灾难恢复的虚拟机

9.3.7.2 IA-2 (1) 标识和身份验证(组织用户)| 对特权帐户的网络访问

此蓝图分配 Azure Policy 定义用于审核拥有所有者和/或写入权限但未启用多重身份验证的帐户，从而帮助你限制和控制特权访问。即使某个身份验证信息片段已泄密，多重身份验证也有助于保护帐户的安全。通过监视未启用多重身份验证的帐户，可以识别出更有可能会泄密的帐户。

- 应在对订阅拥有所有者权限的帐户上启用 MFA
- 应在对订阅拥有写入权限的帐户上启用 MFA

9.3.7.2 IA-2 (2) 标识和身份验证(组织用户)| 网络访问非特权帐户

此蓝图分配一个 Azure Policy 定义，用于审核拥有读取权限但未启用多重身份验证的帐户，从而帮助你限制和控制访问。即使某个身份验证信息片段已泄密，多重身份验证也有助于保护帐户的安全。通过监视未启用多重身份验证的帐户，可以识别出更有可能会泄密的帐户。

- 应在对订阅拥有读取权限的帐户上启用 MFA

9.3.7.5 IA-5 验证器管理

此蓝图分配 Azure Policy 定义，用于审核允许来自无密码帐户的远程连接并/或在密码文件中设置了不正确权限的 Linux 虚拟机。此蓝图还会分配一个策略定义用于审核 Windows 虚拟机密码加密类型的配置。监视这些指标有助于确保系统验证器符合组织的标识和身份验证策略。

- [预览]: 审核未将密码文件权限设为 0644 的 Linux VM
- [预览]: 审核具有不使用密码的帐户的 Linux VM
- [预览]: 审核未存储使用可逆加密的密码的 Windows VM
- [预览]: 部署要求以审核未将密码文件权限设置为 0644 的 Linux VM
- [预览]: 部署要求以审核具有不使用密码的帐户的 Linux VM

- [预览]: 部署要求以审核未存储使用可逆加密的密码的 Windows VM

9.3.7.5 IA-5 (1) 验证器管理 |基于密码的身份验证

此蓝图通过分配 Azure Policy 定义用于审核不强制实施最低强度和其他密码要求的 Windows 虚拟机，来帮助你强制实施强密码。感知虚拟机是否违反密码强度策略有助于采取纠正措施，确保所有虚拟机用户帐户的密码与组织的密码策略相符。

- [预览]: 审核允许重用之前的 24 个密码的 Windows VM
- [预览]: 审核未将最长密码期限设为 70 天的 Windows VM
- [预览]: 审核未将最短密码期限设为 1 天的 Windows VM
- [预览]: 审核未启用密码复杂性设置的 Windows VM
- [预览]: 审核未将最短密码长度限制为 14 个字符的 Windows VM
- [预览]: 审核未存储使用可逆加密的密码的 Windows VM
- [预览]: 部署要求以审核允许重用之前的 24 个密码的 Windows VM
- [预览]: 部署要求以审核未将最长密码期限设为 70 天的 Windows VM
- [预览]: 部署要求以审核未将最短密码期限设为 1 天的 Windows VM
- [预览]: 部署要求以审核未启用密码复杂性设置的 Windows VM
- [预览]: 部署要求以审核未将最短密码长度限制为 14 个字符的 Windows VM
- [预览]: 部署要求以审核未存储使用可逆加密的密码的 Windows VM

9.3.14.3 RA-5 漏洞扫描

此蓝图分配 Azure Policy 定义用于在 Azure 安全中心内监视操作系统漏洞、SQL 漏洞和虚拟机漏洞，来帮助你管理信息系统漏洞。Azure 安全中心提供报告功能，使你能够实时洞察已部署的 Azure 资源的安全状态。此蓝图还会分配策略定义用于审核和强制执行 SQL 服务器上的高级数据安全。高级数据安全包括漏洞评估和高级威胁防护功能，可帮助你了解已部署资源中的漏洞。

- 应在托管实例上启用高级数据安全性
- 应在 SQL 服务器上启用高级数据安全性
- 在 SQL 服务器上部署高级数据安全
- 应该修复虚拟机规模集上安全配置中的漏洞
- 应该修复虚拟机上安全配置中的漏洞
- 应该修复 SQL 数据库中的漏洞
- 应该通过漏洞评估解决方案修复漏洞

9.3.16.4 SC-5 拒绝服务保护

Azure 的分布式拒绝服务 (DDoS) 标准层通过基本服务层提供额外功能和缓解功能。这些额外功能包括 Azure Monitor 集成和查看攻击后的缓解报告的功能。此蓝图分配了一个 Azure Policy 定义，用于审核是否启用 DDoS 标准层。了解服务层之间的功能差异有助于为 Azure 环境选择最佳解决方案来解决拒绝服务保护问题。

- 应启用 DDoS 防护标准版

9.3.16.5 SC-7 边界保护

此蓝图通过分配一个 Azure Policy 定义用于根据 Azure 安全中心的网络安全组强化建议进行监视，以此帮助你管理和控制系统边界。Azure 安全中心分析面向 Internet 的虚拟机的流量模式，并提供网络安全组规则建议，以减少潜在的攻击面。此外，此蓝图还会分配策略定义用于监视不受保护的终结点、应用程序和存储帐户。不受防火墙保护的终结点和应用程序，以及具有无限制访问权限的存储帐户，可能会允许意外访问信息系统中包含的信息。

- 应该强化面向 Internet 的虚拟机的网络安全组规则

- 应该限制通过面向 Internet 的终结点进行访问
- 应该强化 IaaS 上 Web 应用程序的 NSG 规则
- 审核对存储帐户的不受限的网络访问

9.3.16.5 SC-7 (3) 边界保护 | 接入点

实时 (JIT) 虚拟机访问会锁定发往 Azure 虚拟机的入站流量，降低遭受攻击的可能性，同时在需要时还可轻松连接到 VM。实时虚拟机访问有助于限制对 Azure 中资源的外部连接数。此蓝图分配了一个 Azure Policy 定义，有助于你监视能够支持实时访问但尚未配置的虚拟机。

- 应在虚拟机上应用实时网络访问控制

9.3.16.5 SC-7 (4) 边界保护 | 外部电信服务

实时 (JIT) 虚拟机访问会锁定发往 Azure 虚拟机的入站流量，降低遭受攻击的可能性，同时在需要时还可轻松连接到 VM。实时虚拟机访问有助于通过促进访问请求和审批流程来管理流量策略的例外情况。此蓝图分配了一个 Azure Policy 定义，有助于你监视能够支持实时访问但尚未配置的虚拟机。

- 应在虚拟机上应用实时网络访问控制

9.6.16.3 SC-8 (1) 传输保密性和完整性 | 加密或备用物理保护

此蓝图分配 Azure Policy 定义来帮助你监视针对通信协议实施的加密机制，以此帮助你保护传输信息的机密性和完整性。确保通信得到适当的加密可帮助你满足组织的要求，或者防范信息遭到未经授权的透漏和修改。

- 只能通过 HTTPS 访问 API 应用
- 审核未使用安全通信协议的 Windows Web 服务器
- 部署要求以审核未使用安全通信协议的 Windows Web 服务器
- 应该只能通过 HTTPS 访问函数应用
- 应该启用只能通过安全方式连接到 Redis 缓存
- 应该启用安全传输到存储帐户
- 只能通过 HTTPS 访问 Web 应用程序

9.3.16.6 SC-28 (1) 保护静态信息 | 加密保护

此蓝图分配 Azure Policy 定义用于强制实施特定的加密控制措施并审核弱加密设置的使用，从而帮助你强制实施有关通过使用加密控制措施保护静态信息的策略。了解 Azure 资源中的哪些位置采用欠佳的加密配置有助于采取纠正措施，以确保根据信息安全策略配置资源。具体地说，该蓝图分配的策略定义要求对数据湖存储帐户进行加密；要求 SQL 数据库上的透明数据加密；审核 SQL 数据库、虚拟机磁盘和自动化帐户变量上缺少的加密。

- 应在托管实例上启用高级数据安全性
- 应在 SQL 服务器上启用高级数据安全性
- 在 SQL 服务器上部署高级数据安全
- 部署 SQL DB 透明数据加密
- 应在虚拟机上启用磁盘加密
- 要求对 Data Lake Store 帐户加密
- 应在 SQL 数据库上启用透明数据加密

9.3.17.2 SI-2 缺陷修正

此蓝图分配 Azure Policy 定义用于在 Azure 安全中心内监视缺少的系统更新、操作系统漏洞、SQL 漏洞和虚拟机漏洞，从而帮助你管理信息系统缺陷。Azure 安全中心提供报告功能，使你能够实时洞察已部署的 Azure 资源的安全状态。此蓝图还会分配一个策略定义用于确保虚拟机规模集的操作系统的修补。

- 要求自动在虚拟机规模集上执行 OS 映像修补
- 应在虚拟机规模集上安装系统更新
- 应在虚拟机上安装系统更新
- 应该修复虚拟机规模集上安全配置中的漏洞
- 应该修复虚拟机上安全配置中的漏洞
- 应该修复 SQL 数据库中的漏洞
- 应该通过漏洞评估解决方案修复漏洞

9.3.17.3 SI-3 恶意代码防护

此蓝图分配 Azure Policy 定义用于监视 Azure 安全中心中虚拟机上缺失的终结点防护并在 Windows 虚拟机上强制执行 Microsoft 反恶意软件解决方案，从而帮助管理终结点防护，包括恶意代码防护。

- 为 Windows Server 部署默认 Microsoft IaaSAntimalware 扩展
- 应在虚拟机规模集上安装 Endpoint Protection 解决方案
- 监视 Azure 安全中心 Endpoint Protection 的缺失情况

9.3.17.3 SI-3 (1) 恶意代码防护 | 集中管理

此蓝图分配 Azure Policy 定义用于监视 Azure 安全中心中虚拟机上缺失的终结点防护，从而帮助管理终结点防护，包括恶意代码防护。Azure 安全中心提供集中管理和报告功能，用于实时洞察已部署的 Azure 资源的安全状态。

- 应在虚拟机规模集上安装 Endpoint Protection 解决方案
- 监视 Azure 安全中心 Endpoint Protection 的缺失情况

9.3.17.4 SI-4 信息系统监视

此蓝图有助于通过审核和跨 Azure 资源强制执行日志记录和数据安全来监视系统。具体而言，分配的策略审核并强制执行 Log Analytics 代理的部署和 SQL 数据库、存储帐户和网络资源的强化安全设置。这些功能有助于检测异常行为和攻击指标，以便你采取相应措施。

- [预览]: 审核 Log Analytics 代理部署 - VM 映像 (OS) 未列出
- [预览]: 审核 VMSS 中的 Log Analytics 代理部署 - VM 映像 (OS) 未列出
- [预览]: 审核 VM 的 Log Analytics 工作区 — 报告不匹配
- [预览]: 为 Linux VM 规模集(VMSS)部署 Log Analytics 代理
- [预览]: 为 Linux VM 部署 Log Analytics 代理
- [预览]: 为 Windows VM 规模集(VMSS)部署 Log Analytics 代理
- [预览]: 为 Windows VM 部署 Log Analytics 代理
- 应在托管实例上启用高级数据安全性
- 应在 SQL 服务器上启用高级数据安全性
- 在 SQL 服务器上部署高级数据安全
- 在存储帐户上部署高级威胁防护
- 对 SQL 服务器部署审核
- 创建虚拟网络时部署网络观察程序
- 在 SQL 服务器上部署威胁检测

9.3.17.4 SI-4 (18) 信息系统监视 | 分析流量 / 隐蔽性外泄

Azure 存储高级威胁防护会检测试图访问或利用存储帐户的异常或可能有害的企图。保护警报包括异常访问模式、异常提取/上传和可疑存储活动。这些指标有助于检测信息的隐蔽性外泄。

- 在存储帐户上部署高级威胁防护

> **NOTE**
> 特定 Azure Policy 定义的可用性在 Azure 政府和其他国家云中可能会有所不同。

后续步骤

了解 IRS 1075 蓝图的控制映射后，请访问以下文章来了解蓝图和部署此示例的方式：

IRS 1075 蓝图 - 概述

有关蓝图和如何使用这些蓝图的更多文章：

- 了解蓝图生命周期。
- 了解如何使用静态和动态参数。
- 了解如何自定义蓝图排序顺序。
- 了解如何利用蓝图资源锁定。
- 了解如何更新现有分配。

ISO 27001 蓝图示例概述

2019/9/4 • • Edit Online

ISO 27001 蓝图示例提供了监管防护措施，其中使用 Azure Policy 来帮助评估特定 ISO 27001 控制要求。对于 Azure 部署的任何必须实现 ISO 27001 控制要求的体系结构，此蓝图可帮助客户为其部署一组核心策略。此外，还提供了另外两个 ISO 27001 蓝图示例，它们可帮助你部署基础体系结构和 ASE/SQL 工作负荷。

控制映射

控制映射部分提供了有关包含在此蓝图内的策略的详细信息，以及这些策略如何满足 ISO 27001 中的各种控制要求。分配给一个体系结构时，资源由 Azure Policy 评估是否不符合已分配的策略。有关详细信息，请参阅 Azure Policy。

后续步骤

你已查看了 ISO 27001 蓝图示例的概述和体系结构。接下来，请访问以下文章，了解控制映射以及如何部署此示例：

ISO 27001 蓝图 - 控制映射 ISO 27001 蓝图 - 部署步骤

有关蓝图和如何使用这些蓝图的更多文章：

- 了解蓝图生命周期。
- 了解如何使用静态和动态参数。
- 了解如何自定义蓝图排序顺序。
- 了解如何利用蓝图资源锁定。
- 了解如何更新现有分配。

ISO 27001 蓝图示例的控制映射

2019/9/5 • • Edit Online

以下文章详细说明了 Azure 蓝图 ISO 27001 蓝图示例如何映射到 ISO 27001 控制措施。有关控制措施的详细信息，请参阅 ISO 27001。

以下映射适用于 **ISO 27001:2013** 控制措施。使用右侧的导航栏可直接跳转到特定的控制映射。许多的映射控制措施都是使用 Azure Policy 计划实施的。若要查看完整计划，请在 Azure 门户中打开“策略”，并选择“定义”页。然后，找到并选择“[预览] 审核 ISO 27001:2013 控制措施并部署特定 VM 扩展以支持审核要求”内置策略计划。

A.6.1.2 职责分离

仅分配一个 Azure 订阅所有者并不能实现管理冗余。相反，分配过多的 Azure 订阅所有者会增大违规的可能性，因为会有更多的所有者帐户可能会泄密。此蓝图可帮助你通过分配两个用于审核 Azure 订阅所有者数目的 Azure Policy 定义，来保持适当的 Azure 订阅所有者数目。管理订阅所有者权限有助于实现适当的职责分离。

- [预览]: 审核最小订阅所有者数
- [预览]: 审核最大订阅所有者数

A.8.2.1 信息分类

Azure 的 SQL 漏洞评估服务可以帮助你发现数据库中存储的敏感数据并提供用于对该数据进行分类的建议。此蓝图分配了一个 Azure Policy 定义来审核在 SQL 漏洞评估过程中查明的漏洞是否已更正。

- [预览]: 监视 Azure 安全中心的 SQL 漏洞评估结果

A.9.1.2 访问网络和网络服务

Azure 实施基于角色的访问控制 (RBAC) 来管理谁有权访问 Azure 资源。此蓝图可帮助你通过分配七个 Azure Policy 定义来控制对 Azure 资源的访问。这些策略将审核可能允许更高资源访问权限的资源类型和配置的使用。了解违反这些策略的资源有助于采取纠正措施来确保仅限已授权的用户访问 Azure 资源。

- [预览]: 部署 VM 扩展以审核没有密码的 Linux VM 帐户
- [预览]: 部署 VM 扩展以审核允许从没有密码的帐户进行远程连接的 Linux VM
- [预览]: 审核没有密码的 Linux VM 帐户
- [预览]: 审核允许从没有密码的帐户进行远程连接的 Linux VM
- 审核经典存储帐户的使用
- 审核经典虚拟机的使用
- 审核不使用托管磁盘的 VM

A.9.2.3 管理特权访问权限

此蓝图通过分配四个 Azure Policy 定义用于审核拥有所有者和/或写入权限的外部帐户，以及拥有所有者和/或写入权限、但未启用多重身份验证的帐户，来帮助你限制和控制特权访问权限。Azure 实施基于角色的访问控制 (RBAC) 来管理谁有权访问 Azure 资源。此蓝图还分配了三个 Azure Policy 定义，用于审核 Azure Active Directory 身份验证在 SQL 服务器和 Service Fabric 中的使用。使用 Azure Active Directory 身份验证可以简化权限管理，以及集中化数据库用户和其他 Microsoft 服务的标识管理。此蓝图还分配一个 Azure Policy 定义用于审核自定义 RBAC 规则的使用。了解实施自定义 RBAC 规则的位置有助于验证需求以及实施是否适当，因为自定义 RBAC 规则容易出错。

- [预览]: 审核具有所有者权限但未启用 MFA 的订阅帐户

- [预览]: 审核具有写入权限但未启用 MFA 的订阅帐户
- [预览]: 审核具有所有者权限的外部订阅帐户
- [预览]: 审核具有写入权限的外部订阅帐户
- 审核确认已为 SQL Server 预配了 Azure Active Directory 管理员
- 审核确认已在 Service Fabric 中使用 Azure Active Directory，用于实施客户端身份验证
- 审核自定义 RBAC 规则的使用

A.9.2.4 管理用户的机密身份验证信息

此蓝图分配三个 Azure Policy 定义用于审核未启用多重身份验证的帐户。即使某个身份验证信息片段已泄密，多重身份验证也有助于保护帐户的安全。通过监视未启用多重身份验证的帐户，可以识别出更有可能会泄密的帐户。此蓝图还将分配两个 Azure Policy 定义用于审核 Linux VM 密码文件权限，并在这些权限设置不当时发出警报。使用这种设置可以采取纠正措施，以确保验证器不会泄密。

- [预览]: 审核具有所有者权限但未启用 MFA 的订阅帐户
- [预览]: 审核具有读取权限但未启用 MFA 的订阅帐户
- [预览]: 审核具有写入权限但未启用 MFA 的订阅帐户
- [预览]: 部署 VM 扩展以审核 Linux VM 密码文件权限
- [预览]: 审核 Linux VM /etc/密码文件权限是否设置为 0644

A.9.2.5 评审用户访问权限

Azure 实施了基于角色的访问控制 (RBAC) 来帮助你管理谁有权访问 Azure 中的资源。使用 Azure 门户可以评审有权访问 Azure 资源的用户及其权限。此蓝图分配四个 Azure Policy 定义用于审核应该优先评审的帐户，包括已淘汰的帐户，以及具有提升权限的外部帐户。

- [预览]: 审核已弃用的订阅帐户
- [预览]: 审核具有所有者权限但已被弃用的订阅帐户
- [预览]: 审核具有所有者权限的外部订阅帐户
- [预览]: 审核具有写入权限的外部订阅帐户

A.9.2.6 删除或调整访问权限

Azure 实施了基于角色的访问控制 (RBAC) 来帮助你管理谁有权访问 Azure 中的资源。使用 Azure Active Directory 和 RBAC 可以更新用户角色，以反映组织变化。如果需要，可以阻止帐户登录(或将其删除)，这会立即删除其 Azure 资源访问权限。此蓝图分配两个 Azure Policy 定义用于审核应该考虑删除的已淘汰帐户。

- [预览]: 审核已弃用的订阅帐户
- [预览]: 审核具有所有者权限但已被弃用的订阅帐户

A.9.4.2 安全登录过程

此蓝图分配了三个 Azure Policy 定义，以用于审核未启用多重身份验证的帐户。Azure 多重身份验证通过要求使用另一种形式的身份验证提供额外的安全性，从而提供增强式身份验证。通过监视未启用多重身份验证的帐户，可以识别出更有可能会泄密的帐户。

- [预览]: 审核具有所有者权限但未启用 MFA 的订阅帐户
- [预览]: 审核具有读取权限但未启用 MFA 的订阅帐户
- [预览]: 审核具有写入权限但未启用 MFA 的订阅帐户

A.9.4.3 密码管理系统

此蓝图通过分配 10 个 Azure Policy 定义用于审核不强制实施最低强度和其他密码要求的 Windows VM，来帮助你

强制实施强密码。识别违反密码强度策略的 VM 有助于采取纠正措施，以确保所有 VM 用户帐户的密码符合策略。

- [预览]: 部署 VM 扩展以审核 Windows VM 是否强制实施密码复杂性要求
- [预览]: 部署 VM 扩展以审核 Windows VM 最长密码期限是否为 70 天
- [预览]: 部署 VM 扩展以审核 Windows VM 最短密码期限是否为 1 天
- [预览]: 部署 VM 扩展以审核 Windows VM 密码必须至少为 14 个字符
- [预览]: 部署 VM 扩展以审核 Windows VM 不应允许之前的 24 个密码
- [预览]: 审核 Windows VM 是否强制实施密码复杂性要求
- [预览]: 审核 Windows VM 最长密码期限是否为 70 天
- [预览]: 审核 Windows VM 最短密码期限是否为 1 天
- [预览]: 审核 Windows VM 密码必须至少为 14 个字符
- [预览]: 审核 Windows VM 不应允许之前的 24 个密码

A.10.1.1 有关使用加密控制措施的策略

此蓝图通过分配 13 个 Azure Policy 定义用于强制实施特定的加密控制措施并审核弱加密设置的使用，来帮助你针对加密控制措施的使用强制实施自己的策略。了解 Azure 资源中的哪些位置采用欠佳的加密配置有助于采取纠正措施，以确保根据信息安全策略配置资源。具体而言，此蓝图分配的策略要求对 Blob 存储帐户和 Data Lake Storage 帐户加密；要求对 SQL 数据库实施透明数据加密；审核存储帐户、SQL 数据库、虚拟机磁盘和自动化帐户变量是否缺少加密；审核是否与存储帐户、函数应用、Web 应用、API 应用和 Redis 缓存建立了不安全的连接；审核虚拟机弱密码加密；审核未加密的 Service Fabric 通信。

- [预览]: 审核函数应用的仅 HTTPS 访问权限
- [预览]: 审核 Web 应用的仅 HTTPS 访问权限
- [预览]: 审核 API 应用的仅 HTTPS 访问权限
- [预览]: 审核存储帐户是否缺少 blob 加密
- [预览]: 部署 VM 扩展以审核 Windows VM 不应使用可逆加密存储密码
- [预览]: 审核 Windows VM 不应使用可逆加密存储密码
- [预览]: 监视 Azure 安全中心内未加密的 VM 磁盘
- 审核确认已启用自动化帐户变量加密功能
- 审核确认仅启用了到 Redis 缓存的安全连接
- 审核确认指向存储帐户的传输的安全性
- 审核确认 Service Fabric 中的 ClusterProtectionLevel 属性设置为 EncryptAndSign
- 审核透明数据加密状态
- 应在 SQL 数据库上启用透明数据加密

A.12.4.1 事件日志记录

此蓝图通过分配七个 Azure Policy 定义用于审核 Azure 资源的日志设置，来帮助你确保记录系统事件。诊断日志针对 Azure 资源中执行的操作提供见解。

- [预览]: 审核依赖项代理部署 - VM 映像 (OS) 未列出
- [预览]: 审核 VMSS 中的依赖项代理部署 - VM 映像 (OS) 未列出
- [预览]: 审核 Log Analytics 代理部署 - VM 映像 (OS) 未列出
- [预览]: 审核 VMSS 中的 Log Analytics 代理部署 - VM 映像 (OS) 未列出
- 审核诊断设置
- 审核 SQL 服务器级别审核设置
- 应在 SQL Server 的高级数据安全设置上启用审核

A.12.4.3 管理员和操作员日志

此蓝图分配了七个 Azure Policy 定义，以用于审核 Azure 资源的日志设置，从而帮助你确保系统事件会被记录。诊断日志针对 Azure 资源中执行的操作提供见解。

- [预览]: 审核依赖项代理部署 - VM 映像 (OS) 未列出
- [预览]: 审核 VMSS 中的依赖项代理部署 - VM 映像 (OS) 未列出
- [预览]: 审核 Log Analytics 代理部署 - VM 映像 (OS) 未列出
- [预览]: 审核 VMSS 中的 Log Analytics 代理部署 - VM 映像 (OS) 未列出
- 审核诊断设置
- 审核 SQL 服务器级别审核设置
- 应在 SQL Server 的高级数据安全设置上启用审核

A.12.4.4 时钟同步

此蓝图分配了七个 Azure Policy 定义，以用于审核 Azure 资源的日志设置，从而帮助你确保系统事件会被记录。Azure 日志依赖于同步的内部时钟创建各个资源中事件的时间相关记录。

- [预览]: 审核依赖项代理部署 - VM 映像 (OS) 未列出
- [预览]: 审核 VMSS 中的依赖项代理部署 - VM 映像 (OS) 未列出
- [预览]: 审核 Log Analytics 代理部署 - VM 映像 (OS) 未列出
- [预览]: 审核 VMSS 中的 Log Analytics 代理部署 - VM 映像 (OS) 未列出
- 审核诊断设置
- 审核 SQL 服务器级别审核设置
- 应在 SQL Server 的高级数据安全设置上启用审核

A.12.5.1 在可操作的系统上安装软件

自适应应用程序控制是 Azure 安全中心内的一个解决方案，可帮助你控制哪些应用程序可在 Azure 中的 VM 上运行。此蓝图分配一个 Azure Policy 定义用于监视对允许的应用程序集的更改。此功能帮助你控制软件和应用程序在 Azure VM 上的安装。

- [预览]: 监视 Azure 安全中心内列入允许列表的可能的应用

A.12.6.1 管理技术漏洞

此蓝图分配了五个 Azure Policy 定义，以用于在 Azure 安全中心内监视缺少的系统更新、操作系统漏洞、SQL 漏洞和虚拟机漏洞，来帮助你管理信息系统漏洞。Azure 安全中心提供报告功能，使你能够实时洞察已部署的 Azure 资源的安全状态。

- [预览]: 监视 Azure 安全中心 Endpoint Protection 的缺失情况
- [预览]: 监视 Azure 安全中心内系统更新的缺失情况
- [预览]: 监视 Azure 安全中心的 OS 漏洞
- [预览]: 监视 Azure 安全中心的 SQL 漏洞评估结果
- [预览]: 监视 Azure 安全中心的 VM 漏洞

A.12.6.2 软件安装的限制

自适应应用程序控制是 Azure 安全中心内的一个解决方案，可帮助你控制哪些应用程序可在 Azure 中的 VM 上运行。此蓝图分配一个 Azure Policy 定义用于监视对允许的应用程序集的更改。软件安装限制有助于减少出现软件漏洞的可能性。

- [预览]: 监视 Azure 安全中心内列入允许列表的可能的应用

A.13.1.1 网络控制措施

此蓝图通过分配一个 Azure Policy 定义用于监视具有宽松规则的网络安全组，来帮助你管理和控制网络。过于宽松的规则可能会允许意外的网络访问，应该对其进行评审。此蓝图还分配了三个 Azure Policy 定义，以用于监视不受保护的终结点、应用程序和存储帐户。不受防火墙保护的终结点和应用程序，以及具有无限制访问权限的存储帐户，可能会允许意外访问信息系统中包含的信息。

- [预览]: 监视 Azure 安全中心内规则较宽松的网络访问
- [预览]: 监视 Azure 安全中心内未受保护的网络终结点
- [预览]: 监视 Azure 安全中心内未受保护的 Web 应用程序
- 审核对存储帐户的不受限的网络访问

A.13.2.1 信息传输策略和过程

该蓝图通过分配两个 Azure Policy 定义用于审核与存储帐户和 Redis 缓存建立的不安全连接，来帮助你确保与 Azure 服务之间安全传输信息。

- 审核确认仅启用了到 Redis 缓存的安全连接
- 审核确认指向存储帐户的传输的安全性

后续步骤

了解 ISO 27001 蓝图的控制映射后，请访问以下文章来了解体系结构以及如何部署此示例：

ISO 27001 蓝图 - 概述 ISO 27001 蓝图 - 部署步骤

有关蓝图和如何使用这些蓝图的更多文章：

- 了解蓝图生命周期。
- 了解如何使用静态和动态参数。
- 了解如何自定义蓝图排序顺序。
- 了解如何利用蓝图资源锁定。
- 了解如何更新现有分配。

部署 ISO 27001 蓝图示例

2019/9/5 • • Edit Online

若要部署 Azure 蓝图 ISO 27001 蓝图示例，必须执行以下步骤：

- 基于示例创建新的蓝图
- 将示例副本标记为“已发布”
- 将蓝图副本分配到现有的订阅

如果没有 Azure 订阅，请在开始之前创建一个免费帐户。

基于示例创建蓝图

首先，通过使用示例作为起点在环境中创建新的蓝图，来实现蓝图示例。

1. 选择“所有服务”，然后在左窗格中搜索并选择“策略”。在“策略”页上选择“蓝图”。
2. 在左侧的“开始”页中，选择“创建蓝图”下的“创建”按钮。
3. 在“其他示例”下找到“ISO 27001”蓝图示例，然后选择“使用此示例”。
4. 输入该蓝图示例的“基本信息”：
   - **蓝图名称**：提供 ISO 27001 蓝图示例副本的名称。
   - **定义位置**：使用省略号并选择要将示例副本保存到的管理组。
5. 选择页面顶部的“项目”选项卡，或页面底部的“下一步: 项目”。
6. 查看构成蓝图示例的项目列表。许多项目包含稍后我们将要定义的参数。查看完蓝图示例后，选择“保存草稿”。

发布示例副本

现已在环境中创建蓝图示例的副本。该副本在创建后处于“草稿”模式，必须先将其发布，然后才能分配和部署它。可根据环境和需求自定义蓝图示例的副本，但这种修改可能会将该副本移出 ISO 27001 标准。

1. 选择“所有服务”，然后在左窗格中搜索并选择“策略”。在“策略”页上选择“蓝图”。
2. 在左侧选择“蓝图定义”页。使用筛选器找到蓝图示例的副本，然后选择它。
3. 选择页面顶部的“发布蓝图”。在右侧的新窗格中，提供蓝图示例副本的**版本**。以后做出修改时，此属性非常有用。提供**更改注释**，例如，“基于 ISO 27001 蓝图示例发布的第一个版本”。然后选择页面底部的“发布”。

分配示例副本

成功发布蓝图示例的副本后，可将它分配到它所在的管理组中的某个订阅。在此步骤中，需提供参数来使蓝图示例副本的每个部署保持唯一。

1. 选择“所有服务”，然后在左窗格中搜索并选择“策略”。在“策略”页上选择“蓝图”。
2. 在左侧选择“蓝图定义”页。使用筛选器找到蓝图示例的副本，然后选择它。
3. 选择蓝图定义页面顶部的“分配蓝图”。
4. 提供蓝图分配的参数值：

- 基础
  - **订阅**：在蓝图示例副本所保存到的管理组中选择一个或多个订阅。如果选择多个订阅，将使用输入的参数为每个订阅创建一个分配。
  - **分配名称**：系统会根据蓝图的名称预先填充该名称。请根据需要更改该名称，或保留原样。
  - **位置**：选择要在其中创建托管标识的区域。Azure 蓝图使用此托管标识在分配的蓝图中部署所有项目。若要了解详细信息，请参阅 Azure 资源的托管标识。
  - **蓝图定义版本**：选择蓝图示例副本的已发布版本。
- 锁分配

