部署授權代碼授權流程並對其進行故障排除 — OAuth增強功能:思科合作解決方案12.0

目錄

簡介

本文檔介紹授權碼授權流如何基於刷新令牌,以便改善各種裝置(尤其是流動裝置上的Jabber)的 Jabber使用者體驗。

必要條件

需求

思科建議您瞭解以下主題:

- •思科整合通訊管理員(CUCM)12.0版本
- 單一登入(SSO)/SAML
- Cisco Jabber
- Microsoft ADFS
- 身份提供程式(IdP)

若要取得有關這些主題的詳細資訊,請參閱以下連結:

- <u>思科統一通訊SAML SSO部署指南</u>
- Unified Communications Manager SAML SSO配置示例:
- <u>用於SAML SSO的AD FS 2.0版設定配置示例:</u>

採用元件

本檔案中的資訊是根據以下軟體:

- Microsoft ADFS(IdP)
- LDAP Active Directory
- Cisco Jabber使用者端
- CUCM 12.0

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。

背景資訊

目前,基礎設施中的Jabber SSO流基於隱式授權流,其中CUCM Authz服務分配短期訪問令牌。

訪問令牌到期後,CUCM將Jabber重定向到IdP以進行重新身份驗證。

這會導致使用者體驗不佳,尤其是使用Jabber在流動裝置上時,使用者需要經常輸入憑證。

安全重新架構解決方案還提出了授權碼授權流程(使用刷新令牌方法(可擴展到終端/其他合作應用)),以便在SSO和非SSO場景中統一Jabber和終端登入流程。

功能要點

- ·授權碼授權流程基於刷新令牌(可擴展到終端/其他合作應用),以便改善各種裝置之間的 Jabber使用者體驗,尤其是移動版Jabber。
- 支援自包含簽名和加密的OAuth令牌,以允許各種合作應用程式驗證和響應客戶端資源請求。
- 保留隱式授權流模型,允許向後相容。這還允許未遷移到授權代碼授予流程的其他客戶端(如 RTMT)使用無縫路徑。

重要注意事項

- 實現,以便舊jabber客戶端可以與新CUCM配合使用(因為它支援隱式授予和授權碼授予流程)。此外,新的jabber可以與舊CUCM配合使用。Jabber可以確定CUCM是否支援授權碼授權流,並且僅當它支援此模型時,它才切換並使用隱式授權流。
- •身份驗證服務在CUCM伺服器上運行。
- AuthZ僅支援隱式授權流。這表示沒有刷新令牌/離線訪問令牌。每次使用者端需要新的存取權 杖時,使用者需要使用IdP重新進行驗證。
- •僅當部署啟用了SSO時,才會頒發訪問令牌。非SSO部署在此情況下不起作用,訪問令牌未在 所有介面上一致使用。
- 訪問令牌不是獨立的,而是保留在發出它們的伺服器的記憶體中。如果CUCM1發出了訪問令牌 ,則只能由CUCM1進行驗證。如果客戶端嘗試訪問CUCM2上的服務,CUCM2需要在 CUCM1上驗證該令牌。網路延遲(代理模式)。
- 移動客戶端上的使用者體驗非常糟糕,因為使用者使用IdP重新進行身份驗證時,必須在字母數 字鍵盤上重新輸入憑據(通常從1小時到8小時運行,這取決於多個因素)。
- 通過多個介面與多個應用程式進行通訊的客戶端需要維護多個憑據/塊。對於從2個類似客戶端 登入的同一使用者,沒有無縫支援。例如,使用者A從在2個不同iPhone上運行的jabber例項登 入。
- AuthZ,支援SSO和非SSO部署。
- 支援隱式授權流+授權代碼授權流的授權流。因為它具有向後相容,允許RTMT這樣的客戶端繼

