为使用ISE的网络设备配置基于时间的TACACS+访问

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

配置

- 网络图
- 配置ISE
  - 步骤 1：创建时间和日期条件
  - 步骤 2：创建TACACS+命令集
  - 步骤 3：创建TACACS+配置文件
  - 步骤 4：创建TACACS授权策略
- 配置交换机
- 验证

故障排除

- ISE上的调试

相关信息

常见问题解答

简介

本文档介绍如何为思科身份服务引擎(ISE)中的设备管理策略配置基于时间和日期的授权。

先决条件

要求

思科建议您了解Tacacs协议和身份服务引擎(ISE)配置。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco Catalyst 9300交换机，带软件Cisco IOS® XE 17.12.5及更高版本
- 思科ISE版本3.3及更高版本

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

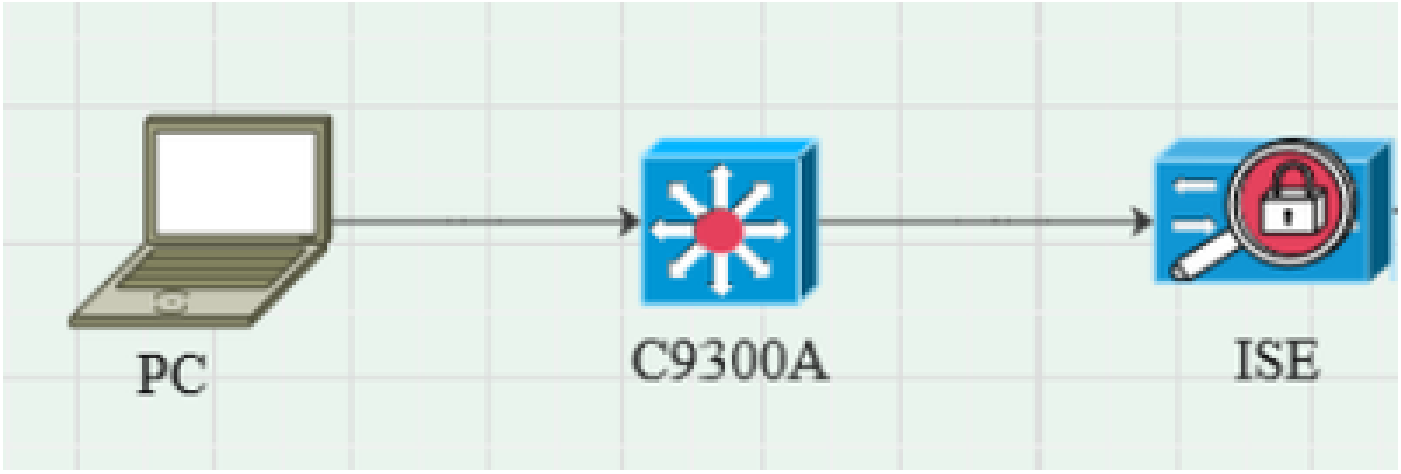
授权策略是思科身份服务引擎(ISE)的关键组件，使您可以为访问网络资源的特定用户或组定义规则和配置授权配置文件。这些策略评估条件以确定应用哪个配置文件。当满足规则的条件时，将返回相应的授权配置文件，授予适当的网络访问权限。

