Amazon Directory Service

管理指南

版本 1.0

亚马逊云科技

Amazon Directory Service: 管理指南

Copyright © 2022 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon 的商标和商业外观不得用于任何非 Amazon 的商品或服务，也不得以任何可能引起客户混淆、贬低或诋毁 Amazon 的方式使用。所有非 Amazon 拥有的其它商标均为各自所有者的财产，这些所有者可能附属于 Amazon、与 Amazon 有关联或由 Amazon 赞助，也可能不是如此。

Amazon Web Services 文档中描述的 Amazon Web Services 服务或功能可能因区域而异。要查看适用于中国区域的差异，请参阅中国的 Amazon Web Services 服务入门。

Table of Contents

什么是 Amazon Directory Service？ 1
- 选择哪一个 1
- Amazon Directory Service选项 1
- 使用 Amazon EC2 3

设置 Amazon Directory Service 5
- 注册 Amazon 账户 5
- 创建 IAM 用户 5

Amazon托管的 Managed 7
- 开始使用 8
  - 先决条件 8
  - 创建您的目录 9
  - 创建的内容 10
  - 管理员账户 14
- 重要概念 15
  - Active Directory 架构 16
  - 修补和维护 16
  - 组托管服务账户 17
  - 委托 Kerberos 约束委托 17
- 使用案例 17
  - 使用案例 1：登录到Amazon应用程序和服务具有 AD 凭证 20
  - 使用案例 2：管理Amazon EC2 实例 23
  - 使用案例 3：将目录服务提供给您的 AD 感知工作负载 23
  - 使用案例 4：至 Office 365 和其他云应用程序的 SSSO 23
  - 使用案例 5：将您的本地 AD 扩展到Amazon云 24
  - 使用案例 6：共享目录以将 Amazon EC2 实例无缝加入域Amazon账户 24
- 如何... 25
  - 保护您的目录 25
  - 监控您的目录 47
  - 配置多区域复制 54
  - 共享您的目录 58
  - 将 EC2 实例加入目录 66
  - 管理用户和组 93
  - Connect 现有的 AD 基础设施 96
  - 扩展你的架构 111
  - 维护您的目录 116
  - 授予访问权限Amazon资源 120
  - 启用访问权限Amazon应用程序和服务 124
  - 允许访问Amazon Web Services Management Console 130
  - 部署额外的域控制器 132
  - 将用户从 AD 迁移到Amazon托管的 Microsoft AD 136
- 最佳实践 136
  - 设置：先决条件 136
  - 设置：创建目录 137
  - 使用目录 138
  - 管理目录 139
  - 为应用程序编程 140
- 配额 141
- 应用程序兼容性 141
  - 兼容性指南 142
  - 已知不兼容的应用程序 143
- Amazon托管的 Microsoft AD 测试实验室教程 143
  - 教程：设置基地Amazon托管的 Microsoft AD 测试实验室 143
  - 教程：创建信任Amazon将微软 AD 托管到 EC2 上的自我管理的 AD 安装 154
- 故障排除 161

Netlogon 和安全渠道通信的问题 ... 161
密码找回 ... 161
DNS 故障排除 ... 162
Linux 域加入错误 ... 162
可用存储空间不足 ... 164
架构扩展错误 ... 166
信托创建状态原因 ... 167
Active Directory Connector ... 171
开始使用 ... 171
AD Connetor ... 171
创建AD Connector ... 181
创建的内容 ... 182
如何... ... 182
保护您的目录 ... 182
监控目录 ... 193
将 EC2 实例加入目录 ... 195
维护您的目录 ... 201
更新 AD Connector 的 DNS 地址 ... 202
最佳实践 ... 203
设置：先决条件 ... 203
为应用程序编程 ... 204
使用目录 ... 204
配额 ... 205
应用程序兼容性 ... 205
故障排除 ... 205
EC2 实例的无缝域加入停止工作 ... 206
使用时，我遇到 “Invalid Credentials” 错误Amazon搜索用户或组的应用 ... 206
当我尝试连接我的本地目录时收到一条“DNS unavailable”错误 ... 206
在尝试连接到我的本地目录时，我收到一条“Connectivity issues detected”错误 ... 206
在尝试连接到我的本地目录时，我收到一条“SRV record”错误 ... 206
我的目录卡在“Requested”状态 ... 207
我在创建目录时遇到“AZ Constrained”错误 ... 207
我的某些用户无法进行向我的目录进行身份验证 ... 207
AD Connector 使用的服务账户尝试进行身份验证时，我遇到 “Invalid Credentials” 错误 ... 207
我无法删除我的 AD Connector ... 207
Simple Active Directory ... 208
开始使用 ... 209
Simple AD 先决条件 ... 209
创建 Simple AD 目录 ... 210
创建的内容 ... 211
配置 DNS ... 211
如何... ... 212
管理用户和组 ... 212
监控目录 ... 215
将 EC2 实例加入目录 ... 218
维护您的目录 ... 234
启用访问权限Amazon应用程序和服务 ... 237
允许访问Amazon Web Services Management Console ... 243
教程：创建 Simple AD 目录 ... 245
先决条件 ... 245
第 1 步：创建和配置 VPC ... 245
第 2 步：创建 Simple AD 目录 ... 246
最佳实践 ... 247
设置：先决条件 ... 248
设置：创建您的目录 ... 249
为应用程序编程 ... 249
配额 ... 250

程序兼容性 250
故障排除 251
密码找回 251
当将用户添加到 Simple AD 时，我收到 “KDC Management option” 错误 251
我无法更新已加入域的实例的 DNS 名称或 IP 地址 (DNS 动态更新) 251
我无法使用 SQL Server 账户登录 SQL Server 251
我的目录卡在 “Regest” 状态 251
我在创建目录时遇到 “AZ Constance” 错误 252
我的某些用户无法进行向我的目录进行身份验证 252
目录状态原因 252
安全性 255
身份和访问管理 256
身份验证 256
访问控制 257
有关管理访问的概述 257
使用基于身份的策略（IAM policy） 260
Amazon Directory Service API 权限参考 265
日志记录和监控 266
合规性验证 266
故障恢复能力 266
基础设施安全性 267
防止跨服务混淆代理 267
服务等级协议 270
区域可用性 271
浏览器兼容性 274
什么是 TLS？ 275
IAM 身份中心支持哪些 TLS 版本 275
如何在浏览器中启用支持的 TLS 版本 275
文档历史记录 276
..... cclxxviii

什么是 Amazon Directory Service？

Amazon Directory Service 提供了多种方式来结合使用 Microsoft Active Directory (AD) 与其他 Amazon 服务。目录中存储有关用户、组和设备的信息，管理员使用这些信息来管理对信息和资源的访问。针对希望在云中使用现有 Microsoft AD 或能够识别轻量目录访问协议 (LDAP) 的应用程序的客户，Amazon Directory Service 提供了多种目录选择。它还为需要目录来管理用户、组、设备和访问权限的开发人员提供了同样的选择。

选择哪一个

您可以选择根据自己需要的功能和可扩展性，选择最适合的目录服务。使用下表可帮助您确定哪种 Amazon Directory Service 目录选项最适合您的组织。

您需要做什么？	建议的 Amazon Directory Service 选项
我需要在云中为应用程序使用 Active Directory 或 LDAP	SelectAmazonMicrosoft Directory Service Directory (p. 1)（标准版或企业版）如果你需要在Amazon支持活动目录感知工作负载的云，或者Amazon应用程序和服务，例如 Amazon WorkSpaces 和 Amazon QuickSight，或者您需要对 Linux 应用程序的 LDAP 支持。 如果您只需要允许本地用户使用其 Active Directory 凭证登录 Amazon 应用程序和服务，可以使用 AD Connector。您还可以使用 AD Connector 将 Amazon EC2 实例加入到现有 Active Directory 域。 使用Simple AD如果您需要小规模、低成本的目录，并且具备基本 Active Directory 兼容性，能够支持 Samba 4 兼容应用程序，或者您需要为能够识别 LDAP 的应用程序提供 LDAP 兼容性
我开发 SaaS 应用程序	如果您开发大规模的 SaaS 应用程序，需要可扩展的目录来管理订阅者和使用社交媒体身份工作的用户并验证他们的身份，可以使用 Amazon Cognito。

Amazon Directory Service选项

Amazon Directory Service 包括若干目录类型供您选择。有关更多信息，请选择以下选项卡之一：

Amazon Directory Service for Microsoft Active Directory

也称作Amazon托管的 Microsoft AD，AmazonMicrosoft Active Directory Directory Service 由实际 Microsoft Windows Server Active Directory (AD) 提供支持，由Amazon中的Amazon云。它允许您将各种感知 Active Directory 的应用程序迁移到Amazon云。AmazonMicrosoft AD 可以与 Microsoft SharePoint、Microsoft SQL Server Always On Availability Groups 和多种 .NET 应用程序配合使用。它还支持Amazon托管应用程序和服务包括Amazon WorkSpaces、Amazon WorkDocs、Amazon QuickSight、Amazon Chime、Amazon Connect, 和Microsoft SQL Server 的 Amazon Relational

Database Service（Amazon RDS for SQL Server 的亚马逊 RDS、针对 Oracle 的 Amazon RDS 和适用于 PostgreSQL 的 Amazon RDS）。

所有兼容的应用程序都使用存储在中的用户凭据Amazon托管微软 AD，或者你可以连接到现有的 AD 基础架构使用在本地或 EC2 Windows 上运行的 Active Directory 中的信任和用户凭证。如果您将 EC2 实例加入您的AmazonMicrosoft AD 托管，你的用户可以在Amazon云与访问本地网络中的工作负载相同的 Windows 单点登录 (SSO) 体验。

AmazonAmazon 托管的 AD 还支持使用 Active Directory 凭证的联合使用案例。独自一人，Amazon使用托管的 Microsoft AD 登录Amazon Web Services Management Console. 借助 Amazon IAM Identity Center (successor to Amazon Single Sign-On)，您还可以获取短期凭证以用于 Amazon 开发工具包和 CLI，并使用预配置的 SAML 集成登录到许多云应用程序。通过添加 Azure AD Connect 以及可选的 Active Directory 联合身份验证服务 (AD FS)，您可以使用存储在中的凭证登录 Microsoft Office 365 和其他云应用程序。Amazon托管的 Microsoft AD。

该服务包括使您能够通过安全套接字层 (SSL)/传输层安全性 (TLS) 协议扩展架构、管理密码策略和实现安全 LDAP 通信的关键功能。您还可以启用多重验证 (MFA)AmazonMicrosoft AD 托管在用户访问时提供了一个额外的安全层Amazon从 Internet 提供的应用程序。由于 Active Directory 是 LDAP 目录，您也可以使用Amazon托管的 Microsoft AD 用于 Linux Secure Shell (SSH) 身份验证以及其他启用 LDAP 的应用程序。

Amazon在服务中提供了监控、每日快照以及恢复功能 — 您将用户和群组添加到AmazonMicrosoft AD 托管，并使用加入了Amazon托管的 Microsoft AD 域。您还可以通过部署更多域控制器来扩展目录，并通过在大量域控制器之间分配请求来帮助提高应用程序性能。

Amazon托管的 Microsoft AD 提供了两种版本：标准版和企业版。

- 标准版：AmazonMicrosoft AD（标准版）经过优化，可以在员工数最高 5000 人的中小型企业中用作主要目录。它提供了足够的存储容量，支持最高 30000* 个目录对象，例如用户、组和计算机。
- 企业版：AmazonMicrosoft AD（企业版）旨在用于支持最高 500000* 个目录对象的企业组织。

* 上限为近似值。根据对象大小、以及应用程序的行为和性能需求，您的目录支持的对象数可能更多，也可能更少。

何时使用

Amazon如果您需要实际的 Active Directory 功能支持，是您的最佳选择。Amazon应用程序或 Windows 工作负载，包括 Amazon for Microsoft SQL Server 的关系数据库服务。如果您希望 Amazon 云中的独立 AD 能够支持 Office 365，或者需要 LDAP 目录支持 Linux 应用程序，这也是最佳之选。有关更多信息，请参阅 Amazon托管的 Managed (p. 7)。

AD Connector

AD Connector 是一种提供了连接兼容的简单方法的代理服务。Amazon应用程序，例如 Amazon WorkSpaces、Amazon QuickSight 和Amazon EC2对于 Windows Server 实例，转移到现有本地部署 Microsoft Active Directory。使用 AD Connector，您只需添加一个服务帐户转到 Active Directory。AD Connector 还可以避免目录同步的需求，也避免了托管联合身份基础设施的成本和复杂性。

当你将用户添加到AmazonAmazon QuickSight、AD Connector 等应用程序读取现有的 Active Directory 创建用户和组列表，以便您从中选择。当用户登录到Amazon应用程序、AD Connector 将登录请求转发到您的本地 Active Directory 域控制器进行身份验证。AD Connector 适用于许多Amazon包括应用程序和服务Amazon WorkSpaces、Amazon WorkDocs、Amazon QuickSight、Amazon Chime、Amazon Connect, 和Amazon WorkMail. 您还可以加入 EC2 Windows 实例使用通过 AD Connector 传入到本地 Active Directory 域无缝域加入. AD Connector 还允许您的用户访问Amazon Web Services Management Console并管理Amazon使用现有 Active Directory 凭证登录。Amazon AD Connector 与 RDS SQL Server 不兼容。

你也可以使用 AD Connector 来启用多重验证(MFA) 为你Amazon将应用程序用户连接到现有的基于 RADIUS 的 MFA 基础结构。这在用户访问 Amazon 应用程序时提供了一个额外的安全层。

使用 AD Connector 时，您可以继续像现在一样管理您的 Active Directory。例如，您在本地 Active Directory 中，使用标准 Active Directory 管理工具添加新用户和组以及更新密码。这帮助您始终如一地实施安全策略（如密码过期、密码历史和账户锁定），无论用户是访问本地还是 Amazon 云中的资源。

何时使用

当您想要将现有本地目录与兼容性一起使用时，AD Connector 是您的最佳选择。Amazon服务。有关更多信息，请参阅 Active Directory Connector (p. 171)。

Simple AD

Simple AD 是 Microsoft Active Directory —兼容目录来自Amazon Directory Service由 Samba 4 提供技术支持。Simple AD 支持基础 Active Directory 功能，例如用户账户、组成员资格、加入 Linux 域或者基于 Windows 的 EC2 实例、基于 Kerberos 的 SSO 以及组策略。Amazon在服务中提供了监控、每日快照以及恢复功能。

Simple AD 是云中的独立目录，您可在其中创建和管理用户身份，以及管理对应用程序的访问。您可以使用许多需要基本 Active Directory 功能的熟悉 Active Directory 应用程序和需要基本 Active Simple AD 与以下内容兼容Amazon应用程序：Amazon WorkSpaces、Amazon WorkDocs、Amazon QuickSight, 和Amazon WorkMail. 您也可以登录Amazon Web Services Management Console使用 Simple AD 用户帐户并进行管理Amazon资源的费用。

Simple AD 不支持多重身份验证 (MFA)、信任关系、DNS 动态更新、架构扩展、通过 LDAPS 的通信、PowerShell AD cmdlet 以及 FSMO 角色转移。Amazon Simple AD 与 RDS SQL Server 不兼容。需要实际 Microsoft Active Directory 功能或者希望将其目录用于 RDS SQL Server 的客户，应使用 Amazon而是托管的 Microsoft AD。使用 Simple AD 之前，请确保您需要的应用程序与 Samba 4 完全兼容。有关更多信息，请访问 https://www.samba.org。

何时使用

在云中，您可以将 Simple AD 用作独立目录，用于支持需要基本 AD 功能的 Windows 工作负载、兼容的基本 AD 功能Amazon应用程序，或者支持需要 LDAP 服务的 Linux 工作负载。有关更多信息，请参阅 Simple Active Directory (p. 208)。

Amazon Cognito

Amazon Cognito 是一种用户目录，它使用 Amazon Cognito 用户池向您的移动应用程序或 Web 应用程序添加注册和登录功能。

何时使用

当您需要创建自定义注册字段并将该元数据存储在您的用户目录中时，您也可以使用 Amazon Cognito。此完全托管的服务经扩展可以支持数亿个用户。有关更多信息，请参阅 Amazon Cognito 开发人员指南中的 Amazon Cognito 用户池。

请参阅区域可用性Amazon Directory Service (p. 271)获得各个区域支持的目录类型的列表。

使用 Amazon EC2

对 Amazon EC2 有基本的了解对于使用非常重要Amazon Directory Service. 我们建议您首先阅读以下主题：

- 什么是 Amazon EC2？中的Windows Amazon EC2 用户指南.
- 启动 EC2 实例中的Windows Amazon EC2 用户指南.
- 安全组中的Windows Amazon EC2 用户指南.
- Amazon VPC 是什么？中的Amazon VPC User Guide.

- 在您的 VPC 中添加硬件虚拟专用网关中的Amazon VPC User Guide.

设置 Amazon Directory Service

要使用Amazon Directory Service，需要满足以下先决条件：Amazon适 Directory Service 于 Microsoft Active Directory、AD Connector 或 Simple AD。有关更多信息，请参阅AmazonMicrosoft AD (p. 8)、AD Connetor (p. 171)或Simple AD 先决条件 (p. 209)。

如果尚未执行此操作，则还需要创建 Amazon 账户，并使用 Amazon Identity and Access Management 服务控制访问。

主题

- 注册 Amazon 账户 (p. 5)
- 创建 IAM 用户 (p. 5)

注册 Amazon 账户

您可以通过 Amazon 账户访问所有服务，但您只需为所使用的资源付费。

如果您还没有 Amazon Web Services 账户，请完成以下步骤创建一个。

注册 Amazon Web Services 账户

1. 打开 https://portal.aws.amazon.com/billing/signup。
2. 按照屏幕上的说明进行操作。

   在注册时，您将接到一通电话，要求您使用电话键盘输入一个验证码。

您的根账户凭证使中的服务可以识别您。Amazon并授予你无限制使用你的Amazon资源，例如您的 Amazon WorkSpaces。允许其他用户管理Amazon Directory Service资源，而无需共享安全凭证，请使用Amazon Identity and Access Management(IAM)。我们建议所有人以 IAM 用户的身份工作，即使是账户所有者。您应该为自己创建一个 IAM 用户，向该 IAM 用户提供管理权限，然后将其用于您的所有工作。

创建 IAM 用户

Amazon Web Services Management Console 需要您提供用户名称和密码，这样服务才能确定您是否有权访问其资源。但是，我们建议您避免访问Amazon为您的 root 使用凭据Amazon相反，我们建议您使用Amazon Identity and Access Management(IAM)，创建 IAM 用户，然后将 IAM 用户添加到具有管理权限的 IAM 组。这将授予 IAM 用户管理权限。然后你可以访问Amazon Web Services Management Console使用 IAM 用户的证书。

如果您已注册 Amazon 但尚未为自己创建一个 IAM 用户，则可以使用 IAM 控制台自行创建。

自行创建管理员用户并将该用户添加到管理员组 (控制台)

1. 选择 Root user（根用户）并输入您的 Amazon Web Services 账户 电子邮件地址，以账户拥有者身份登录 IAM 控制台。在下一页上，输入您的密码。

   Note

   强烈建议您遵守以下使用 **`Administrator`** IAM 用户的最佳实践，妥善保存根用户凭证。只在执行少数账户和服务管理任务时才作为根用户登录。

2. 在导航窗格中，选择 Users（用户），然后选择 Add users（添加用户）。
3. 对于 User name（用户名），输入 **`Administrator`**。
4. 选中 Amazon Web Services Management Console access (Amazon Web Services Management Console 管理控制台访问）旁边的复选框。然后选择自定义密码，并在文本框中输入新密码。
5. （可选）默认情况下，Amazon要求新用户在首次登录时创建新密码。您可以清除 User must create a new password at next sign-in（用户必须在下次登录时创建新密码）旁边的复选框以允许新用户在登录后重置其密码。
6. 选择 Next:。Permissions (下一步：权限)。
7. 在设置权限下，选择将用户添加到组。
8. 选择创建组。
9. 在 Create group（创建组）对话框中，对于 Group name（组名称），输入 **`Administrators`**。
10. 选择 Filter policies（筛选策略），然后选择 Amazon managed - job function（Amazon 托管 – 工作职能）以筛选表内容。
11. 在策略列表中，选中 AdministratorAccess 的复选框。然后选择 Create group（创建组）。

    Note

    您必须先激活 IAM 用户和角色对账单的访问权限，然后才能使用 `AdministratorAccess` 权限访问 Amazon Billing and Cost Management 控制台。为此，请按照"向账单控制台委派访问权限"教程第 1 步中的说明进行操作。
12. 返回到组列表中，选中您的新组所对应的复选框。如有必要，选择 Refresh（刷新）以在列表中查看该组。
13. 选择 Next:。标签。
14. (可选) 通过以键值对的形式附加标签来向用户添加元数据。有关在 IAM 中使用标签的更多信息，请参阅 IAM 用户指南中的标记 IAM 实体。
15. 选择 Next:。审核以查看要添加到新用户的组成员资格的列表。如果您已准备好继续，请选择 Create user（创建用户）。

您可使用这一相同的流程创建更多组和用户，并允许您的用户访问 Amazon Web Services 账户 资源。要了解有关使用策略限制用户对特定 Amazon 资源的权限的信息，请参阅访问管理和示例策略。

要以此新 IAM 用户的身份登录，请从Amazon Web Services Management Console，然后使用以下 URL，其中你的 _aws_帐户_id是您的Amazon不包含连字符的账号（例如，如果您的Amazon账号`1234-5678-9012`，您的Amazon账户 ID`123456789012`):

```
https://your_aws_account_id.signin.aws.amazon.com/console/
```

输入您刚创建的 IAM 用户名和密码。登录后，导航栏显示"your_user_name @ your_aws_account_id"。

如果您不希望您的登录页面 URL 包含 Amazon 账户 ID，可以创建账户别名。从 IAM 控制面板中，单击自定义然后输入一个别名，例如您的公司名称。要在创建账户别名后登录，请使用以下 URL：

```
https://your_account_alias.signin.aws.amazon.com/console/
```

有关使用 IAM 策略控制对您的访问的更多信息Amazon Directory Service请参阅资源为 Amazon Directory Service 使用基于身份的策略（IAM policy）(p. 260).

Amazon托管的 Managed

Amazon Directory Service使您可以将 Microsoft Active Directory (AD) 作为托管服务运行。AmazonDirectory Service ctory，也称为Amazon托管的 Managed 由 Windows Server 2012 R2 提供支持。选择和启动此目录类型时，它会创建为一对连接到 Virtual Private Cloud (VPC) 的高可用域控制器。域控制器在所选区域中的不同可用区内运行。主机监控和恢复、数据复制、快照和软件更新是自动为您配置和管理的。

与Amazon托管的 Microsoft AD，可以在中运行目录感知型工作负载Amazon云，包括微软 SharePoint 以及基于 .NET 和 SQL Server 的自定义应用程序。还可以在之间配置信任关系Amazon在Amazon云和现有本地 Microsoft Active Directory，使用户和组可以使用访问任一域中的资源Amazon IAM Identity Center (successor to Amazon Single Sign-On).

通过 Amazon Directory Service 可以轻松地在 Amazon 云中设置和运行目录，也可以将 Amazon 资源与现有本地 Microsoft Active Directory 连接。目录创建之后，可以将它用于各种任务：

- 管理用户和组
- 向应用程序和服务提供单点登录
- 创建和应用组策略
- 简化基于云的 Linux 和 Microsoft Windows 工作负载的部署和管理
- 您可以使用Amazon托管的 Microsoft AD，通过与基于 RADIUS 的现有 MFA 基础设施集成，托管的 Microsoft AD 启用多重验证，从而在用户访问时增加一层Amazon应用程序。
- 安全地连接到 Amazon EC2 Linux 和 Windows 实例

> **Note**
>
> Amazon为您管理 Windows Server 实例的许可；您只需为使用的实例付费即可。也无需购买额外的 Windows 服务器 CAL，因为访问权限已包含在价格中。每个实例都有两个远程连接，仅用于管理目的。如果您需要两个以上的连接，或者出于管理员以外的目的需要这些连接，则可能需要引入额外的远程桌面服务 CAL 以在Amazon.

请阅读本部分中的主题，以开始创建Amazon托管 Microsoft AD 目录，在两者之间建立信任关系Amazon托管的 Microsoft AD 和本地目录，并扩展您的Amazon托管的 Managed 架构。

主题

- 开始使用AmazonMicrosoft AD (p. 8)
- 的主要概念AmazonMicrosoft AD (p. 15)
- 的使用案例Amazon托管的 Micros (p. 17)
- 如何管理AmazonMicrosoft Managed Microsoft AD (p. 25)
- 的最佳实践Amazon托管的 Microsoft AD (p. 136)
- AmazonManaged Microsoft AD 配额 (p. 141)
- 的应用程序兼容性策略AmazonMicrosoft (p. 141)
- Amazon托管的 Microsoft AD 测试实验室教程 (p. 143)
- 故障排除AmazonMicrosoft Managed Managed Microsoft AD (p. 161)

相关Amazon安全博客文章

- 如何委托管理你的Amazon将微软 AD 目录托管到您的本地活动目录用户

- 如何使用配置更强的密码策略来帮助满足您的安全标准Amazon Directory Service为了Amazon托管的 Managed
- 如何提高您的冗余度和性能Amazon Directory Service为了Amazon通过添加域控制器管理 Microsoft AD
- 如何通过在上部署 Microsoft 远程桌面许可管理器来启用远程桌面的使用Amazon托管的 Managed
- 如何访问Amazon Web Services Management Console使用Amazon托管的 Managed 和本地凭证
- 如何为启用多重验证Amazon通过使用Amazon托管微软 AD 和本地凭据
- 如何轻松登录Amazon通过使用本地Active Directory

开始使用AmazonMicrosoft AD

Amazon将在Amazon在 2012 R2 林和域功能级别上运行云并在 2012 R2 林和域功能级别上运行。当你使用创建目录时Amazon托管的 Microsoft AD，Amazon Directory Service创建两个域控制器并代表您添加 DNS 服务。域控制器在 VPC 的不同子网中创建；此冗余帮助确保您的目录即使在出现故障时仍可访问。如果您需要更多域控制器，您可以在以后添加它们。有关更多信息，请参阅部署额外的域控制器 (p. 132)。

主题

- AmazonMicrosoft AD (p. 8)
- 创建您的Amazon托管的 Microsoft AD 目录 (p. 9)
- 创建的内容 (p. 10)
- 管理员账户 (p. 14)

AmazonMicrosoft AD

创建Amazon托管的 icrosoft AD 目录，则需要一个满足以下条件的 VPC：

- 至少两个子网。每个子网必须位于不同的可用区。
- VPC 必须具有默认硬件租户。
- 您无法创建Amazon使用 198.18.0.0/15 地址空间中的地址在 VPC 中托管的 icrosoft AD。

如果你需要整合你的Amazon托管的 icrosoft AD 域使用现有本地 Active Directory 域时，必须将您本地域的林和域功能级别设置为 Windows Server 2003 或更高版本。

Amazon Directory Service使用双 VPC 结构。组成您的目录的 EC2 实例在您的Amazon账户，并由管理Amazon. 它们有两个网络适配器，`ETH0`和`ETH1`.`ETH0`是管理适配器，存在于您的账户之外。`ETH1`是在您的账户中创建。

您目录的 ETH0 网络的管理 IP 范围是 198.18.0.0/15。

Amazon IAM Identity Center (successor to Amazon Single Sign-On)先决条件

如果您计划将 IAM 身份中心与Amazon托管的 icrosoft AD，则需要确保满足以下条件：

- 您的Amazon托管的 icrosoft AD 目录设置在Amazon组织的管理账户。
- 您的 IAM Ictent Center 实例位于您在其中的Amazon托管的 icrosoft AD 目录已设置。

有关更多信息，请参阅 。IAM 身份中心先决条件中的Amazon IAM Identity Center (successor to Amazon Single Sign-On)用户指南。

多重验证

为了使用您的支持多重Amazon托管 Microsoft AD 目录，你必须配置内部部署或基于云的目录远程身份验证拨入用户服务(RADIUS) 服务器采用以下方式，以便它可以接受来自您的AmazonMicrosoft AD 目录Amazon.

1. 在 RADIUS 服务器上，创建两个 RADIUS 客户端以表示AmazonMicrosoft AD 域控制器 (DC)Amazon. 必须使用以下通用参数配置两个客户端（您的 RADIUS 服务器可能会有所不同）：
   - 地址 (DNS 或 IP)：这是其中一个AmazonMicrosoft AD DC。两个 DNS 地址都可以在Amazon上的 Directory Service 控制台详细信息的页面Amazon您计划在其中使用 MFA 的微软 AD 托管目录。显示的 DNS 地址表示两个Amazon由使用的托管微软 AD DCAmazon.

     Note

     如果 RADIUS 服务器支持 DNS 地址，则您只能创建一个 RADIUS 客户端配置。否则，必须为每个都创建一个 RADIUS 客户端配置AmazonMicrosoft AD DC
   - 端口号：配置 RADIUS 服务器为其接受 RADIUS 客户端连接的端口号。标准 RADIUS 端口是 1812。
   - Shared sec：键入或生成将由 RADIUS 服务器用于与 RADIUS 客户端连接的共享密
   - 协议：您可能需要在Amazon管理微软 AD 域控制器和 RADIUS 服务器。支持的协议有 PAP、CHAP MS-CHAPv1 和 MS-CHAPv2。建议使用 MS-CHAPv2，因为它提供三种选项中最强的安全性。
   - 应用程序名称：在某些 RADIUS 服务器中为可选设置，通常用于在消息或报告中标识应用程序。
2. 配置现有网络以允许从 RADIUS 客户端到 RADIUS 客户端的入站流量 (Amazon托管的 icrosoft AD DNS 地址，请参阅步骤 1) 到 RADIUS 服务器端口的 DNS 地址。
3. 向您中的 Amazon EC2 安全组添加规则Amazon托管的 icrosoft AD 域允许来自以前定义的 RADIUS 服务器 DNS 地址和端口号的入站流量。有关更多信息，请参阅 。在安全组中添加规则中的EC2 用户指南.

有关如何使用的更多信息Amazon使用 MFA 托管微软 AD，请参阅为启用多重验证Amazon托管的 Managed (p. 28).

创建您的Amazon托管的 Microsoft AD 目录

要创建新目录，请执行以下步骤。在开始此过程之前，请确保已满足了AmazonMicrosoft AD (p. 8)中确定的先决条件。

创建 Amazon 托管的 Microsoft AD 目录

1. 在Amazon Directory Service控制台选择导航窗格，目录选择，然后选择设置目录.
2. 在存储库的选择目录类型页面上，选择AmazonMicrosoft AD，然后选择下一步.
3. 在输入目录信息页面上，提供以下信息：

   版本

   从中选择标准版要么企业版的Amazon托管的 Microsoft AD。有关版本的更多信息，请参阅AmazonMicrosoft Active Directory 的 Directory Service (p. 1).

   目录 DNS 名称

   目录的完全限定名称，例如 `corp.example.com`。

   目录 NetBIOS 名称

   目录的短名称，如 `CORP`.

   目录描述

   目录的可选描述。

   管理员密码

   目录管理员的密码。目录创建过程将创建一个具有 `Admin` 用户名和此密码的管理员账户。

密码不能包含单词“admin”。

目录管理员密码区分大小写，且长度必须介于 8 到 64 (含) 个字符之间。至少，它还必须包含下列四种类别中三种类别的一个字符：

- 小写字母 (a-z)
- 大写字母 (A-Z)
- 数字 (0-9)
- 非字母数字字符 (~!@#$%^&*_-+=`|\(){}[]:;'"<>,.?/)

确认密码

重新键入管理员密码。

4. 在 Choose VPC and subnets (选择 VPC 和子网) 页面上，提供以下信息，然后选择 Next (下一步)。

   VPC

   目录的 VPC。

   Subnets (子网)

   为域控制器选择子网。两个子网必须位于不同的可用区。

5. 在 Review & create (检查并创建) 页面上，检查目录信息并进行任何必要的更改。如果信息正确，请选择 Create directory (创建目录)。创建目录需要 20 到 40 分钟。创建后，Status 值将更改为 Active。

创建的内容

当你使用创建目录时Amazon托管的 Microsoft AD，Amazon Directory Service将代表您执行以下任务：

- 自动创建 elastic network interface (ENI) 并将其与每个域控制器相关联。其中每个 ENI 对于您的 VPC 与 Amazon Directory Service 域控制器之间的连接都至关重要，绝不应删除。您可以识别所有保留用于的网络接口Amazon Directory Service通过描述：”Amazon 为目录创建了网络接口目录 ID“。有关更多信息，请参阅 。弹性网络接口适用于 Windows 实例的 Amazon EC2 用户指南中。

  Note

  默认情况下，域控制器将部署在一个区域的两个可用区中，并连接到 Amazon Virtual Private Cloud (VPC)。每天自动进行一次备份，Amazon Elastic Block Store (EBS) 卷将进行加密，以确保静态数据得到安全保护。使用相同的 IP 地址在同一可用区中自动替换出现故障的域控制器，并且可以使用最新的备份执行完整的灾难恢复。

- 使用两个域控制器在 VPC 中预置 Active Directory，以实现容错和高可用性。在成功创建目录且目录处于活动状态后，可以预置更多域控制器以获得更高的恢复能力和性能。有关更多信息，请参阅 部署额外的域控制器 (p. 132)。

  Note

  Amazon不允许在上安装监视代理Amazon托管的 Microsoft AD 域控制器。

- 创建Amazon安全组从而建立针对传入和传出域控制器的流量的网络规则。默认出站规则允许所有流量 ENI 或实例连接到创建的 Amazon 安全组。默认入站规则仅允许来自任何源的通过 Active Directory 所需端口的流量 (0.0.0.0/0)。0.0.0.0/0 规则不会引入安全漏洞，因为到域控制器的流量仅限来自您的 VPC、来自其他对等 VPC 或来自您使用 Amazon Direct Connect、Amazon 中转网关或虚拟专用网络连接的网络的流量。为了提高安全性，创建的 ENI 没有连接弹性 IP，并且您不拥有将弹性 IP 连接到这些 ENI 的权限。因此，唯一可与通信的入站流量Amazon托管的 Microsoft AD 是本地 VPC 和 VPC 路由流量。如果您尝试更改这些规则，请特别小心，因为您可能会破坏与域控制器通信的能力。默认情况下，会创建以下 Amazon 安全组规则：

  入站规则

协议	端口范围	源	流量的类型	Active Directory 使用情况
ICMP	不适用	0.0.0.0/0	Ping	无
TCP 和 UDP	53	0.0.0.0/0	DNS	用户和计算机身份验证、名称解析、信任
TCP 和 UDP	88	0.0.0.0/0	Kerberos	用户和计算机身份验证、林级信任
TCP 和 UDP	389	0.0.0.0/0	LDAP	目录、复制、用户和计算机身份验证组策略、信任
TCP 和 UDP	445	0.0.0.0/0	SMB / CIFS	复制、用户和计算机身份验证、组策略、信任
TCP 和 UDP	464	0.0.0.0/0	Kerberos 更改/设置密码	复制、用户和计算机身份验证、信任
TCP	135	0.0.0.0/0	复制	RPC、EPM
TCP	636	0.0.0.0/0	LDAP SSL	目录、复制、用户和计算机身份验证、组策略、信任
TCP	1024-65535	0.0.0.0/0	RPC	复制、用户和计算机身份验证、组策略、信任
TCP	3268 - 3269	0.0.0.0/0	LDAP GC 和 LDAP GC SSL	目录、复制、用户和计算机身份验证、组策略、信任
UDP	123	0.0.0.0/0	Windows 时间	Windows 时间、信任
UDP	138	0.0.0.0/0	DFSN 和 NetLogon	DFS、组策略
所有	所有	sg-##################	所有流量	

出站规则

协议	端口范围	目标	流量的类型	Active Directory 使用情况
所有	所有	sg-##################	所有流量	

- 使用用户名 Admin 和指定密码创建目录管理员账户。此账户位于 Users OU 下 (例如，Corp > Users)。您可以使用此账户管理 Amazon 云中的目录。有关更多信息，请参阅 管理员账户 (p. 14)。

Important

请务必保存此密码。Amazon Directory Service 不会存储此密码，并且此密码无法检索。但是，您可以通过 Amazon Directory Service 控制台或使用 ResetUserPassword API 重置密码。

- 在域根目录下创建以下三个组织单位 (OU)：

OU 名称	描述
Amazon 委托组	存储您可用于将 Amazon 特定权限委派给用户的所有组。
Amazon 预留	存储所有 Amazon 管理特定账户。

<您的域名>	此 OU 的名称基于您在创建目录时键入的 NetBIOS 名称。如果您未指定 NetBIOS 名称，则此名称将默认为您的目录 DNS 名称的第一部分（例如，如果目录 DNS 名称为 corp.example.com，则 NetBIOS 名称将为 corp）。此 OU 属于 Amazon 并且包含您有权完全控制的所有 Amazon 相关目录对象。默认情况下，此 OU 下存在两个子 OU：Computers 和 Users。例如：
	• Corp
	  • Computers
	  • 用户

- 在 Amazon 委托组 OU 中创建以下组：

Group name	描述
Amazon 账户委托操作员	此安全组的成员拥有有限的账户管理能力，如密码重置
Amazon 委派的基于 Active Directory 的激活管理员	此安全组的成员可以创建 Active Directory 批量许可激活对象，这使企业能够通过与其域的连接激活计算机。
Amazon 在域中添加工作站的委托用户	此安全组的成员可将 10 台计算机加入域中。
Amazon 委托管理员	此安全组的成员可以管理 Amazon Managed Microsoft AD，对您 OU 中的所有对象拥有完全控制权，并可以管理 Amazon 委托组 OU 中包含的组。
Amazon 委托了允许对对象进行身份验证	此安全组的成员可以对 Amazon 预留 OU 中的计算机资源进行身份验证（仅当本地对象具有启用了选择性身份验证的信任时才需要）。
Amazon 委派了允许对域控制器进行身份验证	此安全组的成员可以对域控制器 OU 中的计算机资源进行身份验证（仅当本地对象具有启用了选择性身份验证的信任时才需要）。
Amazon 委派的删除对象生命周期管理员	此安全组的成员可以修改 msDS-DeletedObjectLifetime 对象，它定义了已删除对象可保留在 AD 回收站中以供还原的时长。

Group name	描述
Amazon 分布式文件系统委托管理员	此安全组的成员可以添加和删除 FRS、DFS-R 和 DFS 命名空间。
Amazon 域名系统委托管理员	此安全组的成员可以管理与 Active Directory 集成的 DNS。
Amazon 动态主机配置协议委托管理员	此安全组的成员可以对企业中的 Windows DHCP 服务器进行授权。
Amazon 企业证书颁发机构委托管理员	此安全组的成员可以部署和管理 Microsoft 企业证书颁发机构基础设施。
Amazon 精细密码策略委托管理员	此安全组的成员可以修改预先创建的精细密码策略。
Amazon 委派的 FSx 管理员	此安全组的成员可以管理 Amazon FSx 资源。
Amazon 组策略委托管理员	此安全组的成员可以执行组策略管理任务（创建、编辑、删除、链接）。
Amazon Kerberos 委托管理员	此安全组的成员可以针对计算机和用户账户对象启用委托。
Amazon 托管服务账户委托管理员	此安全组的成员可以创建和删除托管服务账户。
Amazon委托的 MS-NPRC 不合规设备	此安全组的成员将被排除在要求与域控制器之间进行安全通道通信。这组用于计算机帐户。
Amazon 远程访问服务委托管理员	此安全组的成员可以添加和删除 RAS 和 IAS 服务器组中的 RAS 服务器。
Amazon 复制目录变更委托管理员	此安全组的成员可以将 Active Directory 中的配置文件信息与 SharePoint Server 进行同步。
Amazon 服务器委托管理员	此安全组的成员包含在所有加入域的计算机的本地管理员组中。
Amazon 站点和服务委托管理员	此安全组的成员可以重命名 Active Directory 站点和服务中的 Default-First-Site-Name 对象。
Amazon 委派的系统管理员	此安全组的成员可以创建和管理系统管理容器中的对象。
Amazon 终端服务器许可委托管理员	此安全组的成员可以在终端服务器许可服务器组中添加和删除终端服务器许可服务器。
Amazon 用户委托人名称后缀委托管理员	此安全组的成员可以添加和删除用户委托人名称后缀。

- 创建并应用以下组策略对象 (GPO)：

  Note

  您无权删除、修改或解锁这些 GPO 的链接。这是设计的，因为它们是保留的Amazon使用。如果需要，你可以将它们链接到你控制的 OU。

组策略名称	适用于	描述
默认域策略	Domain	包括域密码和 Kerberos 策略。
ServerAdmins	所有非域控制器计算机账户	将“Amazon 委托服务器管理员”添加为 BUILTIN\Administrators 组的成员。
Amazon 保留策略：用户	Amazon 保留的用户账户	对 Amazon 保留 OU 中的所有用户账户设置建议的安全设置。
Amazon Managed Active Directory 策略	所有域控制器	在所有域控制器上设置建议的安全设置。
TimePolicyNT5DS	所有非 PDCe 域控制器	将所有非 PDCe 域控制器时间策略设置为使用 Windows 时间 (NT5DS)。
TimePolicyPDC	PDCe 域控制器	将 PDCe 域控制器的时间策略设置为使用网络时间协议 (NTP)。
默认域控制器策略	未使用	在域创建期间预置，将使用 Amazon Managed Active Directory 策略。

如果要查看每个 GPO 的设置，可以从加入域的 Windows 实例中查看它们。组策略管理控制台 (GPMC)已启用.

管理员账户

创建时Amazon用于 Microsoft Directory Service irectory 目录的目录，Amazon创建组织单位 (OU) 来存储所有Amazon相关组和账户。有关此 OU 的更多信息，请参阅 创建的内容 (p. 10)。其中包括管理员账户。管理员账户有权对您的 OU 执行以下常见的管理活动：

- 添加、更新或删除用户、组和计算机。有关更多信息，请参阅 在中管理用户和组AmazonMicrosoft Managed Microsoft AD (p. 93)。
- 将资源添加到域 (如文件或打印服务器)，然后为 OU 中的用户和组分配这些资源的权限.
- 创建额外的 OU 和容器.
- 委派附加 OU 和容器的权限。有关更多信息，请参阅 为委派目录加入权限Amazon管理 Microsoft AD (p. 90)。
- 创建和链接组策略.
- 从 Active Directory 回收站还原删除的对象.
- 在 Active Directory Web 服务上运行 Active Directory 和 DNS Windows PowerShell 模块。
- 创建和配置组托管服务账户。有关更多信息，请参阅 组托管服务账户 (p. 17)。
- 配置 Kerberos 约束委托。有关更多信息，请参阅 委托 Kerberos 约束委托 (p. 17)。

管理员账户还具有在域范围内进行以下活动的权限：

- 管理 DNS 配置（添加、删除或更新记录、区域和转发器）
- 查看 DNS 事件日志
- 查看安全事件日志

仅允许管理员账户执行此处列出的操作。对于特定 OU 外部 (如在父 OU 上) 的任何目录相关操作，管理员账户也没有权限。

> **Important**
>
> Amazon 域管理员对 Amazon 上托管的所有域拥有完全管理访问权限。请参阅您与的协议Amazon和Amazon数据保护有关如何进一步的信息Amazon处理存储在其上的内容，包括目录信息Amazon系统。

> **Note**
>
> 我们建议您不要删除或重命名此账户。如果您不再想使用该账户，建议您设置一个长密码（最多 64 个随机字符），然后禁用该账户。

企业和域管理员特权帐户

Amazon每 90 天自动将内置的管理员密码轮换为随机密码。任何时候请求内置的管理员密码供人使用Amazon票证已创建并使用Amazon Directory Service团队。账户凭据通过安全渠道进行加密和处理。此外，管理员帐户凭据只能由Amazon Directory Service管理团队。

要对目录执行操作管理，Amazon拥有独占控制管理员和域管理员权限的账户的企业。这包括独占控制 AD 管理员账户。Amazon通过使用密码库自动化密码管理，从而保护此账户。在自动轮换管理员密码期间，Amazon创建一个临时用户账户并授予其域管理员权限。此临时账户已用作备份在发生密码轮换故障的管理员账户。晚于Amazon成功轮换管理员密码，Amazon删除临时管理员账户。

通常Amazon完全自动化操作目录。如果自动化流程无法解决运营问题，Amazon可能需要有一个支持工程师登录到您的域控制器 (DC) 执行诊断。在这些罕见的情况下,Amazon实施请求/通知系统来授予访问权限。在这个过程中,Amazon自动化在您目录中创建一个有限时间内具有域管理员权限的用户账户。Amazon将用户账户与指派的在您目录上工作的工程师相关联。Amazon在我们的日志系统中记录此关联，并为工程师提供相关凭据供其使用。工程师所采取的所有操作都记录在 Windows 事件日志中。当分配的时间到期后，自动化将删除用户账户。

您可以使用目录的日志转发功能监控管理账户的操作。利用此功能，您可以将 AD 安全事件转发到您的 CloudWatch 系统，您可以在其中实施监控解决方案。有关更多信息，请参阅 启用日志转发 (p. 51)。

当有人以交互方式登录 DC 时，安全事件 ID 4624、4672 和 4648 都会被记录。你可以使用事件查看器微软管理控制台 (MMC) 从加入域的 Windows 计算机上查看每个 DC 的 Windows 安全事件日志。您还可以启用日志转发 (p. 51)将所有安全事件日志发送到账户中的 CloudWatch Logs。

您可能偶尔会看到在Amazon已保留 OU。Amazon负责管理此 OU 中的所有对象以及我们尚未向您授予访问和管理权限的任何其他 OU 或容器中的所有对象。你可能会在该 OU 中看到创作和删除。这是因为Amazon Directory Service定期使用自动化轮换域管理员密码。轮换密码时，轮换失败时，将创建备份。轮换成功后，备份帐户将自动删除。另外，如果出于故障排除目的需要对 DC 进行交互式访问的极少数情况，则会为Amazon Directory Service要使用的工程师。工程师完成工作后，临时用户帐户将被删除。请注意，每次为目录请求交互式凭据时，Amazon Directory Service管理团队收到通知。

的主要概念AmazonMicrosoft AD

你会从中获得更多Amazon如果您熟悉以下主要概念，将能够管理 Microsoft AD。

主题

- Active Directory 架构 (p. 16)
- 修补和维护AmazonMicrosoft AD 托管 (p. 16)
- 组托管服务账户 (p. 17)
- 委托 Kerberos 约束委托 (p. 17)

Active Directory 架构

架构是属于分布式目录一部分的属性和类的定义，与数据库中的字段和表类似。架构包含一组规则，它们确定可以在数据库中添加或包含的数据的类型和格式。User 类是存储在数据库中的类 的一个示例。User 类属性的示例如用户的名字、姓氏、电话号码等。

架构元素

属性、类和对象是用于在架构中构建对象定义的基本元素。下面提供了在开始扩展的过程之前务必要了解的架构元素的相关详细信息。Amazon托管的 Microsoft AD 架构。

属性

每个架构属性 (attribute，类似于数据库中的字段) 都具有若干个定义属性 (attribute) 特征的属性 (property)。例如，LDAP 客户端用于读取和写入属性 (attribute) 的属性 (property) 是 `LDAPDisplayName`。`LDAPDisplayName` 属性 (property) 在所有属性 (attribute) 和类中必须是唯一的。有关属性 (attribute) 特征的完整列表，请参阅 MSDN 网站上的 Characteristics of Attributes。有关如何创建新属性 (attribute) 的其他指导，请参阅 MSDN 网站上的 Defining a New Attribute。

类

类与数据库中的表类似，也要定义几个属性 (property)。例如，`objectClassCategory` 定义类的类别。有关类特征的完整列表，请参阅 MSDN 网站上的 Characteristics of Object Classes。有关如何创建新类的更多信息，请参阅 MSDN 网站上的 Defining a New Class。

对象标识符 (OID)

每个类和属性都必须具有一个对所有对象唯一的 OID。软件供应商必须获取自己的 OID 以确保唯一性。当多个应用程序将相同属性用于不同用途时，唯一性可避免冲突。要确保唯一性，可以从 ISO 名称注册机构获取根 OID。或者可以从 Microsoft 获取基本 OID。有关 OID 以及如何获取它们的更多信息，请参阅 MSDN 网站上的 Object Identifiers。

架构链接属性

某些属性使用向前和向后链接在两个类之间进行链接。最好的示例是组。查看某个组时，会显示该组的成员；如果查看某个用户，可以看到它所属的组。将用户添加到组时，Active Directory 会创建指向组的向前链接。随后 Active Directory 会添加从组到用户的向后链接。创建将链接的属性时，必须生成唯一链接 ID。有关更多信息，请参阅 MSDN 网站上的 Linked Attributes。

相关主题

- 什么时候延长Amazon托管的 Microsoft AD 架构 (p. 112)
- 教程：扩展您的Amazon托管的 Microsoft AD 架构 (p. 112)

修补和维护AmazonMicrosoft AD 托管

AmazonDirectory Service by Microsoft Active Directory，也称作AmazonDSAmazonMicrosoft AD 实际上是作为托管服务提供的 Microsoft Active Directory 域服务 (AD DS)。此系统使用 Microsoft Windows Server 2012 R2 作为域控制器 (DC)，Amazon 向 DC 添加软件来用于服务管理目的。Amazon 更新（修补）DC 以添加新功能并使 Microsoft Windows Server 软件保持最新状态。在修补过程中，您的目录仍可供使用。

确保可用性

默认情况下，每个目录由两个 DC 组成，每个 DC 安装在不同的可用区。您可以自行选择增加 DC 来进一步提高可用性。Amazon 按顺序修补 DC，在此期间，Amazon 正在积极修补的 DC 不可用。如果您的一个或多个 DC 暂时停止服务，Amazon 将延迟修补操作，直到您的目录至少有两个可正常工作的 DC。这让您在修

补期间能够使用其他正常工作的 DC。每个 DC 的修补时间通常为 30 到 45 分钟，具体用时可能有所不同。为确保在一个或多个 DC 因任何原因 (包括修补) 不可用时您的应用程序能够访问正常工作的 DC，应用程序应使用 Windows DC 定位器服务，而不要使用静态 DC 地址。

了解修补计划

为使您的 DC 上的 Microsoft Windows Server 软件保持最新状态，Amazon 使用了 Microsoft 更新。Microsoft 每月为 Windows Server 提供汇总补丁，这使得 Amazon 有机会在三个日历周的时间里尽最大努力测试汇总补丁并将其应用至所有客户 DC。此外，Amazon 还将根据 DC 适用性和紧急程度审查 Microsoft 在每月汇总补丁以外发布的更新。对于被 Microsoft 评定为关键 或重要 的 DC 相关安全补丁，Amazon 将尽一切努力在五天内测试和部署补丁。

组托管服务账户

在 Windows Server 2012 中，Microsoft 引入管理员可用于管理服务账户的新方法，称为组托管服务账户 (gMSA)。使用 gMSA，服务管理员不再需要手动管理服务实例之间的密码同步。管理员可以在 Active Directory 中轻松地创建一个 gMSA，然后配置多个服务实例来使用这个 gMSA。

要授予权限以便用户Amazon托管微软 AD 可以创建 gMSA，您必须将其账户添加作为Amazon托管服务账户委托管理员安全组。默认情况下，管理员账户是该组的成员。有关 gMSA 的更多信息，请参阅 Microsoft TechNet 网站上的 组托管服务账户概览。

相关的 Amazon 安全博客文章

- Amazon Managed Microsoft AD 如何帮助简化部署，并提高与 Active Directory 集成的 .NET 应用程序的安全性

委托 Kerberos 约束委托

Kerberos 约束委托是 Windows Server 中的一项功能。此功能使得服务管理员可以限制应用程序能够代表用户执行操作的范围，从而指定和实施应用程序信任边界。这在您需要配置哪些前端服务账户可以委托给其后端服务时非常有用。Kerberos 约束委托还可以防止 gMSA 代表您的 Active Directory 用户连接到所有服务，避免恶意开发人员可能的滥用。

例如，假设用户 jsmith 登录到 HR 应用程序。您希望 SQL Server 应用 jsmith 的数据库权限。但是，默认情况下 SQL Server 使用应用 hr-app-service 权限的服务账户凭证打开数据库连接，而不是 jsmith 配置的权限。您必须使 HR 薪资应用程序能够使用 jsmith 的凭证访问 SQL Server 数据库。要做到这一点，您需要为的 hr-app-service 服务账户启用 Kerberos 约束委托。Amazon中的托管的 Microsoft AD 目录Amazon. 当 jsmith 登录时，Active Directory 提供 Kerberos 票证，当 jsmith 尝试访问网络上的其他服务时，Windows 自动使用该票证。Kerberos 委托使得 hr-app-service 账户在访问数据库时可以重用 jsmith Kerberos 票证，从而在打开数据库连接时将特定权限应用到 jsmith。

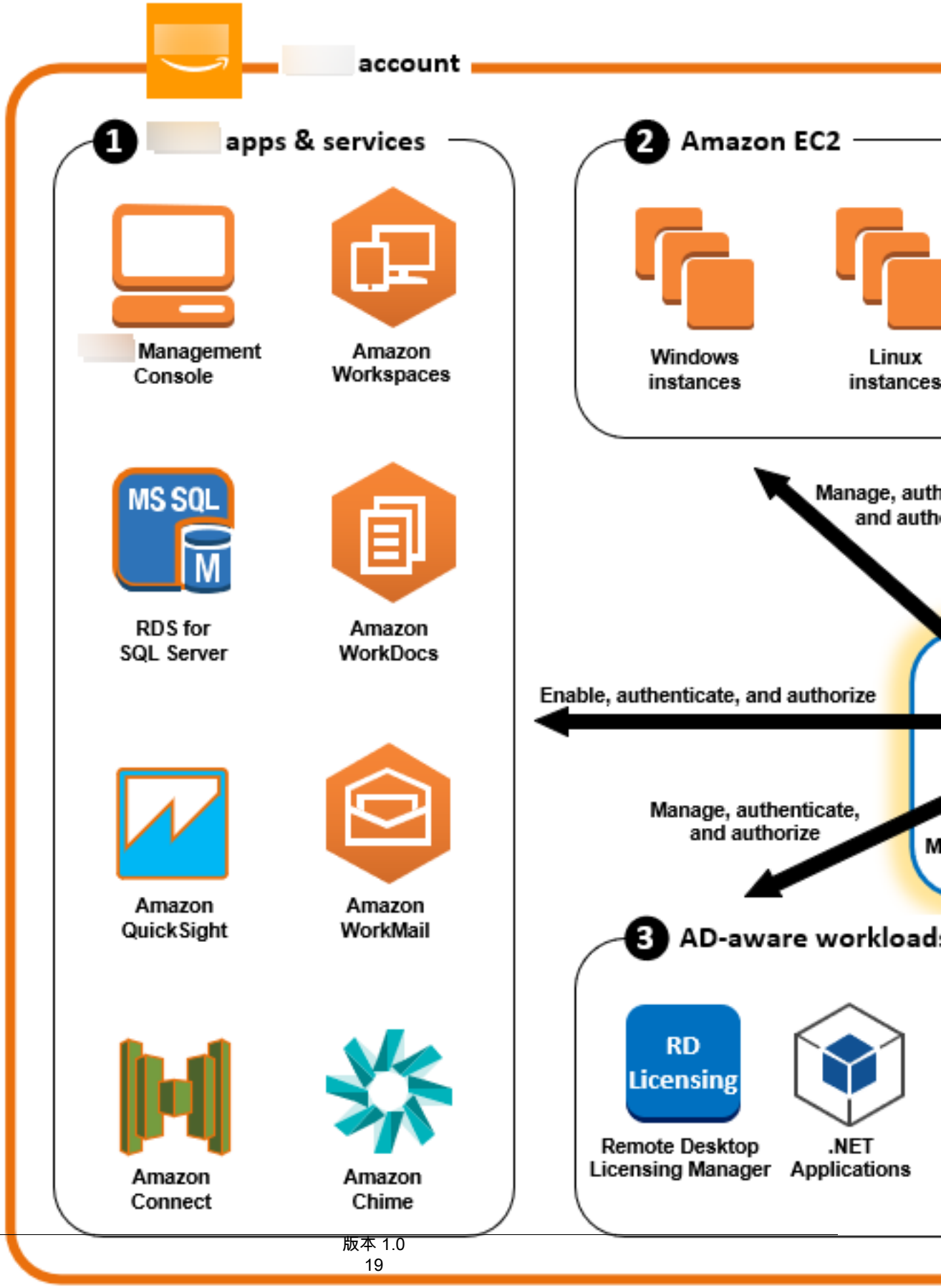
授予允许用户进入的权限Amazon要配置 Kerberos 约束委托，您必须将其账户添加作为AmazonKerberos 委托管理员安全组。默认情况下，管理员账户是该组的成员。有关 Kerberos 约束委托中的更多信息，请参阅 Microsoft TechNet 网站上的 Kerberos 约束委托概览。

Windows Server 2012 中引入了基于资源的约束委托。此功能使后端服务管理员能够为服务配置约束委托。

的使用案例Amazon托管的 Micros

与AmazonManaged Microsoft AD，多个使用案例可以共享单个目录。例如，您可共享目录以对 .NET 应用程序的访问进行身份验证和授权。Amazon RDS for SQL Server和Windows 身份验证启用，和Amazon Chime用于消息传递和视频会议。

下图显示了您的一些使用案例Amazon托管的 Microsoft A 这些案例包括授予用户访问外部云应用程序的功能，以及允许您的本地 AD 用户管理和访问 Amazon 云中资源的功能。


account
1
apps & services
Management Console
Amazon Workspaces
MS SQL
M
RDS for SQL Server
Amazon WorkDocs
Amazon QuickSight
Amazon WorkMail
Amazon Connect
Amazon Chime
2
Amazon EC2
Windows instances
Linux instances
Manage, auth
and auth
Enable, authenticate, and authorize
Manage, authenticate, and authorize
M
3
AD-aware workload
RD Licensing
Remote Desktop Licensing Manager
.NET Applications

使用Amazon为以下任一业务使用案例管理 Microsoft AD。

主题

- 使用案例 1：登录到Amazon应用程序和服务具有 AD 凭证 (p. 20)
- 使用案例 2：管理Amazon EC2 实例 (p. 23)
- 使用案例 3：将目录服务提供给您的 AD 感知工作负载 (p. 23)
- 使用案例 4：至 Office 365 和其他云应用程序的 SSSO (p. 23)
- 使用案例 5：将您的本地 AD 扩展到Amazon云 (p. 24)
- 使用案例 6：共享目录以将 Amazon EC2 实例无缝加入域Amazon账户 (p. 24)

使用案例 1：登录到Amazon应用程序和服务具有 AD 凭证

你可以启用多个Amazon应用程序和服务Amazon Client VPN、Amazon Web Services Management Console、Amazon IAM Identity Center (successor to Amazon Single Sign-On)、Amazon Chime、Amazon Connect、Amazon FSx、亚马逊 QuickSight、Amazon RDS for SQL Server、亚马逊 WorkDocs、亚马逊 WorkMail, 和WorkSpaces以使用您的Amazon托管的 Microsoft A 当您启用目录中的一个 Amazon 应用程序或服务时，您的用户可使用其 AD 凭证访问此应用程序或服务。

例如，您可以允许您的用户使用 AD 凭证登录 Amazon Web Services Management Console。为此，请启用Amazon Web Services Management Console作为目录中的应用程序，然后为您的 AD 用户和组分配 IAM 角色。当您的用户登录到Amazon Web Services Management Console，则他们承担一个 IAM 角色来管理Amazon资源的费用。这使您可以轻松为您的用户授予对 Amazon Web Services Management Console的访问权限，而无需配置和管理单独的 SAML 基础设施。

要进一步增强最终用户体验，您可以启用单点登录Amazon 功能 WorkDocs，让您的用户能够访问亚马逊 WorkDocs 从已加入目录的计算机访问，而无需单独输入其凭证。

您可以向目录或本地 AD 中的用户帐户授予访问权限，以便他们可以登录Amazon Web Services Management Console或者通过Amazon CLI使用他们现有的凭证和权限进行管理Amazon资源，方法是将 IAM 角色直接分配给现有用户账户。

FSx for Windows File Server 与Amazon托管的 Micros

将 FSx for Windows File Server 与Amazon托管 Microsoft AD 提供了一个完全托管的基于 Microsoft Windows 的本机服务器消息块 (SMB) 协议文件系统，允许你轻松地将基于 Windows 的应用程序和客户端（使用共享文件存储）移动到Amazon. 尽管FSx for Windows File Server 可以与自我管理的 Microsoft Active Directory 集成，但我们在此不讨论这种情况。

常见的 Amazon FSx 使用案例和资源

本节提供了有关常见 FSx for Windows File Server 与集成的资源的参考Amazon托管的 Microsoft AD 本节中每个使用案例都以 basic 开头AmazonManaged AD fFSx for Windows File Server 配置。有关如何创建这些配置的更多信息，请参阅：

- 开始使用AmazonMicrosoft AD (p. 8)
- Amazon FSx 入门

FSx for Windows File Server 作为 Windows 容器上的持久存储

Amazon Elac Conine (ECS)支持使用经Amazon ECS 优化的 Windows AMI 启动的容器实例上的 Windows 容器。Windows 容器实例使用其自己的 Amazon ECS 容器代理版本。在经 Amazon ECS 优化的 Windows AMI 上，Amazon ECS 容器代理在主机上作为一项服务运行。

Amazon ECS 通过组 Managed Service Account (gMSA)的特殊服务帐户支持 Windows 容器的 Active Directory 身份验证。由于 Windows 容器无法加入域，因此必须将 Windows 容器配置为使用 gMSA 运行。

相关联项目

- 在 Windows 容器上使用 FSx for Windows File Server 作为持久存储
- 组托管服务账户

亚马逊 AppStream 2.0 支持

亚马逊 AppStream 2.0是一项完全托管的应用程序流服务。它为用户提供了一系列解决方案，通过他们的应用程序保存和访问数据。Amazon FSx 与 AppStream 2.0 提供使用 Amazon FSx 的个人永久存储驱动器，可以配置为提供共享文件夹来访问常用文件。

相关联项目

- 演练4：在Amazon FSx 上使用 AppStream 2.0
- 在Amazon FSx 上使用 AppStream 2.0
- 将 Active Directory 与 结合使用 AppStream 2.0

Microsoft SQ

fsX for Windows File Server 可以用作微软 SQL Server 2012（从 2012 版 11.x 开始）和较新的系统数据库（包括主数据库、Model、MSDB 和 tempDB）以及数据库引擎用户数据库的存储选项。

相关联项目

- 安装带有 SMB 文件共享存储的 SQL Server
- 使用 FSx for Windows File Server 简化您的高可用性部署
- 组托管服务账户

主文件夹和漫游用户配置文件支持

FSx for Windows File Server 可用于将来自 Active Directory 用户主文件夹和 “我的文档” 的数据存储在中央位置。FSx for Windows File Server 也可用于存储漫游用户配置文件中的数据。

相关联项目

- 借助亚马逊 FSX 轻松实现 Windows 主目录
- 部署漫游用户配置文件
- 将 FSx for Windows File Server 与 WorkSpaces

网络文件共享支持

FSx for Windows 文件服务器上的联网文件共享提供了一种托管且可扩展的文件共享解决方案。一个用例是可以手动或通过组策略创建的客户端的映射驱动器。

相关联项目

- 演练6：使用碎片扩展性能
- 驱动器器盘点
- 将 FSx for Windows File Server 与 WorkSpaces

组策略软件安装支持

由于 SYSVOL 文件夹的大小和性能受到限制，因此最好避免在该文件夹中存储诸如软件安装文件之类的数据。作为一种可能的解决方案，可以将 FSx for Windows File Server 配置为存储使用组策略安装的所有软件文件。

相关联项目

- 如何使用组策略在 Windows Server 2008 和 Windows Server 2003 中远程安装软件

Windows 服务器Backup 目标支持

可以使用 UNC 文件共享在 Windows 服务器Backup 中将FSx for Windows File Server 配置为目标驱动器。在这种情况下，您需要指定 FSx for Windows File Server 的 UNC 路径，而不是指向连接的 EBS 卷的 UNC 路径。

相关联项目

- 对服务器执行系统状态恢复

Amazon FSx 也支持Amazon管理 Microsoft AD 目录共享 有关更多信息，请参阅：

- 共享您的目录 (p. 58)
- 将 Amazon FSx 与Amazon在不同的 VPC 或账户中托管微软 AD

Amazon RDS 与Amazon托管的 Micros

Amazon RDS 支持使用 Kerberos 与Microsoft Active Director Kerberos 是一种网络身份验证协议，它使用票证和对称密钥加密，而不再需要通过网络传输密码。Amazon RDS 支持 Kerberos 和 Active Directory，从而为数据库用户提供单一登录和集中身份验证的好处，以便您可以在 Active Directory 中保留您的用户凭证。

要开始使用这个用例，你首先需要设置一个 basicAmazonManaged AD 和 Amazon RDS 配置。

- 开始使用AmazonMicrosoft AD (p. 8)
- 开始使用 Amazon RDS

下面引用的所有用例都将从基础开始Amazon管理微软 AD 和 Amazon RDS，并介绍如何将 Amazon RDS 与Amazon托管Microsoft

- 对 Amazon RDS for SQL Server 数据库实例使用 Windows 身份验证
- 对 MySQL 使用 Kerberos 身份验证
- 将 Kerberos 身份验证与Amazon RDS for Oracle 使用
- 将 Kerberos 身份验证与Amazon RDS for PostgreSQL 使用

Amazon RDS 还支持Amazon管理 Microsoft AD 目录共享 有关更多信息，请参阅：

- 共享您的目录 (p. 58)
- 将多个账户的 Amazon RDS 数据库实例加入到单个共享域

.NET 应用程序使用适用Amazon RDS for SQL Server 和组托管

您可以将适用Amazon RDS for SQL Server 与基本的 .NET 应用程序和组托管服务账户 (gMSAs) 集成。有关更多信息，请参阅 。操作方法AmazonManaged Microsoft AD 有助于简化部署，并提高与 Active Directory 集成的 .N

使用案例 2：管理Amazon EC2 实例

通过使用熟悉的 AD 管理工具，您可以应用 AD 组策略对象 (GPO)，以通过以下方式集中管理 Amazon EC2 for Windows 或 Linux 实例将您的实例加入您的AmazonMicrosoft AD.

此外，您的用户可以使用其 AD 凭证登录您的实例。从而无需使用单独的实例凭证或分配私钥 (PEM) 文件。这使您能够通过使用您已使用的 AD 用户管理工具，更轻松地立即授予或撤销用户的访问权限。

使用案例 3：将目录服务提供给您的 AD 感知工作负载

AmazonManaged Microsoft AD 是使您能够运行传统 AD 感知工作负载 (如远程桌面授权管理器和微软 SharePoint 和 Microsoft SQL Ser中的Amazon云计算。AmazonManaged Microsoft AD 还帮助您简化集成 AD 的 .NET 应用程序并提高此应用程序的安全性组托管服务帐户 (gMSAs) 和 Kerberos 约束委派 (KCD).

使用案例 4：至 Office 365 和其他云应用程序的 SSSO

您可以使用Amazon管理 Microsoft AD 以为云应用程序提供 SSSO。您可以使用 Azure AD Connect 将您的用户同步到 Azure AD，然后使用 Active Directory 联合身份验证服务 (AD FS)，以便您的用户可以访问Microsoft Office 365和其他 SAML 2.0 云应用程序使用其 AD 凭据。

集成Amazon通过 IAM 身份中心管理微软 AD将 SAML 功能添加到您的AmazonManaged Microsoft AD 和/或您的本地可信域。集成后，您的用户就可以将 IAM 身份中心与支持 SAML 的服务结合使用，包括Amazon Web Services Management Console和第三方云应用程序（如 Office 365、Concur 和 Salesforce），而无需配置 SAML 基础设施即可实现。有关允许本地用户使用 IAM Identity Center 的流程的演示，请参阅以下内容 YouTube 视频。

使用案例 5：将您的本地 AD 扩展到Amazon云

如果您已有一个 AD 基础设施并且要在将 AD 感知工作负载迁移至Amazon云计算，Amazon托管的 Microsoft AD 可以 您可以使用AD 信托连接Amazon将Microsoft AD 托管到您的现有AD 这意味着，您的用户可以使用其本地 AD 凭证访问 AD 感知应用程序和 Amazon 应用程序，无需您同步用户、组或密码。

例如，您的用户可以登录Amazon Web Services Management Console和 Amazon WorkSpaces 通过使用其现有 AD 用户名和密码。此外，当您使用广告感知应用程序时，例如 SharePoint 和AmazonManaged Microsoft AD，您的已登录 Windows 用户可以访问这些应用程序，而无需再次输入凭证。

您也可以将您的本地 Active Directory (AD) 域迁移至Amazon使用活动目录迁移工具包 (ADMT)以及密码导出服务 (PES) 来执行迁移。

使用案例 6：共享目录以将 Amazon EC2 实例无缝加入域Amazon账户

在多个 Amazon 账户间共享目录让您可以轻松管理 Amazon 服务（例如 Amazon EC2），无需为每个账户和每个 VPC 操作目录。你可以从任何地方使用你的目录Amazon账户和任何Amazon VPC在Amazon区域。此功能可让您跨多个账户和 VPC，使用单个目录更轻松且更经济高效地管理可感知目录的工作负载。例如，您

现在可以管理您的Windows 工作负载使用单个账户和 VPC 轻松部署在 EC2 实例中Amazon托管的 Microsoft A

当你分享你的Amazon使用另一个 Microsoft AD 目录Amazon账户，您可以使用 Amazon EC2 控制台或Amazon Systems Manager从账户中的任意 Amazon VPC 加入实例Amazon区域。您可以消除手动将实例加入域或者在各个账户和 VPC 中部署目录的需求，从而在 EC2 实例上快速部署可感知目录的工作负载。有关更多信息，请参阅共享您的目录 (p. 58)。

如何管理AmazonMicrosoft Managed Microsoft AD

此节列出了运行和维护的所有过程。Amazon管理的 Microsoft AD 环境。

主题

- 保护您的Amazon托管的 Microsoft AD 目录 (p. 25)
- 监控Amazon托管的 Microsoft AD (p. 47)
- 多区域复制 (p. 54)
- 共享您的目录 (p. 58)
- 将 EC2 实例加入Amazon托管的 Microsoft AD 目录 (p. 66)
- 在中管理用户和组AmazonMicrosoft Managed Microsoft AD (p. 93)
- Connect 到您的现有 AD 基础设施 (p. 96)
- 扩展你的架构 (p. 111)
- 维护您的AmazonMaged Microsoft AD 目录 (p. 116)
- 向用户和组授予访问权限Amazon资源 (p. 120)
- 启用访问权限Amazon应用程序和服务 (p. 124)
- 允许访问Amazon Web Services Management Console使用 AD 凭据 (p. 130)
- 部署额外的域控制器 (p. 132)
- 将用户从 Active Directory 迁移到Amazon托管的 Microsoft AD (p. 136)

保护您的Amazon托管的 Microsoft AD 目录

此节介绍了保护您的Amazon托管的 Microsoft AD 环境。

主题

- 管理密码策略Amazon托管的 Microsoft AD (p. 25)
- 为启用多重验证Amazon托管的 Managed (p. 28)
- 启用安全 LDAP (LDAPS) (p. 30)
- 管理合规性AmazonManaged Mic (p. 37)
- 增强您的Amazon托管的 Microsoft AD 网络安全配置 (p. 38)
- 配置目录安全设置 (p. 44)

管理密码策略Amazon托管的 Microsoft AD

Amazon使您可以为您在中管理的用户组定义和分配不同的精细密码和账户锁定策略 (也称为精细密码策略)。Amazon托管的 Microsoft AD 域。当您创建一个Amazon创建一个默认域策略并将其应用于此目录。此策略包含以下设置：

Policy	设置
强制密码历史	记住 24 个密码
最长密码使用期限	42 天 *
最短密码使用期限	1 天
最短密码长度	7 个字符
密码必须符合复杂性要求	已启用
使用可逆加密存储密码	已禁用

* 注意：最长 42 天的密码使用期限包括管理员密码。

例如，对于仅有权访问敏感度不高的信息的员工，您可以设置较为宽松的策略设置。对于定期访问机密信息的高级经理，您可以应用更严格的设置。

Amazon在中提供了一组精细密码策略Amazon您可以配置这些 AD 并分配给您的组。要配置策略，您可以使用标准的 Microsoft 策略工具，例如Active Directory 管理中心. 要开始使用 Microsoft 策略工具，请参阅安装 Active Directory 管理工具 (p. 93)。

主题

- 支持的策略设置 (p. 26)
- 委托谁可以管理您的密码策略 (p. 27)
- 为您的用户分配密码策略 (p. 28)

相关Amazon安全博客文章

- 如何配置更强大的密码策略以帮助满足您的安全标准Amazon Directory Service为了Amazon托管的 Microsoft AD

支持的策略设置

Amazon托管的 Microsoft AD 包括五个精细策略，这些策略带有不可编辑的优先顺序值。这些策略具有各种属性，您可以配置这些属性，在出现登录失败的情况下实施密码强度和账户锁定操作。您可以将策略分配给零个或多个 Active Directory 组。如果最终用户是多个组的成员并接收多个密码策略，Active Directory 将会强制实施优先顺序值最低的策略。

Amazon预定义密码策略

下表列出了您的Amazon托管的 Microsoft AD 目录及其分配的优先顺序值。有关更多信息，请参阅 优先顺序 (p. 27)。

策略名称	优先顺序
CustomerPSO-01	10
CustomerPSO-02	20
CustomerPSO-03	30
CustomerPSO-04	40

策略名称	优先顺序
CustomerPSO-05	50

密码策略属性

您可以编辑您的密码策略中的以下属性，以便符合合规性标准，从而满足您的业务需求。

- 策略名称
- 强制密码历史
- 最短密码长度
- 最短密码使用期限
- 最长密码使用期限
- 使用可逆加密存储密码
- 密码必须符合复杂性要求

您无法修改这些策略的优先顺序值。有关这些设置如何影响密码强制的更多信息，请参阅广告 DS：精细密码策略在Microsoft TechNet网站. 有关这些策略的一般信息，请参阅密码策略在Microsoft TechNet网站.

账户锁定策略

您还可以修改密码策略的以下属性，以指定 Active Directory 在登录失败时是否以及如何锁定账户：

- 允许的最大失败登录尝试数
- 账户锁定持续时间
- 在一段持续时间后重置失败的登录尝试

有关这些策略的一般信息，请参阅账户锁定策略在Microsoft TechNet网站.

优先顺序

策略的优先顺序值越小，优先级越高。您可以将密码策略分配给 Active Directory 安全组。虽然您应该将一个策略应用到一个安全组，不过单个用户可以接收多个密码策略。例如，假设 `jsmith` 是 HR 组的成员，同时还是经理组的成员。如果您将 CustomerPSO-05 (优先顺序值为 50) 分配给 HR 组，将 CustomerPSO-04 (优先顺序值为 40) 分配给经理组，则 CustomerPSO-04 具有更高的优先级，并且 Active Directory 会将策略应用于 `jsmith`。

如果您将多个策略分配给用户或组，Active Directory 将按照以下方式确定生成的策略：

1. 应用您直接分配给用户对象的策略。
2. 如果未直接向用户对象分配任何策略，由于组成员资格的原因，会应用该用户收到的所有策略中具有最低优先顺序值的策略。

有关其他信息，请参阅广告 DS：精细密码策略在Microsoft TechNet网站.

委托谁可以管理您的密码策略

您可以将管理密码策略的权限委派给您在Amazon通过将帐户添加到Amazon精细密码策略委托管理员安全组。当账户成为该组的成员时，该账户有权编辑和配置前面 (p. 26)列出的任何密码策略。

委托谁可以管理密码策略

1. 启动活动目录管理中心 (ADAC)从您加入到的任何托管 EC2 实例Amazon托管的 Microsoft AD 域。

2. 切换到树视图然后导航到Amazon委托组OU。有关此 OU 的更多信息，请参阅 创建的内容 (p. 10)。
3. 查找Amazon精细密码策略委托管理员用户组。将任何用户或组从您的域添加到该组。

为您的用户分配密码策略

作为成员的用户帐户Amazon精细密码策略委托管理员安全组可以使用以下过程将策略分配给用户和安全组。

为您的用户分配密码策略

1. 启动活动目录管理中心 (ADAC)从您加入到的任何托管 EC2 实例Amazon托管的 Microsoft AD 域。
2. 切换到 Tree View，然后导航到 System\Password Settings Container。
3. 双击您要编辑的精细策略。单击 Add 可编辑策略属性，并将用户或安全组添加到策略。有关随一起提供的默认精细策略的更多信息Amazon托管的 Microsoft AD，请参阅Amazon预定义密码策略 (p. 26).
4. 要验证是否应用了密码策略，请运行以下 PowerShell 命令：

```
Get-ADUserResultantPasswordPolicy -Identity 'username'
```

如果您未配置您的中五个密码策略中的任何一个AmazonActive AD 目录使用默认域组策略。有关使用密码设置容器的其他详细信息，请参阅此 Microsoft 博客文章。

为启用多重验证Amazon托管的 Managed

您可以为启用多重验证 (MFA)Amazon托管的 Microsoft AD 目录，以提高您的用户指定其 AD 凭证来访问时的安全性支持的 Amazon 企业应用程序 (p. 30). 启用 MFA 后，您的用户如常输入其用户名和密码 (第一安全要素)，它们还必须输入通过您的虚拟或硬件 MFA 解决方案获取的身份验证代码 (第二安全要素)。除非用户提供有效的用户凭证和 MFA 代码，否则这些安全要素将通过阻止对您的 Amazon 企业应用程序的访问来提高安全性。

要启用 MFA，您必须有一个 MFA 解决方案远程身份验证拨入用户服务(RADIUS) 服务器，或已在本地基础设施中实现的 RADIUS 服务器必须具有 MFA 插件。您的 MFA 解决方案应实施一次性密码 (OTP)，用户可从硬件设备或在设备 (如手机) 上运行的软件来获取此密码。

RADIUS 是一种行业标准客户端/服务器协议，提供身份验证、授权和账户管理，以使用户能够连接到网络服务。Amazon托管的 Microsoft AD 包括一个 RADIUS 客户端，此客户端将连接到您在其上已实现 MFA 解决方案的 RADIUS 服务器。您的 RADIUS 服务器将验证用户名和 OTP 代码。如果您的 RADIUS 服务器成功验证用户，Amazon然后 Microsoft AD 将针对 AD 对用户进行身份验证。AD 身份验证成功后，用户之后可访问Amazon应用程序. 两者之间的通信Amazon托管的 Microsoft AD RADIUS 客户端和您的 RADIUS 服务器需要您Amazon启用通过端口 1812 进行通信的安全组。

您可以为启用多重验证Amazon通过执行以下过程来管理 Microsoft AD 目录。有关如何配置 RADIUS 服务器以使用 Amazon Directory Service 和 MFA 的更多信息，请参阅多重验证 (p. 9)。

> **Note**
>
> 多重验证对 Simple AD 不可用。但是，可为您的 AD Connector 目录启用 MFA。有关更多信息，请参阅 为 AD Connector 启用多重验证 (p. 183)。

> **Note**
>
> MFA 是AmazonMicrosoft AD 如果您将多区域复制 (p. 54)，则必须在每个区域分别应用以下程序。有关更多信息，请参阅 全球与区域功能 (p. 54)。

为 启用多重验证Amazon托管的 Managed

1. 确定您的 RADIUS MFA 服务器的 IP 地址和您的AmazonManaged 目录。

2. 编辑您的 Virtual Private Cloud (VPC) 安全组以允许通过端口 1812 的通信Amazon托管微软 AD IP 端点和你的 RADIUS MFA 服务器。
3. 在Amazon Directory Service控制台导航窗格中，选择目录.
4. 选择目录ID链接AmazonManaged 目录。
5. 在存储库的目录详细信息页面上，执行以下操作之一：
   - 如果您在下面显示多个区域多区域复制，选择要在其中启用 MFA 的区域，然后选择网络和安全选项卡。有关更多信息，请参阅 主要与其他地区 (p. 55)。
   - 如果您没有在下面显示任何区域多区域复制，选择网络和安全选项卡。
6. 在多重验证部分中，选择操作，然后选择启用。
7. 在存储库的启用多重验证 (MFA)页面上，提供以下值：

   显示标签

   提供标签名称。

   RADIUS 服务器 DNS 名称或 IP 地址

   您的 RADIUS 服务器终端节点的 IP 地址或者您的 RADIUS 服务器负载均衡器的 IP 地址。您可以通过用逗号分隔来输入多个 IP 地址（例如`192.0.0.0,192.0.0.12`)。

   Note

   RADIUS MFA 仅适用于对Amazon Web Services Management Console，或亚马逊企业应用程序和服务，例如 WorkSpaces，Amazon QuickSight，或 Amazon Chime。它不为在 EC2 实例上运行的 Windows 工作负载提供 MFA，也不会为登录 EC2 实例提供 MFA。Amazon Directory Service不支持 RADIUS 质询/响应身份验证。
   用户在输入其用户名和密码时必须具有 MFA 代码。或者，您必须使用执行 MFA 的解决方案 out-of-band 例如用户的 SMS 文本验证。In out-of-band MFA 解决方案，您必须确保为解决方案适当设置 RADIUS 超时值。使用 out-of-band MFA 解决方案，登录页面将提示用户输入 MFA 代码。在这种情况下，用户必须在密码字段和 MFA 字段中输入密码。

   端口

   RADIUS 服务器用来通信的端口。您的本地网络必须允许通过默认 RADIUS 服务器端口 (UDP: 1812) 从Amazon Directory Service服务器。

   Shared secret code

   在创建 RADIUS 终端节点时指定的共享密码。

   Confirm shared secret code (确认共享密码)

   确认您的 RADIUS 终端节点的共享密码。

   协议

   选择在创建 RADIUS 终端节点时指定的协议。

   服务器超时（以秒为单位）

   等待 RADIUS 服务器响应的时间长度 (以秒为单位)。此值必须介于 1 和 50 之间。

   Note

   我们建议将 RADIUS 服务器超时配置为 20 秒或更短。如果超时时间超过 20 秒，系统将无法使用其他 RADIUS 服务器重试，并可能导致超时失败。

   RADIUS 请求重试次数上限

   将尝试与 RADIUS 服务器通信的次数。此值必须介于 0 和 10 之间。

   当 RADIUS Status 更改为 Enabled 时，多重验证将可用。

8. 请选择 Enable。

支持的 Amazon 企业应用程序

所有亚马逊企业 IT 应用程序包括 WorkSpaces，Amazon WorkDocs，Amazon WorkMail，Amazon QuickSight，以及访问权限Amazon IAM Identity Center (successor to Amazon Single Sign-On)和Amazon Web Services Management Console使用时支持AmazonMFA 托管的 Microsoft AD Connector

有关如何使用 Amazon Directory Service 配置对 Amazon 企业应用程序、Amazon Single Sign-On 和 Amazon Web Services Management Console的基本用户访问权限的信息，请参阅启用访问权限Amazon应用程序和服务 (p. 124)和允许访问Amazon Web Services Management Console使用 AD 凭据 (p. 130)。

相关Amazon安全博客文章

- 如何为启用多重验证Amazon通过使用Amazon托管微软 AD 和本地凭据

启用安全 LDAP (LDAPS)

轻量目录访问协议 (LDAP) 是用于与 Active Directory 之间读取和写入数据的标准通信协议。一些应用程序使用 LDAP 在 Active Directory 中添加、删除或搜索用户和组，或者传输凭证以便在 Active Directory 中对用户进行身份验证。每个 LDAP 通信均包括一个客户端（例如应用程序）和一个服务器（例如 Active Directory）。

默认情况下，LDAP 通信未加密。这使得恶意用户能够使用网络监控软件查看传输中的数据包。这就是许多企业安全策略通常要求组织加密所有 LDAP 通信的原因。

为了减轻这种形式的数据泄露，Amazon托管微软 AD 提供了一个选项：您可以启用通过安全套接字层 (SSL)/传输层安全性 (TLS) 的 LDAP 通信（也称为 LDAPS）。利用 LDAPS，您可以提高整个网络的安全性。您还可以通过加密启用了 LDAP 的应用程序和之间的所有通信来满足合规性要求。Amazon托管的 Microsoft AD。

Amazon在以下两种部署方案中，托管的 Microsoft AD 都支持 LDAPS：

- 服务器端 LDAPS对商业或自行开发的 LDAP 感知应用程序（充当 LDAP 客户端）之间的 LDAP 通信进行加密；Amazon托管微软 AD（充当 LDAP 服务器）。有关更多信息，请参阅 使用启用服务器端 LDAPSAmazon托管的 Microsoft AD (p. 30)。
- 客户端 LDAPS加密之间的 LDAP 通信Amazon应用程序，例如 WorkSpaces（充当 LDAP 客户端）和自行管理的 Active Directory（充当 LDAP 服务器）。有关更多信息，请参阅启用客户端 LDAPSAmazonMicroso AD (p. 33)。

主题

- 使用启用服务器端 LDAPSAmazon托管的 Microsoft AD (p. 30)
- 启用客户端 LDAPSAmazonMicroso AD (p. 33)

使用启用服务器端 LDAPSAmazon托管的 Microsoft AD

服务器端 LDAPS 支持加密商业或自行开发的 LDAP 感知应用程序与您的 LDAP 通信Amazon管理 Microsoft AD 目录。这有助于使用安全套接字层 (SSL) 加密协议来提高整个网络的安全性并满足合规性要求。

启用服务器端 LDAPS

有关如何设置和配置服务器端 LDAPS 和证书颁发机构 (CA) 服务器的详细说明，请参阅如何为您的启用服务器端 LDAPSAmazon托管的 Microsoft AD 目录在Amazon安全博客。

您必须从用于管理您的 Amazon EC2 实例执行大多数设置。Amazon托管的 Microsoft AD 域控制器。以下步骤指导您完成在 Amazon 云中为您的域启用 LDAPS 的过程。

如果需要使用自动化设置 PKI 基础设施，可以使用启用 Microsoft 公有密钥基础设施AmazonQuickStart 指南. 具体而言，您需要按照指南中的说明加载模板在 Amazon 上将 Microsoft PKI 部署到现有 VPCAmazon. 加载模板后，一定要选择**AWSManaged**当你到达Active Directory 域服务类型选项。如果你使用了 QuickStart 指南，你可以直接跳转到第 3 步：创建证书模板 (p. 31).

主题

- 第 1 步：谁可以启用 LDAPS (p. 31)
- 第 2 步：设置你的证书颁发机构 (p. 31)
- 第 3 步：创建证书模板 (p. 31)
- 第 4 步：添加安全组规则 (p. 32)

第 1 步：谁可以启用 LDAPS

要启用服务器端 LDAPS，您必须是管理员或Amazon您的企业证书颁发机构委托管理员组Amazon管理 Microsoft AD 目录。或者，您可以是默认管理用户（管理员账户）。如果您愿意，您可以拥有一个管理员账户设置 LDAPS 之外的用户。在这种情况下，将该用户添加到管理员或Amazon您的企业证书颁发机构委托管理员组Amazon管理 Microsoft AD 目录。

第 2 步：设置你的证书颁发机构

您必须先创建一个证书，然后才能启用服务器端 LDAPS。此证书必须由已加入您的 Microsoft 企业 CA 服务器颁发。Amazon托管的 Microsoft AD 域。在创建后，该证书必须安装到该域中您的每个域控制器上。此证书使域控制器上的 LDAP 服务能够侦听并自动接受来自 LDAP 客户端的 SSL 连接。

> **Note**
>
> 使用服务器端 LDAPSAmazon托管的 Microsoft AD 不支持由独立 CA 颁发的证书。此外，它也不支持由第三方证书颁发机构颁发的证书。

根据您的业务需求，您有以下选择来设置或连接到您域中的 CA：

- 创建下属微软企业 CA—（推荐）使用此选项，您可以在Amazon云。服务器可以使用 Amazon EC2，以便与现有根 Microsoft CA 一起使用。有关如何设置从属 Microsoft 企业 CA 的更多信息，请参阅步骤 4: 将微软企业 CA 添加到您的AmazonMicrosoft AD 目录在如何为您的启用服务器端 LDAPSAmazon托管的 Microsoft AD 目录.
- 创建根微软企业 CA— 使用此选项，您可以在Amazon云使用 Amazon EC2 并将其加入Amazon托管的 Microsoft AD 域。此根 CA 可以向您的域控制器颁发证书。有关设置新根 CA 的更多信息，请参阅步骤 3: 安装和配置脱机 CA在如何为您的启用服务器端 LDAPSAmazon托管的 Microsoft AD 目录.