續工作,直到它們適應為止。

- 透過授權碼授權流程,AuthZ會發出存取權杖和刷新權杖。刷新令牌可用於獲取另一個訪問令牌 ,而無需身份驗證。
- •訪問令牌是自包含、簽名和加密的,並使用JWT(JSON Web令牌)標準(與RFC相容)。
- 簽名和加密金鑰對群集是通用的。群集中的任何伺服器都可以驗證訪問令牌。沒有必要在記憶 體中保留。
- 在CUCM 12.0上運行的服務是群集中的集中身份驗證伺服器。
- 刷新令牌儲存在資料庫(DB)中。如果需要,管理員需要能夠撤銷它。吊銷基於使用者ID或使用者ID和客戶端ID。
- 簽名訪問令牌允許不同的產品驗證訪問令牌而無需儲存它們。可配置的訪問令牌和刷新令牌生存期(預設分別為1小時和60天)。
- JWT格式與Spark保持一致,從而可在未來與Spark Hybrid服務實現協同效應。
- 支援同一使用者從2個類似裝置登入。例如:使用者A可以從運行在2個不同iPhone上的jabber例 項登入。

授權碼授權流程要素

- Auth Z Server
- 加密金鑰
- 簽名金鑰
- 刷新令牌

設定

預設情況下未啟用此功能。

步驟1。若要啟用此功能,請導覽至System > Enterprise Parameters。

步驟2.將「Refresh Login Flow」引數設定為「Enabled」,如下圖所示。

DAuth Access Token Expiry Timer (minutes) *	60		60
DAuth Refresh Token Expiry Timer (days) *	60		60
edirect URIs for Third Party SSO Client			
SO Login Behavior for iOS.*	Use embedded browser (WebView)		Use embedded browser (WebView)
Auth with Refresh Login Flow *	Enabled		Disabled
se SSO for RTMT	True	*	True

- 訪問令牌已簽名並加密。簽名和加密金鑰對群集是通用的。這意味著群集中的任何節點都可以 驗證訪問令牌。
- •訪問令牌採用JWT格式(RFC 7519)。
- •訪問令牌重複使用企業引數(OAuth訪問令牌到期計時器),它適用於舊令牌和新令牌格式。
- •預設值 60分鐘。
- 最小值--1分鐘
- 最大值 1440分鐘

eyJhbGciOiJSUzI1NiISInR5cCI6IkpXVCIsImtpZCI6IjhkMGQ1MzIOLWY0ZjAtNGIwYiO4MTFlLTRhNT1mZGI2YjcyMjpj Mjc3MGM5N2JkYT1kMzRmZDA1YTdlYTFhZWQzZTU0Y2E4MGJkZDdlZTM1ZDk3MDNiNjBiNTQ5MTBiZDQ0ODRiIn0.eyJwcml2 YXR1IjoiZX1KaGJHY21PaUprYVhJaUxDSmpkSGtpT21KS1YxUW1MQ0psYm1NaU9pSkJNVEk0UTBKRExVaFRNa1UySW13aWEy bGtJam9pT0dRd1pEVXpNalF0WmpSbU1DMDBZakJpTFRneE1XVXROR0UxT1daa11qWm1Oek15T21Vd1ptUm1ZMk16W1RRMU5E RTFOV0ZpTkRJek5tRTJOM1V4T0RCbU1qWmxZMk13WXpJeE56SX10REJtW1RFe11XWX1Oak14TkRkalpHVXpNR113TjJJaWZR Li5xQWd6aGdRaTVMMkdlaDl5V2RvN25nLmdMTHNpaTRjQk50c1NEUXRJTE51RWRnWTl4WkJVczJ4YzBaeTFGQjZQNmNzWWJf ZkRnaDRZby04V1NaNjUzdXowbnFOalpXT1E1dGdnYW9qMlp6ZFk2ZzN2SWFHbF9JWUtNdkNIWWNscmt4YUFGTk5MWExLQlJm aTA2LVk2V3l1dUdxNmpNWk5DbnlKX1pTbUpkVFQwc1Z4RTdGTXVxaUJsME1rRGdyVDdvOFNXMEY5cXFadndEZDJSaDdqNkRJ WGdkS3VtOWltU2xNU1pjejhueVdic01Udk5yMWY0M25VenJzMkk5WWN6NnBDX0czZmlWYjJsX2VWLVFkcFh4TUo2bnZodXcy djRiUGVkM3VMQlpaVWloQ3B6TUVDdW5NMlh1TVBrTGdlS1NqWG44aGhPRFNVcW1WQ0Uta3RZdnRBc2Q0RnJxcGNxWlZiS0Zi VTFRbU0wV2pMYVJtUk9IVl1QVkc0a3FBdTRWalVMUzVCRWszNnZ4Nmp3U3BMUy1IdTcwbVRNcmR3dmV5Q2ZOYkhyT0FlVmVv ekFIR3JqdGlmaFpmSFVUTWZiNkMtX2tOQVJGQWdDc1ZTZy0wUz1xb1JvTWVkUENETEE4MDJiaWwtNDJjOC15MWo4X1FVaC02 UUtcV2dodV44VWtB0DRpekFFaWl0QTlsSHFKM3Nxd2JFNURkZmhIay05bTJfTTN5MWlWVkdoRVQ3ZW9XVDBqWl1nRGRBQjFz UGwxLTlaSFNYYmsydTE3SkJVRV9FOXI0V0tWMnBqWGtiN0lQSWgtQ3JWQTZkcVdQRHVIbmx1V19wblNLYnYtTkZVbGQ0WEY3 cmZLYmQySlg4eUhhX05pOVVVUnUwZVdsNWxGRUVabklubmFKZEdHLUZrb3VuN2xHSF1wSE4ydXVudmRnOHZVZzZsa0JPbmoz eUFjc1ZTMGxKc1NWdUxFY1dwd2c4YjdBdDM3d3AtMwt2Y1ZQaWpCQ11CV181d2JzbTFYd2k4MVc2WHVpNzMzQVg3cEJVQnBf T2VRNzQ2ZXJJekNUUFZCYUpZUGJuZWEtdFhsU3RmzzBGeVRmbnhnX1Vzaz13QXJkemE4c204T0FQaWMxZmFQOG0uUTdFN0FV X2xUVNNmzFI2bnkydUdhQSJ9.u2fJrVA55NQC3esPb4kcodt5rnjc1o-5uEDdUf-KnCYEPBZ7t2CTsMMVVE3nfRhM39MfT1NS-qV0VpuoW_51NYaENXQMxfx1U9aXp944QiU10eFQKj_g-

