公共云中的高可用性故障转移

本章介绍如何配置主用/备份故障转移，以在公共云环境（如 Microsoft Azure）中实现 ASA Virtual 的高可用性。

关于公共云中的故障转移

为确保冗余，您可以在公共云环境中部署采用主用/备份高可用性 (HA) 配置的 ASA Virtual 。公共云中的高可用性实施无状态主用/备份解决方案，允许主用 ASA Virtual 故障触发系统自动执行故障转移以切换到备份 ASA Virtual。

以下列表介绍高可用性公共云解决方案中的主要组件：

- **主用 ASA Virtual** - 高可用性对中设置为处理高可用性对等体的防火墙流量的 ASA Virtual。
- **备份 ASA Virtual**- ASA Virtual HA 对中未在处理防火墙流量并在主用 ASA Virtual 发生故障的情况下接管作为主用 ASA Virtual 的 。它之所以被称为备份而不是备用 ASAv，是因为它在发生故障转移时不会获取其对等体的身份。
- **HA 代理**- 在 ASA Virtual 上运行并确定 ASA Virtual的 HA 角色，检测其 HA 对等体的故障以及根据其 HA 角色执行操作的轻量级进程。

在物理 ASA 和非公共云虚拟 ASA 上，系统使用免费 ARP 请求处理故障转移条件，在此请求中，备份 ASA 发出免费 ARP，指示其现在与主用 IP 和 MAC 地址相关联。大多数公共云环境不允许此性质的广播流量。因此，公共云中的高可用性配置要求在发生故障转移时重新启动持续连接。

备份设备会对主用设备的运行状况进行监控，以便确定是否符合特定的故障转移条件。如果符合这些条件，将执行故障转移。故障转移时间可能在几秒到一分多钟之间变化，具体取决于公共云基础设施的响应能力。

关于主用/备份故障转移

在主用/备份故障转移中，一台设备是主用设备。它会传送流量。备份设备不会主动与主用设备传递流量或交换任何配置信息。主用/备份故障转移允许您使用备份 ASA Virtual 设备接管故障设备的功能。主用设备出现故障时将变为备份状态，同时备份设备变为主用状态。

主/辅助角色和主用/备份状态

当设置主用/备份故障转移时，需要将一台设备配置为主设备，将另一台配置为辅助设备。此时，两台设备作为两个单独的设备，进行设备和策略配置，以及用于事件、控制面板、报告和运行状况监控。

故障转移对中两台设备之间的主要差别与哪一设备为主用设备，哪一设备为备份设备（即，哪一台设备会主动传送流量）有关。虽然两台设备都能传递流量，但只有主设备会响应负载均衡器的探测，并设定任何已配置的路由将其用作路由目标。备份设备的主要功能是监控主设备的运行状况。如果两台设备同一时间启动（并且运行状况相同），则主设备总是会成为主用设备。

故障转移连接

备份 ASA Virtual 使用在 TCP 上建立的故障转移连接来监控主用 ASA Virtual 的运行状况：

- 主用 ASA Virtual 通过打开一个 侦听端口来充当连接服务器。
- 备份 ASA Virtual 使用 连接端口连接到主用 ASA Virtual 。
- 通常情况下， 侦听端口 和 连接端口 相同，除非您的配置要求在 ASA Virtual 设备之间进行某种类型的网络地址转换。

故障转移连接的状态可用于检测主用 ASA Virtual的故障。当备份 ASA Virtual 看到故障转移连接断开时，它会将主用 ASA Virtual 视为 出现故障。同样，如果备份 ASA Virtual 没有收到发送至主用设备的保持连接消息的响应，它也会将主用 ASA Virtual 视为 出现故障

相关主题

轮询和 Hello 消息

备份 ASA Virtual 通过故障转移连接发送 Hello 消息到主用 ASA Virtual ，并预期在回复中收到 Hello 响应。消息定时使用轮询间隔，即备份 ASA Virtual 设备收到 Hello 响应与发送下一条 Hello 消息之

间的时段。接收响应由被称为保持时间的接收超时来执行。如果接收 Hello 响应发生超时，则主用 ASA Virtual 被视为出现故障。

轮询间隔和保持时间间隔均为可配置参数；请参阅配置故障转移条件和其他设置，第 11 页。

启动时的主用设备确定

主用设备按以下方式确定：

- 如果某台设备启动，并检测到对等体已作为主用设备运行，则该设备将成为备份设备。
- 如果某台设备启动，并且未检测到对等体，则该设备会成为主用设备。
- 如果两台设备同时启动，则主设备成为主用设备，辅助设备成为备份设备。

