使用Azure Active Directory配置ISE 3.0 REST ID

目錄

簡介

本文檔介紹通過REST身份服務通過資源所有者密碼憑據實現的Cisco ISE 3.0與Azure AD的整合。

背景資訊

本文檔介紹如何配置身份服務引擎(ISE)3.0與Microsoft(MS)Azure Active Directory(AD)的整合並對其進行故障排除，該整合是通過在資源所有者密碼憑據(ROPC)的幫助下實現的具象狀態傳輸(REST)身份(ID)服務實現的。

必要條件

需求

思科建議您瞭解以下主題的基本知識：

- ISE
- MS Azure AD
- 瞭解ROPC協定實施和限制；鏈接

採用元件

本文中的資訊係根據以下軟體和硬體版本：

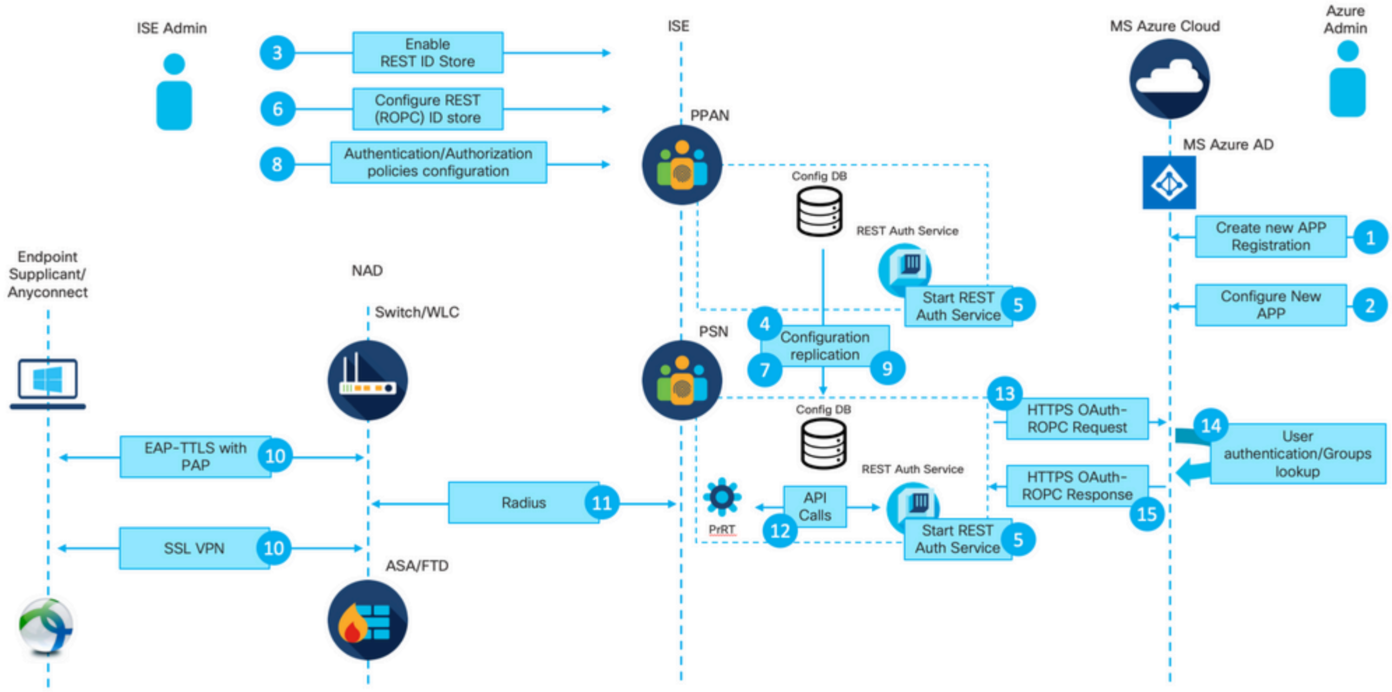
- Cisco ISE版本3.0
- MS Azure AD
- WS-C3850-24P，帶16.9.2軟體
- 採用9.10(1)的ASAv
- Windows 10.0.18363

