對UCCE SSO與Azure IdP的整合進行故障排除

目錄

簡介

本文檔介紹如何解決與Microsoft Azure IdP進行UCCE SSO整合時面臨的一些常見問題。

作者：Anurag Atul Agarwal，思科TAC工程師。

必要條件

需求

思科建議您瞭解以下主題：

- 安全宣告標籤語言(SAML)2.0
- Cisco整合/套裝客服中心企業版UCCE/PCCE
- 單一登入(SSO)
- 思科身分識別服務(IdS)
- 身份提供程式(IdP)

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Azure IdP

- UCCE 12.0.1
- Cisco IdS 12.0.1

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

本文檔介紹在整合基於Azure的SSO的思科身份服務(IdS)和身份提供程式(IdP)期間面臨的一些常見問題及其可能的修復。 建議收集以下日誌以排除SSO整合問題：

- Cisco IdS日誌：指向集合的連結：IDS日誌
- 瀏覽器控制檯日誌
- 來自IdP的任何日誌

問題：證書不匹配

測試SSO失敗，顯示消息「IdS無法處理SAML響應，即使身份驗證成功」，並且IdS日誌列印錯誤消息：「SAML響應處理失敗，異常com.sun.identity.saml2.common.SAML2Exception：簽名證書與實體後設資料中定義的不匹配」

解決方案

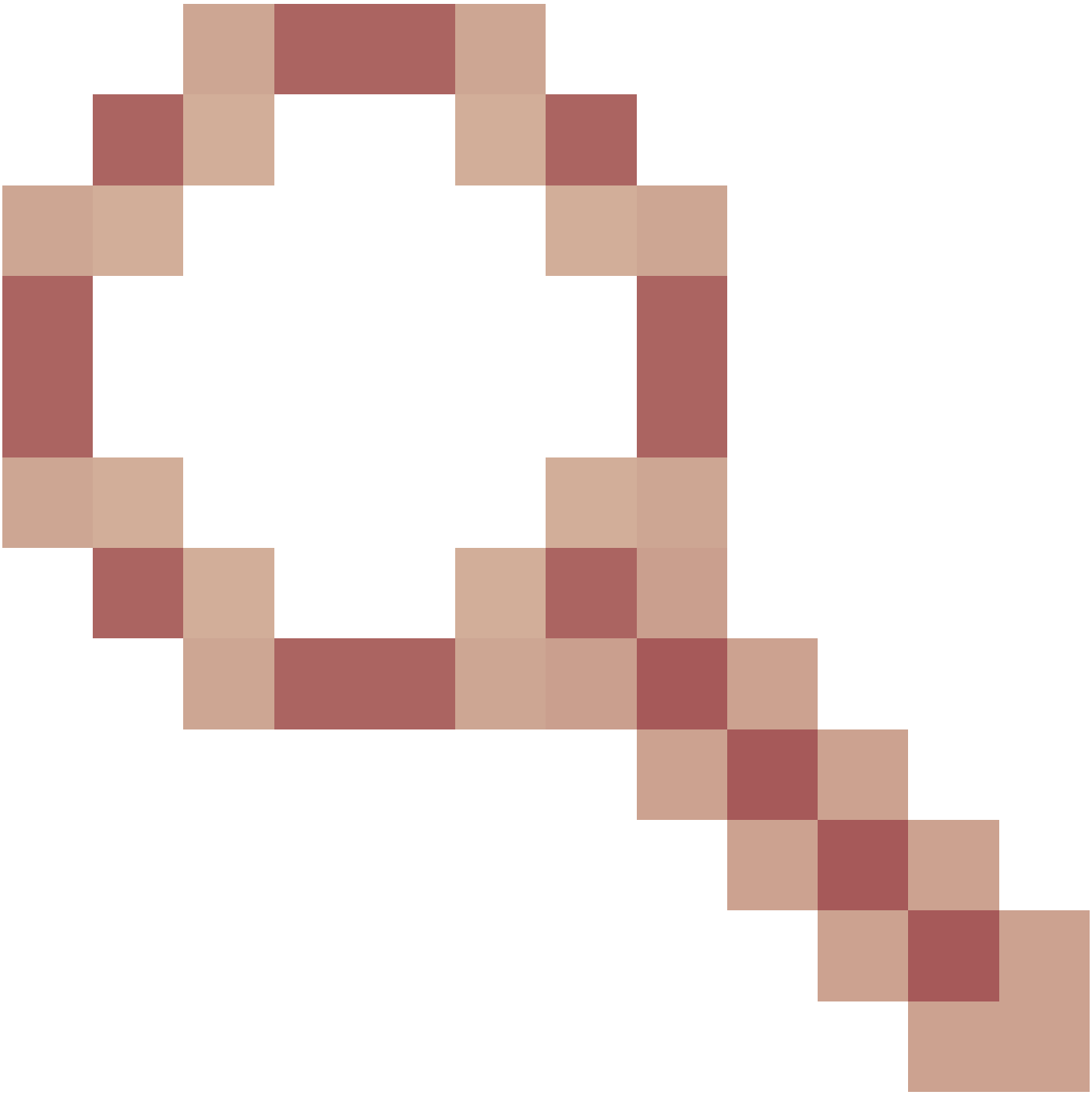
在Azure中驗證證書並設定簽名演算法。確保它與基於IdS版本的支援雜湊演算法匹配。請參閱功能指南中的「單點登入」一章，並驗證支援的安全雜湊演算法。下載最新的IdP後設資料文件，並通過身份服務管理使用者介面將其上傳到Cisco IdS。

