使用Azure Active Directory配置ISE 3.0 REST ID

目录

简介

本文档介绍通过REST身份服务和资源所有者密码凭据实现的Cisco ISE 3.0与Azure AD的集成。

背景信息

本文档介绍如何配置身份服务引擎(ISE)3.0与通过具象状态传输(REST)身份(ID)服务在资源所有者密码凭证(ROPC)的帮助下实施的Microsoft(MS)Azure Active Directory(AD)的集成并对其进行故障排除。

先决条件

要求

Cisco 建议您具有以下主题的基础知识：

- ISE
- MS Azure广告
- 了解ROPC协议的实施及其限制；链路

使用的组件

本文档中的信息基于以下软件和硬件版本：

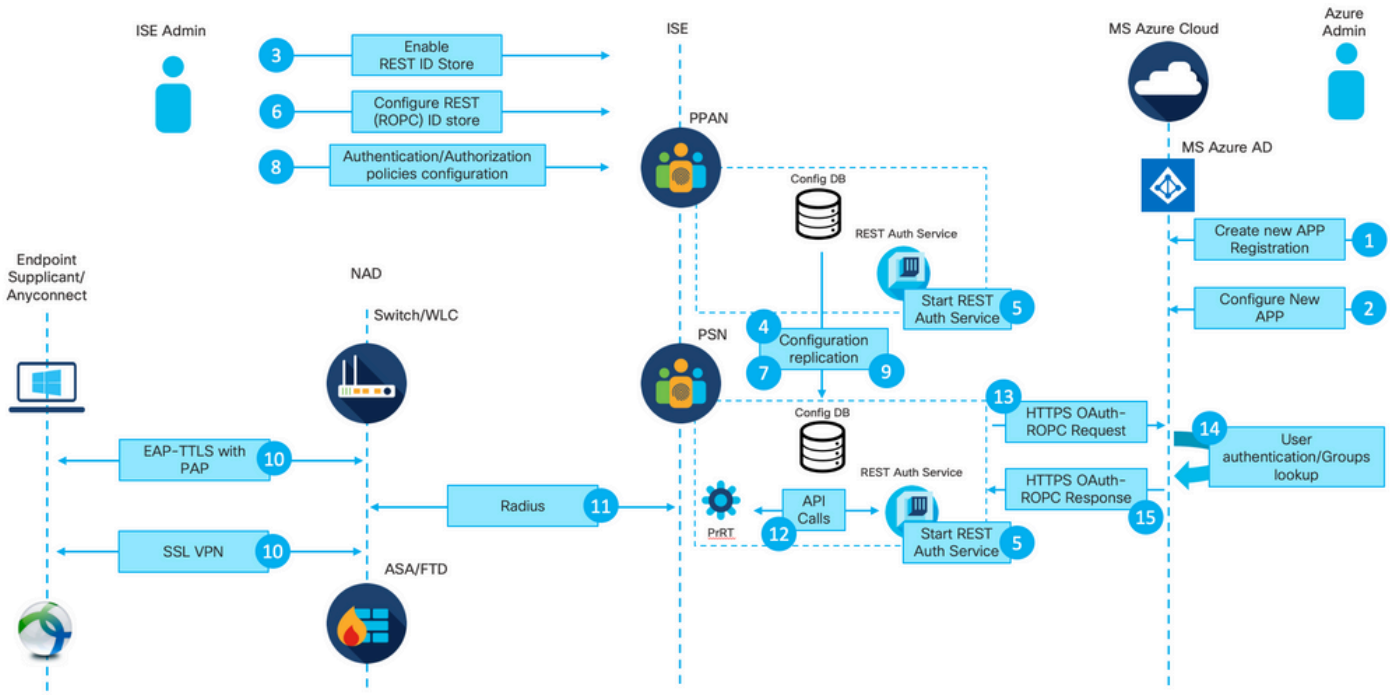
- 思科ISE版本3.0
- MS Azure广告
- WS-C3850-24P，带16.9.2
- 带9.10(1)的ASAv
- Windows 10.0.18363

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。

配置

ISE REST ID功能基于ISE 3.0 - REST身份验证服务中引入的新服务。此服务负责通过开放式授权(OAuth)ROPC交换与Azure AD进行通信，以执行用户身份验证和组检索。 REST身份验证服务默认禁用，在管理员启用后，它将在部署中的所有ISE节点上运行。 由于在用户身份验证时与云进行REST身份验证服务通信，因此路径上的任何延迟都会给身份验证/授权流程带来额外的延迟。此延迟不在ISE控制范围之内，必须仔细规划和测试REST身份验证的任何实施，以避免影响其他ISE服务。