n2dEINRStbtUc3KMKqtz38BFf1g2Z51sdlnBn4XyVWPgGCf4XSfsFIa9fF051awQ0LcCv6YQTGer_6nk7t6F1MzPzBZzja1a bpm--6LNSzjPftEiexpD2oXvW8V10Z9ggNk5Pn3Ne4RzqK09J9WChaJSXkTTE5G39EZcePmVNtcbayq-L2pAK5weDa2k4uYMfAQAwcTOhUrwK3yilwqjHAamcG-CoiPZQ

OAuth Refresh Token Expiry Timer" parameter in enterprise parameters page in CUCM. Path: System -> Enterprise parameters Values are integers ranging from 1 - 90 Minimum lifetime = 1 Day Default lifetime = 60 days Maximum lifetime = 90 days 每次客戶端請求新的訪問令牌時,都會發出新的訪問令牌。舊版本繼續有效,只要:

- 簽名/加密金鑰未更改
- •有效性(儲存在令牌中)中斷。

• JSON Web令牌:它由三個部分組成,分別用點表示:報頭、負載和簽名。 訪問令牌示例:

- 以粗體突出顯示的標籤的起始位置是標頭。
- 中間部分是負載。

• 最後,如果標籤以粗體突出顯示,則其為「簽名」。

網路圖表

下面簡要概述所涉及的呼叫流程:



- •已簽名刷新令牌。
- 刷新令牌作為自身的雜湊值儲存在資料庫的refreshtokendetails表中。這是為了防止DB進行複製,因為它可以被某些人拾取。要複查可以運行的表,請執行以下操作: run sql select * from refreshtokendetails

或有可讀有效日期:

run sql select pkid,refreshtokenindex,userid,clientid,dbinfo('utc_to_datetime',validity) as
validity,state from refreshtokendetails

admin:run sql	select * from refi	reshtokend	details			
pkid	refreshtokenindex	userid	clientid	validity		state
173e2283-1	65483476618891	bvanturn	Clb4b	2019-01-05	14:11:46	1080686546
cd2c634c-7	0bf6b2989db114	bvanturn	Clb4b	2019-01-05	14:28:41	569144456
a3706858-b	b4800f20dbfe0e	bvanturn	Clb4b	2019-01-05	14:38:12	1146722445

