aws

管理指南

AWS Directory Service

版本 1.0

AWS Directory Service: 管理指南

Table of Contents

什么是 AWS Directory Service？ 1
选择哪一个 1
AWS Directory Service 选项 2
使用 Amazon EC2 5
开始使用 6
注册获取 AWS 账户 6
创建具有管理权限的用户 6
更多信息 7
AWS 微软 AD 托管 9
开始使用 10
AWS 微软 AD 托管先决条件 11
创建你的 Microsoft AWS 托管广告 12
用你的 AWS 托管 Microsoft AD 活动目录创建了什么 14
管理员账户权限 21
重要概念 23
Active Directory 架构 23
修补和维护 24
组托管服务账户 25
Kerberos 约束委托 25
最佳实践 26
设置：先决条件 26
设置：创建目录 28
使用目录 29
管理目录 30
为您的应用程序编程 32
使用案例 33
用例 1：使用 Active Directory 凭据登录 AWS 应用程序和服务 34
使用案例 2：管理 Amazon EC2 实例 38
用例 3：为支持 Active Directory 的工作负载提供目录服务 38
用例 4： AWS IAM Identity Center 到 Office 365 和其他云应用程序 38
用例 5：将您的本地 Active Directory 扩展到 AWS 云端 39
用例 6：共享您的目录以跨 AWS 账户将 Amazon EC2 实例无缝加入到域中 39
如何... 39
保护目录 40

监控目录 80
配置多区域复制 93
共享您的目录 100
将实例加入你的 AWS 托管 Microsoft AD 112
管理用户和组 165
Connect 您现有的活动目录基础架构 175
将你的 Microsoft AWS 托管广告连接到 Microsoft Entra Connect Sync 197
扩展架构 202
维护目录 209
授予 AWS 资源访问权限 216
允许访问 AWS 应用程序和服务 222
允许访问 AWS Management Console 232
部署额外的域控制器 234
将用户从 AD 迁移到 AWS Managed Microsoft AD 237
配额 237
应用程序兼容性 238
兼容性指南 240
已知不兼容的应用程序 240
AWS 微软 AD 托管测试实验室教程 241
教程：设置你的基础 AWS 托管 Microsoft AD 测试实验室 241
教程：创建从 AWS 托管 Microsoft AD 到 EC2 上自行管理的 AD 安装的信任 257
故障排除 267
你的 AWS 托管 Microsoft AD 存在问题 267
Netlogon 和安全信道通信存在问题 267
重置用户密码时出现问题 267
密码找回 268
其他 资源 268
使用 Microsoft 事件查看器监控 DNS 服务器 268
Linux 域加入错误 269
低可用存储空间 272
架构扩展错误 275
信任创建状态原因 277
AD Connector 281
开始使用 282
AD Connector 先决条件 282
创建 AD Connector 296

使用 AD Connector 创建了什么 298
如何... 298
保护目录 299
监控目录 318
将 Amazon EC2 实例加入您的 Active Directory 322
维护目录 335
允许访问 AWS 应用程序和服务 337
为 AD Connector 更新 DNS 地址 338
最佳实践 339
设置：先决条件 339
为您的应用程序编程 341
使用目录 341
配额 341
应用程序兼容性 342
故障排除 343
创作问题 343
连接问题 344
身份验证问题 345
维护问题 349
我无法删除我的 AD Connector 350
Simple AD 351
开始使用 352
Simple AD 先决条件 352
制作你的 Simple AD Active Directory 354
用你的 Simple AD 创作了什么 Active Directory 355
为 Simple AD 配置 DNS 356
如何... 357
管理用户和组 357
监控目录 368
将实例加入你的 Simple AD 372
维护目录 403
允许访问 AWS 应用程序和服务 407
允许访问 AWS Management Console 417
教程：制作一个 Simple AD Active Directory 419
教程的先决条件 419
最佳实践 421

设置：先决条件 421
设置：创建目录 423
为您的应用程序编程 423
配额 424
应用程序兼容性 425
故障排除 425
密码找回 426
当将用户添加到 Simple AD 时，我收到“KDC 无法执行所请求的选项”错误 426
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) 426
我无法使用 SQL Server 账户登录 SQL Server 426
我的目录卡在“已请求”状态 427
我在创建目录时遇到“AZ 受限”错误 427
我的某些用户无法进行向我的目录进行身份验证 427
其他 资源 268
目录状态原因 427
安全性 431
Identity and Access Management 432
身份验证 432
访问控制 432
有关管理访问的概述 433
使用基于身份的策略（IAM 策略） 437
AWS Directory Service API 权限参考 445
对应用程序和服务进行授权和取消授权 AWS 445
日记账记录和监控 446
合规性验证 447
弹性 448
基础设施安全性 448
防止跨服务混淆代理 448
AWS PrivateLink 451
注意事项 452
可用性 452
创建接口端点 453
创建 VPC 端点策略 454
服务等级协议 456
区域可用性 457
浏览器兼容性 462

什么是 TLS？ 462
IAM Identity Center 支持的 TLS 版本 462
如何在浏览器中启用支持的 TLS 版本 462
文档历史记录 463
..... cdlxvi

什么是 AWS Directory Service？

AWS Directory Service 提供了多种与其他 AWS 服务一起使用 Microsoft Active Directory (AD) 的方式。目录存储有关用户、群组和设备的信息，管理员使用它们来管理对信息和资源的访问权限。 AWS Directory Service 为想要在云中使用现有 A Microsoft D 或轻型目录访问协议 (LDAP) 感知应用程序的客户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。使用下表可以帮助您确定哪个 AWS Directory Service 目录选项最适合您的组织。

您需要做什么？	推荐 AWS Directory Service 选项
我需要在云中为应用程序使用 Active Directory 或 LDAP	如果你需要 AWS 云端支持Active Directory感知型工作负载或应用程序和服务（例如亚马逊和亚马逊 WorkSpaces ），或者你需要对 Linux AWS 应用程序的 LDAP 支持，请使用AWS Microsoft Active Directory（标准版或企业版）的 Directory Service。Microsoft Active Directory QuickSight 如果您只需要允许本地用户使用其Active Directory凭据登录 AWS 应用程序和服务，请使用 A D Connector。您也可以使用 AD Connector 将 Amazon EC2 实例加入到您的现有 Active Directory域中。 如果您需要一个支持兼容 Samba 4 的应用程序且具有基本Active Directory兼容性的低规模、低成本目录，或者需要支持 LDAP 的应用程序兼容 LDAP 的应用程序，请使用 Simple AD。
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用户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。

有关 AWS Directory Service 目录选项的更多信息，请参阅如何选择Active Directory解决方案 AWS。

AWS Directory Service 选项

AWS Directory Service 包括几种可供选择的目录类型。有关更多信息，请选择以下选项卡之一：

AWS Directory Service for Microsoft Active Directory

微软 A AWS ctive Directory 的 Directory Service 也被称为 AWS 托管 Microsoft AD，由 AWS AWS 云端管理的实际 Microsoft Windows Server Active Directory (AD) 提供支持。它使您能够将各种支持 Active Directory 的应用程序迁移到云端。 AWS AWS 托管 Microsoft AD 可与 Microsoft SharePoint Microsoft SQL Server Always On 可用性组和许多.NET 应用程序配合使用。它还支持 AWS 托管应用程序和服务，包括亚马逊 WorkSpaces、亚马逊、亚马逊、Ama zon Chime WorkDocs QuickSight、Amaz on C onnect 和适用于 P ostgreSQL 的亚马逊关系数据库服务（适用于Microsoft SQL Server亚马逊 RDS、适用于 Amazon RDS 和 SQL Server Amazon RDS for PostgreSQL）。Oracle

AWS 当你为目录启用合规性时，Microsoft AD 已获准用于 AWS 云端应用程序，这些应用程序必须符合《美国健康保险流通与责任法案》(HIPAA) 或支付卡行业数据安全标准 (PCI DSS) 合规性。

所有兼容的应用程序都使用您存储在 AWS 托管 Microsoft AD 中的用户证书，或者您可以通过信任连接到现有 AD 基础设施，并使用来自本地或 EC2 Windows 上Active Directory运行的凭证。如果您将 EC2 实例加入您的 AWS 托管 Microsoft AD，则您的用户可以访问 AWS 云端中的 Windows 工作负载，享受与访问本地网络中的工作负载时相同的 Windows 单点登录 (SSO) 体验。

AWS 托管 Microsoft AD 还支持使用Active Directory凭据的联合用例。仅凭 AWS 托管 Microsoft AD，你就可以登录AWS Management Console。借AWS IAM Identity Center助，您还可以获取与 AWS SDK 和 CLI 配合使用的短期凭证，并使用预配置的 SAML 集成登录许多云应用程序。通过添加Microsoft Entra Connect（以前称为Azure Active Directory Connect）和可选的Active Directory 联合身份验证服务 (AD FS)，您可以使用存储在 AWS 托管 Microsoft AD 中的凭据登录和其他云应用程序。Microsoft Office 365

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。您还可以为AWS 托管 Microsoft AD 启用多因素身份验证 (MFA)，以便在用户从互联网 AWS 访问应用程序时提供额外的安全保护。由于Active Directory是 LDAP 目录，因此您还可以将 AWS 托管 Microsoft AD 用于 Linux 安全外壳 (SSH) 身份验证和其他支持 LDAP 的应用程序。

AWS 作为服务的一部分提供监控、每日快照和恢复，您可以向托管 Microsoft AD 添加用户和群组，并使用在加入托管 M AWS icrosof AWS t AD 域的Windows计算机上运行的熟悉Active Directory工具管理组策略。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。

AWS 托管 Microsoft AD 有两个版本可供选择：标准版和企业版。

- 标准版：AWS Managed Microsoft 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：AWS Managed Microsoft 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

AWS 如果您需要实际Active Directory功能来支持 AWS 应用程序或Windows工作负载（包括适用于 Amazon Relational Database Service）的应用程序或工作负载，那么托管 Microsoft AD 是您的最佳选择Microsoft SQL Server。如果你想要一个支持 Office 365 的独立Active Directory AWS 云端，或者你需要一个 LDAP 目录来支持你的 Linux 应用程序，那也是最好的。有关更多信息，请参阅 AWS 微软 AD 托管。

AD Connector

AD Connector 是一项代理服务，它提供了一种将兼容的 AWS 应用程序（例如亚马逊 WorkSpaces QuickSight、亚马逊和亚马逊 EC2）连接到您现有的本地应用程序的简便方法MicrosoftActive Directory。Windows Server使用 AD Connector，您只需向自己的服务帐户添加一个服务帐户即可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。

当您将用户添加到诸如 Amazon 之类的 AWS 应用程序时 QuickSight，AD Connector 会读取您的现有用户和群组Active Directory以创建可供选择的用户和群组列表。当用户登录 AWS 应用程序时，AD Connector 会将登录请求转发给您的本地Active Directory域控制器进行身份验证。AD Connector 可与许多 AWS 应用程序和服务配合使用，包括亚马逊 WorkSpaces WorkDocs、亚马逊 QuickSight、亚马逊Chime、Ama zon Connect 和亚马逊。 WorkMail您还可以使用无缝Active Directory域加入通过 AD Connector 将您的 EC2 Windows 实例加入您的本地域。AD Connector

还允许您的用户使用现有Active Directory凭证登录来访问和管理 AWS 资源。 AWS Management Console AD Connector 与 RDS SQL Server 不兼容。

您还可以使用 AD Connector AWS 为您的应用程序用户启用多因素身份验证 (MFA)，方法是将其连接到现有的基于 RADIUS 的 MFA 基础架构。这在用户访问 AWS 应用程序时提供了一个额外的安全层。

使用 AD Connector，您可以Active Directory像现在一样继续管理自己的。例如，您可以在本地使用标准Active Directory管理工具添加新用户和群组并更新密码Active Directory。无论用户是在本地还是 AWS 云端访问资源，这都有助于您始终如一地强制执行安全策略，例如密码过期、密码历史记录和帐户锁定。

何时使用

当您想将现有本地目录与兼容 AWS 服务一起使用时，AD Connector 是您的最佳选择。有关更多信息，请参阅 AD Connector。

Simple AD

Simple AD 是一个MicrosoftActive Directory由 AWS Directory Service Samba 4 提供支持的兼容目录。Simple AD 支持基本Active Directory功能，例如用户账户、群组成员资格、加入 Linux 域或Windows基于 EC2 的实例、基于 Kerberos 的 SSO 和群组策略。 AWS 作为服务的一部分，提供监控、每日快照和恢复。

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Active Directory的熟悉的应用程序和工具。Simple AD 与以下 AWS 应用程序兼容：亚马逊 WorkSpaces、亚马逊 WorkDocs QuickSight、亚马逊和亚马逊 WorkMail。您还可以使用 Simple AWS Management Console AD 用户帐户登录并管理 AWS 资源。

Simple AD 不支持多因素身份验证 (MFA)、信任关系、DNS 动态更新、架构扩展、通过 LDAPS 的通信、AD cmd PowerShell let 或 FSMO 角色转移。Simple AD 与 RDS SQL Server 不兼容。需要实际MicrosoftActive Directory功能或计划在 RDS SQL Server 中使用其目录的客户应改用 AWS 托管 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

您可以将 Simple AD 用作云中的独立目录，以支持需要基本Active Directory功能Windows的工作负载、兼容的 AWS 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 AD。

Amazon Cognito

Amazon Cognito 是一种用户目录，它使用 Amazon Cognito 用户池向移动应用程序或 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，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。

有关各个区域支持的目录类型列表，请参阅 的地区可用性 AWS Directory Service。

使用 Amazon EC2

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

- 什么是亚马逊 EC2？ 在 Amazon EC2 用户指南中。
- 在 Ama zon EC2 用户指南中启动 EC2 实例。
- Amazon EC2 用户指南中的@@ 安全组。
- 《Amazon VPC 用户指南》中的 Amazon VPC 是什么？
- 《Amazon VPC 用户指南》中的在您的 VPC 中添加硬件虚拟私有网关。

入门 AWS Directory Service

如果您尚未这样做，则还需要创建一个 AWS 帐户并使用该 AWS Identity and Access Management 服务来控制访问权限。

要使用 AWS Directory Service，你需要满足微软 Active Directory、AD Connector 或 Simple AD 的 AWS 目录服务的先决条件。有关更多信息，请参阅 AWS 微软 AD 托管先决条件、AD Connector 先决条件 或 Simple AD 先决条件。

注册获取 AWS 账户

如果您没有 AWS 账户，请完成以下步骤来创建一个。

要注册 AWS 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，将接到一通电话，要求使用电话键盘输入一个验证码。

   当您注册时 AWS 账户，就会创建AWS 账户根用户一个。根用户有权访问该账户中的所有 AWS 服务 和资源。作为安全最佳实践，应为用户分配管理访问权限，并仅使用 root 用户来执行需要 root 用户访问权限的任务。

AWS 注册过程完成后会向您发送一封确认电子邮件。在任何时候，您都可以通过转至 https://aws.amazon.com/ 并选择我的账户来查看当前的账户活动并管理您的账户。

创建具有管理权限的用户

注册后，请保护您的安全 AWS 账户 AWS 账户根用户 AWS IAM Identity Center，启用并创建管理用户，这样您就不会使用 root 用户执行日常任务。

保护你的 AWS 账户根用户

1. 选择 Root 用户并输入您的 AWS 账户 电子邮件地址，以账户所有者的身份登录。AWS Management Console在下一页上，输入您的密码。

   要获取使用根用户登录方面的帮助，请参阅《AWS 登录 用户指南》中的以根用户身份登录。

2. 为您的根用户启用多重身份验证 (MFA)。

   有关说明，请参阅 I A M 用户指南中的为 AWS 账户 根用户启用虚拟 MFA 设备（控制台）。

创建具有管理权限的用户

1. 启用 IAM Identity Center

   有关说明，请参阅《AWS IAM Identity Center 用户指南》中的启用 AWS IAM Identity Center。

2. 在 IAM 身份中心中，向用户授予管理访问权限。

   有关使用 IAM Identity Center 目录 作为身份源的教程，请参阅《用户指南》 IAM Identity Center 目录中的使用默认设置配置AWS IAM Identity Center 用户访问权限。

以具有管理权限的用户身份登录

- 要使用您的 IAM Identity Center 用户身份登录，请使用您在创建 IAM Identity Center 用户时发送到您的电子邮件地址的登录网址。

  有关使用 IAM Identity Center 用户登录的帮助，请参阅AWS 登录 用户指南中的登录 AWS 访问门户。

为其他用户分配访问权限

1. 在 IAM Identity Center 中，创建一个遵循应用最低权限权限的最佳实践的权限集。

   有关说明，请参阅《AWS IAM Identity Center 用户指南》中的创建权限集。

2. 将用户分配到群组，然后为该群组分配单点登录访问权限。

   有关说明，请参阅《AWS IAM Identity Center 用户指南》中的添加群组。

更多信息

- 有关如何以 IAM 身份中心用户身份登录的更多信息，请参阅登录 IAM 身份中心访问门户。 AWS Management Console
- 有关如何以 IAM 用户 AWS Management Console 身份登录的更多信息，请参阅以 I AM 用户 AWS Management Console 身份登录。

- 有关使用 IAM 策略控制 AWS Directory Service 资源访问权限的更多信息，请参阅使用基于身份的策略（IAM 策略）AWS Directory Service。

AWS 微软 AD 托管

AWS Directory Service 允许您作为托管服务运行 Microsoft Active Directory (AD)。 AWS 微软 Active Directory 的目录服务，也称为 AWS 托管微软 AD，由 Windows Server 2019 提供支持。当您选择并启动此目录类型时，它会被创建为一对连接到您的虚拟私有云 (Amazon VPC) 的高可用性域控制器。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。

借助 AWS 托管 Microsoft AD，你可以在 AWS 云中运行目录感知型工作负载，包括基于.NET Microsoft SharePoint 和 SQL Server 的自定义应用程序。您还可以使用配置 AWS 云端 AWS 托管 Microsoft AD 与您的现有本地部署之间的信任关系 MicrosoftActive Directory，为用户和群组提供对任一域中资源的访问权限 AWS IAM Identity Center。

AWS Directory Service 可以轻松地在 AWS 云中设置和运行目录，或者将您的 AWS 资源与现有的本地资源连接起来MicrosoftActive Directory。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 AWS 托管 Microsoft AD 与现有的基于 RADIUS 的 MFA 基础架构集成，从而在用户访问应用程序时提供额外的安全保护，从而实现多因素身份验证 AWS
- 安全连接亚马逊 EC2 Linux 和Windows实例

> **Note**
>
> AWS 为您管理Windows服务器实例的许可；您所需要做的就是为您使用的实例付费。您也无需购买额外的 Windows Server 客户端访问许可证（CAL），因为价格中已包含访问权限。每个实例都有两个仅用于管理的远程连接。如果您需要两个以上的连接，或者需要这些连接用于管理以外的用途，则可能需要引入额外的远程桌面服务 CAL 才能在 AWS上使用。

阅读本节的主题，开始创建托管的 Microsoft AD 目录，在 AWS 托管的 Microsoft AD 和你的本地目录之间 AWS 创建信任关系，以及扩展你的 AWS 托管微软 AD 架构。

主题

- 微软 AD AWS 托管入门
- AWS Managed Microsoft AD 的主要概念
- Microsoft AD AWS 托管最佳实践
- Microsoft AWS 托管 AD 的用例
- 如何 AWS 管理托管 Microsoft AD
- AWS 托管微软 AD 配额
- AWS 托管 Microsoft AD 的应用程序兼容性
- AWS 微软 AD 托管测试实验室教程
- 微软 AD AWS 托管故障排除

相关 AWS 安全博客文章

- 如何将托 AWS 管 Microsoft AD 目录的管理委托给您的本地 Active Directory 用户
- 如何使用 AWS 托管 Microsoft AD 来配置更严格的密码策略 AWS Directory Service 以帮助满足你的安全标准
- 如何通过添加域控制器来提高 AWS 托管 Microsoft AD 的冗余和性能 AWS Directory Service
- 如何通过在 AWS 托管的 Microsoft AD 上部署 Microsoft 远程桌面许可管理器来启用远程桌面的使用
- 如何 AWS Management Console 使用 AWS 托管 Microsoft AD 和您的本地凭据进行访问
- 如何使用 AWS 托管 Microsoft AD 和本地凭据为 AWS 服务启用多因素身份验证
- 如何使用本地 Active Directory 轻松登录 AWS 服务

微软 AD AWS 托管入门

AWS Managed Microsoft AD 创建了一个完全托管的，Microsoft Active Directory由 Windows Server 2019 提供支持，在 2012 年 R2 Forest 和 Domain 功能级别上运行。 AWS Cloud 当你使用 AWS 托管 Microsoft AD AWS Directory Service 创建目录时，会创建两个域控制器并代表你添加 DNS 服务。域控制器在 Amazon VPC 的不同子网中创建，这种冗余有助于确保即使发生故障也能访问您的目录。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。

主题

- AWS 微软 AD 托管先决条件
- 创建你的 Microsoft AWS 托管广告

- 用你的 AWS 托管 Microsoft AD 活动目录创建了什么
- 管理员账户的权限

AWS 微软 AD 托管先决条件

要创建 AWS 托管 Microsoft ADActive Directory，您需要一个具有以下内容的亚马逊 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。
- 您无法使用 198.18.0.0/15 地址空间中的地址在 VPC 中创建 AWS 托管 Microsoft AD。

如果你需要将你的 Microsoft AD AWS 托管域与现有的本地Active Directory域集成，则必须将本地域的森林和域功能级别设置为 Windows Server 2003 或更高版本。

AWS Directory Service 使用双 VPC 结构。构成您目录的 EC2 实例在您的 AWS 账户之外运行，由管理 AWS。其有 `ETH0` 和 `ETH1` 两个网络适配器。`ETH0` 是管理适配器，存在于您的账户之外。`ETH1` 在您的账户内创建。

您目录的 ETH0 网络的管理 IP 范围是 198.18.0.0/15。

AWS IAM Identity Center 先决条件

如果您计划将 IAM 身份中心与 AWS 托管 Microsoft AD 一起使用，则需要确保满足以下条件：

- 你的 Microsoft AD AWS 托管目录是在你 AWS 组织的管理账户中设置的。
- 您的 IAM 身份中心实例位于设置 AWS 托管 Microsoft AD 目录的同一区域。

有关更多信息，请参阅 AWS IAM Identity Center 用户指南中的 IAM 身份中心先决条件。

多重身份验证先决条件

要支持对 AWS 托管 Microsoft AD 目录进行多因素身份验证，必须按以下方式配置本地或基于云的远程身份验证拨入用户服务 (RADIUS) 服务器，使其能够接受来自托管 AWS Microsoft AD 目录的请求。AWS

1. 在你的 RADIUS 服务器上，创建两个 RADIUS 客户端来代表中的 AWS两个 AWS 托管 Microsoft AD 域控制器 (DC)。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 AWS 托管 Microsoft AD DC 的 DNS 地址。这两个 DNS 地址都可以在你计划使用 MFA 的 AWS 托管 Microsoft AD 目录的详细信息页面的目录服务控制台中找到。 AWS 显示的 DNS 地址代表使用的两个 AWS 托管 Microsoft AD DC 的 IP 地址。 AWS

  > **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 AWS Managed Microsoft AD DC 都创建一个 RADIUS 客户端配置。

- 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。
- 共享密钥：键入或生成将由 RADIUS 服务器用于与 RADIUS 客户端连接的共享密钥。
- 协议：你可能需要在 AWS 托管的 Microsoft AD DC 和 RADIUS 服务器之间配置身份验证协议。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（AWS 托管的 Microsoft AD DC 的 DNS 地址，参见步骤 1）到您的 RADIUS 服务器端口的入站流量。
3. 在您的 AWS 托管 Microsoft AD 域中的 Amazon EC2 安全组中添加一条规则，允许来自之前定义的 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《EC2 用户指南》中的向安全组添加规则。

有关将 AWS 托管 Microsoft AD 与 MFA 配合使用的更多信息，请参阅。为 AWS 托管的 Microsoft AD 启用多因素身份验证

创建你的 Microsoft AWS 托管广告

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AWS 微软 AD 托管先决条件中确定的先决条件。

创建微软 AD AWS 托管目录

1. 在 AWS Directory Service 控制台导航窗格中，选择目录，然后选择设置目录。
2. 在选择目录类型页面上，选择 AWS Managed Microsoft 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 AWS 托管 Microsoft AD 的标准版或企业版中进行选择。有关版本的更多信息，请参阅 AWS Directory Service for Microsoft Active Directory。

目录 DNS 名称

目录的完全限定名称，例如 `corp.example.com`。

> **Note**
>
> 如果您计划使用亚马逊 Route 53 进行 DNS，则您的 AWS 托管 Microsoft AD 的域名必须与您的 Route 53 域名不同。如果 Route 53 和 AWS 托管 Microsoft AD 共享相同的域名，则可能会出现 DNS 解析问题。

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。

   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。

用你的 AWS 托管 Microsoft AD 活动目录创建了什么

当你使用 AWS 托管 Microsoft AD 创建活动目录时， AWS Directory Service 会代表你执行以下任务：

- 自动创建弹性网络接口（ENI）并将其与每个域控制器相关联。这些 ENI 中的每一个 ENI 对于您的 VPC 和 AWS Directory Service 域控制器之间的连接都是必不可少的，因此切勿删除。您可以 AWS Directory Service 通过描述来标识所有保留供使用的网络接口：“为目录目录 ID AWS 创建的网络接口”。有关更多信息，请参阅 Amazon EC2 用户指南中的弹性网络接口。 AWS 托管 Microsoft AD 的默认 DNS 服务器Active Directory是无类域间路由 (CIDR) +2 的 VPC DNS 服务器。有关更多信息，请参阅亚马逊 VPC 用户指南中的亚马逊 DNS 服务器。

  > **Note**
  >
  > 默认情况下，域控制器部署在一个地区的两个可用区中，并连接到您的 Amazon VPC (VPC)。每天自动备份一次，并对 Amazon EBS (EBS) 卷进行加密，以确保静态数据的安全。出现故障的域控制器会在同一可用区中使用相同的 IP 地址自动替换，并且可以使用最新的备份执行完全灾难恢复。

- 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。

> **Note**
>
> AWS 不允许在 AWS 托管的 Microsoft AD 域控制器上安装监控代理。

- 创建 AWS 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 或实例连接到已创建 AWS 的安全组。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，因为流向域控制器的流量仅限于来自您的 VPC、其他对等 VPC 或您使用 Transit AWS Direct Connect Gat AWS eway 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，唯一可以与您的 AWS 托管 Microsoft AD 通信的入站流量是本地 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。有关更多信息，请参阅 Microsoft AD AWS 托管最佳实践。默认情况下会创建以下 AWS 安全组规则：

  入站规则

协议	端口范围	来源	流量的类型	Active Directory 使用情况
ICMP	不适用	0.0.0.0/0	Ping	LDAP 保持活动，DFS
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

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

出站规则

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

- 有关 Active Directory 使用的端口和协议的更多信息，请参阅 Microsoft 文档中的 Windows 服务概述和网络端口要求。
- 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)。您可以使用此帐户来管理您在 AWS 云端的目录。有关更多信息，请参阅 管理员账户的权限。

> **Important**
>
> 请务必保存此密码。 AWS Directory Service 不存储此密码，也无法找回。但是，您可以通过 AWS Directory Service 控制台或使用 ResetUserPasswordAPI 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
AWS 委托组	存储所有可用于向用户委派 AWS 特定权限的群组。
AWS 已保留	存储所有特定于 AWS 管理的账户。
<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 归所有 AWS 并包含您所有 AWS相关的目录对象，您被授予对这些对象的完全控制权。默认情况下，此 OU 下存在两个子 OU：Computers 和 Users。例如： • Corp

OU 名称	描述
	• Computers • 用户

- 在 AWS 授权群组 OU 中创建以下群组：

组名	描述
AWS 委托账户操作员	此安全组的成员拥有有限的账户管理能力，如密码重置
AWS 基于活动目录的授权激活管理员	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。
AWS 委派向域用户添加工作站	此安全组的成员可将 10 台计算机加入域中。
AWS 委派的管理员	该安全组的成员可以管理 AWS 托管的 Microsoft AD，完全控制组织单位中的所有对象，并可以管理 AWS 委派组 OU 中包含的群组。
AWS 已授权允许对对象进行身份验证	该安全组的成员能够对 AWS 预留 OU 中的计算机资源进行身份验证（仅启用了选择性身份验证的本地对象信任才需要）。
AWS 已授权允许向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）。
AWS 委派的已删除对象生命周期管理员	该安全组的成员可以修改 MSD-DeletedObjectLifetime 对象，该对象定义了已删除的对象可以从 AD 回收站中恢复多长时间。
AWS 委派的分布式文件系统管理员	此安全组的成员可以添加和删除 FRS、DFS-R 和 DFS 命名空间。

组名	描述
AWS 委派域名系统管理员	此安全组的成员可以管理与 Active Directory 集成的 DNS。
AWS 委派的动态主机配置协议管理员	此安全组的成员可以对企业中的 Windows DHCP 服务器进行授权。
AWS 委派的企业证书颁发机构管理员	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。
AWS 委派精细密码策略管理员	此安全组的成员可以修改预先创建的精细密码策略。
AWS 已授权的 FSx 管理员	此安全组的成员可以管理 Amazon FSx 资源。
AWS 委派组策略管理员	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）。
AWS 委派的 Kerberos 委派管理员	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。
AWS 委派的托管服务账户管理员	此安全组的成员可以创建和删除托管服务账户。
AWS 委托的 MS-NPRC 不合规设备	该安全组的成员将被排除在与域控制器进行安全通道通信的要求之外。此组适用于计算机账户。
AWS 委派的远程访问服务管理员	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。
AWS 委派的复制目录更改管理员	该安全组的成员可以将 Active Directory 中的配置文件信息与 SharePoint 服务器同步。
AWS 委派服务器管理员	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。
AWS 委派站点和服务管理员	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。

组名	描述
AWS 委派的系统管理管理员	此安全组的成员可以创建和管理系统管理容器中的对象。
AWS 委派的终端服务器许可管理员	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。
AWS 委派用户主体名称后缀管理员	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、修改这些 GPO 或取消其链接。这是设计使然，因为它们是保留供 AWS 使用的。如果需要，可以将它们链接到您控制的 OU。

组策略名称	适用于	描述
默认域策略	域	包括域密码和 Kerberos 策略。
ServerAdmins	所有非域控制器计算机账户	将 “AWS 委派服务器管理员” 添加为 BUILTIN\ Administrators 组的成员。
AWS 保留政策：用户	AWS 保留的用户账户	为 AWS 预留 OU 中的所有用户账户设置推荐的安全设置。
AWS 托管活动目录政策	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)。

组策略名称	适用于	描述
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	在创建域时进行配置，使用 AWS 托管 Active Directory 策略代替它。

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

管理员账户的权限

在为 Microsoft A AWS ctive Directory 目录 AWS 创建目录服务时，会创建一个组织单位 (OU) 来存储所有 AWS 相关的群组和帐户。有关此 OU 的更多信息，请参阅 用你的 AWS 托管 Microsoft AD 活动目录创建了什么。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 AWS Managed Microsoft AD 中管理用户和组。
- 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 委托 AWS Managed Microsoft AD 的目录加入权限。
- 创建和链接组策略。
- 从 Active Directory 回收站还原删除的对象。
- 在活动目录 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。
- 配置 Kerberos 约束委托。有关更多信息，请参阅 Kerberos 约束委托。

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**
>
> AWS 域管理员对托管的所有域拥有完全的管理权限 AWS。有关如何 AWS 处理存储在 AWS 系统上的内容（包括目录信息）的更多信息，请参阅您的协议 AWS 和AWS 数据保护常见问题解答。

> **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账户

AWS 每 90 天自动将内置管理员密码轮换为随机密码。每当要求使用内置的管理员密码供人类使用时，系统都会创建一张 AWS 票证并记录在 AWS Directory Service 团队中。账户凭证通过安全通道进行经过加密和处理。此外，管理员账户凭证只能由 AWS Directory Service 管理团队申请。

要对您的目录进行操作管理， AWS 必须拥有对具有企业管理员和域管理员权限的帐户的独占控制权。这包括对 Active Directory 管理员帐户的独家控制权。 AWS 通过使用密码库自动管理密码，从而保护此帐户。在管理员密码的自动轮换过程中， AWS 创建一个临时用户帐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。 AWS 成功轮换管理员密码后， AWS 删除临时管理员帐户。

通常完全通过自动化 AWS 操作目录。如果自动化过程无法解决操作问题，则 AWS 可能需要让支持工程师登录您的域控制器 (DC) 进行诊断。在这些极少数情况下，会 AWS 实施请求/通知系统来授予访问权限。在此过程中， AWS 自动化会在您的目录中创建一个具有域管理员权限的限时用户帐户。 AWS 将用户帐户与被指派处理您的目录的工程师相关联。 AWS 将这种关联记录在我们的日志系统中，并为工程师提供要使用的凭据。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。此功能使您能够将 AD Security 事件转发到您的 CloudWatch系统，在那里您可以实施监控解决方案。有关更多信息，请参阅 启用日志转发。

当有人以交互方式登录到 DC 时，系统会记录安全事件 ID 4624、4672 和 4648。可以在已加入域的 Windows 计算机上使用事件查看器 Microsoft 管理控制台（MMC）查看每个 DC 的 Windows 安全事件日志。您也可以将所有安全事件日志发送启用日志转发到您账户中的 CloudWatch Logs。

您可能偶尔会看到在 AWS 预留 OU 中创建和删除了用户。 AWS 负责管理此 OU 以及我们未向您委托访问和管理权限的任何其他 OU 或容器中所有对象的管理和安全。您可能会看到该 OU 中创建和删除的内容。这是因为 AWS Directory Service 使用自动化来定期轮换域管理员密码。轮换密码时会创建备份，以防轮换失败。轮换成功后，备份账户会自动删除。此外，在极少数情况下，需要在 DC 上进行交互式访问以进行故障排除，则会创建一个临时用户帐户供 AWS Directory Service 工程师使用。工程师完成工作后，临时用户账户将被删除。请注意，每次为目录请求交互式凭证时，都会通知 AWS Directory Service 管理团队。

AWS Managed Microsoft AD 的主要概念

如果您熟悉以下主要概念，将能够更充分地利用 AWS Managed Microsoft AD。

主题

- Active Directory 架构
- AWS Managed Microsoft AD 的修补和维护
- 组托管服务账户
- Kerberos 约束委托

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 AWS Managed Microsoft AD 架构的过程之前务必要了解的架构元素的相关详细信息。

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

- 何时扩展 AWS Managed Microsoft AD 架构
- 教程：扩展你的 AWS 托管 Microsoft AD 架构

AWS Managed Microsoft AD 的修补和维护

AWS Directory Service for Microsoft Active Directory 也称作 AWS DS for AWS Managed Microsoft 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 2019 作为域控制器（DC），AWS 向 DC 添加软件来用于服务管理目

的。AWS 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。您可以选择添加 DC 以进一步提高可用性。对于需要高可用性和容错能力的关键环境，我们建议部署更多 DC。 AWS按顺序修补您的 DC，在此期间，AWS正在进行修补的 DC 不可用。如果您的一个或多个 DC 暂时停止服务，AWS 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，AWS 使用了 Microsoft 更新。Microsoft 每月为 Windows Server 提供汇总补丁，这使得 AWS 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，AWS 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，AWS 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 AWS Managed Microsoft AD 中的用户可以创建 gMSA，您必须将其账户添加作为 AWS 托管服务账户委托管理员安全组的成员。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 网站上的群组托管服务帐户概述。 TechNet

相关的 AWS 安全博客文章

- AWS 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

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 使用应用权限的服务帐户凭据（而不是 jsmith 配置 hr-app-service的权限）打开数据库连接。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。为此，您可以在中的托管 AWS Microsoft AD 目录中为 hr-app-service 服务帐户启用 Kerberos 受限委托。AWS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 委托使该 hr-app-service 账户能够在访问数据库时重复使用 jsmith Kerberos 票证，从而在打开数据库连接时应用特定于 jsmith 的权限。

要授予权限，允许 AWS Managed Microsoft AD 中的用户配置 Kerberos 约束委托，您必须将其账户添加为 AWS Kerberos 委托管理员安全组的成员。默认情况下，管理员账户是该组的成员。有关 Kerberos 受限委派的更多信息，请参阅 Microsoft 网站上的 Kerberos 约束委派概述。 TechNet

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。

Microsoft AD AWS 托管最佳实践

以下是一些建议和指南，你应该考虑这些建议和指导方针，以避免出现问题并充分利用 AWS 托管 Microsoft AD。

设置：先决条件

创建目录之前请考虑以下这些准则。

验证目录类型是否正确

AWS Directory Service 提供了多种与其他 AWS 服务Microsoft Active Directory配合使用的方式。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：

- AWS 微软目录服务 Active Directory 是一款托管在云端的功能丰富的Microsoft Active Directory托管服务。 AWS AWS 如果您拥有超过 5,000 个用户，并且需要在托管目录和本地目录之间建立信任关系，那么 AWS 托管 Microsoft AD 是您的最佳选择。
- AD Con nector 只需将您的现有本地环境连接Active Directory到 AWS。当您想要将现有本地目录与 AWS 服务一起使用时，AD Connector 是您的最佳选择。
- S@@ imple AD 是一个低规模、低成本的目录，具有基本Active Directory兼容性。其支持 5000 个或更少的用户、兼容 Samba 4 的应用程序，并支持 LDAP 感知型应用程序的 LDAP 兼容性。

有关 AWS Directory Service 选项的更详细比较，请参阅选择哪一个。

确保 VPC 和实例正确配置

要连接到、管理和使用目录，必须正确配置目录所关联的 VPC。有关 VPC 安全和网络要求的信息，请参阅 AWS 微软 AD 托管先决条件、AD Connector 先决条件 或 Simple AD 先决条件。

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 Amazon EC2 实例加入您的 AWS 托管微软 AD Active Directory 中所述。

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可以存储在目录中的对象数量的唯一限制。有关所选目录的详细信息，请参阅 AWS 托管微软 AD 配额、AD Connector 配额 或 Simple AD 限额。

了解目录 AWS 的安全组配置并使用

AWS 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，并允许 Active Directory 通信所必需的流量通过。 AWS 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，安全组接受来自任意 IP 地址到这些端口的流量。 AWS 将安全组附加到您的域控制器的接口，这些接口可从您的对等或调整大小的 VPC 中进行访问。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《Amazon EC2 用户指南》中的适用于 Linux 实例的 Amazon EC2 安全组。不当的更改可能会导致与目标计算机和实例的通信中断。 AWS 建议您不要尝试为域控制器打开其他端口，因为这会降低目录的安全性。请仔细查看 AWS 责任共担模型。

> **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， AWS 建议不要这样做。 AWS 可能有理由在不另行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。该帐户 ID 是 AWS 托管 Microsoft AD 的管理员。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

我们建议您为 AWS Directory Service 目录创建 DHCP 选项集，然后将 DHCP 选项集分配给您的目录所在的 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 创建或更改 DHCP 选项集。

启用条件转发器设置

以下条件转发设置将此条件转发器存储在 Active Directory 中，按如下方式复制：应启用。启用这些设置将防止由于基础架构故障或过载故障而更换节点时，条件转发器设置消失。

部署额外的域控制器

默认情况下， AWS 创建两个存在于不同可用区域中的域控制器。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。

了解 AWS 应用程序的用户名限制

AWS Directory Service 支持大多数可用于构造用户名的字符格式。但是，对于用于登录 AWS 应用程序（例如亚马逊、亚马逊或亚马 QuickSight逊 WorkDocs）的用户名 WorkSpaces，有一些字符限制。WorkMail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。

不要更改预定义用户、组和组织单位

使用 AWS Directory Service 启动目录时， AWS 会创建一个包含目录中所有对象的组织单元 (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。域根由所有和管理 AWS。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。这样做会使您自己和 AWS您的目录都无法访问。有关更多信息，请参阅 用你的 AWS 托管 Microsoft AD 活动目录创建了什么。

自动加入域

启动要成为 AWS Directory Service 域一部分的 Windows 实例时，通常最简单的方法是将域作为实例创建过程的一部分加入该域，而不是稍后手动添加实例。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。可以在将亚马逊 EC2 Windows 实例无缝加入你的 AWS 托管微软 AD Active Directory 中找到详细信息。

正确设置信任

在你的 Microsoft AD AWS 托管目录与其他目录之间设置信任关系时，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。

管理目录

请考虑以下用于管理目录的建议。

跟踪您的域控制器性能

为了帮助优化扩展决策并提高目录弹性和性能，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。

有关如何使用控制 CloudWatch 台设置域控制器指标的说明，请参阅 AWS 安全博客中的如何根据利用率指标自动扩展 Microsoft AD AWS 托管。

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 扩展架构。

关于负载均衡器

请勿在 AWS 托管 Microsoft AD 端点前使用负载平衡器。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 Microsoft 上的负载平衡器和 Active Directory TechNet ，其中建议修复应用程序以正确使用 Active Directory，而不是实现外部负载均衡器。

创建实例的备份

如果您决定手动向现有 AWS Directory Service 域中添加实例，请先对该实例进行备份或拍摄快照。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 为目录拍摄快照或还原目录。

设置 SNS 消息收发

通过 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 状态变为 Impaired 或 Inoperable 状态，您将收到通知。当目录恢复为“活动”状态时，您也会收到通知。

另请记住，如果您有一个 SNS 主题接收来自的消息 AWS Directory Service，则在从 Amazon SNS 控制台删除该主题之前，应将您的目录与其他 SNS 主题相关联。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 使用 Amazon SNS 配置目录状态通知。

应用目录服务设置

AWS 托管 Microsoft AD 允许你定制安全配置，以满足你的合规和安全要求。 AWS Microsoft AD 会将配置部署并维护到您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。您可以按照编辑目录安全设置或通过 UpdateSettings API 中的步骤在控制台中执行此操作。

有关更多信息，请参阅 配置目录安全设置。

在删除目录之前删除 Amazon Enterprise 应用程序

在删除与一个或多个亚马逊企业应用程序（如亚马逊 WorkSpaces 应用程序管理器、亚马逊 WorkSpaces、亚马逊或亚马逊 WorkDocs关系数据库服务 (A WorkMail mazon RDS)）关联的目录之前，必须先删除每个应用程序。 AWS Management Console有关如何删除这些应用程序的更多信息，请参阅删除你的 Microsoft AWS 托管广告。

使用 SMB 2.x 客户端来访问 SYSVOL 和 NETLON 共享

客户端计算机使用服务器消息块 (SMB) 访问托管的 M AWS icrosoft AD 域控制器上的 SYSVOL 和 NETLOGON 共享，以获取组策略、登录脚本和其他文件。 AWS 托管 Microsoft AD 仅支持 SMB 版本 2.0 (SMBv2) 及更高版本。

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。此更改遵循美国计算机应急准备小组和 Microsoft 的建议禁用了 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。你的目录可以正常工作，但你的 SMBv1 客户端将无法连接到 AWS 托管的 Microsoft AD 域控制器的 SYSVOL 和 NETLOGON 共享，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， AWS 建议您将所有 SMB 服务器和客户机更新为 SMBv2 或更高版本。要了解有关在系统上禁用 SMBv1 并将其更新到较新 SMB 版本的更多信息，请参阅 Microsoft 和文档上的这些帖子。 TechNet Microsoft

跟踪 SMBv1 远程连接

你可以远程查看连接到托管微软 AD 域控制器的微软-Windows-smbServer/Audi AWS t Windows 事件日志，该日志中的任何事件都表明 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。要停止审计 SMB1 访问权限，请使用 Windows PowerShell cmdlet Set-。SmbServerConfiguration

为您的应用程序编程

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 AWS 托管 Microsoft AD 的动态 DNS (DDNS) 服务来定位域控制器 (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。此类情况还可能导致 AWS 目录自动化将目录标记为受损，并可能触发替换无响应的 DC 的恢复进程。

交付生产之前的负载测试

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。

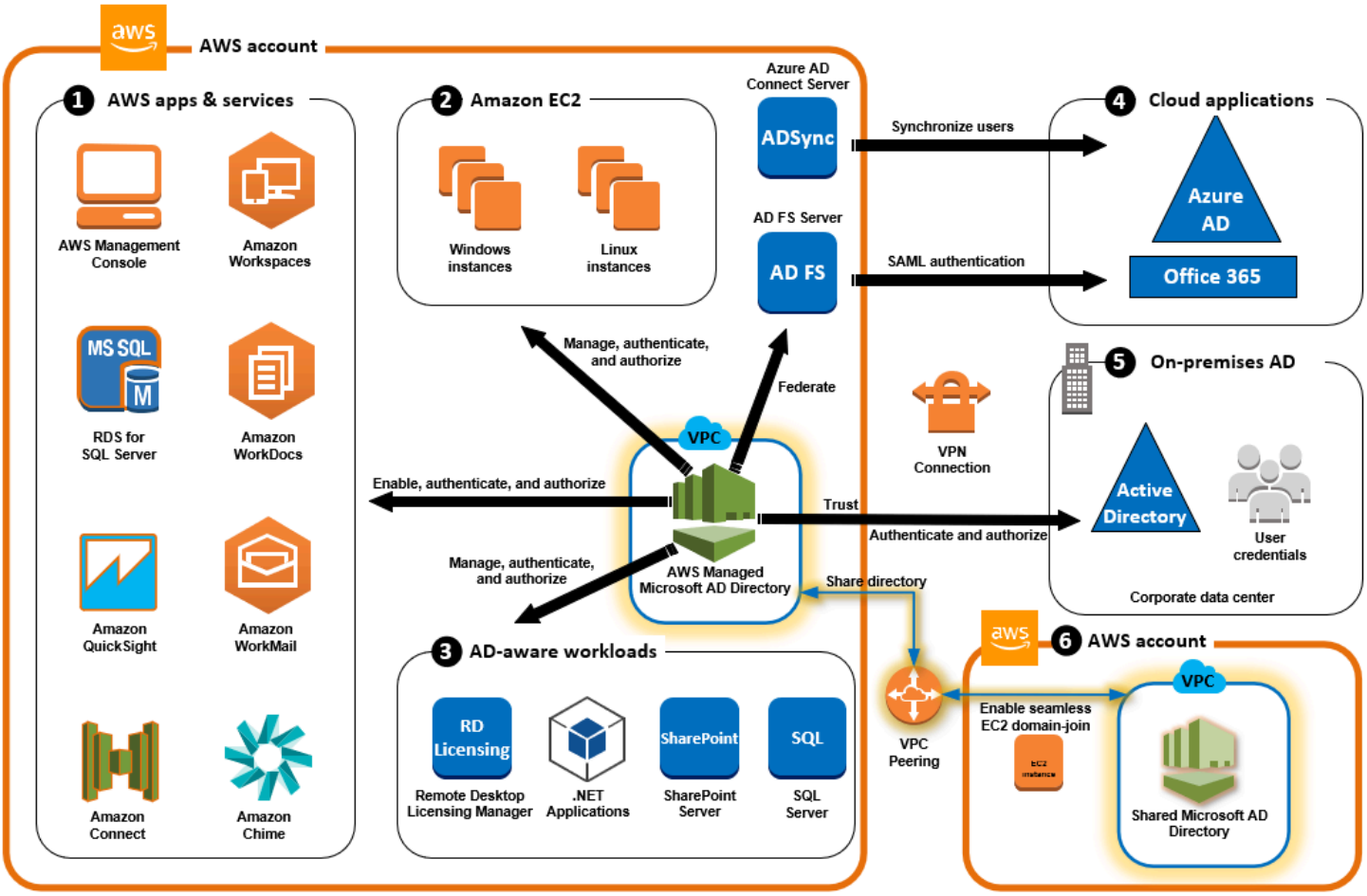
使用高效的 LDAP 查询

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。

Microsoft AWS 托管 AD 的用例

借助 Microsoft AD AWS 托管，你可以为多个用例共享一个目录。例如，您可共享目录以对 .NET 应用程序、启用了 Windows 身份验证的 Amazon RDS for SQL Server 和用于消息收发和视频会议的 Amazon Chime 的访问进行身份验证和授权。

下图显示了你的 Microsoft AD AWS 托管目录的一些用例。其中包括授予用户访问外部云应用程序的权限，并允许您的本地 Active Directory 用户管理和访问 AWS 云中的资源。



将 AWS 托管 Microsoft AD 用于以下任一业务用例。

主题

- 用例 1：使用 Active Directory 凭据登录 AWS 应用程序和服务
- 使用案例 2：管理 Amazon EC2 实例
- 用例 3：为支持 Active Directory 的工作负载提供目录服务
- 用例 4： AWS IAM Identity Center 到 Office 365 和其他云应用程序

- 用例 5：将您的本地 Active Directory 扩展到 AWS 云端
- 用例 6：共享您的目录以跨 AWS 账户将 Amazon EC2 实例无缝加入到域中

用例 1：使用 Active Directory 凭据登录 AWS 应用程序和服务

你可以启用多个 AWS 应用程序和服务，例如、、、Amazon Chime AWS Client VPNAWS Management ConsoleAWS IAM Identity Center、Amazon C onnect、亚马逊 FSx、亚马 QuickSight逊、适用于 SQL Server 的亚马逊 RDS、亚马逊 WorkDocs、 WorkMailWorkSpaces亚马逊，也可以使用你的微软 AD AWS 托管目录。当您在目录中启用 AWS 应用程序或服务时，您的用户可以使用其 Active Directory 凭据访问该应用程序或服务。

例如，您可以允许您的用户使用他们的 Active Directory 凭据登录。 AWS Management Console 为此，您可以在目录中启用 AWS Management Console 作为应用程序，然后将您的 Active Directory 用户和群组分配给 IAM 角色。当您的用户登录时 AWS Management Console，他们将扮演 IAM 角色来管理 AWS 资源。这使您可以轻松为您的用户授予对 AWS Management Console 的访问权限，而无需配置和管理单独的 SAML 基础设施。

为了进一步增强最终用户体验，您可以为 Amazon 启用单点登录功能 WorkDocs，这样您的用户无需单独输入凭证即可 WorkDocs 从加入该目录的计算机访问亚马逊。

您可以向您的目录或本地 Active Directory 中的用户账户授予访问权限，这样他们就可以通过直接向现有用户账户分配 IAM 角色来 AWS CLI 使用现有证书和权限登录 AWS Management Console 或管理 AWS 资源。

for Windows File Server for File Server AWS 与托管微软 AD 集成

将适用于 Windows File Server 的 FSx AWS 与托管微软 AD 集成，提供了一个完全托管的基于微软 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。 AWS尽管 FSx for Windows File Server 可以与自托管式 Microsoft Active Directory 集成，但我们在这里不讨论这种情况。

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 与微软 AD AWS 托管用例集成的资源参考。本节中的每个使用案例都从基本的 AWS Managed Microsoft AD 和 FSx for Windows File Server 配置开始。有关如何创建这些配置的更多信息，请参阅：

- 微软 AD AWS 托管入门

- Amazon FSx 入门

FSx for Windows File Server 作为 Windows 容器上的持久性存储。

Amazon Elastic Container Service（ECS）现在支持使用经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)的特殊服务账户支持 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。

相关术语

- 使用 FSx for Windows File Server 作为 Windows 容器上的持久性存储
- 组托管服务账户

亚马逊 AppStream 2.0 支持

Amazon AppStream 2.0 是一项完全托管的应用程序流媒体服务。它为用户提供了一系列通过其应用程序保存和访问数据的解决方案。带有 AppStream 2.0 版本的 Amazon FSx 提供使用 Amazon FSx 的个人永久存储驱动器，并且可以配置为提供用于访问常用文件的共享文件夹。

相关术语

- 演练 4：在亚马逊 2.0 中使用亚马逊 FSx AppStream
- 在亚马逊 2.0 中使用亚马逊 FSx AppStream
- 在 AppStream 2.0 中使用活动目录

Microsoft SQL Server 支持

FSx for Windows File Server 可用作 Microsoft SQL Server 2012（从 2012 版本 11.x 开始）和更新的系统数据库（包括主数据库、模型数据库、MSDB 和 TempDB）以及数据库引擎用户数据库的存储选项。

相关术语

- 安装带有 SMB 文件共享存储的 SQL Server
- 使用 FSx for Windows File Server 简化 Microsoft SQL Server 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 Active Directory 用户主文件夹和“我的文档”中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。

相关术语

- 使用 Amazon FSx 轻松实现 Windows 主目录
- 部署漫游用户配置文件
- 使用适用于 Windows File Server 的 fsX WorkSpaces

网络文件共享支持

FSx for Windows File Server 上的网络文件共享提供了一种托管且可扩展的文件共享解决方案。一个使用案例是可以手动或通过组策略创建的客户端映射驱动器。

相关术语

- 演练 6：使用分片横向扩展性能
- 驱动器映射
- 使用适用于 Windows File Server 的 fsX WorkSpaces

组策略软件安装支持

由于 SYSVOL 文件夹的大小和性能有限，因此最佳做法是避免在该文件夹中存储诸如软件安装文件之类的数据。作为一种可行的解决方案，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。

相关术语

- 使用组策略远程安装软件

Windows Server Backup 目标支持

使用 UNC 文件共享，可以将 FSx for Windows File Server 配置为 Windows Server Backup 中的目标驱动器。在这种情况下，您需要指定 FSx for Windows File Server 的 UNC 路径，而不是附加的 EBS 卷的 UNC 路径。

相关术语

- 对服务器执行系统状态恢复

亚马逊 FSx 还支持托管 AWS 微软 AD 目录共享。有关更多信息，请参阅：

- 共享您的目录
- 在不同的 VPC 或账户中使用带有托 AWS 管微软 AD 的 Amazon FSx

亚马逊 RDS 与 AWS 托管微软 AD 集成

Amazon RDS 支持使用 Kerberos 和 Microsoft Active Directory 对数据库用户进行外部身份验证。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点登录和集中身份验证的好处，以便您将用户凭证保留在 Active Directory。

要开始使用此用例，您首先需要设置基本的微软 AD 和 Amazon RDS AWS 托管配置。

- 微软 AD AWS 托管入门
- Amazon RDS 入门

下面提到的所有用例都将从基本的 AWS 托管微软 AD 和 Amazon RDS 开始，并介绍如何将 Amazon RDS 与 AWS 托管微软 AD 集成。

- 将 Windows 身份验证与 Amazon RDS for SQL Server 数据库实例结合使用
- 对 MySQL 使用 Kerberos 身份验证
- 为 Amazon RDS for Oracle 配置 Kerberos 身份验证
- 在 Amazon RDS for PostgreSQL 中使用 Kerberos 身份验证

亚马逊 RDS 还支持 AWS 托管微软 AD 目录共享。有关更多信息，请参阅：

- 共享您的目录
- Joining your Amazon RDS DB instances across accounts to a single shared domain

有关将 Amazon RDS for SQL Server 加入 Active Directory 的更多信息，请参阅 Join Amazon RDS for SQL Server to your self-managed Active Directory。

.NET 应用程序使用 Amazon RDS for SQL Server 和组托管服务账户

您可以将 Amazon RDS for SQL Server 与基本的 .NET 应用程序和组托管服务账户（gMSA）集成。有关更多信息，请参阅AWS 托管 Microsoft AD 如何帮助简化 Active Directory（集成.NET 应用程序）的部署并提高其安全性

使用案例 2：管理 Amazon EC2 实例

使用熟悉的 Active Directory 管理工具，您可以将 Active Directory 组策略对象 (GPO) 加入您的 AWS 托管微软 AD 域，从而集中管理适用于 Windows 或 Linux 的 Amazon EC2 实例。

此外，您的用户可以使用他们的 Active Directory 凭据登录您的实例。从而无需使用单独的实例凭证或分配私钥 (PEM) 文件。这样，您就可以更轻松地使用已使用的 Active Directory 用户管理工具即时授予或撤消用户访问权限。

用例 3：为支持 Active Directory 的工作负载提供目录服务

AWS Managed Microsoft AD 是一个真正的微软 Active Directory，它使你能够运行传统的 Active Directory 感知工作负载，例如远程桌面许可管理器以及微软和微 SharePoint 软 SQL Server Alway s On in the AWS AWS Microsoft AD 还可以使用组托管服务帐户 (GMSA) 和 Kerberos 受限授权 (KCD) 来帮助您简化和提高集成了 Active Direc tory 的.NET 应用程序的安全性。

用例 4： AWS IAM Identity Center 到 Office 365 和其他云应用程序

你可以使用 AWS 托管 Microsoft AD 来 AWS IAM Identity Center 提供云应用程序。您可以使用Microsoft Entra Connect（以前称为Azure Active Directory Connect）将用户同步到Microsoft Entra（以前称为 Azure Active Directory (AzureAD)），然后使用活动目录联合身份验证服务 (AD FS)，以便您的用户可以使用其活动目录凭据访问微软 Office 365 和其他 SAML 2.0 云应用程序。

将 AWS 托管的 Microsoft AD 与 IAM 身份中心集成可为您的 AWS 托管 Microsoft AD 和/或本地可信域添加 SAML 功能。集成后，您的用户无需配置 SAML 基础设施即可将 IAM 身份中心与支持 SAML 的服务（包括第三方云应用程序，例如 Office 365、Concur 和 Salesforce）一起使用。AWS Management Console 有关允许本地用户使用 IAM Identity Center 的过程的演示，请参阅以下 YouTube 视频。

> **Note**
>
> AWS 单点登录已重命名为 IAM 身份中心。

用例 5：将您的本地 Active Directory 扩展到 AWS 云端

如果你已经有一个 Active Directory 基础架构，并且想在将支持 Active Directory 的工作负载迁移到 AWS 云端时使用它，那么 AWS Microsoft AD 可以提供帮助 你可以使用 A ctive Directory 信任将 AWS 托管 Microsoft AD 连接到你现有的活动目录。这意味着您的用户可以使用其本地 Active Directory 凭据访问支持 Active Directory 的 AWS 应用程序和应用程序，而无需您同步用户、组或密码。

例如，您的用户可以使用他们现有的 Active Directory 用户名和密码登录和亚马逊 WorkSpaces 。AWS Management Console 此外，当你使用支持 Active Directory 的应用程序（例如托管 M AWS icrosoft AD）时，登录的 Windows 用户无需再次输入 SharePoint 凭据即可访问这些应用程序。

您还可以使用 Active Directory 迁移工具包 (ADMT) 和密码导出服务 (PES) 来执行迁移，将本地 Active Directory 域迁移到免除 Active Directory 基础设施的运营负担。 AWS

用例 6：共享您的目录以跨 AWS 账户将 Amazon EC2 实例无缝加入到域中

通过跨多个 AWS 账户共享您的目录，您可以轻松管理诸如 Amazon EC2 之类的 AWS 服务，而无需为每个账户和每个 VPC 操作一个目录。您可以使用任何 AWS 账户中的目录以及 AWS 区域内的任何 Amazon VPC 中的目录。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，您现在可以使用单个 AWS Managed Microsoft AD 目录，轻松管理部署在 EC2 实例中的多个账户和 VPC 中的 Windows 工作负载。

当您与其他 AWS 账户共享您的 AWS 托管 Microsoft AD 目录时，您可以使用亚马逊 EC2 控制台或AWS Systems Manager从账户和 AWS 区域内的任何 Amazon VPC 无缝加入您的实例。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。

如何 AWS 管理托管 Microsoft AD

本节列出了操作和维护 AWS 托管 Microsoft AD 环境的所有步骤。

主题

- 保护 AWS Managed Microsoft AD 目录
- 监控 AWS Managed Microsoft AD
- 多区域复制

- 共享您的目录
- 将 Amazon EC2 实例加入您的 AWS 托管微软 AD Active Directory
- 在 AWS Managed Microsoft AD 中管理用户和组
- Connect 连接到您现有的活动目录基础架构
- 将你的 Microsoft AWS 托管广告连接到 Microsoft Entra Connect Sync
- 扩展架构
- 维护你的 Microsoft AWS 托管 AD 目录
- 授予用户和组对 AWS 资源的访问权限
- 允许访问 AWS 应用程序和服务
- 允许使用 AD 凭证访问 AWS Management Console
- 部署额外的域控制器
- 将用户从 Active Directory 迁移到 AWS Managed Microsoft AD

保护 AWS Managed Microsoft AD 目录

本节介绍了保护 AWS Managed Microsoft AD 环境的注意事项。

主题

- 管理 AWS 托管 Microsoft AD 的密码策略
- 为 AWS 托管的 Microsoft AD 启用多因素身份验证
- 启用安全 LDAP 或 LDAPS
- 管理 AWS 托管微软 AD 的合规性
- 增强 AWS Managed Microsoft AD 网络安全配置
- 配置目录安全设置
- 为 AD 设置 AWS Private CA 连接器

管理 AWS 托管 Microsoft AD 的密码策略

AWS Microsoft AD 托管允许您为在托管 M AWS icrosoft AD 域中管理的用户组定义和分配不同的密码和帐户锁定策略（也称为细粒度密码策略）。创建 AWS 托管 Microsoft AD 目录时，会创建默认域策略并将其应用于Active Directory。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：42 天的最长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。

以下是详细了解MicrosoftActive Directory精细密码策略和安全策略的资源：

- 配置安全策略设置
- 密码复杂性要求
- 密码复杂性安全注意事项

AWS 在托管 AWS Microsoft AD 中提供了一组精细的密码策略，您可以对其进行配置和分配给您的群组。要配置策略，您可以使用标准Microsoft策略工具，例如Active Directory管理中心。要开始使用Microsoft策略工具，请参阅安装适用于 AWS 托管微软 AD 的 Active Directory 管理工具。

如何应用密码策略

细粒度密码策略的应用方式会有所不同，具体取决于密码是重置还是密码已更改。域用户可以更改自己的密码。Active Directory管理员或具有必要权限的用户可以重置用户的密码。有关更多信息，请参见下表。

Policy	密码重置	密码更改
强制密码历史	 否	 是
最长密码使用期限	 是	 是
最短密码使用期限	 否	 是
最短密码长度	 是	 是
密码必须符合复杂性要求	 是	 是

这些差异会带来安全影响。例如，无论何时重置用户的密码，都不会强制执行密码历史记录和最短密码使用期限政策。有关更多信息，请参阅 Microsoft 文档，了解与强制执行密码历史记录和最低密码使用期限策略相关的安全注意事项。

主题

- 支持的策略设置
- 委托谁可以管理您的密码策略
- 为用户分配密码策略

相关 AWS 安全博客文章

- 如何使用 AWS 托管 Microsoft AD 来配置更严格的密码策略 AWS Directory Service 以帮助满足你的安全标准

支持的策略设置

AWS 托管 Microsoft AD 包括五个具有不可编辑优先级值的细粒度策略。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。

AWS 预定义的密码策略

下表列出了您的 AWS 托管 Microsoft AD 目录中包含的五个策略及其分配的优先级值。有关更多信息，请参阅 优先级。

策略名称	优先级
CustomerPSO-01	10
CustomerPSO-02	20
CustomerPSO-03	30
CustomerPSO-04	40
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执行的更多详细信息，请参阅 M ic TechNet rosoft 网站上的 AD DS：精细密码策略。有关这些策略的一般信息，请参阅 Microsoft TechNet 网站上的密码策略。

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

有关这些政策的一般信息，请参阅 Microsoft TechNet 网站上的帐户锁定政策。

优先级

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。

有关更多详细信息，请参阅 M ic TechNet rosoft 网站上的 AD DS：精细密码策略。

委托谁可以管理您的密码策略

您可以将密码策略管理权限委派给您在托 AWS 管 Microsoft AD 中创建的特定用户帐户，方法是将这些帐户添加到 “AWS 委托精细密码策略管理员” 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列出的任何密码策略。

委托谁可以管理密码策略

1. 从您加入托管的 Microsoft AD 域的任何托管 EC2 实例启动 Active Directory AWS 管理中心 (ADAC)。
2. 切换到树视图，然后导航到 AWS 委托组 OU。有关此 OU 的更多信息，请参阅 用你的 AWS 托管 Microsoft AD 活动目录创建了什么。
3. 查找 AWS 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。

为用户分配密码策略

作为 AWS 精细密码策略委托管理员安全组成员的用户账户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. 从您加入托管的 Microsoft AD 域的任何托管 EC2 实例启动 Active Directory AWS 管理中心 (ADAC)。
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 AWS Managed Microsoft AD 一起提供的默认精细策略的更多信息，请参阅 AWS 预定义的密码策略。
4. 要验证密码策略是否已应用，请运行以下 PowerShell命令：

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

> **Note**
>
> 避免使用 `net user` 命令，因为其结果可能不准确。

如果您未在 AWS 托管 Microsoft AD 目录中配置五个密码策略中的任何一个，则 Active Directory 将使用默认的域组策略。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 AWS 托管的 Microsoft AD 启用多因素身份验证

您可以为 AWS 托管 Microsoft AD 目录启用多重身份验证 (MFA)，以便在用户指定要访问的 AD 凭据时提高安全性。支持的 Amazon Enterprise 应用程序启用 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，您必须具有属于远程身份验证拨入用户服务（RADIUS）服务器的 MFA 解决方案，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。 AWS 托管 Microsoft AD 包括一个 RADIUS 客户端，该客户端可连接到你实施了 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。如果你的 RADIUS 服务器成功验证了用户，Microsoft AD 就会 AWS 根据 Active Directory 对用户进行身份验证。成功进行 Active Directory 身份验证后，用户就可以访问该 AWS 应用程序了。 AWS 托管的 Microsoft AD RADIUS 客户端与你的 RADIUS 服务器之间的通信需要你配置允许通过端口 1812 进行通信 AWS 的安全组。

您可以通过执行以下步骤为 AWS 托管 Microsoft AD 目录启用多因素身份验证。有关如何配置 RADIUS 服务器以使用 AWS Directory Service 和 MFA 的更多信息，请参阅多重身份验证先决条件。

注意事项

以下是 AWS 托管 Microsoft AD 的多因素身份验证的一些注意事项：

- 多重身份验证对 Simple AD 不可用。但是，可为 AD Connector 目录启用 MFA。有关更多信息，请参阅 为 AD Connector 启用多重身份验证。
- MFA 是 M AWS icrosoft AD 托管的一项区域性功能。如果您使用的是 多区域复制，则必须分别在每个区域中应用以下过程。有关更多信息，请参阅 全局与区域特色。
- 如果您打算使用 AWS 托管 Microsoft AD 进行外部通信，我们建议您在网络外部为这些通信配置网络地址转换 (NAT) Internet Gateway 或 Internet Gateway。 AWS
  - 如果您希望支持托管的 Microsoft AD 与 AWS 网络上 AWS 托管的 RADIUS 服务器之间的外部通信，请联系AWS Support。

为 AWS 托管的 Microsoft AD 启用多因素身份验证

以下过程向您展示如何为 AWS 托管 Microsoft AD 启用多因素身份验证。

1. 识别你的 RADIUS MFA 服务器的 IP 地址和你的托管 M AWS icrosoft AD 目录。
2. 编辑您的虚拟私有云 (VPC) 安全组，以启用 AWS 托管的微软 AD IP 端点和 RADIUS MFA 服务器之间通过端口 1812 进行通信。

3. 在 AWS Directory Service 控制台导航窗格中，选择目录。
4. 为你的 AWS 托管 Microsoft AD 目录选择目录 ID 链接。
5. 在报告详细信息页面上，执行以下操作之一：
   - 如果多区域复制下显示多个区域，选择想要启用 MFA 的区域，然后选择网络与安全选项卡。有关更多信息，请参阅 主区域与其他区域。
   - 如果多区域复制下未显示任何区域，选择网络与安全选项卡。
6. 在多重验证部分中，选择操作，然后选择启用。
7. 在启用多重身份验证（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 仅适用于对亚马逊企业应用程序和服务（例如 WorkSpaces亚马逊 QuickSight或 Amazon Chime）的访问进行身份验证。 AWS Management Console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。 AWS 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拥有 MFA 代码。或者，您必须使用执行 MFA 的解决方案， out-of-band 例如对用户进行 SMS 文本验证。在 out-of-band MFA 解决方案中，必须确保为您的解决方案正确设置 RADIUS 超时值。使用 out-of-band 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，用户必须在密码字段和 MFA 字段中均输入密码。

端口

RADIUS 服务器用来通信的端口。您的本地网络必须允许服务器通过默认 RADIUS 服务器端口 (UDP: 1812) 的入站流量。 AWS Directory Service

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。如果超时超过 20 秒，则系统无法使用其他 RADIUS 服务器重试，并可能导致超时失败。

RADIUS 请求最大重试次数

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 启用。

支持的 Amazon Enterprise 应用程序

所有亚马逊企业 IT 应用程序 WorkSpaces，包括亚马逊、亚马逊 WorkDocs WorkMail QuickSight、亚马逊，以及使用带 AWS Management Console 有 MFA 的 Microsoft AD AWS IAM Identity Center 和 AD Connector AWS 托管时均支持访问和支持。

有关如何配置用户对 Amazon Enterprise 应用程序的基本访问权限、 AWS 单点登录和 AWS Management Console 使用的信息 AWS Directory Service，请参阅允许访问 AWS 应用程序和服务和允许使用 AD 凭证访问 AWS Management Console。

相关 AWS 安全博客文章

- 如何使用 AWS 托管 Microsoft AD 和本地凭据为 AWS 服务启用多因素身份验证

启用安全 LDAP 或 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。

为了缓解这种形式的数据泄露，Microsoft AD AWS 托管提供了一个选项：你可以启用基于安全套接字层 (SSL) /传输层安全 (TLS) 的 LDAP，也称为 LDAPS。利用 LDAPS，您可以提高整个网络的安全性。您还可以通过加密支持 LDAP 的应用程序与托管 AWS Microsoft AD 之间的所有通信来满足合规性要求。

AWS 托管 Microsoft AD 在以下部署场景中为 LDAPS 提供支持：

- 服务器端 LDAPS 可加密您的商业或本土开发的 LDAP 感知应用程序（充当 LDAP 客户端）与托管 AWS Microsoft AD（充当 LDAP 服务器）之间的 LDAP 通信。有关更多信息，请参阅 使用托管 AWS Microsoft AD 启用服务器端 LDAPS。
- 客户端 LDAPS 对 AWS 应用程序之间的 LDAP 通信进行加密，例如 WorkSpaces （充当 LDAP 客户端）和您的自我管理（本地）Active Directory（充当 LDAP 服务器）。有关更多信息，请参阅 使用托管 AWS Microsoft AD 启用客户端 LDAPS。

主题

- 使用托管 AWS Microsoft AD 启用服务器端 LDAPS
- 使用托管 AWS Microsoft AD 启用客户端 LDAPS

使用托管 AWS Microsoft AD 启用服务器端 LDAPS

服务器端轻量级目录访问协议安全套接字层 (SSL) /传输层安全 (TLS) (LDAPS) 支持加密您的商业或本地 LDAP 感知应用程序与托管 Microsoft AD 目录之间的 LDAP 通信。 AWS 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 和您的证书颁发机构 (CA) 服务器的详细说明，请参阅安全博客上的如何为托管的 AWS Microsoft AD 目录启用服务器端 LDAPS。 AWS

您必须从用来管理 AWS Managed Microsoft AD 域控制器的 Amazon EC2 实例执行大多数设置。以下步骤将指导您在 AWS 云端为域名启用 LDAPS。

如果你想使用自动化来设置 PKI 基础架构，可以使用 Microsoft 公钥基础架构 AWS QuickStart 指南。具体而言，您需要按照指南中的说明加载模版，以便将 Microsoft PKI 部署到 AWS上的现有 VPC 中。加载模板后，请务必在到达 Active Directory 域服务选项时选择 **AWSManaged**。如果您使用了该 QuickStart 指南，则可以直接跳至步骤 3：创建证书模板。

主题

- 步骤 1：委托谁可以启用 LDAPS
- 步骤 2：设置证书颁发机构
- 步骤 3：创建证书模板
- 步骤 4：添加安全组规则

步骤 1：委托谁可以启用 LDAPS

要启用服务器端 LDAPS，您必须是托管 AWS Microsoft AD 目录中的管理员或企业证书 AWS 授权机构管理员组的成员。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，请将该用户添加到 AWS 托管 Microsoft AD 目录中的管理员或企业证书 AWS 授权机构管理员组中。

步骤 2：设置证书颁发机构

您必须先创建一个证书，然后才能启用服务器端 LDAPS。此证书必须由加入您的 AWS 托管微软 AD 域的微软企业 CA 服务器颁发。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**
>
> 带有托管 AWS Microsoft AD 的服务器端 LDAPS 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 Microsoft Enterprise CA —（推荐）使用此选项，你可以在 AWS 云中部署从属微软企业 CA 服务器。该服务器可以使用 Amazon EC2，这样便能使用您现有的根 Microsoft CA。有关如何设

置下属微软企业 CA 的更多信息，请参阅如何为托管的 Mic rosoft AD 目录启用服务器端 LDAPS 中的步骤 4：将 AWS 微软企业 CA 添加到你的 AWS 微软 AD 目录。

- 创建根微软企业 CA — 使用此选项，您可以使用亚马逊 EC2 在 AWS 云中创建微软企业 CA 根，并将其加入您的微软 AD AWS 托管域。此根 CA 可以向您的域控制器颁发证书。有关设置新的根 CA 的更多信息，请参阅如何为托管的 AWS Microsoft AD 目录启用服务器端 LDAPS 中的步骤 3：安装和配置离线 CA。

有关如何将您的 EC2 实例加入域的更多信息，请参阅将 Amazon EC2 实例加入您的 AWS 托管微软 AD Active Directory。

步骤 3：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。依次选择工具 > 证书颁发机构。
2. 在证书颁发机构窗口中，展开左侧窗格中的证书颁发机构树。右键单击证书模版，然后选择管理。
3. 在证书模版控制台窗口中，右键单击域控制器，然后选择重复模版。
4. 系统将会弹出新模板的属性窗口。
5. 在新模板的属性窗口中，转到兼容性选项卡，然后执行以下操作：
   a. 将证书颁发机构更改为与 CA 匹配的操作系统。
   b. 如果系统弹出生成的更改窗口，选择确定。
   c. 将认证接收者更改为 Windows 10/Windows Server 2016。

      > **Note**
      >
      > AWS 托管微软 AD 由 Windows Server 2019 提供支持。

   d. 如果系统弹出生成的更改窗口，选择确定。
6. 单击常规选项卡，将模板显示名称更改为 LDAPOverSSL 或您偏好的任何其他名称。
7. 单击安全选项卡，然后选择组或用户名称部分中的域控制器 。在域控制器的权限部分，确认已选中读取、注册和自动注册的允许复选框。
8. 选择确定以创建 LDAPOverSSL（或您在上面指定的名称）证书模板。关闭证书模板控制台窗口。
9. 在证书颁发机构窗口中，右键单击证书模版，然后依次选择新建 > 要颁发的证书模版。

10. 在启用证书模板窗口中，选择 LDAPOverSSL（或您在上面指定的名称），然后选择确定。

步骤 4：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. 导航到 Amazon EC2 控制台（网址为 https://console.aws.amazon.com/ec2），然后使用管理员凭证登录。
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 AWS 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：
   - 选择添加规则。
   - 为 Type 选择 All traffic，并为 Source 选择 Custom。
   - 在来源旁边的框中输入目录 AWS 的安全组（例如 sg-123456789）。
   - 选择保存。
6. 现在选择你的 Microsoft AD AWS 托管目录 AWS 的安全组。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：
   - 选择添加规则。
   - 为 Type 选择 All traffic，并为 Destination 选择 Custom。
   - 在目标旁边的框中键入您的 CA AWS 的安全组。
   - 选择保存。

你可以使用 LDP 工具测试 LDAPS 与 AWS 托管微软 AD 目录的连接。LDP 工具随 Active Directory 管理工具一起提供。有关更多信息，请参阅 安装适用于 AWS 托管微软 AD 的 Active Directory 管理工具。

> **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 向域控制器颁发证书。

有关服务器端 LDAPS 的更多详细信息以及如何进行设置的示例用例，请参阅安全博客上的如何为托管 AWS Microsoft AD 目录启用服务器端 LDAPS。 AWS

使用托管 AWS Microsoft AD 启用客户端 LDAPS

托管 AWS Microsoft AD 中的客户端轻量级目录访问协议安全套接字层 (SSL) /传输层安全 (TLS) (LDAPS) 支持加密自我管理（本地）微软活动目录 (AD) 与应用程序之间的通信。 AWS 此类应用程序的示例包括 WorkSpaces、 AWS IAM Identity Center QuickSight、Amazon 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

- 在你的 AWS 托管 Microsoft AD 和自我管理之间建立信任关系 Microsoft Active Directory
- 在 Active Directory 中部署服务器证书
- 证书颁发机构证书要求
- 联网要求

在你的 AWS 托管 Microsoft AD 和自我管理之间建立信任关系 Microsoft Active Directory

首先，你需要在 AWS 托管 Microsoft AD 和自我管理之间建立信任关系，MicrosoftActive Directory以启用客户端 LDAPS。有关更多信息，请参阅 the section called “创建信任关系”。

在 Active Directory 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。

证书颁发机构证书要求

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：

- 需要企业证书颁发机构 (CA) 才能启用客户端 LDAPS。您可以使用Active Directory证书服务、第三方商业证书颁发机构或AWS Certificate Manager。有关Microsoft企业证书颁发机构的更多信息，请参阅Microsoft文档。
- 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 AWS 托管 Microsoft AD 目录最多可以存储五 (5) 个 CA 证书。
- 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

AWS 应用程序 LDAP 流量将仅在 TCP 端口 636 上运行，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 AWS 安全组和网络防火墙，以允许托管 AWS Microsoft AD（出站）和自我管理的 Active Directory（入站）中的端口 636 上进行 TCP 通信。在 AWS Managed Microsoft AD 和自托管式 Active Directory 之间保留开放的 LDAP 端口 389。

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 AWS Managed Microsoft AD，然后在目录上启用 LDAPS。启用后， AWS 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 AWS Management Console 方法或 AWS CLI 方法。