高级流概述



1. Azure云管理员创建新的应用程序（应用）注册。此应用的详细信息稍后将在ISE上使用，以便与Azure AD建立连接。

2. Azure云管理员必须使用以下设置配置应用：

- 创建客户端密码
- 启用ROPC
- 添加组领款申请
- 定义应用编程接口(API)权限

3. ISE管理员启用REST身份验证服务。在执行任何其他操作之前，必须先完成此操作。

4.将更改写入配置数据库并在整个ISE部署中复制。

5.在所有节点上启动REST身份验证服务。

6. ISE管理员使用步骤2中的详细信息配置REST ID存储。

7.将更改写入配置数据库并在整个ISE部署中复制。

8. ISE管理员创建新的身份库序列或修改已有的身份库序列并配置身份验证/授权策略。

9.将更改写入配置数据库并在整个ISE部署中复制。

10.终端发起身份验证。根据ROPC协议规范，必须通过加密HTTP连接以明文形式向Microsoft身份平台提供用户密码；因此，到目前为止，ISE支持的唯一可用身份验证选项为：

- 以密码身份验证协议(PAP)作为内部方法的可扩展身份验证协议 — 隧道传输层安全(EAP-TTLS)
- 使用PAP的AnyConnect SSL VPN身份验证

11.通过Radius与ISE策略服务节点(PSN)交换。

12. Process Runtime(PrRT)通过内部API向REST ID服务发送包含用户详细信息（用户名/密码）的请求。

13. REST ID服务将OAuth ROPC请求发送到Azure AD over HyperText Transfer Protocol Secure(HTTPS)。

14. Azure AD执行用户身份验证并获取用户组。

15.向ISE返回身份验证/授权结果。

在点15之后，身份验证结果和获取的组返回到PrRT，其中涉及策略评估流程并分配最终身份验证/授权结果。Access-Accept with attributes from the authorization profile或Access-Reject returned to Network Access Device(NAD)。

配置Azure AD for Integration

1.查找AppRegistration Service（如图所示）。

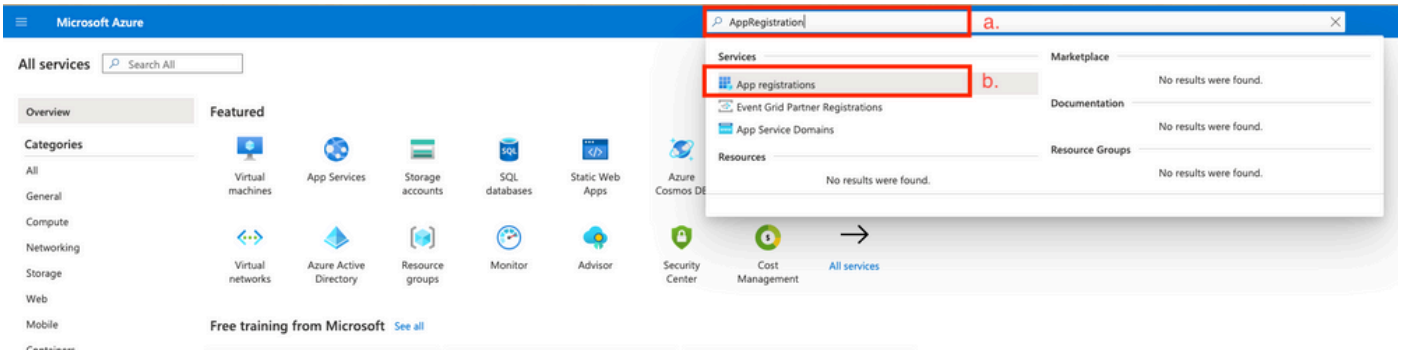


图 2.