思科ISE还支持时间和日期条件，只允许策略在指定的时间或天期间实施。这对于根据基于时间的业务要求应用访问控制尤其有用。

本文档概述了仅在工作时间（周一至周五，08:00-17:00）内允许TACACS+管理访问网络设备的配置，以及在此时间段外拒绝访问的配置。

配置

网络图



配置ISE

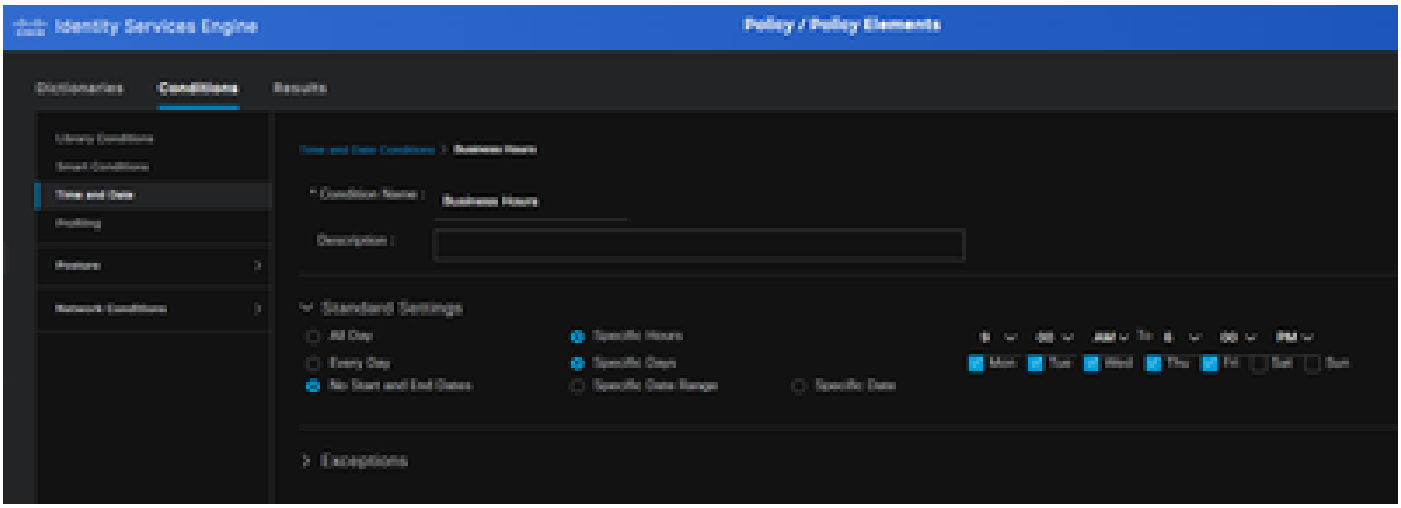
步骤 1：创建时间和日期条件

依次导航到Policy > Policy Elements > Conditions > Time and Date，点击Add。

条件名称：工作时间

设置Time Range Standard Settings > Specific Hours: 09:00 AM - 06:00 PM