有关如何将您的 EC2 实例加入域的更多信息，请参阅将 EC2 实例加入Amazon托管的 Microsoft AD 目录 (p. 66)。

第 3 步：创建证书模板

设置企业 CA 后，即可配置 Kerberos 身份验证证书模板。

创建证书模板

1. 启动Microsoft Windows Server Manager. Select工具 > 证书颁发机构.
2. 在证书颁发机构窗口中，展开证书颁发机构在左侧窗格中显示树。右键单证书模板，然后选择Manage.
3. 在控制台证书模板窗口，右键单击Kerberos 身份验证然后选择复制模板.
4. 这些区域有：新模板的属性窗口将弹出。
5. 在新模板的属性在窗口中，转至兼容性选项卡，然后执行以下操作：

   a. 变更颁发机构转到与您的 CA 匹配的操作系统。

b. 如果产生的更改弹出窗口，选择确定.
c. 变更认证收件人到Windows 8.1 /Windows Server 2012 R2.

Note

Amazon托管的 Microsoft AD 由 Windows Server 2012 R2 提供支持。

d. 如果产生的更改窗口弹出，选择确定.
6. 单击普通的选项卡然后更改模板显示名称到ldapOverSSL或者你喜欢的任何其他名字。
7. 单击安全选项卡，然后选择域控制器中的组或用户名部分。在域控制器的权限部分中，验证Allow复选框Read、注册, 和自动注册已检查。
8. 选择确定创建ldapOverSSL（或您在上面指定的名称）证书模板。关闭控制台证书模板窗口。
9. 在证书颁发机构窗口，右键单击证书模板，然后选择新建 > 要颁发的证书模板.
10. 在启用证书模板窗口中，选择ldapOverSSL（或者你在上面指定的名称），然后选择确定.

第 4 步：添加安全组规则

在最后一步中，您必须打开 Amazon EC2 控制台并添加安全组规则。这些规则将允许您的域控制器连接到企业 CA 以请求证书。为此，请添加入站规则，以便您的企业 CA 可以接受来自您的域控制器的传入流量。然后，添加出站规则以允许从您的域控制器到企业 CA 的流量。

一旦配置了两个规则，您的域控制器会自动从您的企业 CA 请求证书，并为您的目录启用 LDAPS。您的域控制器上的 LDAP 服务现已准备好接受 LDAPS 连接。

配置安全组规则

1. 在以下网址导航至 Amazon EC2 控制台：https://console.aws.amazon.com/ec2然后使用管理员凭据登录。
2. 在左侧窗格中，选择 Network & Security 下方的 Security Groups。
3. 在主窗格中，为您的 CA 选择 Amazon 安全组。
4. 选择 Inbound 选项卡，然后选择 Edit。
5. 在 Edit inbound rules 对话框中，执行以下操作：
   - 选择 Add Rule（添加规则）。
   - 为 Type 选择 All traffic，并为 Source 选择 Custom。
   - 输入你的目录Amazon旁边的框中的安全组（例如 sg-123456789）源.
   - 选择保存。
6. 现在选择Amazon您的安全组Amazon管理 Microsoft AD 目录。选择 Outbound 选项卡，然后选择 Edit。
7. 在 Edit outbound rules 对话框中，执行以下操作：
   - 选择 Add Rule（添加规则）。
   - 为 Type 选择 All traffic，并为 Destination 选择 Custom。
   - 在 AmazonDestination 旁边的框中键入您的 CA 的 安全组。
   - 选择保存。

您可以测试与Amazon使用 LDP 工具托管 Microsoft AD 目录。LDP 工具随 Active Directory 管理工具一起提供。有关更多信息，请参阅 安装 Active Directory 管理工具 (p. 93)。

Note

在测试 LDAPS 连接之前，您必须等待最长 30 分钟时间，以便从属 CA 向您的域控制器颁发证书。

有关服务器端 LDAPS 的详细信息以及若要查看如何设置它的示例使用案例，请参阅如何为您的启用服务器端 LDAPSAmazon托管的 Microsoft AD 目录在Amazon安全博客。

启用客户端 LDAPSAmazonMicroso AD

客户端 LDAPS 支持Amazon托管的 Microsoft Active DirectoryAmazon应用程序。此类应用程序的示例包括 WorkSpaces、Amazon IAM Identity Center (successor to Amazon Single Sign-On)，Amazon QuickSight，和 Amazon Chime. 此加密可帮助您更好地保护您组织的身份数据并满足您的安全要求。

先决条件

启用客户端 LDAPS 之前，您需要满足以下要求。

主题

- 在Active Directory (p. 33)
- CA 证书要求 (p. 33)
- 联网要求 (p. 33)

在Active Directory

要启用客户端 LDAPS，您需要为 Active Directory 中的每个域控制器获取并安装服务器证书。LDAP 服务将使用这些证书来侦听并自动接受来自 LDAP 客户端的 SSL 连接。您可以使用由内部 Active Directory Certificate Services (ADCS) 部署颁发的或从商业颁发机构处购买的 SSL 证书。有关 Active Directory 服务器证书要求的更多信息，请参阅 Microsoft 网站上的 LDAP over SSL (LDAPS) 证书。

CA 证书要求

客户端 LDAPS 操作需要证书颁发机构 (CA) 证书，它表示服务器证书的颁发者。CA 证书将与由 Active Directory 域控制器提供的服务器证书匹配来加密 LDAP 通信。请注意以下 CA 证书要求：

- 要注册一个证书，该证书必须在 90 天以后才到期。
- 证书必须采用隐私增强邮件 (PEM) 格式。如果要从 Active Directory 内部导出 CA 证书，请选择 base64 编码的 X.509 (.CER) 作为导出文件格式。
- 每个命令最多可存储五 (5) 个 CA 证书Amazon管理的微软 AD 目录。
- 使用 RSSAS-PSS 签名算法的证书不受支持。
- 必须注册链接到每个受信任域中的每个服务器证书的 CA 证书。

联网要求

Amazon 应用程序 LDAP 流量将仅在 TCP 端口 636 上运行，而不会回退到 LDAP 端口 389。但是，支持复制、信任等的 Windows LDAP 通信将继续使用带有 Windows 本机安全性的 LDAP 端口 389。配置Amazon安全组和网络防火墙，以允许Amazon托管的 Microsoft AD。在之间保留开放的 LDAP 端口 389Amazon管理的微软AD。

启用客户端 LDAPS

要启用客户端 LDAPS，您需要将证书颁发机构 (CA) 证书导入Amazon管理微软 AD，然后在你的目录上启用 LDAPS。启用后，Amazon 应用程序与您自行管理的 Active Directory 之间的所有 LDAP 通信将通过安全套接字层 (SSL) 通道加密进行传输。

您可以使用两种不同的方法为您的目录启用客户端 LDAPS。您可以使用Amazon Web Services Management Console方法或Amazon CLI方法。

> **Note**
>
> 客户端 LDAPS 是的区域性功能AmazonMicrosoft AD 如果您将多区域复制 (p. 54)，则必须在每个区域分别应用以下程序。有关更多信息，请参阅 全球与区域功能 (p. 54)。

主题

- 第 1 步：在中注册证书Amazon Directory Service (p. 34)
- 第 2 步：检查注册状态 (p. 34)
- 第 3 步：启用客户端 LDAPS (p. 35)
- 第 4 步：检查 LDAPS 状态 (p. 35)

第 1 步：在中注册证书Amazon Directory Service

使用下列方法之一在 Amazon Directory Service 中注册证书。

方法 1：在中注册您的证书Amazon Directory Service(Amazon Web Services Management Console)

1. 在Amazon Directory Service控制台导航窗格中，选择目录.
2. 选择目录的目录 ID 链接。
3. 在存储库的目录详细信息页面，请执行以下操作之一：
   - 如果您在下面显示多个区域多区域复制，选择要注册证书的区域，然后选择要注册证书的区域，然后选择网络与安全选项卡选项卡。有关更多信息，请参阅 主要与其他地区 (p. 55)。
   - 如果没有在下显示的任何区域多区域复制，选择网络与安全选项卡选项卡。
4. 在 Client-side LDAPS (客户端 LDAPS) 部分中，选择 Actions (操作) 菜单，然后选择 Register certificate (注册证书)。
5. 在 Register a CA certificate (注册 CA 证书) 对话框中，选择 Browse (浏览)，然后选择证书并选择 Open (打开)。
6. 选择 Register certificate (注册证书)。

方法 2：在中注册您的证书Amazon Directory Service(Amazon CLI)

- 运行以下命令。对于证书数据，请指向 CA 证书文件的位置。响应中将会提供证书 ID。

```
aws ds register-certificate --directory-id your_directory_id --certificate-data
 file://your_file_path
```

第 2 步：检查注册状态

要查看证书注册的状态或已注册证书的列表，请使用以下任一方法。

方法 1：要在中检查证书注册状态Amazon Directory Service(Amazon Web Services Management Console)

1. 转至客户端 LDAPS的部分目录详细信息页.
2. 查看 Registration status (注册状态) 列下显示的当前证书注册状态。当注册状态值更改为 Registered (已注册) 时，您的证书已成功注册。

方法 2：要在中检查证书注册状态Amazon Directory Service(Amazon CLI)

- 运行以下命令。如果状态值返回 `Registered`，则表示您的证书已成功注册。

```
aws ds list-certificates --directory-id your_directory_id
```

第 3 步：启用客户端 LDAPS

使用者，使用者Amazon Directory Service.

> Note
>
> 您必须已成功注册至少一个证书，然后才能启用客户端 LDAPS。

方法 1：在中启用客户端 LDAPS (Amazon Directory Service(Amazon Web Services Management Console)

1. 转至客户端 LDAPS的部分目录详细信息页.
2. 请选择 Enable。如果此选项不可用，请验证有效证书是否已成功注册，然后重试。
3. 在 Enable client-side LDAPS (启用客户端 LDAPS) 对话框中，选择 Enable (启用)。

方法 2：在中启用客户端 LDAPS (Amazon Directory Service(Amazon CLI)

- 运行以下命令。

```
aws ds enable-ldaps --directory-id your_directory_id --type Client
```

第 4 步：检查 LDAPS 状态

使用以下方法之一检查中的 LDAPS 状态Amazon Directory Service.

方法 1：在中检查 LDAPS 状态Amazon Directory Service(Amazon Web Services Management Console)

1. 转至客户端 LDAPS的部分目录详细信息页.
2. 如果状态值显示为 Enabled (启用)，则 LDAPS 已成功配置。

方法 2：在中检查 LDAPS 状态Amazon Directory Service(Amazon CLI)

- 运行以下命令。如果状态值返回 `Enabled`，则 LDAPS 已成功配置。

```
aws ds describe-ldaps-settings --directory-id your_directory_id
```

管理客户端 LDAPS

使用这些命令可管理 LDAPS 配置。

您可以使用两种不同的方法来管理客户端 LDAPS 设置。您可以使用Amazon Web Services Management Console方法或Amazon CLI方法。

查看证书详细信息

使用下列方法之一查看证书设置为何时过期。

方法 1：要在中查看证书详细信息Amazon Directory Service(Amazon Web Services Management Console)

1. 在Amazon Directory Service控制台导航窗格中，选择目录.
2. 选择目录的目录 ID 链接。

3. 在存储库的目录详细信息页面上，请执行以下操作之一：
   - 如果您在下面显示多个区域多区域复制，选择要查看证书的区域，然后选择要查看证书的区域，然后选择网络与安全选项卡选项卡。有关更多信息，请参阅 主要与其他地区 (p. 55)。
   - 如果没有在下显示的任何区域多区域复制，选择网络与安全选项卡选项卡。
4. 在 Client-side LDAPS (客户端 LDAPS) 部分的 CA certificates (CA 证书) 下，将显示有关证书的信息。

方法 2：在中查看证书详细信息Amazon Directory Service(Amazon CLI)

- 运行以下命令。对于证书 ID，请使用由 `register-certificate` 或 `list-certificates` 返回的标识符。

```
aws ds describe-certificate --directory-id your_directory_id --certificate-
id your_cert_id
```

取消注册证书

使用下列方法之一取消注册证书。

> Note
>
> 如果只注册了一个证书，则必须先禁用 LDAPS，然后才能取消注册证书。

方法 1：取消注册证书Amazon Directory Service(Amazon Web Services Management Console)

1. 在Amazon Directory Service控制台导航窗格中，选择目录.
2. 选择目录的目录 ID 链接。
3. 在存储库的目录详细信息页面上，请执行以下操作之一：
   - 如果您在下面显示多个区域多区域复制，选择要取消注册证书的区域，然后选择要取消注册证书的区域，然后选择网络与安全选项卡选项卡。有关更多信息，请参阅 主要与其他地区 (p. 55)。
   - 如果没有在下显示的任何区域多区域复制，选择网络与安全选项卡选项卡。
4. 在 Client-side LDAPS (客户端 LDAPS) 部分中，选择 Actions (操作)，然后选择 Deregister certificate (取消注册证书)。
5. 在 Deregister a CA certificate (取消注册 CA 证书) 对话框中，选择 Deregister (取消注册)。

方法 2：取消注册证书Amazon Directory Service(Amazon CLI)

- 运行以下命令。对于证书 ID，请使用由 `register-certificate` 或 `list-certificates` 返回的标识符。

```
aws ds deregister-certificate --directory-id your_directory_id --certificate-
id your_cert_id
```

禁用客户端 LDAPS

使用下列方法之一禁用客户端 LDAPS。

方法 1：在中禁注册客户端 LDAPSAmazon Directory Service(Amazon Web Services Management Console)

1. 在Amazon Directory Service控制台导航窗格中，选择目录.

2. 选择目录的目录 ID 链接。
3. 在存储库的目录详细信息页面上，请执行以下操作之一：
   - 如果您在下面显示多个区域多区域复制，选择要禁注册客户端 LDAPS 的区域，然后选择要禁用的网络与安全选项卡选项卡。有关更多信息，请参阅 主要与其他地区 (p. 55)。
   - 如果没有在下显示的任何区域多区域复制，选择网络与安全选项卡选项卡。
4. 在 Client-side LDAPS (客户端 LDAPS) 部分中，选择 Disable (禁用)。
5. 在 Disable client-side LDAPS (禁用客户端 LDAPS) 对话框中，选择 Disable (禁用)。

方法 2：在中禁注册客户端 LDAPSAmazon Directory Service(Amazon CLI)

- 运行以下命令。

```
aws ds disable-ldaps --directory-id your_directory_id --type Client
```

管理合规性AmazonManaged Mic

您可以使用Amazon管理微软 AD 以支持你的 Active Directory 感知应用程序AmazonCloud，受以下合规性要求。但是，如果您使用 Simple AD，则您的应用程序将不符合合规性要求。

支持的合规性标准

AmazonManaged Microsoft AD 已通过以下标准的审计，有资格用作需要获得合规性认证的解决方案的一部分。

FedRAMP	AmazonManaged Microsoft AD Managed Microsoft AD Managed Microsoft AD Managed Microsoft AD Managed Managed Managed Microsoft AD Managed Microsoft AD 有关 FedRAMP 的更多信息，请参阅FedRAMP 合规性.
PCI Security Standards Council PARTICIPATING ORGANIZATION™	AmazonManaged Microsoft AD 具有服务提供商级别 1 的支付卡行业 (PCI) 数据安全标准 (DSS) 版本 3.2 合规性认证。使用的客户Amazon用于存储、处理或传输持卡人数据的产品和服务可以使用Amazon在管理自己的 PCI DSS 合规性认证时管理微软 AD。 有关 PCI DSS 的副本，包括如何请求 PCI DSS 的副本 AmazonPCI 合规Package，请参阅PCI DSS 级别. 重要的是，您必须在中配置精细的密码策略Amazon管理微软 AD 以符

	合 PCI DSS 版本 3.2 的标准。有关必须强制执行哪些策略的详细信息，请参阅以下标题为 “为您启用 PCI 合规性” 的部分AmazonMicrosoft AD 目录。
	Amazon扩大了其《Health 保险流通与责任法案》（HIPAA）合规性计划AmazonManaged Mictt AD符合 HIPAA 条件的服务. 如果您与之签订了商业伙伴协议 (BAA)Amazon，您可以使用 AmazonManaged Microsoft AD 可帮助您构建符合 HIPA 要求的应用程序。 Amazon 提供了一份以 HIPAA 为主题的白皮书，供想要了解如何利用 Amazon 处理和存储医疗信息详情的客户查阅。有关更多信息，请参阅 HIPAA 合规性。

责任共担

安全性（包括 HIPAA 和 PCI 合规性）是一项责任共担工作。重要的是要明白这一点AmazonMicrosoft AD 合规性托管状态不会自动应用于你在Amazon云。您需要确保以符合标准的方式使用 Amazon 服务。

有关所有种类的完整列表Amazon合规性计划AmazonManaged Managed MictAmazon合规性计划范围内的服务.

为您启用 PCI 合规性AmazonMicrosoft AD

为您启用 PCI 合规性Amazon托管 Microsoft AD 目录，必须按照提供的 PCI DSS 合规认证 (AOC) 和责任摘要文档中的规定配置精细的密码策略Amazon Artifact.

有关使用精细密码策略的更多信息，请参阅管理密码策略Amazon托管的 Microsoft AD (p. 25)。

增强您的Amazon托管的 Microsoft AD 网络安全配置

这些区域有：Amazon为Amazon对于为托管的 Microsoft AD 目录，为其配置了支持您的所有已知使用案例所需的最少入站网络端口数Amazon托管的 Microsoft AD 目录。有关预置的 Amazon 安全组的更多信息，请参阅创建的内容 (p. 10)。

为了进一步提高你的网络安全性Amazon您可以修改托管的 Microsoft AD 目录Amazon安全组基于下面列出的常见场景。

主题

- Amazon仅支持应用程序 (p. 38)
- Amazon仅有信任支持的应用程序 (p. 39)
- Amazon应用程序和原生活目录工作负载 (p. 41)
- Amazon应用程序和本机 Active Directory 工作负载支持，并 (p. 42)

Amazon仅支持应用程序

所有用户帐户仅在您的Amazon要与受支持一起使用的托管微软 ADAmazon应用程序，例如以下内容：

- Amazon Chime

- Amazon Connect
- Amazon QuickSight
- Amazon IAM Identity Center (successor to Amazon Single Sign-On)
- Amazon WorkDocs
- Amazon WorkMail
- Amazon Client VPN
- Amazon Web Services Management Console

您可以使用以下命令Amazon您的安全组配置，以阻止指向您的所有非必要通信Amazon托管的 Microsoft AD 域控制器。

Note

- 以下内容与此 Amazon 安全组配置不兼容：
  - Amazon EC2 实例
  - Amazon FSx
  - Amazon RDS for MySQL
  - Amazon RDS for Oracle
  - Amazon RDS for PostgreSQL
  - Amazon RDS for SQL Server
  - WorkSpaces
  - Active Directory 信任
  - 加入域的客户端或服务器

入站规则

无。

出站规则

无。

Amazon仅有信任支持的应用程序

所有用户帐户都在您的Amazon托管微软 AD 或受信任的 Active Directory 与受支持一起使用Amazon应用程序，例如以下内容：

- Amazon Chime
- Amazon Connect
- Amazon QuickSight
- Amazon IAM Identity Center (successor to Amazon Single Sign-On)
- Amazon WorkDocs
- Amazon WorkMail
- Amazon WorkSpaces
- Amazon Client VPN
- Amazon Web Services Management Console

您可以修改预置的Amazon您的安全组配置，以阻止指向您的所有非必要通信Amazon托管的 Microsoft AD 域控制器。

Note

- 以下内容与此 Amazon 安全组配置不兼容：
  - Amazon EC2 实例
  - Amazon FSx
  - Amazon RDS for MySQL
  - Amazon RDS for Oracle
  - Amazon RDS for PostgreSQL
  - Amazon RDS for SQL Server
  - WorkSpaces
  - Active Directory 信任
  - 加入域的客户端或服务器
- 此配置要求您确保“本地 CIDR”网络是安全的。
- TCP 445 仅用于创建信任，可在建立信任后删除。
- 仅当使用基于 SSL 的 LDAP 时，才需要 TCP 636。

入站规则

协议	端口范围	源	流量的类型	Active Directory 使用情况
TCP 和 UDP	53	本地 CIDR	DNS	用户和计算机身份验证、名称解析、信任
TCP 和 UDP	88	本地 CIDR	Kerberos	用户和计算机身份验证、林级信任
TCP 和 UDP	389	本地 CIDR	LDAP	目录、复制、用户和计算机身份验证组策略、信任
TCP 和 UDP	464	本地 CIDR	Kerberos 更改/设置密码	复制、用户和计算机身份验证、信任
TCP	445	本地 CIDR	SMB / CIFS	复制、用户和计算机身份验证、组策略信任
TCP	135	本地 CIDR	复制	RPC、EPM
TCP	636	本地 CIDR	LDAP SSL	目录、复制、用户和计算机身份验证组策略、信任
TCP	49152 - 65535	本地 CIDR	RPC	复制、用户和计算机身份验证、组策略、信任
TCP	3268 - 3269	本地 CIDR	LDAP GC 和 LDAP GC SSL	目录、复制、用户和计算机身份验证组策略、信任
UDP	123	本地 CIDR	Windows 时间	Windows 时间、信任

出站规则

协议	端口范围	源	流量的类型	Active Directory 使用情况
所有	所有	本地 CIDR	所有流量	

Amazon应用程序和原生活目录工作负载

用户帐户仅在您的Amazon要与受支持一起使用的托管微软 ADAmazon应用程序，例如以下内容：

- Amazon Chime
- Amazon Connect
- Amazon EC2 实例
- Amazon FSx
- Amazon QuickSight
- Amazon RDS for MySQL
- Amazon RDS for Oracle
- Amazon RDS for PostgreSQL
- Amazon RDS for SQL Server
- Amazon IAM Identity Center (successor to Amazon Single Sign-On)
- Amazon WorkDocs
- Amazon WorkMail
- WorkSpaces
- Amazon Client VPN
- Amazon Web Services Management Console

您可以修改预置的Amazon您的安全组配置，以阻止指向您的所有非必要通信Amazon托管的 Microsoft AD 域控制器。

Note

- 无法在您之间创建和维护 Active Directory 信任Amazon托管微软 AD 目录和本地域。
- 它要求您确保“客户端 CIDR”网络是安全的。
- 仅当使用基于 SSL 的 LDAP 时，才需要 TCP 636。
- 如果要通过此配置使用企业 CA，则需要创建出站规则“TCP, 443, CA CIDR”。

入站规则

协议	端口范围	源	流量的类型	Active Directory 使用情况
TCP 和 UDP	53	客户端 CIDR	DNS	用户和计算机身份验证、名称解析、信任
TCP 和 UDP	88	客户端 CIDR	Kerberos	用户和计算机身份验证、林级信任

协议	端口范围	源	流量的类型	Active Directory 使用情况
TCP 和 UDP	389	客户端 CIDR	LDAP	目录、复制、用户和计算机身份验证组策略、信任
TCP 和 UDP	445	客户端 CIDR	SMB / CIFS	复制、用户和计算机身份验证、组策略信任
TCP 和 UDP	464	客户端 CIDR	Kerberos 更改/设置密码	复制、用户和计算机身份验证、信任
TCP	135	客户端 CIDR	复制	RPC、EPM
TCP	636	客户端 CIDR	LDAP SSL	目录、复制、用户和计算机身份验证组策略、信任
TCP	49152 - 65535	客户端 CIDR	RPC	复制、用户和计算机身份验证、组策略、信任
TCP	3268 - 3269	客户端 CIDR	LDAP GC 和 LDAP GC SSL	目录、复制、用户和计算机身份验证组策略、信任
TCP	9389	客户端 CIDR	SOAP	AD DS Web 服务
UDP	123	客户端 CIDR	Windows 时间	Windows 时间、信任
UDP	138	客户端 CIDR	DFSN 和 NetLogon	DFS、组策略

出站规则

无。

Amazon应用程序和本机 Active Directory 工作负载支持，并

所有用户帐户都在您的Amazon托管微软 AD 或受信任的 Active Directory 与受支持一起使用Amazon应用程序，例如以下内容：

- Amazon Chime
- Amazon Connect
- Amazon EC2 实例
- Amazon FSx
- Amazon QuickSight
- Amazon RDS for MySQL
- Amazon RDS for Oracle
- Amazon RDS for PostgreSQL
- Amazon RDS for SQL Server
- Amazon IAM Identity Center (successor to Amazon Single Sign-On)
- Amazon WorkDocs

- Amazon WorkMail
- WorkSpaces
- Amazon Client VPN
- Amazon Web Services Management Console

您可以修改预置的Amazon您的安全组配置，以阻止指向您的所有非必要通信Amazon托管的 Microsoft AD 域控制器。

Note

- 它要求您确保“本地 CIDR”和“客户端 CIDR”网络是安全的。
- 带有“本地 CIDR” 的 TCP 445 仅用于创建信任，可在建立信任后删除。
- 带有“客户端 CIDR”的 TCP 445 应保持打开状态，因为它是组策略处理所必需的。
- 仅当使用基于 SSL 的 LDAP 时，才需要 TCP 636。
- 如果要通过此配置使用企业 CA，则需要创建出站规则“TCP, 443, CA CIDR”。

入站规则

协议	端口范围	源	流量的类型	Active Directory 使用情况
TCP 和 UDP	53	本地 CIDR	DNS	用户和计算机身份验证、名称解析、信任
TCP 和 UDP	88	本地 CIDR	Kerberos	用户和计算机身份验证、林级信任
TCP 和 UDP	389	本地 CIDR	LDAP	目录、复制、用户和计算机身份验证组策略、信任
TCP 和 UDP	464	本地 CIDR	Kerberos 更改/设置密码	复制、用户和计算机身份验证、信任
TCP	445	本地 CIDR	SMB / CIFS	复制、用户和计算机身份验证、组策略信任
TCP	135	本地 CIDR	复制	RPC、EPM
TCP	636	本地 CIDR	LDAP SSL	目录、复制、用户和计算机身份验证组策略、信任
TCP	49152 - 65535	本地 CIDR	RPC	复制、用户和计算机身份验证、组策略、信任
TCP	3268 - 3269	本地 CIDR	LDAP GC 和 LDAP GC SSL	目录、复制、用户和计算机身份验证组策略、信任
UDP	123	本地 CIDR	Windows 时间	Windows 时间、信任

协议	端口范围	源	流量的类型	Active Directory 使用情况
TCP 和 UDP	53	客户端 CIDR	DNS	用户和计算机身份验证、名称解析、信任
TCP 和 UDP	88	客户端 CIDR	Kerberos	用户和计算机身份验证、林级信任
TCP 和 UDP	389	客户端 CIDR	LDAP	目录、复制、用户和计算机身份验证组策略、信任
TCP 和 UDP	445	客户端 CIDR	SMB / CIFS	复制、用户和计算机身份验证、组策略信任
TCP 和 UDP	464	客户端 CIDR	Kerberos 更改/设置密码	复制、用户和计算机身份验证、信任
TCP	135	客户端 CIDR	复制	RPC、EPM
TCP	636	客户端 CIDR	LDAP SSL	目录、复制、用户和计算机身份验证组策略、信任
TCP	49152 - 65535	客户端 CIDR	RPC	复制、用户和计算机身份验证、组策略、信任
TCP	3268 - 3269	客户端 CIDR	LDAP GC 和 LDAP GC SSL	目录、复制、用户和计算机身份验证组策略、信任
TCP	9389	客户端 CIDR	SOAP	AD DS Web 服务
UDP	123	客户端 CIDR	Windows 时间	Windows 时间、信任
UDP	138	客户端 CIDR	DFSN 和 NetLogon	DFS、组策略

出站规则

协议	端口范围	源	流量的类型	Active Directory 使用情况
所有	所有	本地 CIDR	所有流量	

配置目录安全设置

您可以为自己配置精细的目录设置Amazon管理 Microsoft AD 以满足您的合规性和安全要求，而不会增加操作工作量。在目录设置中，您可以更新目录中使用的协议和密码的安全通道配置。例如，您可以灵活地禁用单个传统密码（例如 RC4 或 DES）和协议（例如 SSL 2.0/3.0 和 TLS 1.0/1.1）。Amazon然后，托管 Microsoft AD 会将配置部署到你目录中的所有域控制器，管理域控制器的重启，并在你横向扩展或

部署其他域控制器时保持此配置Amazon Web Services 区域. 有关所有可用设置，请参阅目录安全设置列表 (p. 45).

> **Note**
>
> 以下区域不支持配置目录安全设置：非洲（开普敦）、亚太地区（香港）、欧洲（米兰）、中东（巴林）、Amazon GovCloud （美国东部）、Amazon GovCloud （美国西部）、中国（北京）和中国（宁夏）。

编辑目录安全设置

您可以配置和编辑任何目录的设置。

编辑目录设置

1. 登录Amazon管理控制台，打开AmazonDirectory Service 控制台https://console.amazonaws.cn/directoryservicev2/.
2. 在 Directories 页面上，选择您的目录 ID。
3. 下面网络与安全，查找目录设置，然后选择编辑设置.
4. 中编辑设置，更改值查找要编辑的设置。编辑设置时，其状态从默认值到Ready (就绪). 如果您之前编辑过该设置，则其状态将从Updated到Ready (就绪). 然后，选择审核.
5. 中查看和更新设置，请参阅目录设置并确保新值全部正确。如果需要对设置进行任何其他更改，请选择编辑设置. 当你对自己的变更感到满意并准备好实施新价值时，选择更新设置. 然后，您将返回到目录 ID 页面。

   > **Note**
   >
   > 下面目录设置，您可以查看状态您更新的设置。在实现设置的同时，状态显示器正在更新. 显示设置时您无法编辑其他设置正在更新下状态. 这些区域有：状态显示器Updated如果您的编辑成功更新了设置。这些区域有：状态显示器已失败如果设置无法通过您的编辑进行更新。

目录安全设置失败

如果在设置更新期间出现错误，状态显示为已失败. 在 “失败” 状态下，设置不会更新为新值，原始值保持已实现状态。您可以重试更新这些设置或将它们恢复为以前的值。

要解决更新设置失败的问题

- 下面目录设置，选择解决设置失败的问题. 然后，执行以下操作之一：
  - 要将您的设置恢复到失败状态之前的原始值，请选择Revert 失败的设置. 然后，选择REVER在弹出式模式中。
  - 要重试更新您的目录设置，请选择重试失败的设置. 如果要在重试失败的更新之前对目录设置进行其他更改，请选择继续编辑. 开启查看并重试失败的更新，选择更新设置.

目录安全设置列表

以下列表显示了所有可用目录安全设置的类型、设置名称、API 名称、潜在值和设置描述。

类型	设置名称	API 名称	潜在价值	设置说明
安全通道：密码	AES 128/128	AES_128_128	启用、禁用	启用或禁用 AES 128/128 加密密码，以便在目录中的域控制器之

类型	设置名称	API 名称	潜在价值	设置说明
				间进行安全通道通信。
	DES 56/56	DES_56_56	启用、禁用	启用或禁用 DES 56/56 加密密码以实现目录中域控制器之间的安全信道通信。
	RC2 40/128	RC2_40_128	启用、禁用	启用或禁用 RC2 40/128 加密密码，用于目录中域控制器之间的安全信道通信。
	RC2 56/128	RC2_56_128	启用、禁用	启用或禁用 RC2 56/128 加密密码以实现目录中域控制器之间的安全通道通信。
	RC2 128/128	RC2_128_128	启用、禁用	启用或禁用 RC2 128/128 加密密码，以便在您的目录中的域控制器之间进行安全信道通信。
	RC4 40/128	RC4_40_128	启用、禁用	启用或禁用 RC4 40/128 加密密码，用于目录中域控制器之间的安全信道通信。
	RC4 56/128	RC4_56_128	启用、禁用	启用或禁用 RC4 56/128 加密密码以实现目录中域控制器之间的安全通道通信。
	RC4 64/128	RC4_64_128	启用、禁用	启用或禁用 RC4 64/128 加密密码以实现目录中域控制器之间的安全信道通信。
	RC4 128/128	RC4_128_128	启用、禁用	启用或禁用 RC4 128/128 加密密码，以便在您的目录中的域控制器之间进行安全通道通信。

类型	设置名称	API 名称	潜在价值	设置说明
	Triple DES 168/168	3DES_168_168	启用、禁用	启用或禁用 Triple DES 168/168 加密密码，用于目录中域控制器之间的安全通道通信。
安全通道：协议	PCT 1.0	PCT_1_0	启用、禁用	在目录中的域控制器上启用或禁用 PCT 1.0 协议进行安全信道通信（服务器和客户端）。
	SSL 2.0	SSL_2_0	启用、禁用	在目录中的域控制器上启用或禁用 SSL 2.0 协议进行安全信道通信（服务器和客户端）。
	SSL 3.0	SSL_3_0	启用、禁用	在目录中的域控制器上启用或禁用 SSL 3.0 协议进行安全信道通信（服务器和客户端）。
	TLS 1.0	TLS_1_0	启用、禁用	在目录中的域控制器上启用或禁用用于安全通道通信（服务器和客户端）的 TLS 1.0 协议。
	TLS 1.1	TLS_1_1	启用、禁用	在目录中的域控制器上启用或禁用用于安全通道通信（服务器和客户端）的 TLS 1.1 协议。

监控Amazon托管的 Microsoft AD

您可以监控您的Amazon通过以下方法托管 Microsoft AD 目录：

主题

- 了解您的目录状态 (p. 48)
- 配置目录状态通知 (p. 48)
- 审核Amazon托管的 Microsoft AD 目录日志 (p. 50)
- 启用日志转发 (p. 51)
- 使用性能指标监控域控制器 (p. 53)

了解您的目录状态

以下是目录的各种状态。

Active (处于活动状态)

该目录运行正常。Amazon Directory Service 未检测到您的目录存在任何问题。

创建

当前正在创建该目录。目录创建过程通常需要 20 到 45 分钟，但可能因系统负载而异。

Deleted (已删除)

已删除该目录。已释放该目录的所有资源。一旦目录进入此状态，便无法恢复。

Deleting (正在删除)

当前正在删除该目录。目录将保持此状态，直到被完全删除。一旦目录进入此状态，将无法取消删除操作，目录也无法恢复。

已失败

无法创建该目录。请删除此目录。如果此问题仍存在，请联系。Amazon Web Services SupportCenter.

Impaired (受损)

目录正在降级状态下运行。检测到一个或多个问题，可能有的目录操作未在完全有效地工作。目录处于此状态有多个可能的原因。这些原因包括正常的操作维护活动（如打补丁或 EC2 实例轮换）、其中一台域控制器上的某个应用程序临时成为热点，或者您对网络进行了更改（可能无意中破坏目录通信）。有关更多信息，请参阅故障排除AmazonMicrosoft Managed Managed Microsoft AD (p. 161)、排查 AD Connector (p. 205)、排查 Simple AD (p. 251)。对于与正常维护相关的问题，Amazon在 40 分钟内解决。如果在查看故障排除主题后，您的目录处于受损状态的时间超过 40 分钟，我们建议您联系。Amazon Web Services SupportCenter.

> **Important**
>
> 当目录处于受损状态时，请不要还原快照。解决受损问题极少需要快照还原。有关更多信息，请参阅 快照或恢复你的目录 (p. 118)。

Inoperable (不可操作)

该目录无法正常工作。所有目录终端节点都报告有问题。

Requested (已请求)

创建目录的请求当前正在等待处理。

RestoreFailed (还原失败)

从快照还原目录失败。请重试还原操作。如果这种情况继续存在，请尝试其他快照或联系。Amazon Web Services SupportCenter.

Restoring (还原)

当前正从自动或手动快照中还原目录。从快照还原通常需要几分钟时间，具体取决于快照中的目录数据大小。

有关更多信息，请参阅Simple AD 目录状态原因 (p. 252)。

配置目录状态通知

通过使用 Amazon Simple Notification Service (Amazon SNS)，您可以在目录状态发生变化时接收电子邮件或文本 (SMS) 消息。如果您的目录从 Active (活动) 状态变为受损或无法操作状态. 当目录恢复为“Active”状态时，您也会收到通知。

工作方式

Amazon SNS 使用 “主题” 来收集和分发消息。每个主题都有一个或多个订阅者，他们接收发布至该主题的消息。通过使用以下步骤，您可以添加Amazon Directory Service作为 Amazon SNS 主题的发布者。Amazon Directory Service 在检测到您的目录状态发生变化时，会向该主题发布一条消息，该消息随后发送给该主题的订阅者。

您可以关联多个目录作为单个主题的发布者。您还可以将目录状态消息添加到您之前在 Amazon SNS 中创建的主题。您可以对谁能够向主题发布内容和订阅主题进行详细的控制。有关 Amazon SNS 的完整信息，请参阅什么是 Amazon SNS？.

> **Note**
>
> 目录状态通知是Amazon托管的 Microsoft AD。如果您在使用多区域复制 (p. 54)，必须在每个地区单独应用以下程序。有关更多信息，请参阅 全球与区域功能 (p. 54)。

为您的目录启用 SNS 消息发送

1. 登录 Amazon Web Services Management Console，然后打开 Amazon Directory Service 控制台，网址为：https://console.aws.amazon.com/directoryservicev2/。
2. 在 Directories 页面上，选择您的目录 ID。
3. 在存储库的目录详细信息页面，执行以下操作之一：
   - 如果你在下面显示了多个地区多区域复制选择要在其中启用 SNS 消息的区域，然后选择维护选项卡。有关更多信息，请参阅 主要与其他地区 (p. 55)。
   - 如果您没有显示在下面的任何区域多区域复制，选择维护选项卡。
4. 在目录监控选择部分，选择操作选择，然后选择创建通知.
5. 在存储库的创建通知选择页面，选择选择通知类型选择，然后选择创建新通知. 或者，如果您已有一个现有 SNS 主题，您可以选择关联现有 SNS 主题将状态消息从此目录发送到该主题。

   > **Note**
   >
   > 如果选择创建新通知但之后使用与现有 SNS 主题相同的主题名称，Amazon SNS 不会创建新主题，只是向现有主题添加新的订阅信息。
   > 如果选择关联现有 SNS 主题对于，您只能选择与该目录位于同一区域的 SNS 主题。
6. 选择收件人类型然后输入Recipient联系人信息。如果您为 SMS 输入电话号码，请只使用数字。不包括破折号、空格或圆括号。
7. （可选）提供主题的名称和 SNS 显示名称。显示名称为最多 10 个字符的短名称，包含在来自该主题的所有 SMS 消息中。使用 SMS 选项时必需提供显示名称。

   > **Note**
   >
   > 如果您使用仅有DirectoryServiceFullAccess托管策略，主题名称必须以 “DirectoryMonitor” 开头。如果您想进一步自定义主题名称，您需要对 SNS 的额外权限。
8. 选择创建。

如果您要指定更多 SNS 订阅者，例如其他电子邮件地址、Amazon SQS 队列或Amazon Lambda您可通过 Amazon SNS 控制台执行此操作：https://console.aws.amazon.com/sns/v3/home.

从主题移除目录状态消息

1. 登录 Amazon Web Services Management Console，然后打开 Amazon Directory Service 控制台，网址为：https://console.aws.amazon.com/directoryservicev2/。
2. 在 Directories 页面上，选择您的目录 ID。
3. 在存储库的目录详细信息页面，执行以下操作之一：

- 如果你在下面显示了多个地区多区域复制选择要删除状态消息的区域，然后选择维护选项卡。有关更多信息，请参阅 主要与其他地区 (p. 55)。
- 如果您没有显示在下面的任何区域多区域复制，选择维护选项卡。

4. 在目录监控部分中，在列表中选择 SNS 主题名称，然后选择操作选择，然后选择Remove.
5. 选择 Remove。

这会移除您的目录的选定 SNS 主题发布者身份。如果您要删除整个主题，可通过以下位置的 Amazon SNS 控制台执行此操作：https://console.aws.amazon.com/sns/v3/home.

> **Note**
>
> 在使用 SNS 控制台删除 Amazon SNS 主题之前，您应确保目录没有向该主题发送状态消息。
> 如果您使用 SNS 控制台删除 Amazon SNS 主题，则 Directory Services 控制台中不会立即反映出此更改。直到目录下次向已删除的主题发布通知时，您才会获得通知，那时，您将在该目录的 Monitoring 选项卡上看到一个更新状态，指示无法找到该主题。
> 因此，为避免错过重要的目录状态消息，请在删除从接收消息的任何主题之前，Amazon Directory Service将您的目录与其他 Amazon SNS 主题关联。

审核Amazon托管的 Microsoft AD 目录日志

来自安全日志Amazon托管的 Microsoft AD 域控制器实例会存档一年时间。您也可以配置Amazon将域控制器日志近乎实时地转发到 Amazon CloudWatch Logs。有关更多信息，请参阅 启用日志转发 (p. 51)。

Amazon记录以下事件以确保合规性。

监控类别	策略设置	审核状态
账户登录	审核凭证验证	成功，失败
	审核其他账户登录事件	成功，失败
账户管理	审核计算机账户管理	成功，失败
	审核其他账户管理事件	成功，失败
	审核安全组管理	成功，失败
	审核用户账户管理	成功，失败
明细跟踪	审核 DPAPI 活动	成功，失败
	审核 PNP 活动	成功
	审核过程创建	成功，失败
DS 访问	审核目录服务访问	成功，失败
	审核目录服务更改	成功，失败
登录/注销	审核账户锁定	成功，失败
	审核注销	成功
	审核登录	成功，失败
	审核其他登录/注销事件	成功，失败

监控类别	策略设置	审核状态
	审核特殊登录	成功，失败
对象访问	审核其他对象访问事件	成功，失败
	审核可移除存储	成功，失败
	审核中央访问策略存放	成功，失败
策略更改	审核策略更改	成功，失败
	审核身份验证策略更改	成功，失败
	审核授权策略更改	成功，失败
	审核 MPSSVC 规则级别策略更改	成功
	审核其他策略更改事件	失败
特权使用	审核敏感特权使用	成功，失败
系统	审核 IPsec 驱动程序	成功，失败
	审核其他系统事件	成功，失败
	审核安全状态更改	成功，失败
	审核安全系统扩展	成功，失败
	审核系统完整性	成功，失败

启用日志转发

您可以使用Amazon Directory Service将域控制器安全事件日志转发到 Amazon CloudWatch Logs。这为目录中的安全事件提供了透明度，从而帮助您满足安全监控、审计和日志保留策略要求。

CloudWatch Logs 还可将这些事件转发到其他事件Amazon账户，Amazon服务或第三方应用程序。这样一来，您可以更加轻松地集中监控和配置提醒，从而能近乎实时地检测并主动响应异常活动。

启用后，您可以使用 CloudWatch Logs 控制台从启用此服务时指定的日志组中检索数据。此日志组将包含您的域控制器中的安全日志。

有关日志组以及如何读取日志组数据的更多信息，请参阅使用日志组和日志流中的Amazon CloudWatch Logs 用户指南.

> **Note**
>
> 日志转发是一项区域性功能Amazon托管的 Microsoft AD。如果您将多区域复制 (p. 54)，必须在每个地区单独应用以下程序。有关更多信息，请参阅 全球与区域功能 (p. 54)。

启用日志转发

1. 在 Amazon Directory Service 控制台导航窗格中，选择 Directories (目录)。
2. 选择的目录 ID。Amazon要共享的托管微软 AD 目录。
3. 在存储库的目录详细信息页面上，执行以下操作之一：
   - 如果你在下面显示了多个地区多区域复制选择要在其中启用日志转发的区域，然后选择联网和安全选项卡。有关更多信息，请参阅 主要与其他地区 (p. 55)。

- 如果您在下没有显示任何区域多区域复制，选择联网和安全选项卡。

4. 在 Log forwarding (日志转发) 部分中，选择 Enable (启用)。
5. 在 Enable log forwarding to CloudWatch (启用到 CloudWatch 的日志转发) 对话框中，选择以下任一选项：
   a. Select创建新的 CloudWatch 日志组，在CloudWatch 日志组名中，指定您可在 CloudWatch Logs 中引用的名称。
   b. 选择 Choose an existing CloudWatch log group (选择现有 CloudWatch 日志组)，然后在 Existing CloudWatch log groups (现有 CloudWatch 日志组) 下，从菜单中选择日志组。
6. 查看定价信息和链接，然后选择 Enable (启用)。

禁用日志转发

1. 在 Amazon Directory Service 控制台导航窗格中，选择 Directories (目录)。
2. 选择的目录 ID。Amazon要共享的托管微软 AD 目录。
3. 在存储库的目录详细信息页面上，执行以下操作之一：
   - 如果你在下面显示了多个地区多区域复制选择要在其中禁用日志转发的区域，然后选择联网和安全选项卡。有关更多信息，请参阅 主要与其他地区 (p. 55)。
   - 如果您在下没有显示任何区域多区域复制，选择联网和安全选项卡。
4. 在 Log forwarding (日志转发) 部分中，选择 Disable (禁用)。
5. 阅读 Disable log forwarding (禁用日志转发) 对话框中的信息之后，选择 Disable (禁用)。

启用 CLI 启用日志转发

在您可以使用之前`ds create-log-subscription`命令中，您必须先创建 Amazon CloudWatch 日志组，然后创建 IAM 资源策略来向此组授予必需权限。要使用 CLI 启用日志转发，请完成以下所有步骤。

第 1 步：在 CloudWatch Logs 中创建日志组

创建一个将用于接收来自域控制器的安全日志的日志组。我们建议在名称前添加 `/aws/directoryservice/`，但这不是必需的。例如：

示例 CLI 命令

```
aws logs create-log-group --log-group-name '/aws/directoryservice/d-9876543210'
```

示例 POWERSHELL 命令

```
New-CWLLogGroup -LogGroupName '/aws/directoryservice/d-9876543210'
```

有关如何创建 CloudWatch Logs 组的说明，请参阅在 CloudWatch Logs 中创建日志组中的Amazon CloudWatch Logs 用户指南.

第 2 步：在 IAM 中创建 CloudWatch Logs 资源策略

授予 CloudWatch Logs 资源策略Amazon Directory Service在步骤 1 中创建的新日志组添加日志。您可以指定要限制的日志组的确切 ARNAmazon Directory Service对其他日志组的访问权限或使用通配符以包含所有日志组。以下示例策略使用通配符方法来标识以开头的所有日志组。`/aws/directoryservice/`(对于)Amazon您的目录所在的帐户将包括在内。

```
{
    "Version": "2012-10-17",
    "Statement": [
```

```
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "ds.amazonaws.com"
            },
            "Action": [
                "logs:CreateLogStream",
                "logs:PutLogEvents"
            ],
            "Resource": "arn:aws:logs:YOUR_REGION:YOUR_ACCOUNT_NUMBER:log-group:/aws/
directoryservice/*"
        }
    ]
}
```

您需要将此策略保存到您的本地工作站上的文本文件（例如，DSPolicy.json）中，因为您将需要通过 CLI 运行它。例如：

示例 CLI 命令

```
aws logs put-resource-policy --policy-name DSLogSubscription --policy-document
file://DSPolicy.json
```

示例 POWERSHELL 命令

```
$PolicyDocument = Get-Content .\DSPolicy.json -Raw

Write-CWLResourcePolicy -PolicyName DSLogSubscription -PolicyDocument
$PolicyDocument
```

第 3 步：创建Amazon Directory Service日志订阅

在此最终步骤中，您现在可以通过创建日志订阅来继续启用日志转发。例如：

示例 CLI 命令

```
aws ds create-log-subscription --directory-id 'd-9876543210' --log-group-name
'/aws/directoryservice/d-9876543210'
```

示例 POWERSHELL 命令

```
New-DSLogSubscription -DirectoryId 'd-9876543210' -LogGroupName '/aws/
directoryservice/d-9876543210'
```

使用性能指标监控域控制器

Amazon Directory Service与 Amazon CloudWatch 集成，以帮助您为目录中的每个域控制器提供重要的性能指标。这意味着您可以监控域控制器性能计数器，例如 CPU 和内存利用率。您还可以配置警报并启动自动操作以响应高利用率时期。例如，您可以为域控制器 CPU 使用率超过 70% 配置警报，然后创建 SNS 主题以便在发生这种情况时通知您。您可以使用此 SNS 主题启动自动化，例如AmazonLambda 函数，用于增加目录中的域控制器数量。

有关监控域控制器的更多信息，请参阅。使用 Amazon CloudWatch 指标来确定何时添加域控制器 (p. 134).

在 CloudWatch 中查找域控制器性能指标

在 CloudWatch 控制台中，给定服务的指标首先按服务的命名空间进行分组。您可以添加从属于该命名空间的指标筛选器。使用以下过程找到设置所需的正确命名空间和次级指标AmazonCloudWatch 中的 Microsoft AD 域控制器指标。

在 CloudWatch 控制台中查找域控制器指标

1. 访问 https://console.aws.amazon.com/cloudwatch/ 打开 CloudWatch 控制台。
2. 在导航窗格中，选择 Metrics (指标)。
3. 从指标列表中，选择Directory Service命名空间，然后从列表中选择AmazonMicrosoft 托管 AD指标。

有关如何使用 CloudWatch 控制台设置域控制器指标的说明，请参阅如何自动化Amazon基于利用率指标托管 Microsoft AD 扩展中的Amazon安全博客。

多区域复制

可以使用多区域复制来自动复制Amazon跨多个区域托管 Microsoft AD 目录数据。这种复制可以提高分散地理位置的用户和应用程序的性能。Amazon托管 Microsoft AD 使用本机 Active Directory 复制将目录的数据安全地复制到新区域。

仅支持多区域复制企业版的Amazon托管的 Microsoft AD。您可以在大多数地区使用自动化多区域复制Amazon可以使用托管的 Microsoft AD。以下区域不可用此功能。

- 非洲（开普敦）(af-south-1)
- 亚太地区（香港）ap-east-1
- 欧洲（米兰）(eu-south-1)
- 中东（巴林）me-south-1

优点

使用中的多区域复制Amazon托管 Microsoft AD、广告感知应用程序在本地使用该目录实现高性能，并使用多区域功能来实现弹性。您可以将多区域复制用于广告感知应用程序，例如 SharePoint 和 SQL Server 以及Amazon服务，例如 Amazon RDS 版 SQL Server 和 FSx for Windows File Server。以下是多区域复制的额外好处。

- 它可以让你部署一个Amazon快速地在全球范围内管理 Microsoft AD 实例，消除了自我管理全球 AD 基础设施的繁重工作。
- 它使您可以更轻松、更具成本效益地在多个中部署和管理 Windows 和 Linux 工作负载Amazon地区。自动化的多区域复制可实现全球 AD 感知应用程序的最佳性能。Windows 或 Linux 实例中部署的所有应用程序都使用Amazon在该地区本地托管 Microsoft AD，可以对来自尽可能最近的区域的用户请求做出响应。
- 它提供了多区域弹性。部署在高可用性Amazon托管基础设施，Amazon托管 Microsoft AD 处理所有地区的自动软件更新、监控、恢复和底层 AD 基础设施的安全性。这使您可以专注于构建应用程序。

主题

- 全球与区域功能 (p. 54)
- 主要与其他地区 (p. 55)
- 多区域复制的工作原理 (p. 55)
- 添加复制的区域 (p. 57)
- 删除复制区域 (p. 58)

全球与区域功能

当你添加Amazon使用多区域复制到目录的区域，Amazon Directory Service增强了所有功能的范围，使它们变得具有区域意识。这些功能列在详细信息页面的各个选项卡上，当您在Amazon Directory Service控制台。这意味着所有功能都将根据您在多区域复制控制台的部分。您对每个区域中的要素所做的更改可以在全局应用或按区域应用。

全球功能

同时，您对全局要素所做的任何更改主 区域 (p. 55)选定该选项将应用于所有区域。

您可以识别在目录详细信息页面因为它们显示应用于所有复制的区域在他们旁边。或者，如果在列表中选择了另一个不是主要区域的区域，则可以识别全局使用的要素，因为它们显示继承自主区域.

区域功能

对于中的功能所做的任何更改其他区域 (p. 55)将仅适用于该地区。

您可以在目录详细信息页面因为他们确实不显示应用于所有复制的区域要么继承自主区域在他们旁边。

主要与其他地区

使用多区域复制，Amazon托管 Microsoft AD 使用以下两种类型的区域来区分应如何在你的目录中应用全局或区域性功能。

主 区域

首次创建目录的初始区域称为主要的区域。您只能执行全局目录级别的操作，例如创建 Active Directory 信任和从主区域更新 AD 架构。

主要区域始终可以被标识为显示在列表顶部的第一个区域多区域复制部分，然后以-主要. 例如，主要美国东部（弗吉尼亚北部）.

您对此所做的任何更改全球功能 (p. 55)选择主区域时，将应用于所有地区。

您只能在选择主区域的情况下添加区域。有关更多信息，请参阅 添加复制的区域 (p. 57)。

其他区域

将任何添加到目录的区域都称为额外地区。

尽管所有区域都可以在全球范围内管理某些功能，但其他功能则按区域单独管理 要管理其他区域（非主要区域）的功能，您必须首先从多区域复制部分目录详细信息页. 然后，您可以继续管理该功能。

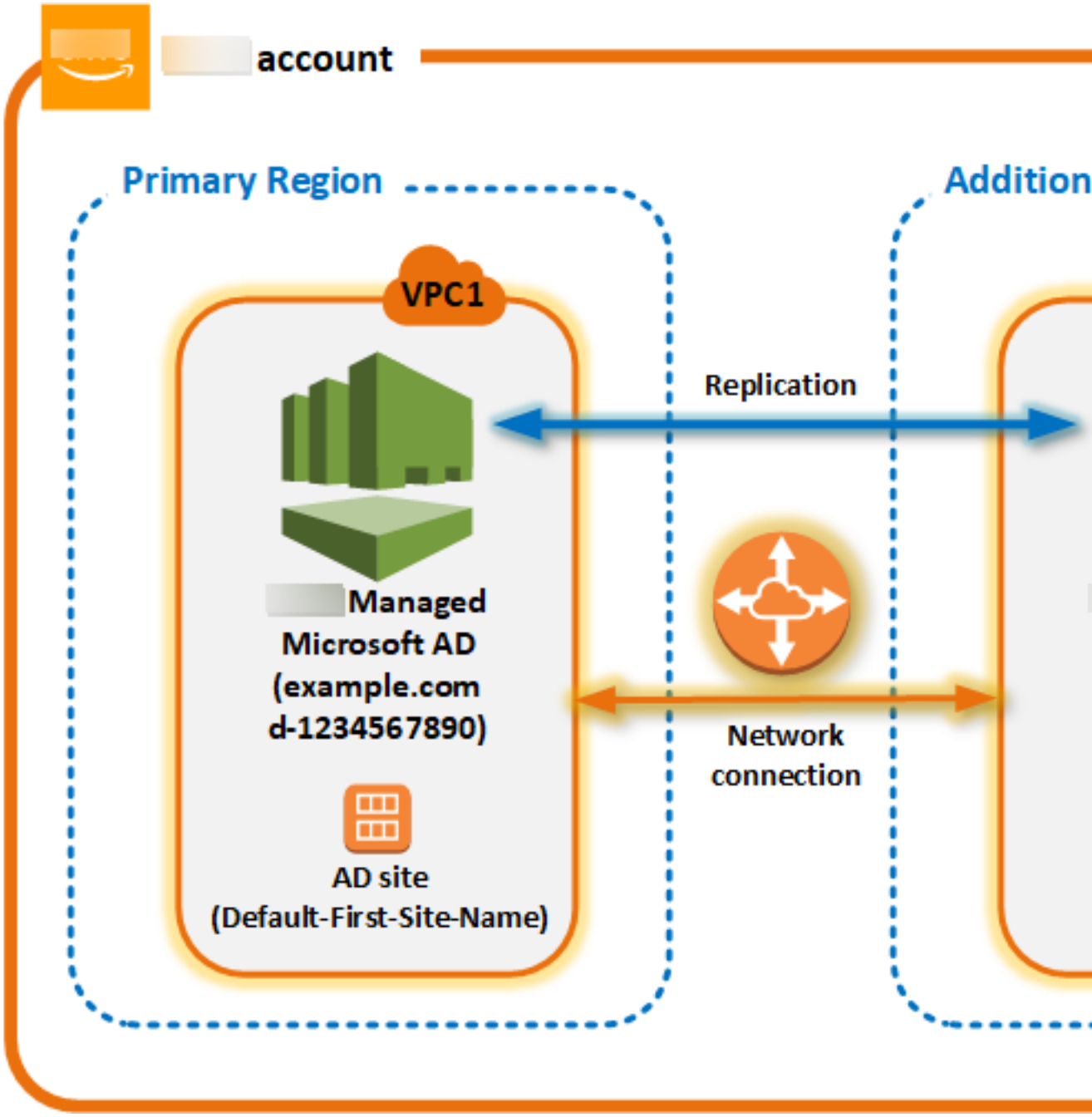
您对此所做的任何更改区域功能 (p. 55)而选择了另一个地区，将仅应用于该区域。

多区域复制的工作原理

使用多区域复制功能，Amazon托管微软 AD 消除了管理全球 AD 基础设施所带来的无差别繁重的工作。配置后，Amazon跨多个复制所有客户目录数据，包括用户、组、组策略和架构Amazon地区。

添加新区域后，将自动执行以下操作，如图所示：

- Amazon托管 Microsoft AD 在选定的 VPC 中创建两个域控制器，然后将它们部署到同一个区域中的新区域 Amazonaccount. 你的目录标识符 (`directory_id`) 在所有区域中保持不变。如果需要，您可以稍后添加额外的域控制器。
- Amazon托管 Microsoft AD 配置主区域和新区域之间的网络连接。
- Amazon托管微软 AD 创建了一个新的 Active Directory 站点，并给它与该地区相同的名称，例如 us-east-1。您也可以稍后使用 Active Directory 站点和服务工具对其进行重命名。
- Amazon托管 Microsoft AD 将所有 AD 对象和配置复制到新区域，包括用户、组、组策略、AD 信任、组织单位和 AD 架构。活动目录站点链接配置为使用更通知. 启用站点之间的更改通知后，更改将以与源站点内传播的频率相同，包括需要紧急复制的更改传播到远程站点。
- 如果这是您添加的第一个区域，Amazon托管微软 AD 使所有功能都能感知多区域。有关更多信息，请参阅 全球与区域功能 (p. 54)。



Active Directory 站点

多区域复制支持多个 Active Directory 站点（每个区域一个 AD 站点）。当添加新区域时，该区域的名称与区域相同，例如 us-east-1。您也可以稍后使用 Active Directory 站点和服务对其进行重命名。

Amazon 服务

AmazonAmazon RDS for SQL Server 和 Amazon FSx 之类的服务会连接到全局目录的本地实例。这允许您的用户登录一次在中运行的 AD 感知应用程序Amazon以及Amazon任何服务，如 Amazon RDS for SQL ServerAmazon区域。为此，用户需要从Amazon托管 Microsoft AD 或本地 Active Directory 当你信任Amazon托管的 Microsoft AD。

您可以使用以下命令Amazon具有多区域复制功能的服务。

- Amazon EC2
- FSx for Windows File Server
- Amazon RDS for SQL Server
- Amazon RDS for Oracle
- Amazon RDS for MySQL
- Amazon RDS for PostgreSQL
- Amazon RDS for MariaDB
- MySQL 的 Amazon Aurora
- PostgreSQL 的 Amazon Aurora

故障转移

如果一个区域中的所有域控制器都关闭了，Amazon托管 Microsoft AD 会恢复域控制器并自动复制目录数据。同时，其他地区的域控制器保持正常运行。

添加复制的区域

当您使用多区域复制 (p. 54)功能，Amazon托管微软 AD 在选定的Amazon区域、Amazon Virtual Private Cloud (VPC) 和子网。Amazon托管 Microsoft AD 还创建相关安全组，使 Windows 工作负载能够连接到新区域中的目录。它还使用相同的方法创建这些资源Amazon您的目录已部署的帐户。您可以通过选择区域、指定 VPC 并提供新区域的配置来完成此操作。

仅支持多区域复制企业版的Amazon托管的 Microsoft AD。

先决条件

在继续执行添加新复制区域的步骤之前，我们建议您首先查看以下先决条件任务。

- 验证您是否满足所需的设备Amazon Identity and Access Management(IAM) 权限、Amazon VPC 设置以及要将目录复制到的新区域中的子网设置。
- 如果您想要在中使用现有本地 Active Directory 凭据访问和管理 AD 感知型工作负载Amazon，你必须在之间创建 AD 信任Amazon托管的 Microsoft AD 和本地 AD 基础设施。有关信托的更多信息，请参阅Connect 到您的现有 AD 基础设施 (p. 96).

添加区域

使用以下过程为您的Amazon托管的 Microsoft AD 目录。

添加复制的区域

1. 在 Amazon Directory Service 控制台导航窗格中，选择 Directories (目录)。
2. 在 Directories 页面上，选择您的目录 ID。
3. 在存储库的目录详细信息页面，下多区域复制，选择Primary从列表中选择区域，然后选择添加区域.

   Note

   只能添加区域，而Primary已选定区域。有关更多信息，请参阅 主 区域 (p. 55)。
4. 在存储库的添加区域页面，下区域从列表中选择要添加的区域。
5. 根据VPC中，选择要用于该区域的 VPC。

   Note

   无类域间路由 (CIDR) 不得与另一区域中该目录所使用的 VPC 重叠。

6. 根据Subnets中，选择要用于该区域的子网。
7. 查看下面的信息定价，然后选择Add.
8. 何时Amazon托管 Microsoft AD 完成域控制器部署过程，区域将显示处于活动状态状态。现在，您可以根据需要更新此区域。

后续步骤

在添加新区域后，您应考虑执行以下后续步骤：

- 根据需要将其他域控制器（最多 20 个）部署到新区域。默认情况下，当您添加新区域时，域控制器的数量为 2，这是实现容错和高可用性目的所需的最小数量。有关更多信息，请参阅 添加或删除额外的域控制器 (p. 134)。
- 与更多共享您的目录Amazon每个地区的账户。目录共享配置不会自动从主区域复制。有关更多信息，请参阅 共享您的目录 (p. 58)。
- 启用日志转发功能以使用亚马逊检索目录的安全日志 CloudWatch 来自新区域的日志。启用日志转发时，必须在复制目录的每个区域中提供日志组名称。有关更多信息，请参阅 启用日志转发 (p. 51)。
- 为新区域启用 Amazon Simple Notification Service (Amazon SNS) 监控，以跟踪每个区域的目录运行状况。有关更多信息，请参阅 配置目录状态通知 (p. 48)。

删除复制区域

为您删除区域，请按照以下过程操作：Amazon托管的 Microsoft AD 目录。在删除区域之前，请确保它没有以下任一内容：

- 附加到它的授权应用程序。
- 与之相关的共享目录。

删除复制的区域

1. 在 Amazon Directory Service 控制台导航窗格中，选择 Directories (目录)。
2. 在 Directories 页面上，选择您的目录 ID。
3. 在存储库的目录详细信息页面，下多区域复制选择删除地区.
4. 在删除地区对话框中，检查信息，然后输入区域名称以进行确认。然后选择 Delete（删除）。

   Note

   删除该区域时，您无法对其进行更新。

共享您的目录

Amazon与托管的 Microsoft AD 紧密集成Amazon Organizations允许跨多个进行无缝的目录共享Amazon账户。您可以将单个目录与相同组织中的其他可信 Amazon 账户分享，也可以将目录与组织外的其他 Amazon 账户分享。您也可以在 Amazon 账户目前不是组织的成员时共享目录。

Note

Amazon 会收取额外的目录共享费用。要了解更多信息，请参阅定价上的页面AmazonDirectory Service 网站。

目录共享使Amazon目录 Microsoft AD 是与多个账户和 VPC 中的 Amazon EC2 进行集成的更经济高效的方式。目录共享在所有中暂不可用Amazon地区AmazonManaged Microsoft AD已提供。

> **Note**
>
> 在Amazon使用中国（宁夏）区域，此功能仅在使用时可用AmazonSystems Manager(SSM) 可无缝加入您的 Amazon EC2 实例。

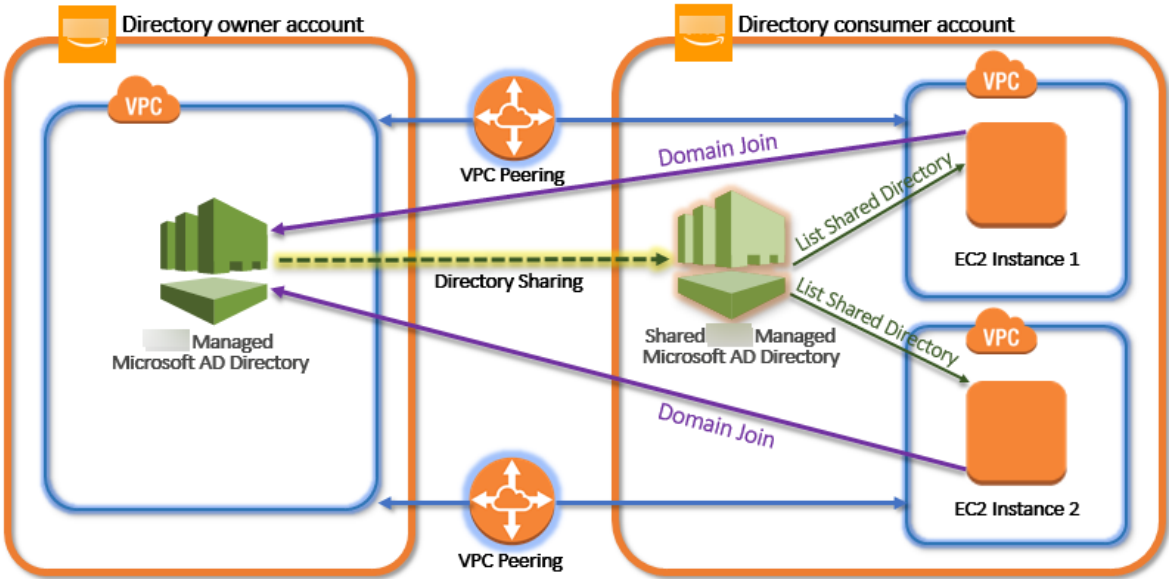
有关目录共享以及如何扩展覆盖范围的更多信息Amazon跨托管的 Microsoft AD 目录Amazon请参阅账户边界，请参阅以下主题。

主题

- 目录共享关键概念 (p. 59)
- 教程：共享您的Amazon用于无缝 EC2 域加入的托管微软 AD 目录 (p. 60)
- 取消共享您的目录 (p. 65)

目录共享关键概念

如果您熟悉以下主要概念，将能够更充分地利用目录共享功能。



目录拥有者账户

目录所有者是Amazon Web Services 账户在共享目录关系中拥有原始目录的持有者。此账户中的管理员通过指定哪些目录启动目录共享工作流。Amazon Web Services 账户与之共享他们的目录。目录所有者可以使用缩放并共享选项卡中给定目录的Amazon Directory Service控制台。

目录使用者账户

在共享目录关系中，目录使用者表示Amazon Web Services 账户目录拥有者与之共享目录。根据所用的共享方法，此账户中的管理员可能需要接受发送自目录所有者的邀请，然后才能开始使用共享目录。

目录共享流程在目录使用者账户中创建共享目录。此共享目录包含元数据，使得 EC2 实例可以无缝加入位于目录所有者账户内原始目录中的域。目录使用者账户中的每个共享目录具有唯一标识符（Shared directory ID (共享目录 ID)）。

共享方法

Amazon托管 Microsoft AD 提供了以下两种目录共享方法：

- Amazon Organizations— 此方法可以轻松地在您的组织中共享目录，因为您可以浏览并验证目录使用者账户。要使用此选项，您的组织必须有所有功能启用，目录必须位于组织管理账户中。此方法简化了您

的设置，因为它无需目录使用者账户接受您的目录共享请求。在控制台中，此方法称为与之共享此目录Amazon Web Services 账户在组织内.

- 握手— 此方法在您未使用时启用目录共享Amazon Organizations. 握手方法要求目录使用者账户接受目录共享请求。在控制台中，此方法称为与其他人共享此目录Amazon Web Services 账户.

网络连接

网络连接是跨使用目录共享关系的先决条件。Amazon Web Services 账户.Amazon支持许多连接 VPC 的解决方案，其中一些包括VPC 对等、中转网关, 和VPN. 要了解其用法，请参阅 教程：共享您的Amazon用于无缝 EC2 域加入的托管微软 AD 目录 (p. 60)。

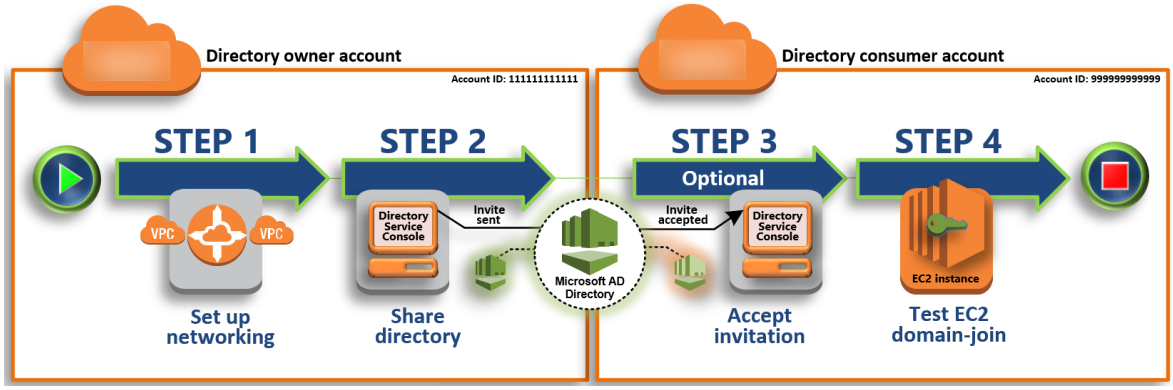
教程：共享您的Amazon用于无缝 EC2 域加入的托管微软 AD 目录

本教程介绍如何共享您的Amazon使用另一个托管微软 AD 目录（目录所有者帐户）Amazon Web Services 账户（目录使用者账户）。一旦完成网络先决条件，您将在两个目录之间共享目录。Amazon Web Services 账户. 然后，您将学习如何将 EC2 实例无缝加入目录使用者账户中的域。

我们建议您在开始学习本教程之前首先查看目录共享关键概念和使用案例内容。有关更多信息，请参阅 目录共享关键概念 (p. 59)。

共享目录的过程会有所不同，具体取决于您是否与另一个目录共享。Amazon Web Services 账户在相同的情况下Amazon组织或帐户不在Amazon组织。有关共享的工作方式的更多信息，请参阅共享方法 (p. 59)。

此工作流程具有四个基本步骤。



第 1 步：设置网络环境 (p. 61)

在目录拥有者账户中，您可以设置目录共享过程所需的所有网络先决条件。

第 2 步：共享您的目录 (p. 62)

使用目录拥有者管理员凭证登录后，您可以打开 Amazon Directory Service 控制台并启动共享目录工作流，该工作流会将邀请发送到目录使用者账户。

第 3 步：接受共享目录邀请（可选）(p. 63)

使用目录拥有者管理员凭证登录后，您可以打开 Amazon Directory Service 控制台并接受目录共享邀请。

第 4 步：测试将适用于 Windows Server 的 EC2 实例无缝加入到域中 (p. 63)

最后，作为目录拥有者管理员，您需要尝试将 EC2 实例加入您的域并验证它是否有效。

其他资源

- 使用案例：跨共享目录以将 Amazon EC2 实例无缝加入到域中Amazon Web Services 账户

- Amazon安全博客文章：如何将 Amazon EC2 实例从多个账户和 VPC 加入到单个账户和 VPC 中Amazon托管的 Microsoft AD 目录

第 1 步：设置网络环境

开始本教程中的步骤之前，必须先执行以下操作：

- 创建两个新的Amazon Web Services 账户用于在同一区域进行测试。创建时Amazon Web Services 账户对于，它会在每个账户中自动创建专用虚拟私有云 (VPC)。记下每个账户中的 VPC ID。您稍后会需要此信息。
- 使用此步骤中的过程在每个账户中的两个 VPC 之间创建 VPC 对等连接。

  Note

  虽然有很多方法可以连接目录拥有者和目录使用者账户 VPC，但本教程只使用 VPC 对等方法。有关其他 VPC 连接选项，请参阅网络连接 (p. 60)。

在目录拥有者和目录使用者账户之间配置 VPC 对等连接

您将创建的 VPC 对等连接位于目录使用者和目录拥有者 VPC 之间。请按照以下步骤配置 VPC 对等连接，以与目录使用者账户建立连接。通过此连接，您可以使用私有 IP 地址在两个 VPC 之间路由流量。

在目录拥有者和目录使用者账户之间创建 VPC 对等连接

1. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。确保以目录拥有者账户中具有管理员凭证的用户身份登录。
2. 在导航窗格中，选择 Peering Connections。然后选择 Create Peering Connection (创建对等连接)。
3. 配置以下信息：
   - 对等连接名称标签：在目录使用者账户中提供一个名称，用于清楚地标识与 VPC 的此连接。
   - VPC（请求者）：为目录拥有者账户选择 VPC ID。
   - 在 Select another VPC to peer with (选择要用作对等的另一个 VPC)，确保选中 My account (我的账户) 和 This region (此区域)。
   - VPC（接受者）：为目录使用者账户选择 VPC ID。
4. 选择 Create Peering Connection (创建对等连接)。在确认对话框中，选择 OK。

由于两个 VPC 位于同一个区域，因此发送 VPC 对等请求的目录拥有者账户的管理员也可以代表目录使用者账户接受对等请求。

代表目录使用者账户接受对等请求

1. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Peering Connections。
3. 选择挂起的 VPC 对等连接。（其状态为“Pending Acceptance (待接受)”。）依次选择 Actions (操作)、Accept Request (接受请求)。
4. 在确认对话框中，选择 Yes, Accept。在下一个确认对话框中，选择 Modify my route tables now (立即修改我的路由表) 直接转到路由表页面。

现在您的 VPC 对等连接已处于活动状态，您必须向目录拥有者账户中的 VPC 的路由表添加条目。这样做可以将流量定向到目录使用者账户中的 VPC。

向目录拥有者账户中的 VPC 路由表添加条目

1. 在路由表在 Amazon VPC 控制台的部分中，选择目录所有者 VPC 的路由表。

2. 选择路由选项卡上，选择编辑路线，然后选择添加路由.
3. 在 Destination (目标) 列中，输入目录使用者 VPC 的 CIDR 块。
4. 在 Target (目标) 列中，输入您之前在目录拥有者账户中创建的对等连接的 VPC 对等连接 ID（例如 **pcx-123456789abcde000**）。
5. 选择保存更改。

向目录使用者账户中的 VPC 路由表添加条目

1. 在路由表在 Amazon VPC 控制台的部分中，选择目录使用者 VPC 的路由表。
2. 选择路由选项卡上，选择编辑路线，然后选择添加路由.
3. 在 Destination (目标) 列中，输入目录拥有者 VPC 的 CIDR 块。
4. 在 Target (目标) 列中，键入您之前在目录使用者账户中创建的对等连接的 VPC 对等连接 ID（例如 **pcx-123456789abcde001**）。
5. 选择保存更改。

确保通过将 Active Directory 协议和端口添加到出站规则表，来配置目录使用者 VPC 的安全组以启用出站流量。有关更多信息，请参阅 。您的 VPC 的安全组和Amazon托管 Microsoft AD 先决条件.

下一步

第 2 步：共享您的目录 (p. 62)

第 2 步：共享您的目录

使用以下过程从目录拥有者账户中开始目录共享工作流。

> **Note**
>
> 目录共享是一项区域性功能Amazon托管的 Microsoft AD。如果您在使用多区域复制 (p. 54)，必须在每个地区单独应用以下程序。有关更多信息，请参阅 全球与区域功能 (p. 54)。

从目录拥有者账户共享您的目录

1. 登录到Amazon Web Services Management Console在目录拥有者账户中使用管理员凭证，然后打开Amazon Directory Service控制台在 https://console.aws.amazon.com/directoryservicev2/。
2. 在导航窗格中，选择 Directories。
3. 选择的目录 ID。Amazon要共享的托管微软 AD 目录。
4. 在存储库的目录详细信息页面上，执行以下操作之一：
   - 如果你有多个地区显示在下面多区域复制中，选择要共享目录的区域，然后选择扩展和共享选项卡。有关更多信息，请参阅 主要与其他地区 (p. 55)。
   - 如果您在下面没有显示任何区域多区域复制，选择扩展和共享选项卡。
5. 在 Shared directories (共享目录) 部分中，选择 Actions (操作)，然后选择 Create new shared directory (创建新共享目录)。
6. 在存储库的选择哪一个Amazon Web Services 账户与共享页面上，根据您的业务需求选择以下共享方法之一：
   a. 与之共享此目录Amazon Web Services 账户在组织内— 有了这个选项，你可以选择Amazon Web Services 账户你想从列表中共享你的目录，显示所有Amazon Web Services 账户在您的内部Amazon组织。在共享目录之前，必须使用 Amazon Directory Service 启用可信访问。有关更多信息，请参阅 。如何允许或禁止可信访问.

      > **Note**
      >
      > 要使用此选项，您的组织必须有所有功能已启用，您的目录必须在组织管理账户中。

i. UNDERAmazon Web Services 账户在组织中，选择Amazon Web Services 账户您要与之共享目录，然后单击Add.
ii. 查看定价详细信息，然后选择 Share (共享)。
iii. 继续执行本指南中的步骤 4 (p. 63)。由于所有Amazon Web Services 账户在同一组织中，您无需遵循步骤 3。

b. 与其他人共享此目录Amazon Web Services 账户-使用此选项，您可以与您的内部或外部的账户共享目录。Amazon组织。当您的目录不是成员时，您也可以使用此选项。Amazon组织，你想与另一个人共享Amazon Web Services 账户.

i. InAmazon Web Services 账户ID，输入所有Amazon Web Services 账户您要与之共享目录的ID，然后单击Add.
ii. In发送备注在另一个中键入发送给管理员的消息Amazon Web Services 账户.
iii. 查看定价详细信息，然后选择 Share (共享)。
iv. 继续执行步骤 3。

下一步

第 3 步：接受共享目录邀请（可选）(p. 63)

第 3 步：接受共享目录邀请（可选）

如果你选择了与其他人共享此目录Amazon Web Services 账户（握手方法）选项，则应使用此过程完成共享目录工作流。如果你选择了与之共享此目录Amazon Web Services 账户在组织内选项中，跳过此步骤并继续执行步骤 4。

接受共享目录邀请

1. 登录到Amazon Web Services Management Console使用目录使用者账户中的管理员凭证并打开Amazon Directory Service控制台在 https://console.aws.amazon.com/directoryservicev2/。
2. 在导航窗格中，选择 Directories shared with me (与我共享的目录)。
3. 在 Shared directory ID (共享目录 ID) 列中，选择 Pending acceptance (待接受) 状态下的目录 ID。
4. 在 Shared directory details (共享目录详细信息) 页面中，选择 Review (审核)。
5. 在 Pending shared directory invitation (待处理的共享目录邀请) 对话框中，查看注释、目录拥有者详细信息以及有关定价的信息。如果您同意，请选择 Accept (接受) 以开始使用该目录。

下一步

第 4 步：测试将适用于 Windows Server 的 EC2 实例无缝加入到域中 (p. 63)

第 4 步：测试将适用于 Windows Server 的 EC2 实例无缝加入到域中

您可以使用以下两种方法之一来测试无缝域加入。

方法1：使用 Amazon EC2 控制台测试域加入

在目录使用者账户中使用此步骤。

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 从导航栏的 Region (区域) 选择器中，选择与现有目录相同的 Region (区域)。
3. 选择 Launch Instance（启动实例）。
4. 在存储库的步骤 1页面上，选择Select获取适当的 AMI。
5. 在存储库的步骤 2页面上，选择合适的实例类型，然后选择后续：配置实例详细信息.
6. 在存储库的步骤 3页面上，执行以下操作，然后选择后续：Add Storage (下一步: 添加存储)：

1. 对于 Network，选择在其中创建了您的目录的 VPC。
2. 适用于子网中，选择 VPC 中的一个公有子网。您选择的子网必须将所有外部流量都路由到 Internet 网关。否则将无法远程连接到实例。
3. 对于 Auto-assign Public IP (自动分配公有 IP)，选择 Enable (启用)。

   有关公有 IP 地址的更多信息，请参阅Amazon EC2 实例 IP 寻址中的Windows 实例 Amazon EC2 用户指南.
4. 适用于域加入目录中，从列表中选择您的域。
5. 对于 IAM role (IAM 角色)，执行以下操作之一：

   选择具有Amazon托管策略AmazonSSMManagedInstanceCore和AmazonSSMDirectoryServiceAccess挂载到它。

   -或者-

   如果您尚未创建具有AmazonSSMManagedInstanceCore和AmazonSSMDirectoryServiceAccess附加到它的托管策略，请选择创建新的 IAM 角色链接，然后执行以下操作：

   a. 选择 Create role（创建角色）。
   b. 在 Select type of trusted entity (选择受信任实体的类型）下，选择 Amazon service (Amazon 服务)。
   c. UNDER选择此角色将使用的服务。在完整的服务列表中，选择EC2.
   d. UNDER选择您的使用案例，选择EC2，然后选择后续：Permissions (下一步：权限)。
   e. 在策略列表中，选择AmazonSSMManagedInstanceCore和AmazonSSMDirectoryServiceAccess政策。（要筛选列表，请键入**SSM**在搜索框中。）

      Note

      AmazonSSMDirectoryServiceAccess提供了将实例加入托管的 Active Directory 的权限 Amazon Directory Service. AmazonSSMManagedInstanceCore提供了使用 Systems Manager 服务所需的最低权限。有关使用这些权限创建角色的更多信息，以及有关可分配给 IAM 角色的其他权限和策略的信息，请参阅为 Systems Manager 创建 IAM 实例配置文件中的Amazon Systems Manager用户指南.
   f. 选择 Next:。标签。
   g. （可选）添加一个或多个标签键值对以组织、跟踪或控制该角色的访问，然后选择后续：审核。
   h. 对于角色名称，请输入新角色的名称，如 **EC2DomainJoin** 或所需的其他名称。
   i. （可选）对于角色描述，请输入描述。
   j. 选择 Create role（创建角色）。
   k. 返回到步骤 3页. 适用于IAM 角色中，选择旁边的刷新图标IAM 角色. 您的新角色应显示在菜单中。选择它并将此页面上的其余设置保留默认值，然后选择后续：添加存储.
7. 在两者上步骤 4和步骤 5页面上，保留默认设置或根据需要进行更改，然后选择下一步按钮。
8. 在存储库的步骤 6页面上，为实例选择已配置为允许从您的网络远程访问实例的安全组，然后选择审核并启动.
9. 在存储库的步骤 7页面上，选择启动中，选择一个 key pair，然后选择启动实例.

方法 2：使用AmazonSystems Manager 控制台

使用在目录使用者账户中使用此步骤。要完成此过程，您需要有关目录所有者账户的一些信息。

Note

请确保附加AmazonSSMManagedInstanceCore和AmazonSSMDirectoryServiceAccess启动此过程中的步骤之前，针对您的实例 IAM 角色权限的托管策略。有关可以附加到 Systems Manager

的 IAM 实例配置文件的其他策略的信息，请参阅为 Systems Manager 创建 IAM 实例配置文件中的Amazon Systems Manager用户指南有关托管策略的信息，请参阅Amazon托管策略中的IAM 用户指南.

1. 登录 Amazon Web Services Management Console 并通过以下网址打开 Amazon Systems Manager 控制台：https://console.amazonaws.cn/systems-manager/。
2. 在导航窗格中，选择Run Command。
3. 选择运行命令。
4. 在存储库的运行命令页面上，搜索`AWS-JoinDirectoryServiceDomain`. 当它显示在搜索结果中时，选择`AWS-JoinDirectoryServiceDomain`选项。
5. 向下滚动到 Command parameters (命令参数) 部分。您必须提供以下参数：
   - 对于 Directory Id (目录 ID)，输入 Amazon Directory Service 目录的名称。

     Note

     您可以在目录 ID返回到价值Amazon Directory Service控制台，选择与我共享的目录，选择你的目录，然后在共享目录详细信息部分。
   - 对于 Directory Name (目录名称)，输入目录的名称（对于目录所有者账户）。
   - 对于 DNS IP Addresses (DNS IP 地址)，输入目录中 DNS 服务器的 IP 地址（对于目录所有者账户）。

     Note

     您可以找到的值目录名和Dns IP 地址返回到Amazon Directory Service控制台，选择与我共享的目录，选择你的目录，然后查看在所有者目录信息部分。
6. 对于 Targets (目标)，选择您希望加入域的实例。
7. 保留窗体的剩余部分设置为其默认值，向下滚动页面，然后选择 Run (运行)。
8. 在导航窗格中，选择托管实例。
9. 通过查看列表中的实例来确认成功加入域的实例。如果 Association Status (关联状态) 显示 Success (成功)，则您的实例已成功加入域。

完成任一过程的步骤之后，您现在应该能够将您的 EC2 实例加入域。完成此操作后，您可以通过远程桌面协议 (RDP) 客户端使用您的凭证登录您的实例。Amazon托管 Microsoft AD 用户账户。

取消共享您的目录

可以使用以下过程可取消共享Amazon托管 Microsoft AD 目录。

取消共享您的目录

1. 在Amazon Directory Service控制台导航窗格，下Active DirectorySelect, 选择目录.
2. 选择的目录 IDAmazon要取消共享的托管 Microsoft AD 目录。
3. 在存储库的目录详细信息对于页面，请执行以下操作之一：
   - 如果你有多个地区显示在下面多区域复制选择要取消共享目录的区域，然后选择扩展和共享选项卡。有关更多信息，请参阅 主要与其他地区 (p. 55)。
   - 如果在下面没有显示任何区域多区域复制，选择扩展和共享选项卡。
4. 在 Shared directories (共享目录) 部分中，选择要取消共享的共享目录，选择 Actions (操作)，然后选择 Unshare (取消共享)。
5. 在 Unshare directory (取消共享目录) 对话框中，选择 Unshare (取消共享)。

其他资源

- 使用案例：共享您的目录以将 Amazon EC2 实例无缝加入到域Amazon账户
- Amazon安全博客文章：如何将 Amazon EC2 实例从多个账户和 VPC 加入单个账户和 VPCAmazonManaged Microsoft AD 目录
- 将您的 Amazon RDS 数据库实例加入到单个共享域

将 EC2 实例加入Amazon托管的 Microsoft AD 目录

当 EC2 实例启动时，您可以使用以下方式将其无缝加入到您的目录域中。Amazon Systems Manager. 有关更多信息，请参阅 。将 Windows 实例无缝地联接到Amazon Directory Service域中的适用于 Windows 实例的 Amazon EC2 用户指南.

如果需要手动将 EC2 实例加入到您的域，则必须在正确的区域和安全组或子网中启动实例，然后将实例加入到域中。

要能够远程连接到这些实例，必须具有从所连接的网络到实例的 IP 连接。在大多数情况下，这要求 Internet 网关连接到 VPC，并且实例具有公有 IP 地址。

主题

- 无缝地联接 Windows EC2 实例 (p. 66)
- 手动加入 Windows 实例 (p. 67)
- 将 Linux EC2 实例无缝地联接到您的Amazon托管的 Microsoft AD 目录 (p. 68)
- 手动加入 Linux 实例 (p. 73)
- 使用 Winbind 手动加入 Linux 实例 (p. 83)
- 为委派目录加入权限Amazon管理 Microsoft AD (p. 90)
- 创建 DHCP 选项集 (p. 92)

无缝地联接 Windows EC2 实例

此过程无缝地将 Windows EC2 实例联接到Amazon托管的 Microsoft AD 目录。如果您需要跨多个域执行无缝域加入Amazon账户，您可选择启用账户目录共享. 有关更多信息，请参阅 教程：共享您的Amazon用于无缝 EC2 域加入的托管微软 AD 目录 (p. 60)。

无缝地联接 Windows EC2 实例

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 从导航栏的区域选择器中，选择与现有目录相同的区域。
3. 选择 Launch Instance（启动实例）。
4. 在存储库的步骤 1选择页面，选择Select获取适当的 AMI。
5. 在存储库的步骤 2页面上，选择合适的实例类型，然后选择后续：配置实例详细信息.
6. 在存储库的步骤 3页面上，执行以下操作，然后选择：后续：Add Storage (下一步: 添加存储)：

   1. 对于 Network，选择在其中创建了您的目录的 VPC。
   2. 适用于子网，在 VPC 中选择一个公有子网。选择的子网必须将所有外部流量都路由到 Internet 网关。否则将无法远程连接到实例。
   3. 对于 Auto-assign Public IP (自动分配公有 IP)，选择 Enable (启用)。

      有关公有 IP 地址的更多信息，请参阅。Amazon EC2 实例 IP 寻址中的适用于 Windows 实例的 Amazon EC2 用户指南.
   4. 适用于域加入目录中，从列表中选择您的域。
   5. 对于 IAM role (IAM 角色)，执行以下操作之一：

选择 IAM 角色，该角色具有Amazon托管策略AmazonSSMManagedInstanceCore和AmazonSSMDirectoryServiceAccess挂载到它。

-或者-

如果您尚未创建具有AmazonSSMManagedInstanceCore和AmazonSSMDirectoryServiceAccess附加到它的托管策略，请选择创建新的 IAM 角色链接，然后执行以下操作：

a. 选择 Create role（创建角色）。
b. 在 Select type of trusted entity (选择受信任实体的类型）下，选择 Amazon service (Amazon 服务)。
c. UNDER选择此角色将使用的服务。在完整的服务列表中，选择EC2.
d. UNDER选择您的使用案例，选择EC2，然后选择后续：Permissions (下一步：权限)。
e. 在策略列表中，选择AmazonSSMManagedInstanceCore和AmazonSSMDirectoryServiceAccess政策。（要筛选列表，请键入**SSM**在搜索框中。）

   Note

   AmazonSSMDirectoryServiceAccess提供了将实例加入由托管的 Active Directory 的权限Amazon Directory Service. AmazonSSMManagedInstanceCore提供了使用 Systems Manager 服务所需的最低权限。有关使用这些权限创建角色的更多信息，以及有关可分配给 IAM 角色的其他权限和策略的信息，请参阅为 Systems Manager 创建 IAM 实例配置文件中的Amazon Systems Manager用户指南.

f. 选择 Next:。标签。
g. （可选）添加一个或多个标签键/值对以组织、跟踪或控制该角色的访问，然后选择后续：审核。
h. 对于角色名称，请输入新角色的名称，如 **EC2DomainJoin** 或所需的其他名称。
i. （可选）对于角色描述，请输入描述。
j. 选择 Create role（创建角色）。
k. 返回到步骤 3页. 适用于IAM 角色中，选择旁边的刷新图标IAM 角色. 您的新角色应显示在菜单中。选择它，将此页面上的其余设置保留默认值，然后选择后续：添加存储.