a.在全局搜索栏中键入AppRegistration。

b.单击App registration服务。

2.创建新的应用注册。

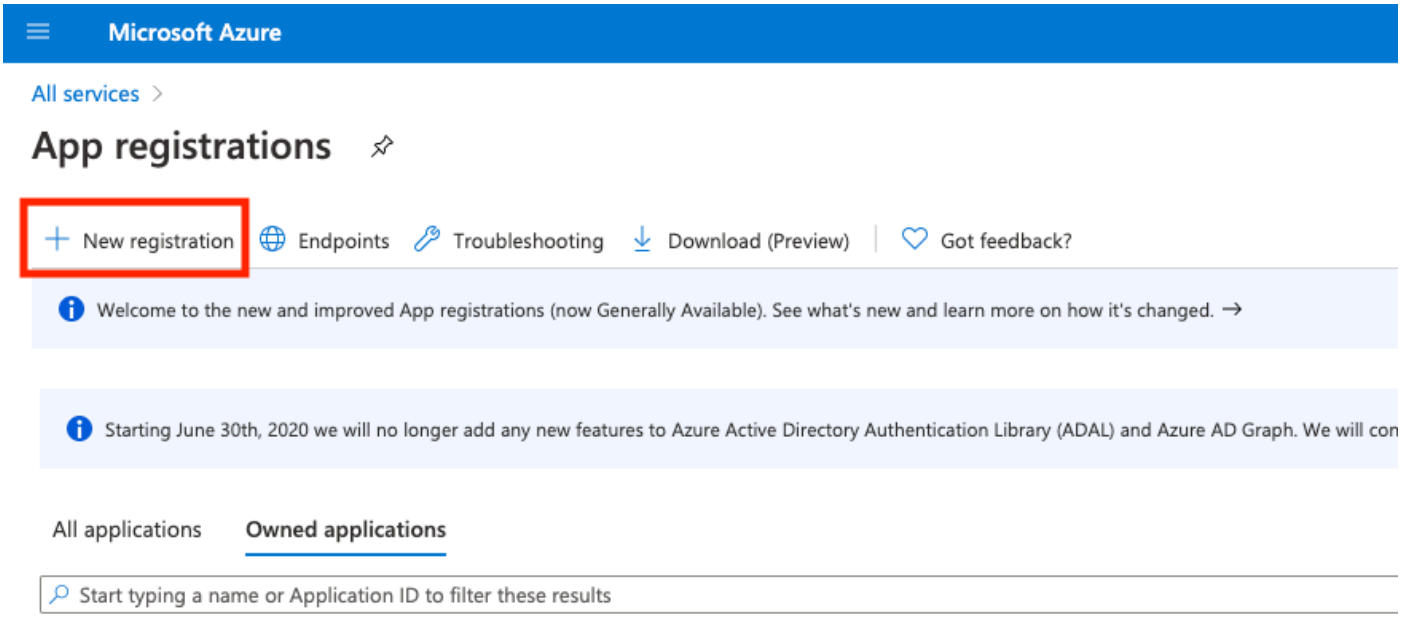


图 3.

