对Office 365的ECE OAUTH2身份验证进行故障排除

目录

简介

先决条件

- 要求
- 使用的组件

背景

检查项目

- 最低版本
- 系统配置
- Azure AD应用程序
- 令牌生成
- 邮箱配置
- Exchange许可证
- 邮箱权限
- 网络连接
  - URL
  - 端口
  - 连通性测试

文档链接

- 11.6(1)
- 12.0(1)
- 12.5(1)
- 12.6(1)

简介

本文档介绍排除企业聊天和电子邮件(ECE)与Microsoft Office 365 (O365)电子邮件集成的故障的步骤。

先决条件

要求

Cisco 建议您了解以下主题：

- 企业聊天和电子邮件(ECE) 12.6
- Microsoft Office 365 (O365)
- Microsoft Azure Active Directory (Azure AD)

使用的组件

本文档中的信息基于以下软件版本：

- 欧洲经委会12.6(1)
- Azure AD
- O365

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

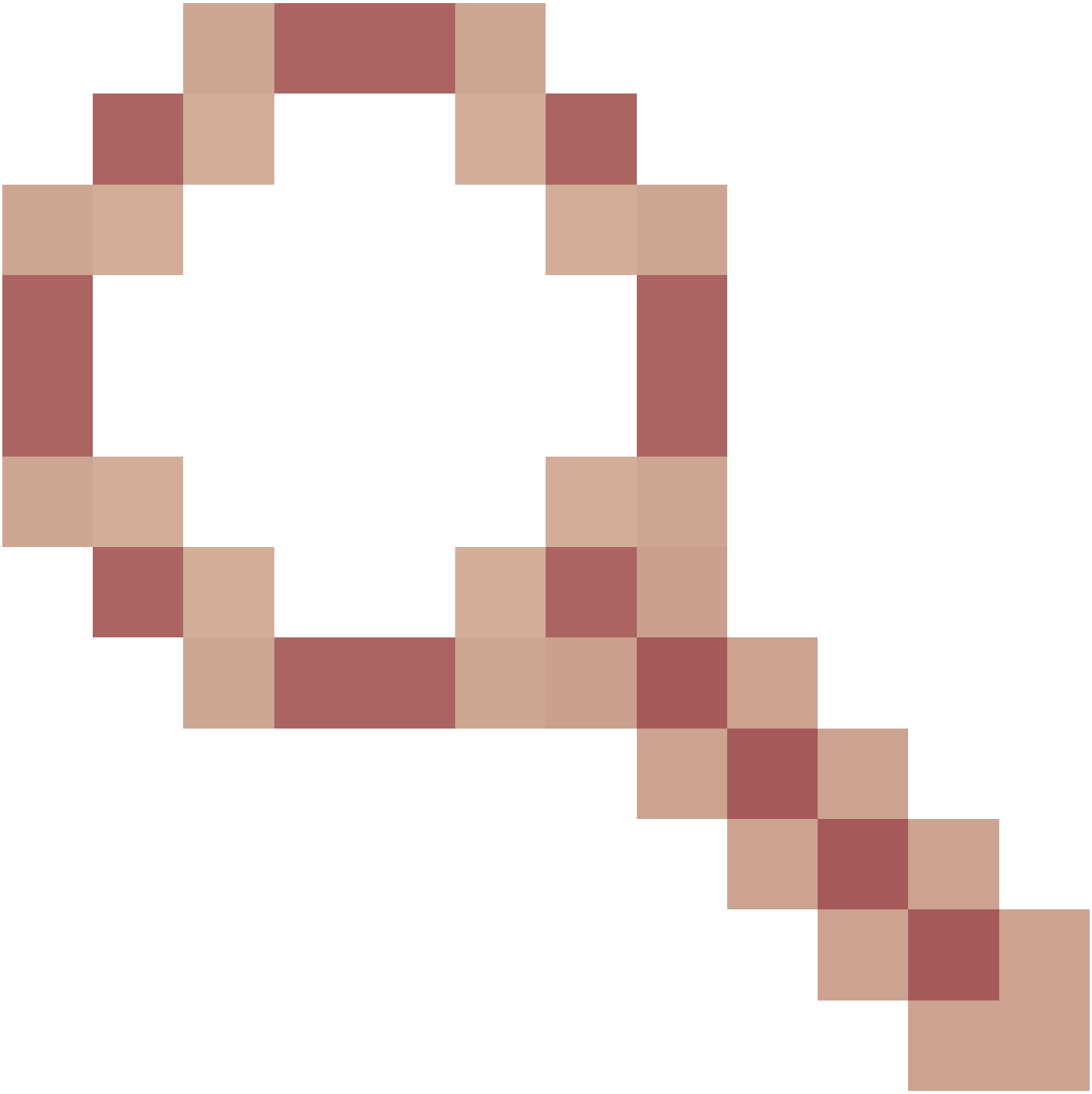
背景

Microsoft已正式弃用O365电子邮件帐户的基本身份验证。该计划于2019年宣布，后因COVID-19推迟至2022年10月。即使在2022年10月的最后期限之后，Microsoft也允许最后一次重新启用基本身份验证。这一最后例外于2022年12月31日结束。在此日期之后，Microsoft不再对任何客户启用基本身份验证。