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

設定

ISE REST ID功能基於ISE 3.0 - REST身份驗證服務中引入的新服務。此服務負責通過Open Authorization(OAuth)ROPC交換與Azure AD通訊，以便執行使用者身份驗證和組檢索。 REST身份驗證服務預設處於禁用狀態，在管理員啟用後，它將在部署中的所有ISE節點上運行。 由於在使用者身份驗證時與雲進行REST身份驗證服務通訊，因此路徑上的任何延遲都會給身份驗證/授權流帶來額外的延遲。此延遲不在ISE控制範圍內，必須仔細規劃和測試REST身份驗證的任何實施，以避免對其他ISE服務產生影響。

高級流概述



1. Azure雲管理員建立新的應用程式（應用）註冊。此應用的詳細資訊稍後將在ISE上使用，以便與Azure AD建立連線。

2. Azure雲管理員必須使用以下內容配置應用：

- 建立客戶端密碼
- 啟用ROPC
- 新增組宣告
- 定義應用程式程式設計介面(API)許可權

3. ISE管理員啟用REST身份驗證服務。在執行任何其他操作之前，必須先完成此操作。

4.將更改寫入配置資料庫並在整個ISE部署中複製。

5.在所有節點上啟動REST身份驗證服務。

6. ISE管理員使用步驟2中的詳細資訊配置REST ID儲存。

7.將更改寫入配置資料庫並在整個ISE部署中複製。

8. ISE管理員建立新的身份庫序列或修改已存在的身份庫序列並配置身份驗證/授權策略。

9.將更改寫入配置資料庫並在整個ISE部署中複製。

10.端點啟動身份驗證。根據ROPC協定規范，必須通過加密的HTTP連線以明文形式向Microsoft身份平台提供使用者密碼；因此，ISE目前支援的唯一可用身份驗證選項為：

- 使用密碼驗證通訊協定(PAP)作為內部方法的可擴充身份驗證通訊協定 — 通道傳輸層安全(EAP-TTLS)
- 使用PAP的AnyConnect SSL VPN身份驗證

11.通過Radius與ISE策略服務節點(PSN)交換。

12. Process Runtime(PrRT)通過內部API向REST ID服務傳送包含使用者詳細資訊（使用者名稱/密碼）的請求。

13. REST ID服務將OAuth ROPC請求通過超文本傳輸協議安全(HTTPS)傳送到Azure AD。

14. Azure AD執行使用者身份驗證並提取使用者組。

15.身份驗證/授權結果返回到ISE。

在點15之後，身份驗證結果和提取的組返回到PrRT，其中涉及策略評估流程並分配最終身份驗證/授權結果。Access-Accept with attributes from the authorization profile或Access-Reject returned to Network Access Device(NAD)。