3.注册新应用。

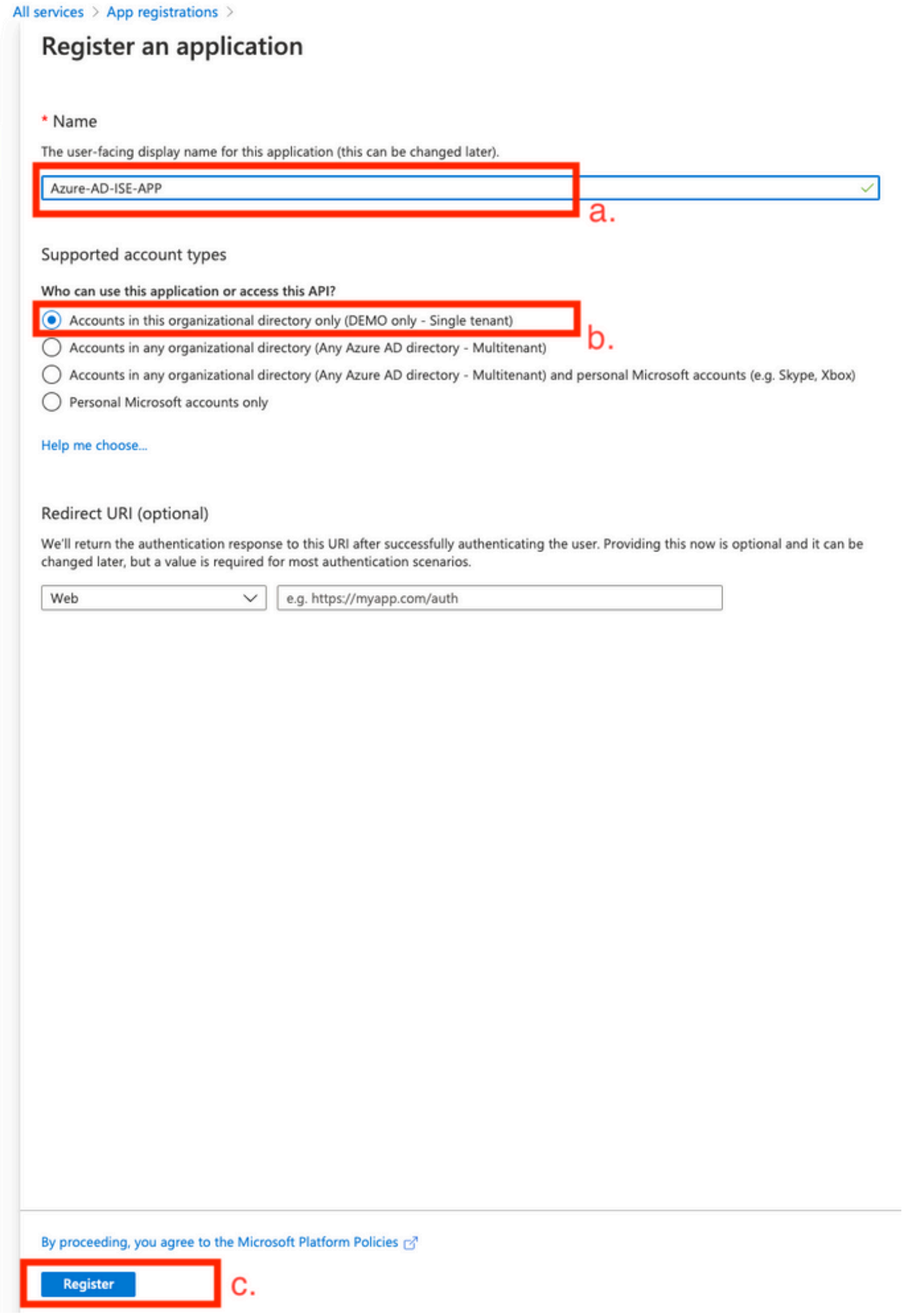

All services > App registrations >
Register an application
* Name
The user-facing display name for this application (this can be changed later).
Azure-AD-ISE-APP
a.
Supported account types
Who can use this application or access this API?
Accounts in this organizational directory only (DEMO only - Single tenant)
b.
Accounts in any organizational directory (Any Azure AD directory - Multitenant)
Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
Personal Microsoft accounts only
Help me choose...
Redirect URI (optional)
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.
Web
e.g. https://myapp.com/auth
By proceeding, you agree to the Microsoft Platform Policies
Register
c.

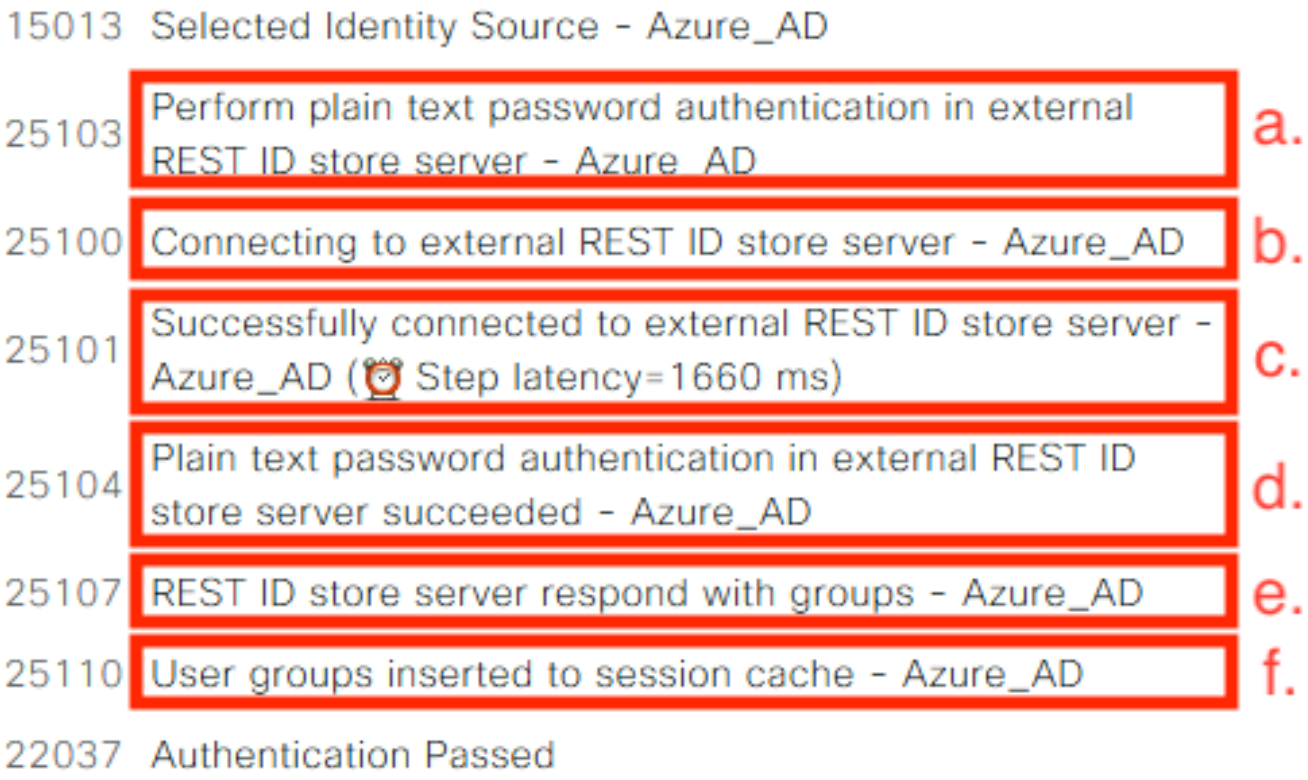
图 4.

```
ISE PROCESS NAME STATE PROCESS ID
--------------------------------------------------------------------
Database Listener running 101790
Database Server running 92 PROCESSES
Application Server running 39355
Profiler Database running 107909
ISE Indexing Engine running 115132
AD Connector running 116376
M&T Session Database running 107694
M&T Log Processor running 112553
Certificate Authority Service running 116226
EST Service running 119875
SXP Engine Service disabled
Docker Daemon running 104217
TC-NAC Service disabled
pxGrid Infrastructure Service disabled
pxGrid Publisher Subscriber Service disabled
pxGrid Connection Manager disabled
pxGrid Controller disabled
PassiveID WMI Service disabled
PassiveID Syslog Service disabled
PassiveID API Service disabled
PassiveID Agent Service disabled
PassiveID Endpoint Service disabled
PassiveID SPAN Service disabled
DHCP Server (dhcpd) disabled
DNS Server (named) disabled
ISE Messaging Service running 104876
ISE API Gateway Database Service running 106853
ISE API Gateway Service running 110426
Segmentation Policy Service disabled
```