7. 在两个上步骤 4和步骤 5页面上，保留默认设置或根据需要进行更改，然后选择下一步按钮。
8. 在存储库的步骤 6页面上，为已配置为允许从您的网络远程访问实例的实例选择安全组，然后选择审核并启动.
9. 在存储库的步骤 7选择页面，选择启动中，选择一个 key pair，然后选择启动实例.

手动加入 Windows 实例

要将现有的 Amazon EC2 Windows 实例手动加入简单广告，或Amazon针对 Microsoft Directory Service tive Directory Directory Directory，该实例必须按照中指定的方式启动无缝地联接 Windows EC2 实例 (p. 66).

将 Windows 实例加入简单 AD，或Amazon托管的 Microsoft AD 目录

1. 使用任何远程桌面协议客户端连接到实例。
2. 在实例上打开 TCP/IPv4 属性对话框。

   a. 打开 Network Connections。

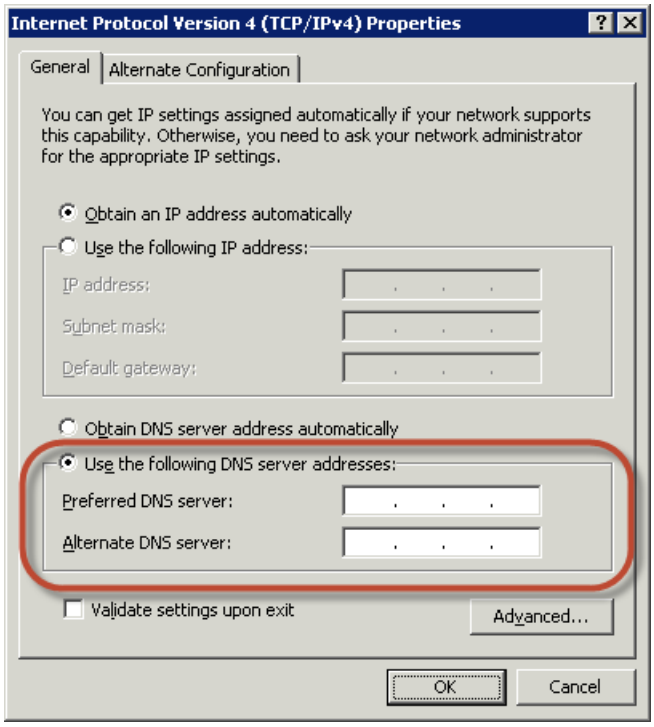
      Tip

      您可以在实例上从命令提示符运行以下命令，直接打开 Network Connections。

```
%SystemRoot%\system32\control.exe ncpa.cpl
```

b. 打开任何已启用网络连接的上下文菜单 (右键单击)，然后选择 Properties。
c. 在连接属性对话框中，打开 (双击) Internet Protocol Version 4。

3. Select使用以下 DNS 服务器地址：，更改首选 DNS 服务器和备用 DNS 服务器的 IP 地址的地址 Amazon Directory Service-提供 DNS 服务器，然后选择确定.



4. 打开实例的 System Properties 对话框，选择 Computer Name 选项卡，然后选择 Change。

   Tip

   您可以在实例上从命令提示符运行以下命令，打开 System Properties 对话框。

```
%SystemRoot%\system32\control.exe sysdm.cpl
```

5. 在成员选择字段，选择域，输入您的完全限定名称Amazon Directory Service目录，然后选择确定.
6. 当系统提示输入域管理员的名称和密码时，输入具有域加入权限的账户的用户名和密码。有关委托这些权限的更多信息，请参阅为委派目录加入权限Amazon管理 Microsoft AD (p. 90)。

   Note

   您可以输入完全限定的域名或 NetBios 名称，后跟反斜杠 (\)，然后是用户名。
   使用 时Amazon管理 Microsoft AD，用户名将为管理员. 例如，corp.example.com\admin 或 corp\admin。
   如果使用 Simple AD，用户名将为管理员. 例如，corp.example.com\ 管理员要么corp\ 管理员.

7. 收到欢迎加入域的消息之后，重新启动实例使更改生效。

现在实例已加入域，您可以远程登录该实例并安装实用工具来管理目录，如添加用户和组。

将 Linux EC2 实例无缝地联接到您的Amazon托管的 Microsoft AD 目录

此过程无缝地将 Linux EC2 实例联接到Amazon托管的 Microsoft AD 目录。如果您需要跨多个域执行无缝域加入Amazon账户，您可选择启用账户目录共享.

支持以下 Linux 实例分发版和版本：

- Amazon Linux AMI 2018.03.0
- Amazon Linux 2（64 位 x86）
- Red Hat Enterprise Linux 8 (HVM)（64 位 x86）
- Ubuntu Server 18.04 LTS 和 Ubuntu Server 16.04 LTS
- CentOS 7 x86-64
- SUSE Linux Enterprise Server 15 SP1

> **Note**
>
> Ubuntu 14 和红帽企业 Linux 7 之前的发行版不支持无缝域加入功能。

先决条件

在设置无缝域加入到 Linux EC2 实例之前，您需要完成本节中的步骤。

选择您的无缝域加入服务帐户

你可以将 Linux 计算机无缝连接到Amazon托管的 Active Directory 域。为此，必须使用具有创建计算机帐户权限的用户帐户才能将计算机加入域。虽然成员Amazon委派管理员或者其他组可能拥有足够权限将计算机加入到域，我们建议不要使用这些权限。作为最佳做法，我们建议您使用具有将计算机加入到域所需的最低权限的服务帐户。

要将具有加入计算机所需的最低权限的帐户委派到域，可以运行以下 PowerShell 命令。你必须从加入域的 Windows 计算机上运行这些命令安装 Active Directory 管理工具 (p. 93)安装。此外，您必须使用有权修改计算机 OU 或容器上的权限的帐户。PowerShell 命令设置权限，允许服务帐户在域的默认计算机容器中创建计算机对象。

```
$AccountName = 'awsSeamlessDomain'
# DO NOT modify anything below this comment.
# Getting Active Directory information.
Import-Module 'ActiveDirectory'
$Domain = Get-ADDomain -ErrorAction Stop
$BaseDn = $Domain.DistinguishedName
$ComputersContainer = $Domain.ComputersContainer
$SchemaNamingContext = Get-ADRootDSE | Select-Object -ExpandProperty 'schemaNamingContext'
[System.GUID]$ServicePrincipalNameGuid = (Get-ADObject -SearchBase $SchemaNamingContext -
Filter { lDAPDisplayName -eq 'Computer' } -Properties 'schemaIDGUID').schemaIDGUID
# Getting Service account Information.
$AccountProperties = Get-ADUser -Identity $AccountName
$AccountSid = New-Object -TypeName 'System.Security.Principal.SecurityIdentifier'
 $AccountProperties.SID.Value
# Getting ACL settings for the Computers container.
$ObjectAcl = Get-ACL -Path "AD:\$ComputersContainer"
# Setting ACL allowing the service account the ability to create child computer objects in
 the Computers container.
$AddAccessRule = New-Object -TypeName 'System.DirectoryServices.ActiveDirectoryAccessRule'
 $AccountSid, 'CreateChild', 'Allow', $ServicePrincipalNameGUID, 'All'
$ObjectAcl.AddAccessRule($AddAccessRule)
Set-ACL -AclObject $ObjectAcl -Path "AD:\$ComputersContainer"
```

如果您更喜欢使用图形用户界面 (GUI)，您可以使用中描述的手动过程。向您的服务账户委派权限 (p. 174).

创建密码以存储域服务帐户

您可以使用Amazon Secrets Manager以存储域服务帐户。

创建密码并存储域服务帐户信息

1. 登录到Amazon Web Services Management Console打开Amazon Secrets Manager在控制台https://console.aws.amazon.com/secretsmanager/.
2. 选择 Store a new secret (存储新密钥)。
3. 在 Store a new secret（存储新密钥）页面上，执行以下操作：
   a. 在 Select secret type (选择密钥类型) 下，选择 Other type of secrets (其他密钥类型)。
   b. UNDER在 secret (指定要存储在密钥中的键-值对) 下中，执行以下操作：
      i. 在第一个框中，输入**awsSeamlessDomainUsername**. 在同一行上，在下一个框中，输入您的服务帐户的用户名。例如，如果您之前使用 PowerShell 命令，则服务帐户名称将为awsSeamlessDomain.

         Note

         你必须输入**awsSeamlessDomainUsername**完全如此。确保没有任何前导或结束空格。否则，域加入将失败。
      ii. 选择添加行.
      iii. 在新行上，在第一个框中，输入**awsSeamlessDomainPassword**. 在同一行的下一个框中，输入服务帐号的密码。

         Note

         你必须输入**awsSeamlessDomainPassword**完全如此。确保没有任何前导或结束空格。否则，域加入将失败。
      iv. UNDER选择加密密钥，选择DefaultenCryptionKey从菜单中。当您选择此选项时，Secret Secrets Manager 始终会对密码进行加密，并免费提供给您。你也可以选择自己创建的密钥。
      v. 选择 Next (下一步)。
4. UNDER密钥名称中，使用以下格式输入包含目录 ID 的密钥名称：

```
aws/directory-services/d-xxxxxxxxx/seamless-domain-join
```

   这将用于检索应用程序中的秘密。

   Note

   你必须输入**aws/directory-services/*d-xxxxxxxxx*/seamless-domain-join**完全一样但是替换*d-xxxxxxxxxxxx*使用目录 ID。确保没有前导空格或结束空格。否则，域加入将失败。
5. 将其他所有内容设置为默认值，然后选择下一步.
6. UNDER配置自动轮换，选择禁用自动旋转选择，然后选择下一步.
7. 查看设置，然后选择存储保存您的更改。Secrets Manager 控制台将返回您的账户中的密钥列表，并且在列表中现在包含您的新密钥。
8. 从列表中选择你新创建的秘密名称，然后记下键 ARN值。您需要在下一节中使用该名称。

创建所需的 IAM 策略和角色

使用以下先决条件步骤创建自定义策略，允许对您的 Secret Secrets Manager 无缝域加入密钥（您之前创建的）进行只读访问，并创建新的 LinuxEC2DomainJoin IAM 角色。

创建秘 Secrets Manager IAM 读取策略

您可以使用 IAM 控制台创建一个策略，授予对 Secret Secrets Manager 钥的只读访问权限。

创建秘 Secrets Manager IAM 读取策略

1. 登录到Amazon Web Services Management Console作为有权创建 IAM 策略的用户。然后在以下网址打开 IAM 控制台https://console.aws.amazon.com/iam/.
2. 在导航窗格中，选择 Policies (策略)。
3. 选择创建策略。
4. 选择 JSON 选项卡，然后复制以下 JSON 策略文档中的文本。然后将其粘贴到JSON文本框。

   Note

   确保你更换`ResourceARN` 与您之前创建的密钥的实际 ARN 相同。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue",
                "secretsmanager:DescribeSecret"
            ],
            "Resource": [
                "arn:aws:secretsmanager:us-east-1:############:secret:aws/directory-
service/d-xxxxxxxxxx/seamless-domain-join-example"
            ]
        }
    ]
}
```

5. 完成后，选择 Review policy（查看策略）。策略验证程序将报告任何语法错误。有关更多信息，请参阅 。验证 IAM 策略.
6. 在存储库的审核策略页面中，输入策略名称，例如**`SM-Secret-Linux-DJ-d-xxxxxxxxxx-Read`**. 查看摘要部分以查看您的策略授予的权限。然后选择 。创建策略保存您的更改。新策略会显示在托管策略列表中，并且现在已准备好附加到身份。

   Note

   我们建议您为每个密码创建一个策略。这样做可以确保实例只能访问适当的机密，并最大限度地减少实例受到攻击时的影响。

创建 linuxEC2DOMAIN 加入角色

您可以使用 IAM 控制台创建用于域加入 Linux EC2 实例的角色。

创建 linuxEC2DomainJoin 角色

1. 登录到Amazon Web Services Management Console作为有权创建 IAM 策略的用户。然后在以下网址打开 IAM 控制台https://console.aws.amazon.com/iam/.
2. 在导航窗格中，选择 Roles（角色）。
3. 在内容窗格中，选择创建角色.
4. 在 Select type of trusted entity (选择受信任实体的类型）下，选择 Amazon service (Amazon 服务)。
5. UNDER选择使用案例选择EC2选择，然后选择后续：Permissions (下一步：权限)。
6. 适用于筛选策略中，执行以下操作：

   a. 输入 **`AmazonSSMManagedInstanceCore`**。然后，在列表中选中该项目的复选框。

   b. 输入 **`AmazonSSMDirectoryServiceAccess`**。然后，在列表中选中该项目的复选框。

c. Enter**SM-Secret-Linux-DJ-*d-xxxxxxxxxx*-Read**(或者您在上一过程中创建的策略名称)。然后在列表中选中该项目的复选框。

Note

AmazonSSMDirectoryServiceAccess 提供了将实例加入由托管的 Active Directory 的权限。Amazon Directory Service. AmazonSSMManagedInstanceCore 提供了使用Amazon Systems Manager服务。有关使用这些权限创建角色的更多信息，以及有关可分配给 IAM 角色的其他权限和策略的信息，请参阅为 Systems Manager 创建 IAM 实例配置文件中的Amazon Systems Manager用户指南.

7. 选择 Next:。标签。
8. （可选）添加一个或多个标签键/值对以组织、跟踪或控制该角色的访问。接下来，选择 Next (下一步)：审核。
9. 在旁边Role name (角色名称)，为新角色输入名称，例如**LinuxEC2DomainJoin**或者你喜欢的另一个名字。
10. （可选）对于角色描述，请输入描述。
11. 选择 Create role（创建角色）。

无缝地加入 Linux EC2 实例

现在您已经配置了所有必备任务，可以使用以下过程无缝加入 Linux EC2 实例。

无缝地加入 Linux EC2 实例

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 从导航栏的区域选择器中，选择与现有目录相同的区域。
3. 选择 Launch Instance（启动实例）。
4. 在存储库的步骤 1选择页面，选择Select获取合适的 Amazon 系统映像 (AMI)。

   Note

   使用的 AMI 必须有Amazon Systems Manager（SSM 代理）版本 2.161644.0 或更高版本。要通过从该 AMI 启动实例来检查 AMI 中已安装的 SSM Agent 版本，请参阅获取当前安装的 SSM Agent 版本. 如果你需要升级 SSM 代理程序，请参阅在适用于 Linux 的 EC2 实例上安装和配置 SSM Agent.
5. 在存储库的步骤 2页面上，选择合适的实例类型，然后选择后续：配置实例详细信息.
6. 在存储库的步骤 3页面上，执行以下操作，然后选择：后续：Add Storage (下一步: 添加存储)：
   a. 对于 Network，选择在其中创建了您的目录的 VPC。
   b. 适用于子网，在 VPC 中选择一个公有子网。选择的子网必须将所有外部流量都路由到 Internet 网关。否则将无法远程连接到实例。
   c. 对于 Auto-assign Public IP (自动分配公有 IP)，选择 Enable (启用)。有关公有 IP 地址的更多信息，请参阅。Amazon EC2 实例 IP 寻址中的适用于 Windows 实例的 Amazon EC2 用户指南.
   d. 适用于域加入目录中，从列表中选择您的域。
   e. 适用于IAM 角色(以上) 选择您之前在先决条件部分创建的 IAM 角色步骤 2: 创建 linuxEC2DOMAIN 加入角色.
7. 在两个上步骤 4和步骤 5页面，保留默认设置或根据需要进行更改。然后选择 。下一步在每个上。
8. 在存储库的步骤 6页面上，选择已配置为允许从您的网络远程访问实例的安全组。然后选择查看和启动。
9. 在存储库的步骤 7选择页面，选择启动，选择 key pair，然后选择启动实例.

> **Note**
>
> 如果您使用 SUSE Linux 执行无缝域加入，则需要重新启动才能进行身份验证。要从 Linux 终端重新启动 SUSE，请键入sudo reboot.

手动加入 Linux 实例

除了 Amazon EC2 Windows 实例外，您还可以将特定 Amazon EC2 Linux 实例加入您的AmazonDirectory Service in Microsoft Active Directory Directory。支持以下 Linux 实例分发版和版本：

- Amazon Linux AMI 2018.03.0
- Amazon Linux 2（64 位 x86）
- Red Hat Enterprise Linux 8 (HVM)（64 位 x86）
- Ubuntu Server 18.04 LTS 和 Ubuntu Server 16.04 LTS
- CentOS 7 x86-64
- SUSE Linux Enterprise Server 15 SP1

> **Note**
>
> 其他 Linux 分发版和版本可能会正常运行，但未经过测试。

将实例加入目录

在将 Amazon Linux、CentOS、红帽或 Ubuntu 实例加入您的目录之前，该实例必须按照中指定的方式启动。无缝地联接 Windows EC2 实例 (p. 66).

> **Important**
>
> 以下某些过程如果未正确执行，可能会使实例无法访问或不可用。因此，我们强烈建议在执行这些过程之前对实例创建备份或拍摄快照。

将 Linux 实例加入目录

使用以下选项卡之一对特定 Linux 实例执行步骤：

Amazon Linux

1. 使用任何 SSH 客户端连接到实例。
2. 配置 Linux 实例以使用的 DNS 服务器 IP 地址Amazon Directory Service-提供的 DNS 服务器。可以通过在附加到 VPC 的 DHCP 选项集中进行设置，或是通过在实例上手动设置，来执行此操作。如果您要手动设置，请参阅如何为私有 Amazon EC2 实例分配静态 DNS 服务器？中的Amazon知识中心获取有关为特定 Linux 发行版和版本设置持久 DNS 服务器的指导。
3. 确保您的 Amazon Linux-64 位实例为最新状态。

```
sudo yum -y update
```

4. 在 Linux 实例上安装所需的 Amazon Linux 程序包。

   > **Note**
   >
   > 其中一些程序包可能已安装。
   > 安装程序包时，可能会遇到几个弹出配置屏幕。通常可以将这些屏幕中的字段保留为空白。

   Amazon Linux 1

```
sudo yum -y install sssd realmd krb5-workstation
```

Amazon Linux 2

```
sudo yum -y install sssd realmd krb5-workstation samba-common-tools
```

Note

有关确定您正在使用的 Amazon Linux 版本的帮助，请参阅识别 Amazon Linux 映像中的适用于 Linux 实例的 Amazon EC2 用户指南.

5. 使用以下命令将实例加入目录。

```
sudo realm join -U join_account@example.com example.com --verbose
```

join_account@example.com

中的账户*example.com*具有域加入权限的域。在出现提示时输入账户的密码。有关委托这些权限的更多信息，请参阅为委派目录加入权限Amazon管理 Microsoft AD (p. 90)。

example.com

目录的完全限定 DNS 名称。

```
...
 * Successfully enrolled machine in realm
```

6. 设置 SSH 服务以允许进行密码身份验证。
   a. 在文本编辑器中打开 `/etc/ssh/sshd_config` 文件。

   ```
   sudo vi /etc/ssh/sshd_config
   ```

   b. 将 `PasswordAuthentication` 设置为 `yes`。

   ```
   PasswordAuthentication yes
   ```

   c. 重新启动 SSH 服务。

   ```
   sudo systemctl restart sshd.service
   ```

   或者：

   ```
   sudo service sshd restart
   ```

7. 重新启动实例之后，使用任何 SSH 客户端连接到它，然后添加Amazon通过执行以下步骤将委托管理员组到 sudoers 列表：
   a. 使用以下命令打开 `sudoers` 文件：

   ```
   sudo visudo
   ```

   b. 将以下内容添加到`sudoers`文件然后保存它。

   ```
   ## Add the "Amazon Delegated Administrators" group from the example.com domain.
   %Amazon\ Delegated\ Administrators@example.com ALL=(ALL:ALL) ALL
   ```

   (以上示例使用 “\<space>” 形成 Linux 空格字符。)

CentOS

1. 使用任何 SSH 客户端连接到实例。
2. 配置 Linux 实例以使用的 DNS 服务器 IP 地址Amazon Directory Service-提供的 DNS 服务器。可以通过在附加到 VPC 的 DHCP 选项集中进行设置，或是通过在实例上手动设置，来执行此操作。如果您要手动设置，请参阅如何为私有 Amazon EC2 实例分配静态 DNS 服务器？中的Amazon知识中心获取有关为特定 Linux 发行版和版本设置持久 DNS 服务器的指导。
3. 确保您的 CentOS 7 实例保持最新状态。

```
sudo yum -y update
```

4. 在 Linux 实例上安装所需的 CentOS 7 程序包。

   Note

   其中一些程序包可能已安装。
   安装程序包时，可能会遇到几个弹出配置屏幕。通常可以将这些屏幕中的字段保留为空白。

```
sudo yum -y install sssd realmd krb5-workstation samba-common-tools
```

5. 使用以下命令将实例加入目录。

```
sudo realm join -U join_account@example.com example.com --verbose
```

   join_account@example.com

   中的账户*example.com*具有域加入权限的域。在出现提示时输入账户的密码。有关委托这些权限的更多信息，请参阅为委派目录加入权限Amazon管理 Microsoft AD (p. 90)。

   example.com

   目录的完全限定 DNS 名称。

```
...
 * Successfully enrolled machine in realm
```

6. 设置 SSH 服务以允许进行密码身份验证。
   a. 在文本编辑器中打开 `/etc/ssh/sshd_config` 文件。

```
sudo vi /etc/ssh/sshd_config
```

   b. 将 `PasswordAuthentication` 设置为 `yes`。

```
PasswordAuthentication yes
```

   c. 重新启动 SSH 服务。

```
sudo systemctl restart sshd.service
```

   或者：

```
sudo service sshd restart
```

7. 重新启动实例之后，使用任何 SSH 客户端连接到它，然后添加Amazon通过执行以下步骤将委托管理员组到 sudoers 列表：
   a. 使用以下命令打开 `sudoers` 文件：

```
sudo visudo
```

b. 将以下内容添加到sudoers文件然后保存它。

```
## Add the "Amazon Delegated Administrators" group from the example.com domain.
%Amazon\ Delegated\ Administrators@example.com ALL=(ALL:ALL) ALL
```

(以上示例使用 “\<space>” 形成 Linux 空格字符。)

Red Hat

1. 使用任何 SSH 客户端连接到实例。
2. 配置 Linux 实例以使用的 DNS 服务器 IP 地址Amazon Directory Service-提供的 DNS 服务器。可以通过在附加到 VPC 的 DHCP 选项集中进行设置，或是通过在实例上手动设置，来执行此操作。如果您要手动设置，请参阅如何为私有 Amazon EC2 实例分配静态 DNS 服务器？中的Amazon知识中心获取有关为特定 Linux 发行版和版本设置持久 DNS 服务器的指导。
3. 确保 Red Hat - 64 位实例为最新状态。

```
sudo yum -y update
```

4. 在 Linux 实例上安装所需的 Red Hat 程序包。

   Note

   其中一些程序包可能已安装。
   安装程序包时，可能会遇到几个弹出配置屏幕。通常可以将这些屏幕中的字段保留为空白。

```
sudo yum -y install sssd realmd krb5-workstation samba-common-tools
```

5. 使用以下命令将实例加入目录。

```
sudo realm join -v -U join_account example.com --install=/
```

join_account

这些区域有：sAMAccountName对于中的账户*example.com*具有域加入权限的域。在出现提示时输入账户的密码。有关委托这些权限的更多信息，请参阅为委派目录加入权限Amazon管理Microsoft AD (p. 90)。

example.com

目录的完全限定 DNS 名称。

```
...
 * Successfully enrolled machine in realm
```

6. 设置 SSH 服务以允许进行密码身份验证。

   a. 在文本编辑器中打开 /etc/ssh/sshd_config 文件。

```
sudo vi /etc/ssh/sshd_config
```

   b. 将 PasswordAuthentication 设置为 yes。

```
PasswordAuthentication yes
```

c. 重新启动 SSH 服务。

```
sudo systemctl restart sshd.service
```

或者：

```
sudo service sshd restart
```

7. 重新启动实例之后，使用任何 SSH 客户端连接到它，然后添加Amazon通过执行以下步骤将委托管理员组到 sudoers 列表：

   a. 使用以下命令打开 `sudoers` 文件：

```
sudo visudo
```

   b. 将以下内容添加到`sudoers`文件然后保存它。

```
## Add the "Amazon Delegated Administrators" group from the example.com domain.
%Amazon\ Delegated\ Administrators@example.com ALL=(ALL:ALL) ALL
```

   (以上示例使用 “\<space>” 形成 Linux 空格字符。)

SUSE

1. 使用任何 SSH 客户端连接到实例。
2. 配置 Linux 实例以使用的 DNS 服务器 IP 地址Amazon Directory Service-提供的 DNS 服务器。可以通过在附加到 VPC 的 DHCP 选项集中进行设置，或是通过在实例上手动设置，来执行此操作。如果您要手动设置，请参阅如何为私有 Amazon EC2 实例分配静态 DNS 服务器？中的Amazon知识中心获取有关为特定 Linux 发行版和版本设置持久 DNS 服务器的指导。
3. 确保您的 SUSE Linux 15 实例为最新状态。

   a. 连接程序包存储库。

```
sudo SUSEConnect -p PackageHub/15.1/x86_64
```

   b. 更新 SUSE。

```
sudo zypper update -y
```

4. 在 Linux 实例上安装所需的 SUSE Linux 15 程序包。

   Note

   其中一些程序包可能已安装。
   安装程序包时，可能会遇到几个弹出配置屏幕。通常可以将这些屏幕中的字段保留为空白。

```
sudo zypper -n install realmd adcli sssd sssd-tools sssd-ad samba-client krb5-client
```

5. 使用以下命令将实例加入目录。

```
sudo realm join -U join_account example.com --verbose
```

join_account

example.com 域中具有域加入权限的 sAMAccountName。在出现提示时输入账户的密码。有关委托这些权限的更多信息，请参阅为委派目录加入权限Amazon管理 Microsoft AD (p. 90)。

example.com

目录的完全限定 DNS 名称。

```
…
realm: Couldn't join realm: Enabling SSSD in nsswitch.conf and PAM failed.
```

请注意，应该有以下两项返回内容。

```
! Couldn't authenticate with keytab while discovering which salt to use:
! Enabling SSSD in nsswitch.conf and PAM failed.
```

6. 手动启用SSSD在PAM.

```
sudo pam-config --add --sss
```

7. 编辑 nsswitch.conf 以在 nsswitch.conf 中启用 SSSD

```
sudo vi /etc/nsswitch.conf
```

```
passwd: compat sss
group:  compat sss
shadow: compat sss
```

8. 将以下行添加到 /etc/pam.d/common-session 中，以便在初始登录期间自动创建主目录

```
sudo vi /etc/pam.d/common-session
```

```
session optional        pam_mkhomedir.so skel=/etc/skel umask=077
```

9. 重新引导实例以完成加入域的过程。

```
sudo reboot
```

10. 使用任何 SSH 客户端重新连接到实例，验证域加入是否已成功完成，然后完成其他步骤。
    a. 确认已在域中注册实例

```
sudo realm list
```

```
example.com
  type: kerberos
  realm-name: EXAMPLE.COM
  domain-name: example.com
  configured: kerberos-member
  server-software: active-directory
  client-software: sssd
  required-package: sssd-tools
  required-package: sssd
```

```
  required-package: adcli
  required-package: samba-client
  login-formats: %U@example.com
  login-policy: allow-realm-logins
```

b. 验证 SSSD 守护程序的状态

```
systemctl status sssd
```

```
sssd.service - System Security Services Daemon
   Loaded: loaded (/usr/lib/systemd/system/sssd.service; enabled; vendor preset:
 disabled)
   Active: active (running) since Wed 2020-04-15 16:22:32 UTC; 3min 49s ago
 Main PID: 479 (sssd)
    Tasks: 4
   CGroup: /system.slice/sssd.service
           ##479 /usr/sbin/sssd -i --logger=files
           ##505 /usr/lib/sssd/sssd_be --domain example.com --uid 0 --gid 0 --
logger=files
           ##548 /usr/lib/sssd/sssd_nss --uid 0 --gid 0 --logger=files
           ##549 /usr/lib/sssd/sssd_pam --uid 0 --gid 0 --logger=files
```

11.允许用户通过 SSH 和控制台进行访问

```
sudo realm permit join_account@example.com
```

允许通过 SSH 和控制台访问域组

```
sudo realm permit -g 'Amazon Delegated Administrators'
```

或者允许所有用户访问

```
sudo realm permit --all
```

12.设置 SSH 服务以允许进行密码身份验证。

a. 在文本编辑器中打开 `/etc/ssh/sshd_config` 文件。

```
sudo vi /etc/ssh/sshd_config
```

b. 将 `PasswordAuthentication` 设置为 `yes`。

```
PasswordAuthentication yes
```

c. 重新启动 SSH 服务。

```
sudo systemctl restart sshd.service
```

或者：

```
sudo service sshd restart
```

13.13. 重新启动实例之后，使用任何 SSH 客户端连接到它，然后添加Amazon通过执行以下步骤将委托管理员组到 sudoers 列表：

a. 使用以下命令打开 sudoers 文件：

```
sudo visudo
```

b. 将以下内容添加到 sudoers 文件的底部并保存该文件。

```
## Add the "Domain Admins" group from the awsad.com domain.
%AWS\ Delegated\ Administrators@example.com ALL=(ALL) NOPASSWD: ALL
```

Ubuntu

1. 使用任何 SSH 客户端连接到实例。
2. 配置 Linux 实例以使用的 DNS 服务器 IP 地址Amazon Directory Service-提供的 DNS 服务器。可以通过在附加到 VPC 的 DHCP 选项集中进行设置，或是通过在实例上手动设置，来执行此操作。如果您要手动设置，请参阅如何为私有 Amazon EC2 实例分配静态 DNS 服务器？中的Amazon知识中心获取有关为特定 Linux 发行版和版本设置持久 DNS 服务器的指导。
3. 确保您的 Ubuntu - 64 位实例为最新状态。

```
sudo apt-get update
sudo apt-get -y upgrade
```

4. 在 Linux 实例上安装所需的 Ubuntu 程序包。

   Note

   其中一些程序包可能已安装。
   安装程序包时，可能会遇到几个弹出配置屏幕。通常可以将这些屏幕中的字段保留为空白。

```
sudo apt-get -y install sssd realmd krb5-user samba-common packagekit adcli
```

5. 禁用反向 DNS 解析，并将默认领域设置为您的域的 FQDN。Ubuntu 实例在 DNS 中必须 可以反向解析，领域才能使用。否则，您必须在 /etc/krb5.conf 中禁用 DNS，如下所示：

```
sudo vi /etc/krb5.conf
```

```
[libdefaults]
default_realm = EXAMPLE.COM
rdns = false
```

6. 使用以下命令将实例加入目录。

```
sudo realm join -U join_account example.com --verbose
```

join_account@example.com

这些区域有：sAMAccountName对于中的账户*example.com*具有域加入权限的域。在出现提示时输入账户的密码。有关委托这些权限的更多信息，请参阅为委派目录加入权限Amazon管理Microsoft AD (p. 90)。

example.com

目录的完全限定 DNS 名称。

```
...
 * Successfully enrolled machine in realm
```

7. 设置 SSH 服务以允许进行密码身份验证。
   a. 在文本编辑器中打开 `/etc/ssh/sshd_config` 文件。

   ```
   sudo vi /etc/ssh/sshd_config
   ```

   b. 将 `PasswordAuthentication` 设置为 `yes`。

   ```
   PasswordAuthentication yes
   ```

   c. 重新启动 SSH 服务。

   ```
   sudo systemctl restart sshd.service
   ```

   或者：

   ```
   sudo service sshd restart
   ```

8. 重新启动实例之后，使用任何 SSH 客户端连接到它，然后添加Amazon通过执行以下步骤将委托管理员组到 sudoers 列表：
   a. 使用以下命令打开 `sudoers` 文件：

   ```
   sudo visudo
   ```

   b. 将以下内容添加到`sudoers`文件然后保存它。

   ```
   ## Add the "Amazon Delegated Administrators" group from the example.com domain.
   %Amazon\ Delegated\ Administrators@example.com ALL=(ALL:ALL) ALL
   ```

   (以上示例使用 “\<space>” 形成 Linux 空格字符。)

限制账户登录访问

因为所有账户都是在 Active Directory 中定义的，因此默认情况下，目录中的所有用户都可以登录该实例。可以在 sssd.conf 中使用 ad_access_filter 来仅允许特定用户登录到实例。例如：

```
ad_access_filter = (memberOf=cn=admins,ou=Testou,dc=example,dc=com)
```

memberOf

指示仅当用户是特定组的成员时，才允许他们访问实例。

cn

应具有访问权限的组的通用名称。在此示例中，组名称是 *admins*。

ou

这是上面的组所在的组织单位。在此示例中，OU 是 *Testou*。

dc

这是您的域的域组成部分。在此示例中是 *example*。

dc

这是附加域组成部分。在此示例中是 *com*。

您必须手动将 ad_access_filter 添加到 /etc/sssd/sssd.conf。

在文本编辑器中打开 /etc/sssd/sssd.conf 文件。

```
sudo vi /etc/sssd/sssd.conf
```

执行此操作之后，sssd.conf 可能类似于下面这样：

```
[sssd]
domains = example.com
config_file_version = 2
services = nss, pam

[domain/example.com]
ad_domain = example.com
krb5_realm = EXAMPLE.COM
realmd_tags = manages-system joined-with-samba
cache_credentials = True
id_provider = ad
krb5_store_password_if_offline = True
default_shell = /bin/bash
ldap_id_mapping = True
use_fully_qualified_names = True
fallback_homedir = /home/%u@%d
access_provider = ad
ad_access_filter = (memberOf=cn=admins,ou=Testou,dc=example,dc=com)
```

要使配置生效，您需要重新启动 sssd 服务：

```
sudo systemctl restart sssd.service
```

或者，您也可以使用：

```
sudo service sssd restart
```

Connect 到实例

当用户使用 SSH 客户端连接到实例时，系统会提示他们输入用户名。用户可以在`username@example.com`要么`EXAMPLE\username`格式的日期和时间。响应将类似于以下内容，具体取决于您使用的 Linux 发行版：

Amazon Linux、Red Hat Enterprise Linux 和 CentOS Linux

```
login as: johndoe@example.com
johndoe@example.com's password:
Last login: Thu Jun 25 16:26:28 2015 from XX.XX.XX.XX
```

SUSE Linux

```
SUSE Linux Enterprise Server 15 SP1 x86_64 (64-bit)

As "root" (sudo or sudo -i) use the:
  - zypper command for package management
  - yast command for configuration management

Management and Config: https://www.suse.com/suse-in-the-cloud-basics
Documentation: https://www.suse.com/documentation/sles-15/
Forum: https://forums.suse.com/forumdisplay.php?93-SUSE-Public-Cloud
```

```
Have a lot of fun...
```

Ubuntu Linux

```
login as: admin@example.com
admin@example.com@10.24.34.0's password:
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-1057-aws x86_64)

* Documentation:  https://help.ubuntu.com
* Management:     https://landscape.canonical.com
* Support:        https://ubuntu.com/advantage

  System information as of Sat Apr 18 22:03:35 UTC 2020

  System load:  0.01               Processes:           102
  Usage of /:   18.6% of 7.69GB    Users logged in:     2
  Memory usage: 16%                IP address for eth0: 10.24.34.1
  Swap usage:   0%
```

使用 Winbind 手动加入 Linux 实例

您可以使用 Winbind 服务手动将 Linux 实例加入到Amazon托管的 Microsoft AD 域。这使您的现有本地 Active Directory 用户能够在访问加入到Amazon托管的 Microsoft AD。支持以下 Linux 实例分发版和版本：

- Amazon Linux AMI 2018.03.0
- Amazon Linux 2（64 位 x86）
- Red Hat Enterprise Linux 8 (HVM)（64 位 x86）
- Ubuntu Server 18.04 LTS 和 Ubuntu Server 16.04 LTS
- CentOS 7 x86-64
- SUSE Linux Enterprise Server 15 SP1

> **Note**
>
> 其他 Linux 分发版和版本可能会正常运行，但未经过测试。

将实例加入目录

在将 Amazon Linux、CentOS、红帽或 Ubuntu 实例加入您的目录之前，该实例必须按照中指定的方式启动。无缝地联接 Windows EC2 实例 (p. 66).

> **Important**
>
> 以下某些过程如果未正确执行，可能会使实例无法访问或不可用。因此，我们强烈建议在执行这些过程之前对实例创建备份或拍摄快照。

将 Linux 实例加入目录

使用以下选项卡之一对特定 Linux 实例执行步骤：

Amazon Linux/CENTOS/REDHAT

1. 使用任何 SSH 客户端连接到实例。
2. 配置 Linux 实例以使用的 DNS 服务器 IP 地址Amazon Directory Service-提供的 DNS 服务器。可以通过在附加到 VPC 的 DHCP 选项集中进行设置，或是通过在实例上手动设置，来执行此操作。如果您要手动设置，请参阅如何为私有 Amazon EC2 实例分配静态 DNS 服务器？中的Amazon知识中心获取有关为特定 Linux 发行版和版本设置持久 DNS 服务器的指导。

3. 确保您的 Linux 实例为最新状态。

```
sudo yum -y update
```

4. 在 Linux 实例上安装所需的 Samba /Winbind 程序包。

```
sudo yum -y install authconfig samba samba-client samba-winbind samba-winbind-clients
```

5. 备份主`smb.conf`这样你就可以在发生任何故障时恢复到它：

```
sudo cp /etc/samba/smb.conf /etc/samba/smb.bk
```

6. 打开原始配置文件 [`/etc/samba/smb.conf`在文本编辑器中。

```
sudo vim /etc/samba/smb.conf
```

填写 Active Directory 域环境信息，如下面的示例所示：

```
[global]
 workgroup = example
 security = ads
 realm = example.com
 idmap config * : rangesize = 1000000
 idmap config * : range = 1000000-19999999
 idmap config * : backend = autorid
 winbind enum users = no
 winbind enum groups = no
 template homedir = /home/%U@%D
 template shell = /bin/bash
 winbind use default domain = false
```

7. 打开 hosts 文件 [`/etc/hosts`在文本编辑器中。

```
sudo vim /etc/hosts
```

按如下方式添加您的 Linux 实例私有 IP 地址：

```
10.x.x.x  Linux_hostname.example.com Linux_hostname
```

> **Note**
>
> 如果你没有在`/etc/hosts`文件中，您可能会收到以下 DNS 错误消息： ：
> `No DNS domain configured for linux-instance. Unable to perform DNS Update. DNS update failed: NT_STATUS_INVALID_PARAMETER`
> 此错误表示加入成功，但 [net ads] 命令无法在 DNS 中注册 DNS 记录。

8. 使用 net 实用程序将 Linux 实例加入 Active Directory。

```
sudo net ads join -U join_account@example.com
```

join_account@example.com

中的账户*example.com*具有域加入权限的域。在出现提示时输入账户的密码。有关委托这些权限的更多信息，请参阅为委派目录加入权限Amazon管理 Microsoft AD (p. 90)。

example.com

目录的完全限定 DNS 名称。

```
Enter join_account@example.com's password:
Using short domain name -- example
Joined 'IP-10-x-x-x' to dns domain 'example.com'
```

9. 修改 PAM 配置文件，使用以下命令添加 winbind 身份验证所需的条目：

```
sudo authconfig --enablewinbind --enablewinbindauth  --enablemkhomedir   --update
```

10. 通过编辑/etc/ssh/sshd_config文件。。
    a. 在文本编辑器中打开 /etc/ssh/sshd_config 文件。

    ```
    sudo vi /etc/ssh/sshd_config
    ```

    b. 将 PasswordAuthentication 设置为 yes。

    ```
    PasswordAuthentication yes
    ```

    c. 重新启动 SSH 服务。

    ```
    sudo systemctl restart sshd.service
    ```

    或者：

    ```
    sudo service sshd restart
    ```

11. 重新启动实例之后，使用任何 SSH 客户端连接到它，然后通过执行以下步骤将域用户或组的 root 权限添加到 sudoers 列表：
    a. 使用以下命令打开 sudoers 文件：

    ```
    sudo visudo
    ```

    b. 如下所示，从您的信任域或受信任域添加所需的组或用户，然后保存它。

    ```
    ## Adding Domain Users/Groups.
    %domainname\\Amazon\ Delegated\ Administrators ALL=(ALL:ALL) ALL
    %domainname\\groupname ALL=(ALL:ALL) ALL
    domainname\\username ALL=(ALL:ALL) ALL
    %Trusted_DomainName\\groupname ALL=(ALL:ALL) ALL
    Trusted_DomainName\\username ALL=(ALL:ALL) ALL
    ```

    (以上示例使用 “\<space>” 形成 Linux 空格字符。)

SUSE

1. 使用任何 SSH 客户端连接到实例。
2. 配置 Linux 实例以使用的 DNS 服务器 IP 地址Amazon Directory Service-提供的 DNS 服务器。可以通过在附加到 VPC 的 DHCP 选项集中进行设置，或是通过在实例上手动设置，来执行此操作。如果您要手动设置，请参阅如何为私有 Amazon EC2 实例分配静态 DNS 服务器？中的Amazon知识中心获取有关为特定 Linux 发行版和版本设置持久 DNS 服务器的指导。
3. 确保您的 SUSE Linux 15 实例为最新状态。
    a. 连接程序包存储库。

```
sudo SUSEConnect -p PackageHub/15.1/x86_64
```

b. 更新 SUSE。

```
sudo zypper update -y
```

4. 在 Linux 实例上安装所需的 Samba /Winbind 程序包。

```
sudo zypper in -y samba samba-winbind
```

5. 备份主`smb.conf`这样你就可以在发生任何故障时恢复到它：

```
sudo cp /etc/samba/smb.conf /etc/samba/smb.bk
```

6. 打开原始配置文件 [`/etc/samba/smb.conf`在文本编辑器中。

```
sudo vim /etc/samba/smb.conf
```

填写 Active Directory 域环境信息，如下面的示例所示：

```
[global]
 workgroup = example
 security = ads
 realm = example.com
 idmap config * : rangesize = 1000000
 idmap config * : range = 1000000-19999999
 idmap config * : backend = autorid
 winbind enum users = no
 winbind enum groups = no
 template homedir = /home/%U@%D
 template shell = /bin/bash
 winbind use default domain = false
```

7. 打开 hosts 文件 [`/etc/hosts`在文本编辑器中。

```
sudo vim /etc/hosts
```

按如下方式添加您的 Linux 实例私有 IP 地址：

```
10.x.x.x  Linux_hostname.example.com Linux_hostname
```

> **Note**
>
> 如果你没有在`/etc/hosts`文件中，您可能会收到以下 DNS 错误消息： ：
> `No DNS domain configured for linux-instance. Unable to perform DNS Update. DNS update failed: NT_STATUS_INVALID_PARAMETER`
> 此错误表示加入成功，但 [net ads] 命令无法在 DNS 中注册 DNS 记录。

8. 使用以下命令将 Linux 实例加入目录。

```
sudo net ads join -U join_account@example.com
```

join_account

example.com 域中具有域加入权限的 sAMAccountName。在出现提示时输入账户的密码。有关委托这些权限的更多信息，请参阅为委派目录加入权限Amazon管理 Microsoft AD (p. 90)。

example.com

目录的完全限定 DNS 名称。

```
Enter join_account@example.com's password:
Using short domain name -- example
Joined 'IP-10-x-x-x' to dns domain 'example.com'
```

9. 修改 PAM 配置文件，使用以下命令添加 Winbind 身份验证所需的条目：

```
sudo pam-config --add --winbind --mkhomedir
```

10. 打开名称服务交换机配置文件 [`/etc/nsswitch.conf`在文本编辑器中。

```
vim /etc/nsswitch.conf
```

添加 Winbind 指令，如下所示。

```
passwd: files winbind
shadow: files winbind
group:  files winbind
```

11. 通过编辑`/etc/ssh/sshd_config`文件。。

a. 在文本编辑器中打开 `/etc/ssh/sshd_config` 文件。

```
sudo vim /etc/ssh/sshd_config
```

b. 将 `PasswordAuthentication` 设置为 `yes`。

```
PasswordAuthentication yes
```

c. 重新启动 SSH 服务。

```
sudo systemctl restart sshd.service
```

或者：

```
sudo service sshd restart
```

12. 重新启动实例之后，使用任何 SSH 客户端连接到它，然后通过执行以下步骤将域用户或组的 root 权限添加到 sudoers 列表：

a. 使用以下命令打开 `sudoers` 文件：

```
sudo visudo
```

b. 如下所示，从您的信任域或受信任域添加所需的组或用户，然后保存它。

```
## Adding Domain Users/Groups.
%domainname\\Amazon\ Delegated\ Administrators ALL=(ALL:ALL) ALL
%domainname\\groupname ALL=(ALL:ALL) ALL
domainname\\username ALL=(ALL:ALL) ALL
%Trusted_DomainName\\groupname ALL=(ALL:ALL) ALL
Trusted_DomainName\\username ALL=(ALL:ALL) ALL
```

(以上示例使用 “\<space>” 形成 Linux 空格字符。)

Ubuntu

1. 使用任何 SSH 客户端连接到实例。
2. 配置 Linux 实例以使用的 DNS 服务器 IP 地址Amazon Directory Service-提供的 DNS 服务器。可以通过在附加到 VPC 的 DHCP 选项集中进行设置，或是通过在实例上手动设置，来执行此操作。如果您要手动设置，请参阅如何为私有 Amazon EC2 实例分配静态 DNS 服务器？中的Amazon知识中心获取有关为特定 Linux 发行版和版本设置持久 DNS 服务器的指导。
3. 确保您的 Linux 实例为最新状态。

```
sudo yum -y update
```

```
sudo apt-get -y upgrade
```

4. 在 Linux 实例上安装所需的 Samba /Winbind 程序包。

```
sudo apt -y install samba winbind libnss-winbind libpam-winbind
```

5. 备份主`smb.conf`文件，以便在出现任何故障时可以恢复到它。

```
sudo cp /etc/samba/smb.conf /etc/samba/smb.bk
```

6. 打开原始配置文件 [`/etc/samba/smb.conf`在文本编辑器中。

```
sudo vim /etc/samba/smb.conf
```

填写 Active Directory 域环境信息，如下面的示例所示：

```
[global]
 workgroup = example
 security = ads
 realm = example.com
 idmap config * : rangesize = 1000000
 idmap config * : range = 1000000-19999999
 idmap config * : backend = autorid
 winbind enum users = no
 winbind enum groups = no
 template homedir = /home/%U@%D
 template shell = /bin/bash
 winbind use default domain = false
```

7. 打开 hosts 文件 [`/etc/hosts`在文本编辑器中。

```
sudo vim /etc/hosts
```

按如下方式添加您的 Linux 实例私有 IP 地址：

```
10.x.x.x  Linux_hostname.example.com Linux_hostname
```

Note

如果你没有在`/etc/hosts`文件中，您可能会收到以下 DNS 错误消息： ：
`No DNS domain configured for linux-instance. Unable to perform DNS Update. DNS update failed: NT_STATUS_INVALID_PARAMETER`
此错误表示加入成功，但 [net ads] 命令无法在 DNS 中注册 DNS 记录。

8. 使用 net 实用程序将 Linux 实例加入 Active Directory。

```
sudo net ads join -U join_account@example.com
```

join_account@example.com

中的账户*example.com*具有域加入权限的域。在出现提示时输入账户的密码。有关委托这些权限的更多信息，请参阅为委派目录加入权限Amazon管理 Microsoft AD (p. 90)。

example.com

目录的完全限定 DNS 名称。

```
Enter join_account@example.com's password:
Using short domain name -- example
Joined 'IP-10-x-x-x' to dns domain 'example.com'
```

9. 修改 PAM 配置文件，使用以下命令添加 Winbind 身份验证所需的条目：

```
sudo pam-auth-update --add --winbind --enable mkhomedir
```

10. 打开名称服务交换机配置文件 [`/etc/nsswitch.conf`在文本编辑器中。

```
vim /etc/nsswitch.conf
```

添加 Winbind 指令，如下所示。

```
passwd: compat winbind
group:  compat winbind
shadow: compat winbind
```

11. 通过编辑`/etc/ssh/sshd_config`文件。。

a. 在文本编辑器中打开 `/etc/ssh/sshd_config` 文件。

```
sudo vim /etc/ssh/sshd_config
```

b. 将 `PasswordAuthentication` 设置为 `yes`。

```
PasswordAuthentication yes
```

c. 重新启动 SSH 服务。

```
sudo systemctl restart sshd.service
```

或者：

```
sudo service sshd restart
```

12. 重新启动实例之后，使用任何 SSH 客户端连接到它，然后通过执行以下步骤将域用户或组的 root 权限添加到 sudoers 列表：

a. 使用以下命令打开 `sudoers` 文件：

```
sudo visudo
```

b. 如下所示，从您的信任域或受信任域添加所需的组或用户，然后保存它。

```
## Adding Domain Users/Groups.
%domainname\\Amazon\ Delegated\ Administrators ALL=(ALL:ALL) ALL
%domainname\\groupname ALL=(ALL:ALL) ALL
domainname\\username ALL=(ALL:ALL) ALL
%Trusted_DomainName\\groupname ALL=(ALL:ALL) ALL
Trusted_DomainName\\username ALL=(ALL:ALL) ALL
```

(以上示例使用 “\<space>” 形成 Linux 空格字符。)

Connect 到实例

当用户使用 SSH 客户端连接到实例时，系统会提示他们输入用户名。用户可以在`username@example.com`要么`EXAMPLE\username`格式的日期和时间。响应将类似于以下内容，具体取决于您使用的 Linux 发行版：

Amazon Linux、Red Hat Enterprise Linux 和 CentOS Linux

```
login as: johndoe@example.com
johndoe@example.com's password:
Last login: Thu Jun 25 16:26:28 2015 from XX.XX.XX.XX
```

SUSE Linux

```
SUSE Linux Enterprise Server 15 SP1 x86_64 (64-bit)

As "root" (sudo or sudo -i) use the:
  - zypper command for package management
  - yast command for configuration management

Management and Config: https://www.suse.com/suse-in-the-cloud-basics
Documentation: https://www.suse.com/documentation/sles-15/
Forum: https://forums.suse.com/forumdisplay.php?93-SUSE-Public-Cloud

Have a lot of fun...
```

Ubuntu Linux

```
login as: admin@example.com
admin@example.com@10.24.34.0's password:
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-1057-aws x86_64)

* Documentation:  https://help.ubuntu.com
* Management:     https://landscape.canonical.com
* Support:        https://ubuntu.com/advantage