配置用於整合的Azure AD

1.找到AppRegistration Service，如下圖所示。

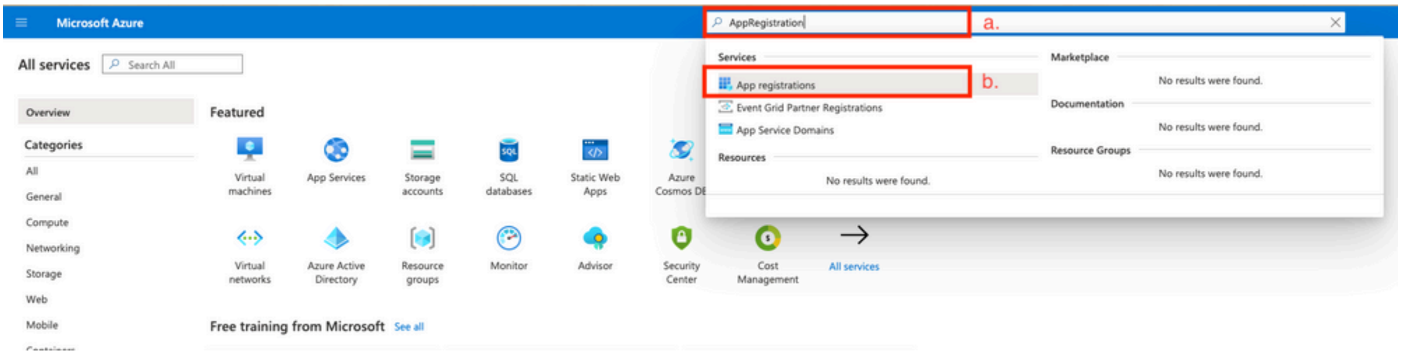
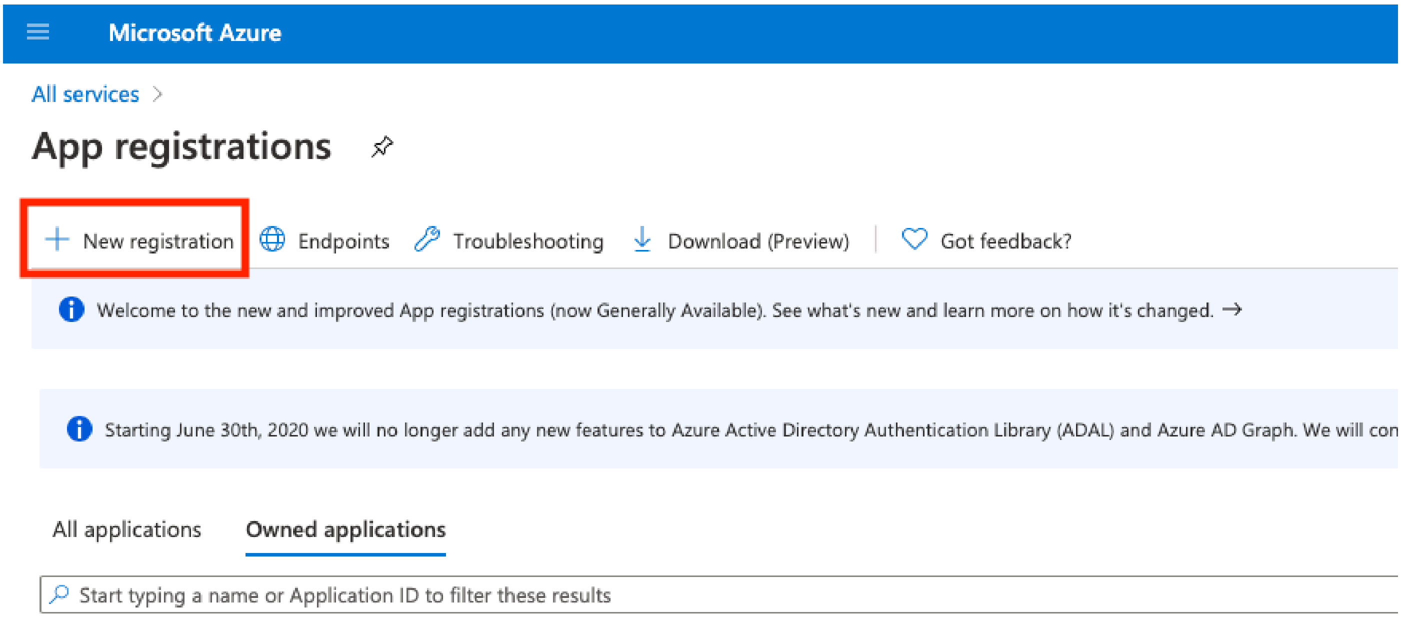


圖2.