故障转移事件

在主用/备份故障转移中，故障转移会在设备级别进行。下表显示了每个故障事件的故障转移操作。对于每种故障事件，该表显示了故障转移策略（故障转移或禁用故障转移）、主用设备执行的操作、备份设备执行的操作，以及有关故障转移条件和操作的所有特别说明。

表 *1:* 故障转移事件

故障事件	策略	主用设备操作	备份操作	说明
备份设备看到故障转移连接关闭	故障转移	不适用	成为主用设备 将主用设备标记为发生故障	这是标准的故障转移使用案例。
主用设备看到故障转移连接关闭	禁用故障转移	将备份设备标记为发生故障	n/a	到非主用设备的故障转移永远不会发生。
主用设备在故障转移链路上看到 TCP 超时	禁用故障转移	将备份设备标记为发生故障	无需操作	如果主用设备未从备份设备获取响应，则不应发生故障转移。
备份设备在故障转移链路上看到 TCP 超时	故障转移	不适用	成为主用设备 将主用设备标记为发生故障 尝试向主用设备发送故障转移命令	备份设备假定主用设备无法继续操作并接管控制权。 如果主用设备仍处于正常运行状态，但无法及时发送响应，备份设备将会发送故障转移命令到主用设备。

故障事件	策略	主用设备操作	备份操作	说明
主用身份验证失败	禁用故障转移	无需操作	无需操作	由于备份设备正在更改路由表，因此它是唯一需要向 Azure 进行身份验证的设备。 主用设备是否已向 Azure 进行身份验证无关紧要。
备份身份验证失败	禁用故障转移	将备份设备标记为未进行身份验证	无需操作	如果备份设备未向 Azure 进行身份验证，则无法进行故障转移。
主用设备有意启动故障转移	故障转移	变为备份设备	成为主用设备	主用设备通过关闭故障转移链路连接来启动故障转移。 备份设备看到连接关闭，并成为主用设备。
备份设备有意启动故障转移	故障转移	变为备份设备	成为主用设备	备份设备通过发送故障转移消息到主用设备来启动故障转移。 当主用设备看到此消息时关闭连接并将成为备份设备。 备份设备看到连接关闭，并成为主用设备。
以前的主用设备恢复	禁用故障转移	变为备份设备	将伙伴设备标记为备份设备	除非绝对必要，否则不应发生故障转移。
主用设备看到发自备份设备的故障转移消息	故障转移	变为备份设备	成为主用设备	由用户启动手动故障转移时，或者当备份设备看到TCP超时，但主用设备能够从备份设备接收消息时可能发生。

准则和限制

本节包括此功能的准则和限制。

公共云中的高可用性ASA Virtual 故障转移

为确保冗余，您可以在公共云环境中部署采用主用/备份高可用性 (HA) 配置的 ASA Virtual 。

- 仅在 Microsoft Azure 公共云上受支持；配置 ASA Virtual VM 时，支持的最大数量 Vcpu 为 8；支持的最大内存为 64GB RAM。有关受支持实例的详细列表，请参阅 ASA Virtual 入门指南。
- 实施无状态主用/备份解决方案，允许主用 ASA Virtual 故障触发系统自动执行故障转移以切换到备份 ASA Virtual。

限制

- 故障转移按秒级别而不是毫秒级别执行。
- 高可用性角色的确定和以高可用性设备角色参与部署的能力取决于高可用性对等体之间以及高可用性设备与 Azure 基础设施之间的 TCP 连接。有几种情况下， ASA Virtual 将无法以高可用性设备角色参与部署：
  - 无法建立到其高可用性对等体的故障转移连接。
  - 无法从 Azure 检索身份验证令牌。
  - 无法与 Azure 进行身份验证。
- 没有从主用设备到备份设备的配置同步。每台设备必须单独配置相似的配置，用于处理故障转移流量。
- 故障转移路由表限制

  关于公共云中 HA 的路由表：
  - 您最多可以配置 16 个路由表。
  - 在路由表中，最多可以配置 64 个路由。

  在每种情况下，系统都会在达到限制时向您发出警报，并建议删除路由表或路由并重试。
- 无 ASDM 支持
- 没有 IPSec 远程访问 VPN 支持。

注释 有关公共云中受支持的 VPN 拓扑的信息，请参阅《思科自适应安全虚拟设备 (ASAv) 快速入门指南 》。

- ASA Virtual 虚拟机实例必须在同一可用性集中。如果您是 Azure 中的当前 ASA Virtual 用户，您将无法从现有部署升级到高可用性部署。您必须删除您的实例，然后部署 Azure 市场提供的 ASA Virtual 4 NIC 高可用性产品。