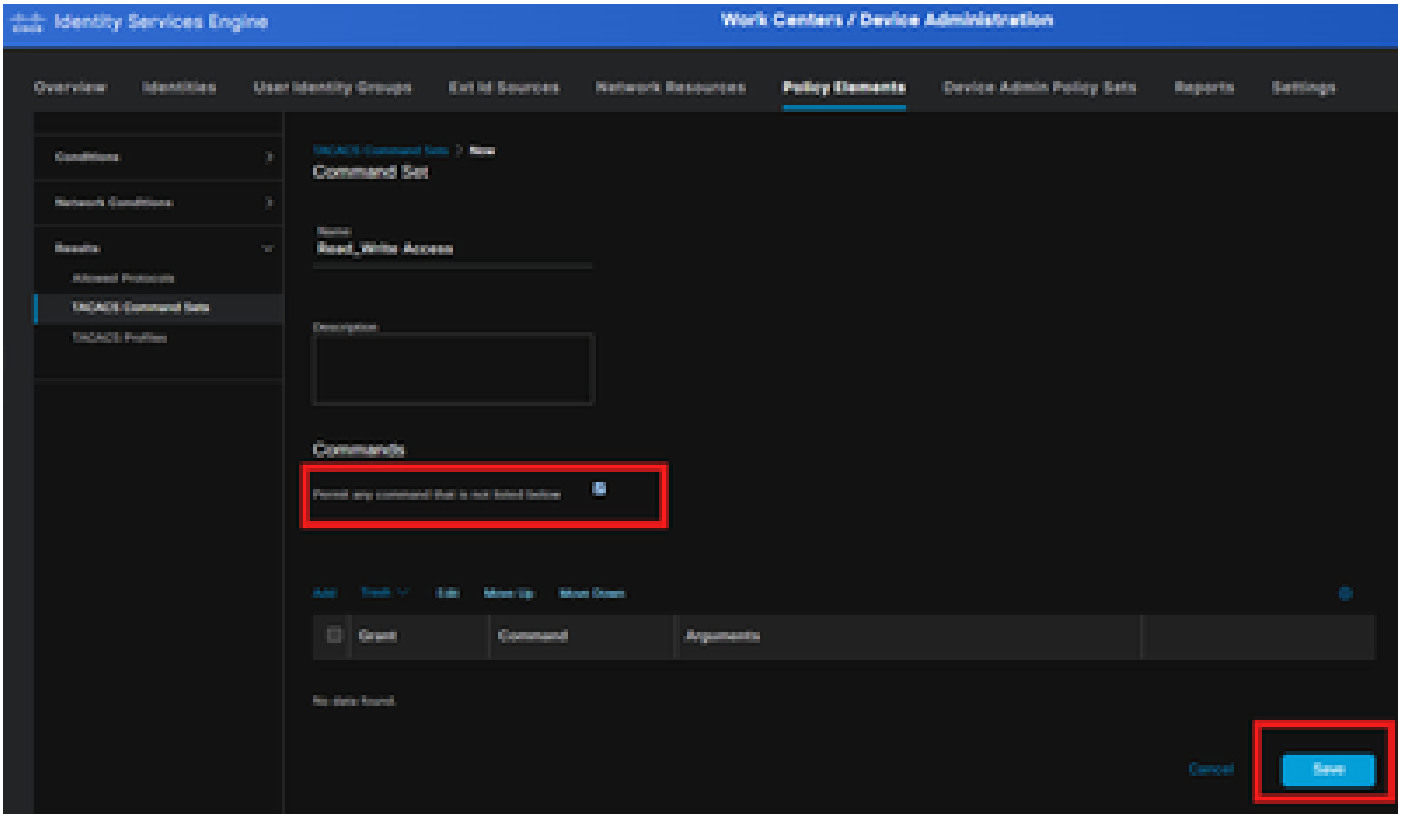
特定天数：星期一到星期五



步骤 2：创建TACACS+命令集

导航到工作中心(Work Centers)>设备管理(Device Administration)>策略元素(Policy Elements)>结果(Results)> Tacacs命令集(Tacacs Command Sets)。

如果要限制某些CLI命令，请选中Permit any command that is not listed below复选框，然后单击Submit或添加Limited Commands以创建命令集。