問題：AADSTS900235 — 身份驗證上下文問題

測試SSO重定向到Microsoft頁面，失敗並顯示以下消息：「很抱歉，您登入時遇到問題。」AADSTS900235: SAML身份驗證請求的RequestedAuthenticationContext Comparison值必須是Exact。接收值：最小

解決方案

可能需要按照錯誤CSCvm中的說明調整AuthContext69290



.請聯絡Cisco TAC以IdS執行解決方法。

問題：SAML響應未簽名

測試SSO失敗並出現消息，即使「身份驗證成功」，IdS仍無法處理SAML響應，並且IdS日誌列印錯誤消息：「SAML響應處理失敗，異常com.sun.identity.saml2.common.SAML2Exception：響應未簽名。」

解決方案

Azure IdP需要將簽名宣告傳送到IdS。 修改Azure設定使其具有簽名選項：對SAML響應和斷言進行簽名

問題：索賠規則問題

測試SSO失敗，出現消息「IdP配置錯誤： SAML處理失敗。無法從SAML響應檢索使用者主體。'且IdS日誌列印錯誤消息：「SAML響應處理失敗，異常com.sun.identity.saml.common.SAMLException：無法從SAML響應檢索使用者主體。」

解決方案

此錯誤指向在Azure中配置的錯誤「宣告名稱」。對於其他屬性（如UID、NameID等），可能會發生這種情況，並且會生成具有不同屬性名稱的類似錯誤。若要修復此問題，請在Azure中查詢此格式的任何屬性，格式為「schemas.xmlsoap.org/ws/2005/05/identity/claims/<attribute_name>」。刪除實際屬性名稱之前的所有內容。

本部分提供功能指南中需要在Azure中複製的ADFS的配置示例。

ADFS示例配置

問題：AADSTS50011 — 回覆URL不匹配

測試SSO重定向到Microsoft頁面，失敗並顯示以下消息：「很抱歉，您在登入時遇到問題。ADSTS50011：請求中指定的回覆URL與為應用程式「 」配置的回覆URL不匹配

解決方案

請與Cisco TAC聯絡。需要在IdS節點的根目錄簽入「Assertion Consumer Service」引數，否則無法通過。如果引數正確，Microsoft Azure必須對此進行故障排除。

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）。