  选择环境的蓝图锁定设置。有关更多信息，请参阅蓝图资源锁定。

- 托管标识

  保留默认的系统分配的托管标识选项。

- 蓝图参数

  蓝图定义中的许多项目使用本部分定义的参数来提供一致性。

  - **资源和资源组的允许位置**：该值指示资源组和资源的允许位置。
- 项目参数

  在本部分定义的参数将应用到定义了这些参数的项目。这些参数属于动态参数，因为它们是在分配蓝图期间定义的。有关完整列表或项目参数及其说明，请参阅项目参数表 。

5. 输入所有参数后，选择页面底部的“分配”。随后将创建蓝图分配，并开始部署项目。部署过程大约需要一小时。若要检查部署状态，请打开蓝图分配。

> **WARNING**
> Azure 蓝图服务和内置蓝图示例是**免费的**。Azure 资源按产品定价 。使用定价计算器 可以估算运行此蓝图示例部署的资源所需的成本。

项目参数表

下表提供了蓝图项目参数的列表：

项目名称	项目类型	参数名称	说明
[预览]：为 Linux VM 规模集 (VMSS)部署 Log Analytics 代理	策略分配	Linux VM 规模集 (VMSS) 的 Log Analytics 工作区	如果此工作区超出分配范围，则必须手动将“Log Analytics 参与者”权限（或类似权限）授予策略分配的主体 ID。
[预览]：为 Linux VM 规模集 (VMSS)部署 Log Analytics 代理	策略分配	可选：支持将 Linux OS 添加到范围的 VM 映像列表	可以使用空数组来表示没有可选参数：[]
[预览]：为 Linux VM 部署 Log Analytics 代理	策略分配	Linux VM 的 Log Analytics 工作区	如果此工作区超出分配范围，则必须手动将“Log Analytics 参与者”权限（或类似权限）授予策略分配的主体 ID。

项目名称	项目类型	参数名称	说明
[预览]: 为 Linux VM 部署 Log Analytics 代理	策略分配	可选: 支持将 Linux OS 添加到范围的 VM 映像列表	可以使用空数组来表示没有可选参数: []
[预览]: 为 Windows VM 规模集(VMSS)部署 Log Analytics 代理	策略分配	Windows VM 规模集 (VMSS) 的 Log Analytics 工作区	如果此工作区超出分配范围，则必须手动将“Log Analytics 参与者”权限(或类似权限)授予策略分配的主体 ID。
[预览]: 为 Windows VM 规模集(VMSS)部署 Log Analytics 代理	策略分配	可选: 支持将 Windows OS 添加到范围的 VM 映像列表	可以使用空数组来表示没有可选参数: []
[预览]: 为 Windows VM 部署 Log Analytics 代理	策略分配	Windows VM 的 Log Analytics 工作区	如果此工作区超出分配范围，则必须手动将“Log Analytics 参与者”权限(或类似权限)授予策略分配的主体 ID。
[预览]: 为 Windows VM 部署 Log Analytics 代理	策略分配	可选: 支持将 Windows OS 添加到范围的 VM 映像列表	可以使用空数组来表示没有可选参数: []
允许的存储帐户 SKU	策略分配	允许的存储 SKU 列表	可为存储帐户指定的 SKU 列表。
允许的虚拟机 SKU	策略分配	允许的虚拟机 SKU 列表	可为虚拟机指定的 SKU 列表。
ISO 27001 的蓝图计划	策略分配	应启用诊断日志的资源类型列表	用于审核是否未启用诊断日志设置的资源类型列表。Azure Monitor 诊断日志架构中提供了可接受的值。

后续步骤

了解 ISO 27001 蓝图示例的部署步骤后，请访问以下文章来了解体系结构和控制映射:

ISO 27001 蓝图 - 概述 ISO 27001 蓝图 - 控制映射

有关蓝图和如何使用这些蓝图的更多文章:

- 了解蓝图生命周期。
- 了解如何使用静态和动态参数。
- 了解如何自定义蓝图排序顺序。
- 了解如何利用蓝图资源锁定。
- 了解如何更新现有分配。

ISO 27001 共享服务蓝图示例的概述

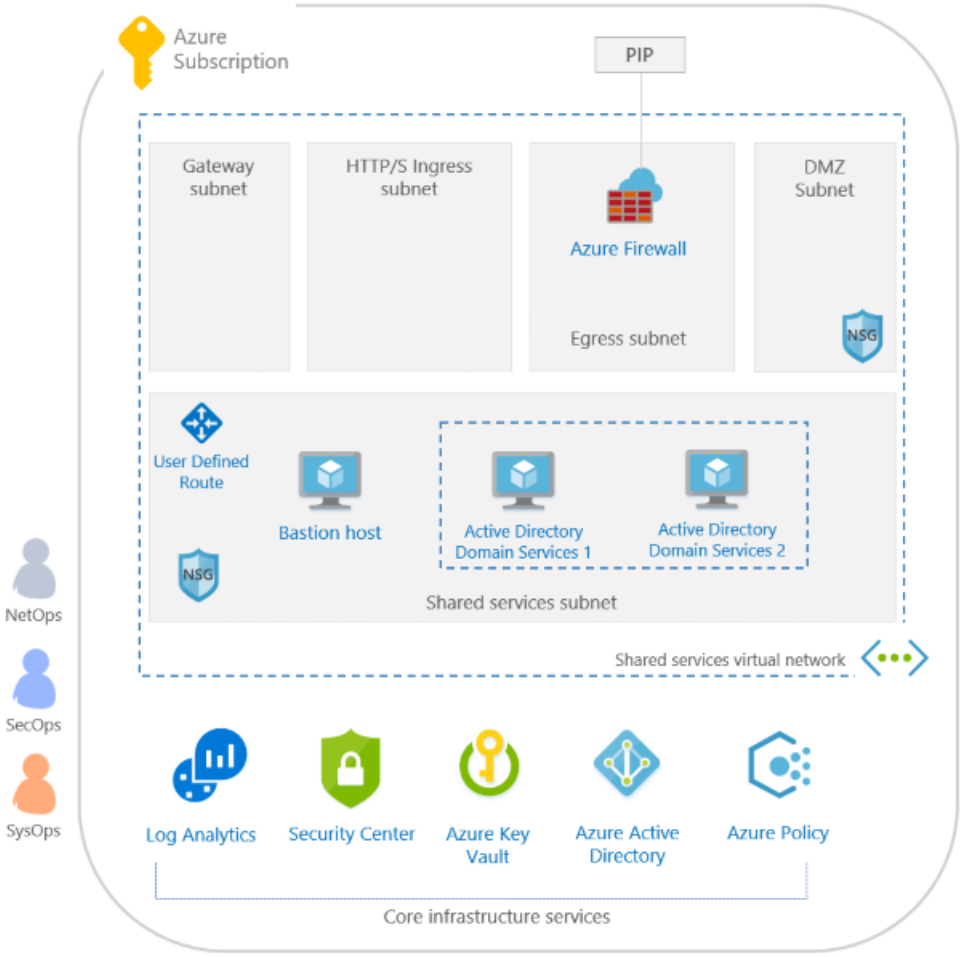
2019/9/4 • • Edit Online

ISO 27001 共享服务蓝图示例提供了一组符合标准的基础结构模式和策略防护机制，以便帮助通过 ISO 27001 认证。此蓝图帮助客户部署基于云的体系结构，以便为有认证或符合性要求的方案提供解决方案。

ISO 27001 应用服务环境/SQL 数据库工作负荷蓝图示例扩展了此示例。

体系结构

ISO 27001 共享服务蓝图示例在 Azure 中部署一个基础结构，该基础结构可供组织用来基于虚拟数据中心 (VDC) 方法托管多个工作负荷。VDC 是一套行之有效的参考体系结构、自动化工具和参与模型，由 Microsoft 用于其最大的企业客户。共享服务蓝图示例基于下面所示的完全原生 Azure VDC 环境。



此环境包括多项 Azure 服务，这些服务用于根据 ISO 27001 标准提供安全的、全面受监视的、面向企业的共享服务基础结构。此环境包括：

- 基于角色的访问控制 (RBAC) 角色，用于从控制平面角度分离职责。三个角色是在部署任何基础结构之前定义的：
  - NetOps 角色有权管理网络环境，包括防火墙设置、NSG 设置、路由和其他网络功能
  - SecOps 角色具有部署和管理 Azure 安全中心、定义 Azure 策略的必要权限，以及其他与安全相关的权限
  - SysOps 角色具有在订阅内定义 Azure 策略、为整个环境管理 Log Analytics 的必要权限，以及其他操作权限
- Log Analytics 作为第一个 Azure 服务进行部署，以便确保从开始安全部署起所有操作和服务都记录到一个

中心位置

- 一个虚拟网络，它支持用于连接回本地数据中心的子网、用于 Internet 连接的入口和出口堆叠、使用 NSG 和 ASG 进行完全微分段的共享服务子网，其中包含：
  - 一个用于管理目的的 Jumpbox 或堡垒主机，只能通过入口堆叠子网中部署的 Azure 防火墙访问
  - 两个运行 Active Directory 域服务 (ADDS) 和 DNS 的虚拟机，只能通过 Jumpbox 访问，可以配置为仅通过 VPN 或 ExpressRoute 连接来复制 AD（不按蓝图部署）
  - 使用 Azure 网络观察程序和标准 DDoS 保护
- 一个 Azure Key Vault 实例，用于托管对共享服务环境中部署的 VM 使用的机密

所有这些元素遵守 Azure 体系结构中心 - 参考体系结构中发布的行之有效的做法。

> **NOTE**
> ISO 27001 共享服务基础结构奠定了适用于工作负荷的基础体系结构的基础。你仍需要部署此基础体系结构后面的工作负荷。

有关详细信息，请参阅虚拟数据中心文档。

后续步骤

你已查看了 ISO 27001 共享服务蓝图示例的概述和体系结构。接下来，请访问以下文章，了解控制映射以及如何部署此示例：

ISO 27001 共享服务蓝图 - 控制映射 ISO 27001 共享服务蓝图 - 部署步骤

有关蓝图和如何使用这些蓝图的更多文章：

- 了解蓝图生命周期。
- 了解如何使用静态和动态参数。
- 了解如何自定义蓝图排序顺序。
- 了解如何利用蓝图资源锁定。
- 了解如何更新现有分配。

ISO 27001 共享服务蓝图示例的控制映射

2019/9/5 • • Edit Online

以下文章详细说明了 Azure 蓝图 ISO 27001 共享服务蓝图示例如何映射到 ISO 27001 控制措施。有关控制措施的详细信息，请参阅 ISO 27001。

以下映射适用于 **ISO 27001:2013** 控制措施。使用右侧的导航栏可直接跳转到特定的控制映射。许多的映射控制措施都是使用 Azure Policy 计划实施的。若要查看完整计划，请在 Azure 门户中打开“策略”，并选择“定义”页。然后，找到并选择“[预览] 审核 ISO 27001:2013 控制措施并部署特定 VM 扩展以支持审核要求”内置策略计划。

A.6.1.2 职责分离

仅分配一个 Azure 订阅所有者并不能实现管理冗余。相反，分配过多的 Azure 订阅所有者会增大违规的可能性，因为会有更多的所有者帐户可能会泄密。此蓝图可帮助你通过分配两个用于审核 Azure 订阅所有者数目的 Azure Policy 定义，来保持适当的 Azure 订阅所有者数目。管理订阅所有者权限有助于实现适当的职责分离。

- [预览]: 审核最小订阅所有者数
- [预览]: 审核最大订阅所有者数

A.8.2.1 信息分类

Azure 的 SQL 漏洞评估服务可以帮助你发现数据库中存储的敏感数据并提供用于对该数据进行分类的建议。此蓝图分配了一个 Azure Policy 定义来审核在 SQL 漏洞评估过程中查明的漏洞是否已更正。

- [预览]: 监视 Azure 安全中心的 SQL 漏洞评估结果

A.9.1.2 访问网络和网络服务

Azure 实施基于角色的访问控制 (RBAC) 来管理谁有权访问 Azure 资源。此蓝图可帮助你通过分配七个 Azure Policy 定义来控制对 Azure 资源的访问。这些策略将审核可能允许更高资源访问权限的资源类型和配置的使用。了解违反这些策略的资源有助于采取纠正措施来确保仅限已授权的用户访问 Azure 资源。

- [预览]: 部署 VM 扩展以审核没有密码的 Linux VM 帐户
- [预览]: 部署 VM 扩展以审核允许从没有密码的帐户进行远程连接的 Linux VM
- [预览]: 审核没有密码的 Linux VM 帐户
- [预览]: 审核允许从没有密码的帐户进行远程连接的 Linux VM
- 审核经典存储帐户的使用
- 审核经典虚拟机的使用
- 审核不使用托管磁盘的 VM

A.9.2.3 管理特权访问权限

此蓝图通过分配四个 Azure Policy 定义用于审核拥有所有者和/或写入权限的外部帐户，以及拥有所有者和/或写入权限、但未启用多重身份验证的帐户，来帮助你限制和控制特权访问权限。Azure 实施基于角色的访问控制 (RBAC) 来管理谁有权访问 Azure 资源。此蓝图还分配了三个 Azure Policy 定义，用于审核 Azure Active Directory 身份验证在 SQL 服务器和 Service Fabric 中的使用。使用 Azure Active Directory 身份验证可以简化权限管理，以及集中化数据库用户和其他 Microsoft 服务的标识管理。此蓝图还分配一个 Azure Policy 定义用于审核自定义 RBAC 规则的使用。了解实施自定义 RBAC 规则的位置有助于验证需求以及实施是否适当，因为自定义 RBAC 规则容易出错。

- [预览]: 审核具有所有者权限但未启用 MFA 的订阅帐户

- [预览]: 审核具有写入权限但未启用 MFA 的订阅帐户
- [预览]: 审核具有所有者权限的外部订阅帐户
- [预览]: 审核具有写入权限的外部订阅帐户
- 审核确认已为 SQL Server 预配了 Azure Active Directory 管理员
- 审核确认已在 Service Fabric 中使用 Azure Active Directory，用于实施客户端身份验证
- 审核自定义 RBAC 规则的使用

A.9.2.4 管理用户的机密身份验证信息

此蓝图分配三个 Azure Policy 定义用于审核未启用多重身份验证的帐户。即使某个身份验证信息片段已泄密，多重身份验证也有助于保护帐户的安全。通过监视未启用多重身份验证的帐户，可以识别出更有可能会泄密的帐户。此蓝图还将分配两个 Azure Policy 定义用于审核 Linux VM 密码文件权限，并在这些权限设置不当时发出警报。使用这种设置可以采取纠正措施，以确保验证器不会泄密。

- [预览]: 审核具有所有者权限但未启用 MFA 的订阅帐户
- [预览]: 审核具有读取权限但未启用 MFA 的订阅帐户
- [预览]: 审核具有写入权限但未启用 MFA 的订阅帐户
- [预览]: 部署 VM 扩展以审核 Linux VM 密码文件权限
- [预览]: 审核 Linux VM /etc/密码文件权限是否设置为 0644

A.9.2.5 评审用户访问权限

Azure 实施了基于角色的访问控制 (RBAC) 来帮助你管理谁有权访问 Azure 中的资源。使用 Azure 门户可以评审有权访问 Azure 资源的用户及其权限。此蓝图分配四个 Azure Policy 定义用于审核应该优先评审的帐户，包括已淘汰的帐户，以及具有提升权限的外部帐户。

- [预览]: 审核已弃用的订阅帐户
- [预览]: 审核具有所有者权限但已被弃用的订阅帐户
- [预览]: 审核具有所有者权限的外部订阅帐户
- [预览]: 审核具有写入权限的外部订阅帐户

A.9.2.6 删除或调整访问权限

Azure 实施了基于角色的访问控制 (RBAC) 来帮助你管理谁有权访问 Azure 中的资源。使用 Azure Active Directory 和 RBAC 可以更新用户角色，以反映组织变化。如果需要，可以阻止帐户登录(或将其删除)，这会立即删除其 Azure 资源访问权限。此蓝图分配两个 Azure Policy 定义用于审核应该考虑删除的已淘汰帐户。

- [预览]: 审核已弃用的订阅帐户
- [预览]: 审核具有所有者权限但已被弃用的订阅帐户

A.9.4.2 安全登录过程

此蓝图分配了三个 Azure Policy 定义，以用于审核未启用多重身份验证的帐户。Azure 多重身份验证通过要求使用另一种形式的身份验证提供额外的安全性，从而提供增强式身份验证。通过监视未启用多重身份验证的帐户，可以识别出更有可能会泄密的帐户。

- [预览]: 审核具有所有者权限但未启用 MFA 的订阅帐户
- [预览]: 审核具有读取权限但未启用 MFA 的订阅帐户
- [预览]: 审核具有写入权限但未启用 MFA 的订阅帐户

A.9.4.3 密码管理系统

此蓝图通过分配 10 个 Azure Policy 定义用于审核不强制实施最低强度和其他密码要求的 Windows VM，来帮助你

强制实施强密码。识别违反密码强度策略的 VM 有助于采取纠正措施，以确保所有 VM 用户帐户的密码符合策略。

- [预览]: 部署 VM 扩展以审核 Windows VM 是否强制实施密码复杂性要求
- [预览]: 部署 VM 扩展以审核 Windows VM 最长密码期限是否为 70 天
- [预览]: 部署 VM 扩展以审核 Windows VM 最短密码期限是否为 1 天
- [预览]: 部署 VM 扩展以审核 Windows VM 密码必须至少为 14 个字符
- [预览]: 部署 VM 扩展以审核 Windows VM 不应允许之前的 24 个密码
- [预览]: 审核 Windows VM 是否强制实施密码复杂性要求
- [预览]: 审核 Windows VM 最长密码期限是否为 70 天
- [预览]: 审核 Windows VM 最短密码期限是否为 1 天
- [预览]: 审核 Windows VM 密码必须至少为 14 个字符
- [预览]: 审核 Windows VM 不应允许之前的 24 个密码

A.10.1.1 有关使用加密控制措施的策略

此蓝图通过分配 13 个 Azure Policy 定义用于强制实施特定的加密控制措施并审核弱加密设置的使用，来帮助你针对加密控制措施的使用强制实施自己的策略。了解 Azure 资源中的哪些位置采用欠佳的加密配置有助于采取纠正措施，以确保根据信息安全策略配置资源。具体而言，此蓝图分配的策略要求对 Blob 存储帐户和 Data Lake Storage 帐户加密；要求对 SQL 数据库实施透明数据加密；审核存储帐户、SQL 数据库、虚拟机磁盘和自动化帐户变量是否缺少加密；审核是否与存储帐户、函数应用、Web 应用、API 应用和 Redis 缓存建立了不安全的连接；审核虚拟机弱密码加密；审核未加密的 Service Fabric 通信。

- [预览]: 审核函数应用的仅 HTTPS 访问权限
- [预览]: 审核 Web 应用的仅 HTTPS 访问权限
- [预览]: 审核 API 应用的仅 HTTPS 访问权限
- [预览]: 审核存储帐户是否缺少 blob 加密
- [预览]: 部署 VM 扩展以审核 Windows VM 不应使用可逆加密存储密码
- [预览]: 审核 Windows VM 不应使用可逆加密存储密码
- [预览]: 监视 Azure 安全中心内未加密的 VM 磁盘
- 审核确认已启用自动化帐户变量加密功能
- 审核确认仅启用了到 Redis 缓存的安全连接
- 审核确认指向存储帐户的传输的安全性
- 审核确认 Service Fabric 中的 ClusterProtectionLevel 属性设置为 EncryptAndSign
- 审核透明数据加密状态
- 应在 SQL 数据库上启用透明数据加密

A.12.4.1 事件日志记录

此蓝图通过分配七个 Azure Policy 定义用于审核 Azure 资源的日志设置，来帮助你确保记录系统事件。诊断日志针对 Azure 资源中执行的操作提供见解。

- [预览]: 审核依赖项代理部署 - VM 映像 (OS) 未列出
- [预览]: 审核 VMSS 中的依赖项代理部署 - VM 映像 (OS) 未列出
- [预览]: 审核 Log Analytics 代理部署 - VM 映像 (OS) 未列出
- [预览]: 审核 VMSS 中的 Log Analytics 代理部署 - VM 映像 (OS) 未列出
- 审核诊断设置
- 审核 SQL 服务器级别审核设置
- 应在 SQL Server 的高级数据安全设置上启用审核

A.12.4.3 管理员和操作员日志

此蓝图分配了七个 Azure Policy 定义，以用于审核 Azure 资源的日志设置，从而帮助你确保系统事件会被记录。诊断日志针对 Azure 资源中执行的操作提供见解。

- [预览]: 审核依赖项代理部署 - VM 映像 (OS) 未列出
- [预览]: 审核 VMSS 中的依赖项代理部署 - VM 映像 (OS) 未列出
- [预览]: 审核 Log Analytics 代理部署 - VM 映像 (OS) 未列出
- [预览]: 审核 VMSS 中的 Log Analytics 代理部署 - VM 映像 (OS) 未列出
- 审核诊断设置
- 审核 SQL 服务器级别审核设置
- 应在 SQL Server 的高级数据安全设置上启用审核

A.12.4.4 时钟同步

此蓝图分配了七个 Azure Policy 定义，以用于审核 Azure 资源的日志设置，从而帮助你确保系统事件会被记录。Azure 日志依赖于同步的内部时钟创建各个资源中事件的时间相关记录。

- [预览]: 审核依赖项代理部署 - VM 映像 (OS) 未列出
- [预览]: 审核 VMSS 中的依赖项代理部署 - VM 映像 (OS) 未列出
- [预览]: 审核 Log Analytics 代理部署 - VM 映像 (OS) 未列出
- [预览]: 审核 VMSS 中的 Log Analytics 代理部署 - VM 映像 (OS) 未列出
- 审核诊断设置
- 审核 SQL 服务器级别审核设置
- 应在 SQL Server 的高级数据安全设置上启用审核

A.12.5.1 在可操作的系统上安装软件

自适应应用程序控制是 Azure 安全中心内的一个解决方案，可帮助你控制哪些应用程序可在 Azure 中的 VM 上运行。此蓝图分配一个 Azure Policy 定义用于监视对允许的应用程序集的更改。此功能帮助你控制软件和应用程序在 Azure VM 上的安装。

- [预览]: 监视 Azure 安全中心内列入允许列表的可能的应用

A.12.6.1 管理技术漏洞

此蓝图分配了五个 Azure Policy 定义，以用于在 Azure 安全中心内监视缺少的系统更新、操作系统漏洞、SQL 漏洞和虚拟机漏洞，来帮助你管理信息系统漏洞。Azure 安全中心提供报告功能，使你能够实时洞察已部署的 Azure 资源的安全状态。

- [预览]: 监视 Azure 安全中心 Endpoint Protection 的缺失情况
- [预览]: 监视 Azure 安全中心内系统更新的缺失情况
- [预览]: 监视 Azure 安全中心的 OS 漏洞
- [预览]: 监视 Azure 安全中心的 SQL 漏洞评估结果
- [预览]: 监视 Azure 安全中心的 VM 漏洞

A.12.6.2 软件安装的限制

自适应应用程序控制是 Azure 安全中心内的一个解决方案，可帮助你控制哪些应用程序可在 Azure 中的 VM 上运行。此蓝图分配一个 Azure Policy 定义用于监视对允许的应用程序集的更改。软件安装限制有助于减少出现软件漏洞的可能性。

- [预览]: 监视 Azure 安全中心内列入允许列表的可能的应用

A.13.1.1 网络控制措施

此蓝图通过分配一个 Azure Policy 定义用于监视具有宽松规则的网络安全组，来帮助你管理和控制网络。过于宽松的规则可能会允许意外的网络访问，应该对其进行评审。此蓝图还分配了三个 Azure Policy 定义，以用于监视不受保护的终结点、应用程序和存储帐户。不受防火墙保护的终结点和应用程序，以及具有无限制访问权限的存储帐户，可能会允许意外访问信息系统中包含的信息。

- [预览]: 监视 Azure 安全中心内规则较宽松的网络访问
- [预览]: 监视 Azure 安全中心内未受保护的网络终结点
- [预览]: 监视 Azure 安全中心内未受保护的 Web 应用程序
- 审核对存储帐户的不受限的网络访问

A.13.2.1 信息传输策略和过程

该蓝图通过分配两个 Azure Policy 定义用于审核与存储帐户和 Redis 缓存建立的不安全连接，来帮助你确保与 Azure 服务之间安全传输信息。

- 审核确认仅启用了到 Redis 缓存的安全连接
- 审核确认指向存储帐户的传输的安全性

后续步骤

了解 ISO 27001 共享服务蓝图的控制映射后，请访问以下文章来了解体系结构以及如何部署此示例：

ISO 27001 共享服务蓝图 - 概述 ISO 27001 共享服务蓝图 - 部署步骤

有关蓝图和如何使用这些蓝图的更多文章：

- 了解蓝图生命周期。
- 了解如何使用静态和动态参数。
- 了解如何自定义蓝图排序顺序。
- 了解如何利用蓝图资源锁定。
- 了解如何更新现有分配。

部署 ISO 27001 共享服务蓝图示例

2019/9/5 • • Edit Online

若要部署 Azure 蓝图 ISO 27001 共享服务蓝图示例，必须执行以下步骤：

- 基于示例创建新的蓝图
- 将示例副本标记为“已发布”
- 将蓝图副本分配到现有的订阅

如果没有 Azure 订阅，请在开始之前创建一个免费帐户。

基于示例创建蓝图

首先，通过使用示例作为起点在环境中创建新的蓝图，来实现蓝图示例。

1. 选择“所有服务”，然后在左窗格中搜索并选择“策略”。在“策略”页上选择“蓝图”。
2. 在左侧的“开始”页中，选择“创建蓝图”下的“创建”按钮。
3. 在“其他示例”下找到“ISO 27001: 共享服务”蓝图示例，然后选择“使用此示例”。
4. 输入该蓝图示例的“基本信息”：
   - **蓝图名称**：提供 ISO 27001 共享服务蓝图示例副本的名称。
   - **定义位置**：使用省略号并选择要将示例副本保存到的管理组。
5. 选择页面顶部的“项目”选项卡，或页面底部的“下一步: 项目”。
6. 查看构成蓝图示例的项目列表。许多项目包含稍后我们将要定义的参数。查看完蓝图示例后，选择“保存草稿”。

发布示例副本

现已在环境中创建蓝图示例的副本。该副本在创建后处于“草稿”模式，必须先将其发布，然后才能分配和部署它。可根据环境和需求自定义蓝图示例的副本，但这种修改可能会将该副本移出 ISO 27001 标准。

1. 选择“所有服务”，然后在左窗格中搜索并选择“策略”。在“策略”页上选择“蓝图”。
2. 在左侧选择“蓝图定义”页。使用筛选器找到蓝图示例的副本，然后选择它。
3. 选择页面顶部的“发布蓝图”。在右侧的新窗格中，提供蓝图示例副本的**版本**。以后做出修改时，此属性非常有用。提供**更改注释**，例如，“基于 ISO 27001 蓝图示例发布的第一个版本”。然后选择页面底部的“发布”。

分配示例副本

成功发布蓝图示例的副本后，可将它分配到它所在的管理组中的某个订阅。在此步骤中，需提供参数来使蓝图示例副本的每个部署保持唯一。

1. 选择“所有服务”，然后在左窗格中搜索并选择“策略”。在“策略”页上选择“蓝图”。
2. 在左侧选择“蓝图定义”页。使用筛选器找到蓝图示例的副本，然后选择它。
3. 选择蓝图定义页面顶部的“分配蓝图”。
4. 提供蓝图分配的参数值：

- 基础
  - **订阅**：在蓝图示例副本所保存到的管理组中选择一个或多个订阅。如果选择多个订阅，将使用输入的参数为每个订阅创建一个分配。
  - **分配名称**：系统会根据蓝图的名称预先填充该名称。请根据需要更改该名称，或保留原样。
  - **位置**：选择要在其中创建托管标识的区域。Azure 蓝图使用此托管标识在分配的蓝图中部署所有项目。若要了解详细信息，请参阅 Azure 资源的托管标识。
  - **蓝图定义版本**：选择蓝图示例副本的已发布版本。
- 锁分配

  选择环境的蓝图锁定设置。有关更多信息，请参阅蓝图资源锁定。

- 托管标识

  保留默认的系统分配的托管标识选项。

- 蓝图参数

  蓝图定义中的许多项目使用本部分定义的参数来提供一致性。

  - **组织名称**：输入组织的短名称。此属性主要用于为资源命名。
  - **共享服务子网地址前缀**：提供用于将部署的资源联网到一起的 CIDR 表示法值。
  - **共享服务位置**：确定要将项目部署到的位置。并非所有服务都可在所有位置使用。部署此类服务的项目会针对该项目要部署到的位置提供一个参数选项。
  - **允许的位置(策略:ISO 27001 的蓝图计划)**：该值指示资源组和资源的允许位置。
  - **VM 代理的 Log Analytics 工作区(策略:ISO 27001 的蓝图计划)**：指定工作区的资源 ID。此参数使用 `concat` 函数来构造资源 ID。
- 项目参数

  在本部分定义的参数将应用到定义了这些参数的项目。这些参数属于动态参数，因为它们是在分配蓝图期间定义的。有关完整列表或项目参数及其说明，请参阅项目参数表 。

5. 输入所有参数后，选择页面底部的“分配”。随后将创建蓝图分配，并开始部署项目。部署过程大约需要一小时。若要检查部署状态，请打开蓝图分配。

> **WARNING**
> Azure 蓝图服务和内置蓝图示例是**免费的**。Azure 资源按产品定价 。使用定价计算器 可以估算运行此蓝图示例部署的资源所需的成本。

项目参数表

下表提供了蓝图项目参数的列表：

项目名称	项目类型	参数名称	说明
[预览]：为 Linux VM 规模集(VMSS)部署 Log Analytics 代理	策略分配	可选：支持将 Linux OS 添加到范围的 VM 映像列表	(可选)默认值为 *["none"]* 。
[预览]：为 Linux VM 部署 Log Analytics 代理	策略分配	可选：支持将 Linux OS 添加到范围的 VM 映像列表	(可选)默认值为 *["none"]* 。

项目名称	项目类型	参数名称	说明
[预览]: 为 Windows VM 规模集(VMSS)部署 Log Analytics 代理	策略分配	可选: 支持将 Windows OS 添加到范围的 VM 映像列表	(可选)默认值为 *["none"]* 。
[预览]: 为 Windows VM 部署 Log Analytics 代理	策略分配	可选: 支持将 Windows OS 添加到范围的 VM 映像列表	(可选)默认值为 *["none"]* 。
允许的资源类型	策略分配	允许的资源类型	允许部署的资源类型列表。此列表包括共享服务中部署的所有资源类型。
允许的存储帐户 SKU	策略分配	允许的存储 SKU	允许的诊断日志存储帐户 SKU 列表。默认值为 *["Standard_LRS"]* 。
允许的虚拟机 SKU	策略分配	允许部署的虚拟机 SKU 列表。默认值为 *["Standard_DS1_v2", "Standard_DS2_v2"]* 。	
ISO 27001 的蓝图计划	策略分配	用于审核诊断日志的资源类型	用于审核是否未启用诊断日志设置的资源类型列表。Azure Monitor 诊断日志架构中提供了可接受的值。
Log Analytics 资源组	Resource group	Name	**已锁定** - 将组织**名称**与 `-sharedsvsc-log-rg` 相连接可使资源组名称保持唯一。
Log Analytics 资源组	Resource group	位置	**已锁定** - 使用蓝图参数。
Log Analytics 模板	资源管理器模板	服务层	设置 Log Analytics 工作区的层。默认值为 *PerNode*。
Log Analytics 模板	资源管理器模板	日志保留期(以天为单位)	日志保留期(以天为单位)。默认值为 *365*。
Log Analytics 模板	资源管理器模板	位置	用于创建 Log Analytics 工作区的区域。默认值为"美国西部 2"。
网络资源组	Resource group	Name	**已锁定** - 将组织**名称**与 `-sharedsvcs-net-rg` 相连接可使资源组名称保持唯一。
网络资源组	Resource group	位置	**已锁定** - 使用蓝图参数。
Azure 防火墙模板	资源管理器模板	Azure 防火墙专用 IP	配置 Azure 防火墙的专用 IP。此值也用作共享服务子网中的默认路由表。应是"Azure 防火墙子网地址前缀"中定义的 CIDR 表示法的一部分。默认值为 *10.0.4.4*。