> **Note**
>
> 客户端 LDAPS 是 AWS Microsoft 托管 AD 的一项区域性功能。如果您使用的是 多区域复制，则必须分别在每个区域中应用以下过程。有关更多信息，请参阅 全局与区域特色。

主题

- 第 1 步：在中注册证书 AWS Directory Service
- 步骤 2：检查注册状态
- 步骤 3：启用客户端 LDAPS
- 步骤 4：查看 LDAPS 状态

第 1 步：在中注册证书 AWS Directory Service

使用以下任一方法在中注册证书 AWS Directory Service。

方法 1：在 AWS Directory Service (AWS Management Console) 中注册您的证书

1. 在 AWS 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. 在报告详细信息页面上，执行以下操作之一：
   - 如果多区域复制下显示多个区域，选择想要注册证书的区域，然后选择网络与安全选项卡。有关更多信息，请参阅 主区域与其他区域。
   - 如果多区域复制下未显示任何区域，选择网络与安全选项卡。
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 AWS Directory Service (AWS CLI) 中注册您的证书

- 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
```

步骤 2：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 AWS Directory Service (AWS Management Console) 中检查证书注册状态

1. 转到目录详细信息页面上的客户端 LDAPS 部分。
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 AWS Directory Service (AWS CLI) 中检查证书注册状态

- 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
```

步骤 3：启用客户端 LDAPS

使用以下任一方法在中启用客户端 LDAPS。 AWS 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 AWS Directory Service 启用客户端 LDAPS AWS Management Console

1. 转到目录详细信息页面上的客户端 LDAPS 部分。
2. 请选择 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。
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 AWS Directory Service 启用客户端 LDAPS AWS CLI

- 运行以下命令。

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

步骤 4：查看 LDAPS 状态

使用以下任一方法在中检查 LDAPS 状态。 AWS Directory Service

方法 1：在 AWS Directory Service ()AWS Management Console中检查 LDAPS 状态

1. 转到目录详细信息页面上的客户端 LDAPS 部分。
2. 如果状态值显示为 Enabled (启用)，则 LDAPS 已成功配置。

方法 2：在 AWS Directory Service ()AWS CLI中检查 LDAPS 状态

- 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 AWS Management Console 方法或 AWS 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 AWS Directory Service (AWS Management Console) 中查看证书详细信息

1. 在 AWS 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. 在报告详细信息页面上，执行以下操作之一：
   - 如果多区域复制下显示多个区域，选择想要查看证书的区域，然后选择网络与安全选项卡。有关更多信息，请参阅 主区域与其他区域。
   - 如果多区域复制下未显示任何区域，选择网络与安全选项卡。
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 AWS Directory Service (AWS CLI) 中查看证书详细信息

- 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 AWS Directory Service ()AWS Management Console中注销证书

1. 在 AWS 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. 在报告详细信息页面上，执行以下操作之一：
   - 如果多区域复制下显示多个区域，选择想要取消注册证书的区域，然后选择网络与安全选项卡。有关更多信息，请参阅 主区域与其他区域。
   - 如果多区域复制下未显示任何区域，选择网络与安全选项卡。
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 AWS Directory Service ()AWS CLI中注销证书

- 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 AWS Directory Service 禁用客户端 LDAPS AWS Management Console

1. 在 AWS 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. 在报告详细信息页面上，执行以下操作之一：
   - 如果多区域复制下显示多个区域，选择想要禁用客户端 LDAPS 的区域，然后选择网络与安全选项卡。有关更多信息，请参阅 主区域与其他区域。
   - 如果多区域复制下未显示任何区域，选择网络与安全选项卡。
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 AWS Directory Service 禁用客户端 LDAPS AWS CLI

- 运行以下命令。

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

证书注册问题

使用 CA 证书注册 AWS 托管 Microsoft AD 域控制器的过程最多可能需要 30 分钟。如果您在证书注册时遇到问题，并且想要重新启动 AWS 托管 Microsoft AD 域控制器，可以联系 AWS Support。要创建支持案例，请参阅创建支持案例和案例管理。

管理 AWS 托管微软 AD 的合规性

你可以使用 AWS 托管 Microsoft AD 来支持 AWS 云端中你的 Active Directory 感知 Active Directory 的应用程序，这些应用程序必须遵守以下合规性要求。不过，如果您使用 Simple AD，应用程序将不符合合规性要求。

支持的合规性标准

AWS 托管 Microsoft AD 已经过以下标准的审计，有资格作为解决方案的一部分使用，你需要获得合规性认证。

AWS 托管 Microsoft AD 符合联邦风险和授权管理计划 (FedRAMP) 的安全要求，并已获得 FedRAMP 中等和高基线的 FedRAMP 联合授权委员会 (JAB) 临时运营授权 (P-ATO)。有关 FedRAMP 的更多信息，请参阅 FedRAMP 合规性。

AWS 托管 Microsoft AD 在服务提供商级别为 1 的支付卡行业 (PCI) 数据安全标准 (DSS) 3.2 版合规性认证。使用 AWS 产品和服务存储、处理或传输持卡人数据的客户可以使用 AWS 托管 Microsoft AD 来管理自己的 PCI DSS 合规性认证。

有关 PCI DSS 的更多信息，包括如何申请 PCI Compliance Package 的副本，请参阅 AWS PCI DSS 第 1 级。重要的是，您必须在托管 AWS Microsoft AD 中配置精细的密码策略，使其与 PCI DSS 版本 3.2 标准保持一致。有关必须强制执行哪些策略的详细信息，请参阅下面标题为 “为 AWS 托管的 Microsoft AD 目录启用 PCI 合规性” 的部分。

AWS 已扩大其《健康保险流通与责任法案》（HIPAA）合规计划，将托管 AWS 微软广告列为符合 HIP AA资格的服务。如果您与签订了商业伙伴协议 (BAA) AWS，则可以使用 AWS 托管 Microsoft AD 来帮助构建符合 HIPAA 标准的应用程序。

AWS 为有兴趣进一步了解如何利用健康信息处理和存储的客户提供了一份以 HIPAA AWS 为重点的白皮书。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。必须明白， AWS 托管 Microsoft AD 合规性状态不会自动应用于你在 AWS 云端运行的应用程序。您需要确保您对 AWS 服务的使用符合标准。

有关 AWS 托管 Microsoft AD 支持的所有各种 AWS 合规计划的完整列表，请参阅按合规计划划分的范围内的AWS 服务。

为你的微软 AD AWS 托管目录启用 PCI 合规性

要为您的 AWS 托管 Microsoft AD 目录启用 PCI 合规性，您必须按照提供的 PCI DSS 合规性证明 (AOC) 和责任摘要文档中的规定配置精细的密码策略。 AWS Artifact

有关使用精细密码策略的更多信息，请参阅管理 AWS 托管 Microsoft AD 的密码策略。

增强 AWS Managed Microsoft AD 网络安全配置

对于为 AWS Managed Microsoft AD 目录预置的 AWS 安全组，为其配置了支持 AWS Managed Microsoft AD 目录的所有已知使用案例所需的最少入站网络端口数。有关预置的 AWS 安全组的更多信息，请参阅用你的 AWS 托管 Microsoft AD 活动目录创建了什么。

为进一步增强 AWS Managed Microsoft AD 目录的网络安全性，您可以根据下面列出的常见方案修改 AWS 安全组。

主题

- 仅支持 AWS 应用程序
- 仅支持具有信任的 AWS 应用程序
- AWS 应用程序和本机 Active Directory 工作负载支持
- AWS 应用程序和本机 Active Directory 工作负载支持以及信任支持

仅支持 AWS 应用程序

所有用户账户仅在 AWS Managed Microsoft AD 中预置为与受支持的 AWS 应用程序一起使用，例如：

- Amazon Chime
- Amazon Connect
- Amazon QuickSight
- AWS IAM Identity Center

- Amazon WorkDocs
- Amazon WorkMail
- AWS Client VPN
- AWS Management Console

您可以使用以下 AWS 安全组配置来阻止指向 AWS Managed Microsoft AD 域控制器的所有非必要通信。

> **Note**
>
> - 以下内容与此 AWS 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。

仅支持具有信任的 AWS 应用程序

所有用户账户都在 AWS Managed Microsoft AD 或受信任的 Active Directory 中预置为与受支持的 AWS 应用程序一起使用，例如：

- Amazon Chime

- Amazon Connect
- Amazon QuickSight
- AWS IAM Identity Center
- Amazon WorkDocs
- Amazon WorkMail
- Amazon WorkSpaces
- AWS Client VPN
- AWS Management Console

您可以修改预置的 AWS 安全组配置，以阻止指向 AWS Managed Microsoft AD 域控制器的所有非必要通信。

> **Note**
>
> - 以下内容与此 AWS 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

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

AWS 应用程序和本机 Active Directory 工作负载支持

用户账户仅在 AWS Managed Microsoft AD 中预置为与受支持的 AWS 应用程序一起使用，例如：

- 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
- AWS IAM Identity Center
- Amazon WorkDocs
- Amazon WorkMail
- WorkSpaces
- AWS Client VPN

- AWS Management Console

您可以修改预置的 AWS 安全组配置，以阻止指向 AWS Managed Microsoft AD 域控制器的所有非必要通信。

> **Note**
>
> - 无法在 AWS Managed Microsoft AD 目录和本地域之间创建和维护 Active Directory 信任。
> - 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
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

协议	端口范围	源	流量的类型	Active Directory 使用情况
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。

AWS 应用程序和本机 Active Directory 工作负载支持以及信任支持

所有用户账户都在 AWS Managed Microsoft AD 或受信任的 Active Directory 中预置为与受支持的 AWS 应用程序一起使用，例如：

- 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
- AWS IAM Identity Center
- Amazon WorkDocs
- Amazon WorkMail
- WorkSpaces
- AWS Client VPN
- AWS Management Console

您可以修改预置的 AWS 安全组配置，以阻止指向 AWS Managed Microsoft AD 域控制器的所有非必要通信。

> **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

协议	端口范围	源	流量的类型	Active Directory 使用情况
				验证组策略、信任
UDP	123	本地 CIDR	Windows 时间	Windows 时间、信任
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

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

配置目录安全设置

您可以为托管 AWS Managed Microsoft AD 配置精细的目录设置，以在不增加运行工作负载的情况下满足您的合规性和安全要求。在目录设置中，您可以更新目录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）。AWS然后，Managed Microsoft AD 会将配置部署到目录中的所有域控制器，管理域控制器的重新启动，并在您横向扩展或部署更多 AWS 区域 时保持此配置。有关所有可用设置的详细信息，请参阅 目录安全设置列表。

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. 前往 https://console.aws.amazon.com/directoryservicev2/，登录到 AWS 管理控制台，打开 AWS Directory Service 控制台。
2. 在目录页面上，选择您的目录 ID。
3. 在网络与安全下，找到目录设置，然后选择编辑设置。
4. 在编辑设置中，更改要编辑的设置的值。编辑设置时，其状态会从默认更改为更新准备就绪。如果您之前编辑过该设置，则其状态将从已更新更改为更新准备就绪。然后选择查看。
5. 在查看和更新设置中，查看目录设置并确保新值全部正确。如果要对设置进行任何其他更改，请选择编辑设置。当您对更改感到满意并准备实施新值时，请选择更新设置。然后，您将返回到目录 ID 页面。

> **Note**
>
> 在目录设置下，您可以查看已更新设置的状态。实施设置后，状态将显示为正在更新。当设置在状态下显示为正在更新时，您无法编辑其他设置。如果您的编辑成功更新了设置，则状态将显示为已更新。如果您的编辑无法更新设置，则状态将显示为失败。

目录安全设置失败

如果在设置更新过程中出现错误，则状态将显示为失败。在失败状态下，设置不会更新为新值，且原始值继续实施。您可以重试更新这些设置或将其恢复到以前的值。

解决更新设置失败的问题

- 在目录设置下，选择解决失败的设置。然后，执行以下操作之一：
  - 要将设置恢复到失败状态之前的原始值，请选择恢复失败的设置。然后，在弹出模式中选择恢复。
  - 要重试更新目录设置，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。在查看并重试失败的更新中，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。

如果禁用了所有其他安全设置，则默认目录安全设置为 TLS 1.2 和 AES 256/256。无法禁用它们。

类型	设置名称	API 名称	潜在值	设置说明
基于证书的身份验证	证书回溯补偿	CERTIFICATE_BACKDATING_COMPENSATION	年数：0 到 50 月数：0 到 11 天数：0 到 30 小时数：0 到 23 分钟数：0 到 59 秒数：0 到 59	指定一个值，以指示证书可以早于 Active Directory 中的用户并且仍可用于 Active Directory 中的身份验证的时间长度。默认值为 10 分钟。您可以将此值设置为 1 秒到 50 年。 要配置此设置，必须为强证书绑定执行选择兼容性类型。 有关更多信息，请参阅 Microsoft Support 文档中的 KB5014754 - Windows 域控制器上基于证书的身份验证更改。

类型	设置名称	API 名称	潜在值	设置说明
	证书强制执行	CERTIFICATE_STRONG_ENFORCEMENT	兼容性，全面执行	指定以下任一种执行类型： • 兼容性（默认）：如果无法将证书强映射到用户，则允许进行身份验证。如果证书早于 Active Directory 中的用户账户，则还必须设置证书回溯补偿，否则身份验证将失败。 • 全面执行（默认）：如果无法将证书强映射到用户，则不允许进行身份验证。如果您选择此执行类型，则无法配置证书回溯补偿。

类型	设置名称	API 名称	潜在值	设置说明
				有关更多信息，请参阅 Microsoft Support 文档中的 KB5014754 - Windows 域控制器上基于证书的身份验证更改。
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间进行安全的信道通信。
	DES 56/56	DES_56_56	启用，禁用	启用或禁用 DES 56/56 加密密码，以便在目录中的域控制器之间进行安全的信道通信。
	RC2 40/128	RC2_40_128	启用，禁用	启用或禁用 RC2 40/128 加密密码，以便在目录中的域控制器之间进行安全的信道通信。

类型	设置名称	API 名称	潜在值	设置说明
	RC2 56/128	RC2_56_128	启用，禁用	启用或禁用 RC2 56/128 加密密码，以便在目录中的域控制器之间进行安全的信道通信。
	RC2 128/128	RC2_128_128	启用，禁用	启用或禁用 RC2 128/128 加密密码，以便在目录中的域控制器之间进行安全的信道通信。
	RC4 40/128	RC4_40_128	启用，禁用	启用或禁用 RC4 40/128 加密密码，以便在目录中的域控制器之间进行安全的信道通信。
	RC4 56/128	RC4_56_128	启用，禁用	启用或禁用 RC4 56/128 加密密码，以便在目录中的域控制器之间进行安全的信道通信。

类型	设置名称	API 名称	潜在值	设置说明
	RC4 64/128	RC4_64_128	启用，禁用	启用或禁用 RC4 64/128 加密密码，以便在目录中的域控制器之间进行安全的信道通信。
	RC4 128/128	RC4_128_128	启用，禁用	启用或禁用 RC4 128/128 加密密码，以便在目录中的域控制器之间进行安全的信道通信。
	Triple DES 168/168	3DES_168_168	启用，禁用	启用或禁用 Triple DES 168/168 加密密码，以便在目录中的域控制器之间进行安全的信道通信。
安全通道：协议	PCT 1.0	PCT_1_0	启用，禁用	启用或禁用 PCT 1.0 协议，以便在目录中的域控制器上进行安全的信道通信（服务器和客户端）。

类型	设置名称	API 名称	潜在值	设置说明
	SSL 2.0	SSL_2_0	启用，禁用	启用或禁用 SSL 2.0 协议，以便在目录中的域控制器上进行安全的信道通信（服务器和客户端）。
	SSL 3.0	SSL_3_0	启用，禁用	启用或禁用 SSL 3.0 协议，以便在目录中的域控制器上进行安全的信道通信（服务器和客户端）。
	TLS 1.0	TLS_1_0	启用，禁用	启用或禁用 TLS 1.0 协议，以便在目录中的域控制器上进行安全的信道通信（服务器和客户端）。

类型	设置名称	API 名称	潜在值	设置说明
	TLS 1.1	TLS_1_1	启用，禁用	启用或禁用 TLS 1.1 协议，以便在目录中的域控制器上进行安全的信道通信（服务器和客户端）。

为 AD 设置 AWS Private CA 连接器

你可以将你的 AWS 托管 Microsoft AD 与 AWS Private Certificate Authority (CA) 集成，为你的 Active Directory 域加入的用户、群组和计算机颁发和管理证书。 AWS Private CA Active Directory 的 Connector 允许您使用完全托管的 AWS Private CA 嵌入式替代方案来代替自行管理的企业 CA，而无需部署、修补或更新本地代理或代理服务器。

> **Note**
>
> 不支持使用 Active Directory AWS Private CA 连接器的托管 M AWS icrosoft AD 域控制器的服务器端 LDAPS 证书注册。要为目录启用服务器端 LDAPS，请参阅如何为托管 AWS Microsoft AD 目录启用服务器端 LDAPS。

您可以通过目录服务控制台、Active Directory 控制台的 AWS Private CA 连接器或通过调用 `CreateTemplate`API 来设置与目录的集 AWS Private CA 成。要通过 Active Directory AWS Private CA 连接器控制台设置私有 CA 集成，请参阅创建连接器模板。有关如何从 AWS Directory Service 控制台设置此集成的步骤，请参阅下文。

为 AD 设置 AWS Private CA 连接器

1. 登录 AWS Management Console 并打开 AWS Directory Service 控制台，网址为https://console.aws.amazon.com/directoryservicev2/。
2. 在目录页面上，选择您的目录 ID。

3. 在 “网络和安全” 选项卡下的 “ADAWS Private CA 连接器” 下，选择 “为 AD 设置 AWS Private CA 连接器”。将出现 “为其创建私有 CA 证书 Active Directory” 页面。按照控制台上的步骤创建您的私有 CA，以便Active Directory连接器注册您的私有 CA。有关更多信息，请参阅 Creating a connector。
4. 创建连接器后，请按照以下步骤查看详细信息，包括连接器的状态和关联的私有 CA 的状态。

查看 AD AWS Private CA 连接器

1. 登录 AWS Management Console 并打开 AWS Directory Service 控制台，网址为https://console.aws.amazon.com/directoryservicev2/。
2. 在目录页面上，选择您的目录 ID。
3. 在网络与安全性下的 AWS Private CA Connector for AD 下，您可以查看您的私有 CA 连接器和关联的私有 CA。默认情况下，您会看到以下字段：

    a. AWS Private CA 连接器 ID- AWS Private CA 连接器的唯一标识符。点击它会进入该 AWS Private CA 连接器的详细信息页面。

    b. AWS Private CA 主题-有关 CA 的可分辨名称的信息。点击该字段会进入该 AWS Private CA 的详细信息页面。

    c. 状态 —基于对 AWS Private CA 连接器的状态检查和 AWS Private CA. 如果两项检查均通过，则会显示活动。如果其中一项检查失败，则会显示 1/2 检查失败。如果两项检查均失败，则会显示失败。有关失败状态的更多信息，请将鼠标悬停在超链接上以了解哪项检查失败。按照控制台中的说明进行修复。

    d. 创建日期- AWS Private CA 连接器的创建日期。

有关更多信息，请参阅 View connector details。

监控 AWS Managed Microsoft AD

您可以通过以下方法监控 AWS Managed Microsoft AD 目录：

主题

- 了解目录状态
- 使用 Amazon SNS 配置目录状态通知
- 查看您的 AWS Managed Microsoft AD 目录日志
- 启用日志转发

- 使用性能指标监控域控制器

了解目录状态

以下是目录的各种状态。

处于活动状态

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

Creating

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

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。如果问题仍存在，请联系 AWS Support 中心。

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，请参阅微软 AD AWS 托管故障排除、AD Connector 故障排除、Simple AD 问题排查。对于与正常维护相关的问题， AWS 可在 40 分钟内解决这些问题。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 AWS Support 中心。

> **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 为目录拍摄快照或还原目录。

Requested (已请求)

创建目录的请求当前正在等待处理。

RestoreFailed

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 AWS Support 中心。

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。

使用 Amazon SNS 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 “活动” 状态变为 “受损” 状态，您会收到通知。当目录恢复为“活动”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用户，他们接收发布至该主题的消息。按照以下步骤，您可以在 Amazon SNS 主题中添加 AWS Directory Service 出版商身份。当 AWS Directory Service 检测到您的目录状态发生变化时，它会向该主题发布一条消息，然后将其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 Microsoft AD AWS 托管的一项区域性功能。如果您使用的是 多区域复制，则必须分别在每个区域中应用以下过程。有关更多信息，请参阅 全局与区域特色。

为您的目录启用 SNS 消息发送

1. 登录 AWS Management Console 并打开AWS Directory Service 控制台。
2. 在目录页面上，选择您的目录 ID。
3. 在报告详细信息页面上，执行以下操作之一：

- 如果多区域复制下显示多个区域，选择要启用 SNS 消息收发的区域，然后选择维护选项卡。有关更多信息，请参阅 主区域与其他区域。
- 如果多区域复制下未显示任何区域，选择维护选项卡。

4. 在目录监控部分，选择操作，然后选择创建通知。
5. 在创建通知页面上，选择选择通知类型，然后选择创建新通知。或者，如果您现在已有一个 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**
>
> 如果您选择创建新通知，但之后使用与现有 SNS 主题相同的主题名称，则 Amazon SNS 不会创建新主题，只是向现有主题添加新的订阅信息。
> 如果您选择关联现有 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，然后输入收件人联系信息。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）为主题和 SNS 显示名称提供名称。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**
>
> 如果您使用只有DirectoryServiceFullAccess托管策略的 IAM 用户或角色登录，则您的主题名称必须以 “DirectoryMonitoring” 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。

如果您想指定其他 SNS 订阅者，例如额外的电子邮件地址、Amazon SQS 队列 AWS Lambda或，则可以从 Amazon SNS 控制台执行此操作。

从主题移除目录状态消息

1. 登录 AWS Management Console 并打开AWS Directory Service 控制台。
2. 在目录页面上，选择您的目录 ID。
3. 在报告详细信息页面上，执行以下操作之一：

- 如果多区域复制下显示多个区域，选择要移除状态消息的区域，然后选择维护选项卡。有关更多信息，请参阅 主区域与其他区域。
- 如果多区域复制下未显示任何区域，选择维护选项卡。

4. 在目录监控部分，在列表中选择一个 SNS 主题名称，选择操作，然后选择移除。
5. 选择移除。

这会移除您目录的选定 SNS 主题发布者身份。如果您想删除整个主题，可以从 Amazon SNS 控制台执行此操作。

> **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，在删除任何从中 AWS Directory Service接收消息的主题之前，请将您的目录与其他 Amazon SNS 主题相关联。

查看您的 AWS Managed Microsoft AD 目录日志

来自 AWS Managed Microsoft AD 域控制器实例的安全日志会存档一年时间。您还可以配置您的 AWS Managed Microsoft AD 目录以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。

AWS 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

监控类别	策略设置	审核状态
	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
	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

监控类别	策略设置	审核状态
	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
System	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 AWS Directory Service 控制台或 API 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至其他 AWS 账户、AWS 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。

有关这些日志组以及如何读取它们的数据的更多信息，请参阅《Amazon CloudWatch Logs 用户指南》中的使用日志组和日志流。

> **Note**
>
> 日志转发是 AWS Managed Microsoft AD 的一项区域功能。如果您使用的是 多区域复制，则必须分别在每个区域中应用以下过程。有关更多信息，请参阅 全局与区域特色。

启用日志转发

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

2. 选择您要共享的 AWS Managed Microsoft AD 目录的目录 ID。
3. 在报告详细信息页面上，执行以下操作之一：
   - 如果多区域复制下显示多个区域，选择想要启用日志转发的区域，然后选择网络与安全选项卡。有关更多信息，请参阅 主区域与其他区域。
   - 如果多区域复制下未显示任何区域，选择网络与安全选项卡。
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. 选择创建新的 CloudWatch 日志组，在 CloudWatch 日志组名称下，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 AWS Directory Service 控制台导航窗格中，选择目录。
2. 选择您要共享的 AWS Managed Microsoft AD 目录的目录 ID。
3. 在报告详细信息页面上，执行以下操作之一：
   - 如果多区域复制下显示多个区域，选择想要禁用日志转发的区域，然后选择网络与安全选项卡。有关更多信息，请参阅 主区域与其他区域。
   - 如果多区域复制下未显示任何区域，选择网络与安全选项卡。
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)。

使用 CLI 启用日志转发

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，然后才能使用 `ds create-log-subscription` 命令。要使用 CLI 启用日志转发，请完成以下所有步骤。

步骤 1：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'
```

有关如何建立 CloudWatch Logs 组的详细说明，请参阅《Amazon CloudWatch Logs 用户指南》中的在 CloudWatch Logs 中创建日志组。

步骤 2：在 IAM 中创建 CloudWatch Logs 资源策略

创建 CloudWatch Logs 资源策略来向 AWS Directory Service 授予权限以向您在步骤 1 中创建的新日志组添加日志。您可以为日志组指定确切的 ARN 以限制 AWS 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将包含您的目录驻留其中的 AWS 账户的以 /aws/directoryservice/ 开头的所有日志组。

```
{
    "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
```

步骤 3：创建 AWS 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

AWS Directory Service 与 Amazon CloudWatch 集成，可帮助您为其中的每个域控制器提供重要的性能指标Active Directory。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。您还可以配置告警并启动自动操作，以应对高利用率时段。例如，您可以为域控制器 CPU 利用率超过 70% 配置告警，并创建一个 SNS 主题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 AWS Lambda 函数），从而增加您的Active Directory域控制器的数量。

有关监控域控制器的更多信息，请参阅 确定何时添加带有 CloudWatch 指标的域控制器。

Amazon 会收取相关费用 CloudWatch。有关更多信息，请参阅CloudWatch账单和费用。

> **Important**
>
> 的域控制器性能指标在加拿大西部（卡尔加里）地区不可用。 CloudWatch

在中查找域控制器性能指标 CloudWatch

在 Amazon 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条件。使用以下步骤找到在中设置 AWS 托管 Microsoft AD 域控制器指标所需的正确命名空间和从属指标 CloudWatch。

在控制台中查找域 CloudWatch 控制器指标

1. 登录 AWS Management Console 并打开 CloudWatch 控制台，网址为 https://console.aws.amazon.com/cloudwatch/。
2. 在导航窗格中，选择指标。
3. 从指标列表中选择 Directory Service 命名空间，然后从列表中选择 AWS Managed Microsoft AD 指标。

有关如何使用控制 CloudWatch 台设置域控制器指标的说明，请参阅 AWS 安全博客中的如何根据利用率指标自动扩展 Microsoft AD AWS 托管。

确定何时添加带有 CloudWatch 指标的域控制器

在所有域控制器之间进行负载平衡对于您的弹性和性能非常重要Active Directory。为了帮助您优化 AWS 托管 Microsoft AD 中域控制器的性能，我们建议您首先监控重要指标 CloudWatch 以形成基准。在此过程中，您可以分析Active Directory一段时间内的平均利用率和峰值Active Directory利用率。确定基准后，您可以定期监控这些指标，以帮助确定何时向您的域控制器添加域控制器Active Directory。

以下指标对于定期监控非常重要。有关中可用域控制器指标的完整列表 CloudWatch，请参阅AWS 托管微软 AD 性能计数器。

- 特定于域控制器的指标，例如：
  - 处理器
  - 内存
  - 逻辑磁盘
  - 网络接口
- AWS 托管 Microsoft AD 目录特定的指标，例如：

- LDAP 搜索
- 绑定
- DNS 查询
- 目录读取
- 目录写入

有关如何使用控制 CloudWatch 台设置域控制器指标的说明，请参阅 AWS 安全博客中的如何根据利用率指标自动扩展 Microsoft AD AWS 托管。有关中指标的一般信息 CloudWatch，请参阅《亚马逊 CloudWatch 用户指南》中的使用亚马逊 CloudWatch 指标。

有关域控制器规划的一般信息，请参阅 Microsoft 网站上的Active Directory域服务容量规划。

AWS 托管微软 AD 性能计数器

下表列出了亚马逊中可用的所有性能计数器， CloudWatch 用于跟踪 AWS 托管 Microsoft AD 中的域控制器和目录性能。

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/秒
	I/O 日志写入平均延迟
DirectoryServices (NTDS)	LDAP 绑定时间
	DRA 挂起的复制操作
	DRA 挂起的复制同步
DNS	递归查询/秒
	递归查询失败/秒
	TCP 接收查询/秒

指标类别	指标名称
	总接收查询/秒
	总发送响应/秒
	UDP 接收查询/秒
LogicalDisk	Avg. Disk Queue Length
	% 可用空间
内存	% Committed Bytes in Use
	长期平均备用缓存寿命（秒）
网络接口	发送的字节数/秒
	Bytes Received/sec
	当前带宽
NTDS	ATQ 估计队列延迟
	ATQ 请求延迟
	DS 目录读取/秒
	DS 目录搜索/秒
	DS 目录写入/秒
	LDAP 客户端会话
	LDAP 搜索/秒
	LDAP 成功绑定/秒
处理器	% 处理器时间
安全系统范围的统计	Kerberos 身份验证

指标类别	指标名称
	NTLM 身份验证

多区域复制

多区域复制可用于在多个 AWS 区域区域之间自动复制你的 Microsoft AD AWS 托管目录数据。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。 AWS 托管 Microsoft AD 使用本机 Active Directory 复制功能将你的目录数据安全地复制到新区域。

只有 AWS 托管 Microsoft AD 的企业版支持多区域复制。

在大多数 AWS Managed Microsoft AD 可用的区域中，可以使用自动多区域复制。

Important

在以下可选择加入的区域中，多区域复制不可用：

- 非洲（开普敦）(af-south-1)
- 亚太地区（香港）ap-east-1
- 亚太地区（海得拉巴）ap-south-2
- 亚太地区（雅加达）ap-southeast-3
- 亚太地区（墨尔本）ap-southeast-4
- 加拿大西部（卡尔加里）ca-west-1
- 欧洲（米兰）(eu-south-1)
- 欧洲（西班牙）eu-south-2
- 欧洲（苏黎世）eu-central-2
- 以色列（特拉维夫）il-central-1
- 中东（巴林）me-south-1
- 中东（阿联酋）me-central-1

有关可选区域以及如何启用这些区域的更多信息，请参阅AWS Account Management 指南中的指定 AWS 区域 您的账户可以使用哪个区域。

优势

借助 AWS 托管 Microsoft AD 中的多区域复制，支持 Active Directory 的应用程序在本地使用目录以获得高性能，使用多区域功能实现弹性。您可以将多区域复制与支持活动目录的应用程序（例如 SharePoint SQL Server Always On）以及适用于 SQL Server 的 Amazon RDS 和适用于 Windows File Server 的 FSX 等 AWS 服务一起使用。多区域复制具备以下额外优势。

- 它允许您在全球范围内快速部署单个 AWS 托管 Microsoft AD 实例，并消除了自我管理全球 Active Directory 基础设施的繁重工作。
- 它使您可以更轻松、更经济地在多个 AWS 区域部署和管理 Windows 和 Linux 工作负载。自动多区域复制可在支持全局 Active Directory 的应用程序中实现最佳性能。部署在 Windows 或 Linux 实例中的所有应用程序都使用该区域的本地 AWS 托管 Microsoft AD，这样可以从尽可能接近的区域响应用户请求。
- 它提供多区域弹性。Microsoft AD AWS 托管部署在高度可用的 AWS 托管基础架构中，可处理所有区域底层 Active Directory 基础设施的自动软件更新、监控、恢复和安全。这使您可以专注于构建应用程序。

主题

- 全局与区域特色
- 主区域与其他区域
- 多区域复制的工作原理
- 添加复制区域
- 删除复制区域

全局与区域特色

使用多区域复制将 AWS 区域添加到目录中时， AWS Directory Service 可以扩大所有功能的范围，使其具有区域感知能力。这些功能列在详细信息页面的各个选项卡上，在 AWS Directory Service 控制台中选择目录 ID 时会显示该页面。这意味着所有功能都将根据您在控制台的多区域复制部分中选择的区域来启用、配置或管理。您对每个区域中的功能所做的更改要么应用于全局，要么应用于每个区域。

只有 AWS 托管 Microsoft AD 的企业版支持多区域复制。

全局功能

您在选择 主 区域 时对全局功能所做的任何更改都将应用于所有区域。

您可以在目录详细信息页面上识别全局使用的功能，因为这些功能旁边会显示应用于所有复制的区域。或者，如果您在列表中选择的另一个区域不是主区域，则可以识别全局使用的功能，因为它们会显示继承自主区域。

区域功能

您对 其他区域 中的功能所做的任何更改都将仅应用于该区域。

您可以在目录详细信息页面上识别区域使用的功能，因为这些功能旁边不会显示应用于所有复制的区域或继承自主区域。

主区域与其他区域

对于多区域复制，Microsoft AD AWS 托管使用以下两种类型的区域来区分如何在目录中应用全球或区域功能。

主 区域

您最初创建目录的初始区域称为主区域。您只能执行全局目录级别的操作，例如创建 Active Directory 信任以及从主区域更新 AD 架构。

主区域始终可以标识为显示在多区域复制部分中列表顶部的第一个区域，并以 – 主结尾。例如，美国东部（弗吉尼亚州北部）– 主。

您在选择主区域时对 全局功能 所做的任何更改都将应用于所有区域。

您只能在选择主区域时添加区域。有关更多信息，请参阅添加复制区域。

其他区域

您添加到目录中的任何区域都称为其他区域。

尽管有些功能可以在所有区域内进行全局管理，但其他功能则按区域单独管理。要管理其他区域（非主区域）的功能，必须先从目录详细信息页面上多区域复制部分的列表中选择其他区域。然后，您可以继续管理该功能。

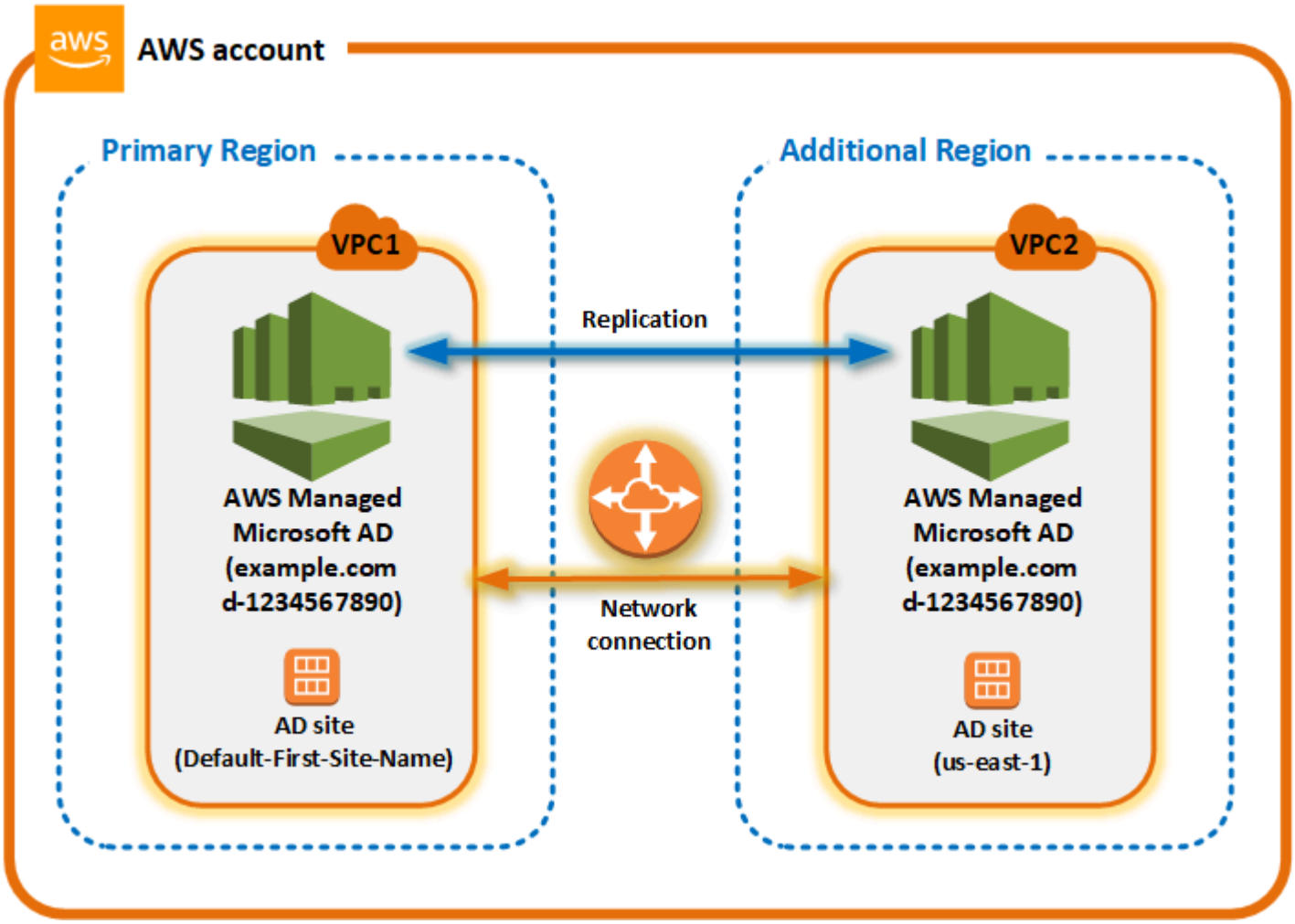
您在选择其他区域时对 区域功能 所做的任何更改都将仅应用于该区域。

多区域复制的工作原理

借助多区域复制功能，Microsoft AD AWS 托管消除了管理全球 Active Directory 基础设施的无差别繁重的工作。配置后，跨多个 AWS 区域 AWS 复制所有客户目录数据，包括用户、群组、群组策略和架构。

添加新区域后，将自动执行以下操作，如图所示：

- AWS 托管 Microsoft AD 在选定的 VPC 中创建两个域控制器，并使用同一个 AWS 账户将它们部署到新的区域。您的目录标识符 (`directory_id`) 在所有地区保持不变。如果需要，您可以稍后添加额外的域控制器。
- AWS 托管 Microsoft AD 配置主区域和新区域之间的网络连接。
- AWS 托管 Microsoft AD 创建了一个新的 Active Directory 站点，并将其命名为与该区域相同的名称，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。
- AWS Microsoft AD 将所有 Active Directory 对象和配置复制到新区域，包括用户、群组、群组策略、活动目录信任、组织单位和活动目录架构。Active Directory 站点链接配置为使用更改通知。启用站点间更改通知后，更改会以与源站点内部相同的频率传播到远程站点，包括需要紧急复制的更改。
- 如果这是你添加的第一个区域，则 AWS 托管 Microsoft AD 会将所有功能设置为多区域感知。有关更多信息，请参阅全局与区域特色。



Active Directory 站点

多区域复制支持多个活动目录站点（每个区域一个 Active Directory 站点）。添加新区域时，其命名的名称与该区域的名称相同，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。

AWS 服务

AWS 诸如 Amazon RDS for SQL Server 和 Amazon FSx 之类的服务连接到全局目录的本地实例。这样，您的用户只需登录一次即可登录任何 AWS 区域中运行的支持活动目录的应用程序以及诸如 Amazon RDS AWS for Amazon SQL Server 之类的 AWS 服务。为此，当你信任 AWS 托管的 Microsoft AD 时，用户需要来自托管 Microsoft AD 或本地 Active Directory 的凭证。 AWS

您可以将以下 AWS 服务与多区域复制功能配合使用。

- 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
- Amazon Aurora for MySQL
- Amazon Aurora for PostgreSQL

失效转移

如果一个区域中的所有域控制器都出现故障，Micro AWS soft AD 会恢复域控制器并自动复制目录数据。同时，其他区域的域控制器保持正常运行。

添加复制区域

当您使用该多区域复制功能添加区域时，Microsoft AD AWS 托管会在选定的 AWS 区域中创建两个域控制器，即亚马逊虚拟私有云 (VPC) Virtual Private Cloud 和子网。 AWS 托管 Microsoft AD 还会创建相关的安全组，使 Windows 工作负载能够连接到你在新区域中的目录。它还使用已部署目录的相同 AWS 帐户创建这些资源。选择区域、指定 VPC 并提供新区域的配置来完成此操作。

只有 AWS 托管 Microsoft AD 的企业版支持多区域复制。

先决条件

在继续执行添加新复制区域的步骤之前，建议先查看以下先决条件任务。

- 确认您在要将目录复制到的新区域中拥有必要的 AWS Identity and Access Management (IAM) 权限、Amazon VPC 设置和子网设置。
- 如果您想使用现有的本地 Active Directory 凭据来访问和管理中支持 Active Directory 的工作负载 AWS，则必须在托管 AWS Microsoft AD 和您的本地 AD 基础设施之间创建活动目录信任。有关信任的更多信息，请参阅 Connect 连接到您现有的活动目录基础架构。
- 如果您的本地 Active Directory 之间存在信任关系，并且想要添加复制区域，则需要确认在要将目录复制到的新区域中是否设置了必要的 Amazon VPC 和子网。

添加区域

使用以下步骤为您的 AWS 托管 Microsoft AD 目录添加复制区域。

添加复制区域

1. 在 AWS Directory Service 控制台导航窗格中，选择目录。
2. 在目录页面上，选择您的目录 ID。
3. 在目录详细信息页面的多区域复制下，从列表中选择主区域，然后选择添加区域。

> **Note**
>
> 您只能在选择主区域时添加区域。有关更多信息，请参阅主 区域。

4. 在添加区域页面的区域下，从列表中选择要添加的区域。
5. 在VPC下，选择要用于该区域的 VPC。

> **Note**
>
> 此 VPC 的无类别域间路由（CIDR）不得与该目录在另一个区域中使用的 VPC 重叠。

6. 在子网下，选择要用于该区域的子网。
7. 查看定价下的信息，然后选择添加。
8. 当 AWS 托管 Microsoft AD 完成域控制器部署过程后，该区域将显示活动状态。现在，您可以根据需要对该区域进行更新。

后续步骤

在添加新区域后，您应考虑执行以下后续步骤：

- 根据需要将额外的域控制器（最多 20 个）部署到新区域。默认情况下，添加新区域时的域控制器数量为 2 个，这是实现容错和高可用性所需的最小数量。有关更多信息，请参阅添加或移除额外的域控制器。
- 与每个地区的更多 AWS 账户共享您的目录。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。
- 启用日志转发功能，使用新区域的 Amazon CloudWatch 日志检索目录的安全日志。启用日志转发时，您必须在复制目录的每个区域中提供一个日志组名称。有关更多信息，请参阅启用日志转发。
- 为新区域启用 Amazon Simple Notification Service（Amazon SNS），以跟踪每个区域的目录运行状况。有关更多信息，请参阅使用 Amazon SNS 配置目录状态通知。

删除复制区域

使用以下步骤删除您的 Microsoft AD AWS 托管目录的区域。在删除某个区域之前，请确保该区域不包含以下任何一项：

- 附加到其上的授权应用程序。
- 与之关联的共享目录。

删除复制区域

1. 在 AWS Directory Service 控制台导航窗格中，选择目录。
2. 在导航栏中，选择区域选择器，然后选择存储目录的区域。
3. 在目录页面上，选择您的目录 ID。
4. 在目录详细信息页面的多区域复制下，选择删除区域。
5. 在删除区域对话框中，查看信息，然后输入区域名称进行确认。然后选择删除。

> **Note**
>
> 在删除该地区期间，您无法对其进行更新。

共享您的目录

AWS Managed Microsoft AD 与 AWS Organizations 紧密集成，以允许跨多个 AWS 账户的无缝目录共享。您可以将单个目录与相同组织中的其他可信 AWS 账户分享，也可以将目录与组织外的其他 AWS 账户分享。您也可以在 AWS 账户目前不是组织的成员时共享目录。

> **Note**
>
> AWS 会收取额外的目录共享费用。要了解更多信息，请参阅 AWS Directory Service 网站上的定价页面。

目录共享使 AWS Managed Microsoft AD 成为了与多个账户和 VPC 中的 Amazon EC2 进行集成的更经济高效的方式。目录共享在所有提供 AWS Managed Microsoft AD 的 AWS 区域中可用。

> **Note**
>
> 在 AWS 中国（宁夏）区域，此功能仅在使用 AWS Systems Manager（SSM）无缝加入 Amazon EC2 实例时可用。

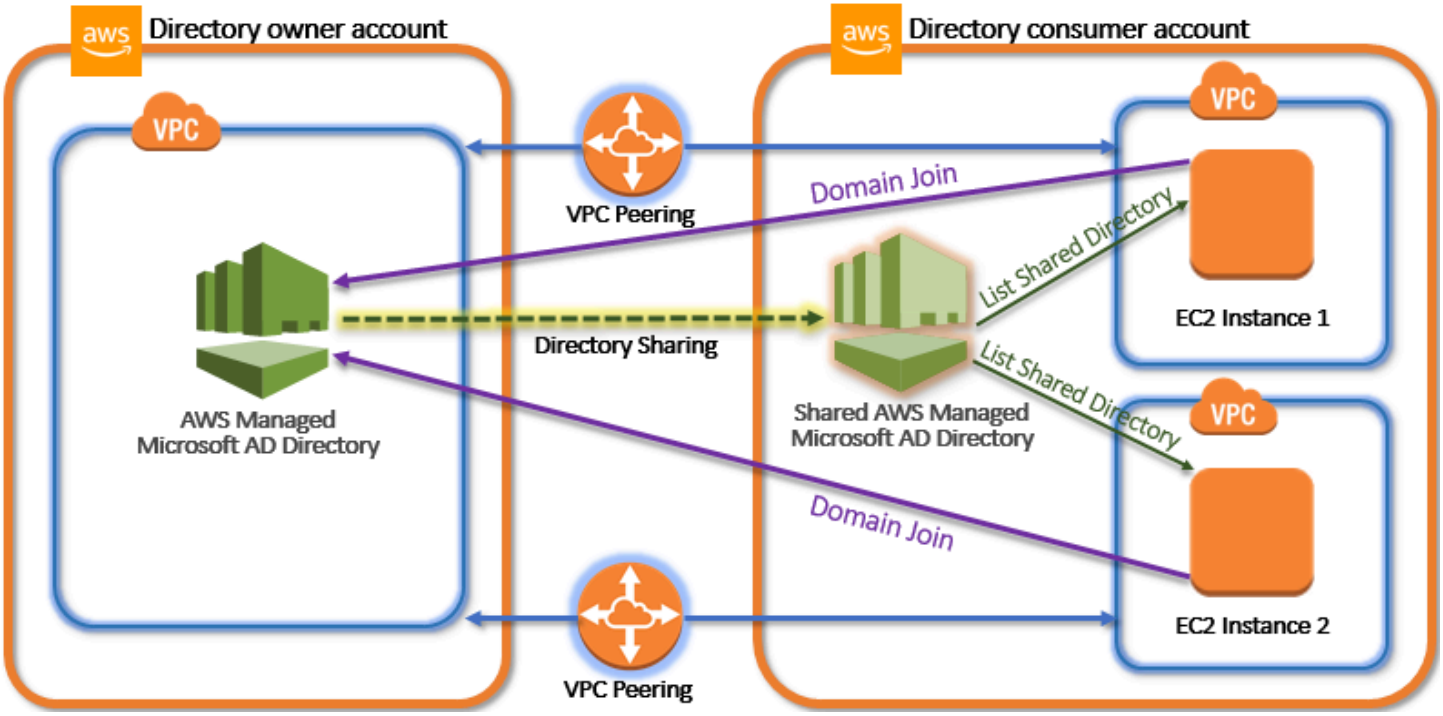
有关目录共享以及如何跨 AWS 账户边界扩展您的 AWS Managed Microsoft AD 目录覆盖范围的更多信息，请参阅以下主题。

主题

- 关键目录共享概念
- 教程：共享您的 AWS 托管 Microsoft AD 目录以实现无缝加入 EC2 域名
- 取消共享您的目录

关键目录共享概念

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

目录拥有者是在共享目录关系中，拥有原始目录的 AWS 账户 持有人。此账户中的管理员可以通过指定与其共享目录的 AWS 账户 来发起目录共享。目录所有者可以在 AWS Directory Service 控制台中使用给定目录的扩展和共享选项卡查看他们与谁共享了该目录。

目录使用者账户

在共享目录关系中，目录使用者表示目录所有者与之共享目录的 AWS 账户。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

AWS Managed Microsoft AD 提供了以下两种目录共享方法：

- AWS 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，您的组织必须启用了所有功能，目录必须在组织的管理账户中。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，此方法被称为将此目录与您组织内的 AWS 账户 共享。
- 握手 – 此方法在您未使用 AWS Organizations 时启用目录共享。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，此方法被称为与其他 AWS 账户 共享此目录。

网络连接

网络连接是跨 AWS 账户 使用目录共享关系的先决条件。AWS 支持多种连接 VPC 的解决方案，其中一些解决方案包括 VPC 对等、传输网关和 VPN。要了解其用法，请参阅 教程：共享您的 AWS 托管 Microsoft AD 目录以实现无缝加入 EC2 域名。

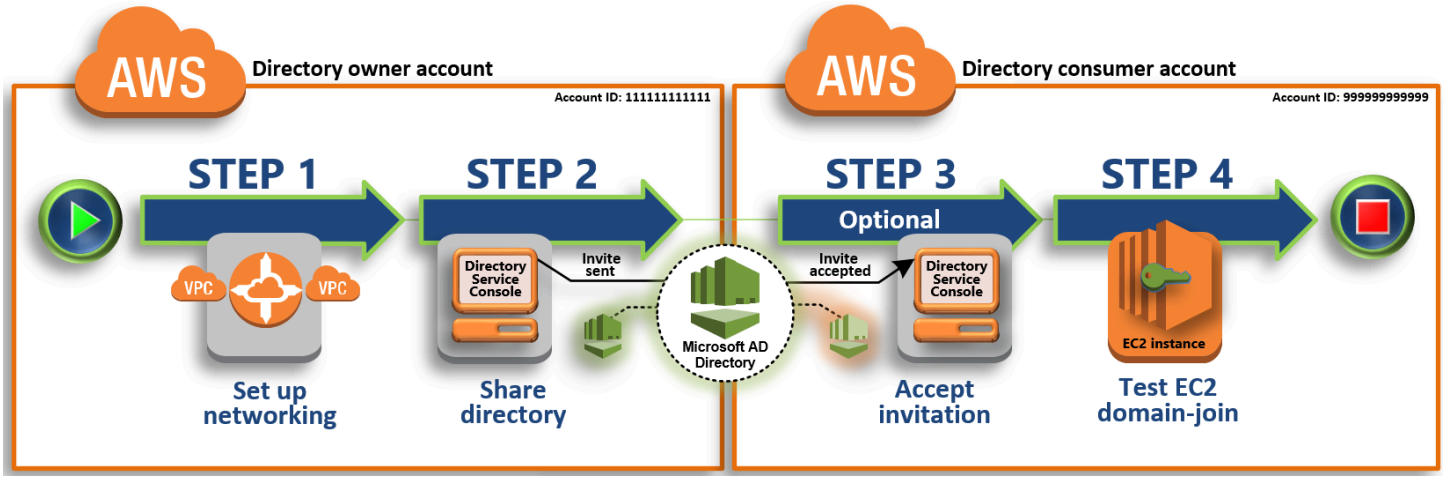
教程：共享您的 AWS 托管 Microsoft AD 目录以实现无缝加入 EC2 域名

本教程向您展示如何与另一个（目录使用者帐户）共享您的 AWS 托管 Microsoft AD 目录 AWS 账户（目录所有者帐户）。完成联网先决条件后，您将在两者之间共享一个目录 AWS 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，请参阅关键目录共享概念。

共享目录的过程会有所不同，具体取决于您是与同一 AWS 组织 AWS 账户 中的其他人共享目录还是与 AWS 组织外部的帐户共享目录。有关共享的工作方式的更多信息，请参阅共享方法。

此工作流程具有四个基本步骤。



步骤 1：设置网络环境

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。

步骤 2：共享目录

使用目录拥有者管理员凭证登录后，您可以打开 AWS 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

使用目录使用者管理员凭据登录后，您可以打开 AWS Directory Service 控制台并接受目录共享邀请。

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

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：共享目录以便将 Amazon EC2 实例无缝加入 AWS 账户账户的域
- AWS 安全博客文章：如何将来自多个账户和 VPC 的 Amazon EC2 实例加入到单个 AWS 托管的 Microsoft AD 目录中

步骤 1：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：

- 在同一个区域中创建两个新的 AWS 账户 用于测试目的。当您创建时 AWS 账户，它会自动在每个账户中创建一个专用的虚拟私有云 (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。

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 https://console.aws.amazon.com/vpc/ 打开 Amazon VPC 控制台。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：
   - Peering connection name tag (对等连接名称标签)：提供一个名称，用于在目录使用者账户中清楚地标识与 VPC 的此连接。
   - VPC (Requester) (VPC (申请方))：选择目录拥有者账户的 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 (Accepter) (VPC (接受方))：选择目录使用者账户的 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 Amazon VPC 控制台的路由表部分，选择目录所有者 VPC 的路由表。
2. 在路由选项卡中选择编辑路由，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 Amazon VPC 控制台的路由表部分，选择目录使用者 VPC 的路由表。
2. 在路由选项卡中选择编辑路由，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 VPC 的安全组和 AWS Managed Microsoft AD 先决条件。

下一步

步骤 2：共享目录

步骤 2：共享目录

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 AWS 托管 Microsoft AD 的一项区域功能。如果您使用的是 多区域复制，则必须分别在每个区域中应用以下过程。有关更多信息，请参阅 全局与区域特色。

从目录拥有者账户共享您的目录

1. 使用目录所有者账户中的管理员 AWS Management Console 凭据登录并打开AWS Directory Service 控制台，网址为 https://console.aws.amazon.com/directoryservicev2/。
2. 在导航窗格中，选择目录。
3. 选择要共享的 AWS 托管 Microsoft AD 目录的目录 ID。
4. 在报告详细信息页面上，执行以下操作之一：
   - 如果多区域复制下显示多个区域，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 主区域与其他区域。
   - 如果多区域复制下未显示任何区域，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 “选择 AWS 账户 要与之共享的对象” 页面上，根据您的业务需求选择以下共享方法之一：

   a. 与组织 AWS 账户 内部共享此目录 — 使用此选项，您可以从显示 AWS 组织 AWS 账户 内部所有内容的列表中选择要与之共享的目录。 AWS 账户 在共享目录 AWS Directory Service 之前，必须启用可信访问权限。有关更多信息，请参阅如何启用或禁用可信访问。

   > **Note**
   >
   > 要使用此选项，您的组织必须启用了所有功能，目录必须在组织的管理账户中。

      i. AWS 账户 在您的组织中，选择要与之 AWS 账户 共享目录的，然后单击 “添加”。

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。由于所有 AWS 账户 人都在同一个组织中，因此您无需执行步骤 3。

b. 与其他人共享此目录 AWS 账户-使用此选项，您可以与 AWS 组织内部或外部的帐户共享该目录。当您的目录不是某个 AWS 组织的成员，而您想与其他人共享时，也可以使用此选项 AWS 账户。

i. 在 AWS 账户 ID 中，输入要与之共享目录的所有 AWS 账户 ID，然后单击添加。

ii. 在发送注释中，键入要发送给其他 AWS 账户中的管理员的消息。

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

第 3 步：接受共享目录邀请-可选

如果您在上一步中选择与其他 AWS 账户共享此目录（握手方法）选项，则应使用此过程完成共享目录工作流。如果您选择了与组织 AWS 账户 内部共享此目录选项，请跳过此步骤并继续执行步骤 4。

接受共享目录邀请

1. 使用目录消费者账户中的管理员 AWS Management Console 凭据登录并打开AWS Directory Service 控制台，网址为 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

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

步骤 4：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将 EC2 实例加入域。

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这些步骤。

1. 登录 AWS Management Console 并打开亚马逊 EC2 控制台，网址为 https://console.aws.amazon.com/ec2/。
2. 在导航栏中，选择与现有目录 AWS 区域 相同的目录。
3. 在 EC2 控制面板的启动实例部分，选择启动实例。
4. 在启动实例页面的名称和标签部分下，输入您要用于 Windows EC2 实例的名称。
5. （可选）选择添加其他标签，添加一个或多个标签密钥值对，以组织、跟踪或控制对此 EC2 实例的访问权限。
6. 在应用程序和操作系统映像（亚马逊机器映像）部分，在快速入门窗格中选择 Windows。您可以从亚马逊机器映像（AMI）下拉列表中更改 Windows 亚马逊机器映像（AMI）。
7. 在实例类型部分，从实例类型下拉列表中选择要使用的实例类型。
8. 在密钥对（登录）部分，您可以选择创建新密钥对，或从现有密钥对中进行选择。

   a. 要创建新的密钥对，请选择新建新密钥对。
   b. 输入密钥对的名称，然后为密钥对类型和私钥文件格式选择一个选项。
   c. 要以可与 OpenSSH 一起使用的格式保存私钥，请选择 pem。要以可与 PuTTY 一起使用的格式保存私钥，请选择 ppk。
   d. 选择创建密钥对。
   e. 您的浏览器会自动下载私有密钥文件。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。

9. 在启动实例页面的网络设置部分下，选择编辑。从 VPC – 必需下拉列表中选择创建目录的 VPC。
10. 从子网下拉列表中选择 VPC 中的其中一个公有子网。选择的子网必须将所有外部流量都路由到互联网网关。否则将无法远程连接到实例。

    有关如何连接到互联网网关的更多信息，请参阅《Amazon VPC 用户指南》中的使用互联网网关连接到互联网。

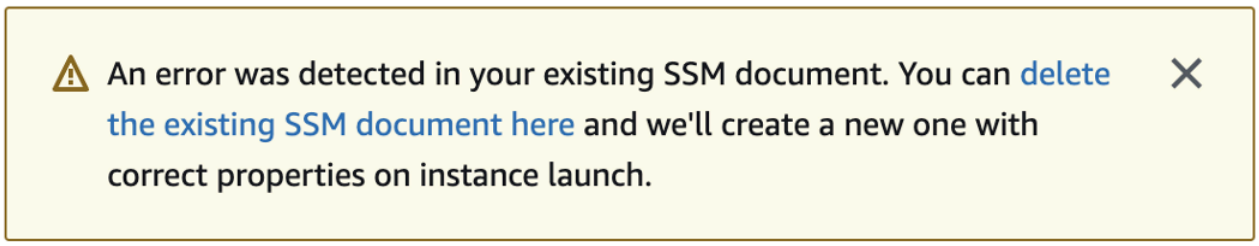
11. 在自动分配公有 IP 下，选择启用。

    有关公有和私有 IP 寻址的更多信息，请参阅《亚马逊 EC2 用户指南》中的 Amazon EC2 实例 IP 寻址。

12. 对于防火墙（安全组）设置，您可以使用默认设置或进行更改以满足您的需求。

13. 对于配置存储设置，您可以使用默认设置或进行更改以满足您的需求。

14. 选择高级详细信息部分，从域加入目录下拉列表中选择您的域。

    > **Note**
    >
    > 选择域加入目录后，您可能会看到：
    >
    > 
    >
    >
    > 如果 EC2 启动向导识别出具有意外属性的现有 SSM 文档，则会发生此错误。您可以执行以下操作之一：
    >
    > - 如果您之前编辑了 SSM 文档并且属性符合预期，请选择关闭并继续启动 EC2 实例，不做任何更改。
    > - 选择 “在此处删除现有 SSM 文档” 链接以删除 SSM 文档。这将允许创建具有正确属性的 SSM 文档。SSM 文档将在您启动 EC2 实例时自动创建。

15. 对于 IAM 实例配置文件，您可以选择现有的 IAM 实例配置文件或创建新的 IAM 实例配置文件。从 IAM 实例配置文件下拉列表中选择一个DirectoryServiceAccess附有 AWS 托管策略 AmazonSSM ManagedInstanceCore 和 AmazonSSM 的 IAM 实例配置文件。要创建新的 IAM 个人资料链接，请选择创建新的 IAM 个人资料链接，然后执行以下操作：

    1. 选择 创建角色。
    2. 在选择受信任的实体下，选择 AWS 服务。
    3. 在 Use case（使用案例）下，选择 EC2。
    4. 在 “添加权限” 下的策略列表中，选择 AmazonSSM ManagedInstanceCore 和 AmazonSSM 政策。DirectoryServiceAccess在搜索框中键入 **SSM** 以筛选列表。选择下一步。

> **Note**
>
> AmazonSSM DirectoryServiceAccess 提供了将实例加入Active Directory托管者的权限。 AWS Directory ServiceAmazonSSM ManagedInstanceCore 提供使用该服务所需的最低权限。 AWS Systems Manager 有关创建具有这些权限的角色的更多信息，以及您可以分配给 IAM 角色的其他权限和策略的信息，请参阅《AWS Systems Manager 用户指南》中的为 Systems Manager 创建 IAM 实例配置文件。

5. 在名称、查看和创建页面上，输入角色名称。您将需要此角色名称来附加到 EC2 实例。
6. （可选）您可以在描述字段中提供 IAM 实例配置文件的描述。
7. 选择 创建角色。
8. 返回启动实例页面，选择 IAM 实例配置文件旁边的刷新图标。您的新 IAM 实例配置文件应显示在 IAM 实例配置文件下拉列表中。选择新的配置文件，其余设置保留默认值。

16. 选择启动实例。

方法 2：使用测试域加入 AWS Systems Manager

在目录使用者账户中使用这些步骤。要完成此过程，您需要有关目录所有者账户的一些信息，例如目录 ID、目录名称和 DNS IP 地址。

先决条件

- 设置 AWS Systems Manager。
  - 有关 Systems Manager 的更多信息，请参阅 AWS Systems Manager的常规设置。
- 您希望加入微软活动目录 AWS 托管域的实例必须附加一个包含 AmazonSSM ManagedInstanceCore 和 A mazonSSM 托管策略的 I A DirectoryServiceAccess M 角色。
  - 有关可以为 Systems Manager 附加的此类托管和其他策略的更多信息，请参阅《AWS Systems Manager 用户指南》中的为 Systems Manager 创建 IAM 实例配置文件。有关托管策略的更多信息，请参阅《IAM 用户指南》中的 AWS 托管策略。

有关使用 Systems Manager 将 EC2 实例加入 AWS 托管的 Microsoft Active Directory 域的更多信息，请参阅AWS Systems Manager 如何使用将正在运行的 EC2 Windows 实例加入我的 AWS 目录服务域？ 。

1. 打开 AWS Systems Manager 控制台，网址为https://console.aws.amazon.com/systems-manager/。
2. 在导航窗格的节点管理下，选择运行命令。
3. 选择 Run command（运行命令）。
4. 在运行命令页面上，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：

   > **Note**
   >
   > 返回 AWS Directory Service 控制台，选择 “与我共享的目录”，然后选择您的目录，即可找到目录 ID、目录名称和 DNS IP 地址。目录 ID 可以在共享目录的详细信息部分下找到。您可以在所有者目录详细信息部分下找到目录名称和 DNS IP 地址的值。

   - 在 “目录 ID” 中，输入 AWS 托管 Microsoft 活动目录的名称。
   - 对于目录名称，输入 AWS Managed Microsoft Active Directory（对于目录所有者账户）。
   - 对于 DNS IP 地址，请在 AWS 托管 Microsoft 活动目录（适用于目录所有者帐户）中输入 DNS 服务器的 IP 地址。
6. 对于目标，选择手动选择实例，然后选择要加入域的实例。
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. 实例成功加入域后，命令状态将从待处理更改为成功。您可以依次选择加入域的实例的实例 ID 和查看输出来查看命令输出。

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，您可以使用来自 AWS 托管 Microsoft AD 用户帐户的凭据使用远程桌面协议 (RDP) 客户端登录您的实例。

取消共享您的目录

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

取消共享您的目录

1. 在 AWS Directory Service 控制台导航窗格的 Active Directory 下，选择目录。
2. 选择您要取消共享的 AWS Managed Microsoft AD 目录的目录 ID。
3. 在报告详细信息页面上，执行以下操作之一：

- 如果多区域复制下显示多个区域，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 主区域与其他区域。
- 如果多区域复制下未显示任何区域，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：共享目录以便将 Amazon EC2 实例无缝加入 AWS 账户的域
- AWS 安全博客文章：How to join Amazon EC2 instances from multiple accounts and VPCs to a single AWS Managed Microsoft AD directory
- Joining your Amazon RDS DB instances across accounts to a single shared domain

将 Amazon EC2 实例加入您的 AWS 托管微软 AD Active Directory

当 Amazon EC2 实例启动时，您可以将该实例无缝加入您的Active Directory域。有关更多信息，请参阅 将亚马逊 EC2 Windows 实例无缝加入你的 AWS 托管微软 AD Active Directory。您还可以使用 A AWS Systems Manager ut omation 直接从 AWS Directory Service 控制台启动 EC2 实例并将其加入 Active Directory域。

如果您需要手动将 EC2 实例加入您的Active Directory域，则必须在相应的区域和安全组或子网中启动该实例，然后将该实例加入域。

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，这要求互联网网关连接到 VPC，并且实例具有公有 IP 地址。

主题

- 在你的 AWS 托管 Microsoft AD 中启动目录管理实例 Active Directory
- 将亚马逊 EC2 Windows 实例无缝加入你的 AWS 托管微软 AD Active Directory
- 手动将 Amazon EC2 Windows 实例加入您的 AWS 托管微软 AD Active Directory
- 将亚马逊 EC2 Linux 实例无缝加入您的 AWS 托管微软 AD 活动目录
- 手动将亚马逊 EC2 Linux 实例加入您的 AWS 托管微软 AD 活动目录
- 使用 Winbind 手动将亚马逊 EC2 Linux 实例加入你的 AWS 托管微软 AD 活动目录

- 手动将亚马逊 EC2 Mac 实例加入您的 AWS 托管微软 AD 活动目录
- 委托 AWS Managed Microsoft AD 的目录加入权限
- 创建或更改 DHCP 选项集

在你的 AWS 托管 Microsoft AD 中启动目录管理实例 Active Directory

此过程在中启动 Amazon EC2 目录管理Windows实例， AWS Management Console 使用 AWS Systems Manager 自动化来管理您的目录。您也可以通过直接在自动化控制台ManagementInstance中运行自动化 AWS-createds 来完成此 AWS Systems Manager 操作。

先决条件

要从控制台启动目录管理 EC2 实例，您必须在账户中启用以下权限。

- `ds:DescribeDirectories`
- `ec2:AuthorizeSecurityGroupIngress`
- `ec2:CreateSecurityGroup`
- `ec2:CreateTags`
- `ec2:DeleteSecurityGroup`
- `ec2:DescribeInstances`
- `ec2:DescribeInstanceStatus`
- `ec2:DescribeKeyPairs`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeVpcs`
- `ec2:RunInstances`
- `ec2:TerminateInstances`
- `iam:AddRoleToInstanceProfile`
- `iam:AttachRolePolicy`
- `iam:CreateInstanceProfile`
- `iam:CreateRole`
- `iam:DeleteInstanceProfile`
- `iam:DeleteRole`

- iam:DetachRolePolicy
- iam:GetInstanceProfile
- iam:GetRole
- iam:ListAttachedRolePolicies
- iam:ListInstanceProfiles
- iam:ListInstanceProfilesForRole
- iam:PassRole
- iam:RemoveRoleFromInstanceProfile
- iam:TagInstanceProfile
- iam:TagRole
- ssm:CreateDocument
- ssm:DeleteDocument
- ssm:DescribeInstanceInformation
- ssm:GetAutomationExecution
- ssm:GetParameters
- ssm:ListCommandInvocations
- ssm:ListCommands
- ssm:ListDocuments
- ssm:SendCommand
- ssm:StartAutomationExecution
- ssm:GetDocument

要在中启动目录管理 EC2 实例 AWS Management Console

1. 登录 AWS Directory Service 控制台。
2. 在 Active Directory 下，选择目录。
3. 选择要在其中启动目录管理 EC2 实例的目录的目录 ID。
4. 在目录页面的右上角，选择操作。
5. 在 “操作” 下拉列表中，选择 “启动目录管理 EC2 实例”。
6. 在启动目录管理 EC2 实例页面的输入参数下，填写字段。

a. （可选）您可以为实例提供 key pair。从 “密钥对名称-可选” 下拉列表中，选择密钥对。

b. （可选）选择 “查看” AWS CLI 命令以查看您在中用于运行此自动化的示例。 AWS CLI

7. 选择提交。
8. 您将返回到目录页面。屏幕顶部会显示一个绿色闪烁栏，表示您已成功开始启动。

查看目录管理 EC2 实例

如果您尚未为目录启动任何 EC2 实例，则会在目录管理 EC2 实例下显示短划线（-）。

1. 在 Active Directory 下，选择目录，然后选择要查看的目录。
2. 在目录详细信息下，在目录管理 EC2 实例下，选择要查看的一个或所有实例。
3. 当您选择实例时，将被路由到 EC2 连接到实例页面，将远程桌面连接到实例。

将亚马逊 EC2 Windows 实例无缝加入你的 AWS 托管微软 AD Active Directory

此过程将亚马逊 EC2 Windows 实例无缝连接到您的 AWS 托管 Microsoft AD。如果您需要跨多个域名进行无缝联接 AWS 账户，请参阅教程：共享您的 AWS 托管 Microsoft AD 目录以实现无缝加入 EC2 域名。有关 Amazon EC2 的更多信息，请参阅什么是 Amazon EC2？。

无缝加入 Amazon EC2 Windows 实例

1. 登录 AWS Management Console 并打开亚马逊 EC2 控制台，网址为 https://console.aws.amazon.com/ec2/。
2. 在导航栏中，选择与现有目录 AWS 区域 相同的目录。
3. 在 EC2 控制面板的启动实例部分，选择启动实例。
4. 在启动实例页面的名称和标签部分下，输入您要用于 Windows EC2 实例的名称。
5. （可选）选择添加其他标签，添加一个或多个标签密钥值对，以组织、跟踪或控制对此 EC2 实例的访问权限。
6. 在应用程序和操作系统映像（亚马逊机器映像）部分，在快速入门窗格中选择 Windows。您可以从亚马逊机器映像（AMI）下拉列表中更改 Windows 亚马逊机器映像（AMI）。
7. 在实例类型部分，从实例类型下拉列表中选择要使用的实例类型。
8. 在密钥对（登录）部分，您可以选择创建新密钥对，或从现有密钥对中进行选择。

a. 要创建新的密钥对，请选择新建新密钥对。

b. 输入密钥对的名称，然后为密钥对类型和私钥文件格式选择一个选项。

c. 要以可与 OpenSSH 一起使用的格式保存私钥，请选择 pem。要以可与 PuTTY 一起使用的格式保存私钥，请选择 ppk。

d. 选择创建密钥对。

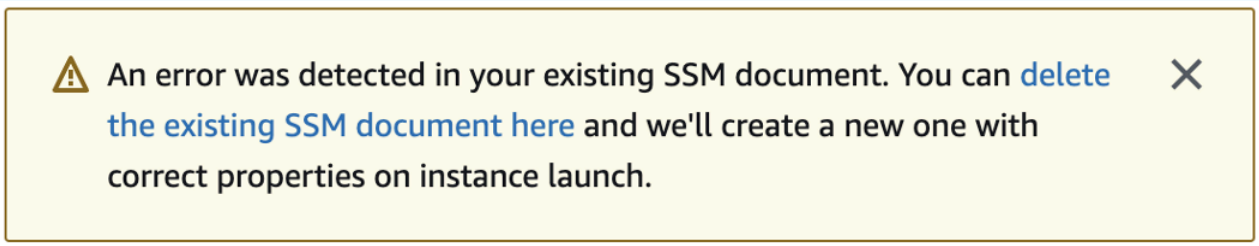
e. 您的浏览器会自动下载私有密钥文件。将私有密钥文件保存在安全位置。

> **Important**
>
> 这是您保存私有密钥文件的唯一机会。

9. 在启动实例页面的网络设置部分下，选择编辑。从 VPC – 必需下拉列表中选择创建目录的 VPC。
10. 从子网下拉列表中选择 VPC 中的其中一个公有子网。选择的子网必须将所有外部流量都路由到互联网网关。否则将无法远程连接到实例。

    有关如何连接到互联网网关的更多信息，请参阅《Amazon VPC 用户指南》中的使用互联网网关连接到互联网。
11. 在自动分配公有 IP 下，选择启用。

    有关公有和私有 IP 寻址的更多信息，请参阅《亚马逊 EC2 用户指南》中的 Amazon EC2 实例 IP 寻址。
12. 对于防火墙（安全组）设置，您可以使用默认设置或进行更改以满足您的需求。
13. 对于配置存储设置，您可以使用默认设置或进行更改以满足您的需求。
14. 选择高级详细信息部分，从域加入目录下拉列表中选择您的域。

> **Note**
>
> 选择域加入目录后，您可能会看到：
>
> 
>
>
> 如果 EC2 启动向导识别出具有意外属性的现有 SSM 文档，则会发生此错误。您可以执行以下操作之一：
>
> - 如果您之前编辑了 SSM 文档并且属性符合预期，请选择关闭并继续启动 EC2 实例，不做任何更改。

- 选择 “在此处删除现有 SSM 文档” 链接以删除 SSM 文档。这将允许创建具有正确属性的 SSM 文档。SSM 文档将在您启动 EC2 实例时自动创建。

15. 对于 IAM 实例配置文件，您可以选择现有的 IAM 实例配置文件或创建新的 IAM 实例配置文件。从 IAM 实例配置文件下拉列表中选择一个DirectoryServiceAccess附有 AWS 托管策略 AmazonSSM ManagedInstanceCore 和 AmazonSSM 的 IAM 实例配置文件。要创建新的 IAM 个人资料链接，请选择创建新的 IAM 个人资料链接，然后执行以下操作：

    1. 选择 创建角色。
    2. 在选择受信任的实体下，选择 AWS 服务。
    3. 在 Use case（使用案例）下，选择 EC2。
    4. 在 “添加权限” 下的策略列表中，选择 AmazonSSM ManagedInstanceCore 和 AmazonSSM 政策。DirectoryServiceAccess在搜索框中键入 **SSM** 以筛选列表。选择下一步。

    > **Note**
    >
    > AmazonSSM DirectoryServiceAccess 提供了将实例加入Active Directory托管者的权限。 AWS Directory ServiceAmazonSSM ManagedInstanceCore 提供使用该服务所需的最低权限。 AWS Systems Manager 有关创建具有这些权限的角色的更多信息，以及您可以分配给 IAM 角色的其他权限和策略的信息，请参阅《AWS Systems Manager 用户指南》中的为 Systems Manager 创建 IAM 实例配置文件。

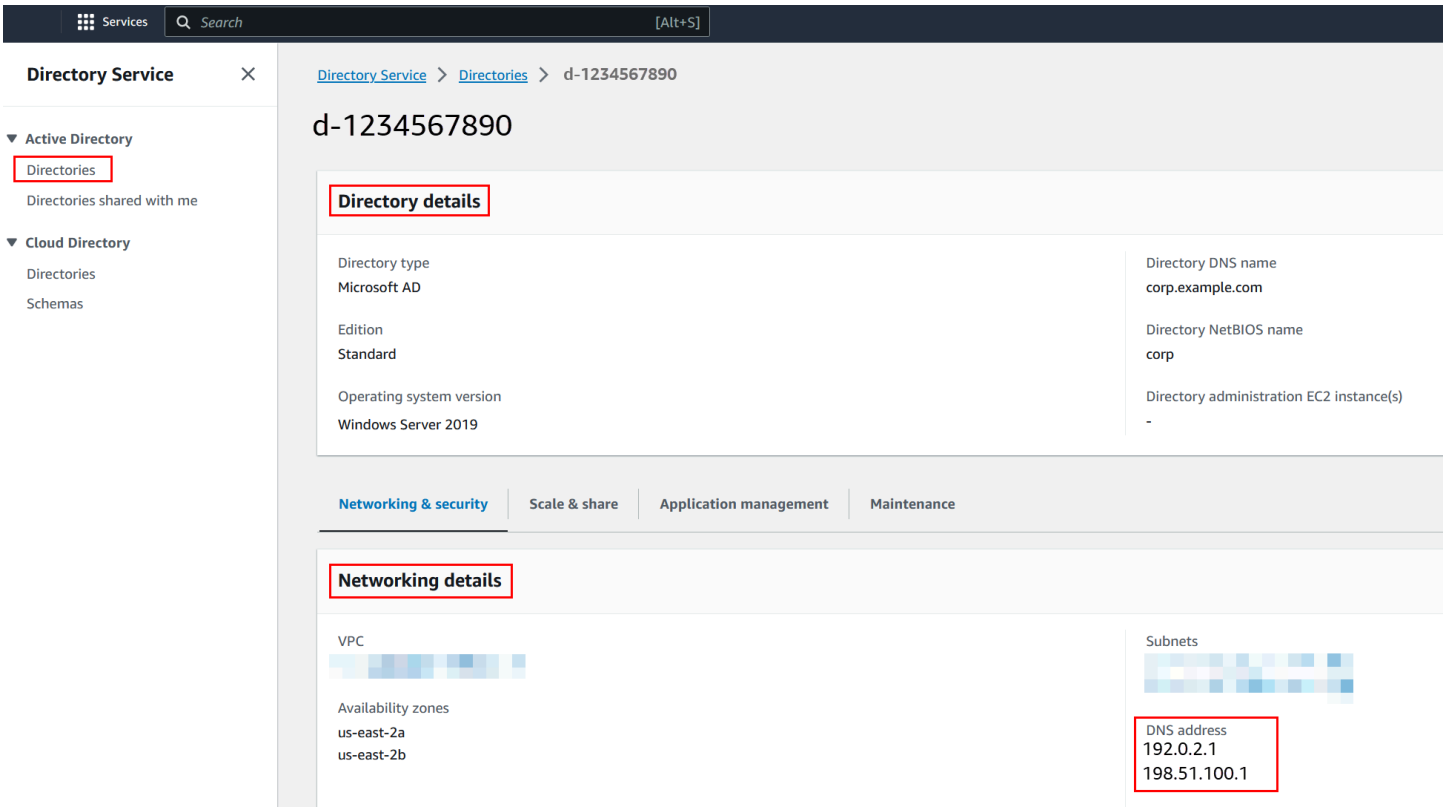
    5. 在名称、查看和创建页面上，输入角色名称。您将需要此角色名称来附加到 EC2 实例。
    6. （可选）您可以在描述字段中提供 IAM 实例配置文件的描述。
    7. 选择 创建角色。
    8. 返回启动实例页面，选择 IAM 实例配置文件旁边的刷新图标。您的新 IAM 实例配置文件应显示在 IAM 实例配置文件下拉列表中。选择新的配置文件，其余设置保留默认值。

16. 选择启动实例。

手动将 Amazon EC2 Windows 实例加入您的 AWS 托管微软 AD Active Directory

要手动将现有 Amazon EC2 Windows 实例加入 AWS 托管 Microsoft ADActive Directory，必须使用中指定的参数启动该实例将亚马逊 EC2 Windows 实例无缝加入你的 AWS 托管微软 AD Active Directory。

你需要微软 AD DNS AWS 托管服务器的 IP 地址。此信息可以在目录服务 > 目录 > 目录的目录 ID 链接 > 目录详细信息以及网络与安全下找到。

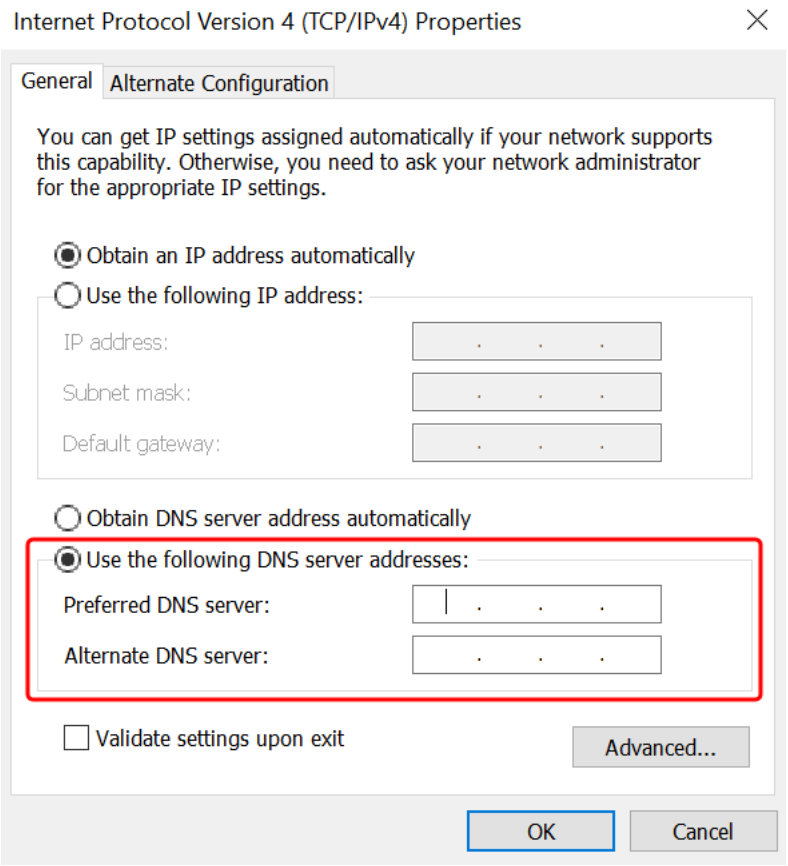


将 Windows 实例加入微软 AWS 托管 AD Active Directory

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. 选择 “使用以下 DNS 服务器地址”，将 “首选 DNS 服务器” 和 “备用 DNS 服务器地址” 更改为 Microsoft AD 提供的 AWS 托管 DNS 服务器的 IP 地址，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”字段中，选择“域”，输入您的 AWS 托管 Microsoft AD Active Directory 的完全限定名称，然后选择“确定”。
6. 当系统提示输入域管理员的用户名和密码时，请输入具有域加入权限的帐户的用户名和密码。有关委托这些权限的更多信息，请参阅委托 AWS Managed Microsoft AD 的目录加入权限。

> **Note**
>
> 您可以输入域的完全限定名称或 NetBIOS 名称，后跟反斜杠 (\)，然后输入用户名。用户名应为“管理员”。例如，**corp.example.com\admin** 或 **corp\admin**。

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，您的实例已加入 AWS 托管 Microsoft AD Active Directory 域，您可以远程登录该实例并安装用于管理目录的实用程序，例如添加用户和群组。Active Directory 管理工具可用于创建用户和群组。有关更多信息，请参阅 安装适用于 AWS 托管微软 AD 的 Active Directory 管理工具。

> **Note**
>
> 您也可以使用 Amazon Route 53 来处理 DNS 查询，而不必手动更改 Amazon EC2 实例上的 DNS 地址。有关更多信息，请参阅将目录服务的 DNS 解析与您的网络集成 Amazon Route 53 Resolver和将出站 DNS 查询转发到您的网络。

将亚马逊 EC2 Linux 实例无缝加入您的 AWS 托管微软 AD 活动目录

此过程将亚马逊 EC2 Linux 实例无缝连接到您的 AWS 托管微软 AD 活动目录。如果您需要跨多个 AWS 账户进行无缝域加入，则可以选择启用目录共享。

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 Red Hat Enterprise Linux 7 之前的发行版不支持无缝域加入功能。

有关将 Linux 实例无缝加入您的 AWS 托管 Microsoft AD Active Directory 的过程的演示，请 YouTube 观看以下视频。

适用于 Linux 的 Amazon EC2 无缝 AD 域加入演示

先决条件

在设置无缝域加入到 Linux 实例之前，您需要完成本节中的步骤。

选择无缝域名加入服务账户

你可以无缝地将 Linux 计算机加入你的 AWS 托管微软 AD Active Directory 域。要执行此操作，您必须使用一个具有创建计算机账户权限的用户账户，才能将计算机加入域。尽管 AWS 委托管理员或其他组的成员可能有足够的权限将计算机加入域，但我们不建议使用这些角色。作为最佳实践，我们建议您使用具有将计算机加入域所需最低权限的服务账户。

要委托具有将计算机加入域所需的最低权限的帐户，可以运行以下 PowerShell 命令。您必须在已安装安装适用于 AWS 托管微软 AD 的 Active Directory 管理工具 的已加入域的 Windows 计算机上运行这些命令。此外，您必须使用有权修改您的计算机 OU 或容器权限的账户。该 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 向您的服务账户委派权限 中所述的手动过程。

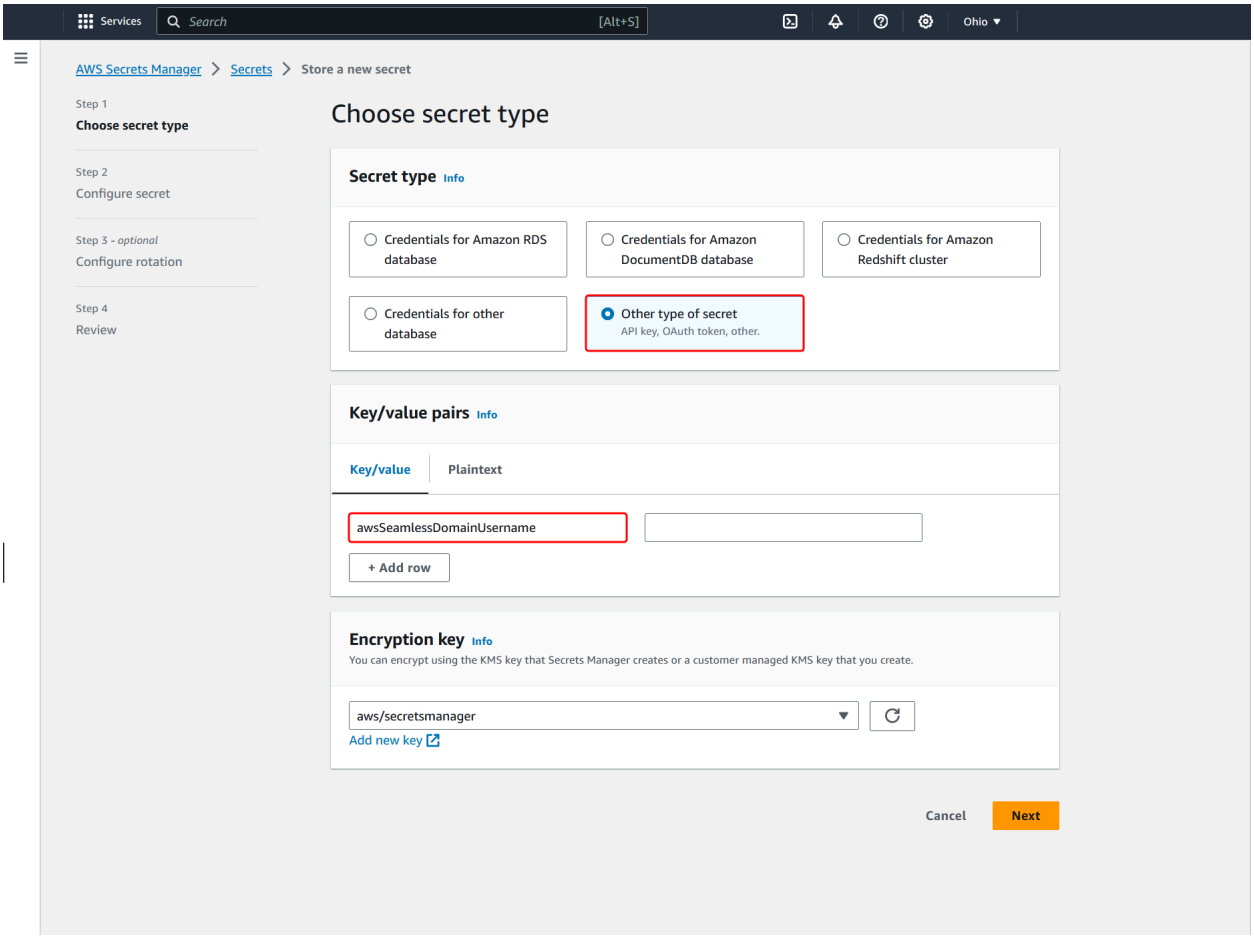
创建密钥以存储域服务账户

您可以使用 AWS Secrets Manager 存储域名服务帐户。

创建密钥并存储域服务账户信息

1. 登录 AWS Management Console 并打开 AWS Secrets Manager 控制台，网址为 https://console.aws.amazon.com/secretsmanager/。
2. 选择 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. 在密钥类型下，选择其他密钥类型。
   b. 在 “键/值对” 下，执行以下操作：
      i. 在第一个框中，输入 **awsSeamlessDomainUsername**。在同一行的下一个框中，输入您的服务帐号的用户名。例如，如果您之前使用过该 PowerShell 命令，则服务帐户名称将为**awsSeamlessDomain**。

> **Note**
>
> 必须完全按照原样输入 **awsSeamlessDomainUsername**。确保前后均没有任何空格。否则，域加入将失败。



ii. 选择添加行。

iii. 在新行的第一个框中输入 **awsSeamlessDomainPassword**。在同一行的下一个框中，输入服务账户密码。

> **Note**
>
> 必须完全按照原样输入 **awsSeamlessDomainPassword**。确保前后均没有任何空格。否则，域加入将失败。

iv. 在“加密密钥”下，保留默认值`aws/secretsmanager`。 AWS Secrets Manager 当您选择此选项时，始终会对密钥进行加密。您也可以选择您创建的密钥。

> **Note**
>
> 根据您使用的密钥 AWS Secrets Manager，会收取与之相关的费用。有关当前完整定价列表，请参阅 AWS Secrets Manager 定价。

你可以使用 Secrets Manager 创建`aws/secretsmanager`的 AWS 托管密钥来免费加密你的秘密。如果您创建自己的 KMS 密钥来加密您的机密，则按当前费 AWS KMS 率向您 AWS 收费。有关更多信息，请参阅AWS Key Management Service 定价。

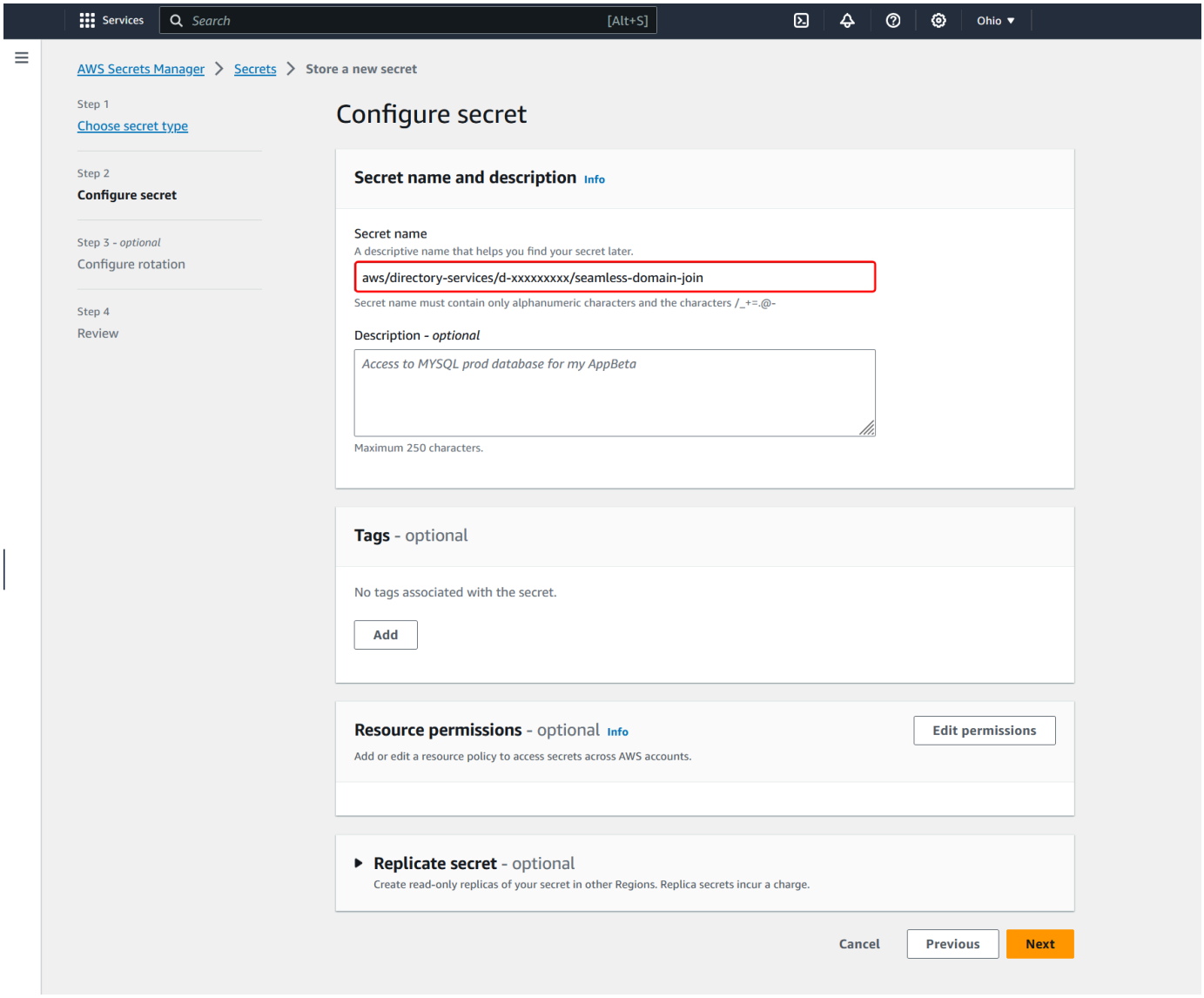
v. 选择下一步。

4. 在“密钥名称”下，使用以下格式输入包含您的目录 ID 的密钥名称，将 *d-xxxxxxxxxx* 替换为您的目录 ID：

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

这将用于检索应用程序中的密钥。

> **Note**
>
> 您必须完全按照原样输入 **aws/directory-services/*d-xxxxxxxxx*/seamless-domain-join**，但请将 *d-xxxxxxxxxx* 替换为您的目录 ID。确保前后均没有空格。否则，域加入将失败。



5. 将其他所有内容都设置为默认值，然后选择下一步。
6. 在配置自动轮换下，选择禁用自动轮换，然后选择下一步。

   存储此密钥后，您可以为其开启轮换功能。
7. 查看设置，然后选择存储以保存更改。Secrets Manager 控制台将返回您账户中的密钥列表，并且列表中现在包含新的密钥。
8. 从列表中选择您新创建的密钥名称，并记下密钥 ARN 值。您需要在下一部分中使用该名称。

开启域名服务账户密钥的轮换

我们建议您定期轮换密钥以改善您的安全状况。

启用域名服务账户密钥的轮换

- 按照《AWS Secrets Manager 用户指南》中为 AWS Secrets Manager 密钥设置自动轮换中的说明进行操作。

  对于第 5 步，请使用AWS Secrets Manager 用户指南中的轮换模板 Microsoft Active Directory 凭据。

  如需帮助，请参阅《AWS Secrets Manager 用户指南》中的AWS Secrets Manager 轮换疑难解答。

创建所需 IAM policy 和角色

使用以下先决条件步骤创建自定义策略，该策略允许对您的 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 LinuxEC2 DomainJoin IAM 角色。

创建 Secrets Manager IAM 读取策略

您可以使用 IAM 控制台创建策略，授予对 Secrets Manager 密钥的只读访问权限。

创建 Secrets Manager IAM 读取策略

1. 以有权创建 IAM 策略的用户 AWS Management Console 身份登录。然后通过以下网址打开 IAM 控制台：https://console.aws.amazon.com/iam/。
2. 在导航窗格的 “访问管理” 中，选择 “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 文本框中。

> **Note**
>
> 请务必将区域和资源 ARN 替换为之前创建的密钥的实际区域和资源 ARN。

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