a.在全域性搜尋欄中鍵入AppRegistration。

b.按一下App registration service。

2.建立新的應用註冊。



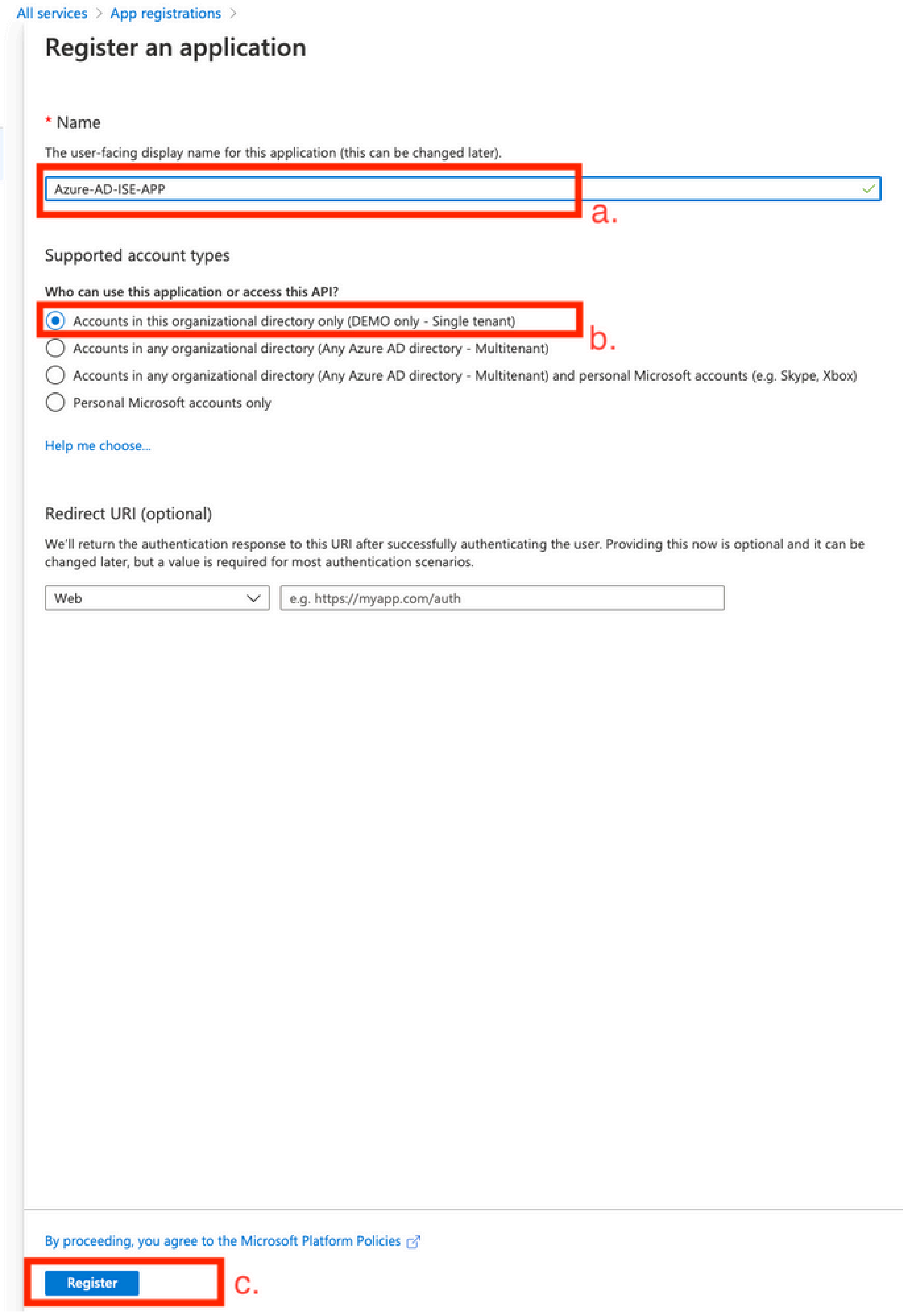
Welcome to the new and improved App registrations (now Generally Available). See what's new and learn more on how it's changed. →

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will con

All applications
Owned applications
Start typing a name or Application ID to filter these results

圖3.