项目名称	项目类型	参数名称	说明
Azure 防火墙模板	资源管理器模板	日志保留期(以天为单位)	日志保留期(以天为单位)。默认值为 *365*。
网络安全组模板	资源管理器模板	日志保留期(以天为单位)	日志保留期(以天为单位)。默认值为 *365*。
虚拟网络和路由表模板	资源管理器模板	虚拟网络地址前缀	虚拟网络的 CIDR 表示法。默认值为 *10.0.0.0/16*。
虚拟网络和路由表模板	资源管理器模板	启用虚拟网络 DDoS 防护	为虚拟网络配置 DDoS 防护。默认值为 *true*。
虚拟网络和路由表模板	资源管理器模板	共享服务子网地址前缀	共享服务子网的 CIDR 表示法。默认值为 *10.0.0.0/24*。
虚拟网络和路由表模板	资源管理器模板	外围网络子网地址前缀	外围网络子网的 CIDR 表示法。默认值为 *10.0.1.0/24*。
虚拟网络和路由表模板	资源管理器模板	应用程序网关子网地址前缀	应用程序网关子网的 CIDR 表示法。默认值为 *10.0.2.0/24*。
虚拟网络和路由表模板	资源管理器模板	虚拟网络网关子网地址前缀	虚拟网络网关子网的 CIDR 表示法。默认值为 *10.0.3.0/24*。
虚拟网络和路由表模板	资源管理器模板	Azure 防火墙子网地址前缀	Azure 防火墙子网的 CIDR 表示法。应包含“Azure 防火墙专用 IP”参数。
密钥保管库资源组	Resource group	Name	**已锁定** - 将组织**名称**与 `-sharedsvcs-kv-rg` 相连接可使资源组名称保持唯一。
密钥保管库资源组	Resource group	位置	**已锁定** - 使用蓝图参数。
Key Vault 模板	资源管理器模板	Jumpbox 管理员用户名	Jumpbox 的用户名。必须与 **Jumpbox 模板**中的相同属性值相匹配。默认值为 *jb-admin-user*。
Key Vault 模板	资源管理器模板	Jumpbox 管理员 SSH 密钥或密码	Jumpbox 上的帐户的密钥或密码。必须与 **Jumpbox 模板**中的相同属性值相匹配。无默认值，且不能留空。
Key Vault 模板	资源管理器模板	域管理员用户名	用于访问 Active Directory VM 以及将其他 VM 加入域的用户名。必须与 **Active Directory 域服务模板**中的“域管理员用户”属性值相匹配。默认值为 *domain-admin-user*。

项目名称	项目类型	参数名称	说明
Key Vault 模板	资源管理器模板	域管理员密码	域管理员用户的密码。无默认值，且不能留空。
Key Vault 模板	资源管理器模板	AAD 对象 ID	需要访问 Key Vault 实例的帐户的 AAD 对象标识符。无默认值，且不能留空。若要在 Azure 门户中查找此值，请在“服务”下搜索并选择“用户”。使用“名称”框筛选帐户名，并选择该帐户。在“用户配置文件”页上，选择“对象 ID”旁边的“单击以复制”图标。
Key Vault 模板	资源管理器模板	日志保留期(以天为单位)	日志保留期（以天为单位）。默认值为 *365*。
Key Vault 模板	资源管理器模板	Key Vault SKU	指定创建的 Key Vault 的 SKU。默认值为“高级”。
Jumpbox 资源组	Resource group	Name	已锁定 - 将组织名称与 `-sharedsvcs-jb-rg` 相连接可使资源组名称保持唯一。
Jumpbox 资源组	Resource group	位置	已锁定 - 使用蓝图参数。
Jumpbox 模板	资源管理器模板	Jumpbox 管理员用户名	用于访问 Jumpbox VM 的用户名。必须与 **Key Vault 模板**中的相同属性值相匹配。默认值为 *jb-admin-user*。
Jumpbox 模板	资源管理器模板	Jumpbox 管理员密码(Key Vault 资源 ID)	Key Vault 的资源 ID。请使用 "/subscriptions/{subscriptionId}/resourceGroups/{orgName}-sharedsvcs-kv-rg/providers/Microsoft.KeyVault/vaults/{orgName}-sharedsvcs-kv"，并将 `{subscriptionId}` 替换为你的订阅 ID，将 `{orgName}` 替换为“组织名称”蓝图参数。
Jumpbox 模板	资源管理器模板	Jumpbox 管理员密码(Key Vault 机密名称)	Jumpbox 管理员的用户名。必须与 **Key Vault 模板**中的“Jumpbox 管理员用户名”属性值相匹配。
Jumpbox 模板	资源管理器模板	Jumpbox 操作系统	确定 Jumpbox VM 的操作系统。默认值为 *Windows*。
Active Directory 域服务资源组	Resource group	Name	已锁定 - 将组织名称与 `-sharedsvcs-adds-rg` 相连接可使资源组名称保持唯一。

项目名称	项目类型	参数名称	说明
Active Directory 域服务资源组	Resource group	位置	**已锁定** - 使用蓝图参数。
Active Directory 域服务模板	资源管理器模板	域管理员用户名	ADDS Jumpbox 的用户名。必须与 **Key Vault 模板**中的相同属性值相匹配。默认值为 *adds-admin-user*。
Active Directory 域服务模板	资源管理器模板	域管理员密码(Key Vault 资源 ID)	Key Vault 的资源 ID。请使用 "/subscriptions/{subscriptionId}/resourceGroups/{orgName}-sharedsvcs-kv-rg/providers/Microsoft.KeyVault/vaults/{orgName}-sharedsvcs-kv"，并将 `{subscriptionId}` 替换为你的订阅 ID，将 `{orgName}` 替换为"组织名称"蓝图参数。
Active Directory 域服务模板	资源管理器模板	域管理员密码(Key Vault 机密名称)	域管理员的用户名。必须与 **Key Vault 模板**中的"域管理员用户名"属性值相匹配。
Active Directory 域服务模板	资源管理器模板	域名	示例创建的 Active Directory 的名称。默认值为 *contoso.com*。
Active Directory 域服务模板	资源管理器模板	域管理员用户	用于 AD 管理员帐户以及将设备加入 AD 域的用户名。必须与 **Key Vault 模板**中的"AD 管理员用户名"属性值相匹配。默认值为 *domain-admin-user*。
Active Directory 域服务模板	资源管理器模板	域管理员密码	设置用于存储密码的 Key Vault 详细信息。无默认值，且不能留空。

后续步骤

了解 ISO 27001 共享服务蓝图示例的部署步骤后，请访问以下文章来了解体系结构和控制映射：

ISO 27001 共享服务蓝图 - 概述 ISO 27001 共享服务蓝图 - 控制映射

有关蓝图和如何使用这些蓝图的更多文章：

- 了解蓝图生命周期。
- 了解如何使用静态和动态参数。
- 了解如何自定义蓝图排序顺序。
- 了解如何利用蓝图资源锁定。
- 了解如何更新现有分配。

ISO 27001 应用服务环境/SQL 数据库工作负荷蓝图示例的概述

2019/9/4 • • Edit Online

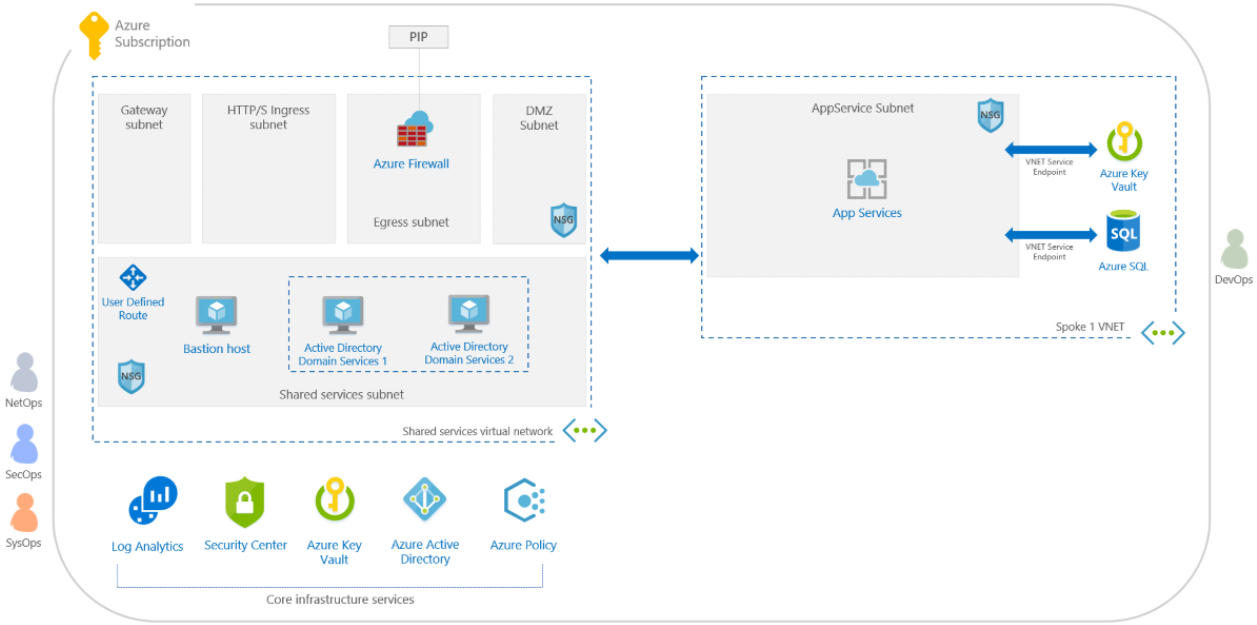
ISO 27001 应用服务环境/SQL 数据库工作负荷蓝图示例为 ISO 27001 共享服务蓝图示例提供了其他基础结构。此蓝图帮助客户部署基于云的体系结构，以便为有认证或符合性要求的方案提供解决方案。

有两个 ISO 27001 蓝图示例：此示例和 ISO 27001 共享服务蓝图示例。

> **IMPORTANT**
> 此示例依赖于按 ISO 27001 共享服务蓝图示例部署的基础结构。它必须先部署。

体系结构

ISO 27001 应用服务环境/SQL 数据库工作负荷蓝图示例部署一个基于平台即服务的 Web 环境。该环境可以用来托管多个遵循 ISO 27001 标准的 Web 应用程序、Web API 和 SQL 数据库实例。此蓝图示例依赖于 ISO 27001 共享服务蓝图示例。



此环境包括多项 Azure 服务，这些服务用于根据 ISO 27001 标准提供安全的、全面受监视的、面向企业的工作负荷基础结构。此环境包括：

- 名为 DevOps 的基于角色的访问控制 (RBAC) 角色，该角色有权在按蓝图示例部署的 Azure 应用服务环境中部署和管理资源
- Azure 策略，用于锁定哪些服务可以部署到该环境，以及拒绝创建任何公共 IP 地址 (PIP) 资源
- 一个虚拟网络，其中包含单个子网，与预先存在的共享服务环境对等互连，并且强制所有流量经由共享服务防火墙传递。该虚拟网络托管以下资源：
  - 一个 Azure 应用服务环境，可用于托管一个或多个 Web 应用程序、Web API 或函数
  - 一个使用 VNet 服务终结点的 Azure Key Vault 实例，用于存储由工作负荷环境中运行的应用程序使用的机密
  - 一个使用 VNet 服务终结点的 Azure SQL 数据库服务器实例，用于托管对工作负荷环境中运行的应用

程序使用的数据库

后续步骤

你已查看了 ISO 27001 应用服务环境/SQL 数据库工作负荷蓝图示例的概述和体系结构。接下来，请访问以下文章，了解控制映射以及如何部署此示例：

ISO 27001 应用服务环境/SQL 数据库工作负荷蓝图 - 控制映射 ISO 27001 应用服务环境/SQL 数据库工作负荷蓝图 - 部署步骤

有关蓝图和如何使用这些蓝图的更多文章：

- 了解蓝图生命周期。
- 了解如何使用静态和动态参数。
- 了解如何自定义蓝图排序顺序。
- 了解如何利用蓝图资源锁定。
- 了解如何更新现有分配。

ISO 27001 ASE/SQL 工作负荷蓝图示例的控制映射

2019/9/5 • • Edit Online

以下文章详细说明了 Azure 蓝图 ISO 27001 ASE/SQL 工作负荷蓝图示例如何映射到 ISO 27001 控制措施。有关控制措施的详细信息，请参阅 ISO 27001。

以下映射适用于 **ISO 27001:2013** 控制措施。使用右侧的导航栏可直接跳转到特定的控制映射。许多的映射控制措施都是使用 Azure Policy 计划实施的。若要查看完整计划，请在 Azure 门户中打开“策略”，并选择“定义”页。然后，找到并选择“[预览] 审核 ISO 27001:2013 控制措施并部署特定 VM 扩展以支持审核要求”内置策略计划。

A.6.1.2 职责分离

仅分配一个 Azure 订阅所有者并不能实现管理冗余。相反，分配过多的 Azure 订阅所有者会增大违规的可能性，因为会有更多的所有者帐户可能会泄密。此蓝图可帮助你通过分配两个用于审核 Azure 订阅所有者数目的 Azure Policy 定义，来保持适当的 Azure 订阅所有者数目。管理订阅所有者权限有助于实现适当的职责分离。

- [预览]: 审核最大订阅所有者数
- [预览]: 审核最大订阅所有者数

A.8.2.1 信息分类

Azure 的 SQL 漏洞评估服务可以帮助你发现数据库中存储的敏感数据并提供用于对该数据进行分类的建议。此蓝图分配了一个 Azure Policy 定义来审核在 SQL 漏洞评估过程中查明的漏洞是否已更正。

- [预览]: 监视 Azure 安全中心的 SQL 漏洞评估结果

A.9.1.2 访问网络和网络服务

Azure 实施基于角色的访问控制 (RBAC) 来管理谁有权访问 Azure 资源。此蓝图可帮助你通过分配七个 Azure Policy 定义来控制对 Azure 资源的访问。这些策略将审核可能允许更高资源访问权限的资源类型和配置的使用。了解违反这些策略的资源有助于采取纠正措施来确保仅限已授权的用户访问 Azure 资源。

- [预览]: 部署 VM 扩展以审核没有密码的 Linux VM 帐户
- [预览]: 部署 VM 扩展以审核允许从没有密码的帐户进行远程连接的 Linux VM
- [预览]: 审核没有密码的 Linux VM 帐户
- [预览]: 审核允许从没有密码的帐户进行远程连接的 Linux VM
- 审核经典存储帐户的使用
- 审核经典虚拟机的使用
- 审核不使用托管磁盘的 VM

A.9.2.3 管理特权访问权限

此蓝图通过分配四个 Azure Policy 定义用于审核拥有所有者和/或写入权限的外部帐户，以及拥有所有者和/或写入权限、但未启用多重身份验证的帐户，来帮助你限制和控制特权访问权限。Azure 实施基于角色的访问控制 (RBAC) 来管理谁有权访问 Azure 资源。此蓝图还分配了三个 Azure Policy 定义，用于审核 Azure Active Directory 身份验证在 SQL 服务器和 Service Fabric 中的使用。使用 Azure Active Directory 身份验证可以简化权限管理，以及集中化数据库用户和其他 Microsoft 服务的标识管理。此蓝图还分配一个 Azure Policy 定义用于审核自定义 RBAC 规则的使用。了解实施自定义 RBAC 规则的位置有助于验证需求以及实施是否适当，因为自定义 RBAC 规则容易出错。

- [预览]: 审核具有所有者权限但未启用 MFA 的订阅帐户

- [预览]: 审核具有写入权限但未启用 MFA 的订阅帐户
- [预览]: 审核具有所有者权限的外部订阅帐户
- [预览]: 审核具有写入权限的外部订阅帐户
- 审核确认已为 SQL Server 预配了 Azure Active Directory 管理员
- 审核确认已在 Service Fabric 中使用 Azure Active Directory，用于实施客户端身份验证
- 审核自定义 RBAC 规则的使用

A.9.2.4 管理用户的机密身份验证信息

此蓝图分配三个 Azure Policy 定义用于审核未启用多重身份验证的帐户。即使某个身份验证信息片段已泄密，多重身份验证也有助于保护帐户的安全。通过监视未启用多重身份验证的帐户，可以识别出更有可能会泄密的帐户。此蓝图还将分配两个 Azure Policy 定义用于审核 Linux VM 密码文件权限，并在这些权限设置不当时发出警报。使用这种设置可以采取纠正措施，以确保验证器不会泄密。

- [预览]: 审核具有所有者权限但未启用 MFA 的订阅帐户
- [预览]: 审核具有读取权限但未启用 MFA 的订阅帐户
- [预览]: 审核具有写入权限但未启用 MFA 的订阅帐户
- [预览]: 部署 VM 扩展以审核 Linux VM 密码文件权限
- [预览]: 审核 Linux VM /etc/密码文件权限是否设置为 0644

A.9.2.5 评审用户访问权限

Azure 实施了基于角色的访问控制 (RBAC) 来帮助你管理谁有权访问 Azure 中的资源。使用 Azure 门户可以评审有权访问 Azure 资源的用户及其权限。此蓝图分配四个 Azure Policy 定义用于审核应该优先评审的帐户，包括已淘汰的帐户，以及具有提升权限的外部帐户。

- [预览]: 审核已弃用的订阅帐户
- [预览]: 审核具有所有者权限但已被弃用的订阅帐户
- [预览]: 审核具有所有者权限的外部订阅帐户
- [预览]: 审核具有写入权限的外部订阅帐户

A.9.2.6 删除或调整访问权限

Azure 实施了基于角色的访问控制 (RBAC) 来帮助你管理谁有权访问 Azure 中的资源。使用 Azure Active Directory 和 RBAC 可以更新用户角色，以反映组织变化。如果需要，可以阻止帐户登录(或将其删除)，这会立即删除其 Azure 资源访问权限。此蓝图分配两个 Azure Policy 定义用于审核应该考虑删除的已淘汰帐户。

- [预览]: 审核已弃用的订阅帐户
- [预览]: 审核具有所有者权限但已被弃用的订阅帐户

A.9.4.2 安全登录过程

此蓝图分配了三个 Azure Policy 定义，以用于审核未启用多重身份验证的帐户。Azure 多重身份验证通过要求使用另一种形式的身份验证提供额外的安全性，从而提供增强式身份验证。通过监视未启用多重身份验证的帐户，可以识别出更有可能会泄密的帐户。

- [预览]: 审核具有所有者权限但未启用 MFA 的订阅帐户
- [预览]: 审核具有读取权限但未启用 MFA 的订阅帐户
- [预览]: 审核具有写入权限但未启用 MFA 的订阅帐户

A.9.4.3 密码管理系统

此蓝图通过分配 10 个 Azure Policy 定义用于审核不强制实施最低强度和其他密码要求的 Windows VM，来帮助你

强制实施强密码。识别违反密码强度策略的 VM 有助于采取纠正措施，以确保所有 VM 用户帐户的密码符合策略。

- [预览]: 部署 VM 扩展以审核 Windows VM 是否强制实施密码复杂性要求
- [预览]: 部署 VM 扩展以审核 Windows VM 最长密码期限是否为 70 天
- [预览]: 部署 VM 扩展以审核 Windows VM 最短密码期限是否为 1 天
- [预览]: 部署 VM 扩展以审核 Windows VM 密码必须至少为 14 个字符
- [预览]: 部署 VM 扩展以审核 Windows VM 不应允许之前的 24 个密码
- [预览]: 审核 Windows VM 是否强制实施密码复杂性要求
- [预览]: 审核 Windows VM 最长密码期限是否为 70 天
- [预览]: 审核 Windows VM 最短密码期限是否为 1 天
- [预览]: 审核 Windows VM 密码必须至少为 14 个字符
- [预览]: 审核 Windows VM 不应允许之前的 24 个密码

A.10.1.1 有关使用加密控制措施的策略

此蓝图通过分配 13 个 Azure Policy 定义用于强制实施特定的加密控制措施并审核弱加密设置的使用，来帮助你针对加密控制措施的使用强制实施自己的策略。了解 Azure 资源中的哪些位置采用欠佳的加密配置有助于采取纠正措施，以确保根据信息安全策略配置资源。具体而言，此蓝图分配的策略要求对 Blob 存储帐户和 Data Lake Storage 帐户加密；要求对 SQL 数据库实施透明数据加密；审核存储帐户、SQL 数据库、虚拟机磁盘和自动化帐户变量是否缺少加密；审核是否与存储帐户、函数应用、Web 应用、API 应用和 Redis 缓存建立了不安全的连接；审核虚拟机弱密码加密；审核未加密的 Service Fabric 通信。

- [预览]: 审核函数应用的仅 HTTPS 访问权限
- [预览]: 审核 Web 应用的仅 HTTPS 访问权限
- [预览]: 审核 API 应用的仅 HTTPS 访问权限
- [预览]: 审核存储帐户是否缺少 blob 加密
- [预览]: 部署 VM 扩展以审核 Windows VM 不应使用可逆加密存储密码
- [预览]: 审核 Windows VM 不应使用可逆加密存储密码
- [预览]: 监视 Azure 安全中心内未加密的 VM 磁盘
- 审核确认已启用自动化帐户变量加密功能
- 审核确认仅启用了到 Redis 缓存的安全连接
- 审核确认指向存储帐户的传输的安全性
- 审核确认 Service Fabric 中的 ClusterProtectionLevel 属性设置为 EncryptAndSign
- 审核透明数据加密状态
- 应在 SQL 数据库上启用透明数据加密

A.12.4.1 事件日志记录

此蓝图通过分配七个 Azure Policy 定义用于审核 Azure 资源的日志设置，来帮助你确保记录系统事件。诊断日志针对 Azure 资源中执行的操作提供见解。

- [预览]: 审核依赖项代理部署 - VM 映像 (OS) 未列出
- [预览]: 审核 VMSS 中的依赖项代理部署 - VM 映像 (OS) 未列出
- [预览]: 审核 Log Analytics 代理部署 - VM 映像 (OS) 未列出
- [预览]: 审核 VMSS 中的 Log Analytics 代理部署 - VM 映像 (OS) 未列出
- 审核诊断设置
- 审核 SQL 服务器级别审核设置
- 应在 SQL Server 的高级数据安全设置上启用审核

A.12.4.3 管理员和操作员日志

此蓝图分配了七个 Azure Policy 定义，以用于审核 Azure 资源的日志设置，从而帮助你确保系统事件会被记录。诊断日志针对 Azure 资源中执行的操作提供见解。

- [预览]: 审核依赖项代理部署 - VM 映像 (OS) 未列出
- [预览]: 审核 VMSS 中的依赖项代理部署 - VM 映像 (OS) 未列出
- [预览]: 审核 Log Analytics 代理部署 - VM 映像 (OS) 未列出
- [预览]: 审核 VMSS 中的 Log Analytics 代理部署 - VM 映像 (OS) 未列出
- 审核诊断设置
- 审核 SQL 服务器级别审核设置
- 应在 SQL Server 的高级数据安全设置上启用审核

A.12.4.4 时钟同步

此蓝图分配了七个 Azure Policy 定义，以用于审核 Azure 资源的日志设置，从而帮助你确保系统事件会被记录。Azure 日志依赖于同步的内部时钟创建各个资源中事件的时间相关记录。

- [预览]: 审核依赖项代理部署 - VM 映像 (OS) 未列出
- [预览]: 审核 VMSS 中的依赖项代理部署 - VM 映像 (OS) 未列出
- [预览]: 审核 Log Analytics 代理部署 - VM 映像 (OS) 未列出
- [预览]: 审核 VMSS 中的 Log Analytics 代理部署 - VM 映像 (OS) 未列出
- 审核诊断设置
- 审核 SQL 服务器级别审核设置
- 应在 SQL Server 的高级数据安全设置上启用审核

A.12.5.1 在可操作的系统上安装软件

自适应应用程序控制是 Azure 安全中心内的一个解决方案，可帮助你控制哪些应用程序可在 Azure 中的 VM 上运行。此蓝图分配一个 Azure Policy 定义用于监视对允许的应用程序集的更改。此功能帮助你控制软件和应用程序在 Azure VM 上的安装。

- [预览]: 监视 Azure 安全中心内列入允许列表的可能的应用

A.12.6.1 管理技术漏洞

此蓝图分配了五个 Azure Policy 定义，以用于在 Azure 安全中心内监视缺少的系统更新、操作系统漏洞、SQL 漏洞和虚拟机漏洞，来帮助你管理信息系统漏洞。Azure 安全中心提供报告功能，使你能够实时洞察已部署的 Azure 资源的安全状态。

- [预览]: 监视 Azure 安全中心 Endpoint Protection 的缺失情况
- [预览]: 监视 Azure 安全中心内系统更新的缺失情况
- [预览]: 监视 Azure 安全中心的 OS 漏洞
- [预览]: 监视 Azure 安全中心的 SQL 漏洞评估结果
- [预览]: 监视 Azure 安全中心的 VM 漏洞

A.12.6.2 软件安装的限制

自适应应用程序控制是 Azure 安全中心内的一个解决方案，可帮助你控制哪些应用程序可在 Azure 中的 VM 上运行。此蓝图分配一个 Azure Policy 定义用于监视对允许的应用程序集的更改。软件安装限制有助于减少出现软件漏洞的可能性。

- [预览]: 监视 Azure 安全中心内列入允许列表的可能的应用

A.13.1.1 网络控制措施

此蓝图通过分配一个 Azure Policy 定义用于监视具有宽松规则的网络安全组，来帮助你管理和控制网络。过于宽松的规则可能会允许意外的网络访问，应该对其进行评审。此蓝图还分配了三个 Azure Policy 定义，以用于监视不受保护的终结点、应用程序和存储帐户。不受防火墙保护的终结点和应用程序，以及具有无限制访问权限的存储帐户，可能会允许意外访问信息系统中包含的信息。

- [预览]: 监视 Azure 安全中心内规则较宽松的网络访问
- [预览]: 监视 Azure 安全中心内未受保护的网络终结点
- [预览]: 监视 Azure 安全中心内未受保护的 Web 应用程序
- 审核对存储帐户的不受限的网络访问

A.13.2.1 信息传输策略和过程

该蓝图通过分配两个 Azure Policy 定义用于审核与存储帐户和 Redis 缓存建立的不安全连接，来帮助你确保与 Azure 服务之间安全传输信息。

- 审核确认仅启用了到 Redis 缓存的安全连接
- 审核确认指向存储帐户的传输的安全性

后续步骤

了解 ISO 27001 应用服务环境/SQL 数据库工作负荷蓝图示例的控制映射后，请访问以下文章来了解体系结构以及如何部署此示例：

ISO 27001 应用服务环境/SQL 数据库工作负荷蓝图 - 概述 ISO 27001 应用服务环境/SQL 数据库工作负荷蓝图 - 部署步骤

有关蓝图和如何使用这些蓝图的更多文章：

- 了解蓝图生命周期。
- 了解如何使用静态和动态参数。
- 了解如何自定义蓝图排序顺序。
- 了解如何利用蓝图资源锁定。
- 了解如何更新现有分配。

部署 ISO 27001 应用服务环境/SQL 数据库工作负荷蓝图示例

2019/9/5 • • Edit Online

若要部署 Azure 蓝图 ISO 27001 应用服务环境/SQL 数据库工作负荷蓝图示例，必须执行以下步骤：

- 部署 ISO 27001 共享服务蓝图示例
- 基于示例创建新的蓝图
- 将示例副本标记为“已发布”
- 将蓝图副本分配到现有的订阅

如果没有 Azure 订阅，请在开始之前创建一个免费帐户。

部署 ISO 27001 共享服务蓝图示例

在部署此蓝图示例之前，必须先将 ISO 27001 共享服务蓝图示例部署到目标订阅。如果未成功部署 ISO 27001 共享服务蓝图示例，则此蓝图示例将会缺少基础结构依赖项，并且在部署期间将会失败。

> **IMPORTANT**
> 必须在 ISO 27001 共享服务蓝图示例所在的同一个订阅中分配此蓝图示例。

基于示例创建蓝图

首先，通过使用示例作为起点在环境中创建新的蓝图，来实现蓝图示例。

1. 选择“所有服务”，然后在左窗格中搜索并选择“策略”。在“策略”页上选择“蓝图”。
2. 在左侧的“开始”页中，选择“创建蓝图”下的“创建”按钮。
3. 在“其他示例”下找到“ISO 27001: ASE/SQL 工作负荷”蓝图示例，然后选择“使用此示例”。
4. 输入该蓝图示例的“基本信息”：
   - **蓝图名称**：提供 ISO 27001 ASE/SQL 工作负荷蓝图示例副本的名称。
   - **定义位置**：使用省略号并选择要将示例副本保存到的管理组。
5. 选择页面顶部的“项目”选项卡，或页面底部的“下一步: 项目”。
6. 查看构成蓝图示例的项目列表。许多项目包含稍后我们将要定义的参数。查看完蓝图示例后，选择“保存草稿”。

发布示例副本

现已在环境中创建蓝图示例的副本。该副本在创建后处于“草稿”模式，必须先将其发布，然后才能分配和部署它。可根据环境和需求自定义蓝图示例的副本，但这种修改可能会将该副本移出 ISO 27001 标准。

1. 选择“所有服务”，然后在左窗格中搜索并选择“策略”。在“策略”页上选择“蓝图”。
2. 在左侧选择“蓝图定义”页。使用筛选器找到蓝图示例的副本，然后选择它。
3. 选择页面顶部的“发布蓝图”。在右侧的新窗格中，提供蓝图示例副本的**版本**。以后做出修改时，此属性非常有用。提供**更改注释**，例如，“基于 ISO 27001 蓝图示例发布的第一个版本”。然后选择页面底部的“发布”。

分配示例副本

成功发布蓝图示例的副本后，可将它分配到它所在的管理组中的某个订阅。在此步骤中，需提供参数来使蓝图示例副本的每个部署保持唯一。

1. 选择“所有服务”，然后在左窗格中搜索并选择“策略”。在“策略”页上选择“蓝图”。
2. 在左侧选择“蓝图定义”页。使用筛选器找到蓝图示例的副本，然后选择它。
3. 选择蓝图定义页面顶部的“分配蓝图”。
4. 提供蓝图分配的参数值：
   - 基础
     - **订阅**：在蓝图示例副本所保存到的管理组中选择一个或多个订阅。如果选择多个订阅，将使用输入的参数为每个订阅创建一个分配。
     - **分配名称**：系统会根据蓝图的名称预先填充该名称。请根据需要更改该名称，或保留原样。
     - **位置**：选择要在其中创建托管标识的区域。Azure 蓝图使用此托管标识在分配的蓝图中部署所有项目。若要了解详细信息，请参阅 Azure 资源的托管标识。
     - **蓝图定义版本**：选择蓝图示例副本的已发布版本。
   - 锁分配

     选择环境的蓝图锁定设置。有关更多信息，请参阅蓝图资源锁定。
   - 托管标识

     保留默认的系统分配的托管标识选项。
   - 蓝图参数

     蓝图定义中的许多项目使用本部分定义的参数来提供一致性。
     - **组织名称**：输入组织的短名称。此属性主要用于为资源命名。
     - **共享服务订阅 ID**：ISO 27001 共享服务蓝图示例所分配到的订阅 ID。
     - **默认子网地址前缀**：虚拟网络默认子网的 CIDR 表示法。默认值为 *10.1.0.0/16*。
     - **工作负荷位置**：确定要将项目部署到的位置。并非所有服务都可在所有位置使用。部署此类服务的项目会针对该项目要部署到的位置提供一个参数选项。
   - 项目参数

     在本部分定义的参数将应用到定义了这些参数的项目。这些参数属于动态参数，因为它们是在分配蓝图期间定义的。有关完整列表或项目参数及其说明，请参阅项目参数表 。
5. 输入所有参数后，选择页面底部的“分配”。随后将创建蓝图分配，并开始部署项目。部署过程大约需要一小时。若要检查部署状态，请打开蓝图分配。