```
                "secretsmanager:GetSecretValue",
                "secretsmanager:DescribeSecret"
            ],
            "Resource": [
                "arn:aws:secretsmanager:us-east-1:xxxxxxxxx:secret:aws/directory-
services/d-xxxxxxxxx/seamless-domain-join"
            ]
        }
    ]
}
```

5. 完成后，选择下一步。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 policy。
6. 在检查策略页面上，输入一个策略名称，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。选择创建策略，保存更改。托管策略列表中将显示新策略，并且现在已准备好附加到身份中。

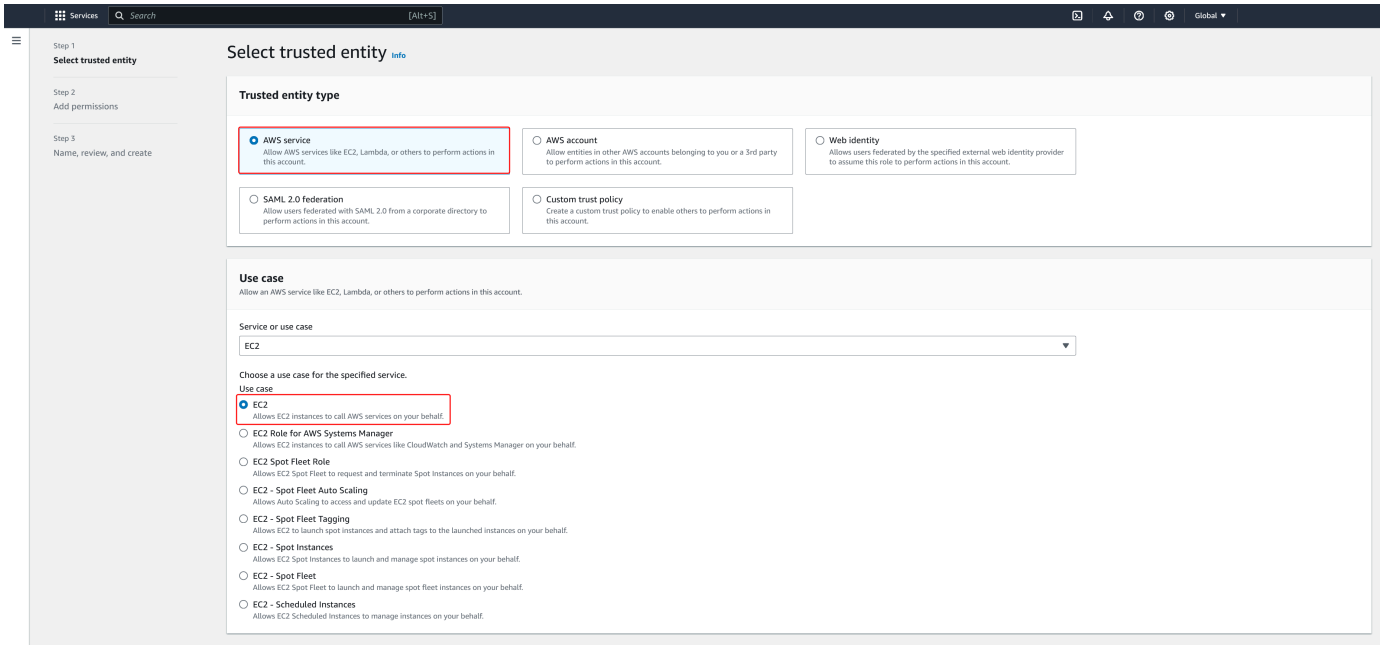
> **Note**
>
> 我们建议您为每个密钥创建一个策略。这样做可以确保实例只能访问相应的密钥，并在实例受损时将影响降至最低。

创建 LinuxEC2 角色 DomainJoin

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 LinuxEC2 角色 DomainJoin

1. 以有权创建 IAM 策略的用户 AWS Management Console 身份登录。然后通过以下网址打开 IAM 控制台：https://console.aws.amazon.com/iam/。
2. 在导航窗格中的访问管理下，选择角色。
3. 在内容窗格中，选择创建角色。
4. 在选择受信任实体的类型下，选择 AWS 服务。
5. 在 “用例” 下，选择 “EC2”，然后选择 “下一步”。



6. 对于筛选策略，执行以下操作：

   a. 输入 **AmazonSSMManagedInstanceCore**。然后选择列表中该项目的复选框。

   b. 输入 **AmazonSSMDirectoryServiceAccess**。然后选择列表中该项目的复选框。

   c. 输入 **SM-Secret-Linux-DJ-*d-xxxxxxxxxx*-Read**（或您在上一过程中创建的策略名称）。然后选择列表中该项目的复选框。

   d. 添加上面列出的三个策略后，选择创建角色。

> **Note**
>
> AmazonSSM DirectoryServiceAccess 提供了将实例加入Active Directory托管者的权限。AWS Directory Service AmazonSSM ManagedInstanceCore 提供使用该服务所需的最低权限。 AWS Systems Manager 有关创建具有这些权限的角色的更多信息，以及您可以分配给 IAM 角色的其他权限和策略的信息，请参阅《AWS Systems Manager 用户指南》中的为 Systems Manager 创建 IAM 实例配置文件。

7. 在角色名称字段中输入新角色的名称，例如**LinuxEC2DomainJoin**或其他您喜欢的名称。
8. （可选）对于角色描述，请输入描述。
9. （可选）在 “步骤 3：添加标签” 下选择 “添加新标签” 以添加标签。标签键值对用于组织、跟踪或控制此角色的访问权限。
10. 选择 创建角色。

无缝加入你的 Linux 实例

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

无缝加入你的 Linux 实例

1. 登录 AWS Management Console 并打开亚马逊 EC2 控制台，网址为 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 AWS 区域 相同的目录。
3. 在 EC2 控制面板的启动实例部分，选择启动实例。
4. 在启动实例页面的名称和标签部分下，输入您要用于 Linux EC2 实例的名称。
5. （可选）选择添加其他标签，添加一个或多个标签密钥值对，以组织、跟踪或控制对此 EC2 实例的访问权限。
6. 在“应用程序和操作系统映像（Amazon 系统映像）”部分，选择要启动的 Linux AMI。

> **Note**
>
> 使用的 AMI 必须具有 AWS 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。如果您需要升级 SSM Agent，请参阅在适用于 Linux 的 EC2 实例上安装和配置 SSM Agent。
> SSM 在将 Linux 实例加入Active Directory域时使用该`aws:domainJoin`插件。该插件将 Linux 实例的主机名更改为 EC2AMAZ-*XXXXXX* X 格式。有关的更多信息`aws:domainJoin`，请参阅《AWS Systems Manager 用户指南》中的AWS Systems Manager 命令文档插件参考。

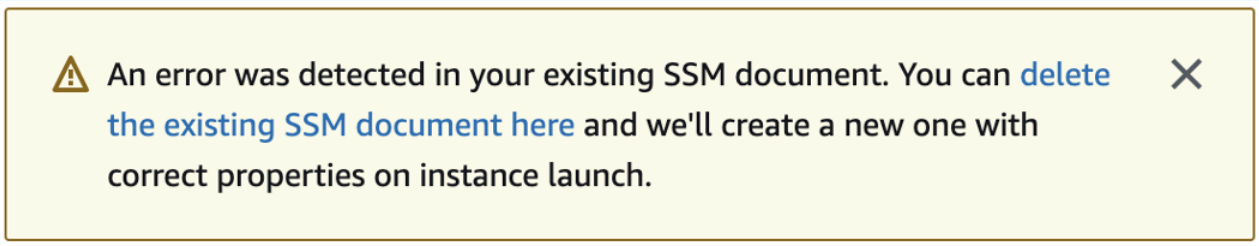
7. 在实例类型部分，从实例类型下拉列表中选择要使用的实例类型。
8. 在密钥对（登录）部分，您可以选择创建新密钥对，或从现有密钥对中进行选择。要创建新的密钥对，请选择新建新密钥对。输入密钥对的名称，然后为密钥对类型和私钥文件格式选择一个选项。要以可与 OpenSSH 一起使用的格式保存私钥，请选择 pem。要以可与 PuTTY 一起使用的格式保存私钥，请选择 ppk。选择创建密钥对。您的浏览器会自动下载私有密钥文件。将私有密钥文件保存在安全位置。

> **Important**
>
> 这是您保存私有密钥文件的唯一机会。

9. 在启动实例页面的网络设置部分下，选择编辑。从 VPC – 必需下拉列表中选择创建目录的 VPC。
10. 从子网下拉列表中选择 VPC 中的其中一个公有子网。选择的子网必须将所有外部流量都路由到互联网网关。否则将无法远程连接到实例。

    有关如何连接到互联网网关的更多信息，请参阅《Amazon VPC 用户指南》中的使用互联网网关连接到互联网。
11. 在自动分配公有 IP 下，选择启用。

    有关公有和私有 IP 寻址的更多信息，请参阅《亚马逊 EC2 用户指南》中的 Amazon EC2 实例 IP 寻址。
12. 对于防火墙（安全组）设置，您可以使用默认设置或进行更改以满足您的需求。
13. 对于配置存储设置，您可以使用默认设置或进行更改以满足您的需求。
14. 选择高级详细信息部分，从域加入目录下拉列表中选择您的域。

> **Note**
>
> 选择域加入目录后，您可能会看到：
>
> 
>
>
> 如果 EC2 启动向导识别出具有意外属性的现有 SSM 文档，则会发生此错误。您可以执行以下操作之一：
>
> - 如果您之前编辑了 SSM 文档并且属性符合预期，请选择关闭并继续启动 EC2 实例，不做任何更改。
> - 选择 “在此处删除现有 SSM 文档” 链接以删除 SSM 文档。这将允许创建具有正确属性的 SSM 文档。SSM 文档将在您启动 EC2 实例时自动创建。

15. 对于 IAM 实例配置文件，请选择您之前在先决条件部分步骤 2：创建 LinuxEC DomainJoin 2 角色中创建的 IAM 角色。
16. 选择启动实例。

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

手动将亚马逊 EC2 Linux 实例加入您的 AWS 托管微软 AD 活动目录

除了亚马逊 EC2 Windows 实例外，您还可以将某些亚马逊 EC2 Linux 实例加入您的 AWS 托管微软 AD 活动目录。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）
- 亚马逊 Linux 2023 AMI
- 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 Linux 实例加入你的 AWS 托管微软 AD

必须先按照 无缝加入你的 Linux 实例 中指定的步骤启动实例，然后才能将 Amazon Linux、CentOS、Red Hat 或 Ubuntu 实例加入目录。

> **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. 将 Linux 实例配置为使用 AWS Directory Service提供的 DNS 服务器的 DNS 服务器 IP 地址。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。如果要手动设置，请参阅 AWS 知识中心的如何为私有 EC2 实例分配静态 DNS 服务器，以了解有关为特定 Linux 分发版和版本设置持久性 DNS 服务器的指导。
3. 确保 64 位 Amazon Linux 实例为最新状态。

```
sudo yum -y update
```

4. 在 Linux 实例上安装所需的 Amazon Linux 软件包。

> **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

```
sudo yum install samba-common-tools realmd oddjob oddjob-mkhomedir sssd adcli
 krb5-workstation
```

> **Note**
>
> 有关确定您所使用的 Amazon Linux 版本的帮助，请参阅《Amazon EC2 用户指南（适用于 Linux 实例）》中的识别 Amazon Linux 映像。

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

example.com 域中具有域加入权限的账户。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，请参阅委托 AWS Managed Microsoft AD 的目录加入权限。

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. 实例重新启动后，使用任何 SSH 客户端连接到该实例，然后通过执行以下步骤将 AWS 委派管理员组添加到 sudoers 列表中：

   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 "AWS Delegated Administrators" group from the example.com domain.
   %AWS\ 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. 将 Linux 实例配置为使用 AWS Directory Service提供的 DNS 服务器的 DNS 服务器 IP 地址。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。如果要手动设置，请参阅 AWS 知识中心的如何为私有 EC2 实例分配静态 DNS 服务器，以了解有关为特定 Linux 分发版和版本设置持久性 DNS 服务器的指导。
3. 确保 CentOS 7 实例为最新状态。

```
sudo yum -y update
```

4. 在 Linux 实例上安装所需 CentOS 7 软件包。

> **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

example.com 域中具有域加入权限的账户。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，请参阅委托 AWS Managed Microsoft AD 的目录加入权限。

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. 实例重新启动后，使用任何 SSH 客户端连接到该实例，然后通过执行以下步骤将 AWS 委派管理员组添加到 sudoers 列表中：

   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 "AWS Delegated Administrators" group from the example.com domain.
   %AWS\ 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. 将 Linux 实例配置为使用 AWS Directory Service提供的 DNS 服务器的 DNS 服务器 IP 地址。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。如果要手动设置，请参阅 AWS 知识中心的如何为私有 EC2 实例分配静态 DNS 服务器，以了解有关为特定 Linux 分发版和版本设置持久性 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

e*x* ***am AccountName*** *ple.com* 域中具有域加入权限的账户的 SaM。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，请参阅委托 AWS Managed Microsoft AD 的目录加入权限。

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. 实例重新启动后，使用任何 SSH 客户端连接到该实例，然后通过执行以下步骤将 AWS 委派管理员组添加到 sudoers 列表中：

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 "AWS Delegated Administrators" group from the example.com domain.
%AWS\ 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 AWS Directory Service提供的 DNS 服务器的 DNS 服务器 IP 地址。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。如果要手动设置，请参阅 AWS 知识中心的如何为私有 EC2 实例分配静态 DNS 服务器，以了解有关为特定 Linux 分发版和版本设置持久性 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

   e *xample.com* 域AccountName 中具有域加入权限的 SaM。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，请参阅委托 AWS Managed Microsoft AD 的目录加入权限。

   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. 在 PAM 中手动启用 SSSD。

```
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.使用任意 SSH 客户端重新连接到实例，验证域加入操作是否已成功完成并完成其他步骤

   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 'AWS 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. 实例重新启动后，使用任何 SSH 客户端连接到该实例，然后通过执行以下步骤将 AWS 委派管理员组添加到 sudoers 列表中：

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. 将 Linux 实例配置为使用 AWS Directory Service提供的 DNS 服务器的 DNS 服务器 IP 地址。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。如果要手动设置，请参阅 AWS 知识中心的如何为私有 EC2 实例分配静态 DNS 服务器，以了解有关为特定 Linux 分发版和版本设置持久性 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

e *x* ***am AccountName*** *ple.com* 域中具有域加入权限的账户的 SaM。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，请参阅委托 AWS Managed Microsoft AD 的目录加入权限。

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. 实例重新启动后，使用任何 SSH 客户端连接到该实例，然后通过执行以下步骤将 AWS 委派管理员组添加到 sudoers 列表中：

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 "AWS Delegated Administrators" group from the example.com domain.
%AWS\ 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)
```

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 restart
```

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。

1. 在文本编辑器中打开 /etc/sssd/sssd.conf 文件。

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

2. 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)
```

3. 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 restart
```

身份映射

可以通过两种方法执行 ID 映射，以维护 UNIX/Linux 用户标识符 (UID) 和组标识符 (GID) 以及 Windows 和Active Directory安全标识符 (SID) 身份之间的统一体验。

1. 集中化
2. 分布式

> **Note**
>
> 中的集中式用户身份映射Active Directory需要便携式操作系统接口或 POSIX。

集中式用户身份映射

Active Directory或其他轻型目录访问协议 (LDAP) 服务为 Linux 用户提供 UID 和 GID。在中Active Directory，这些标识符存储在用户的属性中：

- UID-Linux 用户名（字符串）
- UID 号-Linux 用户 ID 号（整数）
- GID 号码-Linux 群组 ID 号（整数）

要将 Linux 实例配置为使用来自的 UID 和 GID，请在 sssd. Active Directory conf `ldap_id_mapping = False` 文件中进行设置。在设置此值之前，请确认您已向中的用户和群组添加了 UID、UID 号和 GID 号。Active Directory

分布式用户身份映射

如果Active Directory没有 POSIX 扩展名或者您选择不集中管理身份映射，Linux 可以计算 UID 和 GID 值。Linux 使用用户的唯一安全标识符 (SID) 来保持一致性。

要配置分布式用户 ID 映射，请在 sssd.conf 文件`ldap_id_mapping = True`中进行设置。

连接到 Linux 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。用户可以采用 `username@example.com` 或 `EXAMPLE\username` 格式输入用户名。根据您使用的 Linux 发行版，响应将与以下内容类似：

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 手动将亚马逊 EC2 Linux 实例加入你的 AWS 托管微软 AD 活动目录

你可以使用 Winbind 服务手动将你的 Amazon EC2 Linux 实例加入微软 AD Active Directory AWS 托管域。这使您现有的本地 Active Directory 用户能够在访问加入您的 AWS 托管 Microsoft AD 活动目录的 Linux 实例时使用其活动目录凭据。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）
- 亚马逊 Linux 2023 AMI
- 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 Linux 实例加入你的 AWS 托管微软 AD 活动目录

> **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 AWS Directory Service提供的 DNS 服务器的 DNS 服务器 IP 地址。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。如果要手动设置，请参阅 AWS 知识中心的如何为私有 EC2 实例分配静态 DNS 服务器，以了解有关为特定 Linux 分发版和版本设置持久性 DNS 服务器的指导。
3. 确保 Linux 实例为最新状态。

   ```
   sudo yum -y update
   ```

4. 在 Linux 实例上安装所需 Samba/Winbind 软件包。

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

5. 对主 `smb.conf` 文件进行备份，以便在出现任何故障时可以恢复到该文件：

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

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

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

   填写您的 Active Directory 域环境信息，如下例所示：

   ```
   [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. 在文本编辑器中打开主机文件 [/etc/hosts]。

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

按如下方式添加 Linux 实例私有 IP 地址：

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

> **Note**
>
> 如果您未在 /etc/hosts 文件中指定 IP 地址，则在将实例加入域时可能会收到以下 DNS 错误。
> `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，但是 [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

example.com 域中具有域加入权限的账户。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，请参阅委托 AWS Managed Microsoft AD 的目录加入权限。

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通过修改 /etc/ssh/sshd_config 文件设置 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
```

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要为域用户或组授予的根权限添加到 sudoers 列表：

a. 使用以下命令打开 sudoers 文件：

```
sudo visudo
```

b. 按如下方式从信任或可信域中添加所需的组或用户，然后将其保存。

```
## Adding Domain Users/Groups.
%domainname\\AWS\ 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 AWS Directory Service提供的 DNS 服务器的 DNS 服务器 IP 地址。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。如果要手动设置，请参阅 AWS 知识中心的如何为私有 EC2 实例分配静态 DNS 服务器，以了解有关为特定 Linux 分发版和版本设置持久性 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 Samba/Winbind 软件包。

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

5. 对主 smb.conf 文件进行备份，以便在出现任何故障时可以恢复到该文件：

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

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

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

   填写 Active Directory 域环境信息，如下例所示：

   ```
   [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. 在文本编辑器中打开主机文件 [/etc/hosts]。

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

按如下方式添加 Linux 实例私有 IP 地址：

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

> **Note**
>
> 如果您未在 /etc/hosts 文件中指定 IP 地址，则在将实例加入域时可能会收到以下 DNS 错误。
> 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，但是 [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

e *xample.com* 域AccountName 中具有域加入权限的 SaM。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，请参阅委托 AWS Managed Microsoft AD 的目录加入权限。

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. 在文本编辑器中打开 Name Service Switch 配置文件 [/etc/nsswitch.conf]。

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

添加 Winbind 指令，如下所示。

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

11. 通过修改 /etc/ssh/sshd_config 文件设置 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 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要为域用户或组授予的根权限添加到 sudoers 列表：

a. 使用以下命令打开 sudoers 文件：

```
sudo visudo
```

b. 按如下方式从信任或可信域中添加所需的组或用户，然后将其保存。

```
## Adding Domain Users/Groups.
%domainname\\AWS\ 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 AWS Directory Service提供的 DNS 服务器的 DNS 服务器 IP 地址。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。如果您想手动设置，请参阅 AWS 知识中心中的如何将静态 DNS 服务器分配给私有 Amazon EC2 实例，以获取有关为您的特定 Linux 发行版和版本设置永久 DNS 服务器的指导。
3. 确保 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 Samba/Winbind 软件包。

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

5. 对主 `smb.conf` 文件进行备份，以便在出现任何故障时可以恢复到该文件：

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

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

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

   填写 Active Directory 域环境信息，如下例所示：

```
[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. 在文本编辑器中打开主机文件 [/etc/hosts]。

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

按如下方式添加 Linux 实例私有 IP 地址：

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

> **Note**
>
> 如果您未在 /etc/hosts 文件中指定 IP 地址，则在将实例加入域时可能会收到以下 DNS 错误。
> `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，但是 [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

example.com 域中具有域加入权限的账户。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，请参阅委托 AWS Managed Microsoft AD 的目录加入权限。

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. 在文本编辑器中打开 Name Service Switch 配置文件 [/etc/nsswitch.conf]。

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

添加 Winbind 指令，如下所示。

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

11. 通过修改 /etc/ssh/sshd_config 文件设置 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 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要为域用户或组授予的根权限添加到 sudoers 列表：

    a. 使用以下命令打开 sudoers 文件：

    ```
    sudo visudo
    ```

    b. 按如下方式从信任或可信域中添加所需的组或用户，然后将其保存。

    ```
    ## Adding Domain Users/Groups.
    %domainname\\AWS\ 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。）

连接到 Linux 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。用户可以采用 username@example.com 或 EXAMPLE\username 格式输入用户名。根据您使用的 Linux 发行版，响应将与以下内容类似：

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%
```

手动将亚马逊 EC2 Mac 实例加入您的 AWS 托管微软 AD 活动目录

此过程手动将 Amazon EC2 Mac 实例加入您的 AWS 托管微软 AD 活动目录。

先决条件

- 亚马逊 EC2 Mac 实例需要亚马逊 EC2 专用主机。您必须分配一台专用主机并在该主机上启动实例。有关更多信息，请参阅 A mazon EC2 用户指南中的启动 Mac 实例。
- 我们建议您为 AWS 托管的 Microsoft AD 活动目录创建 DHCP 选项集。这将允许您的 Amazon VPC 中的任何实例指向指定的域，并允许 DNS 服务器来解析其域名。请参阅创建或更改 DHCP 选项集了解更多信息。

> **Note**
>
> 专用主机的定价因您选择的付款方式而异。有关更多信息，请参阅 Amazon EC2 用户指南中的定价和账单。

手动加入 Mac 实例

1. 使用以下 SSH 命令连接到您的 Mac 实例。有关连接您的 Mac 实例的更多信息，请参阅连接到您的 Mac 实例。

```
ssh -i /path/key-pair-name.pem ec2-user@my-instance-public-dns-name
```

2. 连接到 Mac 实例后，使用以下命令为 *ec2-user* 帐户创建密码：

```
sudo passwd ec2-user
```

3. 当命令行出现提示时，请提供 *ec2 ##*帐户的密码。您可以按照 Amazon EC2 用户指南中更新操作系统和软件中的步骤更新操作系统和软件。

4. 使用以下 *dsconfigad* 命令将你的 Mac 实例加入托管的 AWS 微软 AD Active Directory 域。确保将域名、计算机名称和组织单位替换为你的 Microsoft AD Active Directory AWS 托管域信息。有关更多信息，请参阅 Apple 网站上的 Mac 上的“目录工具”中配置域访问权限。

> **Warning**
>
> 计算机名称不应包含连字符。连字符可能会阻止绑定到托管的 AWS Microsoft AD Active Directory。

```
sudo dsconfigad -add domainName -computer computerName -username Username -
ou "Your-AWS-Delegated-Organizational-Unit"
```

以下示例是在名为**example.com**域的 Mac 实例上加入管理用户时命令**myec2mac01**的样子：

```
sudo dsconfigad -add example.com -computer myec2mac01 -username admin -
ou "OU=Computers,OU=Example,DC=Example,DC=com"
```

5. 使用以下命令将AWS 委派管理员添加到 Mac 实例上的管理用户：

```
sudo dsconfigad -group "EXAMPLE\aws delegated administrators
```

6. 使用以下命令确认 AWS 托管 Microsoft AD Active Directory 域成功加入：

```
dsconfigad -show
```

你已成功将你的 Mac 实例加入你的 AWS 托管微软 AD 活动目录。现在，您可以使用 AWS 托管的 Microsoft AD Active Directory 凭据登录您的 Mac 实例。

首次登录 Mac 实例时，应提供以 “其他” 用户身份登录的选项。此时，您可以使用您的 Active Directory 域凭据登录 Mac 实例。如果完成这些步骤后，登录屏幕上没有显示 “其他”，请以 ec2-user 身份登录，然后注销。

要使用图形用户界面与域用户登录，请按照 Amazon EC2 用户指南中连接到实例的图形用户界面 (GUI) 中的步骤进行操作。

委托 AWS Managed Microsoft 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 Microsoft AWS Active Directory 的 Directory Service，管理员和AWS 委派服务器管理员组的成员拥有这些权限。

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。

您必须在已加入到目录且已安装 Active Directory 用户和计算机 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。

为托 AWS 管 Microsoft AD 委派加入权限

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。

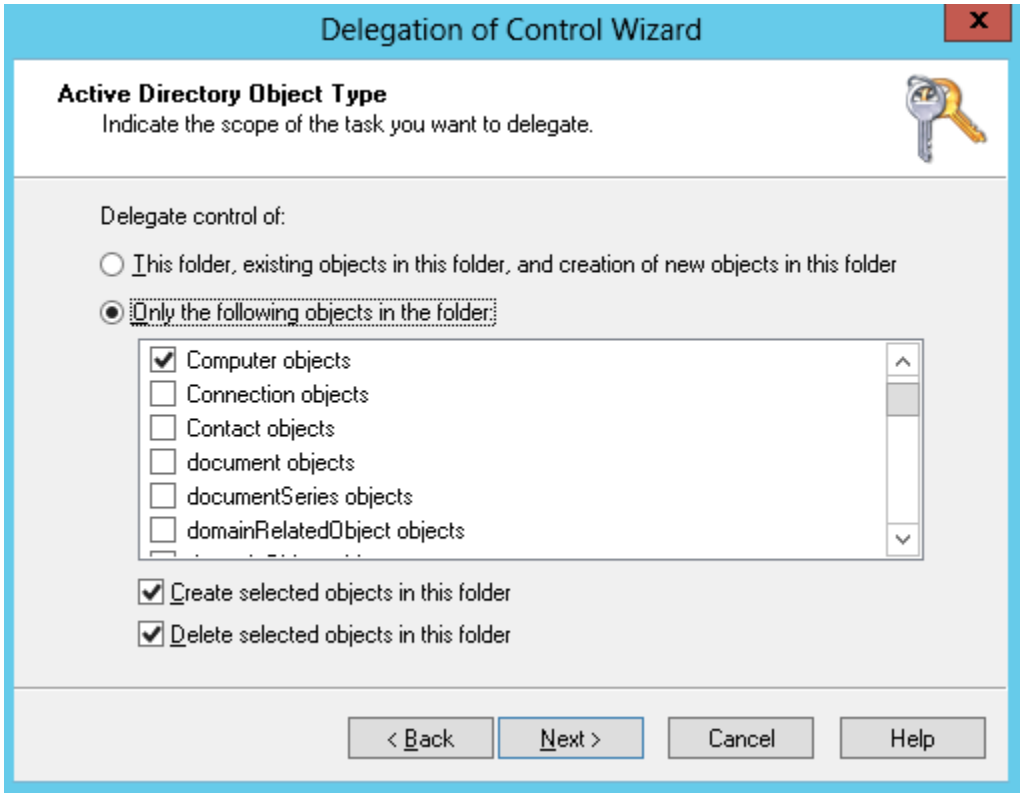
   > **Important**
   >
   > 当你启动 Microsoft Active Directory 的 AWS 目录服务时， AWS 会创建一个包含所有目录对象的组织单位 (OU)。此 OU (具有您在创建目录时键入的 NetBIOS 名称) 位于域根目录中。域根由所有和管理 AWS。无法对域根本身进行更改，因此必须在具有您的 NetBIOS 名称的 OU 中创建 **`Joiners`** 组。

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。

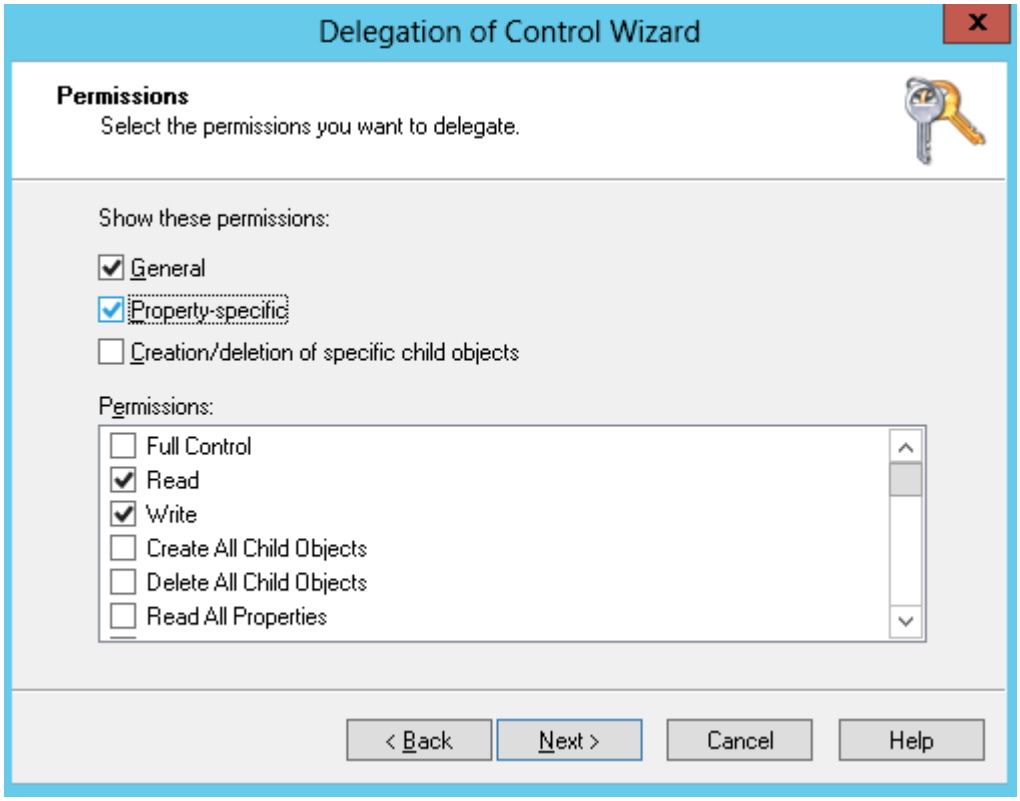
   - 对于 Group name (组名称)，键入 **`Joiners`**。
   - 对于 Group scope，选择 Global。

- 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。

创建或更改 DHCP 选项集

AWS 建议您为 AWS Directory Service 目录创建 DHCP 选项集，并将 DHCP 选项集分配给您的目录所在的 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https://docs.aws.amazon.com/vpc/latest/userguide/VPC_DHCP_Options.html《Amazon VPC 用户指南》中的 DHCP 选项集。

为目录创建 DHCP 选项集

1. 通过 https://console.aws.amazon.com/vpc/ 打开 Amazon VPC 控制台。
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，输入目录的以下值：

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

您 AWS提供的目录的 DNS 服务器的 IP 地址。

> **Note**
>
> 可以转到 AWS Directory Service 控制台导航窗格，选择目录，然后选择正确的目录 ID，从而找到这些地址。

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*)。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 Your VPCs(您的 VPC)。
3. 选择 VPC，然后选择操作、编辑 VPC 设置。

4. 对于 DHCP 选项集，选择一个选项集或选择无 DHCP 选项集，然后选择保存。

要使用命令行更改与 VPC 关联的 DHCP 选项集，请参阅以下内容：

- AWS CLI: associate-dhcp-options
- AWS Tools for Windows PowerShell: Register-EC2DhcpOption

在 AWS Managed Microsoft AD 中管理用户和组

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。

要在 AWS Directory Service 目录中创建用户和组，您必须使用已经加入 AWS Directory Service 目录的任意实例（来自本地或 EC2），并且已作为有权创建用户和组的用户登录。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。

您可以使用 AWS Directory Service 管理控制台中预安装的 Active Directory 管理工具部署预配置的 EC2 实例。有关更多信息，请参阅 在你的 AWS 托管 Microsoft AD 中启动目录管理实例 Active Directory。

如果您需要使用管理工具部署自托管式 EC2 实例并安装必要的工具，请参阅 第 3 步：部署 Amazon EC2 实例来管理您的 AWS 托管微软 AD 活动目录。

> **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

- 安装适用于 AWS 托管微软 AD 的 Active Directory 管理工具
- 创建用户
- 删除用户
- 重置用户密码

- 创建组
- 将用户添加到组

安装适用于 AWS 托管微软 AD 的 Active Directory 管理工具

要通过 Amazon EC2 Windows Server 实例管理你的，你需要在实例Active Directory Domain Services and Active Directory Lightweight Directory Services Tools上安装。Active Directory使用以下过程在 EC2 Windows 服务器实例上安装这些工具。

先决条件

在开始此过程之前，请完成以下操作：

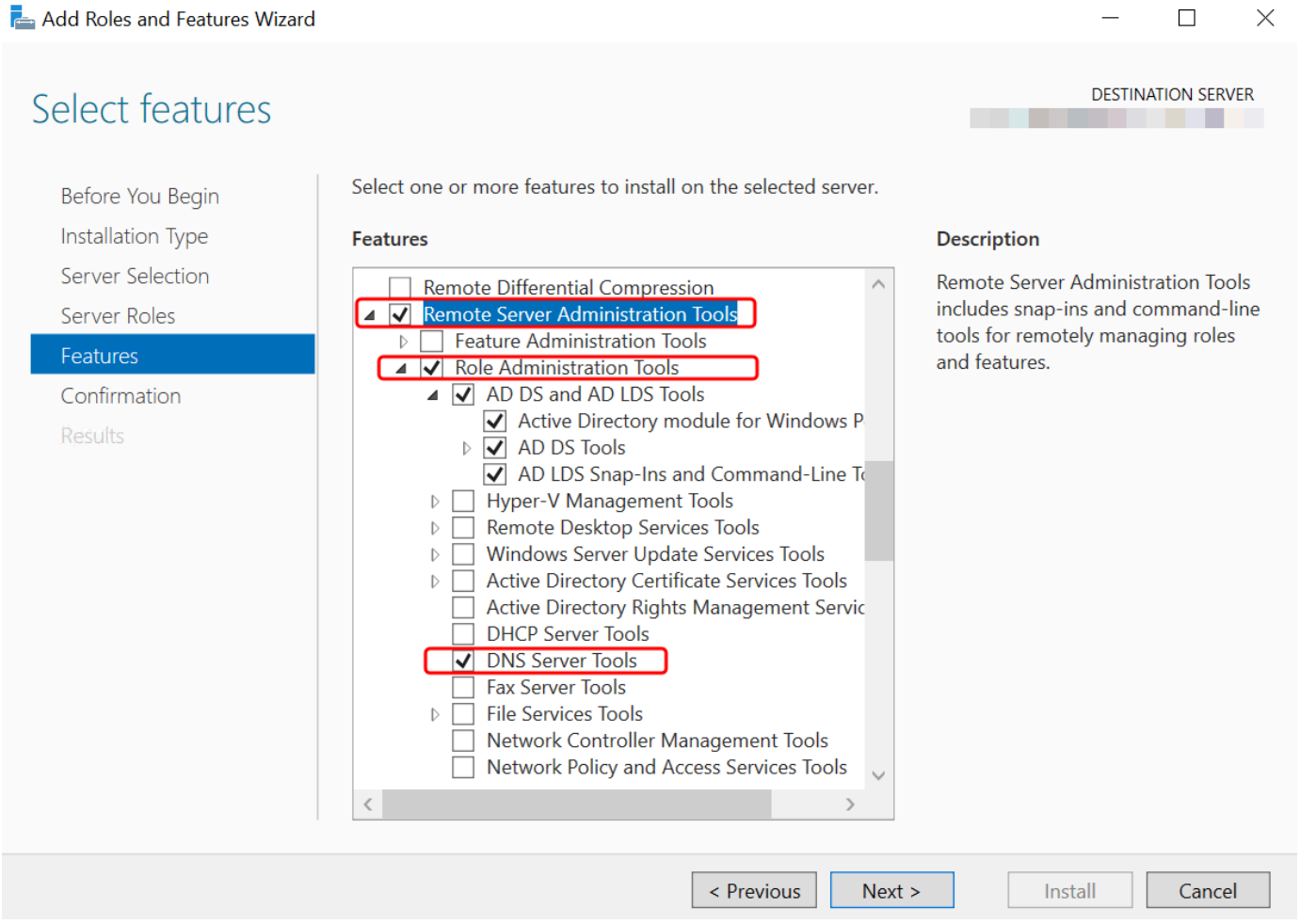
1. 创建 AWS 托管微软 AD Active Directory。有关更多信息，请参阅 创建你的 Microsoft AWS 托管广告。
2. 启动 EC2 Windows 服务器实例并将其加入您的 AWS 托管微软 AD 活动目录。EC2 实例需要以下策略来创建用户和群
   组：**AWSSSMManagedInstanceCore**和**AmazonSSMDirectoryServiceAccess**。有关更多信息，请参阅 在你的 AWS 托管 Microsoft AD 中启动目录管理实例 Active Directory 和 将亚马逊 EC2 Windows 实例无缝加入你的 AWS 托管微软 AD Active Directory。
3. 您将需要Active Directory域管理员的凭证。这些凭据是在创建 AWS 托管 Microsoft AD 时创建的。如果您按照中的步骤操作创建你的 Microsoft AWS 托管广告，则您的管理员用户名将包括您的 NetBIOS 名称。**corp\admin**

在 EC2 Windows 服务器实例上安装 Active Directory 管理工具

在 EC2 Windows 服务器实例上安装 Active Directory 管理工具

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，选择实例，选择 Windows Server 实例，然后选择连接。
3. 在连接到实例页面中，选择 RDP 客户端。
4. 在 RDP 客户端选项卡中，选择下载远程桌面文件，然后选择获取密码，以检索密码。
5. 在获取 Windows 密码中，选择上传私钥文件。选择与 Windows Server 实例关联的 .pem 私钥文件。上传私钥文件后，选择解密密码。

6. 在 Windows 安全对话框中，复制 Windows 服务器计算机的本地管理员凭据进行登录。用户名可以采用以下格式：***NetBIOS-Name*\admin**或***DNS-Name*\admin**。例如，如果您按照中的步骤进行操作，则**corp\admin**将是用户名创建你的 Microsoft AWS 托管广告。
7. 登录 Windows 服务器实例后，从 “开始” 菜单中选择 “服务器管理器”，打开 “服务器管理器”。
8. 在服务器管理器控制面板中，选择添加角色和功能。
9. 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)。
10. 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)。
11. 在功能树中，依次选择并打开远程服务器管理工具、角色管理工具和 AD DS 和 AD LDS 工具。选择 A D DS 和 AD LDS 工具后，将选择Active Directory模块Windows PowerShell、AD DS 工具、AD LDS 管理单元和命令行工具。向下滚动并选择 DNS 服务器工具，然后选择下一步。



12. 检查信息，然后选择安装。当该功能安装完成后，Active Directory 域服务工具和 Active Directory 轻量级目录服务工具将出现在“开始”菜单的管理工具文件夹中。

在 EC2 Windows 服务器实例上安装 Active Directory 管理工具的替代方法

- 以下是安装 Active Directory 管理工具的其他一些方法：
  - 您可以选择使用安装 Active Directory 管理工具Windows PowerShell。例如，您可以使用在 PowerShell 提示符下安装 Active Directory 远程管理工具`Install-WindowsFeature RSAT-ADDS`。有关更多信息，请参阅 Microsoft WindowsFeature 网站上的 “安装-”。
  - 您也可以按照中的步骤在中启动已经安装了 Active Directory 域服务和 Active Directory 轻型目录服务工具的目录管理 EC2 实例在你的 AWS 托管 Microsoft AD 中启动目录管理实例 Active Directory。 AWS Management Console

创建用户

使用以下过程可创建其 EC2 实例加入到 AWS Managed Microsoft AD 目录的用户。在创建用户之前，您需要完成安装 Active Directory 管理工具中的过程。

您可以使用以下任何一种方法来创建用户：

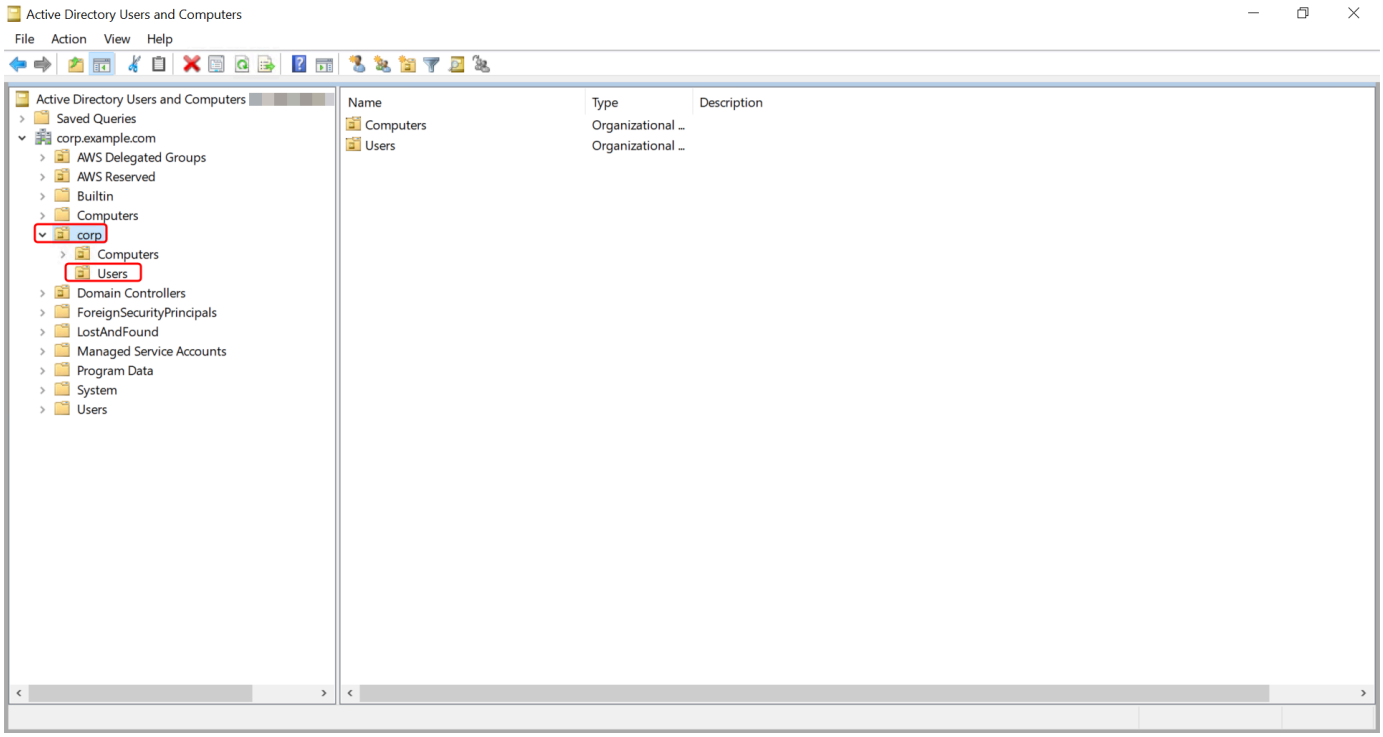
- Active Directory管理工具
- Windows PowerShell

使用Active Directory管理工具创建用户

1. 连接到安装了 Active Directory 管理工具的实例。
2. 从 Windows 的 “开始” 菜单中打开 Active Directory 用户和计算机工具。在 Windows 管理工具文件夹中可以找到此工具的快捷方式。

   > **Tip**
   >
   > 您可以通过实例上的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
   > ```

3. 在目录树中，在目录的 NetBIOS 名称 OU 下选择要存储用户的 OU（例如）。**`corp\Users`**有关中目录使用的 OU 结构的更多信息 AWS，请参阅用你的 AWS 托管 Microsoft AD 活动目录创建了什么。



4. 在操作 菜单上，选择新建，然后选择用户打开新用户向导。
5. 在向导的第一页上，输入以下字段的值，然后选择下一步。
   - 名
   - 姓
   - User logon name
6. 在新用户向导的第二页上，为密码和确认密码输入临时密码。确保选中了用户下次登录时必须更改密码选项。不应选择任何其他选项。选择下一步。
7. 在新用户向导的第三页上，验证新用户的信息正确无误，然后选择完成。新用户会出现在 Users 文件夹中。

在中创建用户 Windows PowerShell

1. 以Active Directory管理员身份连接到已加入您Active Directory域的实例。
2. 打开 Windows PowerShell。
3. 键入以下命令，将用户名**`jane.doe`**替换为要创建的用户的用户名。系统将提示您为Windows PowerShell新用户提供密码。有关Active Directory密码复杂性要求的更多信息，请参阅Microsoft文档。有关 new-aduser 命令的更多信息，请参阅文档。Microsoft

```
New-ADUser -Name "jane.doe" -Enabled $true -AccountPassword (Read-Host -AsSecureString
 'Password')
```

删除用户

使用以下步骤删除已加入您的 AWS 托管 Microsoft AD 的用户Active Directory。

您可以使用以下任何一种方法来删除用户：

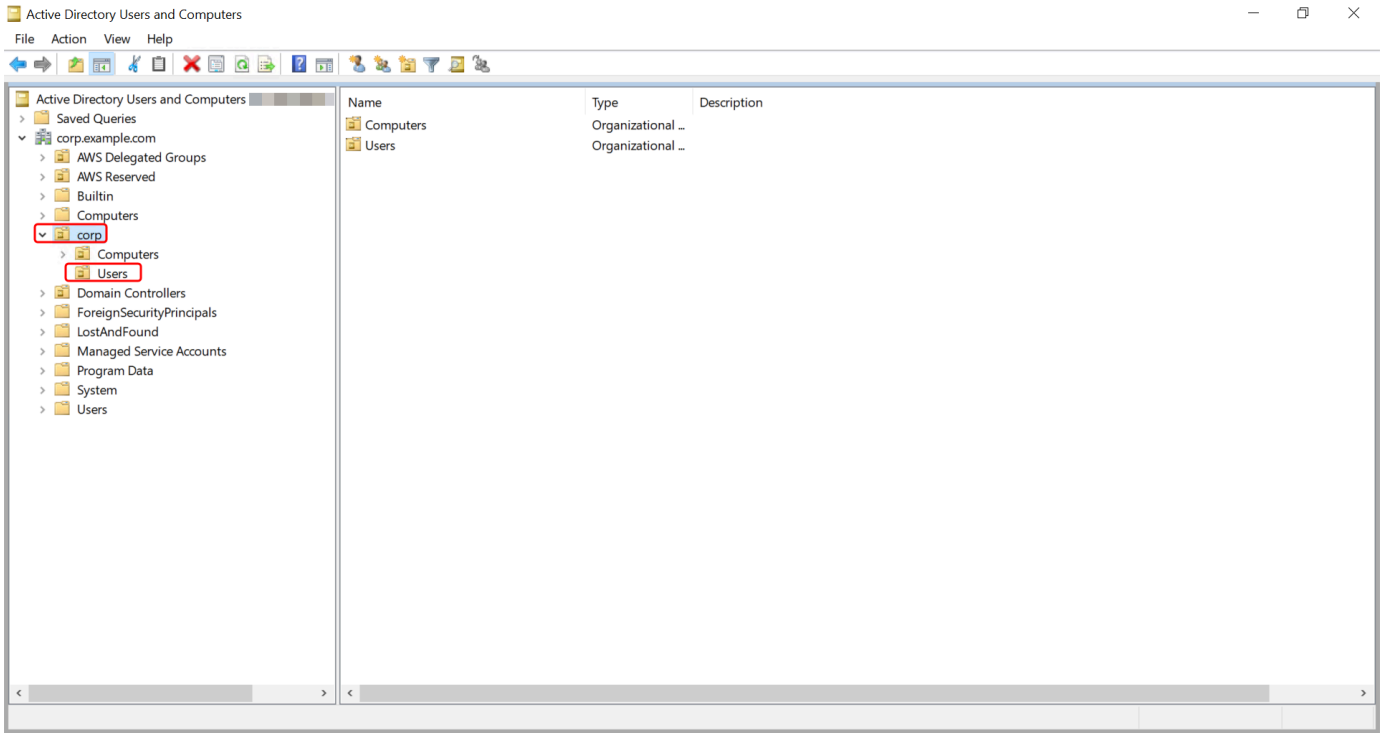
- Active Directory管理工具
- Windows PowerShell

使用Active Directory管理工具删除用户

1. 连接到安装了 Active Directory 管理工具的实例。
2. 从 Windows 的 “开始” 菜单中打开 Active Directory 用户和计算机工具。在 Windows 管理工具文件夹中可以找到此工具的快捷方式。

   > **Tip**
   >
   > 您可以通过实例上的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
   > ```

3. 在目录树中，选择包含要删除的用户的 OU（例如**corp\Users**）。



4. 选择要删除的用户。在操作 菜单上，选择删除。
5. 将出现一个对话框，提示您确认要删除该用户。选择是以删除该用户。此操作将永久删除所选用户。

删除中的用户 Windows PowerShell

1. 以Active Directory管理员身份连接到已加入您Active Directory域的实例。
2. 打开 Windows PowerShell。
3. 键入以下命令，将用户名**jane.doe**替换为要删除的用户的用户名。有关 Remove-aduser 命令的更多信息，请参阅文档。Microsoft

```
Remove-ADUser -Identity "jane.doe"
```

AD 回收站注意事项

已删除的用户会暂时存储在 AD 回收站中。有关 AD 回收站的更多信息，请参阅 “Ask t Microsoft he Directory Services Team” 博客中的 “广告回收站：理解、实施、最佳实践和故障排除”。

重置用户密码

用户必须遵守中定义的密码策略Active Directory。有时，这可以充分利用用户（包括Active Directory管理员），他们会忘记密码。发生这种情况时， AWS Directory Service 如果用户居住在 AWS 托管 Microsoft AD 中，则可以快速重置用户的密码。

您必须以具有必要权限的用户身份登录才能重置密码。有关权限的更多信息，请参阅管理 AWS Directory Service 资源访问权限概述。

您可以为自己的任何用户重置密码Active Directory，但以下情况除外：

- 您可以根据您在创建组织单位 (OU) 时使用的 NetBIOS 名称重置任何用户的密码。Active Directory 例如，如果您按照步骤操作，NetBIOS 名称将为 CORP，而您可以重置的用户密码将是 Corp/Users OU 的成员。创建你的 Microsoft AWS 托管广告
- 您不能根据您在创建 NetBIOS 名称时使用的 NetBIOS 名称重置 OU 以外的任何用户的密码。Active Directory例如，您无法在AWS 预留 OU 中重置用户的密码。有关 AWS 托管 Microsoft AD 的 OU 结构的更多信息，请参阅用你的 AWS 托管 Microsoft AD 活动目录创建了什么。

有关在 AWS 托管 Microsoft AD 中重置密码时如何应用密码策略的更多信息，请参阅如何应用密码策略。

您可以使用以下任何一种方法来重置用户密码：

- AWS Management Console
- AWS CLI
- Windows PowerShell

在中重置用户密码 AWS Management Console

1. 在AWS Directory Service 控制台导航窗格中 Active Directory，选择目录，然后Active Directory在列表中选择要重置用户密码的。
2. 在目录详细信息页面上，选择操作，然后选择重置密码。
3. 在 “重置用户密码” 对话框中，在 “用户名” 中键入需要更改密码的用户的用户名。
4. 在新密码和确认密码中键入密码，然后选择重置密码。

在中重置用户密码 AWS CLI

1. 要安装 AWS CLI，请参阅安装或更新最新版本的 AWS CLI。
2. 打开 AWS CLI.
3. 键入以下命令并将目录 ID **jane.doe**、用户名和密码**P@ssw0rd**替换为您的Active Directory目录 ID 和所需的凭据。有关更多信息 reset-user-password，请参阅《AWS CLI 命令参考》中的。

```
aws ds reset-user-password --directory-id d-1234567890 --user-name "jane.doe" --new-
password "P@ssw0rd"
```

在中重置用户密码 Windows PowerShell

1. 以Active Directory管理员身份连接到已加入您Active Directory域的实例。
2. 打开 Windows PowerShell。
3. 键入以下命令，将用户名**jane.doe**、目录 ID 和密码**P@ssw0rd**替换为您的Active Directory目录 ID 和所需的凭据。有关更多信息，请参阅 reset-ds UserPassword Cmdlet。

```
Reset-DSUserPassword -UserName "jane.doe" -DirectoryId d-1234567890 -NewPassword
 "P@ssw0rd"
```

创建组

使用以下步骤创建包含已加入您的 Microsoft AD AWS 托管目录的 EC2 实例的安全组。在创建安全组之前，您需要完成安装 Active Directory 管理工具中的过程。

您也可以使用Windows PowerShell命令来创建群组。有关更多信息，请参阅 Windows Server 2022 文档中的新增广告组。 PowerShell

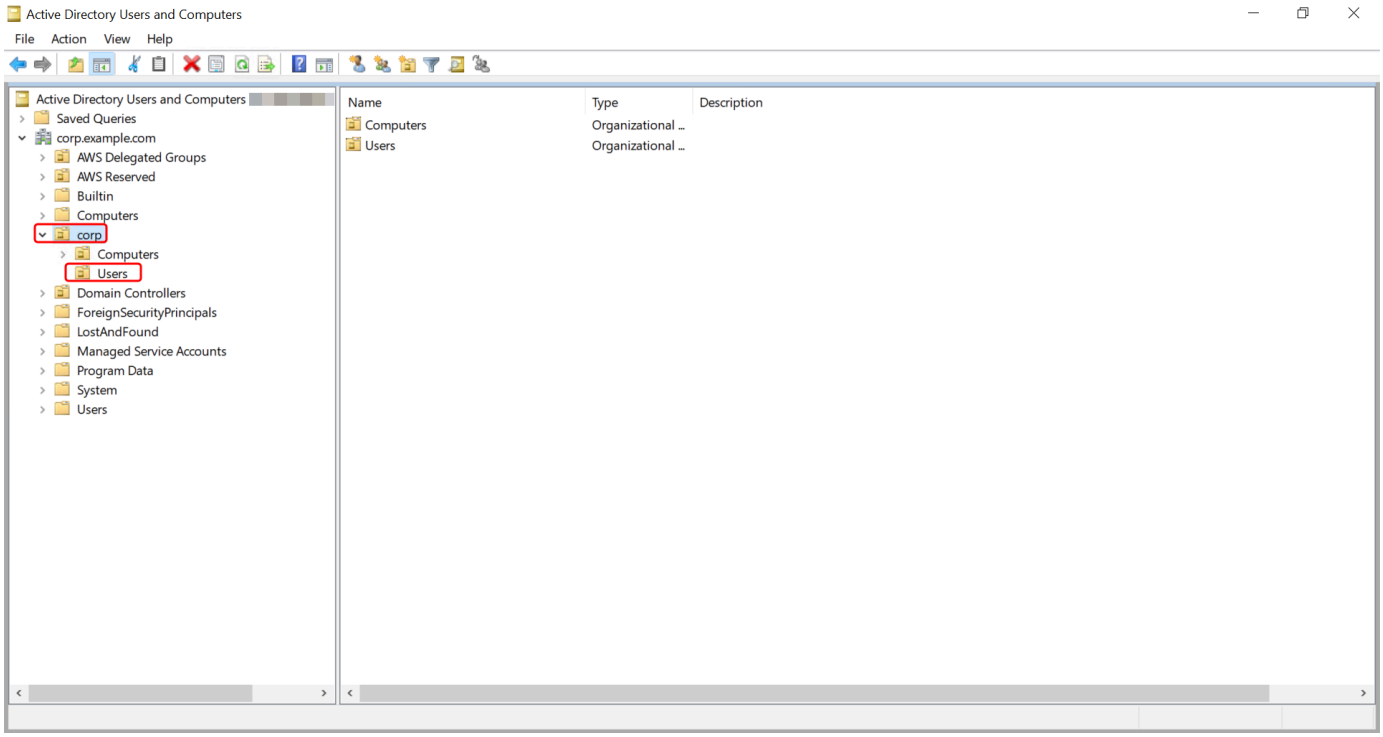
创建组

1. 连接到安装了 Active Directory 管理工具的实例。
2. 打开“Active Directory 用户和计算机”工具。管理工具文件夹中有一个该工具的快捷方式。

> **Tip**
>
> 您可以通过实例上的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
```

3. 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）。有关中目录使用的 OU 结构的更多信息 AWS，请参阅用你的 AWS 托管 Microsoft AD 活动目录创建了什么。



4. 在 Action 菜单上，单击 New，然后单击 Group 打开新组向导。
5. 在组名称中键入组名称，选择满足您需求组范围，然后为组类型选择安全。有关 Active Directory 组范围和安全组的更多信息，请参阅 Microsoft Windows Server 文档中的 Active Directory 安全组。
6. 单击 确定。新安全组会出现在用户文件夹中。

将用户添加到组

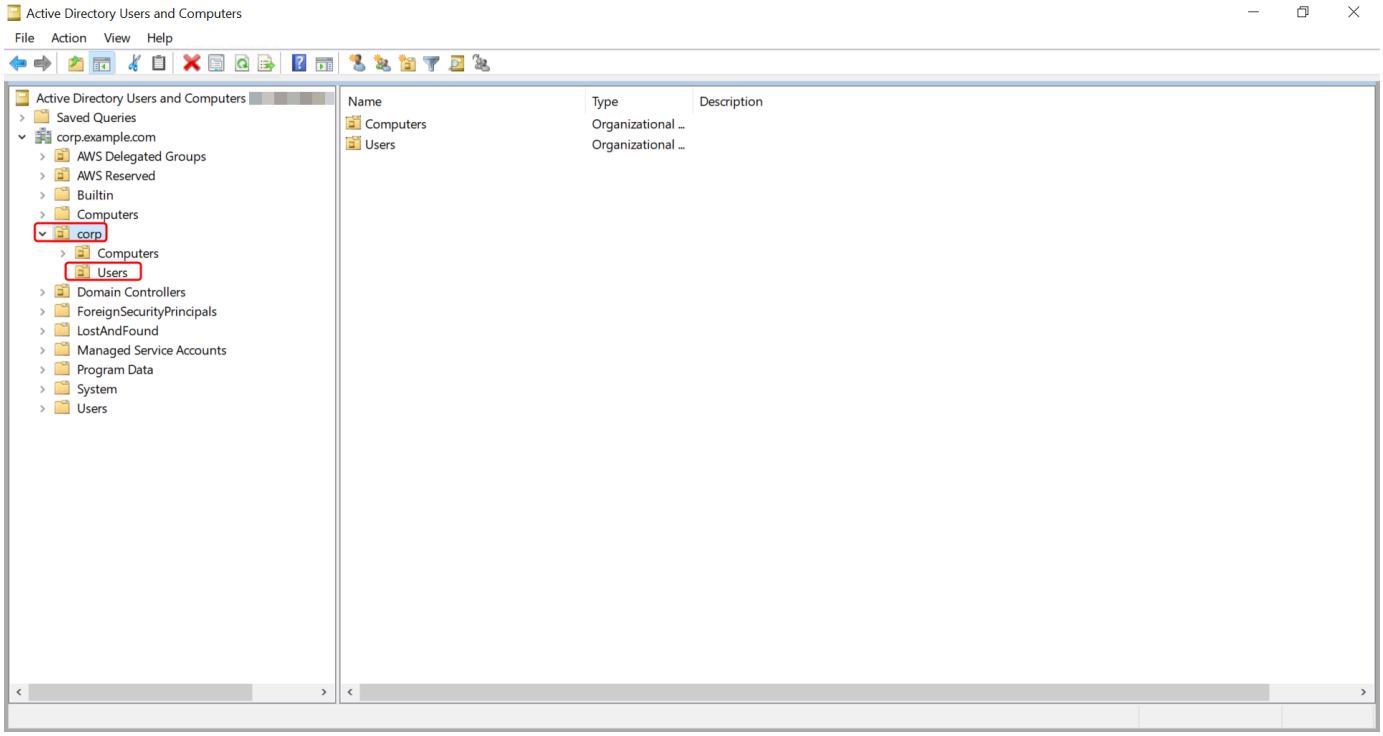
使用以下过程可将用户添加到其 EC2 实例加入到 AWS Managed Microsoft AD 目录的安全组。