REST Auth Service running 63052

```
SSE Connector disabled
```

2.验证身份验证时是否使用了REST ID存储（请检查详细身份验证报告的步骤。部分）。



a. PSN使用选定的REST ID存储启动纯文本身份验证。

b.与Azure云建立的连接。

c.实际身份验证步骤 — 注意此处显示的延迟值。如果所有使用安全云的身份验证都遇到严重延迟，这会影响其他ISE流，因此整个ISE部署变得不稳定。

d.确认身份验证成功。

e.确认答复中提供的群组数据。

f.使用用户组数据填充的会话上下文。有关ISE会话管理流程的更多详细信息，请考虑阅读本文的 — 链接。

3.确认已选择预期身份验证/授权策略（对于详细身份验证报告的此调查概述部分）。

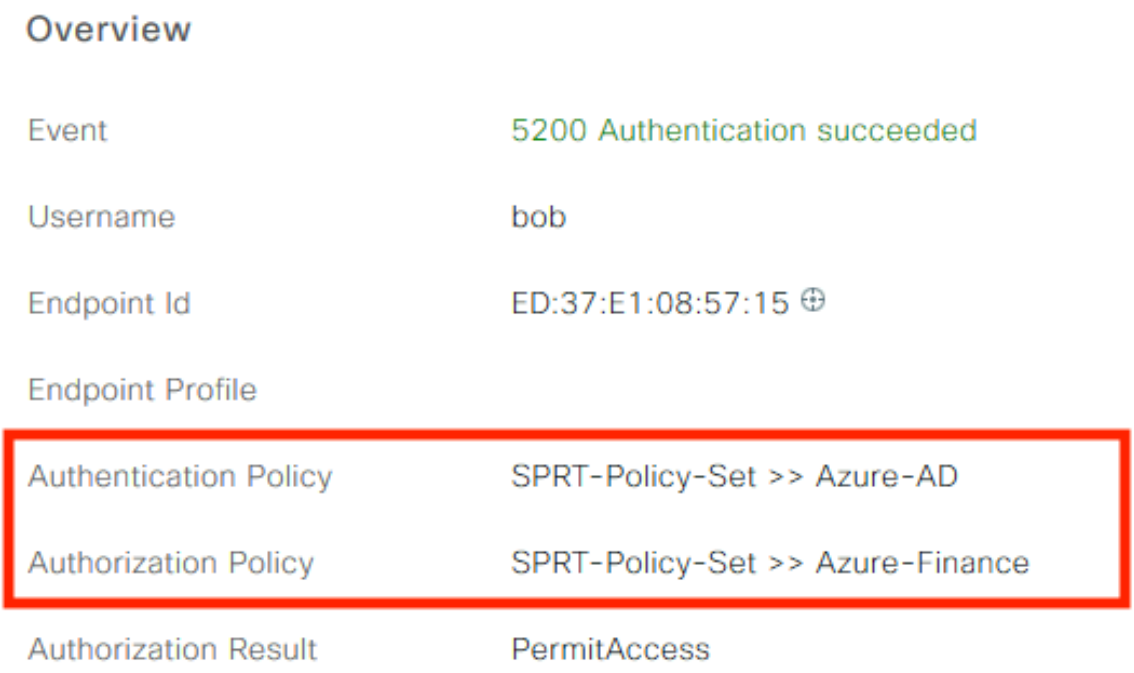


图 30.