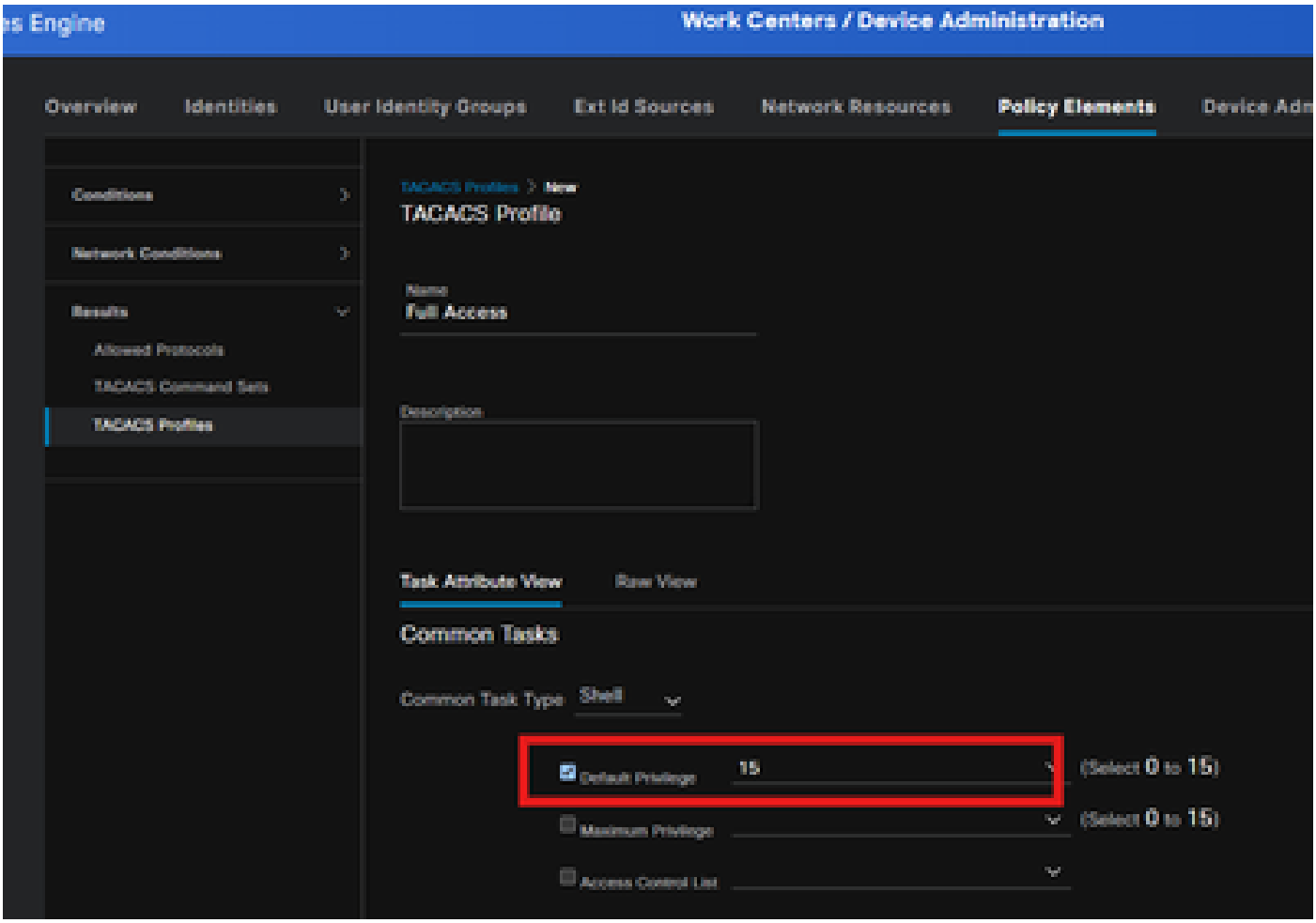


步骤 3：创建TACACS+配置文件

导航到工作中心(Work Centers)>设备管理(Device Administration)>策略元素(Policy Elements)>结果(Results)> TACACS配置文件(TACACS Profiles)。单击 Add。