如何为群组添加用户

1. 连接到安装了 Active Directory 管理工具的实例。
2. 打开“Active Directory 用户和计算机”工具。管理工具文件夹中有一个该工具的快捷方式。

> **Tip**
>
> 您可以通过实例上的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
> ```

3. 在目录树中，选择存储组的目录 NetBIOS 名称 OU 下的 OU，然后选择要添加用户为成员的组。



4. 在操作菜单上，单击属性打开组的属性对话框。
5. 选择成员选项卡并单击添加。
6. 在 “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”。该名称将显示在成员列表中。再次单击 OK 更新组成员资格。
7. 通过在用户文件夹中选择用户，然后单击操作菜单中的属性打开属性对话框，验证该用户现在是否是组的成员。选择成员选项卡。您应该可以在用户所属的组列表中看到组的名称。

Connect 连接到您现有的活动目录基础架构

本节介绍如何配置AWS托管 Microsoft AD 和你现有的 Active Directory 基础设施之间的信任关系。

主题

- 创建信任关系
- 使用公有 IP 地址时添加 IP 路由
- 教程：在 AWS Microsoft AD 与自托管式 Active Directory 域之间创建信任关系
- 教程：在两个 AWS Managed Microsoft AD 域之间创建信任关系

创建信任关系

你可以在 Microsoft Active Directory 的 AWS 目录服务与自我管理（本地）目录之间以及 AWS 云中多个 AWS 托管 Microsoft AD 目录之间配置单向和双向外部和林信任关系。 AWS 托管 Microsoft AD 支持所有三个信任关系方向：传入、传出和双向（双向）。

有关信任关系的更多信息，请参阅你想了解的有关 AWS 托管 Microsoft AD 的信任的所有信息。

> **Note**
>
> 设置信任关系时，必须确保您的自管理目录与兼容，并且始终与 AWS Directory Service s 兼容。有关您的责任的更多信息，请参阅我们的责任共担模型。

AWS 托管 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 AWS Microsoft AD 与自托管式 Active Directory 域之间创建信任关系。

Amazon Chime、Amazon Connect、亚马逊、亚马逊、亚马逊 QuickSight、亚马 AWS IAM Identity Center逊 WorkSpaces、 WorkDocs WorkMail亚马逊等 AWS 企业应用程序需要双向信任。 AWS Management Console AWS 托管 Microsoft AD 必须能够查询你的自我管理Active Directory中的用户和群组。

Amazon EC2、Amazon RDS 和 Amazon FSx 支持单向或双向信任中的任一种。

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**
>
> AWS 托管 Microsoft AD 不支持对单一标签域名的信任。

连接到 VPC

如果您要与自己的自管理目录建立信任关系，则必须先将您的自我管理网络连接到包含您的托管 AWS Microsoft AD 的 Amazon VPC。您的自我 AWS 管理和托管 Microsoft AD 网络的防火墙必须打开 Microsoft文档中 WindowsServer 2008 及更高版本中列出的网络端口。

要使用您的 NetBIOS 名称代替完整域名对亚马逊或 WorkDocs 亚马逊 AWS 等应用程序进行身份验证 QuickSight，则必须允许端口 9389。有关 Active Directory 端口和协议的更多信息，请参阅Microsoft文档Windows中的服务概述和网络端口要求。

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

包含您的 AWS 托管 Microsoft AD 的 VPC 必须具有相应的出站和入站规则。

配置 VPC 出站规则

1. 在AWS Directory Service 控制台的目录详细信息页面上，记下你的 AWS 托管 Microsoft AD 目录 ID。
2. 通过 https://console.aws.amazon.com/vpc/ 打开 Amazon VPC 控制台。
3. 选择 Security Groups。
4. 搜索你的 AWS 托管微软 AD 目录 ID。在搜索结果中，选择描述为 “为目录 ID 目录控制器AWS 创建安全组” 的项目。

   > **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：

   - Type：All Traffic
   - Protocol：All
   - 目的地确定自托管式网络中可以离开域控制器的流量，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)。您还可以指定同一区域中其他安全组的名称或 ID。有关更多信息，请参阅 了解目录 AWS 的安全组配置并使用。

6. 选择保存。

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 上的预身份验证。

在自托管式域中配置 DNS 条件转发器

必须在自托管式域中设置 DNS 条件转发服务器。有关条件转发器的详细信息，请参阅 Microsoft 上 TechNet 为域名分配条件转发器。

要执行以下步骤，自托管式域必须有权访问以下 Windows Server 工具：

- AD DS 和 AD LDS 工具
- DNS

要在自托管式域上配置条件转发器

1. 首先，你必须获得一些关于你的 AWS 托管 Microsoft AD 的信息。登录 AWS Management Console 并打开 AWS Directory Service 控制台。
2. 在导航窗格中，选择 Directories。
3. 选择你的 Microsoft AWS 托管广告的目录 ID。
4. 记下目录的完全限定域名 (FQDN) 和 DNS 地址。
5. 现在，返回自托管式域控制器。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. 在 DNS 域中，键入你之前提到的 AWS 托管 Microsoft AD 的完全限定域名 (FQDN)。
11. 选择主服务器的 IP 地址，然后键入你之前提到的 Microsoft AD AWS 托管目录的 DNS 地址。

    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 as follows: All DNS servers in this domain。选择 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 AWS 托管 Microsoft AD 上设置信任关系时，你需要使用相同的密码。有关更多信息，请参阅在 Microsoft 上管理信任 TechNet。

现在，您可以在 Microsoft AWS 托管广告上创建信任关系了。

NetBIOS 和域名

为了建立信任关系，NetBIOS 和域名必须是唯一的，并且不能相同。

创建、验证或删除信任关系

> **Note**
>
> 信任关系是 Microsoft AWS 托管 AD 的全球特征。如果您使用的是 多区域复制，则必须在 主区域 中执行以下过程。更改将自动应用于所有复制的区域。有关更多信息，请参阅 全局与区域特色。

与你的 Microsoft AWS 托管 AD 建立信任关系

1. 打开AWS Directory Service 控制台。
2. 在目录页面上，选择你的 AWS 托管 Microsoft AD ID。
3. 在报告详细信息页面上，执行以下操作之一：
   - 如果多区域复制下显示多个区域，选择主区域，然后选择网络与安全选项卡。有关更多信息，请参阅 主区域与其他区域。
   - 如果多区域复制下未显示任何区域，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）如果您只想允许授权用户访问 AWS 托管 Microsoft AD 目录中的资源，则可以选择选择性身份验证复选框。有关选择性身份验证的一般信息，请参阅 Microsoft 上信任的安全注意事项 TechNet。
7. 对于条件转发器，键入自托管式 DNS 服务器的 IP 地址。如果以前创建过条件转发服务器，则可键入自托管式域的 FQDN，而不是 DNS IP 地址。

8. （可选）选择添加其他 IP 地址，然后键入另一台自托管式 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. 选择添加。
10. 如果自托管式域的 DNS 服务器或网络使用公有（非 RFC 1918）IP 地址空间，则转到 IP 路由选择部分，选择操作，然后选择添加路由。使用 CIDR 格式键入 DNS 服务器或自托管式网络的 IP 地址块，例如 203.0.113.0/24。如果 DNS 服务器和自托管式网络均使用 RFC 1918 IP 地址空间，此步骤并不是必要的。

> **Note**
>
> 如果使用公有 IP 地址空间，请确保您不会使用 AWS IP 地址范围内的任何地址，因为无法使用它们。

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 AWS 托管的 Microsoft AD 和各个 Active Directory 域之间创建多个信任。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AWS Directory Service 控制台。
2. 在目录页面上，选择你的 AWS 托管 Microsoft AD ID。
3. 在报告详细信息页面上，执行以下操作之一：
   - 如果多区域复制下显示多个区域，选择主区域，然后选择网络与安全选项卡。有关更多信息，请参阅 主区域与其他区域。
   - 如果多区域复制下未显示任何区域，选择网络与安全选项卡。
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。 AWS 不支持验证传入的信任。有关如何验证与您自行管理的 Active Directory 之间的信任的更多信息，请参阅在 Microsoft TechNet 上验证信任。

删除现有信任关系

1. 打开AWS Directory Service 控制台。
2. 在目录页面上，选择你的 AWS 托管 Microsoft AD ID。
3. 在报告详细信息页面上，执行以下操作之一：
   - 如果多区域复制下显示多个区域，选择主区域，然后选择网络与安全选项卡。有关更多信息，请参阅 主区域与其他区域。
   - 如果多区域复制下未显示任何区域，选择网络与安全选项卡。
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 删除。

使用公有 IP 地址时添加 IP 路由

可以使用 AWS Directory Service for Microsoft Active Directory 来利用许多强大的 Active Directory 功能，包括与其他目录建立信任关系。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。

同样，如果 VPC 使用公有 IP 范围，则在将流量从 AWS 上的 AWS Managed Microsoft AD 路由到对等 AWS VPC 时，也必须输入 IP 地址信息。

当您按照创建信任关系中所述添加 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 了解目录 AWS 的安全组配置并使用。

教程：在 AWS Microsoft AD 与自托管式 Active Directory 域之间创建信任关系

本教程指导您完成在 AWS Directory Service for Microsoft Active Directory 与自托管式（本地）Microsoft Active Directory 之间建立信任关系所需的全部步骤。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
- 步骤 1：准备自托管式 AD 域

- 步骤 2：准备 AWS Managed Microsoft AD
- 步骤 3：创建信任关系

另请参阅

创建信任关系

先决条件

本教程假定您已具备以下条件：

> **Note**
>
> AWS Managed Microsoft AD 不支持对单个标签域的信任。

- 一个创建在 AWS 上的 AWS Managed Microsoft AD 目录。如果需要有关执行此操作的帮助，请参阅微软 AD AWS 托管入门。
- 一个添加到该 AWS Managed Microsoft AD 的运行 Windows 的 EC2 实例。如果需要有关执行此操作的帮助，请参阅手动将 Amazon EC2 Windows 实例加入您的 AWS 托管微软 AD Active Directory。

  > **Important**
  >
  > AWS Managed Microsoft AD 的管理员账户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，请参阅安装适用于 AWS 托管微软 AD 的 Active Directory 管理工具。
- 一个自托管式（本地）Microsoft Active Directory

  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。
- 自托管式网络与包含 AWS Managed Microsoft AD 的 VPC 之间的一个活动连接。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。

- 一个正确设置的本地安全策略。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
- 为了建立信任关系，NetBIOS 和域名必须是唯一的，并且不能相同

有关创建信任关系的先决条件的更多信息，请参阅 创建信任关系。

教程配置

在本教程中，我们已经创建了一个 AWS Managed Microsoft AD 和一个自托管式域。自我托管式网络已连接到 AWS Managed Microsoft AD 的 VPC。以下是两个目录的属性：

在 AWS 上运行的 AWS Managed Microsoft AD

- 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

AWS Managed Microsoft AD 位于 VPC ID：vpc-12345678 中。

自托管式或 AWS Managed Microsoft AD 域

- 域名 (FQDN)：corp.example.com
- NetBIOS 名称：CORP
- DNS 地址：172.16.10.153
- 自托管式 CIDR：172.16.0.0/16

下一步

步骤 1：准备自托管式 AD 域

步骤 1：准备自托管式 AD 域

首先需要完成对自托管式（本地）域完成几个先决条件步骤。

配置自托管式防火墙

您必须配置您的自我管理防火墙，以便包含您的托管 AWS Microsoft AD 的 VPC 使用的所有子网的 CIDR 开放以下端口。在本教程中，我们允许来自以下端口的 10.0.0.0/16（我们托管 AWS Microsoft AD 的 VPC 的 CIDR 块）的传入和传出流量：

- TCP/UDP 53 - DNS
- TCP/UDP 88 - Kerberos 身份验证
- TCP/UDP 389-轻量级目录访问协议 (LDAP)
- TCP 445-服务器消息块 (SMB)
- TCP 9389-Active Directory Web 服务 (ADWS)（可选 ——如果你想使用你的 NetBIOS 名称而不是完整的域名来使用亚马逊或 AWS 亚马逊等应用程序进行身份验证，则需要打开此端口。） WorkDocs QuickSight

> **Note**
>
> 不再支持 SMBv1。
> 这些是将 VPC 连接到自托管式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。

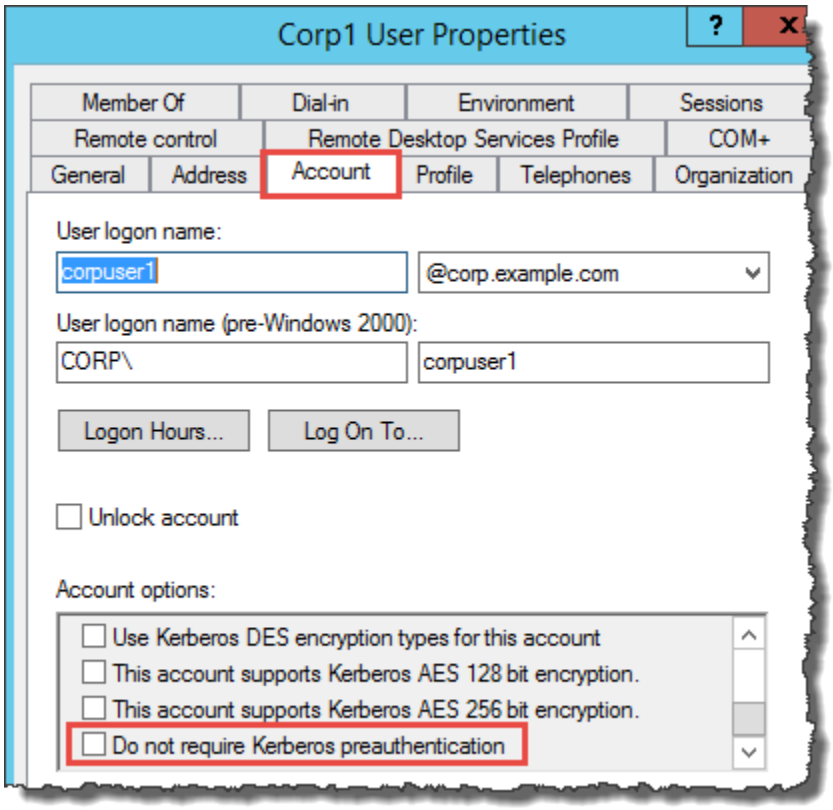
确保已启用 Kerberos 预身份验证

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。

查看用户的 Kerberos 设置

1. 在自托管式域控制器上，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。



为自托管式域配置 DNS 条件转发器

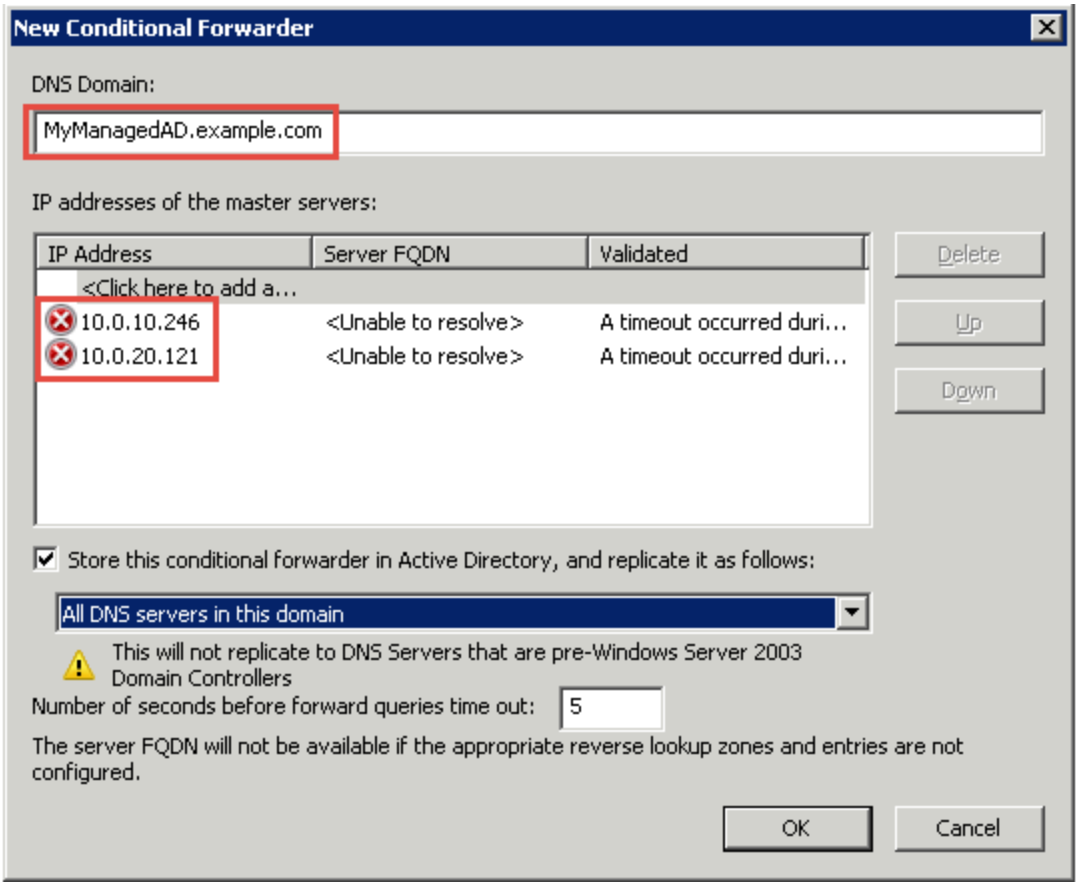
必须在每个域中都设置 DNS 条件转发服务器。在自行管理的域上执行此操作之前，您将首先获得有关您的 AWS 托管 Microsoft AD 的一些信息。

要在自托管式域上配置条件转发器

1. 登录 AWS Management Console 并打开AWS Directory Service 控制台。
2. 在导航窗格中，选择 Directories。
3. 选择你的 Microsoft AWS 托管广告的目录 ID。
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，返回自托管式域控制器。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. 在 DNS 域中，键入你之前提到的 AWS 托管 Microsoft AD 的完全限定域名 (FQDN)。在此示例中，FQDN 是 MyManaged ad.example.com。
11. 选择主服务器的 IP 地址，然后键入你之前提到的 Microsoft AD AWS 托管目录的 DNS 地址。在此示例中，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

步骤 2：准备 AWS Managed Microsoft AD

步骤 2：准备 AWS Managed Microsoft AD

现在，让我们为你的 AWS 托管 Microsoft AD 做好建立信任关系的准备。以下许多步骤与刚才为自托管式域完成的步骤几乎相同。但是，这次你使用的是你的 AWS 托管 Microsoft AD。

配置 VPC 子网和安全组

您必须允许流量从您的自行管理的网络流向包含您的 AWS 托管 Microsoft AD 的 VPC。为此，您需要确保与用于部署托管 AWS Microsoft AD 的子网关联的 ACL 和在域控制器上配置的安全组规则都允许支持信任所需的流量。

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
- TCP/UDP 464 - Kerberos 身份验证
- TCP 636 - LDAPS (通过 TLS/SSL 的 LDAP)
- TCP 3268-3269 – 全局目录
- TCP/UDP 49152-65535 – RPC 的临时端口

> **Note**
>
> 不再支持 SMBv1。

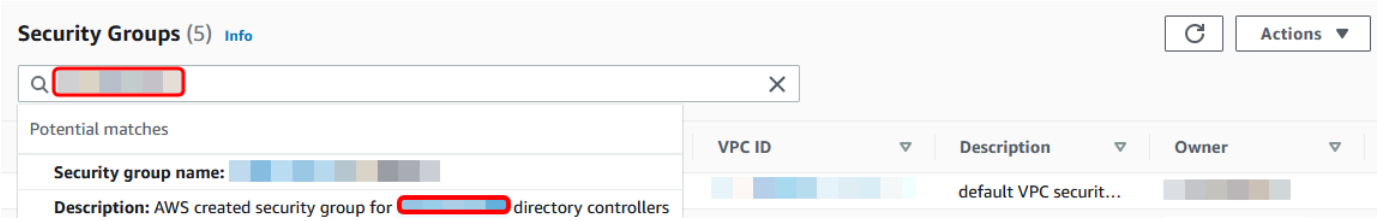
出站

- ALL

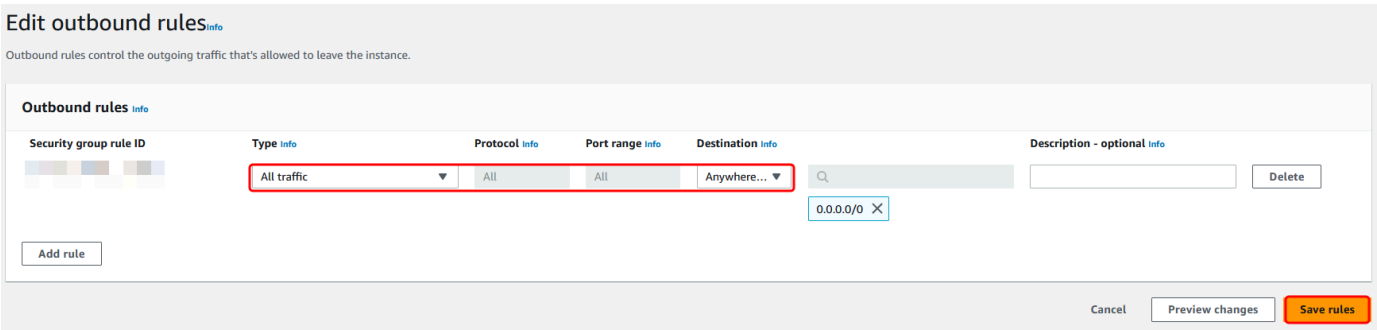
> **Note**
>
> 这些是连接 VPC 和自托管式目录所需的最少端口。根据您的特定配置，您可能需要打开其他端口。

配置你的 AWS 托管 Microsoft AD 域控制器出站和入站规则

1. 返回到 AWS Directory Service 控制台。在目录列表中，记下你的 Microsoft AD AWS 托管目录的目录 ID。
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（安全组）。
4. 使用搜索框搜索你的 AWS 托管 Microsoft AD 目录 ID。在搜索结果中，选择带有描述的安全组**`AWS created security group for yourdirectoryID directory controllers`**。



5. 转到该安全组的 Outbound Rules 选项卡。选择编辑出站规则，然后选择添加规则。对于新规则，输入以下值：
   - Type：ALL Traffic
   - Protocol：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)。您还可以指定同一区域中其他安全组的名称或 ID。有关更多信息，请参阅 了解目录 AWS 的安全组配置并使用。
6. 选择保存规则。

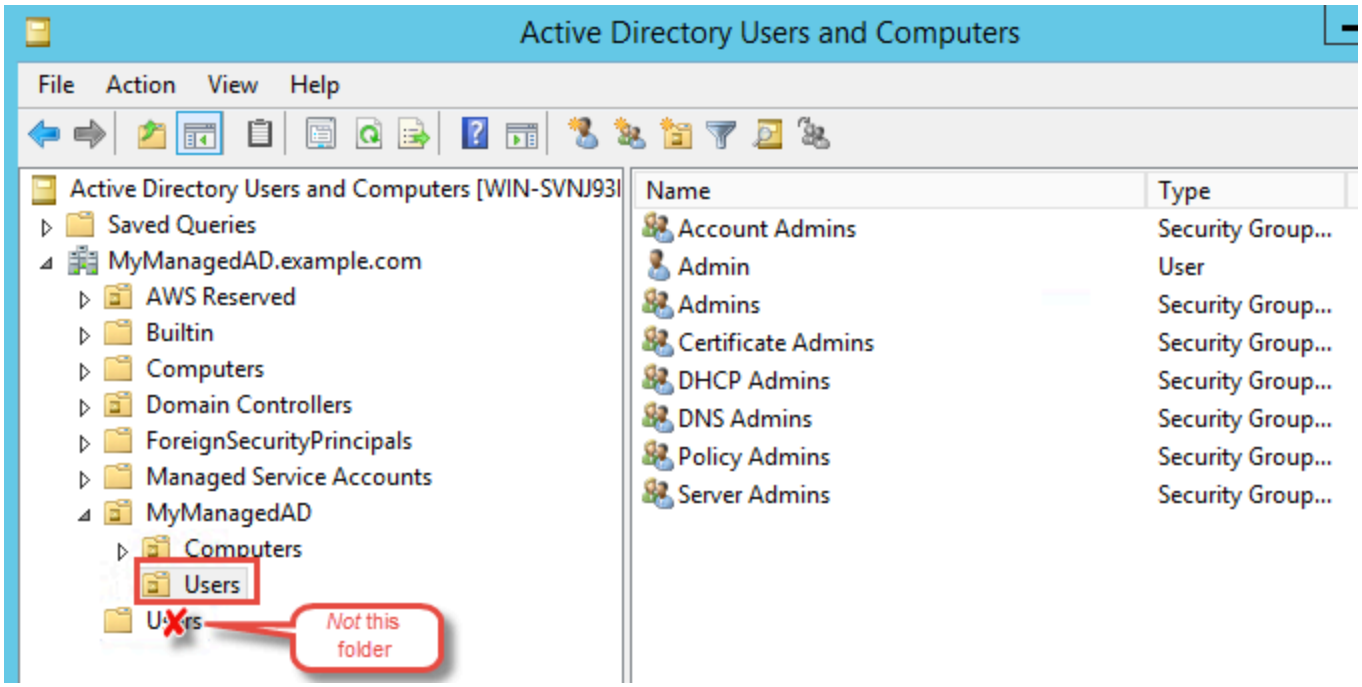


确保已启用 Kerberos 预身份验证

现在，您需要确认您的 AWS 托管 Microsoft AD 中的用户是否也启用了 Kerberos 预身份验证。此过程与针对自托管式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。

要查看用户 Kerberos 设置

1. 使用域名或已被委派 AWS 管理域中用户的权限的账户，登录属于托管 Microsoft AD 目录成员的实例。管理员账户的权限
2. 如果尚未安装，请安装“Active Directory 用户和计算机”工具和 DNS 工具。可在安装适用于 AWS 托管微软 AD 的 Active Directory 管理工具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

步骤 3：创建信任关系

步骤 3：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。首先在自托管式域上创建信任，最后在 AWS Managed Microsoft AD 上创建信任。如果您在创建信任的过程中遇到任何问题，请参阅信任创建状态原因获得帮助。

在自托管式 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，如果在自托管式域上创建单向传出信任，则需要在 AWS Managed Microsoft AD 上创建单向传入信任。

> **Note**
>
> AWS Managed 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。

配置对您自行管理的 Active Directory 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 AWS Managed Microsoft AD 的名称，然后选择下一步。
4. 选择 Forest trust。选择下一步。
5. 选择 Two-way。选择下一步。
6. 选择 This domain only。选择下一步。
7. 选择 Forest-wide authentication。选择下一步。
8. 键入 Trust password。请务必记住此密码，因为在为 AWS Managed Microsoft AD 设置信任时会需要它。
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。选择下一步。
11. 选择 No, do not confirm the incoming trust。选择下一步。

在 AWS Managed Microsoft AD 目录中配置信任

最后，配置与 AWS Managed Microsoft AD 目录的林信任关系。因为已在自托管式域上创建了双向林信任，因此还将使用 AWS Managed Microsoft AD 创建双向信任。

> **Note**
>
> 信任关系是 AWS Managed Microsoft AD 的全局功能。如果您使用的是 多区域复制，则必须在 主 区域 中执行以下过程。更改将自动应用于所有复制的区域。有关更多信息，请参阅全局与区域特色：

要在 AWS Managed Microsoft AD 目录中配置信任

1. 返回到 AWS Directory Service 控制台。
2. 在目录页面上，选择 AWS Managed Microsoft AD ID。
3. 在报告详细信息页面上，执行以下操作之一：
   - 如果多区域复制下显示多个区域，选择主区域，然后选择网络与安全选项卡。有关更多信息，请参阅主区域与其他区域：
   - 如果多区域复制下未显示任何区域，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. 在添加信任关系页面上，指定信任类型。在本例中，我们选择树信任。键入自托管式域的 FQDN（在本教程 **`corp.example.com`** 中）。键入在自托管式域上创建信任时所使用的信任密码。指定方向。在本例中，我们选择双向。
6. 在条件转发器字段中，输入自托管式 DNS 服务器的 IP 地址。在此示例中，输入 172.16.10.153。
7. （可选）选择添加其他 IP 地址，并输入自托管式 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. 选择添加。

祝贺您。现在，你的自我管理域名 (corp.example.com) 和你的托管AWS微软 AD (ad.example.com) 之间存在信任关系。MyManaged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。

教程：在两个 AWS Managed Microsoft AD 域之间创建信任关系

本教程指导您完成在两个 AWS Directory Service for Microsoft Active Directory 域之间建立信任关系所需的全部步骤。

主题

- 步骤 1：准备 AWS Managed Microsoft AD
- 步骤 2：与其他 AWS Managed Microsoft AD 域创建信任关系

另请参阅

创建信任关系

步骤 1：准备 AWS Managed Microsoft AD

在本节中，您将准备好您的 AWS 托管 Microsoft AD 与其他 AWS 托管 Microsoft AD 建立信任关系。以下许多步骤与在 教程：在 AWS Microsoft AD 与自托管式 Active Directory 域之间创建信任关系 中完成的步骤几乎相同。但是，这一次，你要将 AWS 托管 Microsoft AD 环境配置为可以相互协作。

配置 VPC 子网和安全组

您必须允许流量从一个 AWS 托管的微软 AD 网络流向包含您的另一个 AWS 托管微软 AD 的 VPC。为此，您需要确保与用于部署托管 AWS Microsoft AD 的子网关联的 ACL 和在域控制器上配置的安全组规则都允许支持信任所需的流量。

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 3268-3269 – 全局目录
- TCP/UDP 1024-65535 - RPC 的临时端口

出站

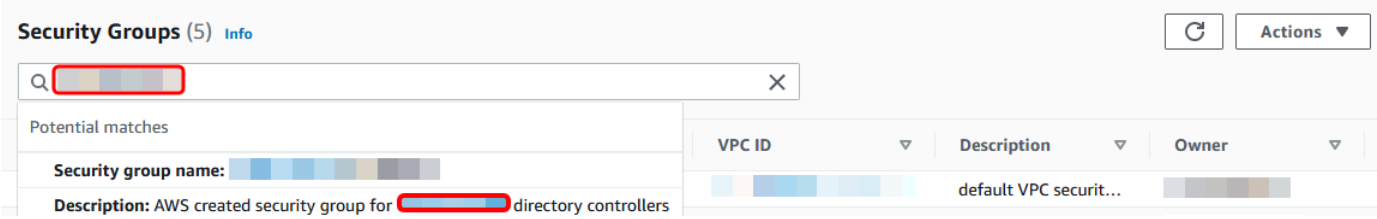
- ALL

> **Note**
>
> 这些是从两个 AWS Managed Microsoft AD 的目录连接 VPC 所需的最低端口。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 Microsoft 网站上的 How to configure a firewall for Active Directory domains and trusts。

配置你的 AWS 托管 Microsoft AD 域控制器出站规则

> **Note**
>
> 对每个目录重复下面的步骤 1-6。

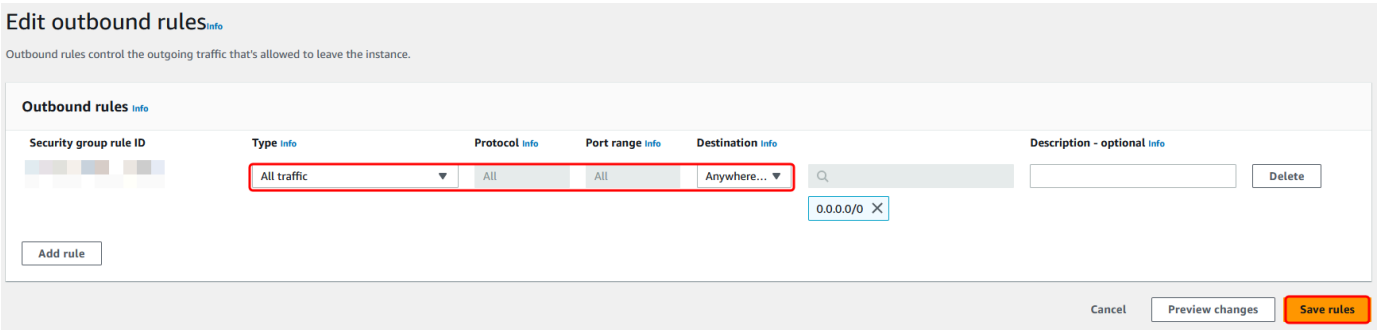
1. 转到 AWS Directory Service 控制台。在目录列表中，记下你的 Microsoft AD AWS 托管目录的目录 ID。
2. 通过以下网址打开 Amazon VPC 控制台：https://console.aws.amazon.com/vpc/。
3. 在导航窗格中，选择 Security Groups（安全组）。
4. 使用搜索框搜索你的 AWS 托管 Microsoft AD 目录 ID。在搜索结果中，选择带 **`AWS created security group for yourdirectoryID directory controllers`** 描述的项目。



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：

   - Type：ALL Traffic
   - Protocol：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)。您还可以指定同一区域中其他安全组的名称或 ID。有关更多信息，请参阅 了解目录 AWS 的安全组配置并使用。

6. 选择保存。

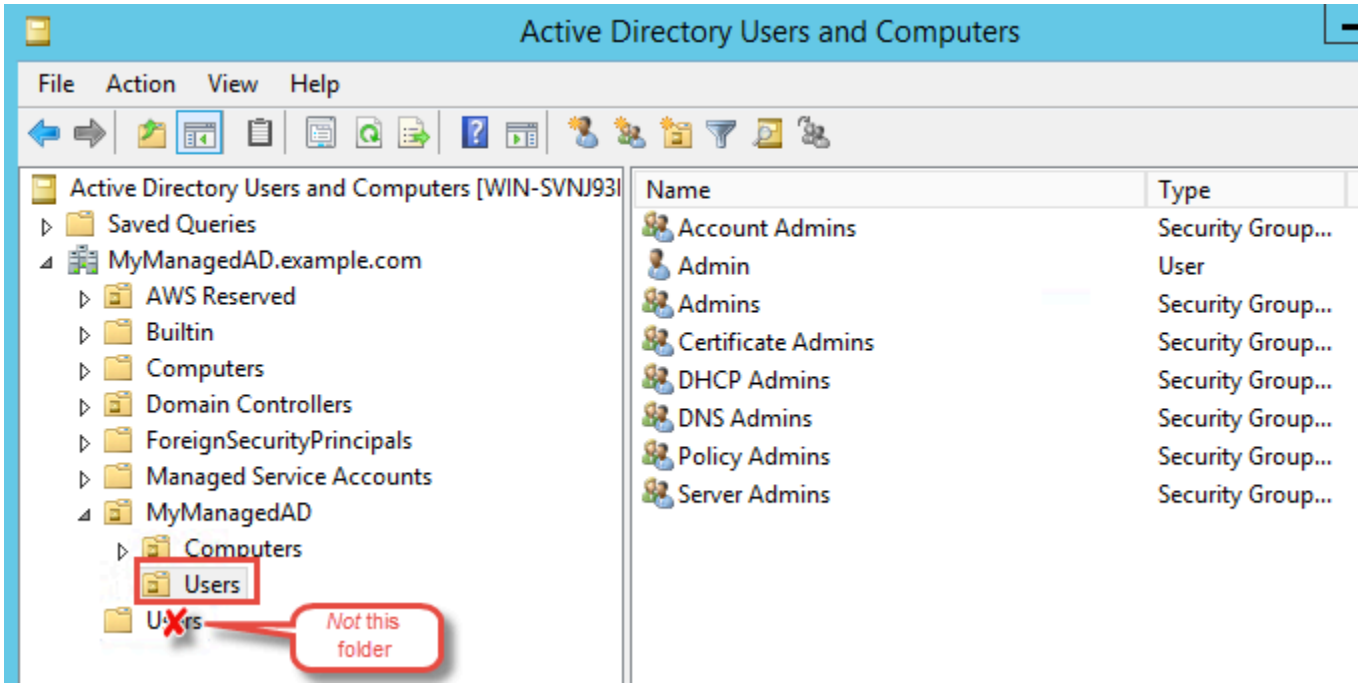


确保已启用 Kerberos 预身份验证

现在，你要确认你的 AWS 托管 Microsoft AD 中的用户是否也启用了 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。

要查看用户 Kerberos 设置

1. 使用域名或已被委派 AWS 管理域中用户的权限的账户，登录属于托管 Microsoft AD 目录成员的实例。管理员账户的权限
2. 如果尚未安装，请安装“Active Directory 用户和计算机”工具和 DNS 工具。可在安装适用于 AWS 托管微软 AD 的 Active Directory 管理工具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

步骤 2：与其他 AWS Managed Microsoft AD 域创建信任关系

步骤 2：与其他 AWS Managed Microsoft AD 域创建信任关系

现在准备工作已完成，最后的几个步骤是在两个 AWS Managed Microsoft AD 之间创建信任。如果您在创建信任的过程中遇到任何问题，请参阅信任创建状态原因获得帮助。

在首个 AWS Managed Microsoft AD 域中配置信任

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，如果在该首个域上创建单向传出信任，则需要在第二个 AWS Managed Microsoft AD 域上创建单向传入信任。

> **Note**
>
> AWS Managed 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。

要在首个 AWS Managed Microsoft AD 域中配置信任

1. 打开 AWS Directory Service 控制台。
2. 在目录页面上，选择首个 AWS Managed Microsoft AD ID。
3. 在报告详细信息页面上，执行以下操作之一：
   - 如果多区域复制下显示多个区域，选择主区域，然后选择网络与安全选项卡。有关更多信息，请参阅 主区域与其他区域。
   - 如果多区域复制下未显示任何区域，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. 在添加信任关系页面上，键入第二个 AWS Managed Microsoft AD 域的 FQDN。请务必记住此密码，因为在为第二个 AWS Managed Microsoft AD 设置信任时会需要它。指定方向。在本例中，选择双向。
6. 在条件转发器字段中，输入 AWS Managed Microsoft AD DNS 服务器的 IP 地址。
7. （可选）选择添加其他 IP 地址，并输入第二个 AWS Managed Microsoft AD 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）。此时信任将失败，我们创建信任的另一端之前，此为预期行为。

在第二个 AWS Managed Microsoft AD 域中配置信任

现在，配置与的第二个 AWS Managed Microsoft AD 目录的林信任关系。因为已在首个 AWS Managed Microsoft AD 域上创建了双向林信任，因此还将使用此 AWS Managed Microsoft AD 域创建双向信任。

要在第二个 AWS Managed Microsoft AD 域中配置信任

1. 返回到 AWS Directory Service 控制台。
2. 在目录页面上，选择第二个 AWS Managed Microsoft AD ID。
3. 在报告详细信息页面上，执行以下操作之一：
   - 如果多区域复制下显示多个区域，选择主区域，然后选择网络与安全选项卡。有关更多信息，请参阅 主区域与其他区域。
   - 如果多区域复制下未显示任何区域，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. 在添加信任关系页面上，键入首个 AWS Managed Microsoft AD 域的 FQDN。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. 在条件转发器字段中，输入首个 AWS Managed Microsoft AD DNS 服务器的 IP 地址。
7. （可选）选择添加其他 IP 地址，并输入首个 AWS Managed Microsoft AD 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）。信任应在不久之后得到验证。
9. 现在，回到您在首个域中创建的信任，然后再次验证信任关系。

祝贺您。现在，您的两个 AWS Managed Microsoft AD 域之间已具有信任关系。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。

将你的 Microsoft AWS 托管广告连接到 Microsoft Entra Connect Sync

本教程将引导你完成必要的安装步骤，以便将你Microsoft Entra ID同步Microsoft Entra Connect Sync到 AWS 托管 Microsoft AD。

在本教程中，您将执行以下操作：

1. 创建 AWS 托管微软 AD 域用户。
2. 下载 Entra Connect Sync。
3. Windows PowerShell用于运行脚本，为新创建的用户提供适当的权限。
4. 安装 Entra Connect Sync。

先决条件

要完成本教程，您需要做以下准备：

- 微软的 AWS 托管广告。有关更多信息，请参阅 the section called “创建你的 Microsoft AWS 托管广告”。
- 亚马逊 EC2 Windows 服务器实例已加入您的 AWS 托管微软 AD。有关更多信息，请参阅 无缝加入 Windows 实例。
- Active DirectoryAdministration Tools安装了用于管理您的 AWS 托管微软 AD 的 EC2 Windows 服务器。有关更多信息，请参阅 the section called “安装适用于 AWS 托管 Microsoft AD 的 AD 管理工具”。

步骤 1：创建Active Directory域用户

本教程假设你已经Active DirectoryAdministration Tools安装了 AWS 托管 Microsoft AD 和一个 EC2 Windows 服务器实例。有关更多信息，请参阅 the section called “安装适用于 AWS 托管 Microsoft AD 的 AD 管理工具”。

1. Connect 连接到安装Active DirectoryAdministration Tools它们的实例。
2. 创建 AWS 托管微软 AD 域用户。此用户将成为 f Active Directory Directory Service (AD DS) Connector account orEntra Connect Sync. 有关此过程的详细步骤，请参阅the section called “创建用户”。

第 2 步：下载 Entra Connect Sync

- Entra Connect Sync从Microsoft网站下载到作为 AWS 托管的 Microsoft AD 管理员的 EC2 实例。

> **Warning**
>
> 此Entra Connect Sync时请勿打开或运行。接下来的步骤将为在步骤 1 中创建的域用户提供必要的权限。

步骤 3：运行Windows PowerShell脚本

- 以@@ 管理员PowerShell身份打开并运行以下脚本。脚本运行时，系统将要求您输入步骤 1 中新创建AccountName的域用户的 SaM。

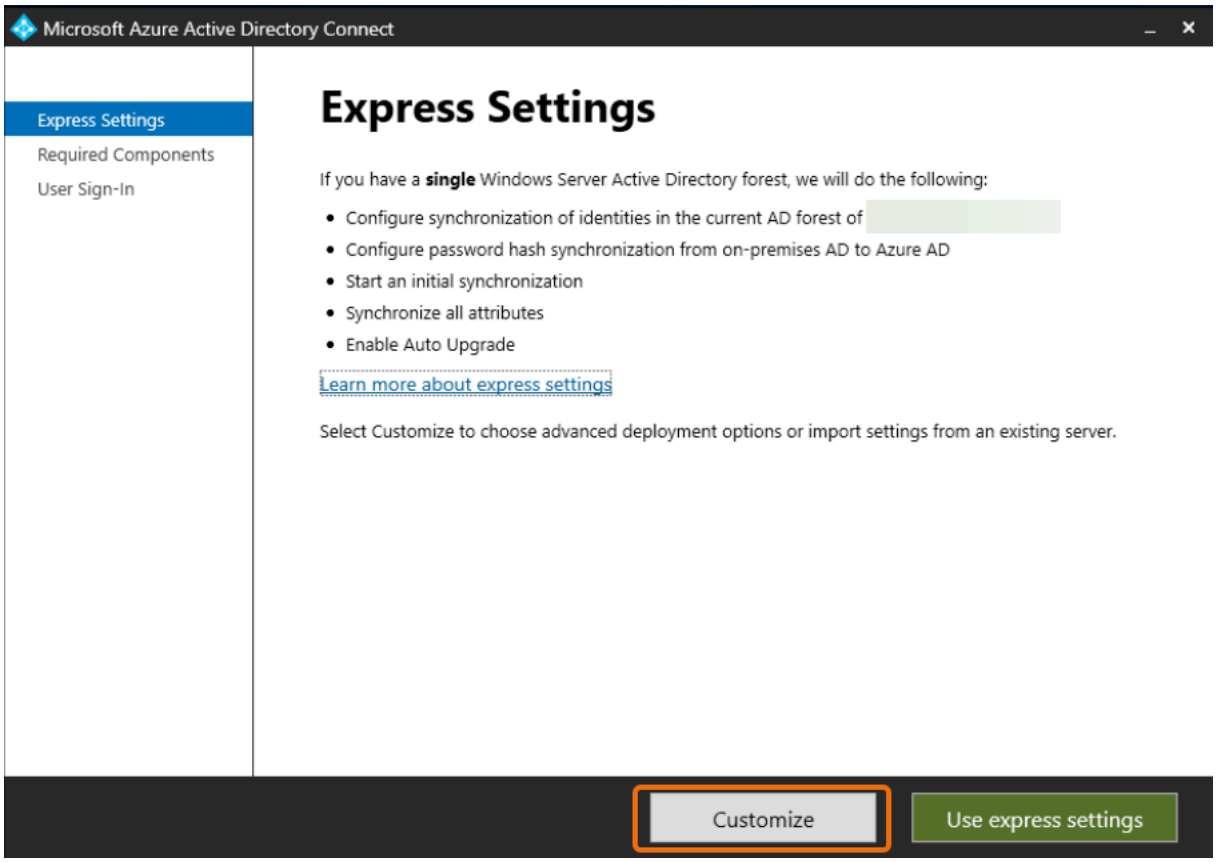
```
$modulePath = "C:\Program Files\Microsoft Azure Active Directory Connect\AdSyncConfig
\AdSyncConfig.psm1"

try {
    # Attempt to import the module
    Write-Host -ForegroundColor Green "Importing Module for Azure Entra Connect..."
    Import-Module $modulePath -ErrorAction Stop
    Write-Host -ForegroundColor Green "Success!"
}
catch {
    # Display the exception message
    Write-Host -ForegroundColor Red "An error occurred: $($_.Exception.Message)"
```

```
}

Function Set-EntraConnectSvcPerms {
    [CmdletBinding()]
    Param (
        [String]$ServiceAccountName
    )

    #Requires -Modules 'ActiveDirectory' -RunAsAdministrator

    Try {
        $Domain = Get-ADDomain -ErrorAction Stop
    } Catch [System.Exception] {
        Write-Output "Failed to get AD domain information $_"
    }

    $BaseDn = $Domain | Select-Object -ExpandProperty 'DistinguishedName'
    $Netbios = $Domain | Select-Object -ExpandProperty 'NetBIOSName'

    Try {
        $OUs = Get-ADOrganizationalUnit -SearchBase "OU=$Netbios,$BaseDn" -
SearchScope 'Onelevel' -Filter * -ErrorAction Stop | Select-Object -ExpandProperty
 'DistinguishedName'
    } Catch [System.Exception] {
        Write-Output "Failed to get OUs under OU=$Netbios,$BaseDn $_"
    }

    Try {
        $ADConnectorAccountDN = Get-ADUser -Identity $ServiceAccountName -ErrorAction
 Stop | Select-Object -ExpandProperty 'DistinguishedName'
    } Catch [System.Exception] {
        Write-Output "Failed to get service account DN $_"
    }

    Foreach ($OU in $OUs) {
        try {
        Set-ADSyncMsDsConsistencyGuidPermissions -ADConnectorAccountDN
 $ADConnectorAccountDN -ADobjectDN $OU -Confirm:$false -ErrorAction Stop
        Write-Host "Permissions set successfully for $ADConnectorAccountDN and $OU"

        Set-ADSyncBasicReadPermissions -ADConnectorAccountDN $ADConnectorAccountDN -
ADobjectDN $OU -Confirm:$false -ErrorAction Stop
        Write-Host "Basic read permissions set successfully for $ADConnectorAccountDN
 on OU $OU"
```

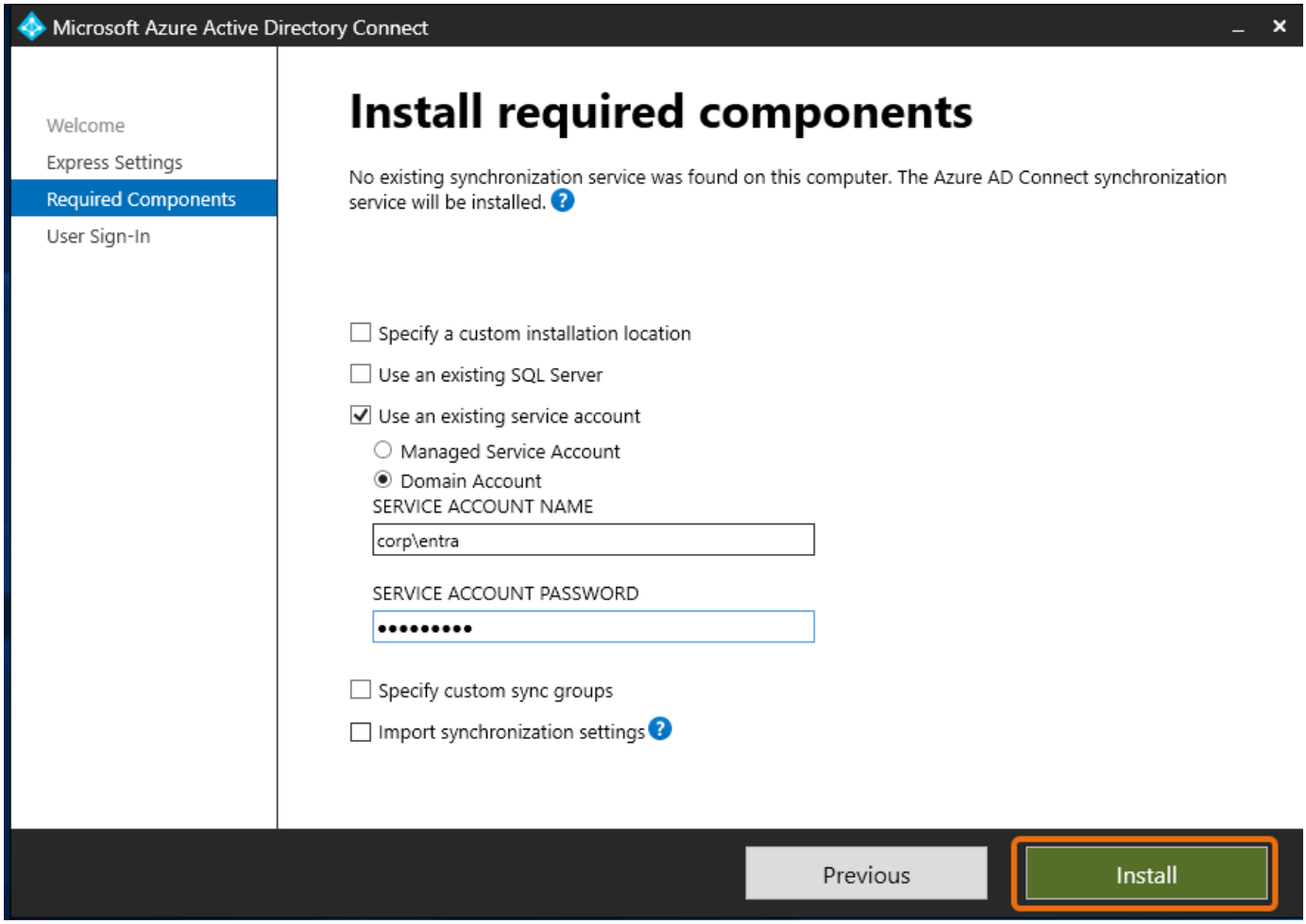
```
    }
    catch {
        Write-Host "An error occurred while setting permissions for
 $ADConnectorAccountDN on OU $OU : $_"
    }
    }
}
```

第 4 步：安装 Entra Connect Sync

1. 脚本完成后，您可以运行下载的Microsoft Entra Connect（以前称为Azure Active Directory Connect）配置文件。
2. 运行上一步中的配置文件后，将打开一个MicrosoftAzure Active Directory Connect窗口。在 “快速设置” 窗口中，选择 “自定义”。



3. 在 “安装所需组件” 窗口中，选中 “使用现有服务帐户” 复选框。在服务帐户名称和服务帐户密码中，输入您在步骤 1 中创建的用户的AD DS Connector account名称和密码。例如，如果你的AD DS Connector account名字是`entra`，那么账户名就是`corp\entra`。然后选择 “安装”。



4. 在 “用户登录” 窗口中，选择以下选项之一：

   a. 直通身份验证-此选项允许您Active Directory使用用户名和密码登录。

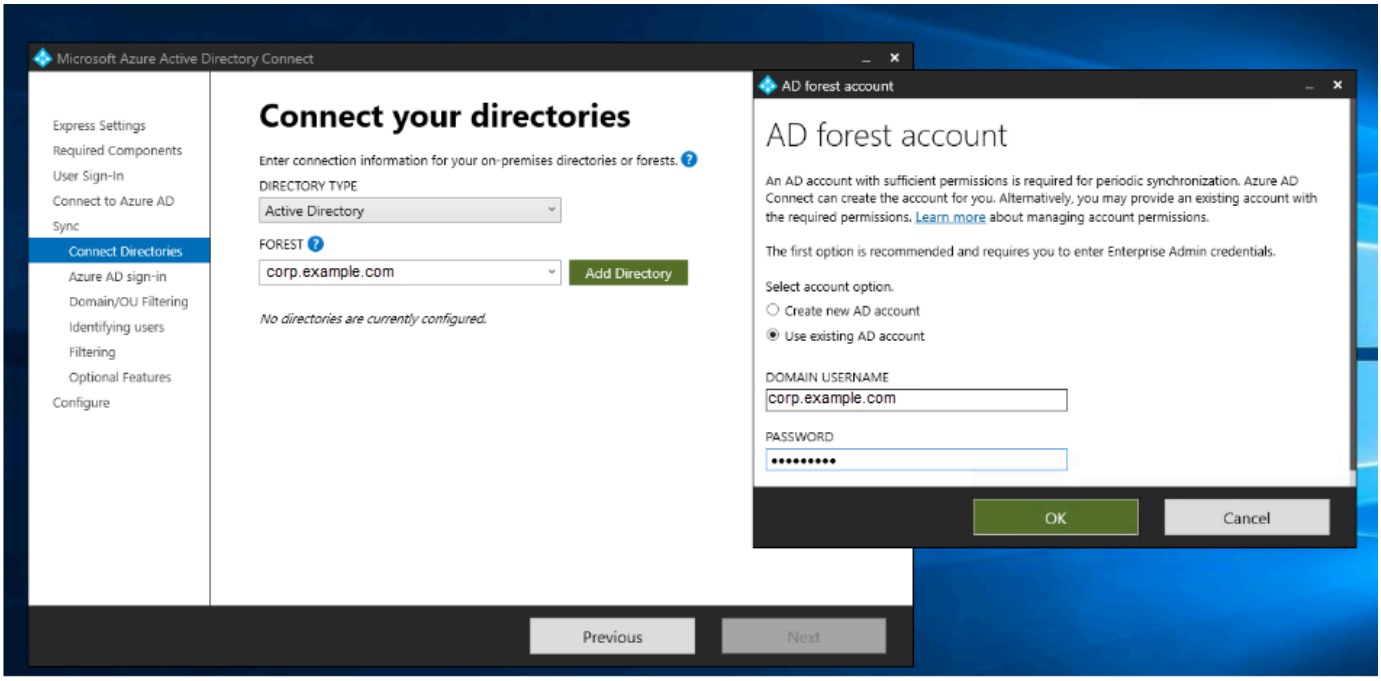
   b. 请勿配置-这允许您使用联合登录Microsoft Entra（以前称为 Azure Active Directory (AzureAD)）或Office 365。

   然后选择下一步。

5. 在 Connect to Azure 窗口中，输入您的全局管理员用户名和密码，然后选择下一步。Entra ID

6. 在 “Connect 您的目录” 窗口中，选择 “Active Directory目录类型”。为你的 FOREST AWS 托管 Microsoft AD 选择森林。然后选择 “添加目录”。

7. 将出现一个弹出框，要求您选择账户选项。选择 “使用现有 AD 账户”。输入在步骤 1 中创建的AD DS Connector account用户名和密码，然后选择确定。然后选择下一步。



8. 在 “Azure AD登录” 窗口中，选择 “继续”，但不要将所有 UPN 后缀与已验证的域名进行匹配，前提是您没有添加经过验证的虚域名。Entra ID然后选择下一步。
9. 在域/OU 筛选窗口中，选择适合您需求的选项。有关更多信息，请参阅 Entra Connect Sync：Microsoft文档中的配置筛选。然后选择下一步。
10. 在 “识别用户、筛选和可选功能” 窗口中，保留默认值并选择 “下一步”。
11. 在配置窗口中，查看配置设置并选择配置。的安装Entra Connect Sync将完成，用户将开始与同步Microsoft Entra ID。

扩展架构

AWS Managed Microsoft AD 使用架构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，您可以使用有效的 LDAP 数据交换格式（LDIF）文件修改 AWS Managed Microsoft AD 目录的架构。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

- 何时扩展 AWS Managed Microsoft AD 架构
- 教程：扩展你的 AWS 托管 Microsoft AD 架构

何时扩展 AWS Managed Microsoft AD 架构

通过添加新对象类和属性可以扩展 AWS Managed 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。在需要将依赖于 AWS Managed Microsoft AD 的企业应用程序迁移到 AWS Cloud 的情况下，这特别有用。

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 AWS Managed Microsoft AD 中。

要了解其用法，请参阅 教程：扩展你的 AWS 托管 Microsoft AD 架构。

相关主题

- 扩展架构
- 架构元素

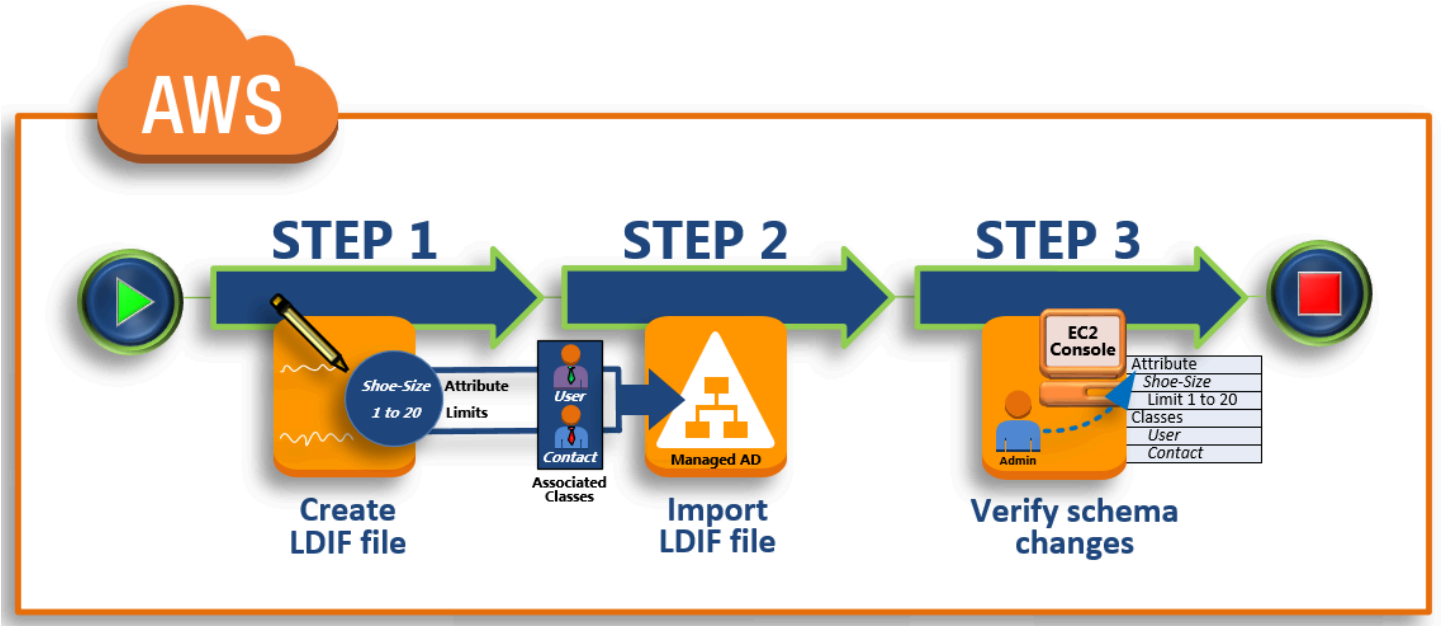
教程：扩展你的 AWS 托管 Microsoft AD 架构

在本教程中，您将学习如何通过添加满足您 AWS 特定要求的独特属性和类来扩展微软活动目录目录的架构，也称为 AWS 托管 Microsoft AD。 AWS 托管 Microsoft AD 架构扩展只能使用有效的 LDIF（轻量级目录交换格式）脚本文件上传和应用。

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，请参阅何时扩展 AWS Managed Microsoft AD 架构。

此工作流程具有三个基本步骤。



步骤 1：创建 LDIF 文件

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。

步骤 2：导入 LDIF 文件

在此步骤中，您将使用 AWS Directory Service 控制台将 LDIF 文件导入到您的 Microsoft Active Directory 环境中。

步骤 3：验证架构扩展是否成功

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。

步骤 1：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。

通过在 AWS Directory Service 托管 AWS Microsoft AD 目录上运行`ldifde.exe`应用程序，导入带有架构更改的 LDIF 文件。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。

- 项目序列 – 确保 LDIF 文件中的项目布局顺序自上而下按照目录信息树（DIT）进行。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。
  - 不支持 defaultSecurityDescriptor 对的更改。

要详细了解如何构建 LDIF 文件并查看可用于测试托管 AWS Microsoft AD 架构扩展的 LDIF 文件示例，请参阅安全博客上的 “如何扩展托管 AWS Microsoft AD 目录架构” 一文。 AWS

下一步

步骤 2：导入 LDIF 文件

步骤 2：导入 LDIF 文件

您可以通过从 AWS Directory Service 控制台导入 LDIF 文件或使用 API 来扩展架构。有关如何使用架构扩展 API 执行此操作的更多信息，请参阅 AWS Directory Service API Reference。目前， AWS 不支持通过外部应用程序（如 Microsoft Exchange）直接执行架构更新。

Important

当你对 AWS 托管的 Microsoft AD 目录架构进行更新时，该操作是不可逆的。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，Mic AWS rosoft AD 会拍摄快照以保留目录的当前状态。

Note

架构扩展是 AWS 托管 Microsoft AD 的一项全球功能。如果您使用的是 多区域复制，则必须在 主 区域 中执行以下过程。更改将自动应用于所有复制的区域。有关更多信息，请参阅 全局与区域特色。

导入 LDIF 文件

1. 在 AWS Directory Service 控制台导航窗格中，选择目录。
2. 在目录页面上，选择您的目录 ID。
3. 在报告详细信息页面上，执行以下操作之一：
   - 如果多区域复制下显示多个区域，选择主区域，然后选择维护选项卡。有关更多信息，请参阅主区域与其他区域。
   - 如果多区域复制下未显示任何区域，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

上传 LDIF 文件后， AWS Microsoft AD 会采取措施保护您的目录免受错误影响，因为它会按以下顺序应用更改。

1. 验证 LDIF 文件。由于 LDIF 脚本可以操作域中的任何对象，因此托管 AWS Microsoft AD 会在您上传后立即运行检查，以帮助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. 将更改应用于单个 DC。 AWS 托管 Microsoft AD 会隔离您的一个数据中心，并将 LDIF 文件中的更新应用于隔离的 DC。然后，它会选择您的一个 DC 作为主架构，将该 DC 从目录复制中删除，然后使用应用您的 LDIF 文件。`Ldifde.exe`
4. 所有 DC 都会进行复制。 AWS 托管 Microsoft AD 将隔离的 DC 重新添加到复制中以完成更新。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

步骤 3：验证架构扩展是否成功

步骤 3：验证架构扩展是否成功

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 验证架构更新是否已应用。您必须在已加入 AWS 托管 Microsoft AD 的域的计算机上运行这些工具。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。还可以对 Amazon

EC2 Windows 实例运行这些工具（请参阅 How to launch a new EC2 instance with seamless domain join）。

使用 Active Directory 架构管理单元进行验证

1. 按照TechNet网站上的说明安装 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。

要进行验证，请使用 PowerShell

1. 打开一 PowerShell 扇窗户。
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

为新属性添加值-可选

为新属性添加值-可选

当您创建了新属性并希望在 AWS 托管 Microsoft AD 目录中为该属性添加新值时，请使用此可选步骤。

向属性中添加值

1. 打开Windows PowerShell命令行实用程序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

维护你的 Microsoft AWS 托管 AD 目录

本节介绍如何维护 AWS 托管 Microsoft AD 环境的常见管理任务。

主题

- 添加备用 UPN 后缀
- 删除你的 Microsoft AWS 托管广告
- 重命名目录的站点名称
- 为目录拍摄快照或还原目录
- 升级你的 AWS 托管微软 AD
- 查看目录信息

添加备用 UPN 后缀

通过向 AWS Managed Microsoft AD 目录添加备用用户主体名称（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验。为此，您必须使用管理员账户或为 AWS 用户主体名称后缀委托管理员组成员的账户登录。有关此组的更多信息，请参阅用你的 AWS 托管 Microsoft AD 活动目录创建了什么。

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 AWS Managed Microsoft AD 目录的 Amazon EC2 实例。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。

删除你的 Microsoft AWS 托管广告

删除 AWS 托管 Microsoft AD 后，所有目录数据和快照都将被删除且无法恢复。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。

要删除目录

1. 在 AWS Directory Service 控制台导航窗格中，选择目录。确保您Active Directory位于您的部署 AWS 区域 位置。有关更多信息，请参阅选择区域。
2. 确保未为要删除的目录启用任何 AWS 应用程序。启用的 AWS 应用程序将阻止你删除 AWS 托管的 Microsoft AD 或 Simple AD。

   a. 在目录页面上，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 “AWS 应用程序和服务” 部分，您可以看到您的目录启用了哪些 AWS 应用程序。

      - 禁用 AWS Management Console 访问权限。有关更多信息，请参阅 禁用 AWS Management Console 访问。
      - 要禁用 Amazon WorkSpaces，您必须从 WorkSpaces 控制台的目录中取消注册该服务。有关更多信息，请参阅《Amazon WorkSpaces 管理指南》中的从目录取消注册。
      - 要禁用亚马逊 WorkDocs，您必须在亚马逊 WorkDocs控制台中删除亚马逊 WorkDocs 网站。有关更多信息，请参阅《Amazon WorkDocs 管理指南》中的删除网站。
      - 要禁用亚马逊 WorkMail，您必须在亚马逊 WorkMail 控制台中删除亚马逊 WorkMail 组织。有关更多信息，请参阅《Amazon WorkMail 管理员指南》中的移除组织。
      - 要禁用适用于 Windows File Server 的 Amazon FSx，必须从域中删除 Amazon FSx 文件系统。有关更多信息，请参阅《亚马逊 FSx for Windows 文件服务器用户指南》中的在 Windows 文件服务器的 FSx 中使用。Active Directory

- 要禁用 Amazon Relational Database Service，必须从域中移除 Amazon RDS 实例。有关更多信息，请参阅《Amazon RDS 用户指南》中的在域中管理数据库实例。
- 要禁用 AWS Client VPN 服务，必须从 Client VPN 端点中删除目录服务。有关更多信息，请参阅《AWS Client VPN 管理员指南》中的Active Directory身份验证。
- 要禁用 Amazon Connect，必须删除 Amazon Connect 实例。有关更多信息，请参阅《Amazon Connect Administration Guide》中的 Deleting an Amazon Connect instance。
- 要禁用亚马逊 QuickSight，您必须取消订阅亚马逊 QuickSight。有关更多信息，请参阅 Amazon QuickSight 用户指南中的关闭 Amazon QuickSight 账户。

> **Note**
>
> 如果您正在使用 AWS IAM Identity Center 并且之前已将其连接到计划删除的 AWS 托管 Microsoft AD 目录，则必须先更改身份源，然后才能将其删除。有关更多信息，请参阅《IAM Identity Center User Guide》中的 Change your identity source。

3. 在导航窗格中，选择目录。
4. 仅选择要删除的目录，然后单击删除。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 AWS Managed 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 AWS Managed Microsoft AD 能够更快地在本地目录中查找现有 AD 用户并对其进行身份验证。最终改善了用户登录您已加入 AWS Managed Microsoft AD 目录的 AWS 资源（如 Amazon EC2 和 Amazon RDS for SQL Server实例）时的体验。

为此，您必须使用 Admin (管理员) 账户或为 AWS 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，请参阅用你的 AWS 托管 Microsoft AD 活动目录创建了什么。

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。

要重命名 AWS Managed 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. 找到将加入您的 AWS Managed Microsoft AD 目录的 Amazon EC2 实例。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。

为目录拍摄快照或还原目录

AWS Directory Service 提供自动每日快照，并能够为 AWS 托管的 Microsoft AD Active Directory 手动拍摄数据快照。这些快照可用于对您的活动目录执行 point-in-time 还原。每个 AWS 托管 Microsoft AD 活动目录仅限于五张手动快照。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。无法拍摄 AD Connector 目录的快照。

> **Note**
>
> 快照是 AWS 托管 Microsoft AD 的一项全球功能。如果您使用的是 多区域复制，则必须在 主区域 中执行以下过程。更改将自动应用于所有复制的区域。有关更多信息，请参阅 全局与区域特色。

主题

- 为目录创建快照
- 从快照还原目录
- 删除快照

为目录创建快照

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 AWS Directory Service 控制台导航窗格中，选择目录。
2. 在目录页面上，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，选择操作，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）。就绪后，选择创建快照。

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。目录快照在创建它们的目录中是唯一的。快照只能恢复到创建它们的目录。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**
>
> 我们建议您在恢复快照之前联系 AWS Support 中心；我们可以帮助您避免进行快照还原。任何快照还原都会导致数据丢失，因为它们是一些时间点。务必要明确的是，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 AWS Directory Service 控制台导航窗格中，选择目录。
2. 在目录页面上，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，在列表中选择一个快照，选择操作，然后选择还原快照。
5. 查看还原目录快照对话框中的信息，然后选择还原。

对于 AWS 托管的 Microsoft AD 目录，恢复该目录可能需要两到三个小时。目录成功还原之后，状态值会更改为 `Active`。会覆盖快照日期之后对目录进行的任何更改。

删除快照

删除快照

1. 在 AWS Directory Service 控制台导航窗格中，选择目录。
2. 在目录页面上，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，选择操作，然后选择删除快照。
5. 确认您要删除快照，然后选择删除。

升级你的 AWS 托管微软 AD

您可以通过联系将标准版 AWS 托管 Microsoft AD 升级Active Directory到企业版 AWS Support。有关更多信息，请参阅《AWS Support 用户指南》中的创建支持案例和案例管理。

> **Note**
>
> 多区域复制仅在以下区域的 Microsoft AD Enterprise AWS 托管版中可用：
>
> - 美国东部（俄亥俄）
> - 美国东部（弗吉尼亚州北部）
> - 美国西部（北加利福尼亚）
> - 美国西部（俄勒冈州）
> - 非洲（开普敦）
> - 亚太地区（香港）
> - 亚太地区（孟买）
> - 亚太地区（海得拉巴）
> - 亚太地区（大阪）
> - 亚太地区（首尔）
> - 亚太地区（新加坡）
> - 亚太地区（悉尼）
> - 亚太地区（雅加达）
> - 亚太地区（墨尔本）
> - 亚太地区（东京）

- 加拿大（中部）
- 加拿大西部（卡尔加里）
- 中国（北京）
- 中国（宁夏）
- 欧洲地区（法兰克福）
- 欧洲（苏黎世）
- 欧洲地区（爱尔兰）
- 欧洲地区（伦敦）
- 欧洲地区（巴黎）
- Europe (Stockholm)
- 欧洲地区（米兰）
- 欧洲（西班牙）
- 以色列（特拉维夫）
- 中东（巴林）
- 中东（阿联酋）
- 南美洲（圣保罗）
- AWS GovCloud （美国西部）
- AWS GovCloud （美国东部）

升级 AWS 托管 Microsoft AD 时需要注意一些限制。它们是：

- 升级将产生额外费用。有关更多信息，请参阅 AWS Directory Service 定价。
- 一旦你的 Active Directory 升级后，它就无法恢复到之前的版本。
- 升级Active Directory后，以前的快照不能用于恢复。
- 升级将在与之商定的预定日期和时间进行 AWS Support。升级发生在太平洋标准时间周一至周五上午 9 点至下午 5 点之间。
- 升级过程需要四到五个小时。
- 在升级过程中，您的 AWS 托管 Microsoft AD 的域控制器将逐一升级。这可能会对您的性能产生负面影响，并可能在维护时段内导致停机。
- 如果您的应用程序使用的是域控制器的主机名或 IP 地址，而不是 Active Directory 的域名，则需要更新这些应用程序。

- 如果您使用的是 LDAPS（基于 SSL 的轻型目录访问协议），则域控制器将需要新的证书。

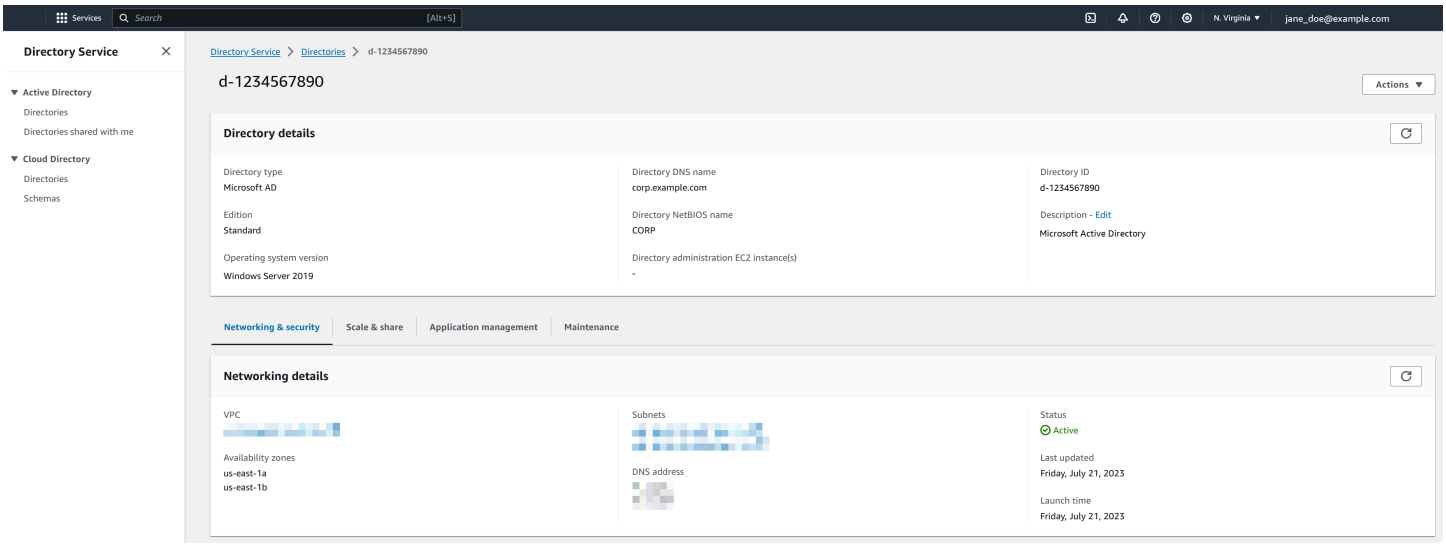
查看目录信息

您可以查看有关目录的详细信息。

查看详细目录信息

1. 在AWS Directory Service 控制台导航窗格中 Active Directory，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面中。

有关 Status 字段的更多信息，请参阅了解目录状态。



授予用户和组对 AWS 资源的访问权限

AWS Directory Service 允许您的目录用户和群组访问 AWS 服务和资源，例如访问 Amazon EC2 控制台。与授予 IAM 用户管理目录的权限（如中所述）类似基于身份的策略（IAM policy），为了使目录中的用户能够访问其他 AWS 资源，例如 Amazon EC2，您必须为这些用户和组分配 IAM 角色和策略。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访问权限的信息 AWS Management Console，请参阅允许使用 AD 凭证访问 AWS Management Console。

主题

- 创建新角色
- 编辑现有角色的信任关系

- 为用户或组分配现有角色
- 查看已分配了角色的用户和组
- 从角色中删除用户或组
- 将 AWS 托管策略与 AWS Directory Service 结合使用

创建新角色

如果您需要创建用于的新 IAM 角色 AWS Directory Service，则必须使用 IAM 控制台创建该角色。创建角色后，您必须与该角色建立信任关系，然后才能在 AWS 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。

> **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）。
>
> - 我是：PassRole
> - 我是：GetRole
> - 我是：CreateRole
> - 我是：PutRolePolicy

要在 IAM 控制台中创建新角色

1. 在 IAM 控制台的导航窗格中，选择角色。有关更多信息，请参阅《IAM 用户指南》中的创建 IAM 角色（AWS Management Console）。
2. 选择 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. 选中要应用于目录用户的策略（例如 AmazonEC2 FullAccess）旁边的复选框，然后选择 “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)。

创建角色以启用 AWS 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对 Amazon EC2 控制台的访问权限。

1. 使用上述过程用 IAM 控制台创建一个角色。当系统提示您输入政策时，请选择 AmazonEC2 FullAccess。
2. 使用 编辑现有角色的信任关系 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。要使角色在下一步中启用访问权限后立即可见， AWS Management Console 必须执行此步骤。
3. 按 允许使用 AD 凭证访问 AWS Management Console 中的步骤操作，配置 AWS Management Console的常规访问权限。
4. 按照 为用户或组分配现有角色 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 角色分配给您的 AWS Directory Service 用户和群组。但是，要做到这一点，角色必须与之建立信任关系 AWS Directory Service。使用 AWS Directory Service 中的过程创建角色时创建新角色，会自动设置此信任关系。您只需为不是由 AWS Directory Service创建的 IAM 角色建立此信任关系。

为现有角色建立信任关系 AWS Directory Service

1. 通过 https://console.aws.amazon.com/iam/ 打开 IAM 控制台。
2. 在 IAM 控制台的导航窗格中的访问权限管理下，选择角色。