3.註冊新應用。



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

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (DEMO only - Single tenant)

○ 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

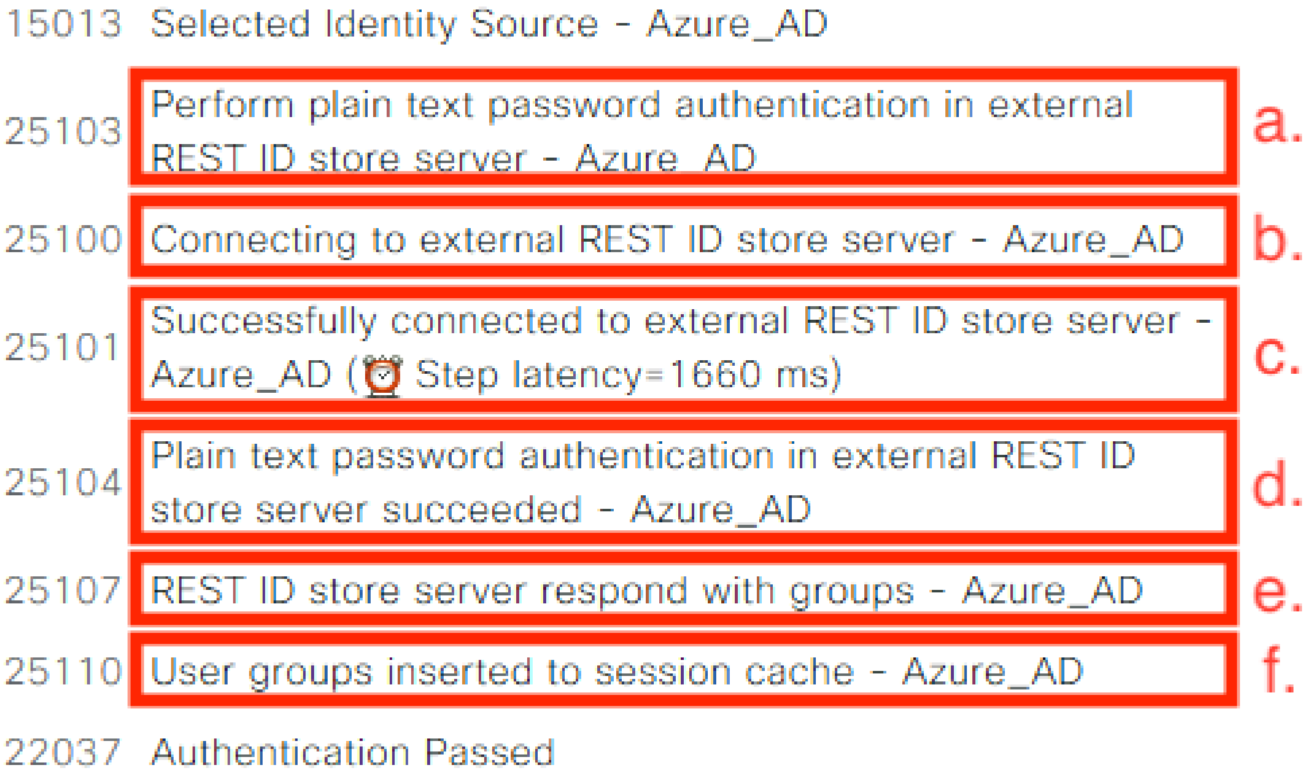
By proceeding, you agree to the Microsoft Platform Policies