故障排除

本节提供可用于对配置进行故障排除的信息。

REST Auth服务问题

要排除REST身份验证服务的所有问题，您需要首先查看ADE.log文件。支持捆绑包位置-/support/adeos/ade

REST身份验证服务的搜索关键字是ROPC-control。

此示例显示REST身份验证服务如何启动：

```
2020-08-30T11:15:38.624197+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] S
2020-08-30T11:15:39.217794+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] i
2020-08-30T11:15:39.290301+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] I
2020-08-30T11:15:39.291858+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] D
2020-08-30T11:15:39.293768+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] L
2020-08-30T11:15:39.359490+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] E
2020-08-30T11:15:42.789242+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] L
2020-08-30T11:15:42.830411+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] D
2020-08-30T11:15:42.832131+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] S
2020-08-30T11:15:42.844051+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] i
2020-08-30T11:15:53.479968+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] C
2020-08-30T11:15:55.325973+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] C
2020-08-30T11:15:57.103245+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] C
2020-08-30T11:15:57.105752+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] C
2020-08-30T11:15:57.278374+02:00 skuchere-ise30-1 admin: info:[application:operation:ROPC-control.sh] C
```

如果服务无法启动或意外中断，最好在出现问题的时间范围内查看ADE.log。

REST ID身份验证问题

如果使用REST ID存储时身份验证失败，则始终需要从详细的身份验证报告开始。在“其他属性”区域中，您可以看到包含由Azure云返回的错误的RestAuthErrorMsg部分：

RestAuthErrorMsg	Error Key - invalid_client | Error Description - AADSTS7000218: The request body must contain the following parameter: 'client_assertion' or 'client_secret'. Trace ID: e33912ff-18af-4f81-acc9-efda91873900 Correlation ID: 519641db-a8ea-49df-85aa-ddd2b53a0c28 Timestamp: 2020-09-13 19:11:47Z | Error Codes - [7000218] | Error URI - https://login.microsoftonline.com/error?code=7000218

图 31.

使用日志文件

在ISE 3.0中，由于REST ID功能的受控引进，默认情况下启用它的调试。所有与REST ID相关的日志都存储在ROPC文件中，可以通过CLI查看：

```
skuchere-ise30-1/admin# sh logging application | i ropc
755573 Oct 04 2020 09:10:29 ropc/ropc.log

skuchere-ise30-1/admin# sh logging application ropc/ropc.log
23:49:31.449 [http-nio-9601-exec-6] DEBUG c.c.i.r.c.ROPCController - Starting ROPC auth flow
23:49:31.788 [http-nio-9601-exec-6] DEBUG c.c.i.r.u.ScimUtility - Found user and pass in the SCIM filte
```

在安装了补丁的ISE 3.0上，请注意文件名是rest-id-store.log，而不是ropc.log。前面提供的搜索示例有效，因为文件夹名称未更改。

也可以从ISE支持捆绑包提取这些文件。

以下是几个显示不同工作和非工作场景的日志示例：

1. Azure Graph不受ISE节点信任时的证书错误。当组未加载到REST ID存储设置中时，可以看到此错误。

```
20:44:54.420 [http-nio-9601-exec-7] DEBUG c.c.i.r.u.HttpClientWrapper - Start proxy load for URI 'https

20:44:54.805 [http-nio-9601-exec-7] ERROR c.c.i.r.p.a.AzureIdentityProviderFacade - Couldn't fetch appl
javax.net.ssl.SSLHandshakeException: sun.security.validator.ValidatorException: No trusted certificate
at sun.security.ssl.Alerts.getSSLException(Alerts.java:192)
at sun.security.ssl.SSLSocketImpl.fatal(SSLSocketImpl.java:1946)
```

```
at sun.security.ssl.Handshaker.fatalSE(Handshaker.java:316)
at sun.security.ssl.Handshaker.fatalSE(Handshaker.java:310)
at sun.security.ssl.ClientHandshaker.serverCertificate(ClientHandshaker.java:1639)
```

此问题表明Microsoft graph API证书不受ISE信任。ISE 3.0.0.458在受信任存储中没有安装DigiCert全局根G2 CA。这记录在缺陷中