公共云中的故障转移许可

ASA Virtual 使用思科智能软件许可。需要安装智能许可证才能正常运行。每个 ASA Virtual 必须使用 ASA Virtual 平台许可证单独进行许可。在安装许可证之前，吞吐量限制为 100 kbps，以便您可以执行初步连接测试。请参阅 思科 ASA 系列功能许可证 页面，查找 ASA Virtual的精确许可要求。

公共云中的故障转移默认值

默认情况下，故障转移策略包含以下内容：

- 仅无状态故障转移。
- 每台设备必须单独配置相似的配置，用于处理故障转移流量。
- 故障转移 TCP 控制端口号是 44442。
- Azure 负载均衡器运行状况探测端口号是 44441。
- 设备轮询时间为 5 秒。
- 设备保持时间为 15 秒。
- ASA Virtual 响应主接口 (Management 0/0) 上的运行状况探测。
- 在主接口 (Management 0/0) 上执行 Azure 服务主体 ASA Virtual 身份验证。

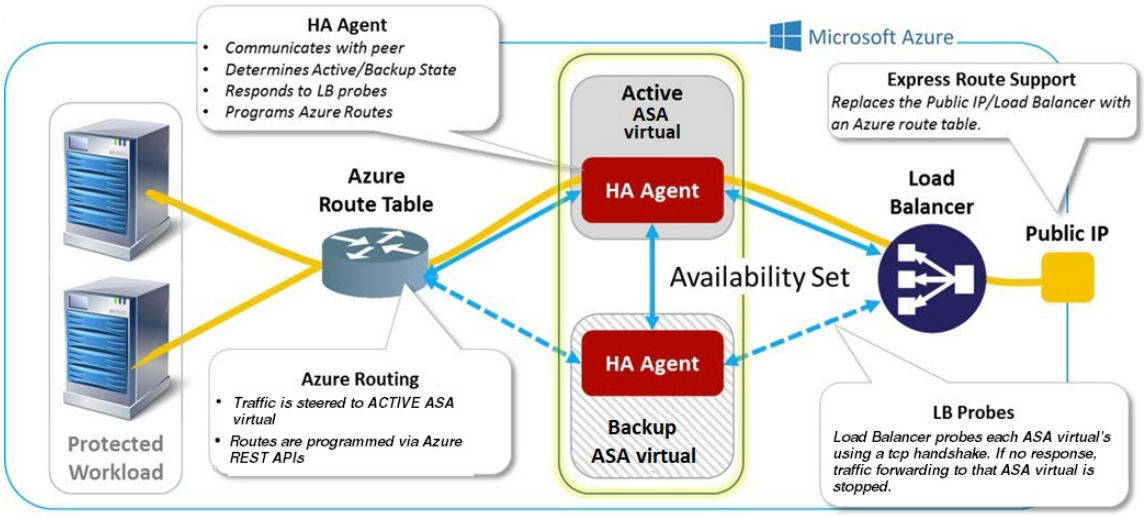
注释 如需获取更改故障转移端口号、运行状况探测端口号、轮询时间和主接口的选项，请参阅配置可选故障转移参数，第 11 页。

关于 Microsoft Azure 中的 ASA Virtual 高可用性

下图简要显示了 Azure 中的 ASA Virtual 高可用性部署的情况。受保护的工作负载位于主用/备份故障转移配置中的两个 ASA Virtual 实例后面。Azure 负载均衡器使用三次 TCP 握手来探测这两个 ASA Virtual 设备。主用 ASA Virtual 完成三次握手，指示其处于正常运行状态，而备份 ASA Virtual 则特意不响应。由于未对负载均衡器做出响应，在负载均衡器看来，备份 ASA Virtual 处于非正常运行状况，进而导致负载均衡器不会向其发送流量。

发生故障转移时，主用 ASA Virtual 停止响应负载均衡器探测，备份 ASA Virtual 则开始响应，从而导致所有新连接被发送到备份 ASA Virtual。备份 ASA Virtual 发送 API 请求至 Azure 交换矩阵以修改路由表，将流量从主用设备重定向至备份设备。此时，备份 ASA Virtual 成为主用设备，主用设备则成为备份设备或离线，具体取决于发生故障转移的原因。

图 *1: Azure* 中的*ASA Virtual* 高可用性部署



为了能够自动进行 API 调用以修改 Azure 路由表， ASA Virtual 高可用性设备需要具有 Azure Active Directory 凭证。Azure 采用服务主体的概念，简单来说，就是服务帐户。服务主体允许您调配帐户，前提是该帐户仅具有在预定义的 Azure 资源集内运行任务所需的足够权限和范围。

通过两个步骤可启用 ASA Virtual 高可用性部署，以使用服务主体管理您的 Azure 订用：

1. 创建 Azure Active Directory 应用和服务主体；请参阅关于 Azure 服务主体 ，第 7 页。
2. 配置 ASA Virtual 实例以使用服务主体向 Azure 进行身份验证；请参阅 配置 Azure 服务主体的身份验证凭证 ，第 13 页。