圖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.驗證身份驗證時是否使用了REST ID儲存（請檢視詳細的身份驗證報告的「步驟。」部分）。



```
15013  Selected Identity Source - Azure_AD
25103  Perform plain text password authentication in external
       REST ID store server - Azure_AD
25100  Connecting to external REST ID store server - Azure_AD
25101  Successfully connected to external REST ID store server -
       Azure_AD (⏰ Step latency=1660 ms)
25104  Plain text password authentication in external REST ID
       store server succeeded - Azure_AD
25107  REST ID store server respond with groups - Azure_AD
25110  User groups inserted to session cache - Azure_AD
22037  Authentication Passed
```

a. PSN使用選定的REST ID儲存啟動純文字檔案身份驗證。

b.已與Azure雲建立連線。

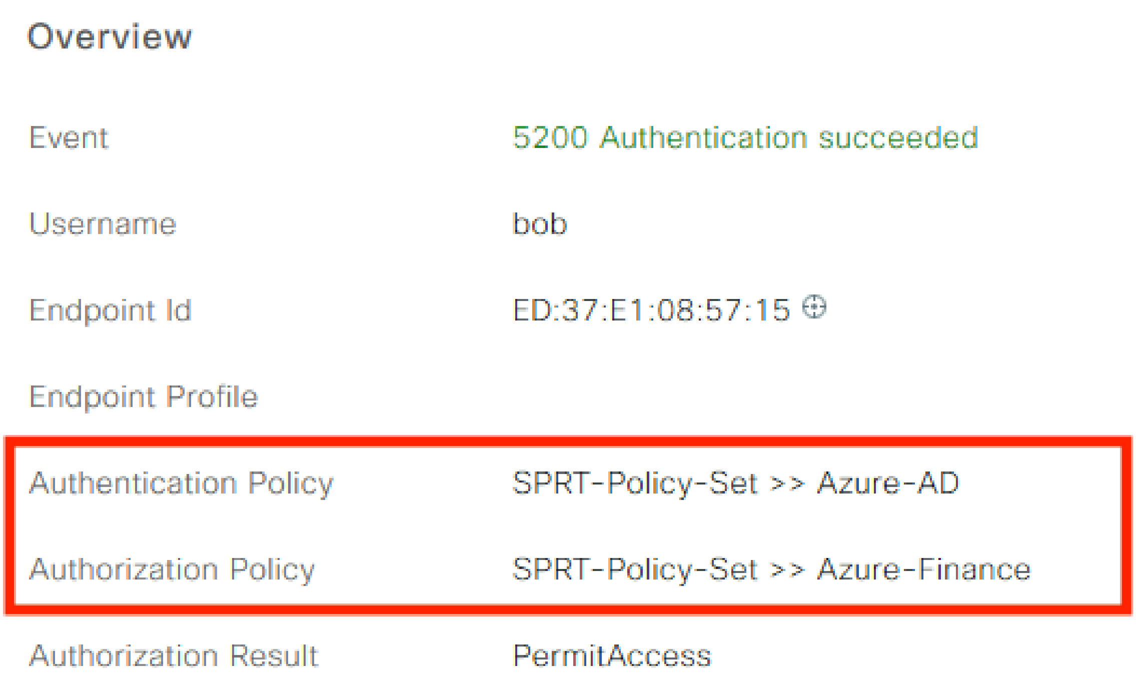
c.實際驗證步驟 — 注意此處顯示的延遲值。如果您使用安全雲的所有身份驗證都遇到嚴重延遲，這會影響其他ISE流，因此整個ISE部署變得不穩定。