选中Command Task Type作为Shell，然后选中Default Privilege复选框，并输入值15。单击

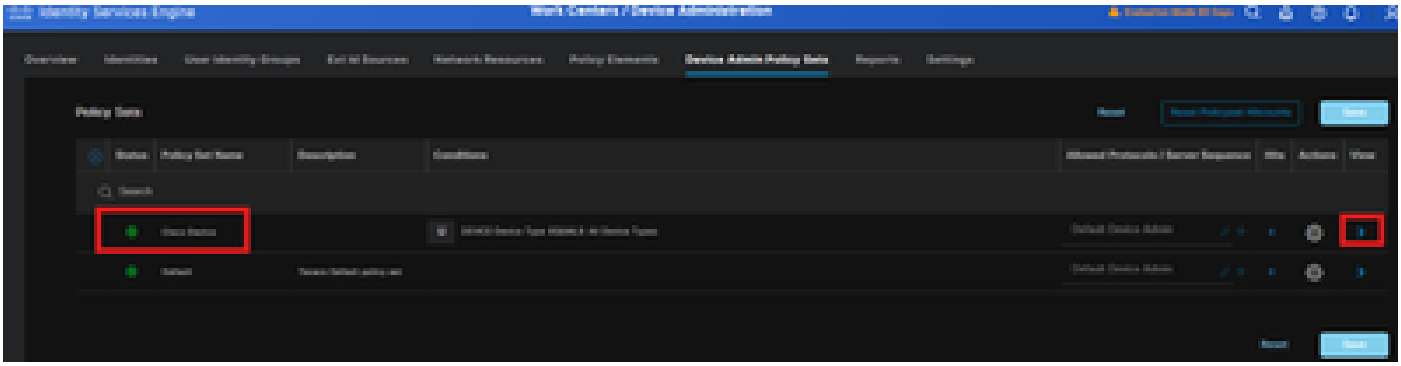
Submit。



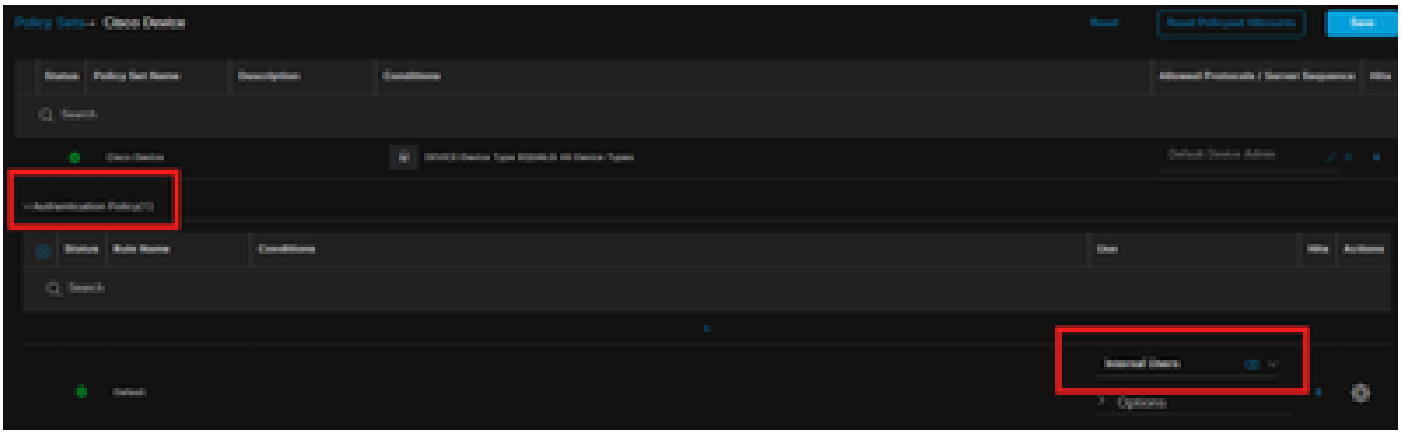
步骤 4： 创建TACACS授权策略

导航到工作中心(Work Centers)>设备管理(Device Administration)>设备管理策略设置(Device Admin Policy Sets)。