相关主题

有关负载均衡器的更多信息，请参阅 Azure 文档。

关于 Azure 服务主体

当您的应用需要访问或修改 Azure 资源，例如路由表时，您必须设置 Azure Active Directory (AD) 应用并为其分配所需的权限。这是在您自己的凭证下运行应用的首选方法，因为：

- 您可以向应用身份分配不同于您自己权限的其他权限。通常，这些权限严格局限于应用需要执行的任务。
- 如果您的责任发生变化，您无需更改应用的凭证。
- 您可以使用证书，在执行无人值守的脚本时自动进行身份验证。

在 Azure 门户注册 Azure AD 应用时，将在您的 Azure AD 租户中创建两个对象：一个应用对象和一个服务主体对象。

- **应用对象** - Azure AD 应用由其仅有的一个应用对象定义，该应用对象位于在其中注册应用的 Azure AD 租户中，此租户也称为应用的“主”租户。

- **服务主体对象** - 服务主体对象定义在特定租户中使用应用的策略和权限，从而为安全主体在运行时代表该应用提供基础。

Azure 在 *Azure* 资源管理器文档中提供了关于如何创建 Azure AD 应用和服务主体的说明。有关完整的说明，请参阅以下主题：

- 使用门户创建可以访问资源的 Azure Active Directory 应用和服务主体
- 使用 Azure PowerShell 创建服务主体以访问资源

注释 设置服务主体后，获取**目录 ID**、**应用 ID** 和**密钥** 。配置 Azure 身份验证需要这些信息；请参阅配置 Azure 服务主体的身份验证凭证 ， 第 13 页。

Azure 中的 ASA Virtual 高可用性配置要求

要部署与#unique_418 unique_418_Connect_42_fig_cgx_dlh_h1b中所述配置相似的配置，您需要以下信息：

- Azure 身份验证信息（请参阅关于 Azure 服务主体 ， 第 7 页）：
  - 目录 ID
  - 应用 ID
  - 秘密密钥
- Azure 路由信息（请参阅配置 Azure 路由表 ， 第 14 页）：
  - Azure 订用 ID
  - 路由表资源组
  - 表名称
  - 地址前缀
  - 下一跳地址
- ASA 配置（请参阅配置主用/备份故障转移 ， 第 9 页、公共云中的故障转移默认值 ， 第 6 页）：
  - 主用/备份 IP 地址
  - 高可用性代理通信端口
  - 负载均衡器探测端口
  - 轮询间隔

注释 在主设备和辅助设备上配置基本故障转移设置。没有主设备到辅助设备的配置同步。每台设备必须单独配置相似的配置，用于处理故障转移流量。

配置主用/备份故障转移

要配置主用/备份故障转移，请在主设备和辅助设备上配置基本故障转移设置。没有主设备到辅助设备的配置同步。每台设备必须单独配置相似的配置，用于处理故障转移流量。

开始之前

- 在 Azure 可用性集中部署您的 ASA Virtual 高可用性对。
- 提供您的 Azure 环境信息，包括您的 Azure 订用 ID 和服务主体的 Azure 身份验证凭证。

配置主用/备份故障转移的主设备

遵循本节介绍的步骤，配置主用/备份故障转移配置中的主设备。这些步骤提供了在主设备上启用故障转移所需的最小配置。

开始之前

- 在单情景模式下，可在系统执行空间中配置这些设置。

示例

以下示例显示如何配置主/主用设备的故障转移参数：

```
ciscoasa(config)# failover cloud unit primary
ciscoasa(config)# failover cloud peer ip 10.4.3.5 port 4444
ciscoasa(config)#
```

您在此处输入的对等体 IP 地址必须是 ASA 虚拟 HA 对等体上管理接口的 IP 地址。

下一步做什么

根据需要配置其他参数：

- 配置备份设备；请参阅配置主用/备份故障转移的辅助设备，第 10 页。
- 配置 Azure 身份验证；请参阅配置 Azure 服务主体的身份验证凭证，第 13 页。
- 配置 Azure 路由信息；请参阅配置 Azure 路由表，第 14 页。
- 查看其他参数；请参阅配置故障转移条件和其他设置，第 11 页。

配置主用/备份故障转移的辅助设备

遵循本节介绍的步骤，配置主用/备份故障转移配置中的辅助设备。这些步骤提供了启用故障转移到辅助设备所需的最小配置。

开始之前

- 在单情景模式下，可在系统执行空间中配置这些设置。

过程

步骤 1 将此设备指定为备份设备：

failover cloud unit secondary

步骤 2 为故障转移链路分配主用 IP 地址：

failover cloud peer ip *ip-address* [**port** *port-number*]