> **WARNING**
> Azure 蓝图服务和内置蓝图示例是**免费的**。Azure 资源按产品定价 。使用定价计算器 可以估算运行此蓝图示例部署的资源所需的成本。

项目参数表

下表提供了蓝图项目参数的列表：

项目名称	项目类型	参数名称	说明
Log Analytics 资源组	Resource group	Name	已锁定 - 将组织名称与 `-workload-log-rg` 相连接可使资源组名称保持唯一。
Log Analytics 资源组	Resource group	位置	已锁定 - 使用蓝图参数。
Log Analytics 模板	资源管理器模板	服务层	设置 Log Analytics 工作区的层。默认值为 *PerNode*。
Log Analytics 模板	资源管理器模板	日志保留期(以天为单位)	日志保留期(以天为单位)。默认值为 *365*。
Log Analytics 模板	资源管理器模板	位置	用于创建 Log Analytics 工作区的区域。默认值为“美国西部 2”。
网络资源组	Resource group	Name	已锁定 - 将组织名称与 `-workload-net-rg` 相连接可使资源组名称保持唯一。
网络资源组	Resource group	位置	已锁定 - 使用蓝图参数。
网络安全组模板	资源管理器模板	日志保留期(以天为单位)	日志保留期(以天为单位)。默认值为 *365*。
虚拟网络和路由表模板	资源管理器模板	Azure 防火墙专用 IP	配置 Azure 防火墙的专用 IP。应是“ISO 27001: 共享服务”项目参数“Azure 防火墙子网地址前缀”中定义的 CIDR 表示法的一部分。默认值为 *10.0.4.4*。
虚拟网络和路由表模板	资源管理器模板	共享服务订阅 ID	用于启用工作负荷与共享服务之间的 VNET 对等互连的值。
虚拟网络和路由表模板	资源管理器模板	虚拟网络地址前缀	虚拟网络的 CIDR 表示法。默认值为 *10.1.0.0/16*。
虚拟网络和路由表模板	资源管理器模板	默认子网地址前缀	虚拟网络默认子网的 CIDR 表示法。默认值为 *10.1.0.0/16*。
虚拟网络和路由表模板	资源管理器模板	ADDS IP 地址	第一个 ADDS VM 的 IP 地址。此值用作自定义 VNET DNS。
密钥保管库资源组	Resource group	Name	已锁定 - 将组织名称与 `-workload-kv-rg` 相连接可使资源组名称保持唯一。
密钥保管库资源组	Resource group	位置	已锁定 - 使用蓝图参数。

项目名称	项目类型	参数名称	说明
Key Vault 模板	资源管理器模板	AAD 对象 ID	需要访问 Key Vault 实例的帐户的 AAD 对象标识符。无默认值，且不能留空。若要在 Azure 门户中查找此值，请在“服务”下搜索并选择“用户”。使用“名称”框筛选帐户名，并选择该帐户。在“用户配置文件”页上，选择“对象 ID”旁边的“单击以复制”图标。
Key Vault 模板	资源管理器模板	日志保留期(以天为单位)	日志保留期（以天为单位）。默认值为 *365*。
Key Vault 模板	资源管理器模板	Key Vault SKU	指定创建的 Key Vault 的 SKU。默认值为“高级”。
Key Vault 模板	资源管理器模板	Azure SQL Server 管理员用户名	用于访问 Azure SQL Server 的用户名。必须与 **Azure SQL 数据库模板**中的相同属性值相匹配。默认值为 *sql-admin-user*。
Azure SQL 数据库资源组	Resource group	Name	**已锁定** - 将组织**名称**与 `-workload-azsql-rg` 相连接可使资源组名称保持唯一。
Azure SQL 数据库资源组	Resource group	位置	**已锁定** - 使用蓝图参数。
Azure SQL 数据库模板	资源管理器模板	Azure SQL Server 管理员用户名	Azure SQL 服务器的用户名。必须与 **Key Vault 模板**中的相同属性值相匹配。默认值为 *sql-admin-user*。
Azure SQL 数据库模板	资源管理器模板	Azure SQL Server 管理员密码(Key Vault 资源 ID)	Key Vault 的资源 ID。请使用 "/subscription/{subscriptionId}/resourceGroups/{orgName}-workload-kv/providers/Microsoft.KeyVault/vaults/{orgName}-workload-kv"，并将 `{subscriptionId}` 替换为你的订阅 ID，将 `{orgName}` 替换为“组织名称”蓝图参数。
Azure SQL 数据库模板	资源管理器模板	Azure SQL Server 管理员密码(Key Vault 机密名称)	SQL Server 管理员的用户名。必须与 **Key Vault 模板**中的“Azure SQL Server 管理员用户名”属性值相匹配。
Azure SQL 数据库模板	资源管理器模板	日志保留期(以天为单位)	日志保留期（以天为单位）。默认值为 *365*。

项目名称	项目类型	参数名称	说明
Azure SQL 数据库模板	资源管理器模板	AAD 管理员对象 ID	分配为 Active Directory 管理员的用户的 AAD 对象 ID。无默认值，且不能留空。若要在 Azure 门户中查找此值，请在“服务”下搜索并选择“用户”。使用“名称”框筛选帐户名，并选择该帐户。在“用户配置文件”页上，选择“对象 ID”旁边的“单击以复制”图标。
Azure SQL 数据库模板	资源管理器模板	AAD 管理员登录名	目前，无法将 Microsoft 帐户（如 live.com 或 outlook.com）设置为管理员。只能将你组织中的用户和安全组设置为管理员。无默认值，且不能留空。若要在 Azure 门户中查找此值，请在“服务”下搜索并选择“用户”。使用“名称”框筛选帐户名，并选择该帐户。在“用户配置文件”页上，复制“用户名”。
应用服务环境资源组	Resource group	Name	已锁定 - 将组织名称与 `-workload-ase-rg` 相连接可使资源组名称保持唯一。
应用服务环境资源组	Resource group	位置	已锁定 - 使用蓝图参数。
应用服务环境模板	资源管理器模板	域名	示例创建的 Active Directory 的名称。默认值为 *contoso.com*。
应用服务环境模板	资源管理器模板	ASE 位置	应用服务环境位置。默认值为“美国西部 2”。
应用服务环境模板	资源管理器模板	应用程序网关日志保留期(天)	日志保留期（以天为单位）。默认值为 *365*。

后续步骤

了解 ISO 27001 应用服务环境/SQL 数据库工作负荷蓝图示例的部署步骤后，请访问以下文章来了解体系结构和控制映射：

ISO 27001 应用服务环境/SQL 数据库工作负荷蓝图 - 概述 ISO 27001 应用服务环境/SQL 数据库工作负荷蓝图 - 控制映射

有关蓝图和如何使用这些蓝图的更多文章：

- 了解蓝图生命周期。
- 了解如何使用静态和动态参数。
- 了解如何自定义蓝图排序顺序。
- 了解如何利用蓝图资源锁定。
- 了解如何更新现有分配。

NIST SP 800-53 R4 蓝图示例的概述

2019/9/4 • • Edit Online

NIST SP 800-53 R4 蓝图示例提供了监管防护措施，其中使用 Azure Policy 来帮助评估特定 NIST SP 800-53 R4 控制要求。对于 Azure 部署的任何必须实现 NIST SP 800-53 R4 控制要求的体系结构，此蓝图可帮助客户为其部署一组核心策略。

控制映射

控制映射部分提供了有关包含在此蓝图内的策略的详细信息，以及这些策略如何满足 NIST SP 800-53 R4 中的各种控制要求。分配给一个体系结构时，资源由 Azure Policy 评估是否不符合已分配的策略。有关详细信息，请参阅 Azure Policy。

后续步骤

你已查看了 NIST SP 800-53 R4 蓝图示例概述。接下来，请访问以下文章，了解控制映射以及如何部署此示例：

NIST SP 800-53 R4 蓝图 - 控制映射 NIST SP 800-53 R4 蓝图 - 部署步骤

有关蓝图和如何使用这些蓝图的更多文章：

- 了解蓝图生命周期。
- 了解如何使用静态和动态参数。
- 了解如何自定义蓝图排序顺序。
- 了解如何利用蓝图资源锁定。
- 了解如何更新现有分配。

NIST SP 800-53 R4 蓝图示例的控制映射

2019/9/2 • • Edit Online

以下文章详细说明了 Azure 蓝图 SP 800-53 R4 蓝图示例如何映射到 NIST SP 800-53 R4 控制措施。有关控制措施的详细信息，请参阅 NIST SP 800-53。

以下映射适用于 NIST SP 800-53 (Rev. 4) 控制措施 。使用右侧的导航栏可直接跳转到特定的控制映射。许多的映射控制措施都是使用 Azure Policy 计划实施的。若要查看完整计划，请在 Azure 门户中打开"策略"，并选择"定义"页。然后，找到并选择"[预览]:审核 NIST SP 800-53 R4 控制措施并部署特定 VM 扩展以支持审核要求"内置策略计划 。

AC-2 帐户管理

此蓝图可帮助你查看可能不符合你组织的帐户管理要求的帐户。此蓝图分配 Azure Policy 定义，这些定义用于审核对订阅和弃用帐户具有读、写和所有者权限的外部帐户。通过查看受到这些策略审核的帐户，可以采取适当的措施，确保满足帐户管理要求。

- 应从订阅中删除弃用的帐户
- 应从订阅中删除拥有所有者权限的已弃用帐户
- 应从订阅中删除拥有所有者权限的外部帐户
- 应从订阅中删除拥有读取权限的外部帐户
- 应从订阅中删除具有写入权限的外部帐户

AC-2 (7) 帐户管理 | 基于角色的方案

Azure 实施了基于角色的访问控制 (RBAC) 来帮助你管理谁有权访问 Azure 中的资源。使用 Azure 门户可以评审有权访问 Azure 资源的用户及其权限。此蓝图还分配 Azure Policy 定义，用于审核 Azure Active Directory 身份验证在 SQL 服务器和 Service Fabric 中的使用。使用 Azure Active Directory 身份验证可以简化权限管理，以及集中化数据库用户和其他 Microsoft 服务的标识管理。此外，此蓝图还分配一个 Azure Policy 定义用于审核自定义 RBAC 规则的使用。了解实施自定义 RBAC 规则的位置有助于验证需求以及实施是否适当，因为自定义 RBAC 规则容易出错。

- 应该为 SQL 服务器预配 Azure Active Directory 管理员
- 审核自定义 RBAC 规则的使用
- Service Fabric 群集只应使用 Azure Active Directory 进行客户端身份验证

AC-2 (12) 帐户管理 | 帐户监视/异常使用

实时 (JIT) 虚拟机访问会锁定发往 Azure 虚拟机的入站流量，降低遭受攻击的可能性，同时在需要时还可轻松连接到 VM。所有访问虚拟机的 JIT 请求都记录在活动日志中，用于监视异常使用情况。此蓝图分配了一个 Azure Policy 定义，有助于你监视能够支持实时访问但尚未配置的虚拟机。

- 应在虚拟机上应用实时网络访问控制

AC-4 信息流强制

跨域资源共享 (CORS) 支持从外部域请求应用服务资源。Microsoft 建议只允许必需的域与 API、函数和 web 应用程序进行交互。此蓝图分配了一个 Azure Policy 定义，有助于你监视 Azure 安全中心中的 CORS 资源访问限制。了解 CORS 实现有助于你验证信息流控制措施是否实现。

- CORS 不应允许所有资源都能访问你的 Web 应用程序

AC-5 职责分离

仅分配一个 Azure 订阅所有者并不能实现管理冗余。相反，分配过多的 Azure 订阅所有者会增大违规的可能性，因为会有更多的所有者帐户可能会泄密。此蓝图可帮助你通过分配用于审核 Azure 订阅所有者数目的 Azure Policy 定义，来保持适当的 Azure 订阅所有者数目。此蓝图还分配 Azure Policy 定义，有助于你控制 Windows 虚拟机上管理员组的成员身份。管理订阅所有者和虚拟机管理员权限有助于实现适当的职责分离。

- 只多只为订阅指定 3 个所有者
- 审核在其管理员组中包含任何指定成员的 Windows VM
- 审核在其管理员组中不包含所有指定成员的 Windows VM
- 部署要求以审核在其管理员组中包含任何指定成员的 Windows VM
- 部署要求以审核在其管理员组中不包含所有指定成员的 Windows VM
- 应该为你的订阅分配了多个所有者

AC-6 (7) 最小特权 | 用户特权评审

Azure 实施了基于角色的访问控制 (RBAC) 来帮助你管理谁有权访问 Azure 中的资源。使用 Azure 门户可以评审有权访问 Azure 资源的用户及其权限。此蓝图分配 Azure Policy 定义，用于审核应优先评审的帐户。评审这些帐户指标可帮助确保实现最低特权控制措施。

- 只多只为订阅指定 3 个所有者
- 审核在其管理员组中包含任何指定成员的 Windows VM
- 审核在其管理员组中不包含所有指定成员的 Windows VM
- 部署要求以审核在其管理员组中包含任何指定成员的 Windows VM
- 部署要求以审核在其管理员组中不包含所有指定成员的 Windows VM
- 应该为你的订阅分配了多个所有者

AC-16 安全属性

Azure SQL 数据库高级数据安全性的数据发现和分类功能提供用于发现、分类、标记和保护数据库中敏感数据的功能。它可用于直观查看数据库分类状态，以及跟踪对数据库内和其边界外的敏感数据的访问。高级数据安全性有助于确保信息与组织的相应安全属性相关联。此蓝图分配 Azure Policy 定义用于在 SQL 服务器上监视和强制使用高级数据安全性。

- 应在托管实例上启用高级数据安全性
- 应在 SQL 服务器上启用高级数据安全性
- 在 SQL 服务器上部署高级数据安全

AC-17 (1) 远程访问 | 自动监视/控制

此蓝图可帮助你监视和控制远程访问，因为它会分配 Azure Policy 定义用于监视 Azure 应用服务应用程序的远程调试处于关闭状态，此蓝图还会分配策略定义用于审核允许来自无密码帐户的远程连接的 Linux 虚拟机。此蓝图还将分配一个 Azure Policy 定义，用于帮助监视对存储帐户的无限制访问。监视这些指标可以帮助确保远程访问方法符合安全策略。

- [预览]: 审核允许通过没有密码的帐户进行远程连接的 Linux VM
- [预览]: 部署要求以审核允许通过没有密码的帐户进行远程连接的 Linux VM
- 审核对存储帐户的不受限的网络访问
- 应为 API 应用禁用远程调试
- 应对函数应用禁用远程调试
- 应禁用 Web 应用程序的远程调试

AU-3 (2) 审核记录的内容 | 计划的审核记录内容的集中管理

Azure Monitor 收集的日志数据存储在支持集中配置和管理的 Log Analytics 工作区中。此蓝图通过分配 Azure Policy 定义来确保事件被记录下来，这些定义审核并强制在 Azure 虚拟机上部署 Log Analytics 代理。

- [预览]: 审核 Log Analytics 代理部署 - VM 映像 (OS) 未列出
- [预览]: 审核 VMSS 中的 Log Analytics 代理部署 - VM 映像 (OS) 未列出
- [预览]: 审核 VM 的 Log Analytics 工作区 — 报告不匹配
- [预览]: 为 Linux VM 规模集(VMSS)部署 Log Analytics 代理
- [预览]: 为 Linux VM 部署 Log Analytics 代理
- [预览]: 为 Windows VM 规模集(VMSS)部署 Log Analytics 代理
- [预览]: 为 Windows VM 部署 Log Analytics 代理

AU-5 对审核处理失败的响应

此蓝图分配 Azure Policy 定义用于监视审核和事件日志记录配置。监视这些配置可以提供审核系统故障或配置错误的指标，帮助你采取纠正措施。

- 审核诊断设置
- 审核 SQL 服务器级别审核设置
- 应在托管实例上启用高级数据安全性
- 应在 SQL 服务器上启用高级数据安全性

AU-6 (4) 审核评审、分析和报告 | 中心评审和分析

Azure Monitor 收集的日志数据存储在支持集中报告和分析的 Log Analytics 工作区中。此蓝图通过分配 Azure Policy 定义来确保事件被记录下来，这些定义审核并强制在 Azure 虚拟机上部署 Log Analytics 代理。

- [预览]: 审核 Log Analytics 代理部署 - VM 映像 (OS) 未列出
- [预览]: 审核 VMSS 中的 Log Analytics 代理部署 - VM 映像 (OS) 未列出
- [预览]: 审核 VM 的 Log Analytics 工作区 — 报告不匹配
- [预览]: 为 Linux VM 规模集(VMSS)部署 Log Analytics 代理
- [预览]: 为 Linux VM 部署 Log Analytics 代理
- [预览]: 为 Windows VM 规模集(VMSS)部署 Log Analytics 代理
- [预览]: 为 Windows VM 部署 Log Analytics 代理

AU-12 审核生成

此蓝图通过分配 Azure Policy 定义来帮助确保记录系统事件，这些定义用于审核在 Azure 资源上的日志设置。这些策略定义审核并强制部署 Azure 虚拟机上的 Log Analytics 代理并强制配置针对其他 Azure 资源类型的审核设置。这些策略定义还审核诊断日志配置，以提供对 Azure 资源内执行的操作的见解。此外，审核和高级数据安全在 SQL 服务器上配置。

- [预览]: 审核 Log Analytics 代理部署 - VM 映像 (OS) 未列出
- [预览]: 审核 VMSS 中的 Log Analytics 代理部署 - VM 映像 (OS) 未列出
- [预览]: 审核 VM 的 Log Analytics 工作区 — 报告不匹配
- [预览]: 为 Linux VM 规模集(VMSS)部署 Log Analytics 代理
- [预览]: 为 Linux VM 部署 Log Analytics 代理
- [预览]: 为 Windows VM 规模集(VMSS)部署 Log Analytics 代理
- [预览]: 为 Windows VM 部署 Log Analytics 代理
- 审核诊断设置
- 审核 SQL 服务器级别审核设置

- 应在托管实例上启用高级数据安全性
- 应在 SQL 服务器上启用高级数据安全性
- 在 SQL 服务器上部署高级数据安全
- 对 SQL 服务器部署审核
- 为网络安全组部署诊断设置

CM-7 (2) 最少的功能 | 防止程序执行

Azure 安全中心中的自适应应用程序控制是一种智能、自动化端到端的应用程序允许列表解决方案，可以阻止或防止特定软件在虚拟机上运行。应用程序控制可以在强制模式下运行，从而禁止未批准的应用程序运行。此蓝图分配了一个 Azure Policy 定义，用于帮助监视建议使用应用程序允许列表但尚未对其进行配置的虚拟机。

- 应在虚拟机上启用自适应应用程序控制

CM-7 (5) 最少的功能 | 授权软件/允许列表

Azure 安全中心中的自适应应用程序控制是一种智能、自动化端到端的应用程序允许列表解决方案，可以阻止或防止特定软件在虚拟机上运行。应用程序控制帮助你为虚拟机创建批准的应用程序列表。此蓝图分配了一个 Azure Policy 定义，用于帮助监视建议使用应用程序允许列表但尚未对其进行配置的虚拟机。

- 应在虚拟机上启用自适应应用程序控制

CM-11 用户安装的软件

Azure 安全中心中的自适应应用程序控制是一种智能、自动化端到端的应用程序允许列表解决方案，可以阻止或防止特定软件在虚拟机上运行。应用程序控制可以帮助你强制执行和监视软件限制策略的符合性。此蓝图分配了一个 Azure Policy 定义，用于帮助监视建议使用应用程序允许列表但尚未对其进行配置的虚拟机。

- 应在虚拟机上启用自适应应用程序控制

CP-7 备用处理站点

Azure Site Recovery 将在虚拟机上运行的工作负荷从主位置复制到辅助位置。如果在主站点发生故障，工作负荷将故障转移到辅助位置。此蓝图分配了一个 Azure Policy 定义，用于审核没有配置灾难恢复的虚拟机。监视此指标可以帮助确保必要的应变控制措施已到位。

- 审核没有配置灾难恢复的虚拟机

IA-2 (1) 标识和身份验证(组织用户) | 对特权帐户的网络访问

此蓝图分配 Azure Policy 定义用于审核拥有所有者和/或写入权限但未启用多重身份验证的帐户，从而帮助你限制和控制特权访问。即使某个身份验证信息片段已泄密，多重身份验证也有助于保护帐户的安全。通过监视未启用多重身份验证的帐户，可以识别出更有可能会泄密的帐户。

- 应在对订阅拥有所有者权限的帐户上启用 MFA
- 应在对订阅拥有写入权限的帐户上启用 MFA

IA-2 (2) 标识和身份验证(组织用户) | 网络访问非特权帐户

此蓝图分配一个 Azure Policy 定义，用于审核拥有读取权限但未启用多重身份验证的帐户，从而帮助你限制和控制访问。即使某个身份验证信息片段已泄密，多重身份验证也有助于保护帐户的安全。通过监视未启用多重身份验证的帐户，可以识别出更有可能会泄密的帐户。

- 应在对订阅拥有读取权限的帐户上启用 MFA

IA-5 验证器管理

此蓝图分配 Azure Policy 定义，用于审核允许来自无密码帐户的远程连接并/或在密码文件中设置了不正确权限的 Linux 虚拟机。此蓝图还会分配一个策略定义用于审核 Windows 虚拟机密码加密类型的配置。监视这些指标有助于确保系统验证器符合组织的标识和身份验证策略。

- [预览]: 审核未将密码文件权限设为 0644 的 Linux VM
- [预览]: 审核具有不使用密码的帐户的 Linux VM
- [预览]: 审核未存储使用可逆加密的密码的 Windows VM
- [预览]: 部署要求以审核未将密码文件权限设置为 0644 的 Linux VM
- [预览]: 部署要求以审核具有不使用密码的帐户的 Linux VM
- [预览]: 部署要求以审核未存储使用可逆加密的密码的 Windows VM

IA-5 (1) 验证器管理 |基于密码的身份验证

此蓝图通过分配 Azure Policy 定义用于审核不强制实施最低强度和其他密码要求的 Windows 虚拟机，来帮助你强制实施强密码。感知虚拟机是否违反密码强度策略有助于采取纠正措施，确保所有虚拟机用户帐户的密码与组织的密码策略相符。

- [预览]: 审核允许重用之前的 24 个密码的 Windows VM
- [预览]: 审核未将最长密码期限设为 70 天的 Windows VM
- [预览]: 审核未将最短密码期限设为 1 天的 Windows VM
- [预览]: 审核未启用密码复杂性设置的 Windows VM
- [预览]: 审核未将最短密码长度限制为 14 个字符的 Windows VM
- [预览]: 审核未存储使用可逆加密的密码的 Windows VM
- [预览]: 部署要求以审核允许重用之前的 24 个密码的 Windows VM
- [预览]: 部署要求以审核未将最长密码期限设为 70 天的 Windows VM
- [预览]: 部署要求以审核未将最短密码期限设为 1 天的 Windows VM
- [预览]: 部署要求以审核未启用密码复杂性设置的 Windows VM
- [预览]: 部署要求以审核未将最短密码长度限制为 14 个字符的 Windows VM
- [预览]: 部署要求以审核未存储使用可逆加密的密码的 Windows VM

RA-5 漏洞扫描

此蓝图分配 Azure Policy 定义用于在 Azure 安全中心内监视操作系统漏洞、SQL 漏洞和虚拟机漏洞，来帮助你管理信息系统漏洞。Azure 安全中心提供报告功能，使你能够实时洞察已部署的 Azure 资源的安全状态。此蓝图还会分配策略定义用于审核和强制执行 SQL 服务器上的高级数据安全。高级数据安全包括漏洞评估和高级威胁防护功能，可帮助你了解已部署资源中的漏洞。

- 应在托管实例上启用高级数据安全性
- 应在 SQL 服务器上启用高级数据安全性
- 在 SQL 服务器上部署高级数据安全
- 应该修复虚拟机规模集上安全配置中的漏洞
- 应该修复虚拟机上安全配置中的漏洞
- 应该修复 SQL 数据库中的漏洞
- 应该通过漏洞评估解决方案修复漏洞

SC-5 拒绝服务保护

Azure 的分布式拒绝服务 (DDoS) 标准层通过基本服务层提供额外功能和缓解功能。这些额外功能包括 Azure Monitor 集成和查看攻击后的缓解报告的功能。此蓝图分配了一个 Azure Policy 定义，用于审核是否启用 DDoS

标准层。了解服务层之间的功能差异有助于为 Azure 环境选择最佳解决方案来解决拒绝服务保护问题。

- 应启用 DDoS 防护标准版

SC-7 边界保护

此蓝图通过分配一个 Azure Policy 定义用于根据 Azure 安全中心的网络安全组强化建议进行监视，以此帮助你管理和控制系统边界。Azure 安全中心分析面向 Internet 的虚拟机的流量模式，并提供网络安全组规则建议，以减少潜在的攻击面。此外，此蓝图还会分配策略定义用于监视不受保护的终结点、应用程序和存储帐户。不受防火墙保护的终结点和应用程序，以及具有无限制访问权限的存储帐户，可能会允许意外访问信息系统中包含的信息。

- 应该强化面向 Internet 的虚拟机的网络安全组规则
- 应该限制通过面向 Internet 的终结点进行访问
- 应该强化 IaaS 上 Web 应用程序的 NSG 规则
- 审核对存储帐户的不受限的网络访问

SC-7 (3) 边界保护 | 接入点

实时 (JIT) 虚拟机访问会锁定发往 Azure 虚拟机的入站流量，降低遭受攻击的可能性，同时在需要时还可轻松连接到 VM。实时虚拟机访问有助于限制对 Azure 中资源的外部连接数。此蓝图分配了一个 Azure Policy 定义，有助于你监视能够支持实时访问但尚未配置的虚拟机。

- 应在虚拟机上应用实时网络访问控制

SC-7 (4) 边界保护 | 外部电信服务

实时 (JIT) 虚拟机访问会锁定发往 Azure 虚拟机的入站流量，降低遭受攻击的可能性，同时在需要时还可轻松连接到 VM。实时虚拟机访问有助于通过促进访问请求和审批流程来管理流量策略的例外情况。此蓝图分配了一个 Azure Policy 定义，有助于你监视能够支持实时访问但尚未配置的虚拟机。

- 应在虚拟机上应用实时网络访问控制

SC-8 (1) 传输保密性和完整性 | 加密或备用物理保护

此蓝图分配 Azure Policy 定义来帮助你监视针对通信协议实施的加密机制，以此帮助你保护传输信息的机密性和完整性。确保通信得到适当的加密可帮助你满足组织的要求，或者防范信息遭到未经授权的透漏和修改。

- 只能通过 HTTPS 访问 API 应用
- 审核未使用安全通信协议的 Windows Web 服务器
- 部署要求以审核未使用安全通信协议的 Windows Web 服务器
- 应该只能通过 HTTPS 访问函数应用
- 应该启用只能通过安全方式连接到 Redis 缓存
- 应该启用安全传输到存储帐户
- 只能通过 HTTPS 访问 Web 应用程序

SC-28 (1) 保护静态信息 | 加密保护

此蓝图分配 Azure Policy 定义用于强制实施特定的加密控制措施并审核弱加密设置的使用，从而帮助你强制实施有关通过使用加密控制措施保护静态信息的策略。了解 Azure 资源中的哪些位置采用欠佳的加密配置有助于采取纠正措施，以确保根据信息安全策略配置资源。具体地说，该蓝图分配的策略定义要求对数据湖存储帐户进行加密；要求 SQL 数据库上的透明数据加密；审核 SQL 数据库、虚拟机磁盘和自动化帐户变量上缺少的加密。

- 应在托管实例上启用高级数据安全性
- 应在 SQL 服务器上启用高级数据安全性

- 在 SQL 服务器上部署高级数据安全
- 部署 SQL DB 透明数据加密
- 应在虚拟机上启用磁盘加密
- 要求对 Data Lake Store 帐户加密
- 应在 SQL 数据库上启用透明数据加密

SI-2 缺陷修正

此蓝图分配 Azure Policy 定义用于在 Azure 安全中心内监视缺少的系统更新、操作系统漏洞、SQL 漏洞和虚拟机漏洞，从而帮助你管理信息系统缺陷。Azure 安全中心提供报告功能，使你能够实时洞察已部署的 Azure 资源的安全状态。此蓝图还会分配一个策略定义用于确保虚拟机规模集的操作系统的修补。

- 要求自动在虚拟机规模集上执行 OS 映像修补
- 应在虚拟机规模集上安装系统更新
- 应在虚拟机上安装系统更新
- 应该修复虚拟机规模集上安全配置中的漏洞
- 应该修复虚拟机上安全配置中的漏洞
- 应该修复 SQL 数据库中的漏洞
- 应该通过漏洞评估解决方案修复漏洞

SI-3 恶意代码防护

此蓝图分配 Azure Policy 定义用于监视 Azure 安全中心中虚拟机上缺失的终结点防护并在 Windows 虚拟机上强制执行 Microsoft 反恶意软件解决方案，从而帮助管理终结点防护，包括恶意代码防护。

- 为 Windows Server 部署默认 Microsoft IaaSAntimalware 扩展
- 应在虚拟机规模集上安装 Endpoint Protection 解决方案
- 监视 Azure 安全中心 Endpoint Protection 的缺失情况

SI-3 (1) 恶意代码防护 | 集中管理

此蓝图分配 Azure Policy 定义用于监视 Azure 安全中心中虚拟机上缺失的终结点防护，从而帮助管理终结点防护，包括恶意代码防护。Azure 安全中心提供集中管理和报告功能，用于实时洞察已部署的 Azure 资源的安全状态。

- 应在虚拟机规模集上安装 Endpoint Protection 解决方案
- 监视 Azure 安全中心 Endpoint Protection 的缺失情况

SI-4 信息系统监视

此蓝图有助于通过审核和跨 Azure 资源强制执行日志记录和数据安全来监视系统。具体而言，分配的策略审核并强制执行 Log Analytics 代理的部署和 SQL 数据库、存储帐户和网络资源的强化安全设置。这些功能有助于检测异常行为和攻击指标，以便你采取相应措施。

- [预览]: 审核 Log Analytics 代理部署 - VM 映像 (OS) 未列出
- [预览]: 审核 VMSS 中的 Log Analytics 代理部署 - VM 映像 (OS) 未列出
- [预览]: 审核 VM 的 Log Analytics 工作区 — 报告不匹配
- [预览]: 为 Linux VM 规模集(VMSS)部署 Log Analytics 代理
- [预览]: 为 Linux VM 部署 Log Analytics 代理
- [预览]: 为 Windows VM 规模集(VMSS)部署 Log Analytics 代理
- [预览]: 为 Windows VM 部署 Log Analytics 代理
- 应在托管实例上启用高级数据安全性
- 应在 SQL 服务器上启用高级数据安全性

- 在 SQL 服务器上部署高级数据安全
- 在存储帐户上部署高级威胁防护
- 对 SQL 服务器部署审核
- 创建虚拟网络时部署网络观察程序
- 在 SQL 服务器上部署威胁检测

SI-4 (18) 信息系统监视 | 分析流量 / 隐蔽性外泄

Azure 存储高级威胁防护会检测试图访问或利用存储帐户的异常或可能有害的企图。保护警报包括异常访问模式、异常提取/上传和可疑存储活动。这些指标有助于检测信息的隐蔽性外泄。