  System information as of Sat Apr 18 22:03:35 UTC 2020

  System load:  0.01               Processes:           102
  Usage of /:   18.6% of 7.69GB    Users logged in:     2
  Memory usage: 16%                IP address for eth0: 10.24.34.1
  Swap usage:   0%
```

为委派目录加入权限Amazon管理 Microsoft AD

要将计算机加入到目录，需要有权将计算机加入到目录的账户。

与AmazonDirectory Service in Microsoft Active Directory (Microsoft Active Directory)Admins和Amazon服务器委托管理员组拥有这些权限。

但是根据最佳实践，应使用只拥有所需的最小权限的账户。以下过程演示如何创建名为 `Joiners` 的新组，并向此组委派将计算机加入到目录所需的权限。

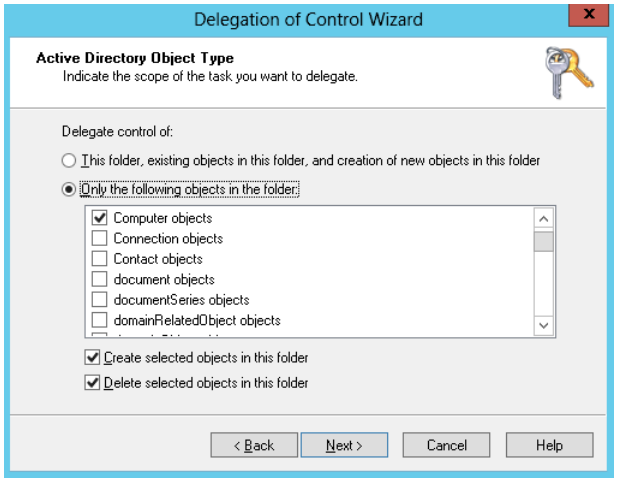
必须在已加入您的目录且具有Active Directory 用户和计算机已安装 MMC 管理单元。您还必须以域管理员身份登录。

为 委派加入权限Amazon管理 Microsoft AD

1. 打开 Active Directory User and Computers，在导航树中选择具有您的 NetBIOS 名称的组织单位 (OU)，然后选择 Users OU。

   Important

   当你启动Amazon为 Microsoft Active Directory 提供 Directory Service，Amazon创建一个包含所有目录对象的组织单位 (OU)。此 OU (具有您在创建目录时键入的 NetBIOS 名称) 位于域根目录中。此域根目录由 Amazon 拥有和管理。无法对域根本身进行更改，因此必须在具有您的 NetBIOS 名称的 OU 中创建 **`Joiners`** 组。
2. 打开 Users 的上下文 (右键单击) 菜单，然后依次选择 New 和 Group。
3. 在 New Object - Group 框中，键入以下内容，然后选择 OK。
   - 对于 Group name (组名称)，键入 **`Joiners`**。
   - 对于 Group scope，选择 Global。
   - 对于 Group type，选择 Security。
4. 在导航树中，选择您的 NetBIOS 名称下的 Computers 容器。从 Action 菜单中选择 Delegate Control。
5. 在 Delegation of Control Wizard 页面上，选择 Next，然后选择 Add。
6. 在 Select Users, Computers, or Groups 框中，键入 `Joiners`，然后选择 OK。如果找到多个对象，请选择上面创建的 `Joiners` 组。选择 Next (下一步)。
7. 在 Tasks to Delegate 页面上，选择 Create a custom task to delegate，然后选择 Next。
8. 选择 Only the following objects in the folder，然后选择 Computer objects。
9. 选择 Create selected objects in this folder，然后选择 Delete selected objects in this folder。然后选择下一步。



10. 选择 Read 和 Write，然后选择 Next。

11. 在 Completing the Delegation of Control Wizard 页面上验证信息，然后选择 Finish。
12. 使用强密码创建一个用户，并将该用户添加到 `Joiners` 组。此用户必须位于您的 NetBIOS 名称下的 Users 容器中。该用户随后拥有足够的权限将实例连接到目录。

创建 DHCP 选项集

Amazon我们建议为Amazon Directory Service目录并将 DHCP 选项集分配给目录所在的 VPC。这使该 VPC 中的任何实例都可以指向指定域和 DNS 服务器以解析其域名。

有关 DHCP 选项集的更多信息，请参阅DHCP 选项集中的Amazon VPC User Guide.

为目录创建 DHCP 选项集

1. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 DHCP Options Sets，然后选择 Create DHCP options set。
3. 在存储库的创建 DHCP 选项集页面上，为目录输入以下值：

   名称

   选项集的可选标签。

   域名

   目录的完全限定名称，例如`corp.example.com`.

   域名服务器

   你的 IP 地址Amazon-提供目录的 DNS 服务器。

   > **Note**
   >
   > 可以转到Amazon Directory Service控制台导航窗格，选择目录然后选择正确的目录 ID。

   NTP 服务器

   将此字段留空。

   NetBIOS 名称服务器

   将此字段留空。

   NetBIOS 节点类型

   将此字段留空。

4. 选择创建 DHCP 选项集。新的 DHCP 选项集会出现在您的 DHCP 选项列表中。
5. 记录新增 DHCP 选项集的 ID (dopt-*xxxxxxxx*)。您可以使用它将新选项集与 VPC 相关联。

更改与 VPC 相关联的 DHCP 选项集。

在您创建 DHCP 选项集之后，您便无法再修改这些选项。如果您希望 VPC 使用不同的 DHCP 选项集，您必须创建新的选项集，并将其与您的 VPC 相关联。您还可以设置 VPC，让其不使用任何 DHCP 选项。

1. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择您的 VPC
3. 选择 VPC，然后选择操作、编辑 DHCP 选项集.
4. 适用于DHCP 选项集，选择一个选项集或选择未设置 DHCP 选项选择，然后选择Save（保存）.

在中管理用户和组AmazonMicrosoft Managed Microsoft AD

用户表示有权访问您的目录的独立个人或实体。对于针对用户组授予或拒绝权限非常有用，从而不必将这些权限应用于每个独立用户。如果用户移动到不同的组织，您将该用户移动到不同的组后，他们会自动接收新组织所需的权限。

在中创建用户和组Amazon Directory Service目录中，您必须使用已加入到Amazon Directory Service以具有创建用户和组权限的用户身份登录。您还需要在 EC2 实例上安装 Active Directory 工具，以便添加具有 Active Directory 用户和计算机管理单元的用户和组。有关如何设置 EC2 实例和安装所需工具的更多信息，请参阅 第 3 步：部署 EC2 实例以管理您的AmazonMicrosoft Managed Microsoft AD (p. 151)。

> **Note**
>
> 用户账户必须启用 Kerberos 预身份验证。这是新用户账户的默认设置，但它不应进行修改。有关此设置的更多信息，请参阅 Microsoft TechNet 上的 Preauthentication。

以下主题介绍了有关如何创建和管理用户和组的说明。

主题

- 安装 Active Directory 管理工具 (p. 93)
- 创建用户 (p. 94)
- 重置用户密码 (p. 94)
- 创建组 (p. 95)
- 如何为群组添加用户 (p. 96)

安装 Active Directory 管理工具

要从 EC2 Windows 实例中管理您的目录，您需要在该实例中安装 Active Directory Domain Services 和 Active Directory Lightweight Directory Services 工具。按照以下过程操作，在 Windows Server 2012、Windows Server 2016 或 Windows Server 2019 上安装这些工具。

您可以选择使用 Windows PowerShell 安装 Active Directory 管理工具。例如，您可以使用 `Install-WindowsFeature RSAT-ADDS` 从 PowerShell 提示符安装 Active Directory 远程管理工具。有关详细信息，请参阅 Microsoft 网站上的 Install-WindowsFeature。

在 Windows Server 2012 到 Windows Server 2019 上安装 Active Directory 管理工具

在 Windows Server 2012 到 Windows Server 2019 上安装 Active Directory 管理工具

1. 通过从“开始”屏幕选择服务器管理器，打开服务器管理器。
2. 在 Server Manager Dashboard (服务器管理器控制面板) 中，选择 Add roles and features (添加角色和功能)。
3. 在 Add Roles and Features Wizard (添加角色和功能向导) 中，依次选择 Installation Type (安装类型)、Role-based or feature-based installation (基于角色或基于功能的安装) 和 Next (下一步)。
4. 在 Server Selection (服务器选择) 下，确保已选中本地服务器，然后选择左侧导航栏中的 Features (功能)。
5. 在 Features (功能) 树中，打开 Remote Server Administration Tools (远程服务器管理工具)、Role Administration Tools (角色管理工具)，选择 AD DS and AD LDS Tools (AD DS 和 AD LDS 工具)，向下滚动并选择 DNS Server Tools (DNS 服务器工具)，然后选择 Next (下一步)。
6. 检查信息，然后选择安装。当该功能安装完成后，Active Directory Domain Services 和 Active Directory Lightweight Directory Services 工具将出现在“开始”屏幕的管理工具文件夹中。

创建用户

使用以下过程可创建其 EC2 实例加入到您的Amazon托管 Microsoft AD 目录。

创建用户

1. 打开“Active Directory 用户和计算机”工具。中有一个快捷方式访问此工具管理工具folder。

   Tip

   您可以在实例上从命令提示符运行以下命令，直接打开 Active Directory 用户和计算机工具框。

   ```
   %SystemRoot%\system32\dsa.msc
   ```

2. 在目录树中，在目录的 NetBIOS 名称 OU 下选择要存储用户（例如 Corp\ Users）的 OU。有关目录使用的 OU 结构的更多信息，请参阅Amazon，请参阅创建的内容 (p. 10).
3. 在 Action 菜单上，单击 New，然后单击 User 打开新用户向导。
4. 在向导的第一页上，输入以下字段的值，然后单击。下一步.
   - 名
   - 姓
   - User logon name
5. 在向导的第二页上，在密码和Confirm Password (确认密码). 确保用户必须在下次登录时更改密码选项已选中。不应选择任何其他选项。单击 Next（下一步）。
6. 在向导的第三页上，验证新用户的信息正确无误，然后单击。Finish. 新用户会出现在 Users 文件夹中。

重置用户密码

用户必须遵守目录中定义的密码策略。有时这可以获得最好的用户，包括目录管理员，然后他们忘记了密码。发生这种情况时，您可以使用Amazon Directory Service如果用户驻留在 Simple AD 或Amazon托管的 Microsoft AD 目录。

除以下例外情况，您可以重置目录中的任何用户的密码：

- 对于 Simple AD，您不能为任何属于Domain Admins要么Enterprise Admins组（管理员用户除外）。
- 适用于Amazon托管 Microsoft AD，您无法重置 OU 中的任何用户的密码，此 OU 基于您在创建目录时键入的 NetBIOS 名称。例如，您无法在Amazon预留OU。有关的 OU 结构的更多信息Amazon托管的 Microsoft AD 目录，请参阅创建的内容 (p. 10).

您可以使用以下任何方法重置用户的密码。

方法 1：重置用户密码（Amazon Web Services Management Console）

1. 在Amazon Directory Service控制台导航窗格，下Active Directory，选择目录，然后在列表中选择要重置用户密码的目录。
2. 在存储库的目录详细信息页面，选择重置用户密码.
3. 在重置用户密码对话，在用户名键入需要更改其密码的用户的用户名。
4. 在中键入密码新密码和确认密码，然后选择Reset password.

方法 2：重置用户密码（Windows PowerShell）

1. 打开 Windows PowerShell。
2. 键入以下命令，然后将用户名 “joebob” 和密码 “P @ssw0rd” 替换为所需的凭据。请参阅重置dsuserPassword Cmdlet有关.

   ```
   Reset-DSUserPassword -UserName joebob -DirectoryId d-1234567890 -NewPassword
   P@ssw0rd
   ```

方法 3：重置用户密码（Amazon CLI）

1. 打开 Amazon CLI。
2. 键入以下命令，然后将用户名 “joebob” 和密码 “P @ssw0rd” 替换为所需的凭据。请参阅重置用户密码中的Amazon CLI命令参考有关.

   ```
   aws ds reset-user-password --directory-id d-1234567890 --user-name joebob --
   new-password P@ssw0rd
   ```

创建组

使用以下过程可创建其 EC2 实例加入到您的安全组。Amazon托管 Microsoft AD 目录。

创建组

1. 打开“Active Directory 用户和计算机”工具。中有一个快捷方式访问此工具管理工具folder。

   Tip

   您可以在实例上从命令提示符运行以下命令，直接打开 Active Directory 用户和计算机工具框。

   ```
   %SystemRoot%\system32\dsa.msc
   ```

2. 在目录树中，在目录的 NetBIOS 名称 OU 下选择要存储组的 OU（例如，Corp\ Users）。有关目录使用的 OU 结构的更多信息，请参阅Amazon请参阅创建的内容 (p. 10).
3. 在 Action 菜单上，单击 New，然后单击 Group 打开新组向导。
4. 键入组的名称Group nameSelect,Group scopeSelect, 然后选择安全(对于)Group type.
5. 单击 OK（确定）。新的安全组将出现在用户folder。

如何为群组添加用户

使用以下过程可将用户添加到其 EC2 实例加入到您的安全组。Amazon托管 Microsoft AD 目录。

如何为群组添加用户

1. 打开“Active Directory 用户和计算机”工具。在中有这个工具的快捷方式管理工具folder。

   Tip

   您可以在实例上从命令提示符运行以下命令，直接打开 Active Directory 用户和计算机工具框。

   ```
   %SystemRoot%\system32\dsa.msc
   ```

2. 在目录树中，选择存储组的目录的 NetBIOS 名称 OU 下的 OU，然后选择要将用户添加为成员的组。
3. 在存储库的操作菜单中，单击属性以打开组的属性对话框。
4. Select成员Stab，然后单击Add.
5. 适用于输入要选择的对象名称中，键入要添加的用户名，然后单击确定. 名称将显示在成员列表。再次单击 OK 更新组成员资格。
6. 通过在用户文件夹然后单击属性中的操作菜单可打开属性对话框。Select的成员选项卡。您应该在用户所属的组的列表中看到组的名称。

Connect 到您的现有 AD 基础设施

此部分介绍如何配置之间的信任关系Amazon托管微软 AD 和您的现有 AD 基础设施。

主题

- 创建信任关系 (p. 96)
- 使用公有 IP 地址时添加 IP 路由 (p. 99)
- 教程：在您之间创建信任关系Amazon托管微软 AD 和你的自我管理的 Active Directory 域 (p. 100)
- 教程：在两者之间创建信任关系Amazon托管的 Microsoft AD 域 (p. 107)

创建信任关系

可以在您的之间配置单向和双向外部信任关系和林信任关系Amazon适用于 Microsoft Active Directory 和自我管理（本地）目录以及多个目录之间的 Directory ServiceAmazon中的 Managed Microsoft AD 目录Amazon云。Amazon托管微软 AD 支持所有三个信任关系方向：传入、传出和双向。

Note

在设置信任关系时，必须确保自行管理目录始终兼容并保持兼容性Amazon Directory Service。有关您的责任的更多信息，请参阅我们的责任共担模型。

Amazon Managed Microsoft AD 支持外部信任和林信任。要演练演示如何创建林信任的示例方案，请参阅教程：在您之间创建信任关系Amazon托管微软 AD 和你的自我管理的 Active Directory 域 (p. 100)。

需要双向信任Amazon企业应用程序，例如 Amazon Chime、Amazon Connect、Amazon QuickSight、Amazon IAM Identity Center (successor to Amazon Single Sign-On)、Amazon WorkDocs、Amazon WorkMail、Amazon WorkSpaces 和Amazon Web Services Management Console.Amazon 托管 Microsoft AD 必须能够查询自我管理的 AD 中的用户和组。

Amazon EC2、Amazon RDS 和 Amazon FSx 将使用单向或双向信任。

先决条件

创建信任只需几个步骤，但是在设置信任之前必须先完成一些先决条件步骤。

> Note
>
> Amazon Managed Microsoft AD 不支持信任单一标签域.

连接到 VPC

如果要创建与自行管理目录的信任关系，则必须先将自行管理网络连接到包含的 VPC。Amazon托管的 Microsoft AD。自行管理的防火墙Amazon托管 Microsoft AD 网络必须打开中列出的网络端口Windows Server 2008 及更高版本.

这些是能够连接到目录所需的最少端口。根据您的特定配置，您可能需要打开其他端口。

配置 VPC

包含的 VPCAmazon Managed Microsoft AD 必须具有适当的出站和入站规则。

配置 VPC 出站规则

1. 在Amazon Directory Service控制台，在详细目录页面，请注意你的Amazon托管的 Microsoft AD 目录 ID。
2. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
3. 选择 Security Groups。
4. 搜索您的Amazon托管的 Microsoft AD 目录 ID。在搜索结果中，选择带描述的项目”Amazon为创建安全组目录 ID目录控制器”。

   > Note
   >
   > 所选安全组是在最初创建目录时自动创建的安全组。

5. 转到该安全组的 Outbound Rules 选项卡。依次选择 Edit、Add another rule。对于新规则，输入以下值：

   - 类型：所有流量
   - 协议：全部
   - 目的地确定可以离开您的域控制器的流量，以及它可以传送到自行管理网络的位置。用 CIDR 表示法指定单个 IP 地址或 IP 地址范围 (例如 203.0.113.5/32)。您还可以在同一区域中指定其他安全组的名称或 ID。有关更多信息，请参阅 了解你的目录Amazon安全组配置和使用 (p. 137)。
6. 选择 Save。

启用 Kerberos 预身份验证

用户账户必须启用 Kerberos 预身份验证。有关此设置的更多信息，请查看 Microsoft TechNet 上的 Preauthentication。

在自我管理的域中配置 DNS 条件转发器

必须在自行管理域中设置 DNS 条件转发服务器。请参阅为域名分配有条件代理在 Microsoft 上 TechNet 了解有关条件代理的详细信息。

要执行以下步骤，必须具有针对自行管理域的以下 Windows Server 工具的访问权限：

- AD DS 和 AD LDS 工具
- DNS

在自行管理域中配置条件转发服务器

1. 首先必须获取有关的一些信息Amazon托管的 Microsoft AD。登录到Amazon Web Services Management Console然后打开Amazon Directory Service控制台在 https://console.aws.amazon.com/directoryservicev2/。
2. 在导航窗格中，选择 Directories。
3. 选择的目录 IDAmazon托管的 Microsoft AD。
4. 记下目录的完全限定域名 (FQDN) 和 DNS 地址。
5. 现在返回到自行管理域控制器。打开服务器管理器。
6. 在 Tools 菜单上，选择 DNS。
7. 在控制台树中，展开为其设置信任的域的 DNS 服务器。
8. 在控制台树中，选择 Conditional Forwarders。
9. 在 Action 菜单上，选择 New conditional forwarder。
10. InDNS 域，键入您的完全限定域名 (FQDN)Amazon你之前注意到的托管微软 AD。
11. 选择主服务器的 IP 地址然后键入你的 DNS 地址Amazon前面记下的 Microsoft AD 目录。

    输入 DNS 地址之后，可能遇到“超时”或“无法解析”错误。通常可以忽略这些错误。
12. Select将此条件转发服务器存储在 Active Directory 中，如下所示复制：此域中的所有 DNS 服务器. 选择 OK（确定）。

信任关系密码

如果要创建与现有域的信任关系，则使用 Windows Server 管理工具对该域设置信任关系。执行此操作时，请记下所使用的信任密码。在上设置信任关系时，需要使用该密码。Amazon托管的 Microsoft AD。有关更多信息，请参阅 Microsoft TechNet 上的管理信任。

现在您已准备就绪，可在上创建信任关系Amazon托管的 Microsoft AD。

创建、验证或删除信任关系

> **Note**
>
> 信任关系是Amazon托管的 Microsoft AD。如果您在使用多区域复制 (p. 54)，必须在主 区域 (p. 55). 这些更改将自动应用于所有复制的区域。有关更多信息，请参阅 全球与区域功能 (p. 54)。

创建与 的信任关系Amazon托管的 Microsoft AD

1. 打开 Amazon Directory Service 控制台。
2. 在存储库的目录页面上，选择Amazon托管的 Microsoft AD ID。
3. 在存储库的目录详细信息页面上，执行以下操作之一：
   - 如果你在下面显示了多个地区多区域复制，选择主要区域，然后选择网络 & 安全选项卡。有关更多信息，请参阅 主要与其他地区 (p. 55)。
   - 如果在下面没有显示任何地区多区域复制，选择网络 & 安全选项卡。
4. 在信任关系部分中，选择操作，然后选择添加信任关系。
5. 在添加信任关系页面上，提供所需信息，包括信任类型、受信任域的完全限定域名 (FQDN)、信任密码和信任方向。
6. （可选）如果您希望仅允许授权用户访问您的中的资源Amazon托管微软 AD 目录，你可以选择选择性验证”复选框。有关选择性身份验证的一般信息，请参阅 Microsoft TechNet 上的信任的安全注意事项。
7. 适用于条件转发器，键入自行管理 DNS 服务器的 IP 地址。如果以前创建过条件转发服务器，可以键入自行管理域的 FQDN，而不是 DNS IP 地址。
8. （可选）选择添加另一个 IP 地址然后键入另一台自行管理 DNS 服务器的 IP 地址。可以为每台适用的 DNS 服务器地址重复此步骤，总共可输入四个地址。

9. 选择 Add（添加）。
10. 如果自行管理域的 DNS 服务器或网络使用公有（非 RFC 1918）IP 地址空间，则转至IP 路由部分，选择操作，然后选择添加路由. 使用 CIDR 格式键入 DNS 服务器或自行管理网络的 IP 地址块，例如 203.0.113.0/24。如果您的 DNS 服务器和自行管理网络均使用 RFC 1918 IP 地址空间，此步骤并不是必要的。

    Note

    在使用公有 IP 地址空间时，请确保不要使用任何AmazonIP 地址范围因为无法使用。
11. （可选）我们建议，当您位于添加路由页面上时，您还可以选择向此目录的 VPC 的安全组添加路由。这样会按照上面“配置 VPC”中的详细说明来配置安全组。这些安全规则会影响未公开的内部网络接口。如果此选项不可用，则您会看到一条消息，指示已自定义了安全组。

必须对两个域都设置信任关系。关系必须互相补充。例如，如果在一个域上创建传出信任，则必须在另一个域上创建传入信任。

如果要创建与现有域的信任关系，则使用 Windows Server 管理工具对该域设置信任关系。

您可以在之间创建多个信任Amazon管理微软 AD 和各种活动目录域。但是，每次只能有一个信任关系存在。例如，如果有一个“传入方向”的现有单向信任，随后要设置“传出方向”的另一个信任关系，则需要删除现有信任关系，再创建新的“双向”信任。

验证传出信任关系

1. 打开 Amazon Directory Service 控制台。
2. 在存储库的目录页面上，选择Amazon托管的 Microsoft AD ID。
3. 在存储库的目录详细信息页面上，执行以下操作之一：
   - 如果你在下面显示了多个地区多区域复制，选择主要区域，然后选择网络 & 安全选项卡。有关更多信息，请参阅 主要与其他地区 (p. 55)。
   - 如果在下面没有显示任何地区多区域复制，选择网络 & 安全选项卡。
4. 在信任关系部分中，选择您想要验证的信任，选择操作，然后选择验证信任关系。

此过程仅验证双向信任的传出方向。Amazon不支持验证传入信任。有关如何验证传入或传出自行管理 Active Directory 的信任的更多信息，请参阅验证信任在 Microsoft TechNet 上。

删除现有信任关系

1. 打开 Amazon Directory Service 控制台。
2. 在存储库的目录页面上，选择Amazon托管的 Microsoft AD ID。
3. 在存储库的目录详细信息页面上，执行以下操作之一：
   - 如果你在下面显示了多个地区多区域复制，选择主要区域，然后选择网络 & 安全选项卡。有关更多信息，请参阅 主要与其他地区 (p. 55)。
   - 如果在下面没有显示任何地区多区域复制，选择网络 & 安全选项卡。
4. 在信任关系部分中，选择您想要删除的信任，选择操作，然后选择删除信任关系。
5. 选择 Delete。

使用公有 IP 地址时添加 IP 路由

您可以使用Amazon使用 Microsoft Active Directory 的 Directory Service，可以利用许多强大的 Active Directory 功能，包括与其他目录建立信任。但是，如果其他目录网络的 DNS 服务器使用公有 (非 RFC 1918) IP 地址，则必须在配置信任的过程中指定这些 IP 地址。有关执行此操作的说明位于创建信任关系 (p. 96)。

同样，在路由来自Amazon开启托管的 Microsoft AD 的项Amazon对同行AmazonVPC，如果 VPC 使用公有 IP 范围。

当您按照创建信任关系 (p. 96)中所述添加 IP 地址时，您可以选择 Add routes to the security group for this directory's VPC。除非以前自定义了安全组以允许所需流量 (如下所示)，否则应选择此选项。有关更多信息，请参阅了解你的目录Amazon安全组配置和使用 (p. 137)。

教程：在您之间创建信任关系Amazon托管微软 AD 和你的自我管理的 Active Directory 域

本教程将引导您完成所有在之间设置信任关系所需的所有步骤。Amazon针对 Microsoft Active Directory 和自行管理的（本地）Microsoft Active Directory 的 Directory Service。虽然创建信任只需执行几个步骤，但是必须先完成以下先决条件步骤。

主题

- 先决条件 (p. 100)
- 第 1 步：准备自我管理的 AD 域 (p. 101)
- 第 2 步：准备您的Amazon托管的 Microsoft AD (p. 103)
- 第 3 步：创建信任关系 (p. 106)

另请参阅

创建信任关系 (p. 96)

先决条件

本教程假定您已具备以下条件：

> **Note**
>
> Amazon托管的 Microsoft AD 不支持与的信任单个标签域.

- 网络 ACL 和安全组都允许 (因此可到达您的实例) 的发起 ping 的Amazon在上创建托管的 Microsoft AD 目录Amazon. 如果需要有关执行此操作的帮助，请参阅开始使用AmazonMicrosoft AD (p. 8)。
- 添加到该的运行 Windows 的 EC2 实例Amazon托管的 Microsoft AD。如果需要有关执行此操作的帮助，请参阅手动加入 Windows 实例 (p. 67)。

  > **Important**
  >
  > 您的管理员帐户Amazon托管的 Microsoft AD 必须拥有此实例的管理访问权限。
- 在该实例上安装了以下 Windows Server 工具：
  - AD DS 和 AD LDS 工具
  - DNS

  如果需要有关执行此操作的帮助，请参阅安装 Active Directory 管理工具 (p. 93)。
- 自我管理的（本地）微软活动目录

  您必须拥有此目录的管理访问权限。上面列出的相同 Windows Server 工具还必须可用于此目录。
- 自行管理的网络与包含您的 VPC 之间的活动连接Amazon托管的 Microsoft AD。如果需要有关执行此操作的帮助，请参阅 Amazon Virtual Private Cloud 连接选项。
- 正确设置的本地安全策略。Check`Local Security Policy > Local Policies > Security Options > Network access: Named Pipes that can be accessed anonymously`并确保其至少包含以下三个命名管道：
  - netlogon
  - samr

- lsarpc

教程配置

在本教程中，我们已创建了Amazon托管微软 AD 和自我管理的域。自我管理的网络已连接到Amazon托管 Microsoft AD 的 VPC。以下是两个目录的属性：

Amazon在上运行托管的 Microsoft AD 的项Amazon

- 域名 (FQDN)：myManagedad.example.com
- NetBIOS 名称：MyManagedAD
- DNS 地址：10.0.10.246、10.0.20.121
- VPC CIDR：10.0.0.0/16

这些区域有：Amazon托管的 Microsoft AD 位于 VPC ID：vpc-12345678 中。

自行管理或Amazon托管的 Microsoft AD 域

- 域名 (FQDN)：corp.example.com
- NetBIOS 名称：CORP
- DNS 地址：172.16.10.153
- 自行管理的 CIDR：172.16.0.0/16

下一步

第 1 步：准备自我管理的 AD 域 (p. 101)

第 1 步：准备自我管理的 AD 域

首先需要完成对自行管理（本地）域完成几个先决条件步骤。

配置自行管理的防火墙

必须配置自行管理的防火墙，以便为包含的 VPC 所使用的所有子网，面向 CIDR 打开以下端口。AmazonAD 托管的 Microsoft AD。在本教程中，我们允许来自 10.0.0.0/16（的 CIDR 数据块）的传入和传出流量。Amazon在以下端口上托管微软 AD 的 VPC）：

- TCP/UDP 53 - DNS
- TCP/UDP 88 - Kerberos 身份验证
- TCP/UDP 389 - LDAP
- TCP 445 - SMB

  > **Note**
  >
  > 不再支持 SMBv1。

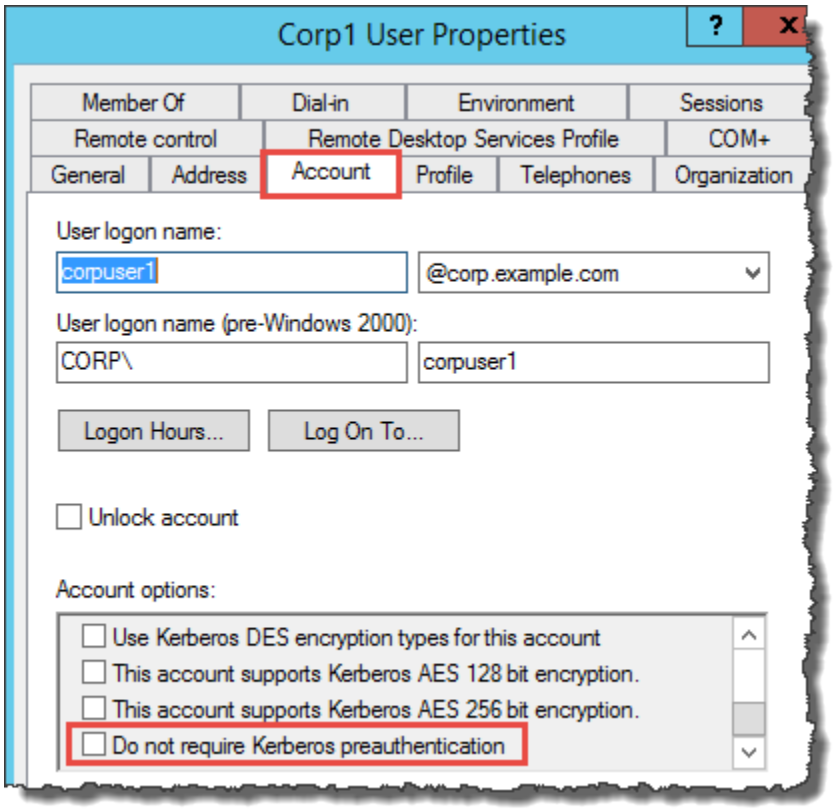
> **Note**
>
> 这些是将 VPC 连接到自行管理目录所需的最少端口。根据您的特定配置，您可能需要打开其他端口。

确保启用 Kerberos 预身份验证

这两个目录中的用户账户必须启用 Kerberos 预身份验证。这是默认值，但让我们检查任何随机用户的属性以确保无任何更改。

要查看用户 kerberos 设置

1. 在自行管理的域控制器上，打开服务器管理器。
2. 在 Tools 菜单上，选择 Active Directory Users and Computers。
3. 选择 Users 文件夹并打开上下文（右键单击）菜单。选择右窗格中列出的任何随机用户账户。选择 Properties (属性)。
4. 选择 Account 选项卡。在 Account options 列表中，向下滚动并确保未 选中 Do not require Kerberos preauthentication。



为自管域配置 DNS 条件转发器

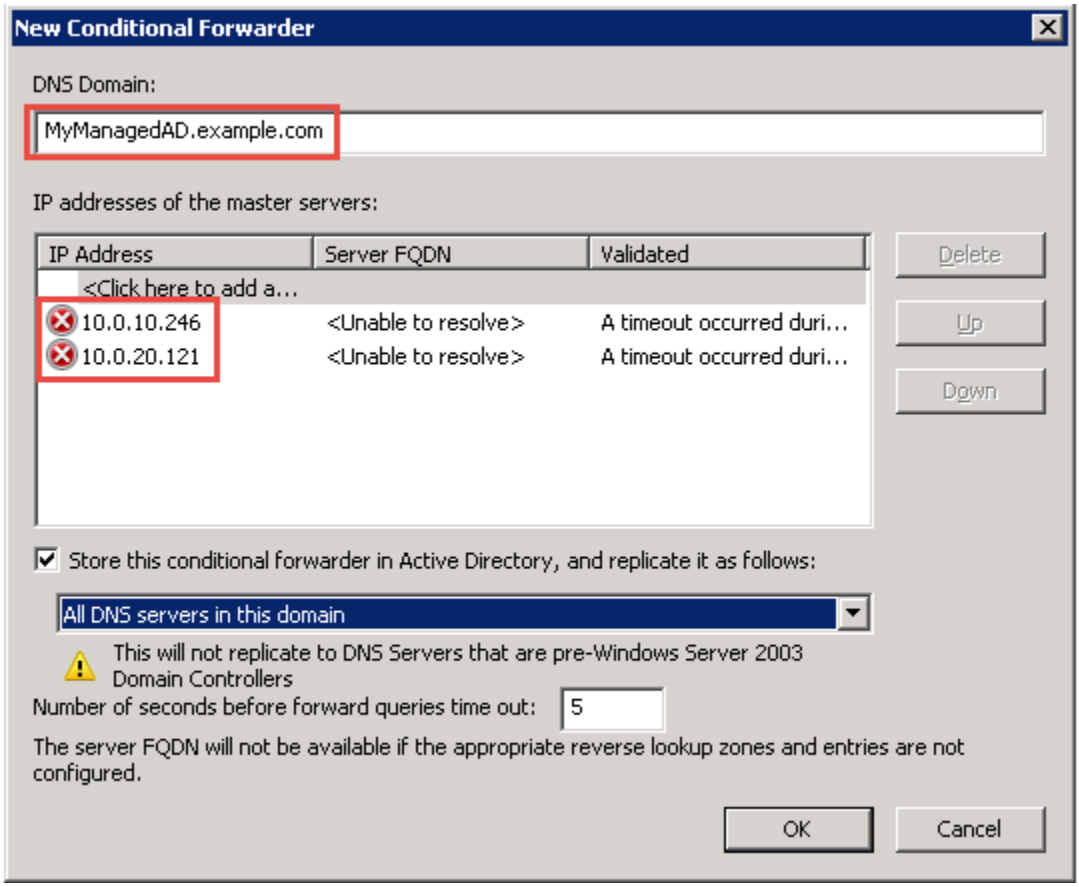
必须在每个域中都设置 DNS 条件转发服务器。对自行管理域执行此操作之前，首先会获取有关的一些信息。AmazonAD 托管的 Microsoft AD。

在自行管理域中配置条件转发服务器

1. 登录到Amazon Web Services Management Console然后打开Amazon Directory Service控制台在 https://console.aws.amazon.com/directoryservicev2/。
2. 在导航窗格中，选择 Directories。
3. 选择的目录 IDAmazonAD 托管的 Microsoft AD。
4. 在详细信息页面上，记下您的目录的目录名称和 DNS 地址中的值。
5. 现在返回到自行管理的域控制器。打开服务器管理器。
6. 在 Tools 菜单上，选择 DNS。
7. 在控制台树中，展开为其设置信任的域的 DNS 服务器。我们的服务器是 WIN-5V70CN7VJ0.corp.example.com。

8. 在控制台树中，选择 Conditional Forwarders。
9. 在 Action 菜单上，选择 New conditional forwarder。
10. In域 DNS 域，键入完全限定域名 (FQDN)Amazon你之前注意到的托管微软 AD。在此示例中，FQDN 是 MyManagedAD.example.com。
11. 选择主服务器的 IP 地址然后键入你的 DNS 地址Amazon前面记下的 Microsoft AD 目录。在这个例子中，这些是：10.0.10.246、10.0.20.121

    输入 DNS 地址之后，可能遇到“超时”或“无法解析”错误。通常可以忽略这些错误。



12. 选择 Store this conditional forwarder in Active Directory, and replicate it as follows。
13. 选择 All DNS servers in this domain，然后选择 OK。

下一步

第 2 步：准备您的Amazon托管的 Microsoft AD (p. 103)

第 2 步：准备您的Amazon托管的 Microsoft AD

现在我们来找您的Amazon为信任关系准备 Microsoft AD。以下许多步骤与刚才为自管理域完成的步骤几乎相同。但是，这次是使用的是Amazon托管的 Microsoft AD。

配置 VPC 子网和安全组

您必须允许流量从自我管理的网络流向包含的 VPCAmazon托管的 Microsoft AD。为此，您需要确保与子网关联的 ACL 用于部署Amazon在您的域控制器上配置托管的 Microsoft AD 和安全组规则，二者都允许必需的流量以支持信任。

端口要求因域控制器使用的 Windows Server 版本和将利用信任的服务或应用程序而异。在本教程中，您将需要打开以下端口：

入站

- TCP/UDP 53 - DNS
- TCP/UDP 88 - Kerberos 身份验证
- UDP 123 - NTP
- TCP 135 - RPC
- TCP/UDP 389 - LDAP
- TCP/UDP 445 - SMB

  Note

  不再支持 SMBv1。
- TCP/UDP 464 - Kerberos 身份验证
- TCP 636 - LDAPS (通过 TLS/SSL 的 LDAP)
- TCP 3269 - 全局目录
- TCP/UDP 49152-65535-RPC 的临时端口

出站

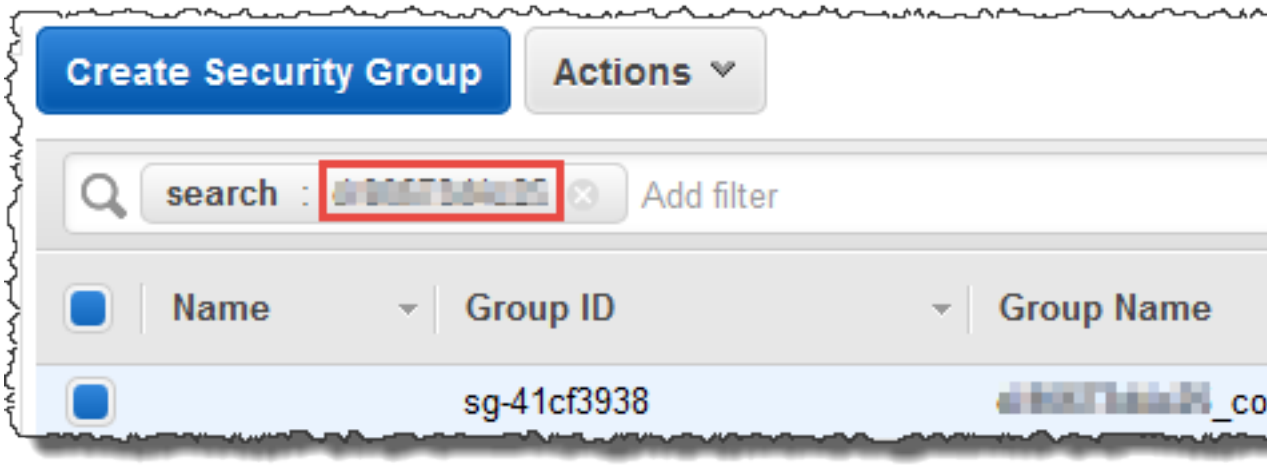
- ALL

Note

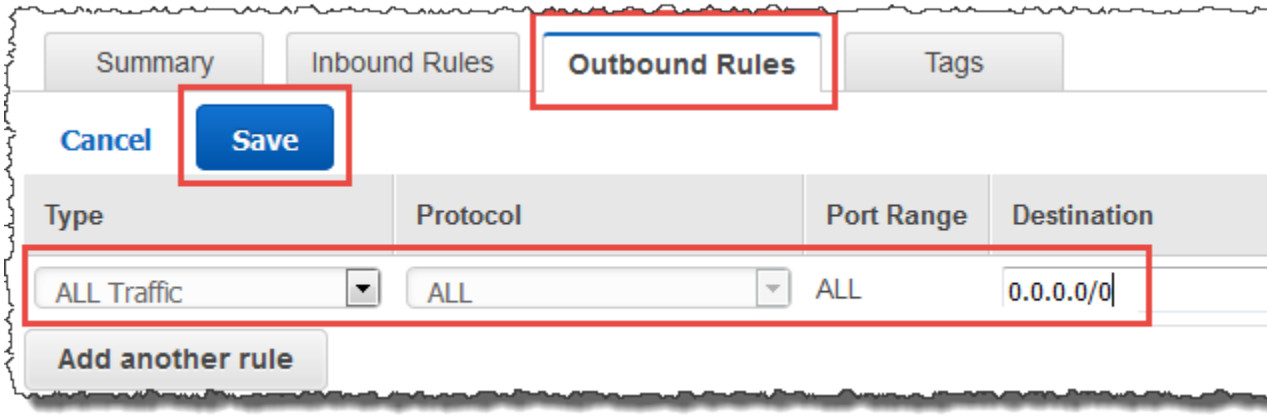
这些是连接 VPC 和自我管理目录所需的最少端口。根据您的特定配置，您可能需要打开其他端口。

配置Amazon托管的 Microsoft AD 域控制器出站和入站规则

1. 返回到 Amazon Directory Service 控制台。在目录列表中，请记下您的目录 IDAmazon托管的 Microsoft AD 目录。
2. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
3. 在导航窗格中，选择 Security Groups。
4. 使用搜索框搜索您的Amazon托管的 Microsoft AD 目录 ID。在搜索结果中，选择带描述的项Amazon为 <yourdirectoryID>目录控制器创建了安全组.



5. 转到该安全组的 Outbound Rules 选项卡。依次选择 Edit、Add another rule。对于新规则，输入以下值：
   - 类型：所有流量
   - 协议：ALL
   - Destination 确定可以离开您的域控制器的流量，以及它可以传送到何处。用 CIDR 表示法指定单个 IP 地址或 IP 地址范围 (例如 203.0.113.5/32)。您还可以在同一区域中指定其他安全组的名称或 ID。有关更多信息，请参阅 了解你的目录Amazon安全组配置和使用 (p. 137)。
6. 选择 Save。

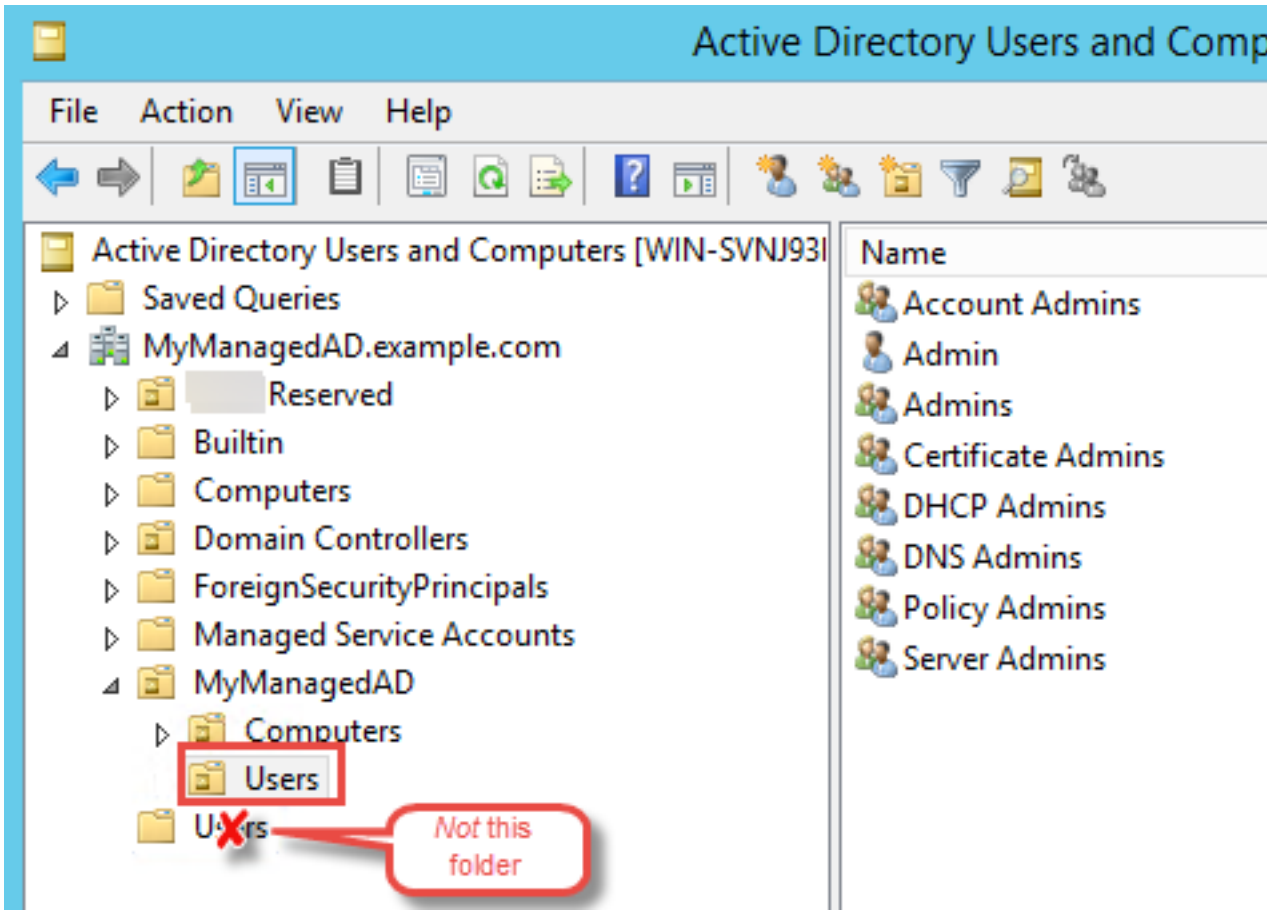


确保启用 Kerberos 预身份验证

现在要确认用户在Amazon此外，托管的 Microsoft AD 还启用了 Kerberos 预身份验证。这与为自我管理目录完成的过程相同。这是默认设置，但是我们来检查一下以确保未更改任何内容。

查看用户 kerberos 设置

1. 登录作为您的成员的实例Amazon使用管理员账户 (p. 14)用于域或已委派管理域中用户的权限的账户。
2. 如果尚未安装，请安装“Active Directory 用户和计算机”工具和 DNS 工具。可在安装 Active Directory 管理工具 (p. 93)中了解如何安装这些工具。
3. 打开服务器管理器。在 Tools 菜单上，选择 Active Directory Users and Computers。
4. 选择您的域中的 Users 文件夹。请注意，这是您的 NetBIOS 名称下的用户文件夹，而不是全限定域名 (FQDN) 下的用户文件夹。



5. 在用户列表中，右键单击一名用户，然后选择属性。
6. 选择 Account 选项卡。在 Account options 列表中，确保未 选中 Do not require Kerberos preauthentication。

下一步

第 3 步：创建信任关系 (p. 106)

第 3 步：创建信任关系

现在准备工作已完成，最后的几个步骤是创建信任。首先在自我管理的域上创建信任，最后在上创建信任。Amazon托管的 Microsoft AD。如果您在创建信任的过程中遇到任何问题，请参阅信托创建状态原因 (p. 167)获得帮助。

在自我管理的 Active Directory 中配置信任

在本教程中，将配置一个双向林信任。但是，如果创建单向林信任，请注意，每个域上的信任方向必须互相补充。例如，如果在自管的域上创建单向传出信任，则需要在上创建单向传入信任。Amazon托管的 Microsoft AD。

> Note
>
> Amazon托管的 Microsoft AD 还支持外部信任。但是，在此教程中，您将创建一个双向林信任。

配置对自我管理 AD 的信任

1. 打开服务器管理器，然后在 Tools 菜单上，选择 Active Directory Domains and Trusts。

2. 打开域的上下文 (右键单击) 菜单，选择 Properties。
3. 选择 Trusts 选项卡，然后选择 New trust。键入你的名字Amazon选择托管的 Microsoft AD 并选择下一步.
4. 选择 Forest trust。选择 Next (下一步)。
5. 选择 Two-way。选择 Next (下一步)。
6. 选择 This domain only。选择 Next (下一步)。
7. 选择 Forest-wide authentication。选择 Next (下一步)。
8. 键入 Trust password。请务必记住此密码，因为在为设置信任时会需要它。Amazon托管的 Microsoft AD。
9. 在下一个对话框中，确认设置，然后选择 Next。确认已成功创建信任，再次选择 Next。
10. 选择 No, do not confirm the outgoing trust。选择 Next (下一步)。
11. 选择 No, do not confirm the incoming trust。选择 Next (下一步)。

配置信任Amazon托管的 Microsoft AD 目录

最后，配置与您的林信任关系Amazon托管的 Microsoft AD 目录。因为已在自管理域上创建了双向林信任，所以也使用Amazon托管的 Microsoft AD 目录。

> **Note**
>
> 信任关系是Amazon托管的 Microsoft AD。如果您使用多区域复制 (p. 54)，必须在主 区域 (p. 55). 这些更改将自动应用于所有复制的区域。有关更多信息，请参阅 全球与区域功能 (p. 54)。

在您的项中配置信任Amazon托管的 Microsoft AD 目录

1. 返回到 Amazon Directory Service 控制台。
2. 在存储库的目录页面上，选择Amazon托管的 Microsoft AD ID。
3. 在存储库的目录详细信息页面上，执行以下操作之一：
   - 如果你在下面显示了多个地区多区域复制，选择主要区域，然后选择网络与安全选项卡。有关更多信息，请参阅 主要与其他地区 (p. 55)。
   - 如果您在下面没有显示任何区域多区域复制，选择网络与安全选项卡。
4. 在信任关系部分中，选择操作，然后选择添加信任关系。
5. 在存储库的添加信任关系页面中，指定信任类型。在本例中，我们选择林信任. 键入自管域的 FQDN (本教程中)**`corp.example.com`**)。键入在自管域上创建信任时使用的信任密码。指定方向。在本例中，我们选择双向.
6. 在条件转发器字段中，输入自管的 DNS 服务器的 IP 地址。在此示例中，输入 172.16.10.153。
7. (可选) 选择添加另一个 IP 地址并输入自管的 DNS 服务器的第二个 IP 地址。最多可以指定总共四个 DNS 服务器。
8. 选择 Add (添加)。

祝贺您。现在，自管域 (corp.example.com) 与您的Amazon管理微软广告（myManagedad.example.com）。这两个域之间只能设置一个关系。例如，如果要将信任方向更改为单向，则需要先删除现有信任关系，然后才能创建新关系。

有关更多信息 (包括有关验证或删除信任的说明)，请参阅创建信任关系 (p. 96)。

教程：在两者之间创建信任关系Amazon托管的 Microsoft AD 域

本教程将引导您完成所有在两者之间设置信任关系所需的所有步骤。AmazonMicrosoft Active Directory 域的 Directory Service。

主题

- 第 1 步：准备您的AmazonMicrosoft AD 托管的 Microsoft AD (p. 108)
- 第 2 步：创建与另一个信任关系Amazon托管的 Microsoft AD 域 (p. 110)

另请参阅

创建信任关系 (p. 96)

第 1 步：准备您的AmazonMicrosoft AD 托管的 Microsoft AD

在本部分中，您将获得Amazon为与另一个 AD 建立信任关系准备Amazon管理 Microsoft AD。以下许多步骤与您在中完成的步骤几乎相同。教程：在您之间创建信任关系Amazon托管微软 AD 和你的自我管理的 Active Directory 域 (p. 100). 但是，这次是配置Amazon托管微软 AD 环境以相互协作。

配置 VPC 子网和安全组

你必须允许来自一个人的流量Amazon托管微软 AD 网络连接到包含你的其他人的 VPCAmazon管理 Microsoft AD。为此，您需要确保与子网关联的 ACL 用于部署Amazon在您的域控制器上配置托管的 Microsoft AD 和安全组规则，二者都允许必需的流量以支持信任。

端口要求因域控制器使用的 Windows Server 版本和将利用信任的服务或应用程序而异。在本教程中，您将需要打开以下端口：

入站

- TCP/UDP 53 - DNS
- TCP/UDP 88 - Kerberos 身份验证
- UDP 123 - NTP
- TCP 135 - RPC
- TCP/UDP 389 - LDAP
- TCP/UDP 445 - SMB

  Note

  不再支持 SMBv1。
- TCP/UDP 464 - Kerberos 身份验证
- TCP 636 - LDAPS (通过 TLS/SSL 的 LDAP)
- TCP 3269 - 全局目录
- TCP/UDP 1024-65535 - RPC 的临时端口

出站

- ALL

  Note

  这些是从两者连接 VPC 所需的最少端口。Amazon管理 Microsoft AD 的。根据您的特定配置，您可能需要打开其他端口。有关更多信息，请参阅 。如何为 Active Directory 域和信任配置防火墙在微软的网站上。

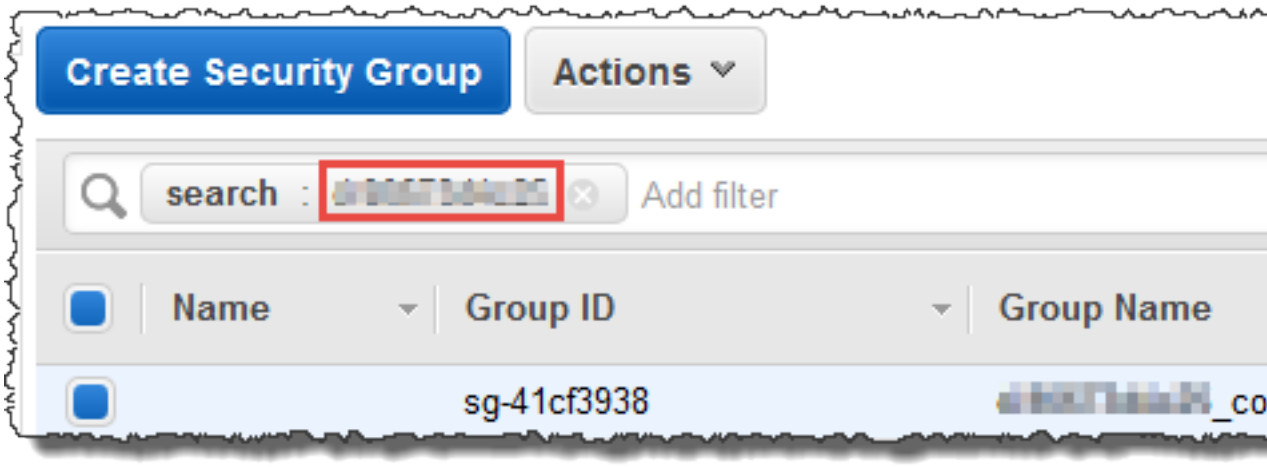
配置Amazon托管的 Microsoft AD 域控制器出站规则

Note

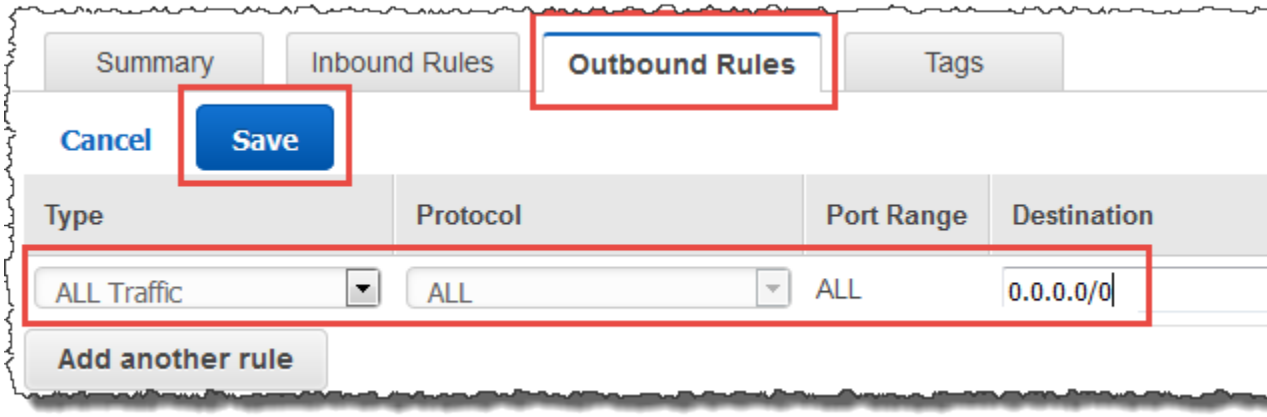
对每个目录重复以下步骤 1-6。

1. 转到 Amazon Directory Service 控制台。在目录列表中，请记下您的目录 IDAmazon管理 Microsoft AD 目录。

2. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
3. 在导航窗格中，选择 Security Groups。
4. 使用搜索框搜索Amazon托管的 Microsoft AD 目录 ID。在搜索结果中，选择带描述的项Amazon为 <yourdirectoryID>目录控制器创建了安全组.



5. 转到该安全组的 Outbound Rules 选项卡。依次选择 Edit、Add another rule。对于新规则，输入以下值：
   - 类型：所有流量
   - 协议：ALL
   - Destination 确定可以离开您的域控制器的流量，以及它可以传送到何处。用 CIDR 表示法指定单个 IP 地址或 IP 地址范围 (例如 203.0.113.5/32)。您还可以在同一区域中指定其他安全组的名称或 ID。有关更多信息，请参阅 了解你的目录Amazon安全组配置和使用 (p. 137)。
6. 选择 Save。



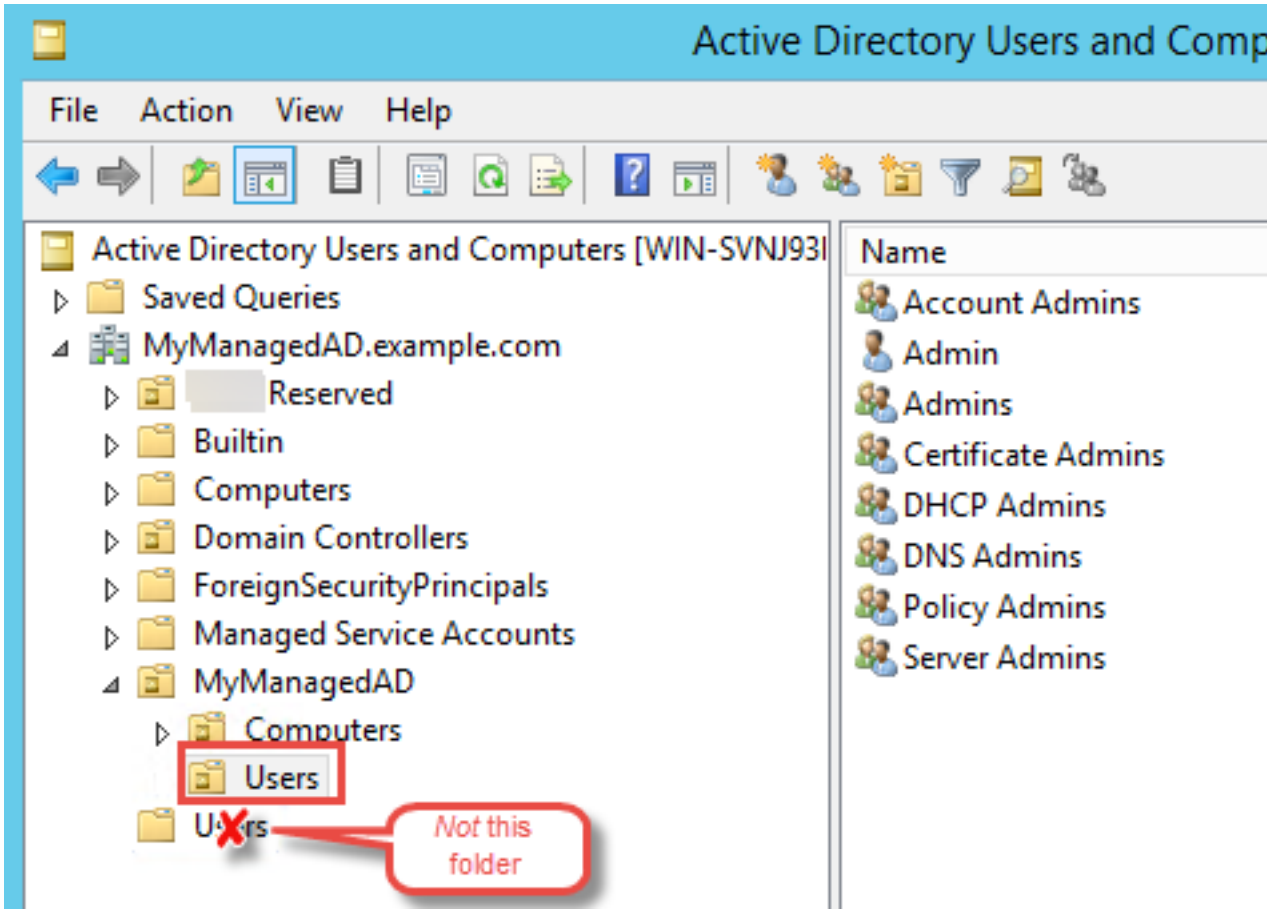
确保启用 Kerberos 预身份验证

现在要确认用户在Amazon此外，托管的 Microsoft AD 还启用了 Kerberos 预身份验证。此过程与针对本地目录完成的过程相同。这是默认设置，但是我们来检查一下以确保未更改任何内容。

查看用户 kerberos 设置

1. 登录作为成员的实例Amazon使用管理员账户 (p. 14)用于域或已委派管理域中用户的权限的账户。

2. 如果尚未安装，请安装“Active Directory 用户和计算机”工具和 DNS 工具。可在安装 Active Directory 管理工具 (p. 93)中了解如何安装这些工具。
3. 打开服务器管理器。在 Tools 菜单上，选择 Active Directory Users and Computers。
4. 选择您的域中的 Users 文件夹。请注意，这是您的 NetBIOS 名称下的用户文件夹，而不是全限定域名 (FQDN) 下的用户文件夹。



5. 在用户列表中，右键单击一名用户，然后选择属性。
6. 选择 Account 选项卡。在 Account options 列表中，确保未 选中 Do not require Kerberos preauthentication。

下一步

第 2 步：创建与另一个信任关系Amazon托管的 Microsoft AD 域 (p. 110)

第 2 步：创建与另一个信任关系Amazon托管的 Microsoft AD 域

现在准备工作已完成，最后的几个步骤是在两个之间创建信任。Amazon托管的 Microsoft AD 域。如果您在创建信任的过程中遇到任何问题，请参阅信托创建状态原因 (p. 167)获得帮助。

在第一个中配置信任Amazon托管的 Microsoft AD 域

在本教程中，将配置一个双向林信任。但是，如果创建单向林信任，请注意，每个域上的信任方向必须互相补充。例如，如果在第一个域上创建单向传出信任，则需要在第二个域上创建单向传入信任。Amazon托管的 Microsoft AD 域。

Note

Amazon托管的 Microsoft AD 还支持外部信任。但是，在此教程中，您将创建一个双向林信任。

在第一个中配置信任Amazon托管的 Microsoft AD 域

1. 打开 Amazon Directory Service 控制台。
2. 在存储库的目录第一页，选择第一页Amazon托管的 Microsoft AD ID。
3. 在存储库的目录详细信息页面上，执行以下操作之一：
   - 如果你有多个地区显示在下面多区域复制，选择主要区域，然后选择联网 & 安全选项卡。有关更多信息，请参阅 主要与其他地区 (p. 55)。
   - 如果在下面没有显示任何区域多区域复制，选择联网 & 安全选项卡。
4. 在信任关系部分中，选择操作，然后选择添加信任关系。
5. 在存储库的添加信任关系页面，键入第二个 FQDNAmazon托管的 Microsoft AD 域。请务必记住此密码，因为在为第二个设置信任时会需要它Amazon托管的 Microsoft AD。指定方向。在本例中，选择双向.
6. 在条件转发器在字段中，输入第二个 IP 地址Amazon托管的 Microsoft AD 服务器。
7. (可选) 选择添加另一个 IP 地址然后为第二个 IP 地址输入第二个 IP 地址Amazon托管的 Microsoft AD 服务器。最多可以指定总共四个 DNS 服务器。
8. 选择 Add (添加)。此时信任将失败，预计直到我们建立信任的另一端。

在第二个中配置信任Amazon托管的 Microsoft AD 域

现在，将林信任关系配置为第二个Amazon托管的 Microsoft AD 目录。因为第一次创建了双向林信任Amazon使用托管的 Microsoft AD 域，还将创建双向信任。Amazon托管的 Microsoft AD 域。

在第二个中配置信任Amazon托管的 Microsoft AD 域

1. 返回到 Amazon Directory Service 控制台。
2. 在存储库的目录第二页，选择第二页Amazon托管的 Microsoft AD ID。
3. 在存储库的目录详细信息页面上，执行以下操作之一：
   - 如果你有多个地区显示在下面多区域复制，选择主要区域，然后选择联网 & 安全选项卡。有关更多信息，请参阅 主要与其他地区 (p. 55)。
   - 如果在下面没有显示任何区域多区域复制，选择联网 & 安全选项卡。
4. 在信任关系部分中，选择操作，然后选择添加信任关系。
5. 在存储库的添加信任关系页面，键入第一个 FQDNAmazon托管的 Microsoft AD 域。键入在本地域上创建信任时所使用的信任密码。指定方向。在本例中，选择双向.
6. 在条件转发器在字段中，输入第一个 IP 地址Amazon托管的 Microsoft AD 服务器。
7. (可选) 选择添加另一个 IP 地址然后为第一个 IP 地址输入第二个 IP 地址Amazon托管的 Microsoft AD 服务器。最多可以指定总共四个 DNS 服务器。
8. 选择 Add (添加)。之后不久应该对信任进行验证。
9. 现在，返回您在第一个域中创建的信任并再次验证信任关系。

祝贺您。现在你两个之间有信任关系Amazon托管的 Microsoft AD 域。这两个域之间只能设置一个关系。例如，如果要将信任方向更改为单向，则需要先删除现有信任关系，然后才能创建新关系。

扩展你的架构

Amazon使用架构托管的 Microsoft AD 来组织和实施目录数据的存储。向架构添加定义的过程称为“扩展架构”。利用架构扩展，您可以修改您的架构。Amazon使用有效的 LDAP 数据交换格式 (LDIF) 文件托管的 Microsoft AD 目录。有关 AD 架构以及如何扩展架构的更多信息，请参阅下面列出的主题。

主题

- 什么时候延长Amazon托管的 Microsoft AD 架构 (p. 112)
- 教程：扩展您的Amazon托管的 Microsoft AD 架构 (p. 112)

什么时候延长Amazon托管的 Microsoft AD 架构

你可以延长Amazon通过添加新对象类和属性来管理 Microsoft AD 架构。例如，如果具有需要更改架构以便支持单点登录功能的应用程序，可以执行此操作。

还可以使用架构扩展为依赖于特定 Active Directory 对象类和属性的应用程序启用支持。在需要迁移依赖于的企业应用程序的情况下，这特别有用。Amazon转到托管的 Microsoft AD 的项Amazon云。

添加到现有 Active Directory 架构的每个属性或类都必须使用唯一 ID 进行定义。这样在公司向架构添加扩展时，这些扩展可以保证是唯一的，不会相互冲突。这些 ID 称为 AD 对象标识符 (OID)，存储在Amazon托管的 Microsoft AD。

要了解其用法，请参阅 教程：扩展您的Amazon托管的 Microsoft AD 架构 (p. 112)。

相关主题

- 扩展你的架构 (p. 111)
- 架构元素 (p. 16)

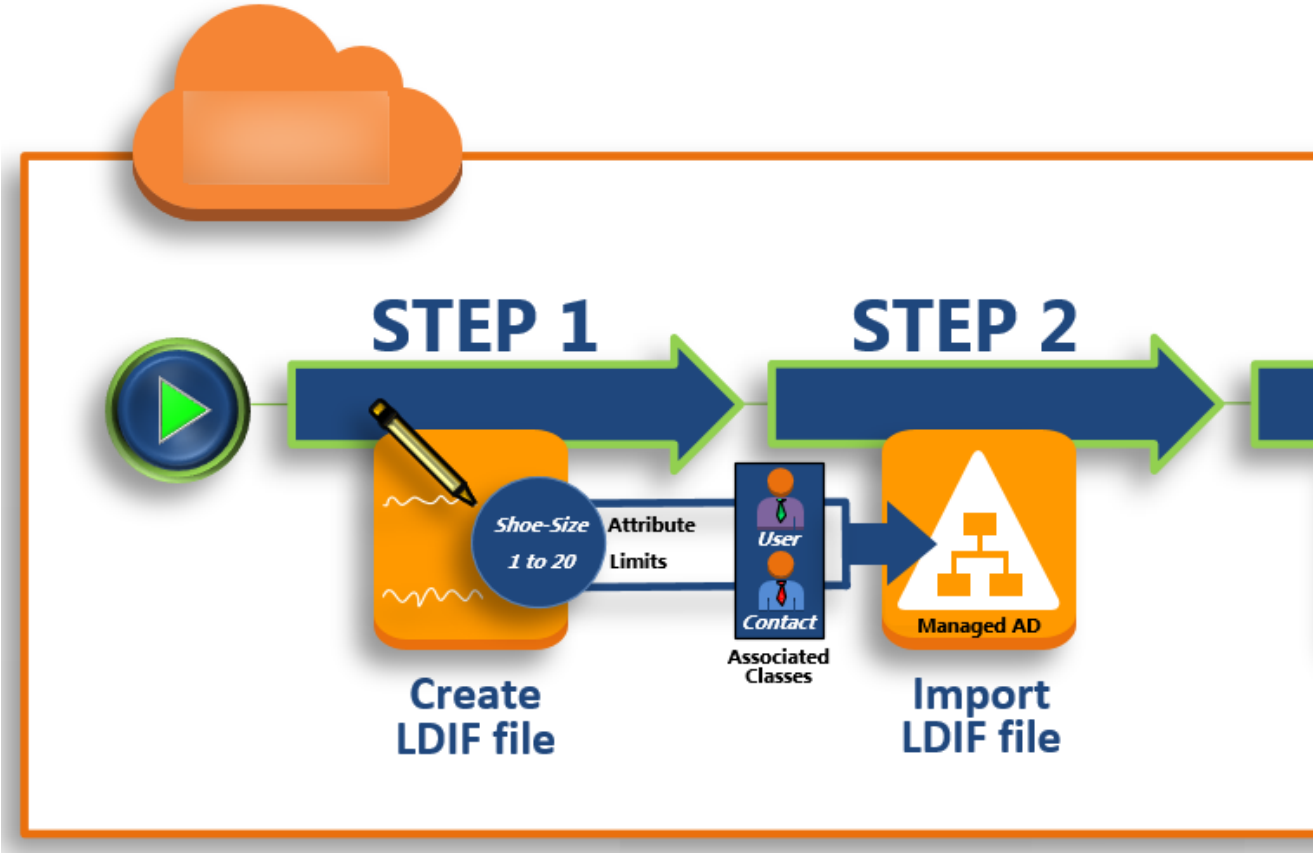
教程：扩展您的Amazon托管的 Microsoft AD 架构

在本教程中，您将学习如何扩展架构。AmazonMicrosoft Active Directory Directory Service，也称为Amazon通过添加独特的管理微软 AD属性和类别满足您的特定要求。Amazon只能使用有效的 LDIF (轻量目录交换格式) 脚本文件来上传和应用托管的 Microsoft AD 架构扩展。

属性 (attributeSchema) 定义数据库中的字段，而类 (classSchema) 定义数据库中的表。例如，Active Directory 中的所有用户对象均由架构类 User 定义，而用户的各个属性 (如电子邮件地址或电话号码) 由每个属性定义。

如果您要添加新属性 (如 Shoe-Size)，您需要定义一个 integer 类型的新属性。您还可以定义下限和上限，如 1 到 20。创建 Shoe-Size attributeSchema 对象后，可以更改 User classSchema 对象以包含该属性。属性可以关联到多个类。例如，也可以将 Shoe-Size 添加到 Contact 类。有关 Active Directory 架构的更多信息，请参阅什么时候延长Amazon托管的 Microsoft AD 架构 (p. 112)。

此工作流程具有三个基本步骤。



第 1 步：创建 LDIF 文件 (p. 113)

首先，创建一个 LDIF 文件并定义新属性和应将这项属性添加到的任何类。您可以将此文件用于工作流程的下一阶段。

第 2 步：导入 LDIF 文件 (p. 114)

在此步骤中，您将使用 Amazon Directory Service 控制台将 LDIF 文件导入您的 Microsoft AD 环境。

第 3 步：验证模式扩展是否成功 (p. 115)

最后，您以管理员身份使用 EC2 实例来验证新扩展是否出现在 Active Directory 架构管理单元中。

第 1 步：创建 LDIF 文件

LDIF 文件是用于表示 LDAP (轻量目录访问协议) 目录内容和更新请求的标准纯文本数据交换格式。LDIF 将目录内容作为一组记录来传递，每个对象 (或条目) 对应一条记录。它将更新请求 (如添加、修改、删除和重命名) 也表示为一组记录，每个更新请求对应一条记录。

这些区域有：Amazon Directory Service通过运行包含架构更改的 LDIF 文件`ldifde.exe`在您的应用程序Amazon托管的 Microsoft AD 目录。因此，您会发现理解 LDIF 脚本语法很有帮助。有关更多信息，请参阅 LDIF 脚本。

多种第三方 LDIF 工具均可提取、清理和更新您的架构更新。无论您使用哪种工具，都要了解 LDIF 文件中使用的所有标识符都必须唯一，这一点很重要。

强烈建议您在创建自己的 LDIF 文件之前先查看以下概念和提示。

- 架构元素— 了解架构元素，如属性、类、对象 ID 和关联属性。有关更多信息，请参阅 架构元素 (p. 16)。

- 物品序列— 确保 LDIF 文件中的项目布局顺序按照目录信息树 (DIT)从上而下。LDIF 文件中确定顺序的一般规则如下：
  - 各项目之间以空白行分隔。
  - 子项目列在其父项目之后。
  - 确保架构中存在属性或对象类等项目。如果不存在，则必须先将其添加到架构中，然后才能使用。例如，在将属性分配给类之前，必须先创建该属性。
- DN 的格式— 对于 LDIF 文件中的每个新指令，将可分辨名称 (DN) 定义为指令的第一行。DN 在 Active Directory 对象树中标识 Active Directory 对象，并且必须包含目录的域组件。例如，在本教程中，目录的域组件为 `DC=example,DC=com`。

  DN 还必须包含 Active Directory 对象的公用名 (CN)。第一个 CN 条目是属性或类名称。接下来，必须使用 `CN=Schema,CN=Configuration`。此 CN 可确保您能够扩展 Active Directory 架构。如前所述，您无法添加或修改 Active Directory 对象的内容。DN 的一般格式如下所示。

  ```
  dn: CN=[attribute or class name],CN=Schema,CN=Configuration,DC=[domain_name]
  ```

  在本教程中，新 Shoe-Size 属性的 DN 类似于：

  ```
  dn: CN=Shoe-Size,CN=Schema,CN=Configuration,DC=example,DC=com
  ```

- 警告 – 请在扩展架构前查看下面的警告。
  - 在扩展 Active Directory 架构之前，必须先查看 Microsoft 有关此操作的影响的警告。有关更多信息，请参阅在扩展架构之前需要了解的事项。
  - 您不能删除架构属性或类。因此，如果您犯了错误且不想从备份中还原，则只能禁用该对象。有关更多信息，请参阅禁用现有的类和属性。

要了解有关 LDIF 文件构造方式的更多信息并查看可用于测试的示例 LDIF 文件Amazon托管微软 AD 架构扩展，请参阅文章如何扩展您的Amazon托管的 Microsoft AD 目录架构在Amazon安全博客。

下一步

第 2 步：导入 LDIF 文件 (p. 114)

第 2 步：导入 LDIF 文件

您可以通过从 Amazon Directory Service 控制台或使用 API 导入 LDIF 文件来扩展您的架构。有关如何使用架构扩展 API 执行此操作的更多信息，请参阅Amazon Directory ServiceAPI 参考. 目前，Amazon 不支持通过外部应用程序（如 Microsoft Exchange）直接执行架构更新。

> **Important**
>
> 当您对您的更新时Amazon托管的 Microsoft AD 目录架构，此操作无法撤消。换言之，新类或属性一旦创建，Active Directory 不允许您将其删除。但是，您可以将其禁用。
> 如果您必须删除架构更改，一个选项是从之前的快照中还原目录。还原快照会将架构和目录数据都回滚到以前的时间点，而不仅仅是回滚架构。请注意，快照支持的最长期限为 180 天。有关更多信息，请参阅 Microsoft 网站上的 Active Directory 的系统状态备份的有用保质期。

在更新过程开始之前，Amazon托管的 Microsoft AD 会拍摄快照来保留目录的当前状态。

> **Note**
>
> 模式扩展是Amazon托管的 Microsoft AD。如果您在使用多区域复制 (p. 54)，必须在主 区域 (p. 55). 这些更改将自动应用于所有复制的区域。有关更多信息，请参阅 全球与区域功能 (p. 54)。

导入 LDIF 文件

1. 在Amazon Directory Service控制台导航窗格中，选择目录.
2. 在 Directories 页面上，选择您的目录 ID。
3. 在存储库的目录详细信息页面上，执行下列操作之一：
   - 如果你在下面显示了多个地区多区域复制，选择主要区域，然后选择维护选项卡。有关更多信息，请参阅 主要与其他地区 (p. 55)。
   - 如果您在下面没有显示任何区域多区域复制，选择维护选项卡。
4. 在架构扩展部分中，选择操作，然后选择上传和更新架构。
5. 在对话框中，单击 Browse，选择有效的 LDIF 文件，键入描述，然后选择 Update Schema。

   Important

   扩展架构是一项至关重要的操作。在开发或测试环境中使用您的应用程序对架构更新进行测试之前，请勿在生产环境中应用任何架构更新。

如何应用 LDIF 文件

在你的 LDIF 文件上传之后，Amazon当托管的 Microsoft AD 按以下顺序执行步骤来保护您的目录，以防在应用更改时出现错误。

1. 验证 LDIF 文件。由于 LDIF 脚本可以操纵域中的任何对象，Amazon上传后，托管的 Microsoft AD 将立即运行检查，以确保导入操作不会失败。其中包括用于确保以下事项的检查：
   - 要更新的对象仅保留在架构容器中
   - DC (域控制器) 部分与运行 LDIF 脚本所在域的名称匹配
2. 拍摄目录的快照。在更新架构后如果应用程序出现任何问题，可以使用该快照来还原目录。
3. 将更改应用到单个 DC。 Amazon托管的 Microsoft AD 将隔离其中一个 DC 并将 LDIF 文件中的更新应用于隔离的 DC。然后，它选择其中一个 DC 作为主架构，从目录复制中删除该 DC，并使用 `Ldifde.exe` 应用 LDIF 文件。
4. 复制将针对所有 DC 进行。 Amazon托管的 Microsoft AD 将隔离的 DC 重新添加到复制内容中，以完成更新。在执行这些操作的过程中，您的目录会继续为您的应用程序提供 Active Directory 服务，而不发生中断。

下一步

第 3 步：验证模式扩展是否成功 (p. 115)

第 3 步：验证模式扩展是否成功

完成导入过程后，需要验证架构更新是否已应用到您的目录中，这一点很重要。在迁移或更新依赖架构更新的任何应用程序之前，这一点尤其重要。您可以使用各种不同的 LDAP 工具或通过编写能够发出相应 LDAP 命令的测试工具来进行此验证。

此过程使用 Active Directory 架构管理单元和/或 PowerShell 来验证是否已应用架构更新。您必须从域加入的计算机上运行这些工具。Amazon托管的 Microsoft AD。这可以是本地网络中通过访问 Virtual Private Cloud (VPC) 或通过虚拟专用网络 (VPN) 连接运行的 Windows 服务器。您还可以在 Amazon EC2 Windows 实例上运行这些工具（请参阅如何启动带无缝域加入的新 EC2 实例)。

使用 Active Directory 架构管理单元进行验证

1. 根据 TechNet 网站中的说明安装 Active Directory 架构管理单元。
2. 打开 Microsoft 管理控制台 (MMC) 并展开目录的 AD 架构树。

3. 浏览 Classes 和 Attributes 文件夹，直至找到您以前所做的架构更改。

使用 PowerShell 进行验证

1. 打开 PowerShell 窗口。
2. 使用如下所示的 `Get-ADObject` cmdlet 来验证架构更改。例如：

```
get-adobject -Identity 'CN=Shoe-
Size,CN=Schema,CN=Configuration,DC=example,DC=com' -Properties *
```

可选步骤

(可选) 向新属性中添加值 (p. 116)

(可选) 向新属性中添加值

当您已在您的中创建新属性并且要向该属性中添加新值时，可使用此可选步骤。Amazon托管的 Microsoft AD 目录。

向属性中添加值

1. 打开 Windows PowerShell 命令行实用工具，并使用以下命令设置新属性。在本示例中，我们将向特定计算机的属性添加新的 EC2InstanceID 值。

```
PS C:\> set-adcomputer -Identity computer name -add @{example-EC2InstanceID
= 'EC2 instance ID'}
```

2. 可通过运行以下命令来验证是否已将 EC2InstanceID 值添加至计算机对象：

```
PS C:\> get-adcomputer -Identity computer name -Property example-
EC2InstanceID
```

相关资源

以下资源链接位于 Microsoft 网站上，并提供了相关信息。

- 扩展架构 (Windows)
- Active Directory 架构 (Windows)
- Active Directory 架构
- Windows 管理：扩展 Active Directory 架构
- 架构扩展限制 (Windows)
- Ldifde

维护您的AmazonMaged Microsoft AD 目录

此节介绍如何为您的维护常见管理任务。Amazon托管的 Microsoft AD 环境。

主题

- 添加备用 UPN 后缀 (p. 117)
- 删除目录 (p. 117)
- 重命名目录的站点名称 (p. 118)
- 快照或恢复你的目录 (p. 118)

- 查看目录信息 (p. 120)

添加备用 UPN 后缀

通过向您的备用户委托人名称 (UPN) 后缀添加备用户委托人名称 (UPN) 后缀，您可以简化 Active Directory (AD) 登录名的管理并改善用户登录体Amazon托管 Microsoft AD 目录。为此，应对管理员账户或是成员的账户Amazon用户委托人名称后缀委托管理员组中)。有关此组的更多信息，请参阅创建的内容 (p. 10)。

添加备用 UPN 后缀

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 找到将加入您的 Amazon EC2 实例所在位置Amazon托管 Microsoft AD 目录。选择该实例，然后选择 Connect (连接)。
3. 在 Server Manager (服务器管理器) 窗口中，选择 Tools (工具)。然后选择 Active Directory Domains and Trusts (Active Directory 域和信任)。
4. 在左侧窗格中，右键单击 Active Directory Domains and Trusts (Active Directory 域和信任)，然后选择 Properties (属性)。
5. 在 UPN Suffixes (UPN 后缀) 选项卡中，键入备用 UPN 后缀（如 **`sales.example.com`**）。选择 Add (添加)，然后选择 Apply (应用)。
6. 如果您需要添加其他备用 UPN 后缀，请重复步骤 5 直至您具有所需的 UPN 后缀。

删除目录

Simple AD 或AmazonMicrosoft Acte Director 目录，所有目录的连接，所有目录数据和快照都会删除，并且无法恢复。删除目录之后，加入到目录的所有实例都保持不变。但是，不能使用目录凭证登录这些实例。需要使用实例的本地用户账户登录这些实例。

删除 AD Connector 目录时，本地目录时，本地目录时，本地目录时，保持不变。加入到目录的所有实例也保持不变，并保持加入本地目录。仍可以使用目录凭证登录这些实例。

要删除目录

1. 在Amazon Directory Service控制台导航窗格中，选择目录.
2. 确保你没有使用多区域复制 (p. 54)用于要删除的目录。您必须先删除所有复制的区域，才能删除此目录时，才能删除此目录时，才能删除所有复制的区域。有关更多信息，请参阅 删除复制区域 (p. 58)。
3. 确保没有为目录启用任何 Amazon 应用程序。
   a. 在 Directories 页面上，选择您的目录 ID。
   b. 在 Directory details (目录详细信息) 页面上，选择 Application management (应用程序管理) 选项卡。在Amazon应用程序和服务部分，你可以看到哪个Amazon应用程序已为目录启用了应用程序。
      - 禁用 WorkSpaces，则必须从 WorkSpaces 控制台。有关更多信息，请参阅 。从目录中取消注册中的亚马逊 WorkSpaces 管理指南.
      - 禁用亚马逊 WorkSpaces 应用程序管理器，您必须在 Amazon WAM 控制台中删除所有应用程序分配。有关更多信息，请参阅 。删除所有应用程序分配中的Amazon WAM 管理指南.
      - 禁用亚马逊 WorkDocs，您必须删除Amazon，Amazon WorkDocs 亚马逊的站点 WorkDocs控制台。有关更多信息，请参阅 。删除站点中的亚马逊 WorkDocs 管理指南.
      - 禁用亚马逊 WorkMail，您必须移除亚马逊 WorkMail 亚马逊的组织 WorkMail 控制台。有关更多信息，请参阅 。删除组织中的亚马逊 WorkMail 管理员指南.
      - 禁用Amazon Web Services Management Console访问。
      - 要禁用 Amazon Relational Database Service，您必须从域中删除 Amazon RS Amazon RS Amazon RDS 有关更多信息，请参阅 。在域中管理数据库实例中的Amazon RDS 用户指南.

- 禁用亚马逊 QuickSight，您必须从Amazon 取消订阅 QuickSight. 有关更多信息，请参阅 。关闭 Amazon QuickSight 帐户中的亚马逊 QuickSight 用户指南.
- 要禁用 Amazon Connect，您必须删除Amazon Connect 实例。有关更多信息，请参阅 。删除 Amazon Connecter中的Amazon Connect.
- 要禁用 Amazon For Windows FSx ile Server er er er er er erver er er er erver er er er er erver er er er er er 有关更多信息，请参阅 。使用 Ave Server er er er erver er er er erver er er er中的Amazon FSx for Windows File Server.

  Note

  如果您将Amazon IAM Identity Center (successor to Amazon Single Sign-On)并且之前已将其连接到Amazon您计划删除的托管 Microsoft AD 目录，必须先删除它，然后才能删除它。有关更多信息，请参阅 。更改您的身份来源中的IAM 身份中心用户指南.

4. 在导航窗格中，选择 Directories。
5. 仅选择要删除的目录，然后单击Delete. 删除目录需要几分钟时间。目录删除之后，它会从目录列表中删除。

重命名目录的站点名称

您可以重命名您的Amazon获取托管的 Microsoft AD 目录的默认站点名称，以便它与您的现有 Microsoft Active Directory (AD) 站点名称匹配。这使得它更快Amazon您可以在您的本地目录中查找现有 AD 用户并对其进行身份验证。结果是用户登录时获得更好的体验Amazon资源，例如Amazon EC2和Amazon RDS for SQL Server你已加入你的实例Amazon托管的 Microsoft AD 目录。

为此，您必须使用 Admin (管理员) 账户或为 Amazon Delegated Sites and Services Administrators (站点和服务委托管理员) 组成员的账户登录。有关此组的更多信息，请参阅创建的内容 (p. 10)。

有关重命名与信任相关的站点的其他好处，请参阅 Microsoft 网站上的跨林信任的域定位器。

重命名Amazon托管的 Microsoft AD 站点名称

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 找到 Amazon EC2 加入您的Amazon托管的 Microsoft AD 目录。选择该实例，然后选择 Connect (连接)。
3. 在 Server Manager (服务器管理器) 窗口中，选择 Tools (工具)。然后选择 Active Directory Sites and Services (Active Directory 站点和服务)。
4. 在左侧窗格中，展开 Sites (站点) 文件夹，右键单击站点名称 (默认名称为 Default-Site-Name)，然后选择 Rename (重命名)。
5. 键入新的站点名称，然后选择 Enter。

快照或恢复你的目录

Amazon Directory Service让您拍摄数据的手动快照Amazon托管的 Microsoft AD 目录。这些快照可以用于执行 point-in-time 还原目录。无法拍摄 AD Connector 目录的快照。

Note

快照是一项全球性功能Amazon托管的 Microsoft AD。如果您在使用多区域复制 (p. 54)，必须在主 区域 (p. 55). 更改将自动应用于所有复制的区域。有关更多信息，请参阅 全球与区域功能 (p. 54)。

主题

- 创建目录的快照 (p. 119)
- 从快照还原目录 (p. 119)
- 删除快照 (p. 119)

创建目录的快照

快照可以用于将目录还原到拍摄快照的时间点时的状态。要创建目录的手动快照，请执行以下步骤。

> Note
>
> 对于每个目录，限制为 5 个手动快照。如果已达到此限制，必须先删除一个现有手动快照才能创建另一个快照。

创建手动快照

1. 在Amazon Directory Service控制台选择导航窗格，选择目录.
2. 在 Directories 页面上，选择您的目录 ID。
3. 在存储库的目录详细信息页面上，选择维护选项卡。
4. 在快照部分，选择操作选择，然后选择创建快照.
5. 在创建目录快照对话框中，提供快照的名称（如果需要）。准备就绪后，选择Create.

根据目录的大小，可能需要几分钟时间来创建快照。快照准备就绪之后，Status 值更改为 `Completed`。

从快照还原目录

从快照还原目录等效于将目录移动回到以前的时间。目录快照对于创建它们的目录来说是唯一的。快照只能恢复到创建快照的目录。此外，手动快照支持的最长期限为 180 天。有关更多信息，请参阅 Microsoft 网站上的 Active Directory 的系统状态备份的有用保质期。

> Warning
>
> 我们建议您联系Amazon Web Services SupportCenter在任何快照还原之前；我们或许能够帮助您避免执行快照还原的需要。任何快照还原都会导致数据丢失，因为它们是一些时间点。必须了解与目录关联的所有 DC 和 DNS 服务器会处于离线状态，直到还原操作完成。

要从快照还原目录，请执行以下步骤。

从快照还原目录

1. 在Amazon Directory Service控制台选择导航窗格，选择目录.
2. 在 Directories 页面上，选择您的目录 ID。
3. 在存储库的目录详细信息页面上，选择维护选项卡。
4. 在快照部分中，在列表中选择快照，然后选择操作选择，然后选择还原快照.
5. 查看中的信息还原目录快照对话框，然后选择还原.

对于Amazon还原 Microsoft AD 目录，可能需要两到三小时。成功还原之后，状态目录的值更改为`Active`. 会覆盖快照日期之后对目录进行的任何更改。

删除快照

如何删除快照

1. 在Amazon Directory Service控制台选择导航窗格，选择目录.

2. 在 Directories 页面上，选择您的目录 ID。
3. 在存储库的目录详细信息页面上，选择维护选项卡。
4. 在快照部分，选择操作选择，然后选择删除快照.
5. 确认您要删除快照，然后选择。Delete.

查看目录信息

您可以查看有关目录的详细信息。

查看详细目录信息

1. 在Amazon Directory Service控制台导航窗格中，选择目录.
2. 单击目录的目录 ID 链接。有关目录的信息显示在目录详细信息页.

有关 Status 字段的更多信息，请参阅了解您的目录状态 (p. 48)。

向用户和组授予访问权限Amazon资源

Amazon Directory Service能够为您的目录用户和组提供对的访问权限Amazon访问 Amazon EC2 控制台等服务和资源。类似于向 IAM 用户授予管理目录的访问权限，如中所述基于身份的策略（IAM policy）(p. 258)，以便目录中的用户能够访问其他Amazon资源，例如 Amazon EC2，您必须将 IAM 角色和策略分配给这些用户和组。有关更多信息，请参阅 IAM 用户指南中的 IAM 角色。

有关如何向用户授予对 Amazon Web Services Management Console的访问权限的信息，请参阅允许访问Amazon Web Services Management Console使用 AD 凭据 (p. 130)。

主题

- 创建新角色 (p. 120)
- 编辑现有角色的信任关系 (p. 121)
- 向现有角色分配用户或组 (p. 122)
- 查看已分配给角色的用户和组 (p. 122)
- 从角色中删除用户或组 (p. 123)
- 使用Amazon具有托管策略Amazon Directory Service (p. 123)

创建新角色

如果需要创建用于 Amazon Directory Service 的新 IAM 角色，必须使用 IAM 控制台来创建。在创建角色后，必须设置与该角色的信任关系，然后才能在 Amazon Directory Service 控制台中看到该角色。有关更多信息，请参阅 编辑现有角色的信任关系 (p. 121)。

> **Note**
>
> 执行此任务的用户必须有权执行以下 IAM 操作。有关更多信息，请参阅 基于身份的策略（IAM policy）(p. 258)。
>
> - iam:PassRole
> - iam:GetRole
> - iam:CreateRole
> - iam:PutRolePolicy

在 IAM 控制台中创建新角色

1. 在 IAM 控制台的导航窗格中，选择 Roles。有关更多信息，请参阅 。创建角色 (Amazon Web Services Management Console) 中的IAM 用户指南.
2. 选择 Create role（创建角色）。
3. 在 Choose the service that will use this role (选择将使用此角色的服务) 下面，选择 Directory Service，然后选择 Next (下一步)。
4. 选中您希望应用到目录用户的策略（例如，AmazonEC2FullAccess）旁边的复选框，然后选择 Next (下一步)。
5. 如有必要，将标签添加到该角色，然后选择 Next (下一步)。
6. 提供 Role name (角色名称) 和可选 Description (描述), 然后选择 Create role (创建角色)。

示例：创建角色以启用Amazon Web Services Management Console访问

以下核对清单提供了您创建新角色所必须完成的任务示例，该角色将向特定目录用户提供 Amazon EC2 控制台访问权限。

1. 使用上述过程用 IAM 控制台创建一个角色。当系统提示策略时，请选择 AmazonEC2FullAccess。
2. 使用 编辑现有角色的信任关系 (p. 121) 中的步骤来编辑刚刚创建的角色，然后将所需的信任关系信息添加到策略文档。要使角色在下一步骤中启用 Amazon Web Services Management Console 的访问权限后立即可见，需要完成此步骤。
3. 按 允许访问Amazon Web Services Management Console使用 AD 凭据 (p. 130) 中的步骤操作，配置 Amazon Web Services Management Console 的常规访问权限。
4. 按照 向现有角色分配用户或组 (p. 122) 中的步骤操作，将需要 EC2 资源的完全访问权限的用户添加到新角色。

编辑现有角色的信任关系

您可以将现有 IAM 角色分配至您的Amazon Directory Service用户和组。但要执行此操作，该角色必须与 Amazon Directory Service 具有信任关系。当您使用 Amazon Directory Service 通过创建新角色 (p. 120)中的步骤创建角色时，会自动设置此信任关系。您只需为不是由创建的 IAM 角色建立该信任关系Amazon Directory Service.

为现有角色建立与 Amazon Directory Service 的信任关系

1. 在 IAM 控制台的导航窗格中，选择 Roles。

   控制台显示您账户的角色。
2. 选择您要修改的角色的名称，然后在详细信息页面中选择 Trust relationships 选项卡。
3. 选择 Edit trust relationship (编辑信任关系)。
4. 在 Policy Document 下，粘贴以下内容，然后选择 Update Trust Policy。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "ds.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
```

```
}
```

您还可以使用 IAM CLI 更新此策略文档。有关更多信息，请参阅 。更新信任中的IAM 命令行参考.

向现有角色分配用户或组

您可以将现有 IAM 角色分配至Amazon Directory Service用户或组。该角色必须与 Amazon Directory Service 具有信任关系。有关更多信息，请参阅 编辑现有角色的信任关系 (p. 121)。

向现有 IAM 角色分配用户或组

1. 在 Amazon Directory Service 控制台导航窗格中，选择 Directories (目录)。
2. 在 Directories 页面上，选择您的目录 ID。
3. 在存储库的目录详细信息页面上，执行以下操作之一：
   - 如果你在下面显示了多个地区多区域复制中，选择要在其中进行作业的区域，然后选择要在其中执行作业的区域应用程序管理选项卡。有关更多信息，请参阅 主要与其他地区 (p. 55)。
   - 如果在下面没有显示任何区域多区域复制，选择应用程序管理选项卡。
4. 在Amazon Web Services Management Console位置在部分下委托控制台访问对于您要将用户分配到的现有 IAM 角色，选择 IAM 角色的 IAM 角色名称。如果尚未创建该角色，请参阅创建新角色 (p. 120)。
5. 在 Selected role (所选角色) 页面的 Manage users and groups for this role (管理此角色的用户和组) 下，选择 Add (添加)。
6. 在存储库的向角色添加用户和组页面，下选择 Active Directory 林中，选择Amazon托管 Microsoft AD 林 (此林) 或本地林 (受信任林)，也就是需要访问的账户所在林Amazon Web Services Management Console. 有关如何设置受信任林的更多信息，请参阅教程：在您之间创建信任关系Amazon托管微软 AD 和你的自我管理的 Active Directory 域 (p. 100)。
7. 在 Specify which users or groups to add (指定要添加的用户或组) 下，选择 Find by user (按用户查找) 或 Find by group (按组查找)，然后键入用户或组的名称。在可能匹配项的列表中，选择您要添加的用户或组。
8. 选择添加以完成向角色分配用户和组的工作。

   Note

   不支持目录中的嵌套组中的用户进行访问。父组的成员拥有控制台访问权限，但是子组成员不拥有。

查看已分配给角色的用户和组

要查看已分配给角色的用户和组，请执行以下步骤。

查看已分配给角色的用户和组

1. 在 Amazon Directory Service 控制台导航窗格中，选择 Directories (目录)。
2. 在 Directories 页面上，选择您的目录 ID。
3. 在存储库的目录详细信息页面上，执行以下操作之一：
   - 如果你在下面显示了多个地区多区域复制在区域中，选择要查看作业的区域，然后选择应用程序管理选项卡。有关更多信息，请参阅 主要与其他地区 (p. 55)。
   - 如果在下面没有显示任何区域多区域复制，选择应用程序管理选项卡。
4. 在Amazon Web Services Management Console在部分中，选择要查看的角色。
5. 在 Selected role (所选角色) 页面的 Manage users and groups for this role (管理此角色的用户和组) 下，您可以查看已分配给该角色的用户和组。

从角色中删除用户或组

要从角色中删除用户或组，请执行以下步骤。

从角色中删除用户或组

1. 在 Amazon Directory Service 控制台导航窗格中，选择 Directories (目录)。
2. 在 Directories 页面上，选择您的目录 ID。
3. 在存储库的目录详细信息页面上，执行以下操作之一：
   - 如果你在下面显示了多个地区多区域复制在区域中，选择要删除作业的区域，然后选择应用程序管理选项卡。有关更多信息，请参阅 主要与其他地区 (p. 55)。
   - 如果在下面没有显示任何区域多区域复制，选择应用程序管理选项卡。
4. 在Amazon Web Services Management Console在部分中，选择要查看的角色。
5. 在 Selected role (所选角色) 页面的 Manage users and groups for this role (管理此角色的用户和组) 下，选择要从该角色中删除的用户或组，然后选择 Remove (删除)。将从指定的用户和组中删除该角色，但不会从您的账户中删除该角色。

使用Amazon具有托管策略Amazon Directory Service

Amazon Directory Service提供以下功能Amazon向您的用户和组提供对访问权限的托管策略Amazon访问 Amazon EC2 控制台等服务和资源。您必须登录到 Amazon Web Services Management Console，然后才能查看这些策略。

- 只读访问权限
- 访问高级用户
- Amazon Directory Service全访问权限
- Amazon Directory Service只读访问权限
- 完全访问 Amazon Cloud Directory
- 访问 Amazon Cloud Directory
- 完全访问 Amazon EC2
- Amazon EC2 只读访问
- 完全访问 Amazon VPC
- 亚马逊 VPC 只读访问
- Amazon RDS 完全访问权限
- Amazon RDS 只读访问权限
- 完全访问 Amazon DynamoDB
- Amazon DynamoDB 只读访问
- Amazon S3 完全访问权限
- Amazon S3 只读访问
- Amazon CloudTrail全访问权限
- Amazon CloudTrail只读访问权限
- 完全访问 Amazon CloudWatch
- Amazon CloudWatch 只读访问
- 完全访问 Amazon CloudWatch Logs
- 访问 Amazon CloudWatch Logs

有关如何创建自己的策略的更多信息，请参阅管理策略示例Amazon资源中的IAM 用户指南.

启用访问权限Amazon应用程序和服务

Amazon Directory Service可以给其他AmazonAmazon WorkSpaces 等应用程序和服务 (如 Amazon WorkSpaces) 可以访问目录用户 以下Amazon可以启用或禁用应用程序和服务以使用Amazon Directory Service.

Amazon应用程序/服务	更多信息...
Amazon Chime	有关更多信息，请参阅 。Amazon Chime 管理指南.
Amazon Connect	有关更多信息，请参阅 。Amazon Connect 管理指南.
FSx for Windows File Server	有关更多信息，请参阅 。将 Amazon FSxAmazonMicrosoft Active Directory 的 Directory Service中的FSx for Windows File Server 用户指南.
Amazon QuickSight	有关更多信息，请参阅Amazon QuickSight 用户指南。
Amazon Relational Database Service	有关更多信息，请参阅 Amazon RDS 用户指南。
Amazon Transfer Family	有关更多信息，请参阅 Amazon Transfer Family 用户指南。
Amazon WorkDocs	有关更多信息，请参阅 。Amazon WorkDocs 管理指南.
Amazon WorkMail	有关更多信息，请参阅 。Amazon WorkMail 管理员指南.
WorkSpaces	你可以创建一个 Simple AD，Amazon直接从 WorkSpaces 托管微软 AD 或 AD Connector。只需在创建工作区时启动 Advanced Setup。 有关更多信息，请参阅 。Amazon WorkSpaces 管理指南.
Amazon WorkSpaces Application Manager	有关更多信息，请参阅 。Amazon WAM 管理指南.
Amazon Web Services Management Console	有关更多信息，请参阅 允许访问Amazon Web Services Management Console使用 AD 凭据 (p. 130)。

启用之后，可在要向其授予目录访问权限的应用程序或服务的控制台中管理对目录的访问。要查找Amazon上述应用程序和服务链接Amazon Directory Service控制台，请执行以下步骤。

显示适用于目录的应用程序和服务

1. 在 Amazon Directory Service 控制台导航窗格中，选择 Directories (目录)。
2. 在 Directories 页面上，选择您的目录 ID。
3. 在 Directory details (目录详细信息) 页面上，选择 Application management (应用程序管理) 选项卡。
4. 查看Amazon应用程序和服务部分。

主题

- 创建访问 URL (p. 125)

- 单点登录 (p. 125)

创建访问 URL

访问 URL 用于Amazon应用程序和服务 (如 Amazon WorkDocs) 用来访问与目录关联的登录页面。此 URL 必须全局唯一。可以通过执行以下步骤为目录创建访问 URL。

> **Warning**
>
> 一旦为此目录创建应用程序访问 URL，就无法更改它。创建访问 URL 之后，其他人便无法使用它。如果删除目录，则访问 URL 也会删除，随后可以由任何其他账户所使用。

> **Note**
>
> 访问 URL 是一项区域性功能Amazon管理 Microsoft AD。如果您在使用多区域复制 (p. 54)，必须在每个地区单独应用以下程序。有关更多信息，请参阅 全球与区域功能 (p. 54)。

创建访问 URL

1. 在Amazon Directory Service控制台选择导航窗格，选择目录.
2. 在 Directories 页面上，选择您的目录 ID。
3. 在存储库的目录详细信息页面上，执行下列操作之一：
   - 如果你在下面显示了多个地区多区域复制对于，选择要在其中创建访问 URL 的区域，然后选择应用程序管理选项卡。有关更多信息，请参阅 主要与其他地区 (p. 55)。
   - 如果没有在下面显示任何区域多区域复制，选择应用程序管理选项卡。
4. 在 Application access URL (应用程序访问 URL) 部分中，如果尚未向目录分配访问 URL，则会显示 Create (创建) 按钮。输入目录别名，然后选择 Create (创建)。如果实体已存在返回错误，则指定目录别名已分配。选择另一个别名并重复此过程。

   您的访问 URL 将以格式显示`<alias>`.awsapps.com。默认情况下，此 URL 将带您进入 Amazon WorkDocs 的登录页面。

单点登录

Amazon Directory Service提供允许您的用户访问亚马逊的能力 WorkDocs 从已加入目录的计算机中，而无需单独输入其凭证。

启用单点登录之前，您需要执行其他步骤，以便使用户可以支持单点登录。用户可能需要修改其 Web 浏览器设置来启用单点登录。

> **Note**
>
> 只有在已加入到 Amazon Directory Service 目录中的计算机上才支持单点登录。未加入目录中的计算机上无法使用单点登录。

如果您的目录是 AD Connector 目录，且 AD Connector 服务账户没有权限添加或删除其服务委托人名称属性，则对于下面的步骤 5 和 6，您有两个选项：

1. 您可以继续操作，系统将提示您输入具有以下权限的目录用户的用户名和密码：可在 AD Connector 服务账户上添加或删除服务委托人名称属性。这些凭证仅用于启用单点登录，不由服务进行存储。不会更改 AD Connector 服务账户权限。
2. 您可以委派权限以允许 AD Connector 服务账户在自身上添加或删除服务委托人名称属性，您可以运行以下 PowerShell 从加入域的计算机发出命令，该账户有权修改 AD Connector 服务账户的权限。以下命令将使 AD Connector 服务账户能够仅为其自身添加和删除服务委托人名称属性。

```
$AccountName = 'ConnectorAccountName'
```

```
# DO NOT modify anything below this comment.
# Getting Active Directory information.
Import-Module 'ActiveDirectory'
$RootDse = Get-ADRootDSE
[System.GUID]$ServicePrincipalNameGuid = (Get-ADObject -SearchBase
 $RootDse.SchemaNamingContext -Filter { lDAPDisplayName -eq 'servicePrincipalName' } -
Properties 'schemaIDGUID').schemaIDGUID
# Getting AD Connector service account Information.
$AccountProperties = Get-ADUser -Identity $AccountName
$AclPath = $AccountProperties.DistinguishedName
$AccountSid = New-Object -TypeName 'System.Security.Principal.SecurityIdentifier'
 $AccountProperties.SID.Value
# Getting ACL settings for AD Connector service account.
$ObjectAcl = Get-ACL -Path "AD:\$AclPath"
# Setting ACL allowing the AD Connector service account the ability to add and remove a
 Service Principal Name (SPN) to itself
$AddAccessRule = New-Object -TypeName 'System.DirectoryServices.ActiveDirectoryAccessRule'
 $AccountSid, 'WriteProperty', 'Allow', $ServicePrincipalNameGUID, 'None'
$ObjectAcl.AddAccessRule($AddAccessRule)
Set-ACL -AclObject $ObjectAcl -Path "AD:\$AclPath"
```

使用亚马逊启用或禁用单点登录 WorkDocs

1. 在Amazon Directory Service控制台导航窗格中，选择。目录.
2. 在 Directories 页面上，选择您的目录 ID。
3. 在 Directory details (目录详细信息) 页面上，选择 Application management (应用程序管理) 选项卡。
4. 在应用程序访问 URL部分，选择。启用为亚马逊启用单点登录 WorkDocs.

   如果您没有看到启用按钮，则可能需要首先创建访问 URL，然后才能显示此选项。有关如何创建访问 URL 的更多信息，请参阅创建访问 URL (p. 125)。
5. 在为此目录启用单点登录对话框中，选择。启用. 单点登录已为目录启用。
6. 如果您以后想禁用Amazon 单点登录 WorkDocs，选择禁用，然后在禁用单点登录对话框中，选择。禁用。

主题

- IE 和 Chrome 的单点登录 (p. 126)
- Firefox 的单点登录 (p. 129)

IE 和 Chrome 的单点登录

要使 Microsoft Internet Explorer (IE) 和 Google Chrome 浏览器可以支持单点登录，必须在客户端计算机上执行以下任务：

- 添加您的访问网址（例如 https://*<alias>*.awsapps.com) 添加到适用于单点登录的经审批站点列表中。
- 启用活动脚本 (JavaScript)。
- 允许自动登录。
- 启用集成身份验证。

您或您的用户手动执行这些任务，也可以使用组策略设置更改这些设置。

主题

- Windows 上的单点登录 (p. 127)
- OS X 上的单点登录 (p. 127)
- Single Sign-On 的组策略设置 (p. 128)

Windows 上的单点登录

要在 Windows 计算机上手动启用单点登录，请在客户端计算机上执行以下步骤。其中一些设置可能已正确设置。

在 Windows 上为 Internet Explorer 和 Chrome 手动启用单点登录

1. 要打开 Internet Properties 对话框，请选择 Start 菜单，在搜索框中键入 `Internet Options`，然后选择 Internet Options。
2. 通过执行以下步骤将访问 URL 添加到适用于单点登录的经审批站点列表中：
   a. 在 Internet Properties 对话框中选择 Security 选项卡。
   b. 选择 Local intranet，然后选择 Sites。
   c. 在 Local intranet 对话框中，选择 Advanced。
   d. 将访问 URL 添加到网站列表，然后选择 Close。
   e. 在 Local intranet 对话框中，选择 OK。
3. 要启用活动脚本，请执行以下步骤：
   a. 在 Internet Properties 对话框的 Security 选项卡中，选择 Custom level。
   b. 在 Security Settings - Local Intranet Zone 对话框中，向下滚动到 Scripting，然后在 Active scripting 下选择 Enable。
   c. 在 Security Settings - Local Intranet Zone 对话框中，选择 OK。
4. 要启用自动登录，请执行以下步骤：
   a. 在 Internet Properties 对话框的 Security 选项卡中，选择 Custom level。
   b. 在 Security Settings - Local Intranet Zone 对话框中，向下滚动到 User Authentication 并在 Logon 下选择 Automatic logon only in Intranet zone。
   c. 在 Security Settings - Local Intranet Zone 对话框中，选择 OK。
   d. 在 Security Settings - Local Intranet Zone 对话框中，选择 OK。
5. 要启用集成身份验证，请执行以下步骤：
   a. 在 Internet Properties 对话框中选择 Advanced 选项卡。
   b. 向下滚动到 Security，然后选择 Enable Integrated Windows Authentication。
   c. 在 Internet Properties 对话框中，选择 OK。
6. 关闭并重新打开浏览器让这些更改生效。

OS X 上的单点登录

要在 OS X 上为 Chrome 手动启用单点登录，请在客户端计算机上执行以下步骤。需要计算机上的管理员权限才能完成这些步骤。

在 OS X 上为 Chrome 手动启用单点登录

1. 将访问 URL 添加到AuthServerWhitelist通过运行以下命令执行策略：

```
defaults write com.google.Chrome AuthServerWhitelist "https://<alias>.awsapps.com"
```

2. 打开 System Preferences，转到 Profiles 面板，然后删除 `Chrome Kerberos Configuration` 配置文件。
3. 重新启动 Chrome，然后在 Chrome 中打开 chrome://policy 以确认新设置已实施。

Single Sign-On 的组策略设置

域管理员可以实施组策略设置以在加入域的客户端计算机上进行单点登录更改。

> **Note**
>
> 如果您在域中的计算机上使用 Chrome 策略管理 Chrome Web 浏览器，则必须将访问 URL 添加到AuthServerWhitelist政策。有关设置 Chrome 策略的更多信息，请转到 Policy Settings in Chrome。

使用组策略设置为 Internet Explorer 和 Chrome 启用单点登录

1. 通过执行以下步骤创建新的组策略对象：
   a. 打开组策略管理工具，导航到您的域并选择 Group Policy Objects。
   b. 在主菜单中，选择 Action，然后选择 New。
   c. 在新 GPO对话框中，请输入组策略对象的描述性名称，例如`IAM Identity Center Policy`，然后离开来源 Starter GPO设置为(无). 单击 OK（确定）。
2. 通过执行以下步骤将访问 URL 添加到适用于单点登录的经审批站点列表中：
   a. 在组策略管理工具中，导航到您的域，选择。组策略对象，打开 IAM Identity Center 策略的上下文（右键单击）菜单，然后选择。编辑.
   b. 在策略树中，导航到 User Configuration > Preferences > Windows Settings。
   c. 在 Windows Settings 列表中，打开 Registry 的上下文 (右键单击) 菜单并选择 New registry item。
   d. 在 New Registry Properties 对话框中，输入以下设置，然后选择 OK：

      Action

      ```
      Update
      ```

      Hive

      ```
      HKEY_CURRENT_USER
      ```

      路径

      ```
      Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap
      \Domains\awsapps.com\<alias>
      ```

      的值`<alias>`派生自访问 URL。如果访问 URL 是 `https://examplecorp.awsapps.com`，则别名是 `examplecorp`，注册表项是 `Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Domains\awsapps.com\examplecorp`。

      Value name

      ```
      https
      ```

      值类型

      ```
      REG_DWORD
      ```

      Value data

      ```
      1
      ```
3. 要启用活动脚本，请执行以下步骤：
   a. 在组策略管理工具中，导航到您的域，选择。组策略对象，打开 IAM Identity Center 策略的上下文（右键单击）菜单，然后选择。编辑.
   b. 在策略树中，导航到 Computer Configuration > Policies > Administrative Templates > Windows Components > Internet Explorer > Internet Control Panel > Security Page > Intranet Zone。

c. 在 Intranet Zone 列表中，打开 Allow active scripting 的上下文 (右键单击) 菜单，选择 Edit。
d. 在 Allow active scripting 对话框中，输入以下设置，然后选择 OK：
   - 选择 Enabled 单选按钮。
   - 在 Options 下，将 Allow active scripting 设置为 Enable。

4. 要启用自动登录，请执行以下步骤：
   a. 在组策略管理工具中，导航到您的域，选择“Group Policy Objects”，打开 SSO 策略的上下文 (右键单击) 菜单，然后选择 Edit。
   b. 在策略树中，导航到 Computer Configuration > Policies > Administrative Templates > Windows Components > Internet Explorer > Internet Control Panel > Security Page > Intranet Zone。
   c. 在 Intranet Zone 列表中，打开 Logon options 的上下文 (右键单击) 菜单，选择 Edit。
   d. 在 Logon options 对话框中，输入以下设置，然后选择 OK：
      - 选择 Enabled 单选按钮。
      - 在 Options 下，将 Logon options 设置为 Automatic logon only in Intranet zone。
5. 要启用集成身份验证，请执行以下步骤：
   a. 在组策略管理工具中，导航到您的域，选择。组策略对象，打开 IAM Identity Center 策略的上下文（右键单击）菜单，然后选择。编辑.
   b. 在策略树中，导航到 User Configuration > Preferences > Windows Settings。
   c. 在 Windows Settings 列表中，打开 Registry 的上下文 (右键单击) 菜单并选择 New registry item。
   d. 在 New Registry Properties 对话框中，输入以下设置，然后选择 OK：

      Action

      ```
      Update
      ```

      Hive

      ```
      HKEY_CURRENT_USER
      ```

      路径

      ```
      Software\Microsoft\Windows\CurrentVersion\Internet Settings
      ```

      Value name

      ```
      EnableNegotiate
      ```

      值类型

      ```
      REG_DWORD
      ```

      Value data

      ```
      1
      ```
6. 如果 Group Policy Management Editor 窗口仍打开，关闭该窗口。
7. 通过执行以下步骤将新策略分配给您的域：
   a. 在组策略管理树中，打开您的域的上下文 (右键单击) 菜单，然后选择 Link an Existing GPO。
   b. 在组策略对象列表中，选择 IAM 身份中心策略，然后选择。确定.

这些更改会在客户端上的下一次策略更新之后，或是在下次用户登录时生效。

Firefox 的单点登录

要使 Mozilla Firefox 浏览器可以支持单点登录，请添加访问 URL (例如 https://*<alias>*.awsapps.com) 添加到适用于单点登录的经审批站点列表中。这可以手动执行，也可以使用脚本自动进行。

主题

- Single Sign-On 的手动更新 (p. 130)
- Single Sign-On 的自动更新 (p. 130)

Single Sign-On 的手动更新

要在 Firefox 中将访问 URL 手动添加到经审批站点列表中，请在客户端计算机上执行以下步骤。

在 Firefox 中将访问 URL 手动添加到经审批站点列表中

1. 打开 Firefox，然后打开 `about:config` 页面。
2. 打开`network.negotiate-auth.trusted-uris`首选项，然后将访问 URL 添加到站点列表中。使用逗号 (,) 分隔多个条目。

Single Sign-On 的自动更新

作为域管理员，可以使用脚本将访问 URL 添加到 Firefox`network.negotiate-auth.trusted-uris`网络中所有计算机上的用户首选项。有关更多信息，请转到 https://support.mozilla.org/en-US/questions/939037。

允许访问Amazon Web Services Management Console使用 AD 凭据

Amazon Directory Service 允许向目录的成员授予 Amazon Web Services Management Console访问权限。默认情况下，目录成员无权访问任何 Amazon 资源。可将 IAM 角色分配给目录成员，以便向其授予各种Amazon服务和资源。IAM 角色定义目录成员所拥有的服务、资源和访问权限级别。

目录必须首先具有访问 URL，然后您才能向目录成员授予控制台访问权限。有关如何查看目录详细信息和获取访问 URL 的更多信息，请参阅查看目录信息 (p. 120). 有关如何创建访问 URL 的更多信息，请参阅创建访问 URL (p. 125)。

有关如何创建 IAM 角色以及将它们分配给目录成员的更多信息，请参阅向用户和组授予访问权限Amazon资源 (p. 120).

主题

- 启用Amazon Web Services Management Console访问 (p. 130)
- 禁用Amazon Web Services Management Console访问 (p. 131)
- 设置登录会话长度 (p. 131)

相关Amazon安全博客文章

- 如何访问Amazon Web Services Management Console使用Amazon托管微软 AD 和你的本地凭证

> **Note**
>
> 对Amazon Web Services Management Console是的区域特征Amazon托管微软 AD。如果您在使用多区域复制 (p. 54)，必须在每个地区单独应用以下程序。有关更多信息，请参阅 全球与区域功能 (p. 54)。

启用Amazon Web Services Management Console访问

默认情况下，不会为任何目录启用控制台访问。要为目录用户和组启用控制台访问，请执行以下步骤：

启用控制台访问

1. 在 Amazon Directory Service 控制台导航窗格中，选择 Directories (目录)。
2. 在 Directories 页面上，选择您的目录 ID。
3. 在存储库的目录详细信息页面上，执行以下操作之一：
   - 如果你在下面显示了多个地区多区域复制中，选择要在其中允许访问Amazon Web Services Management Console，然后选择应用程序管理选项卡。有关更多信息，请参阅 主要与其他地区 (p. 55)。
   - 如果您在下面没有显示任何区域多区域复制，选择应用程序管理选项卡。
4. 在Amazon Web Services Management Console部分中，选择启用. 控制台访问现在已为目录启用。

   必须先将用户添加到角色中，然后用户才能使用访问 URL 登录控制台。有关将用户分配给 IAM 角色的一般信息，请参阅向现有角色分配用户或组 (p. 122). 分配 IAM 角色之后，用户可以使用访问 URL 访问控制台。例如，如果目录访问 URL 是例如 corp.awsapps.com，则用于访问控制台的 URL 是 https://example-corp.awsapps.com/console/。

禁用Amazon Web Services Management Console访问

要为目录用户和组禁用控制台访问，请执行以下步骤：

禁用控制台访问

1. 在 Amazon Directory Service 控制台导航窗格中，选择 Directories (目录)。
2. 在 Directories 页面上，选择您的目录 ID。
3. 在存储库的目录详细信息页面上，执行以下操作之一：
   - 如果你在下面显示了多个地区多区域复制对于区域，选择要在其中禁用访问Amazon Web Services Management Console，然后选择应用程序管理选项卡。有关更多信息，请参阅 主要与其他地区 (p. 55)。
   - 如果您在下面没有显示任何区域多区域复制，选择应用程序管理选项卡。
4. 在Amazon Web Services Management Console部分中，选择禁用. 控制台访问现在已为目录禁用。
5. 如果有任何 IAM 角色已分配给目录中的用户或组，则禁用按钮可能不可用。在这种情况下，您必须删除目录的所有 IAM 角色分配再继续，包括您目录中已删除的用户或组的分配，这将显示为删除的用户要么删除组.

   删除所有 IAM 角色分配之后，重复以上步骤。

设置登录会话长度

默认情况下，用户在成功登录控制台之后以及注销之前，有 1 小时时间可使用其会话。在此之后，用户必须再次登录才能开始下一个 1 小时会话，然后再次注销。可以使用以下过程对每个会话将时间长度更改为最长 12 小时。

设置登录会话长度

1. 在 Amazon Directory Service 控制台导航窗格中，选择 Directories (目录)。
2. 在 Directories 页面上，选择您的目录 ID。
3. 在存储库的目录详细信息页面上，执行以下操作之一：
   - 如果你在下面显示了多个地区多区域复制中，选择要在其中设置登录会话长度的区域，然后选择应用程序管理选项卡。有关更多信息，请参阅 主要与其他地区 (p. 55)。
   - 如果您在下面没有显示任何区域多区域复制，选择应用程序管理选项卡。

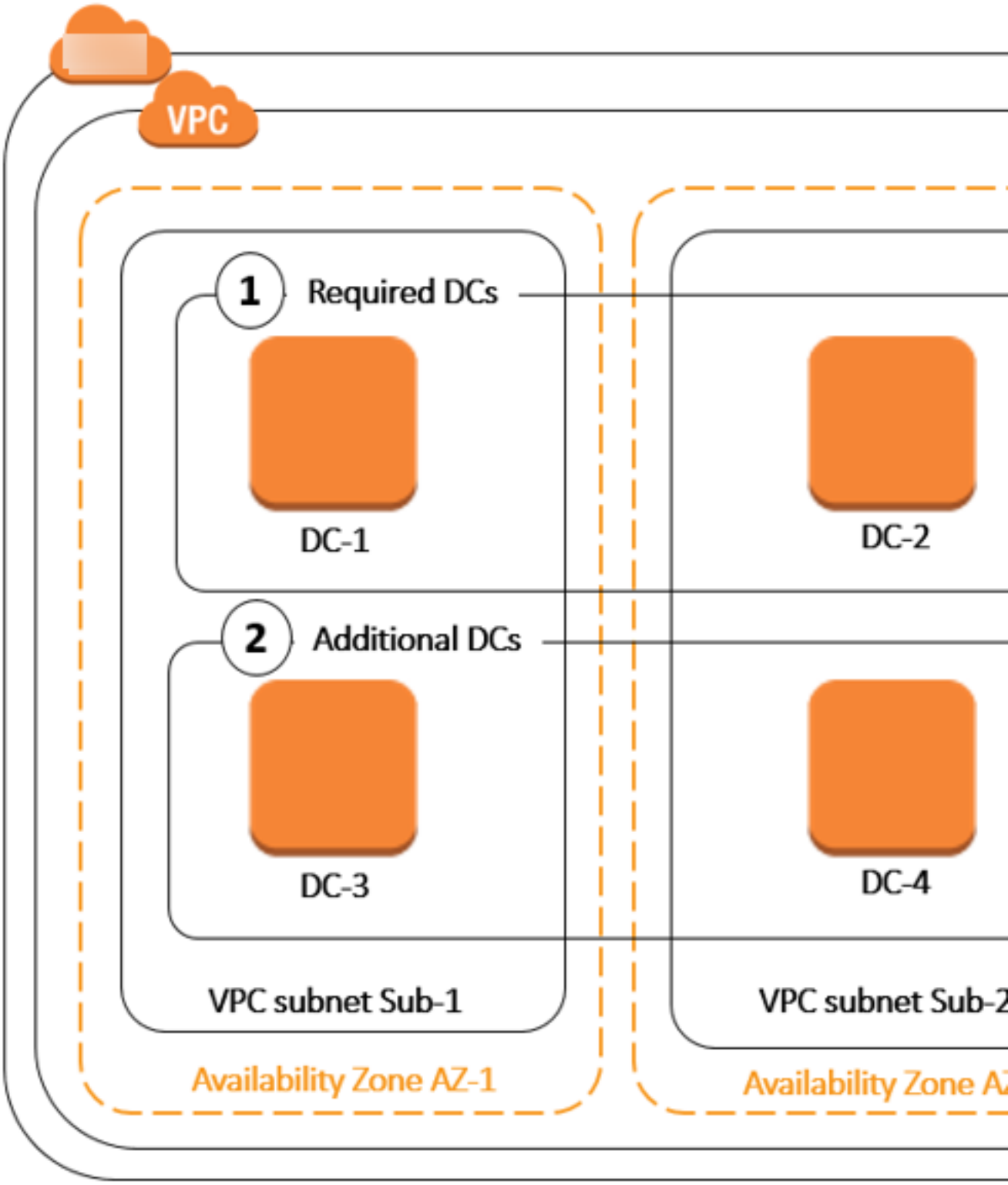
4. 在Amazon应用程序和服务部分中，选择Amazon管理控制台.
5. 在管理对 的访问Amazon资源对话框中，选择。Continue.
6. 在 Assign users and groups to IAM roles 页面中的 Set login session length 下方，编辑编号的值，然后选择 Save。

部署额外的域控制器

部署额外的域控制器将增加冗余度，从而提供更好的恢复能力和更高的可用性。这种做法还可以通过支持更多的 Active Directory 请求，改善目录的性能。例如，您现在可以使用Amazon托管微软 AD，支持部署在大量 Amazon EC2 和 Amazon RDS for SQL Server 实例上的多个 .NET 应用程序。

当你第一次创建目录时，Amazon在多个可用区中，托管的 Microsoft AD 部署两个域控制器，这是实现高可用性目的所必需的。之后，您可以通过Amazon Directory Service控制台只需指定所需域控制器的总数。Amazon托管的 Microsoft AD 会向其上正在运行您的目录的可用区和 VPC 子网分配额外的域控制器。

例如，在下图中，DC-1 和 DC-2 代表最初随您的目录一起创建的两个域控制器。这些区域有：Amazon Directory Service控制台将这些默认域控制器称为必需.Amazon 在目录创建过程中，托管 Microsoft AD 特意将各个域控制器放入分隔的可用区中。之后，您可能决定添加另两个域控制器，以帮助分布峰值登录时间的身份验证负载。DC-3 和 DC-4 均表示新的域控制器，在控制台中，现在将它们表示为额外控制器。和以前一样，Amazon托管 Microsoft AD 会再次自动将新域控制器放置在不同的可用区中，以确保您的域的高可用性。



通过此过程，您将不再需要手动配置目录数据复制、自动化每日快照或对额外域控制器进行监控。此外，您可以更轻松地在Amazon云无需部署和维护自己的 Active Directory 基础架构。您还可以针对以下部署或删除额外的域控制器Amazon使用UpdateNumberOfDomainControllersAPI。

Note

额外的域控制器是Amazon托管的 Microsoft AD。如果您在使用多区域复制 (p. 54)，必须在每个地区单独应用以下程序。有关更多信息，请参阅 全球与区域功能 (p. 54)。

添加或删除额外的域控制器

使用以下过程可在您的中部署或删除额外的域控制器。Amazon托管的 Microsoft AD 目录。

Note

如果你已经配置了Amazon托管的 Microsoft AD 来启用 LDAPS，则您添加的任意额外域控制器也会自动启用 LDAPS。有关更多信息，请参阅 启用安全 LDAP (LDAPS) (p. 30)。

添加或删除额外的域控制器

1. 在 Amazon Directory Service 控制台导航窗格中，选择 Directories (目录)。
2. 在 Directories 页面上，选择您的目录 ID。
3. 在存储库的目录详细信息页面上，请执行以下操作之一：
   - 如果你在下面显示了多个地区多区域复制中，选择要在其中添加或删除域控制器的区域，然后选择扩展和共享选项卡。有关更多信息，请参阅 主要与其他地区 (p. 55)。
   - 如果您没有在下面显示任何区域多区域复制，选择扩展和共享选项卡。
4. 在 Domain controllers (域控制器) 部分中，选择编辑。
5. 指定要在您的目录中添加或删除的域控制器数量，然后选择 Modify (修改)。
6. 何时Amazon托管 Microsoft AD 完成了部署过程，所有域控制器都显示处于活动状态状态，并出现分配的可用区和 VPC 子网。新的域控制器会均等地分布在已部署您的目录的可用区和子网中。

Note

在部署额外的域控制器后，您可以将域控制器的数量减少为两个，这是实现容错和高可用性目的所需的最小数量。

相关的Amazon安全博客文章

- 如何提高您的冗余度和性能Amazon Directory Service为了Amazon通过添加域控制器来管理 Microsoft AD

使用 Amazon CloudWatch 指标来确定何时添加域控制器

在所有域控制器之间进行负载均衡对于目录的恢复能力和性能非常重要。为了帮助您优化域控制器的性能Amazon托管 Microsoft AD，我们建议你首先监控 CloudWatch 中的重要指标以形成基准。在此过程中，您随着时间的推移分析目录以确定平均目录利用率和峰值目录利用率。确定基准后，您可以定期监控这些指标，以帮助确定何时向目录中添加域控制器。有关更多信息，请参阅 使用性能指标监控域控制器 (p. 53)。

定期监控以下指标很重要。有关 CloudWatch 中可用域控制器指标的完整列表，请参阅。Amazon托管的 Microsoft AD 性能计数器 (p. 135).