此 IP 地址用于建立到高可用性对等体的 TCP 故障转移控制连接。尝试打开到高可用性对等体（可能已经是主用设备）的故障转移连接时使用此端口。如果在高可用性对等体之间部署了 NAT，则可能需要在此处配置该端口。大多数情况下不需要配置该端口。

您在此处输入的对等体 IP 地址必须是 ASA 虚拟 HA 对等体上管理接口的 IP 地址。

示例

以下示例显示如何配置辅助/备份设备的故障转移参数：

```
failover cloud unit secondary
failover cloud peer ip 10.4.3.4 port 4444
```

下一步做什么

根据需要配置其他参数：

- 配置 Azure 身份验证；请参阅配置 Azure 服务主体的身份验证凭证，第 13 页。
- 配置 Azure 路由信息；请参阅配置 Azure 路由表，第 14 页。
- 查看其他参数；请参阅配置故障转移条件和其他设置，第 11 页。

配置可选故障转移参数

您可以在必要时自定义故障转移设置。

配置故障转移条件和其他设置

有关您可在本节中更改的许多参数的默认设置，请参阅公共云中的故障转移默认值，第 6 页。

开始之前

- 在单情景模式下，可在系统执行空间中配置这些设置。
- 在主设备和辅助设备上配置这些设置。配置未从主设备同步到辅助设备。

过程

步骤 1 指定 TCP 端口以用于与高可用性对等体的通信：

failover cloud port control *port-number*

示例：

```
ciscoasa(config)# failover cloud port control 4444
```

port-number 参数为用于对等通信的 TCP 端口分配编号。

这将配置处于主用设备角色时，在其上接受连接的故障转移连接 TCP 端口。这是在备份 ASA Virtual 连接到的主用 ASA Virtual 上开放的端口。

注释
我们建议您保持默认值 44442，它是两个高可用性对等体的默认值。如果您更改了其中一个高可用性对等体的默认值，则最佳做法是对另一个高可用性设备进行相同的更改。

步骤 2 更改设备的轮询和保持时间：

failover polltime *poll_time* [**holdtime** *time*]

示例：

```
ciscoasa(config)# failover polltime 10 holdtime 30
```

polltime 的范围为 1 至 15 秒。保持时间用于确定从一个呼叫数据包丢失到将设备标记为发生故障之间的时长。 **holdtime** 的范围介于 3 和 60 秒之间。输入的保持时间值不得短于设备轮询时间的 3 倍。设置的轮询时间越快，ASA 便可越快检测到故障并触发故障转移。但是，当网络临时堵塞时，更快的检测会导致不必要的切换。

步骤 3 指定用于 Azure 负载均衡器运行状况探测的 TCP 端口：

failover cloud port probe *port-number*

示例：

```
ciscoasa(config)# failover cloud port probe 4443
```

如果您的部署使用 Azure 负载均衡器，则主用 ASA Virtual 必须响应来自负载均衡器的 TCP 探测，以便将传入连接定向至主用设备。

步骤 4 指定 Azure 负载均衡器运行状况探测器的辅助接口：

failover cloud port probe *port-number* **interface** *if-name*

示例：

```
ciscoasa(config)# failover cloud port probe 4443 interface inside
```

云 HA 中使用的 TCP 探测的源 IP 地址为 168.63.129.16。此地址是 Azure 的虚拟公共 IP 地址。此地址既是 Azure DHCP 数据包的源地址，也是 Azure 中 DNS 名称服务器的地址。

默认情况下，根据 ASA 路由表， ASA Virtual 响应可到达 168.63.129.16 的探测。由于存在默认路由，这最终成为主接口 (Management0/0)。

要在除 Management0/0 以外的接口上支持负载均衡器，请为端口探测器配置另一个接口。您还需要配置两条静态路由：一条用于主接口，一条用于为负载均衡器探测器配置的接口。

步骤 5 为主接口和为负载均衡器探测器配置的接口添加静态路由：

route *if-name dest_ip mask gateway_ip* **[distance]**

示例：

```
ciscoasa(config)# route outside 168.63.129.16 255.255.255.255 10.22.0.1 1
ciscoasa(config)# route inside 168.63.129.16 255.255.255.255 10.22.1.1 2
```

distance 参数是路由的管理距离。如果未指定值，则默认值为 **1**。管理距离是用于比较不同路由协议之间路由的参数。当存在通向同一目标 (168.63.129.16) 的多个路由时，路由的管理距离即可确定优先级。

管理距离为 1 的主接口（外部）的静态路由将主接口设定为发往 168.63.129.16 的数据包的首选接口，但也允许为负载均衡器探测器配置的接口将数据包发送到 168.63.129.16。