选择活动策略集。



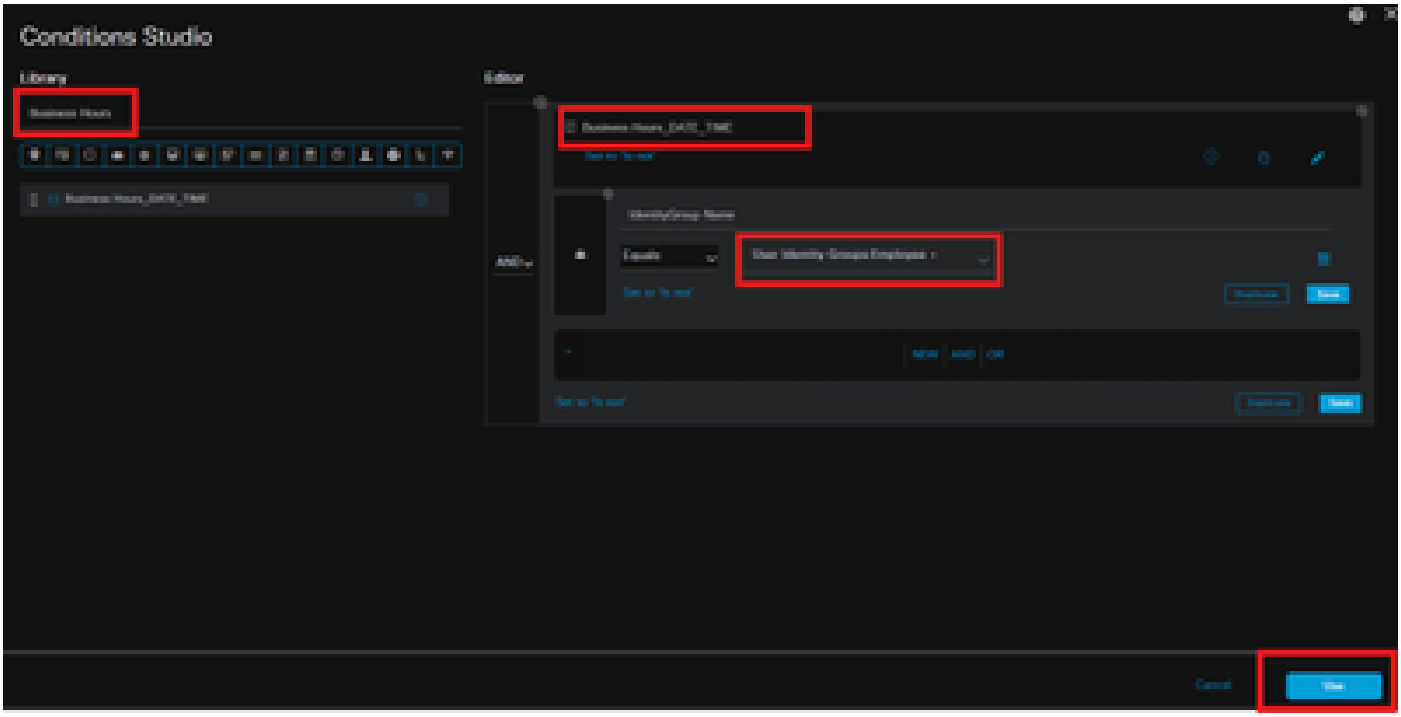
根据内部或Active Directory用户配置身份验证策略。



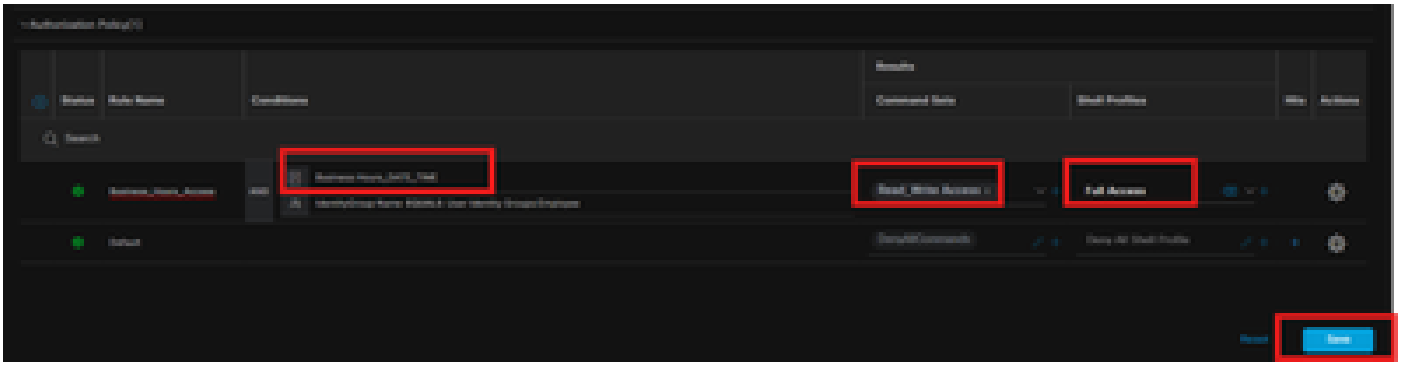
在Authorization Policy部分下，点击Add Rule以提供Rule Name，然后点击+以添加授权条件。