- 域控制器特定的指标，例如：
  - 处理器
  - 内存
  - 逻辑磁盘
  - 网络接口

- Amazon托管 Microsoft AD 目录特定的指标，例如：
  - LDAP 搜索
  - 绑定
  - DNS 查询
  - 目录读
  - 写入目录

有关如何使用 CloudWatch 控制台设置域控制器指标的说明，请参阅。如何自动化Amazon基于利用率指标托管 Microsoft AD 扩展中的Amazon安全博客。有关 CloudWatch 中的指标的一般信息，请参阅。使用 Amazon CloudWatch 指标中的Amazon CloudWatch 用户指南.

有关域控制器规划的一般信息，请参阅。Active Directory 域服务的容量规划在 Microsoft 网站上。

Amazon托管的 Microsoft AD 性能计数器

下表列出了 Amazon CloudWatch 中可用于跟踪域控制器和目录性能的所有性能计数器Amazon托管的 Microsoft AD。

指标类别	指标名称
数据库 ==> 实例 (NTDSA)	数据库缓存% 命中
	I/O 数据库读取平均延迟
	I/O数据库读取数/秒
	I/O 日志写入平均延迟
目录服务 (NTDS)	LDAP 绑定时间
	DRA 挂起的复制操作
	DRA 挂起的复制同步
DNS	Processage Sent/秒
	递归查询失败/秒
	PCT查询Receives/秒
	Processage
	Message Sent/秒
	MUDP 查询Receiv/秒
LogicalDisk	平均。Disk Queue Length
	% 可用空间
内存	使用中的已承诺字节数
	长期平均备用缓存寿命
网络接口	Message Sent/秒
	Bytes Received/sec
	当前的带宽

指标类别	指标名称
NTDS	ATQ 预计队列延迟
	ATQ 请求延迟
	DDS Directory Reads/秒
	DS 目录搜索/秒
	D目录写入/秒
	LDAP 客户端会话
	LDAP 搜索/秒
	LDAP 成功绑定/秒
处理器	% Processage
安全全系统统计	Kerberos 身份验证
	NTLM 身份验证

将用户从 Active Directory 迁移到Amazon托管的 Microsoft AD

您可以使用 Active Directory 迁移工具包 (ADMT) 和密码导出服务 (PES) 将用户从自托管 AD 迁移到Amazon托管的 Microsoft AD 目录。这使您能够更轻松地为用户迁移 AD 对象和加密密码。

有关详细说明，请参阅如何将本地域迁移到Amazon使用 ADMT 托管 Microsoft AD在Amazon安全博客.

的最佳实践Amazon托管的 Microsoft AD

为避免问题并充分利用，您应该考虑以下建议和准则。Amazon托管的 Microsoft AD。

设置：先决条件

创建目录之前请考虑以下这些准则。

验证你有正确的目录类型

Amazon Directory Service 提供了多种方式来结合使用 Microsoft Active Directory 与其他 Amazon 服务。您可以根据预算成本选择具有适当功能的目录服务以满足您的需求：

- AmazonMicrosoft Directory Service Directory是一种功能丰富的托管 Microsoft Active Directory，托管在Amazon云。Amazon如果您的用户数超过 5000，并且需要在某些用户数之间建立信任关系，则托管 Microsoft AD 是您的最佳选择。Amazon和本地目录。
- AD Connector将现有本地 Active Directory 直接连接到Amazon. 当您想要将现有本地目录与Amazon服务。
- Simple AD是具有常用目录功能并与 Active Directory 兼容的低成本服务。在大多数情况下，Simple AD 是成本最低的选择，如果您的用户数不超过 5000，并且不需要更高级的 Microsoft Active Directory 功能，这是您的最佳选择。

有关 Amazon Directory Service 选项的更详细比较，请参阅选择哪一个 (p. 1)。

确保您的 VPC 和实例配置正确

要连接到、管理和使用目录，必须正确配置目录所关联的 VPC。或者请参阅AmazonMicrosoft AD (p. 8)、AD Connetor (p. 171)，或者Simple AD 先决条件 (p. 209)有关 VPC 安全和网络要求的信息。

如果要将实例添加到域，请确保您具有实例连接并且可以远程访问实例，如将 EC2 实例加入Amazon托管的 Microsoft AD 目录 (p. 66) 中所述。

请注意自己的限制

了解特定目录类型的各种限制。对象的可用存储空间和总大小是对象可以存储在目录中的对象数量的唯一限制。或者请参阅AmazonManaged Microsoft AD 配额 (p. 141)、AD Connector 配额 (p. 205)，或者Simple AD 配额 (p. 250)有关您选择目录的详细信息。

了解你的目录Amazon安全组配置和使用

Amazon创建安全组并将其附加到目录的域控制器弹性网络接口. 此安全组阻止传向域控制器的不必要流量，允许 Active Directory 通信所必需的流量通过。Amazon将安全组配置为仅打开 Active Directory 通信所需的端口。在默认配置中，安全组接受从任意 IP 地址到这些端口的流量。Amazon将安全组附加到您的域控制器接口，可从您的、对等的或调整大小的接口访问该接口。VPC. 即使您修改路由表、更改与 VPC 的网络连接以及配置 NAT 网关服务，这些接口也无法从 Internet 访问。因此，只有具有指向 VPC 的网络路径的实例和计算机可以访问目录。这消除了配置特定地址范围的需求，从而简化了设置。而您只需要配置到 VPC 的路由和安全组，使其仅允许来自可信实例和计算机的流量。

修改目录安全组

如果您希望提升目录安全组的安全性，可以修改它们，接受来自更严格控制的 IP 地址列表的流量。例如，您可以将接受的地址从 0.0.0.0/0 更改为特定于单个子网或计算机的 CIDR 范围。同样，您可以选择将目标地址限制为您的域控制器可以与之通信的地址。只有在您完全了解安全组的筛选如何工作时，才进行这样的更改。有关更多信息，请参阅 。适用于 Linux 实例的 Amazon EC2 安全组中的Amazon EC2 用户指南. 不正确的更改可能会导致丢失与目标计算机和实例的通信。Amazon为了降低您目录的安全性，不要尝试打开到域控制器的其他端口。请仔细查看Amazon责任共担模式.

> **Warning**
>
> 从技术上来说，您可以将目录使用的安全组与您创建的其他 EC2 实例关联。但是，Amazon建议不要采用这种做法。Amazon可能会由于某些原因在未经通知的情况下修改安全组，以满足托管目录的功能或安全需求。此类更改会影响目录安全组相关联的任何实例。此外，将目录安全组与您的 EC2 实例关联起来会导致 EC2 实例潜在的安全风险。目录安全组在所需 Active Directory 端口上接收来自任何 IP 地址流量。如果您将此安全组与 EC2 实例关联而该实例具有连接到 Internet 的公共 IP 地址，则 Internet 上的任意计算机都可以在开放端口上与 EC2 实例通信。

设置：创建目录

下面是创建目录时应考虑的一些建议。

记住管理员 ID 和密码

设置目录时，需要提供管理员账户的密码。该账户 ID管理员为了Amazon托管的 Microsoft AD。请记住为此账户创建的密码；否则无法向您的目录中添加对象。

创建 DHCP 选项集

我们建议为 Amazon Directory Service 目录创建 DHCP 选项集并将 DHCP 选项集分配给该目录所在的 VPC。这样，该 VPC 中的任何实例都可以指向指定域，并且 DNS 服务器可以解析其域名。

有关 DHCP 选项集的更多信息，请参阅 创建 DHCP 选项集 (p. 92)。

部署额外的域控制器

默认情况下，Amazon创建两个域控制器，它们存在于单独的可用区中。在软件修补期间以及出现其他事件导致一个域控制器无法访问或不可用时，这提供了故障恢复能力。我们建议您部署额外的域控制器，以进一步提高恢复能力，并在出现较长期事件影响对某个域控制器或某个可用区的访问时，确保向外扩展性能。

有关更多信息，请参阅 使用 Windows DC 定位器服务 (p. 140)。

了解用户名限制Amazon应用程序

Amazon Directory Service 支持大多数可用于构造用户名的字符格式。但是，对于登录到所用的用户名有一些字符限制。Amazon应用程序，例如 WorkSpaces, Amazon WorkDocs, Amazon WorkMail或 Amazon QuickSight. 这些限制要求不使用以下字符：

- 空格
- 多字节字符
- !"#$%&'()*+,/:;<=>?@[\]^`{|}~

> Note
>
> 仅允许在 UPN 后缀之前使用 @ 符号。

使用目录

下面是使用目录时应记住的一些建议。

不要更改预定义的用户、组和组织单位

使用 Amazon Directory Service 启动目录时，Amazon 会创建一个包含所有目录对象的组织部门 (OU)。此 OU (具有您在创建目录时键入的 NetBIOS 名称) 位于域根目录中。此域根目录由 Amazon 拥有和管理。还会创建几个组和一个管理用户。

不要移动、删除或以任何其他方式更改这些预定义对象。否则，可能会使您自己和 Amazon 都无法访问您的目录。有关更多信息，请参阅 创建的内容 (p. 10)。

自动加入域

启动属于 Amazon Directory Service 域的一部分的 Windows 实例时，最简单的方法通常是在实例创建过程中加入域而不是在以后手动添加实例。要自动加入域，只需在启动新实例时为 Domain join directory 选择正确的目录。可以在无缝地联接 Windows EC2 实例 (p. 66) 中找到详细信息。

正确设置信托

在你之间建立信任关系时Amazon请记住以下准则：

- 信任类型必须在两侧匹配（林或外部）
- 如果使用单向信任（在信任域上传出、在信任域上传入），请确保正确设置信任方向。
- 完全限定域名 (FQDN) 和 NetBIOS 名称在林/域之间都必须唯一

有关设置信任关系的更多详细信息和特定说明，请参阅创建信任关系 (p. 96)。

管理目录

请考虑以下用于管理目录的建议。

跟踪域控制器的性能

为了帮助优化扩展决策并提高目录恢复能力和性能，我们建议您使用 CloudWatch 指标。有关更多信息，请参阅 使用性能指标监控域控制器 (p. 53)。

有关如何使用设置域控制器指标的说明 CloudWatch 控制台，请参阅如何自动化Amazon基于利用率指标托管 Microsoft AD 扩展中的Amazon安全博客。

仔细规划架构扩展

应用架构扩展时进行周全考虑，针对重要和频繁的查询为您的目录编制索引。慎重使用以免为目录过度地编制索引，因为索引将占用目录空间并且快速更改的索引值可能会导致性能问题。要添加索引，您必须创建一个轻型目录访问协议 (LDAP) 目录交换格式 (LDIF) 文件并扩展您的架构更改。有关更多信息，请参阅 扩展你的架构 (p. 111)。

关于负载均衡器

请勿在前面使用负载均衡器Amazon托管微软 AD 端点。Microsoft 设计了与域控制器 (DC) 发现算法 (查找在无外部负载平衡的情况下最易响应的运行 DC) 一起使用的 Active Directory (AD)。外部网络负载均衡器不正确地检测活动 DC，可能会导致您的应用程序发送给将出现、但未做好使用准备的 DC。有关更多信息，请参阅 。负载均衡器和活动目录在 Microsoft TechNet 建议修复应用程序以正确使用 AD 而不是实施外部负载均衡器。

备份实例

如果决定将实例手动添加到现有 Amazon Directory Service 域，请先对该实例创建备份或拍摄快照。这在加入 Linux 实例时尤其重要。用于添加实例的某些过程如果执行不正确，可能使实例无法访问或不可用。有关更多信息，请参阅 快照或恢复你的目录 (p. 118)。

设置 SNS 消息

通过使用亚马逊 Simple Notification Service (Amazon SNS)，您可以在目录状态发生变化时接收电子邮件或文本 (SMS) 消息。如果您的目录从 Active 状态变为 Impaired 或 Inoperable 状态，您将收到通知。当目录恢复为“Active”状态时，您也会收到通知。

另请记住，如果你有接收来自的消息的 SNS 主题Amazon Directory Service在从 Amazon SNS 控制台删除该主题之前，应将目录与不同的 SNS 主题关联。否则您可能错过重要的目录状态消息。有关如何设置 Amazon SNS 的信息，请参阅配置目录状态通知 (p. 48).

应用目录服务设置

Amazon托管 Microsoft AD 允许你定制安全配置以满足合规性和安全要求。Amazon托管 Microsoft AD 将配置部署并维护到目录中的所有域控制器，包括在添加新区域或其他域控制器时。您可以为所有新目录和现有目录配置和应用这些安全设置。您可以执行此操作中的按照中的步骤操作控制台编辑目录安全设置 (p. 45)或者通过UpdateSettings API.

有关更多信息，请参阅 配置目录安全设置 (p. 44)。

删除目录前删除亚马逊企业应用程序

删除与一个或多个 Amazon 企业应用程序关联的目录之前， WorkSpaces, Amazon WorkSpaces Amazon Application Manager WorkDocs, Amazon WorkMail、Amazon Web Services Management Console或

Amazon Relational Database Service (Amazon RDS)，您必须先删除每个应用程序。有关如何删除这些应用程序的更多信息，请参阅删除目录 (p. 117)。

访问 SYSVOL 和 NETLOGON 共享时，请使用 SMB 2.x 客户端

客户端计算机使用服务器消息块 (SMB) 来访问上的 SYSVOL 和 NETLOGON 共享Amazon针对组策略、登录脚本和其他文件的托管 Microsoft AD 域控制器。AmazonMicrosoft AD 仅支持 SMB 2.0 版 (SMBv2) 和更新版本。

SMBv2 和更新版本的协议增加了许多功能，可以提高客户端性能以及域控制器和客户端的安全性。此更改遵循了美国计算机应急准备小组和微软以禁用 smbv1。

> **Important**
>
> 如果您当前使用 SMBv1 客户端来访问域控制器的 SYSVOL 和 NETLON 共享，请务必更新这些客户端以使用 SMBv2 或更新版本。您的目录可以正常工作，但您的 SMBv1 客户端将无法连接到您的 SYSVOL 和 NETLON 共享。Amazon托管 Microsoft AD 域控制器，也将无法处理组策略。

SMBv1 客户端将与您拥有的任何其他兼容 SMBv1 的文件服务器配合使用。但是，Amazon建议您将所有 SMB 服务器和客户端更新为 SMBv2 或更新版本。有关在系统中禁用 SMBv1 并将其更新为更新 SMB 版本的更多信息，请参阅上发布的相关文章。微软 TechNet和支持.

跟踪 SMBv1 远程连接

你可以查看微软-Windowss-smB服务器/审计Windows 事件日志远程连接到Amazon托管 Microsoft AD 域控制器，此日志中的任何事件都表示 smbv1 连接。以下是您可能会在某个日志中看到的信息示例：

SMB1 访问

客户端地址：###.###.###.###

指南：

此事件表示客户端尝试使用 SMB1 访问服务器。要停止审核 SMB1 访问，请使用 Windows PowerShell cmdlet SetSmbServerConfiguration.

为应用程序编程

在为您的应用程序编程之前，请考虑以下事项：

使用 Windows DC 定位器服务

开发应用程序时，请使用 Windows DC 定位器服务或使用的动态 DNS (DDNS) 服务。Amazon管理微软 AD 以查找域控制器 (DC)。请勿使用 DC 的地址对应用程序进行硬编码。DC 定位器服务有助于确保分配目录负载，使您能够通过将域控制器添加到部署来利用水平扩展。如果您将应用程序绑定到固定 DC 并且 DC 进行修补或恢复，则您的应用程序将失去对 DC 的访问权限而不是使用其余的 DC。而且，DC 的硬编码可能导致在单一 DC 上出现热点。情况严重时，热点可能导致您的 DC 无法响应。此类情况可能还会导致 Amazon 目录自动化功能将目录标记为“受损”，并且可能触发更换无响应 DC 的恢复过程。

在推出生产之前进行加载测试

请务必对代表您的生产工作负载的对象和请求执行实验室测试，以确认目录将扩展至您的应用程序负载。如果您需要更多容量，请在 DC 间分配请求时测试其他 DC。有关更多信息，请参阅部署额外的域控制器 (p. 132)。

使用高效的 LDAP 查询

对域控制器进行的针对数万个对象的广泛 LDAP 查询在单个 DC 中会产生明显的 CPU 周期消耗，从而导致热点。这可能影响在查询期间共享同一 DC 的应用程序。

AmazonManaged Microsoft AD 配额

以下是针对的默认配额AmazonManaged Microsoft AD。除非另有说明，否则每个区域具有各自。

AmazonManaged Microsoft AD 配额

资源	默认配额
AmazonManaged Microsoft AD 目录	10
手动快照*	每个集群 5 个AmazonManaged Microsoft AD
手动快照期限 **	180 天
每个目录的最大域控制器数量	20
每个标准 Microsoft AD 的共享域 ***	5
每个企业 Microsoft AD 的共享域 ***	125
每个目录的最大注册证书颁发机构 (CA) 证书数	5
的最大总数量Amazon单个地区Amazon**** Managed Microsoft AD（企业版）目录	5

* 手动快照配额无法更改。

** 手动快照支持的最长期限为 180 天，无法更改。这是由于删除对象的 Tombstone-Life 属性，该属性定义了 Active Directory 的系统状态备份的有用保质期。无法从超过 180 天的快照进行还原。有关更多信息，请参阅 Microsoft 网站上的 Active Directory 的系统状态备份的有用保质期。

*** 共享域默认配额是指单个目录可以共享到的账户数量。

**** 这包括 1 个主要区域和最多 4 个额外地区。有关更多信息，请参阅 主要与其他地区 (p. 55)。

> **Note**
>
> 不能将公有 IP 地址附加到您的 Amazon 弹性网络接口 (ENI)。

有关应用程序设计和负载分配的信息，请参阅为应用程序编程 (p. 140)。

有关存储和对象配额，请参阅比较表在AmazonDirectory Service 定价页.

的应用程序兼容性策略AmazonMicrosoft

AmazonMicrosoft Active DireAmazon托管 Microsoft AD) 与多个Amazon服务和第三方应用程序。

下面列出了兼容的 Amazon 应用程序和服务：

- Amazon Chime-有关详细说明，请参阅。Connect 您的活动目录.
- Amazon Connect-有关更多信息，请参阅。Amazon Connect 的工作原理.
- Amazon EC2 — 有关更多信息，请参阅。将 EC2 实例加入Amazon托管的 Microsoft AD 目录 (p. 66).
- FSx for Windows File Server — 有关更多信息，请参阅。FSx for Windows File Server 是什么？.
- 亚马逊 QuickSight -有关更多信息，请参阅。在Amazon 中管理用户账户 QuickSight 企业版.
- Amazon RDS for MySQL-有关更多信息，请参阅。对 MySQL 使用 Kerberos 身份验证.
- Amazon RDS for SQL Server — 有关更多信息，请参阅。对 Amazon RDS Microsoft SQL Server 数据库实例使用.

- Amazon RDS for Oracle-有关更多信息，请参阅。将 Kerberos 身份验证与 Amazon RDS for Oracle.
- Amazon RDS for PostgreSQL-有关更多信息，请参阅。将 Kerberos 身份验证与 Amazon RDS for PostgreSQL.
- Amazon IAM Identity Center (successor to Amazon Single Sign-On)-有关详细说明，请参阅。将 IAM 身份中心连接到本地活动目录.
- 亚马逊 WorkDocs -有关详细说明，请参阅。使用连接到本地目录AmazonMicrosoft.
- 亚马逊 WorkMail -有关详细说明，请参阅。集成Amazon WorkMail使用现有目录（标准设置）.
- WorkSpaces -有关详细说明，请参阅。启动 WorkSpace 使用AmazonMicrosoft.
- Amazon Client VPN - 有关详细说明，请参阅客户端身份验证和授权。
- Amazon Web Services Management Console – 有关更多信息，请参阅允许访问Amazon Web Services Management Console使用 AD 凭据 (p. 130)。

由于定制和商业的规模 off-the-shelf 使用活动目录的应用程序，Amazon不会且不能对与兼容的第三方应用程序执行正式或综合性验证AmazonMicrosoft Active DireAmazonMicrosoft AD。虽然Amazon与客户尝试克服任何潜在应用程序安装中遇到的挑战，我们不能保证任何应用程序与或将继续兼容。AmazonMicrosoft AD

下列第三方应用程序与兼容AmazonMicrosoft AD

- 基于 Active Directory 的激活 (ADBA)
- 活动目录证书服务 (AD CS)：企业证书颁发机构
- Active Directory 联合身份验证服务 (AD FS)
- Active Directory 用户和计算机 (ADUC)
- 应用程序服务器 (.NET)
- Azure Active Directory (Azure AD)
- Azure Active Directory (AD) Connect
- 分布式文件系统复制 (DFSR)
- 分布式文件系统命名空间 (DFSN)
- Microsoft 远程桌面服务许可服务器
- 微软 SharePoint 服务器
- Microsoft SQL Server（包括 SQL Server 永不停机可用性组）
- Microsoft System Center Configuration Manager (SCCM) — 部署 SCCM 的用户必须是。Amazon委派的系统管理的管理员组。
- Microsoft Windows 和 Windows Server 操作系统
- Office 365

请注意，并非这些应用程序的所有配置都受支持。

兼容性指南

尽管应用程序可能具有不兼容的配置，但应用程序部署配置通常都可以克服不兼容问题。下面介绍了应用程序不兼容最常见的原因。客户可以使用此信息调查所需应用程序的兼容性特征并确定可能的部署更改。

- 域管理员或其他特权权限 – 部分应用程序指明您必须以域管理员身份安装它们。由于 Amazon 必须保留对此权限级别的独占控制才能将 Active Directory 作为托管服务交付，因此您不能充当域管理员来安装此类应用程序。但是，您通常可通过将特定的、低特权和 Amazon 支持的权限委派给执行安装的人来安装此类应用程序。有关您的应用程序所需确切权限的详细信息，请询问您的应用程序提供商。有关 Amazon 允许您委派的权限的更多信息，请参阅创建的内容 (p. 10)。
- 访问特权活动目录容器 —在你的目录中，AmazonMicrosoft AD 提供了一个您对其具有完整管理控制权限的组织部门 (OU)。对于 Active Directory 树中高于您的 OU 的容器，您没有创建或写入权限，可能具有有限的读取权限。用于创建或访问您对其无权限的容器的应用程序可能不会正常工作。但是，此类应用程序

通常能够使用您在 OU 中创建的容器作为替代。请咨询您的应用程序提供商，以找到在 OU 中创建并使用容器做作为替代的方法。有关管理 OU 的更多信息，请参阅如何管理AmazonMicrosoft Managed Microsoft AD (p. 25)。

- 安装工作流程期间的架构更改 – 一些 Active Directory 应用程序需要对默认 Active Directory 架构进行更改，并且它们将尝试在应用程序安装工作流程中安装这些更改。由于架构扩展的特权性质，Amazon 通过仅使用 Amazon Directory Service 控制台、CLI 或开发工具包导入轻量目录交换格式 (LDIF) 文件来实现上述操作。此类应用程序通常附带一个 LDIF 文件，您可以通过 Amazon Directory Service 架构更新过程将此文件应用于目录。有关 LDIF 导入过程工作原理的更多信息，请参阅教程：扩展您的Amazon托管的 Microsoft AD 架构 (p. 112)。安装过程中，您可通过一种绕过架构安装的方式来安装应用程序。

已知不兼容的应用程序

以下列出了常见的商业广告 off-the-shelf 我们尚未为其找到可用于的配置的应用程序AmazonMicrosoft ADAmazon出于好意， 将会不时更新此列表，以帮助您避免做无用功。Amazon对于当前或未来的兼容性，对此信息的提供不做任何保证或声明。

- 活动目录证书服务 (AD CS)：证书注册 Web 服务
- 活动目录证书服务 (AD CS)：证书注册策略 Web 服务
- Microsoft Exchange Server
- 适用于 Business Server 的 Microsoft Skype

Amazon托管的 Microsoft AD 测试实验室教程

本部分提供了一系列指导式教程，可帮助您在中建立测试实验室环境。Amazon你可以在哪里尝试AmazonAD 的托管的 Microsoft AD。

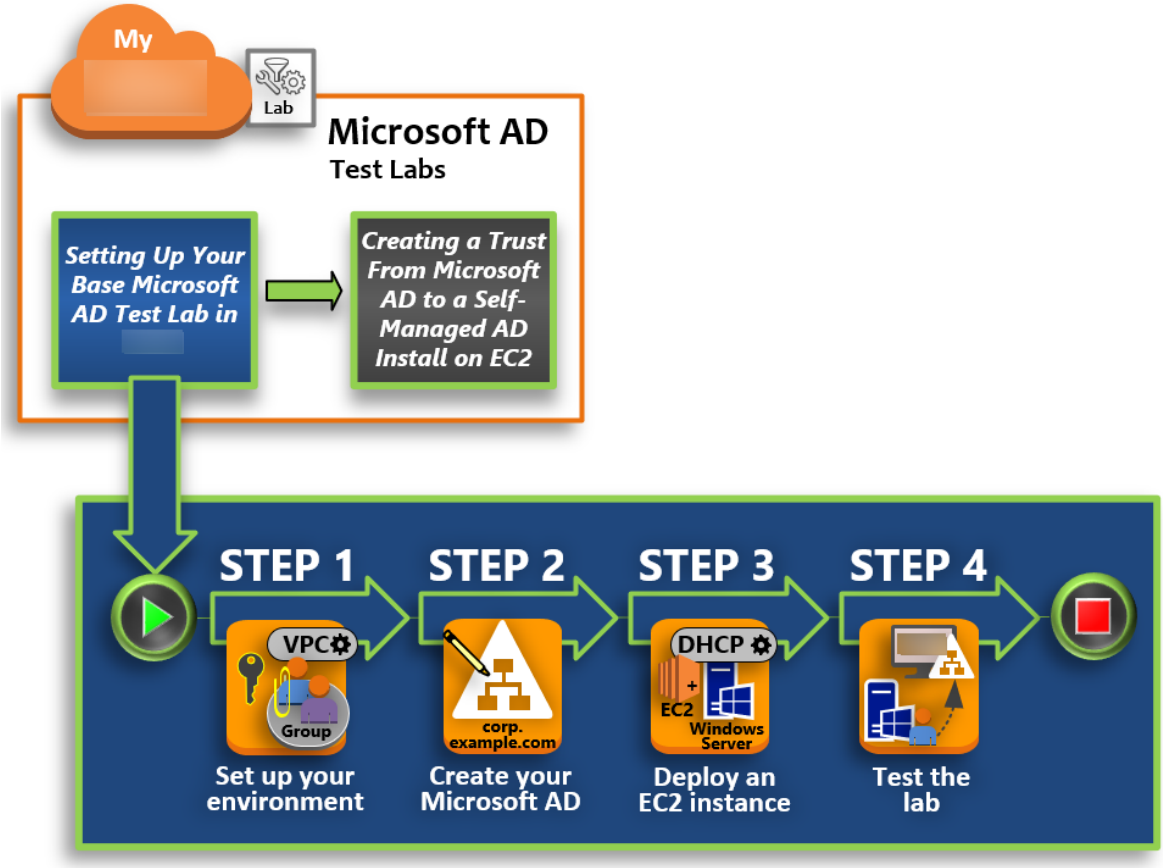
主题

- 教程：设置基地Amazon中托管的 Microsoft AD 测试实验室Amazon (p. 143)
- 教程：创建信任Amazon将微软 AD 托管到 Amazon EC2 上的自管 Active Directory 安装 (p. 154)

教程：设置基地Amazon中托管的 Microsoft AD 测试实验室Amazon

本教程将介绍如何设置Amazon为新的准备环境Amazon托管 Microsoft AD 安装，使用运行 Windows Server 2019 的新 EC2 实例。然后，本教程会介绍常用 Active Directory 管理工具管理Amazon从你的 Windows 系统管理微软 AD 环境。在您完成本教程后，您将满足设置网络的先决条件并配置了新的Amazon托管的 Microsoft AD 林。

如下图中所示，您在本教程中创建的实验室将成为有关的动手学习的基础组件。Amazon托管的 Microsoft AD。您可以在以后添加可选教程，以获得更多动手体验。本教程系列非常适合任意新接触的人Amazon托管 Microsoft AD 并希望测试实验室以进行评估。完成本教程需要大约 1 个小时。



第 1 步：设置Amazon用于的环境AmazonMicrosoft Managed Microsoft AD (p. 145)

在完成先决任务之后，您可以在 EC2 实例中创建和配置 VPC。

第 2 步：创建Amazon中托管的 Microsoft AD 目录Amazon (p. 150)

在此步骤中，您将设置Amazon在托管的 Microsoft ADAmazon这是第一次。

第 3 步：部署 EC2 实例以管理您的AmazonMicrosoft Managed Microsoft AD (p. 151)

在这里，您将演练将客户端计算机连接到新域以及在 EC2 中设置新 Windows Server 系统所需的各种部署后任务。

第 4 步：验证基本测试实验室正常工作 (p. 154)

最后，作为管理员，您将验证您可以登录并连接到Amazon从 EC2 中的 Windows 服务器系统托管微软 AD。在成功测试了实验室可以运行之后，您可以继续添加其他实验室指南模块。

先决条件

如果您计划仅使用本教程中的 UI 步骤创建测试实验室，则可以跳过先决条件部分并转到步骤 1。不过，如果您计划使用 Amazon CLI 命令或 Amazon Tools for Windows PowerShell 模块来创建测试实验室环境，则必须先配置以下内容：

- IAM user and secret 访问key— 如果您希望使用访问密钥的 IAM 用户，则需要具有访问密钥的 IAM 用户。Amazon CLI要么Amazon Tools for Windows PowerShell模块。如果您没有访问密钥，请参阅创建、修改和查看访问密钥 (Amazon Web Services Management Console)。

- Amazon Command Line Interface（可选）下载和安装Amazon CLIWindows 上的. 安装之后，打开命令提示符或者 Windows PowerShell 窗口，然后键入 `aws configure`。请注意，您需要访问密钥和私有密钥以完成设置。有关如何完成此任务的步骤，请查看第一个先决条件。先决条件将提示以下内容：
  - Amazon访问密钥 ID [无]：`AKIAIOSFODNN7EXAMPLE`
  - Amazon私有访问密钥 [无]：`wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`
  - 默认区域名称 [无]：`us-west-2`
  - 默认输出格式 [无]：`json`
- Amazon Tools for Windows PowerShell（可选）— 下载并安装最新版本的Amazon Tools for Windows PowerShell从https://aws.amazon.com/powershell/，然后运行以下命令。请注意，您需要访问密钥和私有密钥以完成设置。有关如何完成此任务的步骤，请查看第一个先决条件。

```
Set-AWSCredentials -AccessKey {AKIAIOSFODNN7EXAMPLE} -SecretKey
{wJalrXUtnFEMI/K7MDENG/ bPxRfiCYEXAMPLEKEY} -StoreAs {default}
```

第 1 步：设置Amazon用于的环境AmazonMicrosoft Managed Microsoft AD

在你可以创建之前Amazon在您的托管的 Microsoft ADAmazon测试实验室，您首先需要设置 Amazon EC2 key pair 以对所有登录数据进行加密。

创建密钥对

如果您已有已密钥对，可跳过本步骤。有关 Amazon EC2 密钥对的更多信息，请参阅http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-key-pairs.html.

创建密钥对

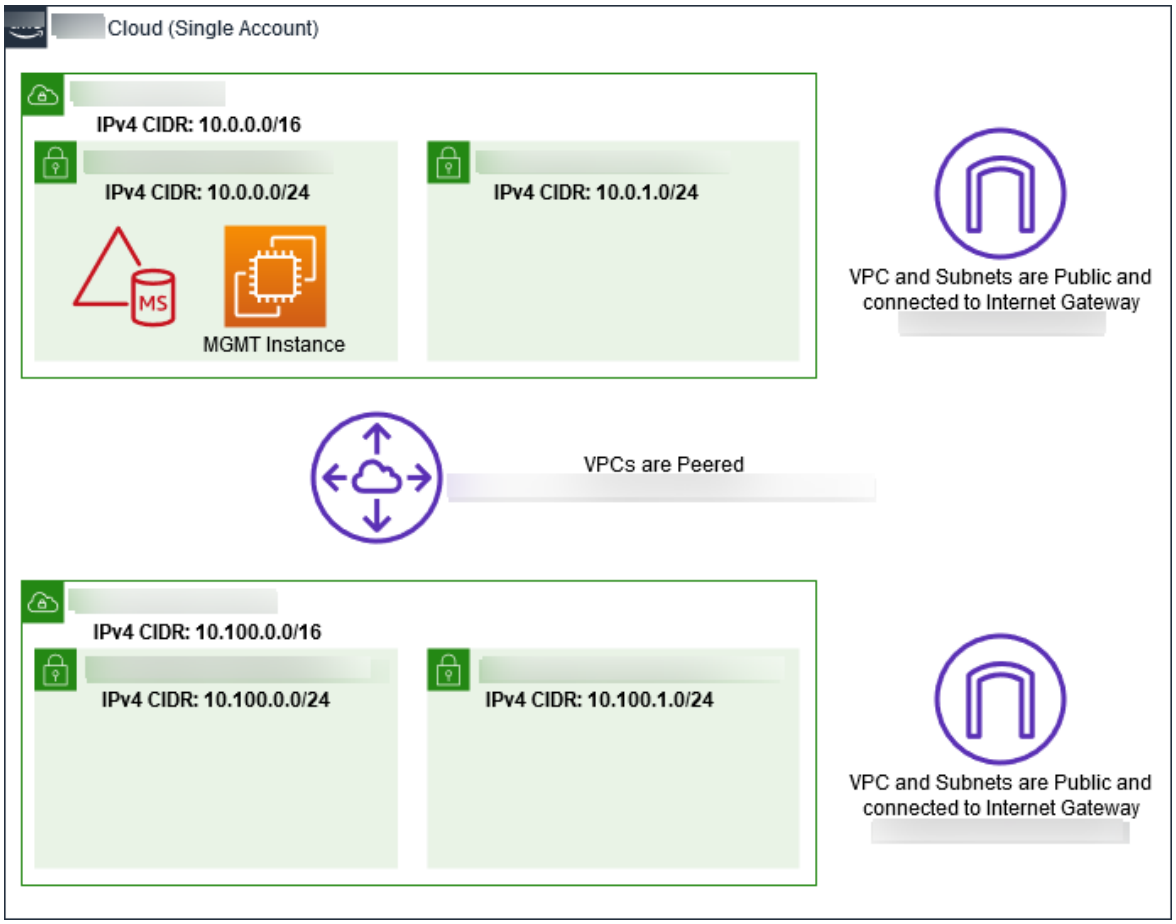
1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在导航窗格中的 Network & Security 下，选择 Key Pairs，然后选择 Create Key Pair。
3. 对于 Key pair name (密钥对名称)，键入 **`Amazon-DS-KP`**。对于 Key pair file format (密钥对文件格式)，选择 pem，然后选择 Create (创建)。
4. 您的浏览器会自动下载私有密钥文件。该文件名是您在创建密钥对时指定的名称，扩展名为 `.pem`。将私有密钥文件保存在安全位置。

   Important

   这是您保存私有密钥文件的唯一机会。当您启动实例时，需要提供密钥对的名称；当您解密实例密码时，需要提供相应的私有密钥。

创建、配置和对等两个 VPC

如下图所示，在完成这一多步骤过程后，您就创建并配置了两个公有 VPC、每个 VPC 两个公有子网、每个 VPC 一个 Internet 网关以及这两个 VPC 之间的一个 VPC 对等连接。为了简化和降低成本，我们选择使用公有 VPC 和子网。对于生产工作负载，我们建议您使用私有 VPC。有关提高 VPC 安全性的更多信息，请参阅 Amazon Virtual Private Cloud 中的安全性。



所有Amazon CLIPowerShell 示例使用下面的 VPC 信息，并在 us-west-2 中构建。您可以选择任何区域支持在中构建环境。有关一般信息，请参阅 Amazon VPC 是什么？。

第 1 步：创建两个 VPC

在此步骤中，您需要使用下表中的指定参数在同一账户中创建两个 VPC。Amazon托管微软 AD 支持将单独的帐户与共享您的目录 (p. 58)功能。将用于第一个 VPCAmazon托管的 Microsoft AD。第二个 VPC 将用于以后可能在 教程：创建信任Amazon将微软 AD 托管到 Amazon EC2 上的自管 Active Directory 安装 (p. 154)中使用的资源。

托管 AD VPC 信息	本地 VPC 信息
名称标签：Amazon-DS-VPC01 IPv4 CIDR block：10.0.0.0/16 IPv6 CIDR 块：无 IPv6 CIDR 块 租赁：默认值	名称标签：Amazon-OnPre-MVPC01 IPv4 CIDR block：10.100.0.0/16 IPv6 CIDR 块：无 IPv6 CIDR 块 租赁：默认值

有关详细说明，请参阅创建 VPC。

步骤 2: 每个 VPC 创建两个子网

创建 VPC 后，您将需要使用下表中的指定参数为每个 VPC 创建两个子网。对于本测试实验室，每个子网将是 /24。这将允许每个子网最多发出 256 个地址。每个子网必须位于单独的可用区中。将每个子网单独放在可用区中是 AmazonMicrosoft AD (p. 8)之一。

Amazon-DS-VPC01 子网信息：	Amazon-OnPrem VPC01 子网信息
名称标签：Amazon-DS-VPC01-Subnet01 VPC：vpc-xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxAmazon-DS-VPC01 可用区：us-west-2a IPv4 CIDR block：10.0.0.0/24	名称标签：Amazon-OnPrem-VPC01-Subnet01 VPC：vpc-xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxAmazon-OnPre-MVPC01 可用区：us-west-2a IPv4 CIDR block：10.100.0.0/24
名称标签：Amazon-DS-VPC01-Subnet02 VPC：vpc-xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxAmazon-DS-VPC01 可用区：us-west-2b IPv4 CIDR block：10.0.1.0/24	名称标签：Amazon-OnPrem-VPC01-Subnet02 VPC：vpc-xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxAmazon-OnPre-MVPC01 可用区：us-west-2b IPv4 CIDR block：10.100.1.0/24

有关详细说明，请参阅在 VPC 中创建子网。

步骤 3: 创建 Internet Gateway 并将其连接到您的 VPC

由于我们使用的是公有 VPC，因此需要使用下表中的指定参数创建 Internet 网关并将其连接到 VPC。这将允许您连接和管理您的 EC2 实例。

Amazon-DS-VPC01 Internet Gateway 信息	Amazon-OnPre-MVPC01 Internet Gateway 信息
名称标签：Amazon-DS-VPC01-IGW VPC：vpc-xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxAmazon-DS-VPC01	名称标签：Amazon-OnPrem-VPC01-IGW VPC：vpc-xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxAmazon-OnPre-MVPC01

有关详细说明，请参阅 Internet 网关。

步骤 4: 配置 VPC 对等连接Amazon-DS-VPC01 和Amazon-OnPre-MVPC01

由于您之前已经创建了两个 VPC，因此您需要使用下表中的指定参数通过 VPC 对等方式将它们联网在一起。尽管有很多方法可以连接您的 VPC，但本教程只使用 VPC 对等。Amazon托管 Microsoft AD 支持许多连接 VPC 的解决方案，其中一些包括VPC 对等、中转网关, 和VPN.

对等连接名称标签：Amazon-DS-VPC01Amazon-OnPrem-VPC01-Prem VPC（请求者）：vpc-xxxxxxxxxxxxxxxxxxxxxxxxAmazon-DS-VPC01 账户：我的账户

区域: 此区域

VPC（接受者）：vpc-xxxxxxxxxxxxxxxxxxxxxxxxAmazon-OnPre-MVPC01

有关如何在您账户中的两个 VPC 之间创建 VPC 对等连接的说明，请参阅在您账户中的两个 VPC 之间创建 VPC 对等连接。

第 5 步：向每个 VPC 的主路由表添加两条路由

为了使在前面步骤中创建的 Internet 网关和 VPC 对等连接能够正常起作用，您需要使用下表中的指定参数更新这两个 VPC 的主路由表。您将添加两条路由：0.0.0.0/0（它将路由到路由表未明确知道的所有目的地）和 10.0.0.0/16 或 10.100.0.0/16（它将通过上面建立的 VPC 对等连接路由到每个 VPC）。

您可以通过筛选 VPC 名称标签（Amazon-DS-VPC01 或Amazon-OnPre-MVPC01)。

Amazon-DS-VPC01 路由 1 信息	Amazon-DS-VPC01 路由 2 信息	Amazon-OnPre-MVPC01 路由 1 信息	Amazon-OnPre-MVPC01 路由 2 信息
目标：0.0.0.0/0 目标：igw-xxxxxxxxxxxxxxxxxxxxxxxxAmazon-DS-VPC01-IGW	目标：10.100.0.0/16 目标：pcx-xxxxxxxxxxxxxxxxxxxxxxxxAmazon-DS-VPC01Amazon-OnPrem-VPC01-Prem	目标：0.0.0.0/0 目标：igw-xxxxxxxxxxxxxxxxxxxxxxxxAmazon-OnPre-MVPC01	目标：10.0.0.0/16 目标：pcx-xxxxxxxxxxxxxxxxxxxxxxxxAmazon-DS-VPC01Amazon-OnPrem-VPC01-Prem

有关如何向 VPC 路由表添加路由的说明，请参阅从路由表添加和删除路由。

为 EC2 实例创建安全组

默认情况下，Amazon托管 Microsoft AD 创建安全组用于管理其域控制器之间的流量。在本节中，您需要创建 2 个安全组（每个 VPC 一个），它们用于使用下表中的指定参数管理 EC2 实例的 VPC 内流量。您还需要添加规则，允许从任意位置的 RDP (3389) 入站，以及来自本地 VPC 的所有流量类型入站。有关更多信息，请参阅 。适用于 Windows 实例的 Amazon EC2 安全组.

Amazon-DS-VPC01 安全组信息：
安全组名称：AmazonDS 测试实验室安全组 描述：AmazonDS 测试实验室安全组 VPC：vpc-xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxAmazon-DS-VPC01

用于的安全组入站规则Amazon-DS-VPC01

类型	协议	端口范围	源	流量的类型
自定义 TCP 规则	TCP	3389	我的 IP	远程桌面
所有流量	All	所有	10.0.0.0/16	所有本地 VPC 流量

Security Group Outbound Rules for Amazon-DS-VPC01

类型	协议	端口范围	目标	流量的类型
所有流量	All	All	0.0.0.0/0	所有流量

Amazon-OnPre-MVPC01 安全组信息：
安全组名称：AmazonOnPrem 测试实验室安全组。 描述：AmazonOnPrem 测试实验室安全组。 VPC：vpc-xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxAmazon-OnPre-MVPC01

用于的安全组入站规则Amazon-OnPre-MVPC01

类型	协议	端口范围	源	流量的类型
自定义 TCP 规则	TCP	3389	我的 IP	远程桌面
自定义 TCP 规则	TCP	53	10.0.0.0/16	DNS
自定义 TCP 规则	TCP	88	10.0.0.0/16	Kerberos
自定义 TCP 规则	TCP	389	10.0.0.0/16	LDAP
自定义 TCP 规则	TCP	464	10.0.0.0/16	Kerberos 更改/设置密码
自定义 TCP 规则	TCP	445	10.0.0.0/16	SMB / CIFS
自定义 TCP 规则	TCP	135	10.0.0.0/16	复制
自定义 TCP 规则	TCP	636	10.0.0.0/16	LDAP SSL
自定义 TCP 规则	TCP	49152 - 65535	10.0.0.0/16	RPC
自定义 TCP 规则	TCP	3268 - 3269	10.0.0.0/16	LDAP GC 和 LDAP GC SSL
自定义 UDP 规则	UDP	53	10.0.0.0/16	DNS
自定义 UDP 规则	UDP	88	10.0.0.0/16	Kerberos
自定义 UDP 规则	UDP	123	10.0.0.0/16	Windows 时间
自定义 UDP 规则	UDP	389	10.0.0.0/16	LDAP
自定义 UDP 规则	UDP	464	10.0.0.0/16	Kerberos 更改/设置密码
所有流量	All	所有	10.100.0.0/16	所有本地 VPC 流量

Security Group Outbound Rules for Amazon-OnPre-MVPC01

类型	协议	端口范围	目标	流量的类型
所有流量	All	All	0.0.0.0/0	所有流量

有关如何创建规则并将规则添加到安全组的详细说明，请参阅使用安全组。

第 2 步：创建Amazon中托管的 Microsoft AD 目录Amazon

您可以使用三种不同的方法来创建目录。您可以使用 Amazon Web Services Management Console 过程（本教程的建议方法），或者您可以使用 Amazon CLI 或 Amazon Tools for Windows PowerShell 过程创建您的目录。

方法 1：创建Amazon托管的 Microsoft AD 目录（Amazon Web Services Management Console）

1. 在Amazon Directory Service控制台选择导航窗格，目录选择，然后选择设置目录.
2. 在存储库的选择目录类型页面，选择AmazonMicrosoft Managed Microsoft AD，然后选择下一步.
3. 在 Enter directory information (输入目录信息) 页面上，提供以下信息，然后选择 Next (下一步)。
   - 对于 Edition (版本)，选择 Standard Edition (标准版) 或 Enterprise Edition (企业版)。有关版本的更多信息，请参阅AmazonMicrosoft Active Directory 的 Directory Service (p. 1).
   - 对于 Directory DNS name (目录 DNS 名称)，键入 **`corp.example.com`**。
   - 对于 Directory NetBIOS name (目录 NetBIOS 名称)，键入 **`corp`**。
   - 对于 Directory description (目录描述)，键入 **`Amazon DS Managed`**。
   - 对于 Admin password，键入您要用于此账户的密码，并在 Confirm password 中再次键入密码。此 Admin 账户在目录创建过程中自动创建。密码不能包含单词 admin。目录管理员密码区分大小写，且长度必须介于 8 到 64 (含) 个字符之间。至少，它还必须包含下列四种类别中三种类别的一个字符：
     - 小写字母 (a-z)
     - 大写字母 (A-Z)
     - 数字 (0-9)
     - 非字母数字字符 (~!@#$%^&*_-+=`\|\(){}[]:;"'<>,.?/)
4. 在 Choose VPC and subnets (选择 VPC 和子网) 页面上，提供以下信息，然后选择 Next (下一步)。
   - 适用于VPC，选择以开头的选项Amazon-DS-VPC01并以结束(10.0.0/16).
   - 对于 Subnets (子网)，选择 10.0.0.0/24 和 10.0.1.0/24 公有子网。
5. 在 Review & create (检查并创建) 页面上，检查目录信息并进行任何必要的更改。如果信息正确，请选择 Create directory (创建目录)。创建目录需要 20 到 40 分钟。创建后，Status 值将更改为 Active。

方法 2：创建Amazon托管的 Microsoft AD (Windows PowerShell) (可选)

1. 打开 Windows PowerShell。
2. 键入以下命令。请确保使用前述 Amazon Web Services Management Console 过程中步骤 4 提供的值。

```
New-DSMicrosoftAD -Name corp.example.com -ShortName corp -Password P@ssw0rd
-Description “Amazon DS Managed” - VpcSettings_VpcId vpc-xxxxxxxx -
VpcSettings_SubnetId subnet-xxxxxxxx, subnet-xxxxxxxx
```

方法 3：创建AmazonMicrosoft Managed Microsoft AD（Amazon CLI) (可选)

1. 打开 Amazon CLI。

2. 键入以下命令。请确保使用前述 Amazon Web Services Management Console 过程中步骤 4 提供的值。

```
aws ds create-microsoft-ad --name corp.example.com --short-name corp --
password P@ssw0rd --description "Amazon DS Managed" --vpc-settings VpcId=
vpc-xxxxxxxx,SubnetIds= subnet-xxxxxxxx, subnet-xxxxxxxx
```

第 3 步：部署 EC2 实例以管理您的AmazonMicrosoft Managed Microsoft AD

对于本实验，我们将使用具有公有 IP 地址的 EC2 实例，使其易于从任意位置访问管理实例。在生产设置中，您可以使用在私有 VPC 中的实例，这些实例只能通过 VPN 或 Amazon Direct Connect 链接访问。对于实例是否具有公有 IP 地址没有要求。

在此部分中，您将演练在新 EC2 实例上，使用 Windows Server 将客户端计算机连接到域所需的各种部署后任务。在下一步中，您将使用 Windows Server 来验证实验室正常运行。

可选：在中创建 DHCP 选项Amazon-DS-VPC01 适用于您的目录

在此可选过程中，您设置 DHCP 选项范围，使得 VPC 中的 EC2 实例自动将您的Amazon用于 DNS 解析的管理微软 AD。有关更多信息，请参阅 DHCP 选项集。

为目录创建 DHCP 选项集

1. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 DHCP Options Sets，然后选择 Create DHCP options set。
3. 在创建 DHCP 选项集页面上，提供目录的以下值：
   - 对于名称，键入 **`Amazon DS DHCP`**。
   - 对于 Domain name (域名)，键入 **`corp.example.com`**。
   - 对于 Domain name servers (域名服务器)，键入 Amazon 所提供目录的 DNS 服务器的 IP 地址。

     Note

     要查找这些地址，请转到Amazon Directory Service 目录页面，然后选择适用的目录 ID。在存储库的详细信息页面，识别并使用中显示的 IPDNS 地址.
     或者，要查找这些地址，请转到Amazon Directory Service 目录页面，然后选择适用的目录 ID。然后，选择扩展和分享. 在域控制器，识别并使用中显示的 IPIP 地址.
   - 将 NTP servers、NetBIOS name servers 和 NetBIOS node type 的设置留空。
4. 选择创建 DHCP 选项集，然后选择关闭。新的 DHCP 选项集会出现在您的 DHCP 选项列表中。
5. 记录新增 DHCP 选项集的 ID (dopt-**`xxxxxxxx`**)。在此过程的末尾，您将新选项集与 VPC 关联时使用此项。

   Note

   无缝域加入发挥作用，而无需配置 DHCP 选项集。
6. 在导航窗格中，选择 Your VPCs。
7. 在 VPC 列表中，选择AmazonDS VPC，选择操作，然后选择编辑 DHCP 选项集.
8. 在编辑 DHCP 选项集页面上，选择您在步骤 5 中记录的选项集，然后选择保存。

创建角色，将 Windows 实例加入Amazon托管的 Microsoft AD 域

使用此过程可配置将 EC2 Windows 实例加入域中的角色。有关更多信息，请参阅 。无缝加入 Windows EC2 实例中的适用于 Windows 实例的 Amazon EC2 用户指南.

配置 EC2 以将 Windows 实例加入域中

1. 通过以下网址打开 IAM 控制台：https://console.aws.amazon.com/iam/。
2. 在 IAM 控制台的导航窗格中，选择 Roles，然后选择 Create role。
3. 在 Select type of trusted entity (选择受信任实体的类型）下，选择 Amazon service (Amazon 服务)。
4. 下面的马上选择将使用此角色的服务，选择EC2，然后选择后续：Permissions (下一步：权限)。
5. 在附加的权限策略页面上，执行以下操作：

   - 选中 AmazonSSMManagedInstanceCore 托管策略旁的复选框。此策略提供了使用 Systems Manager 服务所需的最低权限。
   - 选中 AmazonSSMDirectoryServiceAccess 托管策略旁的复选框。该策略提供了将实例加入由 Amazon Directory Service 托管的 Active Directory 的权限。

   有关这些托管策略和其他策略的信息，您可以将其附加到 Systems Manager 的 IAM 实例配置文件，请参阅为 Systems Manager 创建 IAM 实例配置文件中的Amazon Systems Manager用户指南. 有关托管策略的信息，请参阅Amazon托管策略中的IAM 用户指南.
6. 选择 Next:。标签。
7. （可选）添加一个或多个标签键/值对以组织、跟踪或控制该角色的访问，然后选择后续：审核。
8. 对于角色名称，输入角色的名称，该名称描述可使用此角色将实例加入到域，例如 EC2DomainJoin。
9. （可选）对于角色描述，请输入描述。
10. 选择 Create role (创建角色)。系统将让您返回到 Roles (角色) 页面。

创建 EC2 实例并自动加入目录

在此过程中，您将在 Amazon EC2 中设置 Windows Server 系统，该系统稍后可用于在 Active Directory 中管理用户、组和策略。

创建 EC2 实例并自动加入目录

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 选择 Launch Instance（启动实例）。
3. 在 Step 1 (步骤 1) 页面上的 Microsoft Windows Server 2019 Base - ami-***xxxxxxxxxxxxxxxxx*** 旁，选择 Select (选择)。
4. 在存储库的步骤 2页面上，选择t3.micro（注意，您可以选择更大的实例类型），然后选择后续：配置实例详细信息.
5. 在 Step 3 页面中，执行以下操作：

   - 适用于网络中，选择以结尾的 VPCAmazon-DS-VPC01（例如，vpc-***xxxxxxxxxxxxxxxxxx***|Amazon-DS-VPC01)。
   - 适用于子网选择公有子网 1，应该为您的首选可用区进行预配置（例如，子网-***xxxxxxxxxxxxxxxxxx***|Amazon-DS-VPC01-Subnet01 |***us-west-2a***)。
   - 对于 Auto-assign Public IP，选择 Enable (如果子网设置未默认设置为启用)。
   - 对于 Domain join directory，选择 corp.example.com (d-***xxxxxxxxxx***)。
   - 对于 IAM 角色，选择您在创建角色，将 Windows 实例加入Amazon托管的 Microsoft AD 域 (p. 151)中为实例角色提供的名称，例如 EC2DomainJoin。
   - 将其他设置保留为默认值。
   - 选择 Next:。添加存储.
6. 在存储库的步骤 4页面上，保留默认设置，然后选择后续：添加标签.
7. 在 Step 5 页面上，选择 Add Tag。在密钥类型**corp.example.com-mgmt**选择，然后选择后续：配置安全组.

8. 在存储库的步骤 6页面，选择选择现有安全组，选择AmazonDS 测试实验室安全组（您之前在基本教程 (p. 148)），然后选择查看和启动以查看您的实例。
9. 在 Step 7 页面上，查看页面，然后选择 Launch。
10. 在 Select an existing key pair or create a new key pair 对话框上，执行下列操作之一：
    - 选择 Choose an existing key pair。
    - 在选择一个密钥对，选择Amazon-DS-KP.
    - 选中 I acknowledge... 复选框。
    - 选择 Launch Instances。
11. 选择查看实例返回 Amazon EC2 控制台并查看部署的状态。

在 EC2 实例上安装 Active Directory 工具

您可以从两种方法中选择，在 EC2 实例上安装 Active Directory 域管理工具。您可以使用 Server Manager UI (本教程的建议方法) 或 Windows PowerShell。

在 EC2 实例上安装 Active Directory 工具 (Server Manager)

1. 在 Amazon EC2 控制台中，选择实例，选择您刚刚创建的实例，然后选择Connect (连接).
2. 在连接到您的实例对话框中，选择获取密码以检索您的密码（如果您尚未这样做），然后选择下载远程桌面文件。
3. 在 Windows Security (Windows 安全) 对话框中，键入 Windows Server 计算机的本地管理员凭证以登录（例如，**administrator**）。
4. 从 Start 菜单中选择 Server Manager。
5. 在 Dashboard 中，选择 Add Roles and Features。
6. 在 Add Roles and Features Wizard 中，选择 Next。
7. 在 Select installation type 页面上选择 Role-based or feature-based installation，然后选择 Next。
8. 在 Select destination server 页面上，请确保选中了本地服务器，然后选择 Next。
9. 在 Select server roles 页面上，选择 Next。
10. 在 Select features 页面中，执行以下操作：
    - 选中 Group Policy Management 复选框。
    - 展开 Remote Server Administration Tools，然后展开 Role Administration Tools。
    - 选中 AD DS and AD LDS Tools 复选框。
    - 选中 DNS Server Tools 复选框。
    - 选择 Next (下一步)。
11. 在 Confirm installation selections 页面上，查看信息，然后选择 Install。功能安装完成后，以下新工具或管理单元将在“开始”菜单的“Windows 管理工具”文件夹中可用。
    - Active Directory 管理中心
    - Active Directory 域和信任
    - 适用于 Windows PowerShell 的 Active Directory 模块
    - Active Directory 站点和服务
    - Active Directory 用户和计算机
    - ADSI 编辑
    - DNS
    - 组策略管理

在 EC2 实例上安装 Active Directory 工具 (Windows PowerShell) (可选)

1. 启动 Windows PowerShell。
2. 键入以下命令。

```
Install-WindowsFeature -Name GPMC,RSAT-AD-PowerShell,RSAT-AD-
AdminCenter,RSAT-ADDS-Tools,RSAT-DNS-Server
```

第 4 步：验证基本测试实验室正常工作

在添加其他测试实验室指南模块之前，使用以下过程验证已成功设置该测试实验室。此过程验证您的 Windows Server 已正确配置、可以连接到 corp.example.com 域，并用于管理您的Amazon托管的 Microsoft AD 林。

验证基本测试实验室正常工作

1. 从您以本地管理员身份登录的 EC2 实例中注销
2. 返回 Amazon EC2 控制台，选择实例在导航窗格中。然后选择已创建的实例。选择 Connect（连接）。
3. 在 Connect To Your Instance 对话框中，选择 Download Remote Desktop File。
4. 在 Windows Security (Windows 安全) 对话框中，键入您的 CORP 域的管理员凭证以便登录（例如，**corp\admin**）。
5. 登录之后，在 Start 菜单中的 Windows Administrative Tools 下，选择 Active Directory Users and Computers。
6. 您应看到 corp.example.com 显示了所有默认 OU 以及与新域关联的账户。在域控制器中，记录在您创建时自动创建的域控制器的名称Amazon在本教程的第 2 步中托管微软 AD。

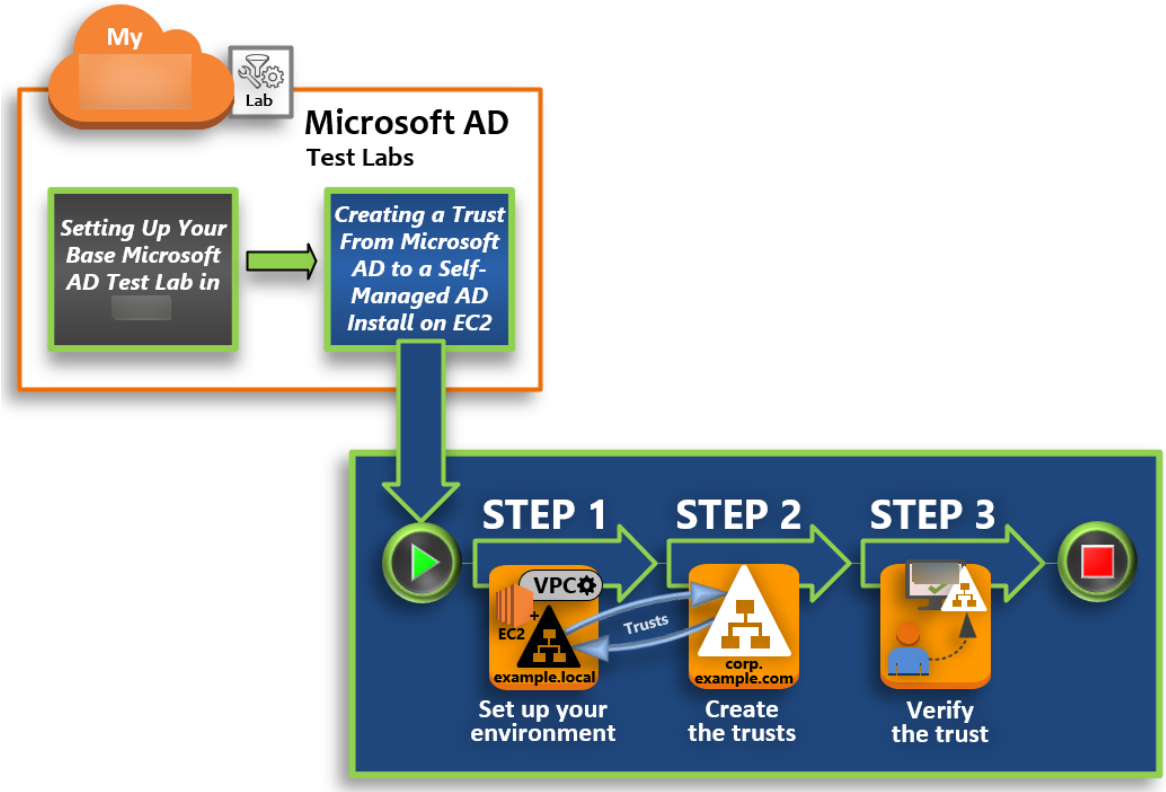
恭喜您！您的Amazon现在，托管的 Microsoft AD 基本测试实验室环境已经配置。您可以随时开始添加该系列中的下一个测试实验室。

下一个教程：教程：创建信任Amazon将微软 AD 托管到 Amazon EC2 上的自管 Active Directory 安装 (p. 154)

教程：创建信任Amazon将微软 AD 托管到 Amazon EC2 上的自管 Active Directory 安装

在本教程中，您了解如何在Amazon创建的 Microsoft Active Directory 林的 Directory Service基本教程 (p. 143). 您还将学习在 Amazon EC2 中的 Windows Server 上创建新的本机 Active Directory 林。如下图中所示，通过本教程创建的实验室，对于设置完整的第二个构建基块来说是第二个必不可少的构建基块。Amazon托管的 Microsoft AD 测试实验室。您可以使用测试实验室来测试基于纯云或基于混合云的项Amazon解决方案。

您只需要创建本教程一次。然后，您可以根据需要添加可选的教程，提供更多的体验。



第 1 步：为信任设置环境 (p. 155)

在新 Active Directory 林与之间建立信任之前Amazon管理的微软 AD 林你在基本教程 (p. 143)，您需要准备 Amazon EC2 环境。为此，您首先需要创建一个 Windows Server 2019 服务器，将该服务器提升为域控制器，然后相应地配置您的 VPC。

第 2 步：创建信任 (p. 159)

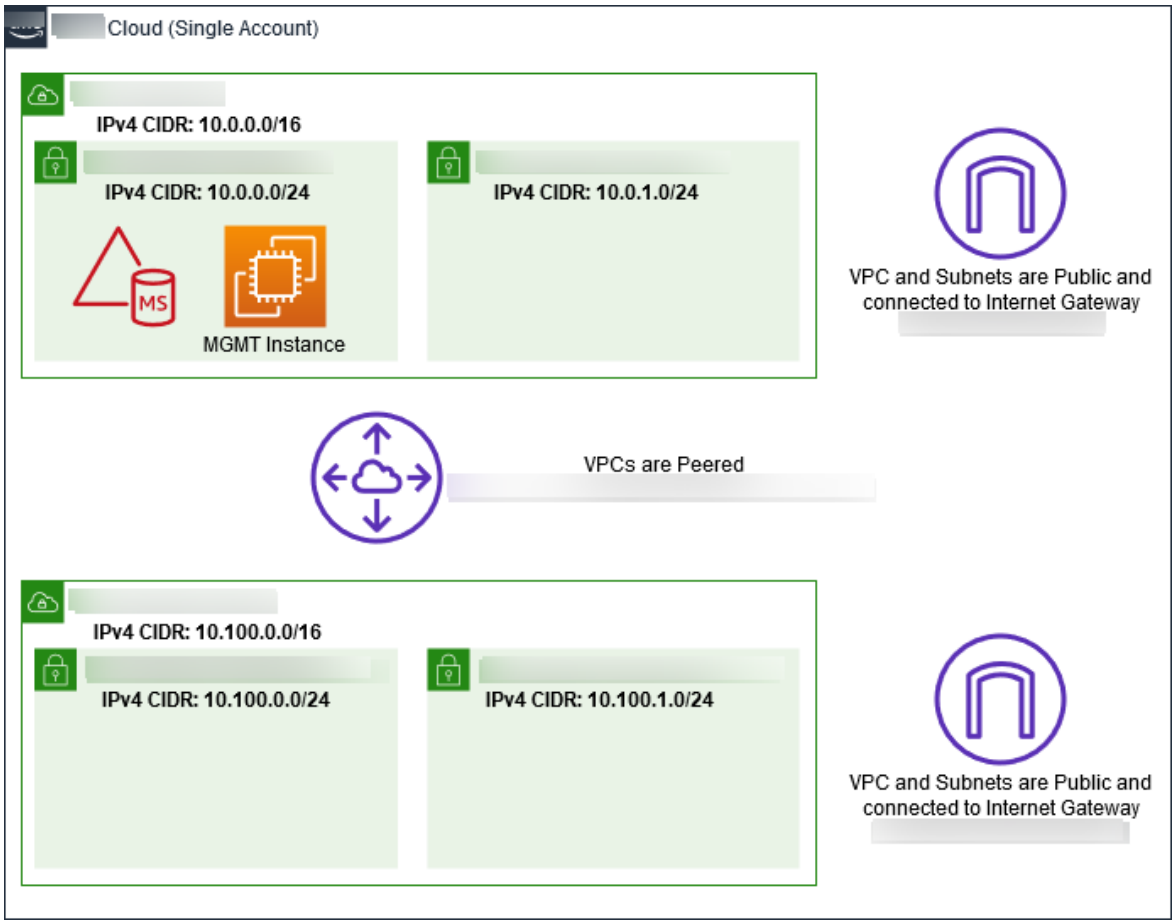
在此步骤中，您将在新创建的 Amazon EC2 中托管的 Active Directory 林与您的Amazon在中托管的 Microsoft AD 林Amazon.

第 3 步：验证信任 (p. 161)

最后，作为管理员，您可以使用 Amazon Directory Service 控制台来验证新的信任是否正常运行。

第 1 步：为信任设置环境

在此部分中，设置您的 Amazon EC2 环境，部署新的林，并准备您的 VPC 以便与之间建立信任。Amazon.



创建一个 Windows Server 2019 EC2 实例

使用以下过程在 Amazon EC2 中创建一个 Windows Server 2019 成员服务器。

创建 Windows Server 2019 EC2 实例

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在 Amazon EC2 控制台中，选择启动实例.
3. 在 Step 1 (步骤 1) 页面上，在列表中找到 Microsoft Windows Server 2019 Base - ami-**xxxxxxxxxxxxxxxxx**。然后选择 Select。
4. 在存储库的步骤 2页面上，选择t2.large选择，然后选择后续：配置实例详细信息.
5. 在 Step 3 页面中，执行以下操作：
   - 适用于网络选择，选择vpc-**xxxxxxxxxxxxxxxxxxxx** Amazon-OnPre-M-VPC01（您之前在基本教程 (p. 145))。
   - 适用于子网选择，选择子网-**xxxxxxxxxxxxxxxxxxxx**|Amazon-OnPre-MP-VPC01-Subnet01 | Amazon-OnPre-M-VPC01.
   - 对于 Auto-assign Public IP 列表，选择 Enable (如果子网设置未默认设置为 Enable)。
   - 将其他设置保留为默认值。
   - 选择 Next:。添加存储.
6. 在存储库的步骤 4页面，保留默认设置，然后选择后续：添加标签.
7. 在 Step 5 页面上，选择 Add Tag。UNDER密钥类型**`example.local-DC01`**选择，然后选择后续：配置安全组.

8. 在存储库的步骤 6页面，选择选择现有安全组选择，选择Amazon本地测试实验室安全组（您之前在基本教程 (p. 148)），然后选择查看和启动查看实例。
9. 在 Step 7 页面上，查看页面，然后选择 Launch。
10. 在 Select an existing key pair or create a new key pair 对话框上，执行下列操作之一：
    - 选择 Choose an existing key pair。
    - UNDER选择一个密钥对，选择Amazon-DS-KP（您之前在基本教程 (p. 145)）。
    - 选中 I acknowledge... 复选框。
    - 选择 Launch Instances。
11. 选择查看实例返回 Amazon EC2 控制台并查看部署的状态。

将您的服务器提升为域控制器

在创建信任之前，您必须为新林构建和部署第一个域控制器。在此过程中，您需要配置新的 Active Directory 林，安装 DNS，并将此服务器设置为使用本地 DNS 服务器来解析名称。在此过程结束时，您必须重新启动服务器。

> **Note**
>
> 如果你想在中创建域控制器Amazon与您的本地网络复制，您将首先手动将 EC2 实例加入到您的本地域。然后，您可以将服务器提升为域控制器。

将您的服务器提升为域控制器

1. 在 Amazon EC2 控制台中，选择实例，选择您刚创建的实例，然后选择Connect (连接).
2. 在 Connect To Your Instance 对话框中，选择 Download Remote Desktop File。
3. 在 Windows Security (Windows 安全) 对话框中，键入 Windows Server 计算机的本地管理员凭证以登录（例如，**`administrator`**）。如果您还没有本地管理员密码，请返回 Amazon EC2 控制台，右键单击该实例，然后选择获取 Windows 密码. 导航到您的 `Amazon DS KP.pem` 文件或您的个人 `.pem` 密钥，然后选择 Decrypt Password。
4. 从 Start 菜单中选择 Server Manager。
5. 在 Dashboard 中，选择 Add Roles and Features。
6. 在 Add Roles and Features Wizard 中，选择 Next。
7. 在 Select installation type 页面上选择 Role-based or feature-based installation，然后选择 Next。
8. 在 Select destination server 页面上，请确保选中了本地服务器，然后选择 Next。
9. 在 Select server roles 页面上，选择 Active Directory Domain Services。在 Add Roles and Features Wizard 对话框中，确认 Include management tools (如果适用) 复选框已选中。选择 Add Features，然后选择 Next。
10. 在选择功能页面上，选择下一步。
11. 在 Active Directory Domain Services 页面上，选择 Next。
12. 在 Confirm installation selections 页面上，选择 Install。
13. 在安装 Active Directory 二进制文件后，选择 Close。
14. 打开 Server Manager 后，查找顶部单词 Manage 旁边的标记。当此标记变成黄色后，即可提升服务器。
15. 选择黄色标记，然后选择 Promote this server to a domain controller。
16. 在 Deployment Configuration 页面上，选择 Add a new forest。在 Root domain name (根域名) 中，键入 **`example.local`**，然后选择 Next (下一步)。
17. 在 Domain Controller Options 页面上，执行以下操作：
    - 在 Forest functional level 和 Domain functional level 中，选择 Windows Server 2016。
    - 在 Specify domain controller capabilities 下，确保 Domain Name System (DNS) server 和 Global Catalog (GC) 都处于选中状态。

- 键入并确认目录服务还原模式 (DSRM) 密码。然后选择下一步。

18. 在 DNS Options 页面上，忽略有关委托的警告，然后选择 Next。
19. 在 Additional options (其他选项) 页面上，确保 EXAMPLE 作为 NetBios 域名列出。
20. 在 Paths 页面上，保留默认设置，然后选择 Next。
21. 在 Review Options 页面上，选择 Next。现在，服务器会检查以确保域控制器的所有先决条件都得到满足。您可能会看到显示一些警告，不过您可以安全地忽略它们。
22. 选择安装。安装完成后，服务器会重启，然后变为正常运行的域控制器。

配置 VPC

下面三个过程将指导您完成在 Amazon 上为连接配置 VPC 的各个步骤。

配置 VPC 出站规则

1. 在Amazon Directory Service记录控制台，记录下Amazon您之前在中创建的 corp.example.com 的托管的 Microsoft AD 目录 ID基本教程 (p. 150).
2. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
3. 在导航窗格中，选择 Security Groups。
4. 搜索您的Amazon托管的 Microsoft AD 目录 ID。在搜索结果中，选择带描述的项目Amazon为创建安全组***xxxxxx***目录控制器.

   Note

   此安全组在您最初创建目录时自动创建。
5. 选择该安全组下方的 Outbound Rules 选项卡。依次选择 Edit 和 Add another rule，然后添加以下值：
   - 对于 Type，选择 All Traffic。
   - 对于 Destination，键入 **`0.0.0.0/0`**。
   - 将其他设置保留为默认值。
   - 选择 Save。

确保已启用 kerberos 预身份验证

1. 在 example.local 域控制器上，打开 Server Manager。
2. 在 Tools 菜单上，选择 Active Directory Users and Computers。
3. 导航到 Users (用户) 目录，右键单击任意用户并选择 属性，然后选择 Account (账户) 选项卡。在 Account options 列表中，向下滚动并确保未 选中 Do not require Kerberos preauthentication。
4. 从 corp.example.com-mgmt 实例对 corp.example.com 域执行相同的步骤。

配置 DNS 条件转发服务器

Note

条件转发器是网络上的 DNS 服务器，用于根据查询中的 DNS 域名转发 DNS 查询。例如，可以将 DNS 服务器配置为将它接收到的针对以 widgets.example.com 结尾的名称的所有查询转发到某个特定 DNS 服务器的 IP 地址或多个 DNS 服务器的 IP 地址。

1. 首先必须获取有关的一些信息AmazonManaged Microsoft AD。

   登录 Amazon Web Services Management Console，然后打开 Amazon Directory Service 控制台，网址为：https://console.aws.amazon.com/directoryservicev2/。

2. 在导航窗格中，选择 Directories。
3. 选择目录 ID适用于的AmazonManaged Microsoft AD。
4. 记下目录的完全限定域名 (FQDN) corp.example.com 和 DNS 地址。
5. 现在，返回到您的 example.local 域控制器，然后打开 Server Manager。
6. 在 Tools 菜单上，选择 DNS。
7. 在控制台树中，展开为其设置信任的域的 DNS 服务器，然后导航到 Conditional Forwarders。
8. 右键单击 Conditional Forwarders，然后选择 New Conditional Forwarder。
9. 在 DNS 域中，键入 **`corp.example.com`**。
10. UNDERIP 地址：主服务器的 IP 地址，选择< 点击这里添加... >，键入您的第一个 DNS 地址Amazon在托管的 Microsoft AD 目录（您已在上一个过程中记录），然后按Enter. 对第二个 DNS 地址执行相同的操作。在键入 DNS 地址之后，可能遇到“超时”或“无法解析”错误。通常可以忽略这些错误。
11. 选中 Store this conditional forwarder in Active Directory, and replicate as follows 复选框。在下拉菜单中，选择 All DNS servers in this Forest，然后选择 OK。

第 2 步：创建信任

在本部分中，您将创建两个单独的林信任。创建一个从 EC2 实例上的 Active Directory 域创建，另一个从上的创建。Amazon在托管的 Microsoft ADAmazon.

创建从 EC2 域到 的信任AmazonManaged Microsoft AD

1. 登录到 example.local。
2. 打开 Server Manager，然后在控制台树中选择 DNS。记下列出的服务器 IPv4 地址。在下一过程中，当您创建从 corp.example.com 到 example.local 目录的条件转发服务器时，您将需要此地址。
3. 在 Tools 菜单中，选择 Active Directory Domains and Trusts。
4. 在控制台树中，右键单击 example.local，然后选择 Properties。
5. 在 Trusts 选项卡上，选择 New Trust，然后选择 Next。
6. 在 Trust Name (信任名称) 页面上，键入 **`corp.example.com`**，然后选择 Next (下一步)。
7. 在 Trust Type 页面上，选择 Forest trust，然后选择 Next。

   Note

   Amazon托管的 Microsoft AD 还支持外部信任。但是，在此教程中，您将创建一个双向林信任。
8. 在 Direction of Trust 页面上，选择 Two-way，然后选择 Next。

   Note

   如果您稍后决定使用单向信任来尝试此操作，请确保正确设置信任方向（在信任域上传出，在信任域上传入）。有关一般信息，请参阅了解信任方向在微软的网站上。
9. 在 Sides of Trust 页面上，选择 This domain only，然后选择 Next。

10. 在 Outgoing Trust Authentication Level 页面上，选择 Forest-wide authentication，然后选择 Next。

    Note

    虽然 Selective authentication (选择性身份验证) 是一个选项，但为本教程简单起见，我们建议您在此处不要启用它。配置后，它会将对外部或林信任的访问仅限制为受信任域或林中的以下这类用户：已明确向这些用户提供对位于该受信任域或林中的计算机对象（资源计算机）的身份验证权限。有关更多信息，请参阅 。配置选择性验证设置.

11. 在 Trust Password 页面上，键入信任密码两次，然后选择 Next。在下一个过程中，您将使用这个相同的新密码。
12. 在 Trust Selections Complete 页面上，检查结果，然后选择 Next。
13. 在 Trust Creation Complete 页面上，检查结果，然后选择 Next。
14. 在 Confirm Outgoing Trust 页面上，选择 No, do not confirm the outgoing trust。然后选择下一个
15. 在 Confirm Incoming Trust 页面上，选择 No, do not confirm the incoming trust。然后选择下一个
16. 在 Completing the New Trust Wizard 页面上，选择 Finish。

Note

信任关系是AmazonManaged Microsoft AD。如果您正在使用多区域复制 (p. 54)，必须在主区域 (p. 55). 这些更改将自动应用于所有复制的区域。有关更多信息，请参阅 全球与区域功能 (p. 54)。

从中创建信任Amazon将微软 AD 托管到你的 EC2 域

1. 打开 Amazon Directory Service 控制台。
2. 选择 corp.example.com 目录。
3. 在存储库的目录详细信息页面上，执行以下操作之一：
   - 如果你在下面显示了多个地区多区域复制，选择主要区域，然后选择联网和安全“选项卡。有关更多信息，请参阅 主要与其他地区 (p. 55)。
   - 如果您没有在下方显示任何地区多区域复制，选择联网和安全“选项卡。
4. 在信任关系部分中，选择操作，然后选择添加信任关系。
5. 在 Add a trust relationship 对话框中，执行以下操作：
   - 在 Trust type (信任类型) 下，选择 Forest trust (林信任)。

     Note

     确保信任类型在此处选择与在之前过程中配置的相同信任类型匹配（创建从 EC2 域到的信任。AmazonManaged Microsoft AD)。
   - 对于 Existing or new remote domain name (现有或新的远程域名)，键入 example.local。
   - 对于 Trust password，键入您在上一过程中提供的相同密码。
   - 在 Trust direction (信任方向) 下，选择 Two-way (双向)。

     Note

     - 如果您稍后决定使用单向信任来尝试此操作，请确保正确设置信任方向（在信任域上传出，在信任域上传入）。有关一般信息，请参阅了解信任方向在微软的网站上。
     - 虽然 Selective authentication (选择性身份验证) 是一个选项，但为本教程简单起见，我们建议您在此处不要启用它。配置后，它会将对外部或林信任的访问仅限制为受信任域或林中的以下这类用户：已明确向这些用户提供对位于该受信任域或林中的计算机对象（资源计算机）的身份验证权限。有关更多信息，请参阅 。配置选择性验证设置.
   - 对于 Conditional forwarder (条件转发器)，键入 example.local 林中您的 DNS 服务器的 IP 地址（您在上一个过程中记录的地址）。

Note

条件转发器是网络上的 DNS 服务器，用于根据查询中的 DNS 域名转发 DNS 查询。例如，可以将 DNS 服务器配置为将它接收到的针对以 widgets.example.com 结尾的名称的所有查询转发到某个特定 DNS 服务器的 IP 地址或多个 DNS 服务器的 IP 地址。

6. 选择 Add (添加)。

第 3 步：验证信任

在此部分中，您将测试是否已成功在之间设置信任。Amazon和 Amazon EC2 上的活动目录。

验证信任

1. 打开 Amazon Directory Service 控制台。
2. 选择 corp.example.com 目录。
3. 在存储库的目录详细信息页面上，执行以下操作之一：
   - 如果你在下面显示了多个地区多区域复制，选择主要区域，然后选择联网和安全“选项卡。有关更多信息，请参阅 主要与其他地区 (p. 55)。
   - 如果您没有在下方显示任何地区多区域复制，选择联网和安全“选项卡。
4. 在信任关系部分中，选择刚创建的信任关系。
5. 选择 Actions，然后选择 Verify trust relationship。

一旦验证完成后，您应该可以看到 Status 下方显示 Verified。

祝贺您完成本教程！您现在有一个功能完备的包含多个林的 Active Directory 环境，您可以从该环境开始测试各种场景。其他测试实验室教程计划在 2018 年推出，因此，请不时回来了解新增功能。

故障排除AmazonMicrosoft Managed Managed Microsoft AD

以下内容可以帮助排查在创建或使用目录时可能会遇到的一些常见问题。

Netlogon 和安全渠道通信的问题

作为针对的缓解措施CVE 2020-1472，微软发布了修补程序，修改了域控制器处理 Netlogon 安全通道通信的方式。自引入这些安全的 Netlogon 更改以来，您可能无法接受某些 Netlogon 连接（服务器、工作站和信任验证）AmazonMicrosoft Managed Managed Microsoft AD。

要验证您的问题是否与 Netlogon 或安全渠道通信有关，请在 Amazon CloudWatch Logs 中搜索事件 ID 5827（与设备身份验证相关的问题）或 5828（与 AD 信任验证相关的问题）。有关 CloudWatch 的信息，请参阅Amazon请参阅托管的 Microsoft AD 的项启用日志转发 (p. 51).

有关针对 CVE-2020-1472 的缓解措施的更多信息，请参阅如何管理与 CVE-2020-1472 相关的 Netlogon 安全通道连接中的更改在微软的网站上。

密码找回

如果用户忘记密码或在登录到 Simple AD 时遇到问题或在登录时遇到问题Amazon托管 Microsoft AD 目录，你可以使用Amazon Web Services Management Console、Windows PowerShell 或AmazonCLI。

有关更多信息，请参阅重置用户密码 (p. 94)。

主题

- DNS 故障排除 (p. 162)
- Linux 域加入错误 (p. 162)
- 活动目录的可用存储空间不足 (p. 164)
- 架构扩展错误 (p. 166)
- 信托创建状态原因 (p. 167)

DNS 故障排除

你可以审核你的Amazon服务 Microsoft AD DNS 事件，从而更轻松地确定和排查 DNS 问题。例如，如果一条 DNS 记录缺失，您可以使用 DNS 审核事件日志帮助确定根本原因并修复该问题。通过检测和阻止来自可疑 IP 地址的请求，您还可以使用 DNS 审核事件日志提高安全性。

为此，您必须使用管理员账户或是成员的账户Amazon域名系统管理员组中)。有关此组的更多信息，请参阅创建的内容 (p. 10)。

排查问题AmazonDNS 托管的 Microsoft AD DNS

1. 通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 在左侧导航窗格中，选择 Instances (实例)。
3. 找到已加入您的 Amazon EC2 实例的位置Amazon托管 Microsoft AD 目录。选择该实例，然后选择 Connect (连接)。
4. 打开位于 Administrative Tools (管理工具) 文件夹中的 Event Viewer (事件查看器)。
5. 在 Event Viewer (事件查看器) 窗口中，选择 Action (操作)，然后选择 Connect to Another Computer (连接到另一台计算机)。
6. Select一台计算机，键入您的命令之一Amazon选择托管 Microsoft AD DNS 服务器名称或 IP 地址，然后选择确定.
7. 在左侧窗格中，导航到 Applications and Services Logs (应用程序和服务日志) >Microsoft>Windows>DNS-Server (DNS 服务器)，然后选择 Audit (审核)。

Linux 域加入错误

以下内容可帮助您排查在将 EC2 Linux 实例加入领域时可能遇到的一些错误消息：Amazon托管的 Microsoft AD 目录。

Linux 实例无法加入域或进行身份验证

Ubuntu 14.04、16.04 和 18.04 实例在 DNS 中必须可以反向解析，领域才能使用 Microsoft AD。否则，您可能会遇到以下两种场景之一：

方案 1: Ubuntu 实例尚未加入领域

对于尝试加入领域的 Ubuntu 实例，则该 `sudo realm join` 命令可能不会提供加入域所需的权限并可能显示以下错误：

！ 无法向活动目录进行身份验证：SASL (-1)：通用失败：GSSAPI 错误：提供了无效的名称（成功）adcli：无法连接到 EXAMPLE.COM 域名：无法向活动目录进行身份验证：SASL (-1)：通用失败：GSSAPI 错误：提供了无效的名字（成功）！没有足够的权限加入域名领域：无法加入领域：没有足够的权限加入域

方案 2: Ubuntu 实例已加入领域

对于已加入 Microsoft AD 域的 Ubuntu 实例，SSH 尝试使用域凭证进入实例可能会失败，并显示以下错误：

$ ssh admin@EXAMPLE.COM@198.51.100

没有这样的身份：/username/.ssh/ID_ed25519：没有这样的文件或目录

admin@EXAMPLE.COM@198.51.100 的密码：

权限被拒绝，请重试。

admin@EXAMPLE.COM@198.51.100 的密码：

如果您使用公钥登录到实例并检查`/var/log/auth.log`，您可能会看到以下有关无法找到用户的错误：

5 月 12 日 01:02:12 ip-192-0-2-0 sshd[2251]：pam_unix(sshd:auth)：身份验证失败；logname= uid=0 euid=0 tty=ssh ruser= rhost=203.0.113.0

5 月 12 日 01:02:12 ip-192-0-2-0 sshd[2251]：pam_sss(sshd:auth)：身份验证失败；logname= uid=0 euid=0 tty=ssh ruser= rhost=203.0.113.0 user=admin@EXAMPLE.COM

5 月 12 日 01:02:12 ip-192-0-2-0 sshd [2251]：pam_sss (sshd: auth)：已收到用户 admin@EXAMPLE.COM：10（底层身份验证模块不知道的用户）

5 月 12 日 01:02:14 ip-192-0-2-0 sshd [2251]：来自 203.0.113.0 端口 13344 ssh2 的无效用户 admin@EXAMPLE.COM 的密码失败

5 月 12 日 01:02:15 ip-192-0-2-0 sshd [2251]：已通过 203.0.113.0 [preauth] 关闭连接

但是，`kinit`因为用户仍然有效。看这个例子：

ubuntu @ip -192-0-2-0：~$ kinit admin@EXAMPLE.COM admin@EXAMPLE.COM 的密码：ubuntu @ip -192-0-2-0：~$ klist 票证缓存：文件：/tmp/krb5cc_1000 默认主体：admin@EXAMPLE.COM

解决办法

这两种场景当前推荐的解决方法是禁用反向 DNS，`/etc/krb5.conf`在 [libdefault] 部分中，如下所示：

```
[libdefaults]
default_realm = EXAMPLE.COM
rdns = false
```

无缝域加入的单向信任身份验证问题

如果你在你之间建立了单向传出信任Amazon托管 Microsoft AD 和你的本地 AD，当尝试使用 Winbind 的受信任 AD 凭据对加入域的 Linux 实例进行身份验证时，你可能会遇到身份验证问题。

错误

7 月 31 日 00:00:00 ec2amaz-lsmwqt sshd [23832]：来自 xxx.xxx.xxx.xxx 端口 18309 ssh2 的 user@corp.example.com 密码失败

7 月 31 日 00:05:00 ec2amaz-lsmwqt sshd [23832]：pam_winbind (sshd: auth)：获取密码 (0x00000390)

7 月 31 日 00:05:00 ec2amaz-lsmwqt sshd [23832]：pam_winbind (sshd: auth)：pam_get_item 返回了密码

7 月 31 日 00:05:00 ec2amaz-lsmwqt sshd [23832]：pam_winbind (sshd: auth)：请求 WBcLOGONUN 用户失败：WBC_ERR_AUTH_ERROR，PAM 错误：PAM_SYSTEM_ERR (4)，NTSTATUS: **NT_STATUS_OBJECT_NAME_NOT_NOT_FOUND**，错误消息是：找不到对象名称。

7 月 31 日 00:05:00 ec2amaz-lsmWQT sshd [23832]：pam_winbind (sshd: auth)：内部模块错误（retval = PAM_SYSTEM_ERR (4)，用户 = '公司\ 用户'）

解决办法

要解决此问题，您需要注释掉或从 PAM 模块配置文件中删除指令 (`/etc/security/pam_winbind.conf`) 使用以下步骤。

1. 在文本编辑器中打开 `/etc/security/pam_winbind.conf` 文件。

```
sudo vim /etc/security/pam_winbind.conf
```

2. 注释掉或删除以下指令krb5_auth = 是.

```
[global]

cached_login = yes
krb5_ccache_type = FILE
#krb5_auth = yes
```

3. 停止 Winbind 服务，然后重新启动它。

```
service winbind stop or systemctl stop winbind
net cache flush
service winbind start or systemctl start winbind
```

活动目录的可用存储空间不足

当你的Amazon由于 Active Directory 的可用存储空间不足而受损，需要立即采取措施才能将目录恢复到活动状态。这种损伤的两个最常见原因在以下章节中介绍：

1. SYSVOL 文件夹存储的不仅仅是重要的组策略对象 (p. 164)
2. Active Directory 数据库已填满卷 (p. 164)

有关的定价信息Amazon请参阅托管的 Microsoft AD 存储空间Amazon Directory Service定价.