注释
响应探测的机制是在接口上创建 TCP 套接字。云 HA 使用 168.63.129.16 的路由查找来决定要在哪个接口上创建套接字。由于存在默认路由，这最终成为主接口。如果没有为探测配置接口的静态路由，ASA 将不会响应负载均衡器发送的 TCP 数据包。

配置 Azure 服务主体的身份验证凭证

您可以使 ASA Virtual 高可用性对等体使用 Azure 服务主体来访问或修改 Azure 资源，例如路由表。您必须设置一个 Azure Active Directory (AD) 应用，并为其分配所需的权限。以下命令允许 ASA Virtual 使用服务主体向 Azure 进行身份验证。有关 Azure 服务主体的详细信息，请参阅《ASA Virtual 快速入门指南》的 Azure 一章。

开始之前

- 在单情景模式下，可在系统执行空间中配置这些设置。
- 在主设备和辅助设备上配置这些设置。配置未从主设备同步到辅助设备。

过程

步骤 1 配置 Azure 服务主体的 Azure 订用 ID：

failover cloud subscription-id *subscription-id*

示例：

```
(config)# failover cloud subscription-id ab2fe6b2-c2bd-44
```

修改Azure路由表需要Azure订用ID，例如，当云高可用性用户想要将内部路由定向至主用设备时。

步骤 2 配置 Azure 服务主体的凭证信息：

failover cloud authentication {**application-id** | **directory-id** | **key**}

要在故障转移期间更改 Azure 路由表，您需要从 Azure 基础设施获取访问密钥，才能访问路由表。您可以使用应用 ID、目录 ID 以及控制高可用性对的 Azure 服务主体的密钥来获取访问密钥。

步骤 3 配置 Azure 服务主体的应用 ID：

failover cloud authentication application-id *appl-id*

示例：

```
(config)# failover cloud authentication application-id dfa92ce2-fea4-67b3-ad2a-6931704e4201
```

当您从 Azure 基础设施请求访问密钥时，需要此应用 ID。

步骤 4 配置 Azure 服务主体的目录 ID：

failover cloud authentication directory-id *dir-id*

示例：

```
(config)# failover cloud authentication directory-id 227b0f8f-684d-48fa-9803-c08138b77ae9
```

当您从 Azure 基础设施请求访问密钥时，需要此目录 ID。

步骤 5 配置 Azure 服务主体的密钥 ID：

failover cloud authentication key *secret-key* [**encrypt**]

示例：

```
(config)# failover cloud authentication key 5yOhH593dtD/O8gzAlWgulrkWz5dH02d2STk3LDbI4c=
```

当您从 Azure 基础设施请求访问密钥时，需要此密钥。如果 **encrypt** 关键字存在，密钥将在 **running-config** 中加密。

配置 Azure 路由表

路由表配置包含在 ASA Virtual 承担主用角色时需要更新的用户定义的 Azure 路由的相关信息。在故障转移时，您需要将内部路由定向至主用设备，主用设备则使用配置的路由表信息将路由自动定向至自身。

注释 您需要同时在主用和备份设备上配置任何 Azure 路由表信息。

开始之前

- 在单情景模式下，可在系统执行空间中配置这些设置。
- 在主设备和辅助设备上配置这些设置。配置未从主设备同步到辅助设备。
- 提供您的 Azure 环境信息，包括您的 Azure 订用 ID 和服务主体的 Azure 身份验证凭证。

过程

步骤 1 配置在故障转移期间需要更新的 Azure 路由表：

failover cloud route-table *table-name* [**subscription-id** *sub-id*]

示例：

```
ciscoasa(config)# failover cloud route-table inside-rt
```

（可选）要更新多个 Azure 订用中用户定义的路由，请包括 **subscription-id** 参数。

示例：

```
ciscoasa(config)# failover cloud route-table inside-rt subscription-id cd5fe6b4-d2ed-45
```

route-table 命令级别的 **subscription-id** 参数将会覆盖在全局级别指定的 Azure 订用 ID。如果您输入 **route-table** 命令，而未指定 Azure 订用 ID，则将使用全局 **subscription-id** 参数。有关 Azure 订用 ID 的信息，请参阅 配置 Azure 服务主体的身份验证凭证，第 13 页。

注释
当您输入 **route-table** 命令时， ASA Virtual 将会切换到 **cfg-fover-cloud-rt** 模式。

步骤 2 配置路由表的 Azure 资源组：

rg *resource-group*

示例：

```
ciscoasa(cfg-fover-cloud-rt)# rg east-rg
```

Azure 中的路由表更新请求需要一个资源组。

步骤 3 配置在故障转移期间需要更新的路由：

route name *route-name* **prefix** *address-prefix* **nexthop** *ip-address*

示例：

```
ciscoasa(cfg-fover-cloud-rt)# route route-to-outside prefix 10.4.2.0/24 nexthop 10.4.1.4
```