- 在存储帐户上部署高级威胁防护

> **NOTE**
> 特定 Azure Policy 定义的可用性在 Azure 政府和其他国家云中可能会有所不同。

后续步骤

了解 NIST SP 800-53 R4 蓝图的控制映射后，请访问以下文章来了解蓝图和部署此示例的方式：

NIST SP 800-53 R4 蓝图 - 概述 NIST SP 800-53 R4 蓝图 - 部署步骤

有关蓝图和如何使用这些蓝图的更多文章：

- 了解蓝图生命周期。
- 了解如何使用静态和动态参数。
- 了解如何自定义蓝图排序顺序。
- 了解如何利用蓝图资源锁定。
- 了解如何更新现有分配。

部署 NIST SP 800-53 R4 蓝图示例

2019/9/5 • • Edit Online

若要部署 Azure 蓝图 NIST SP 800-53 R4 蓝图示例，必须执行以下步骤：

- 基于示例创建新的蓝图
- 将示例副本标记为“已发布”
- 将蓝图副本分配到现有的订阅

如果没有 Azure 订阅，请在开始之前创建一个免费帐户。

基于示例创建蓝图

首先，通过使用示例作为起点在环境中创建新的蓝图，来实现蓝图示例。

1. 选择“所有服务”，然后在左窗格中搜索并选择“策略”。在“策略”页上选择“蓝图”。
2. 在左侧的“开始”页中，选择“创建蓝图”下的“创建”按钮。
3. 在“其他示例”下找到“NIST SP 800-53 R4”蓝图示例，然后选择“使用此示例”。
4. 输入该蓝图示例的“基本信息”：
   - **蓝图名称**：提供 NIST SP 800-53 R4 蓝图示例副本的名称。
   - **定义位置**：使用省略号并选择要将示例副本保存到的管理组。
5. 选择页面顶部的“项目”选项卡，或页面底部的“下一步: 项目”。
6. 查看构成蓝图示例的项目列表。许多项目包含稍后我们将要定义的参数。查看完蓝图示例后，选择“保存草稿”。

发布示例副本

现已在环境中创建蓝图示例的副本。该副本在创建后处于“草稿”模式，必须先将其发布，然后才能分配和部署它。可根据环境和需求自定义蓝图示例的副本，但这种修改可能不符合 NIST SP 800-53 控制要求。

1. 选择“所有服务”，然后在左窗格中搜索并选择“策略”。在“策略”页上选择“蓝图”。
2. 在左侧选择“蓝图定义”页。使用筛选器找到蓝图示例的副本，然后选择它。
3. 选择页面顶部的“发布蓝图”。在右侧的新窗格中，提供蓝图示例副本的**版本**。以后做出修改时，此属性非常有用。提供**更改注释**，例如，“基于 NIST SP 800-53 R4 蓝图示例发布的第一个版本”。然后选择页面底部的“发布”。

分配示例副本

成功发布蓝图示例的副本后，可将它分配到它所在的管理组中的某个订阅。在此步骤中，需提供参数来使蓝图示例副本的每个部署保持唯一。

1. 选择“所有服务”，然后在左窗格中搜索并选择“策略”。在“策略”页上选择“蓝图”。
2. 在左侧选择“蓝图定义”页。使用筛选器找到蓝图示例的副本，然后选择它。
3. 选择蓝图定义页面顶部的“分配蓝图”。
4. 提供蓝图分配的参数值：

- 基础
  - **订阅**：在蓝图示例副本所保存到的管理组中选择一个或多个订阅。如果选择多个订阅，将使用输入的参数为每个订阅创建一个分配。
  - **分配名称**：系统会根据蓝图的名称预先填充该名称。请根据需要更改该名称，或保留原样。
  - **位置**：选择要在其中创建托管标识的区域。Azure 蓝图使用此托管标识在分配的蓝图中部署所有项目。若要了解详细信息，请参阅 Azure 资源的托管标识。
  - **蓝图定义版本**：选择蓝图示例副本的已发布版本。
- 锁分配

  选择环境的蓝图锁定设置。有关更多信息，请参阅蓝图资源锁定。

- 托管标识

  保留默认的系统分配的托管标识选项。

- 项目参数

  在本部分定义的参数将应用到定义了这些参数的项目。这些参数属于动态参数，因为它们是在分配蓝图期间定义的。有关完整列表或项目参数及其说明，请参阅项目参数表 。

5. 输入所有参数后，选择页面底部的“分配”。随后将创建蓝图分配，并开始部署项目。部署过程大约需要一小时。若要检查部署状态，请打开蓝图分配。

> **WARNING**
> Azure 蓝图服务和内置蓝图示例是**免费的**。Azure 资源按产品定价 。使用定价计算器 可以估算运行此蓝图示例部署的资源所需的成本。

项目参数表

下表提供了蓝图项目参数的列表：

项目名称	项目类型	参数名称	说明
[预览]：审核 NIST SP 800-53 R4 控制措施并部署特定 VM 扩展以支持审核要求	策略分配	应为 VM 配置的 Log Analytics 工作区 ID	这是应为 VM 配置的 Log Analytics 工作区的 ID (GUID)。
[预览]：审核 NIST SP 800-53 R4 控制措施并部署特定 VM 扩展以支持审核要求	策略分配	应启用诊断日志的资源类型列表	用于审核是否未启用诊断日志设置的资源类型列表。Azure Monitor 诊断日志架构中提供了可接受的值。
[预览]：审核 NIST SP 800-53 R4 控制措施并部署特定 VM 扩展以支持审核要求	策略分配	应该从 Windows VM 管理员组中排除的用户的列表	以分号分隔的应从管理员本地组中排除的成员列表。例如：管理员；myUser1；myUser2
[预览]：审核 NIST SP 800-53 R4 控制措施并部署特定 VM 扩展以支持审核要求	策略分配	应该包括在 Windows VM 管理员组中的用户的列表	以分号分隔的应包括在管理员本地组中的成员列表。例如：管理员；myUser1；myUser2

项目名称	项目类型	参数名称	说明
[预览]:为 Linux VM 规模集(VMSS)部署 Log Analytics 代理	策略分配	Linux VM 规模集 (VMSS) 的 Log Analytics 工作区	如果此工作区超出分配范围，则必须手动将“Log Analytics 参与者”权限(或类似权限)授予策略分配的主体 ID。
[预览]:为 Linux VM 规模集(VMSS)部署 Log Analytics 代理	策略分配	可选:支持将 Linux OS 添加到范围的 VM 映像列表	可以使用空数组来表示没有可选参数:[]
[预览]:为 Linux VM 部署 Log Analytics 代理	策略分配	Linux VM 的 Log Analytics 工作区	如果此工作区超出分配范围，则必须手动将“Log Analytics 参与者”权限(或类似权限)授予策略分配的主体 ID。
[预览]:为 Linux VM 部署 Log Analytics 代理	策略分配	可选:支持将 Linux OS 添加到范围的 VM 映像列表	可以使用空数组来表示没有可选参数:[]
[预览]:为 Windows VM 规模集(VMSS)部署 Log Analytics 代理	策略分配	Windows VM 规模集 (VMSS) 的 Log Analytics 工作区	如果此工作区超出分配范围，则必须手动将“Log Analytics 参与者”权限(或类似权限)授予策略分配的主体 ID。
[预览]:为 Windows VM 规模集(VMSS)部署 Log Analytics 代理	策略分配	可选:支持将 Windows OS 添加到范围的 VM 映像列表	可以使用空数组来表示没有可选参数:[]
[预览]:为 Windows VM 部署 Log Analytics 代理	策略分配	Windows VM 的 Log Analytics 工作区	如果此工作区超出分配范围，则必须手动将“Log Analytics 参与者”权限(或类似权限)授予策略分配的主体 ID。
[预览]:为 Windows VM 部署 Log Analytics 代理	策略分配	可选:支持将 Windows OS 添加到范围的 VM 映像列表	可以使用空数组来表示没有可选参数:[]
在存储帐户上部署高级威胁防护	策略分配	效果	有关策略效果的信息，可参阅了解 Azure Policy 效果
对 SQL 服务器部署审核	策略分配	保持期的值(天数，0 表示保持期无限制)	保留天数(可选，如果未指定，则为 180 天)
对 SQL 服务器部署审核	策略分配	要进行 SQL Server 审核的存储帐户的资源组名称	审核针对 Azure 存储帐户(将在 SQL Server 所在的每个区域中创建的存储帐户，由该区域中的所有服务器共享)中审核日志的写入数据库事件。重要提示 - 为了正确地进行审核，请勿删除或重命名资源组或存储帐户。
为网络安全组部署诊断设置	策略分配	适用于网络安全组诊断的存储帐户前缀	此前缀将与网络安全组位置结合使用，一起构成已创建的存储帐户的名称。

项目名称	项目类型	参数名称	说明
为网络安全组部署诊断设置	策略分配	适用于网络安全组诊断的存储帐户的资源组名称(必须存在)	将在其中创建存储帐户的资源组。此资源组必须已存在。

后续步骤

了解 NIST SP 800-53 R4 蓝图示例的部署步骤后，请访问以下文章来了解蓝图和控制映射：

NIST SP 800-53 R4 蓝图 - 概述 NIST SP 800-53 R4 蓝图 - 控制映射

有关蓝图和如何使用这些蓝图的更多文章：

- 了解蓝图生命周期。
- 了解如何使用静态和动态参数。
- 了解如何自定义蓝图排序顺序。
- 了解如何利用蓝图资源锁定。
- 了解如何更新现有分配。

PCI-DSS v3.2.1 蓝图示例概述

2019/9/4 • • Edit Online

PCI-DSS v3.2.1 蓝图示例是一组帮助实现 PCI-DSS v3.2.1 合规性的策略。此蓝图可帮助客户治理带有 PCI-DSS 工作负荷且基于云的环境。PCI-DSS 蓝图为 Azure 部署的任何需要此认证的体系结构部署一组核心策略。

控制映射

控件映射部分提供了有关包含在此计划内的策略的详细信息，以及这些策略如何帮助满足由 PCI-DSS v3.2.1 定义的各种控制要求。分配给一个体系结构时，资源由 Azure Policy 评估是否不符合已分配的策略。

分配此蓝图后，请在 Azure Policy 合规性仪表板中查看Azure 环境合规性级别。

后续步骤

你已查看了 PCI-DSS v3.2.1 蓝图示例概述。接下来，请访问以下文章，了解控制映射以及如何部署此示例：

PCI-DSS v3.2.1 蓝图 - 控制映射 PCI-DSS v3.2.1 蓝图 - 部署步骤

有关蓝图和如何使用这些蓝图的更多文章：

- 了解蓝图生命周期。
- 了解如何使用静态和动态参数。
- 了解如何自定义蓝图排序顺序。
- 了解如何利用蓝图资源锁定。
- 了解如何更新现有分配。

控制 PCI DSS v 3.2.1 蓝图示例的映射

2019/9/4 • • Edit Online

下面的文章详细介绍了如何将 Azure 蓝图-DSS v2.0 蓝图示例映射到 PCI-DSS 伏特版控制。有关控件的详细信息，请参阅PCI-DSSv2.0。

以下映射适用于**PCI-DSS v 3.2.1: 2018**控件。使用右侧的导航栏可直接跳转到特定的控制映射。许多的映射控制措施都是使用 Azure Policy 计划实施的。若要查看完整计划，请在 Azure 门户中打开"策略"，并选择"定义"页。然后，查找并选择 **[预览版] audit pci-x 3.2.1: 2018 控件并部署特定的 VM 扩展，以支持审核要求**内置策略计划。

1.3.2 和1.3.4 边界保护

此蓝图通过分配用于监视具有可许可规则的网络安全组的Azure 策略定义，帮助你管理和控制网络。过于宽松的规则可能会允许意外的网络访问，应该对其进行评审。此蓝图分配一个 Azure 策略定义，用于监视未受保护的终结点、应用程序和存储帐户。不受防火墙保护的终结点和应用程序，以及具有无限制访问权限的存储帐户，可能会允许意外访问信息系统中包含的信息。

- 审核对存储帐户的不受限的网络访问
- 应该限制通过面向 Internet 的终结点进行访问

3.4. a、4.1、4.1. g、4.1 和6.5.3 加密保护

此蓝图通过分配Azure 策略定义 (强制执行特定的如何控件并审核弱加密设置的使用)，帮助你通过使用如何控件来强制实施策略。了解 Azure 资源中的哪些位置采用欠佳的加密配置有助于采取纠正措施，以确保根据信息安全策略配置资源。具体而言，此蓝图分配的策略需要对 SQL 数据库进行透明数据加密;审核存储帐户和自动化帐户变量上缺少加密。此外，还提供了用于处理与存储帐户、Function Apps、WebApp、API 应用和 Redis 缓存的不安全连接的策略，以及审核未加密 Service Fabric 通信。

- 应该只能通过 HTTPS 访问函数应用
- 只能通过 HTTPS 访问 Web 应用程序
- 只能通过 HTTPS 访问 API 应用
- 应在 SQL 数据库上启用透明数据加密
- 应在虚拟机上启用磁盘加密
- 自动化帐户变量应进行加密
- 应该启用只能通过安全方式连接到 Redis 缓存
- 应该启用安全传输到存储帐户
- Service Fabric 群集应将 ClusterProtectionLevel 属性设置为 EncryptAndSign
- 应在 SQL 数据库上启用透明数据加密
- 部署 SQL DB 透明数据加密

5.1、6.2、6.6 和11.2.1 漏洞扫描和系统更新

此蓝图通过分配用于监视 Azure 中缺少系统更新、操作系统漏洞、SQL 漏洞和虚拟机漏洞的Azure 策略定义，帮助你管理信息系统漏洞安全中心。Azure 安全中心提供报告功能，使你能够实时洞察已部署的 Azure 资源的安全状态。

- 监视 Azure 安全中心 Endpoint Protection 的缺失情况
- 为 Windows Server 部署默认 Microsoft IaaSAntimalware 扩展
- 在 SQL Server 上部署威胁检测

- 应在计算机上安装系统更新
- 应该修复计算机上安全配置中的漏洞
- 应该修复 SQL 数据库中的漏洞
- 应该通过漏洞评估解决方案修复漏洞

7.1.1. 7.1.2 和7.1.3 的职责分离

仅分配一个 Azure 订阅所有者并不能实现管理冗余。相反，分配过多的 Azure 订阅所有者会增大违规的可能性，因为会有更多的所有者帐户可能会泄密。此蓝图可帮助你维护合适数量的 Azure 订阅所有者，方法是分配Azure 策略定义，用于审核 azure 订阅的所有者数量。管理订阅所有者权限有助于实现适当的职责分离。

- 应该为你的订阅分配了多个所有者
- 只多只为订阅指定 3 个所有者

3.2、7.2.1、8.3.1 和8.3.1 管理特权访问权限

此蓝图通过以下方式来帮助你限制和控制特权访问权限: 将Azure 策略定义分配给审核外部帐户，其中所有者、写入和/或读取权限以及具有不具有的所有者和/或写入权限的员工帐户已启用多重身份验证。Azure 实施基于角色的访问控制 (RBAC) 来管理谁有权访问 Azure 资源。了解实施自定义 RBAC 规则的位置有助于验证需求以及实施是否适当，因为自定义 RBAC 规则容易出错。此蓝图还会分配Azure 策略定义，以审核对 SQL server Azure Active Directory 身份验证的使用。使用 Azure Active Directory 身份验证可简化权限管理，并集中管理数据库用户和其他 Microsoft
服务器.

- 应从订阅中删除拥有所有者权限的外部帐户
- 应从订阅中删除具有写入权限的外部帐户
- 应从订阅中删除拥有读取权限的外部帐户
- 应在对订阅拥有所有者权限的帐户上启用 MFA
- 应为 MFA 启用对订阅具有写入权限的帐户
- 应在对订阅拥有读取权限的帐户上启用 MFA
- 应该为 SQL 服务器预配 Azure Active Directory 管理员
- 审核自定义 RBAC 规则的使用

8.1.2 和8.1.5 最小权限和用户访问权限检查

Azure 实施基于角色的访问控制 (RBAC)，以帮助你管理哪些用户有权访问 Azure 中的资源。使用 Azure 门户可以评审有权访问 Azure 资源的用户及其权限。此蓝图将Azure 策略定义分配到审核帐户，这些帐户应优先排序，包括具有提升权限的帐户和外部帐户。

- 应从订阅中删除弃用的帐户
- 应从订阅中删除拥有所有者权限的已弃用帐户
- 应从订阅中删除拥有所有者权限的外部帐户
- 应从订阅中删除具有写入权限的外部帐户
- 应从订阅中删除拥有读取权限的外部帐户

8.1.3 删除或调整访问权限

Azure 实施基于角色的访问控制 (RBAC)，以帮助你管理哪些用户有权访问 Azure 中的资源。使用 Azure Active Directory 和 RBAC，可以更新用户角色以反映组织更改。如果需要，可以阻止帐户登录(或将其删除)，这会立即删除其 Azure 资源访问权限。此蓝图将Azure 策略定义分配给审核折旧帐户，以便删除。

- 应从订阅中删除弃用的帐户
- 应从订阅中删除拥有所有者权限的已弃用帐户

8.2.3, b, 8.2.4, b 和8.2.5 基于密码的身份验证

此蓝图通过分配Azure 策略定义来帮助你强制实施强密码, 这些策略定义用于审核不强制实施最低强度的 Windows vm 和其他密码要求。识别违反密码强度策略的 VM 有助于采取纠正措施，以确保所有 VM 用户帐户的密码符合策略。

- [预览]: 审核未将最长密码期限设为 70 天的 Windows VM
- [预览]: 部署要求以审核未将最长密码期限设为 70 天的 Windows VM
- [预览]: 审核未将最短密码长度限制为 14 个字符的 Windows VM
- [预览]: 部署要求以审核未将最短密码长度限制为 14 个字符的 Windows VM
- [预览]: 审核允许重用之前的 24 个密码的 Windows VM
- [预览]: 部署要求以审核允许重用之前的 24 个密码的 Windows VM

10.3 和10.5.4 审核生成

此蓝图通过分配 Azure Policy 定义来帮助确保记录系统事件，这些定义用于审核在 Azure 资源上的日志设置。诊断日志针对 Azure 资源中执行的操作提供见解。Azure 日志依赖于同步的内部时钟创建各个资源中事件的时间相关记录。

- 应在 SQL Server 的高级数据安全设置上启用审核
- 审核诊断设置
- 审核 SQL 服务器级别审核设置
- 在 SQL Server 上部署审核
- 应将存储帐户迁移到新的 Azure 资源管理器资源
- 应将虚拟机迁移到新的 Azure 资源管理器资源

12.3.6 和12.3.7 信息安全性

此蓝图可帮助你管理和控制网络, 方法是分配审核可接受网络位置和环境允许的已批准公司产品的Azure 策略定义。每个公司通过其中每个策略中的策略参数可自定义这些设置。

- 允许的位置
- 资源组允许的位置

后续步骤

现在, 你已查看了 PCI-DSS v1.0 蓝图的控件映射, 请访问以下文章了解概述以及如何部署此示例:

Pci-dss v2.0 3.2.1 蓝图-概述 PCI-dss v2.0 蓝图-部署步骤

有关蓝图和如何使用这些蓝图的更多文章:

- 了解蓝图生命周期。
- 了解如何使用静态和动态参数。
- 了解如何自定义蓝图排序顺序。
- 了解如何利用蓝图资源锁定。
- 了解如何更新现有分配。

部署 PCI-X 3.2.1 蓝图蓝图示例

2019/9/4 • • Edit Online

若要部署 Azure 蓝图 pci-e pci-e 蓝图示例, 必须执行以下步骤:

- 基于示例创建新的蓝图
- 将示例副本标记为"已发布"
- 将蓝图副本分配到现有的订阅

如果没有 Azure 订阅，请在开始之前创建一个免费帐户。

基于示例创建蓝图

首先，通过使用示例作为起点在环境中创建新的蓝图，来实现蓝图示例。

1. 选择"所有服务"，然后在左窗格中搜索并选择"策略"。在"策略"页上选择"蓝图"。
2. 在左侧的"开始"页中，选择"创建蓝图"下的"创建"按钮。
3. 在_其他示例_下, 找到**PCI-DSS v 3.2.1**蓝图示例, 然后选择 "**使用此示例**"。
4. 输入该蓝图示例的"基本信息":
   - **蓝图名称**:提供 PCI-DSS v2.0 蓝图蓝图示例的副本名称。
   - **定义位置**:使用省略号并选择要将示例副本保存到的管理组。
5. 选择页面顶部的"项目"选项卡，或页面底部的"下一步:项目"。
6. 查看构成蓝图示例的项目列表。许多项目包含稍后我们将要定义的参数。查看完蓝图示例后，选择"保存草稿"。

发布示例副本

现已在环境中创建蓝图示例的副本。该副本在创建后处于"草稿"模式，必须先将其发布，然后才能分配和部署它。可以根据您的环境和需要自定义蓝图示例的副本, 但修改后可以将其移出 PCI-DSS v 3.2.1 标准版。

1. 选择"所有服务"，然后在左窗格中搜索并选择"策略"。在"策略"页上选择"蓝图"。
2. 在左侧选择"蓝图定义"页。使用筛选器找到蓝图示例的副本，然后选择它。
3. 选择页面顶部的"发布蓝图"。在右侧的新窗格中，提供蓝图示例副本的**版本**。以后做出修改时，此属性非常有用。提供如 "从 PCI-DSS v2.0 蓝图蓝图发布的第一个版本" 之类的**更改说明**。然后选择页面底部的"发布"。

分配示例副本

成功发布蓝图示例的副本后，可将它分配到它所在的管理组中的某个订阅。在此步骤中，需提供参数来使蓝图示例副本的每个部署保持唯一。

1. 选择"所有服务"，然后在左窗格中搜索并选择"策略"。在"策略"页上选择"蓝图"。
2. 在左侧选择"蓝图定义"页。使用筛选器找到蓝图示例的副本，然后选择它。
3. 选择蓝图定义页面顶部的"分配蓝图"。
4. 提供蓝图分配的参数值:

- 基本
  - **订阅**：在蓝图示例副本所保存到的管理组中选择一个或多个订阅。如果选择多个订阅，将使用输入的参数为每个订阅创建一个分配。
  - **分配名称**：系统会根据蓝图的名称预先填充该名称。请根据需要更改该名称，或保留原样。
  - **位置**：选择要在其中创建托管标识的区域。Azure 蓝图使用此托管标识在分配的蓝图中部署所有项目。若要了解详细信息，请参阅 Azure 资源的托管标识。
  - **蓝图定义版本**：选择蓝图示例副本的已发布版本。
- 锁定分配

  选择环境的蓝图锁定设置。有关更多信息，请参阅蓝图资源锁定。

- 托管标识

  保留默认的系统分配的托管标识选项。

- 项目参数

  在本部分定义的参数将应用到定义了这些参数的项目。这些参数属于动态参数，因为它们是在分配蓝图期间定义的。有关完整列表或项目参数及其说明，请参阅项目参数表 。

5. 输入所有参数后，选择页面底部的“分配”。随后将创建蓝图分配，并开始部署项目。部署过程大约需要一小时。若要检查部署状态，请打开蓝图分配。

> **WARNING**
> Azure 蓝图服务和内置蓝图示例是**免费的**。Azure 资源按产品定价 。使用定价计算器 可以估算运行此蓝图示例部署的资源所需的成本。

项目参数表

下表提供了蓝图项目参数的列表：

项目名称	项目类型	参数名称	描述
[预览版] audit pci-x 3.2.1:2018 控制和部署特定 VM 扩展以支持审核要求	策略分配	资源类型列表	所选资源类型的审核诊断设置。默认值为 "所有资源"
允许的位置	策略分配	允许的位置列表	允许部署到其中的任何资源的数据中心位置的列表。此列表可在全球范围内自定义到所需的 Azure 位置。选择要允许的位置。
允许的资源组位置	策略分配	允许的位置	此策略使你能够限制你的组织可在中创建资源组的位置。用于强制执行异地符合性要求。
在 SQL Server 上部署审核	策略分配	保留天数	数据保留，单位为天。默认值为 180，但 PCI 需要365。

项目名称	项目类型	参数名称	描述
在 SQL Server 上部署审核	策略分配	存储帐户的资源组名称	审核针对 Azure 存储帐户（将在 SQL Server 所在的每个区域中创建的存储帐户，由该区域中的所有服务器共享）中审核日志的写入数据库事件。

后续步骤

现在，你已经查看了用于部署 PCI-X 3.2.1 蓝图蓝图示例的步骤，接下来请访问以下文章来了解概述和控件映射：

Pci-dss v2.0 3.2.1 蓝图-概述 PCI-dss v2.0 蓝图-控件映射

有关蓝图和如何使用这些蓝图的更多文章：

- 了解蓝图生命周期。
- 了解如何使用静态和动态参数。
- 了解如何自定义蓝图排序顺序。
- 了解如何利用蓝图资源锁定。
- 了解如何更新现有分配。

英国官方和英国 NHS 蓝图示例的概述

2019/9/4 • • Edit Online

英国官方和英国 NHS 蓝图示例提供了一组监管防护措施，这些措施使用 Azure Policy 来帮助用户通过英国官方和英国 NHS 认证。这些蓝图示例可帮助客户为 Azure 部署的任何需要符合英国官方和英国 NHS 框架或通过其认证的体系结构部署一组核心策略。

控制映射

控件映射部分提供了有关包含在此计划内的策略的详细信息，以及这些策略如何帮助满足由英国官方和英国 NHS 框架定义的各种控制要求。分配给一个体系结构时，资源由 Azure Policy 评估是否不符合已分配的策略。有关详细信息，请参阅 Azure Policy。

后续步骤

你已查看了英国官方和英国 NHS 蓝图示例的概述和体系结构。接下来，请访问以下文章，了解控制映射以及如何部署此示例：

英国官方和英国 NHS 蓝图 - 控制映射 英国官方和英国 NHS 蓝图 - 部署步骤

有关蓝图和如何使用这些蓝图的更多文章：

- 了解蓝图生命周期。
- 了解如何使用静态和动态参数。
- 了解如何自定义蓝图排序顺序。
- 了解如何利用蓝图资源锁定。
- 了解如何更新现有分配。

控制英国官方和英国 NHS 蓝图示例的映射

2019/8/26 • • Edit Online

以下文章详细介绍了英国官方和英国 NHS 蓝图示例如何映射到英国官方和英国 NHS 控件。有关控件的详细信息, 请参阅UK 官方。

以下映射适用于英国官方和英国 NHS控件。使用右侧的导航栏可直接跳转到特定的控制映射。许多的映射控制措施都是使用 Azure Policy 计划实施的。若要查看完整计划, 请在 Azure 门户中打开"策略", 并选择"定义"页。然后, 找到并选择 " [预览]审核 UK 官方和英国 NHS 控件并部署特定的 VM 扩展", 以支持审核要求内置策略计划。

1传输防护中的数据

该蓝图通过分配用于审核与存储帐户和 Redis 缓存的不安全连接的Azure 策略定义, 帮助确保信息通过 azure 服务进行传输。

- 只应启用与 Redis 缓存的安全连接
- 应该启用安全传输到存储帐户

2.3 静态数据保护

此蓝图通过分配Azure 策略定义 (强制执行特定的如何控件并审核弱加密设置的使用), 帮助你在使用如何控件时执行策略。了解 Azure 资源中的哪些位置采用欠佳的加密配置有助于采取纠正措施, 以确保根据信息安全策略配置资源。具体而言, 此蓝图分配的策略需要 data lake 存储帐户的加密;需要对 SQL 数据库进行透明数据加密;审核存储帐户、SQL 数据库、虚拟机磁盘和自动化帐户变量上缺少的加密;审核到存储帐户和 Redis 缓存的不安全连接;审核弱虚拟机密码加密;和审核未加密 Service Fabric 通信。

- 在 Azure 安全中心监视未加密的 SQL 数据库
- 应在虚拟机上应用磁盘加密
- 自动化帐户变量应进行加密
- 应该启用安全传输到存储帐户
- Service Fabric 群集应将 ClusterProtectionLevel 属性设置为 EncryptAndSign
- 应启用 SQL 数据库上的透明数据加密
- 部署 SQL DB 透明数据加密
- Data Lake Store 帐户上需要加密
- 允许的位置 (已硬编码为 "英国南部" 和 "英国西部")
- 允许的资源组位置 (已硬编码为 "英国南部" 和 "英国西部")

5.2 漏洞管理

此蓝图通过分配用于监视缺少的 endpoint protection、缺少系统更新、操作系统漏洞、SQL 漏洞和虚拟的Azure 策略定义, 帮助你管理信息系统漏洞计算机漏洞。这些见解提供有关已部署资源的安全状态的实时信息, 可帮助你指定补救措施的优先级。

- 监视 Azure 安全中心 Endpoint Protection 的缺失情况
- 应在计算机上安装系统更新
- 应修复计算机上安全配置中的漏洞
- 应修正 SQL 数据库上的漏洞
- 应通过漏洞评估解决方案修复漏洞

5.3 保护性监视

此蓝图通过分配Azure 策略定义来帮助保护信息系统资产，这些策略定义针对无限制访问、白名单活动和威胁提供保护性监视。

- 审核对存储帐户的不受限的网络访问
- 应在虚拟机上启用自适应应用程序控件
- 在 SQL 服务器上部署威胁检测
- 为 Windows Server 部署默认的 Microsoft IaaS 反恶意软件扩展

9保护用户管理/10 身份验证和身份验证

Azure 实施基于角色的访问控制 (RBAC)，以帮助你管理哪些用户有权访问 Azure 中的资源。使用 Azure 门户可以评审有权访问 Azure 资源的用户及其权限。此蓝图通过以下方法来限制和控制访问权限：向所有者和/或读/写权限指定所有者和/或读/写权限的外部帐户，并使用具有不具有多重身份的 "读取" 和/或 "写入" 权限的帐户身份验证已启用。

- 应在订阅上拥有所有者权限的帐户上启用 MFA
- 应为 MFA 启用对订阅具有写入权限的帐户
- 应在对订阅拥有读取权限的帐户上启用 MFA
- 应从订阅中删除具有所有者权限的外部帐户
- 应从订阅中删除具有写入权限的外部帐户
- 应从订阅中删除具有读取权限的外部帐户

此蓝图分配 Azure 策略定义，以审核对 SQL server 和 Service Fabric 的 Azure Active Directory 身份验证的使用。使用 Azure Active Directory 身份验证可以简化权限管理，以及集中化数据库用户和其他 Microsoft 服务的标识管理。

- 应为 SQL server 设置 Azure Active Directory 管理员
- Service Fabric 群集应仅使用 Azure Active Directory 进行客户端身份验证

此蓝图还会将 Azure 策略定义分配给审核帐户，这些帐户应优先考虑，包括折旧帐户和外部帐户。如果需要，可以阻止帐户登录（或将其删除），这会立即删除其 Azure 资源访问权限。此蓝图将两个 Azure 策略定义分配给审核折旧帐户，以便删除。

- 应从订阅中删除弃用的帐户
- 应从订阅中删除不推荐使用的具有所有者权限的帐户
- 应从订阅中删除具有所有者权限的外部帐户
- 应从订阅中删除具有写入权限的外部帐户

此蓝图还会分配一个 Azure 策略定义，用于审核 Linux VM 密码文件权限，以在设置不正确时进行警报。此设计使你可以采取纠正措施以确保验证器不会受到侵害。

- [预览]：Audit Linux VM/etc/passwd 文件权限设置为0644

此蓝图通过分配 Azure 策略定义来帮助你强制实施强密码，这些策略定义用于审核不强制实施最低强度的 Windows Vm 和其他密码要求。识别违反密码强度策略的 VM 有助于采取纠正措施，以确保所有 VM 用户帐户的密码符合策略。

- [预览]：部署要求以审核未启用密码复杂性设置的 Windows Vm
- [预览]：部署要求，以审核不具有最长密码期限70天的 Windows Vm
- [预览]：部署要求，以审核不具有最短密码期限1天的 Windows Vm
- [预览]：部署要求以审核不将最短密码长度限制为14个字符的 Windows Vm
- [预览]：部署用于审核 Windows Vm 的要求，这些虚拟机允许重复使用以前的24个密码

- [预览]: 审核未启用密码复杂性设置的 Windows Vm
- [预览]: 审核未使用最长密码期限70天的 Windows Vm
- [预览]: 审核未使用最短密码期限为1天的 Windows Vm
- [预览]: 审核不将最短密码长度限制为14个字符的 Windows Vm
- [预览]: 审核允许重复使用以前24密码的 Windows Vm