SYSVOL 文件夹存储的不仅仅是重要的组策略对象

此损伤的一个常见原因是由于存储在 SYSVOL 文件夹中进行组策略处理的非必要文件。这些非必要文件可以是 EXE、MSI 或进行组策略处理时不必要的任何其他文件。要处理的组策略的基本对象是组策略对象、登录/注销脚本和组策略对象的中央存储。任何非必要文件都应存储在以外的文件服务器上Amazon托管 Microsoft AD 域控制器。

如果需要文件进行组策略软件安装，则应使用文件服务器来存储这些安装文件。如果您不希望自行管理文件服务器，Amazon提供受管文件服务器选项，Amazon FSx.

要删除任何不必要的文件，您可以通过通用命名约定 (UNC) 路径访问 SYSVOL 共享。例如，如果您的域的完全限定域名 (FQDN) 是 example.com，则 SYSVOL 的 UNC 路径将为“\\example.local\SYSVOL\example.local\”。一旦找到并删除组策略处理目录时不必要的对象，该目录应该在 30 分钟内恢复到活动状态。如果 30 分钟后该目录未处于活动状态，请联系AmazonSupport。

仅在 SYSVOL 共享中存储基本的组策略文件的作法可确保您不会因 SYSVOL 膨胀而损害您的目录。

Active Directory 数据库已填满卷

此损害的一个常见原因是由于 Active Directory 数据库填充卷。要验证是否属于这种情况，您可以查看目录中对象的总计数量。我们将总计文字加粗，以确保您了解已删除的对象仍然计入目录中的对象总数。

默认情况下Amazon在成为回收对象之前，托管 Microsoft AD 会将项目保留在 AD 回收站中 180 天。一旦一个对象成为回收对象（逻辑删除），它会再保留 180 天，然后才最终从目录中清除。因此，当一个对象被删除时，它会在目录数据库中存在 360 天，然后再清除。这就是需要评估对象总数的原因。

有关更多详细信息Amazon受管 Microsoft AD 支持的对象计数，请参阅Amazon Directory Service定价.

要获取包含已删除对象的目录中的对象总数，可以从加入 Windows 实例的域运行以下 PowerShell 命令。有关如何设置管理实例的步骤，请参阅在中管理用户和组AmazonMicrosoft Managed Microsoft AD (p. 93)。

```
Get-ADObject -Filter * -IncludeDeletedObjects | Measure-Object -Property 'Count' | Select-
Object -Property 'Count'
```

下面是运行上述命令的示例输出：

```
Count
10000
```

如果总计数高于上述注释中列出的目录大小支持的对象计数，则表示您已超出目录的容量。

以下选项用于解决此损害：

1. 清理 AD
   a. 删除任何不需要的 AD 对象。
   b. 从 AD 回收站中删除任何不需要的对象。请注意，此操作是破坏性的，恢复这些已删除对象的唯一方法是执行目录的还原。
   c. 以下命令将从 AD 回收站中删除所有已删除的对象。

      Important

      请谨慎使用此命令，因为这是一个破坏性命令，恢复这些已删除对象的唯一方法是执行目录的还原。

```
$DomainInfo = Get-ADDomain
$BaseDn = $DomainInfo.DistinguishedName
$NetBios = $DomainInfo.NetBIOSName
$ObjectsToRemove = Get-ADObject -Filter { isDeleted -eq $true } -
IncludeDeletedObjects -SearchBase "CN=Deleted Objects,$BaseDn" -Properties
 'LastKnownParent','DistinguishedName','msDS-LastKnownRDN' | Where-Object
 { ($_.LastKnownParent -Like "*OU=$NetBios,$BaseDn") -or ($_.LastKnownParent -Like '*
\0ADEL:*') }
ForEach ($ObjectToRemove in $ObjectsToRemove) { Remove-ADObject -Identity
 $ObjectToRemove.DistinguishedName -IncludeDeletedObjects }
```

   d. 打开一个案例AmazonSupport 要求Amazon Directory Service收回可用空间。
2. 如果您的目录类型为标准版，请向创建一个案例AmazonSupport 请求将您的目录升级到企业版。这也会增加您目录的成本。有关定价信息，请参阅 Amazon Directory Service 定价。

InAmazon托管微软 AD，成员Amazon委派的删除对象生命周期管理员组有能力修改`msDS-DeletedObjectLifetime`属性，该属性可设置已删除对象在成为回收对象之前保留在 AD 回收站中的天数。

Note

这是一个高级主题。如果配置不当，则可能导致数据丢失。我们强烈建议您先查看AD 回收站：了解、实施、最佳实践和故障排除以便更好地了解这些过程。

将 `msDS-DeletedObjectLifetime` 属性值更改为较低的数值的能力有助于确保您的对象计数不会超过支持的级别。此属性可设置为的最低有效值为 2 天。超过该值后，您将无法再使用 AD 回收站恢复已删除的对

象。需要从快照还原目录才能恢复这样的对象。有关更多信息，请参阅 快照或恢复你的目录 (p. 118)。任何快照还原都会导致数据丢失，因为它们是一些时间点。

要更改目录的已删除对象生命周期，请运行以下命令：

> Note
>
> 如果按原样运行命令，它会将“Deleted Object Lifetime (删除对象生命周期)”属性值设置为 30 天。如果您想使生命周期更长或更短，请用您希望的任何数字替换“30”。但是，我们建议您不要高于默认数字 180。

```
$DeletedObjectLifetime = 30
$DomainInfo = Get-ADDomain
$BaseDn = $DomainInfo.DistinguishedName
Set-ADObject -Identity "CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration,
$BaseDn" -Partition "CN=Configuration,$BaseDn" -Replace:@{"msDS-DeletedObjectLifetime" =
 $DeletedObjectLifetime}
```

架构扩展错误

以下内容可帮助您排查在为您的架构扩展时可能遇到的一些错误消息。Amazon托管的 Microsoft AD 目录。

引用

错误

从第 1 行开始添加输入错误：引用 The server side error is: 0x202b A 引用站点。扩展服务器错误是：0000202B：引用: DSID-0310082F, data 0, 1 个接入点\ tref 1: 'example.com' Number for Objects Modified: 0 0

故障排除

确保所有可分辨名称字段都具有正确的域名。在上述示例中，`DC=example,dc=com` 应替换为 cmdlet `Get-ADDomain` 显示的 `DistinguishedName`。

无法读取导入文件

错误

Unable to read the import file. Number for Objects Modified: 0

故障排除

导入的 LDIF 文件为空 (0 字节)。确保已上传正确的文件。

语法错误

错误

There is a syntax error in the input file Failed on line 21. The last token starts with 'q'. Number for Objects Modified: 0

故障排除

第 21 行的文本格式不正确。无效文本的第一个字母是 `A`。用有效的 LDIF 语法更新第 21 行。有关如何设置 LDIF 文件格式的更多信息，请参阅第 1 步：创建 LDIF 文件 (p. 113)。

属性或值存在

错误

从第 1 行开始添加输入错误：属性或值存在 The server side error is: 0x2083 The 指定的值已存在。扩展服务器错误是：00002083: AreRR：DSID-03151830, #1:\ t0: 00002083: DSID-03151830, 问题1006 (ATT_OR_VALUE_EXISTS), data 0, Att 20019 (可能包含): len 4 Number for Objects Modified: 0 0

故障排除

架构更改已应用。

没有此类属性

错误

从第 1 行开始添加输入错误：无此类属性 The server side error is: 0x2085 The Attribute value 无法删除, 因为对象上不存在属性值。扩展服务器错误是：00002085: AreRR：DSID-03152367, #1:\ t0: 00002085: DSID-03152367, 问题1001 (NO_ATTRIBETE_OR_VAL), data 0, Att 20019 (可能包含): len 4 Number for Objects Modified: 0 0

故障排除

LDIF 文件正尝试从一个类中删除属性，但该属性当前未附加到该类。可能已应用架构更改。

错误

Add error on entry entry line 41: 无此类属性 0x57 The parameter is error. The extended server error is: 0x208d Directory object not found. 扩展服务器错误是：“00000057: IdPaperR：DSID-0C090D8A，评论：Number in 属性转换操作, data 0, v2580" Number for Objects Modified: 0 0

故障排除

第 41 行中列出的属性不正确。请复查拼写。

没有此类对象

错误

从第 1 行开始添加输入错误：无此类对象 The server side error is: 0x208d Directory object 找不到. 扩展服务器错误是：0000208D: NameErr：DSID-03100238，问题 2001 年（NO_OBJECT），数据 0，最佳匹配：'CN=Schema, CN=Configuration, DC=example, DC=com 'Number for Objects Modified: 0 0

故障排除

可分辨名称 (DN) 引用的对象不存在。

信托创建状态原因

信任创建失败时，状态消息中将包含其他信息。以下信息可帮助您理解这些消息的含义。

访问被拒绝

尝试创建信任时访问被拒绝。信任密码不正确，或远程域的安全设置不允许配置信任。要解决此问题，请尝试以下操作：

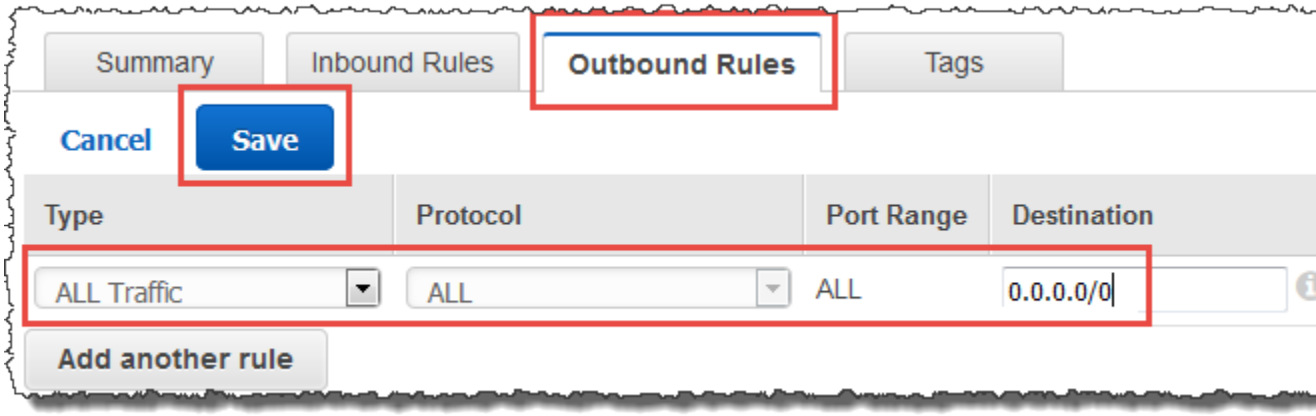
- 请验证使用的信任密码与在远程域上创建相应信任时使用的密码相同。
- 验证域安全设置允许创建信任。

- 验证本地安全策略设置是否正确。具体来说，检查 `Local Security Policy > Local Policies > Security Options > Network access: Named Pipes that can be accessed anonymously` 并确保其至少包含以下三个命名管道：
  - netlogon
  - samr
  - lsarpc
- 验证上述命名管道是否作为上的值存在NULL 会话管道注册表路径中的注册表项HKLM\ SYSTEM\ CurrentControlSet\ 服务\ LanManan 服务器\ 参数. 必须将这些值插入到分隔的行上。

> **Note**
>
> 默认情况下，`Network access: Named Pipes that can be accessed anonymously` 未设置并显示 `Not Defined`。这是正常的，因为域控制器对于 `Network access: Named Pipes that can be accessed anonymously` 的有效默认设置为 `netlogon`、`samr`、`lsarpc`。

指定域名不存在或无法访问

目的回复要解决此问题，请确保域的安全组设置和 VPC 的访问控制列表 (ACL) 正确，并已准确输入条件转发服务器信息。Amazon将安全组配置为仅打开 Active Directory 通信所需的端口。在默认配置中，安全组接受从任意 IP 地址到这些端口的流量。出站流量仅限于安全组。您需要更新安全组上的出站规则，以允许流量进入本地网络。有关安全要求的更多信息，请参阅第 2 步：准备您的Amazon托管的 Microsoft AD (p. 103).



如果其他目录网络的 DNS 服务器使用公有 (非 RFC 1918) IP 地址，则需要在目录服务控制台到 DNS 服务器的目录上添加 IP 路由。有关更多信息，请参阅创建、验证或删除信任关系 (p. 98)和先决条件 (p. 97)。

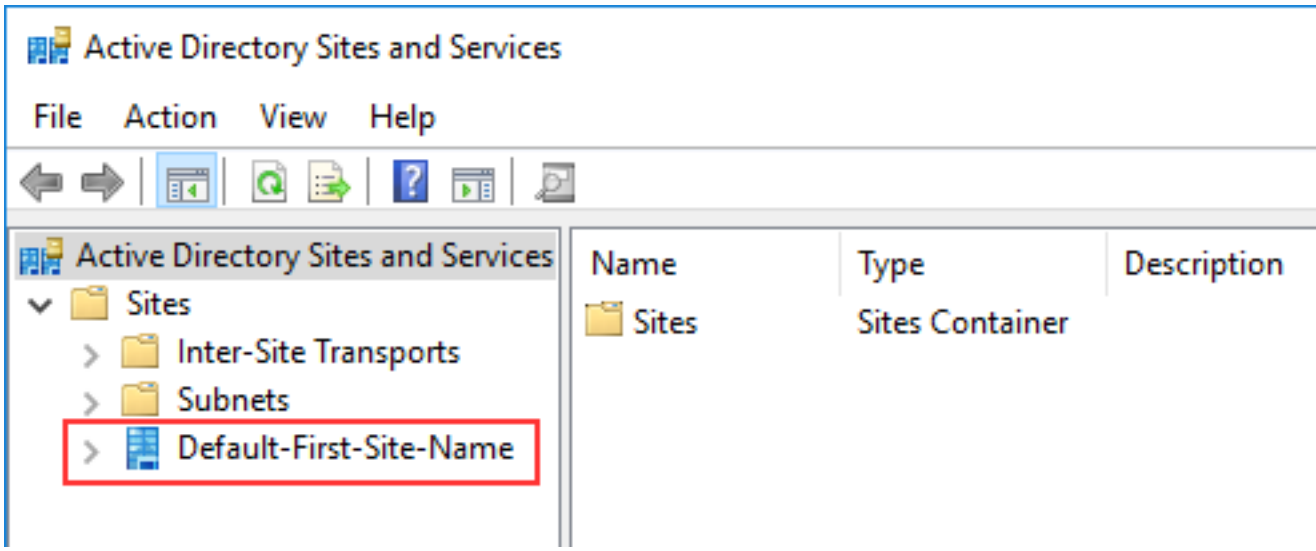
互联网号码分配机构 (IANA) 为私有互联网预留了以下三个 IP 地址空间块：

- 10.0.0.0 - 10.255.255.255（10/8 前缀）
- 172.16.0.0 - 172.31.255.255（172.16/12 前缀）
- 192.168.0.0 - 192.168.255.255（192.168/16 前缀）

有关更多信息，请参阅 。https://tools.ietf.org/html/rfc1918.

验证默认 AD 站点名称为了您的Amazon托管的 Microsoft AD 与默认 AD 站点名称在本地基础设施中。计算机使用计算机所属的域而不是用户的域来确定站点名称。重命名站点以匹配最近的本地可确保 DC 定位器将使用来自最近站点的域控制器。如果这样做不能解决问题，则可能是缓存了以前创建的条件转发服务器的信息，从而阻止创建新信任。请等待几分钟，然后再次尝试创建信任和条件转发服务器。

有关其工作方式的更多信息，请参阅。森林信托中的域定位器在微软的网站上。



操作无法在此域中执行。

要解决此问题，请确保两个域/目录都没有重叠的 NETBIOS 名称。如果域/目录确实有重叠的 NETBIOS 名称，请使用不同的 NETBIOS 名称重新创建其中一个，然后重试。

信任创建失败是因为错误 “必需且有效的域名”

DNS 名称只能包含字母字符 (A-Z)、数字字符 (0-9)、减号 (-) 和句点 (.)。仅当句点字符用于分隔域样式名称的组成部分时，才允许使用它们。另外，请考虑以下事项：

- Amazon托管 Microsoft AD 不支持使用单一标签域的信任。有关更多信息，请参阅 。微软对单一标签域的支持.
- 根据 RFC 1123 (https://tools.ietf.org/html/rfc1123) ，DNS 标签中唯一可以使用的字符是 “A” 到 “Z”、“a” 到 “z”、“0” 到 “9" 以及连字符 (“-”)。DNS 名称中也使用句点 [.]，但仅在 DNS 标签之间和 FQDN 结束时使用。
- 根据 RFC 952 (https://tools.ietf.org/html/rfc952)，“名称” (网络、主机、网关或域名) 是从字母表 (A-Z) 、数字 (0-9) 、减号 (-) 和句点 (.) 中抽取的最多 24 个字符的文本字符串。请注意，只有在句点用于分隔 “域样式名称” 的组成部分时才允许使用。

有关更多信息，请参阅 。遵守主机和域名的名称限制在微软的网站上。

测试信任的常用工具

以下是可用于排除各种信任相关问题的工具。

AmazonSystems Manager 自动化排除工具

Support 自动化工作流 (SAW)杠杆作用AmazonSystems Manager 自动化为您提供预定义的运行手册 Amazon Directory Service. 这些区域有：AWSSupport-TroubleshootDirectoryTrustrunbook 工具可以帮助您诊断之间的常见信任创建问题AmazonMicrosoft AD 和本地 Microsoft Active Directory。

DirectoryServicePortTest 工具

这些区域有：DirectoryServicePortTest测试工具在排除之间的信任创建问题时非常有用。Amazon托管微软 AD 和本地活动目录。有关如何使用工具的示例，请参阅测试 AD Connector (p. 175)。

NETDOM 和 NLTEST 工具

管理员可以使用Netdom和最新用于查找、显示、创建、删除和管理信任的命令行工具。这些工具直接与域控制器上的 LSA 授权机构进行通信。有关如何使用这些工具的示例，请参阅Netdom和NLTEST在微软的网站上。

数据包捕获工具

你可以使用内置的 Windows 软件包捕获实用程序来调查和解决潜在的网络问题。有关更多信息，请参阅 。无需安装任何东西即可捕获网络.

Active Directory Connector

AD Connector 是一种目录网关，借助它可以将目录请求重定向到本地 Microsoft Active Directory，而无需在云中缓存任何信息。AD Connector 有两种大小，即小型和大型。您可以跨多个 AD Connector 分布应用程序负载，根据您的性能需求进行扩展。没有强制实施的用户或连接限制。

AD Connector 不支持 AD 传递信任。AD 连接器和本地 AD 域具有 1 对 1 关系。也就是说，对于每个本地域，包括 AD 林中您要针对其进行身份验证的子域，必须创建唯一的 AD Connector。

> Note
>
> AD Connector 不能与其他人共享Amazon账户。如果这是一项要求，请考虑使用Amazon将 Microsoft AD 托管到共享您的目录 (p. 58). AD Connector 也不知道多 VPC，这意味着AmazonLIKE 应用WorkSpaces需要将与 AD Connector 配置到与 AD 连接器相同的 VPC 中。

设置之后，AD Connector 具备以下优势：

- 最终用户和 IT 管理员可以使用其现有企业凭证登录Amazon应用程序，如 WorkSpaces、Amazon WorkDocs 或 Amazon WorkMail。
- 你可以管理Amazon通过基于 IAM 角色的访问权限，例如 Amazon EC2 实例或 Amazon S3 存储桶。Amazon Web Services Management Console.
- 您可以始终如一地实施现有安全策略（如密码过期、密码历史和账户锁定），无论用户或 IT 管理员是访问本地基础设施还是 Amazon 云中的资源。
- 可以通过与基于 RADIUS 的现有 MFA 基础设施集成，使用 AD Connector 启用多重验证，从而在用户访问时增加一层安全性。Amazon应用程序。

继续阅读本节中的主题，了解如何连接到目录以及充分利用 AD Connector 功能。

主题

- AD Connector 入门 (p. 171)
- 如何管理 AD Connector (p. 182)
- AD Connector 的最佳实践 (p. 203)
- AD Connector 配额 (p. 205)
- AD Connector 的应用程序兼容性策略 (p. 205)
- 排查 AD Connector (p. 205)

AD Connector 入门

有了 AD Connector，你可以连接Amazon Directory Service使用转到您的现有企业目录。当连接到您的现有目录时，您的所有目录数据仍保留在域控制器上。Amazon Directory Service 不复制您的任何目录数据。

主题

- AD Connetor (p. 171)
- 创建AD Connector (p. 181)
- 创建的内容 (p. 182)

AD Connetor

要使用 AD Connector，您需要以下内容：

VPC

对 VPC 进行如下设置：

- 至少两个子网。每个子网必须位于不同的可用区。
- 必须通过虚拟专用网络 (VPN) 连接或 Amazon Direct Connect 将 VPC 连接到您的现有网络。
- VPC 必须具有默认硬件租户。

Amazon Directory Service使用双 VPC 结构。组成您的目录的 EC2 实例在您的Amazon账户，并由管理Amazon. 它们有两个网络适配器，`ETH0`和`ETH1`.`ETH0`是管理适配器，存在于您的账户之外。`ETH1`是在您的账户中创建的。

您的目录的管理 IP 范围`ETH0`network 是以编程方式选择的，以确保它不会与部署目录的 VPC 冲突。此 IP 范围可以是以下任意一对（因为目录在两个子网中运行）：

- 10.0.1.0/24 和 10.0.2.0/24
- 192.168.1.0/24 和 192.168.1.0/24

我们通过检查第一个二进制八位数来避免冲突`ETH1`CIDR。如果它以 10 开头，则我们选择子网 192.168.1.0/24 和 192.168.1.0/24 和 192.168.1.0/24 选择子网192.168.1.0/24。如果第一个二进制八位数不是 10，则选择子网10.0.0/16 VPC，子网10.0.0/24 和 10.0.1.0/24 选择子网10.0.0/16 VPC。

选择算法不包括您的 VPC 上的路由。因此，这种情况可能会导致 IP 路由冲突。

不得 使用以下 VPC 终端节点配置 VPC：

- 路线 53 VPC 终端节点其中包含 *.amazonaws.com 的 DNS 条件覆盖，这些覆盖解析为非公开 AmazonIP 地址
- CloudWatch VPC 终端节点
- Systems Manager VPC 端点
- Service VPC 终端节

有关更多信息，请参阅 Amazon VPC 用户指南 中的以下主题：

- Amazon VPC 是什么？
- 您 VPC 中的子网
- 在您的 VPC 中添加硬件虚拟专用网关

有关 Amazon Direct Connect 的更多信息，请参阅《Amazon Direct Connect 用户指南》。

现有 Active Directory

您将需要连接到具有 Active Directory 域的现有网络。

> **Note**
>
> AD Connector 不支持单标签域.

此域的功能级别必须是`Windows Server 2003`或更高版本。AD Connector 还支持连接到 Amazon EC2 实例上托管的域。

> **Note**
>
> AD Connector 在与 Amazon EC2 域加入功能结合使用时，不支持只读域控制器 (RODC)。

服务账户

您必须拥有现有目录中被委派了以下权限的服务账户的凭证：

- 读取用户和组 – 必需
- 将计算机加入域 - 仅当使用“无缝域加入”功能和 时是必需的 WorkSpaces
- 创建计算机对象 – 仅当使用无缝域加入和 时必需 WorkSpaces

有关更多信息，请参阅 向您的服务账户委派权限 (p. 174)。

> **Note**
>
> AD Connector 使用 Kerberos 进行身份验证和授权Amazon应用程序。LDAP 仅用于用户和组对象查找（读取操作）。对于 LDAP 事务，没有任何内容是可变的，凭据也不会以明文形式传递。身份验证由Amazon内部服务，它使用 Kerberos 票证以用户身份执行 LDAP 操作。

用户权限

所有 Active Directory 用户必须有权读取自己的属性。具体而言，包括以下属性：

- GivenName
- SurName
- Mail
- SamAccountName
- UserPrincipalName
- UserAccountControl
- MemberOf

默认情况下，Active Directory 用户确实有权读取这些属性。但是，管理员可以随时修改这些权限，因此您可能希望在设置 AD Connector 之前，验证用户是否具有这些读取权限。

IP 地址

获取您现有目录域中两个 DNS 服务器或域控制器的 IP 地址。

AD Connector 获得`_ldap._tcp.`*`<DnsDomainName>`*和`_kerberos._tcp.`*`<DnsDomainName>`*连接到您的目录时将来自这些服务器的 SRV 记录，因此这些服务器必须包含这些 SRV 记录。AD Connector 尝试查找将同时提供 LDAP 和 Kerberos 服务的公用域控制器，因此这些 SRV 记录必须至少包含一个公用域控制器。有关 SRV 记录的更多信息，请转至SRV 资源记录在Micros TechNet.

子网的端口

为使 AD Connector 能够将目录请求重定向到您的现有 Active Directory 域控制器，现有网络的防火墙必须对 Amazon VPC 中的两个子网的 CIDR 开放以下端口。

- TCP/UDP 53 - DNS
- TCP/UDP 88 - Kerberos 身份验证
- TCP/UDP 389 - LDAP

这些是 AD Connector 能够连接到目录所需的最少端口。根据您的特定配置，您可能需要打开其他端口。

> **Note**
>
> 如果现有 Active Directory 域的 DNS 服务器或域控制器服务器在 VPC 内，与这些服务器相关的安全组必须向 VPC 中的两个子网的 CIDR 开放上述端口。

有关其他端口要求，请参阅AD 和 AD DS 端口要求在Micros TechNet.

Kerberos 预身份验证

用户账户必须启用 Kerberos 预身份验证。有关如何启用此设置的详细说明，请参阅确保启用 Kerberos 预身份验证 (p. 101)。有关此设置的一般信息，请转至预身份验证在Micros TechNet.

加密类型

当通过 Kerberos 对您的 Active Directory 域控制器进行身份验证时，AD Connector 支持以下加密类型：

- AES-256-HMAC
- AES-128-HMAC
- RC4-HMAC

Amazon IAM Identity Center (successor to Amazon Single Sign-On)先决条件

如果计划将 IAM Identice Center 与AD Connector，则需要确保满足以下条件：

- 您的 AD Connector 已在您的Amazon组织的管理账户。
- 您的 IAM 身份中心实例位于您在其中设置AD Connector 的同一区域中。

有关更多信息，请参阅 。IAM 身份中心先决条件中的Amazon IAM Identity Center (successor to Amazon Single Sign-On)用户指南。

多重验证先决条件

为了使用您的 AD Connector 目录支持多重验证，您需要以下内容：

- 现有网络中具有两个客户端终端节点的远程身份验证拨入用户服务 (RADIUS) 服务器。RADIUS 客户端终端节点具有以下要求：
  - 要创建终端节点，您需要 Amazon Directory Service 服务器的 IP 地址。这些 IP 地址可以从目录详细信息的 Directory IP Address 字段中获取。
  - 两个 RADIUS 终端节点必须使用相同的共享密码。
- 您的现有网络必须允许通过默认的 RADIUS 服务器端口 (1812) 从 Amazon Directory Service 服务器传入入站流量。
- 您的 RADIUS 服务器与您的现有目录的用户名必须相同。

有关将 AD Connector 与 MFA 结合使用的更多信息，请参阅为 AD Connector 启用多重验证 (p. 183).

向您的服务账户委派权限

要连接到现有目录，您必须在现有目录中拥有被委派了某些权限的 AD Connector 服务账户的凭证。尽管 Domain Admins 组的成员有足够的权限连接到目录，但是作为最佳实践，您应使用仅具有连接到目录所需的最小权限的服务账户。以下过程演示如何创建名为 `Connectors` 的新组，委派将 Amazon Directory Service 连接到该组所需的必要权限，然后将新服务账户添加到该组。

必须在已加入到目录且已安装 Active Directory User and Computers MMC 管理单元的计算机上执行此过程。您还必须以域管理员身份登录。

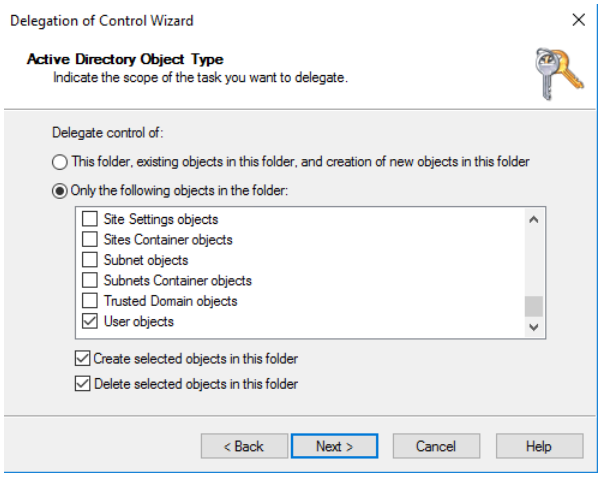
向您的服务账户委派权限

1. 打开 Active Directory User and Computers 并在导航树中选择您的域根。
2. 在左侧窗格的列表中，右键单击 Users，选择 New，然后选择 Group。
3. 在 New Object - Group 对话框中，输入以下内容，然后单击 OK。

字段	值/选择
Group name	`Connectors`
Group scope	Global
Group type	安全性

4. 在 Active Directory User and Computers 导航树中，选择您的域根。在菜单中，选择 Action，然后选择 Delegate Control。如果您的 AD Connector 已连接到Amazon托管 Microsoft AD，你将无权访问域根级别的委派控制权。在这种情况下，要委派控制权，请在目录 OU 下选择将在其中创建计算机对象的 OU。

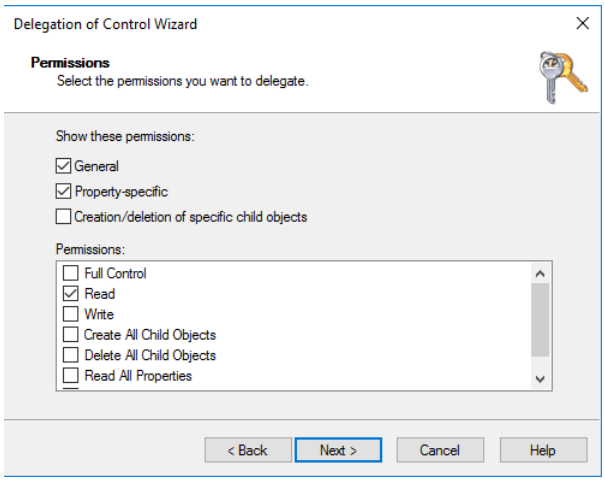
5. 在 Delegation of Control Wizard 页面上，单击 Next，然后单击 Add。
6. 在 Select Users, Computers, or Groups 对话框中，输入 `Connectors`，然后单击 OK。如果找到多个对象，请选择上面创建的 `Connectors` 组。单击 Next（下一步）。
7. 在 Tasks to Delegate 页面上，选择 Create a custom task to delegate，然后选择 Next。
8. 选择 Only the following objects in the folder，然后选择 Computer objects 和 User objects。
9. 选择 Create selected objects in this folder，然后选择 Delete selected objects in this folder。然后选择下一步。



10. 选择 Read，然后选择 Next。

    Note

    如果您要使用无缝域加入或 WorkSpaces，您还必须启用Write权限，这样 Active Directory 就可以创建计算机对象。



11. 在 Completing the Delegation of Control Wizard 页面上验证信息，然后单击 Finish。
12. 使用强密码创建一个用户账户，并将该用户添加到 `Connectors` 组。此用户将被称为您的 AD Connector 服务账户，由于它现在是`Connectors`组它现在具有足够的权限将连接Amazon Directory Service使用转到目录。

测试 AD Connector

为使 AD Connector 能够连接到您的现有目录，现有网络的防火墙必须对 VPC 中的两个子网的 CIDR 开放特定的端口。要测试是否满足这些条件，请执行以下步骤：

测试 连接

1. 在 VPC 中启动一个 Windows 实例并通过 RDP 连接它。实例必须是您现有域的成员。在该 VPC 实例上执行剩余步骤。
2. 下载并解压缩DirectoryServicePortTest测试应用程序。其中包含源代码及 Visual Studio 项目文件，您可以根据需要修改该测试应用程序。

   Note

   Windows Server 2003 及更低版本的操作系统不支持此脚本。
3. 在 Windows 命令提示符下，使用以下选项运行 DirectoryServicePortTest 测试应用程序：

   Note

   这些区域有： DirectoryServicePortTest 测试应用程序只能在域和林功能级别设置为 Windows Server 2012 R2 及更低版本时使用。

```
DirectoryServicePortTest.exe -d <domain_name> -ip <server_IP_address> -tcp "53,88,389"
 -udp "53,88,389"
```

<domain_name>

完全限定域名。这可用于测试林和域功能级别。如果不指定域名，则不测试功能级别。

<server_IP_address>

现有域中域控制器的 IP 地址。将针对该 IP 地址来测试端口。如果不指定 IP 地址，则不测试端口。

此测试应用程序确定是否打开了从 VPC 到域的必要端口，并验证最低的林和域功能级别。

该输出值将类似于以下内容：

```
Testing forest functional level.
Forest Functional Level = Windows2008R2Forest : PASSED

Testing domain functional level.
Domain Functional Level = Windows2008R2Domain : PASSED

Testing required TCP ports to <server_IP_address>:
Checking TCP port 53: PASSED
Checking TCP port 88: PASSED
Checking TCP port 389: PASSED

Testing required UDP ports to <server_IP_address>:
Checking UDP port 53: PASSED
Checking UDP port 88: PASSED
Checking UDP port 389: PASSED
```

以下是 DirectoryServicePortTest 应用程序的源代码。

```
/*
   Copyright 2010-2019 Amazon.com, Inc. or its affiliates. All Rights Reserved.

   This file is licensed under the Apache License, Version 2.0 (the "License").
   You may not use this file except in compliance with the License. A copy of
   the License is located at

    http://aws.amazon.com/apache2.0/
```

```
   This file is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR
   CONDITIONS OF ANY KIND, either express or implied. See the License for the
   specific language governing permissions and limitations under the License.
*/
using System;
using System.Collections.Generic;
using System.IO;
using System.Linq;
using System.Net;
using System.Net.Sockets;
using System.Text;
using System.Threading.Tasks;
using System.DirectoryServices.ActiveDirectory;
using System.Threading;
using System.DirectoryServices.AccountManagement;
using System.DirectoryServices;
using System.Security.Authentication;
using System.Security.AccessControl;
using System.Security.Principal;

namespace DirectoryServicePortTest
{
    class Program
    {
        private static List<int> _tcpPorts;
        private static List<int> _udpPorts;

        private static string _domain = "";
        private static IPAddress _ipAddr = null;

        static void Main(string[] args)
        {
            if (ParseArgs(args))
            {
                try
                {
                    if (_domain.Length > 0)
                    {
                        try
                        {
                            TestForestFunctionalLevel();

                            TestDomainFunctionalLevel();
                        }
                        catch (ActiveDirectoryObjectNotFoundException)
                        {
                            Console.WriteLine("The domain {0} could not be found.\n",
 _domain);
                        }
                    }

                    if (null != _ipAddr)
                    {
                        if (_tcpPorts.Count > 0)
                        {
                            TestTcpPorts(_tcpPorts);
                        }

                        if (_udpPorts.Count > 0)
                        {
                            TestUdpPorts(_udpPorts);
                        }
                    }
                }
                catch (AuthenticationException ex)
                {
```

```
                Console.WriteLine(ex.Message);
            }
        }
        else
        {
            PrintUsage();
        }

        Console.Write("Press <enter> to continue.");
        Console.ReadLine();
    }

    static void PrintUsage()
    {
        string currentApp =
Path.GetFileName(System.Reflection.Assembly.GetExecutingAssembly().Location);
        Console.WriteLine("Usage: {0} \n-d <domain> \n-ip \"<server IP address>\"
\n[-tcp \"<tcp_port1>,<tcp_port2>,etc\"] \n[-udp \"<udp_port1>,<udp_port2>,etc\"]",
currentApp);
    }

    static bool ParseArgs(string[] args)
    {
        bool fReturn = false;
        string ipAddress = "";

        try
        {
            _tcpPorts = new List<int>();
            _udpPorts = new List<int>();

            for (int i = 0; i < args.Length; i++)
            {
                string arg = args[i];

                if ("-tcp" == arg | "/tcp" == arg)
                {
                    i++;
                    string portList = args[i];
                    _tcpPorts = ParsePortList(portList);
                }

                if ("-udp" == arg | "/udp" == arg)
                {
                    i++;
                    string portList = args[i];
                    _udpPorts = ParsePortList(portList);
                }

                if ("-d" == arg | "/d" == arg)
                {
                    i++;
                    _domain = args[i];
                }

                if ("-ip" == arg | "/ip" == arg)
                {
                    i++;
                    ipAddress = args[i];
                }
            }
        }
        catch (ArgumentOutOfRangeException)
        {
            return false;
        }
```

```
            if (_domain.Length > 0 || ipAddress.Length > 0)
            {
                fReturn = true;
            }

            if (ipAddress.Length > 0)
            {
                _ipAddr = IPAddress.Parse(ipAddress);
            }

            return fReturn;
        }

        static List<int> ParsePortList(string portList)
        {
            List<int> ports = new List<int>();

            char[] separators = {',', ';', ':'};

            string[] portStrings = portList.Split(separators);
            foreach (string portString in portStrings)
            {
                try
                {
                    ports.Add(Convert.ToInt32(portString));
                }
                catch (FormatException)
                {
                }
            }

            return ports;
        }

        static void TestForestFunctionalLevel()
        {
            Console.WriteLine("Testing forest functional level.");

            DirectoryContext dirContext = new DirectoryContext(DirectoryContextType.Forest,
_domain, null, null);
            Forest forestContext = Forest.GetForest(dirContext);

            Console.Write("Forest Functional Level = {0} : ", forestContext.ForestMode);

            if (forestContext.ForestMode >= ForestMode.Windows2003Forest)
            {
                Console.WriteLine("PASSED");
            }
            else
            {
                Console.WriteLine("FAILED");
            }

            Console.WriteLine();
        }

        static void TestDomainFunctionalLevel()
        {
            Console.WriteLine("Testing domain functional level.");

            DirectoryContext dirContext = new DirectoryContext(DirectoryContextType.Domain,
_domain, null, null);
            Domain domainObject = Domain.GetDomain(dirContext);

            Console.Write("Domain Functional Level = {0} : ", domainObject.DomainMode);
```

```
            if (domainObject.DomainMode >= DomainMode.Windows2003Domain)
            {
                Console.WriteLine("PASSED");
            }
            else
            {
                Console.WriteLine("FAILED");
            }

            Console.WriteLine();
        }

        static List<int> TestTcpPorts(List<int> portList)
        {
            Console.WriteLine("Testing TCP ports to {0}:", _ipAddr.ToString());

            List<int> failedPorts = new List<int>();

            foreach (int port in portList)
            {
                Console.Write("Checking TCP port {0}: ", port);

                TcpClient tcpClient = new TcpClient();

                try
                {
                    tcpClient.Connect(_ipAddr, port);

                    tcpClient.Close();
                    Console.WriteLine("PASSED");
                }
                catch (SocketException)
                {
                    failedPorts.Add(port);
                    Console.WriteLine("FAILED");
                }
            }

            Console.WriteLine();

            return failedPorts;
        }

        static List<int> TestUdpPorts(List<int> portList)
        {
            Console.WriteLine("Testing UDP ports to {0}:", _ipAddr.ToString());

            List<int> failedPorts = new List<int>();

            foreach (int port in portList)
            {
                Console.Write("Checking UDP port {0}: ", port);

                UdpClient udpClient = new UdpClient();

                try
                {
                    udpClient.Connect(_ipAddr, port);
                    udpClient.Close();
                    Console.WriteLine("PASSED");
                }
                catch (SocketException)
                {
                    failedPorts.Add(port);
                    Console.WriteLine("FAILED");
```

```
                }
            }

            Console.WriteLine();

            return failedPorts;
        }
    }
}
```

创建AD Connector

要使用AD Connector，请执行以下步骤。在开始此过程之前，请确保您已满足了AD Connetor (p. 171)中确定的先决条件。

> **Note**
>
> 您无法使用 Cloud Formation 模板创建 AD 连接器。

使用 AD Connector

1. 在Amazon Directory Service控制台导航窗格中，选择目录然后选择设置目录.
2. 在存储库的选择目录类型页面上，选择AD Connector，然后选择下一步.
3. 在 Enter AD Connector information (输入 AD Connector 信息) 页面上，提供以下信息：

   目录大小

   从小型或大型大小选项中进行选择。有关大小的更多信息，请参阅Active Directory Connector (p. 171)。

   目录描述

   目录的可选描述。
4. 在 Choose VPC and subnets (选择 VPC 和子网) 页面上，提供以下信息，然后选择 Next (下一步)。

   VPC

   目录的 VPC。

   Subnets (子网)

   为域控制器选择子网。两个子网必须位于不同的可用区。
5. 在 Connect to AD (连接到 AD) 页面上，提供以下信息：

   目录 DNS 名称

   现有目录的完全限定名称，例如 `corp.example.com`。

   目录 NetBIOS 名称

   现有目录的短名称，例如 `CORP`。

   DNS IP 地址

   现有目录中至少一个 DNS 服务器的 IP 地址。这些服务器必须可从以下部分中指定的每个子网访问。

   服务账户用户名

   现有目录中用户的用户名称。有关该账户的更多信息，请参阅AD Connetor (p. 171)。

服务账户密码

现有用户账户的密码。此密码区分大大小大小写，且长度必须介于 8 到 128 个字符之间。至少，它还必须包含下列四种类别中三种类别的一个字符：

- 小写字母 (a-z)
- 大写字母 (A-Z)
- 数字 (0-9)
- 非字母数字字符 (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)

确认密码

重新键入现有用户账户的密码。

6. 在 Review & create (检查并创建) 页面上，检查目录信息并进行任何必要的更改。如果信息正确，请选择 Create directory (创建目录)。目录创建需要几分钟时间。创建后，Status 值将更改为 Active。

创建的内容

创建 AD ConnectorAmazon Directory Service自动创建elastic network interface (ENI) 并将其与每个 AD Connector 实例相关联。其中每个 ENI 对于您的 VPC 与 VPC 之间的连接都至关重要Amazon Directory ServiceAD Connector，永远不应删除。您可以识别保留用于的所有网络接口Amazon Directory Service通过描述："Amazon 为目录创建了网络接口目录 ID"。有关更多信息，请参阅 。弹性网络接口在适用于 Windows 实例的 Amazon EC2 用户指南中。

Note

默认情况下，AD Connector 实例部署在一个地区的两个可用区中，并连接到您的 Amazon Virtual Private Cloud (VPC)。失败的 AD Connector 实例将在同一可用区中使用相同的 IP 地址自动替换。

当你登录任何Amazon与 AD Connector 集成的应用程序或服务 (Amazon IAM Identity Center (successor to Amazon Single Sign-On)包括），应用程序或服务会将您的身份验证请求转发给 AD Connector，AD Connector 然后将该请求转发到自我管理 AD 中的域控制器进行身份验证。如果您成功通过了自我管理 AD 的身份验证，则 AD Connector 会将身份验证令牌返回到应用程序或服务（类似于 Kerberos 令牌）。此时，您现在可以访问Amazon应用程序或服务。

如何管理 AD Connector

此节列出了运行和维护 AD Connector 环境的所有过程。

主题

- 保护 AD Connector (p. 182)
- 监控 AD Connector 目录 (p. 193)
- 将 EC2 实例加入 AD Connector 目录 (p. 195)
- 维护 AD Connector 目录 (p. 201)
- 更新 AD Connector 的 DNS 地址 (p. 202)

保护 AD Connector

此节介绍了保护 AD Connector 环境的注意事项。

主题

- 在中更新AD Connector 账户凭证Amazon Directory Service (p. 183)
- 为 AD Connector 启用多重验证 (p. 183)
- 使用 AAD Connector 启用客户端 LDAPS (p. 184)
- 在 AD Connector 中启用 MTL 身份验证以便与智能卡一起使用 (p. 188)

在中更新AD Connector 账户凭证Amazon Directory Service

您在中提供的 AD Connector 凭据Amazon Directory Service表示用于访问现有本地目录的服务账户。您可以通过执行以下步骤在 Amazon Directory Service 中修改这些服务账户凭证。

> **Note**
>
> 如果Amazon IAM Identity Center (successor to Amazon Single Sign-On)为目录启用，Amazon Directory Service必须将服务委托人名称 (SPN) 从当前服务账户传输到新的服务账户。如果当前服务账户无权删除 SPN 或新服务账户无权添加 SPN，则系统会提示输入有权执行这两个操作的目录账户的凭证。这些凭证仅用于传输 SPN，不会由服务进行存储。

在中更新服务AD Connector 凭证凭证Amazon Directory Service

1. 在Amazon Directory Service控制台导航窗格中，选择目录.
2. 选择目录的目录 ID 链接。
3. 在 Directory details (目录详细信息) 页面上，选择 Networking & security (网络和安全性) 选项卡。
4. 在 Service account credentials (服务账户凭据) 部分中，选择 Update (更新)。
5. 在 Update service account credentials (更新服务账户凭证) 对话框中，键入新用户名称和密码，然后选择 Update Directory (更新目录)。

为 AD Connector 启用多重验证

当您在本地或 EC2 实例中运行 Active Directory 时，可以为 AD Connector 启用多重身份验证。有关多重验证与 Amazon Directory Service 结合使用的更多信息，请参阅 AD Connetor (p. 171)。

> **Note**
>
> 多重验证对 Simple AD 不可用。但是，可为您启用 MFAAmazon托管 Microsoft AD 目录。有关更多信息，请参阅 为启用多重验证Amazon托管的 Managed (p. 28)。

为 AD Connector 启用多重验证

1. 在Amazon Directory Service控制台选择导航窗格。目录.
2. 选择 AD Connector 目录的目录 ID 链接。
3. 在目录详细信息页面上，选择 Networking & security (联网和安全性) 选项卡。
4. 在多重验证部分中，选择操作，然后选择启用。
5. 在存储库的启用多重验证 (MFA)页面上，提供以下值：

   显示标签

   提供标签名称。

   RADIUS 服务器 DNS 名称或 IP 地址

   您的 RADIUS 服务器终端节点的 IP 地址或者您的 RADIUS 服务器负载均衡器的 IP 地址。可以输入多个 IP 地址 (用逗号分隔开)，例如`192.0.0.0,192.0.0.12`)。

Note

RADIUS MFA 仅适用于验证对Amazon Web Services Management Console，或者适用于 WorkSpaces、Amazon QuickSight 或 Amazon Chime 等亚马逊企业应用程序和服务。它不向 EC2 实例上运行的 Windows 工作负载提供 MFA，也不会为登录 EC2 实例提供 MFA。Amazon Directory Service不支持 RADIUS 质询/响应身份验证。
用户输入其用户名和密码时必须拥有 MFA 代码。或者，您必须使用执行带外 MFA 的解决方案，例如为用户进行短信文本验证。在带外 MFA 解决方案中，您必须确保为解决方案适当地设置了 RADIUS 超时值。使用带外 MFA 解决方案时，登录页面将提示用户输入 MFA 代码。在这种情况下，最佳做法是用户在密码字段和 MFA 字段中输入密码。

端口

RADIUS 服务器用来通信的端口。您的本地网络必须允许通过默认 RADIUS 服务器端口 (UDP: 1812) 从Amazon Directory Service服务器。

Shared secret code

在创建 RADIUS 终端节点时指定的共享密码。

Confirm shared secret code (确认共享密码)

确认您的 RADIUS 终端节点的共享密码。

协议

选择在创建 RADIUS 终端节点时指定的协议。

服务器超时（以秒为单位）

等待 RADIUS 服务器响应的时间长度 (以秒为单位)。此值必须介于 1 和 50 之间。

最大 RADIUS 请求重试次

将尝试与 RADIUS 服务器通信的次数。此值必须介于 0 和 10 之间。

当 RADIUS Status 更改为 Enabled 时，多重验证将可用。

6. 选择 Enable。

使用 AAD Connector 启用客户端 LDAPS

中的客户端 LDAPS 支持对 Microsoft AD Connector ctive Directory (AD) 和Amazon应用程序。此类应用程序的示例包括 WorkSpaces、Amazon IAM Identity Center (successor to Amazon Single Sign-On)，Amazon QuickSight，和Amazon Chime。此加密可帮助您更好地保护您组织的身份数据并满足您的安全要求。

主题

- 先决条件 (p. 184)
- 启用客户端 LDAPS (p. 185)
- 管理客户端 LDAPS (p. 187)

先决条件

启用客户端 LDAPS 之前，您需要满足以下要求。

主题

- 在活动目录中部署服务器证书 (p. 185)
- CA 证书要求 (p. 185)
- 联网要求 (p. 185)

在活动目录中部署服务器证书

要启用客户端 LDAPS，您需要为 Active Directory 中的每个域控制器获取并安装服务器证书。LDAP 服务将使用这些证书来侦听并自动接受来自 LDAP 客户端的 SSL 连接。您可以使用由内部 Active Directory Certificate Services (ADCS) 部署颁发的或从商业颁发机构处购买的 SSL 证书。有关 Active Directory 服务器证书要求的更多信息，请参阅 Microsoft 网站上的 LDAP over SSL (LDAPS) 证书。

CA 证书要求

客户端 LDAPS 操作需要证书颁发机构 (CA) 证书，它表示服务器证书的颁发者。CA 证书将与由 Active Directory 域控制器提供的服务器证书匹配来加密 LDAP 通信。请注意以下 CA 证书要求：

- 要注册一个证书，该证书必须在 90 天以后才到期。
- 证书必须采用隐私增强邮件 (PEM) 格式。如果要从 Active Directory 内部导出 CA 证书，请选择 base64 编码的 X.509 (.CER) 作为导出文件格式。
- 每个 AAD Connector Conctory（5）个 CA 证书。
- 使用 RSSAS-PSS 签名算法的证书不受支持。

联网要求

Amazon 应用程序 LDAP 流量将仅在 TCP 端口 636 上运行，而不会回退到 LDAP 端口 389。但是，支持复制、信任等的 Windows LDAP 通信将继续使用带有 Windows 本机安全性的 LDAP 端口 389。配置Amazon 安全组和网络防火墙，以允许（出站）和自行管理的 AD Connector ctive Directory（出站）中的端口 636 上的 TCP 通信。

启用客户端 LDAPS

要启用客户端 LDAPS，您需要将证书颁发机构 (CA) 证书颁发机构 (CA) 证书颁发机构 (CA) 证书颁发机构 (CA) 证书颁发机构 (CA) 证书颁发机构 (CA) 启用后，Amazon 应用程序与您自行管理的 Active Directory 之间的所有 LDAP 通信将通过安全套接字层 (SSL) 通道加密进行传输。

您可以使用两种不同的方法为您的目录启用客户端 LDAPS。您可以使用Amazon Web Services Management Console方法或Amazon CLI方法。

主题

- 第 1 步：在中注册证书Amazon Directory Service (p. 185)
- 第 2 步：检查注册状态 (p. 186)
- 第 3 步：启用客户端 LDAPS (p. 186)
- 第 4 步：检查 LDAPS 状态 (p. 186)

第 1 步：在中注册证书Amazon Directory Service

使用下列方法之一在 Amazon Directory Service 中注册证书。

方法 1：在中注册您的证书Amazon Directory Service(Amazon Web Services Management Console）

1. 在Amazon Directory Service控制台导航窗格中，选择目录.
2. 选择目录的目录 ID 链接。
3. 在 Directory details (目录详细信息) 页面上，选择 Networking & security (网络和安全性) 选项卡。
4. 在 Client-side LDAPS (客户端 LDAPS) 部分中，选择 Actions (操作) 菜单，然后选择 Register certificate (注册证书)。
5. 在 Register a CA certificate (注册 CA 证书) 对话框中，选择 Browse (浏览)，然后选择证书并选择 Open (打开)。
6. 选择 Register certificate (注册证书)。

方法 2：在中注册您的证书Amazon Directory Service(Amazon CLI)

- 运行以下命令。对于证书数据，请指向 CA 证书文件的位置。响应中将会提供证书 ID。

```
aws ds register-certificate --directory-id your_directory_id --certificate-data
 file://your_file_path
```

第 2 步：检查注册状态

要查看证书注册的状态或已注册证书的列表，请使用以下任一方法。

方法 1：在中检查证书注册状态Amazon Directory Service(Amazon Web Services Management Console)

1. Go to the 客户端 LDAPS的部分目录详细信息页.
2. 查看 Registration status (注册状态) 列下显示的当前证书注册状态。当注册状态值更改为 Registered (已注册) 时，您的证书已成功注册。

方法 2：在中检查证书注册状态Amazon Directory Service(Amazon CLI)

- 运行以下命令。如果状态值返回 `Registered`，则表示您的证书已成功注册。

```
aws ds list-certificates --directory-id your_directory_id
```

第 3 步：启用客户端 LDAPS

使用下列方法之一在中启用客户端 LDAPSAmazon Directory Service.

> **Note**
>
> 您必须已成功注册至少一个证书，然后才能启用客户端 LDAPS。

方法 1：在中启用客户端 LDAPSAmazon Directory Service(Amazon Web Services Management Console)

1. Go to the 客户端 LDAPS的部分目录详细信息页.
2. 请选择 Enable。如果此选项不可用，请验证有效证书是否已成功注册，然后重试。
3. 在 Enable client-side LDAPS (启用客户端 LDAPS) 对话框中，选择 Enable (启用)。

方法 2：在中启用客户端 LDAPSAmazon Directory Service(Amazon CLI)

- 运行以下命令。

```
aws ds enable-ldaps --directory-id your_directory_id --type Client
```

第 4 步：检查 LDAPS 状态

使用下列方法之一检查 LDAPS 状态Amazon Directory Service.

方法 1：在中检查 LDAPS 状态Amazon Directory Service(Amazon Web Services Management Console)

1. Go to the 客户端 LDAPS的部分目录详细信息页.

2. 如果状态值显示为 Enabled (启用)，则 LDAPS 已成功配置。

方法 2：在中检查 LDAPS 状态Amazon Directory Service(Amazon CLI)

- 运行以下命令。如果状态值返回 `Enabled`，则 LDAPS 已成功配置。

```
aws ds describe-ldaps-settings -directory-id your_directory_id
```

管理客户端 LDAPS

使用这些命令可管理 LDAPS 配置。

您可以使用两种不同的方法来管理客户端 LDAPS 设置。您可以使用Amazon Web Services Management Console方法或Amazon CLI方法。

查看证书详细信息

使用下列方法之一查看证书设置为何时过期。

方法 1：在中查看证书详细信息Amazon Directory Service(Amazon Web Services Management Console)

1. 在Amazon Directory Service控制台导航窗格中，选择目录.
2. 选择目录的目录 ID 链接。
3. 在 Directory details (目录详细信息) 页面上，选择 Networking & security (网络和安全性) 选项卡。
4. 在 Client-side LDAPS (客户端 LDAPS) 部分的 CA certificates (CA 证书) 下，将显示有关证书的信息。

方法 2：在中查看证书详细信息Amazon Directory Service(Amazon CLI)

- 运行以下命令。对于证书 ID，请使用由 `register-certificate` 或 `list-certificates` 返回的标识符。

```
aws ds describe-certificate --directory-id your_directory_id --certificate-
id your_cert_id
```

取消注册证书

使用下列方法之一取消注册证书。

> **Note**
>
> 如果只注册了一个证书，则必须先禁用 LDAPS，然后才能取消注册证书。

方法 1：在中取消注册证书Amazon Directory Service(Amazon Web Services Management Console)

1. 在Amazon Directory Service控制台导航窗格中，选择目录.
2. 选择目录的目录 ID 链接。
3. 在 Directory details (目录详细信息) 页面上，选择 Networking & security (网络和安全性) 选项卡。
4. 在 Client-side LDAPS (客户端 LDAPS) 部分中，选择 Actions (操作)，然后选择 Deregister certificate (取消注册证书)。

5. 在 Deregister a CA certificate (取消注册 CA 证书) 对话框中，选择 Deregister (取消注册)。

方法 2：在中取消注册证书Amazon Directory Service(Amazon CLI)

- 运行以下命令。对于证书 ID，请使用由 `register-certificate` 或 `list-certificates` 返回的标识符。

```
aws ds deregister-certificate --directory-id your_directory_id --certificate-
id your_cert_id
```

禁用客户端 LDAPS

使用下列方法之一禁用客户端 LDAPS。

方法 1：在中禁用客户端 LDAPSAmazon Directory Service(Amazon Web Services Management Console)

1. 在Amazon Directory Service控制台导航窗格中，选择目录.
2. 选择目录的目录 ID 链接。
3. 在 Directory details (目录详细信息) 页面上，选择 Networking & security (网络和安全性) 选项卡。
4. 在 Client-side LDAPS (客户端 LDAPS) 部分中，选择 Disable (禁用)。
5. 在 Disable client-side LDAPS (禁用客户端 LDAPS) 对话框中，选择 Disable (禁用)。

方法 2：在中禁用客户端 LDAPSAmazon Directory Service(Amazon CLI)

- 运行以下命令。

```
aws ds disable-ldaps --directory-id your_directory_id --type Client
```

在 AD Connector 中启用 MTL 身份验证以便与智能卡一起使用

您可以对智能卡使用基于证书的相互传输层安全 (MTL) 身份验证，通过自我管理的 Active Directory (AD) 和 AD Connector 对用户进入 Amazon WorkSpaces 进行身份验证。启用后，用户可以在 WorkSpaces 登录屏幕上选择自己的智能卡，然后输入 PIN 进行身份验证，而不是使用用户名和密码。从那里，Windows 或 Linux 虚拟桌面使用智能卡从本机桌面操作系统对 AD 进行身份验证。

> **Note**
>
> AD Connector 中的智能卡身份验证仅在以下区域可用，并且仅适用于 WorkSpaces。其他Amazon 目前不支持应用程序。
>
> - 美国东部（弗吉尼亚北部）
> - 美国西部（俄勒冈）
> - 亚太地区（悉尼）
> - 亚太区域（东京）
> - 欧洲（爱尔兰）
> - Amazon GovCloud（美国西部）

主题

- 先决条件 (p. 189)

- 启用智能卡身份验证 (p. 190)
- 管理智能卡身份验证设置 (p. 191)

先决条件

要为 Amazon WorkSpaces 客户端启用使用智能卡的 MTL 身份验证，您需要一个与自我管理的 AD 集成的运营智能卡基础设施。有关如何使用 Amazon WorkSpaces 和 AD 设置智能卡身份验证的更多信息，请参阅Amazon WorkSpaces 管理指南.

在为 WorkSpaces 启用智能卡身份验证之前，请查看以下注意事项：

- CA 证书要求 (p. 189)
- 用户证书要求 (p. 189)
- 证书吊销检查过程 (p. 189)
- 其它考虑因素 (p. 190)

CA 证书要求

AD Connector 需要证书颁发机构 (CA) 证书，该证书表示用户证书的颁发者，以实现智能卡身份验证。AD Connector 将 CA 证书与用户提供的证书与智能卡相匹配。请注意以下 CA 证书要求：

- 要注册 CA 证书，该证书必须在 90 天以后才到期。
- CA 证书必须采用隐私增强邮件 (PEM) 格式。如果要从 Active Directory 内部导出 CA 证书，请选择 base64 编码的 X.509 (.CER) 作为导出文件格式。
- 必须上传从颁发 CA 到用户证书链接的所有根证书和中间 CA 证书，才能成功进行智能卡身份验证。
- 每个 AD Connector 目录最多可存储 100 个 CA 证书。
- AD Connector 不支持 CA 证书的 RSSAS-PSS 签名算法。

用户证书要求

向 AD Connector 提供的用户证书必须包含`userPrincipalName (UPN)`中的 AD 用户`subjectAltName (SAN)`证书的字段。

证书吊销检查过程

为了执行智能卡身份验证，AD Connector 必须使用在线证书状态协议 (OCSP) 检查用户证书的吊销状态。要执行证书吊销检查，OCSP 响应程序 URL 必须可以互联网访问。如果使用 DNS 名称，OCSP 响应程序 URL 必须使用互联网编号分配机构 (IANA) 根区域数据库.

AD Connector 证书吊销检查使用以下过程：

- AD Connector 必须检查用户证书中的授权信息访问 (AIA) 扩展名以获取 OCSP 响应程序 URL，然后 AD Connector 使用该 URL 检查是否撤销。
- 如果 AD Connector 无法解析在用户证书 AIA 扩展中找到的 URL，或者在用户证书中找到 OCSP 响应程序 URL，则 AD Connector 将使用在根 CA 证书注册过程中提供的可选 OCSP URL。

  如果用户证书 AIA 扩展中的 URL 解析但没有响应，则用户身份验证将失败。
- 如果在根 CA 证书注册期间提供的 OCSP 响应程序 URL 无法解析、无响应或未提供 OCSP 响应程序 URL，则用户身份验证将失败。

  Note

  AD Connector 需要HTTPOCSP 响应程序 URL 的 URL。

其它考虑因素

在 AD Connector 中启用智能卡身份验证之前，请考虑以下事项：

- AD Connector 使用基于证书的相互传输层安全身份验证 (双向 TLS) 使用基于硬件或软件的智能卡证书向 Active Directory 验证用户身份。目前只支持普通访问卡 (CAC) 和个人身份验证 (PIV) 卡。其他类型的硬件或基于软件的智能卡可能有效，但尚未经过与 WorkSpaces 流协议一起使用的测试。
- 智能卡身份验证将替换 WorkSpaces 的用户名和密码身份

  如果有其他Amazon在 AD Connector 目录上配置的应用程序启用了智能卡身份验证，这些应用程序仍然显示用户名和密码输入屏幕
- 启用智能卡身份验证可将 Kerberos 服务票证的用户会话长度限制为最长生命周期。您可以使用组策略配置此设置，默认情况下设置为 10 小时。有关此设置的更多信息，请参阅Microsoft 文档.

启用智能卡身份验证

要启用智能卡身份验证，请使用以下步骤将证书颁发机构 (CA) 证书导入 AD Connector 中，使用Amazon Directory Service控制台，API要么CLI. 然后在 AD Connector 上为 WorkSpaces 启用智能卡身份验证。

主题

- 第 1 步：为 AD Connector 服务帐户启用 Kerberos 受限委派 (p. 190)
- 第 2 步：在 AD Connector 中注册 CA 证书 (p. 190)
- 第 3 步：为支持启用智能卡身份验证Amazon应用程序和服务 (p. 191)

第 1 步：为 AD Connector 服务帐户启用 Kerberos 受限委派

要将智能卡身份验证与 AD Connector 一起使用，必须启用Kerberos 约束委托 (KCD)用于 AD Connector 服务帐户转移到自管 AD. 目录中的 LDAP 服务。

Kerberos 约束委托是 Windows Server 中的一项功能。此功能使得管理员可以限制应用程序能够代表用户执行操作的范围，从而指定和实施应用程序信任边界。有关更多信息，请参阅 。Kerberos 约束委托.

1. 使用`SetSpn`命令为自管 AD 中的 AD Connector 服务帐户设置服务主体名称 (SPN)。这将启用服务帐户进行委派配置。

   SPN 可以是任何服务或名称组合，但不能是现有 SPN 的副本。这些区域有：`-s`检查重复项。

   ```
   setspn -s my/spn service_account
   ```

2. InAD 用户和计算机，右键单击 AD Connector 服务帐户，然后选择属性。
3. 选择委托选项卡。
4. 选择信任此用户仅委派给指定的服务和使用任何验证协议单选按钮。
5. 选择Add然后用户或计算机找到域控制器。
6. 选择确定以显示用于委托的可用服务列表。
7. 选择LDAP服务类型，然后单击确定.
8. 单击确定再次保存配置。
9. 对 AD 中的其他域控制器重复此过程。或者，您可以使用 PowerShell 自动化该过程。

第 2 步：在 AD Connector 中注册 CA 证书

使用下列方法之一为 AD Connector 目录注册 CA 证书。

方法 1：要在 AD Connector 中注册您的 CA 证书 (Amazon Web Services Management Console)

1. 在Amazon Directory Service控制台选择导航窗格，选择目录.
2. 选择目录的目录 ID 链接。
3. 在 Directory details (目录详细信息) 页面上，选择 Networking & security (网络和安全性) 选项卡。
4. 在智能卡身份验证部分中，选择操作菜单，然后选择注册证书.
5. 在注册证书对话框中，选择选择文件，然后选择一个证书然后选择打开. 您可以选择提供联机证书状态协议 (OCSP) 响应程序 URL，从而对此证书执行吊销检查。有关 OCSP 的更多信息，请参阅证书吊销检查过程 (p. 189).
6. 选择 Register certificate (注册证书)。当你看到证书状态更改为已注册，注册过程已成功完成。

方法 2：要在 AD Connector 中注册您的 CA 证书 (Amazon CLI)

- 运行以下 命令。对于证书数据，请指向 CA 证书文件的位置。要提供辅助 OCSP 响应方地址，请使用可选`ClientCertAuthSettings`对象。

```
aws ds register-certificate --directory-id your_directory_id --certificate-
data file://your_file_path --type ClientCertAuth --client-cert-auth-settings
 OCSPUrl=http://your_OCSP_address
```

  如果成功，响应将提供证书 ID。您还可以运行以下 CLI 命令，验证 CA 证书是否成功注册：

```
aws ds list-certificates --directory-id your_directory_id
```

  如果状态值返回`Registered`，您已成功注册证书。

第 3 步：为支持启用智能卡身份验证Amazon应用程序和服务

使用下列方法之一为 AD Connector 目录注册 CA 证书。

方法 1：在 AD Connector 中启用智能卡身份验证 (Amazon Web Services Management Console)

1. 转至智能卡身份验证在部分中目录详细信息页面，然后选择启用. 如果此选项不可用，请验证有效证书是否已成功注册，然后重试。
2. 在启用智能卡身份验证对话框中，选择启用.

方法 2：在 AD Connector 中启用智能卡身份验证 (Amazon CLI)

- 运行以下 命令。

```
aws ds enable-client-authentication --directory-id your_directory_id --type SmartCard
```

  如果成功，AD Connector 将返回`HTTP 200`用空的 HTTP 正文进行响应。

管理智能卡身份验证设置

您可以使用两种不同的方法来管理智能卡设置。您可以使用Amazon Web Services Management Console或Amazon CLI方法。

主题

- 查看证书信息 (p. 192)

- 取消注册证书 (p. 192)
- 禁用智能卡身份验证 (p. 193)

查看证书信息

使用下列方法之一查看证书设置为何时过期。

方法 1：要在中查看证书详细信息Amazon Directory Service(Amazon Web Services Management Console)

1. 在Amazon Directory Service控制台选择导航窗格，选择目录.
2. 选择 AD Connector 目录的目录 ID 链接。
3. 在 Directory details (目录详细信息) 页面上，选择 Networking & security (网络和安全性) 选项卡。
4. 在智能卡身份验证位置在部分下CA 证书中，选择证书 ID 以显示有关该证书的详细信息。

方法 2：要在中查看证书详细信息Amazon Directory Service(Amazon CLI)

- 运行以下 命令。对于证书 ID，请使用由 `register-certificate` 或 `list-certificates` 返回的标识符。

```
aws ds describe-certificate --directory-id your_directory_id --certificate-
id your_cert_id
```

取消注册证书

使用下列方法之一取消注册证书。

> **Note**
>
> 如果只注册了一个证书，则必须先禁用智能卡身份验证，然后才能取消注册证书。

方法 1：在中取消注册证书Amazon Directory Service(Amazon Web Services Management Console)

1. 在Amazon Directory Service控制台选择导航窗格，选择目录.
2. 选择 AD Connector 目录的目录 ID 链接。
3. 在 Directory details (目录详细信息) 页面上，选择 Networking & security (网络和安全性) 选项卡。
4. 在智能卡身份验证位置在部分下CA 证书中，选择要取消注册的证书，然后选择操作，然后选择取消注册证书.

   > **Important**
   >
   > 确保您即将取消注册的证书处于活动状态，或者当前正在用作 CA 证书链的一部分进行智能卡身份验证。

5. 在 Deregister a CA certificate (取消注册 CA 证书) 对话框中，选择 Deregister (取消注册)。

方法 2：在中取消注册证书Amazon Directory Service(Amazon CLI)

- 运行以下 命令。对于证书 ID，请使用由 `register-certificate` 或 `list-certificates` 返回的标识符。

```
aws ds deregister-certificate --directory-id your_directory_id --certificate-
id your_cert_id
```

禁用智能卡身份验证

使用下列方法之一禁用智能卡身份验证。

方法 1：要在中禁用智能卡身份验证Amazon Directory Service(Amazon Web Services Management Console)

1. 在Amazon Directory Service控制台选择导航窗格，选择目录.
2. 选择 AD Connector 目录的目录 ID 链接。
3. 在 Directory details (目录详细信息) 页面上，选择 Networking & security (网络和安全性) 选项卡。
4. 在智能卡身份验证选择部分，选择禁用.
5. 在禁用智能卡身份验证选择对话框中，选择禁用.

方法 2：要在中禁用智能卡身份验证Amazon Directory Service(Amazon CLI)

- 运行以下 命令。

```
aws ds disable-client-authentication --directory-id your_directory_id --type SmartCard
```

监控 AD Connector 目录

您可以通过以下方法监控 AD Connector 目录：

主题

- 了解您的目录状态 (p. 193)
- 配置目录状态通知 (p. 194)

了解您的目录状态

以下是目录的各种状态。

Active (处于活动状态)

该目录运行正常。Amazon Directory Service 未检测到您的目录存在任何问题。

创建

当前正在创建该目录。目录创建过程通常需要 20 到 45 分钟，但可能因系统负载而异。

Deleted (已删除)

已删除该目录。已释放该目录的所有资源。一旦目录进入此状态，便无法恢复。

Deleting (正在删除)

当前正在删除该目录。目录将保持此状态，直到被完全删除。一旦目录进入此状态，将无法取消删除操作，目录也无法恢复。

已失败

无法创建该目录。请删除此目录。如果此问题仍存在，请联系。Amazon Web Services SupportCenter.

Impaired (受损)

目录正在降级状态下运行。检测到一个或多个问题，可能有的目录操作未在完全有效地工作。目录处于此状态有多个可能的原因。这些原因包括正常的操作维护活动（如打补丁或 EC2 实例轮换）、其中一台域控制器上的某个应用程序临时成为热点，或者您对网络进行了更改（可能无意中破坏目录通

信）。有关更多信息，请参阅故障排除AmazonMicrosoft Managed Managed Microsoft AD (p. 161)、排查 AD Connector (p. 205)、排查 Simple AD (p. 251)。对于与正常维护相关的问题，Amazon在 40 分钟内解决。如果在查看故障排除主题后，您的目录处于受损状态的时间超过 40 分钟，我们建议您联系。Amazon Web Services SupportCenter.

Important

当目录处于受损状态时，请不要还原快照。解决受损问题极少需要快照还原。有关更多信息，请参阅 快照或恢复你的目录 (p. 118)。

Inoperable (不可操作)

该目录无法正常工作。所有目录终端节点都报告有问题。

Requested (已请求)

创建目录的请求当前正在等待处理。

RestoreFailed (还原失败)

从快照还原目录失败。请重试还原操作。如果这种情况继续存在，请尝试其他快照或联系。Amazon Web Services SupportCenter.

Restoring (还原)

当前正从自动或手动快照中还原目录。从快照还原通常需要几分钟时间，具体取决于快照中的目录数据大小。

有关更多信息，请参阅Simple AD 目录状态原因 (p. 252)。

配置目录状态通知

通过使用 Amazon Simple Notification Service (Amazon SNS)，您可以在目录状态发生变化时接收电子邮件或文本 (SMS) 消息。如果目录从 Active 状态变为受损或无法操作状态. 当目录恢复为“Active”状态时，您也会收到通知。

工作方式

Amazon SNS 使用 “主题” 来收集和分发消息。每个主题都有一个或多个订阅者，他们接收发布至该主题的消息。使用以下步骤你可以添加Amazon Directory Service作为 Amazon SNS 主题的发布者。Amazon Directory Service 在检测到您的目录状态发生变化时，会向该主题发布一条消息，该消息随后发送给该主题的订阅者。

您可以关联多个目录作为单个主题的发布者。您还可以将目录状态消息添加到您之前在 Amazon SNS 中创建的主题。您可以对谁能够向主题发布内容和订阅主题进行详细的控制。有关 Amazon SNS 的完整信息，请参阅什么是 Amazon SNS？.

为您的目录启用 SNS 消息发送

1. 登录 Amazon Web Services Management Console，然后打开 Amazon Directory Service 控制台，网址为：https://console.aws.amazon.com/directoryservicev2/。
2. 在 Directories 页面上，选择您的目录 ID。
3. 选择维护“选项卡。
4. 在目录监控部分，选择操作选择，然后选择创建通知.
5. 在存储库的创建通知“页面”，选择选择通知类型选择，然后选择创建新通知. 或者，如果您已有一个 SNS 主题，您可以选择关联现有 SNS 主题以向该主题发送此目录的状态消息。

   Note

   如果选择创建新通知但之后使用与现有 SNS 主题相同的主题名称，Amazon SNS 不会创建新主题，只是向现有主题添加新的订阅信息。

如果选择关联现有 SNS 主题，您只能选择与该目录位于同一区域的 SNS 主题。

6. 选择收件人类型然后输入Recipient联系人信息。如果您为 SMS 输入电话号码，请只使用数字。不包括破折号、空格或圆括号。
7. (可选) 提供主题的名称和 SNS 显示名称。显示名称为最多 10 个字符的短名称，包含在来自该主题的所有 SMS 消息中。使用 SMS 选项时必需提供显示名称。

   Note

   如果您使用仅有DirectoryServiceFullAccess托管策略，主题名称必须以 “DirectoryMonitor” 开头。如果您想进一步自定义主题名称，您需要对 SNS 的额外权限。
8. 选择创建。

如果您要指定更多 SNS 订阅者，例如其他电子邮件地址、Amazon SQS 队列或Amazon Lambda您可通过 Amazon SNS 控制台完成这一操作：https://console.aws.amazon.com/sns/v3/home.

从主题移除目录状态消息

1. 登录 Amazon Web Services Management Console，然后打开 Amazon Directory Service 控制台，网址为：https://console.aws.amazon.com/directoryservicev2/。
2. 在 Directories 页面上，选择您的目录 ID。
3. 选择维护“选项卡。
4. 在目录监控部分中，在列表中选择 SNS 主题名称，然后选择操作选择，然后选择Remove.
5. 选择 Remove。

这会移除您的目录的选定 SNS 主题发布者身份。如果您要删除整个主题，可通过处的 Amazon SNS 控制台执行此操作：https://console.aws.amazon.com/sns/v3/home.

Note

在使用 SNS 控制台删除 Amazon SNS 主题之前，您应确保目录没有在向该主题发送状态消息。如果您使用 SNS 控制台删除 Amazon SNS 主题，则 Directory Services 控制台中不会立即反映出此更改。直到目录下次向已删除的主题发布通知时，您才会获得通知，那时，您将在该目录的 Monitoring 选项卡上看到一个更新状态，指示无法找到该主题。
因此，为避免错过重要的目录状态消息，请在删除从接收消息的任何主题之前，Amazon Directory Service将您的目录与其他 Amazon SNS 主题关联。

将 EC2 实例加入 AD Connector 目录

当 EC2 实例启动时，您可以使用以下方式无缝地将其加入到您的目录域中。Amazon Systems Manager. 有关更多信息，请参阅 。无缝地将 Windows 实例联接到Amazon Directory Service域中的Windows 实例 Amazon EC2 用户指南.

如果需要手动将 EC2 实例加入到您的域，则必须在正确的区域和安全组或子网中启动实例，然后将实例加入到该域。

要能够远程连接到这些实例，必须具有从所连接的网络到实例的 IP 连接。在大多数情况下，这要求 Internet 网关连接到 VPC，并且实例具有公有 IP 地址。

Note

将实例加入到自管理 Active Directory（本地）后，实例将直接与 Active Directory 通信并且绕过 AD Connector。

主题

- 无缝地联接 Windows EC2 实例 (p. 196)

- 将 Linux EC2 实例无缝地联接到 AD Connector 目录 (p. 197)

无缝地联接 Windows EC2 实例

此过程无缝地将 Windows EC2 实例联接到 AD Connector 目录。

无缝地联接 Windows EC2 实例

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 从导航栏的 Region (区域) 选择器中，选择与现有目录相同的 Region (区域)。
3. 选择 Launch Instance（启动实例）。
4. 在存储库的步骤 1页面上，选择Select获取适当的 AMI。
5. 在存储库的步骤 2页面上，选择合适的实例类型，然后选择后续：配置实例详细信息.
6. 在存储库的步骤 3页面上，执行以下操作，然后选择后续：Add Storage (下一步: 添加存储)：

   1. 对于 Network，选择在其中创建了您的目录的 VPC。
   2. 适用于子网在 VPC 中，选择一个公有子网。您选择的子网必须将所有外部流量都路由到 Internet 网关。否则将无法远程连接到实例。
   3. 对于 Auto-assign Public IP (自动分配公有 IP)，选择 Enable (启用)。

      有关公有 IP 地址和私有 IP 地址的更多信息，请参阅Amazon EC2 实例 IP 寻址中的Windows 实例 Amazon EC2 用户指南.
   4. 适用于域加入目录中，从列表中选择您的域。
   5. 对于 IAM role (IAM 角色)，执行以下操作之一：

      选择具有Amazon托管策略AmazonSSMManagedInstanceCore和AmazonSSMDirectoryServiceAccess挂载到它。

      -或者-

      如果您尚未创建具有AmazonSSMManagedInstanceCore和AmazonSSMDirectoryServiceAccess附加到它的托管策略，请选择创建新的 IAM 角色链接，然后执行以下操作：

      a. 选择 Create role（创建角色）。
      b. 在 Select type of trusted entity (选择受信任实体的类型）下，选择 Amazon service (Amazon 服务)。
      c. UNDER选择此角色将使用的服务在完整的服务列表中，选择EC2.
      d. UNDER选择您的使用案例，选择EC2，然后选择后续：Permissions (下一步：权限)。
      e. 在策略列表中，选择AmazonSSMManagedInstanceCore和AmazonSSMDirectoryServiceAccess政策。（要筛选列表，请键入**SSM**在搜索框中。）

         Note

         AmazonSSMDirectoryServiceAccess提供将实例加入由托管的 Active Directory 的权限。Amazon Directory Service. AmazonSSMManagedInstanceCore提供了使用 Systems Manager 服务所需的最低权限。有关使用这些权限创建角色的更多信息，以及有关可分配给 IAM 角色的其他权限和策略的信息，请参阅为 Systems Manager 创建 IAM 实例配置文件中的Amazon Systems Manager用户指南.
      f. 选择 Next:。标签。
      g. （可选）添加一个或多个标签键/值对以组织、跟踪或控制该角色的访问，然后选择后续：审核。
      h. 对于角色名称，请输入新角色的名称，如 **EC2DomainJoin** 或所需的其他名称。
      i. （可选）对于角色描述，请输入描述。

j. 选择 Create role（创建角色）。
k. 返回到步骤 3页. 适用于IAM 角色中，选择旁边的刷新图标IAM 角色. 您的新角色应显示在菜单中。选择它并将本页面上的其余设置保留默认值，然后选择后续：添加存储.

7. 在两者上步骤 4和步骤 5页面上，保留默认设置或根据需要进行更改，然后选择下一步按钮。
8. 在存储库的步骤 6页面上，为实例选择已配置为允许从您的网络远程访问实例的安全组，然后选择审核和启动.
9. 在存储库的步骤 7页面上，选择启动中，选择一个 key pair，然后选择实例启动.

将 Linux EC2 实例无缝地联接到 AD Connector 目录

此过程无缝地将 Linux EC2 实例联接到 AD Connector 目录。

支持以下 Linux 实例分发版和版本：

- Amazon Linux AMI 2018.03.0
- Amazon Linux 2（64 位 x86）
- Red Hat Enterprise Linux 8 (HVM)（64 位 x86）
- Ubuntu Server 18.04 LTS 和 Ubuntu Server 16.04 LTS
- CentOS 7 x86-64
- SUSE Linux Enterprise Server 15 SP1

> **Note**
>
> Ubuntu 14 和红帽企业 Linux 7 之前的发行版不支持无缝域加入功能。

先决条件

在设置无缝域加入到 Linux EC2 实例之前，您需要完成本节中的步骤。

选择您的无缝域加入服务帐户

您可以通过 AD Connector 将 Linux 计算机无缝加入到本地 Active Directory 域。为此，必须创建具有创建计算机帐户权限的用户帐户才能将计算机加入到该域。如果您愿意，您可以使用 AD Connector 服务帐户。或者，您可以使用具有足够权限的任何其他账户将计算机加入域。虽然成员Domain Admins或者其他组可能拥有足够权限将计算机加入到该域，我们不建议使用。作为最佳做法，我们建议您使用具有将计算机加入到该域所需的最低权限的服务帐户。

要使用将计算机加入域所需的最低权限委派帐户，可以运行以下 PowerShell 命令。你必须从加入域的 Windows 计算机上运行这些命令安装 Active Directory 管理工具 (p. 93)已安装。此外，您必须使用有权修改计算机 OU 或容器上的权限的帐户。PowerShell 命令设置允许服务帐户在域的默认计算机容器中创建计算机对象的权限。如果您更喜欢使用图形用户界面 (GUI)，则可使用中所述的手动过程。向您的服务账户委派权限 (p. 174).

```
$AccountName = 'awsSeamlessDomain'
# DO NOT modify anything below this comment.
# Getting Active Directory information.
Import-Module 'ActiveDirectory'
$Domain = Get-ADDomain -ErrorAction Stop
$BaseDn = $Domain.DistinguishedName
$ComputersContainer = $Domain.ComputersContainer
$SchemaNamingContext = Get-ADRootDSE | Select-Object -ExpandProperty 'schemaNamingContext'
[System.GUID]$ServicePrincipalNameGuid = (Get-ADObject -SearchBase $SchemaNamingContext -
Filter { lDAPDisplayName -eq 'Computer' } -Properties 'schemaIDGUID').schemaIDGUID
# Getting Service account Information.
$AccountProperties = Get-ADUser -Identity $AccountName
```

```
$AccountSid = New-Object -TypeName 'System.Security.Principal.SecurityIdentifier'
 $AccountProperties.SID.Value
# Getting ACL settings for the Computers container.
$ObjectAcl = Get-ACL -Path "AD:\$ComputersContainer"
# Setting ACL allowing the service account the ability to create child computer objects in
 the Computers container.
$AddAccessRule = New-Object -TypeName 'System.DirectoryServices.ActiveDirectoryAccessRule'
 $AccountSid, 'CreateChild', 'Allow', $ServicePrincipalNameGUID, 'All'
$ObjectAcl.AddAccessRule($AddAccessRule)
Set-ACL -AclObject $ObjectAcl -Path "AD:\$ComputersContainer"
```

如果您更喜欢使用图形用户界面 (GUI)，则可以使用手动流程来描述向您的服务账户委派权限 (p. 174).

创建密码以存储域服务帐户

您可以使用Amazon Secrets Manager以存储域服务帐户。

创建密码并存储域服务帐户信息

1. 登录到Amazon Web Services Management Console然后打开Amazon Secrets Manager控制台https://console.aws.amazon.com/secretsmanager/.
2. 选择 Store a new secret (存储新密钥)。
3. 在 Store a new secret（存储新密钥）页面上，执行以下操作：
   a. 在 Select secret type (选择密钥类型) 下，选择 Other type of secrets (其他密钥类型)。
   b. UNDER指定要存储在secret 中的键/值对。中，执行以下操作：
      i. 在第一个框中，输入**awsSeamlessDomainUsername**. 在同一行上，在下一个框中，输入服务帐户的用户名。例如，如果您之前使用 PowerShell 命令，则服务帐户名称将为`awsSeamlessDomain`.

         Note

         你必须输入**awsSeamlessDomainUsername**完全如此。确保没有任何前导或结束空格。否则，域名加入将失败。
      ii. 选择添加行.
      iii. 在新行上，在第一个框中，输入**awsSeamlessDomainPassword**. 在同一行的下一个框中，输入服务帐号的密码。

         Note

         你必须输入**awsSeamlessDomainPassword**完全如此。确保没有任何前导或结束空格。否则，域名加入将失败。
      iv. UNDER选择加密钥，选择DefaultenCryptionKey从菜单中选择。当您选择此选项时，Secret Secrets Manager 始终会对密码进行加密，并免费提供给您。你也可以选择自己创建的密钥。
      v. 选择 Next (下一步)。
4. UNDER密钥名称中，使用以下格式输入包含目录 ID 的密钥名称：

   ```
   aws/directory-services/d-xxxxxxxxx/seamless-domain-join
   ```

   这将用于检索应用程序中的秘密。

   Note

   你必须输入**aws/directory-services/*d-xxxxxxxxx*/seamless-domain-join**完全一样但是替换*d-xxxxxxxxxx*使用您的目录 ID。确保没有前导或结束空格。否则，域名加入将失败。
5. 将其他所有内容设置为默认值，然后选择下一步.