   该控制台会显示您账户的角色。
3. 选择您要修改的角色的名称，然后在角色页面中选择信任关系选项卡。
4. 选择编辑信任策略。
5. 在编辑信任策略下，粘贴以下内容，然后选择更新策略。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
```

```
        "Service": "ds.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

您还可以使用 AWS CLI更新此策略文档。有关更多信息，请参阅《AWS CLI Command Reference》中的 update-trust。

为用户或组分配现有角色

您可以将现有 IAM 角色分配给 AWS Directory Service 用户或群组。为此，请确保您已完成以下操作。

先决条件

- 创建 AWS 托管微软 AD。
- 创建用户或创建群组。
- 创建一个与之有信任关系的角色 AWS Directory Service。您可以编辑现有角色的信任关系。

> **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。

向现有 IAM 角色分配用户或组

1. 在 AWS Directory Service 控制台导航窗格的 Active Directory 下，选择目录。
2. 在目录页面上，选择您的目录 ID。
3. 在报告详细信息页面上，执行以下操作之一：
   - 如果多区域复制下未显示任何区域，选择应用程序管理选项卡。
   - 如果多区域复制下显示多个区域，选择要执行分配的区域，然后选择应用程序管理选项卡。有关更多信息，请参阅 主区域与其他区域。
4. 向下滚动到该AWS Management Console部分，选择 “操作” 和 “启用”。

5. 在 “委派控制台访问权限” 部分下，为要向其分配用户的现有 IAM 角色选择 IAM 角色名称。
6. 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)。
7. 在为用户和组分配角色页面的选择 Active Directory 林下，选择 AWS Managed Microsoft AD 林（此林）或本地林（受信任林），也就是需要访问 AWS Management Console的账户所在的林。有关如何设置受信任林的更多信息，请参阅教程：在 AWS Microsoft AD 与自托管式 Active Directory 域之间创建信任关系。
8. 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。
9. 选择添加以完成向角色分配用户和组的工作。

查看已分配了角色的用户和组

要查看已分配给角色的用户和组，请执行以下步骤。

先决条件

- 将您的用户或群组分配给现有角色。

查看已分配给角色的用户和组

1. 在 AWS Directory Service 控制台导航窗格的 Active Directory 下，选择目录。
2. 在目录页面上，选择您的目录 ID。
3. 在报告详细信息页面上，执行以下操作之一：
   - 如果多区域复制下显示多个区域，选择要查看分配的区域，然后选择应用程序管理选项卡。有关更多信息，请参阅 主区域与其他区域。
   - 如果多区域复制下未显示任何区域，选择应用程序管理选项卡。
4. 在委托控制台访问权限部分下，选择要查看的 IAM 角色。
5. 在所选角色 页面的管理此角色的用户和组下，您可以查看已分配该角色的用户和组。

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 AWS Directory Service 控制台导航窗格中，选择目录。
2. 在目录页面上，选择您的目录 ID。
3. 在报告详细信息页面上，执行以下操作之一：
   - 如果多区域复制下显示多个区域，选择要删除分配的区域，然后选择应用程序管理选项卡。有关更多信息，请参阅 主区域与其他区域。
   - 如果多区域复制下未显示任何区域，选择应用程序管理选项卡。
4. 在 AWS Management Console 部分下，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。

将 AWS 托管策略与 AWS Directory Service 结合使用

AWS Directory Service 提供以下 AWS 托管策略，用于向用户和组提供对 AWS 服务和资源的访问权限，如对 Amazon EC2 控制台的访问权限。您必须登录到 AWS Management Console，然后才能查看这些策略。

- 只读访问权限
- 高级用户访问
- AWS Directory Service 完全访问权限
- AWS Directory Service 只读访问权限
- Amazon Cloud Directory 完全访问权限
- Amazon Cloud Directory 只读访问权限
- Amazon EC2 完全访问权限
- Amazon EC2 只读访问权限
- Amazon VPC 完全访问权限
- Amazon VPC 只读访问权限
- Amazon RDS 完全访问权限
- Amazon RDS 只读访问权限
- Amazon DynamoDB 完全访问权限
- Amazon DynamoDB 只读访问权限

- Amazon S3 完全访问权限
- Amazon S3 只读访问权限
- AWS CloudTrail 完全访问权限
- AWS CloudTrail 只读访问权限
- Amazon CloudWatch 完全访问权限
- Amazon CloudWatch 只读访问权限
- Amazon CloudWatch Logs 完全访问权限
- Amazon CloudWatch Logs 只读访问权限

有关如何创建自己的策略的更多信息，请参阅《IAM 用户指南》中的管理 AWS 资源的策略示例。

允许访问 AWS 应用程序和服务

用户可以授权 AWS 托管 Microsoft AD 授予 AWS 应用程序和服务（例如亚马逊 WorkSpaces）访问您的权限Active Directory。可以启用或禁用以下 AWS 应用程序和服务，以便与 AWS 托管 Microsoft AD 配合使用。

AWS 应用程序/服务	更多信息……
Amazon Chime	有关更多信息，请参阅 Amazon Chime Administration Guide。
Amazon Connect	有关更多信息，请参阅 Amazon Connect Administration Guide。
Amazon FSx for Windows File Server	有关更多信息，请参阅将 Amazon FSx 与 Microsoft Active Directory 的 AWS 目录服务配合使用。
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 WorkDocs	有关更多信息，请参阅《Amazon WorkDocs 管理指南》。

AWS 应用程序/服务	更多信息……
Amazon WorkMail	有关更多信息，请参阅《Amazon WorkMail 管理员指南》。
Amazon WorkSpaces	你可以直接从中创建 Simple AD、 AWS 托管 Microsoft AD 或 AD Connecto WorkSpaces r。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》。
AWS Client VPN	有关更多信息，请参阅《AWS Client VPN 用户指南》。
AWS IAM Identity Center	有关更多信息，请参阅《AWS IAM Identity Center 用户指南》。
AWS License Manager	有关更多信息，请参阅 License Manager 用户指南。
AWS Management Console	有关更多信息，请参阅 允许使用 AD 凭证访问 AWS Management Console。
AWS Private Certificate Authority	有关更多信息，请参阅的AWS Private CA 连接器Active Directory。
AWS Transfer Family	有关更多信息，请参阅《AWS Transfer Family 用户指南》。

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权限。要在 AWS Directory Service 控制台中查找上述 AWS 应用程序和服务链接，请执行以下步骤。

显示适用于目录的应用程序和服务

1. 在 AWS Directory Service 控制台导航窗格中，选择目录。
2. 在目录页面上，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 AWS 应用程序和服务部分下的列表。

有关如何使用对 AWS 应用程序和服务进行授权或取消授权的更多信息 AWS Directory Service，请参阅使用对 AWS 应用程序和服务的授权 AWS Directory Service。

主题

- 创建访问 URL
- 单点登录

创建访问 URL

访问 URL 供 AWS 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**
>
> 使用多区域目录时，只能从主区域配置访问 URL。

创建访问 URL

1. 在 AWS Directory Service 控制台导航窗格中，选择目录。
2. 在目录页面上，选择您的目录 ID。
3. 在报告详细信息页面上，执行以下操作之一：
   - 如果多区域复制下显示多个区域，选择主区域，然后选择应用程序管理选项卡。有关更多信息，请参阅 主区域与其他区域。
   - 如果多区域复制下未显示任何区域，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)。如果返回 Entity Already Exists 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 以 *<alias>*.awsapps.com 的格式显示。默认情况下，此 URL 会将您引导至 Amazon WorkDocs 的登录页面。

单点登录

AWS Directory Service 允许您的用户通过加入目录 WorkDocs 的计算机访问 Amazon，而无需单独输入凭证。

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 AWS 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. 您可以委托权限以允许 AD Connector 服务帐户添加或删除自身的服务主体名称属性，您可以使用有权修改 AD Connector 服务帐户权限的帐户在加入域的计算机上运行以下 PowerShell 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"
```

启用或禁用 Amazon 单点登录 WorkDocs

1. 在 AWS Directory Service 控制台导航窗格中，选择目录。
2. 在目录页面上，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 “应用程序访问网址” 部分，选择 “启用” 以启用 Amazon WorkDocs 的单点登录。

   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。
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 的单点登录 WorkDocs，请选择 “禁用”，然后在 “禁用此目录的单点登录” 对话框中，再次选择 “禁用”。

主题

- IE 和 Chrome 的单点登录
- Firefox 的单点登录

IE 和 Chrome 的单点登录

要使 Microsoft 的 Internet Explorer（IE）和 Google 的 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：

- 将访问 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。
- 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 上单点登录的手动更新
- OS X 上单点登录的手动更新
- 单点登录的组策略设置

Windows 上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. 通过运行以下命令将您的访问网址添加到AuthServerAllowlist策略中：

```
defaults write com.google.Chrome AuthServerAllowlist "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。

单点登录的组策略设置

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**
>
> 如果您使用 Chrome 政策管理网域内计算机上的 Chrome 网络浏览器，则必须将访问网址添加到AuthServerAllowlist政策中。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. 在新建 GPO 对话框中，为组策略对象输入一个描述性名称（如 `IAM Identity Center Policy`），将源 Starter GPO 保留为（无）。单击 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：

      操作

      ```
      Update
      ```

      Hive

      ```
      HKEY_CURRENT_USER
      ```

      路径

      ```
      Software\Microsoft\Windows\CurrentVersion\Internet Settings
      \ZoneMap\Domains\awsapps.com\<alias>
      ```

      <alias> 的值派生自访问 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：

操作

```
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 Identity Center 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 的 Firefox 浏览器可以支持单点登录，请将访问 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

- 单点登录的手动更新
- 单点登录的自动更新

单点登录的手动更新

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，可以使用脚本在网络上的所有计算机上将访问 URL 添加到 Firefox `network.negotiate-auth.trusted-uris` 用户首选项。有关更多信息，请转到 https://support.mozilla.org/en-US/questions/939037。

允许使用 AD 凭证访问 AWS Management Console

AWS Directory Service 允许向目录的成员授予 AWS Management Console访问权限。默认情况下，目录成员无权访问任何 AWS 资源。可将 IAM 角色分配给目录成员，以便向其授予各种 AWS 服务和资源的访问权限。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。有关如何创建访问 URL 的更多信息，请参阅创建访问 URL。

有关如何创建 IAM 角色以及将其分配给目录成员的更多信息，请参阅 授予用户和组对 AWS 资源的访问权限。

主题

- 启用 AWS Management Console 访问
- 禁用 AWS Management Console 访问
- 设置登录会话长度

相关的 AWS 安全博客文章

- How to Access the AWS Management Console Using AWS Managed Microsoft AD and Your On-Premises Credentials

> **Note**
>
> 对 AWS Management Console 的访问权限是 AWS Managed Microsoft AD 的一项区域性功能。如果您使用的是 多区域复制，则必须分别在每个区域中应用以下过程。有关更多信息，请参阅 全局与区域特色。

启用 AWS 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 AWS Directory Service 控制台导航窗格中，选择目录。
2. 在目录页面上，选择您的目录 ID。
3. 在报告详细信息页面上，执行以下操作之一：
   - 如果多区域复制下显示多个区域，选择要为其启用 AWS Management Console 访问的区域，然后选择应用程序管理选项卡。有关更多信息，请参阅 主区域与其他区域。
   - 如果多区域复制下未显示任何区域，选择应用程序管理选项卡。
4. 在 AWS Management Console 部分下，选择启用。控制台访问现在已为目录启用。

   在用户使用访问网址登录控制台之前，您必须先将用户添加到角色中。有关为用户分配 IAM 角色的一般信息，请参阅 为用户或组分配现有角色。分配 IAM 角色之后，用户就可以使用访问 URL 访问控制台了。例如，如果目录的访问 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 AWS 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 AWS Directory Service 控制台导航窗格中，选择目录。
2. 在目录页面上，选择您的目录 ID。
3. 在报告详细信息页面上，执行以下操作之一：

- 如果多区域复制下显示多个区域，选择要为其禁用 AWS Management Console 访问的区域，然后选择应用程序管理选项卡。有关更多信息，请参阅 主区域与其他区域。
- 如果多区域复制下未显示任何区域，选择应用程序管理选项卡。

4. 在 AWS Management Console 部分下，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，包括目录中已删除的针对用户或组的分配，分别显示为已删除用户或已删除组。

   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 AWS Directory Service 控制台导航窗格中，选择目录。
2. 在目录页面上，选择您的目录 ID。
3. 在报告详细信息页面上，执行以下操作之一：

   - 如果多区域复制下显示多个区域，选择要为其设置登录会话时长的区域，然后选择应用程序管理选项卡。有关更多信息，请参阅 主区域与其他区域。
   - 如果多区域复制下未显示任何区域，选择应用程序管理选项卡。

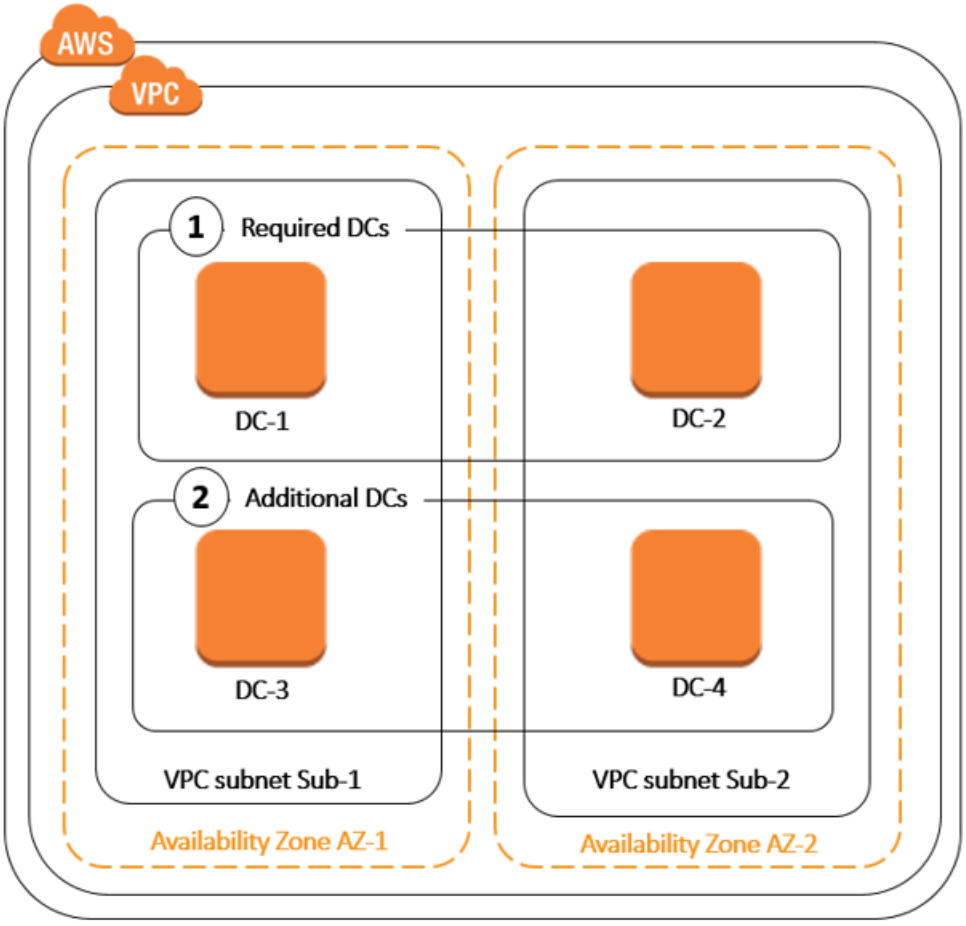
4. 在 AWS 应用程序和服务 部分下，选择 AWS 管理控制台。
5. 在管理对 AWS 资源的访问对话框中，选择继续。
6. 在 Assign users and groups to IAM roles 页面中的 Set login session length 下方，编辑编号的值，然后选择 Save。

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 AWS 托管 Microsoft AD 来支持部署在大型亚马逊 EC2 和 Amazon RDS for SQL Server 实例上的多个.NET 应用程序。

首次创建目录时，Microsoft AD AWS 托管会在多个可用区部署两个域控制器，这是实现高可用性目的所必需的。稍后，您只需指定所需的域控制器总数，即可通过控制 AWS Directory Service 台轻松部署其他域控制器。 AWS 托管 Microsoft AD 会将额外的域控制器分发到运行您的目录的可用区和亚马逊 VPC 子网。

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。 AWS Directory Service 控制台将这些默认域控制器称为 “必需”。 AWS 在目录创建过程中，托管 Microsoft AD 会故意将这些域控制器中的每一个放置在不同的可用区中。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。与以前一样，Microsoft AD AWS 托管再次自动将新的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 AWS Cloud 中迁移和运行任务关键型 Active Directory 集成工作负载，而不必部署和维护您自己的 Active Directory 基础设施。您还可以使用 UpdateNumberOfDomainControllersAPI 为 AWS 托管 Microsoft AD 部署或移除其他域控制器。

> **Note**
>
> 其他域控制器是 AWS 托管 Microsoft AD 的一项区域功能。如果您使用的是 多区域复制，则必须分别在每个区域中应用以下过程。有关更多信息，请参阅 全局与区域特色。

添加或移除额外的域控制器

在添加或移除额外的域控制器之前，请查看以下有关域控制器要求的更多信息：

- 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。
- 已删除的域控制器将从额外域控制器列表中删除。主域控制器和辅助域控制器是必需的，无法删除。
- 如果您已将 AWS 托管 Microsoft AD 配置为启用 LDAPS，那么您添加的任何其他域控制器也将自动启用 LDAPS。有关更多信息，请参阅 启用安全 LDAP 或 LDAPS。

使用以下过程可在您的 AWS Managed Microsoft AD 目录中部署或删除额外的域控制器。

添加或删除额外的域控制器

1. 在 AWS Directory Service 控制台导航窗格中，选择目录。
2. 在目录页面上，选择您的目录 ID。
3. 在报告详细信息页面上，执行以下操作之一：
   - 如果多区域复制下显示多个区域，选择要添加或移除域控制器的区域，然后选择扩展和共享选项卡。有关更多信息，请参阅 主区域与其他区域。
   - 如果多区域复制下未显示任何区域，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. AWS 托管 Microsoft AD 完成部署过程后，所有域控制器都将显示活动状态，并且会显示分配的可用区和亚马逊 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。

相关 AWS 安全博客文章

- 如何通过添加域控制器来提高 AWS 托管 Microsoft AD 的冗余和性能 AWS Directory Service

将用户从 Active Directory 迁移到 AWS Managed Microsoft AD

你可以使用 Active Directory 迁移工具包 (ADMT) 和密码导出服务 (PES)，将用户从你自己管理的 Active Directory 迁移到你的托管 AWS Microsoft AD 目录。这使您能够更轻松地为用户迁移 Active Directory 对象和加密密码。

有关详细说明，请参阅 AWS 安全博客中的 How to migrate your on-premises domain to AWS Managed Microsoft AD using ADMT。

AWS 托管微软 AD 配额

以下是 AWS 托管 Microsoft AD 的默认配额。除非另有说明，否则每个限额均与区域一一对应。

AWS 托管微软 AD 配额

资源	默认限额
AWS 微软 AD 托管目录	20
手动快照*	每个 Microsoft AWS 托管 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
每个企业版 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
单个 AWS 托管 Microsoft AD（企业版）目录中的最大 AWS 区域总数****	5

* 手动快照限额无法更改。

** 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。

*** 共享域默认限额是指可以共享单个目录的账户数量。

**** 这包括 1 个主要区域和最多 4 个其他区域。有关更多信息，请参阅 主区域与其他区域。

> **Note**
>
> 您不能将公有 IP 地址附加到您的 AWS 弹性网络接口 (ENI)。

有关应用程序设计和负载分配的信息，请参阅为您的应用程序编程。

有关存储和对象限额，请参阅 AWS Directory Service 定价页面上的对照表。

AWS 托管 Microsoft AD 的应用程序兼容性

AWS 微软 Active Directory（AWS 托管 Microsoft AD）的目录 AWS 服务与多种服务和第三方应用程序兼容。

以下是兼容的 AWS 应用程序和服务的列表：

- Amazon Chime – 有关详细说明，请参阅连接到 Active Directory。
- Amazon Connect – 有关更多信息，请参阅 Amazon Connect 如何工作。
- Amazon EC2 – 有关更多信息，请参阅 将 Amazon EC2 实例加入您的 AWS 托管微软 AD Active Directory。
- Amazon QuickSight -有关更多信息，请参阅在亚马逊 QuickSight 企业版中管理用户账户。
- 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 Oracle – 有关更多信息，请参阅为 Amazon RDS for Oracle 配置 Kerberos 身份验证。
- Amazon RDS for PostgreSQL – 有关更多信息，请参阅在 Amazon RDS for PostgreSQL 中使用 Kerberos 身份验证。
- Amazon RDS for SQL Server – 有关更多信息，请参阅将 Windows 身份验证与 Amazon RDS Microsoft SQL Server 数据库实例结合使用。
- Amazon WorkDocs -有关详细说明，请参阅使用AWS 托管 Microsoft AD 连接到您的本地目录。
- 亚马逊 WorkMail -有关详细说明，请参阅将亚马逊 WorkMail与现有目录集成（标准设置）。
- AWS Client VPN -有关详细说明，请参阅客户端身份验证和授权。

- AWS IAM Identity Center -有关详细说明，请参阅将 IAM 身份中心连接到本地 Active Directory。
- AWS License Manager -有关更多信息，请参阅中的基于用户的订阅。 AWS License Manager
- AWS Management Console — 有关更多信息，请参阅允许使用 AD 凭证访问 AWS Management Console。
- FSx for Windows File Server – 有关更多信息，请参阅 What is FSx for Windows File Server?。
- WorkSpaces -有关详细说明，请参阅 WorkSpace 使用 AWS 托管 Microsoft AD 启动。

由于大量使用Active Directory的定制和商业 off-the-shelf 应用程序，他们 AWS 不会也无法对第三方应用程序与Microsoft Active Directory（Microsoft AD AWS 托管）的 AWS 目录服务兼容性进行正式或广泛的验证。尽管我们与客户 AWS 合作，努力克服他们可能遇到的任何潜在应用程序安装难题，但我们无法保证任何应用程序现在或将来都与 AWS 托管 Microsoft AD 兼容。

以下第三方应用程序与 AWS 托管 Microsoft AD 兼容：

- 基于 Active Directory 的激活 (ADBA)
- Active Directory Certificate Services (AD CS): Enterprise Certificate Authority
- Active Directory Federation Services (AD FS)
- Active Directory Users and Computers (ADUC)
- 应用程序服务器 (.NET)
- Microsoft Entra（以前称为 Azure Active Directory (AzureAD)）
- Microsoft Entra Connect（以前称为Azure Active Directory Connect）
- 分布式文件系统复制 (DFSR)
- 分布式文件系统命名空间 (DFSN)
- Microsoft Remote Desktop Services Licensing Server
- Microsoft SharePoint Server
- Microsoft SQL Server（包括 SQL Server 始终开启可用性组）
- Microsoft System Center Configuration Manager(SCCM)-部署 SCCM 的用户必须是 AWS 委派系统管理管理员组的成员。
- Microsoft Windows and Windows Server OS
- 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 AWS 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，您通常可以通过向执行安装的人员委派特定、较低权限和 AWS 支持的权限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 AWS 允许您委派的权限的更多信息，请参阅用你的 AWS 托管 Microsoft AD 活动目录创建了什么。
- 访问特权Active Directory容器 — 在你的目录中，Microsoft AD AWS 托管提供了一个组织单位 (OU)，你可以对其进行完全的管理控制。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 AWS 管理托管 Microsoft AD。
- 安装工作流程中的架构更改- 某些Active Directory应用程序需要更改默认 Active Directory 架构，它们可能会尝试将这些更改作为应用程序安装工作流程的一部分进行安装。由于架构扩展的特权性质，仅通过 AWS Directory Service 控制台、 AWS CLI 或 SDK 导入轻量级目录交换格式 (LDIF) 文件即可实现这一点。此类应用程序通常附带一个 LDIF 文件，您可以通过 AWS Directory Service 架构更新过程将其应用于该目录。有关 LDIF 导入过程工作原理的更多信息，请参阅教程：扩展你的 AWS 托管 Microsoft AD 架构。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

以下列出了我们尚未找到适用于 AWS 托管 Microsoft AD 的配置的常见商业 off-the-shelf 应用程序。AWS 出于礼貌的考虑，不时更新此列表，以帮助您避免徒劳的努力。 AWS 提供此信息时不对当前或将来的兼容性提出任何保证或索赔。

- Active Directory Certificate Services (AD CS): Certificate Enrollment Web Service
- Active Directory Certificate Services (AD CS): Certificate Enrollment Policy Web Service
- Microsoft Exchange Server
- Microsoft Skype for Business Server

AWS 微软 AD 托管测试实验室教程

本节提供了一系列指导性教程，可帮助您建立测试实验室环境，您可以在 AWS 其中试用 AWS 托管 Microsoft AD。

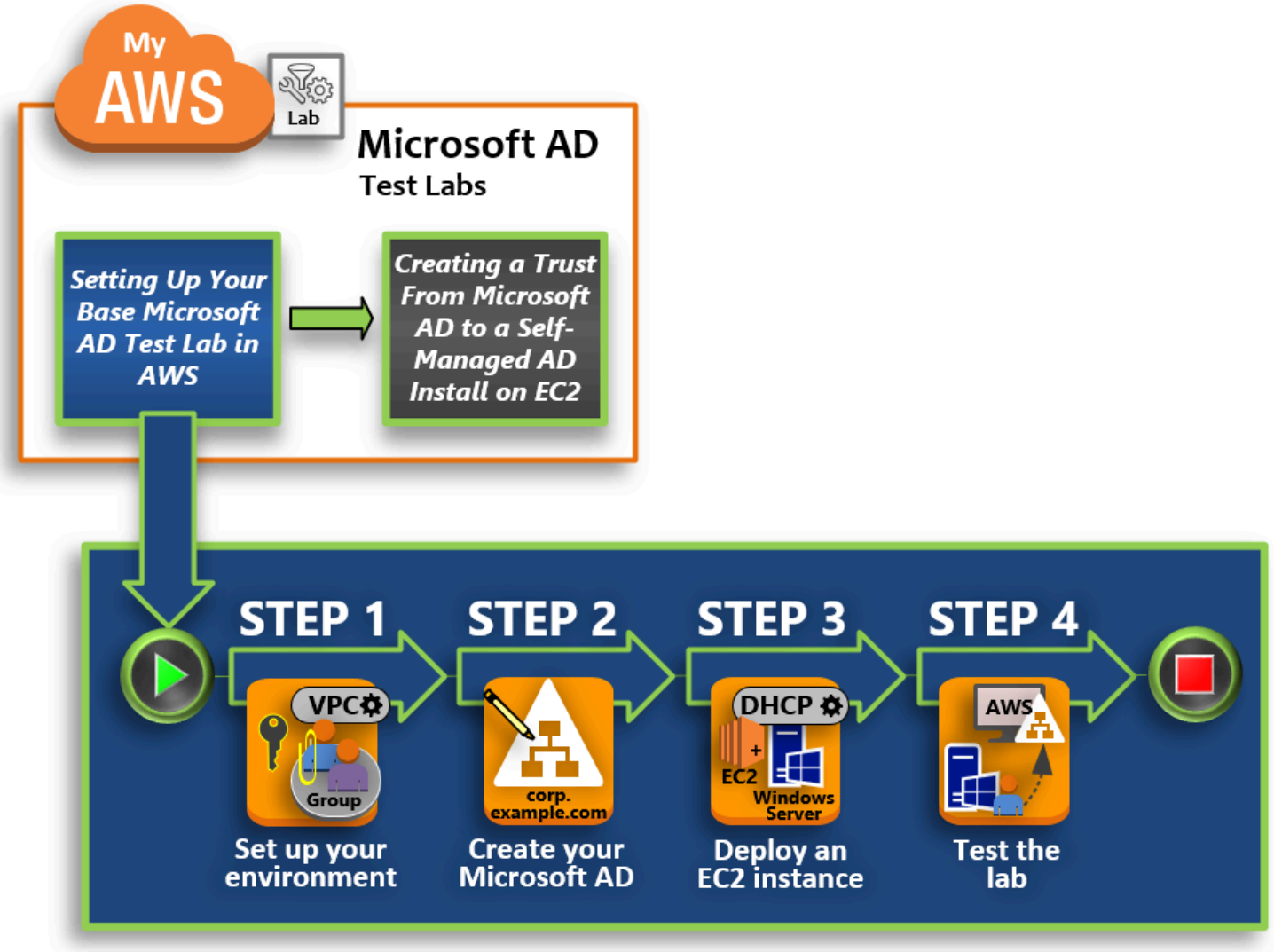
主题

- 教程：在中设置基础 AWS 托管 Microsoft AD 测试实验室 AWS
- 教程：创建从 AWS 托管 Microsoft AD 到亚马逊 EC2 上自行管理的 Active Directory 安装的信任

教程：在中设置基础 AWS 托管 Microsoft AD 测试实验室 AWS

本教程将教你如何设置 AWS 环境，为使用运行 Windows Server 2019 的新 Amazon EC2 实例安装全新 Microsoft AD AWS 托管做好准备。然后，它会教你使用典型的 Active Directory 管理工具从 EC2 Windows 实例 AWS 管理你的 Microsoft AD 托管环境。当你完成本教程时，你已经设置好了网络先决条件并配置了新的 AWS 托管 Microsoft AD 林。

如下图所示，您根据本教程创建的实验室是动手学习 AWS 托管 Microsoft AD 的基础组件。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 AWS Managed Microsoft AD 并需要测试实验室以进行评估的用户。完成本教程需要大约 1 个小时。



步骤 1：为 AWS 托管 Microsoft AD Active Directory 设置 AWS 环境

完成必备任务后，您可以在 EC2 实例中创建和配置 Amazon VPC。

第 2 步：创建你的 AWS 托管微软 AD 活动目录

在此步骤中，您首次在中 AWS 设置了 AWS 托管 Microsoft AD。

第 3 步：部署 Amazon EC2 实例来管理您的 AWS 托管微软 AD 活动目录

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。

步骤 4：验证基本测试实验室正常工作

最后，作为管理员，您将验证您可以从 EC2 中的 Windows Server 系统登录并连接到 AWS Managed Microsoft 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。但是，如果您计划使用 AWS CLI 命令或 AWS 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：

- 拥有访问密钥和私有访问密钥的 IAM 用户 — 如果您要使用 AWS CLI 或 AWS Tools for Windows PowerShell 模块，则需要拥有访问密钥的 IAM 用户。如果您没有访问密钥，请参阅创建、修改或删除您自己的访问密钥（AWS Management Console）。
- AWS Command Line Interface（可选）— AWS CLI 在 Windows 上下载并安装。安装完成后，打开命令提示符或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：
  - AWS 访问密钥 ID [无]: `AKIAIOSFODNN7EXAMPLE`
  - AWS 秘密访问密钥 [无]: `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`
  - 默认区域名称 [无]：`us-west-2`
  - 默认输出格式 [无]：`json`
- AWS Tools for Windows PowerShell（可选）– 通过 https://aws.amazon.com/powershell/ 下载并安装最新版本的 AWS Tools for Windows PowerShell ，然后运行下方的命令。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}
```

步骤 1：为 AWS 托管 Microsoft AD Active Directory 设置 AWS 环境

在 AWS 测试实验室中创建 AWS 托管 Microsoft AD 之前，您首先需要设置您的 Amazon EC2 密钥对，以便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，请参阅创建密钥对。

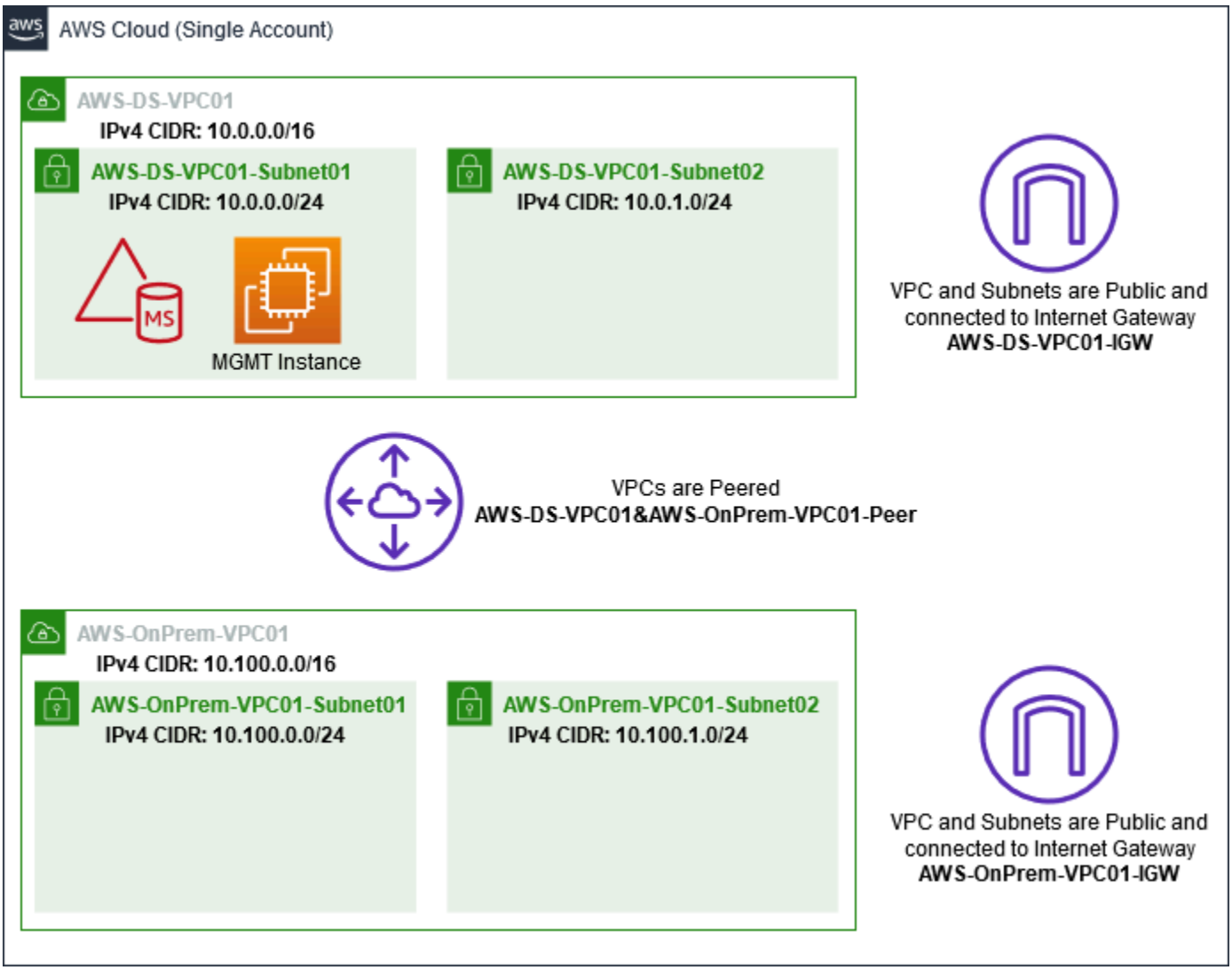
创建密钥对

1. 登录 AWS Management Console 并打开亚马逊 EC2 控制台，网址为 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 **AWS-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、配置两个 Amazon VPC 并对其进行对等

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 AWS CLI 和 PowerShell 示例都使用下面的 VPC 信息，并且是在 us-west-2 中内置的。您可以选择任何受支持的区域来构建环境。有关一般信息，请参阅 Amazon VPC 是什么？。

步骤 1：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个账户中创建两个 VPC。 AWS 托管 Microsoft AD 支持使用具有该共享您的目录功能的单独帐户。第一个 VPC 将用于 AWS 托管 Microsoft AD。第二个 VPC 将用于以后可能在 教程：创建从 AWS 托管 Microsoft AD 到亚马逊 EC2 上自行管理的 Active Directory 安装的信任中使用的资源。

托管活动目录 VPC 信息	本地 VPC 信息
姓名标签： AWS-DS-VPC01	姓名标签： AWS-OnPrem-VPC01

托管活动目录 VPC 信息	本地 VPC 信息
IPv4 CIDR 块：10.0.0.0/16	IPv4 CIDR 块：10.100.0.0/16
IPv6 CIDR block：无 IPv6 CIDR 块	IPv6 CIDR block：无 IPv6 CIDR 块
租赁：默认	租赁：默认

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 AWS 微软 AD 托管先决条件之一。

AWS-DS-VPC01 子网信息：	AWS-OnPrem-VPC01 子网信息
姓名标签： AWS-ds-vpc01-subnet01	姓名标签： AWS OnPrem-vpc01-subnet01
VPC：vpc-xxxxxxxxxxxxxxxxxxxxxxx-ds-VPC01 AWS	VPC：vpc-xxxxxxxxxxxxxxxxxxxxxx--VPC01 AWS OnPrem
可用区：us-west-2a	可用区：us-west-2a
IPv4 CIDR 块：10.0.0.0/24	IPv4 CIDR 块：10.100.0.0/24
姓名标签： AWS-ds-vpc01-subnet02	姓名标签： AWS OnPrem-vpc01-subnet02
VPC：vpc-xxxxxxxxxxxxxxxxxxxxxxx-ds-VPC01 AWS	VPC：vpc-xxxxxxxxxxxxxxxxxxxxxx--VPC01 AWS OnPrem
可用区：us-west-2b	可用区：us-west-2b
IPv4 CIDR 块：10.0.1.0/24	IPv4 CIDR 块：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 网关并将其连接到您的 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。

AWS-DS-VPC01 互联网网关信息	AWS-OnPrem-VPC01 Internet Gateway 信息
姓名标签： AWS-DS-VPC01-IGW	姓名标签：OnPrem- AWS-VPC01-IGW
VPC：vpc-xxxxxxxxxxxxxxxxxxxxxxx-ds-V PC01 AWS	VPC：vpc-xxxxxxxxxxxxxxxxxxxxxx--VPC01 AWS OnPrem

有关详细说明，请参阅 Internet 网关。

步骤 4：在 AWS-DS-VPC01 和-VPC01 之间配置 VPC 对等连接 AWS OnPrem

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。虽然有很多方法可以连接您的 VPC，但本教程将使用 VPC 对等连接。 AWS 托管 Microsoft AD 支持多种连接你的 VPC 的解决方案，其中一些包括 V PC 对等互连、T ransit Gat eway 和 VPN。

对等连接名称标签： AWS-ds-VPC01&-AWS vpc01-Peer OnPrem

VPC（请求者）：vpc-xxxxxxxxxxxxxxxxxxxxx-ds-V AWS PC01

账户：我的账户

区域：此区域

VPC（接受者）：vpc-xxxxxxxxxxxxxxxxxxxx--VPC01 AWS OnPrem

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。

步骤 5：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）。

通过筛选 VPC 名称标签（AWS-DS-VPC01 或-VPC01），您可以轻松找到每个 VPC 的正确路由表。AWS OnPrem

AWS-DS-VPC01 路由 1 信息	AWS-DS-VPC01 路由 2 信息	AWS-OnPrem-VPC01 路线 1 信息	AWS-OnPrem-VPC01 路线 2 信息
目的地：0.0.0.0/0 目标：igw-xx xxxxxxxxxxxxxxxxx xxxx-ds-vpc01-IGW AWS	目的地：10.10 0.0.0/16 目标：pcx-xx xxxxxxxxxxxxxxxxx xxx-ds-vpc AWS 01&-vpc01-Peer AWS OnPrem	目的地：0.0.0.0/0 目标：igw-xx xxxxxxxxxxxxxxxxx xxx-onPrem-vpc01 AWS	目的地：10.0.0.0/16 目标：pcx-xx xxxxxxxxxxxxxxxxx xxx-ds-vpc AWS 01&-vpc01-Peer AWS OnPrem

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 Amazon EC2 实例创建安全组

默认情况下， AWS 托管 Microsoft AD 会创建一个安全组来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。

AWS-DS-VPC01 安全组信息：
安全组名称： AWS DS 测试实验室安全组
描述： AWS DS 测试实验室安全组
VPC：vpc-xxxxxxxxxxxxxxxxxxxxxxx-ds-VPC01 AWS

-DS AWS-VPC01 的安全组入站规则

Type	协议	端口范围	来源	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	全部	10.0.0.0/16	所有本地 VPC 流量

-DS AWS-VPC01 的安全组出站规则

Type	协议	端口范围	目标位置	流量的类型
所有流量	All	全部	0.0.0.0/0	所有流量

AWS-OnPrem-VPC01 安全组信息：
安全组名称： AWS OnPrem 测试实验室安全组。
描述： AWS OnPrem 测试实验室安全组。
VPC：vpc-xxxxxxxxxxxxxxxxxxxxxx--VPC01 AWS OnPrem

AWS-OnPrem-VPC01 的安全组入站规则

Type	协议	端口范围	来源	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

Type	协议	端口范围	来源	流量的类型
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	全部	10.100.0.0/16	所有本地 VPC 流量

AWS OnPrem-VPC01 的安全组出站规则

Type	协议	端口范围	目标位置	流量的类型
所有流量	All	全部	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：创建你的 AWS 托管微软 AD 活动目录

您可以使用三种不同的方法来创建目录。您可以使用该 AWS Management Console 过程（建议在本教程中使用），也可以使用 AWS CLI 或 AWS Tools for Windows PowerShell 过程来创建您的目录。

方法 1：创建你的 Microsoft AD AWS 托管目录 (AWS Management Console)

1. 在 AWS Directory Service 控制台导航窗格中，选择目录，然后选择设置目录。
2. 在选择目录类型页面上，选择 AWS 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 AWS Directory Service for Microsoft Active Directory。
- 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 **AWS 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)。
   - 对于 VPC，选择以 AWS-DS-VPC01 开头并以 (10.0.0.0/16) 结尾的选项。
   - 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：创建你的 Microsoft AWS 托管 AD (Windows PowerShell)（可选）

1. 打开 Windows PowerShell。
2. 键入以下命令。请务必使用前述 AWS Management Console 过程的步骤 4 中提供的值。

```
New-DSMicrosoftAD -Name corp.example.com -ShortName corp -Password P@ssw0rd
 -Description “AWS DS Managed” - VpcSettings_VpcId vpc-xxxxxxxx -
VpcSettings_SubnetId subnet-xxxxxxxx, subnet-xxxxxxxx
```

方法 3：创建你的 Microsoft AWS 托管 AD (AWS CLI)（可选）

1. 打开 AWS CLI.

2. 键入以下命令。请务必使用前述 AWS Management Console 过程的步骤 4 中提供的值。

```
aws ds create-microsoft-ad --name corp.example.com --short-name corp --
password P@ssw0rd --description "AWS DS Managed" --vpc-settings VpcId= vpc-
xxxxxxxx,SubnetIds= subnet-xxxxxxxx, subnet-xxxxxxxx
```

第 3 步：部署 Amazon EC2 实例来管理您的 AWS 托管微软 AD 活动目录

在本实验中，我们使用具有公有 IP 地址的 Amazon EC2 实例，便于从任何地方访问管理实例。在生产环境中，您可以使用私有 VPC 中只能通过 VPN 或 AWS Direct Connect 链接访问的实例。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：为目录创建-D AWS S-VPC01 中设置的 DHCP 选项

在此可选步骤中，您将设置 DHCP 选项范围，以便您的 VPC 中的 EC2 实例自动使用您的 AWS 托管 Microsoft AD 进行 DNS 解析。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 https://console.aws.amazon.com/vpc/ 打开 Amazon VPC 控制台。
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 **AWS 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 AWS 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 AWS Directory Service 目录页面，然后选择适用的目录 ID。在详细信息页面上，识别并使用 DNS 地址中显示的 IP。
     > 或者，要查找这些地址，请转到 AWS Directory Service 目录页面，然后选择适用的目录 ID。然后，选择扩展和共享。在域控制器下，识别并使用 IP 地址中显示的 IP。

   - 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，选择您的 VPC。
7. 在 VPC 列表中，依次选择 AWS DS VPC、操作和编辑 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。

创建角色以将 Windows 实例加入你的 AWS 托管微软 AD 域

使用此过程配置将 Amazon EC2 Windows 实例加入域的角色。有关更多信息，请参阅 将亚马逊 EC2 Windows 实例无缝加入你的 AWS 托管微软 AD Active Directory。

配置 EC2 以将 Windows 实例加入域中

1. 通过 https://console.aws.amazon.com/iam/ 打开 IAM 控制台。
2. 在 IAM 控制台的导航窗格中，选择角色，然后选择创建角色。
3. 在 选择受信任实体的类型 下，选择 AWS 服务。
4. 在紧靠选择将使用此角色的服务下面，选择 EC2，然后选择下一步: 权限。
5. 在附加的权限策略页面上，执行以下操作：

   - 选中 AmazonSSM ManagedInstanceCore 托管政策旁边的复选框。此策略提供了使用 Systems Manager 服务所需的最低权限。
   - 选中 AmazonSSM DirectoryServiceAccess 托管策略旁边的复选框。该策略提供了将实例加入由 AWS Directory Service托管的 Active Directory 的权限。

   有关可以为 Systems Manager 附加的此类托管和其他策略的信息，请参阅《AWS Systems Manager 用户指南》中的为 Systems Manager 创建 IAM 实例配置文件。有关托管策略的更多信息，请参阅《IAM 用户指南》中的 AWS 托管策略。
6. 选择下一步：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，然后选择下一步: 审核。
8. 在角色名称中，输入角色的名称，描述该角色用于将实例加入域（例如 EC2）DomainJoin。

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 角色 页面。

创建 Amazon EC2 实例并自动加入该目录

在此过程中，您将在 EC2 实例中设置 Windows 服务器系统，该系统以后可用于管理 Active Directory 中的用户、群组和策略。

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 Step 2 (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 Next: Configure Instance Details (下一步：配置实例详细信息)。
5. 在 Step 3 页面中，执行以下操作：
   - 对于网络，选择以 AWS-DS-VPC01 结尾的 VPC（例如，vpc-***xxxxxxxxxxxxxxxxx*** | AWS-DS-VPC01）。
   - 对于子网，选择公有子网 1，这应已为您首选的可用区预配置（例如，subnet-***xxxxxxxxxxxxxxxxx*** | AWS-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，请选择您为实例角色指定的名称创建角色以将 Windows 实例加入你的 AWS 托管微软 AD 域，例如 EC2 DomainJoin。
   - 将其他设置保留为默认值。
   - 选择下一步：添加存储。
6. 在 Step 4 页面上，保留默认设置，然后选择 Next: Add Tags。
7. 在 Step 5 页面上，选择 Add Tag。在 Key (键) 下，键入 **corp.example.com-mgmt**，然后选择 Next: Configure Security Group (下一步: 配置安全组)。
8. 在步骤 6 页面上，依次选择选择现有安全组、AWS DS RDP 安全组（您以前在基本教程中已设置）和查看并启动以查看实例。
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：

    - 选择选择现有密钥对。

    - 在选择密钥对下，选择 AWS-DS-KP。
    - 选中 I acknowledge... 复选框。
    - 选择启动新实例。

11. 选择查看实例以返回 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。您可以使用服务器管理器用户界面（本教程推荐使用）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
    - 的活动目录模块 Windows PowerShell
    - Active Directory 站点和服务
    - Active Directory 用户和计算机
    - ADSI 编辑
    - DNS
    - 组策略管理

在您的 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
```

步骤 4：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 服务器配置是否正确，是否可以连接到 corp.example.com 域，以及是否用于管理您的托管 AWS 微软 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，在导航窗格中选择实例。然后选择已创建的实例。选择连接。
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” 下，请注意在本教程的步骤 2 中创建 AWS 托管 Microsoft AD 时自动创建的域控制器的名称。

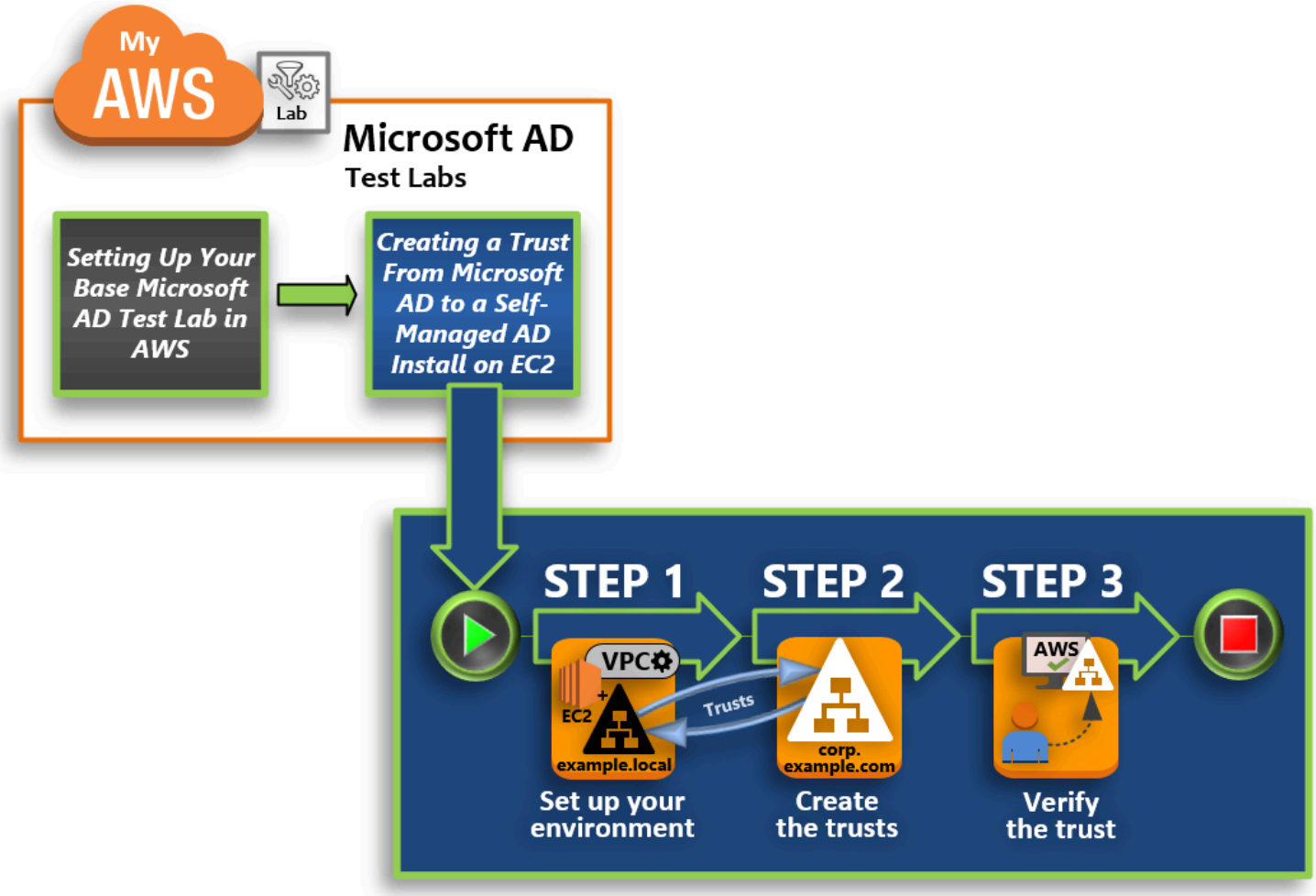
恭喜您！您的 AWS 托管 Microsoft AD 基础测试实验室环境现已配置完毕。您可以随时开始添加该系列中的下一个测试实验室。

下一个教程：教程：创建从 AWS 托管 Microsoft AD 到亚马逊 EC2 上自行管理的 Active Directory 安装的信任

教程：创建从 AWS 托管 Microsoft AD 到亚马逊 EC2 上自行管理的 Active Directory 安装的信任

在本教程中，您将学习如何在基础教程中创建的 Microsoft A AWS ctive Directory 目录林之间创建信任关系。您还将学习在 Amazon EC2 中的 Windows Server 上创建新的本机 Active Directory 林。如下图所示，您根据本教程创建的实验是设置完整的 AWS 托管 Microsoft AD 测试实验室时所需的第二个构建块。您可以使用测试实验室来测试您的纯云或基于混合云的解决方案 AWS 。

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。



步骤 1：为建立信任设置环境

在新的 Active Directory 林与您在基本教程中创建的 AWS Managed Microsoft AD 林之间建立信任前，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。

步骤 2：创建信任

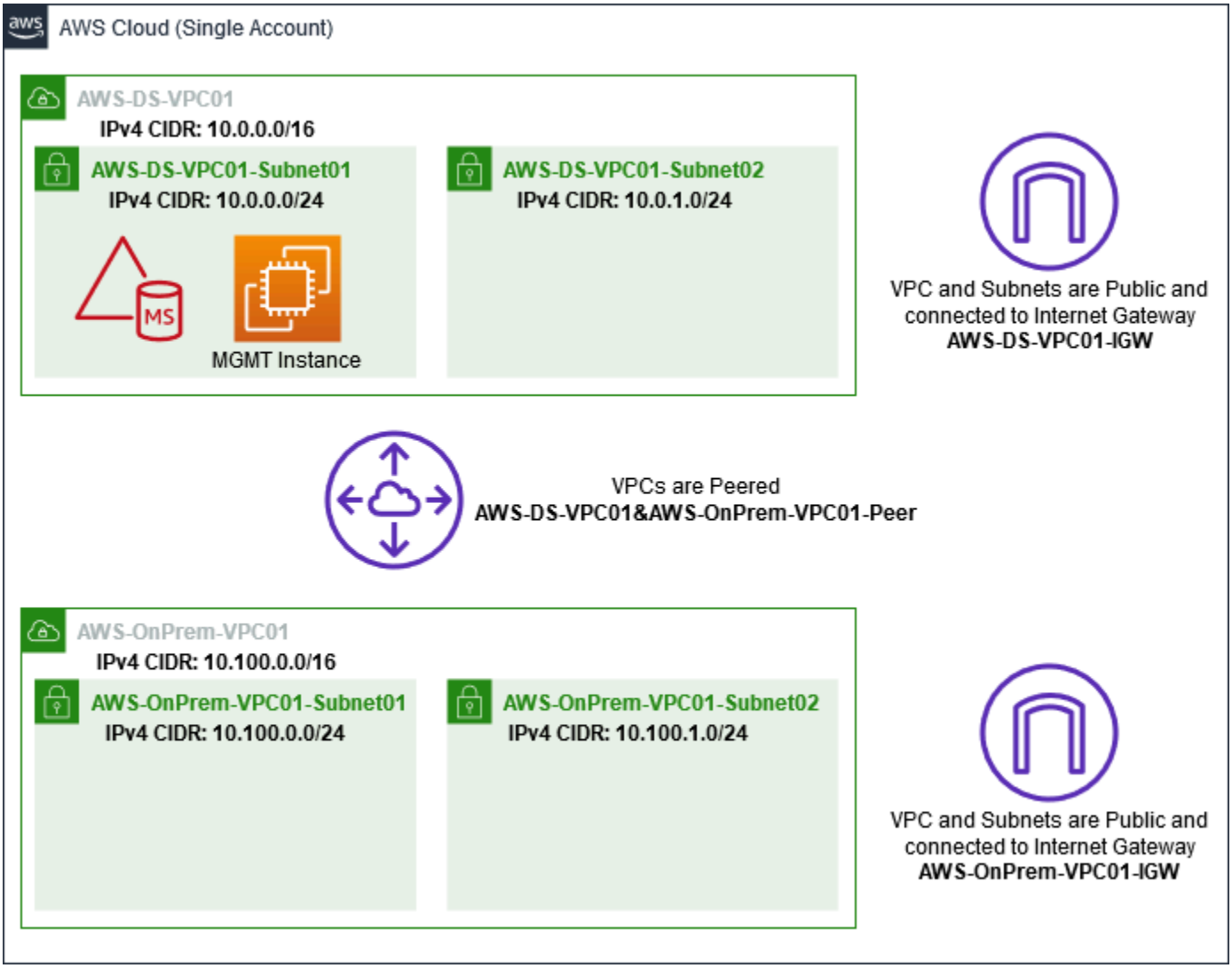
在此步骤中，您将在 Amazon EC2 中托管的新创建的 Active Directory 林与中的托管 Microsoft AD 林之间创建双向林信任关系 AWS。 AWS

步骤 3：验证信任

最后，作为管理员，您可以使用 AWS Directory Service 控制台来验证新的信任是否正常运行。

步骤 1：为建立信任设置环境

在本节中，您将设置您的 Amazon EC2 环境，部署您的新林，并准备好您的 VPC 以备与之建立信任 AWS。



创建 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-***xxxxxxxxxxxxxxxx***。然后选择 Select。

4. 在 Step 2 页面上，选择 t2.large，然后选择 Next: Configure Instance Details。
5. 在 Step 3 页面中，执行以下操作：
   - 对于网络，选择 vpc-***xxxxxxxxxxxxxxxxxxxxxxxx*** OnPrem- AWS-VPC01（你之前在基础教程中进行了设置）。
   - 对于子网，选择子网 -***xxxxxxxxxxxxxxxxxx*** **/**- vpc01-subnet01 |-VPC01 |-VPC01。 AWS OnPrem AWS OnPrem
   - 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。
   - 选择下一步：添加存储。
6. 在 Step 4 页面上，保留默认设置，然后选择 Next: Add Tags。
7. 在 Step 5 页面上，选择 Add Tag。在 Key (键) 下，键入 **`example.local-DC01`**，然后选择 Next: Configure Security Group (下一步: 配置安全组)。
8. 在步骤 6 页面上，依次选择选择现有安全组、AWS On-Prem DS RDP 安全组（您以前在基本教程中已设置）和查看并启动以查看实例。
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：
    - 选择选择现有密钥对。
    - 在选择密钥对下，选择 AWS-DS-KP（您以前在基本教程中已设置）。
    - 选中 I acknowledge... 复选框。
    - 选择启动新实例。
11. 选择查看实例以返回 Amazon EC2 控制台并查看部署的状态。

将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**
>
> 如果您想在中创建可复制本地网络 AWS 的域控制器，则需要先手动将 EC2 实例加入您的本地域。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，选择您刚刚创建的实例，然后选择连接。
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，请返回到 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 AWS 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 “指定域控制器功能” 下，确认已选择 DNS 服务器和全局目录 (GC)。
    - 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. 在其他选项页面上，确保将 EX AM PLE 列为 NetBios 域名。
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 AWS上为连接配置 VPC 的各个步骤。

配置 VPC 出站规则

1. 在AWS Directory Service 控制台中，记下你之前在基础教程中创建的 corp.example.com 的 AWS 托管微软 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. 在导航窗格中，选择 Security Groups（安全组）。
4. 搜索你的 AWS 托管微软 AD 目录 ID。在搜索结果中，选择带 AWS 已为 d-***xxxxxx*** 目录控制器创建安全组说明的项。

   > **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。
   - 选择保存。

要确保已启用 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. 打开AWS Directory Service 控制台。
2. 在导航窗格中，选择目录。
3. 选择你的 Microsoft AWS 托管广告的目录 ID。
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. 在主服务器的 IP 地址下，选择 <单击此处添加... >，键入你的 Microsoft AD AWS 托管目录的第一个 DNS 地址（你在前面的过程中记下了这个地址），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。

步骤 2：创建信任

在本部分中，您将创建两个单独的林信任。一个信任是从你的 EC2 实例上的 Active Directory 域创建的，另一个是从你的 AWS 托管 Microsoft AD 中创建的 AWS。

创建从你的 EC2 域到你的 AWS 托管 Microsoft AD 的信任

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**
>
> AWS 托管 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 Microsoft 网站上的了解信任方向。

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 Configuring selective authentication settings。

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 Microsoft AWS 托管广告的全球特征。如果您使用的是 多区域复制，则必须在 主区域 中执行以下过程。更改将自动应用于所有复制的区域。有关更多信息，请参阅 全局与区域特色。

创建从您的 AWS 托管 Microsoft AD 到您的 EC2 域的信任

1. 打开AWS Directory Service 控制台。
2. 选择 corp.example.com 目录。
3. 在报告详细信息页面上，执行以下操作之一：
   - 如果多区域复制下显示多个区域，选择主区域，然后选择网络与安全选项卡。有关更多信息，请参阅 主区域与其他区域。
   - 如果多区域复制下未显示任何区域，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 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**
     >
     > 请确保您在此处选择的信任类型与前一步骤中配置的信任类型相同（创建从您的 EC2 域到 AWS 托管 Microsoft AD 的信任）。
   - 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 Microsoft 网站上的了解信任方向。
> - 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 Configuring selective authentication settings。

- 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. 选择添加。

步骤 3：验证信任

在本节中，您将测试是否已成功在 AWS 与 Amazon EC2 上的 Active Directory 之间设置信任。

验证信任

1. 打开AWS Directory Service 控制台。
2. 选择 corp.example.com 目录。
3. 在报告详细信息页面上，执行以下操作之一：
   - 如果多区域复制下显示多个区域，选择主区域，然后选择网络与安全选项卡。有关更多信息，请参阅 主区域与其他区域。
   - 如果多区域复制下未显示任何区域，选择网络与安全选项卡。

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。

微软 AD AWS 托管故障排除

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。

你的 AWS 托管 Microsoft AD 存在问题

某些故障排除任务只能通过完成 AWS Support。以下是一些任务：

- 重新启动您 AWS Directory Service提供的域控制器。
- 升级你的 AWS 托管微软 AD.

要创建支持案例，请参阅创建支持案例和案例管理。

Netlogon 和安全信道通信存在问题

作为 CVE-2020-1472 的缓解措施，Microsoft 发布了补丁，该补丁会修改域控制器处理 Netlogon 安全信道通信的方式。自从引入这些安全 Netlogon 变更以来，你的托管 Microsoft AD 可能不接受某些 Netlogon 连接（服务器、工作站和信任验证）。 AWS

要验证您的问题是否与 Netlogon 或安全渠道通信有关，请在您的 Amazon CloudWatch 日志中搜索事件 ID 5827（设备身份验证相关问题）或 5828（查看 AD 信任验证相关问题）。有关 CloudWatch AWS 托管 Microsoft AD 的信息，请参阅启用日志转发。

有关针对 CVE-2020-1472 的缓解措施的更多信息，请参阅 Microsoft 网站上的如何管理与 CVE-2020-1472 相关联的 Netlogon 安全频道连接中的更改。

重置用户密码时出现问题

尝试重置用户密码时，您会收到一条类似于以下内容的错误消息：

```
Response Status: 400 Bad Request
```

当你的 AWS 托管 Microsoft AD 组织单位 (OU) 中存在具有相同用户登录名的重复对象时，你可能会遇到此问题。用户登录名必须是唯一的。有关更多信息，请参阅Microsoft文档中的目录数据问题疑难解答。

密码找回

如果用户忘记密码或者在登录你的 Simple AD 或 Microsoft AD AWS 托管目录时遇到问题，你可以使用 AWS Management Console、Windows PowerShell或重置他们的密码。 AWS CLI

有关更多信息，请参阅 重置用户密码。

其他 资源

以下资源可以帮助您在使用时进行故障排除 AWS。

- AWS 知识中心-查找常见问题解答和其他资源链接，以帮助您解决问题。
- AWS S@@ upport Center —获取技术支持。
- AWS Premium Support Center —获取高级技术支持。

以下资源可以帮助您解决常见Active Directory问题。

- Active Directory 文档
- AD DS故障排除

主题

- 使用 Microsoft 事件查看器监控 DNS 服务器
- Linux 域加入错误
- Active Directory 低可用存储空间
- 架构扩展错误
- 信任创建状态原因

使用 Microsoft 事件查看器监控 DNS 服务器

您可以审核您的 AWS Managed 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为 AWS 域名系统管理员组成员的账户登录。有关此组的更多信息，请参阅用你的 AWS 托管 Microsoft AD 活动目录创建了什么。

访问 AWS Managed Microsoft AD DNS 的事件查看器

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. 找到将加入您的 AWS Managed Microsoft AD 目录的 Amazon EC2 实例。选择该实例，然后选择 Connect (连接)。
4. 连接到 Amazon EC2 实例后，打开开始菜单并选择 Windows 管理工具文件夹。在管理工具文件夹中，选择事件查看器。
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. 选择另一台计算机，键入 AWS Managed Microsoft AD DNS 服务器名称或 IP 地址之一，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 AWS Managed Microsoft AD 目录时可能遇到的一些错误消息。

Linux 实例无法加入域或进行身份验证

Ubuntu 14.04、16.04 和 18.04 实例必须在 DNS 中可以反向解析，然后才能使用微软 Active Directory。否则，您可能会遇到以下两种场景之一：

场景 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：

! Couldn't authenticate to active directory: SASL(-1): generic failure: GSSAPI Error: An invalid name was supplied (Success) adcli: couldn't connect to EXAMPLE.COM domain: Couldn't authenticate to active directory: SASL(-1): generic failure: GSSAPI Error: An invalid name was supplied (Success) ! Insufficient permissions to join the domain realm: Couldn't join realm: Insufficient permissions to join the domain

场景 2：Ubuntu 实例已加入领域

对于已经加入 Microsoft Active Directory 域的 Ubuntu 实例，尝试使用域凭据通过 SSH 连接到该实例可能会失败，并出现以下错误：

$ ssh admin@EXAMPLE.COM@198.51.100

没有此类身份：/Users/username/.ssh/id_ed25519：没有找到此文件或目录

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：

如果使用公钥登录到实例并勾选 `/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)：用户 admin@EXAMPLE.COM 已收到：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，用户的 `kinit` 仍然有效。参阅此示例：

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：FILE:/tmp/krb5cc_1000 默认委托人：admin@EXAMPLE.COM

解决办法

这两种场景当前推荐的解决方法是禁用 [libdefaults] 部分 `/etc/krb5.conf` 中的反向 DNS，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

如果您在AWS托管的 Microsoft AD 和您的本地 Active Directory 之间建立了单向传出信任，则在尝试使用带有 Winbind 的可信 Active Directory 凭据对已加入域的 Linux 实例进行身份验证时，可能会遇到身份验证问题。

错误

Jul 31 00:00:00 EC2AMAZ-LSMWqT sshd[23832]: Failed password for user@corp.example.com from xxx.xxx.xxx.xxx port 18309 ssh2

Jul 31 00:05:00 EC2AMAZ-LSMWqT sshd[23832]: pam_winbind(sshd:auth): getting password (0x00000390)

Jul 31 00:05:00 EC2AMAZ-LSMWqT sshd[23832]: pam_winbind(sshd:auth): pam_get_item returned a password

7 月 31 日 00:05:00 ec2amaz-lsmwqt sshd [23832]：pam_winbind (sshd: auth)：请求 wbcLogonUser 失败：WBC_ERR_AUTH_ERROR，PAM 错误：PAM_SYSTEM_ERR (4)，NTSTATUS：**NT_STATUS_OBJECT_NAME_NOT_FOUND**，错误消息是：找不到对象名称。

Jul 31 00:05:00 EC2AMAZ-LSMWqT sshd[23832]: pam_winbind(sshd:auth): internal module error (retval = PAM_SYSTEM_ERR(4), user = 'CORP\user')

解决办法

要解决此问题，您需要使用以下步骤注释掉或从 PAM 模块配置文件 (`/etc/security/pam_winbind.conf`) 中删除指令。

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 = yes。

   ```
   [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
```

Active Directory 低可用存储空间

当您的 AWS 托管 Microsoft AD 因活动目录的可用存储空间不足而受损时，需要立即采取措施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 文件夹存储多个基本组策略对象
2. Active Directory 数据库已填充卷

有关 AWS 托管 Microsoft AD 存储的定价信息，请参阅AWS Directory Service 定价。

SYSVOL 文件夹存储多个基本组策略对象

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 AWS 托管 Microsoft AD 域控制器以外的文件服务器上。

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。如果您不想自行管理文件服务器， AWS 可提供托管文件服务器选项 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 分钟后目录处于非活动状态，请联系 Su AWS pport。

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 数据库已填充卷

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，Microsoft AD AWS 托管项目在广告回收箱中保存 180 天，然后才会变成回收对象。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 AWS 托管 Microsoft AD 支持的对象计数的更多详细信息，请参阅AWS Directory Service 定价。

要获取包含已删除对象的目录中的对象总数，您可以从已加入域的 Windows 实例中运行以下 PowerShell 命令。有关如何设置管理实例的步骤，请参阅在 AWS Managed Microsoft AD 中管理用户和组。

```
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. 向 Su AWS pport 提交案例， AWS Directory Service 请求回收可用空间。

2. 如果您的目录类型为标准版，请向 Support 提出申请，要求将您的目录升级到企业版。 AWS 这也会增加您目录的成本。有关定价信息，请参阅 AWS Directory Service 定价。

在 M AWS anaged Microsoft AD 中，“AWS 委派已删除对象生命周期管理员” 组的成员可以修改属性，该msDS-DeletedObjectLifetime属性用于设置已删除对象在变成 “回收对象” 之前在 AD 回收站中保存的时间（以天为单位）。

> **Note**
>
> 这是一个高级主题。如果配置不当，则可能导致数据丢失。我们强烈建议您首先查看 AD 回收站：了解、实施、最佳实践和故障排除，以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 为目录拍摄快照或还原目录。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 AWS Managed Microsoft AD 目录扩展架构时可能遇到的一些错误消息。

引用

错误

> Add error on entry starting on line 1: Referral The server side error is: 0x202b A referral was returned from the server. The extended server error is: 0000202B: RefErr: DSID-0310082F, data 0, 1 access points \tref 1: 'example.com' Number of Objects Modified: 0

问题排查

> 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 of Objects Modified: 0

问题排查

> 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 of Objects Modified: 0

问题排查

> 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，请参阅步骤 1：创建 LDIF 文件。

属性或值存在

错误

Add error on entry starting on line 1: Attribute Or Value Exists The server side error is: 0x2083 The specified value already exists. The extended server error is: 00002083: AtrErr: DSID-03151830, #1: \t0: 00002083: DSID-03151830, problem 1006 (ATT_OR_VALUE_EXISTS), data 0, Att 20019 (mayContain):len 4 Number of Objects Modified: 0

问题排查

架构更改已应用。

无此类属性

错误

Add error on entry starting on line 1: No Such Attribute The server side error is: 0x2085 The attribute value cannot be removed because it is not present on the object. The extended server error is: 00002085: AtrErr: DSID-03152367, #1: \t0: 00002085: DSID-03152367, problem 1001 (NO_ATTRIBUTE_OR_VAL), data 0, Att 20019 (mayContain):len 4 Number of Objects Modified: 0

问题排查

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 starting on line 41: No Such Attribute 0x57 The parameter is incorrect. The extended server error is: 0x208d Directory object not found。The extended server error is: "00000057: LdapErr: DSID-0C090D8A, comment: Error in attribute conversion operation, data 0, v2580" Number of Objects Modified: 0

问题排查

第 41 行中列出的属性不正确。请复查拼写。

无此类对象

错误

Add error on entry starting on line 1: No Such Object The server side error is: 0x208d Directory object not found. The extended server error is: 0000208D:

NameErr: DSID-03100238, problem 2001 (NO_OBJECT), data 0, best match of: 'CN=Schema,CN=Configuration,DC=example,DC=com' Number of Objects Modified: 0

问题排查

可分辨名称 (DN) 引用的对象不存在。

信任创建状态原因

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：

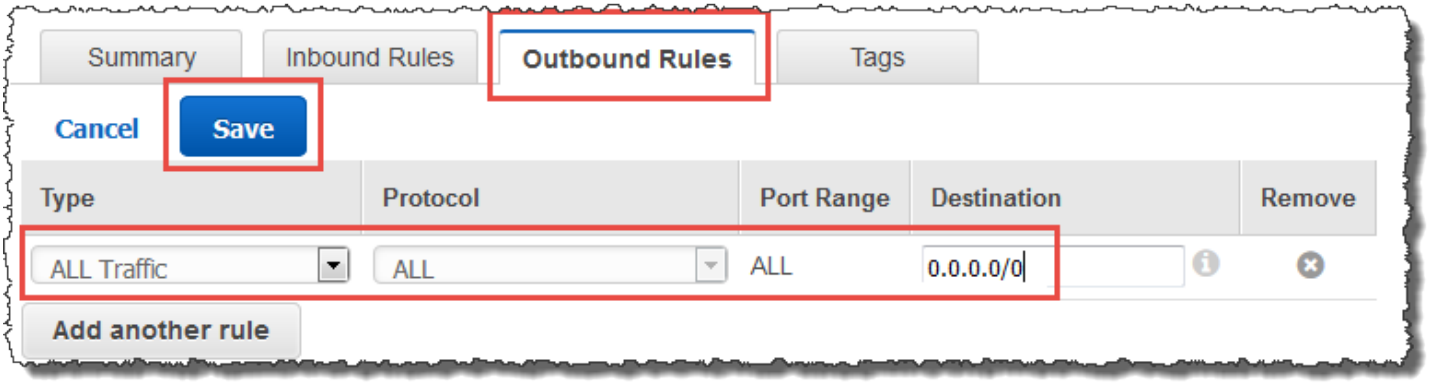
- AWS 托管 Microsoft AD Active Directory 和Active Directory你希望与之建立信任关系的自我管理广告必须具有相同的第一个站点名称。“第一个站点” 名称设置为`Default-First-Site-Name`。如果域名之间存在差异，则会出现拒绝访问错误。
- 请验证使用的信任密码与在远程域上创建相应信任时使用的密码相同。
- 验证域安全设置允许创建信任。
- 验证本地安全策略设置是否正确。具体来说，检查 `Local Security Policy > Local Policies > Security Options > Network access: 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
- 验证上面命名的管道是否作为注册表项的值存在，该注册表项位于NullSessionPipes注册表路径 HKLM\ SYSTEM\\ services\\ Par CurrentControlSet am eters 中。LanmanServer这些值必须插入到分隔的行上。

> **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`。

- 验证默认域控制器策略中的以下服务器消息块 (SMB) 签名设置。这些设置可以在 “计算机配置” > “Windows 设置” > “安全设置” > “本地策略/ 安全选项” 下找到。它们应与以下设置相匹配：
  - Microsoft网络客户端：对通信进行数字签名（总是）：默认：启用
  - Microsoft网络客户端：对通信进行数字签名（如果服务器同意）：默认：启用
  - Microsoft网络服务器：对通信进行数字签名（总是）：已启用
  - Microsoft网络服务器：对通信进行数字签名（如果客户同意）：默认：启用

指定域名不存在或无法访问

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。 AWS 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。您需要更新安全组的出站规则，以允许流量流入本地网络。有关安全要求的更多信息，请参阅 步骤 2：准备 AWS Managed Microsoft AD。



如果其他目录网络的 DNS 服务器使用公用（非 RFC 1918）IP 地址，则需要在目录上添加一条从 Directory Services 控制台到 DNS 服务器的 IP 路由。有关更多信息，请参阅 创建、验证或删除信任关系 和 先决条件 。

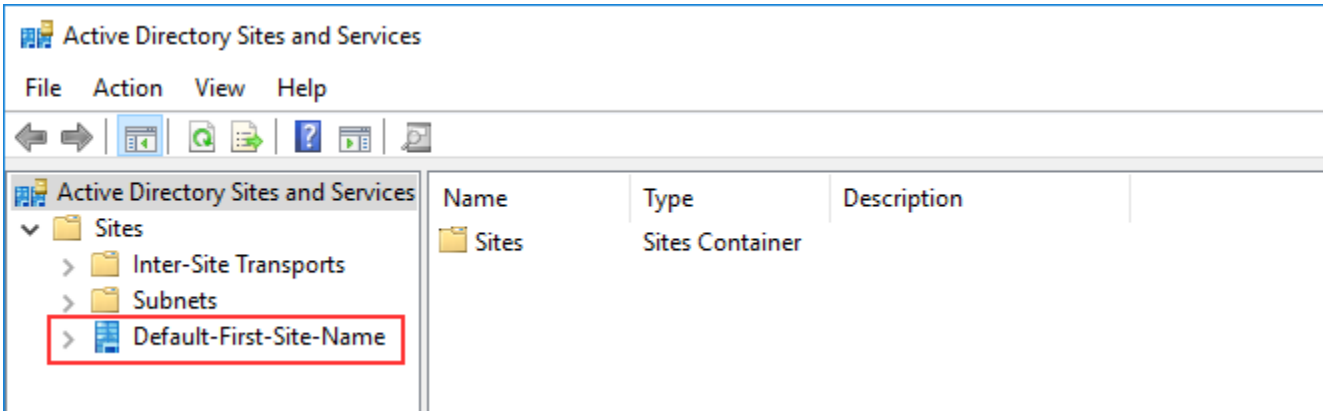
互联网号码分配机构（IANA）已为私有互联网保留了以下 3 块 IP 地址空间：

- 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）

欲了解更多信息，请参阅 https://tools.ietf.org/html/rfc1918。

验证 AWS 托管 Microsoft AD 的默认 AD 站点名称是否与本地基础架构中的默认 AD 站点名称相匹配。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。将站点重命名为与最近的本地站点相匹配，可确保 DC 定位器使用最近站点的域控制器。如果这样做不能解决问题，则可能是因为缓存了以前创建的条件转发服务器的信息，从而阻止了创建新的信任。等待几分钟，然后再次尝试创建信任和条件转发服务器。

有关其工作原理的更多信息，请参阅Microsoft网站上的跨森林信托的域定位器。



无法在此域上执行该操作

要解决此问题，请确保两个域/目录的 NETBIOS 名称不重叠。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。

由于出现“必填且有效的域名”错误，信任创建失败

DNS 名称只能包含字母字符（A-Z）、数字字符（0-9）、减号（-）和句点（.）。只有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。另请考虑以下事项：

- AWS 托管 Microsoft AD 不支持使用单标签域名的信任。有关更多信息，请参阅对单标签域的Microsoft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-Z、a-z、0-9 以及连字符（-）。DNS 名称中也使用句点 [.]，但只能在 DNS 标签之间和 FQDN 结尾处使用。
- 根据 RFC 952（https://tools.ietf.org/html/rfc952），名称（网络、主机、网关或域名）是一个不超过 24 个字符的文本字符串，可使用字母（A-Z）、数字（0-9）、减号（-）和句点（.）创建。请注意，只有当句点用于分隔域名样式名称的组成部分时，才允许使用。