- Cisco Bug ID CSCvv80297要解决此问题，您需要在ISE受信任存储中安装DigiCert全局根G2 CA，并将其标记为思科服务的受信任项。

可以从此处下载证书 — https://www.digicert.com/kb/digicert-root-certificates.htm

2.错误的应用程序密钥。

```
10:57:53.200 [http-nio-9601-exec-1] DEBUG c.c.i.r.e.c.CertificateCache - SSLContext initialized with tr
10:57:54.205 [http-nio-9601-exec-1] ERROR c.c.i.r.u.RestUtility - Error response in 'POST' request. Sta
10:57:54.206 [http-nio-9601-exec-1] ERROR c.c.i.r.c.ROPCController - Request related Error
com.cisco.ise.ROPC.entities.exceptions.InvalidApplicationAuthException: AADSTS7000215: Invalid client s
Trace ID: 99cc29f7-502a-4aaa-b2cf-1daeb071b900
Correlation ID: a697714b-5ab2-4bd1-8896-f9ad40d625e5
Timestamp: 2020-09-29 09:01:36Z - Error Codes: [7000215]
at com.cisco.ise.ROPC.providers.azure.AzureIdentityProviderFacade.authenticateApplication(AzureIdentity
```

3.错误的应用ID。

```
21:34:36.090 [http-nio-9601-exec-4] DEBUG c.c.i.r.e.c.CertificateCache - SSLContext initialized with tr
21:34:36.878 [http-nio-9601-exec-4] ERROR c.c.i.r.u.RestUtility - Error response in 'POST' request. Sta
21:34:36.879 [http-nio-9601-exec-4] ERROR c.c.i.r.c.ROPCController - Request related Error
com.cisco.ise.ROPC.entities.exceptions.InvalidApplicationAuthException: AADSTS700016: Application with
Trace ID: 6dbd0fdd-0128-4ea8-b06a-5e78f37c0100
Correlation ID: eced0c34-fcc1-40b9-b033-70e5abe75985
Timestamp: 2020-08-31 19:38:34Z - Error Codes: [700016]
```

4.未找到用户。

```
10:43:01.351 [http-nio-9601-exec-2] ERROR c.c.i.r.u.RestUtility - Error response in 'POST' request. Sta
10:43:01.352 [http-nio-9601-exec-2] ERROR c.c.i.r.c.ROPCController - Request related Error
com.cisco.ise.ROPC.entities.exceptions.ROPCResponseErrorException: {"error":"invalid_grant","error_desc
at com.cisco.ise.ROPC.providers.azure.AzureIdentityProviderFacade.authenticateUser(AzureIdentityProvide
at com.cisco.ise.ROPC.providers.azure.AzureROPCFlow.authenticateUser(AzureROPCFlow.java:100)
at com.cisco.ise.ROPC.providers.azure.AzureROPCFlow.doEntireFlow(AzureROPCFlow.java:69)
at com.cisco.ise.ROPC.controllers.ROPCController.ROPCAuthFlow(ROPCController.java:168)
at com.cisco.ise.ROPC.controllers.ROPCController.get(ROPCController.java:85)
at sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method)
at sun.reflect.NativeMethodAccessorImpl.invoke(NativeMethodAccessorImpl.java:62)
at sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:43)
at java.lang.reflect.Method.invoke(Method.java:498)
```

5.用户密码已过期 — 通常可以为新创建的用户发生，因为Azure管理员定义的密码需要在登录到Office365时更改。

```
10:50:55.096 [http-nio-9601-exec-4] ERROR c.c.i.r.u.RestUtility - Error response in 'POST' request. Sta
10:50:55.097 [http-nio-9601-exec-4] ERROR c.c.i.r.c.ROPCController - Request related Error
com.cisco.ise.ROPC.entities.exceptions.ROPCResponseErrorException: {"error":"invalid_grant","error_desc
at com.cisco.ise.ROPC.providers.azure.AzureIdentityProviderFacade.authenticateUser(AzureIdentityProvide
at com.cisco.ise.ROPC.providers.azure.AzureROPCFlow.authenticateUser(AzureROPCFlow.java:100)
at com.cisco.ise.ROPC.providers.azure.AzureROPCFlow.doEntireFlow(AzureROPCFlow.java:69)
at com.cisco.ise.ROPC.controllers.ROPCController.ROPCAuthFlow(ROPCController.java:168)
at com.cisco.ise.ROPC.controllers.ROPCController.get(ROPCController.java:85)
at sun.reflect.GeneratedMethodAccessor53.invoke(Unknown Source)
at sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:43)
at java.lang.reflect.Method.invoke(Method.java:498)
```

6.由于API权限错误，无法加载组。

```
12:40:06.624 [http-nio-9601-exec-9] ERROR c.c.i.r.u.RestUtility - Error response in 'GET' request. Statu
"error": {
"code": "Authorization_RequestDenied",
"message": "Insufficient privileges to complete the operation.",
"innerError": {
"date": "2020-08-30T10:43:59",
"request-id": "da458fa4-cc8a-4ae8-9720-b5370ad45297"
}
}
}'
```