此时将出现新的Condition Studio窗口，在Search by Name字段中，输入在步骤1中创建的名称并将其拖到Editor中。

根据用户组添加其他条件，然后单击Save。



在Results中，选择在步骤2和步骤3中创建的Tacacs Command Set和Shell Profile，然后单击Save。



配置交换机

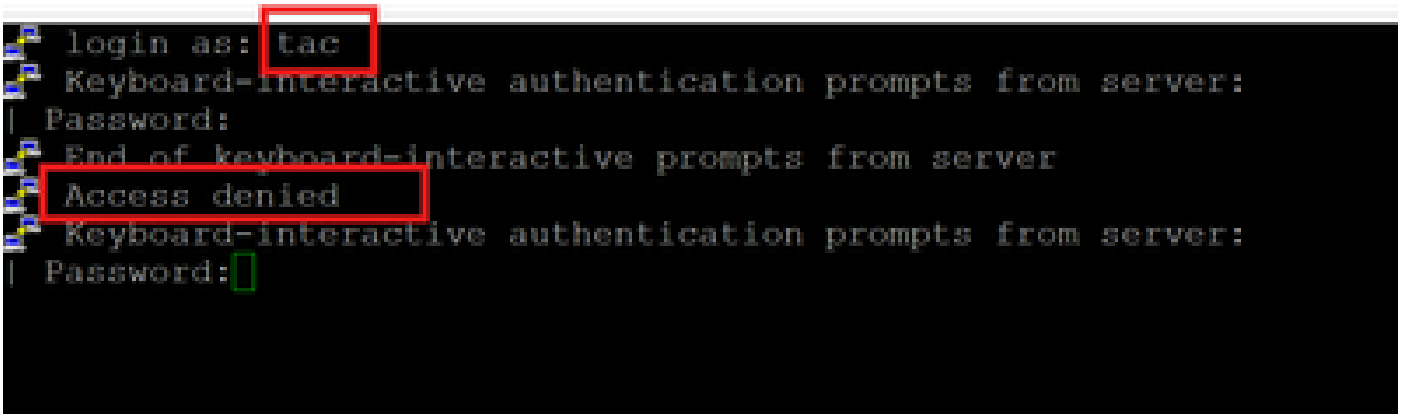
```
aaa new-model

aaa authentication login default local group tacacs+
aaa authentication enable default enable group tacacs+
aaa authorization config-commands
aaa authorization exec default local group tacacs+
aaa authorization commands 0 default local group tacacs+
aaa authorization commands 1 default local group tacacs+
aaa authorization commands 15 default local group tacacs+

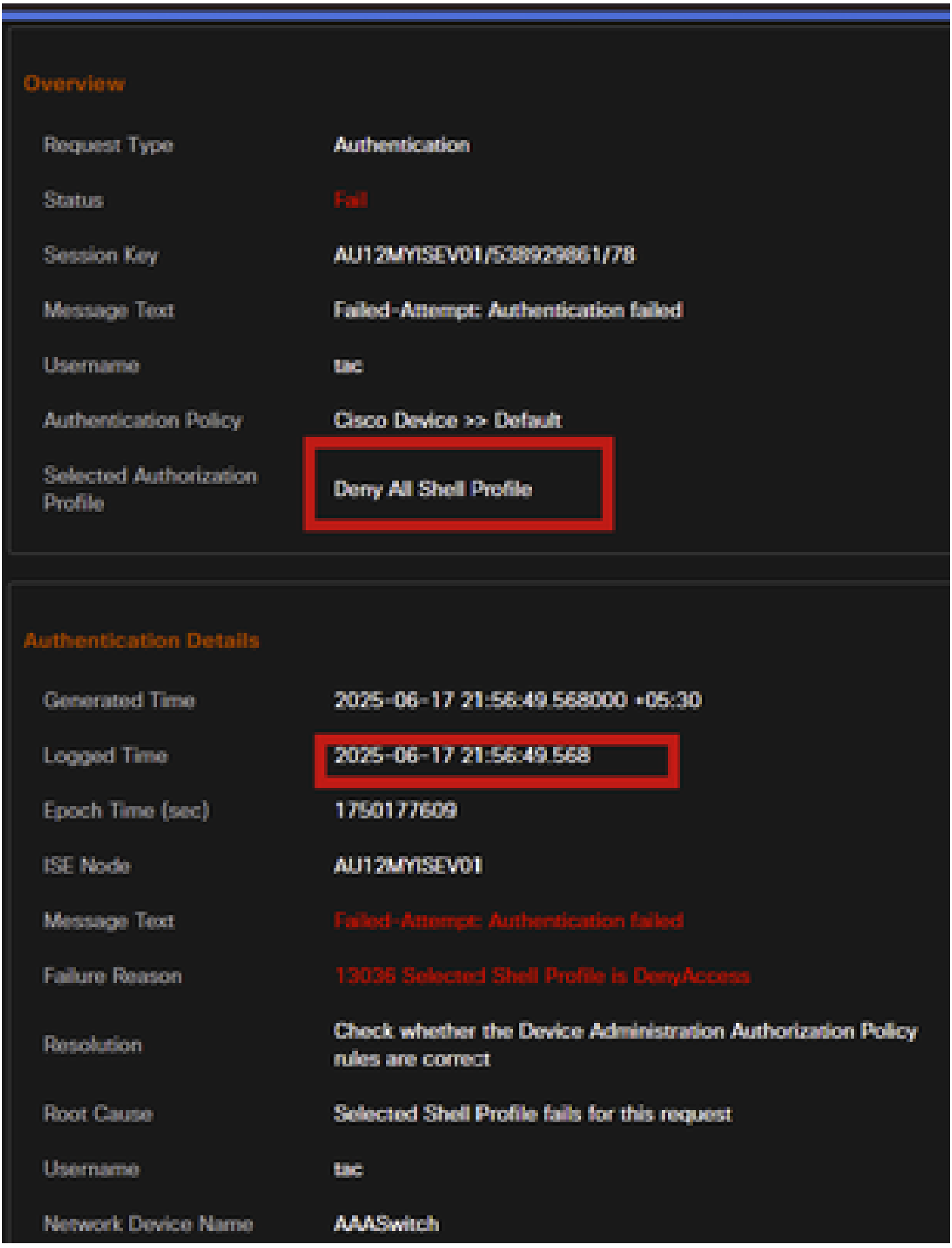
tacacs服务器ISE
address ipv4 10.127.197.53
key Qwerty123
```