地址前缀配置为 IP 地址前缀、斜线 (‘/’) 和数字网络掩码。例如 *192.120.0.0/16*。

示例

完整的配置示例：

```
ciscoasa(config)# failover cloud route-table inside-rt
ciscoasa(cfg-fover-cloud-rt)# rg east-rg
ciscoasa(cfg-fover-cloud-rt)# route route-to-outside prefix 10.4.2.0/24 nexthop 10.4.1.4

ciscoasa(config)# failover cloud route-table outside-rt
ciscoasa(cfg-fover-cloud-rt)# rg east-rg
ciscoasa(cfg-fover-cloud-rt)# route route-to-inside prefix 10.4.1.0/24 nexthop 10.4.2.4
```

启用主用/备份故障转移

在主设备和辅助设备上配置设置后，启用主用/备份故障转移。没有主设备到辅助设备的配置同步。每台设备必须单独配置相似的配置，用于处理故障转移流量。

启用主用/备份故障转移的主设备

遵循本节介绍的步骤，启用主用/备份故障转移配置中的主设备。

开始之前

- 在单情景模式下，可在系统执行空间中配置这些设置。

过程

步骤 1 启用故障转移：

ciscoasa(config)# failover

步骤 2 将系统配置保存到闪存：

ciscoasa(config)# write memory

示例

以下示例显示了主设备的完整配置：

```
ciscoasa(config)# failover cloud unit primary
ciscoasa(config)# failover cloud peer ip 10.4.3.4

ciscoasa(config)# failover cloud authentication application-id dfa92ce2-fea4-67b3-ad2a-693170
ciscoasa(config)# failover cloud authentication directory-id 227b0f8f-684d-48fa-9803-c08138
ciscoasa(config)# failover cloud authentication key 5yOhH593dtD/O8gzAWguH02d2STk3LDbI4c=
ciscoasa(config)# failover cloud authentication subscription-id ab2fe6b2-c2bd-44

ciscoasa(config)# failover cloud route-table inside-rt
ciscoasa(cfg-fover-cloud-rt)# rg east-rg
ciscoasa(cfg-fover-cloud-rt)# route route-to-outside prefix 10.4.2.0/24 nexthop 10.4.1.4

ciscoasa(config)# failover cloud route-table outside-rt
ciscoasa(cfg-fover-cloud-rt)# rg east-rg
ciscoasa(cfg-fover-cloud-rt)# route route-to-inside prefix 10.4.1.0/24 nexthop 10.4.2.4

ciscoasa(config)# failover
ciscoasa(config)# write memory
```

下一步做什么

启用辅助设备。

启用主用/备份故障转移的辅助设备

遵循本节介绍的步骤，启用主用/备份故障转移配置中的辅助设备。

开始之前

- 在单情景模式下，可在系统执行空间中配置这些设置。

过程

步骤 1 启用故障转移：

ciscoasa(config)# **failover**

步骤 2 将系统配置保存到闪存：

ciscoasa(config)# **write memory**

示例

以下示例显示了辅助设备的完整配置：

```
ciscoasa(config)# failover cloud unit secondary
ciscoasa(config)# failover cloud peer ip 10.4.3.5

ciscoasa(config)# failover cloud authentication application-id dfa92ce2-fea4-67b3-ad2a-693170
ciscoasa(config)# failover cloud authentication directory-id 227b0f8f-684d-48fa-9803-c08138
ciscoasa(config)# failover cloud authentication key 5yOhH593dtD/O8gzAWguH02d2STk3LDbI4c=
ciscoasa(config)# failover cloud authentication subscription-id ab2fe6b2-c2bd-44

ciscoasa(config)# failover cloud route-table inside-rt
ciscoasa(cfg-fover-cloud-rt)# rg east-rg
ciscoasa(cfg-fover-cloud-rt)# route route-to-outside prefix 10.4.2.0/24 nexthop 10.4.1.4

ciscoasa(config)# failover cloud route-table outside-rt
ciscoasa(cfg-fover-cloud-rt)# rg east-rg
ciscoasa(cfg-fover-cloud-rt)# route route-to-inside prefix 10.4.1.0/24 nexthop 10.4.2.4

ciscoasa(config)# failover
ciscoasa(config)# write memory
```