警告:當有效期到期時,刷新令牌來自資料庫。計時器執行緒每天凌晨2點運行(不可通過 UI配置,但可以通過遠端支援帳戶進行修改)。如果表具有大量訪問令牌,這些令牌無效且需 要清空。這可能導致CPU峰值。

Sample refresh token:

eyJhbGciOiJSUzI1NiISInR5cCI6IkpXVCISImtpZCI6IjhkMGQ1MzIOLWY0ZjAtNGIwYiO4MTFlLTRhNT1mZGI2YjcyMjpj Mjc3MGM5N2JkYT1kMzRmZDA1YTdlYTFhZWQzZTUOY2E4MGJkZDdlZTM1ZDk3MDNiNjBiNTQ5MTBiZDQ0ODRiIn0.eyJleHAi OjE1MDI2MjAwNTISIm1zcyI6IjhkMGQ1MzIOLWY0ZjAtNGIwYiO4MTFlLTRhNT1mZGI2YjcyMiISInR5cCI6InVzZXIiLCJO aWQiOiJiOTkxMjIxZi1mNDJlLTR1NTItODg3MS1jODc2ZTYzNWRkNWIiLCJjdH1wIjoicmVmcmVzaCISImNjaWQiOiJDM2Iw YWZmZWZ1MTQzOTA0MTY4M2U5YzJjMzdkMzZmNDM4ZWYwZWYyN2MwOTM4YWRjNjIyNmUwYzAzZDE2OWYyYSJ9.creRusfwSYA MAtttS2FIPAgIVvCiREvnzlouxeyGVndalJ1Ma-ZpRqv8F0BrsYwqEyulr1-

TeM8XGGQCUvFaqO9IkhJqSYz3zvFvvySWzDhl_pPyWIQteAhL1GaQkue6a5ZegeHRp1sjEczKMLC6H68CHCfletn5j2FNrAUOX99Vg5h4mHvlhfjJEel3dU_rciAIni12e3LOKajkzFxF6W0cXzzujyi2yPbY9gZsp9HoBbkkfThaZQbS1CEpvB3t 7yRfEMIEaHhEUU4M3-uSybuvitUWJnUIdTONiWGRh_fOFR9LV3Iv9J54dbsecpsncc369pYhu5IHwvsg1NKEQ

撤消刷新令牌

管理員能夠通過userID或userID和ClientID撤消使用者的全部刷新令牌或使用者的裝置專用刷新令牌 。

要撤銷使用者的基於裝置的RT:

- 撤消由client_id abc標識的使用者xyz和裝置的RT。
- https://cucm-193:8443/ssosp/token/revoke?user_id=xyz&client_id=abc

簽名和加密金鑰

- 簽名金鑰基於RSA,具有公鑰/私鑰對。
- 加密金鑰是對稱金鑰。
- 這些金鑰僅在發佈伺服器上建立,並且分佈於群集中的所有節點。
- 可以使用列出的選項重新生成簽名金鑰和加密金鑰。但是,僅當管理員認為金鑰已被入侵時 ,才能執行此操作。重新生成這兩個金鑰之一的影響在於AuthZ服務頒發的所有訪問令牌均無效 。
- •可以使用UI和CLI重新生成簽名金鑰。
- 只能使用CLI重新生成加密金鑰。

從CUCM上的Cisco Unified OS Administration頁面重新生成授權證書(簽名金鑰)如下圖所示。

Certificate Details(Self-signed)	ned) - Internet Explorer provided by Cisco Systems, Inc.	
https:// 10.77.29.184/cmp	atform/certificateEdit.do?cert=/usr/local/platform/.security/a	uthz/certs/authz.j 😵 Certificate error
Certificate Details for	AUTHZ_CUCM-184, authz	
Regenerate D		
_ Status]
G Status: Ready		
-Certificate Settings—		
File Name	authz.pem	
Certificate Purpose	authz	
Certificate Type	certs	
Certificate Group	product-cpi	
Description(friendly nan	ne) Self-signed certificate generated by system	
-Certificate File Data -		
ř		^
Version: V3		
Subject: L=i, ST=i, Cl	N=AUTHZ_CUCM-184, OU=i, O=i, C=IN	
Signature Algorithm:	SHA256WithRSA, OID = 1.2.840.113549.1.1.11	
Key: CiscoJ RSA Publ	ic Key, 2048 bits	
modulus:		
3100889524121327740	55004152539262916723787971093575362193467184	3
2566635685074138492	24784529267545217985007767514188438331472676	3
5200239027846515539	94182651149496273115152109016789237562341950	1
7398119889112109168	82081206974895761530299141436201546582466906	3
3197798662644249364	12824902919309822330684688872356018271786023 15424514678030814532577523613700736308360068	8 ~
01010220000020700		-
Regenerate Down	load .PEM File Download .DER File	