此蓝图还有助于通过分配 Azure 策略定义来控制对 Azure 资源的访问。这些策略将审核可能允许更高资源访问权限的资源类型和配置的使用。了解违反这些策略的资源有助于采取纠正措施来确保仅限已授权的用户访问 Azure 资源。

- [预览]: 部署要求以审核具有无密码帐户的 Linux Vm
- [预览]: 部署要求以审核 Linux Vm, 这些 Vm 允许无密码的帐户进行远程连接
- [预览]: 审核帐户没有密码的 Linux Vm
- [预览]: 审核 Linux Vm, 允许无密码的帐户进行远程连接
- 应将存储帐户迁移到新的 Azure 资源管理器资源
- 应将虚拟机迁移到新的 Azure 资源管理器资源
- 审核不使用托管磁盘的 VM

11外部接口保护

除了为适当的安全用户管理使用超过25个策略之外, 此蓝图还有助于通过分配用于监视不受限制的存储帐户的Azure 策略定义, 来保护服务接口免受未经授权的访问。具有不受限制访问权限的存储帐户可允许对信息系统中包含的信息进行意外访问。此蓝图还会分配一个策略, 该策略启用虚拟机上的自适应应用程序控制。

- 审核对存储帐户的不受限的网络访问
- 应在虚拟机上启用自适应应用程序控件

12安全服务管理

Azure 实施基于角色的访问控制 (RBAC), 以帮助你管理哪些用户有权访问 Azure 中的资源。使用 Azure 门户可以评审有权访问 Azure 资源的用户及其权限。此蓝图通过以下方法来帮助你限制和控制特权访问权限: 分配5个Azure 策略定义, 以审核具有所有者和/或写入权限的外部帐户, 以及拥有所有者和/或写入权限的具有以下权限的帐户:已启用多重身份验证。

用于云服务管理的系统将具有高特权来访问该服务。其泄露将产生重大影响，包括绕过安全控制、窃取或操纵大量数据的手段。服务提供商管理员用于管理操作服务的方法应设计为缓解可能破坏服务安全的任何攻击风险。如果未实现此原则, 攻击者可能会绕过安全控制并盗取或处理大量数据。

- 应在订阅上拥有所有者权限的帐户上启用 MFA
- 应为 MFA 启用对订阅具有写入权限的帐户
- 应从订阅中删除具有所有者权限的外部帐户
- 应从订阅中删除具有写入权限的外部帐户

此蓝图分配 Azure 策略定义, 以审核对 SQL server 和 Service Fabric 的 Azure Active Directory 身份验证的使用。使用 Azure Active Directory 身份验证可以简化权限管理，以及集中化数据库用户和其他 Microsoft 服务的标识管理。

- 应为 SQL server 设置 Azure Active Directory 管理员
- Service Fabric 群集应仅使用 Azure Active Directory 进行客户端身份验证

此蓝图还会将 Azure 策略定义分配给审核帐户, 这些帐户应优先排序, 包括具有提升权限的帐户和外部帐户。如果需要，可以阻止帐户登录(或将其删除)，这会立即删除其 Azure 资源访问权限。此蓝图将两个 Azure 策略定义分配给审核折旧帐户, 以便删除。

- 应从订阅中删除弃用的帐户
- 应从订阅中删除不推荐使用的具有所有者权限的帐户
- 应从订阅中删除具有所有者权限的外部帐户
- 应从订阅中删除具有写入权限的外部帐户

此蓝图还会分配一个 Azure 策略定义，用于审核 Linux VM 密码文件权限，以在设置不正确时进行警报。此设计使你可以采取纠正措施以确保验证器不会受到侵害。

- [预览]：Audit Linux VM/etc/passwd 文件权限设置为0644

13个用户的审核信息

此蓝图可帮助你确保通过分配审核 Azure 资源上的日志设置的Azure 策略定义来记录系统事件。分配的策略还会审核虚拟机是否不向指定的 Log Analytics 工作区发送日志。

- 监视 Azure 安全中心中的未经审核 SQL server
- 审核诊断设置
- 审核 SQL 服务器级别审核设置
- [预览]：为 Linux VM 部署 Log Analytics 代理
- [预览]：为 Windows VM 部署 Log Analytics 代理
- 创建虚拟网络时部署网络观察程序

后续步骤

现在，你已经查看了英国官方和英国 NHS 蓝图的控件映射，接下来请访问以下文章来了解概述以及如何部署此示例：

英国官方和英国 NHS 蓝图-概述 英国官方和英国 NHS 蓝图-部署步骤

有关蓝图和如何使用这些蓝图的更多文章：

- 了解蓝图生命周期。
- 了解如何使用静态和动态参数。
- 了解如何自定义蓝图排序顺序。
- 了解如何利用蓝图资源锁定。
- 了解如何更新现有分配。

部署英国官方和英国 NHS 蓝图示例

2019/9/4 • • Edit Online

若要部署英国官方和英国 NHS 蓝图示例，必须执行以下步骤：

- 基于示例创建新的蓝图
- 将示例副本标记为“已发布”
- 将蓝图副本分配到现有的订阅

如果没有 Azure 订阅，请在开始之前创建一个免费帐户。

基于示例创建蓝图

首先，通过使用示例作为起点在环境中创建新的蓝图，来实现蓝图示例。

1. 选择“所有服务”，然后在左窗格中搜索并选择“策略”。在“策略”页上选择“蓝图”。
2. 在左侧的“开始”页中，选择“创建蓝图”下的“创建”按钮。
3. 在_其他示例_中查找**英国官方或英国 NHS**蓝图示例，然后选择 "**使用此示例**"。
4. 输入该蓝图示例的“基本信息”：
   - **蓝图名称**：提供蓝图示例副本的名称。
   - **定义位置**：使用省略号并选择要将示例副本保存到的管理组。
5. 选择页面顶部的“项目”选项卡，或页面底部的“下一步:项目”。
6. 查看构成蓝图示例的项目列表。许多项目包含稍后我们将要定义的参数。查看完蓝图示例后，选择“保存草稿”。

发布示例副本

现已在环境中创建蓝图示例的副本。该副本在创建后处于“草稿”模式，必须先将其发布，然后才能分配和部署它。可以根据您的环境和需要自定义蓝图示例的副本，但这种修改可能会远离标准版本。

1. 选择“所有服务”，然后在左窗格中搜索并选择“策略”。在“策略”页上选择“蓝图”。
2. 在左侧选择“蓝图定义”页。使用筛选器找到蓝图示例的副本，然后选择它。
3. 选择页面顶部的“发布蓝图”。在右侧的新窗格中，提供蓝图示例副本的**版本**。以后做出修改时，此属性非常有用。提供如 "从英国官方或英国 NHS 蓝图示例发布的第一个版本" 之类的**更改注释**。然后选择页面底部的“发布”。

分配示例副本

成功发布蓝图示例的副本后，可将它分配到它所在的管理组中的某个订阅。在此步骤中，需提供参数来使蓝图示例副本的每个部署保持唯一。

1. 选择“所有服务”，然后在左窗格中搜索并选择“策略”。在“策略”页上选择“蓝图”。
2. 在左侧选择“蓝图定义”页。使用筛选器找到蓝图示例的副本，然后选择它。
3. 选择蓝图定义页面顶部的“分配蓝图”。
4. 提供蓝图分配的参数值：

- 基本
  - **订阅**：在蓝图示例副本所保存到的管理组中选择一个或多个订阅。如果选择多个订阅，将使用输入的参数为每个订阅创建一个分配。
  - **分配名称**：系统会根据蓝图的名称预先填充该名称。请根据需要更改该名称，或保留原样。
  - **位置**：选择要在其中创建托管标识的区域。Azure 蓝图使用此托管标识在分配的蓝图中部署所有项目。若要了解详细信息，请参阅 Azure 资源的托管标识。
  - **蓝图定义版本**：选择蓝图示例副本的已发布版本。
- 锁定分配

  选择环境的蓝图锁定设置。有关更多信息，请参阅蓝图资源锁定。

- 托管标识

  保留默认的系统分配的托管标识选项。

- 项目参数

  在本部分定义的参数将应用到定义了这些参数的项目。这些参数属于动态参数，因为它们是在分配蓝图期间定义的。有关完整列表或项目参数及其说明，请参阅项目参数表 。

5. 输入所有参数后，选择页面底部的“分配”。随后将创建蓝图分配，并开始部署项目。部署过程大约需要一小时。若要检查部署状态，请打开蓝图分配。

> **WARNING**
> Azure 蓝图服务和内置蓝图示例是**免费的**。Azure 资源按产品定价 。使用定价计算器 可以估算运行此蓝图示例部署的资源所需的成本。

项目参数表

下表提供了蓝图项目参数的列表：

项目名称	项目类型	参数名称	描述
英国官方或英国 NHS 蓝图计划	策略分配	用于审核诊断日志的资源类型 (策略:英国官方或英国 NHS 蓝图计划	"诊断日志" 设置为 "已启用" 时要审核的资源类型的列表。有关可接受的值，请参阅Azure 诊断日志支持的服务、架构和类别。
[预览]：为 Linux VM 部署 Log Analytics 代理	策略分配	可选：支持添加到作用域的 Linux OS 的 VM 映像列表 (策略:[预览]：部署适用于 Linux Vm 的 Log Analytics 代理)	可有可无默认值为_none_。有关详细信息，请参阅在 Azure 门户中创建 Log Analytics 工作区。
[预览]：为 Windows VM 部署 Log Analytics 代理	策略分配	可选：支持添加到作用域的 Windows OS 的 VM 映像列表 (策略:[预览]：部署适用于 Windows Vm 的 Log Analytics 代理)	可有可无默认值为_none_。有关详细信息，请参阅在 Azure 门户中创建 Log Analytics 工作区。

后续步骤

现在，你已查看部署英国官方和英国 NHS 蓝图示例的步骤，请访问以下文章了解概述和控件映射：

英国官方和英国 NHS 蓝图-概述 英国官方和英国 NHS 蓝图-控件映射

有关蓝图和如何使用这些蓝图的更多文章：

- 了解蓝图生命周期。
- 了解如何使用静态和动态参数。
- 了解如何自定义蓝图排序顺序。
- 了解如何利用蓝图资源锁定。
- 了解如何更新现有分配。

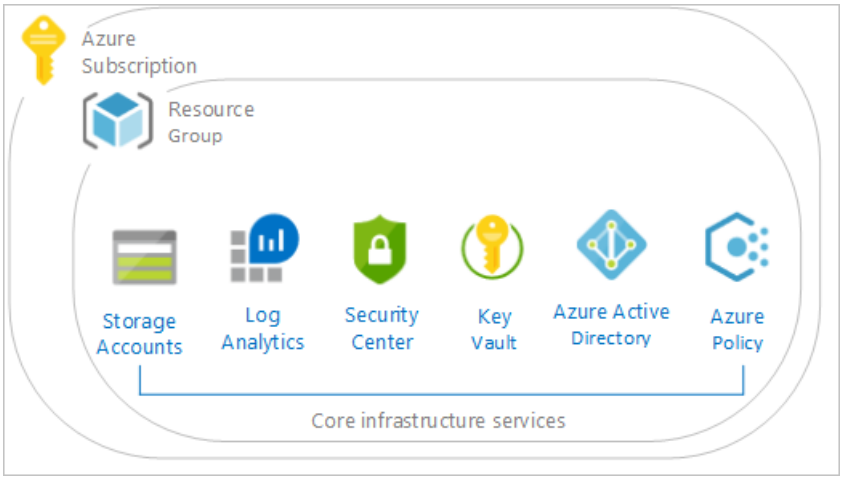
适用于 Azure 的 Microsoft 云采用框架基础蓝图示例概述

2019/9/4 • • Edit Online

适用于 Azure 的 Microsoft 云采用框架 (CAF) 基础蓝图部署了你的第一个生产级别 Azure 应用程序所需的一组核心基础结构资源和策略控制。此基础蓝图基于在 CAF 中找到的建议模式。

体系结构

CAF 基础蓝图示例在 Azure 中部署建议的基础结构资源，这些资源可供组织用来将管理其云资产所需的基础控制实施到位。此示例将部署并强制实施资源、策略和模板，从而使组织能够自信地开始使用 Azure。



此实现纳入多项 Azure 服务，这些服务用于提供安全的、全面受监视的、面向企业的基础。此环境包括：

- 一个 Azure Key Vault 实例，用于托管对共享服务环境中部署的 VM 使用的机密
- 部署 Log Analytics，以便确保从开始安全部署起所有操作和服务都记录到一个中心位置的存储帐户，用于诊断日志记录
- 部署 Azure 安全中心（标准版），从而为已迁移的工作负荷提供威胁防护
- 该蓝图还定义并部署 Azure 策略，用于
  - 应用于资源组的标记功能 (CostCenter)
  - 使用 CostCenter 标记追加资源组中的资源
  - 资源和资源组允许的 Azure 区域
  - 允许的存储帐户 SKU（在部署时选择）
  - 允许的 Azure VM SKU（在部署时选择）
  - 要求部署网络监视
  - 要求 Azure 存储帐户安全传输加密
  - 拒绝资源类型（在部署时选择）
- 计划
  - 在 Azure 安全中心启用监视（89 个策略）

所有这些元素遵守 Azure 体系结构中心 - 参考体系结构中发布的行之有效的做法。

> **NOTE**
> CAF 基础布设了用于工作负荷的基础体系结构。你仍需要部署此基础体系结构后面的工作负荷。

有关详细信息，请参阅适用于 Azure 的 Microsoft 云采用框架 - 就绪。

后续步骤

你已查看了 CAF 基础蓝图示例的概述和体系结构。

CAF 基础蓝图 - 部署步骤

有关蓝图和如何使用这些蓝图的更多文章：

- 了解蓝图生命周期。
- 了解如何使用静态和动态参数。
- 了解如何自定义蓝图排序顺序。
- 了解如何利用蓝图资源锁定。
- 了解如何更新现有分配。

部署适用于 Azure 的 Microsoft 云采用框架基础蓝图示例

2019/9/5 • • Edit Online

若要部署适用于 Azure 的 Microsoft 云采用框架 (CAF) 基础蓝图示例，必须执行以下步骤：

- 基于示例创建新的蓝图
- 将示例副本标记为“已发布”
- 将蓝图副本分配到现有的订阅

如果没有 Azure 订阅，请在开始之前创建一个免费帐户。

基于示例创建蓝图

首先，通过使用示例作为起点在环境中创建新的蓝图，来实现蓝图示例。

1. 选择“所有服务”，然后在左窗格中搜索并选择“策略”。在“策略”页上选择“蓝图”。
2. 在左侧的“开始”页中，选择“创建蓝图”下的“创建”按钮。
3. 在“其他示例”下找到“CAF 基础”蓝图示例，然后选择“使用此示例”。
4. 输入该蓝图示例的“基本信息”：
   - **蓝图名称**：提供“CAF 基础”蓝图示例副本的名称。
   - **定义位置**：使用省略号并选择要将示例副本保存到的管理组。
5. 选择页面顶部的“项目”选项卡，或页面底部的“下一步: 项目”。
6. 查看构成蓝图示例的项目列表。许多项目包含稍后我们将要定义的参数。查看完蓝图示例后，选择“保存草稿”。

发布示例副本

现已在环境中创建蓝图示例的副本。该副本在创建后处于“草稿”模式，必须先将其发布，然后才能分配和部署它。可根据环境和需求自定义蓝图示例的副本，但这种修改可能会使该副本偏离 CAF 基础蓝图。

1. 选择“所有服务”，然后在左窗格中搜索并选择“策略”。在“策略”页上选择“蓝图”。
2. 在左侧选择“蓝图定义”页。使用筛选器找到蓝图示例的副本，然后选择它。
3. 选择页面顶部的“发布蓝图”。在右侧的新窗格中，提供蓝图示例副本的**版本**。以后做出修改时，此属性非常有用。提供**更改注释**，例如，“基于 CAF 基础蓝图示例发布的第一个版本”。然后选择页面底部的“发布”。

分配示例副本

成功发布蓝图示例的副本后，可将它分配到它所在的管理组中的某个订阅。在此步骤中，需提供参数来使蓝图示例副本的每个部署保持唯一。

1. 选择“所有服务”，然后在左窗格中搜索并选择“策略”。在“策略”页上选择“蓝图”。
2. 在左侧选择“蓝图定义”页。使用筛选器找到蓝图示例的副本，然后选择它。
3. 选择蓝图定义页面顶部的“分配蓝图”。
4. 提供蓝图分配的参数值：
   - 基础
     - **订阅**：在蓝图示例副本所保存到的管理组中选择一个或多个订阅。如果选择多个订阅，将使用输入的参数为每个订阅创建一个分配。
     - **分配名称**：系统会根据蓝图的名称预先填充该名称。请根据需要更改该名称，或保留原样。
     - **位置**：选择要在其中创建托管标识的区域。

- Azure 蓝图使用此托管标识在分配的蓝图中部署所有项目。若要了解详细信息，请参阅 Azure 资源的托管标识。
- **蓝图定义版本**：选择蓝图示例副本的已发布版本。

- 锁分配

  选择环境的蓝图锁定设置。有关更多信息，请参阅蓝图资源锁定。

- 托管标识

  选择默认的_系统分配_的托管标识选项或_用户分配_的标识选项。

- 蓝图参数

  蓝图定义中的许多项目使用本部分定义的参数来提供一致性。

  - **组织**：输入组织名称（例如 Contoso），必须唯一。
  - **Azure 区域**：选择要部署的 Azure 区域。
  - **允许的位置**：你将允许哪些 Azure 区域内置资源？

- 项目参数

  在本部分定义的参数将应用到定义了这些参数的项目。这些参数属于动态参数，因为它们是在分配蓝图期间定义的。有关完整列表或项目参数及其说明，请参阅项目参数表 。

5. 输入所有参数后，选择页面底部的“分配”。随后将创建蓝图分配，并开始部署项目。部署过程大约需要一小时。若要检查部署状态，请打开蓝图分配。

> **WARNING**
> Azure 蓝图服务和内置蓝图示例是免费的。Azure 资源按产品定价 。使用定价计算器 可以估算运行此蓝图示例部署的资源所需的成本。

项目参数表

下表提供了蓝图项目参数的列表：

项目名称	项目类型	参数名称	说明
允许的存储帐户 SKU	策略分配	Policy_Allowed-StorageAccount-SKUs	诊断日志存储帐户中使用的 SKU
允许的虚拟机 SKU	策略分配	Policy_Allowed-VM-SKUs	允许的虚拟机 SKU
将 CostCenter 标记追加到资源组	策略分配	Policy_CostCenter_Tag	从资源组追加 CostCenter 标记及其值
你不想在环境中允许的资源类型	策略分配	Policy _Allowed-Resource-Types	你希望在环境中允许哪些 Azure 资源
部署 Key Vault	资源管理器模板	KV-AccessPolicy	已锁定 - 在 Key Vault 中向其授予权限的 Azure AD 组或用户
部署 Log Analytics	资源管理器模板	LogAnalytics_DataRetention	已锁定 - 数据将在 Log Analytics 中保留的天数

项目名称	项目类型	参数名称	说明
部署 Log Analytics	资源管理器模板	LogAnalytics_Location	已锁定 - 建立工作区时使用的区域

后续步骤

查看了部署 CAF 基础蓝图示例的步骤后，请访问以下文章来了解体系结构：

CAF 基础蓝图 - 概述

有关蓝图和如何使用这些蓝图的更多文章：

- 了解蓝图生命周期。
- 了解如何使用静态和动态参数。
- 了解如何自定义蓝图排序顺序。
- 了解如何利用蓝图资源锁定。
- 了解如何更新现有分配。

适用于 Azure 的 Microsoft 云采用框架迁移登陆区域蓝图示例概述

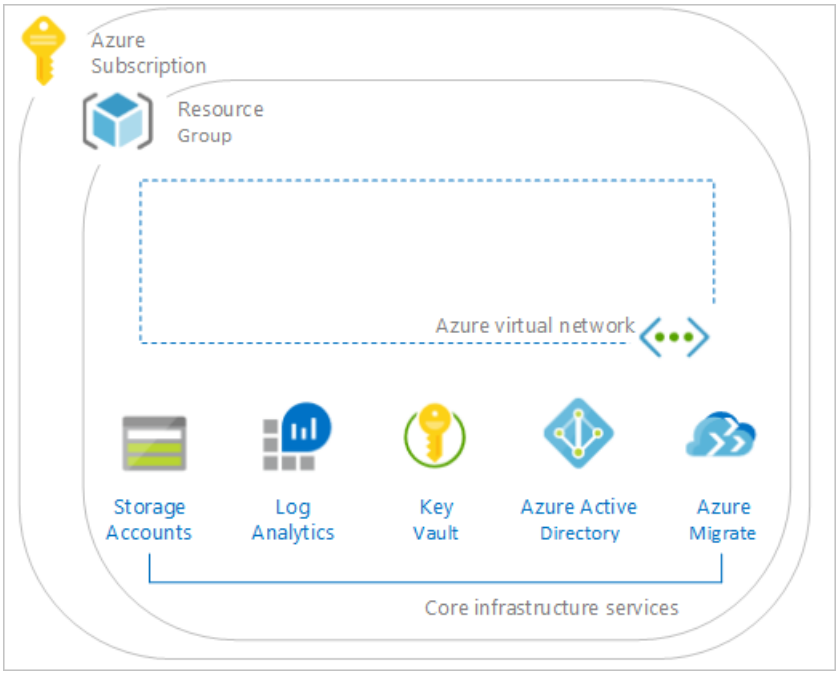
2019/9/4 • • Edit Online

适用于 Azure 的 Microsoft 云采用框架 (CAF) 迁移登陆区域蓝图是一组基础结构，用于帮助你安排迁移你的第一个工作负荷并管理你的云资产，使其与 CAF 相符合。

CAF 基础蓝图示例扩展了此示例。

体系结构

CAF 迁移登陆区域蓝图示例在 Azure 中部署基础结构资源，这些资源可供组织用来准备订阅，以便将虚拟机迁移到其中。它还可帮助将管理云资产所需的治理控制实施到位。此示例将部署并强制实施资源、策略和模板，从而使组织能够自信地开始使用 Azure。



此环境包括多项 Azure 服务，这些服务用于根据 ISO 27001 标准提供安全的、全面受监视的、面向企业的治理。此环境包括：

- 一个 Azure Key Vault 实例，用于托管对共享服务环境中部署的证书、密钥和机密使用的机密
- 部署 Log Analytics，以便确保从开始迁移起所有操作和服务都记录到一个中心位置
- 部署 Azure 安全中心（标准版），从而为已迁移的工作负荷提供威胁防护。
- 部署 Azure 虚拟网络，以便为虚拟机提供隔离的网络和子网。
- 部署 Azure Migrate 项目以用于发现和评估。我们正在添加用于服务器评估、服务器迁移、数据库评估和数据库迁移的工具。

所有这些元素遵守 Azure 体系结构中心 - 参考体系结构中发布的行之有效的做法。

> **NOTE**
> CAF 迁移蓝图为你的工作负荷布设了登陆区域。你仍需要基于此基础架构执行虚拟机/数据库的评估和迁移。

有关详细信息，请参阅适用于 Azure 的 Microsoft 云采用框架 - 迁移。

后续步骤

你已查看了 CAF 迁移登陆区域蓝图示例的概述和体系结构。

CAF 迁移登陆区域蓝图 - 部署步骤

有关蓝图和如何使用这些蓝图的更多文章：

- 了解蓝图生命周期。
- 了解如何使用静态和动态参数。
- 了解如何自定义蓝图排序顺序。
- 了解如何利用蓝图资源锁定。
- 了解如何更新现有分配。

部署适用于 Azure 的 Microsoft 云采用框架迁移登陆区域蓝图示例

2019/9/5 • • Edit Online

若要部署 Azure 蓝图 CAF 迁移登陆区域蓝图示例，必须执行以下步骤：

- 建议部署 CAF 基础蓝图示例
- 基于示例创建新的蓝图
- 将示例副本标记为“已发布”
- 将蓝图副本分配到现有的订阅

如果没有 Azure 订阅，请在开始之前创建一个免费帐户。

基于示例创建蓝图

首先，通过使用示例作为起点在环境中创建新的蓝图，来实现蓝图示例。

1. 选择“所有服务”，然后在左窗格中搜索并选择“策略”。在“策略”页上选择“蓝图”。
2. 在左侧的“开始”页中，选择“创建蓝图”下的“创建”按钮。
3. 在“其他示例”下找到“CAF 迁移登陆区域”蓝图示例，然后选择“使用此示例”。
4. 输入该蓝图示例的“基本信息”：
   - 蓝图名称提供 CAF 迁移登陆区域蓝图示例副本的名称。
   - 定义位置使用省略号并选择要将示例副本保存到的管理组。
5. 选择页面顶部的“项目”选项卡，或页面底部的“下一步: 项目”。
6. 查看构成蓝图示例的项目列表。许多项目包含稍后我们将要定义的参数。查看完蓝图示例后，选择“保存草稿”。

发布示例副本

现已在环境中创建蓝图示例的副本。该副本在创建后处于“草稿”模式，必须先将其发布，然后才能分配和部署它。可根据环境和需求自定义蓝图示例的副本，但这种修改可能会使其偏离 CAF 迁移登陆区域指南。

1. 选择“所有服务”，然后在左窗格中搜索并选择“策略”。在“策略”页上选择“蓝图”。
2. 在左侧选择“蓝图定义”页。使用筛选器找到蓝图示例的副本，然后选择它。
3. 选择页面顶部的“发布蓝图”。在右侧的新窗格中，提供蓝图示例副本的版本。以后做出修改时，此属性非常有用。提供更改注释，例如，“基于 CAF 迁移登陆区域蓝图示例发布的第一个版本”。然后选择页面底部的“发布”。

分配示例副本

成功发布蓝图示例的副本后，可将它分配到它所在的管理组中的某个订阅。在此步骤中，需提供参数来使蓝图示例副本的每个部署保持唯一。

1. 选择“所有服务”，然后在左窗格中搜索并选择“策略”。在“策略”页上选择“蓝图”。
2. 在左侧选择“蓝图定义”页。使用筛选器找到蓝图示例的副本，然后选择它。

3. 选择蓝图定义页面顶部的“分配蓝图”。

4. 提供蓝图分配的参数值：

   - 基础

     - **订阅**：在蓝图示例副本所保存到的管理组中选择一个或多个订阅。如果选择多个订阅，将使用输入的参数为每个订阅创建一个分配。
     - **分配名称**：系统会根据蓝图的名称预先填充该名称。请根据需要更改该名称，或保留原样。
     - **位置**：选择要在其中创建托管标识的区域。
     - Azure 蓝图使用此托管标识在分配的蓝图中部署所有项目。若要了解详细信息，请参阅 Azure 资源的托管标识。
     - **蓝图定义版本**：选择蓝图示例副本的已发布版本。

   - 锁分配

     选择环境的蓝图锁定设置。有关更多信息，请参阅蓝图资源锁定。

   - 托管标识

     选择默认的_系统分配_的托管标识选项或_用户分配_的标识选项。

   - 蓝图参数

     蓝图定义中的许多项目使用本部分定义的参数来提供一致性。

     - **组织**：输入组织名称（例如 Contoso 或 Fabrikam），必须唯一。
     - **Azure 区域**：选择要部署的一个 Azure 区域。

   - 项目参数

     在本部分定义的参数将应用到定义了这些参数的项目。这些参数属于动态参数，因为它们是在分配蓝图期间定义的。有关完整列表或项目参数及其说明，请参阅项目参数表 。

5. 输入所有参数后，选择页面底部的“分配”。随后将创建蓝图分配，并开始部署项目。部署大约需要五分钟。若要检查部署状态，请打开蓝图分配。

> **WARNING**
> Azure 蓝图服务和内置蓝图示例是免费的。Azure 资源按产品定价 。使用定价计算器 可以估算运行此蓝图示例部署的资源所需的成本。

项目参数表

下表提供了蓝图项目参数的列表：

项目名称	项目类型	参数名称	说明
部署 vNET 登陆区域	资源管理器模板	IPAddress_Space	**已锁定** - 提供前两个八位字节示例 10.0
部署 Key Vault	资源管理器模板	KV-AccessPolicy	**已锁定** - 在 Key Vault 中向其授予权限的组或用户对象 ID
部署 Log Analytics	资源管理器模板	LogAnalytics_DataRetention	**已锁定** - 数据将在 Log Analytics 中保留的天数

项目名称	项目类型	参数名称	说明
部署 Log Analytics	资源管理器模板	LogAnalytics_Location	**已锁定** - 建立工作区时使用的区域
部署 Azure Migrate	资源管理器模板	Azure_Migrate_Location	**已锁定** - 选择要部署 Azure Migrate 的区域

后续步骤

查看了部署 CAF 迁移登陆区域蓝图示例的步骤后，请访问以下文章来了解体系结构：

CAF 迁移登陆区域蓝图 - 概述

有关蓝图和如何使用这些蓝图的更多文章：

- 了解蓝图生命周期。
- 了解如何使用静态和动态参数。
- 了解如何自定义蓝图排序顺序。
- 了解如何利用蓝图资源锁定。
- 了解如何更新现有分配。

了解 Azure 蓝图的生命周期

2019/8/26 • • Edit Online

与 Azure 中的众多资源一样，Azure 蓝图中的蓝图也有一个典型的自然生命周期。这些蓝图会被创建、部署，并在不再需要或相关时被删除。蓝图支持标准的生命周期操作。它将在这些操作的基础之上进行构建，以提供附加的状态级别，用于支持常见的持续集成和持续部署管道，供管理基础结构即代码（DevOps 中的一项关键要素）的组织使用。

为了让你完全了解蓝图及其各个阶段，我们将讲解标准生命周期：

- 创建和编辑蓝图
- 发布蓝图
- 创建和编辑新版本的蓝图
- 发布新版本的蓝图
- 删除特定版本的蓝图
- 删除蓝图

创建和编辑蓝图

创建蓝图时，请向其添加项目、将其保存到管理组或订阅，并提供唯一名称和唯一版本。目前，蓝图处于“草稿”模式，尚不可分配。但在“草稿”模式下，仍可继续更新和更改此蓝图。

如果“草稿”模式下的某个蓝图从未发布过，则它在“蓝图定义”页面上显示的图标将与已发布的蓝图所显示的不同。对于这些从未发布蓝图，**最新版本**显示为**草稿**。

使用 Azure 门户或 REST API 创建和编辑蓝图。

发布蓝图

在对“草稿”模式下的蓝图进行所有计划的更改之后，此蓝图即可发布并可进行分配。已发布的蓝图版本不可更改。一旦发布，该蓝图显示的图标就与“草稿”蓝图的不同，并在“最新版本”列中显示所提供的版本号。

使用 Azure 门户或 REST API 发布蓝图。

创建和编辑新版本的蓝图

已发布的蓝图版本不可更改。但是，可向现有蓝图添加新版蓝图且可按需更改此新版本。通过编辑对现有蓝图进行更改。保存新更改时，蓝图将包含未发布的更改。这些更改是蓝图的新草稿版本。

使用 Azure 门户创建蓝图。

发布新版本的蓝图

蓝图的每个编辑版本必须在发布之后才可分配。当对蓝图进行未发布的更改，但它们尚未发布时，“发布蓝图”按钮在“编辑蓝图”页面上可用。如果未显示该按钮，则表示蓝图已发布，但具有“未发布的更改”。

> **NOTE**
> 一个蓝图可具有多个已发布的版本，每个版本都可分配到订阅。

若要发布包含未发布更改的蓝图，请使用发布新蓝图的相同步骤。

删除特定版本的蓝图

蓝图的每一个版本都是唯一对象，可单独发布。因此，还可以删除蓝图的每个版本。删除其中一个蓝图版本将不对该蓝图的其他版本造成任何影响。

> **NOTE**
> 不能删除具有活动分配项的蓝图。请先删除分配项，再删除要移除的版本。

1. 在左侧窗格中，选择“所有服务”。搜索并选择“蓝图”。
2. 从左侧页面中选择 "蓝图定义"，并使用筛选器选项查找要删除其版本的蓝图。单击它以打开“编辑”页面。
3. 单击“已发布的版本”选项卡，找到要删除的版本。
4. 右键单击要删除的版本，然后选择 "**删除此版本**"。