管理公共云中的故障转移

本节介绍在启用故障转移后，如何管理云中的故障转移设备，包括如何更改为强制从一台设备故障转移到另一台设备。

强制故障转移

要强制要求备用设备成为主用设备，请执行以下命令。

开始之前

在单情景模式下的系统执行空间中使用此命令。

过程

步骤 1 在备用设备上输入时强制进行故障转移：

failover active

示例：

```
ciscoasa# failover active
```

备用设备将成为主用设备。

步骤 2 在主用设备上输入时强制进行故障转移：

no failover active

示例：

```
ciscoasa# no failover active
```

主用设备将成为备用设备。

更新路由

如果 Azure 中的路由状态与处于 主用 角色的 ASA Virtual 状态不一致，您可以使用以下 EXEC 命令在 ASA Virtual 上强制进行路由更新：

开始之前

在单情景模式下的系统执行空间中使用此命令。

过程

更新主用设备上的路由：

failover cloud update routes

示例：

```
ciscoasa# failover cloud update routes
Beginning route-table updates
Routes changed
```

此命令仅在处于 主用 角色的 ASA Virtual 上有效。如果身份验证失败，命令输出将是 `Route changes failed`。

验证 Azure 身份验证

要在 Azure 中成功完成 ASA Virtual 高可用性部署，服务主体配置必须完整、准确。没有适当的 Azure 授权， ASA Virtual 设备将无法访问处理故障转移和执行路由更新的资源。您可以测试您的故障转移配置，以检测与以下 Azure 服务主体元素相关的错误：

- 目录 ID
- 应用 ID
- 身份验证密钥

开始之前

在单情景模式下的系统执行空间中使用此命令。

过程

测试 ASA Virtual 高可用性配置中的 Azure 身份验证元素：

test failover cloud authentication

示例：

```
ciscoasa(config)# test failover cloud authentication
Checking authentication to cloud provider
Authentication Succeeded
```

如果身份验证失败，命令输出将是 `Authentication Failed`。

如果未正确配置目录 ID 或应用 ID，Azure 将无法识别 REST 请求中所述的资源，以获取身份验证令牌。此条件条目的事件历史记录将显示：

```
Error Connection - Unexpected status in response to access token request: Bad Request
```

如果目录 ID 或应用 ID 正确，但未正确配置身份验证密钥，Azure 将不会授予生成身份验证令牌的权限。此条件条目的事件历史记录将显示：

```
Error Connection - Unexpected status in response to access token request: Unauthorized
```

监控公共云中的故障转移

本节介绍如何监控故障转移状态。

故障转移状态

要监控故障转移状态，请输入以下其中一个命令：

- **show failover**

  显示有关设备的故障转移状态的信息。尚未配置的配置元素的值将显示未配置 。

  仅显示主用设备的路由更新信息。

- **show failover history**

  显示故障转移事件历史记录与时间戳、严重性级别、事件类型和事件文本。

故障转移消息

故障转移系统日志消息

ASA 在优先级别 2 发出大量与故障转移有关的系统日志消息，级别 2 表示一种关键情况。要查看这些消息，请参阅系统日志消息指南。系统日志消息的范围是 1045xx 到 1055xx 之间。

注释 故障转移期间，ASA 按照逻辑先关闭接口，再启动接口，从而生成系统日志消息。这是正常活动。

以下是在切换期间生成的系统日志示例：

```
%ASA-3-105509: (Primary) Error sending Hello message to peer unit 10.22.3.5, error: Unknown
 error
%ASA-1-104500: (Primary) Switching to ACTIVE - switch reason: Unable to send message to
Active unit
%ASA-5-105522: (Primary) Updating route-table wc-rt-inside
%ASA-5-105523: (Primary) Updated route-table wc-rt-inside
%ASA-5-105522: (Primary) Updating route-table wc-rt-outside
%ASA-5-105523: (Primary) Updated route-table wc-rt-outside
%ASA-5-105542: (Primary) Enabling load balancer probe responses
%ASA-5-105503: (Primary) Internal state changed from Backup to Active no peer
%ASA-5-105520: (Primary) Responding to Azure Load Balancer probes
```

每个与公共云部署相关的系统日志均以设备角色：(Primary) 或 (Secondary) 作为前缀。

故障转移调试消息

要查看调试消息，请输入 **debug fover** 命令。有关更多信息，请参阅命令参考。

注释 由于调试输出在CPU进程中分配的高优先级，它可能会极大地影响系统性能。为此，应仅在对特定问题进行故障排除或与思科 TAC 进行故障排除会话过程中使用 **debug fover** 命令。

SNMP 故障转移陷阱

要接收故障转移的 SNMP 系统日志陷阱，请将 SNMP 代理配置为发送 SNMP 陷阱到 SNMP 管理站、定义系统日志主机，并将思科系统日志 MIB 汇集到 SNMP 管理站中。

公共云中的故障转移历史记录

功能名称	版本	功能信息
Microsoft Azure 上的主用/备份故障转移	9.8(200)	引入了此功能。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。