d.確認身份驗證成功。

e.確認答覆中提供的群組資料。

f.使用使用者組資料填充的會話上下文。有關ISE會話管理流程的更多詳細資訊，請考慮閱讀本文的 — 連結。

3.確認已選擇預期的身份驗證/授權策略（對於詳細的身份驗證報告的此調查概述部分）。



Overview

Event 5200 Authentication succeeded

Username bob

Endpoint Id ED:37:E1:08:57:15

Endpoint Profile

Authentication Policy SPRT-Policy-Set >> Azure-AD

Authorization Policy SPRT-Policy-Set >> Azure-Finance

Authorization Result PermitAccess

圖30

疑難排解

本節提供的資訊用於對組態進行疑難排解。

REST Auth服務問題

若要疑難排解REST身份驗證服務的所有問題，需要首先複查ADE.log文件。支援捆綁包位置- /support/adeos/ade

REST Auth Service的搜尋關鍵字是 — ROPC-control。

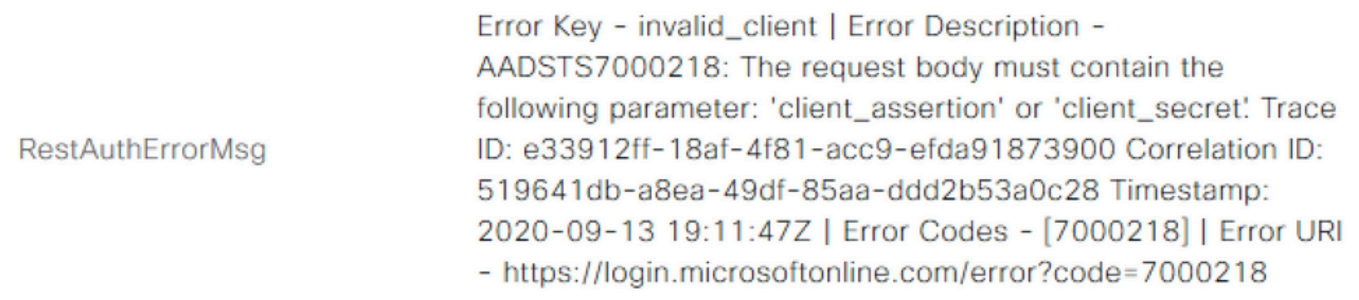
此範例顯示REST身份驗證服務如何啟動：

```
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
```

在服務無法啟動或意外中斷的情況下，始終應在有問題的時間範圍內檢視ADE.log。

REST ID身份驗證問題

在使用REST ID儲存區時，如果身份驗證失敗，則始終需要從詳細的身份驗證報告開始。在「其他屬性」區域中，您可以檢視包含由Azure雲返回的錯誤的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

圖31

使用日誌檔案

在ISE 3.0中，由於REST ID功能的受控引進，預設情況下啟用它的調試。所有與REST ID相關的日誌都儲存在ROPC檔案中，這些檔案可以通過CLI檢視：

```
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
```

在安裝了補丁的ISE 3.0上，請注意檔名是rest-id-store.log，而不是ropc.log。提供的上一個搜尋示例有效，因為資料夾名稱未更改。

或者從ISE支援包提取這些檔案。

以下是幾個顯示不同工作和非工作場景的日誌示例：

1. ISE節點不信任Azure Graph時的證書錯誤。當組未載入到REST ID儲存設定中時，可以看到此錯誤。

```
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)
```

此問題表示Microsoft graph API證書不受ISE信任。ISE 3.0.0.458未在受信任儲存中安裝DigiCert全域性根G2 CA。這一點記錄在缺陷中

— 思科錯誤ID CSCvv80297要解決此問題，您需要在ISE受信任儲存中安裝DigiCert全域性根G2 CA，並將其標籤為受思科服務信任。

證書可從此處下載 — https://www.digicert.com/kb/digicert-root-certificates.htm

2.錯誤的應用程式密碼。

```
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.錯誤的應用程式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.未找到使用者。

```
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.使用者密碼已過期 — 通常可以為新建立的使用者生成，因為Azure管理員定義的密碼需要在登入到Office365時更改。

```
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.由於API許可權錯誤，無法載入組。

```
12:40:06.624 [http-nio-9601-exec-9] ERROR c.c.i.r.u.RestUtility - Error response in 'GET' request. Stat
"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.當Azure端上不允許使用ROPC時，身份驗證失敗。

```
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.身份驗證失敗，因為使用者不屬於Azure端的任何組。

```
21:54:55.976 [http-nio-9601-exec-5] DEBUG c.c.i.r.e.c.CertificateCache - SSLContext initialized with tru
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 toke
at com.cisco.ise.ROPC.providers.azure.AzureROPCFlow.validateIdTokenPayload(AzureROPCFlow.java:93)
```

9.成功的使用者身份驗證和組檢索。

```
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 f
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 tru
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" : [ ]
}
```

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。