有关更多信息，请参阅Microsoft网站上的遵守主机和域名的名称限制。

用于测试信任的一般工具

以下是可用于排查各种信任相关问题的工具。

AWS Systems Manager 自动化疑难解答工具

S@@ upport Automation Workflows (SAW) 利用 S AWS ystems Manager 自动化为你提供预定义的运行手册。 AWS Directory ServiceTroubleshootDirectoryTrust运行手册工具可帮助您诊断 AWS 托管 Microsoft AD 和本地部署MicrosoftActive Directory之间常见的信任创建问题。AWSSupport

DirectoryServicePortTest 工具

在解决 AWS 托管 Microsoft AD 和本地 Active Directory 之间的信任创建问题时，该DirectoryServicePortTest测试工具可能很有用。有关如何使用工具的示例，请参阅测试 AD Connector。

NETDOM 和 NLTEST 工具

管理员可以同时使用 Netdom 和 Nltest 命令行工具来查找、显示、创建、删除和管理信任。这些工具直接与域控制器上的 LSA 机构通信。有关如何使用这些工具的示例，请参阅网站上的 Netdom 和 NLTEST。Microsoft

数据包捕获工具

您可以使用内置的 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 Capture a Network Trace without installing anything。

AD Connector

AD Connector 是一个目录网关，您可以使用该网关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。小型 AD Connector 专门用于规模较小的组织，每秒处理的操作数量少。大型 AD Connector 专门用于规模较大的组织，每秒处理的操作数量从中等到很多。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 Directory 传递信任。AD 连接器和您的本地 Active Directory 域是一对一的关系。也就是说，对于每个本地域，包括要进行身份验证的 Active Directory 林中的子域，都必须创建一个唯一的 AD Connector。

> **Note**
>
> AD Connector 不能与其他 AWS 账户共享。如果需要这样做，可以考虑使用 AWS 托管 Microsoft AD 来共享您的目录。AD Connector 也不支持多 VPC，这意味着需要将诸如WorkSpaces此类的 AWS 应用程序配置到与 AD 连接器相同的 VPC 中。

设置之后，AD Connector 具备以下优势：

- 您的最终用户和 IT 管理员可以使用他们现有的公司证书登录 AWS 应用程序 WorkSpaces，例如 Amazon 或 Ama WorkDocs zon WorkMail。
- 您可以通过基于 IAM 角色的访问权限来管理诸如 Amazon EC2 实例或 Amazon S3 存储桶之类的 AWS 资源。 AWS Management Console
- 无论用户还是 IT 管理员访问您的本地基础设施还是 AWS 云中的资源，您都可以始终如一地强制执行现有的安全策略（例如密码过期、密码历史记录和帐户锁定）。
- 您可以使用 AD Connector 通过与现有的基于 RADIUS 的 MFA 基础设施集成来启用多因素身份验证，从而在用户访问应用程序时提供额外的安全保护。 AWS

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

- 开始使用 AD Connector
- 如何管理 AD Connector
- AD Connector 最佳实践

- AD Connector 配额
- AD Connector 的应用程序兼容性策略
- AD Connector 故障排除

开始使用 AD Connector

使用 AD Connecto AWS Directory Service r，您可以连接到现有企业Active Directory。连接到现有目录后，所有目录数据仍保留在域控制器上。 AWS Directory Service 不会复制您的任何目录数据。

主题

- AD Connector 先决条件
- 创建 AD Connector
- 使用 AD Connector 创建了什么

AD Connector 先决条件

要使用 AD Connector 连接到您的现有目录，您需要：

Amazon 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 AWS Direct Connect将 VPC 连接到您的现有网络。
- VPC 必须具有默认硬件租户。

AWS Directory Service 使用双 VPC 结构。构成您目录的 EC2 实例在您的 AWS 账户之外运行，并由管理 AWS。其有 `ETH0` 和 `ETH1` 两个网络适配器。`ETH0` 是管理适配器，存在于您的账户之外。`ETH1` 在您的账户内创建。

目录的 `ETH0` 网络的管理 IP 范围以编程方式选择，以确保其不会与部署目录的 VPC 发生冲突。此 IP 范围可以是以下任一对（因为目录在两个子网中运行）：

- 10.0.1.0/24 和 10.0.2.0/24
- 169.254.0.0/16
- 192.168.1.0/24 和 192.168.2.0/24

我们通过检查 ETH1 CIDR 的第一个八位字节来避免冲突。如果以 10 开头，那么我们就选择一个 192.168.0.0/16 VPC，其子网为 192.168.1.0/24 和 192.168.2.0/24。如果第一个八位字节不是 10，则我们选择一个 10.0.0.0/16 VPC，其子网为 10.0.1.0/24 和 10.0.2.0/24。

选择算法不包括您 VPC 上的路由。因此，这种情况可能会导致 IP 路由冲突。

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

有关的更多信息 AWS Direct Connect，请参阅《AWS Direct Connect 用户指南》。

现有 Active Directory

您需要使用Active Directory域连接到现有网络。

> **Note**
>
> AD Connector 不支持单个标签域。

此Active Directory域的功能级别必须等于`Windows Server 2003`或更高。AD Connector 还支持连接到 Amazon EC2 实例上托管的域。

> **Note**
>
> 与 Amazon EC2 域加入功能结合使用时，AD Connector 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-仅在使用无缝域加入时才需要使用和 WorkSpaces
- 创建计算机对象-仅在使用无缝域加入时才需要和 WorkSpaces
- 服务账号密码应符合 AWS 密码要求。 AWS 密码应为：
  - 长度介于 8 到 128 个字符之间（含）。
  - 至少包含以下四个类别中的三个类别中的一个字符：

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

有关更多信息，请参阅 向您的服务账户委派权限。

> **Note**
>
> AD Connector 使用 Kerberos 对 AWS 应用程序进行身份验证和授权。LDAP 仅用于用户和组对象查找（读取操作）。对于 LDAP 事务，所有都不可变，凭证也不以明文形式传递。身份验证由 AWS 内部服务处理，该服务使用 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
- 邮件
- 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，您可能希望在首次设置 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 在连接到您的目录时将从这些服务器获取 `_ldap._tcp.<DnsDomainName>` 和 `_kerberos._tcp.<DnsDomainName>` 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，请访问 Microsoft 上的 SRV 资源记录。 TechNet

子网的端口

为了让 AD Connector 将目录请求重定向到您的现有Active Directory域控制器，您现有网络的防火墙必须向您 Amazon VPC 中两个子网的 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 能够连接到目录之前所需的最少端口。根据您的特定配置，您可能需要打开其他端口。

如果你想使用 AD Connector 和 Amazon WorkSpaces，则需要将域控制器的 disablevLVSupportLDAP 属性设置为 0。这是域控制器的默认设置。如果启用了 disablevLVSupportLDAP 属性，AD Connector 将无法查询目录中的用户。这会阻止 AD Connector 使用 Amazon WorkSpaces。

> **Note**
>
> 如果您现有Active Directory域的 DNS 服务器或域控制器服务器位于 VPC 内，则与这些服务器关联的安全组必须向 VPC 中两个子网的 CIDR 开放上述端口。

有关其他端口要求，请参阅Microsoft文档中的 AD 和 AD DS 端口要求。

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，请参阅确保已启用 Kerberos 预身份验证。有关此设置的一般信息，请转到开启的预身份验证。Microsoft 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

AWS IAM Identity Center 先决条件

如果计划将 IAM Identity Center 与 AD Connector 结合使用，则需要确保满足以下条件：

- 您的 AD Connector 是在您 AWS 组织的管理账户中设置的。
- 您的 IAM Identity Center 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 AWS IAM Identity Center 用户指南中的 IAM 身份中心先决条件。

多重身份验证先决条件

为了使用您的 AD Connector 目录支持多重身份验证，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 AWS 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服务器通过默认 RADIUS 服务器端口 (1812) 的 AWS Directory Service 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。

有关通过 MFA 使用 AD Connector 的更多信息，请参阅 为 AD Connector 启用多重身份验证。

向您的服务账户委派权限

要连接到您的现有目录，必须在现有目录中拥有被委托了某些权限的 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的新组`Connectors`，委派连接到该组所需的必要权限，然后 AWS Directory Service 向该组添加新的服务帐户。

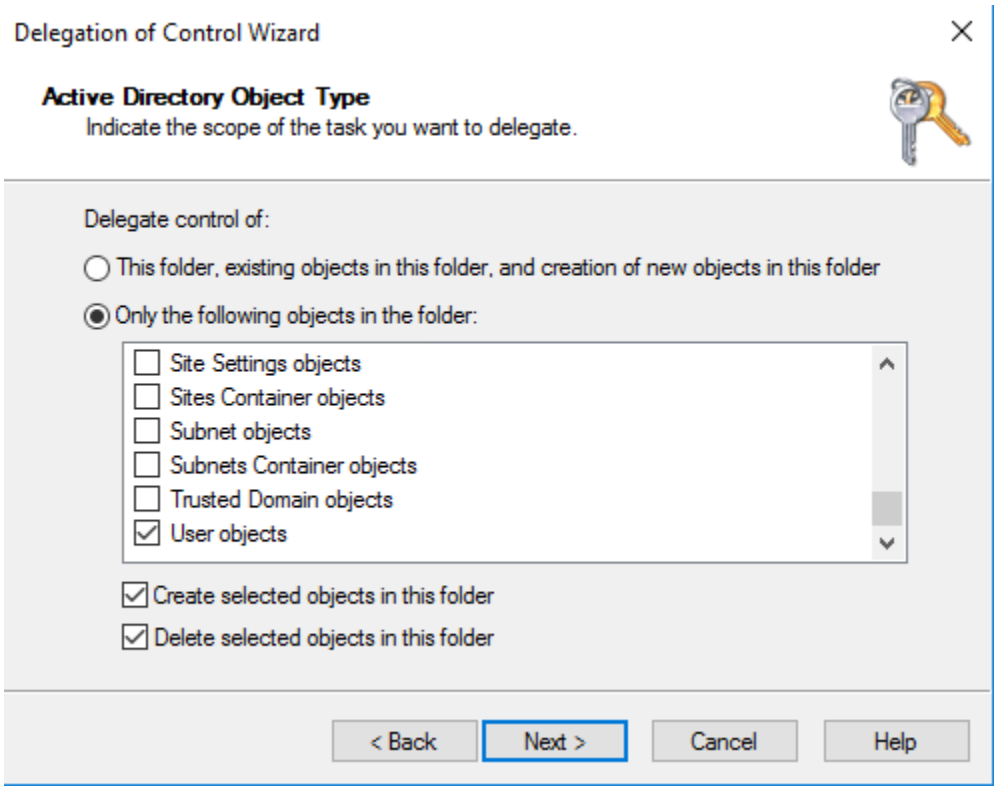
必须在已加入到目录且已安装 Active Directory User and Computers MMC 管理单元的计算机上执行此过程。您还必须以域管理员身份登录。

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。

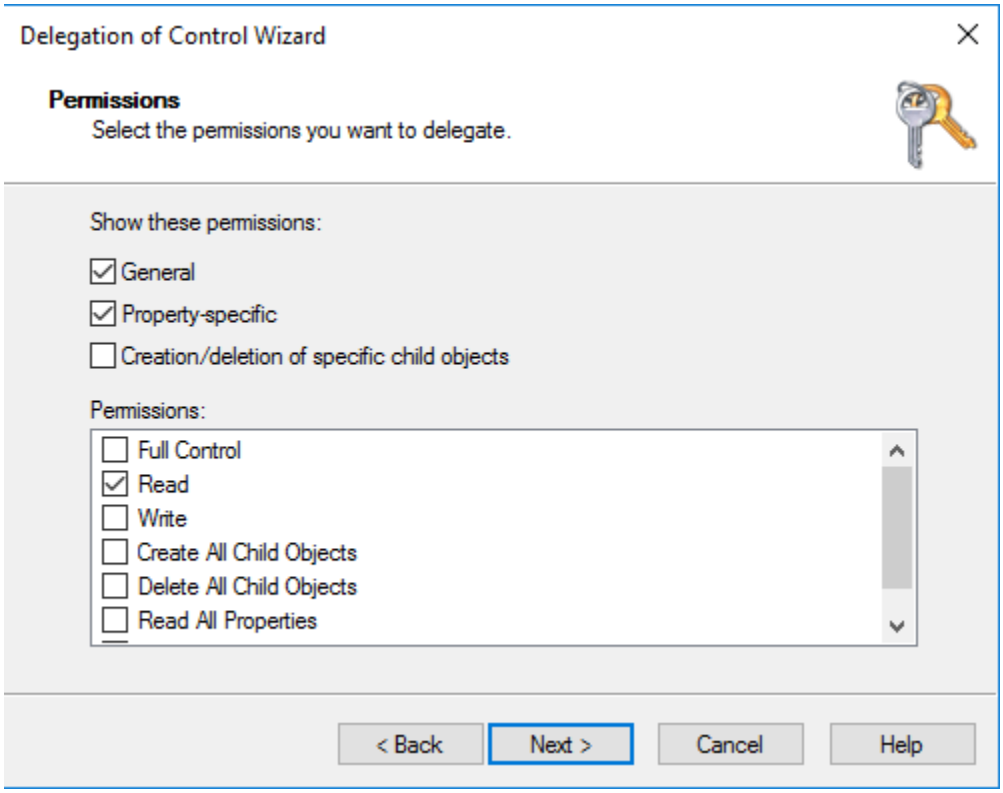
字段	值/选择
组名	`Connectors`
Group scope	Global
Group type	安全性

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 AWS 托管的 Microsoft AD，则您将无法访问域根级别的委托控制。在这种情况下，要委托控制权，请在您的目录 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，则还必须启用写入权限，这样 Active Directory 才能创建计算机对象。



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 服务帐户，由于它现在是该`Connectors`组的成员，因此现在它具有足够的权限 AWS Directory Service 来连接到该目录。

测试 AD Connector

为使 AD Connector 能够连接您的现有目录，现有网络的防火墙必须向 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**
   >
   > 只有将域和林功能级别设置为 Windows Server 2012 R2 及更低版本时，才能使用 DirectoryServicePortTest 测试应用程序。

```
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。

```
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 连接到现有目录，请执行以下步骤。在开始此过程之前，请确保您已满足了AD Connector 先决条件中确定的先决条件。

> **Note**
>
> 您无法使用 Cloud Formation 模板创建 AD Connector。

使用 AD Connector 连接

1. 在 AWS Directory Service 控制台导航窗格中，选择目录，然后选择设置目录。
2. 在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AD Connector。

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。

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步骤 4 中指定的每个子网访问。只要指定的子网和 DNS 服务器 IP 地址之间存在网络连接，这些服务器就可以位于外部。AWS

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 Connector 先决条件。

服务账户密码

现有用户账户的密码。此密码区分大小写，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。

使用 AD Connector 创建了什么

创建 AD 连接器时， AWS Directory Service 会自动创建弹性网络接口 (ENI) 并将其与每个 AD 连接器实例关联。这些 ENI 中的每一个 ENI 对于您的 VPC 和 AWS Directory Service AD Connector 之间的连接都是必不可少的，因此切勿将其删除。您可以 AWS Directory Service 通过描述来标识所有保留供使用的网络接口：“为目录目录 ID AWS 创建的网络接口”。有关更多信息，请参阅《Amazon EC2 用户指南》中的弹性网络接口。

> **Note**
>
> 默认情况下，AD Connector 实例部署在一个区域的两个可用区中，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。

当您登录任何与 AD Connector（AWS IAM Identity Center 包括在内）集成的 AWS 应用程序或服务时，应用程序或服务会将您的身份验证请求转发给 AD Connector，AD Connector 随后会将请求转发到您自行管理的 Active Directory 中的域控制器进行身份验证。如果您成功通过自我管理的 Active Directory 的身份验证，AD Connector 会向应用程序或服务返回身份验证令牌（类似于 Kerberos 令牌）。此时，您现在可以访问该 AWS 应用程序或服务了。

如何管理 AD Connector

本节列出了运行和维护 AD Connector 环境的所有过程。

主题

- 保护您的 AD Connector 目录
- 监控您的 AD Connector 目录

- 将 Amazon EC2 实例加入您的 Active Directory
- 维护您的 AD Connector 目录
- 允许访问 AWS 应用程序和服务
- 为 AD Connector 更新 DNS 地址

保护您的 AD Connector 目录

本节介绍了保护 AD Connector 环境的注意事项。

主题

- 在 AWS Directory Service 中更新 AD Connector 服务账户凭证
- 为 AD Connector 启用多重身份验证
- 使用 AD Connector 启用客户端 LDAPS
- 在 AD Connector 中启用 mTLS 身份验证以便与智能卡一起使用
- 为 AD 设置 AWS Private CA 连接器

在 AWS Directory Service 中更新 AD Connector 服务账户凭证

您在 AWS Directory Service 中提供的 AD Connector 凭证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 AWS Directory Service 中修改这些服务账户凭证。

> **Note**
>
> 如果为目录启用了 AWS IAM Identity Center，则 AWS Directory Service 必须将服务主体名称（SPN）从当前服务账户转移到新的服务账户。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 AWS Directory Service 中更新 AD Connector 服务账户凭证

1. 在 AWS Directory Service 控制台导航窗格的 Active Directory 下，选择目录。
2. 选择目录的目录 ID 链接。
3. 在目录详细信息页面上，向下滚动到服务账户凭证部分。
4. 在 Service account credentials (服务账户凭据) 部分中，选择 Update (更新)。

5. 在更新服务账户凭证对话框中，键入服务账户的用户名和密码。重新输入密码进行确认，然后选择更新。

为 AD Connector 启用多重身份验证

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 AWS Directory Service 结合使用的更多信息，请参阅 AD Connector 先决条件。

> **Note**
>
> 多重身份验证对 Simple AD 不可用。但是，可为 AWS Managed Microsoft AD 目录启用 MFA。有关更多信息，请参阅为 AWS 托管的 Microsoft AD 启用多因素身份验证：

为 AD Connector 启用多重身份验证

1. 在 AWS Directory Service 控制台导航窗格中，选择目录。
2. 选择您 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. 在启用多重身份验证（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 仅适用于对亚马逊企业应用程序和服务（例如 WorkSpaces亚马逊 QuickSight或 Amazon Chime）的访问进行身份验证。AWS Management Console其不为在 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。AWS Directory Service 不支持 RADIUS 质询/响应身份验证。
   > 用户在输入用户名和密码时必须有 MFA 代码。或者，您必须使用执行 MFA 的解决方案， out-of-band 例如对用户进行 SMS 文本验证。在 out-of-band MFA 解决方案中，

必须确保为您的解决方案正确设置 RADIUS 超时值。使用 out-of-band 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，最佳做法是让用户在密码字段和 MFA 字段中均输入密码。

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的 RADIUS 服务器端口（UDP:1812）从 AWS Directory Service 服务器传入入站流量。

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。

RADIUS 请求最大重试次数

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. 请选择启用。

使用 AD Connector 启用客户端 LDAPS

AD Connector 中的客户端 LDAPS 支持对 Microsoft Active Directory（AD）和 AWS 应用程序之间的通信进行加密。此类应用程序的示例包括 WorkSpaces、AWS IAM Identity Center、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
- 启用客户端 LDAPS

- 管理客户端 LDAPS

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 中部署服务器证书
- CA 证书要求
- 联网要求

在 Active Directory 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 AD Connector 目录最多可存储五（5）个 CA 证书。
- 使用 RSSAS-PSS 签名算法的证书不受支持。

联网要求

AWS 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 AWS 安全组和网络防火墙，以允许 AD Connector（出站）和自托管式 Active Directory（入站）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）证书导入 AD Connector，然后在您的目录上启用 LDAPS。启用后，AWS 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 AWS Management Console 方法或 AWS CLI 方法。

主题

- 步骤 1：在 AWS Directory Service 中注册证书
- 步骤 2：检查注册状态
- 步骤 3：启用客户端 LDAPS
- 步骤 4：查看 LDAPS 状态

步骤 1：在 AWS Directory Service 中注册证书

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

方法 1：在 AWS Directory Service 中注册您的证书 (AWS Management Console)

1. 在 AWS 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 AWS Directory Service 中注册您的证书 (AWS 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
```

步骤 2：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 AWS Directory Service 中检查证书注册状态 (AWS Management Console)

1. 转到目录详细信息页面上的客户端 LDAPS 部分。
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 AWS Directory Service 中检查证书注册状态 (AWS 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
```

步骤 3：启用客户端 LDAPS

使用下列方法之一在 AWS Directory Service 中启用客户端 LDAPS。

> **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 AWS Directory Service 中启用客户端 LDAPS (AWS Management Console)

1. 转到目录详细信息页面上的客户端 LDAPS 部分。
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 AWS Directory Service 中启用客户端 LDAPS (AWS CLI)

- 运行以下命令。

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

步骤 4：查看 LDAPS 状态

使用下列方法之一检查 AWS Directory Service 中的 LDAPS 状态。

方法 1：在 AWS Directory Service 中检查 LDAPS 状态 (AWS Management Console)

1. 转到目录详细信息页面上的客户端 LDAPS 部分。
2. 如果状态值显示为 Enabled (启用)，则 LDAPS 已成功配置。

方法 2：在 AWS Directory Service 中检查 LDAPS 状态 (AWS 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 AWS Management Console 方法或 AWS 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 AWS Directory Service 中查看证书详细信息 (AWS Management Console)

1. 在 AWS 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 AWS Directory Service 中查看证书详细信息 (AWS 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 AWS Directory Service 中取消注册证书 (AWS Management Console)

1. 在 AWS 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 AWS Directory Service 中取消注册证书 (AWS 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 AWS Directory Service 中禁用客户端 LDAPS (AWS Management Console)

1. 在 AWS 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 AWS Directory Service 中禁用客户端 LDAPS (AWS CLI)

- 运行以下命令。

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

在 AD Connector 中启用 mTLS 身份验证以便与智能卡一起使用

您可以将基于证书的相互传输层安全 (mTLS) 身份验证与智能卡一起使用， WorkSpaces 通过您自行管理的 Active Directory (AD) 和 AD Connector 对用户进行身份验证，进入亚马逊。启用后，用户将在 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。Windows 或 Linux 虚拟桌面可在此使用智能卡从本机桌面操作系统进行 AD 身份验证。

> **Note**
>
> AD Connector 中的智能卡身份验证仅在以下情况下可用 AWS 区域，并且仅适用于 WorkSpaces。目前不支持其他 AWS 应用程序。
>
> - 美国东部（弗吉尼亚州北部）
> - US West（Oregon）
> - 亚太地区（悉尼）
> - 亚太地区（东京）
> - 欧洲地区（爱尔兰）
> - AWS GovCloud （美国西部）

主题

- 先决条件
- 启用智能卡身份验证
- 管理智能卡身份验证设置

先决条件

要使用智能卡为 Amazon WorkSpaces 客户端启用基于证书的相互传输层安全 (mTLS) 身份验证，您需要将可操作的智能卡基础设施与您的自我管理相集成。Active Directory有关如何使用亚马逊 WorkSpaces 和设置智能卡身份验证的更多信息Active Directory，请参阅《亚马逊 WorkSpaces 管理指南》。

在为启用智能卡身份验证之前 WorkSpaces，请查看以下注意事项：

- CA 证书要求
- 用户证书要求
- 证书吊销检查流程
- 其他考虑因素

CA 证书要求

AD Connector 需要证书颁发机构（CA）证书（代表用户证书的颁发者）用于智能卡身份验证。AD Connector 将 CA 证书与用户通过其智能卡提供的证书进行匹配。请注意以下 CA 证书要求：

- CA 证书的有效期必须大于 90 天才能进行注册。
- 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。
- 必须上传从颁发证书 CA 链接到用户证书的所有根证书和中间 CA 证书，智能卡身份验证才能成功。
- 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 RSASSA-PSS 签名算法。
- 验证证书传播服务是否设置为 “自动” 且正在运行。

用户证书要求

以下是用户证书的一些要求：

- 用户的智能卡证书具有用户的使用者备用名称 (SAN) userPrincipalName (UPN)。
- 用户的智能卡证书使用增强型密钥用法作为智能卡登录 (1.3.6.1.4.1.311.20.2.2) 客户端身份验证 (1.3.6.1.5.5.7.3.2)。
- 用户智能卡证书的在线证书状态协议 (OCSP) 信息应为 “权限信息访问” 中的 “访问方法=在线证书状态协议 (1.3.6.1.5.5.7.48.1)”。

有关 AD Connector 和智能卡身份验证要求的更多信息，请参阅《亚马逊 WorkSpaces 管理指南》中的要求。有关解决亚马逊 WorkSpaces 问题（例如登录 WorkSpaces、重置密码或连接到）的帮助 WorkSpaces，请参阅《亚马逊 WorkSpaces 用户指南》中的 “解决 WorkSpaces 客户问题”。

证书吊销检查流程

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 必须可通过互联网访问。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）根区域数据库中找到的顶级域。

AD Connector 证书吊销检查过程如下：

- AD Connector 必须检查用户证书中的颁发机构信息访问（AIA）扩展以获取 OCSP 响应程序 URL，然后 AD Connector 使用该 URL 检查是否已吊销。
- 如果 AD Connector 无法解析在用户证书 AIA 扩展中找到的 URL，也无法在用户证书中找到 OCSP 响应程序 URL，则 AD Connector 将使用在根 CA 证书注册期间提供的可选 OCSP URL。

  如果用户证书 AIA 扩展中的 URL 已解析但没有响应，则用户身份验证失败。
- 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，则用户身份验证失败。
- OCSP 服务器必须符合 RFC 6960。此外，对于总共小于或等于 255 字节的请求，OCSP 服务器必须支持使用 GET 方法的请求。

> **Note**
>
> AD Connector 需要 OCSP 响应程序 URL 的 HTTP URL。

其他考虑因素

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行协议身份验证（相互 TLS），通过基于硬件或软件的智能卡证书对 Active Directory 的用户进行身份验证。目前仅支持通用访问卡（CAC）和个人身份验证（PIV）卡。其他类型的基于硬件或软件的智能卡可能可以使用，但尚未经过与 WorkSpaces流媒体协议配合使用的测试。
- 智能卡身份验证取代了用户名和密码身份验证 WorkSpaces。

如果您在 AD Connector 目录中配置了其他 AWS 应用程序并启用了智能卡身份验证，则这些应用程序仍会显示用户名和密码输入屏幕。

- 启用智能卡身份验证会将用户会话时长限制为 Kerberos 服务票证的最大生命周期。您可以使用组策略配置此设置，默认情况下将其设置为 10 小时。有关该设置的更多信息，请参阅 Microsoft 文档。
- AD Connector 服务账户支持的 Kerberos 加密类型应与每个域控制器支持的 Kerberos 加密类型相匹配。

启用智能卡身份验证

要在 AD Connecto WorkSpaces r 上启用智能卡身份验证，首先需要将证书颁发机构 (CA) 证书导入 AD Connector。您可以使用 AWS Directory Service 控制台、API 或 CLI 将您的 CA 证书导入 AD Connecto r。按照以下步骤导入您的 CA 证书，然后启用智能卡身份验证。

主题

- 步骤 1：为 AD Connector 服务账户启用 Kerberos 约束委托
- 步骤 2：在 AD Connector 中注册 CA 证书
- 步骤 3：为支持的 AWS 应用程序和服务启用智能卡身份验证

步骤 1：为 AD Connector 服务账户启用 Kerberos 约束委托

要对 AD Connector 使用智能卡身份验证，必须为 AD Connector 服务账户对自行管理 AD 目录中的 LDAP 服务启用 Kerberos 约束委托（KCD）。

Kerberos 约束委托是 Windows Server 中的一项功能。此功能使管理员能够通过限制应用程序服务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。

> **Note**
>
> K@@ erberos 约束委托 (KCD) 要求 AD Connector 服务帐户的用户名部分与同一用户的 SaM AccountName 相匹配。SaM 限制AccountName 为 20 个字符。saM AccountName 是 Microsoft 的 Active Directory 属性，用作先前版本的 Windows 客户端和服务器的登录名。

1. 使用 `SetSpn` 命令为自行管理 AD 中的 AD Connector 服务账户设置服务主体名称（SPN）。这将启用委托配置的服务账户。

SPN 可以是任何服务或名称组合，但不能与现有 SPN 重复。-s 检查是否存在重复项。

```
setspn -s my/spn service_account
```

2. 在 AD 用户和计算机中，打开“上下文”（右键单击）菜单并选择“AD Connector 服务账户”，然后选择属性。
3. 选择委托选项卡。
4. 选择仅信任此用户以委托到指定服务和使用任何身份验证协议选项。
5. 选择添加，然后选择用户或计算机以查找域控制器。
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，然后选择确定。
8. 再次选择确定以保存配置。
9. 对 Active Directory 中的其他域控制器重复此过程。或者，您可以使用自动执行该过程 PowerShell。

步骤 2：在 AD Connector 中注册 CA 证书

使用以下任一方法为您的 AD Connector 目录注册 CA 证书。

方法 1：在 AD Connector（AWS Management Console）中注册您的证书

1. 在 AWS 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. 在智能卡身份验证部分，选择操作，然后选择注册证书。
5. 在注册 CA 证书对话框中，选择选择文件，然后选择证书并选择打开。您可以选择通过提供在线证书状态协议（OCSP）响应程序 URL 来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流程。
6. 选择 Register certificate (注册证书)。当您看到证书状态更改为已注册时，表示注册过程已成功完成。

方法 2：在 AD Connector（AWS CLI）中注册您的证书

- 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 响应程序地址，请使用可选的 `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。您也可以通过运行以下 CLI 命令来验证您的 CA 证书是否注册成功：

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

如果状态值返回 `Registered`，则表示您的证书已成功注册。

步骤 3：为支持的 AWS 应用程序和服务启用智能卡身份验证

使用以下任一方法为您的 AD Connector 目录注册 CA 证书。

方法 1：在 AD Connector（AWS Management Console）中启用智能卡身份验证

1. 导航到目录详细信息页面上的智能卡身份验证部分，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（AWS CLI）中启用智能卡身份验证

- 运行以下命令。

```
aws ds enable-client-authentication --directory-id your_directory_id --type
 SmartCard
```

如果成功，则 AD Connector 会返回带有空 HTTP 正文的 `HTTP 200` 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 AWS Management Console 方法或 AWS CLI 方法。

主题

- 查看证书详细信息

- 取消注册证书
- 禁用智能卡身份验证

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 AWS Directory Service (AWS Management Console) 中查看证书详细信息

1. 在 AWS Directory Service 控制台导航窗格中，选择目录。
2. 选择您 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. 在智能卡身份验证部分的 CA 证书下，选择证书 ID 以显示有关该证书的详细信息。

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

- 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 AWS Directory Service ()AWS Management Console中注销证书

1. 在 AWS Directory Service 控制台导航窗格中，选择目录。
2. 选择您 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. 在智能卡身份验证部分的 CA 证书下，选择要取消注册的证书，选择操作，然后选择取消注册证书。

> **Important**
>
> 确保您要取消注册的证书未处于活动状态或当前正作为智能卡身份验证 CA 证书链的一部分。

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 AWS Directory Service ()AWS CLI中注销证书

- 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

使用以下任何一种方法来禁用智能卡身份验证。

方法 1：在 AWS Directory Service (AWS Management Console) 中禁用智能卡身份验证

1. 在 AWS Directory Service 控制台导航窗格中，选择目录。
2. 选择您 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. 在智能卡身份验证部分，选择禁用。
5. 在禁用智能卡身份验证对话框中，选择禁用。

方法 2：在 AWS Directory Service (AWS CLI) 中禁用智能卡身份验证

- 运行以下命令。

```
aws ds disable-client-authentication --directory-id your_directory_id --type
 SmartCard
```

为 AD 设置 AWS Private CA 连接器

您可以将自己管理的 Active Directory (AD) 与 AWS Private Certificate Authority (CA) 与 AD Connector 集成，从而为您的 AD 域加入的用户、群组和计算机颁发和管理证书。 AWS Private CA Connector for AD 允许您使用完全托管的 AWS Private CA 嵌入式替代方案来代替自我管理的企业 CA，而无需部署、修补或更新本地代理或代理服务器。

您可以通过 Directory Service 控制台、AD AWS Private CA 连接器控制台或通过调用 `CreateTemplate`API 来设置与目录的集 AWS Private CA 成。要通过 Active Directory AWS Private CA 连接器控制台设置私有 CA 集成，请参阅 Act ive DirectoryAWS Private CA 连接器。有关如何从 AWS Directory Service 控制台设置此集成的步骤，请参阅下文。

先决条件

使用 AD Connector 时，您需要向服务账户委托额外权限。在您的服务账户上设置访问控制列表（ACL），以便自己能够执行以下操作。

- 向其自身添加和删除服务主体名称（SPN）。
- 在以下容器中创建和更新证书颁发机构：

```
#containers
CN=Public Key Services,CN=Services,CN=Configuration
CN=AIA,CN=Public Key Services,CN=Services,CN=Configuration
CN=Certification Authorities,CN=Public Key Services,CN=Services,CN=Configuration
```

- 创建和更新 NT AuthCertificates 证书颁发机构对象，如下例所示。如果 NT AuthCertificates 证书颁发机构对象存在，则必须为其委派权限。如果对象不存在，则必须委托在公钥服务容器上创建子对象的权限。

```
#objects
CN=NTAuthCertificates,CN=Public Key Services,CN=Services,CN=Configuration
```

> **Note**
>
> 如果你使用的是 AWS 托管 Microsoft AD，那么当你在目录中授权 Conn AWS Private CA ector for AD 服务时，系统会自动委派额外的权限。

您可以使用以下 PowerShell 脚本委派其他权限并创建 NT AuthCertifiates 证书颁发机构对象。将“myconnectoraccount”替换为服务账户名称。

```
$AccountName = 'myconnectoraccount'

# DO NOT modify anything below this comment.
# Getting Active Directory information.
Import-Module -Name 'ActiveDirectory'
$RootDSE = Get-ADRootDSE

# Getting AD Connector service account Information
$AccountProperties = Get-ADUser -Identity $AccountName
$AccountSid = New-Object -TypeName 'System.Security.Principal.SecurityIdentifier'
 $AccountProperties.SID.Value
[System.GUID]$ServicePrincipalNameGuid = (Get-ADObject -SearchBase
 $RootDse.SchemaNamingContext -Filter { lDAPDisplayName -eq 'servicePrincipalName' } -
Properties 'schemaIDGUID').schemaIDGUID
$AccountAclPath = $AccountProperties.DistinguishedName

# Getting ACL settings for AD Connector service account.
$AccountAcl = Get-ACL -Path "AD:\$AccountAclPath"

# Setting ACL allowing the AD Connector service account the ability to add and remove a
 Service Principal Name (SPN) to itself
$AccountAccessRule = New-Object -TypeName
 'System.DirectoryServices.ActiveDirectoryAccessRule' $AccountSid, 'WriteProperty',
 'Allow', $ServicePrincipalNameGuid, 'None'
$AccountAcl.AddAccessRule($AccountAccessRule)
Set-ACL -AclObject $AccountAcl -Path "AD:\$AccountAclPath"

# Add ACLs allowing AD Connector service account the ability to create certification
 authorities
[System.GUID]$CertificationAuthorityGuid = (Get-ADObject -SearchBase
 $RootDse.SchemaNamingContext -Filter { lDAPDisplayName -eq 'certificationAuthority' }
 -Properties 'schemaIDGUID').schemaIDGUID
$CAAccessRule = New-Object -TypeName
 'System.DirectoryServices.ActiveDirectoryAccessRule' $AccountSid,
 'ReadProperty,WriteProperty,CreateChild,DeleteChild', 'Allow',
 $CertificationAuthorityGuid, 'None'
$PKSDN = "CN=Public Key Services,CN=Services,CN=Configuration,
$($RootDSE.rootDomainNamingContext)"
$PKSACL = Get-ACL -Path "AD:\$PKSDN"
$PKSACL.AddAccessRule($CAAccessRule)
```

```
Set-ACL -AclObject $PKSACL -Path "AD:\$PKSDN"

$AIADN = "CN=AIA,CN=Public Key Services,CN=Services,CN=Configuration,
$($RootDSE.rootDomainNamingContext)"
$AIAACL = Get-ACL -Path "AD:\$AIADN"
$AIAACL.AddAccessRule($CAAccessRule)
Set-ACL -AclObject $AIAACL -Path "AD:\$AIADN"

$CertificationAuthoritiesDN = "CN=Certification Authorities,CN=Public Key
 Services,CN=Services,CN=Configuration,$($RootDSE.rootDomainNamingContext)"
$CertificationAuthoritiesACL = Get-ACL -Path "AD:\$CertificationAuthoritiesDN"
$CertificationAuthoritiesACL.AddAccessRule($CAAccessRule)
Set-ACL -AclObject $CertificationAuthoritiesACL -Path "AD:\$CertificationAuthoritiesDN"

$NTAuthCertificatesDN = "CN=NTAuthCertificates,CN=Public Key
 Services,CN=Services,CN=Configuration,$($RootDSE.rootDomainNamingContext)"
If (-Not (Test-Path -Path "AD:\$NTAuthCertificatesDN")) {
New-ADObject -Name 'NTAuthCertificates' -Type 'certificationAuthority' -OtherAttributes
 @{certificateRevocationList=[byte[]]'00';authorityRevocationList=[byte[]]'00';cACertificate=[b
 -Path "CN=Public Key Services,CN=Services,CN=Configuration,
$($RootDSE.rootDomainNamingContext)"
}

$NTAuthCertificatesACL = Get-ACL -Path "AD:\$NTAuthCertificatesDN"
$NullGuid = [System.GUID]'00000000-0000-0000-0000-000000000000'
$NTAuthAccessRule = New-Object -TypeName
 'System.DirectoryServices.ActiveDirectoryAccessRule' $AccountSid,
 'ReadProperty,WriteProperty', 'Allow', $NullGuid, 'None'
$NTAuthCertificatesACL.AddAccessRule($NTAuthAccessRule)
Set-ACL -AclObject $NTAuthCertificatesACL -Path "AD:\$NTAuthCertificatesDN"
```

为 AD 设置 AWS Private CA 连接器

1. 登录 AWS Management Console 并打开 AWS Directory Service 控制台，网址为https://console.aws.amazon.com/directoryservicev2/。
2. 在目录页面上，选择您的目录 ID。
3. 在 “网络和安全” 选项卡下的 “ADAWS Private CA 连接器” 下，选择 “为 AD 设置 AWS Private CA 连接器”。将出现 “为其创建私有 CA 证书 Active Directory” 页面。按照控制台上的步骤创建您的私有 CA，以便Active Directory连接器注册您的私有 CA。有关更多信息，请参阅 Creating a connector。
4. 创建连接器后，请按照以下步骤查看详细信息，包括连接器的状态和关联的私有 CA 的状态。

查看 AD AWS Private CA 连接器

1. 登录 AWS Management Console 并打开 AWS Directory Service 控制台，网址为https://console.aws.amazon.com/directoryservicev2/。
2. 在目录页面上，选择您的目录 ID。
3. 在网络与安全性下的 AWS Private CA Connector for AD 下，您可以查看您的私有 CA 连接器和关联的私有 CA。默认情况下，您会看到以下字段：
   a. AWS Private CA 连接器 ID- AWS Private CA 连接器的唯一标识符。点击它会进入该 AWS Private CA 连接器的详细信息页面。
   b. AWS Private CA 主题-有关 CA 的可分辨名称的信息。点击该字段会进入该 AWS Private CA 的详细信息页面。
   c. 状态 —基于对 AWS Private CA 连接器的状态检查和 AWS Private CA. 如果两项检查均通过，则会显示活动。如果其中一项检查失败，则会显示 1/2 检查失败。如果两项检查均失败，则会显示失败。有关失败状态的更多信息，请将鼠标悬停在超链接上以了解哪项检查失败。按照控制台中的说明进行修复。
   d. 创建日期- AWS Private CA 连接器的创建日期。

有关更多信息，请参阅 View connector details。

监控您的 AD Connector 目录

您可以通过以下方法监控您的 AD Connector 目录：

主题

- 了解目录状态
- 使用 Amazon SNS 配置目录状态通知

了解目录状态

以下是目录的各种状态。

处于活动状态

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

Creating

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

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。如果问题仍存在，请联系 AWS Support 中心。

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，请参阅微软 AD AWS 托管故障排除、AD Connector 故障排除、Simple AD 问题排查。对于与正常维护相关的问题， AWS 可在 40 分钟内解决这些问题。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 AWS Support 中心。

> **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 为目录拍摄快照或还原目录。

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。

使用 Amazon SNS 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“活动”状态变为“受损”或“不可操作”状态，您将收到通知。当目录恢复为“活动”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用户，他们接收发布至该主题的消息。按照以下步骤，您可以在 Amazon SNS 主题中添加 AWS Directory Service 出版商身份。当 AWS Directory Service 检测到您的目录状态发生变化时，它会向该主题发布一条消息，然后将其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 AWS Management Console 并打开AWS Directory Service 控制台。
2. 在目录页面上，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，然后选择创建通知。
5. 在创建通知页面上，选择选择通知类型，然后选择创建新通知。或者，如果您现在已有一个 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**
   >
   > 如果您选择创建新通知，但之后使用与现有 SNS 主题相同的主题名称，则 Amazon SNS 不会创建新主题，只是向现有主题添加新的订阅信息。
   > 如果您选择关联现有 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，然后输入收件人联系信息。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）为主题和 SNS 显示名称提供名称。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**
>
> 如果您使用只有DirectoryServiceFullAccess托管策略的 IAM 用户或角色登录，则您的主题名称必须以 “DirectoryMonitoring” 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。

如果您想指定其他 SNS 订阅者，例如额外的电子邮件地址、Amazon SQS 队列 AWS Lambda或，则可以从 Amazon SNS 控制台执行此操作。

从主题移除目录状态消息

1. 登录 AWS Management Console 并打开AWS Directory Service 控制台。
2. 在目录页面上，选择您的目录 ID。
3. 选择维护选项卡。
4. 在目录监控部分，在列表中选择一个 SNS 主题名称，选择操作，然后选择移除。
5. 选择移除。

这会移除您目录的选定 SNS 主题发布者身份。如果您想删除整个主题，可以从 Amazon SNS 控制台执行此操作。

> **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，在删除任何从中 AWS Directory Service接收消息的主题之前，请将您的目录与其他 Amazon SNS 主题相关联。

将 Amazon EC2 实例加入您的 Active Directory

AD Connector 是一个目录网关，您可以使用该网关将目录请求重定向到本地，MicrosoftActive Directory而无需在云中缓存任何信息。以下是有关如何将 Amazon EC2 加入 Active Directory 域的更多信息：

- 当 Amazon EC2 实例启动时，您可以将该实例无缝加入您的Active Directory域。有关更多信息，请参阅 使用 AD Connector 将亚马逊 EC2 Windows 实例无缝加入您的 AWS 托管微软 AD。
- 如果您需要手动将 EC2 实例加入您的Active Directory域，则必须在相应 AWS 区域 的安全组或子网中启动该实例，然后将该实例加入Active Directory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，这要求互联网网关连接到 Amazon VPC，并且实例具有公有 IP 地址。有关使用互联网网关连接到互联网的更多信息，请参阅《Amazon VPC 用户指南》中的使用互联网网关连接到互联网。

> **Note**
>
> 将实例加入您的自管理Active Directory（本地）后，该实例将直接与您的实例通信Active Directory并绕过 AD Connector。

主题

- 使用 AD Connector 将亚马逊 EC2 Windows 实例无缝加入您的 AWS 托管微软 AD
- 使用 AD Connector 将亚马逊 EC2 Linux 实例无缝加入你的 AWS 托管微软 AD

使用 AD Connector 将亚马逊 EC2 Windows 实例无缝加入您的 AWS 托管微软 AD

此过程将亚马逊 EC2 Windows 实例无缝连接到您的 AWS 托管 Microsoft AD Active Directory。

无缝加入 EC2 Windows 实例

1. 登录 AWS Management Console 并打开亚马逊 EC2 控制台，网址为 https://console.aws.amazon.com/ec2/。
2. 在导航栏中，选择与现有目录 AWS 区域 相同的目录。
3. 在 EC2 控制面板的启动实例部分，选择启动实例。
4. 在启动实例页面的名称和标签部分下，输入您要用于 Windows EC2 实例的名称。

5. （可选）选择添加其他标签，添加一个或多个标签密钥值对，以组织、跟踪或控制对此 EC2 实例的访问权限。
6. 在应用程序和操作系统映像（亚马逊机器映像）部分，在快速入门窗格中选择 Windows。您可以从亚马逊机器映像（AMI）下拉列表中更改 Windows 亚马逊机器映像（AMI）。
7. 在实例类型部分，从实例类型下拉列表中选择要使用的实例类型。
8. 在密钥对（登录）部分，您可以选择创建新密钥对，或从现有密钥对中进行选择。

   a. 要创建新的密钥对，请选择新建新密钥对。

   b. 输入密钥对的名称，然后为密钥对类型和私钥文件格式选择一个选项。

   c. 要以可与 OpenSSH 一起使用的格式保存私钥，请选择 pem。要以可与 PuTTY 一起使用的格式保存私钥，请选择 ppk。

   d. 选择创建密钥对。

   e. 您的浏览器会自动下载私有密钥文件。将私有密钥文件保存在安全位置。

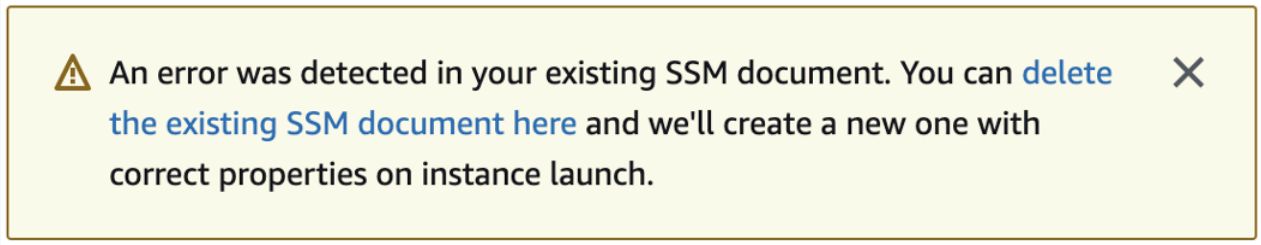
   > **Important**
   >
   > 这是您保存私有密钥文件的唯一机会。

9. 在启动实例页面的网络设置部分下，选择编辑。从 VPC – 必需下拉列表中选择创建目录的 VPC。
10. 从子网下拉列表中选择 VPC 中的其中一个公有子网。选择的子网必须将所有外部流量都路由到互联网网关。否则将无法远程连接到实例。

    有关如何连接到互联网网关的更多信息，请参阅《Amazon VPC 用户指南》中的使用互联网网关连接到互联网。
11. 在自动分配公有 IP 下，选择启用。

    有关公有和私有 IP 寻址的更多信息，请参阅《亚马逊 EC2 用户指南》中的 Amazon EC2 实例 IP 寻址。
12. 对于防火墙（安全组）设置，您可以使用默认设置或进行更改以满足您的需求。
13. 对于配置存储设置，您可以使用默认设置或进行更改以满足您的需求。
14. 选择高级详细信息部分，从域加入目录下拉列表中选择您的域。

    > **Note**
    >
    > 选择域加入目录后，您可能会看到：



如果 EC2 启动向导识别出具有意外属性的现有 SSM 文档，则会发生此错误。您可以执行以下操作之一：

- 如果您之前编辑了 SSM 文档并且属性符合预期，请选择关闭并继续启动 EC2 实例，不做任何更改。
- 选择 “在此处删除现有 SSM 文档” 链接以删除 SSM 文档。这将允许创建具有正确属性的 SSM 文档。SSM 文档将在您启动 EC2 实例时自动创建。

15. 对于 IAM 实例配置文件，您可以选择现有的 IAM 实例配置文件或创建新的 IAM 实例配置文件。从 IAM 实例配置文件下拉列表中选择一个DirectoryServiceAccess附有 AWS 托管策略 AmazonSSM ManagedInstanceCore 和 AmazonSSM 的 IAM 实例配置文件。要创建新的 IAM 个人资料链接，请选择创建新的 IAM 个人资料链接，然后执行以下操作：

    1. 选择 创建角色。
    2. 在选择受信任的实体下，选择 AWS 服务。
    3. 在 Use case（使用案例）下，选择 EC2。
    4. 在 “添加权限” 下的策略列表中，选择 AmazonSSM ManagedInstanceCore 和 AmazonSSM 政策。DirectoryServiceAccess在搜索框中键入 **SSM** 以筛选列表。选择下一步。

    > **Note**
    >
    > AmazonSSM DirectoryServiceAccess 提供了将实例加入Active Directory托管者的权限。 AWS Directory ServiceAmazonSSM ManagedInstanceCore 提供使用该服务所需的最低权限。 AWS Systems Manager 有关创建具有这些权限的角色的更多信息，以及您可以分配给 IAM 角色的其他权限和策略的信息，请参阅《AWS Systems Manager 用户指南》中的为 Systems Manager 创建 IAM 实例配置文件。

    5. 在名称、查看和创建页面上，输入角色名称。您将需要此角色名称来附加到 EC2 实例。
    6. （可选）您可以在描述字段中提供 IAM 实例配置文件的描述。
    7. 选择 创建角色。

8. 返回启动实例页面，选择 IAM 实例配置文件旁边的刷新图标。您的新 IAM 实例配置文件应显示在 IAM 实例配置文件下拉列表中。选择新的配置文件，其余设置保留默认值。

16. 选择启动实例。

使用 AD Connector 将亚马逊 EC2 Linux 实例无缝加入你的 AWS 托管微软 AD

此过程将亚马逊 EC2 Linux 实例无缝连接到您的微软 AD AWS 托管目录。

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 Red Hat Enterprise 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 EC2 Linux 实例之前，您需要完成本节中的步骤。

选择无缝域名加入服务账户

您可以通过 AD Connector 将 Linux 计算机无缝连接到您的本地Active Directory域。要执行此操作，您必须创建一个具有创建计算机账户权限的用户账户，才能将计算机加入域。如果您愿意，可以使用 AD Connector 服务账户。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。尽管域管理员或其他组的成员可能有足够的权限将计算机加入域，但我们不建议使用这些权限。作为最佳实践，我们建议您使用具有将计算机加入域所需最低权限的服务账户。

要委托具有将计算机加入域所需的最低权限的帐户，可以运行以下 PowerShell 命令。您必须在已安装的已加入域的Windows计算机上运行这些命令。安装适用于 AWS 托管微软 AD 的 Active Directory 管理工具此外，您必须使用有权修改您的计算机 OU 或容器权限的账户。该 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。如果您更喜欢使用图形用户界面（GUI），您可以使用 向您的服务账户委派权限 中所述的手动过程。

```
$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 向您的服务账户委派权限 中所述的手动过程。

创建密钥以存储域服务账户

您可以使用 AWS Secrets Manager 存储域名服务帐户。

创建密钥并存储域服务账户信息

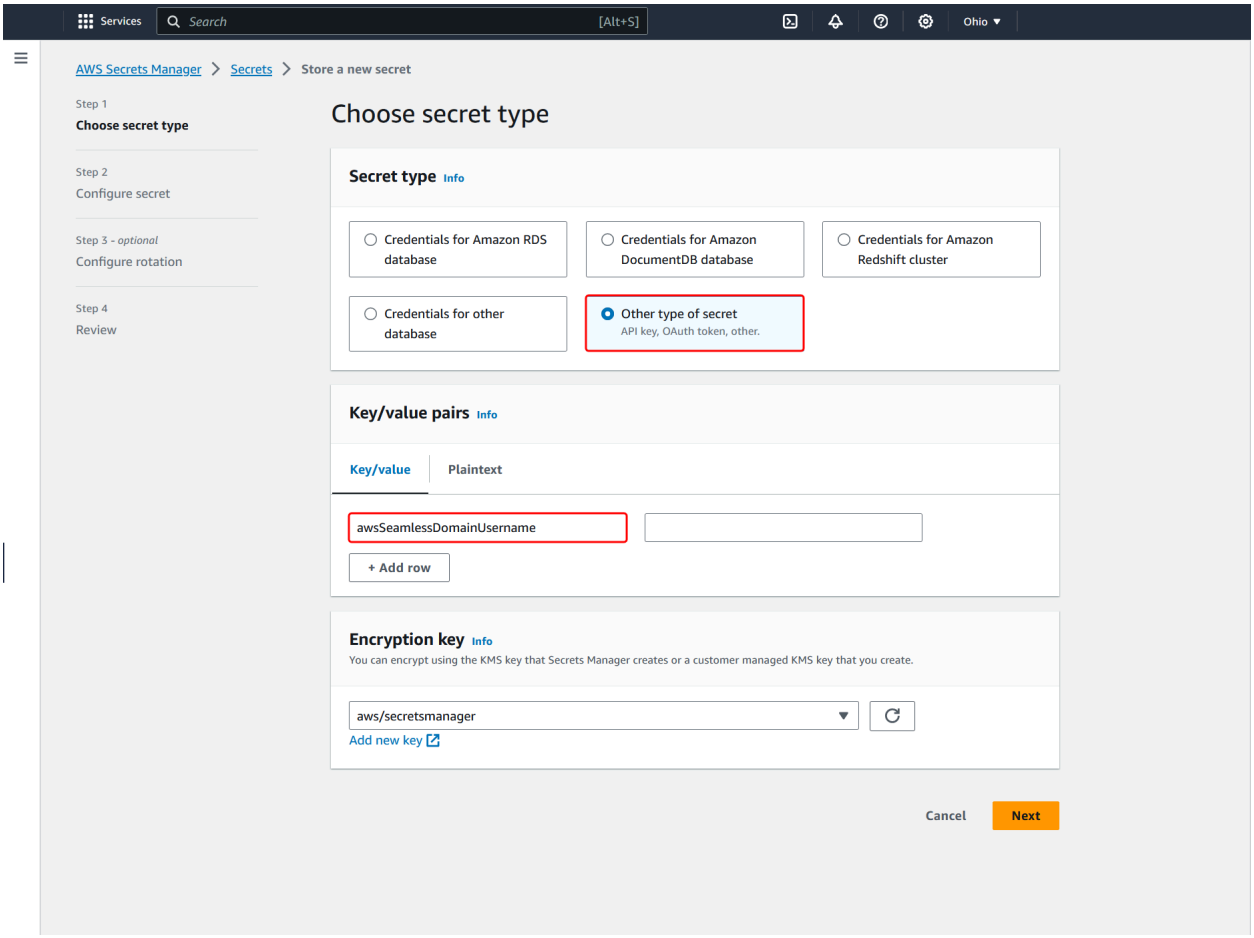
1. 登录 AWS Management Console 并打开 AWS Secrets Manager 控制台，网址为 https://console.aws.amazon.com/secretsmanager/。
2. 选择 存储新密钥。
3. 在 Store a new secret（存储新密钥）页面上，执行以下操作：

   a. 在密钥类型下，选择其他密钥类型。

b. 在“键/值对”下，执行以下操作：

i. 在第一个框中，输入 **awsSeamlessDomainUsername**。在同一行的下一个框中，输入您的服务帐号的用户名。例如，如果您之前使用过该 PowerShell 命令，则服务帐户名称将为**awsSeamlessDomain**。

> **Note**
>
> 必须完全按照原样输入 **awsSeamlessDomainUsername**。确保前后均没有任何空格。否则，域加入将失败。



ii. 选择添加行。

iii. 在新行的第一个框中输入 **awsSeamlessDomainPassword**。在同一行的下一个框中，输入服务账户密码。

> **Note**
>
> 必须完全按照原样输入 **awsSeamlessDomainPassword**。确保前后均没有任何空格。否则，域加入将失败。

iv. 在“加密密钥”下，保留默认值aws/secretsmanager。 AWS Secrets Manager 选择此选项时，始终会加密密钥。您也可以选择您创建的密钥。

> **Note**
>
> 根据您使用的密钥 AWS Secrets Manager，会收取与之相关的费用。有关当前完整定价列表，请参阅 AWS Secrets Manager 定价。
> 你可以使用 Secrets Manager 创建aws/secretsmanager的 AWS 托管密钥来免费加密你的秘密。如果您创建自己的 KMS 密钥来加密您的机密，则按当前费 AWS KMS 率向您 AWS 收费。有关更多信息，请参阅AWS Key Management Service 定价。

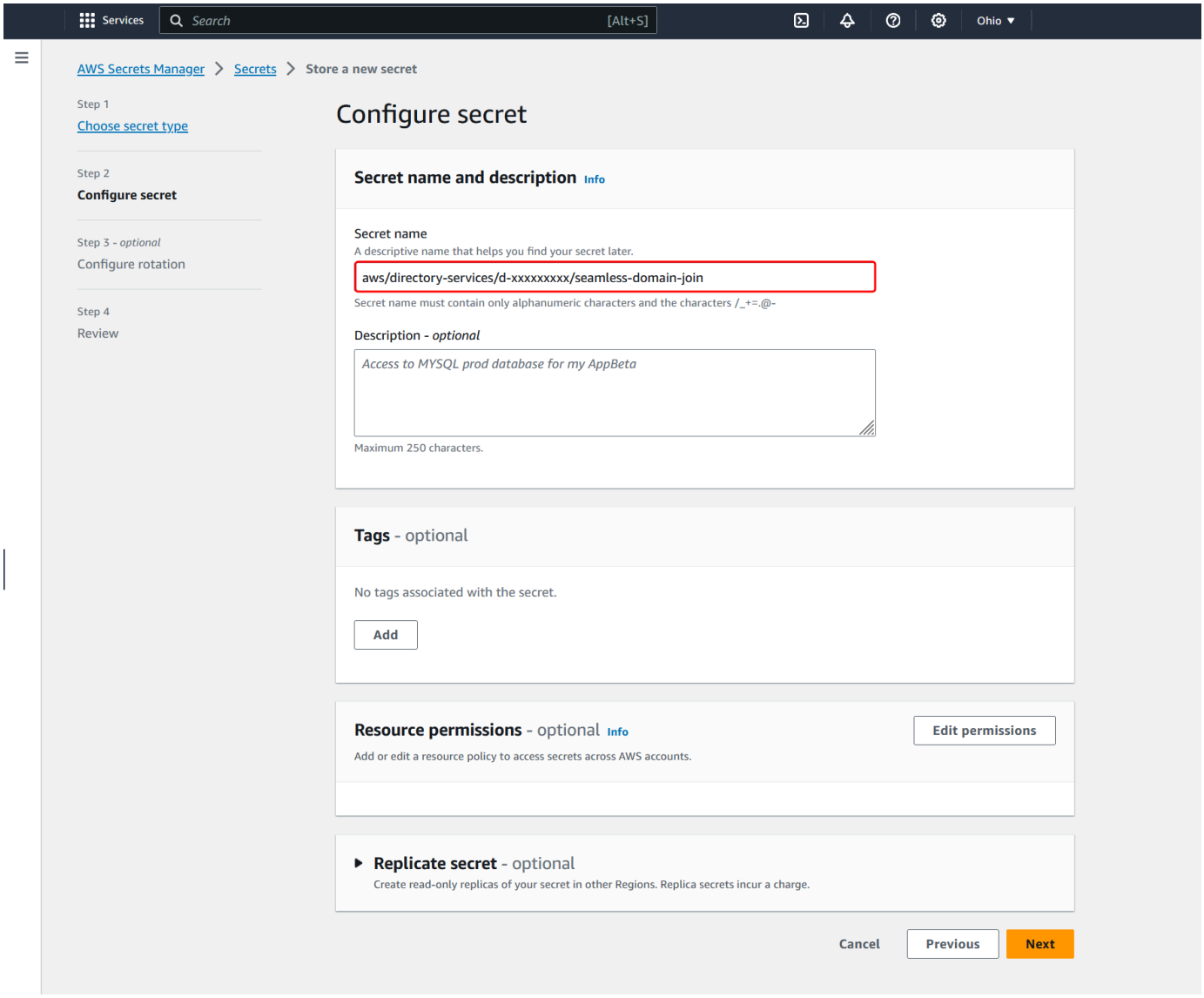
v. 选择下一步。

4. 在“密钥名称”下，使用以下格式输入包含您的目录 ID 的机密名称，将 *d-xxxxxxxxxx* 替换为您的目录 ID：

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

这将用于检索应用程序中的密钥。

> **Note**
>
> 您必须完全按照原样输入 **aws/directory-services/*d-xxxxxxxxx*/seamless-domain-join**，但请将 *d-xxxxxxxxxx* 替换为您的目录 ID。确保前后均没有空格。否则，域加入将失败。



5. 将其他所有内容都设置为默认值，然后选择下一步。
6. 在配置自动轮换下，选择禁用自动轮换，然后选择下一步。

   存储此密钥后，您可以为其启用轮换。
7. 查看设置，然后选择存储以保存更改。Secrets Manager 控制台将返回您账户中的密钥列表，并且列表中现在包含新的密钥。
8. 从列表中选择您新创建的密钥名称，并记下密钥 ARN 值。您需要在下一部分中使用该名称。

启用域名服务账户密钥的轮换

我们建议您定期轮换密钥以改善您的安全状况。

启用域名服务账户密钥的轮换

- 按照《AWS Secrets Manager 用户指南》中为 AWS Secrets Manager 密钥设置自动轮换中的说明进行操作。

  对于第 5 步，请使用AWS Secrets Manager 用户指南中的轮换模板 Microsoft Active Directory 凭据。

  如需帮助，请参阅《AWS Secrets Manager 用户指南》中的AWS Secrets Manager 轮换疑难解答。

创建所需 IAM policy 和角色

使用以下先决条件步骤创建自定义策略，该策略允许对您的 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 LinuxEC2 DomainJoin IAM 角色。

创建 Secrets Manager IAM 读取策略

您可以使用 IAM 控制台创建策略，授予对 Secrets Manager 密钥的只读访问权限。

创建 Secrets Manager IAM 读取策略

1. 以有权创建 IAM 策略的用户 AWS Management Console 身份登录。然后通过以下网址打开 IAM 控制台：https://console.aws.amazon.com/iam/。
2. 在导航窗格的 “访问管理” 中，选择 “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 文本框中。

> **Note**
>
> 请务必将区域和资源 ARN 替换为之前创建的密钥的实际区域和资源 ARN。

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

```
                "secretsmanager:GetSecretValue",
                "secretsmanager:DescribeSecret"
            ],
            "Resource": [
                "arn:aws:secretsmanager:us-east-1:xxxxxxxxx:secret:aws/directory-
services/d-xxxxxxxxx/seamless-domain-join"
            ]
        }
    ]
}
```

5. 完成后，选择下一步。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 policy。
6. 在检查策略页面上，输入一个策略名称，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。选择创建策略，保存更改。托管策略列表中将显示新策略，并且现在已准备好附加到身份中。

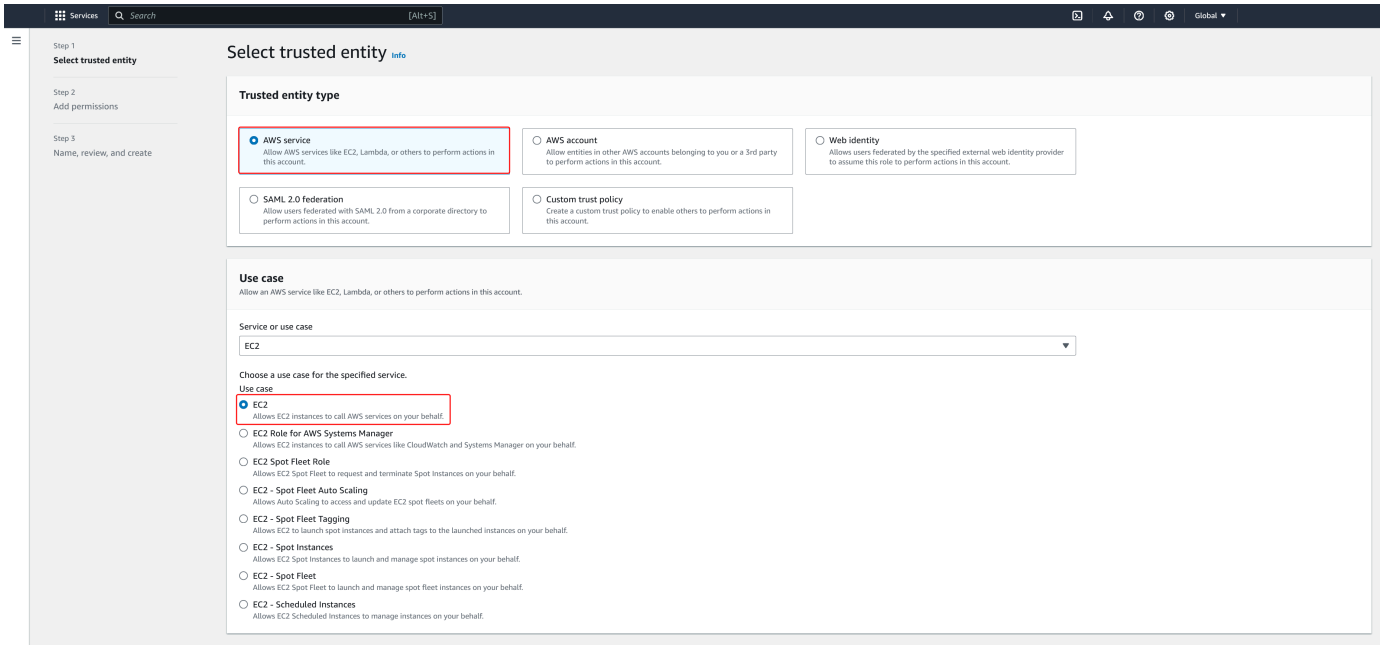
> **Note**
>
> 我们建议您为每个密钥创建一个策略。这样做可以确保实例只能访问相应的密钥，并在实例受损时将影响降至最低。

创建 LinuxEC2 角色 DomainJoin

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 LinuxEC2 角色 DomainJoin

1. 以有权创建 IAM 策略的用户 AWS Management Console 身份登录。然后通过以下网址打开 IAM 控制台：https://console.aws.amazon.com/iam/。
2. 在导航窗格中的访问管理下，选择角色。
3. 在内容窗格中，选择创建角色。
4. 在选择受信任实体的类型下，选择 AWS 服务。
5. 在 “用例” 下，选择 “EC2”，然后选择 “下一步”。



6. 对于筛选策略，执行以下操作：

   a. 输入 **AmazonSSMManagedInstanceCore**。然后选择列表中该项目的复选框。

   b. 输入 **AmazonSSMDirectoryServiceAccess**。然后选择列表中该项目的复选框。

   c. 输入 **SM-Secret-Linux-DJ-*d-xxxxxxxxxx*-Read**（或您在上一过程中创建的策略名称）。然后选择列表中该项目的复选框。

   d. 添加上面列出的三个策略后，选择创建角色。

> **Note**
>
> AmazonSSM DirectoryServiceAccess 提供了将实例加入Active Directory托管者的权限。AWS Directory Service AmazonSSM ManagedInstanceCore 提供使用该服务所需的最低权限。 AWS Systems Manager 有关创建具有这些权限的角色的更多信息，以及您可以分配给 IAM 角色的其他权限和策略的信息，请参阅《AWS Systems Manager 用户指南》中的为 Systems Manager 创建 IAM 实例配置文件。

7. 在角色名称字段中输入新角色的名称，例如**LinuxEC2DomainJoin**或其他您喜欢的名称。
8. （可选）对于角色描述，请输入描述。
9. （可选）在 “步骤 3：添加标签” 下选择 “添加新标签” 以添加标签。标签键值对用于组织、跟踪或控制此角色的访问权限。
10. 选择 创建角色。

将您的亚马逊 EC2 Linux 实例无缝加入您的 AWS 托管微软 AD Active Directory

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

无缝加入你的 Linux 实例

1. 登录 AWS Management Console 并打开亚马逊 EC2 控制台，网址为 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 AWS 区域 相同的目录。
3. 在 EC2 控制面板的启动实例部分，选择启动实例。
4. 在启动实例页面的名称和标签部分下，输入您要用于 Linux EC2 实例的名称。
5. （可选）选择添加其他标签，添加一个或多个标签密钥值对，以组织、跟踪或控制对此 EC2 实例的访问权限。
6. 在“应用程序和操作系统映像（Amazon 系统映像）”部分，选择要启动的 Linux AMI。

> **Note**
>
> 使用的 AMI 必须具有 AWS 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。如果您需要升级 SSM Agent，请参阅在适用于 Linux 的 EC2 实例上安装和配置 SSM Agent。
> SSM 在将 Linux 实例加入Active Directory域时使用该`aws:domainJoin`插件。该插件将 Linux 实例的主机名更改为 EC2AMAZ-*XXXXXX* X 格式。有关的更多信息`aws:domainJoin`，请参阅《AWS Systems Manager 用户指南》中的AWS Systems Manager 命令文档插件参考。

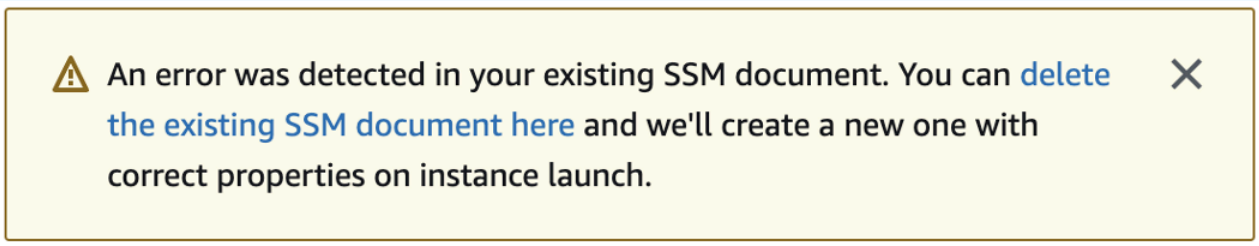
7. 在实例类型部分，从实例类型下拉列表中选择要使用的实例类型。
8. 在密钥对（登录）部分，您可以选择创建新密钥对，或从现有密钥对中进行选择。要创建新的密钥对，请选择新建新密钥对。输入密钥对的名称，然后为密钥对类型和私钥文件格式选择一个选项。要以可与 OpenSSH 一起使用的格式保存私钥，请选择 pem。要以可与 PuTTY 一起使用的格式保存私钥，请选择 ppk。选择创建密钥对。您的浏览器会自动下载私有密钥文件。将私有密钥文件保存在安全位置。

> **Important**
>
> 这是您保存私有密钥文件的唯一机会。

9. 在启动实例页面的网络设置部分下，选择编辑。从 VPC – 必需下拉列表中选择创建目录的 VPC。
10. 从子网下拉列表中选择 VPC 中的其中一个公有子网。选择的子网必须将所有外部流量都路由到互联网网关。否则将无法远程连接到实例。

    有关如何连接到互联网网关的更多信息，请参阅《Amazon VPC 用户指南》中的使用互联网网关连接到互联网。
11. 在自动分配公有 IP 下，选择启用。

    有关公有和私有 IP 寻址的更多信息，请参阅《亚马逊 EC2 用户指南》中的 Amazon EC2 实例 IP 寻址。
12. 对于防火墙（安全组）设置，您可以使用默认设置或进行更改以满足您的需求。
13. 对于配置存储设置，您可以使用默认设置或进行更改以满足您的需求。
14. 选择高级详细信息部分，从域加入目录下拉列表中选择您的域。

> **Note**
>
> 选择域加入目录后，您可能会看到：
>
> 
>
>
> 如果 EC2 启动向导识别出具有意外属性的现有 SSM 文档，则会发生此错误。您可以执行以下操作之一：
>
> - 如果您之前编辑了 SSM 文档并且属性符合预期，请选择关闭并继续启动 EC2 实例，不做任何更改。
> - 选择 “在此处删除现有 SSM 文档” 链接以删除 SSM 文档。这将允许创建具有正确属性的 SSM 文档。SSM 文档将在您启动 EC2 实例时自动创建。

15. 对于 IAM 实例配置文件，请选择您之前在先决条件部分步骤 2：创建 LinuxEC DomainJoin 2 角色中创建的 IAM 角色。
16. 选择启动实例。

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

维护您的 AD Connector 目录

本节介绍如何为您的 AD Connector 环境维护常见管理任务。

主题

- 删除 AD Connector
- 查看目录信息

删除 AD Connector

删除 AD Connector 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。

删除 AD Connector

1. 在 AWS Directory Service 控制台导航窗格中，选择目录。确保您位于部署 AD Connector AWS 区域 的地方。有关更多信息，请参阅选择区域。
2. 确保没有为要删除的 AD Connector 启用任何 AWS 应用程序。启用的 AWS 应用程序将阻止您删除 AD Connector。

   a. 在目录页面上，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AWS 应用程序和服务部分，您可以看到哪些 AWS 应用程序已为您的 AD Connector 启用。

      - 禁用 AWS Management Console 访问权限。有关更多信息，请参阅 禁用 AWS Management Console 访问。
      - 要禁用 Amazon WorkSpaces，您必须从 WorkSpaces 控制台的目录中取消注册该服务。有关更多信息，请参阅《Amazon WorkSpaces 管理指南》中的从目录取消注册。
      - 要禁用亚马逊 WorkDocs，您必须在亚马逊 WorkDocs控制台中删除亚马逊 WorkDocs 网站。有关更多信息，请参阅《Amazon WorkDocs 管理指南》中的删除网站。

- 要禁用亚马逊 WorkMail，您必须在亚马逊 WorkMail 控制台中删除亚马逊 WorkMail 组织。有关更多信息，请参阅《Amazon WorkMail 管理员指南》中的移除组织。
- 要禁用适用于 Windows File Server 的 Amazon FSx，必须从域中删除 Amazon FSx 文件系统。有关更多信息，请参阅《亚马逊 FSx for Windows 文件服务器用户指南》中的在 Windows 文件服务器的 FSx 中使用。Active Directory
- 要禁用 Amazon Relational Database Service，必须从域中移除 Amazon RDS 实例。有关更多信息，请参阅《Amazon RDS 用户指南》中的在域中管理数据库实例。
- 要禁用 AWS Client VPN 服务，必须从 Client VPN 端点中删除目录服务。有关更多信息，请参阅《AWS Client VPN 管理员指南》中的Active Directory身份验证。
- 要禁用 Amazon Connect，必须删除 Amazon Connect 实例。有关更多信息，请参阅《Amazon Connect Administration Guide》中的 Deleting an Amazon Connect instance。
- 要禁用亚马逊 QuickSight，您必须取消订阅亚马逊 QuickSight。有关更多信息，请参阅 Amazon QuickSight 用户指南中的关闭 Amazon QuickSight 账户。

> **Note**
>
> 如果您正在使用 AWS IAM Identity Center 并且之前已将其连接到计划删除的 AWS 托管 Microsoft AD 目录，则必须先更改身份源，然后才能将其删除。有关更多信息，请参阅《IAM Identity Center User Guide》中的 Change your identity source。

3. 在导航窗格中，选择目录。
4. 仅选择要删除的 AD Connector，然后单击删除。删除 AD Connector 需要几分钟时间。AD Connector 删除之后，其会从目录列表中删除。

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AWS Directory Service 控制台导航窗格中 Active Directory，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面中。

有关 Status 字段的更多信息，请参阅了解目录状态。

允许访问 AWS 应用程序和服务

用户可以授权 AD Connector 授予 AWS 应用程序和服务（例如亚马逊 WorkSpaces）访问您的权限 Active Directory。为了与 AD Connector 配合使用，可以启用或禁用以下 AWS 应用程序和服务。

AWS 应用程序/服务	更多信息……
Amazon Chime	有关更多信息，请参阅 Amazon Chime Administration Guide。
Amazon Connect	有关更多信息，请参阅 Amazon Connect Administration Guide。
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》。
Amazon WorkSpaces	你可以直接从中创建 Simple AD、 AWS 托管 Microsoft AD 或 AD Connecto WorkSpaces r。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》。
AWS Client VPN	有关更多信息，请参阅 AWS Client VPN 用户指南。
AWS IAM Identity Center	有关更多信息，请参阅 AWS IAM Identity Center 用户指南。
AWS Management Console	有关更多信息，请参阅允许使用 AD 凭证访问 AWS Management Console。
AWS Transfer Family	有关更多信息，请参阅 AWS Transfer Family 用户指南。

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权限。要在 AWS Directory Service 控制台中查找上述 AWS 应用程序和服务链接，请执行以下步骤。

显示适用于目录的应用程序和服务

1. 在 AWS Directory Service 控制台导航窗格中，选择目录。
2. 在目录页面上，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 AWS 应用程序和服务部分下的列表。

有关如何使用对 AWS 应用程序和服务进行授权或取消授权的更多信息 AWS Directory Service，请参阅使用对 AWS 应用程序和服务的授权 AWS Directory Service。

为 AD Connector 更新 DNS 地址

按照以下步骤更新 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。
> 如果您将 WorkSpaces 与 AD Connector 配合使用，请确保 WorkSpace 的 DNS 地址也已更新。有关更多信息，请参阅 Update DNS servers for WorkSpaces。

为 AD Connector 更新 DNS 设置

1. 在 AWS Directory Service 控制台导航窗格的 Active Directory 下，选择目录。
2. 选择目录的目录 ID 链接。
3. 在目录详细信息页面上，选择网络与安全性选项卡。
4. 向下滚动到现有 DNS 设置部分，然后选择更新。
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)。

有关 AD Connector 故障排除的更多信息，请参阅 AD Connector 故障排除。

AD Connector 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。

验证目录类型是否正确

AWS Directory Service 提供了多种与其他 AWS 服务Microsoft Active Directory配合使用的方式。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：

- AWS 微软目录服务 Active Directory 是一款托管在云端的功能丰富的Microsoft Active Directory托管服务。 AWS AWS 如果您拥有超过 5,000 个用户，并且需要在托管目录和本地目录之间建立信任关系，那么 AWS 托管 Microsoft AD 是您的最佳选择。
- AD Con nector 只需将您的现有本地环境连接Active Directory到 AWS。当您想要将现有本地目录与 AWS 服务一起使用时，AD Connector 是您的最佳选择。
- S@@ imple AD 是一个低规模、低成本的目录，具有基本Active Directory兼容性。其支持 5000 个或更少的用户、兼容 Samba 4 的应用程序，并支持 LDAP 感知型应用程序的 LDAP 兼容性。

有关 AWS Directory Service 选项的更详细比较，请参阅选择哪一个。

确保 VPC 和实例正确配置

要连接到、管理和使用目录，必须正确配置目录所关联的 VPC。有关 VPC 安全和网络要求的信息，请参阅 AWS 微软 AD 托管先决条件、AD Connector 先决条件 或 Simple AD 先决条件。

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 Amazon EC2 实例加入您的 AWS 托管微软 AD Active Directory 中所述。

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可以存储在目录中的对象数量的唯一限制。有关所选目录的详细信息，请参阅 AWS 托管微软 AD 配额、AD Connector 配额 或 Simple AD 限额。

了解目录 AWS 的安全组配置并使用

AWS 创建安全组并将其附加到目录的弹性网络接口，这些接口可从对等连接或调整大小的 VPC 中进行访问。 AWS 将安全组配置为阻止不必要的目录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《Amazon EC2 用户指南》中的适用于 Linux 实例的 Amazon EC2 安全组。不当的更改可能会导致与目标计算机和实例的通信中断。 AWS 建议您不要尝试打开目录的其他端口，因为这会降低目录的安全性。请仔细查看 AWS 责任共担模型。

> **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， AWS 建议不要这样做。 AWS 可能有理由在不另行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 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 AWS 应用程序的用户名限制

AWS Directory Service 为大多数可用于构建用户名的字符格式提供支持。但是，对于用于登录 AWS 应用程序（例如亚马逊、亚马逊或亚马 QuickSight逊 WorkDocs）的用户名 WorkSpaces，有一些字符限制。 WorkMail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。

为您的应用程序编程

在为您的应用程序编程之前，请考虑以下事项：

交付生产之前的负载测试

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。

定期交替管理员凭证

定期更改您的 AD Connector 服务账户管理员密码，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 AWS Directory Service 中更新 AD Connector 服务账户凭证。

对每个域使用唯一的 AD Connector

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，您必须创建唯一的 AD Connector。您创建的每个 AD Connector 都必须使用不同的服务账户，即使将其连接到同一目录时也是如此。

兼容性检查

使用 AD Connector 时，必须确保您的本地目录与兼容，并且始终与 AWS Directory Service s 兼容。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

下面是 AD Connector 的默认限额。除非另有说明，否则每个限额均与区域一一对应。

AD Connector 限额

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 AWS Directory Service for Microsoft Active Directory（AWS 微软 AD 托管）的替代方案，AD Connector 是仅适用于 AWS 创建的应用程序和服务的 Active Directory 代理。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。没有可以使用 AD Connector 的第三方应用程序。

下面列出了兼容的 AWS 应用程序和服务：

- Amazon Chime – 有关详细说明，请参阅连接到 Active Directory。
- Amazon Connect – 有关更多信息，请参阅 Amazon Connect 如何工作。
- 适用于 Windows 或 Linux 的 Amazon EC2 — 您可以使用亚马逊 EC2 Windows 或 Linux 的无缝活动目录域加入功能，将您的实例加入您自行管理的 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 Amazon EC2 实例加入您的 Active Directory：
- AWS Management Console – 您可使用 AD Connector 对使用其 Active Directory 凭证的 AWS Management Console 用户进行身份验证，无需设置 SAML 基础设施。有关更多信息，请参阅允许使用 AD 凭证访问 AWS Management Console：
- Amazon QuickSight -有关更多信息，请参阅在亚马逊 QuickSight 企业版中管理用户账户。
- AWS IAM Identity Center – 有关详细说明，请参阅 Connect IAM Identity Center to an on-premises Active Directory。
- AWS Transfer Family – 有关详细说明，请参阅 Working with AWS Directory Service for Microsoft Active Directory。
- AWS Client VPN – 有关详细说明，请参阅客户端身份验证和授权。
- Amazon WorkDocs -有关详细说明，请参阅使用 AD Connector 连接到您的本地目录。
- 亚马逊 WorkMail -有关详细说明，请参阅将亚马逊 WorkMail与现有目录集成（标准设置）。
- WorkSpaces -有关详细说明，请参阅 WorkSpace 使用 AD Connector 启动。

> **Note**
>
> Amazon RDS 仅与 AWS Managed Microsoft AD 兼容，与 AD Connector 不兼容。有关更多信息，请参阅AWS Directory Service常见问题页面中的AWS托管 Microsoft AD 部分。

AD Connector 故障排除

以下内容可以帮助您解决在创建或使用 AD Connector 时可能遇到的一些常见问题。

主题

- 创作问题
- 连接问题
- 身份验证问题
- 维护问题
- 我无法删除我的 AD Connector

创作问题

以下是 AD Connector 的常见创建问题

- 我在创建目录时遇到“AZ Constrained”错误
- 我在尝试创建 AD Connector 时收到 “检测到连接问题” 错误

我在创建目录时遇到“AZ Constrained”错误

在 2012 年之前创建的某些 AWS 账户可能有权访问美国东部（弗吉尼亚北部）、美国西部（加利福尼亚北部）或亚太地区（东京）不支持 AWS Directory Service 目录的可用区。如果您在创建时收到类似这样的错误Active Directory，请在不同的可用区中选择一个子网，然后再次尝试创建该目录。

我在尝试创建 AD Connector 时收到 “检测到连接问题” 错误

如果您在尝试创建 AD Connector 时收到 “检测到连接问题” 错误，则该错误可能是由于端口可用性或 AD Connector 密码复杂所致。您可以测试 AD 连接器的连接，以查看以下端口是否可用：

- 53 (DNS)

- 88 (Kerberos)
- 389 (LDAP)

要测试您的连接，请参阅测试 AD Connector。应在连接到 AD 连接器的 IP 地址关联的两个子网的实例上执行连接测试。

如果连接测试成功并且实例已加入域，请检查您的 AD Connector 的密码。AD Connector 必须满足 AWS 密码复杂度要求。有关更多信息，请参阅中的服务帐号AD Connector 先决条件。

如果您的 AD 连接器不符合这些要求，请使用符合这些要求的密码重新创建 AD 连接器。

连接问题

以下是 AD Connector 的常见连接问题

- 在尝试连接到我的本地目录时，我收到一条“Connectivity issues detected”错误
- 当我尝试连接我的本地目录时收到一条“DNS unavailable”错误
- 在尝试连接到我的本地目录时，我收到一条“SRV record”错误

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 Connector 先决条件。

- 88 (Kerberos)
- 389 (LDAP)

根据您的需求，您可能需要其他 TCP/UDP 端口。有关其中一些端口，请参阅以下列表。有关使用的端口的更多信息Active Directory，请参阅Microsoft文档中的如何为Active Directory域和信任配置防火墙。

- 135（RPC 端点映射器）
- 646 (LDAP SSL)
- 3268 (LDAP GC)
- 3269 (LDAP GC SSL)

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 Connector 先决条件。

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>
```

