ISE RADIUS上下文耗尽导致节点停止响应

目录

问题

思科身份服务引擎(ISE)节点间歇性停止响应RADIUS身份验证请求，导致网络设备将其标记为“RADIUS DEAD”。 受影响节点收到RADIUS请求（通过防火墙日志和数据包捕获确认），但无法响应。观察到以下症状：

- 网络设备上的RADIUS重传消息
- ISE中出现“Radius Context Allocation Failed”严重警报
- 日志消息指示“Hit context count limit.正在丢弃请求！”
- ISE GUI在问题期间变得不可访问，尽管所有服务都显示为正在运行
- 节点重新启动后，大约需要30分钟才能解决此问题

观察到的具体错误消息包括：

```
033057: Mar 11 09:33:59.015: RADIUS: Retransmit to (10.0.5.11:1812,1813) for id 1645/127
033058: Mar 11 09:33:59.015: RADIUS: PAC key found while sending request (rctx:0x75EB6A555690)
033059: Mar 11 09:33:59.015: RADIUS: Message Authenticator encoded
033060: Mar 11 09:33:59.015: RADIUS(00000000): Started 4 sec timeout
```

在ISE日志中：

```
RadiusListener,2026-06-28 23:21:22,149,WARN ,0x7efea2055700,NIL-CONTEXT,Hit context count limit. Droppi
```

环境

- 思科身份服务引擎(ISE)版本3.5.0.331（补丁3）
- 提供多个角色的节点：主管理节点(PAN)、会话管理和故障排除(SMNT)以及策略服务节点(PSN)
- 身份验证方法：在接入交换机端口上同时启用802.1X和MAB
- 外部身份源：Microsoft Entra ID集成
- 将ISE配置为RADIUS服务器以进行身份验证的网络设备

分辨率

通过应用Cisco提供的修复，解决ISE SessionUpdater进程中的死锁条件，解决了此问题。按照以下步骤实施解决方案：

步骤 1：获取并安装修补程序

从思科下载修补程序文件并将其传输到ISE节点存储库。修补程序文件包括：

- ise-apply-CSCwv71473_3.5.0.527_patch3-SPA.tar.gz（安装文件）
- ise-rollback-CSCwv71473_3.5.0.527_patch3-SPA.tar.gz（回滚文件）

步骤 2：应用修补程序

使用CLI命令安装修补程序：

```
application install ise-apply-CSCwv71473_3.5.0.527_patch3-SPA.tar.gz <repository name>
```

⚠警告：有可能。此处提到的详细信息似乎包含执行后可能会产生重大影响的过程或命令。请确保SME或业务部门在执行或推荐之前已评估上述程序或命令。

步骤 3：验证安装

使用以下命令之一验证修补程序安装：

```
show logging application hotpatch.log
```

或者:

```
show version
```

步骤 4：监控系统

安装后，请监控ISE节点至少两周，以确保问题不再出现。修补程序安装需要重新启动服务，因此请在维护窗口期间规划安装。

可选：回滚过程

如果需要，可以使用rollback命令删除修补程序：

```
application install ise-rollback-CSCwv71473_3.5.0.527_patch3-SPA.tar.gz <repository name>
```

用于监控的故障排除命令

要监控RADIUS环境分配，请使用：

```
show logging application prrt-server.log | include ContextN
```

在将来的任何故障排除之前启用运行时AAA调试：

```
debug aaa runtime
```

原因

根本原因被识别为ISE SessionUpdater进程中的死锁条件。当同一会话同时发生记帐开始和停止事件时，两个线程进入循环等待方案：

- 线程–162:拥有的cacheLock，等待SessionInfo锁定
- 线程–125:拥有的SessionInfo锁，等待cacheLock

这种循环等待导致ContextN泄漏和持续增长的RADIUS处理队列。队列累积最终耗尽可用的RADIUS情景，导致身份验证延迟和网络设备将ISE节点标记为RADIUS DEAD。

Cisco Bug ID CSCwv71473（仅限注册用户）中记录了此问题。

相关内容

- 思科漏洞ID CSCwv71473
- 思科技术支持和下载

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）。