6. UNDER配置自动轮换，选择禁用自动旋转，然后选择下一步.
7. 审核设置，然后选择存储保存您的更改。Secrets Manager 控制台将返回您的账户中的密钥列表，并且在列表中现在包含您的新密钥。
8. 从列表中选择你新创建的秘密名称，然后记下键 ARN值。您需要在下一节中使用该名称。

创建所需的 IAM 策略和角色

使用以下先决条件步骤创建自定义策略，允许对您的 Secret Secrets Manager 无缝域加入密钥（您之前创建的）进行只读访问，并创建新的 LinuxEC2DomainJoin IAM 角色。

创建秘 Secrets Manager IAM 读取策略

您可以使用 IAM 控制台创建一个策略，授予对 Secret Secrets Manager 钥的只读访问权限。

创建秘 Secrets Manager IAM 读取策略

1. 登录到Amazon Web Services Management Console作为有权创建 IAM 策略的用户。然后在以下网址打开 IAM 控制台https://console.aws.amazon.com/iam/.
2. 在导航窗格中，选择 Policies (策略)。
3. 选择创建策略。
4. 选择 JSON 选项卡，然后复制以下 JSON 策略文档中的文本。然后将其粘贴到JSON文本框。

   Note

   确保你更换`ResourceARN` 与您之前创建的密钥的实际 ARN 相同。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue",
                "secretsmanager:DescribeSecret"
            ],
            "Resource": [
                "arn:aws:secretsmanager:us-east-1:############:secret:aws/directory-
service/d-xxxxxxxxxx/seamless-domain-join-example"
            ]
        }
    ]
}
```

5. 完成后，选择 Review policy（查看策略）。策略验证程序将报告任何语法错误。有关更多信息，请参阅 。验证 IAM 策略.
6. 在存储库的审核策略页面中，输入策略名称，例如**`SM-Secret-Linux-DJ-`*`d-xxxxxxxxxx`***`-Read`. 查看摘要部分以查看您的策略授予的权限。然后选择 。创建策略保存您的更改。新策略将显示在托管策略列表中，现在已准备好附加到身份。

   Note

   我们建议您为每个密码创建一个策略。这样做可以确保实例只能访问适当的机密，并最大限度地减少实例受到攻击时的影响。

创建 linuxEC2DOMAIN 加入角色

您可以使用 IAM 控制台创建用于域加入 Linux EC2 实例的角色。

创建 linuxEC2DomainJoin 角色

1. 登录到Amazon Web Services Management Console作为有权创建 IAM 策略的用户。然后在以下网址打开 IAM 控制台https://console.aws.amazon.com/iam/.
2. 在导航窗格中，选择 Roles（角色）。
3. 在内容窗格中，选择创建角色.
4. 在 Select type of trusted entity (选择受信任实体的类型）下，选择 Amazon service (Amazon 服务)。
5. UNDER选择使用案例选择EC2，然后选择后续：Permissions (下一步：权限)。
6. 适用于筛选策略中，执行以下操作：
   a. 输入 **AmazonSSMManagedInstanceCore**。然后，在列表中选中该项目的复选框。
   b. 输入 **AmazonSSMDirectoryServiceAccess**。然后，在列表中选中该项目的复选框。
   c. Enter**SM-Secret-Linux-DJ-*d-xxxxxxxxxx*-Read**（或您在上一流程中创建的策略名称）。然后，在列表中选中该项目的复选框。

   Note

   AmazonSSMDirectoryServiceAccess 提供了将实例加入由托管的 Active Directory 的权限。Amazon Directory Service. AmazonSSMManagedInstanceCore 提供了使用Amazon Systems Manager服务。有关使用这些权限创建角色的更多信息，以及有关可分配给 IAM 角色的其他权限和策略的信息，请参阅为 Systems Manager 创建 IAM 实例配置文件中的Amazon Systems Manager用户指南.
7. 选择 Next:。标签。
8. （可选）添加一个或多个标签键-值对以组织、跟踪或控制该角色的访问。接下来，选择 Next (下一步)：审核。
9. 在旁边Role name (角色名称)，输入新角色的名称，例如**LinuxEC2DomainJoin**或者你喜欢的另一个名字。
10. （可选）对于角色描述，请输入描述。
11. 选择 Create role（创建角色）。

无缝地联接 Linux EC2 实例

现在您已经配置了所有必备任务，可以使用以下过程无缝加入 Linux EC2 实例。

无缝地联接 Linux EC2 实例

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 从导航栏的 Region (区域) 选择器中，选择与现有目录相同的 Region (区域)。
3. 选择 Launch Instance（启动实例）。
4. 在存储库的步骤 1页面上，选择Select获取合适的 Amazon 系统映像 (AMI)。

   Note

   使用的 AMI 必须有Amazon Systems Manager（SSM Agent）版本 2.3.3.3.1644.0 或更高版本。要通过从该 AMI 启动实例来检查 AMI 中已安装的 SSM Agent 版本，请参阅获取当前安装的 SSM Agent 版本. 如果你需要升级 SSM 代理，请参阅在适用于 Linux 的 EC2 实例上安装和配置 SSM Agent.
5. 在存储库的步骤 2页面上，选择合适的实例类型，然后选择后续：配置实例详细信息.
6. 在存储库的步骤 3页面上，执行以下操作，然后选择后续：Add Storage (下一步: 添加存储)：
   a. 对于 Network，选择在其中创建了您的目录的 VPC。

b. 适用于子网在 VPC 中，选择一个公有子网。您选择的子网必须将所有外部流量都路由到 Internet 网关。否则将无法远程连接到实例。
c. 对于 Auto-assign Public IP (自动分配公有 IP)，选择 Enable (启用)。有关公有 IP 地址和私有 IP 地址的更多信息，请参阅Amazon EC2 实例 IP 寻址中的Windows 实例 Amazon EC2 用户指南.
d. 适用于域加入目录中，从列表中选择您的域。
e. 适用于IAM 角色中，选择您之前在先决条件部分创建的 IAM 角色步骤 2: 创建 linuxEC2Domain 加入角色.

7. 在两者上步骤 4和步骤 5页面，保留默认设置或根据需要进行更改。然后选择 。下一步在每个上调。
8. 在存储库的步骤 6页面上，选择已配置为允许从您的网络远程访问实例的安全组。然后选择查看和启动。
9. 在存储库的步骤 7页面上，选择启动，选择一个 key pair，然后选择实例启动.

Note

如果您使用 SUSE Linux 执行无缝域加入，则需要重新启动才能进行身份验证。要从 Linux 终端重新启动 SUSE，请键入sudo reboot.

维护 AD Connector 目录

此节介绍如何为您的 AD Connector 环境维护常见管理任务。

主题

- 删除目录 (p. 201)
- 查看目录信息 (p. 202)

删除目录

Simple AD 或AmazonDirectory Service，所有目录数据和快照都会删除，所有目录数据和快照都会删除，并且无法恢复。删除目录之后，加入到目录的所有实例都保持不变。但是，不能使用目录凭证登录这些实例。需要使用实例的本地用户账户登录这些实例。

删除 AAD Connector 目录时，本地目录保持不变。加入到目录的所有实例也保持不变，并保持加入本地目录。仍可以使用目录凭证登录这些实例。任何指向现已删除的 AD Connector 资源都将无法解析。

要删除目录

1. 在Amazon Directory Service控制台导航窗格，选择目录.
2. 确保没有Amazon应用程序已为要删除的目录。

   a. 在 Directories 页面上，选择您的目录 ID。
   b. 在 Directory details (目录详细信息) 页面上，选择 Application management (应用程序管理) 选项卡。在Amazon应用程序和服务部分，你可以看到哪个Amazon应用程序已为目录启用。

      - 禁用 WorkSpaces，则必须从目录中取消注册服务 WorkSpaces 控制台。有关更多信息，请参阅 。要从目录中取消注册中的亚马逊 WorkSpaces 管理指南.
      - 要禁用亚马逊 WorkSpaces 应用程序管理器，您必须在 Amazon WAM 控制台中删除所有应用程序分配。有关更多信息，请参阅 。移除所有应用程序分配中的Amazon WAM 管理指南.
      - 要禁用亚马逊 WorkDocs，您必须删除Amazon WorkDocs 亚马逊的站点 WorkDocs控制台。有关更多信息，请参阅 。删除站点中的亚马逊 WorkDocs 管理指南.
      - 要禁用亚马逊 WorkMail，您必须移除亚马逊 WorkMail 亚马逊的组织 WorkMail 控制台。有关更多信息，请参阅 。删除组织中的亚马逊 WorkMail 管理员指南.
      - 禁用Amazon Web Services Management Console访问。

- 要禁用 Amazon Relational Database Service 实例，必须从域中删除 Amazon RDS 实例。有关更多信息，请参阅 。在域中管理数据库实例中的Amazon RDS 用户指南.
- 要禁用亚马逊 QuickSight，您必须取消订阅 Amazon QuickSight. 有关更多信息，请参阅 。关闭 Amazon QuickSight 帐户中的亚马逊 QuickSight 用户指南.
- 要禁用 Amazon Connect，您必须删除Amazon Connect 实例。有关更多信息，请参阅 。删除 Amazon Connect中的Amazon Connect.
- 要禁用 FSx for Windows File Server for Windows for Windows FSx for Windows for Windows for Windows File e 有关更多信息，请参阅 。在 FSx or for Windows for Windows for for Windows for Windows中的Amazon FSx for Windows File Server.

  Note

  如果您将Amazon IAM Identity Center (successor to Amazon Single Sign-On)并且之前已将其连接到Amazon您计划删除的托管 Microsofor Microsoft AD 目录，然后才能删除它。有关更多信息，请参阅 。更改您的身份来源中的IAM 身份中心用户指南.

3. 在导航窗格中，选择 Directories。
4. 仅选择要删除的目录，然后单击Delete. 删除目录需要几分钟时间。目录删除之后，它会从目录列表中删除。

要删除无法使用的 AD Connector，请参阅我无法删除我的 AD Connector (p. 207).

查看目录信息

您可以查看有关目录的详细信息。

查看详细目录信息

1. 在Amazon Directory Service控制台选择导航窗格目录.
2. 单击目录的目录 ID 链接。有关目录的信息显示在目录详细信息页.

有关 Status 字段的更多信息，请参阅了解您的目录状态 (p. 48)。

更新 AD Connector 的 DNS 地址

使用以下步骤可更新 AD Connector 所指向的 DNS 地址。

Note

如果正在进行更新，则必须等待更新完成才能提交另一个更新。

Note

如果您将 WorkSpaces 与 AD Connector 一起使用，请确保您的 WorkSpaces 的 DNS 地址也已更新。有关更多信息，请参阅 。更新 WorkSpaces 的 DNS 服务器.

为 AD Connector 更新 DNS 设置

1. 在 Amazon Directory Service 控制台导航窗格中，选择 Directories (目录)。
2. 选择目录的目录 ID 链接。
3. 在 Directory details (目录详细信息) 页面上，选择 Network & security (网络与安全性)。
4. 在 Existing DNS settings (现有 DNS 设置) 部分中，选择 Update (更新)。
5. 在 Update existing DNS addresses (更新现有 DNS 地址) 对话框中，键入更新后的 DNS IP 地址，然后选择 Update (更新)。

AD Connector 的最佳实践

为避免问题并充分利用 AD Connector，您应该考虑以下建议和准则。

设置：先决条件

创建目录之前请考虑以下这些准则。

验证你有正确的目录类型

Amazon Directory Service 提供了多种方式来结合使用 Microsoft Active Directory 与其他 Amazon 服务。您可以根据预算成本选择具有适当功能的目录服务以满足您的需求：

- Amazon为 Microsoft Active Directory 提供 Directory Service是一种功能丰富的托管 Microsoft Active Directory。Amazon云。Amazon如果您的用户数超过 5000，并且需要在Amazon托管目录和本地目录。
- AD Connector将您现有的本地 Active Directory 连接到Amazon. 当您想要将现有本地目录与一起使用时，AD Connector 是您的最佳选择。Amazon服务。
- Simple AD是具有常用目录功能并与 Active Directory 兼容的低成本服务。在大多数情况下，Simple AD 成本最低的选择，如果您的用户数不超过 5000，并且不需要更高级的 Microsoft Active Directory 功能，这是您的最佳选择。

有关 Amazon Directory Service 选项的更详细比较，请参阅选择哪一个 (p. 1)。

确保您的 VPC 和实例配置正确

要连接到、管理和使用目录，必须正确配置目录所关联的 VPC。或者AmazonMicrosoft AD (p. 8)、AD Connetor (p. 171)，或者Simple AD 先决条件 (p. 209)有关 VPC 安全和网络要求的信息。

如果要将实例添加到域，请确保您具有实例连接并且可以远程访问实例，如将 EC2 实例加入Amazon托管的 Microsoft AD 目录 (p. 66) 中所述。

请注意限制

了解特定目录类型的各种限制。对象的可用存储空间和总大小是对象可以存储在目录中的对象数量的唯一限制。或者AmazonManaged Microsoft AD 配额 (p. 141)、AD Connector 配额 (p. 205)，或者Simple AD 配额 (p. 250)有关您所选目录的详细信息。

了解你的目录Amazon配置安全组并使用

Amazon创建安全组然后将其附加到你的目录弹性网络接口可以从对等互连或调整大小内部访问VPC.Amazon将配置安全组以阻止到目录的不必要的流量并允许必要的流量。

修改目录安全组

如果要修改目录的安全组的安全性，则可以这样做。只有在您完全了解安全组的筛选如何工作时，才进行这样的更改。有关更多信息，请参阅 。适用于 Linux 实例的 Amazon EC2 安全组中的Amazon EC2 用户指南. 不正确的更改可能会导致丢失与目标计算机和实例的通信。Amazon建议您不要尝试打开到您的目录的其他端口，因为这会降低目录的安全性。请仔细查看Amazon责任共担模式.

> **Warning**
>
> 从技术上来说，您可以将目录的安全组与您创建的其他 EC2 实例关联。但是，Amazon建议不要采用这种做法。Amazon为满足托管目录的功能或安全需求，可能会由于某些原因在未经通知的情况下修改安全组。此类更改会影响您将目录安全组关联到的任何实例，并可能中断关联实例的操作。此外，将目录安全组与您的 EC2 实例关联可能为 EC2 实例带来潜在的安全风险。

使用 AD Connector 时正确配置本地站点和子网

如果您的本地网络中已定义 Active Directory 站点，您必须确保在 Active Directory 站点中您 AD Connector 所在的 VPC 内定义了子网，并且 VPC 中的子网与您其他站点中的子网之间不存在冲突。

为发现域控制器，AD Connector 将使用子网 IP 地址范围与包含 AD Connector 的 VPC 中的子网 IP 地址范围接近的 Active Directory 站点。如果您的一个站点具有 IP 地址范围与您 VPC 中的 IP 地址范围相同的子网，则 AD Connector 将发现该站点中的域控制器，但该站点的实际地点不一定靠近您的区域。

了解用户名限制Amazon应用程序

Amazon Directory Service 支持大多数可用于构造用户名的字符格式。不过，对于登录时将使用的用户名实施了字符限制。Amazon应用程序，例如 WorkSpaces、Amazon WorkDocs、Amazon WorkMail 或 Amazon QuickSight。这些限制要求不使用以下字符：

- 空格
- 多字节字符
- !"#$%&'()*+,/:;<=>?@[\]^`{|}~

> **Note**
>
> 仅允许在 UPN 后缀之前使用 @ 符号。

为应用程序编程

在为您的应用程序编程之前，请考虑以下事项：

在推出生产之前进行加载测试

请务必对代表您的生产工作负载的应用程序和请求执行实验室测试，以确认目录将扩展至您的应用程序负载。如果您需要更多容量，请将您的负载分布在多个 AD Connector 目录中。

使用目录

下面是使用目录时应记住的一些建议。

定期轮换管理员凭证

定期更改 AD Connector 服务帐户管理员密码，并确保密码与您现有的 Active Directory 密码策略一致。有关如何更改服务账户密码的说明，请参阅 在中更新AD Connector 账户凭证Amazon Directory Service (p. 183)。

为每个域使用唯一的 AD 连接器

AD Connector 和本地 AD 域具有 1 对 1 关系。也就是说，对于每个本地域，包括 AD 林中您要针对其进行身份验证的子域，必须创建唯一的 AD Connector。您创建的每个 AD Connector 都必须使用不同的服务帐户，即使将它们连接到同一目录时也是如此。

兼容性检查

在使用 AD Connector 时，必须确保本地目录与Amazon Directory Service。有关您的责任的更多信息，请参阅我们的责任共担模型。

AD Connector 配额

以下是 AD Connector 的默认配额。除非另有说明，否则每个配额为每个区域

AD Connector 配额

资源	默认配额
AD Connector 目录	10
每个目录的最大注册证书颁发机构 (CA) 证书数	5

AD Connector 的应用程序兼容性策略

作为替代项AmazonDirectory Service Directory (Amazon托管的 Managed (p. 7))，AD Connector 是的活动目录代理Amazon仅创建了应用程序和服务。将此代理配置为使用指定 Active Directory 域。当应用程序必须在 Active Directory 中查找用户或组时，AD Connector 将代理对目录的请求。同样，当用户登录应用程序时，AD Connector 将代理对目录的身份验证请求。没有对 AD Connector 有效的第三方应用程序。

下面列出了兼容的 Amazon 应用程序和服务：

- Amazon Chime 更多信息，请参阅Connect 您的活动目录.
- 有关更多信息，请参阅Amazon Connect 的工作原理.
- Amazon EC2 for Windows 或 Linux — 您可使用 Amazon EC2 Windows 或 Linux 的无缝域加入功能将实例加入您的自管理 Active Directory (本地)。加入后，实例将直接与您的 Active Directory 通信并且绕过 AD Connector。有关更多信息，请参阅 将 EC2 实例加入 AD Connector 目录 (p. 195)。
- Amazon Web Services Management Console— 您可以使用 AD Connector 进行身份验证Amazon Web Services Management Console使用其 Active Directory 凭证的用户没有设置 SAML 基础设施。有关更多信息，请参阅 允许访问Amazon Web Services Management Console使用 AD 凭据 (p. 130)。
- 亚马逊 QuickSight 有关更多信息，请参阅在Amazon 管理用户账户 QuickSight 企业版.
- Amazon IAM Identity Center (successor to Amazon Single Sign-On)有关详细说明，请参阅将 IAM 身份中心连接到本地活动目录.
- Amazon Transfer Family有关详细说明，请参阅使用Amazon Directory Servicefor Microsoft Active Directory.
- AmazonClient VPN 更多信息，请参阅客户端身份验证和授权.
- 亚马逊 WorkDocs 有关详细说明，请参阅使用 AD Connector 连接到本地目录.
- 亚马逊 WorkMail 有关详细说明，请参阅集成Amazon WorkMail 使用现有目录（标准设置）.
- WorkSpaces 有关详细说明，请参阅启动 WorkSpace 使用AD Connector.

> **Note**
>
> Amazon RDS 与Amazon仅托管微软 AD，与 AD Connector 不兼容。有关更多信息，请参阅 Amazon 常见问题Amazon Directory Service页面中的 Microsoft AD 部分。

排查 AD Connector

以下内容可以帮助排查在创建或使用目录时可能会遇到的一些常见问题。

下面是 AD Connector 的一些常见问题。

EC2 实例的无缝域加入停止工作

如果 EC2 实例的无缝域加入之前正常工作，然后在 AD Connector 激活时停止，则表示您的凭证可能已过期。过期的凭证可能阻止 AD Connector 在 Active Directory 中创建计算机对象。

要解决此问题，请按以下顺序更新服务账户密码，以使密码匹配：

1. 在 Active Directory 中更新服务账户的密码
2. 在中的 AD Connector 中更新服务账户的密码Amazon Directory Service

仅在 Amazon Directory Service 中更新密码无法将密码更改推送到现有本地 Active Directory，因此务必按显示的顺序进行更新。

使用时，我遇到 “Invalid Credentials” 错误Amazon搜索用户或组的应用

使用时搜索用户时可能会遇到错误Amazon应用程序，例如 WorkSpaces 或 Amazon QuickSight，即使 AD Connector 状态处于活动状态。过期的凭证可能阻止 AD Connector 完成对 Active Directory 中的对象的查询。请使用上面提供的有序步骤更新服务账户的密码。

当我尝试连接我的本地目录时收到一条“DNS unavailable”错误

在连接您的本地目录时，您收到类似于以下内容的错误消息：

```
DNS unavailable (TCP port 53) for IP: <DNS IP address>
```

AD Connector 必须能够通过 TCP 和 UDP 经由端口 53 与您的本地 DNS 服务器通信。验证您的安全组和本地防火墙是否允许经由此端口进行 TCP 和 UDP 通信。有关更多信息，请参阅 AD Connetor (p. 171)。

在尝试连接到我的本地目录时，我收到一条“Connectivity issues detected”错误

在连接您的本地目录时，您收到类似于以下内容的错误消息：

```
Connectivity issues detected: LDAP unavailable (TCP port 389) for IP: <IP address>
Kerberos/authentication unavailable (TCP port 88) for IP: <IP address>
Please ensure that the listed ports are available and retry the operation.
```

AD Connector 必须能够通过 TCP 和 UDP 经由以下端口与您的本地域控制器通信。验证您的安全组和本地防火墙是否允许经由这些端口进行 TCP 和 UDP 通信。有关更多信息，请参阅 AD Connetor (p. 171)。

- 88 (Kerberos)
- 389 (LDAP)

在尝试连接到我的本地目录时，我收到一条“SRV record”错误

在连接您的本地目录时，您收到类似于以下一项或多项内容的错误消息：

```
SRV record for LDAP does not exist for IP: <DNS IP address>

SRV record for Kerberos does not exist for IP: <DNS IP address>
```

AD Connector 需要获取`_ldap._tcp.`*`<DnsDomainName>`*和`_kerberos._tcp.`*`<DnsDomainName>`*在连接您的目录时，SRV 记录。如果服务无法从您在连接到目录时所指定的 DNS 服务器上获取这些记录，则您将收到此错误。有关这些 SRV 记录的更多信息，请参阅 SRV record requirements (p. 173)。

我的目录卡在“Requested”状态

如果有一个目录处于“Requested”状态的时间超过 5 分钟，请尝试删除并重新创建该目录。如果此问题仍然存在，请联系Amazon Web Services SupportCenter.

我在创建目录时遇到“AZ Constrained”错误

一段时间Amazon2012 年之前创建的账户可能有权访问美国东部（弗吉利亚北部）、美国西部（加利福利亚北部）或亚太地区（东京）区域中不支持的可用区域Amazon Directory Service目录。如果在创建目录时遇到错误 (如上面的错误)，请选择其他可用区中的子网，再尝试创建目录。

我的某些用户无法进行向我的目录进行身份验证

用户账户必须启用 Kerberos 预身份验证。这是新用户账户的默认设置，但它不应进行修改。有关此设置的更多信息，请参阅 Microsoft TechNet 上的 Preauthentication。

AD Connector 使用的服务账户尝试进行身份验证时，我遇到 “Invalid Credentials” 错误

如果域控制器上的硬盘空间不足，则可能发生这种情况。确保域控制器的硬盘未满。

我无法删除我的 AD Connector

如果 AD Connector 切换到不可操作状态，则无法再访问域控制器。当还有应用程序链接到 AD Connector 时，我们会阻止删除 AD Connector，因为其中一个应用程序可能仍在使用该目录。请联系 Amazon Support。

Simple Active Directory

Simple AD 是由 Samba 4 Active Directory Compatible Server 提供支持的一个独立托管目录。它具有两种大小。

- 小型 - 支持最多 500 个用户 (大约 2000 个对象，包括用户、组和计算机)。
- 大型 - 支持最多 5000 个用户 (大约 20000 个对象，包括用户、组和计算机)。

Simple AD 提供的功能的子集Amazon托管 Microsoft AD，包括能够管理用户账户和组成员资格、创建和应用组策略、安全地连接到 Amazon EC2 实例以及提供基于 Kerberos 的单点登录 (SSO)。但是请注意，Simple AD 不支持与其他域的信任关系、Active MFA irectory 管理中心、PowerShell 支持、Active Directory 回收站、组托管服务账户以及适用于 POSIX 和 Microsoft 的架构扩展这类功能。应用程序。

Simple AD 具备许多优势：

- Simple AD 可让您更轻松地管理运行 Linux 和 Windows 的 Amazon EC2 实例并将 Windows 应用程序部署到Amazon云。
- 现在使用的很多需要 Microsoft Active Directory 支持的应用程序和工具可与 Simple AD 一起使用。
- Simple AD 中的用户帐户允许访问Amazon应用程序，如 WorkSpaces、Amazon WorkDocs 或 Amazon WorkMail。
- 你可以管理Amazon资源通过基于 IAM 角色的访问Amazon Web Services Management Console.
- 每日自动快照可实现时间点恢复。

Simple AD 不支持以下任何服务之一：

- Amazon AppStream 2.0
- Amazon Chime
- Amazon RDS for SQL Server
- Amazon RDS for Oracle
- Amazon IAM Identity Center (successor to Amazon Single Sign-On)
- 与其他域的信任关系
- Active Directory 管理中心
- PowerShell
- Active Directory 回收站
- 组托管服务账户
- 适用于 POSIX 和 Microsoft 应用程序的架构扩展

继续阅读本部分中的主题，了解如何创建自己的 Simple AD。

主题

- Simple AD 入门 (p. 209)
- 如何管理 Simple AD (p. 212)
- 教程：创建 Simple AD 目录 (p. 245)

- Simple AD 的最佳实践 (p. 247)
- Simple AD 配额 (p. 250)
- Simple AD 的应用程序兼容性策略 (p. 250)
- 排查 Simple AD (p. 251)

Simple AD 入门

Simple AD 在Amazon云。使用 Simple AD 创建目录时，Amazon Directory Service将代表您创建两个域控制器和 DNS 服务器。域控制器在 VPC 的不同子网中创建；此冗余帮助确保即使在出现故障时您的目录仍可访问。

主题

- Simple AD 先决条件 (p. 209)
- 创建 Simple AD 目录 (p. 210)
- 创建的内容 (p. 211)
- 配置 DNS (p. 211)

Simple AD 先决条件

要创建 Simple AD 目录，需要一个满足以下条件的 VPC：

- 至少两个子网。要正确安装 Simple AD，您必须将两个域控制器安装在位于不同可用区的单独子网中。另外，这两个子网必须处于同一无类别域间路由 (CIDR) 范围内。如果您想针对您的目录扩展或调整 VPC 大小，请确保为扩展的 VPC CIDR 范围同时选择这两个域控制器子网。
- VPC 必须具有默认硬件租户。
- 不得 使用以下 VPC 终端节点配置 VPC：
  - Route53 VPC 终端节点其中包括 *.amazonaws.com 的 DNS 条件覆盖，解析为非公开AmazonIP 地址
  - CloudWatch VPC 终端节点
  - VPC 终端节点
  - VPC 终端节点
- 如果 Simple AD 需要 LDAPS 支持，我们建议您使用连接到端口 389 的 Network Load Balancer 进行配置。通过此模型，可以针对 LDAPS 连接使用强证书，通过单个 NLB IP 地址简化对 LDAPS 的访问，并通过 NLB 自动进行故障转移。Simple AD 不支持在端口 636 上使用自签名证书。有关如何使用 Simple AD 配置 LDAPS 的详细信息，请参阅如何为 Simple AD 配置 LDAPS 终端节点中的AmazonSecurity 博客.
- 在目录中，必须启用下列加密类型：
  - RC4_HMAC_MD5
  - AES128_HMAC_SHA1
  - AES256_HMAC_SHA1
  - 未来的加密类型

    > **Note**
    >
    > 禁用这些加密类型会导致与 RSAT (远程服务器管理工具) 的通信问题，并影响可用性或您的目录。

Amazon Directory Service使用两个 VPC 结构。构成目录的 EC2 实例在您的外部运行Amazon账户，并由管理Amazon. 他们有两个网络适配器，`ETH0`和`ETH1`.`ETH0`是管理适配器，存在于您的账户之外。`ETH1`是在您的账户中创建的。

你的目录的管理 IP 范围`ETH0`以编程方式选择网络，以确保它不会与部署目录的 VPC 发生冲突。此 IP 范围可以在以下任一对中（因为目录在两个子网中运行）：

- 10.0.1.0/24 & 10.0.2.0/24
- 192.168.1.0/24 & 192.168.2.0/24

我们通过检查第一个八位字节来避免冲突`ETH1`CIDR。如果它以 10 开始，那么我们将选择一个 192.168.0.0/16 VPC，其中有 192.168.0.0/24 和 192.168.2.0/24 子网。如果第一个八位组不是 10，我们将选择 10.0.0/16 VPC，其中有 10.0.1.0/24 和 10.0.2.0/24 子网。

选择算法不包括 VPC 上的路由。因此，这种情况可能会导致 IP 路由冲突。

创建 Simple AD 目录

要创建新目录，请执行以下步骤。在开始此过程之前，请确保您已满足了Simple AD 先决条件 (p. 209)中确定的先决条件。

创建 Simple AD 目录

1. 在Amazon Directory Service控制台选择导航窗格，选择目录然后选择设置目录.
2. 在存储库的选择目录类型页面，选择Simple AD，然后选择下一步.
3. 在输入目录信息页面上，提供以下信息：

   目录大小

   从小型或大型大小选项中进行选择。有关大小的更多信息，请参阅Simple Active Directory (p. 208)。

   组织名称

   将用于注册客户端设备的目录的唯一组织名称。

   只有在作为启动 WorkSpaces 的一部分创建目录时，此字段才可用。

   目录 DNS 名称

   目录的完全限定名称，例如 `corp.example.com`。

   目录 NetBIOS 名称

   目录的短名称，如 `CORP`.

   管理员密码

   目录管理员的密码。目录创建过程将创建一个具有 `Administrator` 用户名和此密码的管理员账户。

   目录管理员密码区分大小写，且长度必须介于 8 到 64 (含) 个字符之间。至少，它还必须包含下列四种类别中三种类别的一个字符：

   - 小写字母 (a-z)
   - 大写字母 (A-Z)
   - 数字 (0-9)
   - 非字母数字字符 (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)

   确认密码

   重新键入管理员密码。

   目录描述

   目录的可选描述。

4. 在 Choose VPC and subnets (选择 VPC 和子网) 页面上，提供以下信息，然后选择 Next (下一步)。

   VPC

   目录的 VPC。

   Subnets (子网)

   为域控制器选择子网。两个子网必须位于不同的可用区。

5. 在 Review & create (检查并创建) 页面上，检查目录信息并进行任何必要的更改。如果信息正确，请选择 Create directory (创建目录)。目录创建需要几分钟时间。创建后，Status 值将更改为 Active。

创建的内容

使用 Simple AD 创建目录时，Amazon Directory Service将代表您执行以下任务：

- 在 VPC 中设置基于 Samba 的目录。
- 创建具有用户名 `Administrator` 和指定密码的目录管理员账户。您可以使用此账户管理您的目录。

  Important

  请务必保存此密码。Amazon Directory Service 不会存储此密码，并且此密码无法检索。但是，您可以通过 Amazon Directory Service 控制台或使用 ResetUserPassword API 重置密码。

- 为目录控制器创建安全组。
- 创建一个名为 `AWSAdminD-xxxxxxxx` 具有域管理员权限的账户。此账户由 Amazon Directory Service 用于为目录维护操作执行自动操作，如拍摄目录快照和 FSMO 角色移交。此账户的凭证由 Amazon Directory Service 进行安全存储。
- 自动创建 elastic network interface (ENI) 并将其与每个域控制器相关联。其中每个 ENI 对于您的 VPC 与 Amazon Directory Service 域控制器之间的连接都至关重要，绝不应删除。您可以识别所有保留用于的网络接口Amazon Directory Service通过描述："Amazon 为目录创建了网络接口目录 ID"。有关更多信息，请参阅 。弹性网络接口在适用于 Windows 实例的 Amazon EC2 用户指南中。

  Note

  默认情况下，域控制器将部署在一个区域的两个可用区域中，并连接到您的 Amazon Virtual Private Cloud (VPC)。每天自动进行一次备份，Amazon Elastic Block Store (EBS) 卷将进行加密，以确保静态数据得到安全保护。使用相同的 IP 地址在同一可用区中自动替换出现故障的域控制器，并且可以使用最新的备份执行完整的灾难恢复。

配置 DNS

Simple AD 将 DNS 请求转发到 Amazon 针对您 VPC 提供的 DNS 服务器的 IP 地址。这些 DNS 服务器将解析您 Route 53 私有托管区域中配置的名称。通过将您的本地计算机指向 Simple AD，您现在可以将 DNS 请求解析到私有托管区域。

请注意，要使您的 Simple AD 能够响应外部 DNS 查询，必须将包含您 Simple AD 的 VPC 的网络访问控制列表 (ACL) 配置为允许来自 VPC 外部的流量。

如果您没有使用 Route 53 私有托管区域，您的 DNS 请求将被转发到公有 DNS 服务器。

如果您使用的是 VPC 外部的自定义 DNS 服务器，并且您想要使用私有 DNS，则必须重新进行配置，以便使用您 VPC 中 EC2 实例上的自定义 DNS 服务器。有关更多信息，请参阅使用私有托管区域。

如果您想让 Simple AD 同时使用您 VPC 中的 DNS 服务器以及 VPC 外部的私有 DNS 服务器解析名称，则可以使用 DHCP 选项集执行此操作。有关详细示例，请参阅此文章。

> **Note**
>
> Simple AD 域中不支持 DNS 动态更新。可以改为通过在加入域的实例上使用 DNS 管理器连接到目录，直接进行更改。

有关 Route 53 的更多信息，请参阅Route 53 是.

如何管理 Simple AD

此节列出了运行和维护 Simple AD 环境的所有过程。

主题

- 在 Simple AD 中管理用户和群组 (p. 212)
- 监控您的 Simple AD 目录 (p. 215)
- 将 EC2 实例加入 Simple AD 目录 (p. 218)
- 维护您的 Simple AD 目录 (p. 234)
- 启用访问权限Amazon应用程序和服务 (p. 237)
- 允许访问Amazon Web Services Management Console使用 AD 凭据 (p. 243)

在 Simple AD 中管理用户和群组

用户表示有权访问您的目录的独立个人或实体。对于针对用户组授予或拒绝权限非常有用，从而不必将这些权限应用于每个独立用户。如果用户移动到不同的组织，您将该用户移动到不同的组后，他们会自动接收新组织所需的权限。

在中创建用户和组Amazon Directory Service目录中，您必须使用已加入到Amazon Directory Service以具有创建用户和组权限的用户身份登录。您还需要在 EC2 实例上安装 Active Directory 工具，以便添加具有 Active Directory 用户和计算机管理单元的用户和组。有关如何设置 EC2 实例和安装所需工具的更多信息，请参阅 将 Linux EC2 实例无缝地加入您的 Simple AD 目录。 (p. 220)。

> **Note**
>
> 用户账户必须启用 Kerberos 预身份验证。这是新用户账户的默认设置，但它不应进行修改。有关此设置的更多信息，请参阅 Microsoft TechNet 上的 Preauthentication。

以下主题介绍了如何创建和管理用户和组。

主题

- 安装 Active Directory 管理工具 (p. 212)
- 创建用户 (p. 213)
- 删除用户 (p. 214)
- 重置用户密码 (p. 214)
- 创建组 (p. 215)
- 如何为群组添加用户 (p. 215)

安装 Active Directory 管理工具

要从 EC2 Windows 实例中管理您的目录，您需要在该实例中安装 Active Directory Domain Services 和 Active Directory Lightweight Directory Services 工具。按照以下过程操作，在 Windows Server 2012、Windows Server 2016 或 Windows Server 2019 上安装这些工具。

您可以选择使用 Windows PowerShell 安装 Active Directory 管理工具。例如，您可以使用 `Install-WindowsFeature RSAT-ADDS` 从 PowerShell 提示符安装 Active Directory 远程管理工具。有关详细信息，请参阅 Microsoft 网站上的 Install-WindowsFeature。

在 Windows Server 2012 到 Windows Server 2019 上安装 Active Directory 管理工具

在 Windows Server 2012 到 Windows Server 2019 上安装 Active Directory 管理工具

1. 通过从“开始”屏幕选择服务器管理器，打开服务器管理器。
2. 在 Server Manager Dashboard (服务器管理器控制面板) 中，选择 Add roles and features (添加角色和功能)。
3. 在 Add Roles and Features Wizard (添加角色和功能向导) 中，依次选择 Installation Type (安装类型)、Role-based or feature-based installation (基于角色或基于功能的安装) 和 Next (下一步)。
4. 在 Server Selection (服务器选择) 下，确保已选中本地服务器，然后选择左侧导航栏中的 Features (功能)。
5. 在 Features (功能) 树中，打开 Remote Server Administration Tools (远程服务器管理工具)、Role Administration Tools (角色管理工具)，选择 AD DS and AD LDS Tools (AD DS 和 AD LDS 工具)，向下滚动并选择 DNS Server Tools (DNS 服务器工具)，然后选择 Next (下一步)。
6. 检查信息，然后选择安装。当该功能安装完成后，Active Directory Domain Services 和 Active Directory Lightweight Directory Services 工具将出现在“开始”屏幕的管理工具文件夹中。

创建用户

> **Note**
>
> 使用 Simple AD 时，如果在 Linux 实例上创建用户账户时使用了 “强制用户在首次登录时更改密码” 选项，则该用户无法使用首次更改其密码。kpasswd. 要首次更改密码，域管理员必须使用 Active Directory 管理工具更新用户密码。

使用以下过程可创建其 EC2 实例加入到 Simple AD 目录的用户。

创建用户

1. 打开“Active Directory 用户和计算机”工具。中有一个快捷方式访问此工具管理工具folder。

   > **Tip**
   >
   > 您可以在实例上从命令提示符运行以下命令，直接打开 Active Directory 用户和计算机工具箱。

   ```
   %SystemRoot%\system32\dsa.msc
   ```

2. 在目录树中，在目录的 NetBIOS 名称 OU 下选择要存储用户（例如 Corp\ Users）的 OU。有关目录使用的 OU 结构的更多信息，请参阅Amazon，请参阅创建的内容 (p. 10).
3. 在 Action 菜单上，单击 New，然后单击 User 打开新用户向导。
4. 在向导的第一页上，输入以下字段的值，然后单击。下一步.
   - 名
   - 姓
   - User logon name
5. 在向导的第二页上，在密码和Confirm Password (确认密码). 确保用户必须在下次登录时更改密码选项已选中。不应选择任何其他选项。单击 Next（下一步）。
6. 在向导的第三页上，验证新用户的信息正确无误，然后单击。Finish. 新用户会出现在 Users 文件夹中。

删除用户

使用以下过程可删除其 EC2 Windows 实例加入到 Simple AD 目录的用户。

删除用户

1. 打开“Active Directory 用户和计算机”工具。在中有一个快捷方式访问此工具管理工具folder。

   Tip

   您可以在实例上从命令提示符运行以下命令，直接打开 Active Directory 用户和计算机工具框。

   ```
   %SystemRoot%\system32\dsa.msc
   ```

2. 在目录树中，选择包含要删除的用户（例如，Corp\ Users）的 OU。
3. 选择 账户。然后，选择要删除的用户。右键击名称然后选择Delete从上下文菜单中。
4. 选择是在对话框中是否确定要删除此对象？ 此操作将永久删除所选的用户。

重置用户密码

用户必须遵守目录中定义的密码策略。有时这可以获得最好的用户，包括目录管理员，然后他们忘记了密码。发生这种情况时，您可以使用Amazon Directory Service如果用户驻留在 Simple AD 或Amazon托管 Microsoft AD 目录。

除以下情况外，您可以重置目录中的任何用户的密码：

- 对于 Simple AD，您不能为任何属于Domain Admins要么Enterprise Admins组（管理员用户除外）。
- 适用于Amazon托管 Microsoft AD，您不能重置 OU 中的任何用户的密码，此 OU 中基于您在创建目录时键入的 NetBIOS 名称。例如，您无法在Amazon预留OU。有关的 OU 结构的更多信息Amazon托管 Microsoft AD 目录，请参阅创建的内容 (p. 10).

您可以使用以下任何方法重置用户的密码。

方法 1：重置用户密码（Amazon Web Services Management Console）

1. 在Amazon Directory Service控制台导航窗格，下Active Directory，选择目录，然后在列表中选择要重置用户密码的目录。
2. 在存储库的目录详细信息页面，选择重置用户密码.
3. 在重置用户密码在对话框中用户名键入需要更改其密码的用户的用户的名称。
4. 在中键入密码新建新密码和确认密码，然后选择Reset password.

方法 2：重置用户密码（Windows PowerShell）

1. 打开 Windows PowerShell。
2. 键入以下命令，然后将用户名 “joebob” 和密码 “P @ssw0rd” 替换为所需的凭据。请参阅重置 dsuserPassword Cmdlet有关.

   ```
   Reset-DSUserPassword -UserName joebob -DirectoryId d-1234567890 -NewPassword
   P@ssw0rd
   ```

方法 3：重置用户密码（Amazon CLI）

1. 打开 Amazon CLI。

2. 键入以下命令，然后将用户名 “joebob” 和密码 “P @ssw0rd” 替换为所需的凭据。请参阅重置用户密码中的Amazon CLI命令参考有关.

```
aws ds reset-user-password --directory-id d-1234567890 --user-name joebob --
new-password P@ssw0rd
```

创建组

使用以下过程可创建其 EC2 实例加入到 Simple AD 目录的安全组。

创建组

1. 打开“Active Directory 用户和计算机”工具。中有一个快捷方式访问此工具管理工具folder。

   Tip

   您可以在实例上从命令提示符运行以下命令，直接打开 Active Directory 用户和计算机工具框。

   ```
   %SystemRoot%\system32\dsa.msc
   ```

2. 在目录树中，在目录的 NetBIOS 名称 OU 下选择要存储组的 OU（例如，Corp\ Users）。有关目录使用的 OU 结构的更多信息，请参阅Amazon请参阅创建的内容 (p. 10).
3. 在 Action 菜单上，单击 New，然后单击 Group 打开新组向导。
4. 键入组的名称Group nameSelect,Group scopeSelect, 然后选择安全(对于)Group type.
5. 单击 OK（确定）。新的安全组将出现在用户folder。

如何为群组添加用户

使用以下过程可将用户添加到其 EC2 实例加入到 Simple AD 目录的安全组。

如何为群组添加用户

1. 打开“Active Directory 用户和计算机”工具。在中有这个工具的快捷方式管理工具folder。

   Tip

   您可以从实例上从命令提示符运行以下命令，直接打开 Active Directory 用户和计算机工具框。

   ```
   %SystemRoot%\system32\dsa.msc
   ```

2. 在目录树中，选择存储组的目录的 NetBIOS 名称 OU 下的 OU，然后选择要将用户添加为成员的组。
3. 在存储库的操作按菜单中，单击属性以打开组的属性对话框。
4. Select成员Select, 然后单击Add.
5. 适用于输入要选择的对象名称，键入要添加的用户名，然后单击确定. 名称将显示在成员的列表。再次单击 OK 更新组成员资格。
6. 通过在用户文件夹然后单击属性中的操作从菜单中打开属性对话框。Select的成员选项卡。您应该在用户所属的组列表中看到组的名称。

监控您的 Simple AD 目录

您可以通过以下方法监控您的 Simple AD 目录：

主题

- 了解您的目录状态 (p. 216)
- 配置目录状态通知 (p. 217)

了解您的目录状态

以下是目录的各种状态。

Active (处于活动状态)

该目录运行正常。Amazon Directory Service 未检测到您的目录存在任何问题。

创建

当前正在创建该目录。目录创建过程通常需要 20 到 45 分钟，但可能因系统负载而异。

Deleted (已删除)

已删除该目录。已释放该目录的所有资源。一旦目录进入此状态，便无法恢复。

Deleting (正在删除)

当前正在删除该目录。目录将保持此状态，直到被完全删除。一旦目录进入此状态，将无法取消删除操作，目录也无法恢复。

已失败

无法创建该目录。请删除此目录。如果此问题仍存在，请联系Amazon Web Services SupportCenter.

Impaired (受损)

目录正在降级状态下运行。检测到一个或多个问题，可能有的目录操作未在完全有效地工作。目录处于此状态有多个可能的原因。这些原因包括正常的操作维护活动（如打补丁或 EC2 实例轮换）、其中一台域控制器上的某个应用程序临时成为热点，或者您对网络进行了更改（可能无意中破坏目录通信）。有关更多信息，请参阅故障排除AmazonMicrosoft Managed Managed Microsoft AD (p. 161)、排查 AD Connector (p. 205)、排查 Simple AD (p. 251)。对于与正常维护相关的问题，Amazon在 40 分钟内解决。如果在查看故障排除主题后，您的目录处于受损状态的时间超过 40 分钟，我们建议您联系。Amazon Web Services SupportCenter.

> **Important**
>
> 当目录处于受损状态时，请不要还原快照。解决受损问题极少需要快照还原。有关更多信息，请参阅 快照或恢复你的目录 (p. 118)。

Inoperable (不可操作)

该目录无法正常工作。所有目录终端节点都报告有问题。

Requested (已请求)

创建目录的请求当前正在等待处理。

RestoreFailed (还原失败)

从快照还原目录失败。请重试还原操作。如果这种情况继续存在，请尝试其他快照或联系。Amazon Web Services SupportCenter.

Restoring (还原)

当前正从自动或手动快照中还原目录。从快照还原通常需要几分钟时间，具体取决于快照中的目录数据大小。

有关更多信息，请参阅Simple AD 目录状态原因 (p. 252)。

配置目录状态通知

通过使用 Amazon Simple Notification Service (Amazon SNS)，您可以在目录状态发生变化时接收电子邮件或文本 (SMS) 消息。如果目录从 Active 状态变为受损或无法操作状态. 当目录恢复为“Active”状态时，您也会收到通知。

工作方式

Amazon SNS 使用 “主题” 来收集和分发消息。每个主题都有一个或多个订阅者，他们接收发布至该主题的消息。使用以下步骤你可以添加Amazon Directory Service作为 Amazon SNS 主题的发布者。Amazon Directory Service 在检测到您的目录状态发生变化时，会向该主题发布一条消息，该消息随后发送给该主题的订阅者。

您可以关联多个目录作为单个主题的发布者。您还可以将目录状态消息添加到您之前在 Amazon SNS 中创建的主题。您可以对谁能够向主题发布内容和订阅主题进行详细的控制。有关 Amazon SNS 的完整信息，请参阅什么是 Amazon SNS？.

为您的目录启用 SNS 消息发送

1. 登录 Amazon Web Services Management Console，然后打开 Amazon Directory Service 控制台，网址为：https://console.aws.amazon.com/directoryservicev2/。
2. 在 Directories 页面上，选择您的目录 ID。
3. 选择维护选项卡。
4. 在目录监控部分，选择操作选择，然后选择创建通知.
5. 在存储库的创建通知页面，选择选择通知类型选择，然后选择创建新通知. 或者，如果您已有一个现有 SNS 主题，您可以选择关联现有 SNS 主题将状态消息从此目录发送到该主题。

   Note

   如果选择创建新通知但之后使用与现有 SNS 主题相同的主题名称，Amazon SNS 不会创建新主题，只是向现有主题添加新的订阅信息。
   如果选择关联现有 SNS 主题，您只能选择与该目录位于同一区域的 SNS 主题。
6. 选择收件人类型然后输入Recipient联系信息。如果您为 SMS 输入电话号码，请只使用数字。不包括破折号、空格或圆括号。
7. (可选) 提供主题的名称和 SNS 显示名称。显示名称为最多 10 个字符的短名称，包含在来自该主题的所有 SMS 消息中。使用 SMS 选项时必需提供显示名称。

   Note

   如果您使用仅有DirectoryServiceFullAccess托管策略，您的主题名称必须以 “DirectoryMonitor” 开头。如果您想进一步自定义主题名称，您需要对 SNS 的额外权限。
8. 选择创建。

如果您要指定更多 SNS 订阅者，例如其他电子邮件地址、Amazon SQS 队列或Amazon Lambda您可通过 Amazon SNS 控制台完成这一操作：https://console.aws.amazon.com/sns/v3/home.

从主题移除目录状态消息

1. 登录 Amazon Web Services Management Console，然后打开 Amazon Directory Service 控制台，网址为：https://console.aws.amazon.com/directoryservicev2/。
2. 在 Directories 页面上，选择您的目录 ID。
3. 选择维护选项卡。
4. 在目录监控部分中，在列表中选择 SNS 主题名称，然后选择操作选择，然后选择Remove.
5. 选择 Remove。

这会移除您的目录的选定 SNS 主题发布者身份。如果您要删除整个主题，可通过处的 Amazon SNS 控制台执行此操作：https://console.aws.amazon.com/sns/v3/home.

> **Note**
>
> 在使用 SNS 控制台删除 Amazon SNS 主题之前，您应确保目录没有在向该主题发送状态消息。如果您使用 SNS 控制台删除 Amazon SNS 主题，则 Directory Services 控制台中不会立即反映出此更改。直到目录下次向已删除的主题发布通知时，您才会获得通知，那时，您将在该目录的 Monitoring 选项卡上看到一个更新状态，指示无法找到该主题。
> 因此，为避免错过重要的目录状态消息，请在删除从接收消息的任何主题之前，Amazon Directory Service将您的目录与其他 Amazon SNS 主题关联。

将 EC2 实例加入 Simple AD 目录

EC2 实例在启动时，您可以使用以下方式将其无缝加入到您的目录域中。Amazon Systems Manager. 有关更多信息，请参阅 。无缝地联接 Windows 实例Amazon Directory Service域中的Windows 实例 Amazon EC2 用户指南.

如果需要手动将 EC2 实例加入到您的域，则必须在正确的区域和安全组或子网中启动实例，然后将实例加入到该域。

要能够远程连接到这些实例，必须具有从所连接的网络到实例的 IP 连接。在大多数情况下，这要求 Internet 网关连接到 VPC，并且实例具有公有 IP 地址。

主题

- 无缝加入 Windows EC2 实例 (p. 218)
- 手动加入 Windows 实例 (p. 219)
- 将 Linux EC2 实例无缝地加入您的 Simple AD 目录。 (p. 220)
- 手动加入 Linux 实例 (p. 224)
- 委派 Simple AD 的目录加入权限 (p. 232)
- 创建 DHCP 选项集 (p. 233)

无缝加入 Windows EC2 实例

此过程无缝地将 Windows EC2 实例联接到 Simple AD 目录。

无缝地联接 Windows EC2 实例

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。
2. 从导航栏的 Region (区域) 选择器中，选择与现有目录相同的 Region (区域)。
3. 选择 Launch Instance（启动实例）。
4. 在存储库的步骤 1在页面上，选择Select获取适当的 AMI。
5. 在存储库的步骤 2页面上，选择合适的实例类型，然后选择后续：配置实例详细信息.
6. 在存储库的步骤 3页面上，执行以下操作，然后选择：后续：Add Storage (下一步: 添加存储)：

   1. 对于 Network，选择在其中创建了您的目录的 VPC。
   2. 适用于子网在 VPC 中选择一个公有子网。选择的子网必须将所有外部流量都路由到 Internet 网关。否则将无法远程连接到实例。
   3. 对于 Auto-assign Public IP (自动分配公有 IP)，选择 Enable (启用)。

      有关公有 IP 地址和私有 IP 地址的更多信息，请参阅Amazon EC2 实例 IP 寻址中的Windows 实例 Amazon EC2 用户指南.
   4. 适用于域加入目录中，从列表中选择您的域。
   5. 对于 IAM role (IAM 角色)，执行以下操作之一：

选择具有Amazon托管策略AmazonSSMManagedInstanceCore和AmazonSSMDirectoryServiceAccess附加到它。

-或者-

如果您尚未创建具有AmazonSSMManagedInstanceCore和AmazonSSMDirectoryServiceAccess附加到它的托管策略，请选择创建新的 IAM 角色链接，然后执行以下操作：

a. 选择 Create role（创建角色）。
b. 在 Select type of trusted entity (选择受信任实体的类型）下，选择 Amazon service (Amazon 服务)。
c. UNDER选择此角色将使用的服务。在完整的服务列表中，选择EC2.
d. UNDER选择您的使用案例，选择EC2，然后选择后续：Permissions (下一步：权限)。
e. 在策略列表中，选择AmazonSSMManagedInstanceCore和AmazonSSMDirectoryServiceAccess政策。（要筛选列表，请键入**SSM**在搜索框中。）

   Note

   AmazonSSMDirectoryServiceAccess提供将实例加入由托管的 Active Directory 的权限 Amazon Directory Service. AmazonSSMManagedInstanceCore提供了使用 Systems Manager 服务所需的最低权限。有关使用这些权限创建角色的更多信息，以及有关可分配给 IAM 角色的其他权限和策略的信息，请参阅为 Systems Manager 创建 IAM 实例配置文件中的Amazon Systems Manager用户指南.

f. 选择 Next:。标签。
g. （可选）添加一个或多个标签键/值对以组织、跟踪或控制该角色的访问，然后选择后续：审核。
h. 对于角色名称，请输入新角色的名称，如 **EC2DomainJoin** 或所需的其他名称。
i. （可选）对于角色描述，请输入描述。
j. 选择 Create role（创建角色）。
k. 返回到步骤 3页. 适用于IAM 角色中，选择旁边的刷新图标IAM 角色. 您的新角色应显示在菜单中。选择该角色，将此页面上的其余设置保留默认值，然后选择后续：添加存储.

7. 在两者上步骤 4和步骤 5页面上，保留默认设置或根据需要进行更改，然后选择下一步按钮。
8. 在存储库的步骤 6页面上，为已配置为允许从您的网络远程访问实例的实例选择安全组，然后选择审核并启动.
9. 在存储库的步骤 7在页面上，选择启动，选择 key pair，然后选择实例启动.

手动加入 Windows 实例

要将现有的 Amazon EC2 Windows 实例手动加入简单广告，或者Amazon对于 Microsoft Active Directory 目录的 Directory Service，该实例必须按照中指定的方式启动无缝地联接 Windows EC2 实例 (p. 66).

将 Windows 实例加入 Simple AD 或Amazon托管 Microsoft AD 目录

1. 使用任何远程桌面协议客户端连接到实例。
2. 在实例上打开 TCP/IPv4 属性对话框。

   a. 打开 Network Connections。

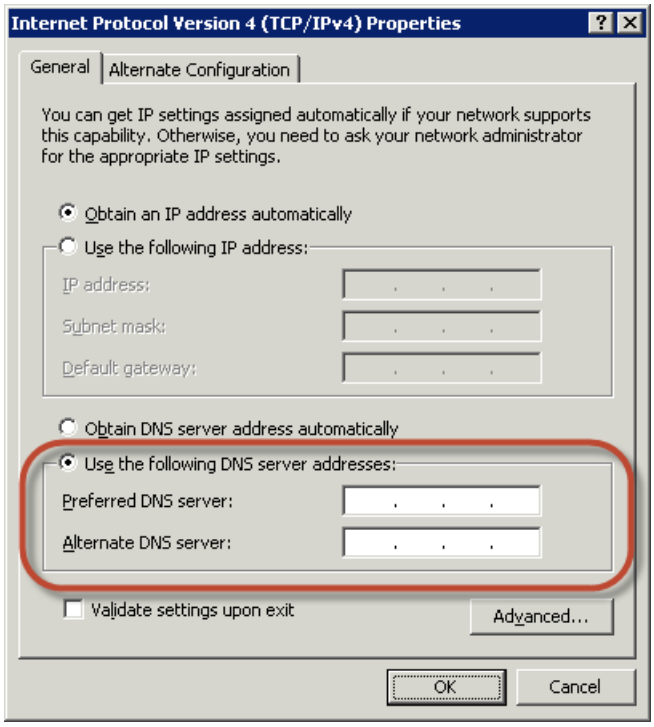
      Tip

      您可以在实例上从命令提示符运行以下命令，直接打开 Network Connections。

```
%SystemRoot%\system32\control.exe ncpa.cpl
```

b. 打开任何已启用网络连接的上下文菜单 (右键单击)，然后选择 Properties。
c. 在连接属性对话框中，打开 (双击) Internet Protocol Version 4。

3. Select使用以下 DNS 服务器地址：，更改首选 DNS 服务器和备用 DNS 服务器的 IP 地址的地址 Amazon Directory Service-提供 DNS 服务器，然后选择确定.



4. 打开实例的 System Properties 对话框，选择 Computer Name 选项卡，然后选择 Change。

   Tip

   您可以在实例上从命令提示符运行以下命令，打开 System Properties 对话框。

```
%SystemRoot%\system32\control.exe sysdm.cpl
```

5. 在成员选择字段，选择域中，输入您的完全限定姓名Amazon Directory Service选择目录，然后选择确定.
6. 当系统提示输入域管理员的名称和密码时，输入具有域加入权限的账户的用户名和密码。有关委托这些权限的更多信息，请参阅为委派目录加入权限Amazon管理 Microsoft AD (p. 90)。

   Note

   可以输入完全限定的域名或 NetBios 名称，后跟反斜杠 (\)，然后是用户名。
   使用 时Amazon管理 Microsoft AD，用户名将为管理员. 例如，corp.example.com\admin 或 corp\admin。
   如果使用 Simple AD，用户名将为管理员. 例如，corp.example.com\ 管理员要么corp\ 管理员.

7. 收到欢迎加入域的消息之后，重新启动实例使更改生效。

现在实例已加入域，您可以远程登录该实例并安装实用工具来管理目录，如添加用户和组。

将 Linux EC2 实例无缝地加入您的 Simple AD 目录。

此过程无缝地将 Linux EC2 实例联接到 Simple AD 目录。

支持以下 Linux 实例分发版和版本：

- Amazon Linux AMI 2018.03.0
- Amazon Linux 2（64 位 x86）
- Red Hat Enterprise Linux 8 (HVM)（64 位 x86）
- Ubuntu Server 18.04 LTS 和 Ubuntu Server 16.04 LTS
- CentOS 7 x86-64
- SUSE Linux Enterprise Server 15 SP1

> **Note**
>
> Ubuntu 14 和红帽企业 Linux 7 之前的发行版不支持无缝域加入功能。

先决条件

在设置无缝域加入到 Linux EC2 实例之前，您需要完成本节中的步骤。

选择您的无缝域加入服务帐户

你可以将 Linux 计算机无缝连接到你的 Simple AD 域。为此，必须创建具有创建计算机账户权限的用户账户，以将计算机加入到该域。虽然成员Domain Admins或者其他组可能拥有足够权限将计算机加入到该域，我们不建议这样做。作为最佳做法，我们建议您使用具有将计算机加入域所需的最低权限的服务帐户。

有关如何处理和委派服务帐户以创建计算机帐户的权限的信息，请参阅向您的服务账户委派权限 (p. 174).

创建密码以存储域服务帐户

您可以使用Amazon Secrets Manager以存储域服务帐户。

创建密码并存储域服务帐户信息

1. 登录到Amazon Web Services Management Console然后打开Amazon Secrets Manager在控制台https://console.aws.amazon.com/secretsmanager/.
2. 选择 Store a new secret (存储新密钥)。
3. 在 Store a new secret（存储新密钥）页面上，执行以下操作：
   a. 在 Select secret type (选择密钥类型) 下，选择 Other type of secrets (其他密钥类型)。
   b. UNDER在密钥中指定要存储在密钥中的键-值对中，执行以下操作：
      i. 在第一个框中，输入**`awsSeamlessDomainUsername`**. 在同一行上，在下一个框中，输入服务帐户的用户名。例如，如果您之前使用 PowerShell 命令，则服务帐户名称将为`awsSeamlessDomain`.

         > **Note**
         >
         > 你必须输入**`awsSeamlessDomainUsername`**完全如此。确保没有任何前导或结束空格。否则，域加入将失败。

      ii. 选择添加行.
      iii. 在新行中，在第一个框中，输入**`awsSeamlessDomainPassword`**. 在同一行的下一个框中，输入服务帐号的密码。

         > **Note**
         >
         > 你必须输入**`awsSeamlessDomainPassword`**完全如此。确保没有任何前导或结束空格。否则，域加入将失败。

      iv. UNDER选择加密密钥，选择DefaultenCryptionKey从菜单中。当您选择此选项时，Secret Secrets Manager 始终会对密码进行加密，并免费提供给您。你也可以选择自己创建的密钥。
      v. 选择 Next (下一步)。

4. UNDER密钥名称中，使用以下格式输入包含目录 ID 的密钥名称：

```
aws/directory-services/d-xxxxxxxxx/seamless-domain-join
```

这将用于检索应用程序中的秘密。

> **Note**
>
> 你必须输入**aws/directory-services/*d-xxxxxxxxx*/seamless-domain-join**完全一样但是替换*d-xxxxxxxxxxxxxxxxxxx*使用您的目录 ID。确保没有前导空格或结束空格。否则，域加入将失败。

5. 将其他所有内容设置为默认值，然后选择下一步.
6. UNDER配置自动轮换，选择禁用自动轮换选择，然后选择下一步.
7. 查看设置，然后选择：存储以保存您的更改。Secrets Manager 控制台将返回您的账户中的密钥列表，并且在列表中现在包含新的密钥。
8. 从列表中选择你新创建的秘密名称，然后记下键 ARN值。您需要在下一节中使用该名称。

创建所需的 IAM 策略和角色

使用以下先决条件步骤创建自定义策略，允许对您的 Secret Secrets Manager 无缝域加入密钥（您之前创建的）进行只读访问，并创建新的 LinuxEC2DomainJoin IAM 角色。

创建秘 Secrets Manager IAM 读取策略

您可以使用 IAM 控制台创建一个策略，授予对 Secret Secrets Manager 钥的只读访问权限。

创建秘 Secrets Manager IAM 读取策略

1. 登录到Amazon Web Services Management Console作为有权创建 IAM 策略的用户。然后，使用打开 IAM 控制台：https://console.aws.amazon.com/iam/.
2. 在导航窗格中，选择 Policies (策略)。
3. 选择创建策略。
4. 选择 JSON 选项卡，然后复制以下 JSON 策略文档中的文本。然后将其粘贴到JSON文本框。

> **Note**
>
> 确保你更换`ResourceARN` 与之前创建的密钥的实际 ARN 相同。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue",
                "secretsmanager:DescribeSecret"
            ],
            "Resource": [
                "arn:aws:secretsmanager:us-east-1:############:secret:aws/directory-
service/d-xxxxxxxxxx/seamless-domain-join-example"
            ]
        }
    ]
}
```

5. 完成后，选择 Review policy（查看策略）。策略验证程序将报告任何语法错误。有关更多信息，请参阅 。验证 IAM 策略.

6. 在存储库的审核策略页面中，输入策略名称，例如**SM-Secret-Linux-DJ-*d-xxxxxxxxxx*-Read**. 查看摘要部分以查看策略授予的权限。然后选择 。创建策略以保存您的更改。新策略会显示在托管策略列表中，并且已准备好附加到身份。

   Note

   我们建议您为每个密码创建一个策略。这样做可以确保实例只能访问适当的机密，并最大限度地减少实例受到攻击时的影响。

创建 linuxEC2DOMAIN 加入角色

您可以使用 IAM 控制台创建用于域加入 Linux EC2 实例的角色。

创建 linuxEC2DomainJoin 角色

1. 登录到Amazon Web Services Management Console作为有权创建 IAM 策略的用户。然后，使用打开 IAM 控制台：https://console.aws.amazon.com/iam/.
2. 在导航窗格中，选择 Roles（角色）。
3. 在内容窗格中，选择创建角色.
4. 在 Select type of trusted entity (选择受信任实体的类型）下，选择 Amazon service (Amazon 服务)。
5. UNDER选择使用案例选择EC2选择，然后选择后续：Permissions (下一步：权限)。
6. 适用于筛选策略中，执行以下操作：
   a. 输入 **AmazonSSMManagedInstanceCore**。然后，在列表中选中该项目的复选框。
   b. 输入 **AmazonSSMDirectoryServiceAccess**。然后，在列表中选中该项目的复选框。
   c. Enter**SM-Secret-Linux-DJ-*d-xxxxxxxxxx*-Read**(或者您在上一过程中创建的策略名称)。）然后，在列表中选中该项目的复选框。

      Note

      AmazonSSMDirectoryServiceAccess 提供了将实例加入由托管的 Active Directory 的权限。Amazon Directory Service. AmazonSSMManagedInstanceCore 提供了使用Amazon Systems Manager服务。有关使用这些权限创建角色的更多信息，以及有关可分配给 IAM 角色的其他权限和策略的信息，请参阅为 Systems Manager 创建 IAM 实例配置文件中的Amazon Systems Manager用户指南.
7. 选择 Next:。标签。
8. （可选）添加一个或多个标签键/值对以组织、跟踪或控制该角色的访问。接下来，选择 Next (下一步)：审核。
9. 在旁边Role name (角色名称)中，输入新角色的名称，例如**LinuxEC2DomainJoin**或者你喜欢的另一个名字。
10. （可选）对于角色描述，请输入描述。
11. 选择 Create role（创建角色）。

无缝加入 Linux EC2 实例

现在您已经配置了所有必备任务，可以使用以下过程无缝加入 Linux EC2 实例。

无缝加入 Linux EC2 实例

1. 登录到 Amazon Web Services Management Console，然后通过以下网址打开 Amazon EC2 控制台：https://console.aws.amazon.com/ec2/。

2. 从导航栏的 Region (区域) 选择器中，选择与现有目录相同的 Region (区域)。
3. 选择 Launch Instance（启动实例）。
4. 在存储库的步骤 1在页面上，选择Select获取合适的 Amazon 系统映像 (AMI)。

   Note

   使用的 AMI 必须有Amazon Systems Manager（SSM 代理）版本 2.3.1644.0 或更高版本。要通过从该 AMI 启动实例来检查 AMI 中已安装的 SSM Agent 版本，请参阅获取当前安装的 SSM Agent 版本. 如果你需要升级 SSM 代理，请参阅在适用于 Linux 的 EC2 实例上安装和配置 SSM 代理.
5. 在存储库的步骤 2页面上，选择合适的实例类型，然后选择后续：配置实例详细信息.
6. 在存储库的步骤 3页面上，执行以下操作，然后选择：后续：Add Storage (下一步: 添加存储)：
   a. 对于 Network，选择在其中创建了您的目录的 VPC。
   b. 适用于子网在 VPC 中选择一个公有子网。选择的子网必须将所有外部流量都路由到 Internet 网关。否则将无法远程连接到实例。
   c. 对于 Auto-assign Public IP (自动分配公有 IP)，选择 Enable (启用)。有关公有 IP 地址和私有 IP 地址的更多信息，请参阅Amazon EC2 实例 IP 寻址中的Windows 实例 Amazon EC2 用户指南.
   d. 适用于域加入目录中，从列表中选择您的域。
   e. 适用于IAM 角色下，选择您之前在先决条件部分中创建的 IAM 角色步骤 2: 创建 linuxEC2Domain 加入角色.
7. 在两者上步骤 4和步骤 5页面，保留默认设置或根据需要进行更改。然后选择 。下一步在每个上调用。
8. 在存储库的步骤 6页面上，选择已配置为允许从您的网络远程访问实例的安全组。然后选择查看和启动。
9. 在存储库的步骤 7在页面上，选择启动，选择 key pair，然后选择实例启动.

   Note

   如果您使用 SUSE Linux 执行无缝域加入，则需要重新启动才能进行身份验证。要从 Linux 终端重新启动 SUSE，请键入sudo reboot.

手动加入 Linux 实例

除 Amazon EC2 Windows 实例外，您还可以将特定 Amazon EC2 Linux 实例加入您的 Simple AD 目录。支持以下 Linux 实例分发版和版本：

- Amazon Linux AMI 2018.03.0
- Amazon Linux 2（64 位 x86）
- Red Hat Enterprise Linux 8 (HVM)（64 位 x86）
- Ubuntu Server 18.04 LTS 和 Ubuntu Server 16.04 LTS
- CentOS 7 x86-64
- SUSE Linux Enterprise Server 15 SP1

Note

其他 Linux 分发版和版本可能会正常运行，但未经过测试。

将实例加入目录

在将 Amazon Linux、CentOS、红帽或 Ubuntu 实例加入您的目录之前，该实例必须按照中指定的方式启动。无缝地联接 Windows EC2 实例 (p. 66).

> **Important**
>
> 以下某些过程如果未正确执行，可能会使实例无法访问或不可用。因此，我们强烈建议在执行这些过程之前对实例创建备份或拍摄快照。

将 Linux 实例加入目录

使用以下选项卡之一对特定 Linux 实例执行步骤：

Amazon Linux

1. 使用任何 SSH 客户端连接到实例。
2. 配置 Linux 实例以使用Amazon Directory Service-提供的 DNS 服务器。可以通过在附加到 VPC 的 DHCP 选项集中进行设置，或是通过在实例上手动设置，来执行此操作。如果您要手动设置，请参阅如何为私有 Amazon EC2 实例分配静态 DNS 服务器？中的Amazon知识中心获取有关为特定 Linux 发行版和版本设置持久 DNS 服务器的指导。
3. 确保您的 Amazon Linux-64 位实例为最新状态。

```
sudo yum -y update
```

4. 在 Linux 实例上安装所需的 Amazon Linux 程序包。

   > **Note**
   >
   > 其中一些程序包可能已安装。
   > 安装程序包时，可能会遇到几个弹出配置屏幕。通常可以将这些屏幕中的字段保留为空白。

   Amazon Linux 1

   ```
   sudo yum -y install sssd realmd krb5-workstation
   ```

   Amazon Linux 2

   ```
   sudo yum -y install sssd realmd krb5-workstation samba-common-tools
   ```

   > **Note**
   >
   > 有关确定您使用的 Amazon Linux 版本的帮助，请参阅识别 Amazon Linux 映像中的适用于 Linux 实例的 Amazon EC2 用户指南.

5. 使用以下命令将实例加入目录。

   ```
   sudo realm join -U join_account@example.com example.com --verbose
   ```

   join_account@example.com

   中的账户*example.com*具有域加入权限的域。在出现提示时输入账户的密码。有关委托这些权限的更多信息，请参阅为委派目录加入权限Amazon管理 Microsoft AD (p. 90)。

   example.com

   目录的完全限定 DNS 名称。

   ```
   ...
    * Successfully enrolled machine in realm
   ```

6. 设置 SSH 服务以允许进行密码身份验证。

a. 在文本编辑器中打开 `/etc/ssh/sshd_config` 文件。

```
sudo vi /etc/ssh/sshd_config
```

b. 将 `PasswordAuthentication` 设置为 `yes`。

```
PasswordAuthentication yes
```

c. 重新启动 SSH 服务。

```
sudo systemctl restart sshd.service
```

或者：

```
sudo service sshd restart
```

7. 重新启动实例之后，使用任何 SSH 客户端连接到它，然后通过执行以下步骤将域管理员组添加到 sudoers 列表：

   a. 使用以下命令打开 `sudoers` 文件：

```
sudo visudo
```

   b. 将以下内容添加到`sudoers`文件然后保存它。

```
## Add the "Domain Admins" group from the example.com domain.
%Domain\ Admins@example.com ALL=(ALL:ALL) ALL
```

   (以上示例使用 “\<space>” 形成 Linux 空格字符。)

CentOS

1. 使用任何 SSH 客户端连接到实例。
2. 配置 Linux 实例以使用Amazon Directory Service-提供的 DNS 服务器。可以通过在附加到 VPC 的 DHCP 选项集中进行设置，或是通过在实例上手动设置，来执行此操作。如果您要手动设置，请参阅如何为私有 Amazon EC2 实例分配静态 DNS 服务器？中的Amazon知识中心获取有关为特定 Linux 发行版和版本设置持久 DNS 服务器的指导。
3. 确保您的 CentOS 7 实例为最新状态。

```
sudo yum -y update
```

4. 在 Linux 实例上安装所需的 CentOS 7 程序包。

   Note

   其中一些程序包可能已安装。
   安装程序包时，可能会遇到几个弹出配置屏幕。通常可以将这些屏幕中的字段保留为空白。

```
sudo yum -y install sssd realmd krb5-workstation samba-common-tools
```

5. 使用以下命令将实例加入目录。

```
sudo realm join -U join_account@example.com example.com --verbose
```

join_account@example.com

中的账户*example.com*具有域加入权限的域。在出现提示时输入账户的密码。有关委托这些权限的更多信息，请参阅为委派目录加入权限Amazon管理 Microsoft AD (p. 90)。

example.com

目录的完全限定 DNS 名称。

```
...
 * Successfully enrolled machine in realm
```

6. 设置 SSH 服务以允许进行密码身份验证。
   a. 在文本编辑器中打开 `/etc/ssh/sshd_config` 文件。

   ```
   sudo vi /etc/ssh/sshd_config
   ```

   b. 将 `PasswordAuthentication` 设置为 `yes`。

   ```
   PasswordAuthentication yes
   ```

   c. 重新启动 SSH 服务。

   ```
   sudo systemctl restart sshd.service
   ```

   或者：

   ```
   sudo service sshd restart
   ```

7. 重新启动实例之后，使用任何 SSH 客户端连接到它，然后通过执行以下步骤将域管理员组添加到 sudoers 列表：
   a. 使用以下命令打开 `sudoers` 文件：

   ```
   sudo visudo
   ```

   b. 将以下内容添加到`sudoers`文件然后保存它。

   ```
   ## Add the "Domain Admins" group from the example.com domain.
   %Domain\ Admins@example.com ALL=(ALL:ALL) ALL
   ```

   (以上示例使用 “\<space>” 形成 Linux 空格字符。)

Red hat

1. 使用任何 SSH 客户端连接到实例。
2. 配置 Linux 实例以使用Amazon Directory Service-提供的 DNS 服务器。可以通过在附加到 VPC 的 DHCP 选项集中进行设置，或是通过在实例上手动设置，来执行此操作。如果您要手动设置，请参阅如何为私有 Amazon EC2 实例分配静态 DNS 服务器？中的Amazon知识中心获取有关为特定 Linux 发行版和版本设置持久 DNS 服务器的指导。
3. 确保 Red Hat - 64 位实例为最新状态。

```
sudo yum -y update
```

4. 在 Linux 实例上安装所需的 Red Hat 程序包。

   Note

   其中一些程序包可能已安装。
   安装程序包时，可能会遇到几个弹出配置屏幕。通常可以将这些屏幕中的字段保留为空白。

```
sudo yum -y install sssd realmd krb5-workstation samba-common-tools
```

5. 使用以下命令将实例加入目录。

```
sudo realm join -v -U join_account example.com --install=/
```

   join_account

   这些区域有：sAMAccountName对于中的账户*example.com*具有域加入权限的域。在出现提示时输入账户的密码。有关委托这些权限的更多信息，请参阅为委派目录加入权限Amazon管理Microsoft AD (p. 90)。

   example.com

   目录的完全限定 DNS 名称。

```
...
 * Successfully enrolled machine in realm
```

6. 设置 SSH 服务以允许进行密码身份验证。

   a. 在文本编辑器中打开 `/etc/ssh/sshd_config` 文件。

```
sudo vi /etc/ssh/sshd_config
```

   b. 将 `PasswordAuthentication` 设置为 `yes`。

```
PasswordAuthentication yes
```

   c. 重新启动 SSH 服务。

```
sudo systemctl restart sshd.service
```

   或者：

```
sudo service sshd restart
```

7. 重新启动实例之后，使用任何 SSH 客户端连接到它，然后通过执行以下步骤将域管理员组添加到 sudoers 列表：

   a. 使用以下命令打开 `sudoers` 文件：

```
sudo visudo
```

   b. 将以下内容添加到`sudoers`文件然后保存它。

```
## Add the "Domain Admins" group from the example.com domain.
%Domain\ Admins@example.com ALL=(ALL:ALL) ALL
```

   (以上示例使用 “\<space>” 形成 Linux 空格字符。)

Ubuntu

1. 使用任何 SSH 客户端连接到实例。
2. 配置 Linux 实例以使用Amazon Directory Service-提供的 DNS 服务器。可以通过在附加到 VPC 的 DHCP 选项集中进行设置，或是通过在实例上手动设置，来执行此操作。如果您要手动设置，请参阅如何为私有 Amazon EC2 实例分配静态 DNS 服务器？中的Amazon知识中心获取有关为特定 Linux 发行版和版本设置持久 DNS 服务器的指导。
3. 确保您的 Ubuntu - 64 位实例为最新状态。

```
sudo apt-get update
sudo apt-get -y upgrade
```

4. 在 Linux 实例上安装所需的 Ubuntu 程序包。

   Note

   其中一些程序包可能已安装。
   安装程序包时，可能会遇到几个弹出配置屏幕。通常可以将这些屏幕中的字段保留为空白。

```
sudo apt-get -y install sssd realmd krb5-user samba-common packagekit adcli
```

5. 禁用反向 DNS 解析，并将默认领域设置为您的域的 FQDN。Ubuntu 实例在 DNS 中必须 可以反向解析，领域才能使用。否则，您必须在 /etc/krb5.conf 中禁用 DNS，如下所示：

```
sudo vi /etc/krb5.conf
```

```
[libdefaults]
default_realm = EXAMPLE.COM
rdns = false
```

6. 使用以下命令将实例加入目录。

```
sudo realm join -U join_account example.com --verbose
```

   join_account@example.com

   这些区域有：sAMAccountName对于中的账户*example.com*具有域加入权限的域。在出现提示时输入账户的密码。有关委托这些权限的更多信息，请参阅为委派目录加入权限Amazon管理Microsoft AD (p. 90)。

   example.com

   目录的完全限定 DNS 名称。

```
...
 * Successfully enrolled machine in realm
```

7. 设置 SSH 服务以允许进行密码身份验证。
   a. 在文本编辑器中打开 `/etc/ssh/sshd_config` 文件。

```
sudo vi /etc/ssh/sshd_config
```

   b. 将 `PasswordAuthentication` 设置为 `yes`。

```
PasswordAuthentication yes
```

c. 重新启动 SSH 服务。

```
sudo systemctl restart sshd.service
```

或者：

```
sudo service sshd restart
```

8. 重新启动实例之后，使用任何 SSH 客户端连接到它，然后通过执行以下步骤将域管理员组添加到 sudoers 列表：

   a. 使用以下命令打开 sudoers 文件：

```
sudo visudo
```

   b. 将以下内容添加到sudoers文件然后保存它。

```
## Add the "Domain Admins" group from the example.com domain.
%Domain\ Admins@example.com ALL=(ALL:ALL) ALL
```

   (以上示例使用 “\<space>” 形成 Linux 空格字符。)

Note

使用 Simple AD 时，如果在 Linux 实例上创建用户账户时使用了 “强制用户在首次登录时更改密码” 选项，则该用户无法使用首次更改其密码。kpasswd. 要首次更改密码，域管理员必须使用 Active Directory 管理工具更新用户密码。

通过 Linux 实例管理账户

要通过 Linux 实例管理 Simple AD 中的账户，您必须更新您的 Linux 实例上的特定配置文件，如下所示：

1. Setkrb5_use_kdcinfo到False中的/etc/sssd/sssd.conf文件。例如：

```
[domain/example.com]
    krb5_use_kdcinfo = False
```

2. 需要重启 sssd 服务配置才能生效：

```
$ sudo systemctl restart sssd.service
```

或者，您也可以使用：

```
$ sudo service sssd start
```

3. 如果您将通过 CentOS Linux 实例管理用户，还必须编辑文件 /etc/smb.conf 以包括：

```
[global]
  workgroup = EXAMPLE.COM
  realm = EXAMPLE.COM
  netbios name = EXAMPLE
  security = ads
```

限制账户登录访问

因为所有账户都是在 Active Directory 中定义的，因此默认情况下，目录中的所有用户都可以登录该实例。可以在 sssd.conf 中使用 ad_access_filter 来仅允许特定用户登录到实例。例如：

```
ad_access_filter = (memberOf=cn=admins,ou=Testou,dc=example,dc=com)
```

memberOf

指示仅当用户是特定组的成员时，才允许他们访问实例。

cn

应具有访问权限的组的通用名称。在此示例中，组名称是 *admins*。

ou

这是上面的组所在的组织单位。在此示例中，OU 是 *Testou*。

dc

这是您的域的域组成部分。在此示例中是 *example*。

dc

这是附加域组成部分。在此示例中是 *com*。

您必须手动将 ad_access_filter 添加到 /etc/sssd/sssd.conf。

在文本编辑器中打开 /etc/sssd/sssd.conf 文件。

```
sudo vi /etc/sssd/sssd.conf
```

执行此操作之后，sssd.conf 可能类似于下面这样：

```
[sssd]
domains = example.com
config_file_version = 2
services = nss, pam

[domain/example.com]
ad_domain = example.com
krb5_realm = EXAMPLE.COM
realmd_tags = manages-system joined-with-samba
cache_credentials = True
id_provider = ad
krb5_store_password_if_offline = True
default_shell = /bin/bash
ldap_id_mapping = True
use_fully_qualified_names = True
fallback_homedir = /home/%u@%d
access_provider = ad
ad_access_filter = (memberOf=cn=admins,ou=Testou,dc=example,dc=com)
```

为了使配置生效，您需要重启 sssd 服务：

```
sudo systemctl restart sssd.service
```

或者，您也可以使用：

```
sudo service sssd restart
```

Connect 到实例

当用户使用 SSH 客户端连接到实例时，系统会提示他们输入自己的用户名。用户可以在以下任一内容中输入用户名：`username@example.com`要么`EXAMPLE\username`格式的日期和时间。响应将类似于以下内容，具体取决于您使用的 Linux 发行版：

Amazon Linux、Red Hat Enterprise Linux 和 CentOS Linux

```
login as: johndoe@example.com
johndoe@example.com's password:
Last login: Thu Jun 25 16:26:28 2015 from XX.XX.XX.XX
```

SUSE Linux

```
SUSE Linux Enterprise Server 15 SP1 x86_64 (64-bit)

As "root" (sudo or sudo -i) use the:
  - zypper command for package management
  - yast command for configuration management

Management and Config: https://www.suse.com/suse-in-the-cloud-basics
Documentation: https://www.suse.com/documentation/sles-15/
Forum: https://forums.suse.com/forumdisplay.php?93-SUSE-Public-Cloud

Have a lot of fun...
```

Ubuntu Linux

```
login as: admin@example.com
admin@example.com@10.24.34.0's password:
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-1057-aws x86_64)

* Documentation:  https://help.ubuntu.com
* Management:     https://landscape.canonical.com
* Support:        https://ubuntu.com/advantage

  System information as of Sat Apr 18 22:03:35 UTC 2020

  System load:  0.01               Processes:           102
  Usage of /:   18.6% of 7.69GB    Users logged in:     2
  Memory usage: 16%                IP address for eth0: 10.24.34.1
  Swap usage:   0%
```

委派 Simple AD 的目录加入权限

要将计算机加入到目录，需要有权将计算机加入到目录的账户。

使用 Simple AD，成员Domain Admins组拥有足够权限将计算机加入到目录。

但是根据最佳实践，应使用只拥有所需的最小权限的账户。以下过程演示如何创建名为 `Joiners` 的新组，并向此组委派将计算机加入到目录所需的权限。

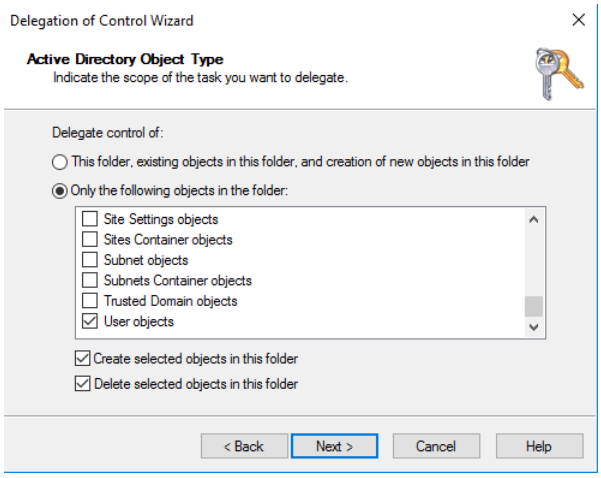
您必须在已加入到目录且具有Active Directory 用户和计算机已安装 MMC 管理单元。您还必须以域管理员身份登录。

委派 Simple AD 的加入权限

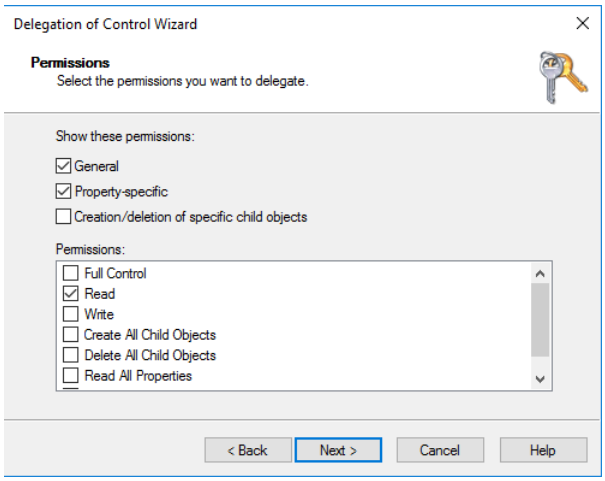
1. 打开 Active Directory User and Computers 并在导航树中选择您的域根。
2. 在左侧的导航树中，打开 Users 的上下文菜单 (右键单击)，选择 New，然后选择 Group。
3. 在 New Object - Group 框中，键入以下内容，然后选择 OK。

- 对于 Group name (组名称)，键入 **`Joiners`**。
- 对于 Group scope，选择 Global。
- 对于 Group type，选择 Security。

4. 在导航树中，选择您的域根。从 Action 菜单中选择 Delegate Control。
5. 在 Delegation of Control Wizard 页面上，选择 Next，然后选择 Add。
6. 在 Select Users, Computers, or Groups 框中，键入 `Joiners`，然后选择 OK。如果找到多个对象，请选择上面创建的 `Joiners` 组。选择 Next (下一步)。
7. 在 Tasks to Delegate 页面上，选择 Create a custom task to delegate，然后选择 Next。
8. 选择 Only the following objects in the folder，然后选择 Computer objects。
9. 选择 Create selected objects in this folder，然后选择 Delete selected objects in this folder。然后选择下一步。



10. 选择 Read 和 Write，然后选择 Next。



11. 在 Completing the Delegation of Control Wizard 页面上验证信息，然后选择 Finish。
12. 使用强密码创建一个用户，并将该用户添加到 `Joiners` 组。该用户随后拥有足够的权限将 Amazon Directory Service 连接到目录。

创建 DHCP 选项集

Amazon我们建议为Amazon Directory Service目录并将 DHCP 选项集分配给目录所在的 VPC。这使该 VPC 中的任何实例都可以指向指定域和 DNS 服务器以解析其域名。

有关 DHCP 选项集的更多信息，请参阅。DHCP 选项集中的Amazon VPC User Guide.

为目录创建 DHCP 选项集

1. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 DHCP Options Sets，然后选择 Create DHCP options set。
3. 在存储库的创建 DHCP 选项集页面上，为目录输入以下值：

   名称

   选项集的可选标签。

   域名

   目录的完全限定名称，例如`corp.example.com`.

   域名服务器

   你的 IP 地址Amazon-提供目录的 DNS 服务器。

   Note

   可以转到以下网址：Amazon Directory Service控制台导航窗格，选择目录然后选择正确的目录 ID。

   NTP 服务器

   将此字段留空。

   NetBIOS 名称服务器

   将此字段留空。

   NetBIOS 节点类型

   将此字段留空。
4. 选择创建 DHCP 选项集。新的 DHCP 选项集会出现在您的 DHCP 选项列表中。
5. 记录新增 DHCP 选项集的 ID (dopt-xxxxxxxx)。您可以使用它将新选项集与 VPC 相关联。

更改与 VPC 相关联的 DHCP 选项集。

在您创建 DHCP 选项集之后，您便无法再修改这些选项。如果您希望 VPC 使用不同的 DHCP 选项集，您必须创建新的选项集，并将其与您的 VPC 相关联。您还可以设置 VPC，让其不使用任何 DHCP 选项。

1. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择您的 VPC
3. 选择 VPC，然后选择：操作、编辑 DHCP 选项集.
4. 适用于DHCP 选项集，选择一个选项集或选择无 DHCP 选项集选择，然后选择Save（保存）.

维护您的 Simple AD 目录

此节介绍如何为您的 Simple AD 环境维护常见管理任务。

主题

- 删除目录 (p. 235)
- 快照或恢复你的目录 (p. 235)
- 查看目录信息 (p. 237)

删除目录

当Simple AD 或AmazonDirectory Service，所有目录时，所有目录数据和快照都会删除，所有目录数据和快照都会删除，并且无法恢复。删除目录之后，加入到目录的所有实例都保持不变。但是，不能使用目录凭证登录这些实例。需要使用实例的本地用户账户登录这些实例。

删除 AAD Connector 目录时，本地目录保持不变。加入到目录的所有实例也保持不变，并保持加入本地目录。仍可以使用目录凭证登录这些实例。

要删除目录

1. 在Amazon Directory Service控制台导航窗格，选择目录.
2. 确保没有Amazon应用程序已为您想要删除的目录。
   a. 在 Directories 页面上，选择您的目录 ID。
   b. 在 Directory details (目录详细信息) 页面上，选择 Application management (应用程序管理) 选项卡。在Amazon应用程序和服务部分，你可以看到哪个Amazon已为目录启用。
      - 禁用 WorkSpaces，则必须从目录中取消注册服务 WorkSpaces 控制台。有关更多信息，请参阅 。从目录中取消注册中的亚马逊 WorkSpaces 管理指南.
      - 要禁用亚马逊 WorkSpaces 应用程序管理器，您必须在 Amazon WAM 控制台中删除所有应用程序分配。有关更多信息，请参阅 。移除所有应用程序分配中的Amazon WAM 管理指南.
      - 要禁用亚马逊 WorkDocs，您必须删除Amazon WorkDocs 亚马逊的站点 WorkDocs控制台。有关更多信息，请参阅 。删除站点中的亚马逊 WorkDocs 管理指南.
      - 要禁用亚马逊 WorkMail，您必须移除亚马逊 WorkMail 亚马逊的组织 WorkMail 控制台。有关更多信息，请参阅 。删除组织中的亚马逊 WorkMail 管理员指南.
      - 禁用Amazon Web Services Management Console访问。
      - 要禁用 Amazon Relational Database Service，必须从域中删除 Amazon RDS 实例。有关更多信息，请参阅 。在域中管理数据库实例中的Amazon RDS 用户指南.
      - 要禁用亚马逊 QuickSight，您必须从Amazon 取消订阅 QuickSight. 有关更多信息，请参阅 。关闭Amazon QuickSight 帐户中的亚马逊 QuickSight 用户指南.
      - 要禁用 Amazon Connect，您必须删除Amazon Connect 实例。有关更多信息，请参阅 。删除AAmazon Connect 实例中的Amazon Connect 管理指南.
      - 要禁用 FSx for Windows For Windows For Windows For Windows File Sx for Windows File Sx for Windows For Windows 有关更多信息，请参阅 。在 For Windows For Windows For WindowFSx for Windows File Server中的Amazon For Windows For Windows For Windows File.