在连接您的目录时，AD Connector 需要获取 `_ldap._tcp.<DnsDomainName>` 和 `_kerberos._tcp.<DnsDomainName>` 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。

身份验证问题

以下是 AD Connector 的一些常见身份验证问题：

- 当我尝试使用智能卡登录时，我收到 “证书验证失败” 错误 Amazon WorkSpaces
- AD Connector 使用的服务账户尝试进行身份验证时，我收到“Invalid Credentials”的错误消息
- 在使用 AWS 应用程序搜索用户或群组时，我收到 “无法进行身份验证” 错误
- 当我尝试更新 AD Connector 服务帐户时，我收到有关我的目录凭据的错误消息
- 我的某些用户无法进行向我的目录进行身份验证

当我尝试使用智能卡登录时，我收到 “证书验证失败” 错误 Amazon WorkSpaces

当您尝试使用智能卡登录时，您会收到一条类似于以下内容的错误消息： WorkSpaces

```
ERROR: Certificate Validation failed. Please try again by restarting your browser or
 application and make sure you select the correct certificate.
```

如果智能卡的证书未正确存储在使用证书的客户端上，则会发生错误。有关 AD Connector 和智能卡要求的更多信息，请参阅先决条件。

使用以下过程对智能卡在用户证书存储中存储证书的能力进行故障排除：

1. 在无法访问证书的设备上，访问 Microsoft Management Console (MMC)。

   > **Important**
   >
   > 在继续操作之前，请创建智能卡证书的副本。

2. 导航到 MMC 中的证书存储区。从证书存储中删除用户的智能卡证书。有关在 MMC 中查看证书存储的更多信息，请参阅文档中的如何：使用 MMC 管理单元查看证书。Microsoft
3. 取出智能卡。
4. 重新插入智能卡，使其可以在用户的证书存储区中重新填充智能卡证书。

   > **Warning**
   >
   > 如果智能卡没有将证书重新填充到用户存储中，则无法将其用于 WorkSpaces 智能卡身份验证。

AD 连接器的服务帐户应具有以下内容：

- `my/spn`已添加到服务原则名称中
- 为 LDAP 服务委派

在智能卡上重新填充证书后，应检查本地域控制器，以确定它们是否被禁止映射主题备用名称的用户主体名称 (UPN)。有关此更改的更多信息，请参阅Microsoft文档中的如何禁用 UPN 映射的主题备用名称。

使用以下步骤检查您的域控制器的注册表项：

1. 在注册表编辑器中，导航到以下 Hive 密钥

   HKEY_LOCAL_MACHINE\ SYSTEM\\ 服务\ Kdc\ CurrentControlSet UseSubjectAltName
2. 选择UseSubjectAltName。确保该值设置为 0。

> **Note**
>
> 如果在本地域控制器上设置了注册表项，那么 AD Connector 将无法在中找到用户Active Directory并导致出现上述错误消息。

证书颁发机构 (CA) 证书应上传到 AD Connector 智能卡证书。证书应包含 OCSP 信息。以下列出了 CA 的其他要求：

- 证书应位于域控制器的可信根颁发机构、证书颁发机构服务器和 WorkSpaces。
- 脱机证书和根 CA 证书将不包含 OSCP 信息。这些证书包含有关其吊销的信息。
- 如果您使用第三方 CA 证书进行智能卡身份验证，则需要将 CA 和中间证书发布到 Active Directory NTauth 存储区。它们必须安装在所有域控制器、证书颁发机构服务器和的可信根颁发机构中 WorkSpaces。
  - 您可以使用以下命令将证书发布到 Active Directory NTauth 存储区：

```
certutil -dspublish -f Third_Party_CA.cer NTAuthCA
```

有关向 NTauth 商店发布证书的更多信息，请参阅《使用通用访问卡访问亚马 WorkSpaces 逊 Amazon 安装指南》中的 “将颁发的 CA 证书导入企业 nTauth 商店”。

您可以按照以下步骤检查用户证书或 CA 链证书是否已通过 OCSP 验证：

1. 将智能卡证书导出到本地计算机上的某个位置，例如 C: 驱动器。
2. 打开命令行提示符并导航到存储导出的智能卡证书的位置。
3. 输入以下 命令：

```
certutil -URL Certficate_name.cer
```

4. 命令后面应该会出现一个弹出窗口。选择右上角的 OCSP 选项，然后选择 “检索”。状态应返回为已验证。

有关 certutil 命令的更多信息，请参阅文档中的 c er tutil Microsoft

AD Connector 使用的服务账户尝试进行身份验证时，我收到“Invalid Credentials”的错误消息

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。

在使用 AWS 应用程序搜索用户或群组时，我收到 “无法进行身份验证” 错误

即使 AD Connector 状态处于活动状态，在使用 AWS 应用程序（例如 WorkSpaces 或 Amazon QuickSight）时搜索用户时也可能会遇到错误。过期的凭证可以阻止 AD Connector 在您的 Active Directory 中完成对对象的查询。使用中提供的顺序步骤更新服务帐户的密码Amazon EC2 实例的无缝域加入已停止工作。

当我尝试更新 AD Connector 服务帐户时，我收到有关我的目录凭据的错误消息

尝试更新 AD Connector 服务帐号时，您会收到一条类似于以下一条或多条错误消息：

```
Message:An Error Has Occurred
Your directory needs a credential update. Please update the directory credentials.
```

```
An Error Has Occurred
Your directory needs a credential update. Please update the directory credentials
following Update your AD Connector Service Account Credentials
```

```
Message:
An Error Has Occurred
Your request has a problem. Please see the following details.
There was an error with the service account/password combination
```

时间同步和 Kerberos 可能存在问题。AD Connector 向发送 Kerberos 身份验证请求。Active Directory 这些请求对时间敏感，如果请求延迟，它们就会失败。要解决此问题，请参阅文档中的建议-为根 PDC 配置权威时间源并避免广泛的时间偏差。Microsoft有关时间服务和同步的更多信息，请参见下文：

- 计Windows时服务的工作原理

- 计算机时钟同步的最大容差
- Windows时间服务工具和设置

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，请转到开启的预身份验证。Microsoft TechNet

维护问题

以下是 AD Connector 的常见维护问题

- 我的目录卡在“Requested”状态
- Amazon EC2 实例的无缝域加入已停止工作

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。如果问题仍存在，请联系 AWS Support。

Amazon EC2 实例的无缝域加入已停止工作

如果 EC2 实例的无缝域加入之前正常工作，然后在 AD Connector 处于活动状态时停止，则表示您的 AD Connector 服务账户的凭证可能已过期。过期的凭据可能会阻止 AD Connector 在您的中创建计算机对象Active Directory。

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. 更新您的服务帐户的密码Active Directory。
2. 在中更新您的 AD Connector 中服务帐号的密码 AWS Directory Service。有关更多信息，请参阅在 AWS Directory Service 中更新 AD Connector 服务账户凭证。

> **Important**
>
> 仅在中更新密码 AWS Directory Service 不会将密码更改推送到您现有的本地环境，Active Directory因此请务必按照上一个步骤中显示的顺序进行更改。

我无法删除我的 AD Connector

如果您的 AD Connector 切换到不可操作状态，则您将无法再访问您的域控制器。当仍有应用程序链接到 AD Connector 时，我们会阻止将其删除，因为其中一个应用程序可能仍在使用该目录。有关需要禁用才能删除 AD Connector 的应用程序列表，请参阅删除 AD Connector。如果您仍然无法删除 AD Connector，则可以通过请求帮助AWS Support。

Simple AD

Simple AD 是由 Samba 4 Active Directory Compatible Server 提供支持的独立托管目录。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 提供了 AWS 托管 Microsoft AD 提供的部分功能，包括管理用户账户和群组成员资格、创建和应用群组策略、安全连接到 Amazon EC2 实例以及提供基于 Kerberos 的单点登录 (SSO) 的功能。但是，请注意，Simple AD 不支持多因素身份验证 (MFA)、与其他域的信任关系、Active Directory 管理中心 PowerShell 、支持、Active Directory 回收站、群组托管服务帐户以及 POSIX 和 Microsoft 应用程序的架构扩展等功能。

Simple AD 具备许多优势：

- Simple AD 可以更轻松地管理运行 Linux 和 Windows 的亚马逊 EC2 实例以及在 AWS 云中部署 Windows 应用程序。
- 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 中的用户账户允许访问诸如 WorkSpaces亚马逊或亚马逊 WorkDocs之类的 AWS 应用程序 WorkMail。
- 您可以通过基于 IAM 角色的访问权限来管理 AWS 资源。 AWS Management Console
- 每日自动快照支持 point-in-time 恢复。

Simple AD 不支持以下任何服务之一：

- 亚马逊 AppStream 2.0
- Amazon Chime
- Amazon RDS for SQL Server
- Amazon RDS for Oracle
- AWS IAM Identity Center
- 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
- 如何管理 Simple AD
- 教程：制作一个 Simple AD Active Directory
- Simple AD 的最佳实践
- Simple AD 限额
- Simple AD 的应用程序兼容性策略
- Simple AD 问题排查

Simple AD 入门

Simple AD 在云中创建一个完全托管的、基于 Samba 的 AWS 目录。使用 Simple AD 创建目录时，AWS Directory Service 会代表您创建两个域控制器和 DNS 服务器。域控制器在 Amazon VPC 的不同子网中创建，这种冗余有助于确保即使发生故障，您的目录仍可访问。

主题

- Simple AD 先决条件
- 制作你的 Simple AD Active Directory
- 用你的 Simple AD 创作了什么 Active Directory
- 为 Simple AD 配置 DNS

Simple AD 先决条件

要创建 Simple ADActive Directory，您需要一个具有以下内容的 Amazon VPC：

- 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，其中包含*.amazonaws.com 的 DNS 条件替换，可解析为非公有 IP 地址 AWS
  - CloudWatch VPC 终端节点
  - Systems Manager VPC 端点
  - Security Token Service VPC 端点
- 两个不同的可用区中至少有两个子网。子网必须处于相同的无类域间路由 (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。创建 Simple AD 时， AWS Directory Service 会代表您创建两个域控制器和 DNS 服务器。
  - 有关 CIDR 范围的更多信息，请参阅 Amazon VPC 用户指南中的您的 VP C 和子网的 IP 地址。
- 如果您需要 Simple AD 支持 LDAPS，我们建议您使用连接到端口 389 的网络负载均衡器进行配置。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。有关如何针对 Simple AD 配置 LDAPS 的更多信息，请参阅 AWS 安全博客中的 How to configure an LDAPS endpoint for Simple AD。
- 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。
- 有关更多信息，请参阅《Amazon VPC 用户指南》中的什么是 Amazon VPC？。

AWS Directory Service 使用双 VPC 结构。构成您目录的 EC2 实例在您的 AWS 账户之外运行，由管理 AWS。其有 `ETH0` 和 `ETH1` 两个网络适配器。`ETH0` 是管理适配器，存在于您的账户之外。`ETH1` 在您的账户内创建。

目录的 `ETH0` 网络的管理 IP 范围以编程方式选择，以确保其不会与部署目录的 VPC 发生冲突。此 IP 范围可以是以下任一对（因为目录在两个子网中运行）：

- 10.0.1.0/24 和 10.0.2.0/24

- 169.254.0.0/16
- 192.168.1.0/24 和 192.168.2.0/24

我们通过检查 ETH1 CIDR 的第一个八位字节来避免冲突。如果以 10 开头，那么我们就选择一个 192.168.0.0/16 VPC，其子网为 192.168.1.0/24 和 192.168.2.0/24。如果第一个八位字节不是 10，则我们选择一个 10.0.0.0/16 VPC，其子网为 10.0.1.0/24 和 10.0.2.0/24。

选择算法不包括您 VPC 上的路由。因此，这种情况可能会导致 IP 路由冲突。

制作你的 Simple AD Active Directory

要创建新的 Simple ADActive Directory，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 先决条件中确定的先决条件。

创建 Simple AD Active Directory

1. 在 AWS Directory Service 控制台导航窗格中，选择目录，然后选择设置目录。
2. 在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 AD。

   组织名称

   您的目录的唯一组织名称，将用于注册客户端设备。

   只有在启动时创建目录时，此字段才可用 WorkSpaces。

   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。

   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。

用你的 Simple AD 创作了什么 Active Directory

使用 Simple Active Directory AD 创建时， AWS Directory Service 会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。 AWS Directory Service 不存储此密码，也无法找回。但是，您可以通过 AWS Directory Service 控制台或使用 ResetUserPasswordAPI 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。此帐户用于执行目录维护操作的自动操作，例如拍摄目录快照和 FSMO 角色 AWS Directory Service 转移。此账户的凭证由 AWS Directory Service进行安全存储。
- 自动创建弹性网络接口（ENI）并将其与每个域控制器相关联。这些 ENI 中的每一个 ENI 对于您的 VPC 和 AWS Directory Service 域控制器之间的连接都是必不可少的，因此切勿删除。您可以 AWS Directory Service 通过描述来标识所有保留供使用的网络接口：“为目录目录 ID AWS 创建的网络接口”。有关更多信息，请参阅 Amazon EC2 用户指南中的弹性网络接口。 AWS 托管 Microsoft AD 的默认 DNS 服务器Active Directory是无类域间路由 (CIDR) +2 的 VPC DNS 服务器。有关更多信息，请参阅亚马逊 VPC 用户指南中的亚马逊 DNS 服务器。

> **Note**
>
> 默认情况下，域控制器部署在一个区域的两个可用区，并连接到您的 Amazon 虚拟私有云（VPC）。每天自动备份一次，且加密 Amazon Elastic Block Store（EBS）卷以确保静态数据的安全。出现故障的域控制器会在同一可用区中使用相同的 IP 地址自动替换，并且可以使用最新的备份执行完全灾难恢复。

为 Simple AD 配置 DNS

Simple AD 会将 DNS 请求转发到 Amazon 针对 Amazon VPC 提供的 DNS 服务器的 IP 地址。这些 DNS 服务器将解析在 Amazon Route 53 私有托管区中配置的名称。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。有关 Route 53 的更多信息，请参阅什么是 Route 53？。

请注意，要使 Simple AD 能够响应外部 DNS 查询，必须将包含 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，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 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。

如何管理 Simple AD

本节列出了运行和维护 Simple AD 环境的所有过程。

主题

- 在 Simple AD 中管理用户和组
- 监控 Simple AD 目录
- 将 Amazon EC2 实例加入您的 Simple AD 活动目录
- 维护 Simple AD 目录
- 允许访问 AWS 应用程序和服务
- 允许使用 AD 凭证访问 AWS Management Console

在 Simple AD 中管理用户和组

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。

要在 AWS Directory Service 目录中创建用户和组，您必须使用已经加入 AWS Directory Service 目录的任意实例（来自本地或 EC2），并且已作为有权创建用户和组的用户登录。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 Amazon EC2 实例加入您的 Simple AD 活动目录。

> **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，请转到 Microsoft TechNet 上的预身份验证。

以下主题介绍了如何创建和管理用户和组。

主题

- 安装 Simple AD 的 Active Directory 管理工具
- 创建 Simple AD 用户
- 删除 Simple AD 用户
- 重置 Simple AD 用户密码
- 创建 Simple AD 群组
- 将 Simple AD 用户添加到群组

安装 Simple AD 的 Active Directory 管理工具

要通过 Amazon EC2 Windows Server 实例管理您的活动目录，您需要在该实例上安装 Active Directory 域服务和活动目录轻量级目录服务工具。使用以下过程在 EC2 Windows 服务器实例上安装这些工具。

先决条件

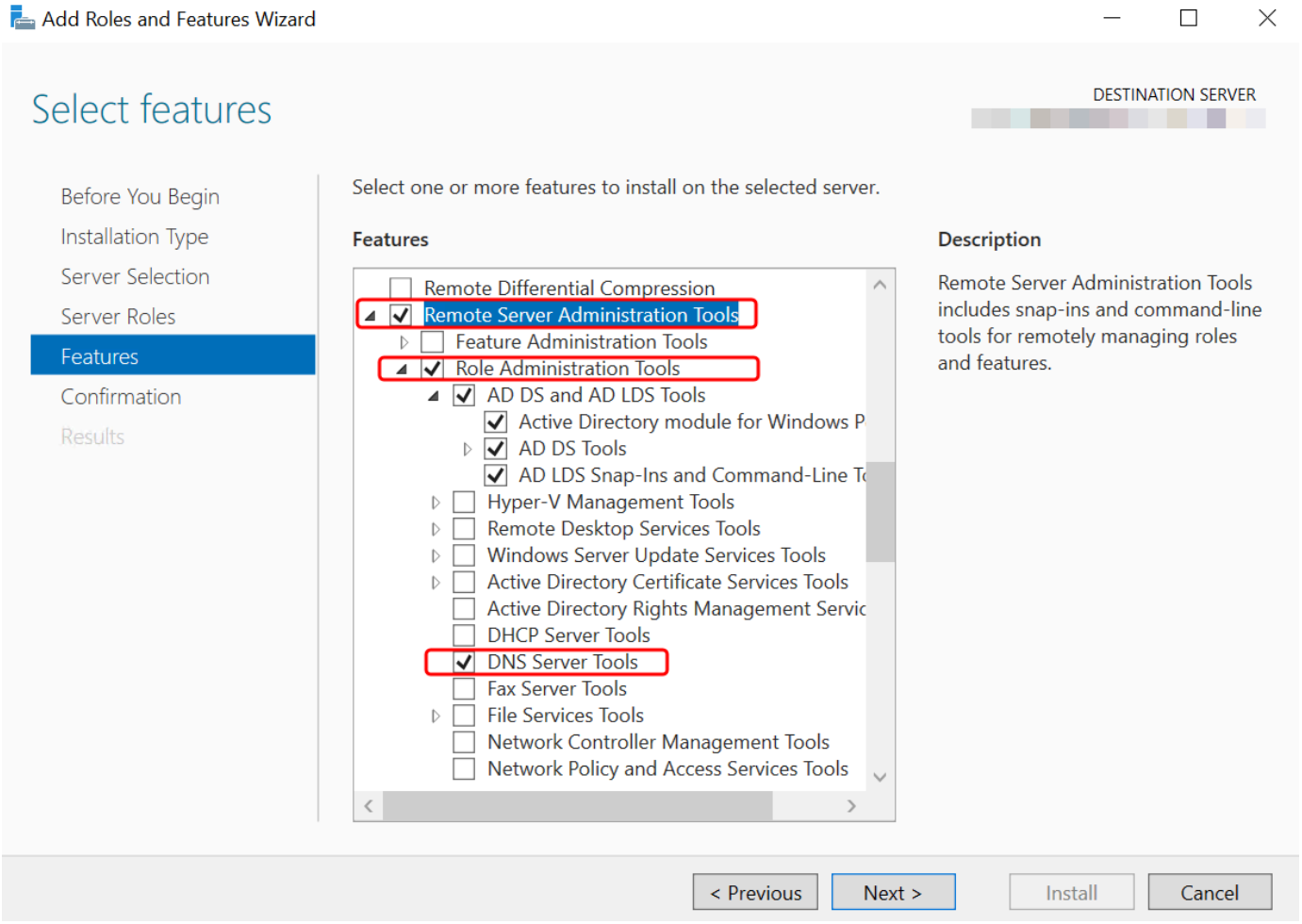
在开始此过程之前，请完成以下操作：

1. 创建一个 Simple AD 活动目录。有关更多信息，请参阅 制作你的 Simple AD Active Directory。
2. 启动 EC2 Windows Server 实例并将其加入到您的 Simple AD 活动目录。EC2 实例需要以下策略来创建用户和群组：**AWSSSMManagedInstanceCore**和**AmazonSSMDirectoryServiceAccess**。有关更多信息，请参阅 将 Amazon EC2 Windows 实例无缝加入你的 Simple AD 活动目录。
3. 您将需要您的活动目录域管理员的凭证。这些凭证是在创建 Simple AD 时创建的。如果您按照中的步骤操作制作你的 Simple AD Active Directory，则您的管理员用户名将包括您的 NetBIOS 名称。**corp\administrator**

在 EC2 Windows 服务器实例上安装 Active Directory 管理工具

在 EC2 Windows 服务器实例上安装 Active Directory 管理工具

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，选择实例，选择 Windows Server 实例，然后选择连接。
3. 在连接到实例页面中，选择 RDP 客户端。
4. 在 RDP 客户端选项卡中，选择下载远程桌面文件，然后选择获取密码，以检索密码。
5. 在获取 Windows 密码中，选择上传私钥文件。选择与 Windows Server 实例关联的 .pem 私钥文件。上传私钥文件后，选择解密密码。
6. 在 Windows 安全对话框中，复制 Windows 服务器计算机的本地管理员凭据进行登录。用户名可以采用以下格式：***NetBIOS-Name*\administrator**或***DNS-Name*\administrator**。例如，如果您按照中的步骤进行操作，则**corp\administrator**将是用户名制作你的 Simple AD Active Directory。
7. 登录 Windows Server 实例后，从 “开始” 菜单中选择 “服务器管理器”，打开 “服务器管理器”。
8. 在服务器管理器控制面板中，选择添加角色和功能。
9. 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)。
10. 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)。
11. 在功能树中，依次选择并打开远程服务器管理工具、角色管理工具和 AD DS 和 AD LDS 工具。选择 A D DS 和 AD LDS 工具后，将选择Active Directory模块Windows PowerShell、AD DS 工具、AD LDS 管理单元和命令行工具。向下滚动并选择 DNS 服务器工具，然后选择下一步。



12. 检查信息，然后选择安装。当该功能安装完成后，Active Directory 域服务工具和 Active Directory 轻量级目录服务工具将出现在“开始”菜单的管理工具文件夹中。

在 EC2 Windows 服务器实例上安装 Active Directory 管理工具的替代方法

- 以下是安装 Active Directory 管理工具的另一种方法：
  - 您可以选择使用安装 Active Directory 管理工具Windows PowerShell。例如，您可以使用在 PowerShell 提示符下安装 Active Directory 远程管理工具`Install-WindowsFeature RSAT-ADDS`。有关更多信息，请参阅 Microsoft WindowsFeature 网站上的 “安装-”。

创建 Simple AD 用户

使用以下过程创建具有已加入您的 Simple AD 目录的 Amazon EC2 实例的用户。在创建用户之前，您需要完成安装 Active Directory 管理工具中的过程。

> **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 kpasswd 首次更改其密码。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。

您可以使用以下任何一种方法来创建用户：

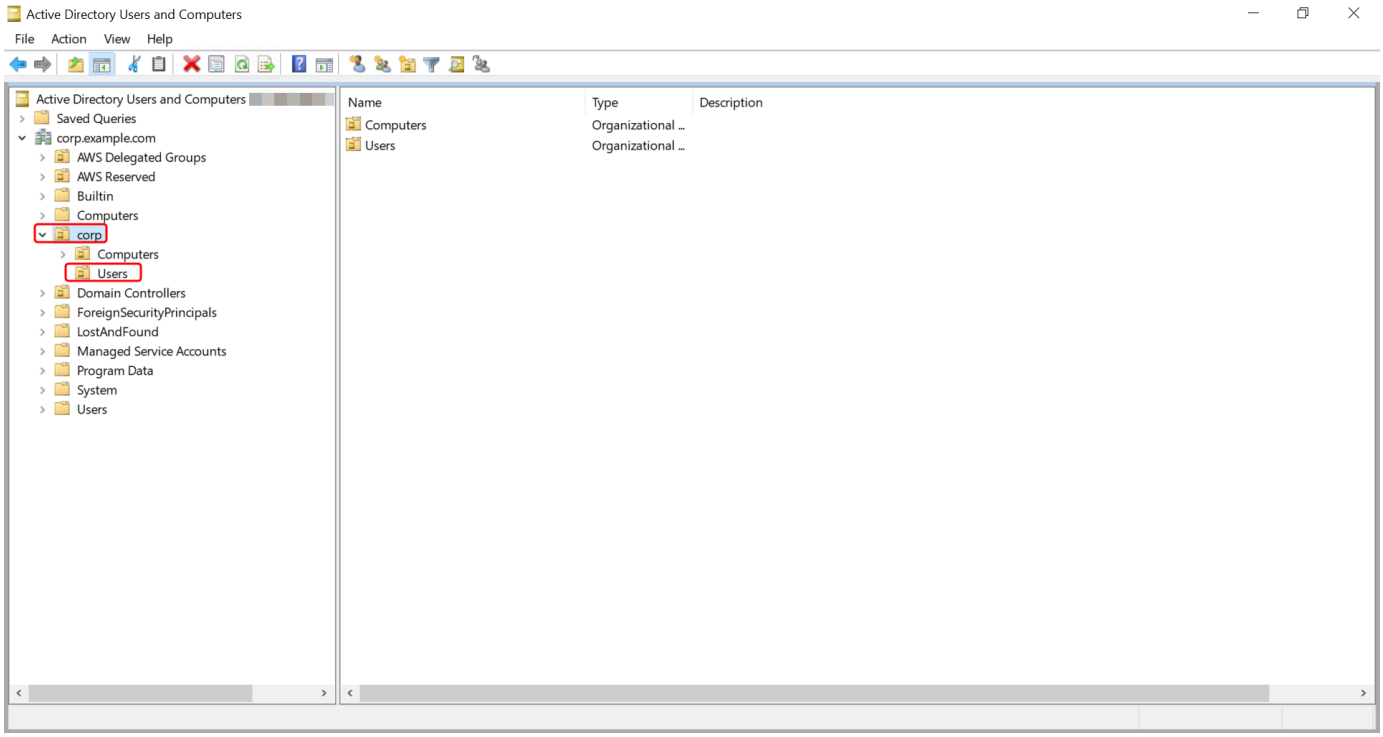
- Active Directory管理工具
- Windows PowerShell

使用Active Directory管理工具创建用户

1. 连接到安装了 Active Directory 管理工具的实例。
2. 从 Windows 的 “开始” 菜单中打开 Active Directory 用户和计算机工具。在 Windows 管理工具文件夹中可以找到此工具的快捷方式。

   > **Tip**
   >
   > 您可以通过实例上的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
   > ```

3. 在目录树中，在目录的 NetBIOS 名称 OU 下选择要存储用户的 OU（例如）。**corp\Users**有关中目录使用的 OU 结构的更多信息 AWS，请参阅用你的 AWS 托管 Microsoft AD 活动目录创建了什么。



4. 在操作 菜单上，选择新建，然后选择用户打开新用户向导。
5. 在向导的第一页上，输入以下字段的值，然后选择下一步。
   - 名
   - 姓
   - User logon name
6. 在新用户向导的第二页上，为密码和确认密码输入临时密码。确保选中了用户下次登录时必须更改密码选项。不应选择任何其他选项。选择下一步。
7. 在新用户向导的第三页上，验证新用户的信息正确无误，然后选择完成。新用户会出现在 Users 文件夹中。

在中创建用户 Windows PowerShell

1. 以Active Directory管理员身份连接到已加入您Active Directory域的实例。
2. 打开 Windows PowerShell。
3. 键入以下命令，将用户名**`jane.doe`**替换为要创建的用户的用户名。系统将提示您为Windows PowerShell新用户提供密码。有关Active Directory密码复杂性要求的更多信息，请参阅Microsoft文档。有关 new-aduser 命令的更多信息，请参阅文档。Microsoft

```
New-ADUser -Name "jane.doe" -Enabled $true -AccountPassword (Read-Host -AsSecureString
 'Password')
```

删除 Simple AD 用户

使用以下过程删除已加入您的 Simple AD 目录的 Amazon EC2 Windows 实例的用户。

您可以使用以下任何一种方法来删除用户：

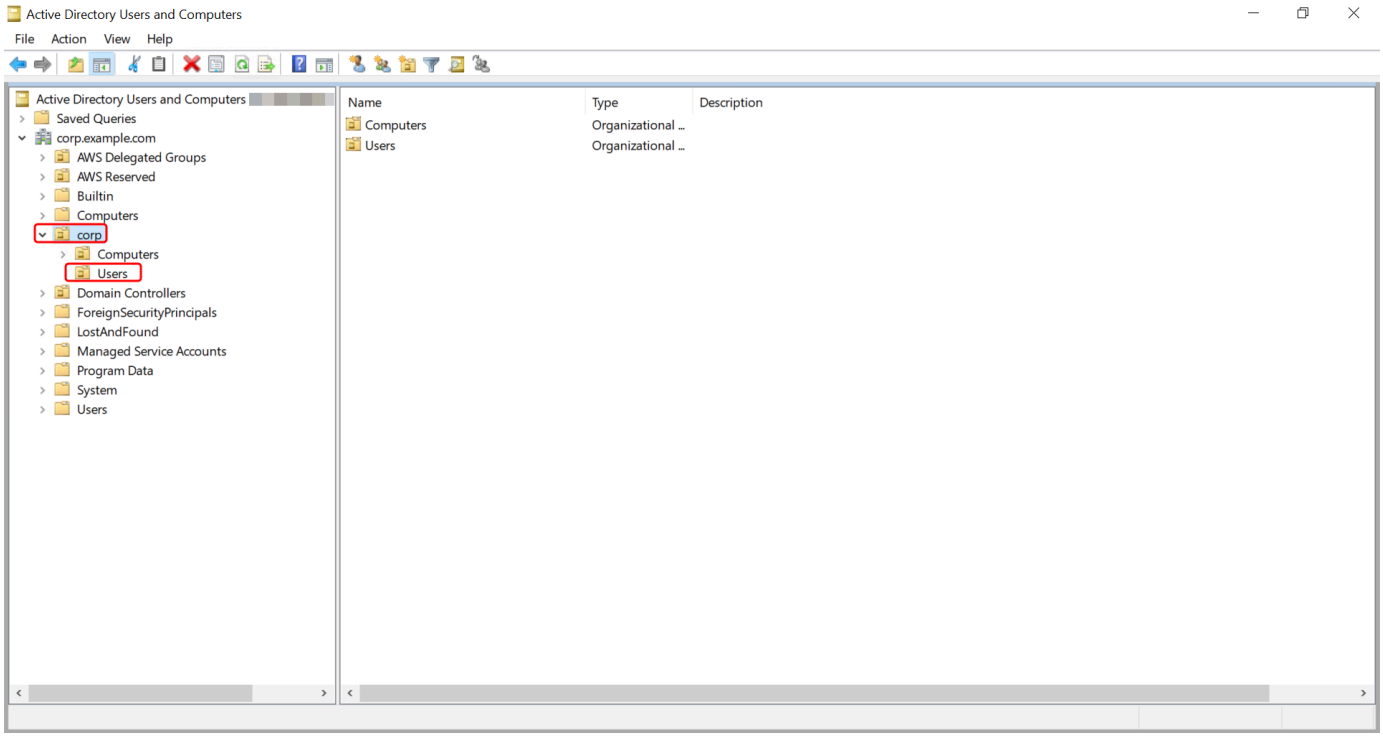
- Active Directory管理工具
- Windows PowerShell

使用Active Directory管理工具删除用户

1. 连接到安装了 Active Directory 管理工具的实例。
2. 从 Windows 的 “开始” 菜单中打开 Active Directory 用户和计算机工具。在 Windows 管理工具文件夹中可以找到此工具的快捷方式。

   > **Tip**
   >
   > 您可以通过实例上的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
   > ```

3. 在目录树中，选择包含要删除的用户的 OU（例如**corp\Users**）。



4. 选择要删除的用户。在操作 菜单上，选择删除。
5. 将出现一个对话框，提示您确认要删除该用户。选择是以删除该用户。此操作将永久删除所选用户。

删除中的用户 Windows PowerShell

1. 以Active Directory管理员身份连接到已加入您Active Directory域的实例。
2. 打开 Windows PowerShell。
3. 键入以下命令，将用户名**jane.doe**替换为要删除的用户的用户名。有关 Remove-aduser 命令的更多信息，请参阅文档。Microsoft

```
Remove-ADUser -Identity "jane.doe"
```

重置 Simple AD 用户密码

用户必须遵守中定义的密码策略Active Directory。有时，这可以充分利用用户（包括Active Directory管理员），而他们却忘记了自己的密码。发生这种情况时， AWS Directory Service 如果用户居住在 Simple AD 中，则可以使用快速重置用户的密码。

您必须以具有必要权限的用户身份登录才能重置密码。有关权限的更多信息，请参阅管理 AWS Directory Service 资源访问权限概述。

您可以为自己的任何用户重置密码Active Directory，但以下情况除外：

- 您可以根据您在创建组织单位 (OU) 时使用的 NetBIOS 名称重置任何用户的密码。Active Directory 例如，如果您按照中的制作你的 Simple AD Active Directory步骤操作，则您的 NetBIOS 名称将为 CORP，而您可以重置的用户密码将是 Corp/Users OU 的成员。
- 您不能根据您在创建 NetBIOS 名称时使用的 NetBIOS 名称重置 OU 以外的任何用户的密码。Active Directory有关 Simple AD 的 OU 结构的更多信息，请参阅用你的 Simple AD 创作了什么 Active Directory。
- 您不能为属于两个域的任何用户重置密码。除管理员用户外，您也无法重置任何属于域管理员或企业管理员组成员的用户的密码。
- 除了管理员用户之外，您无法重置任何属于域管理员或企业管理员组成员的用户的密码。

您可以使用以下任何一种方法来重置用户密码：

- AWS Management Console
- AWS CLI
- Windows PowerShell

在中重置用户密码 AWS Management Console

1. 在AWS Directory Service 控制台导航窗格中 Active Directory，选择目录，然后Active Directory在列表中选择要重置用户密码的目录。
2. 在目录详细信息页面上，选择操作，然后选择重置密码。
3. 在 “重置用户密码” 对话框中，在 “用户名” 中键入需要更改密码的用户的用户名。
4. 在新密码和确认密码中键入密码，然后选择重置密码。

在中重置用户密码 AWS CLI

1. 要安装 AWS CLI，请参阅安装或更新最新版本的 AWS CLI。
2. 打开 AWS CLI.
3. 键入以下命令并将目录 ID **jane.doe**、用户名和密码**P@ssw0rd**替换为您的Active Directory目录 ID 和所需的凭据。有关更多信息 reset-user-password，请参阅《AWS CLI 命令参考》中的。

```
aws ds reset-user-password --directory-id d-1234567890 --user-name "jane.doe" --new-
password "P@ssw0rd"
```

在中重置用户密码 Windows PowerShell

1. 以Active Directory管理员身份连接到已加入您Active Directory域的实例。
2. 打开 Windows PowerShell。
3. 键入以下命令，将用户名**jane.doe**、目录 ID 和密码**P@ssw0rd**替换为您的Active Directory目录 ID 和所需的凭据。有关更多信息，请参阅 reset-ds UserPassword Cmdlet。

```
Reset-DSUserPassword -UserName "jane.doe" -DirectoryId d-1234567890 -NewPassword
 "P@ssw0rd"
```

创建 Simple AD 群组

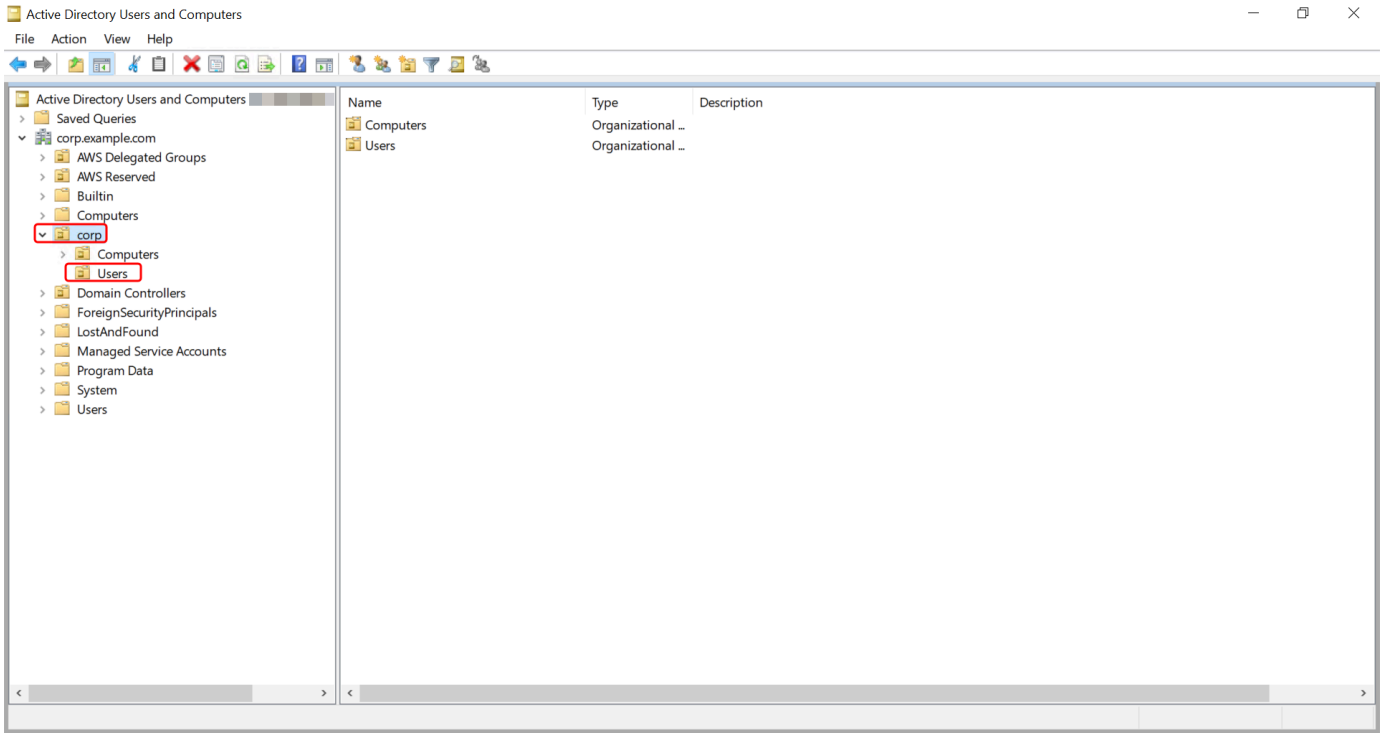
使用以下过程创建包含已加入您的 Simple AD 目录的 Amazon EC2 实例的安全组。在创建安全组之前，您需要完成安装 Active Directory 管理工具中的过程。

创建组

1. 连接到安装了 Active Directory 管理工具的实例。
2. 打开“Active Directory 用户和计算机”工具。管理工具文件夹中有一个该工具的快捷方式。

> **Tip**
>
> 您可以通过实例上的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
> ```

3. 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）。有关中目录使用的 OU 结构的更多信息 AWS，请参阅用你的 AWS 托管 Microsoft AD 活动目录创建了什么。



4. 在 Action 菜单上，单击 New，然后单击 Group 打开新组向导。
5. 在组名称中键入组名称，选择满足您需求组范围，然后为组类型选择安全。有关 Active Directory 组范围和安全组的更多信息，请参阅 Microsoft Windows Server 文档中的 Active Directory 安全组。
6. 单击 确定。新安全组会出现在用户文件夹中。

将 Simple AD 用户添加到群组

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。

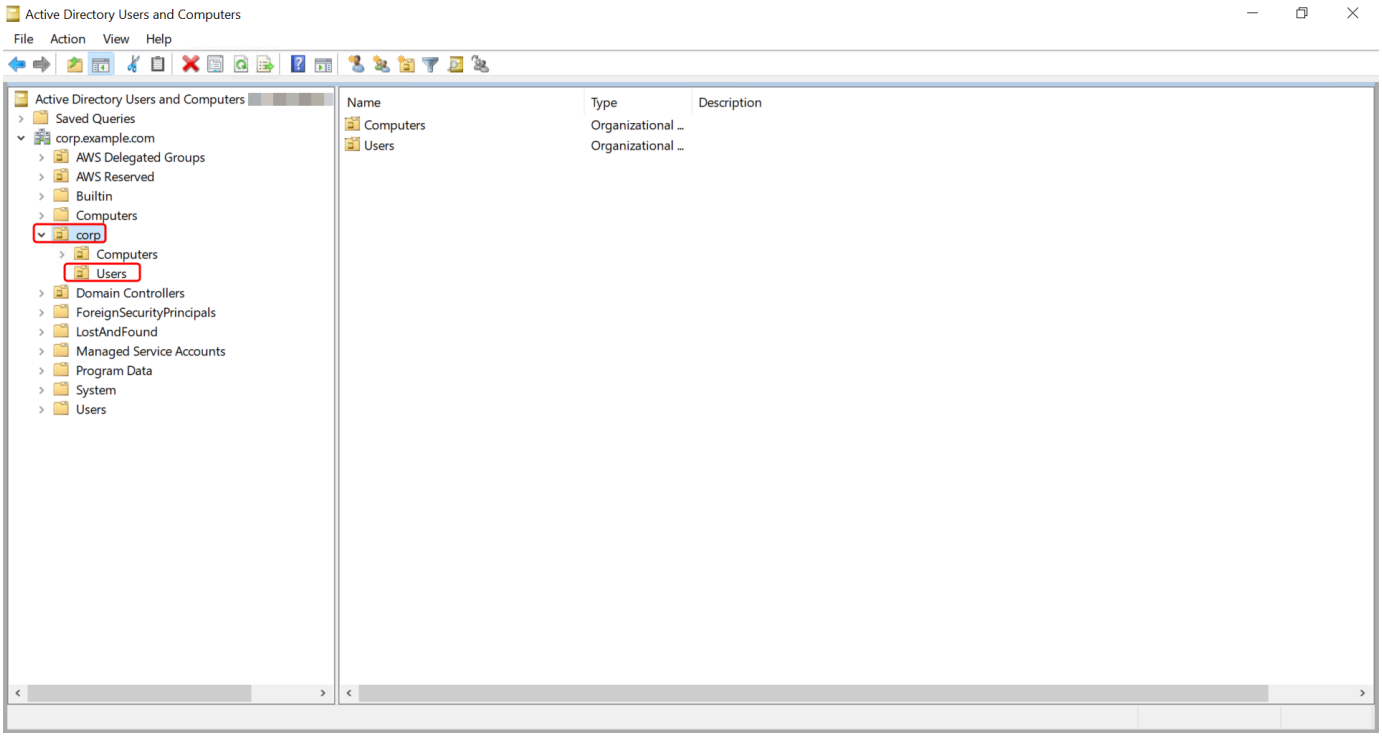
如何为群组添加用户

1. 连接到安装了 Active Directory 管理工具的实例。
2. 打开“Active Directory 用户和计算机”工具。管理工具文件夹中有一个该工具的快捷方式。

> **Tip**
>
> 您可以通过实例上的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
```

3. 在目录树中，选择存储组的目录 NetBIOS 名称 OU 下的 OU，然后选择要添加用户为成员的组。



4. 在操作菜单上，单击属性打开组的属性对话框。
5. 选择成员选项卡并单击添加。
6. 在 “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”。该名称将显示在成员列表中。再次单击 OK 更新组成员资格。
7. 通过在用户文件夹中选择用户，然后单击操作菜单中的属性打开属性对话框，验证该用户现在是否是组的成员。选择成员选项卡。您应该可以在用户所属的组列表中看到组的名称。

监控 Simple AD 目录

您可以通过以下方法监控 Simple AD 目录：

主题

- 了解目录状态
- 使用 Amazon SNS 配置目录状态通知

了解目录状态

以下是目录的各种状态。

处于活动状态

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

Creating

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

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。如果问题仍存在，请联系 AWS Support 中心。

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，请参阅微软 AD AWS 托管故障排除、AD Connector 故障排除、Simple AD 问题排查。对于与正常维护相关的问题， AWS 可在 40 分钟内解决这些问题。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 AWS Support 中心。

> **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 为目录拍摄快照或还原目录。

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

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 AWS Support 中心。

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。

使用 Amazon SNS 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“活动”状态变为“受损”或“不可操作”状态，您将收到通知。当目录恢复为“活动”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用户，他们接收发布至该主题的消息。按照以下步骤，您可以在 Amazon SNS 主题中添加 AWS Directory Service 出版商身份。当 AWS Directory Service 检测到您的目录状态发生变化时，它会向该主题发布一条消息，然后将其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 AWS Management Console 并打开AWS Directory Service 控制台。
2. 在目录页面上，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，然后选择创建通知。
5. 在创建通知页面上，选择选择通知类型，然后选择创建新通知。或者，如果您现在已有一个 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**
>
> 如果您选择创建新通知，但之后使用与现有 SNS 主题相同的主题名称，则 Amazon SNS 不会创建新主题，只是向现有主题添加新的订阅信息。
> 如果您选择关联现有 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，然后输入收件人联系信息。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）为主题和 SNS 显示名称提供名称。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**
>
> 如果您使用只有DirectoryServiceFullAccess托管策略的 IAM 用户或角色登录，则您的主题名称必须以 “DirectoryMonitoring” 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。

如果您想指定其他 SNS 订阅者，例如额外的电子邮件地址、Amazon SQS 队列 AWS Lambda或，则可以从 Amazon SNS 控制台执行此操作。

从主题移除目录状态消息

1. 登录 AWS Management Console 并打开AWS Directory Service 控制台。
2. 在目录页面上，选择您的目录 ID。
3. 选择维护选项卡。
4. 在目录监控部分，在列表中选择一个 SNS 主题名称，选择操作，然后选择移除。
5. 选择移除。

这会移除您目录的选定 SNS 主题发布者身份。如果您想删除整个主题，可以从 Amazon SNS 控制台执行此操作。

> **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，在删除任何从中 AWS Directory Service接收消息的主题之前，请将您的目录与其他 Amazon SNS 主题相关联。

将 Amazon EC2 实例加入您的 Simple AD 活动目录

当 Amazon EC2 实例启动时，您可以将该实例无缝加入您的Active Directory域。有关更多信息，请参阅 将亚马逊 EC2 Windows 实例无缝加入你的 AWS 托管微软 AD Active Directory。您还可以使用 A AWS Systems Manager ut omation 直接从 AWS Directory Service 控制台启动 EC2 实例并将其加入 Active Directory域。

如果您需要手动将 EC2 实例加入您的Active Directory域，则必须在相应的区域和安全组或子网中启动该实例，然后将该实例加入域。

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，这要求互联网网关连接到 VPC，并且实例具有公有 IP 地址。

主题

- 将 Amazon EC2 Windows 实例无缝加入你的 Simple AD 活动目录
- 手动将 Amazon EC2 Windows 实例加入你的 Simple AD 活动目录
- 将 Amazon EC2 Linux 实例无缝加入你的 Simple AD 活动目录
- 手动将 Amazon EC2 Linux 实例加入您的 Simple AD 活动目录
- 委托 Simple AD 的目录加入权限
- 创建 DHCP 选项集

将 Amazon EC2 Windows 实例无缝加入你的 Simple AD 活动目录

此过程将 Amazon EC2 Windows 实例无缝连接到您的 Simple AD 活动目录。

无缝加入 EC2 Windows 实例

1. 登录 AWS Management Console 并打开亚马逊 EC2 控制台，网址为 https://console.aws.amazon.com/ec2/。
2. 在导航栏中，选择与现有目录 AWS 区域 相同的目录。
3. 在 EC2 控制面板的启动实例部分，选择启动实例。
4. 在启动实例页面的名称和标签部分下，输入您要用于 Windows EC2 实例的名称。
5. （可选）选择添加其他标签，添加一个或多个标签密钥值对，以组织、跟踪或控制对此 EC2 实例的访问权限。
6. 在应用程序和操作系统映像（亚马逊机器映像）部分，在快速入门窗格中选择 Windows。您可以从亚马逊机器映像（AMI）下拉列表中更改 Windows 亚马逊机器映像（AMI）。
7. 在实例类型部分，从实例类型下拉列表中选择要使用的实例类型。
8. 在密钥对（登录）部分，您可以选择创建新密钥对，或从现有密钥对中进行选择。

   a. 要创建新的密钥对，请选择新建新密钥对。
   b. 输入密钥对的名称，然后为密钥对类型和私钥文件格式选择一个选项。
   c. 要以可与 OpenSSH 一起使用的格式保存私钥，请选择 pem。要以可与 PuTTY 一起使用的格式保存私钥，请选择 ppk。
   d. 选择创建密钥对。
   e. 您的浏览器会自动下载私有密钥文件。将私有密钥文件保存在安全位置。

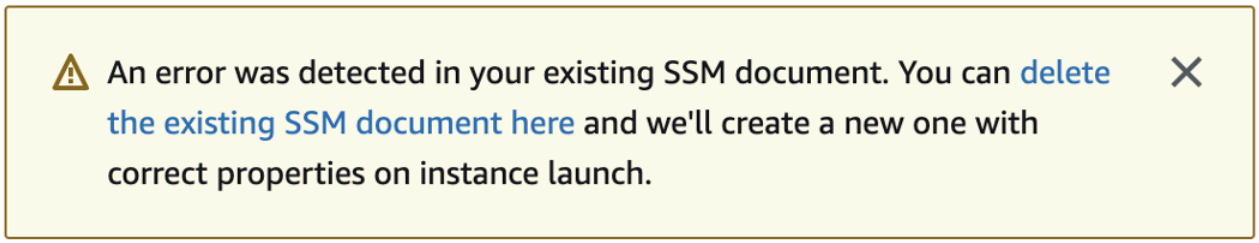
   > **Important**
   >
   > 这是您保存私有密钥文件的唯一机会。

9. 在启动实例页面的网络设置部分下，选择编辑。从 VPC – 必需下拉列表中选择创建目录的 VPC。
10. 从子网下拉列表中选择 VPC 中的其中一个公有子网。选择的子网必须将所有外部流量都路由到互联网网关。否则将无法远程连接到实例。

    有关如何连接到互联网网关的更多信息，请参阅《Amazon VPC 用户指南》中的使用互联网网关连接到互联网。
11. 在自动分配公有 IP 下，选择启用。

    有关公有和私有 IP 寻址的更多信息，请参阅《亚马逊 EC2 用户指南》中的 Amazon EC2 实例 IP 寻址。
12. 对于防火墙（安全组）设置，您可以使用默认设置或进行更改以满足您的需求。
13. 对于配置存储设置，您可以使用默认设置或进行更改以满足您的需求。

14. 选择高级详细信息部分，从域加入目录下拉列表中选择您的域。

> **Note**
>
> 选择域加入目录后，您可能会看到：
>
> 
>
>
> 如果 EC2 启动向导识别出具有意外属性的现有 SSM 文档，则会发生此错误。您可以执行以下操作之一：
>
> - 如果您之前编辑了 SSM 文档并且属性符合预期，请选择关闭并继续启动 EC2 实例，不做任何更改。
> - 选择 “在此处删除现有 SSM 文档” 链接以删除 SSM 文档。这将允许创建具有正确属性的 SSM 文档。SSM 文档将在您启动 EC2 实例时自动创建。

15. 对于 IAM 实例配置文件，您可以选择现有的 IAM 实例配置文件或创建新的 IAM 实例配置文件。从 IAM 实例配置文件下拉列表中选择一个DirectoryServiceAccess附有 AWS 托管策略 AmazonSSMManagedInstanceCore 和 AmazonSSM 的 IAM 实例配置文件。要创建新的 IAM 个人资料链接，请选择创建新的 IAM 个人资料链接，然后执行以下操作：

    1. 选择 创建角色。
    2. 在选择受信任的实体下，选择 AWS 服务。
    3. 在 Use case（使用案例）下，选择 EC2。
    4. 在 “添加权限” 下的策略列表中，选择 AmazonSSM ManagedInstanceCore 和 AmazonSSM 政策。DirectoryServiceAccess在搜索框中键入 **SSM** 以筛选列表。选择下一步。

    > **Note**
    >
    > AmazonSSM DirectoryServiceAccess 提供了将实例加入Active Directory托管者的权限。 AWS Directory ServiceAmazonSSM ManagedInstanceCore 提供使用该服务所需的最低权限。 AWS Systems Manager 有关创建具有这些权限的角色的更多信息，以及您可以分配给 IAM 角色的其他权限和策略的信息，请参阅《AWS Systems Manager 用户指南》中的为 Systems Manager 创建 IAM 实例配置文件。

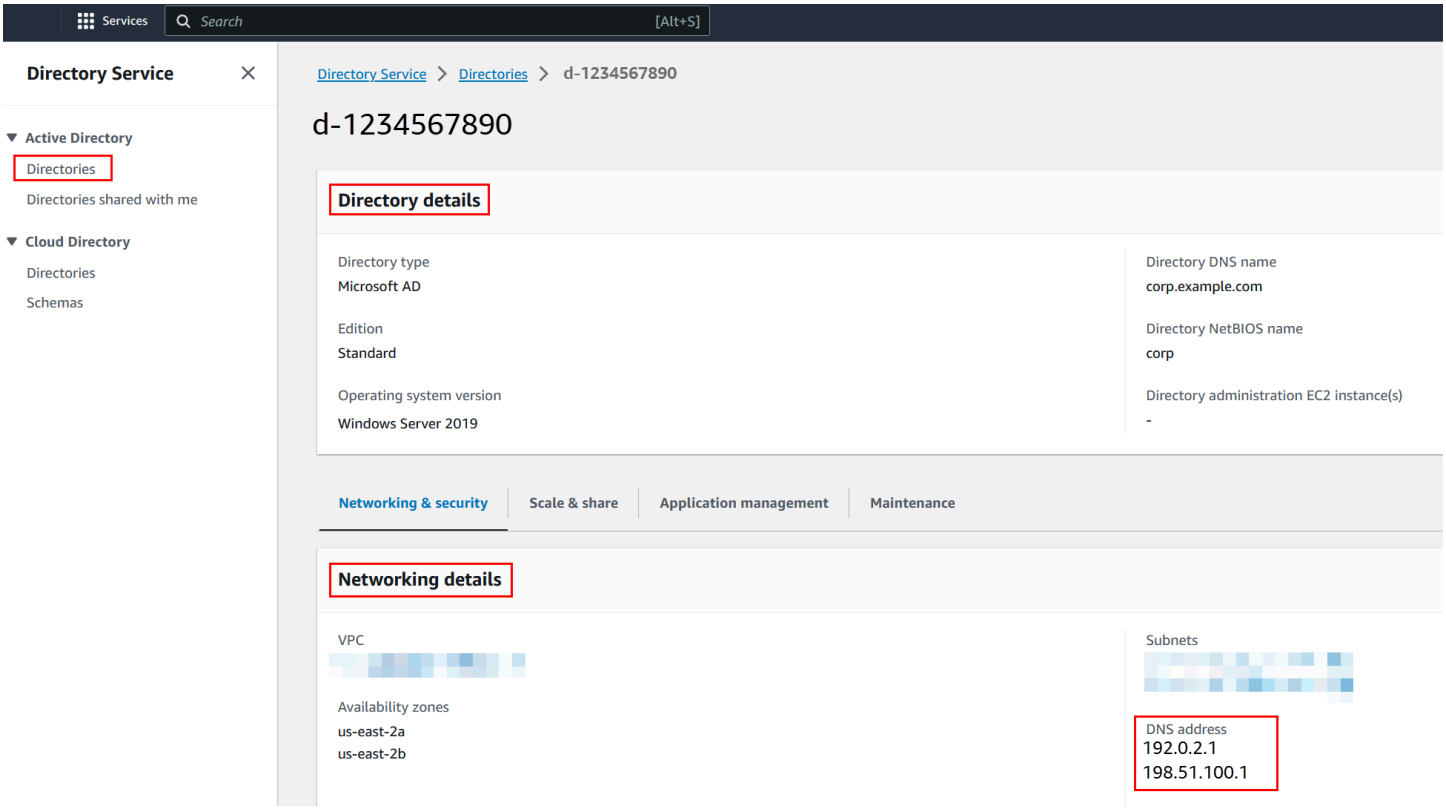
5. 在名称、查看和创建页面上，输入角色名称。您将需要此角色名称来附加到 EC2 实例。
6. （可选）您可以在描述字段中提供 IAM 实例配置文件的描述。
7. 选择 创建角色。
8. 返回启动实例页面，选择 IAM 实例配置文件旁边的刷新图标。您的新 IAM 实例配置文件应显示在 IAM 实例配置文件下拉列表中。选择新的配置文件，其余设置保留默认值。

16. 选择启动实例。

手动将 Amazon EC2 Windows 实例加入你的 Simple AD 活动目录

要手动将现有 Amazon EC2 Windows 实例加入简单的 AD 活动目录，必须使用中指定的参数启动该实例[将 Amazon EC2 Windows 实例无缝加入你的 Simple AD 活动目录](#)。

您将需要 Simple AD DNS 服务器的 IP 地址。此信息可以在目录服务 > 目录 > 目录的目录 ID 链接 > 目录详细信息以及网络与安全下找到。



将 Windows 实例加入 Simple AD 活动目录

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。

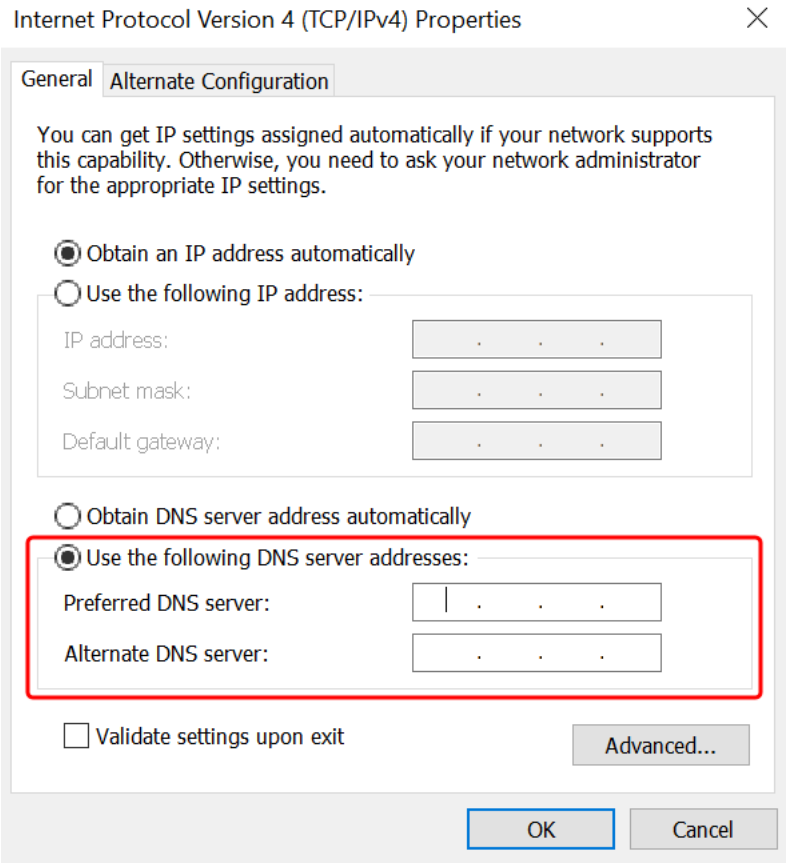
a. 打开 Network Connections。

> **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. 选择 “使用以下 DNS 服务器地址”，将 “首选 DNS 服务器” 和 “备用 DNS 服务器地址” 更改为 Simple AD 提供的 DNS 服务器的 IP 地址，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” 字段中，选择 “域”，输入 Simple AD Active Directory 的完全限定名称，然后选择 “确定”。
6. 当系统提示输入域管理员的用户名和密码时，请输入具有域加入权限的帐户的用户名和密码。有关委托这些权限的更多信息，请参阅委托 Simple AD 的目录加入权限。

> **Note**
>
> 您可以输入域的完全限定名称或 NetBIOS 名称，后跟反斜杠 (\)，然后输入用户名。用户名应为 “管理员”。例如，**corp.example.com\administrator** 或 **corp\administrator**。

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，您的实例已加入 Simple AD Active Directory 域，您可以远程登录该实例并安装用于管理该目录的实用程序，例如添加用户和组。Active Directory 管理工具可用于创建用户和群组。有关更多信息，请参阅 安装 Simple AD 的 Active Directory 管理工具。

将 Amazon EC2 Linux 实例无缝加入你的 Simple AD 活动目录

此过程将 Amazon EC2 Linux 实例无缝连接到您的 Simple AD 活动目录。

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 Red Hat Enterprise 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 实例之前，您需要完成本节中的步骤。

选择无缝域名加入服务账户

您可以将 Linux 计算机无缝加入 Simple AD 域。要执行此操作，您必须创建一个具有创建计算机账户权限的用户账户，才能将计算机加入域。尽管域管理员或其他组的成员可能有足够的权限将计算机加入域，但我们不建议使用此角色。作为最佳实践，我们建议您使用具有将计算机加入域所需最低权限的服务账户。

有关如何处理并委托权限到服务账户委托权限以创建计算机账户的信息，请参阅 向您的服务账户委派权限。

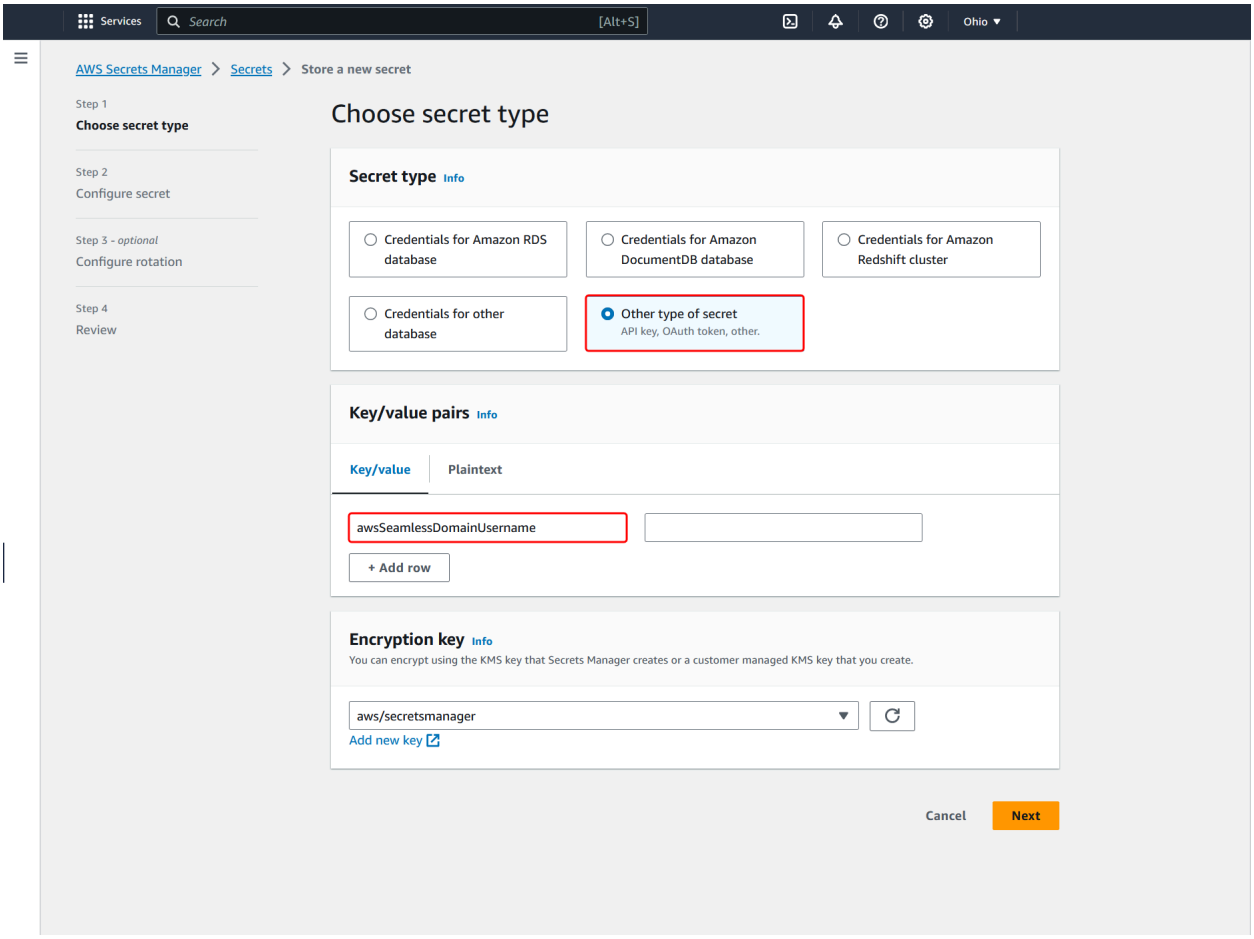
创建密钥以存储域服务账户

您可以使用 AWS Secrets Manager 存储域名服务帐户。

创建密钥并存储域服务账户信息

1. 登录 AWS Management Console 并打开 AWS Secrets Manager 控制台，网址为 https://console.aws.amazon.com/secretsmanager/。
2. 选择 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. 在密钥类型下，选择其他密钥类型。
   b. 在 “键/值对” 下，执行以下操作：
      i. 在第一个框中，输入 **awsSeamlessDomainUsername**。在同一行的下一个框中，输入您的服务帐号的用户名。例如，如果您之前使用过该 PowerShell 命令，则服务帐户名称将为**awsSeamlessDomain**。

> **Note**
>
> 必须完全按照原样输入 **awsSeamlessDomainUsername**。确保前后均没有任何空格。否则，域加入将失败。



ii. 选择添加行。

iii. 在新行的第一个框中输入 **awsSeamlessDomainPassword**。在同一行的下一个框中，输入服务账户密码。

> **Note**
>
> 必须完全按照原样输入 **awsSeamlessDomainPassword**。确保前后均没有任何空格。否则，域加入将失败。

iv. 在“加密密钥”下，保留默认值`aws/secretsmanager`。 AWS Secrets Manager 选择此选项时，始终会加密密钥。您也可以选择您创建的密钥。

> **Note**
>
> 根据您使用的密钥 AWS Secrets Manager，会收取相关费用。有关当前完整定价列表，请参阅 AWS Secrets Manager 定价。

你可以使用 Secrets Manager 创建`aws/secretsmanager`的 AWS 托管密钥来免费加密你的秘密。如果您创建自己的 KMS 密钥来加密您的机密，则按当前费 AWS KMS 率向您 AWS 收费。有关更多信息，请参阅AWS Key Management Service 定价。

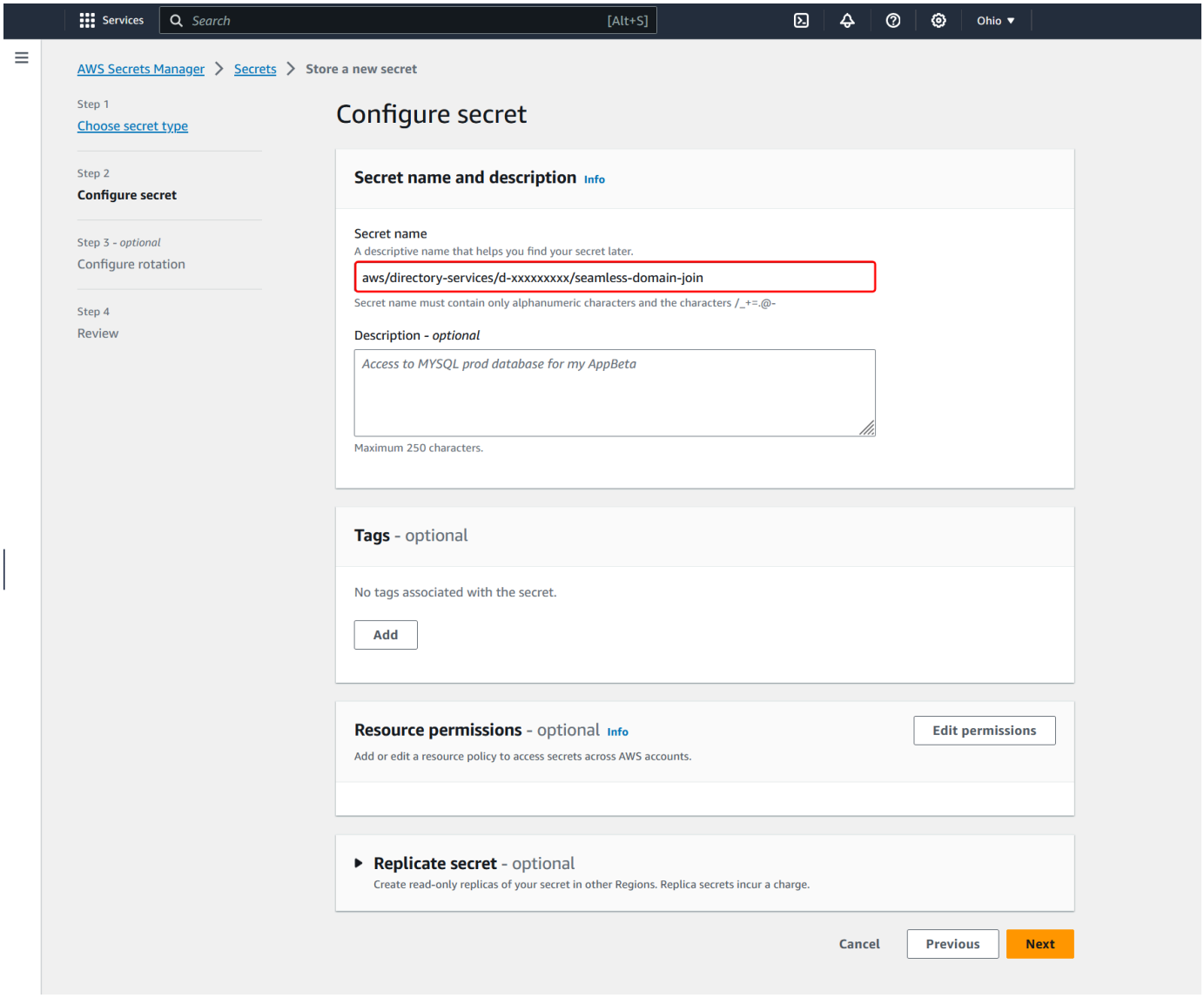
v. 选择下一步。

4. 在“密钥名称”下，使用以下格式输入包含您的目录 ID 的机密名称，将 *d-xxxxxxxxxx* 替换为您的目录 ID：

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

这将用于检索应用程序中的密钥。

> **Note**
>
> 您必须完全按照原样输入 **aws/directory-services/*d-xxxxxxxxx*/seamless-domain-join**，但请将 *d-xxxxxxxxxx* 替换为您的目录 ID。确保前后均没有空格。否则，域加入将失败。



5. 将其他所有内容都设置为默认值，然后选择下一步。
6. 在配置自动轮换下，选择禁用自动轮换，然后选择下一步。

   存储此密钥后，您可以为其开启轮换功能。
7. 查看设置，然后选择存储以保存更改。Secrets Manager 控制台将返回您账户中的密钥列表，并且列表中现在包含新的密钥。
8. 从列表中选择您新创建的密钥名称，并记下密钥 ARN 值。您需要在下一部分中使用该名称。

启用域名服务账户密钥的轮换

我们建议您定期轮换密钥以改善您的安全状况。

启用域名服务账户密钥的轮换

- 按照《AWS Secrets Manager 用户指南》中为 AWS Secrets Manager 密钥设置自动轮换中的说明进行操作。

  对于步骤 5，使用AWS Secrets Manager 用户指南中的轮换模板 Microsoft Active Directory 凭据。

  如需帮助，请参阅《AWS Secrets Manager 用户指南》中的AWS Secrets Manager 轮换疑难解答。

创建所需 IAM policy 和角色

使用以下先决条件步骤创建自定义策略，该策略允许对您的 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 LinuxEC2 DomainJoin IAM 角色。

创建 Secrets Manager IAM 读取策略

您可以使用 IAM 控制台创建策略，授予对 Secrets Manager 密钥的只读访问权限。

创建 Secrets Manager IAM 读取策略

1. 以有权创建 IAM 策略的用户 AWS Management Console 身份登录。然后通过以下网址打开 IAM 控制台：https://console.aws.amazon.com/iam/。
2. 在导航窗格的 “访问管理” 中，选择 “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 文本框中。

> **Note**
>
> 请务必将区域和资源 ARN 替换为之前创建的密钥的实际区域和资源 ARN。

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