使用CLI命令重新生成Authz簽名金鑰的過程如下圖所示。



管理員可以使用CLI顯示授權簽名和加密金鑰。顯示金鑰的雜湊值,而不是原始金鑰。

用於顯示金鑰的命令有:

簽名金鑰: show key authz signing和,如下圖所示。

admin:show key authz signing

authz signing key with checksum: a155d81be734850226f990a62816f1ae last synced on: 06/09/2017 13:04:47

加密金鑰:show key authz encryption和,如下圖所示。

```
admin:show key authz encryption
authz encryption key with checksum: 88edce92173e33f9cedbbfb09cd0e8c4 last synced on: 06/14/2017 16:22:06
```

附註:簽名授權和加密授權始終不同。

驗證

使用本節內容,確認您的組態是否正常運作。

當在Cisco Unity Connection(CUC)伺服器上使用OAuth時,網路管理員必須執行兩個步驟。

步驟1.配置Unity Connection伺服器以從CUCM獲取OAuth令牌簽名和加密金鑰。

步驟2.在CUC伺服器上啟用OAuth服務。

注意:要獲取簽名和加密金鑰,必須使用CUCM主機詳細資訊和CUCM AXL訪問啟用的使用 者帳戶配置Unity。如果未進行配置,則Unity Server無法從CUCM檢索OAuth令牌,並且使用 者的語音郵件登入不可用。

導航至Cisco Unity Connection Administration > System Settings > Authz Servers

New Authz Se	rver		
Authz Servers	Reset	Help	
Save			
New Authz Se	erver		
Display Name*	Authz Ser	er	
Authz Server*	CUCMPubl	her.miguecas.lv	
Port*	8443		
Username*	miguecas		
Password*	•••••		
Ignore Cer	tificate Erro	s	
Save			
Fields marked	with an ast	risk (*) are required.	

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

附註:如果使用OAuth且Cisco Jabber使用者無法登入,請始終檢視CUCM和即時消息和線上 狀態(IM&P)伺服器的簽名和加密金鑰。

網路管理員需要在所有CUCM和IM&P節點上運行以下兩個命令:

- · show key authz signing
- show key authz encryption

如果所有節點的簽名authz和加密authz輸出不匹配,則需要重新生成它們。為此,需要在所有 CUCM和IM&P節點上運行以下兩個命令:

- set key regen authz encryption
- set key regen authz signing

然後,需要在所有節點上重新啟動Cisco Tomcat服務。

除了金鑰不匹配之外,在Cisco Jabber日誌中還可以找到此錯誤行:

```
2021-03-30 14:21:49,631 WARN [0x0000264c] [vices\impl\system\SingleSignOn.cpp(1186)] [Single-Sign-On-
Logger] [CSFUnified::SingleSignOn::Impl::handleRefreshTokenFailure] - Failed to get valid access token
from refresh token, maybe server issue.
在以下位置生成SSO應用日誌:
```

- file view activelog platform/log/ssoApp.log 這不需要對日誌收集進行任何跟蹤配置。每次完成SSO App操作時,都會在ssoApp.log檔案中生成新的日誌條目。
- SSOSP日誌: file list activivelog tomcat/logs/ssosp/log4j

每次啟用sso時,都會在此位置建立一個名為**ssosp00XXX.log**的新日誌檔案。任何其他 SSO操作和所有Oauth操作也登入到該檔案中。

• 證書日誌: file list activelog platform/log/certMgmt*.log 每次重新生成AuthZ證書(UI或CLI)時,都會為此事件生成新的日誌檔案。 為了重新生成授權加密金鑰,將為此事件生成一個新的日誌檔案。

相關資訊

使用思科合作解決方案版本12.0部署OAuth