        Note

        如果您将Amazon IAM Identity Center (successor to Amazon Single Sign-On)并且之前已将其连接到Amazon您计划删除的托管 Microsofor 删除它，然后才能删除它。有关更多信息，请参阅 。更改您的身份来源中的IAM 身份中心用户指南.
3. 在导航窗格中，选择 Directories。
4. 仅选择要删除的目录，然后单击Delete. 删除目录需要几分钟时间。目录删除之后，它会从目录列表中删除。

快照或恢复你的目录

Amazon Directory Service让您能让您拍摄数据 Simple AD 目录的手动快照。这些快照可以用于为目录执行时间点还原。无法拍摄 AD Connector 目录的快照。

主题

- 创建目录的快照 (p. 236)

- 从快照还原目录 (p. 236)
- 删除快照 (p. 236)

创建目录的快照

快照可以用于将目录还原到拍摄快照的时间点时的状态。要创建目录的手动快照，请执行以下步骤。

> **Note**
>
> 对于每个目录，限制为 5 个手动快照。如果已达到此限制，必须先删除一个现有手动快照才能创建另一个快照。

创建手动快照

1. 在Amazon Directory Service控制台导航窗格中，选择。目录.
2. 在 Directories 页面上，选择您的目录 ID。
3. 在目录详细信息页面上，选择维护选项卡。
4. 在快照部分，选择操作选择，然后选择。创建快照.
5. 在创建目录快照对话框中，提供快照的名称（如果需要）。准备好之后，选择。Create.

根据目录的大小，可能需要几分钟时间来创建快照。快照准备就绪之后，Status 值更改为 `Completed`。

从快照还原目录

从快照还原目录等效于将目录移动回到以前的时间。目录快照对于创建它们的目录来说是唯一的。快照只能恢复到创建快照的目录中。此外，手动快照支持的最长期限为 180 天。有关更多信息，请参阅 Microsoft 网站上的 Active Directory 的系统状态备份的有用保质期。

> **Warning**
>
> 建议您联系Amazon Web Services SupportCenter在任何快照还原之前；我们或许能够帮助您避免执行快照还原的需要。任何快照还原都会导致数据丢失，因为它们是一些时间点。必须了解与目录关联的所有 DC 和 DNS 服务器会处于离线状态，直到还原操作完成。

要从快照还原目录，请执行以下步骤。

从快照还原目录

1. 在Amazon Directory Service控制台导航窗格中，选择。目录.
2. 在 Directories 页面上，选择您的目录 ID。
3. 在目录详细信息页面上，选择维护选项卡。
4. 在快照部分中，在列表中选择快照，然后选择操作选择，然后选择。还原快照.
5. 查看中的信息。还原目录快照对话框，然后选择。还原.

对于 Simple AD 目录，可能需要几分钟时间来还原目录。还原成功后，状态目录的值更改为`Active`. 会覆盖快照日期之后对目录进行的任何更改。

删除快照

如何删除快照

1. 在Amazon Directory Service控制台导航窗格中，选择。目录.

2. 在 Directories 页面上，选择您的目录 ID。
3. 在目录详细信息页面上，选择维护选项卡。
4. 在快照部分，选择操作选择，然后选择。删除快照.
5. 确认您要删除快照，然后选择。Delete.

查看目录信息

您可以查看有关目录的详细信息。

查看详细目录信息

1. 在Amazon Directory Service控制台选择导航窗格，选择目录.
2. 单击目录的目录 ID 链接。有关目录的信息显示在目录详细信息页.

有关 Status 字段的更多信息，请参阅了解您的目录状态 (p. 48)。

启用访问权限Amazon应用程序和服务

Amazon Directory Service可以给其他Amazon可以将应用程序和服务 (如 Amazon WorkSpaces) 访问权限授予目录用户。以下Amazon可以启用或禁用应用程序和服务以使用Amazon Directory Service.

Amazon应用程序/服务	更多信息...
Amazon Chime	有关更多信息，请参阅 。Amazon Chime 管理指南.
Amazon Connect	有关更多信息，请参阅 。Amazon Connect 管理指南.
FSx for Windows File Server	有关更多信息，请参阅 。将 Amazon FSxAmazonMicrosoft Directory Service Directory中的FSx for Windows File Server.
Amazon QuickSight	有关更多信息，请参阅Amazon QuickSight 用户指南。
Amazon Relational Database Service	有关更多信息，请参阅 Amazon RDS 用户指南。
Amazon Transfer Family	有关更多信息，请参阅 Amazon Transfer Family 用户指南。
Amazon WorkDocs	有关更多信息，请参阅 。Amazon WorkDocs 管理指南.
Amazon WorkMail	有关更多信息，请参阅 。Amazon WorkMail 管理员指南.
WorkSpaces	你可以创建一个 Simple AD，Amazon直接从 WorkSpaces 托管微软 AD 或 AD Connector。只需在创建工作区时启动 Advanced Setup。 有关更多信息，请参阅 。Amazon WorkSpaces 管理指南.
Amazon WorkSpaces Application Manager	有关更多信息，请参阅 。Amazon WAM 管理指南.

Amazon应用程序/服务	更多信息...
Amazon Web Services Management Console	有关更多信息，请参阅 允许访问Amazon Web Services Management Console使用 AD 凭据 (p. 130)。

启用之后，可在要向其授予目录访问权限的应用程序或服务的控制台中管理对目录的访问。要查找Amazon上述应用程序和服务链接Amazon Directory Service请执行以下步骤。

显示适用于目录的应用程序和服务

1. 在 Amazon Directory Service 控制台导航窗格中，选择 Directories (目录)。
2. 在 Directories 页面上，选择您的目录 ID。
3. 在 Directory details (目录详细信息) 页面上，选择 Application management (应用程序管理) 选项卡。
4. 查看Amazon应用程序和服务部分。

主题

- 创建访问 URL (p. 238)
- 单点登录 (p. 238)

创建访问 URL

访问 URL 用于Amazon应用程序和服务 (如 Amazon WorkDocs)，以访问与目录关联的登录页面。此 URL 必须全局唯一。可以通过执行以下步骤为目录创建访问 URL。

> **Warning**
>
> 一旦为此目录创建应用程序访问 URL，就无法更改它。创建访问 URL 之后，其他人便无法使用它。如果删除目录，则访问 URL 也会删除，随后可以由任何其他账户所使用。

创建访问 URL

1. 在Amazon Directory Service控制台导航窗格中，选择目录.
2. 在 Directories 页面上，选择您的目录 ID。
3. 在 Directory details (目录详细信息) 页面上，选择 Application management (应用程序管理) 选项卡。
4. 在 Application access URL (应用程序访问 URL) 部分中，如果尚未向目录分配访问 URL，则会显示 Create (创建) 按钮。输入目录别名，然后选择 Create (创建)。如果实体已存在返回错误，则指定目录别名已分配。选择另一个别名并重复此过程。

   您的访问 URL 将以格式显示`<alias>`.awsapps.com。

单点登录

Amazon Directory Service提供允许您的用户访问亚马逊的能力 WorkDocs 从已加入目录的计算机中，而无需单独输入其凭证。

启用单点登录之前，您需要执行其他步骤，以便使用户的 Web 浏览器可以支持单点登录。用户可能需要修改其 Web 浏览器设置来启用单点登录。

> **Note**
>
> 只有在已加入到 Amazon Directory Service 目录中的计算机上才支持单点登录。未加入目录中的计算机上无法使用单点登录。

如果您的目录是 AD Connector 目录，且 AD Connector 服务账户没有权限添加或删除其服务委托人名称属性，则对于下面的步骤 5 和 6，您有两个选项：

1. 您可以继续操作，系统将提示您输入具有以下权限的目录用户的用户名和密码：可在 AD Connector tor 服务账户上添加或删除服务委托人名称属性。这些凭证仅用于启用单点登录，不由服务进行存储。不会更改 AD Connector 服务账户权限。
2. 您可以委派权限以允许 AD Connector 服务账户在自身上添加或删除服务委托人名称属性，您可以运行以下 PowerShell 从加入域的计算机使用某个账户（该账户有权修改 AD Connector 服务账户的权限）从加入域的计算机发出命令。以下命令将使 AD Connector 服务账户能够仅为其自身添加和删除服务委托人名称属性。

```
$AccountName = 'ConnectorAccountName'
# DO NOT modify anything below this comment.
# Getting Active Directory information.
Import-Module 'ActiveDirectory'
$RootDse = Get-ADRootDSE
[System.GUID]$ServicePrincipalNameGuid = (Get-ADObject -SearchBase
 $RootDse.SchemaNamingContext -Filter { lDAPDisplayName -eq 'servicePrincipalName' } -
Properties 'schemaIDGUID').schemaIDGUID
# Getting AD Connector service account Information.
$AccountProperties = Get-ADUser -Identity $AccountName
$AclPath = $AccountProperties.DistinguishedName
$AccountSid = New-Object -TypeName 'System.Security.Principal.SecurityIdentifier'
 $AccountProperties.SID.Value
# Getting ACL settings for AD Connector service account.
$ObjectAcl = Get-ACL -Path "AD:\$AclPath"
# Setting ACL allowing the AD Connector service account the ability to add and remove a
 Service Principal Name (SPN) to itself
$AddAccessRule = New-Object -TypeName 'System.DirectoryServices.ActiveDirectoryAccessRule'
 $AccountSid, 'WriteProperty', 'Allow', $ServicePrincipalNameGUID, 'None'
$ObjectAcl.AddAccessRule($AddAccessRule)
Set-ACL -AclObject $ObjectAcl -Path "AD:\$AclPath"
```

使用亚马逊启用或禁用单点登录 WorkDocs

1. 在Amazon Directory Service控制台导航窗格中，选择。目录.
2. 在 Directories 页面上，选择您的目录 ID。
3. 在 Directory details (目录详细信息) 页面上，选择 Application management (应用程序管理) 选项卡。
4. 在应用程序访问 URL部分，选择。启用为亚马逊启用单点登录 WorkDocs.

   如果您没有看到启用按钮，则可能需要首先创建访问 URL，然后才能显示此选项。有关如何创建访问 URL 的更多信息，请参阅创建访问 URL (p. 125)。
5. 在为此目录启用单点登录对话框中，选择。启用. 单点登录已为目录启用。
6. 如果您以后想禁用亚马逊的单点登录 WorkDocs，选择禁用，然后在禁用此目录的单点登录对话框中，选择。禁用。

主题

- IE 和 Chrome 的单点登录 (p. 126)
- Firex 的单点登录 (p. 129)

IE 和 Chrome 的单点登录

要使 Microsoft Internet Explorer (IE) 和 Google Chrome 浏览器可以支持单点登录，必须在客户端计算机上执行以下任务：

- 添加您的访问网址（例如 https://<alias>.awsapps.com) 添加到适用于单点登录的经审批站点列表中。
- 启用活动脚本 (JavaScript)。
- 允许自动登录。
- 启用集成身份验证。

您或您的用户手动执行这些任务，也可以使用组策略设置更改这些设置。

主题

- Windows 上的单点登录的手动更新 (p. 127)
- OS X 上的单点登录的手动更新 (p. 127)
- Single Sign-On 的组策略设置 (p. 128)

Windows 上的单点登录的手动更新

要在 Windows 计算机上手动启用单点登录，请在客户端计算机上执行以下步骤。其中一些设置可能已正确设置。

在 Windows 上为 Internet Explorer 和 Chrome 手动启用单点登录

1. 要打开 Internet Properties 对话框，请选择 Start 菜单，在搜索框中键入 `Internet Options`，然后选择 Internet Options。
2. 通过执行以下步骤将访问 URL 添加到适用于单点登录的经审批站点列表中：
   a. 在 Internet Properties 对话框中选择 Security 选项卡。
   b. 选择 Local intranet，然后选择 Sites。
   c. 在 Local intranet 对话框中，选择 Advanced。
   d. 将访问 URL 添加到网站列表，然后选择 Close。
   e. 在 Local intranet 对话框中，选择 OK。
3. 要启用活动脚本，请执行以下步骤：
   a. 在 Internet Properties 对话框的 Security 选项卡中，选择 Custom level。
   b. 在 Security Settings - Local Intranet Zone 对话框中，向下滚动到 Scripting，然后在 Active scripting 下选择 Enable。
   c. 在 Security Settings - Local Intranet Zone 对话框中，选择 OK。
4. 要启用自动登录，请执行以下步骤：
   a. 在 Internet Properties 对话框的 Security 选项卡中，选择 Custom level。
   b. 在 Security Settings - Local Intranet Zone 对话框中，向下滚动到 User Authentication 并在 Logon 下选择 Automatic logon only in Intranet zone。
   c. 在 Security Settings - Local Intranet Zone 对话框中，选择 OK。
   d. 在 Security Settings - Local Intranet Zone 对话框中，选择 OK。
5. 要启用集成身份验证，请执行以下步骤：
   a. 在 Internet Properties 对话框中选择 Advanced 选项卡。
   b. 向下滚动到 Security，然后选择 Enable Integrated Windows Authentication。
   c. 在 Internet Properties 对话框中，选择 OK。
6. 关闭并重新打开浏览器让这些更改生效。

OS X 上的单点登录的手动更新

要在 OS X 上为 Chrome 手动启用单点登录，请在客户端计算机上执行以下步骤。需要计算机上的管理员权限才能完成这些步骤。

在 OS X 上为 Chrome 手动启用单点登录

1. 将访问 URL 添加到AuthServerWhitelist通过运行以下命令执行策略：

```
defaults write com.google.Chrome AuthServerWhitelist "https://<alias>.awsapps.com"
```

2. 打开 System Preferences，转到 Profiles 面板，然后删除 `Chrome Kerberos Configuration` 配置文件。
3. 重新启动 Chrome，然后在 Chrome 中打开 chrome://policy 以确认新设置已实施。

Single Sign-On 的组策略设置

域管理员可以实施组策略设置以在加入域的客户端计算机上进行单点登录更改。

> **Note**
>
> 如果您在域中的计算机上使用 Chrome 策略管理 Chrome Web 浏览器，则必须将访问 URL 添加到AuthServerWhitelist政策。有关设置 Chrome 策略的更多信息，请转到 Policy Settings in Chrome。

使用组策略设置为 Internet Explorer 和 Chrome 启用单点登录

1. 通过执行以下步骤创建新的组策略对象：
   a. 打开组策略管理工具，导航到您的域并选择 Group Policy Objects。
   b. 在主菜单中，选择 Action，然后选择 New。
   c. 在新 GPO对话框中，输入组策略对象的描述性名称，例如`IAM Identity Center Policy`，然后离开来源 Starrer GPO设置为(无). 单击 OK（确定）。
2. 通过执行以下步骤将访问 URL 添加到适用于单点登录的经审批站点列表中：
   a. 在组策略管理工具中，导航到您的域，选择。组策略对象，打开IAM Identity Centare 策略的上下文（右键单击）菜单，然后选择。编辑.
   b. 在策略树中，导航到 User Configuration > Preferences > Windows Settings。
   c. 在 Windows Settings 列表中，打开 Registry 的上下文 (右键单击) 菜单并选择 New registry item。
   d. 在 New Registry Properties 对话框中，输入以下设置，然后选择 OK：

      Action

      `Update`

      Hive

      `HKEY_CURRENT_USER`

      路径

      `Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Domains\awsapps.com\<alias>`

      的值`<alias>`派生自访问 URL。如果访问 URL 是 `https://examplecorp.awsapps.com`，则别名是 `examplecorp`，注册表项是 `Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\Domains\awsapps.com\examplecorp`。

Value name

```
https
```

值类型

```
REG_DWORD
```

Value data

```
1
```

3. 要启用活动脚本，请执行以下步骤：
   a. 在组策略管理工具中，导航到您的域，选择。组策略对象，打开IAM Identity Centare 策略的上下文（右键单击）菜单，然后选择。编辑.
   b. 在策略树中，导航到 Computer Configuration > Policies > Administrative Templates > Windows Components > Internet Explorer > Internet Control Panel > Security Page > Intranet Zone。
   c. 在 Intranet Zone 列表中，打开 Allow active scripting 的上下文 (右键单击) 菜单，选择 Edit。
   d. 在 Allow active scripting 对话框中，输入以下设置，然后选择 OK：
      - 选择 Enabled 单选按钮。
      - 在 Options 下，将 Allow active scripting 设置为 Enable。
4. 要启用自动登录，请执行以下步骤：
   a. 在组策略管理工具中，导航到您的域，选择“Group Policy Objects”，打开 SSO 策略的上下文 (右键单击) 菜单，然后选择 Edit。
   b. 在策略树中，导航到 Computer Configuration > Policies > Administrative Templates > Windows Components > Internet Explorer > Internet Control Panel > Security Page > Intranet Zone。
   c. 在 Intranet Zone 列表中，打开 Logon options 的上下文 (右键单击) 菜单，选择 Edit。
   d. 在 Logon options 对话框中，输入以下设置，然后选择 OK：
      - 选择 Enabled 单选按钮。
      - 在 Options 下，将 Logon options 设置为 Automatic logon only in Intranet zone。
5. 要启用集成身份验证，请执行以下步骤：
   a. 在组策略管理工具中，导航到您的域，选择。组策略对象，打开IAM Identity Centare 策略的上下文（右键单击）菜单，然后选择。编辑.
   b. 在策略树中，导航到 User Configuration > Preferences > Windows Settings。
   c. 在 Windows Settings 列表中，打开 Registry 的上下文 (右键单击) 菜单并选择 New registry item。
   d. 在 New Registry Properties 对话框中，输入以下设置，然后选择 OK：

      Action

      ```
      Update
      ```

      Hive

      ```
      HKEY_CURRENT_USER
      ```

      路径

      ```
      Software\Microsoft\Windows\CurrentVersion\Internet Settings
      ```

      Value name

      ```
      EnableNegotiate
      ```

      值类型

      ```
      REG_DWORD
      ```

Value data

1

6. 如果 Group Policy Management Editor 窗口仍打开，关闭该窗口。
7. 通过执行以下步骤将新策略分配给您的域：
   a. 在组策略管理树中，打开您的域的上下文 (右键单击) 菜单，然后选择 Link an Existing GPO。
   b. 在组策略对象列表中，选择 IAM Identy Centare 策略，然后选择。确定.

这些更改会在客户端上的下一次策略更新之后，或是在下次用户登录时生效。

Firex 的单点登录

要使 Mozilla Firex 浏览器可以支持单点登录，请添加访问 URL (例如 https://`<alias>`.awsapps.com) 添加到适用于单点登录的经审批站点列表中。这可以手动执行，也可以使用脚本自动进行。

主题

- Single Sign-On 的手动更新 (p. 130)
- 单点登录的自动更新 (p. 130)

Single Sign-On 的手动更新

要在 Firefox 中将访问 URL 手动添加到经审批站点列表中，请在客户端计算机上执行以下步骤。

在 Firefox 中将访问 URL 手动添加到经审批站点列表中

1. 打开 Firefox，然后打开 `about:config` 页面。
2. 打开`network.negotiate-auth.trusted-uris`首选项，然后将访问 URL 添加到站点列表中。使用逗号 (,) 分隔多个条目。

单点登录的自动更新

作为域管理员，可以使用脚本将访问 URL 添加到 Firex。`network.negotiate-auth.trusted-uris`网络中所有计算机上的用户首选项。有关更多信息，请转到 https://support.mozilla.org/en-US/questions/939037。

允许访问Amazon Web Services Management Console使用 AD 凭据

Amazon Directory Service 允许向目录的成员授予 Amazon Web Services Management Console访问权限。默认情况下，目录成员无权访问任何 Amazon 资源。您可将 IAM 角色分配给目录成员，以便向其授予各种Amazon服务和资源。IAM 角色定义目录成员所拥有的服务、资源和访问权限级别。

目录必须首先具有访问 URL，然后您才能向目录成员授予控制台访问权限。有关如何查看目录详细信息和获取访问 URL 的更多信息，请参阅查看目录信息 (p. 120). 有关如何创建访问 URL 的更多信息，请参阅创建访问 URL (p. 125)。

有关如何创建 IAM 角色并将它们分配给目录成员的更多信息，请参阅。向用户和组授予访问权限Amazon资源 (p. 120).

主题

- 启用Amazon Web Services Management Console访问 (p. 244)

- 禁用Amazon Web Services Management Console访问 (p. 244)
- 设置登录会话长度 (p. 244)

相关Amazon安全博客文章

- 如何访问Amazon Web Services Management Console使用Amazon托管 Microsoft AD 和您的本地凭证

启用Amazon Web Services Management Console访问

默认情况下，不会为任何目录启用控制台访问。要为目录用户和组启用控制台访问，请执行以下步骤：

启用控制台访问

1. 在 Amazon Directory Service 控制台导航窗格中，选择 Directories (目录)。
2. 在 Directories 页面上，选择您的目录 ID。
3. 在 Directory details (目录详细信息) 页面上，选择 Application management (应用程序管理) 选项卡。
4. 在Amazon Web Services Management Console部分，选择。启用. 控制台访问现在已为目录启用。

   必须先将用户添加到角色中，然后用户才能使用访问 URL 登录控制台。有关将用户分配给 IAM 角色的一般信息，请参阅。向现有角色分配用户或组 (p. 122). 分配 IAM 角色之后，用户可以使用访问 URL 访问控制台。例如，如果目录访问 URL 是 example-corp.awsapps.com，则用于访问控制台的 URL 是 https://example-corp.awsapps.com/console/。

禁用Amazon Web Services Management Console访问

要为目录用户和组禁用控制台访问，请执行以下步骤：

禁用控制台访问

1. 在 Amazon Directory Service 控制台导航窗格中，选择 Directories (目录)。
2. 在 Directories 页面上，选择您的目录 ID。
3. 在 Directory details (目录详细信息) 页面上，选择 Application management (应用程序管理) 选项卡。
4. 在Amazon Web Services Management Console部分，选择。禁用. 控制台访问现在已为目录禁用。
5. 如果有任何 IAM 角色已分配给目录中的用户或组，则禁用按钮可能不可用。在这种情况下，您必须删除目录的所有 IAM 角色分配再继续，包括您目录中已删除的用户或组的分配，这将显示为删除用户要么删除组.

   删除所有 IAM 角色分配之后，重复以上步骤。

设置登录会话长度

默认情况下，用户在成功登录控制台之后以及注销之前，有 1 小时时间可使用其会话。在此之后，用户必须再次登录才能开始下一个 1 小时会话，然后再次注销。可以使用以下过程对每个会话将时间长度更改为最长 12 小时。

设置登录会话长度

1. 在 Amazon Directory Service 控制台导航窗格中，选择 Directories (目录)。
2. 在 Directories 页面上，选择您的目录 ID。
3. 在 Directory details (目录详细信息) 页面上，选择 Application management (应用程序管理) 选项卡。
4. 在Amazon应用和服务部分，选择。Amazon管理控制台.

5. 在管理对 的访问Amazon资源对话框中，选择。Continue.
6. 在 Assign users and groups to IAM roles 页面中的 Set login session length 下方，编辑编号的值，然后选择 Save。

教程：创建 Simple AD 目录

以下教程将引导您完成设置Amazon Directory Service对于 Simple AD 目录。它的目的是让您快速轻松地开始使用 Amazon Directory Service，但不适用于大规模生产环境。

主题

- 先决条件 (p. 245)
- 第 1 步：创建和配置 VPC (p. 245)
- 第 2 步：创建 Simple AD 目录 (p. 246)

先决条件

本教程假定：

- 您已经有一个有效的 Amazon 账户。
- 对于要在其中使用的区域中，账户尚未达到 VPC 限制。Amazon Directory Service. 有关 Amazon VPC 的更多信息，请参阅Amazon VPC 是什么？和您 VPC 中的子网中的Amazon VPC User Guide.
- 您在 CIDR 为 10.0.0/16 的区域中没有现有 VPC。

第 1 步：创建和配置 VPC

下一节演示如何创建和配置 VPC 以用于 Amazon Directory Service。

主题

- 创建新的 VPC (p. 245)
- 添加另一个子网 (p. 246)

创建新的 VPC

本教程使用一个 VPC 创建向导来创建以下内容：

- VPC
- 一个子网
- Internet 网关

要使用 VPC 向导创建您的 VPC，请执行以下步骤：

1. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在存储库的VPC 控制面板，选择启动 VPC 向导.
3. UNDLE第 1 步：选择 VPC 配置，开带单个公有子网的 VPC，选择Select.
4. 在向导中输入以下信息并选择创建 VPC.

   IP CIDR 数据块

   ```
   10.0.0.0/16
   ```

VPC 名称

`ADS VPC`

公有子网

`10.0.0.0/24`

可用区：

无首选项

子网名称

`ADS Subnet 1`

启用 DNS 主机名

保留默认选择

硬件租赁

默认值

5. 创建 VPC 需要几分钟时间。创建 VPC 之后，继续按照下一节的说明再添加一个子网。

添加另一个子网

Amazon Directory Service 要求 VPC 中有两个子网，并且每个子网必须位于不同的可用区中。VPC 向导仅创建一个子网，因此必须手动创建第二个子网，并指定与第一个子网不同的可用区。通过执行以下步骤创建第二个子网。

创建子网

1. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
2. 在导航窗格中，选择 Subnets，然后选择名为 `ADS Subnet 1` 的子网，最后选择页面底部的 Summary 选项卡。请记下此子网的可用区。
3. 单击 Create Subnet，然后在 Create Subnet 对话框中输入以下信息并单击 Yes, Create。

   名称标签

   `ADS Subnet 2`

   VPC

   选择您的 VPC。这是名为 `ADS VPC` 的 VPC。

   可用区：

   选择任意其他可用区，不要选择步骤 2 中的可用区。Amazon Directory Service 使用的两个子网必须位于不同的可用区中。

   CIDR Block

   `10.0.1.0/24`

第 2 步：创建 Simple AD 目录

要创建新目录，请执行以下步骤。在开始此过程之前，请确保您已满足了Simple AD 先决条件 (p. 209)中确定的先决条件。

创建 Simple AD 目录

1. 在Amazon Directory Service控制台选择导航窗格。目录然后选择设置目录.
2. 在存储库的选择目录类型页面上，选择。Simple AD，然后选择，下一步.
3. 在输入目录信息页面上，提供以下信息：

   目录大小

   从小型或大型大小选项中进行选择。有关大小的更多信息，请参阅Simple Active Directory (p. 208)。

   组织名称

   将用于注册客户端设备的目录的唯一组织名称。

   只有在作为启动 WorkSpaces 的一部分创建目录时，此字段才可用。

   目录 DNS 名称

   目录的完全限定名称，例如 `corp.example.com`。

   目录 NetBIOS 名称

   目录的短名称，如 `CORP`.

   管理员密码

   目录管理员的密码。目录创建过程将创建一个具有 `Administrator` 用户名和此密码的管理员账户。

   目录管理员密码区分大小写，且长度必须介于 8 到 64 (含) 个字符之间。至少，它还必须包含下列四种类别中三种类别的一个字符：

   - 小写字母 (a-z)
   - 大写字母 (A-Z)
   - 数字 (0-9)
   - 非字母数字字符 (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)

   确认密码

   重新键入管理员密码。

   目录描述

   目录的可选描述。
4. 在 Choose VPC and subnets (选择 VPC 和子网) 页面上，提供以下信息，然后选择 Next (下一步)。

   VPC

   目录的 VPC。

   Subnets (子网)

   为域控制器选择子网。两个子网必须位于不同的可用区。
5. 在 Review & create (检查并创建) 页面上，检查目录信息并进行任何必要的更改。如果信息正确，请选择 Create directory (创建目录)。目录创建需要几分钟时间。创建后，Status 值将更改为 Active。

Simple AD 的最佳实践

为避免问题并充分利用，您应该考虑以下建议和准则。AmazonManaged Microsoft AD。

设置：先决条件

创建目录之前请考虑以下这些准则。

验证你有正确的目录类型

Amazon Directory Service 提供了多种方式来结合使用 Microsoft Active Directory 与其他 Amazon 服务。您可以根据预算成本选择具有适当功能的目录服务以满足您的需求：

- Amazon针对 Microsoft Active Directory 的 Directory Service是一种功能丰富的托管 Microsoft Active Directory，托管在Amazon云。Amazon如果您的用户数超过 5000，并且需要在以下项之间建立信任关系，则是您的最佳选择。Amazon托管目录和您的本地目录。
- AD Connector将您现有本地 Active Directory 直接连接到Amazon. 当您想要将现有本地目录与一起使用时，AD Connector 是您的最佳选择。Amazon服务。
- Simple AD是具有常用目录功能并与 Active Directory 兼容的低成本服务。在大多数情况下，Simple AD 是成本最低的选择，如果您的用户数不超过 5000，并且不需要更高级的 Microsoft Active Directory 功能，这是您的最佳选择。

有关 Amazon Directory Service 选项的更详细比较，请参阅选择哪一个 (p. 1)。

确保您的 VPC 和实例配置正确

要连接到、管理和使用目录，必须正确配置目录所关联的 VPC。或者请参阅AmazonMicrosoft AD (p. 8)、AD Connetor (p. 171)，或者Simple AD 先决条件 (p. 209)以获取有关 VPC 安全和网络要求的信息。

如果要将实例添加到域，请确保您具有实例连接并且可以远程访问实例，如将 EC2 实例加入Amazon托管的 Microsoft AD 目录 (p. 66) 中所述。

请注意您的限制

了解特定目录类型的各种限制。对象的可用存储空间和总大小是对象可以存储在目录中的对象数量的唯一限制。或者请参阅AmazonManaged Microsoft AD 配额 (p. 141)、AD Connector 配额 (p. 205)，或者Simple AD 配额 (p. 250)有关所选目录的详细信息。

了解你的目录Amazon安全组配置和使用

Amazon创建安全组并将其附加到目录的域控制器弹性网络接口.Amazon将配置安全组以阻止到目录的不必要的流量并允许必要的流量。

修改目录安全组

如果要修改目录的安全组的安全性，则可以这样做。只有在您完全了解安全组的筛选如何工作时，才进行这样的更改。有关更多信息，请参阅 。适用于 Linux 实例的 Amazon EC2 安全组中的Amazon EC2 用户指南. 不正确的更改可能会导致丢失与目标计算机和实例的通信。Amazon建议您不要尝试打开到您的目录的其他端口，因为这会降低目录的安全性。请仔细查看Amazon责任共担模式.

> **Warning**
>
> 从技术上来说，您可以将目录的安全组与您创建的其他 EC2 实例关联。但是，Amazon建议不要采用这种做法。Amazon可能会由于某些原因在未经通知的情况下修改安全组，以满足托管目录的功能或安全需求。此类更改会影响您将目录安全组关联到的任何实例，并可能中断关联实例的操作。此外，将目录安全组与您的 EC2 实例关联可能为 EC2 实例带来潜在的安全风险。

使用Amazon管理 Microsoft AD（如果需要信任）

Simple AD 不支持信任关系。如果您需要在您的位置建立信任，则Amazon Directory Service目录和另一个目录，则应使用Amazon针对 Microsoft Active Directory 的 Directory Service。

设置：创建您的目录

下面是创建目录时应考虑的一些建议。

记住管理员 ID 和密码

设置目录时，需要提供管理员账户的密码。账户 ID 是管理员对于 Simple AD。请记住为此账户创建的密码；否则无法向您的目录中添加对象。

了解用户名限制Amazon应用程序

Amazon Directory Service 支持大多数可用于构造用户名的字符格式。但是，对于登录到所用的用户名有一些字符限制。Amazon应用程序，例如 WorkSpaces、Amazon WorkDocs、Amazon WorkMail 或 Amazon QuickSight。这些限制要求不使用以下字符：

- 空格
- 多字节字符
- !"#$%&'()*+,/:;<=>?@[\]^`{|}~

> Note
>
> 仅允许在 UPN 后缀之前使用 @ 符号。

为应用程序编程

在为您的应用程序编程之前，请考虑以下事项：

使用 Windows DC 定位器服务

开发应用程序时，请使用 Windows DC 定位器服务或使用的动态 DNS (DDNS) 服务Amazon管理微软 AD 以查找域控制器 (DC)。请勿使用 DC 的地址对应用程序进行硬编码。DC 定位器服务有助于确保分配目录负载，使您能够通过将域控制器添加到部署来利用水平扩展。如果您将应用程序绑定到固定 DC 并且 DC 进行修补或恢复，则您的应用程序将失去对 DC 的访问权限而不是使用其余的 DC。而且，DC 的硬编码可能导致在单一 DC 上出现热点。情况严重时，热点可能导致您的 DC 无法响应。此类情况可能还会导致 Amazon 目录自动化功能将目录标记为“受损”，并且可能触发更换无响应 DC 的恢复过程。

在推出生产之前进行加载测试

请务必对代表您的生产工作负载的对象和请求执行实验室测试，以确认目录将扩展至您的应用程序负载。如果您需要更多容量，则应使用Amazon Directory Service适用于 Microsoft Active Directory，使您能添加域控制器以获得高性能。有关更多信息，请参阅 部署额外的域控制器 (p. 132)。

使用高效的 LDAP 查询

对域控制器进行的针对数千个对象的广泛 LDAP 查询在单个 DC 中会产生明显的 CPU 周期消耗，从而导致热点。这可能影响在查询期间共享同一 DC 的应用程序。

Simple AD 配额

一般而言，您不应将 500 以上的用户添加到小型 Simple AD 目录，并且不应将 5000 以上的用户添加到大型 Simple AD 目录。有关更多灵活扩展选项和其他 Active Directory 功能，请考虑使用Amazon而是针对 Microsoft Active Directory（标准版或企业版）。

下面是 Simple AD 的默认配额。除非另有说明，否则每个配额是每个区域

Simple AD 配额

资源	默认配额
Simple AD 目录	10
手动快照*	每个 Simple AD 5 次

* 手动快照配额无法更改。

> **Note**
>
> 不能将公有 IP 地址附加到您的 Amazon 弹性网络接口 (ENI)。

Simple AD 的应用程序兼容性策略

Simple AD 是 Samba 的实现，具备 Active Directory 的许多基本功能。由于使用 Active Directory 的自定义和商业现成应用程序众多，Amazon不会且不能对与 Simple AD 兼容的第三方应用程序执行正式或综合性验证。虽然Amazon与客户一起努力尝试克服他们可能遇到的任何潜在应用程序安装难题，我们无法保证任何应用程序现在或将来继续与 Simple AD 兼容。

下列第三方应用程序与 Simple AD 兼容：

- 以下平台上的 Microsoft Internet Information Services (IIS)：
  - Windows Server 2003 R2
  - Windows Server 2008 R1
  - Windows Server 2008 R2
  - Windows Server 2012
  - Windows Server 2012 R2
- Microsoft SQL Server:
  - SQL Server 2005 R2 (Express、Web 和 Standard 版本)
  - SQL Server 2008 R2 (Express、Web 和 Standard 版本)
  - SQL Server 2012 (Express、Web 和 Standard 版本)
  - SQL Server 2014 (Express、Web 和 Standard 版本)
- Microsoft SharePoint：
  - SharePoint 2010 Foundation
  - SharePoint 2010 Enterprise
  - SharePoint 2013 Enterprise

客户可以选择使用AmazonMicrosoft Active Directory 的 Directory Service (Amazon托管的 Managed (p. 7))，以基于实际 Active Directory 实现更高级别的兼容性。

排查 Simple AD

以下内容可以帮助排查在创建或使用目录时可能会遇到的一些常见问题。

主题

- 密码找回 (p. 251)
- 当将用户添加到 Simple AD 时，我收到 “KDC Management option” 错误 (p. 251)
- 我无法更新已加入域的实例的 DNS 名称或 IP 地址 (DNS 动态更新) (p. 251)
- 我无法使用 SQL Server 账户登录 SQL Server (p. 251)
- 我的目录卡在 “Regest” 状态 (p. 251)
- 我在创建目录时遇到 “AZ Constance” 错误 (p. 252)
- 我的某些用户无法进行向我的目录进行身份验证 (p. 252)
- Simple AD 目录状态原因 (p. 252)

密码找回

如果用户忘记密码或在登录 Simple AD 或时遇到问题，Amazon托管 Microsoft AD 目录，你可以使用 Amazon Web Services Management Console、Windows PowerShell 或AmazonCLI。

有关更多信息，请参阅 重置用户密码 (p. 214)。

当将用户添加到 Simple AD 时，我收到 “KDC Management option” 错误

当 Samba CLI 客户端未正确将“net”命令发送到所有域控制器时，会出现此错误。如果您使用“net ads”命令将用户添加到 Simple AD 目录时看到此错误消息，请使用 -S 参数并指定任一域控制器的 IP 地址。如果您仍看到此错误，请尝试另一个域控制器。您还可以使用 Active Directory 管理工具将用户添加到您的目录中。有关更多信息，请参阅 安装 Active Directory 管理工具 (p. 212)。

我无法更新已加入域的实例的 DNS 名称或 IP 地址 (DNS 动态更新)

Simple AD 域中不支持 DNS 动态更新。可以改为通过在加入域的实例上使用 DNS 管理器连接到目录，直接进行更改。

我无法使用 SQL Server 账户登录 SQL Server

如果尝试结合使用 SQL Server Management Studio (SSMS) 与 SQL Server 账户登录在 Windows 2012 R2 EC2 实例上或 Amazon RDS 中运行的 SQL Server，则可能遇到错误。这种错误在 SSMS 作为域用户运行时发生，可能导致错误“Login failed for user”，即使提供了有效凭证时也是如此。这是一个已知问题，Amazon 正在积极努力解决它。

要解决该问题，可以使用 Windows 身份验证而不是 SQL 身份验证来登录 SQL Server。或者作为本地用户而不是 Simple AD 域用户来启动 SSMS。

我的目录卡在 “Regest” 状态

如果有一个目录处于“Requested”状态的时间超过 5 分钟，请尝试删除并重新创建该目录。如果问题仍然存在，请联系。Amazon Web Services SupportCenter.

我在创建目录时遇到 “AZ Constance” 错误

一段时间Amazon2012 年之前创建的账户可能访问美国东部（弗吉利亚北部）、美国西部（加利福尼亚北部）或亚太地区（东京）区域中不支持的可用区域。Amazon Directory Service目录。如果在创建目录时遇到错误 (如上面的错误)，请选择其他可用区中的子网，再尝试创建目录。

我的某些用户无法进行向我的目录进行身份验证

用户账户必须启用 Kerberos 预身份验证。这是新用户账户的默认设置，不应进行修改。有关此设置的更多信息，请参阅 Microsoft TechNet 上的 Preauthentication。

主题

- Simple AD 目录状态原因 (p. 252)

Simple AD 目录状态原因

当某个目录受损或不可操作时，目录状态消息会包含更多信息。状态消息显示在 Amazon Directory Service 控制台中，或者由 `DirectoryDescription.StageReason` API 在 `DescribeDirectories` 成员中返回。有关目录状态的更多信息，请参阅了解您的目录状态 (p. 48)。

以下是 Simple AD 目录的状态消息：

主题

- 目录服务的 elastic network interface 未连接 (p. 252)
- 实例检测到的问题 (p. 252)
- 关键Amazon Directory Service目录中缺少预留用户 (p. 253)
- 关键Amazon Directory Service该预留用户需要属于域管理员组 (p. 253)
- 关键Amazon Directory Service已禁用预留用户 (p. 253)
- 主域控制器没有所有 FSMO 角色 (p. 253)
- 域控制器复制失败 (p. 253)

目录服务的 elastic network interface 未连接

描述

在创建目录期间为与 VPC 建立网络连接而代表您创建的关键 elastic network interface (ENI) 未附加到目录实例。Amazon由此目录支持的应用程序将无法正常工作。您的目录无法连接到您的本地网络。

故障排除

如果 ENI 已分离但仍然存在，请联系Amazon Web Services Support. 如果弹性网卡被删除，则无法解决问题，并且您的目录永久无法使用。您必须删除目录，然后创建一个新目录。

实例检测到的问题

描述

实例检测到内部错误。这通常表示监控服务正在积极尝试恢复受损的实例。

故障排除

在大多数情况下，这是一个暂时性的问题，目录最终返回到活动状态。如果问题仍存在，请联系Amazon Web Services Support获得更多帮助。

关键Amazon Directory Service目录中缺少预留用户

描述

创建 Simple AD 时，Amazon Directory Service在该目录中创建一个名为的服务账户`AWSAdmin`*`D-xxxxxxxxx`*. 当无法找到此服务账户时会收到此错误。如果没有此账户，Amazon Directory Service 无法在该目录上执行管理功能，使该目录表现为不可用。

故障排除

要更正此问题，应将该目录还原到删除此服务账户之前创建的快照。Simple AD 目录每天自动拍摄一次快照。如果删除此账户已超过五天，您可能无法将该目录还原到此账户存在时的状态。如果您无法从存在此账户的快照中还原，您的目录可能会变得永久不可用。如果是这种情况，您必须删除目录，然后创建一个新目录。

关键Amazon Directory Service该预留用户需要属于域管理员组

描述

创建 Simple AD 时，Amazon Directory Service在该目录中创建一个名为的服务账户`AWSAdmin`*`D-xxxxxxxxx`*. 当此服务账户不是 `Domain Admins` 组的成员时会收到此错误。Amazon Directory Service 需要此组的成员资格才能获得执行维护和恢复操作所需的权限，例如转移 FSMO 角色、将新的目录控制器加入域，以及从快照还原。

故障排除

使用 Active Directory 用户和计算机工具将此服务账户重新添加到 `Domain Admins` 组。

关键Amazon Directory Service已禁用预留用户

描述

创建 Simple AD 时，Amazon Directory Service在该目录中创建一个名为的服务账户`AWSAdmin`*`D-xxxxxxxxx`*. 当此服务账户已禁用时会收到此错误。必须启用此账户，Amazon Directory Service 才能够在该目录上执行维护和恢复操作。

故障排除

使用 Active Directory 用户和计算机工具重新启用此服务账户。

主域控制器没有所有 FSMO 角色

描述

Simple AD 目录控制器并不拥有所有 FSMO 角色。Amazon Directory Service如果 FSMO 角色不属于正确的 Simple AD 目录控制器，则无法保证特定行为和功能。

故障排除

使用 Active Directory 工具将 FSMO 角色移回原始工作目录控制器。有关移动 FSMO 角色的更多信息，请转至https://docs.microsoft.com/troubleshoot/windows-server/identity/transfer-or-seize-fsmo-roles-in-ad-ds. 如果这样做不能解决此问题，请联系 Amazon Web Services Support 以获得更多帮助。

域控制器复制失败

描述

Simple AD 目录控制器未能完成相互复制。这可能是由以下一个或多个问题导致的：

- 这些目录控制器的安全组没有打开正确的端口。
- 网络 ACL 限制性过高。
- VPC 路由表没有正确路由这些目录控制器之间的网络流量。
- 已将另一个实例提升为该目录中的域控制器。

故障排除

有关您的 VPC 网络要求的更多信息，请参阅Amazon管理 Microsoft ADAmazonMicrosoft AD (p. 8)、AD ConnectorAD Connetor (p. 171)或 Simple ADSimple AD 先决条件 (p. 209). 如果您的目录中有未知的域控制器，则必须将其降级。如果您的 VPC 网络设置正确，但仍然出现该错误，请联系 Amazon Web Services Support 以获得更多帮助。

Amazon Directory Service 中的安全性

Amazon 十分重视云安全性。作为 Amazon 客户，您将从专为满足大多数安全敏感型企业的要求而打造的数据中心和网络架构中受益。

安全性是 Amazon 和您的共同责任。责任共担模式将其描述为云的安全性和云中的安全性：

- 云的安全性 – Amazon负责保护在Amazon云中运行Amazon服务的基础设施。Amazon还向您提供可安全使用的服务。作为 Amazon 合规性计划的一部分，第三方审核人员将定期测试和验证安全性的有效性。要了解适用于 Amazon Directory Service 的合规性计划，请参阅合规性计划范围内的 Amazon 服务。
- 云中的安全性 - 您的责任由您使用的 Amazon 服务决定。您还需要对其它因素负责，包括您的数据的敏感性、您公司的要求以及适用的法律法规。

此文档将帮助您了解如何在使用 Amazon Directory Service 时应用责任共担模型 以下主题说明如何配置 Amazon Directory Service 以实现您的安全性和合规性目标。您还会了解如何使用其它 Amazon 服务以帮助您监控和保护 Amazon Directory Service 资源。

安全主题

在此部分中可以找到以下安全性主题：

- 适用于 Amazon Directory Service 的 Identity and Access Management (p. 256)
- Amazon Directory Service 中的日志记录和监控 (p. 266)
- Amazon Directory Service 的合规性验证 (p. 266)
- Amazon Directory Service 中的故障恢复能力 (p. 266)
- Amazon Directory Service 中的基础设施安全性 (p. 267)

其他安全主题

在此指南中可以找到以下其他安全性主题：

账户、信托和Amazon资源访问权限

- 管理员账户 (p. 14)
- 组托管服务账户 (p. 17)
- 创建信任关系 (p. 96)
- 委托 Kerberos 约束委托 (p. 17)
- 向用户和组授予访问权限Amazon资源 (p. 120)
- 启用访问权限Amazon应用程序和服务 (p. 124)

保护您的目录

- 保护您的Amazon托管的 Microsoft AD 目录 (p. 25)
- 保护 AD Connector (p. 182)

日志记录和监控

- 监控Amazon托管的 Microsoft AD (p. 47)
- 监控 AD Connector 目录 (p. 193)

恢复功能

- 修补和维护AmazonMicrosoft AD 托管 (p. 16)

适用于 Amazon Directory Service 的 Identity and Access Management

访问 Amazon Directory Service 时需要可供 Amazon 用来验证您的请求的凭证。这些凭证必须有权访问 Amazon 资源，如 Amazon Directory Service 目录。下面几节提供详细的信息来说明如何使用 Amazon Identity and Access Management (IAM) 和 Amazon Directory Service 控制谁能访问您的资源，从而对这些资源进行保护：

- 身份验证 (p. 256)
- 访问控制 (p. 257)

身份验证

您可以以下面任一类型的身份访问 Amazon：

- Amazon Web Services 账户 根用户

  当您创建 Amazon Web Services 账户时，最初使用的是一个对账户中所有 Amazon Web Services和资源拥有完全访问权限的登录身份。此身份称为 Amazon Web Services 账户根用户，使用您创建账户时所用的电子邮件地址和密码登录，即可获得该身份。强烈建议您不要使用根用户执行日常任务。保护好根用户凭证，并使用这些凭证来执行仅根用户可以执行的任务。有关要求您以根用户身份登录的任务的完整列表，请参阅《Amazon 一般参考》中的需要根用户凭证的任务。
- IAM 用户和组

  IAM 用户是Amazon Web Services 账户内对某个人员或应用程序具有特定权限的一个身份。在可能的情况下，我们建议依赖于临时凭证，而不是创建具有长期凭证（如密码和访问密钥）的 IAM 用户。但是，如果您有一些特定的使用场景需要长期凭证以及 IAM 用户，我们建议您轮换访问密钥。有关更多信息，请参阅《IAM 用户指南》中的对于需要长期凭证的使用场景定期轮换访问密钥。

  IAM 组是一个指定一组 IAM 用户的身份。您不能使用组的身份登录。您可以使用组来一次性为多个用户指定权限。如果有大量用户，使用组可以更轻松地管理用户权限。例如，您可能具有一个名为 IAMAdmins 的组，并为该组授予权限以管理 IAM 资源。

  用户与角色不同。用户唯一地与某个人员或应用程序关联，而角色旨在让需要它的任何人代入。用户具有永久的长期凭证，而角色提供临时凭证。要了解更多信息，请参阅 IAM 用户指南中的何时创建 IAM 用户（而不是角色）。
- IAM 角色

  IAM 角色是可在账户中创建的一种具有特定权限的 IAM 身份。IAM 角色类似于 IAM 用户，因为它是一个 Amazon 身份，具有确定其在 Amazon 中可执行和不可执行的操作的权限策略。但是，角色旨在让需要它的任何人代入，而不是唯一地与某个人员关联。此外，角色没有关联的标准长期凭证（如密码或访问密钥）。相反，当您代入角色时，它会为您提供角色会话的临时安全凭证。具有临时凭证的 IAM 角色在以下情况下很有用：

- Federated user access（联合用户访问）– 要向联合身份分配权限，请创建角色并为角色定义权限。当联合身份进行身份验证时，该身份将与角色相关联并被授予由此角色定义的权限。有关联合身份验证的角色的信息，请参阅《IAM 用户指南》中的为第三方身份提供商创建角色。
- Amazon Web Service 访问 – 服务角色是一个 IAM 角色，服务代入该角色以代表您执行操作。IAM 管理员可以在 IAM 中创建、修改和删除服务角色。有关更多信息，请参阅 IAM 用户指南中的创建向 Amazon Web Service 委派权限的角色。
- 在 Amazon EC2 上运行的应用程序 – 您可以使用 IAM 角色管理在 EC2 实例上运行并发出 Amazon CLI 或 Amazon API 请求的应用程序的临时凭证。这优先于在 EC2 实例中存储访问密钥。要将 Amazon 角色分配给 EC2 实例并使其对该实例的所有应用程序可用，您可以创建一个附加到实例的实例配置文件。实例配置文件包含角色，并使 EC2 实例上运行的程序能够获得临时凭证。有关更多信息，请参阅 IAM 用户指南中的使用 IAM 角色为 Amazon EC2 实例上运行的应用程序授予权限。

访问控制

您可以使用有效的凭证来对自己的请求进行身份验证，但您还必须拥有权限才能创建或访问 Amazon Directory Service 资源。例如，您必须有权创建 Amazon Directory Service 目录或创建目录快照。

下面几节介绍如何管理 Amazon Directory Service 的权限。我们建议您先阅读概述。

- 管理 Amazon Directory Service 资源的访问权限的概述 (p. 257)
- 为 Amazon Directory Service 使用基于身份的策略（IAM policy）(p. 260)
- Amazon Directory ServiceAPI 权限：操作、资源和条件参考 (p. 265)

管理 Amazon Directory Service 资源的访问权限的概述

每个 Amazon 资源都归某个 Amazon 账户所有，创建或访问这些资源的权限由权限策略控制。账户管理员可以向 IAM 身份（即：用户、组和角色）附加权限策略，某些服务（如 Amazon Lambda）也支持向资源附加权限策略。

> Note
>
> 账户管理员（或管理员用户）是具有管理员权限的用户。有关更多信息，请参阅 IAM 用户指南中的 IAM 最佳实践。

在授予权限时，您要决定谁获得权限，获得对哪些资源的权限，以及您允许对这些资源执行的具体操作。

主题

- Amazon Directory Service 资源和操作 (p. 257)
- 了解资源所有权 (p. 258)
- 管理对资源的访问 (p. 258)
- 指定策略元素：操作、效果、资源和主体 (p. 259)
- 在策略中指定条件 (p. 260)

Amazon Directory Service 资源和操作

在 Amazon Directory Service 中，目录 是主要资源。Amazon Directory Service 还支持目录快照资源。不过，只能在现有目录的上下文中创建快照。因此，快照称为子资源。

这些资源具有关联的唯一 Amazon 资源名称 (ARN)，如下表所示。

资源类型	ARN 格式
目录	`arn:aws:ds:region:account-id:directory/external-directory-id`
快照	`arn:aws:ds:region:account-id:snapshot/external-snapshot-id`

Amazon Directory Service 提供一组操作来处理相应资源。有关可用操作的列表，请参阅目录服务操作。

了解资源所有权

资源所有者是创建资源的 Amazon 账户。也就是说，资源拥有者是 主体实体（根账户、IAM 用户或 IAM 角色）的 Amazon 账户，该账户会对创建资源的请求进行身份验证。以下示例说明了它的工作原理：

- 如果使用您的 Amazon 账户的根账户凭证来创建 Amazon Directory Service 资源（如目录），则您的 Amazon 账户就是该资源的拥有者。
- 如果您在中创建 IAM 用户Amazon账户并授予创建权限Amazon Directory Service资源提供给该用户，用户还可以创建Amazon Directory Service资源。但是，该用户所属的 Amazon 账户拥有这些资源。
- 如果您在中创建 IAM 角色Amazon拥有创建权限的账户Amazon Directory Service资源，任何可以担任该角色的人都可以创建Amazon Directory Service资源。该角色所属的 Amazon 账户拥有这些 Amazon Directory Service 资源。

管理对资源的访问

权限策略规定谁可以访问哪些内容。下一节介绍创建权限策略时的可用选项。

> **Note**
>
> 本节讨论如何在 Amazon Directory Service 范围内使用 IAM。这里不提供有关 IAM 服务的详细信息。有关完整的 IAM 文档，请参阅 IAM 用户指南中的什么是 IAM？。有关 IAM 策略语法和说明的信息，请参阅IAM JSON 策略参考在里面IAM 用户指南.

附加到 IAM 身份的策略称为基于身份的 策略（IAM 策略），而附加到资源的策略称为基于资源的 策略。Amazon Directory Service 仅支持基于身份的策略（IAM 策略）。

主题

- 基于身份的策略（IAM policy）(p. 258)
- 基于资源的策略 (p. 259)

基于身份的策略（IAM policy）

您可以向 IAM 身份附加策略。例如，您可以执行以下操作：

- 向您账户中的用户或组附加权限策略 – 账户管理员可以使用与特定用户关联的权限策略授予该用户创建 Amazon Directory Service 资源 (如新目录) 的权限。
- 向角色附加权限策略（授予跨账户权限） – 您可以向 IAM 角色附加基于身份的权限策略，以授予跨账户的权限。例如，账户 A 中的管理员可以创建一个角色，以向其他Amazon账户（如账户 B）或某项Amazon服务授予跨账户权限，如下所述：

  1. 账户 A 管理员可以创建一个 IAM 角色，然后向该角色附加授予其访问账户 A 中资源的权限策略。
  2. 账户 A 管理员可以把信任策略附加至用来标识账户 B 的角色，账户 B 由此可以作为主体代入该角色。

3. 之后，账户 B 管理员可以委派权限，指派账户 B 中的任何用户担任该角色。这样，账户 B 中的用户就可以创建或访问账户 A 中的资源了。如果您需要授予 Amazon 服务权限以便用户担任该角色，信任策略中的主体也可以是 Amazon 服务主体。

有关使用 IAM 委派权限的更多信息，请参阅 IAM 用户指南中的访问权限管理。

以下权限策略对用户授予权限以运行以 `Describe` 开头的所有操作。这些操作显示有关 Amazon Directory Service 资源（如目录或快照）的信息。请注意，`Resource` 元素中的通配符 (*) 表示可对该账户拥有的所有 Amazon Directory Service 资源执行操作。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":"ds:Describe*",
         "Resource":"*"
      }
   ]
}
```

有关对 Amazon Directory Service 使用基于身份的策略的更多信息，请参阅为 Amazon Directory Service 使用基于身份的策略（IAM policy）(p. 260)。有关用户、组、角色和权限的更多信息，请参阅 IAM 用户指南中的身份（用户、组和角色）。

基于资源的策略

其他服务 [如Simple Storage Service（Amazon S3）] 还支持基于资源的权限策略。例如，您可以将基于资源的策略附加到 S3 存储桶以管理对该存储桶的访问权限。Amazon Directory Service 不支持基于资源的策略。

指定策略元素：操作、效果、资源和主体

对于每种 Amazon Directory Service 资源，该服务都定义了一组 API 操作。有关更多信息，请参阅 Amazon Directory Service 资源和操作 (p. 257)。有关可用 API 操作的列表，请参阅目录服务操作。

为授予这些 API 操作的权限，Amazon Directory Service 定义了一组您可以在策略中指定的操作。请注意，执行某项 API 操作可能需要执行多个操作的权限。

以下是基本的策略元素：

- Resource（资源）- 在策略中，您可以使用 Amazon Resource Name (ARN) 标识策略应用到的资源。对于 Amazon Directory Service 资源，您随时可以在 IAM 策略中使用通配符 (*)。有关更多信息，请参阅 Amazon Directory Service 资源和操作 (p. 257)。
- 操作 – 您可以使用操作关键字标识要允许或拒绝的资源操作。例如，`ds:DescribeDirectories` 权限允许执行 Amazon Directory Service `DescribeDirectories` 操作的用户权限。
- 效果— 您可以指定当用户请求特定操作。可以是允许或拒绝。如果没有显式授予（允许）对资源的访问权限，则隐式拒绝访问。您也可显式拒绝对资源的访问，这样可确保用户无法访问该资源，即使有其他策略授予了访问权限的情况下也是如此。
- 主体 – 在基于身份的策略 (IAM policy) 中，附加了策略的用户是隐式主体。对于基于资源的策略，您可以指定要接收权限的用户、账户、服务或其他实体（仅适用于基于资源的策略）。Amazon Directory Service 不支持基于资源的策略。

要了解有关 IAM 策略语法和说明的更多信息，请参阅IAM JSON 策略参考在里面IAM 用户指南.

有关显示所有 Amazon Directory Service API 操作及其适用的资源的表，请参阅 Amazon Directory ServiceAPI 权限：操作、资源和条件参考 (p. 265)。

在策略中指定条件

当您授予权限时，可使用访问策略语言来指定规定策略何时生效的条件。例如，您可能希望策略仅在特定日期后应用。有关使用策略语言指定条件的更多信息，请参阅 IAM 用户指南中的条件。

要表示条件，您可以使用预定义的条件键。没有特定于 Amazon Directory Service 的条件键。但是有 Amazon 条件键，您可以根据需要使用。有关以下内容的完整列表Amazon钥匙，请参阅可用的全局条件键在里面IAM 用户指南.

为 Amazon Directory Service 使用基于身份的策略（IAM policy）

本主题提供了基于身份的策略的示例，在这些策略中，账户管理员可以向 IAM 身份（即：用户、组和角色）附加权限策略。

> **Important**
>
> 我们建议您首先阅读以下介绍性主题，这些主题讲解了管理 Amazon Directory Service 资源访问的基本概念和选项。有关更多信息，请参阅 管理 Amazon Directory Service 资源的访问权限的概述 (p. 257)。

本主题的各个部分涵盖以下内容：

- 使用 Amazon Directory Service 控制台所需的权限 (p. 261)
- 适用于 Amazon Directory Service 的 Amazon 托管（预定义）策略 (p. 261)
- 客户管理的策略示例 (p. 262)
- 在 IAM 策略中使用标签 (p. 263)

下面介绍权限策略示例。

```
{
   "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowDsEc2IamGetRole",
            "Effect": "Allow",
            "Action": [
                "ds:CreateDirectory",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:CreateNetworkInterface",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeVpcs",
                "ec2:CreateSecurityGroup",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:DeleteSecurityGroup",
                "ec2:DeleteNetworkInterface",
                "ec2:DescribeSubnets",
                "iam:GetRole"
            ],
            "Resource": "*"
        },
        {
            "Sid": "WarningAllowsCreatingRolesWithDirSvcPrefix",
```

```
            "Effect": "Allow",
            "Action": [
                "iam:CreateRole",
                "iam:PutRolePolicy"
            ],
            "Resource": "arn:aws:iam::111122223333:role/DirSvc*"
        },
        {
            "Sid": "AllowPassRole",
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": "cloudwatch.amazonaws.com"
                }
            }
        }
    ]
}
```

策略包括以下内容：

- 第一条语句授予创建 Amazon Directory Service 目录的权限。Amazon Directory Service 在资源级别不支持此特定操作的权限。因此，该策略指定通配符 (*) 作为 `Resource` 值。
- 第二条语句授予针对特定 IAM 操作的权限。需要访问 IAM 操作，以便Amazon Directory Service可以代表你读取和创建 IAM 角色。`Resource` 值末尾的通配符 (*) 表示该语句允许任何 IAM 角色执行 IAM 操作的权限。要将此权限限制到特定角色，请使用特定角色名称替换资源 ARN 中的通配符 (*)。有关更多信息，请参阅 IAM 操作。
- 第三条语句向一组特定 Amazon EC2 资源授予权限，这些权限是允许所必需的Amazon Directory Service创建、配置和销毁其目录。`Resource` 值末尾的通配符 (*) 表示该语句允许对任何 EC2 资源或子资源执行 EC2 操作的权限。要将此权限限制到特定角色，请使用特定资源或子资源替换资源 ARN 中的通配符 (*)。有关更多信息，请参阅 。Amazon EC2 操作

该策略不指定 `Principal` 元素，因为在基于身份的策略中，您未指定获取权限的委托人。附加了策略的用户是隐式委托人。向 IAM 角色附加权限策略后，该角色的信任策略中标识的委托人将获取权限。

有关显示所有 Amazon Directory Service API 操作及其适用的资源的表，请参阅 Amazon Directory ServiceAPI 权限：操作、资源和条件参考 (p. 265)。

使用 Amazon Directory Service 控制台所需的权限

要使用户可以使用 Amazon Directory Service 控制台，该用户必须拥有上面策略中列出的权限或是 Directory Service 完全访问角色或 Directory Service 只读角色所授予的权限，如适用于 Amazon Directory Service 的 Amazon 托管（预定义）策略 (p. 261)中所述。

如果创建比必需的最低权限更为严格的 IAM policy，对于附加了该 IAM policy 的用户， 控制台将无法按预期正常运行。

适用于 Amazon Directory Service 的 Amazon 托管（预定义）策略

Amazon通过提供由创建和管理的独立 IAM policy来满足许多常用案例的要求。Amazon托管式策略可授予常用案例的必要权限，因此，您可以免去调查都需要哪些权限的工作。有关更多信息，请参阅《IAM 用户指南》中的 Amazon 托管式策略。

以下 Amazon 托管策略（可附加到您账户中的用户）特定于 Amazon Directory Service：

- AWSDirectoryServiceReadOnlyAccess— 授予用户或群组对所有进行只读访问Amazon Directory Service资源、EC2 子网、EC2 网络接口和亚马逊SSimple Notification Service (Amazon SNS) 主题和根订阅Amazon账户。有关更多信息，请参阅 使用Amazon具有托管策略Amazon Directory Service (p. 123)。
- AWSDirectoryServiceFullAccess— 向用户或群组授予以下权限：
  - 对 Amazon Directory Service 的完全访问权限
  - 访问需要使用的 Amazon EC2 关键服务Amazon Directory Service
  - 可以列出 Amazon SNS 主题
  - 能够创建、管理和删除名称以" 开头的 Amazon SNS 主题DirectoryMonitoring"

  有关更多信息，请参阅 使用Amazon具有托管策略Amazon Directory Service (p. 123)。

此外，还有其他Amazon适合与其他 IAM 角色一起使用的托管策略。这些策略分配给与您的 Amazon Directory Service 目录中的用户相关联的角色。这些用户需要这些策略才能访问其他用户Amazon资源，例如 Amazon EC2。有关更多信息，请参阅 向用户和组授予访问权限Amazon资源 (p. 120)。

还可创建自定义 IAM 策略来允许用户访问必需的 操作和资源。您可以将这些自定义策略附加到需要这些权限的 IAM 用户或组。

客户管理的策略示例

本节的用户策略示例介绍如何授予各 Amazon Directory Service 操作的权限。

> Note
>
> 所有示例都使用美国西部 (俄勒冈) 区域 (`us-west-2`) 并且包含虚构的账户 ID。

示例

- 示例 1：允许用户对任何 Describe 执行任何 Describe 操作Amazon Directory Service资源 (p. 262)
- 示例 2：允许用户创建目录 (p. 262)

示例 1：允许用户对任何 Describe 执行任何 Describe 操作Amazon Directory Service资源

以下权限策略对用户授予权限以运行以 `Describe` 开头的所有操作。这些操作显示有关 Amazon Directory Service 资源（如目录或快照）的信息。请注意，`Resource` 元素中的通配符 (*) 表示可对该账户拥有的所有 Amazon Directory Service 资源执行操作。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":"ds:Describe*",
         "Resource":"*"
      }
   ]
}
```

示例 2：允许用户创建目录

以下权限策略授予权限以允许用户创建目录和所有其他相关资源 (如快照和信任)。要执行此操作，还需要针对特定 Amazon EC2 服务的权限。

```
{
   "Version":"2012-10-17",
```

```
   "Statement":[
      {
         "Effect":"Allow",
         "Action": [
                "ds:Create*",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateNetworkInterface",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteNetworkInterface",
                "ec2:DeleteSecurityGroup",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress"
                  ],
         "Resource":"*"
         ]
      }
   ]
}
```

在 IAM 策略中使用标签

可以在用于大多数 Amazon Directory Service API 操作的 IAM 策略中应用基于标签的资源级权限。这可让您更好地控制用户可创建、修改或使用哪些资源。在 IAM 策略中将 `Condition` 元素（也称作 `Condition` 块）与以下条件上下文键和值结合使用来基于资源标签控制用户访问（权限）：

- 使用 `aws:ResourceTag/`**`tag-key`**: **`tag-value`** 可允许或拒绝对带特定标签的资源的用户操作。
- 使用 `aws:ResourceTag/`**`tag-key`**: **`tag-value`** 可要求在发出创建或修改允许标签的资源的 API 请求时使用（或不使用）特定标签。
- 使用 `aws:TagKeys`: [**`tag-key`**, ...] 可要求在发出创建或修改允许标签的资源的 API 请求时使用（或不使用）一组特定标签键。

> **Note**
>
> IAM 策略中的条件上下文键和值仅适用于能够标记的资源的标识符是必需参数的那些 Amazon Directory Service 操作。

使用标签控制访问在里面IAM 用户指南包含有关使用标签的更多信息。这些区域有：IAM JSON 策略参考该指南的一部分包含 IAM 中的 JSON 策略的元素、变量和评估逻辑的详细语法、描述和示例。

以下标签策略示例允许所有 `ds` 调用，前提是它包含标签键/对 `"fooKey":"fooValue"`。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"VisualEditor0",
         "Effect":"Allow",
         "Action":[
            "ds:*"
         ],
         "Resource":"*",
         "Condition":{
            "StringEquals":{
               "aws:ResourceTag/fooKey":"fooValue"
            }
         }
```

```
        },
        {
            "Effect":"Allow",
            "Action":[
                "ec2:*"
            ],
            "Resource":"*"
        }
    ]
}
```

以下标签策略示例允许所有 ds 调用，前提是资源包含目录 ID“d-1234567890”。

```
{
    "Version":"2012-10-17",
    "Statement":[
        {
            "Sid":"VisualEditor0",
            "Effect":"Allow",
            "Action":[
                "ds:*"
            ],
            "Resource":"arn:aws:ds:us-east-1:123456789012:directory/d-1234567890"
        },
        {
            "Effect":"Allow",
            "Action":[
                "ec2:*"
            ],
            "Resource":"*"
        }
    ]
}
```

有关 ARN 的更多信息，请参阅 Amazon 资源名称 (ARN) 和 Amazon 服务命名空间。

以下 Amazon Directory Service API 操作支持基于标记的资源级权限：

- AcceptSharedDirectory
- AddIpRoutes
- AddTagsToResource
- CancelSchemaExtension
- CreateAlias
- CreateComputer
- CreateConditionalForwarder
- CreateSnapshot
- CreateLogSubscription
- CreateTrust
- DeleteConditionalForwarder
- DeleteDirectory
- DeleteLogSubscription
- DeleteSnapshot
- DeleteTrust
- DeregisterEventTopic
- DescribeConditionalForwarders
- DescribeDomainControllers

- DescribeEventTopics
- DescribeSharedDirectories
- DescribeSnapshots
- DescribeTrusts
- DisableRadius
- DisableSso
- EnableRadius
- EnableSso
- GetSnapshotLimits
- ListIpRoutes
- ListSchemaExtensions
- ListTagsForResource
- RegisterEventTopic
- RejectSharedDirectory
- RemoveIpRoutes
- RemoveTagsFromResource
- ResetUserPassword
- RestoreFromSnapshot
- ShareDirectory
- StartSchemaExtension
- UnshareDirectory
- UpdateConditionalForwarder
- UpdateNumberOfDomainControllers
- UpdateRadius
- UpdateTrust
- VerifyTrust

Amazon Directory ServiceAPI 权限：操作、资源和条件参考

在设置 访问控制 (p. 257) 和编写您可挂载到 IAM 身份的权限策略（基于身份的策略）时，可以使用下表作为参考。列表包含以下内容：

- 各个 Amazon Directory Service API 操作
- 您可授予执行该操作的权限的对应操作
- 您可以授予权限的 Amazon 资源

您在策略的 `Action` 字段中指定操作，并在策略的 `Resource` 字段中指定资源值。

> **Note**
>
> 一些 Amazon 应用程序可能需要在自身的策略中使用非公共 Amazon Directory Service API 操作 `ds:AuthorizeApplication`、`ds:CheckAlias`、`ds:CreateIdentityPoolDirectory` 和 `ds:UnauthorizeApplication`。

您可以在 Amazon Directory Service 策略中使用 Amazon 全局条件键来表示条件。有关以下内容的完整列表 Amazon钥匙，请参阅可用的全局条件密钥在里面IAM 用户指南.

Note

要指定操作，请在 API 操作名称之前使用 `ds:` 前缀 (例如，`ds:CreateDirectory`)。

相关主题

- 访问控制 (p. 257)

Amazon Directory Service 中的日志记录和监控

最佳做法是监控您的组织以确保记录变更。这有助于确保能够调查任何意外的更改，并回滚不需要的更改。Amazon Directory Service 目前支持以下两种 Amazon 服务，让您能够监控组织和组织内部的活动。

- 亚马逊 CloudWatch -您可以使用 CloudWatch 与AmazonMicrosoft AD 目录类型。有关更多信息，请参阅启用日志转发 (p. 51)。此外，你可以使用 CloudWatch监控域控制器性能的指标。有关更多信息，请参阅使用 Amazon CloudWatch 指标来确定何时添加域控制器 (p. 134)。
- Amazon CloudTrail-您可以使用 CloudTrail 与所有Amazon Directory Service目录类型。有关更多信息，请参阅 。日志记录Amazon Directory ServiceAPI 调用 CloudTrail.

Amazon Directory Service 的合规性验证

作为多个 Amazon Directory Service 合规性计划的一部分，第三方审核员将评估 Amazon 的安全性和合规性。与AmazonMicrosoft AD，其中包括 SOC、FedRAMP、FedRAMP、HIPAA 及其他。有关更多信息，请参阅 管理合规性AmazonManaged Mic (p. 37)。

有关特定合规性计划范围内的 Amazon 服务的列表，请参阅合规性计划范围内的 Amazon 服务。有关一般信息，请参阅 Amazon 合规性计划。

您可以使用 Amazon Artifact 下载第三方审计报告。有关更多信息，请参阅在 Amazon Artifact 中下载报告。

使用 Amazon Directory Service 时，您的合规性责任由您数据的敏感性、贵公司的合规性目标以及适用的法律法规决定。Amazon 提供以下资源来帮助满足合规性：

- 安全性与合规性快速入门指南 – 这些部署指南讨论了架构注意事项，并提供了在Amazon上部署基于安全性和合规性的基准环境的步骤。
- HIPAA 安全与合规架构白皮书— 本白皮书描述了公司如何使用Amazon创建符合 HIPAA 要求的应用程序。
- Amazon合规性资源 – 此业务手册和指南集合可能适用于您的行业和位置。
- Amazon Config – 此Amazon服务评估您的资源配置对内部实践、行业指南和法规的遵循情况。
- Amazon Security Hub – 此 Amazon 服务提供了 Amazon 中安全状态的全面视图，可帮助您检查是否符合安全行业标准和最佳实践。

Amazon Directory Service 中的故障恢复能力

Amazon全球基础设施围绕Amazon区域和可用区构建。Amazon区域提供多个在物理上独立且隔离的可用区，这些可用区通过延迟低、吞吐量高且冗余性高的网络连接在一起。利用可用区，您可以设计和操作在可用区之间无中断地自动实现故障转移的应用程序和数据库。与传统的单个或多个数据中心基础设施相比，可用区具有更高的可用性、容错性和可扩展性。

有关 Amazon 区域和可用区的更多信息，请参阅 Amazon 全球基础设施。

除了 Amazon 全球基础设施之外，Amazon Directory Service 还提供了在任何时间点为数据制作手动快照的功能，帮助支持您的数据弹性和备份需求。有关更多信息，请参阅 快照或恢复你的目录 (p. 118)。

Amazon Directory Service 中的基础设施安全性

作为一项托管服务，Amazon Directory Service受保护Amazon全局网络安全程序，如中所述Amazon Web Services：安全过程概述白皮书。

您可以使用 Amazon 发布的 API 调用通过网络访问 Amazon Directory Service。客户端必须支持传输层安全性（TLS）。建议使用 TLS 1.2 或更高版本。客户端还必须支持具有完全向前保密 (PFS) 的密码套件，例如 Ephemeral Diffie-Hellman (DHE) 或 Elliptic Curve Ephemeral Diffie-Hellman (ECDHE)。大多数现代系统（如 Java 7 及更高版本）都支持这些模式。

如果在通过命令行界面或 API 访问 Amazon 时需要经过 FIPS 140-2 验证的加密模块，请使用 FIPS 端点。有关可用 FIPS 终端节点的更多信息，请参阅联邦信息处理标准 (FIPS) 140-2.

此外，必须使用访问密钥 ID 和与 IAM 委托人关联的秘密访问密钥来对请求进行签名。或者，您可以使用 Amazon Security Token Service (Amazon STS) 生成临时安全凭证来对请求进行签名。

防止跨服务混淆代理

混淆代理问题是一个安全性问题，即不具有操作执行权限的实体可能会迫使具有更高权限的实体执行该操作。在 Amazon 中，跨服务模拟可能会导致混淆代理问题。一个服务（呼叫服务) 调用另一项服务（所谓的服务)时，可能会发生跨服务模拟。可以操纵调用服务，使用其权限以在其他情况下该服务不应有访问权限的方式对另一个客户的资源进行操作。为了防止这种情况，Amazon 提供可帮助您保护所有服务的服务委托人数据的工具，这些服务委托人有权限访问账户中的资源。

我们建议使用`aws:SourceArn`和`aws:SourceAccount`资源策略中的全局条件上下文密钥用于限制以下权限AmazonMicrosoft Active Dictory Service 为资源提供另 如果 `aws:SourceArn` 值不包含账户 ID，例如 Amazon S3 存储桶 ARN，您必须使用两个全局条件上下文密钥来限制权限。如果同时使用全局条件上下文密钥和包含账户 ID 的 `aws:SourceArn` 值，则 `aws:SourceAccount` 值和 `aws:SourceArn` 值中的账户在同一策略语句中使用时，必须使用相同的账户 ID。如果您只希望将一个资源与跨服务访问相关联，请使用 `aws:SourceArn`。如果您想允许该账户中的任何资源与跨服务使用操作相关联，请使用 `aws:SourceAccount`。

在以下示例中，的值为`aws:SourceArn`必须是 CloudWatch 日志组。

防范混淆代理问题最有效的方法是使用 `aws:SourceArn` 全局条件上下文键和资源的完整 ARN。如果不知道资源的完整 ARN，或者正在指定多个资源，请针对 ARN 未知部分使用带有通配符 (`*`) 的 `aws:SourceArn` 全局上下文条件键。例如，`arn:aws:servicename:*:123456789012:*`。

以下示例说明如何使用`aws:SourceArn`和`aws:SourceAccount`中的全局条件上下文键AmazonMicrosoft AD 以防止混淆代理问题。

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "ConfusedDeputyPreventionExamplePolicy",
    "Effect": "Allow",
    "Principal": {
      "Service": "ds.amazonaws.com"
    },
    "Action": [
                "logs:CreateLogStream",
                "logs:PutLogEvents"
            ],
    "Resource": [
```

```
      "arn:aws:logs:YOUR_REGION:YOUR_ACCOUNT_NUMBER:log-group:/aws/
directoryservice/YOUR_LOG_GROUP:*"
    ],
    "Condition": {
      "ArnLike": {
        "aws:SourceArn":
 "arn:aws:ds:YOUR_REGION:YOUR_ACCOUNT_NUMBER:directory/YOUR_DIRECTORY_ID"
      },
      "StringEquals": {
        "aws:SourceAccount": "123456789012"
      }
    }
  }
}
```

在以下示例中，的值为`aws:SourceArn`必须是您账户中的 SNS 主题。例如，你可以使用类似的东西`arn:aws:sns:ap-southeast-1:123456789012:DirectoryMonitoring_d-966739499f`其中 “ap-southeast-1” 是您所在的地区，“123456789012” 是您的客户 ID，”DirectoryMonitoring_d-96673949f” 是您创建的 Amazon SNS 主题名称。

防范混淆代理问题最有效的方法是使用 `aws:SourceArn` 全局条件上下文键和资源的完整 ARN。如果不知道资源的完整 ARN，或者正在指定多个资源，请针对 ARN 未知部分使用带有通配符 (`*`) 的 `aws:SourceArn` 全局上下文条件键。例如，`arn:aws:servicename:*:123456789012:*`。

以下示例说明如何使用`aws:SourceArn`和`aws:SourceAccount`中的全局条件上下文键AmazonMicrosoft AD 以防止混淆代理问题。

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "ConfusedDeputyPreventionExamplePolicy",
    "Effect": "Allow",
    "Principal": {
      "Service": "ds.amazonaws.com"
    },
    "Action": ["SNS:GetTopicAttributes",
     "SNS:SetTopicAttributes",
        "SNS:AddPermission",
     "SNS:RemovePermission",
     "SNS:DeleteTopic",
     "SNS:Subscribe",
     "SNS:ListSubscriptionsByTopic",
     "SNS:Publish"],
    "Resource": [
      "arn:aws:sns:YOUR_REGION:YOUR_ACCOUNT_NUMBER:YOUR_SNS_TOPIC_NAME"
    ],
    "Condition": {
      "ArnLike": {
        "aws:SourceArn":
 "arn:aws:sns:YOUR_REGION:YOUR_ACCOUNT_NUMBER:directory/YOUR_EXTERNAL_DIRECTORY_ID"
      },
      "StringEquals": {
        "aws:SourceAccount": "123456789012"
      }
    }
  }
}
```

以下示例显示了已委托控制台访问权限的角色的 IAM 信任策略。的值`aws:SourceArn`必须是您账户中的目录资源。有关更多信息，请参阅 。定义的资源类型Amazon Directory Service. 例如，您可以使用`arn:aws:ds:us-east-1:123456789012:directory/d-1234567890`哪里`123456789012`是你的客户 ID 和`d-1234567890`是你的目录 ID。

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "ConfusedDeputyPreventionExamplePolicy",
    "Effect": "Allow",
    "Principal": {
      "Service": "ds.amazonaws.com"
    },
    "Action": [
                "sts:AssumeRole"
            ],
    "Condition": {
      "ArnLike": {
        "aws:SourceArn":
 "arn:aws:ds:YOUR_REGION:YOUR_ACCOUNT_NUMBER:directory/YOUR_DIRECTORY_ID"
      },
      "StringEquals": {
        "aws:SourceAccount": "123456789012"
      }
    }
  }
}
```

服务等级协议Amazon Directory Service

Amazon Directory Service是一项高度可用的服务，构建在Amazon-托管基础设施。它由定义服务可用性策略的服务等级协议提供支持。

有关更多信息，请参阅 。服务等级协议Amazon Directory Service.

区域可用性Amazon Directory Service

下表提供了一份列表，描述了目录类型支持特定于区域的端点列表。

区域名称	区域	端点	协议	AmazonM	AD Connecto	Simple AD
美国东部（俄亥俄州）	us-east-2	ds.us-east-2.amazonaws.com	HTTPS	是	是	否
美国东部（弗吉尼亚州北部）	us-east-1	ds.us-east-1.amazonaws.com	HTTPS	是	是	是
美国西部（北加利福尼亚）	us-west-1	ds.us-west-1.amazonaws.com	HTTPS	是	是	否
美国西部（俄勒冈州）	us-west-2	ds.us-west-2.amazonaws.com	HTTPS	是	是	是
非洲（开普敦）	af-south-1	ds.af-south-1.amazonaws.com	HTTPS	是	是	否
亚太地区（香港）	ap-east-1	ds.ap-east-1.amazonaws.com	HTTPS	是	是	否
亚太地区（孟买）	ap-south-1	ds.ap-south-1.amazonaws.com	HTTPS	是	是	否
亚太地区（大阪）	ap-northeast-3	ds.ap-northeast-3.amazonaws.com	HTTPS	是	是	否
亚太地区（首尔）	ap-northeast-2	ds.ap-northeast-2.amazonaws.com	HTTPS	是	是	否
亚太地区（新加坡）	ap-southeast-1	ds.ap-southeast-1.amazonaws.com	HTTPS	是	是	是
Asia Pacific (Sydney)	ap-southeast-2	ds.ap-southeast-2.amazonaws.com	HTTPS	是	是	是

区域名称	区域	端点	协议	AmazonM	AD Connecto	Simple AD
亚太地区（雅加达）	ap-southeast-3	ds.ap-southeast-3.amazonaws.com	HTTPS	是	是	否
亚太地区（东京)	ap-northeast-1	ds.ap-northeast-1.amazonaws.com	HTTPS	是	是	是
Canada (Central)	ca-central-1	ds.ca-central-1.amazonaws.com	HTTPS	是	是	否
中国（北京）	cn-north-1	ds.cn-north-1.amazonaws.com.cn	HTTPS	是	是	否
中国（宁夏）	cn-northwest-1	ds.cn-northwest-1.amazonaws.com.cn	HTTPS	是	是	否
欧洲（法兰克福）	eu-central-1	ds.eu-central-1.amazonaws.com	HTTPS	是	是	否
Europe (Ireland)	eu-west-1	ds.eu-west-1.amazonaws.com	HTTPS	是	是	是
欧洲（伦敦）	eu-west-2	ds.eu-west-2.amazonaws.com	HTTPS	是	是	否
欧洲（巴黎）	eu-west-3	ds.eu-west-3.amazonaws.com	HTTPS	是	是	否
欧洲（斯德哥尔摩）	eu-north-1	ds.eu-north-1.amazonaws.com	HTTPS	是	是	否
欧洲（米兰）	eu-south-1	ds.eu-south-1.amazonaws.com	HTTPS	是	是	否
中东（巴林）	me-south-1	ds.me-south-1.amazonaws.com	HTTPS	是	是	否
South America (São Paulo)	sa-east-1	ds.sa-east-1.amazonaws.com	HTTPS	是	是	否
Amazon GovCloud（美国西部）	us-gov-west-1	ds。us-gov-west-1.amazonaws.com	HTTPS	是	是	否

区域名称	区域	端点	协议	AmazonM	AD Connecto	Simple AD
Amazon GovCloud（美国东部）	us-gov-east-1	ds。us-gov-east-1.amazonaws.com	HTTPS	是	是	否

有关使用内容的信息Amazon Directory Service在里面Amazon GovCloud（US-West）区域和Amazon GovCloud（US-East）区域，请参阅服务端点.

有关使用内容的信息Amazon Directory Service在北京和宁夏地区，请参阅中国Amazon Web Services 终端节点和 ARN.

浏览器兼容性

Amazon应用程序和服务，例如 WorkSpaces，Amazon WorkMail、Amazon Connect、Amazon Chime、亚马逊 WorkDocs，以及Amazon IAM Identity Center (successor to Amazon Single Sign-On)所有这些都需要来自兼容浏览器的有效登录凭证才能访问它们。下表仅列出了兼容登录的浏览器和浏览器版本。

浏览器	版本	兼容性
Microsoft Internet Explorer	Desktop IE 版本 7 及更低版本	不兼容
	Desktop IE 版本 8、9 和 10	仅在运行 Windows 7 或更高版本并启用 TLS 1.1 时兼容。参阅 什么是 TLS？ (p. 275) 了解更多信息。
	Desktop IE 版本 11 及更高版本	兼容
	Mobile IE 版本 10 及更低版本	不兼容
	Mobile IE 版本 11 及更高版本	兼容
Microsoft Edge	所有版本	兼容
Mozilla Firefox	Firefox 23 及更低版本	不兼容
	Firefox 24 至 26	兼容，但默认情况下不兼容。
	Firefox 27 及更高版本	兼容
Google Chrome	Google Chrome 21 及更低版本	不兼容
	Google Chrome 22 至 37	兼容，但默认情况下不兼容。
	Google Chrome 38 及更高版本	兼容
Apple Safari	适用于 OS X 10.8 (Mountain Lion) 及更低版本的 Desktop Safari 版本 6 及更低版本	不兼容
	适用于 OS X 10.9 (Mavericks) 及更高版本的 Desktop Safari 版本 7 及更高版本	兼容
	适用于 iOS 4 及更低版本的 Mobile Safari	不兼容
	适用于 iOS 5 及更高版本的Mobile Safari 版本 5 及更高版本	兼容

现在，您已经验证了您使用的是受支持的浏览器版本，我们建议您继续阅读以下部分，验证您的浏览器是否已配置为使用 Amazon 要求的传输层安全性 (TLS) 设置。

什么是 TLS？

TLS 是一种协议，供 Web 浏览器和其他应用程序用来通过网络安全地交换数据。TLS 通过加密和终端节点身份验证来确保连接到的远程终端节点是预期的终端节点。截至目前，TLS 有 TLS 1.0、1.1、1.2 和 1.3 四个版本。

IAM 身份中心支持哪些 TLS 版本

Amazon 应用程序和服务支持 TLS 1.1、1.2 和 1.3 进行安全登录。自 2019 年 10 月 30 日起，TLS 1.0 将不再受支持，因此，请务必将所有浏览器配置为支持 TLS 1.1 或更高版本。这意味着，如果您在 TLS 1.0 启用后访问 Amazon 应用程序和服务，则将无法登录。要获取有关如何作出此更改的帮助，请联系管理员。

如何在浏览器中启用支持的 TLS 版本

这取决于您的浏览器。通常情况下，您可以在浏览器设置中的高级设置区域下找到此设置。例如，在 Internet Explorer 中，您可以在 Internet Properties (互联网属性)、Advanced (高级) 选项卡、Security (安全性) 部分下找到各种 TLS 选项。查看您的浏览器制造商帮助网站，获取具体说明。

文档历史记录

下表介绍了自上次发布 Amazon Directory Service 管理员指南以来的重要更改。

- 文档最新更新：2021 年 8 月 25 日

变更	说明	日期
Simple AD VPC	添加了有关不应配置哪些 VPC 终端节点的内容。	2021 年 8 月 25 日
AD Connector VPC	添加了有关不应配置哪些 VPC 终端节点的内容。	2021 年 8 月 25 日
智能卡支持	添加了有关支持智能卡和亚马逊的内容 WorkSpaces 应用程序管理器在Amazon GovCloud （US-West）区域	2020 年 12 月 1 日
密码重置	添加了有关如何使用重置用户密码的内容Amazon Web Services Management Console，Windows PowerShell 和AmazonCLI。	2019 年 1 月 2 日
目录共享	增加了有关使用 Directory 共享的文档AmazonMicrosoft AD	2018 年 9 月 25 日
已将内容迁移到新的Amazon Cloud Directory 开发者指南	本指南先前的 Amazon Cloud Directory 内容已移至新的Amazon Cloud Directory.	2018 年 6 月 21 日
全面检修管理员指南 TOC	重新组织了内容以更直接地联系客户需求，并在需要的位置新增了内容。	2018 年 5 月 4 日
Amazon委托群组	添加了清单Amazon可以分配给本地用户的委托群组。	2018 年 3 月 8 日
精细的密码策略	新增新的密码策略内容。	2017 年 5 月 7 日
其他域控制器	添加了有关向您的添加更多域控制器的信息AmazonMicrosoft AD	2017 年 6 月 30 日
教程	添加了用于测试 a 的新教程 AmazonMicrosoft AD 实验室环境。	2017 年 6 月 21 日
MFA 和AmazonManaged Mic	添加了使用 MFA 的文档 AmazonMicrosoft AD	2017 年 2 月 13 日
Amazon Cloud Directory	引入了新目录类型。	2017 年 1 月 26 日
架构扩展	增加了有关使用 Schema 扩展的文档AmazonMicrosoft Acte Acte	2016 年 11 月 14 日
Directory Service 管理指南的重大重组	重新组织了内容，更直接地反映客户需求。	2016 年 11 月 14 日

SNS 通知	添加了有关 SNS 通知的文档。	2016 年 2 月 25 日
授权和认证	添加了有关将 IAM 与 Directory Services 结合使用的其他文档。	2016 年 2 月 25 日
AmazonManaged Mic	添加了的文档Amazon托管 Microsoft AD，并将指南合并为一个指南。	2015 年 11 月 17 日
允许 Linux 实例加入到简单 AD 目录中	添加了有关将 Linux 实例加入简单 AD 目录的文档。	2015 年 7 月 23 日
指导Secarat	Amazon Directory Service 管理员指南拆分为单独的指南，即 Simple AD 指南和 AD Connector 指南。	2015 年 7 月 14 日
单点登录支持	添加了单点登录文档。	2015 年 3 月 31 日
新指南	这是的第一个版本Amazon Directory Service管理指南.	2014 年 10 月 21 日

本文属于机器翻译版本。若本译文内容与英语原文存在差异，则一律以英文原文为准。