删除蓝图

此外，还可删除核心蓝图。删除核心蓝图也会删除该蓝图的任何蓝图版本，包括草稿和已发布的蓝图。与删除蓝图版本一样，删除核心蓝图时不会删除任何蓝图版本的现有分配项。

> **NOTE**
> 不能删除具有活动分配项的蓝图。请先删除分配项，再删除要移除的版本。

使用 Azure 门户或 REST API 删除蓝图。

作业

可在蓝图生命周期的多个时间点向订阅分配此蓝图。当蓝图版本处于“已发布”模式时，可向订阅分配此版本。在开发较新的版本期间，此生命周期使蓝图版本可供使用和主动分配。

由于蓝图的版本已分配，因此有必要了解其分配位置及其分配有的具体参数。参数可以是静态的，也可以是动态的。要了解详细信息，请参阅静态和动态参数。

更新分配

分配蓝图时可更新分配。众多原因导致要更新现有分配，其中包括：

- 添加或删除资源锁定
- 更改动态参数的值
- 将分配升级到新发布的蓝图版本

要了解操作方式，请参阅更新现有分配。

取消分配赋值

如果不再需要该蓝图，则可以将其从管理组或订阅中取消分配。在蓝图取消分配期间，会发生以

下情况:

- 删除蓝图资源锁定
- 删除蓝图分配对象
- 增值税如果使用系统分配的托管标识, 还会将其删除

> **NOTE**
> 蓝图分配部署的所有资源都将保留原样, 但不再受 Azure 蓝图的保护。

后续步骤

- 了解如何使用静态和动态参数。
- 了解如何自定义蓝图排序顺序。
- 了解如何利用蓝图资源锁定。
- 了解如何更新现有分配。
- 使用一般故障排除在蓝图的分配期间解决问题。

蓝图部署的阶段

2019/8/26 • • Edit Online

获取部署蓝图，一系列操作均由 Azure 蓝图服务部署蓝图中定义的资源。本文提供了有关每个步骤涉及的详细信息。

通过将蓝图分配给订阅触发蓝图部署或更新现有分配。部署过程中，蓝图采用以下高级步骤：

- 蓝图授予所有者权限
- 创建蓝图分配对象
- 可选-蓝图创建系统分配托管标识
- 托管的标识部署蓝图项目
- 蓝图服务和系统分配托管的标识权限被吊销

蓝图授予所有者权限

Azure 蓝图服务主体授予对已分配的订阅或订阅的所有者权限。授予的角色允许创建，并在以后撤销，蓝图系统分配的托管标识。

如果通过门户完成分配自动授予权限。但是，如果分配通过 REST API 中，授予权限需要能够完成与一个单独的 API 调用。Azure Blueprint AppId 是 `f71766dc-90d9-4b7d-bd9d-4499c4331c3f`，但因租户而异的服务主体。使用Azure Active Directory 图形 API和 REST 终结点servicePrincipals获取服务主体。然后，授予 Azure 蓝图_所有者_通过角色门户， Azure CLI， Azure PowerShell， RESTAPI，或资源管理器模板。

蓝图服务不会直接部署的资源。

创建蓝图分配对象

用户、组或服务主体将蓝图分配到订阅。在订阅级别分配蓝图其中存在分配对象。由部署创建的资源不是在部署实体的上下文中完成的。

创建蓝图分配的类型时托管标识处于选中状态。默认值是系统分配托管标识。一个用户分配，可以选择托管的标识。使用时用户分配托管标识，必须定义和之前创建蓝图分配，授予权限。

可选-蓝图创建系统分配给托管的标识

当系统分配的托管标识处于选中状态期间分配，蓝图创建标识，并授予托管的标识所有者角色。如果升级现有分配，蓝图使用以前创建的托管的标识。

与蓝图分配相关的托管的标识用于部署或重新部署蓝图中定义的资源。这种设计避免了无意中彼此间相互影响的分配。这种设计还支持资源锁定通过控制每个已部署资源的蓝图的安全功能。

托管的标识部署蓝图项目

托管的标识，然后触发中定义的蓝图中的项目资源管理器部署序列化顺序。可以调整顺序以确保按正确的顺序部署依赖于其他项目的项目。

部署了访问错误通常是访问的授予给托管标识权限级别的结果。该蓝图服务管理的安全生命周期系统分配托管标识。但是，用户负责管理的权限和生命周期用户分配托管标识。

蓝图服务和系统分配的托管的标识权限被吊销

完成部署后，蓝图，撤消的权限系统分配从订阅中托管标识。然后，蓝图服务撤消其从订阅的权限。权限删除阻止蓝图变得对某一订阅的永久所有者。

后续步骤

- 了解如何使用静态和动态参数。
- 了解如何自定义蓝图排序顺序。
- 了解如何利用蓝图资源锁定。
- 了解如何更新现有分配。
- 使用一般故障排除在蓝图的分配期间解决问题。

通过参数创建动态蓝图

2019/9/4 • • Edit Online

具有各种项目（如资源组、资源管理器模板、策略或角色分配）的完全定义蓝图可在 Azure 中快速一致地创建对象。为灵活使用这些可重复使用的设计模式和容器，Azure 蓝图支持参数。参数在定义和分配期间均创建灵活性，以更改蓝图部署的项目的属性。

一个简单的示例是资源组项目。创建资源组后，必须向其提供两个所需值：名称和位置。将资源组添加到蓝图时，如果参数不存在，则应为蓝图的每次使用定义该名称和位置。这种重复会导致每次使用蓝图时都在同一资源组中创建项目。资源组内的资源会重复并产生冲突。

> **NOTE**
> 对于两个不同的蓝图，包含具有相同名称的资源组不是问题。如果包含在蓝图中的资源组已存在，蓝图会继续在该资源组中创建相关项目。这可能会产生冲突，因为订阅中不能存在具有相同名称和资源类型的两个资源。

使用参数可以解决此问题。使用蓝图可在分配到订阅期间定义每个项目属性的值。通过参数还可以重复使用在一个订阅中创建资源组和其他资源的蓝图，且不会产生冲突。

蓝图参数

通过 REST API 可以在蓝图自身上创建参数。这些参数不同于每个受支持项目中的参数。在蓝图上创建参数时，该蓝图中的项目可使用该参数。示例可能是资源组命名的前缀。项目可以使用蓝图参数创建"基本上动态的"参数。由于还可以在分配期间定义参数，因此，此模式可以实现遵守命名规则的一致性。有关步骤，请参阅设置静态参数 - 蓝图级别参数。

使用 secureString 和 secureObject 参数

虽然资源管理器模板项目支持"secureString"和"secureObject"类型的参数，但 Azure 蓝图要求每个参数与 Azure Key Vault 连接。此安全措施可防止将机密与蓝图一起存储的不安全做法，并有利于采用安全模式。Azure 蓝图支持此安全措施，它可以检测是否在资源管理器模板项目中包含了任一安全参数。然后，该服务会在分配期间提示输入每个检测到的安全参数的以下 Key Vault 属性：

- Key Vault 资源 ID
- Key Vault 机密名称
- Key Vault 机密版本

如果蓝图分配使用**系统分配的托管**标识，则引用的 Key Vault_必须_存在于指定了蓝图定义的同一订阅中。

如果蓝图分配使用**用户分配的托管**标识，则引用的 Key Vault_可能_存在于集中订阅中。在蓝图分配之前，必须向托管标识授予对 Key Vault 的适当权限。

> **IMPORTANT**
> 在这两种情况下，Key Vault 必须对在 "**访问策略**" 页上配置的**模板部署启用**对 **Azure 资源管理器的访问**。有关如何启用此功能的说明，请参阅 Key Vault - 启用模板部署。

有关 Azure Key Vault 的详细信息，请参阅 概述。

参数类型

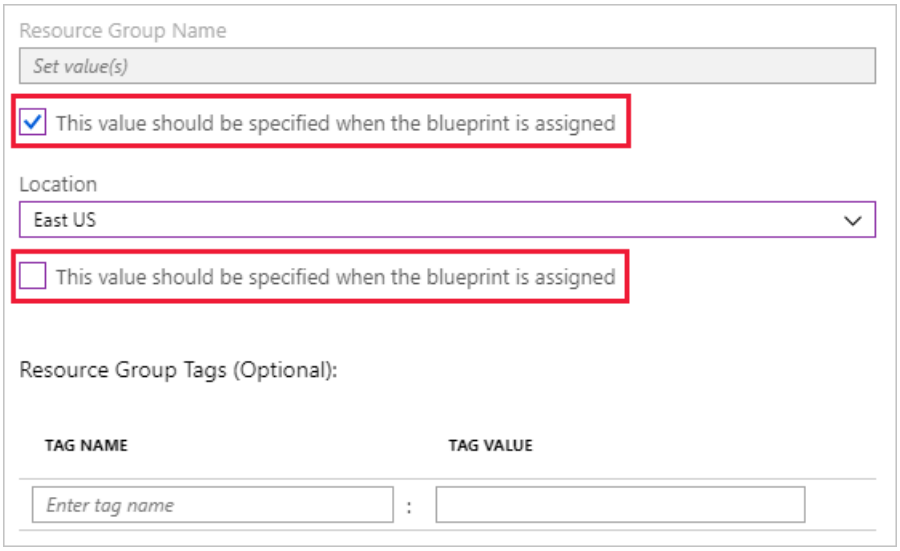
静态参数

蓝图定义中定义的参数值称为**静态参数**，因为每次使用蓝图都会部署使用该静态值的项目。在资源组示例中，这对资源组名称没有意义，但可能对位置有意义。然后，蓝图的每次分配都会在同一位置创建资源组，无论分配期间其名称为何。借助这种灵活性，可以选择定义为分配期间必需的内容或可更改的内容。

在门户中设置静态参数

1. 在左侧窗格中，选择“所有服务”。搜索并选择“蓝图”。
2. 从左侧页面中选择“蓝图定义”。
3. 单击现有蓝图，然后单击 "编辑蓝图" 或单击 " + 创建蓝图"，并在 "基本信息" 选项卡上填写信息。
4. 单击“下一步:项目”或单击“项目”选项卡。
5. 添加到蓝图中的项目（具有参数选项）会在“参数”列中显示“填充了 X 个参数，共 Y 个参数”。单击项目行，编辑项目参数。

6. “编辑项目”页会显示适用于所单击项目的值选项。项目上的每个参数具有标题、值框和复选框。将框设置为未选中状态，使其称为“静态参数”。在以下示例中，只有“位置”是“静态参数”，因为它处于未选中状态，同时“资源组名称”已选中。



从 REST API 设置静态参数

在每个 REST API URI 中，包含替换为自己的值所使用的变量：

- `{YourMG}` - 替换为管理组的名称
- `{subscriptionId}` - 替换为订阅 ID

蓝图级别参数

通过 REST API 创建蓝图时，可以创建蓝图参数。为此，请使用以下 REST API URI 和正文格式：

- REST API URI

```
PUT
https://management.azure.com/providers/Microsoft.Management/managementGroups/{Your
MG}/providers/Microsoft.Blueprint/blueprints/MyBlueprint?api-version=2018-11-01-
preview
```

- 请求正文

```
{
    "properties": {
        "description": "This blueprint has blueprint level parameters.",
        "targetScope": "subscription",
        "parameters": {
            "owners": {
                "type": "array",
                "metadata": {
                    "description": "List of AAD object IDs that is assigned Owner
role at the resource group"
                }
            }
        },
        "resourceGroups": {
            "storageRG": {
                "description": "Contains the resource template deployment and a
role assignment."
            }
        }
    }
}
```

创建蓝图级别参数后，便可在添加到该蓝图的项目上使用该参数。以下 REST API 示例在蓝图上创建角色分配项目，并使用蓝图级别参数。

- REST API URI

```
PUT
https://management.azure.com/providers/Microsoft.Management/managementGroups/{Your
MG}/providers/Microsoft.Blueprint/blueprints/MyBlueprint/artifacts/roleOwner?api-
version=2018-11-01-preview
```

- 请求正文

```
{
    "kind": "roleAssignment",
    "properties": {
        "resourceGroup": "storageRG",
        "roleDefinitionId":
"/providers/Microsoft.Authorization/roleDefinitions/8e3af657-a8ff-443c-a75c-
2fe8c4bcb635",
        "principalIds": "[parameters('owners')]"
    }
}
```

在此示例中，**principalIds** 属性通过 `[parameters('owners')]` 的值使用 **owners** 蓝图级参数。使用蓝图级参数在项目中设置参数仍是静态参数的示例。蓝图级参数无法在蓝图分配期间设置，每次分配时都是同一个值。

项目级别参数

在项目上创建"静态参数"情况相似，但采用直接值而不是使用 `parameters()` 函数。以下示例创建了两个静态参数："tagName"和"tagValue"。每个参数的值直接提供，且不使用函数调用。

- REST API URI

```
PUT
https://management.azure.com/providers/Microsoft.Management/managementGroups/{YourMG}/providers/Microsoft.Blueprint/blueprints/MyBlueprint/artifacts/policyStorageTags?api-version=2018-11-01-preview
```

- 请求正文

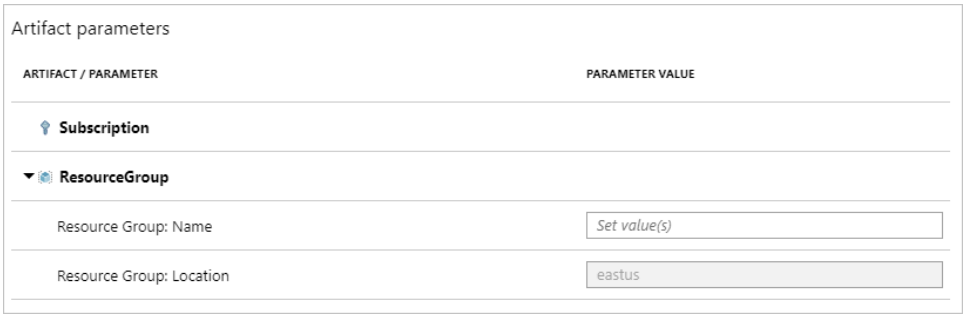
```
{
    "kind": "policyAssignment",
    "properties": {
        "description": "Apply storage tag and the parameter also used by the template to resource groups",
        "policyDefinitionId": "/providers/Microsoft.Authorization/policyDefinitions/49c88fc8-6fd1-46fd-a676-f12d1d3a4c71",
        "parameters": {
            "tagName": {
                "value": "StorageType"
            },
            "tagValue": {
                "value": "Premium_LRS"
            }
        }
    }
}
```

动态参数

与静态参数相对的是“动态参数”。此参数未在蓝图中定义，而是在每次分配蓝图期间定义的。在资源组示例中，使用动态参数对资源组名称有意义。每次分配蓝图时，它将提供不同的名称。有关蓝图函数的列表，请参阅蓝图函数参考。

在门户中设置动态参数

1. 在左侧窗格中，选择“所有服务”。搜索并选择“蓝图”。
2. 从左侧页面中选择“蓝图定义”。
3. 右键单击要分配的蓝图。选择 "**分配蓝图**" 或单击要分配的蓝图，然后单击 "**分配蓝图**" 按钮。
4. 在 "**分配蓝图**" 页上，找到 "**项目参数**" 部分。具有至少一个“动态参数”的每个项目会显示项目和配置选项。分配蓝图前，请向参数提供所需值。在以下示例中，“名称”是“动态参数”，必须对其定义以完成蓝图分配。



从 REST API 设置动态参数

在分配期间设置动态参数是通过直接输入值完成的。提供的值不是使用函数(如参数 ())，而是提供一个合适的字符串。资源组的项目是使用“模板名称”、**name** 和 **location** 属性定义的。包含的项目的其他所有参数在 **parameters** 下使用 **<名称>** 和值键对进行定义。如果为分配

期间未提供的动态参数配置了蓝图，则分配将会失败。

- REST API URI

```
PUT
https://management.azure.com/subscriptions/{subscriptionId}/providers/Microsoft.Bl
ueprint/blueprintAssignments/assignMyBlueprint?api-version=2018-11-01-preview
```

- 请求正文

```
{
    "properties": {
        "blueprintId": "/providers/Microsoft.Management/managementGroups/{YourMG}
/providers/Microsoft.Blueprint/blueprints/MyBlueprint",
        "resourceGroups": {
            "storageRG": {
                "name": "StorageAccount",
                "location": "eastus2"
            }
        },
        "parameters": {
            "storageAccountType": {
                "value": "Standard_GRS"
            },
            "tagName": {
                "value": "CostCenter"
            },
            "tagValue": {
                "value": "ContosoIT"
            },
            "contributors": {
                "value": [
                    "7be2f100-3af5-4c15-bcb7-27ee43784a1f",
                    "38833b56-194d-420b-90ce-cff578296714"
                ]
              },
            "owners": {
                "value": [
                    "44254d2b-a0c7-405f-959c-f829ee31c2e7",
                    "316deb5f-7187-4512-9dd4-21e7798b0ef9"
                ]
            }
        }
    },
    "identity": {
        "type": "systemAssigned"
    },
    "location": "westus"
}
```

后续步骤

- 请参阅蓝图函数的列表。
- 了解蓝图生命周期。
- 了解如何自定义蓝图排序顺序。
- 了解如何利用蓝图资源锁定。
- 了解如何更新现有分配。
- 使用一般故障排除在蓝图的分配期间解决问题。

了解 Azure 蓝图中的部署排序

2019/9/4 • • Edit Online

在处理蓝图定义的分配时, Azure 蓝图使用排序顺序来确定创建资源的顺序。本文解释了以下概念:

- 使用的默认序列化顺序
- 如何自定义顺序
- 自定义顺序是如何处理的

JSON 示例中的有些变量需要用自己的值替换:

- `{YourMG}` - 替换为管理组的名称

默认排序顺序

如果蓝图定义为部署项目的顺序不包含指令, 或者指令为 null, 则使用以下顺序:

- 订阅级别"角色分配"项目按项目名称排序
- 订阅级别"策略分配"项目按项目名称排序
- 订阅级别"Azure 资源管理器模板"项目按项目名称排序
- "资源组"项目(包括子项目)按占位符名称排序

在每个资源组项目中, 将按照以下顺序排列在该资源组中创建的项目:

- 资源组子"角色分配"项目按项目名称排序
- 资源组子"策略分配"项目按项目名称排序
- 资源组子"Azure 资源管理器模板"项目按项目名称排序

> **NOTE**
> 使用伪像 ()可对所引用的项目创建隐式依赖项。

自定义排序顺序

编写大型蓝图定义时, 可能需要按特定顺序创建资源。此方案的最常见使用模式是蓝图定义包含多个 Azure 资源管理器模板。蓝图通过允许定义排序顺序来处理此模式。

排序是通过在 JSON 中定义 `dependsOn` 属性来实现的。资源组和项目对象的蓝图定义支持此属性。 `dependsOn` 是在创建特定项目之前需要创建的项目名称的字符串数组。

> **NOTE**
> 创建蓝图对象时, 如果使用REST API, 则每个项目资源都将从文件名中获取其名称 (如果使用POWERSHELL) 或 URL 端点。项目中的 ResourceGroup 引用必须与蓝图定义中定义的_资源_组引用匹配。

示例-有序资源组

此示例蓝图定义具有一个资源组, 该资源组通过声明的值 `dependsOn` 以及标准资源组定义了自定义的排序顺序。在这种情况下, 名为"assignPolicyTags"的项目将在"ordered-rg"资源组之前

进行处理。standard-rg 将按默认排序顺序进行处理。

```
{
    "properties": {
        "description": "Example blueprint with custom sequencing order",
        "resourceGroups": {
            "ordered-rg": {
                "dependsOn": [
                    "assignPolicyTags"
                ],
                "metadata": {
                    "description": "Resource Group that waits for 'assignPolicyTags'
creation"
                }
            },
            "standard-rg": {
                "metadata": {
                    "description": "Resource Group that follows the standard sequence
ordering"
                }
            }
        },
        "targetScope": "subscription"
    },
    "type": "Microsoft.Blueprint/blueprints"
}
```

示例 - 使用自定义顺序的项目

此示例是一个策略项目，它依赖于一个 Azure 资源管理器模板。根据默认排序，策略项目将先于 Azure 资源管理器模板创建。此排序允许策略项目等待 Azure 资源管理器模板完成创建。

```
{
    "properties": {
        "displayName": "Assigns an identifying tag",
        "policyDefinitionId":
"/providers/Microsoft.Authorization/policyDefinitions/2a0e14a6-b0a6-4fab-991a-
187a4f81c498",
        "resourceGroup": "standard-rg",
        "dependsOn": [
            "customTemplate"
        ]
    },
    "kind": "policyAssignment",
    "type": "Microsoft.Blueprint/artifacts"
}
```

示例-根据资源组的订阅级别模板项目

此示例适用于在订阅级别部署的资源管理器模板，以依赖于资源组。默认排序中，将在这些资源组中的任何资源组和子项目之前创建订阅级别项目。资源组在蓝图定义中定义，如下所示：

```
"resourceGroups": {
    "wait-for-me": {
        "metadata": {
            "description": "Resource Group that is deployed prior to the subscription
level template artifact"
        }
    }
}
```

根据 "**等待我**" 资源组的定义，订阅级别模板项目的定义如下所示：

```
{
    "properties": {
        "template": {
            ...
        },
        "parameters": {
            ...
        },
        "dependsOn": ["wait-for-me"],
        "displayName": "SubLevelTemplate",
        "description": ""
    },
    "kind": "template",
    "type": "Microsoft.Blueprint/blueprints/artifacts"
}
```

处理自定义排序

在创建过程中，将使用拓扑排序来创建蓝图项目的依赖项关系图。此检查可确保资源组与项目之间每个级别的依赖项都得到支持。

如果声明了不会更改默认顺序的依赖项，则不会进行任何更改。一个示例是依赖于订阅级策略的资源组。另一个示例是资源组“standard-rg”子策略分配，它依赖于资源组“standard-rg”子角色分配。这两种情况下，`dependsOn` 都不会更改默认的排序顺序且不会进行任何更改。

后续步骤

- 了解蓝图生命周期。
- 了解如何使用静态和动态参数。
- 了解如何利用蓝图资源锁定。
- 了解如何更新现有分配。
- 使用一般故障排除在蓝图的分配期间解决问题。

了解 Azure 蓝图中的资源锁定

2019/9/4 • • Edit Online

仅当存在一个可以维护该一致性的机制时，大规模创建一致的环境才会真正有价值。本文介绍 Azure 蓝图中的资源锁定的工作原理。若要查看资源锁定的示例以及_拒绝分配_的应用，请参阅保护新资源教程。

锁定模式和状态

锁定模式适用于蓝图分配，具有三个选项："不锁定"、"只读"或"不要删除"。在蓝图分配过程中的项目部署过程中配置锁定模式。可以通过更新蓝图分配来设置不同的锁定模式。但是，不能在蓝图外部更改锁定模式。

蓝图分配中由项目创建的资源具有四种状态："未锁定"、"只读"、"无法编辑/删除"或"无法删除"。每种项目类型都可以处于"未锁定"状态。下表可以用于确定资源的状态：

模式	项目资源类型	状态	描述
不锁定	*	未锁定	资源不受蓝图保护。此状态也用于从蓝图分配外部添加到"只读"或"不要删除"资源组项目的资源。
只读	资源组	无法编辑/删除	资源组是只读的，资源组上的标记无法修改。可以从此资源组添加、移动、更改或删除"未锁定"资源。
只读	非资源组	只读	以任何方式都无法更改资源 -- 无更改且无法将其删除。
请勿删除	*	无法删除	资源可以更改，但无法删除。可以从此资源组添加、移动、更改或删除"未锁定"资源。

重写锁定状态

通常可以允许在订阅上具有合适的基于角色的访问控制 (RBAC) 的某人（例如"所有者"角色）更改或删除任何资源。当蓝图在已部署的分配中应用了锁定时，无法进行此访问。如果使用"只读"或"不要删除"选项设置了分配，则即使订阅所有者也无法对受保护资源执行阻止的操作。

此安全措施可以保护已定义的蓝图与设计用于通过意外或以编程方式删除或更改创建的环境之间的一致性。

删除锁定状态

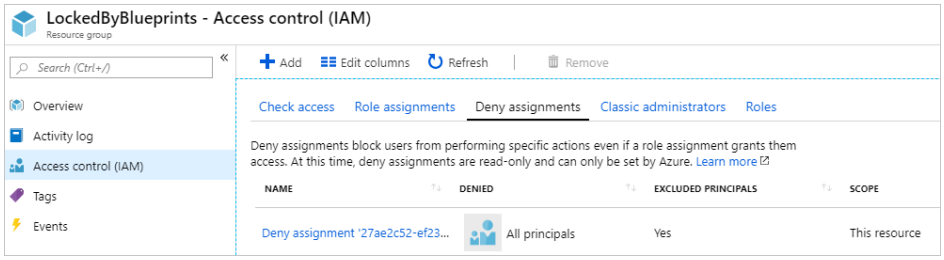
如果需要修改或删除受分配保护的资源，则可通过两种方法来实现。

- 将蓝图分配更新为"不锁定"锁定模式
- 删除蓝图分配

删除分配后，将删除由蓝图创建的锁定。但是，资源会留在原地，需要通过正常方式删除。

蓝图锁定的工作原理

如果蓝图分配选择了"只读"或"不要删除"选项，则会在分配期间将 RBAC 拒绝分配拒绝操作应用于项目资源。该拒绝操作由蓝图分配的托管标识添加，并且只能通过同一托管标识从项目资源中删除。此安全措施将强制实施锁定机制，并防止在蓝图外部删除蓝图锁定。



每个模式的拒绝分配属性如下所示:

模式	PERMISSIONS.ACTIONS	PERMISSIONS.NOTACTIONS	PRINCIPALS[I].TYPE	EXCLUDEPRINCIPALS[I].ID	DONOTAPPLYTOCHILDSCOPES
只读	*	*/read	SystemDefined (Everyone)	excludedPrincipals中的蓝图分配和用户定义	资源组-*true*;资源-*false*
请勿删除	*/delete		SystemDefined (Everyone)	excludedPrincipals中的蓝图分配和用户定义	资源组-*true*;资源-*false*

> **IMPORTANT**
> Azure 资源管理器可以将角色分配详细信息缓存最多 30 分钟。因此，蓝图资源上的拒绝分配拒绝操作可能不会立即完全生效。在此时间段内，可能无法删除将由蓝图锁保护的资源。

从拒绝分配中排除主体

在某些设计或安全方案中，可能需要将主体从蓝图分配创建的拒绝分配中排除。这是在 REST API 中完成的，方法是在创建分配时，将最多五个值添加到 "锁定" 属性中的**excludedPrincipals**数组。下面是包含**excludedPrincipals**的请求正文示例:

```
{
  "identity": {
    "type": "SystemAssigned"
  },
  "location": "eastus",
  "properties": {
    "description": "enforce pre-defined simpleBlueprint to this XXXXXXXX
subscription.",
    "blueprintId":
"/providers/Microsoft.Management/managementGroups/{mgId}/providers/Microsoft.Blu
eprint/blueprints/simpleBlueprint",
    "locks": {
        "mode": "AllResourcesDoNotDelete",
        "excludedPrincipals": [
            "7be2f100-3af5-4c15-bcb7-27ee43784a1f",
            "38833b56-194d-420b-90ce-cff578296714"
        ]
    },
    "parameters": {
      "storageAccountType": {
        "value": "Standard_LRS"
      },
      "costCenter": {
        "value": "Contoso/Online/Shopping/Production"
      },
      "owners": {
        "value": [
          "johnDoe@contoso.com",
          "johnsteam@contoso.com"
        ]
      }
    },
    "resourceGroups": {
      "storageRG": {
        "name": "defaultRG",
        "location": "eastus"
      }
    }
  }
}
```

后续步骤

- 按照保护新资源教程操作。
- 了解蓝图生命周期。
- 了解如何使用静态和动态参数。
- 了解如何自定义蓝图排序顺序。
- 了解如何更新现有分配。
- 使用一般故障排除在蓝图的分配期间解决问题。

如何通过 PowerShell 管理分配

2019/9/4 • • Edit Online

可以使用**Az** Azure PowerShell module 管理蓝图分配。模块支持提取、创建、更新和删除分配。模块还可以获取有关现有蓝图定义的详细信息。本文介绍如何安装该模块并开始使用它。

添加 Az module 模块

若要启用 Azure PowerShell 来管理蓝图分配，必须添加模块。此模块可以与在本地安装的 PowerShell 以及 Azure Cloud Shell 一起使用，也可以与 Azure PowerShell Docker 映像一起使用。

基本要求

Azure 蓝图模块需要以下软件：

- Azure PowerShell 1.5.0 或更高版本。若尚未安装，请遵循这些说明。
- PowerShellGet 2.0.1 或更高版本。若尚未安装或更新，请遵循这些说明。

安装模块

适用于 PowerShell 的蓝图模块为**Az**。

1. 从管理 PowerShell 提示符运行以下命令：

```
# Install the Blueprints module from PowerShell Gallery
Install-Module -Name Az.Blueprint
```

> **NOTE**
> 如果**Az**已安装，则可能需要使用 `-AllowClobber` 来强制安装。

2. 验证是否已导入该模块且是否为正确版本 (0.1.0)：

```
# Get a list of commands for the imported Az.Blueprint module
Get-Command -Module 'Az.Blueprint' -CommandType 'Cmdlet'
```

获取蓝图定义

处理赋值的第一步通常是获取对蓝图定义的引用。`Get-AzBlueprint` Cmdlet 获取一个或多个蓝图定义。Cmdlet 可以从管理组 `-ManagementGroupId {mgId}` 或使用 `-SubscriptionId {subId}` 订阅获取蓝图定义。**Name**参数获取蓝图定义，但必须与**ManagementGroupId**或**SubscriptionId**一起使用。**版本**可与**名称**一起使用，以便更明确地了解返回的蓝图定义。开关 `-LatestPublished` 用于获取最近发布的版本，而不是**版本**。

下面的示例使用 `Get-AzBlueprint` 从表示为 `{subId}` 的特定订阅获取名为 "101-蓝图-定义-订阅" 的所有版本的蓝图定义：

```
# Login first with Connect-AzAccount if not using Cloud Shell

# Get all versions of the blueprint definition in the specified subscription
$blueprints = Get-AzBlueprint -SubscriptionId '{subId}' -Name '101-blueprints-definition-subscription'

# Display the blueprint definition object
$blueprints
```

具有多个版本的蓝图定义的示例输出如下所示:

```
Name                : 101-blueprints-definition-subscription
Id                  : /subscriptions/{subId}/providers/Microsoft.Blueprint/blueprints/101
                      -blueprints-definition-subscription
DefinitionLocationId : {subId}
Versions            : {1.0, 1.1}
TimeCreated         : 2019-02-25
TargetScope         : Subscription
Parameters          : {storageAccount_storageAccountType, storageAccount_location,
                      allowedlocations_listOfAllowedLocations,
[Usergrouporapplicationname]:Reader_RoleAssignmentName}
ResourceGroups      : ResourceGroup
```

可以展开蓝图定义上的蓝图参数以提供详细信息。

```
$blueprints.Parameters
```

```
Key                                                 Value
---                                                 -----
storageAccount_storageAccountType
Microsoft.Azure.Commands.Blueprint.Models.PSParameterDefinition
storageAccount_location
Microsoft.Azure.Commands.Blueprint.Models.PSParameterDefinition
allowedlocations_listOfAllowedLocations
Microsoft.Azure.Commands.Blueprint.Models.PSParameterDefinition
[Usergrouporapplicationname]:Reader_RoleAssignmentName
Microsoft.Azure.Commands.Blueprint.Models.PSParameterDefinition
```

