

使用PingID联合RADIUS令牌时ISE管理员GUI登录失败

目录

问题

当使用PingID联合作为RADIUS令牌时，管理员GUI登录思科ISE失败，尽管数据包捕获显示Ping联合返回访问接受响应。即使RADIUS身份验证从网络角度显示成功，也会发生登录失败，从而阻止对ISE接口的管理访问。网络数据包分析确认PingID服务器(10.32.154.200)向ISE(10.2.200.241)发送预期的Access-Accept响应，但ISE管理员登录过程仍无法成功完成。

环境

- 思科身份服务引擎(ISE)版本3.3补丁7
- 4节点VM部署
- 配置为RADIUS令牌身份验证的PingID联合
- ISE IP地址：10.2.200.241
- PingID服务器IP地址：10.32.154.200
- 管理员访问权限配置在管理>管理员访问权限下审核

分辨率

通过应用启用成功管理员登录功能的解决方法，问题得以解决。下面几节中介绍的步骤用于解决此问题。

步骤 1：证据收集和分析

收集并分析数据包捕获证据，以确认ISE和PingID服务器之间的RADIUS身份验证流程。分析验证Ping联盟是否正确发送了Access-Accept响应。

步骤 2：来自prrt-server.log的证据

###

prrt-server.log

```
RadiusTokenIDStore,2026-03-27 13:25:04,534,DEBUG,0x7f4942ebb700,cntx=0180887321,sesn=SIT2194/554866250/  
RadiusClient,2026-03-27 13:25:04,534,DEBUG,0x7f4942ebb700,cntx=0180887321,sesn=SIT2194/554866250/183397  
RadiusClient,2026-03-27 13:25:05,074,DEBUG,0x7f490d6b9700,NIL-CONTEXT,onProcessResponse: Processing Res  
RadiusClient,2026-03-27 13:25:05,074,WARN ,0x7f49444c6700,cntx=0180887321,sesn=SIT2194/554866250/183397
```

###

步骤 3：什么是消息验证器？

Message-Authenticator是RADIUS数据包中使用的安全属性，用于确保网络设备和RADIUS服务器之间交换的消息的完整性和真实性。它是使用HMAC-MD5对具有共享密钥的整个RADIUS数据包计算的加密签名。此属性有助于防止RADIUS消息的篡改和欺骗，尤其是那些涉及可扩展身份验证协议(EAP)身份验证流的消息。

步骤 4：解决方法实施

禁用“响应时需要消息验证器”：管理/身份管理/外部身份源/RADIUS令牌。点击RADIUS令牌名称，然后转至Authentication。取消选中“Message Authenticator Required On Response”。

步骤 5：验证测试

应用该解决方法后，执行管理员登录测试以验证解决方案。这些测试确认身份验证成功以及使用 PingID 联合作为 RADIUS 令牌访问 ISE 管理员 GUI。

步骤 6：监控周期

已建立监控和验证期，以确保解决方案的稳定性。在此期间，继续进行了管理员登录测试，未报告错误或故障。

原因

ISE 管理员 GUI 登录失败是由思科 ISE 3.3 补丁 7 和 PingID (Ping Federate) 在 MFA 身份验证期间的 RADIUS 协议安全实施不匹配引起的。

具体来说：

- 思科 ISE 要求外部 RADIUS 令牌服务器的 Access-Accept 响应中存在 RADIUS Message-Authenticator 属性。
- PingID 返回的 Access-Accept 响应没有 Message-Authenticator 属性。
- 由于 ISE 启用了设置 Message Authenticator Required On Response，因此它以静默方式拒绝 RADIUS 响应无效，即使身份验证本身在 PingID 端成功也是如此。
- 此实施是 Cisco ISE 安全加固的一部分，以缓解 Blast-RADIUS 漏洞 (CVE-2024-3596)。

相关内容

- [Blast-RADIUS 协议欺骗缓解 \(CVE-2024-3596\)](#)

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）。