```
                "secretsmanager:GetSecretValue",
                "secretsmanager:DescribeSecret"
            ],
            "Resource": [
                "arn:aws:secretsmanager:us-east-1:xxxxxxxxx:secret:aws/directory-
services/d-xxxxxxxxx/seamless-domain-join"
            ]
        }
    ]
}
```

5. 完成后，选择下一步。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 policy。
6. 在检查策略页面上，输入一个策略名称，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。选择创建策略，保存更改。托管策略列表中将显示新策略，并且现在已准备好附加到身份中。

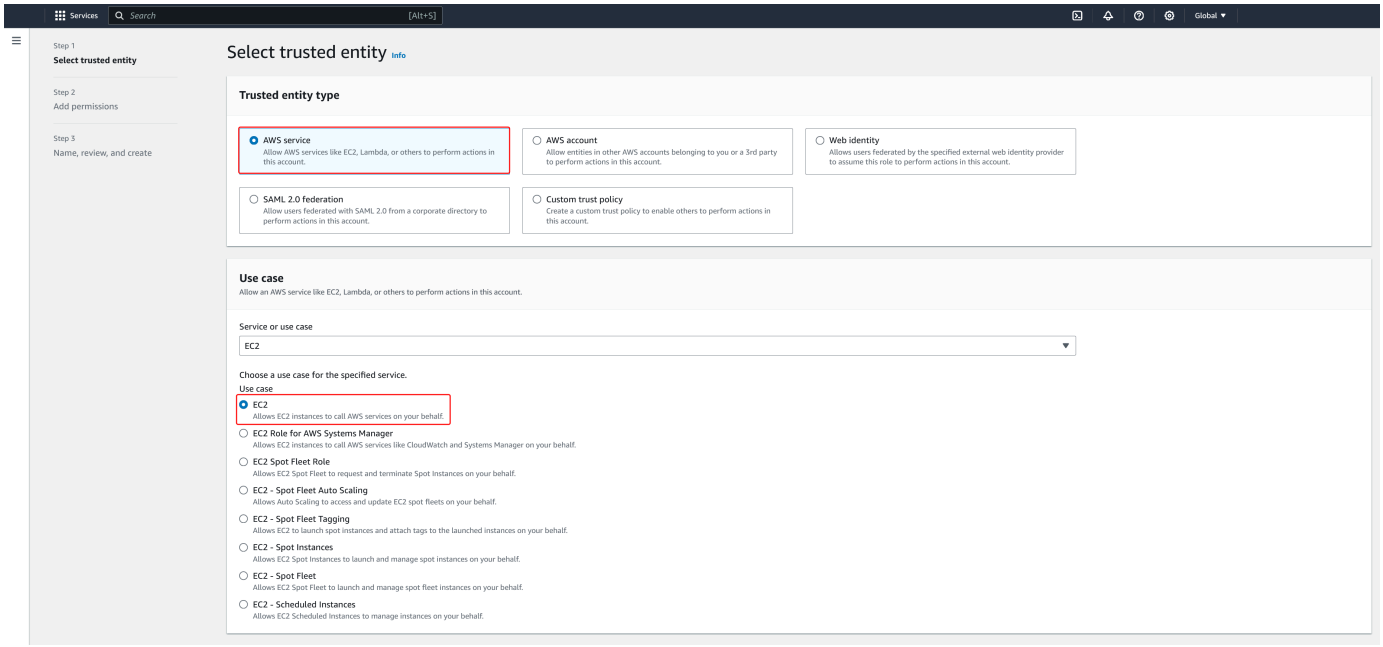
> **Note**
>
> 我们建议您为每个密钥创建一个策略。这样做可以确保实例只能访问相应的密钥，并在实例受损时将影响降至最低。

创建 LinuxEC2 角色 DomainJoin

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 LinuxEC2 角色 DomainJoin

1. 以有权创建 IAM 策略的用户 AWS Management Console 身份登录。然后通过以下网址打开 IAM 控制台：https://console.aws.amazon.com/iam/。
2. 在导航窗格中的访问管理下，选择角色。
3. 在内容窗格中，选择创建角色。
4. 在选择受信任实体的类型下，选择 AWS 服务。
5. 在 “用例” 下，选择 EC2，然后选择 “下一步”。



6. 对于筛选策略，执行以下操作：

   a. 输入 **AmazonSSMManagedInstanceCore**。然后选择列表中该项目的复选框。

   b. 输入 **AmazonSSMDirectoryServiceAccess**。然后选择列表中该项目的复选框。

   c. 输入 **SM-Secret-Linux-DJ-*d-xxxxxxxxxx*-Read**（或您在上一过程中创建的策略名称）。然后选择列表中该项目的复选框。

   d. 添加上面列出的三个策略后，选择创建角色。

> **Note**
>
> AmazonSSM DirectoryServiceAccess 提供了将实例加入Active Directory托管者的权限。AWS Directory Service AmazonSSM ManagedInstanceCore 提供使用该服务所需的最低权限。 AWS Systems Manager 有关创建具有这些权限的角色的更多信息，以及您可以分配给 IAM 角色的其他权限和策略的信息，请参阅《AWS Systems Manager 用户指南》中的为 Systems Manager 创建 IAM 实例配置文件。

7. 在角色名称字段中输入新角色的名称，例如**LinuxEC2DomainJoin**或其他您喜欢的名称。
8. （可选）对于角色描述，请输入描述。
9. （可选）在 “步骤 3：添加标签” 下选择 “添加新标签” 以添加标签。标签键值对用于组织、跟踪或控制此角色的访问权限。
10. 选择 创建角色。

将 Linux 实例无缝加入你的 Simple AD 活动目录

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

无缝加入你的 Linux 实例

1. 登录 AWS Management Console 并打开亚马逊 EC2 控制台，网址为 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 AWS 区域 相同的目录。
3. 在 EC2 控制面板的启动实例部分，选择启动实例。
4. 在启动实例页面的名称和标签部分下，输入您要用于 Linux EC2 实例的名称。
5. （可选）选择添加其他标签，添加一个或多个标签密钥值对，以组织、跟踪或控制对此 EC2 实例的访问权限。
6. 在“应用程序和操作系统映像（Amazon 系统映像）”部分，选择要启动的 Linux AMI。

> **Note**
>
> 使用的 AMI 必须具有 AWS 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。如果您需要升级 SSM Agent，请参阅在适用于 Linux 的 EC2 实例上安装和配置 SSM Agent。
> SSM 在将 Linux 实例加入Active Directory域时使用该`aws:domainJoin`插件。该插件将 Linux 实例的主机名更改为 EC2AMAZ-*XXXXXX* X 格式。有关的更多信息`aws:domainJoin`，请参阅《AWS Systems Manager 用户指南》中的AWS Systems Manager 命令文档插件参考。

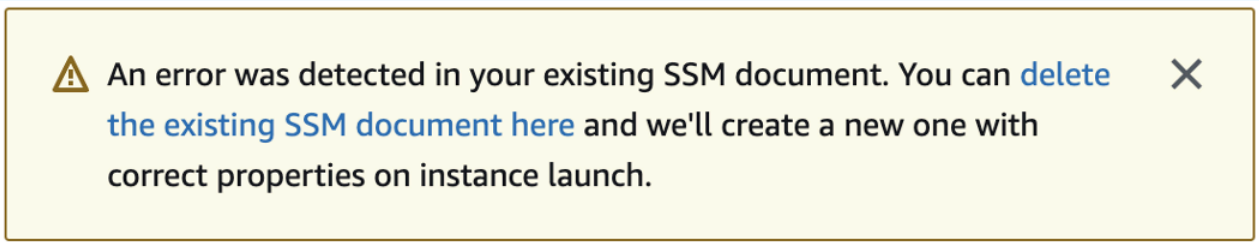
7. 在实例类型部分，从实例类型下拉列表中选择要使用的实例类型。
8. 在密钥对（登录）部分，您可以选择创建新密钥对，或从现有密钥对中进行选择。要创建新的密钥对，请选择新建新密钥对。输入密钥对的名称，然后为密钥对类型和私钥文件格式选择一个选项。要以可与 OpenSSH 一起使用的格式保存私钥，请选择 pem。要以可与 PuTTY 一起使用的格式保存私钥，请选择 ppk。选择创建密钥对。您的浏览器会自动下载私有密钥文件。将私有密钥文件保存在安全位置。

> **Important**
>
> 这是您保存私有密钥文件的唯一机会。

9. 在启动实例页面的网络设置部分下，选择编辑。从 VPC – 必需下拉列表中选择创建目录的 VPC。
10. 从子网下拉列表中选择 VPC 中的其中一个公有子网。选择的子网必须将所有外部流量都路由到互联网网关。否则将无法远程连接到实例。

    有关如何连接到互联网网关的更多信息，请参阅《Amazon VPC 用户指南》中的使用互联网网关连接到互联网。
11. 在自动分配公有 IP 下，选择启用。

    有关公有和私有 IP 寻址的更多信息，请参阅《亚马逊 EC2 用户指南》中的 Amazon EC2 实例 IP 寻址。
12. 对于防火墙（安全组）设置，您可以使用默认设置或进行更改以满足您的需求。
13. 对于配置存储设置，您可以使用默认设置或进行更改以满足您的需求。
14. 选择高级详细信息部分，从域加入目录下拉列表中选择您的域。

> **Note**
>
> 选择域加入目录后，您可能会看到：
>
> 
>
>
> 如果 EC2 启动向导识别出具有意外属性的现有 SSM 文档，则会发生此错误。您可以执行以下操作之一：
>
> - 如果您之前编辑了 SSM 文档并且属性符合预期，请选择关闭并继续启动 EC2 实例，不做任何更改。
> - 选择 “在此处删除现有 SSM 文档” 链接以删除 SSM 文档。这将允许创建具有正确属性的 SSM 文档。SSM 文档将在您启动 EC2 实例时自动创建。

15. 对于 IAM 实例配置文件，请选择您之前在先决条件部分步骤 2：创建 LinuxEC DomainJoin 2 角色中创建的 IAM 角色。
16. 选择启动实例。

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

手动将 Amazon EC2 Linux 实例加入您的 Simple AD 活动目录

除了亚马逊 EC2 Windows 实例外，您还可以将某些亚马逊 EC2 Linux 实例加入您的 Simple AD 活动目录。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）
- 亚马逊 Linux 2023 AMI
- 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。

先决条件

必须先按照 将 Amazon EC2 Linux 实例无缝加入你的 Simple AD 活动目录 中指定的步骤启动实例，然后才能将 Amazon Linux、CentOS、Red Hat 或 Ubuntu 实例加入目录。

> **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. 将 Linux 实例配置为使用 AWS Directory Service提供的 DNS 服务器的 DNS 服务器 IP 地址。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。如果要手动设置，请参阅 AWS 知识中心的如何为私有 EC2 实例分配静态 DNS 服务器，以了解有关为特定 Linux 分发版和版本设置持久性 DNS 服务器的指导。
3. 确保 64 位 Amazon Linux 实例为最新状态。

```
sudo yum -y update
```

4. 在 Linux 实例上安装所需的 Amazon Linux 软件包。

> **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

```
sudo yum install samba-common-tools realmd oddjob oddjob-mkhomedir sssd adcli
 krb5-workstation
```

> **Note**
>
> 有关确定您所使用的 Amazon Linux 版本的帮助，请参阅《Amazon EC2 用户指南（适用于 Linux 实例）》中的识别 Amazon Linux 映像。

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

example.com 域中具有域加入权限的账户。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，请参阅委托 AWS Managed Microsoft AD 的目录加入权限。

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 文件的底部并保存该文件。

   ```
   ## 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. 将 Linux 实例配置为使用 AWS Directory Service提供的 DNS 服务器的 DNS 服务器 IP 地址。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。如果要手动设置，请参阅 AWS 知识中心的如何为私有 EC2 实例分配静态 DNS 服务器，以了解有关为特定 Linux 分发版和版本设置持久性 DNS 服务器的指导。
3. 确保 CentOS 7 实例为最新状态。

```
sudo yum -y update
```

4. 在 Linux 实例上安装所需 CentOS 7 软件包。

> **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

example.com 域中具有域加入权限的账户。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，请参阅委托 AWS Managed Microsoft AD 的目录加入权限。

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 文件的底部并保存该文件。

   ```
   ## 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. 将 Linux 实例配置为使用 AWS Directory Service提供的 DNS 服务器的 DNS 服务器 IP 地址。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。如果要手动设置，请参阅 AWS 知识中心的如何为私有 EC2 实例分配静态 DNS 服务器，以了解有关为特定 Linux 分发版和版本设置持久性 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

e *x* ***am AccountName*** *ple.com* 域中具有域加入权限的账户的 SaM。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，请参阅委托 AWS Managed Microsoft AD 的目录加入权限。

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 文件的底部并保存该文件。

```
## 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. 将 Linux 实例配置为使用 AWS Directory Service提供的 DNS 服务器的 DNS 服务器 IP 地址。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。如果要手动设置，请参阅 AWS 知识中心的如何为私有 EC2 实例分配静态 DNS 服务器，以了解有关为特定 Linux 分发版和版本设置持久性 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

e *x* ***am AccountName*** *ple.com* 域中具有域加入权限的账户的 SaM。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，请参阅委托 AWS Managed Microsoft AD 的目录加入权限。

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 文件的底部并保存该文件。

   ```
   ## 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 kpasswd 首次更改其密码。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. 将在 /etc/sssd/sssd.conf 文件中将 krb5_use_kdcinfo 设置为 False。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)
```

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 restart
```

身份映射

可以通过两种方法执行 ID 映射，以维护 UNIX/Linux 用户标识符 (UID) 和组标识符 (GID) 以及 Windows 和Active Directory安全标识符 (SID) 身份之间的统一体验。

1. 集中化
2. 分布式

> **Note**
>
> 中的集中式用户身份映射Active Directory需要便携式操作系统接口或 POSIX。

集中式用户身份映射

Active Directory或其他轻型目录访问协议 (LDAP) 服务为 Linux 用户提供 UID 和 GID。在中Active Directory，这些标识符存储在用户的属性中：

- UID-Linux 用户名（字符串）
- UID 号-Linux 用户 ID 号（整数）
- GID 号码-Linux 群组 ID 号（整数）

要将 Linux 实例配置为使用来自的 UID 和 GID，请在 sssd. Active Directory conf `ldap_id_mapping = False` 文件中进行设置。在设置此值之前，请确认您已向中的用户和群组添加了 UID、UID 号和 GID 号。Active Directory

分布式用户身份映射

如果Active Directory没有 POSIX 扩展名或者您选择不集中管理身份映射，Linux 可以计算 UID 和 GID 值。Linux 使用用户的唯一安全标识符 (SID) 来保持一致性。

要配置分布式用户 ID 映射，请在 sssd.conf 文件`ldap_id_mapping = True`中进行设置。

连接到 Linux 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。用户可以采用 username@example.com 或 EXAMPLE\username 格式输入用户名。根据您使用的 Linux 发行版，响应将类似于以下内容：

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%
```

委托 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。

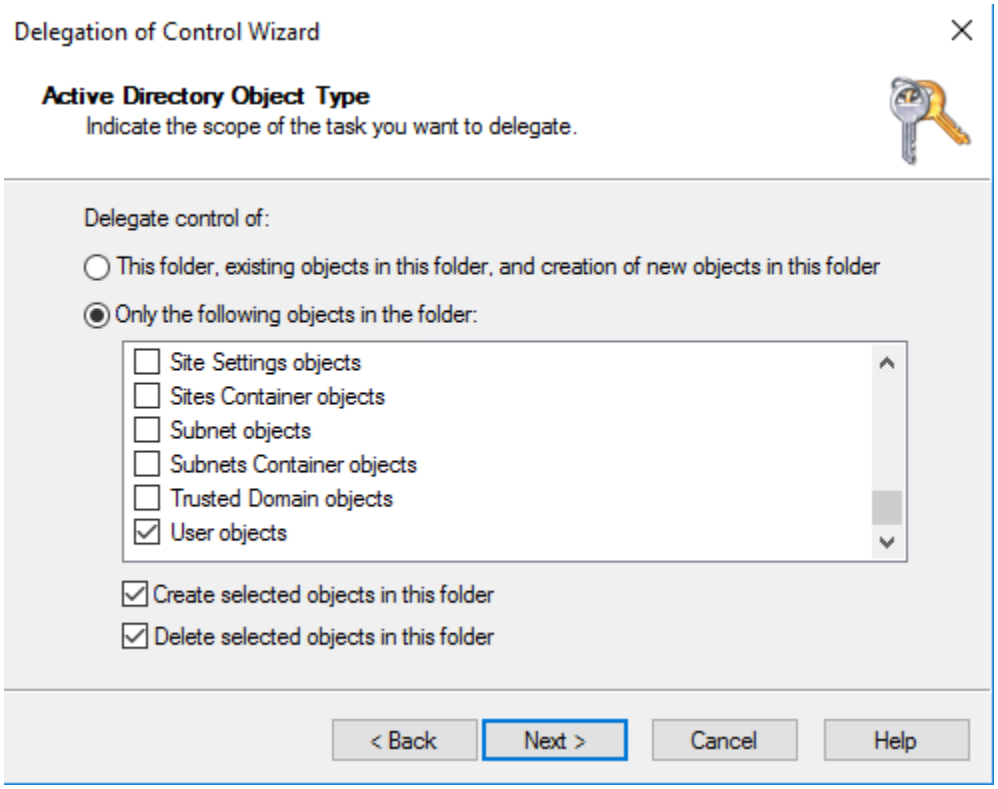
对于 Simple AD，域管理员组的成员拥有足够权限将计算机加入到目录。

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。

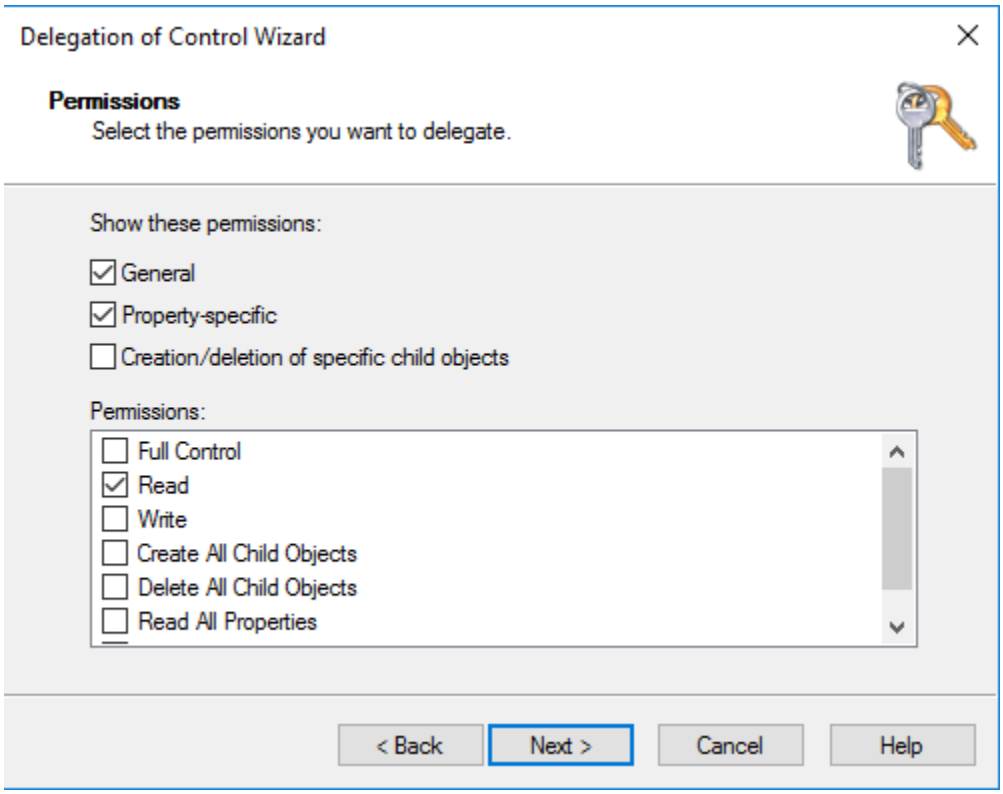
您必须在已加入到目录且已安装 Active Directory 用户和计算机 MMC 管理单元的计算机上执行此过程。您还必须以域管理员身份登录。

要委托 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。然后，用户将有足够的权限 AWS Directory Service 连接到该目录。

创建 DHCP 选项集

AWS 建议您为 AWS Directory Service 目录创建 DHCP 选项集，并将 DHCP 选项集分配给您的目录所在的 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https://docs.aws.amazon.com/vpc/latest/userguide/VPC_DHCP_Options.html《Amazon VPC 用户指南》中的 DHCP 选项集。

为目录创建 DHCP 选项集

1. 通过 https://console.aws.amazon.com/vpc/ 打开 Amazon VPC 控制台。
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，输入目录的以下值：

   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

   您 AWS提供的目录的 DNS 服务器的 IP 地址。

   > **Note**
   >
   > 可以转到 AWS Directory Service 控制台导航窗格，选择目录，然后选择正确的目录 ID，从而找到这些地址。

   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*)。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 Your VPCs(您的 VPC)。
3. 选择 VPC，然后选择操作、编辑 VPC 设置。
4. 对于 DHCP 选项集，选择一个选项集或选择无 DHCP 选项集，然后选择保存。

要使用命令行更改与 VPC 关联的 DHCP 选项集，请参阅以下内容：

- AWS CLI: associate-dhcp-options
- AWS Tools for Windows PowerShell: Register-EC2DhcpOption

维护 Simple AD 目录

本节介绍如何为 Simple AD 环境维护常见管理任务。

主题

- 删除 Simple AD
- 为目录拍摄快照或还原目录
- 查看目录信息

删除 Simple AD

删除 Simple AD 后，所有目录数据和快照都将被删除且无法恢复。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。

要删除目录

1. 在 AWS Directory Service 控制台导航窗格中，选择目录。确保您Active Directory位于您的部署 AWS 区域 位置。有关更多信息，请参阅选择区域。
2. 确保未为要删除的目录启用任何 AWS 应用程序。启用的 AWS 应用程序将阻止你删除 AWS 托管的 Microsoft AD 或 Simple AD。

   a. 在目录页面上，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 “AWS 应用程序和服务” 部分，您可以看到您的目录启用了哪些 AWS 应用程序。

   - 禁用 AWS Management Console 访问权限。有关更多信息，请参阅 禁用 AWS Management Console 访问。
   - 要禁用 Amazon WorkSpaces，您必须从 WorkSpaces 控制台的目录中取消注册该服务。有关更多信息，请参阅《Amazon WorkSpaces 管理指南》中的从目录取消注册。
   - 要禁用亚马逊 WorkDocs，您必须在亚马逊 WorkDocs控制台中删除亚马逊 WorkDocs 网站。有关更多信息，请参阅《Amazon WorkDocs 管理指南》中的删除网站。
   - 要禁用亚马逊 WorkMail，您必须在亚马逊 WorkMail 控制台中删除亚马逊 WorkMail 组织。有关更多信息，请参阅《Amazon WorkMail 管理员指南》中的移除组织。
   - 要禁用适用于 Windows File Server 的 Amazon FSx，必须从域中删除 Amazon FSx 文件系统。有关更多信息，请参阅《亚马逊 FSx for Windows 文件服务器用户指南》中的在 Windows 文件服务器的 FSx 中使用。Active Directory
   - 要禁用 Amazon Relational Database Service，必须从域中移除 Amazon RDS 实例。有关更多信息，请参阅《Amazon RDS 用户指南》中的在域中管理数据库实例。
   - 要禁用 AWS Client VPN 服务，必须从 Client VPN 端点中删除目录服务。有关更多信息，请参阅《AWS Client VPN 管理员指南》中的Active Directory身份验证。
   - 要禁用 Amazon Connect，必须删除 Amazon Connect 实例。有关更多信息，请参阅《Amazon Connect Administration Guide》中的 Deleting an Amazon Connect instance。
   - 要禁用亚马逊 QuickSight，您必须取消订阅亚马逊 QuickSight。有关更多信息，请参阅 Amazon QuickSight 用户指南中的关闭 Amazon QuickSight 账户。

> **Note**
>
> 如果您正在使用 AWS IAM Identity Center 并且之前已将其连接到计划删除的 AWS 托管 Microsoft AD 目录，则必须先更改身份源，然后才能将其删除。有关更多信息，请参阅《IAM Identity Center User Guide》中的 Change your identity source。

3. 在导航窗格中，选择目录。
4. 仅选择要删除的目录，然后单击删除。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。

为目录拍摄快照或还原目录

AWS Directory Service 提供了为 Simple AD 目录手动拍摄数据快照的功能。这些快照可用于 point-in-time 恢复您的目录。无法拍摄 AD Connector 目录的快照。

主题

- 为目录创建快照
- 从快照还原目录
- 删除快照

为目录创建快照

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 AWS Directory Service 控制台导航窗格中，选择目录。
2. 在目录页面上，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，选择操作，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）。就绪后，选择创建快照。

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。目录快照在创建它们的目录中是唯一的。快照只能恢复到创建它们的目录。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**
>
> 我们建议您在恢复快照之前联系 AWS Support 中心；我们可以帮助您避免进行快照还原。任何快照还原都会导致数据丢失，因为它们是一些时间点。务必要明确的是，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 AWS Directory Service 控制台导航窗格中，选择目录。
2. 在目录页面上，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，在列表中选择一个快照，选择操作，然后选择还原快照。
5. 查看还原目录快照对话框中的信息，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。目录成功还原之后，状态值会更改为 `Active`。会覆盖快照日期之后对目录进行的任何更改。

删除快照

删除快照

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

2. 在目录页面上，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，选择操作，然后选择删除快照。
5. 确认您要删除快照，然后选择删除。

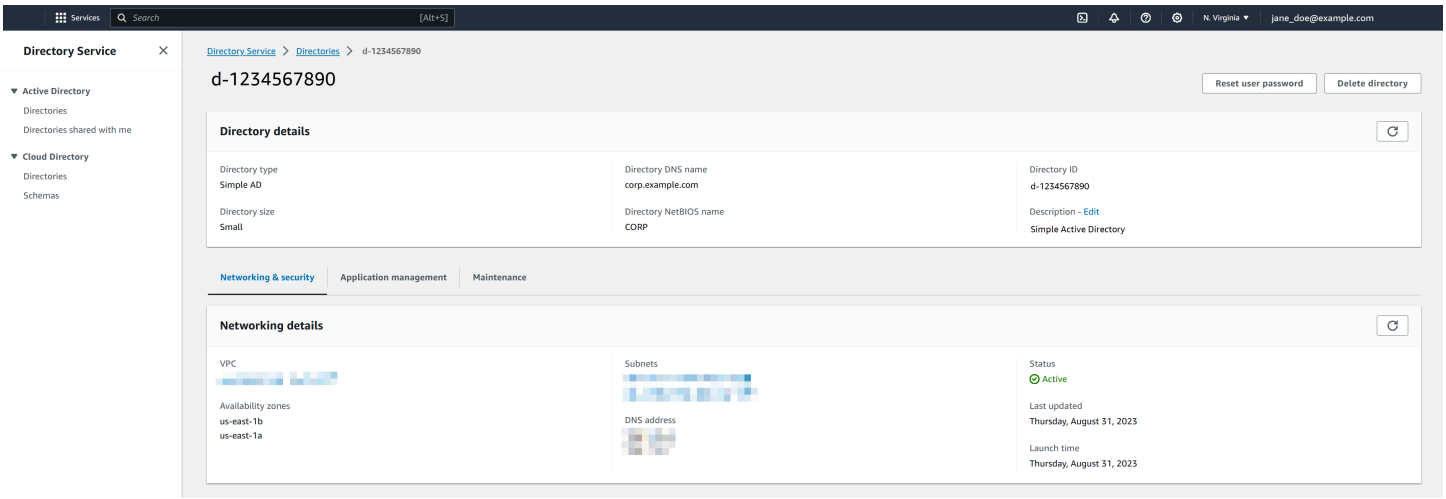
查看目录信息

您可以查看有关目录的详细信息。

查看详细目录信息

1. 在AWS Directory Service 控制台导航窗格中 Active Directory，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面中。

有关 Status 字段的更多信息，请参阅了解目录状态。



允许访问 AWS 应用程序和服务

用户可以授权 Simple AD 授予 AWS 应用程序和服务（例如亚马逊 WorkSpaces）访问您的权限Active Directory。可以启用或禁用以下 AWS 应用程序和服务以使用 Simple AD。

AWS 应用程序/服务	更多信息……
Amazon Chime	有关更多信息，请参阅 Amazon Chime Administration Guide。

AWS 应用程序/服务	更多信息……
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》。
Amazon WorkSpaces	你可以直接从中创建 Simple AD、 AWS 托管 Microsoft AD 或 AD Connecto WorkSpaces r。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》。
AWS Management Console	有关更多信息，请参阅允许使用 AD 凭证访问 AWS Management Console。

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权限。要在 AWS Directory Service 控制台中查找上述 AWS 应用程序和服务链接，请执行以下步骤。

显示适用于目录的应用程序和服务

1. 在 AWS Directory Service 控制台导航窗格中，选择目录。
2. 在目录页面上，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 AWS 应用程序和服务部分下的列表。

有关如何使用对 AWS 应用程序和服务进行授权或取消授权的更多信息 AWS Directory Service，请参阅使用对 AWS 应用程序和服务的授权 AWS Directory Service。

主题

- 创建访问 URL
- 单点登录

创建访问 URL

访问 URL 供 AWS 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。

创建访问 URL

1. 在 AWS Directory Service 控制台导航窗格中，选择目录。
2. 在目录页面上，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)。如果返回 Entity Already Exists 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 以 *<alias>*.awsapps.com 的格式显示。

单点登录

AWS Directory Service 允许您的用户通过加入目录 WorkDocs 的计算机访问 Amazon，而无需单独输入凭证。

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 AWS 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. 您可以委托权限以允许 AD Connector 服务帐户添加或删除自身的服务主体名称属性，您可以使用有权修改 AD Connector 服务帐户权限的帐户在加入域的计算机上运行以下 PowerShell 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"
```

启用或禁用 Amazon 单点登录 WorkDocs

1. 在 AWS Directory Service 控制台导航窗格中，选择目录。
2. 在目录页面上，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 “应用程序访问网址” 部分，选择 “启用” 以启用 Amazon WorkDocs 的单点登录。

   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。

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 的单点登录 WorkDocs，请选择 “禁用”，然后在 “禁用此目录的单点登录” 对话框中，再次选择 “禁用”。

主题

- IE 和 Chrome 的单点登录
- Firefox 的单点登录

IE 和 Chrome 的单点登录

要使 Microsoft 的 Internet Explorer（IE）和 Google 的 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：

- 将访问 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。
- 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 上单点登录的手动更新
- OS X 上单点登录的手动更新
- 单点登录的组策略设置

Windows 上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. 通过运行以下命令将您的访问网址添加到AuthServerAllowlist策略中：

```
defaults write com.google.Chrome AuthServerAllowlist "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。

单点登录的组策略设置

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**
>
> 如果您使用 Chrome 政策管理网域内计算机上的 Chrome 网络浏览器，则必须将访问网址添加到AuthServerAllowlist政策中。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. 在新建 GPO 对话框中，为组策略对象输入一个描述性名称（如 IAM Identity Center Policy），将源 Starter GPO 保留为（无）。单击 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：

操作

```
Update
```

Hive

```
HKEY_CURRENT_USER
```

路径

```
Software\Microsoft\Windows\CurrentVersion\Internet Settings
\ZoneMap\Domains\awsapps.com\<alias>
```

<alias> 的值派生自访问 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：

操作

```
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 Identity Center 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 的 Firefox 浏览器可以支持单点登录，请将访问 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

- 单点登录的手动更新
- 单点登录的自动更新

单点登录的手动更新

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，可以使用脚本在网络上的所有计算机上将访问 URL 添加到 Firefox `network.negotiate-auth.trusted-uris` 用户首选项。有关更多信息，请转到 https://support.mozilla.org/en-US/questions/939037。

允许使用 AD 凭证访问 AWS Management Console

AWS Directory Service 允许向目录的成员授予 AWS Management Console访问权限。默认情况下，目录成员无权访问任何 AWS 资源。可将 IAM 角色分配给目录成员，以便向其授予各种 AWS 服务和资源的访问权限。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。有关如何创建访问 URL 的更多信息，请参阅创建访问 URL。

有关如何创建 IAM 角色以及将其分配给目录成员的更多信息，请参阅 授予用户和组对 AWS 资源的访问权限。

主题

- 启用 AWS Management Console 访问
- 禁用 AWS Management Console 访问
- 设置登录会话长度

相关的 AWS 安全博客文章

- How to Access the AWS Management Console Using AWS Managed Microsoft AD and Your On-Premises Credentials

启用 AWS 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 AWS Directory Service 控制台导航窗格中，选择目录。
2. 在目录页面上，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 AWS Management Console 部分下，选择启用。控制台访问现在已为目录启用。

   在用户使用访问网址登录控制台之前，您必须先将用户添加到角色中。有关为用户分配 IAM 角色的一般信息，请参阅 为用户或组分配现有角色。分配 IAM 角色之后，用户就可以使用访问 URL

访问控制台了。例如，如果目录的访问 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 AWS 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 AWS Directory Service 控制台导航窗格中，选择目录。
2. 在目录页面上，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 AWS Management Console 部分下，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，包括目录中已删除的针对用户或组的分配，分别显示为已删除用户或已删除组。

   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 AWS Directory Service 控制台导航窗格中，选择目录。
2. 在目录页面上，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 AWS 应用程序和服务 部分下，选择 AWS 管理控制台。
5. 在管理对 AWS 资源的访问对话框中，选择继续。
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：制作一个 Simple AD Active Directory

以下教程将引导您完成设置 Simple AD AD Active Directory 所需的所有步骤。它旨在帮助您Active Directory快速轻松地开始使用 Simple AD，但不适用于大规模制作环境。

教程的先决条件

本教程假定：

- 你有一个活跃 AWS 账户的。
- 您的账户尚未达到您想要使用 Simple AD 的地区的亚马逊 VPC 上限。有关 VPC 的更多信息，请参阅什么是 Amazon VPC？ 以及 Amazon VPC 用户指南中的您的 VPC 中的子网。
- 您在该区域中没有 CIDR 为的现有 VPC。`10.0.0.0/16`

有关更多信息，请参阅 Simple AD 先决条件。

第 1 步：为 Simple AD 创建和配置您的亚马逊 VPC Active Directory

创建和配置用于 Simple AD 的 Amazon VPC。在开始此过程之前，请确保您已完成 教程的先决条件

为您的 Simple AD 创建一个 VPC Active Directory

创建具有两个公有子网的 VPC。 AWS Directory Service 在您的 VPC 中需要两个子网，并且每个子网必须位于不同的可用区中。

1. 通过 https://console.aws.amazon.com/vpc/ 打开 Amazon VPC 控制台。
2. 在 VPC 控制面板上，选择创建 VPC。
3. 在 VPC 设置页面上，选择 VPC 等。
4. 完成字段，如下所示：
   - 将名称标签自动生成下的自动生成的保持选中状态。将项目更改到 `ADS  VPC`。
   - IPv4 CIDR 块应为 `10.0.0.0/16`。
   - 保持 无 IPv6 CIDR 块选项为选中状态。
   - 租赁应保持为默认。
   - 然后，对于可用区（AZ）数量，选择 2。
   - 对于公有子网数量，选择 2。私有子网的数量可以更改为 0。

- 选择自定义子网 CIDR 块以配置公有子网 IP 地址范围。公有子网 CIDR 块应为 `10.0.0.0/20` 和 `10.0.16.0/20`。

5. 选择创建 VPC。创建 VPC 需要几分钟时间。

第 2 步：创建你的 Simple AD 活动目录

要创建新的 Simple AD 活动目录，请执行以下步骤。在开始此过程之前，请确保您已完成步骤 1：为 Simple AD 创建教程的先决条件和配置您的 Amazon VPC 中确定的先决条件Active Directory。

创建 Simple AD 活动目录

1. 在 AWS Directory Service 控制台导航窗格中，选择目录，然后选择设置目录。
2. 在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 AD。

   组织名称

   您的目录的唯一组织名称，将用于注册客户端设备。

   只有在启动时创建目录时，此字段才可用 WorkSpaces。

   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。目录创建过程将使用用户名 `Administrator` 和此密码创建一个管理员账户。

   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。

   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

以下是您应考虑的一些建议和指南，以避免出现问题并充分利用 Simple AD。

设置：先决条件

创建目录之前请考虑以下这些准则。

验证目录类型是否正确

AWS Directory Service 提供了多种与其他 AWS 服务Microsoft Active Directory配合使用的方式。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：

- AWS 微软目录服务 Active Directory 是一款托管在云端的功能丰富的Microsoft Active Directory托管服务。 AWS AWS 如果您拥有超过 5,000 个用户，并且需要在托管目录和本地目录之间建立信任关系，那么 AWS 托管 Microsoft AD 是您的最佳选择。

- AD Con nector 只需将您的现有本地环境连接Active Directory到 AWS。当您想要将现有本地目录与 AWS 服务一起使用时，AD Connector 是您的最佳选择。
- S@@ imple AD 是一个低规模、低成本的目录，具有基本Active Directory兼容性。其支持 5000 个或更少的用户、兼容 Samba 4 的应用程序，并支持 LDAP 感知型应用程序的 LDAP 兼容性。

有关 AWS Directory Service 选项的更详细比较，请参阅选择哪一个。

确保 VPC 和实例正确配置

要连接到、管理和使用目录，必须正确配置目录所关联的 VPC。有关 VPC 安全和网络要求的信息，请参阅 AWS 微软 AD 托管先决条件、AD Connector 先决条件 或 Simple AD 先决条件。

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 Amazon EC2 实例加入您的 AWS 托管微软 AD Active Directory 中所述。

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可以存储在目录中的对象数量的唯一限制。有关所选目录的详细信息，请参阅 AWS 托管微软 AD 配额、AD Connector 配额 或 Simple AD 限额。

了解目录 AWS 的安全组配置并使用

AWS 创建安全组并将其附加到目录的域控制器弹性网络接口。 AWS 将安全组配置为阻止不必要的目录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《Amazon EC2 用户指南》中的适用于 Linux 实例的 Amazon EC2 安全组。不当的更改可能会导致与目标计算机和实例的通信中断。 AWS 建议您不要尝试打开目录的其他端口，因为这会降低目录的安全性。请仔细查看 AWS 责任共担模型。

> **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， AWS 建议不要这样做。 AWS 可能有理由在不另行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。

如果需要信任，请使用 AWS 托管 Microsoft AD

Simple AD 不支持信任关系。如果你需要在你的 AWS Directory Service 目录和其他目录之间建立信任，你应该使用 Microsoft Active Directory 的 AWS 目录服务。

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。此账户 ID 是 Simple AD 的 管理员 ID。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 AWS 应用程序的用户名限制

AWS Directory Service 支持大多数可用于构造用户名的字符格式。但是，对于用于登录 AWS 应用程序（例如 WorkSpaces亚马逊、亚马逊或亚马 QuickSight逊 WorkDocs）的用户名有一些字符限制。WorkMail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。

为您的应用程序编程

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 AWS 托管 Microsoft AD 的动态 DNS (DDNS) 服务来定位域控制器 (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。此类情况还可能导致 AWS 目录自动化将目录标记为受损，并可能触发替换无响应的 DC 的恢复进程。

交付生产之前的负载测试

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 AWS Directory Service Microsoft Active Directory，它允许您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。

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 限额

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 AWS Service for Microsoft Active Directory（标准版或企业版）。

下面是 Simple AD 的默认限额。除非另有说明，否则每个限额均与区域一一对应。

Simple AD 限额

资源	默认配额
Simple AD 目录	10
手动快照*	每个 Simple AD 5 个

* 手动快照限额无法更改。

> **Note**
>
> 不能将公有 IP 地址附加到您的 AWS 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，AWS 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。尽管 AWS 与客户尝试克服任何潜在应用程序安装中遇到的挑战，但我们不能保证任何应用程序与或将继续与 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 AWS Directory Service for Microsoft Active Directory（AWS 微软 AD 托管），以基于实际 Active Directory 实现更高级别的兼容性。

Simple AD 问题排查

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

- 当将用户添加到 Simple AD 时，我收到“KDC 无法执行所请求的选项”错误
- 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)
- 我无法使用 SQL Server 账户登录 SQL Server
- 我的目录卡在“已请求”状态
- 我在创建目录时遇到“AZ 受限”错误
- 我的某些用户无法进行向我的目录进行身份验证
- 其他 资源
- Simple AD 目录状态原因

密码找回

如果用户忘记密码或者在登录你的 Simple AD 或 Microsoft AD AWS 托管目录时遇到问题，你可以使用 AWS Management Console、Windows PowerShell或重置他们的密码。 AWS CLI

有关更多信息，请参阅 重置 Simple AD 用户密码。

当将用户添加到 Simple AD 时，我收到“KDC 无法执行所请求的选项”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 Simple AD 的 Active Directory 管理工具。

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“用户登录失败”，即使提供了有效凭证时也是如此。这是一个已知问题， AWS 正在积极努力解决这个问题。

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“已请求”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。如果问题仍存在，请联系 AWS Support 中心。

我在创建目录时遇到“AZ 受限”错误

在 2012 年之前创建的某些 AWS 账户可能有权访问美国东部（弗吉尼亚北部）、美国西部（加利福尼亚北部）或亚太地区（东京）不支持 AWS Directory Service 目录的可用区。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，请转到 Microsoft TechNet 上的预身份验证。

其他 资源

以下资源可以帮助您在使用时进行故障排除 AWS。

- AWS 知识中心-查找常见问题解答和其他资源链接，以帮助您解决问题。
- AWS S@@ upport Center —获取技术支持。
- AWS Premium Support Center —获取高级技术支持。

主题

- Simple AD 目录状态原因

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 AWS 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，请参阅了解目录状态。

以下是 Simple AD 目录的状态消息：

主题

- 目录服务的弹性网络接口未连接

- 实例检测到的问题
- 目录中缺少关键 AWS Directory Service 保留用户
- 关键 AWS Directory Service 预留用户须属于域管理员组
- 关键 AWS Directory Service 预留用户已被禁用
- 主域控制器没有所有 FSMO 角色
- 域控制器复制失败

目录服务的弹性网络接口未连接

描述

在创建目录时代表您创建的用于与 VPC 建立网络连接的关键弹性网络接口（ENI）未连接到目录实例。此目录支持的 AWS 应用程序将无法正常运行。目录无法连接到本地网络。

问题排查

如果 ENI 已分离但仍然存在，请联系 AWS Support。如果 ENI 被删除，则无法解决问题，并且目录将永久不可用。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实例。

问题排查

在大多数情况下，这是一个暂时性问题，目录最终会返回到“活动”状态。如果问题仍然存在，请联系 AWS Support 寻求帮助。

目录中缺少关键 AWS Directory Service 保留用户

描述

在创建 Simple AD 时，AWS Directory Service 会在该目录中创建一个名为 `AWSAdminD-xxxxxxxxx` 的服务账户。当无法找到此服务账户时会收到此错误。如果没有此账户，AWS 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。

问题排查

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 AWS Directory Service 预留用户须属于域管理员组

描述

在创建 Simple AD 时，AWS Directory Service 会在该目录中创建一个名为 `AWSAdmin`*`D-xxxxxxxxx`* 的服务账户。当此服务账户不是 `Domain Admins` 组的成员时会收到此错误。AWS 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。

问题排查

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 AWS Directory Service 预留用户已被禁用

描述

在创建 Simple AD 时，AWS Directory Service 会在该目录中创建一个名为 `AWSAdmin`*`D-xxxxxxxxx`* 的服务账户。当此服务账户已禁用时会收到此错误。必须启用此账户，AWS Directory Service 才能够在该目录上执行维护和恢复操作。

问题排查

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。如果 FSMO 角色不属于正确的 Simple AD 目录控制器，则 AWS Directory Service 无法保证特定行为和功能。

问题排查

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，请转到 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 AWS 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。

问题排查

有关您 VPC 网络要求的更多信息，请参阅 AWS Managed Microsoft AD AWS 微软 AD 托管先决条件、AD Connector AD Connector 先决条件 或 Simple AD Simple AD 先决条件。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 AWS Support 以获得更多帮助。

安全性 AWS Directory Service

云安全 AWS 是重中之重。作为 AWS 客户，您可以从专为满足大多数安全敏感型组织的要求而构建的数据中心和网络架构中受益。

安全是双方共同承担 AWS 的责任。责任共担模式将其描述为云的 安全性和云中 的安全性：

- 云安全 — AWS 负责保护在 AWS 云中运行 AWS 服务的基础架构。 AWS 还为您提供可以安全使用的服务。作为 AWS 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。要了解适用的合规计划 AWS Directory Service，请参阅按合规计划划分的范围内的AWS 服务。
- 云端安全-您的责任由您使用的 AWS 服务决定。您还需要对其他因素负责，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。

本文档可帮助您了解在使用时如何应用分担责任模型 AWS Directory Service。以下主题向您介绍如何进行配置 AWS Directory Service 以满足您的安全和合规性目标。您还将学习如何使用其他 AWS 服务来帮助您监控和保护您的 AWS Directory Service 资源。

安全性主题

在此部分中可以找到以下安全性主题：

- 的身份和访问管理 AWS Directory Service
- 登录和监控 AWS Directory Service
- 合规性验证 AWS Directory Service
- 韧性在 AWS Directory Service
- 中的基础设施安全 AWS Directory Service

其他安全性主题

在此指南中可以找到以下其他安全性主题：

账户、信托和 AWS 资源访问权限

- 管理员账户的权限
- 组托管服务账户
- 创建信任关系
- Kerberos 约束委托

- 授予用户和组对 AWS 资源的访问权限
- 使用对 AWS 应用程序和服务的授权 AWS Directory Service

保护目录

- 保护 AWS Managed Microsoft AD 目录
- 保护您的 AD Connector 目录

日志记录和监控

- 监控 AWS Managed Microsoft AD
- 监控您的 AD Connector 目录

恢复功能

- AWS Managed Microsoft AD 的修补和维护

的身份和访问管理 AWS Directory Service

访问 AWS Directory Service 需要 AWS 可用于对您的请求进行身份验证的证书。这些证书必须具有访问 AWS 资源（例如 AWS Directory Service 目录）的权限。以下各节详细介绍了如何使用 AWS Identity and Access Management (IAM)，以及 AWS Directory Service 如何通过控制谁可以访问资源来帮助保护您的资源：

- 身份验证
- 访问控制

身份验证

了解如何 AWS 使用 IAM 身份进行访问。

访问控制

您可以拥有有效的凭证来验证您的请求，但是除非您拥有权限，否则您无法创建或访问 AWS Directory Service 资源。例如，您必须具有创建 AWS Directory Service 目录或创建目录快照的权限。

以下各节介绍如何管理的权限 AWS Directory Service。我们建议您先阅读概述。

- 管理 AWS Directory Service 资源访问权限概述
- 使用基于身份的策略（IAM 策略） AWS Directory Service
- AWS Directory Service API 权限：操作、资源和条件参考

管理 AWS Directory Service 资源访问权限概述

每个 AWS 资源都归一个 AWS 账户所有，创建或访问资源的权限受权限策略的约束。账户管理员可以向 IAM 身份（即用户、群组和角色）附加权限策略，某些服务（例如 AWS Lambda）还支持向资源附加权限策略。

> **Note**
>
> 帐户管理员（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。

主题

- AWS Directory Service 资源和运营
- 了解资源所有权
- 管理对资源的访问
- 指定策略元素：操作、效果、资源和主体
- 在策略中指定条件

AWS Directory Service 资源和运营

在中 AWS Directory Service，主要资源是一个目录。 AWS 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*

AWS Directory Service 提供了一组使用相应资源的操作。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 AWS 账户。也就是说，资源所有者是对创建资源的请求进行身份验证的委托人实体（根账户、IAM 用户或 IAM 角色）的账户。 AWS 以下示例说明了它的工作原理：

- 如果您使用账户的根账户证书创建 AWS Directory Service 资源（例如目录），则您的 AWS 账户就是该资源的所有者。 AWS
- 如果您在 AWS 账户中创建 IAM 用户并向该用户授予创建 AWS Directory Service 资源的权限，则该用户也可以创建 AWS Directory Service 资源。但是，该用户所属的您的 AWS 账户拥有这些资源。
- 如果您在 AWS 账户中创建具有创建 AWS Directory Service 资源权限的 IAM 角色，则任何能够担任该角色的人都可以创建 AWS Directory Service 资源。该角色所属的 AWS 账户拥有这些 AWS 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**
>
> 本节讨论在的上下文中使用 IAM AWS Directory Service。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 policy 语法和说明的信息，请参阅《IAM 用户指南》中的 IAM JSON 策略参考。

附加到 IAM 身份的策略称为基于身份的策略（IAM 策略），附加到资源的策略称为基于资源的策略。AWS 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）
- 基于资源的策略

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：

- 将@@ 权限策略附加到您账户中的用户或群组-账户管理员可以使用与特定用户关联的权限策略向该用户授予创建 AWS Directory Service 资源（例如新目录）的权限。
- 向角色附加权限策略（授予跨帐户权限）– 您可以向 IAM 角色附加基于身份的权限策略，以授予跨帐户的权限。

  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 AWS Directory Service 资源的信息，例如目录或快照。请注意，`Resource`元素中的通配符 (*) 表示允许对账户拥有的所有 AWS Directory Service 资源执行这些操作。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":"ds:Describe*",
         "Resource":"*"
      }
   ]
}
```

有关将基于身份的策略与配合使用的更多信息 AWS Directory Service，请参阅。使用基于身份的策略（IAM 策略）AWS Directory Service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 Amazon S3）还支持基于资源的权限策略。例如，您可以将策略附加到 S3 存储桶，以管理对该存储桶的访问权限。 AWS 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 AWS 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 AWS Directory Service 资源和运营。有关可用 API 操作的列表，请参阅目录服务操作。

要授予这些 API 操作的权限，请 AWS Directory Service 定义一组可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：

- 资源 - 在策略中，您可以使用 Amazon 资源名称（ARN）标识策略应用到的资源。对于 AWS Directory Service 资源，您始终在 IAM 策略中使用通配符 (*)。有关更多信息，请参阅 AWS Directory Service 资源和运营。
- 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 AWS Directory Service `DescribeDirectories` 操作的用户权限。
- 效果 – 用于指定当用户请求特定操作时的效果。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 策略）中，附加了策略的用户是隐式主体。对于基于资源的策略，您可以指定要获得权限的用户、账户、服务或其他实体（仅适用于基于资源的策略）。 AWS Directory Service 不支持基于资源的策略。

要了解 IAM policy 语法和说明的更多信息，请参阅《IAM 用户指南》中的 IAM JSON 策略参考。

有关显示所有 AWS Directory Service API 操作及其适用的资源的表格，请参阅AWS Directory Service API 权限：操作、资源和条件参考。

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 AWS Directory Service的条件键。但是，您可以根据需要使用一些 AWS 条件键。有关 AWS 密钥的完整列表，请参阅 IAM 用户指南中的可用全局条件密钥。

使用基于身份的策略（IAM 策略） AWS Directory Service

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**
>
> 我们建议您先阅读介绍性主题，这些主题解释了管理 AWS Directory Service 资源访问权限的基本概念和选项。有关更多信息，请参阅 管理 AWS Directory Service 资源访问权限概述。

本主题的各个部分涵盖以下内容：

- 使用 AWS Directory Service 控制台所需的权限
- AWS 的托管（预定义）策略 AWS Directory Service
- 客户管理的策略示例
- 在 IAM 策略中使用标签

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 AWS Directory Service 目录的权限。 AWS Directory Service 不支持在资源级别执行此特定操作的权限。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 操作才能代表您读取和创建 IAM 角色。AWS Directory Service `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 AWS Directory Service 予创建、配置和销毁其目录所需的权限。`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 AWS Directory Service API 操作及其适用的资源的表格，请参阅AWS Directory Service API 权限：操作、资源和条件参考。

使用 AWS Directory Service 控制台所需的权限

要使用 AWS Directory Service 控制台，该用户必须拥有上述策略中列出的权限，或者拥有目录服务完全访问角色或目录服务只读角色所授予的权限，如中所述AWS 的托管（预定义）策略 AWS Directory Service。

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。

AWS 的托管（预定义）策略 AWS Directory Service

AWS 通过提供由创建和管理的独立 IAM 策略来解决许多常见用例 AWS。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 AWS 托管式策略。

您可以将以下 AWS 托管策略附加到账户中的用户，这些策略特定于 AWS Directory Service：

- AWSDirectoryServiceReadOnlyAccess— 向用户或群组授予对根账户的所有 AWS Directory Service 资源、EC2 子网、EC2 网络接口以及亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 主题和订阅的只读访问权限。 AWS 有关更多信息，请参阅 将 AWS 托管策略与 AWS Directory Service 结合使用。
- AWSDirectoryServiceFullAccess – 向用户或组授予以下权限：
  - 完全访问权限 AWS Directory Service
  - 访问使用所需的关键 Amazon EC2 服务 AWS Directory Service
  - 能够列出 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 将 AWS 托管策略与 AWS Directory Service 结合使用。

此外，还有其他适用于其他 IAM 角色的 AWS 托管策略。这些策略将分配给与您 AWS Directory Service 目录中的用户关联的角色。这些用户需要这些策略才能访问其他 AWS 资源，例如 Amazon EC2。有关更多信息，请参阅 授予用户和组对 AWS 资源的访问权限。

还可创建自定义 IAM policy 来允许用户访问必需的 API 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

在本节中，您可以找到授予各种 AWS Directory Service 操作权限的用户策略示例。

> **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 AWS Directory Service 资源执行任何 “描述” 操作
- 示例 2：允许用户创建目录

示例 1：允许用户对任何 AWS Directory Service 资源执行任何 “描述” 操作

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 AWS Directory Service 资源的信息，例如目录或快照。请注意，Resource元素中的通配符 (*) 表示允许对账户拥有的所有 AWS Directory Service 资源执行这些操作。

```
{
   "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

您可以在用于大多数 AWS 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 policy 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 policy 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 AWS Directory Service 操作。

《IAM 用户指南》中的使用标签控制访问具有有关使用标签的其他信息。该指南的 IAM JSON 策略参考部分包含 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 AWS 服务命名空间。

以下 AWS Directory Service API 操作列表支持基于标签的资源级权限：

- 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

AWS Directory Service API 权限：操作、资源和条件参考

在设置 访问控制 和编写您可附加到 IAM 身份的权限策略（基于身份的策略）时，可以使用 AWS Directory Service API 权限：操作、资源和条件参考 表作为参考。中的每个 API 条目都包含以下内容：

- AWS Directory Service API 操作的名称
- 您可授予执行该操作的权限的对应操作
- 您可以为其授予权限的 AWS 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。要指定操作，请在 API 操作名称之前使用 `ds:` 前缀（例如，`ds:CreateDirectory`）。某些 AWS 应用程序可能需要在其策略中使用非公共 AWS Directory Service API 操作，例如`ds:AuthorizeApplicationds:CheckAliasds:CreateIdentityPoolDirectoryds:GetAuthor`和`ds:UnauthorizeApplication`。

有些 AWS Directory Service API 只能通过调用 AWS Management Console。从某种意义上说，它们不是公共 API，因为它们不能以编程方式调用，也不是由任何 SDK 提供的。他们接受用户证书。这些 API 操作包括`ds:DisableRoleAccessds:EnableRoleAccess`、和`ds:UpdateDirectory`。

您可以在 AWS Directory Service 策略中使用 AWS 全局条件密钥来表达条件。有关 AWS 密钥的完整列表，请参阅 IAM 用户指南中的可用全局条件密钥。

相关主题

- 访问控制

使用对 AWS 应用程序和服务的授权 AWS Directory Service

在 Active Di AWS rectory 上授权应用程序

AWS Directory Service 授予所选应用程序的特定权限，以便在您授权应用程序时与您的 Active Directory 无缝集成。 AWS AWS 应用程序仅被授予其用例所需的访问权限。授权后授予应用程序和应用程序管理员的内部权限集如下所示：

> **Note**
>
> 授权新 AWS 应用程序使用 Active Directory 需要该`ds:AuthorizationApplication`权限。只能向配置与 Directory Service 集成的管理员提供此操作的权限。

- 在托管的微软 AD、Simple AD、AD Connector 目录中的所有组织单位 (OU) 以及 AWS 托管微软 AD 的可信域中，读取对 Active Directory 用户、群组、组织单位、计算机或证书颁发机构数据的访问权限（如果信任关系允许）。 AWS
- 写入对 AWS 托管 Microsoft AD 组织单位中的用户、群组、群组成员资格、计算机或证书颁发机构数据的访问权限。对 Simple AD 的所有 OU 的写入权限。
- 对所有目录类型的 Active Directory 用户的身份验证和会话管理权限。

某些 AWS 托管的 Microsoft AD 应用程序，例如亚马逊 RDS 和 Amazon FSx，通过直接的网络连接集成到您的 Active Directory。在这种情况下，目录交互使用本机 Active Directory 协议，例如 LDAP 和 Kerberos。这些 AWS 应用程序的权限由应用程序授权期间在 AWS 预留组织单位 (OU) 中创建的目录用户帐户控制，其中包括对为应用程序创建的自定义 OU 的 DNS 管理和完全访问权限。要使用此账户，应用程序需要通过调用者凭证或 IAM 角色执行 `ds:GetAuthorizedApplicationDetails` 操作的权限。

有关 AWS Directory Service API 权限的更多信息，请参阅AWS Directory Service API 权限：操作、资源和条件参考。

有关为 AWS 托管 Microsoft AD 启用 AWS 应用程序和服务的更多信息，请参阅允许访问 AWS 应用程序和服务。有关为 AD Connector 启用 AWS 应用程序和服务的更多信息，请参阅允许访问 AWS 应用程序和服务。有关为 Simple AD 启用 AWS 应用程序和服务的更多信息，请参阅允许访问 AWS 应用程序和服务。

取消对 Active Direct AWS ory 上应用程序的授权

要删除 AWS 应用程序访问活动目录的权限，需要该`ds:UnauthorizedApplication`权限。按照应用程序提供的步骤将其禁用。

登录和监控 AWS Directory Service

对组织进行监控，确保对所做的更改进行记录，这是最佳实践。这可以帮助您确保可以调查任何意外更改并回退不需要的更改。 AWS Directory Service 目前支持以下两项 AWS 服务，因此您可以监控您的组织及其内部发生的活动。

- 亚马逊 CloudWatch -您可以将 CloudWatch 事件与微软 AD AWS 托管目录类型一起使用。有关更多信息，请参阅 启用日志转发。此外，您还可以使用 CloudWatch Metrics 来监控域控制器的性能。有关更多信息，请参阅 确定何时添加带有 CloudWatch 指标的域控制器。
- AWS CloudTrail -您可以 CloudTrail 与所有 AWS Directory Service 目录类型一起使用。有关更多信息，请参阅使用记录 AWS Directory Service API 调用 CloudTrail。

合规性验证 AWS Directory Service

要了解是否属于特定合规计划的范围，请参阅AWS 服务 “按合规计划划分的范围” ”，然后选择您感兴趣的合规计划。 AWS 服务 有关一般信息，请参阅AWS 合规计划AWS。

您可以使用下载第三方审计报告 AWS Artifact。有关更多信息，请参阅中的 “下载报告” 中的 “ AWS Artifact。

您在使用 AWS 服务 时的合规责任取决于您的数据的敏感性、贵公司的合规目标以及适用的法律和法规。 AWS 提供了以下资源来帮助实现合规性：

- 安全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，并提供了部署以安全性和合规性为重点 AWS 的基准环境的步骤。
- 在 A@@ mazon Web Services 上构建 HIPAA 安全与合规性 — 本白皮书描述了各公司如何使用 AWS 来创建符合 HIPAA 资格的应用程序。

> **Note**
>
> 并非所有 AWS 服务 人都符合 HIPAA 资格。有关更多信息，请参阅符合 HIPAA 要求的服务参考。

- AWS 合AWS 规资源 — 此工作簿和指南集可能适用于您的行业和所在地区。
- AWS 客户合规指南 — 从合规角度了解责任共担模式。这些指南总结了保护的最佳实践， AWS 服务并将指南映射到跨多个框架（包括美国国家标准与技术研究院 (NIST)、支付卡行业安全标准委员会 (PCI) 和国际标准化组织 (ISO)）的安全控制。
- 使用AWS Config 开发人员指南中的规则评估资源 — 该 AWS Config 服务评估您的资源配置在多大程度上符合内部实践、行业准则和法规。
- AWS Security Hub— 这 AWS 服务 提供了您内部安全状态的全面视图 AWS。Security Hub 通过安全控件评估您的 AWS 资源并检查其是否符合安全行业标准和最佳实践。有关受支持服务及控件的列表，请参阅 Security Hub 控件参考。

- Amazon GuardDuty — 它通过监控您的 AWS 账户环境中是否存在可疑和恶意活动，来 AWS 服务检测您的工作负载、容器和数据面临的潜在威胁。 GuardDuty 通过满足某些合规性框架规定的入侵检测要求，可以帮助您满足各种合规性要求，例如 PCI DSS。
- AWS Audit Manager— 这 AWS 服务 可以帮助您持续审计 AWS 使用情况，从而简化风险管理以及对法规和行业标准的合规性。

韧性在 AWS Directory Service

AWS 全球基础设施是围绕 AWS 区域和可用区构建的。 AWS 区域提供多个物理隔离和隔离的可用区，这些可用区通过低延迟、高吞吐量和高度冗余的网络相连。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架构相比，可用区具有更高的可用性、容错性和可扩展性。

有关 AWS 区域和可用区的更多信息，请参阅AWS 全球基础设施。

除了 AWS 全球基础架构外，还 AWS Directory Service 提供随时手动拍摄数据快照的功能，以帮助支持您的数据弹性和备份需求。有关更多信息，请参阅 为目录拍摄快照或还原目录。

中的基础设施安全 AWS Directory Service

作为一项托管服务， AWS Directory Service 受到《Amazon Web Services：安全流程概述》白皮书中描述的 AWS 全球网络安全程序的保护。

您可以使用 AWS 已发布的 API 调用 AWS Directory Service 通过网络进行访问。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。

如果您在 AWS 通过命令行界面或 API 进行访问时需要经过 FIPS 140-2 验证的加密模块，请使用 FIPS 端点。有关可用的 FIPS 端点的更多信息，请参阅美国联邦信息处理标准（FIPS）140-2。

此外，必须使用访问密钥 ID 和与 IAM 主体关联的秘密访问密钥来对请求进行签名。或者，您可以使用 AWS Security Token Service（AWS 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。在中 AWS，跨服务模仿可能会导致混乱的副手问题。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。为防止这种情况，AWS 提供可帮助您保护所有服务的数据的工具，而这些服务中的服务主体有权限访问账户中的资源。

我们建议在资源策略中使用aws:SourceArn和aws:SourceAccount全局条件上下文密钥来限制适用于 Microsoft Active Directory 的 AWS 目录服务为资源提供的其他服务的权限。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 托管 Microsoft AD 中的aws:SourceArn和aws:SourceAccount全局条件上下文键来防止出现混淆的副手问题。

```
{
  "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"
      }
    }
  }
}
```

对于以下示例，aws:SourceArn 的值必须是您账户中的 SNS 主题。例如，你可以使用这样的内容，arn:aws:sns:ap-southeast-1:123456789012:DirectoryMonitoring_d-966739499f其中 “ap-southeast-1” 是你的区域，“123456789012” 是你的客户编号，“_d-966739499f” 是你创建的亚马逊 SNS 主题名称。DirectoryMonitoring

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 托管 Microsoft AD 中的aws:SourceArn和aws:SourceAccount全局条件上下文键来防止出现混淆的副手问题。

```
{
  "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。aws:SourceArn 的值必须是您账户中的目录资源。有关更多信息，请参阅由定义的资源类型 AWS Directory Service。例如，您可以使用 arn:aws:ds:us-east-1:123456789012:directory/d-1234567890，其中 123456789012 是您的客户 ID，d-1234567890 是您的目录 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"
      }
    }
  }
}
```

AWS Directory Service API 和接口 Amazon VPC 终端节点使用 AWS PrivateLink

您可以通过创建接口 VPC 终端节点在您的 Amazon VPC 和 AWS Directory Service API 终端节点之间建立私有连接。接口端点由 AWS PrivateLink 提供支持。

AWS PrivateLink 使您无需互联网网关、NAT 设备、VPN 连接或 AWS Direct Connect 连接即可私密访问 AWS Directory Service API 操作。您的 VPC 和 VPC 之间的流量 AWS Directory Service 不会离开 AWS 网络。

每个接口端点均由子网中的一个或多个弹性网络接口表示。有关弹性网络接口的更多信息，请参阅 Amazon EC2 用户指南中的弹性网络接口。

有关 VPC 终端节点的更多信息，请参阅 Amazon VPC 用户指南中的 AWS 服务 使用接口 VPC 终端节点访问和。有关 AWS Directory Service API 操作的更多信息，请参阅 AWS Directory Service API 参考。

VPC 终端节点注意事项

在为 AWS Directory Service API 终端节点设置接口 VPC 终端节点之前，请务必查看AWS PrivateLink 指南中的使用接口 VPC 终端节点访问和 AWS 服务 使用接口 VPC 终端节点。

所有与管理 AWS Directory Service 资源相关的 AWS Directory Service API 操作均可通过您的 VPC 使用 AWS PrivateLink。

Directory Service API 终端节点支持 VPC 终端节点策略。默认情况下，允许通过终端节点对 Directory Service API 操作进行完全访问。有关更多信息，请参阅 Amazon VPC 用户指南中的使用终端节点策略控制 VPC 终端节点的访问权限。

可用性

AWS Directory Service 支持以下 VPC 终端节点 AWS 区域：

AWS 区域 可用性

- 美国东部（弗吉尼亚州北部）
- 美国东部（俄亥俄州）
- 美国西部（加利福尼亚北部）
- 美国西部（俄勒冈州）
- 非洲（开普敦）
- 亚太地区（香港）
- 亚太地区（海得拉巴）
- 亚太地区（雅加达）
- 亚太地区（墨尔本）

- 亚太地区（孟买）
- 亚太地区（大阪）
- 亚太地区（首尔）
- 亚太地区（新加坡）
- 亚太地区（悉尼）
- 亚太地区（东京）
- 加拿大（中部）
- 加拿大西部（卡尔加里）
- 中国（北京和宁夏）
- 亚太地区（香港）
- 欧洲地区（法兰克福）
- 欧洲地区（爱尔兰）
- 欧洲地区（伦敦）
- 欧洲地区（米兰）
- 欧洲地区（巴黎）
- 欧洲（西班牙）
- 欧洲地区（斯德哥尔摩）
- 欧洲（苏黎世）
- 以色列（特拉维夫）
- 中东（巴林）
- 中东（阿联酋）
- 南美洲（圣保罗）
- AWS GovCloud （美国东部）
- AWS GovCloud （美国西部）

为 API 创建 AWS Directory Service 接口端点

您可以使用 Amazon VPC 控制台或 AWS Command Line Interface (AWS CLI) 为 AWS Directory Service API 创建 VPC 接口终端节点。有关更多信息，请参阅 AWS PrivateLink 指南中的创建 VPC 端点。

使用以下服务名称为 AWS Directory Service API 创建接口终端节点：`com.amazonaws.region.ds`

中国除外 AWS 区域 ，如果您为终端节点启用私有 DNS，则可以使用 VPC 终端节点 AWS Directory Service 的默认 DNS 名称向 VPC 终端节点发 AWS 区域出 API 请求`ds.us-east-1.amazonaws.com`。对于中国（北京和宁夏） AWS 区域，您可以分别使用`ds-api.cn-north-1.amazonaws.com.cn`和`ds-api.cn-northwest-1.amazonaws.com.cn`向 VPC 终端节点发出 API 请求。

有关更多信息，请参阅 Amazon VPC 用户指南中的 AWS 服务 使用接口 VPC 终端节点访问。

为 AWS Directory Service API 创建 VPC 终端节点策略

您可以为 VPC 终端节点附加控制对 AWS Directory Service API 的访问的终端节点策略。该策略指定以下信息：

- 可执行操作的主体。
- 可执行的操作。
- 可对其执行操作的资源。

有关更多信息，请参阅 Amazon VPC 用户指南中的使用终端节点策略控制 VPC 终端节点的访问权限。

示例：适用于 AWS Directory Service API 操作的 VPC 终端节点策略

以下是 AWS Directory Service API 的终端节点策略示例。当您将此策略附加到您的接口终端节点时，它会向所有资源的所有委托人授予对所列 AWS Directory Service API 操作的访问权限。

```
{
   "Statement": [
      {
         "Principal": "*",
         "Effect": "Allow",
         "Action": [
            "ds:DescribeDirectories",
            "ds:DescribeCertificate",
         ],
         "Resource":"*"
      }
   ]
}
```

示例：拒绝来自指定服务器的所有访问的 VPC 终端节点策略 AWS 账户

以下 VPC 终端节点策略拒绝所有使用该终端节点访问资源的 AWS 账户 *123456789012*。此策略允许来自其他账户的所有操作。

```
{
   "Statement": [
      {
         "Action": "*",
            "Effect": "Allow",
            "Resource": "*",
            "Principal:" "*"
      },
      {
        "Action": "*",
        "Effect": "Deny",
        "Resource": "*",
        "Principal": {
            "AWS": [
               "123456789012"
            ]
         }
      ]
}
```

AWS Directory Service 的服务水平协议

AWS Directory Service 是一种高度可用的服务，构建在 AWS 托管的基础设施上。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 Service level agreement for AWS Directory Service。

的地区可用性 AWS Directory Service

下表提供了一个列表，按目录类型介绍了支持的区域特定的端点。

区域名称	区域	端点	协议	AWS 微软 AD 托管	AD Connect	Simple AD
美国东部（弗吉尼亚州北部）	us-east-1	ds.us-east-1.amazonaws.com	HTTPS	 是	 是	 是
美国东部（俄亥俄州）	us-east-2	ds.us-east-2.amazonaws.com	HTTPS	 是	 是	 否
美国西部（加利福尼亚北部）	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

区域名称	区域	端点	协议	AWS 微软 AD 托管	AD Connect	Simple AD
亚太地区（香港）	ap-east-1	ds.ap-east-1.amazonaws.com	HTTPS	 是	 是	 否
亚太地区（海得拉巴）	ap-south-2	ds.ap-south-2.amazonaws.com	HTTPS	 是	 是	 否
亚太地区（雅加达）	ap-southeast-3	ds.ap-southeast-3.amazonaws.com	HTTPS	 是	 是	 否
亚太地区（墨尔本）	ap-southeast-4	ds.ap-southeast-4.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
Asia Pacific (Osaka)	ap-northeast-3	ds.ap-northeast-3.amazonaws.com	HTTPS	 是	 是	 否
Asia Pacific (Seoul)	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

区域名称	区域	端点	协议	AWS 微软 AD 托管	AD Connect	Simple AD
亚太地区（悉尼）	ap-southeast-2	ds.ap-southeast-2.amazonaws.com	HTTPS	 是	 是	 是
Asia Pacific (Tokyo)	ap-northeast-1	ds.ap-northeast-1.amazonaws.com	HTTPS	 是	 是	 是
加拿大（中部）	ca-central-1	ds.ca-central-1.amazonaws.com	HTTPS	 是	 是	 否
加拿大西部（卡尔加里）	ca-west-1	ds.ca-west-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
欧洲地区（爱尔兰）	eu-west-1	ds.eu-west-1.amazonaws.com	HTTPS	 是	 是	 是

区域名称	区域	端点	协议	AWS 微软 AD 托管	AD Connect	Simple AD
欧洲（伦敦）	eu-west-2	ds.eu-west-2.amazonaws.com	HTTPS	是	是	否
欧洲（米兰）	eu-south-1	ds.eu-south-1.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（西班牙）	eu-south-2	ds.eu-south-2.amazonaws.com	HTTPS	是	是	否
欧洲地区（斯德哥尔摩）	eu-north-1	ds.eu-north-1.amazonaws.com	HTTPS	是	是	否
欧洲（苏黎世）	eu-central-2	ds.eu-central-2.amazonaws.com	HTTPS	是	是	否
以色列（特拉维夫）	il-central-1	ds.il-central-1.amazonaws.com	HTTPS	是	是	否
中东（巴林）	me-south-1	ds.me-south-1.amazonaws.com	HTTPS	是	是	否

区域名称	区域	端点	协议	AWS 微软 AD 托管	AD Connect	Simple AD
中东（阿联酋）	me-central-1	ds.me-central-1.amazonaws.com	HTTPS	 是	 是	 否
南美洲（圣保罗）	sa-east-1	ds.sa-east-1.amazonaws.com	HTTPS	 是	 是	 否
AWS GovClou（美国西部）	us-gov-west-1	ds。 us-gov-west-1.amazonaws.com	HTTPS	 是	 是	 否
AWS GovClou（美国东部）	us-gov-east-1	ds。 us-gov-east-1.amazonaws.com	HTTPS	 是	 是	 否

有关 AWS Directory Service 在 AWS GovCloud （美国西部）地区和 AWS GovCloud （美国东部）地区使用的信息，请参阅服务终端节点。

有关 AWS Directory Service 在北京和宁夏区域使用的信息，请参阅中国 Amazon Web Services 的终端节点和 ARN。

浏览器兼容性

AWS 诸如亚马逊 WorkSpaces、Amazon WorkMail Connect、Amazon Chime WorkDocs、Amazon 等应用程序和服务 AWS IAM Identity Center 都需要通过兼容的浏览器提供有效的登录凭证才能访问。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 Edge	最新 3 个版本	兼容
Mozilla Firefox	最新 3 个版本	兼容
Google Chrome	最新 3 个版本	兼容
Apple Safari	最新 3 个版本	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 AWS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 Identity Center 支持的 TLS 版本

AWS 应用程序和服务支持 TLS 1.1、1.2 和 1.3 以实现安全登录。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 AWS 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 AWS Directory Service 管理员指南以来的重要更改。

变更	说明	日期
基于证书的身份验证设置	添加了有关 AWS 托管 Microsoft AD 的两个新安全设置的内容。	2023 年 4 月 11 日
AWS PrivateLink	添加了有关 AWS PrivateLink 的内容。	2023 年 3 月 31 日
Simple AD VPC 端点	添加了有关不应配置哪些 VPC 端点的内容。	2021 年 8 月 25 日
AD Connector VPC 端点	添加了有关不应配置哪些 VPC 端点的内容。	2021 年 8 月 25 日
智能卡支持	添加了有关在 AWS GovCloud（美国西部）地区支持智能卡和 Amazon WorkSpaces 应用程序管理器的内容	2020 年 12 月 1 日
密码重置	添加了有关如何使用 AWS Management Console、Windows PowerShell和重置用户密码的内容 AWS CLI。	2019 年 1 月 2 日
目录共享	添加了有关如何在 AWS 托管 Microsoft AD 中使用目录共享的内容。	2018 年 9 月 25 日
已将内容迁移到新的 Amazon Cloud Directory 开发人员指南	将本指南中的 Amazon Cloud Directory 内容迁移到新的《Amazon Cloud Directory Developer Guide》。	2018 年 6 月 21 日

全面修订管理员指南 TOC	重新组织了内容，更直接地满足客户需求。还根据需要添加了新内容。	2018 年 4 月 5 日
AWS 委托群组	添加了可以分配给本地用户的 AWS 委派群组列表。	2018 年 3 月 8 日
精细密码策略	添加了有关新的密码策略的内容。	2017 年 7 月 5 日
额外的域控制器	在 AWS 托管 Microsoft AD 中添加了有关如何向目录中添加更多域控制器的内容。	2017 年 6 月 30 日
教程	添加了用于测试 AWS 托管 Microsoft AD 实验室环境的新教程。	2017 年 6 月 21 日
MFA（使用托管 M AWS icrosoft AD）	添加了有关在托管 M AWS icrosoft AD 中使用 MFA 的内容。	2017 年 2 月 13 日
Amazon Cloud Directory	添加了有关新目录类型的内容。	2017 年 1 月 26 日
架构扩展	添加了有关微软 Active AWS Directory 目录的 Directory Service 架构扩展	2016 年 11 月 14 日
《AWS Directory Service 管理员指南》的重大重组	重新组织了内容，更直接地满足客户需求。	2016 年 11 月 14 日
SNS 通知	添加了有关 SNS 通知的内容。	2016 年 2 月 25 日
授权和身份验证	添加了有关如何将 IAM 与配合使用的内容 AWS Directory Service。	2016 年 2 月 25 日

AWS 微软 AD 托管	将有关 AWS 托管 Microsoft AD 的内容以及将指南合并到一个指南中。	2015 年 11 月 17 日
允许 Linux 实例加入 Simple AD 目录	添加了有关如何将 Linux 实例加入 Simple AD 目录的内容。	2015 年 7 月 23 日
指南分离	将《AWS Directory Service 管理指南》拆分为不同指南。	2015 年 7 月 14 日
单点登录支持	添加了有关单点登录支持的内容。	2015 年 3 月 31 日
新指南	这是《AWS Directory Service 管理指南》的第一个版本。	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。