7.当Azure端上不允许使用ROPC时，身份验证失败。

```
11:23:10.824 [http-nio-9601-exec-2] DEBUG c.c.i.r.e.c.CertificateCache - SSLContext initialized with tr
11:23:11.776 [http-nio-9601-exec-2] ERROR c.c.i.r.u.RestUtility - Error response in 'POST' request. Sta
11:23:11.777 [http-nio-9601-exec-2] ERROR c.c.i.r.c.ROPCController - Request related Error
com.cisco.ise.ROPC.entities.exceptions.ROPCResponseErrorException: {"error":"invalid_client","error_des
at com.cisco.ise.ROPC.providers.azure.AzureIdentityProviderFacade.authenticateUser(AzureIdentityProvide
at com.cisco.ise.ROPC.providers.azure.AzureROPCFlow.authenticateUser(AzureROPCFlow.java:100)
at com.cisco.ise.ROPC.providers.azure.AzureROPCFlow.doEntireFlow(AzureROPCFlow.java:69)
at com.cisco.ise.ROPC.controllers.ROPCController.ROPCAuthFlow(ROPCController.java:168)
at com.cisco.ise.ROPC.controllers.ROPCController.get(ROPCController.java:85)
at sun.reflect.GeneratedMethodAccessor53.invoke(Unknown Source)
at sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:43)
at java.lang.reflect.Method.invoke(Method.java:498)
```

8.身份验证失败，因为用户不属于Azure端上的任何组。

```
21:54:55.976 [http-nio-9601-exec-5] DEBUG c.c.i.r.e.c.CertificateCache - SSLContext initialized with tr
21:54:57.312 [http-nio-9601-exec-5] ERROR c.c.i.r.p.a.AzureROPCFlow - Missing claims in the id token: "
21:54:57.313 [http-nio-9601-exec-5] ERROR c.c.i.r.c.ROPCController - Server Error
com.cisco.ise.ROPC.entities.exceptions.JsonParseException: Json exception: Missing claims in the id tok
at com.cisco.ise.ROPC.providers.azure.AzureROPCFlow.validateIdTokenPayload(AzureROPCFlow.java:93)
```

9.成功的用户身份验证和组检索。

```
11:46:03.035 [http-nio-9601-exec-7] DEBUG c.c.i.r.c.ROPCController - Starting ROPC auth flow
11:46:03.037 [http-nio-9601-exec-7] DEBUG c.c.i.r.u.ScimUtility - Found user and pass in the SCIM filte
11:46:03.037 [http-nio-9601-exec-7] DEBUG c.c.i.r.c.ROPCController - Getting the right ROPC handler for
11:46:03.037 [http-nio-9601-exec-7] DEBUG c.c.i.r.c.ROPCController - Getting user groups from handler
11:46:03.038 [http-nio-9601-exec-7] DEBUG c.c.i.r.u.HttpClientWrapper - Start building http client
11:46:03.039 [http-nio-9601-exec-7] DEBUG c.c.i.r.u.HttpClientWrapper - Start proxy load for URI 'https
11:46:03.039 [http-nio-9601-exec-7] DEBUG c.c.i.r.u.HttpClientWrapper - Start check if host is bypass
11:46:03.039 [http-nio-9601-exec-7] DEBUG c.c.i.r.u.HttpClientWrapper - Iterating bypass hosts '192.168
11:46:03.040 [http-nio-9601-exec-7] DEBUG c.c.i.r.u.HttpClientWrapper - Proxy server found with address
11:46:03.040 [http-nio-9601-exec-7] DEBUG c.c.i.r.u.HttpClientWrapper - Start adding proxy credentials
11:46:03.040 [http-nio-9601-exec-7] DEBUG c.c.i.r.u.HttpClientWrapper - No credentials found for proxy
11:46:03.040 [http-nio-9601-exec-7] DEBUG c.c.i.r.e.c.CertificateCache - Created SSLContext with TLSv1.
11:46:03.041 [http-nio-9601-exec-7] DEBUG c.c.i.r.e.c.CertificateCache - SSLContext initialized with tr
11:46:04.160 [http-nio-9601-exec-7] DEBUG c.c.i.r.c.ROPCController - The ROPCHandlerResponse is: {
"schemas" : [ "urn:ietf:params:scim:schemas:core:2.0:User" ],
"userName" : "username",
"name" : {
"formatted" : "bob"
},
"displayName" : "bob",
"groups" : [ {
"value" : "17db2c79-fb87-4027-ae13-88eb5467f25b"
} ],
"roles" : [ ]
}
```

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）。