此检查列表中的项目来自TAC与客户合作以配置此功能的服务请求。由于O365和Azure AD的许可方式，TAC无法在实验室中重新创建或检查这些项目。如果您需要有关这些内容的帮助，请联系Microsoft支持或您的内部IT支持团队。

检查项目

最低版本



为了响应思科漏洞ID CSCvr86493，ECE工程特别计划引入了OAuth对ECE O365的支持。您必须确保ECE安装了正确的ES并使用正确的文档。

- ECE 11.6(1) -需要ES12和ES12_ET1
- ECE 12.0(1) -需要ES6
- ECE 12.5(1) -需要ES3
- ECE 12.6(1) -需要ES1

最佳实践是安装适用于您的版本的最新ES。

系统配置

必须正确配置Web URL。具体设置根据ECE的版本而变化。必须配置该链接，使其与代理和管理员用于登录ECE的URL匹配，格式为https://ece.example.com。

在每个版本中设置名称：

11.5 – 12.5：分区级别设置，“Web服务器URL或负载均衡器URL”

12.6 + ：分区>应用>常规设置>“应用的外部URL”

此设置也用于单点登录(SSO)和聊天入口点的默认HTML。在OAuth for O365发行之前的版本中，除非使用代理SSO，否则此设置不是必需的。在使用OAuth的所有部署中，必须配置此功能。此外，这必须与用于登录管理控制台的FQDN匹配。

Azure AD应用程序

请确保在配置Azure AD应用程序时严格遵守文档。

具体说明：

1. 重定向URL - FQDN必须与ECE中应用程序设置的外部URL匹配，并且必须在访问管理控制台时使用。
2. 访问令牌-刷新令牌必须持续60分钟。

令牌生成

令牌生成过程是配置过程中最重要的步骤之一。最佳实践是，在您尝试发出令牌之前，确保浏览器已以隐名模式或专用模式打开。这将提示用户输入凭证。确保为其创建令牌的用户对邮箱具有完全控制权。

对此的解释是，大多数客户也使用Azure AD进行用户身份验证。当用户打开浏览器时，其凭证将通过Kerberos传递到login.microsoft.com站点。这反过来会导致向登录到工作站或服务器的用户（而不是可以访问邮箱的帐户）颁发令牌。

邮箱配置

确保邮箱启用了所需的协议。至少必须启用SMTP以允许发送邮件。您还必须根据设计启用IMAP或POP3。

Exchange许可证

确保已为Exchange Online中的邮箱分配了至少E3许可证。

邮箱权限

ECE支持两种邮箱访问用户帐户。

1. 邮箱帐户-此方法要求您为要进行ECE检查的每个邮箱创建一个帐户和访问令牌。例如，如果您有两个邮箱sales@example.com和support@example.com，则必须在部门中创建两个电子邮件帐户。对于一个帐户，您必须创建令牌并使用sales@example.com用户名和密码登录。必须使用support@example.com用户名和密码创建第二个帐户令牌。

2. 共享帐户-通过此方法，您可以使用可以访问多个邮箱的单个邮件帐户。要继续使用销售和支持邮箱，请在此处创建一个帐户，但使用已授予完全控制邮箱的Azure AD帐户的用户名和密码创建令牌。

两种访问方法各有利弊，但哪种方法最适合您的特定环境，由您决定。

网络连接

ECE要求服务服务器和所有应用服务器均可访问O365域以及login.microsoft.com域。在应用服务器上创建初始令牌时，所有后续令牌更新均在服务服务器上进行。服务服务器具有检索器和调度器进程，因此IMAP/POP3和SMTP端口必须对此服务器开放。此外，应用服务器必须能够发送电邮，以便警报通知正常运行。在您尝试设置或使用O365集成之前，请确认已打开《安装指南》中调用的所有端口。

URL

服务服务器和应用服务器必须至少能够访问这些URL。

- *.office365.com

-login.microsoftonline.com

您的特定实施可能需要其他URL。

端口

服务服务器和应用服务器必须至少能够访问这些端口。

- TCP 443 - (HTTPS)用于生成和更新访问令牌并刷新令牌

- TCP 587 - (通过STARTTLS的SMTP) 由调度程序进程和警报通知进程使用

- TCP 993 - (SSL/TLS上的IMAP) 由检索器进程使用

- TCP 995 - (通过SSL/TLS的POP3) 供检索器进程使用

参考：[POP、IMAP和SMTP设置]

连通性测试

Microsoft创建了一个可用于测试连通性的网站。这不是思科或eGain提供的工具，TAC无法为其使用提供任何支持。您可以从应用和服务服务器使用它来测试您的配置和连接。ECE仅支持SMTP用于出站，IMAP或POP3用于入站。请同时使用来自Microsoft网站的“出站SMTP电子邮件”测试和“POP电子邮件”测试以及“IMAP电子邮件”测试。

https://testconnectivity.microsoft.com/tests/o365

文档链接

11.6(1)

- UCCE/PCCE -电子邮件资源管理员指南

12.0(1)

- UCCE -邮件资源管理员指南(UCCE)
- PCCE - 聊天和电子邮件资源管理员指南(PCCE)

12.5(1)

- UCCE -邮件资源管理员指南(UCCE)
- PCCE - 聊天和电子邮件资源管理员指南(PCCE)

12.6(1)

- UCCE/PCCE -电子邮件和路由资源管理员指南

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。