获取蓝图分配

如果蓝图分配已存在, 可以使用 `Get-AzBlueprintAssignment` cmdlet 获取对它的引用。Cmdlet 采用**SubscriptionId**和**Name**作为可选参数。如果未指定**SubscriptionId** , 则使用当前的订阅上下文。

下面的示例使用 `Get-AzBlueprintAssignment` 从表示为 `{subId}` 的特定订阅获取名为 "分配-锁定资源组" 的单一蓝图分配:

```
# Login first with Connect-AzAccount if not using Cloud Shell

# Get the blueprint assignment in the specified subscription
$blueprintAssignment = Get-AzBlueprintAssignment -SubscriptionId '{subId}' -Name 'Assignment-lock-resource-
groups'

# Display the blueprint assignment object
$blueprintAssignment
```

蓝图分配的示例输出如下所示:

```
Name              : Assignment-lock-resource-groups
Id                : /subscriptions/{subId}/providers/Microsoft.Blueprint/blueprintAssignme
                    nts/Assignment-lock-resource-groups
Scope             : /subscriptions/{subId}
LastModified      : 2019-02-19
LockMode          : AllResourcesReadOnly
ProvisioningState : Succeeded
Parameters        :
ResourceGroups    : ResourceGroup
```

创建蓝图分配

如果蓝图分配尚不存在, 则可以用 `New-AzBlueprintAssignment` cmdlet 创建。此 cmdlet 使用以下参数:

- **名称**请求
  - 指定蓝图分配的名称
  - 必须是唯一的, 且**SubscriptionId**中不存在
- **蓝图**请求
  - 指定要分配的蓝图定义
  - 用于 `Get-AzBlueprint` 获取 reference 对象
- **位置**请求
  - 指定要在其中创建系统分配的托管标识和订阅部署对象的区域。
- **订阅**可有可无
  - 指定将分配部署到的订阅
  - 如果未提供, 则默认为当前订阅上下文
- **锁定**可有可无
  - 定义要用于已部署资源的蓝图资源锁定
  - 支持的选项:*None*、*AllResourcesReadOnly*、*AllResourcesDoNotDelete*
  - 如果未提供, 默认值为 "*无*"
- **SystemAssignedIdentity**可有可无
  - 选择此项可为分配创建系统分配的托管标识并部署资源
  - "Identity" 参数集的默认值
  - 不能与**UserAssignedIdentity**一起使用
- **UserAssignedIdentity**可有可无
  - 指定用于分配并部署资源的用户分配的托管标识
  - "Identity" 参数集的一部分
  - 不能与**SystemAssignedIdentity**一起使用
- **参数**可有可无
  - 用于在蓝图分配上设置动态参数的键/值对的哈希表
  - 动态参数的默认值是定义中的**defaultValue**
  - 如果未提供参数且没有**defaultValue**, 则参数不是可选的

> **NOTE**
> 参数不支持 secureStrings。

- **ResourceGroupParameter**可有可无
  - 资源组项目的哈希表
  - 每个资源组项目占位符都有一个键/值对, 用于动态设置该资源组项目的**名称**和/或**位置**
  - 如果未提供资源组参数并且没有**defaultValue**, 则资源组参数不是可选的

下面的示例创建使用`Get-AzBlueprint`提取的 "我的蓝图" 蓝图定义的版本 "1.1" 的新分配, 将托管标识和分配对象位置设置为 "westus2", 使用_AllResourcesReadOnly 锁定资源。_ , 并为指定为`{subId}`的特定订阅设置参数和**ResourceGroupParameter**的哈希表:

```
# Login first with Connect-AzAccount if not using Cloud Shell

# Get version '1.1' of the blueprint definition in the specified subscription
$bpDefinition = Get-AzBlueprint -SubscriptionId '{subId}' -Name 'my-blueprint' -Version '1.1'

# Create the hash table for Parameters
$bpParameters = @{storageAccount_storageAccountType='Standard_GRS'}

# Create the hash table for ResourceGroupParameters
# ResourceGroup is the resource group artifact placeholder name
$bpRGParameters = @{ResourceGroup=@{name='storage_rg';location='westus2'}}

# Create the new blueprint assignment
$bpAssignment = New-AzBlueprintAssignment -Name 'my-blueprint-assignment' -Blueprint $bpDefinition `
    -SubscriptionId '{subId}' -Location 'westus2' -Lock AllResourcesReadyOnly `
    -Parameter $bpParameters -ResourceGroupParameter $bpRGParameters
```

用于创建蓝图分配的示例输出如下所示:

```
Name              : my-blueprint-assignment
Id                : /subscriptions/{subId}/providers/Microsoft.Blueprint/blueprintAssi
                    gnments/my-blueprint-assignment
Scope             : /subscriptions/{subId}
LastModified      : 2019-03-13
LockMode          : AllResourcesReadyOnly
ProvisioningState : Creating
Parameters        : {storageAccount_storageAccountType}
ResourceGroups    : ResourceGroup
```

更新蓝图分配

有时, 必须更新已创建的蓝图分配。`Set-AzBlueprintAssignment` Cmdlet 处理此操作。该 cmdlet 将使用该`New-AzBlueprintAssignment` cmdlet 执行的大部分相同参数, 从而允许更新在分配上设置的任何内容。这种情况的例外是_名称_、*蓝图_和_SubscriptionId*。仅更新所提供的值。

若要了解更新蓝图分配时所发生的情况, 请参阅更新分配的规则。

- **名称**请求
  - 指定要更新的蓝图分配的名称
  - 用于查找要更新的分配, 而不是更改分配
- 蓝图请求
  - 指定蓝图分配的蓝图定义
  - 用于`Get-AzBlueprint`获取 reference 对象
  - 用于查找要更新的分配, 而不是更改分配
- **位置**可有可无

  - 指定要在其中创建系统分配的托管标识和订阅部署对象的区域。
- 订阅可有可无
  - 指定将分配部署到的订阅
  - 如果未提供, 则默认为当前订阅上下文
  - 用于查找要更新的分配, 而不是更改分配
- 锁定可有可无
  - 定义要用于已部署资源的蓝图资源锁定
  - 支持的选项:*None*、*AllResourcesReadOnly*、*AllResourcesDoNotDelete*
- **SystemAssignedIdentity**可有可无
  - 选择此项可为分配创建系统分配的托管标识并部署资源
  - "Identity" 参数集的默认值
  - 不能与**UserAssignedIdentity**一起使用
- **UserAssignedIdentity**可有可无
  - 指定用于分配并部署资源的用户分配的托管标识
  - "Identity" 参数集的一部分
  - 不能与**SystemAssignedIdentity**一起使用
- **参数**可有可无
  - 用于在蓝图分配上设置动态参数的键/值对的哈希表
  - 动态参数的默认值是定义中的**defaultValue**
  - 如果未提供参数且没有**defaultValue**, 则参数不是可选的

    > **NOTE**
    > **参数**不支持 secureStrings。

- **ResourceGroupParameter**可有可无
  - 资源组项目的哈希表
  - 每个资源组项目占位符都有一个键/值对, 用于动态设置该资源组项目的**名称**和/或**位置**
  - 如果未提供资源组参数并且没有**defaultValue**, 则资源组参数不是可选的

下面的示例`Get-AzBlueprint`通过更改锁定模式, 更新通过获取的 "我的蓝图" 蓝图定义的版本 "1.1" 的分配:

```
# Login first with Connect-AzAccount if not using Cloud Shell

# Get version '1.1' of the blueprint definition in the specified subscription
$bpDefinition = Get-AzBlueprint -SubscriptionId '{subId}' -Name 'my-blueprint' -Version '1.1'

# Update the existing blueprint assignment
$bpAssignment = Set-AzBlueprintAssignment -Name 'my-blueprint-assignment' -Blueprint $bpDefinition `
    -SubscriptionId '{subId}' -Lock AllResourcesDoNotDelete
```

用于创建蓝图分配的示例输出如下所示:

```
Name              : my-blueprint-assignment
Id                : /subscriptions/{subId}/providers/Microsoft.Blueprint/blueprintAssi
                    gnments/my-blueprint-assignment
Scope             : /subscriptions/{subId}
LastModified      : 2019-03-13
LockMode          : AllResourcesDoNotDelete
ProvisioningState : Updating
Parameters        : {storageAccount_storageAccountType}
ResourceGroups    : ResourceGroup
```

删除蓝图分配

当需要删除蓝图分配时，该 cmdlet 将 `Remove-AzBlueprintAssignment` 处理此操作。该 cmdlet 使用**Name**或**InputObject**来指定要删除的蓝图分配。**SubscriptionId**是_必需_的，并且必须在所有情况下提供。

下面的示例使用 `Get-AzBlueprintAssignment` 获取现有蓝图分配，然后将其从表示为 `{subId}` 的特定订阅中删除：

```
# Login first with Connect-AzAccount if not using Cloud Shell

# Get the blueprint assignment in the specified subscription
$blueprintAssignment = Get-AzBlueprintAssignment -Name 'Assignment-lock-resource-groups'

# Remove the existing blueprint assignment
Remove-AzBlueprintAssignment -InputObject $blueprintAssignment -SubscriptionId '{subId}'
```

端到端代码示例

将所有步骤组合在一起后，以下示例将获取蓝图定义，然后创建、更新和删除特定订阅中表示为 `{subId}` 的蓝图分配：

```
# Login first with Connect-AzAccount if not using Cloud Shell

#region GetBlueprint
# Get version '1.1' of the blueprint definition in the specified subscription
$bpDefinition = Get-AzBlueprint -SubscriptionId '{subId}' -Name 'my-blueprint' -Version '1.1'
#endregion

#region CreateAssignment
# Create the hash table for Parameters
$bpParameters = @{storageAccount_storageAccountType='Standard_GRS'}

# Create the hash table for ResourceGroupParameters
# ResourceGroup is the resource group artifact placeholder name
$bpRGParameters = @{ResourceGroup=@{name='storage_rg';location='westus2'}}

# Create the new blueprint assignment
$bpAssignment = New-AzBlueprintAssignment -Name 'my-blueprint-assignment' -Blueprint $bpDefinition `
    -SubscriptionId '{subId}' -Location 'westus2' -Lock AllResourcesReadyOnly `
    -Parameter $bpParameters -ResourceGroupParameter $bpRGParameters
#endregion CreateAssignment

# Wait for the blueprint assignment to finish deployment prior to the next steps

#region UpdateAssignment
# Update the existing blueprint assignment
$bpAssignment = Set-AzBlueprintAssignment -Name 'my-blueprint-assignment' -Blueprint $bpDefinition `
    -SubscriptionId '{subId}' -Lock AllResourcesDoNotDelete
#endregion UpdateAssignment

# Wait for the blueprint assignment to finish deployment prior to the next steps

#region RemoveAssignment
# Remove the existing blueprint assignment
Remove-AzBlueprintAssignment -InputObject $bpAssignment -SubscriptionId '{subId}'
#endregion
```

后续步骤

- 了解蓝图生命周期。
- 了解如何使用静态和动态参数。
- 了解如何自定义蓝图排序顺序。
- 了解如何利用蓝图资源锁定。
- 使用一般故障排除在蓝图的分配期间解决问题。

如何更新现有蓝图分配

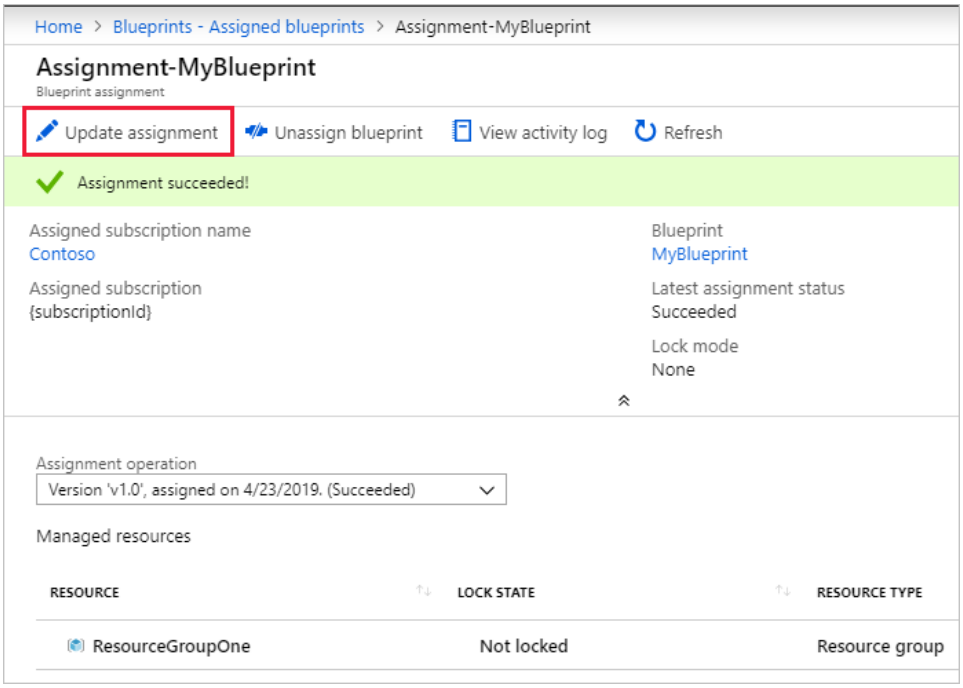
2019/9/4 • • Edit Online

分配蓝图时可以更新分配。众多原因导致要更新现有分配，其中包括：

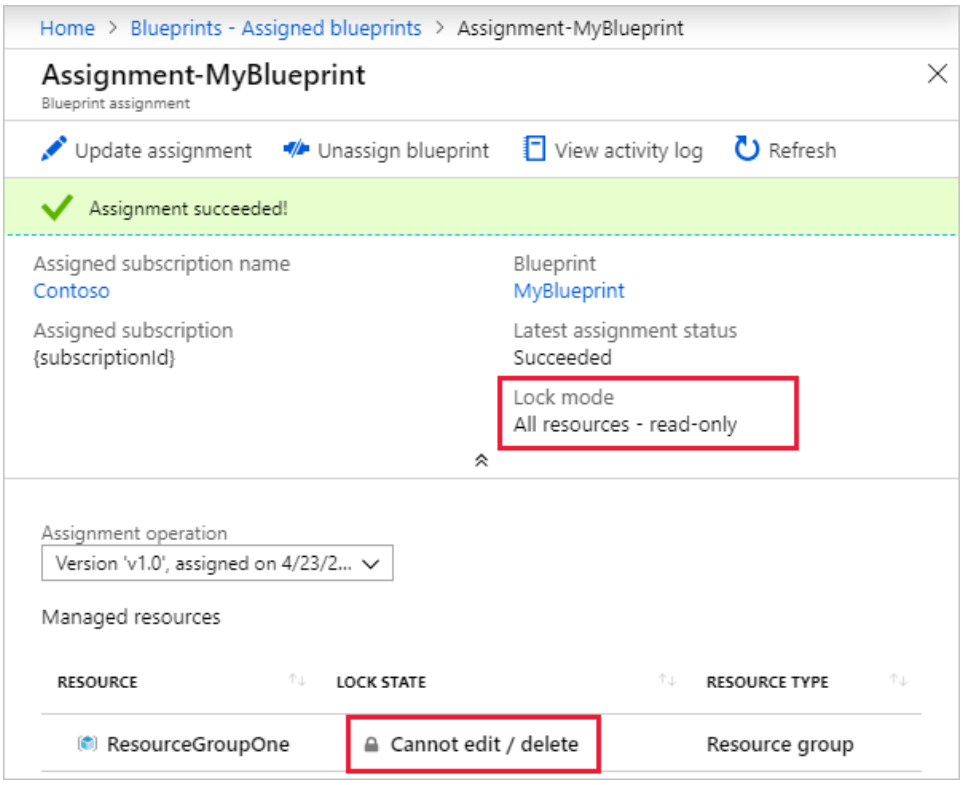
- 添加或删除资源锁定
- 更改动态参数的值
- 将分配升级到新发布的蓝图版本

更新分配

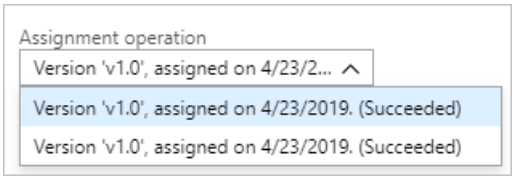
1. 在左侧窗格中，选择“所有服务”。搜索并选择“蓝图”。
2. 从左侧页面选择“分配的蓝图”。
3. 在蓝图列表中，左键单击蓝图分配。然后单击 "**更新分配**" 按钮，或右键单击蓝图分配，然后选择 "**更新分配**"。



4. "**分配蓝图**" 页将加载原始赋值中的所有值。可以更改“蓝图定义版本”、“锁定分配”状态，以及蓝图定义上存在的任何动态参数。完成更改时，单击“分配”。
5. 在更新后的分配详细信息页上，查看新状态。在此示例中，我们向分配添加了“锁定”。



6. 使用下拉菜单浏览有关其他**分配操作**的详细信息。**托管资源**的表由所选的分配操作更新。



更新分配规则

更新分配部署遵循几个重要规则。这些规则决定了已部署的资源会发生什么情况。所请求的更改和要部署或更新的项目资源决定了要采取的操作。

- 角色分配
  - 如果角色或角色代理人(用户、组或应用程序)发生更改，则创建新的角色分配。以前部署的角色分配将会保留。
- 策略分配数
  - 如果策略分配的参数已发生更改，则更新现有分配。
  - 如果策略分配的定义已发生更改，则会创建一个新的策略分配。以前部署的策略分配将会保留。
  - 如果从蓝图中删除策略分配项目，已部署的策略分配将会保留。
- Azure 资源管理器模板
  - 该模板通过资源管理器作为 PUT 处理。由于每个资源类型以不同的方式处理此操作，因此请查看包含的每个资源的文档，以确定在蓝图运行时该操作的影响。

更新分配上可能出现的错误

更新分配时，在执行期间进行更改可能会导致中断。一个示例是在部署完成后更改资源组的位置。Azure 资源管理器支持的任何更改都可以进行，但是任何会在 Azure 资源管理器中导致错误的更改也将导致分配失败。

可以更新分配的次数没有限制。如果发生错误，请确定该错误并对分配进行其他更新。示例

错误场景：

- 不正确的参数
- 已经存在的对象
- Azure 资源管理器不支持的更改

后续步骤

- 了解蓝图生命周期。
- 了解如何使用静态和动态参数。
- 了解如何自定义蓝图排序顺序。
- 了解如何利用蓝图资源锁定。
- 使用一般故障排除在蓝图的分配期间解决问题。

为蓝图操作员配置环境

2019/9/4 • • Edit Online

可以将蓝图定义和蓝图分配的管理分配给不同的团队。在运营团队负责管理这些集中控制的蓝图定义的分配时，架构师或调控团队通常负责管理蓝图定义的生命周期管理。

蓝图运算符内置的基于角色的访问控制 (RBAC) 专用于在此类方案中使用。角色允许操作类型团队管理组织蓝图定义的分配，但不允许对其进行修改。执行此操作需要在 Azure 环境中进行一些配置，本文介绍必要的步骤。

向蓝图运算符授予权限

第一步是向要分配蓝图的帐户或安全组 (推荐) 授予蓝图操作员角色。应在管理组层次结构中的最高级别完成此操作，该管理组层次结构包含操作团队应对其进行蓝图分配访问的所有管理组和订阅。建议在授予这些权限时遵循最低权限原则。

1. 您创建安全组并添加成员
2. 向帐户或安全组添加蓝图操作员角色分配

用户-分配托管标识

蓝图定义可以使用系统分配的或用户分配的托管标识。但是，在使用蓝图运算符角色时，需要将蓝图定义配置为使用用户分配的托管标识。此外，要向其授予蓝图操作员角色的帐户或安全组需要向用户分配的托管标识授予托管标识操作员角色。如果没有此权限，则蓝图分配由于缺少权限而失败。

1. 创建用户分配的托管标识，供分配的蓝图使用
2. 向帐户或安全组添加托管标识操作员的角色分配。将角色分配的范围限定为新的用户分配的托管标识。
3. 作为蓝图运算符，分配一个使用新的用户分配的托管标识的蓝图。

后续步骤

- 了解蓝图生命周期。
- 了解如何使用静态和动态参数。
- 了解如何自定义蓝图排序顺序。
- 了解如何利用蓝图资源锁定。
- 使用一般故障排除在蓝图的分配期间解决问题。

排查使用 Azure 蓝图时出现的错误

2019/9/5 • • Edit Online

创建或分配蓝图时可能会出现问题。本文描述可能会发生的各种错误及其解决方法。

查找错误详细信息

将蓝图分配到作用域是许多错误产生的原因。分配失败时，蓝图会提供失败部署的详细信息。此信息会指出存在的问题，以便可以修复问题并确保后续部署成功进行。

1. 在左侧窗格中，选择“所有服务”。搜索并选择“蓝图”。
2. 从左侧页面中选择 "**分配的蓝图**"，然后使用 "**搜索**" 框筛选蓝图分配，查找失败的分配。还可以按“预配状态”列对分配表进行排序，集中查看失败的分配项。
3. 左键单击状态为 "*失败*" 的蓝图，或右键单击并选择 "**查看分配详细信息**"。
4. 蓝图分配页面顶部有一个红色横幅警告，指出此分配已失败。单击横幅任意位置可获取更多详细信息。

错误通常是由某个项目导致的，而不是由蓝图整体导致的。如果某个项目创建密钥保管库但是 Azure Policy 阻止密钥保管库创建，则整个分配将失败。

常规错误

场景：策略冲突

问题

由于策略冲突而导致模板部署失败。

原因

如下多个原因可能会导致策略与部署相冲突：

- 正在创建的资源受到策略的限制（通常为 SKU 或位置限制）
- 部署是由策略配置的设置字段（通常带有标记）

分辨率

更改蓝图，使其不与错误详细信息中的策略冲突。如果无法进行此更改，替代方法是更改策略分配的作用域，以使蓝图不再与策略冲突。

场景：蓝图参数是一个函数

问题

作为函数的蓝图参数在传递到项目之前处理。

原因

将使用函数的蓝图参数（例如 `[resourceGroup().tags.myTag]`）传递到项目会导致在项目上设置的函数的处理结果而不是动态函数。

分辨率

若要将函数作为参数传递，请使用 `[` 转义整个字符串，使蓝图参数如 `[[resourceGroup().tags.myTag]`。转义字符会导致蓝图在处理蓝图时将值视为字符串。然后，蓝图将该函数放置在项目中，使其按预期动态化。有关详细信息，请参阅Azure 资源管理器模板中的语法和表达式。

后续步骤

如果你的问题未在本文中列出，或者无法解决问题，请访问以下渠道之一获取更多支持：

- 通过Azure 论坛获取 azure 专家的解答。
- 与 @AzureSupport（Microsoft Azure 官方帐户）联系，它可以将 Azure 社区引导至适当的资源来改进客户体验：提供解答、支持和专业化服务。
- 如需更多帮助，可以提交 Azure 支持事件。请转到 Azure 支持站点并选择 获取支持。

与 Azure 蓝图一起使用的函数

2019/9/4 • • Edit Online

Azure 蓝图提供使蓝图定义更动态的函数。这些函数可用于蓝图定义和蓝图项目。资源管理器模板项目除了通过蓝图参数获取动态值外，还支持资源管理器函数的全部使用。

支持以下函数：

- artifacts
- concat
- parameters
- resourceGroup
- resourceGroups
- subscription

诸如

```
artifacts(artifactName)
```

返回使用该蓝图项目输出填充的属性的对象。

Parameters

参数	必填	类型	描述
artifactName	是	string	蓝图项目的名称。

返回值

输出属性的对象。输出属性取决于所引用的蓝图项目的类型。所有类型都遵循以下格式：

```
{
  "outputs": {collectionOfOutputProperties}
}
```

策略分配项目

```
{
    "outputs": {
        "policyAssignmentId": "{resourceId-of-policy-assignment}",
        "policyAssignmentName": "{name-of-policy-assignment}",
        "policyDefinitionId": "{resourceId-of-policy-definition}",
    }
}
```

资源管理器模板项目

返回对象的输出属性在资源管理器模板中定义，并由部署返回。

角色分配项目

```
{
    "outputs": {
        "roleAssignmentId": "{resourceId-of-role-assignment}",
        "roleDefinitionId": "{resourceId-of-role-definition}",
        "principalId": "{principalId-role-is-being-assigned-to}",
    }
}
```

示例

ID 为_myTemplateArtifact_的资源管理器模板项目, 其中包含以下示例输出属性:

```
{
    "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
    ...
    "outputs": {
        "myArray": {
            "type": "array",
            "value": ["first", "second"]
        },
        "myString": {
            "type": "string",
            "value": "my string value"
        },
        "myObject": {
            "type": "object",
            "value": {
                "myProperty": "my value",
                "anotherProperty": true
            }
        }
    }
}
```

从_myTemplateArtifact_示例中检索数据的一些示例如下:

表达式	类型	REPLTEST1
`[artifacts("myTemplateArtifact").outputs.myArray]`	阵列	["first", "second"]
`[artifacts("myTemplateArtifact").outputs.myArray[0]]`	String	1
`[artifacts("myTemplateArtifact").outputs.myString]`	String	"我的字符串值"
`[artifacts("myTemplateArtifact").outputs.myObject]`	Object	{"t.myproperty": "my value", "anotherProperty": true}
`[artifacts("myTemplateArtifact").outputs.myObject.myProperty]`	String	"my value"
`[artifacts("myTemplateArtifact").outputs.myObject.anotherProperty]`	Bool	True

concat

`concat(string1, string2, string3, ...)`

组合多个字符串值并返回串联的字符串。

Parameters

参数	必填	TYPE	描述
string1	是	string	串联的第一个值。
其他参数	否	string	串联的顺序的其他值

返回值

串联值的字符串。

备注

Azure 蓝图函数不同于 Azure 资源管理器模板功能, 因为它仅适用于字符串。

示例

```
concat(parameters('organizationName'), '-vm')
```

参数

```
parameters(parameterName)
```

返回蓝图参数值。指定的参数名称必须在蓝图定义或蓝图项目中定义。

Parameters

参数	必填	类型	描述
parameterName	是	string	要返回的参数名称。

返回值

指定的蓝图或蓝图项目参数的值。

备注

Azure 蓝图函数不同于 Azure 资源管理器模板功能, 因为它仅适用于蓝图参数。

示例

在蓝图定义中定义参数_principalIds_ :

```
{
    "type": "Microsoft.Blueprint/blueprints",
    "properties": {
        ...
        "parameters": {
            "principalIds": {
                "type": "array",
                "metadata": {
                    "displayName": "Principal IDs",
                    "description": "This is a blueprint parameter that any artifact can reference. We'll
display these descriptions for you in the info bubble. Supply principal IDs for the users,groups, or service
principals for the RBAC assignment.",
                    "strongType": "PrincipalId"
                }
            }
        },
        ...
    }
}
```

然后, 将_principalIds_用作蓝图项目 `parameters()` 中的的参数:

```
{
    "type": "Microsoft.Blueprint/blueprints/artifacts",
    "kind": "roleAssignment",
    ...
    "properties": {
        "roleDefinitionId": "/providers/Microsoft.Authorization/roleDefinitions/8e3af657-a8ff-443c-a75c-
2fe8c4bcb635",
        "principalIds": "[parameters('principalIds')]",
        ...
    }
}
```

resourceGroup

`resourceGroup()`

返回表示当前资源组的对象。

返回值

返回的对象采用以下格式：

```
{
  "name": "{resourceGroupName}",
  "location": "{resourceGroupLocation}",
}
```

备注

Azure 蓝图功能不同于 Azure 资源管理器模板功能。此 `resourceGroup()` 函数不能在订阅级别项目或蓝图定义中使用。它只能在属于资源组项目的蓝图项目中使用。

`resourceGroup()` 函数的一个常见用途是在与资源组项目相同的位置创建资源。

示例

若要使用资源组的位置，请在蓝图定义中或在分配期间设置为另一个项目的位置，在蓝图定义中声明资源组占位符对象。在此示例中，_NetworkingPlaceholder_是资源组占位符的名称。

```
{
    "type": "Microsoft.Blueprint/blueprints",
    "properties": {
        ...
        "resourceGroups": {
            "NetworkingPlaceholder": {
                "location": "eastus"
            }
        }
    }
}
```

然后，在 `resourceGroup()` 面向资源组占位符对象的蓝图项目的上下文中使用该函数。在此示例中，模板项目部署到_NetworkingPlaceholder_资源组中，并提供参数_resourceLocation_，并将_NetworkingPlaceholder_资源组位置动态填充到模版. 可以在蓝图定义上静态定义_NetworkingPlaceholder_资源组的位置，也可以在分配过程中动态定义该位置。无论是哪种情况，模板项目都作为参数提供，并使用它将资源部署到正确的位置。

```
{
  "type": "Microsoft.Blueprint/blueprints/artifacts",
  "kind": "template",
  "properties": {
      "template": {
        ...
      },
      "resourceGroup": "NetworkingPlaceholder",
      ...
      "parameters": {
        "resourceLocation": {
          "value": "[resourceGroup().location]"
        }
      }
  }
}
```

resourceGroups

`resourceGroups(placeholderName)`

返回一个对象, 该对象表示指定的资源组项目。与 `resourceGroup()` 要求项目上下文的不同, 此函数用于获取特定资源组占位符的属性, 而不是在该资源组的上下文中。

Parameters

参数	必填	类型	描述
placeholderName	是	string	要返回的资源组项目的占位符名称。

返回值

返回的对象采用以下格式:

```
{
  "name": "{resourceGroupName}",
  "location": "{resourceGroupLocation}",
}
```

示例

若要使用资源组的位置, 请在蓝图定义中或在分配期间设置为另一个项目的位置, 在蓝图定义中声明资源组占位符对象。在此示例中, _NetworkingPlaceholder_是资源组占位符的名称。

```
{
    "type": "Microsoft.Blueprint/blueprints",
    "properties": {
        ...
        "resourceGroups": {
            "NetworkingPlaceholder": {
                "location": "eastus"
            }
        }
    }
}
```

然后, 使用 `resourceGroups()` 任何蓝图项目上下文中的函数获取对资源组占位符对象的引用。在此示例中, 模板项目部署在_NetworkingPlaceholder_资源组外部, 并提供参数_artifactLocation_ , 并将_NetworkingPlaceholder_资源组位置动态填充到模版. 可以在蓝图定义上静态定义_NetworkingPlaceholder_资源组的位置, 也可以在分配过程中

动态定义该位置。无论是哪种情况，模板项目都作为参数提供，并使用它将资源部署到正确的位置。

```
{
  "kind": "template",
  "properties": {
      "template": {
          ...
      },
      ...
      "parameters": {
        "artifactLocation": {
          "value": "[resourceGroups('NetworkingPlaceholder').location]"
        }
      }
  },
  "type": "Microsoft.Blueprint/blueprints/artifacts",
  "name": "myTemplate"
}
```

subscription

`subscription()`

返回有关当前蓝图分配的订阅的详细信息。

返回值

返回的对象采用以下格式：

```
{
    "id": "/subscriptions/{subscriptionId}",
    "subscriptionId": "{subscriptionId}",
    "tenantId": "{tenantId}",
    "displayName": "{name-of-subscription}"
}
```

示例

使用订阅的显示名称和 `concat()` 函数创建作为参数名称传递到模板项目的命名约定。

```
{
  "kind": "template",
  "properties": {
      "template": {
          ...
      },
      ...
      "parameters": {
        "resourceName": {
          "value": "[concat(subscription().displayName, '-vm')]"
        }
      }
  },
  "type": "Microsoft.Blueprint/blueprints/artifacts",
  "name": "myTemplate"
}
```

后续步骤

- 了解蓝图生命周期。
- 了解如何使用静态和动态参数。

- 了解如何自定义蓝图排序顺序。
- 了解如何利用蓝图资源锁定。
- 了解如何更新现有分配。
- 使用一般故障排除在蓝图的分配期间解决问题。