验证

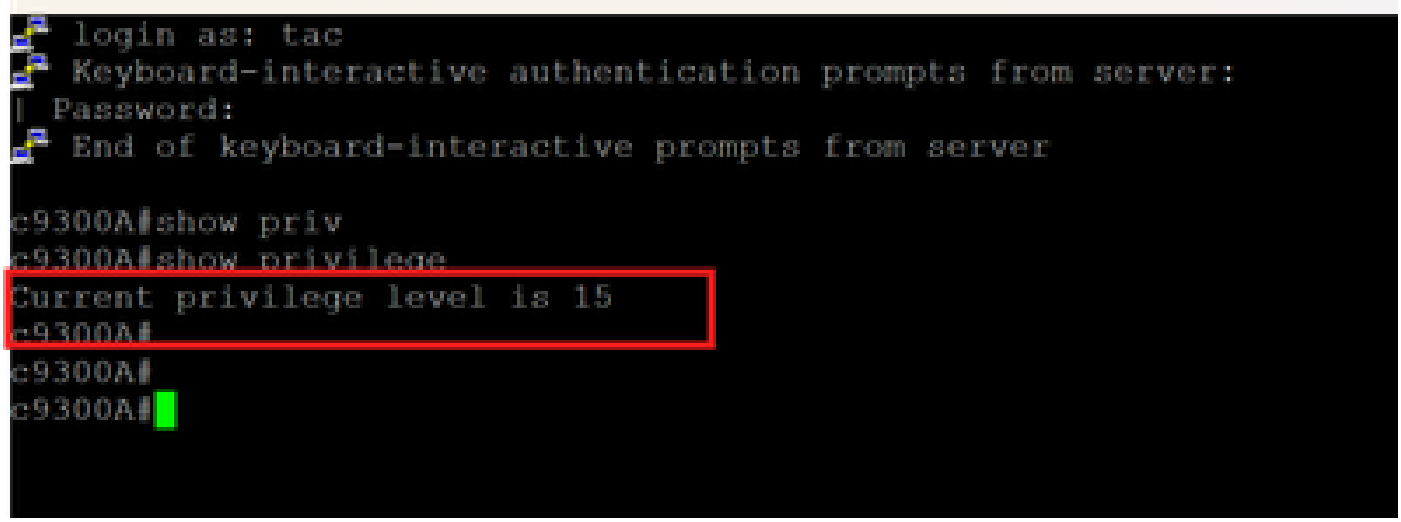
在工作时间外尝试通过SSH连接到交换机的用户被ISE拒绝访问。



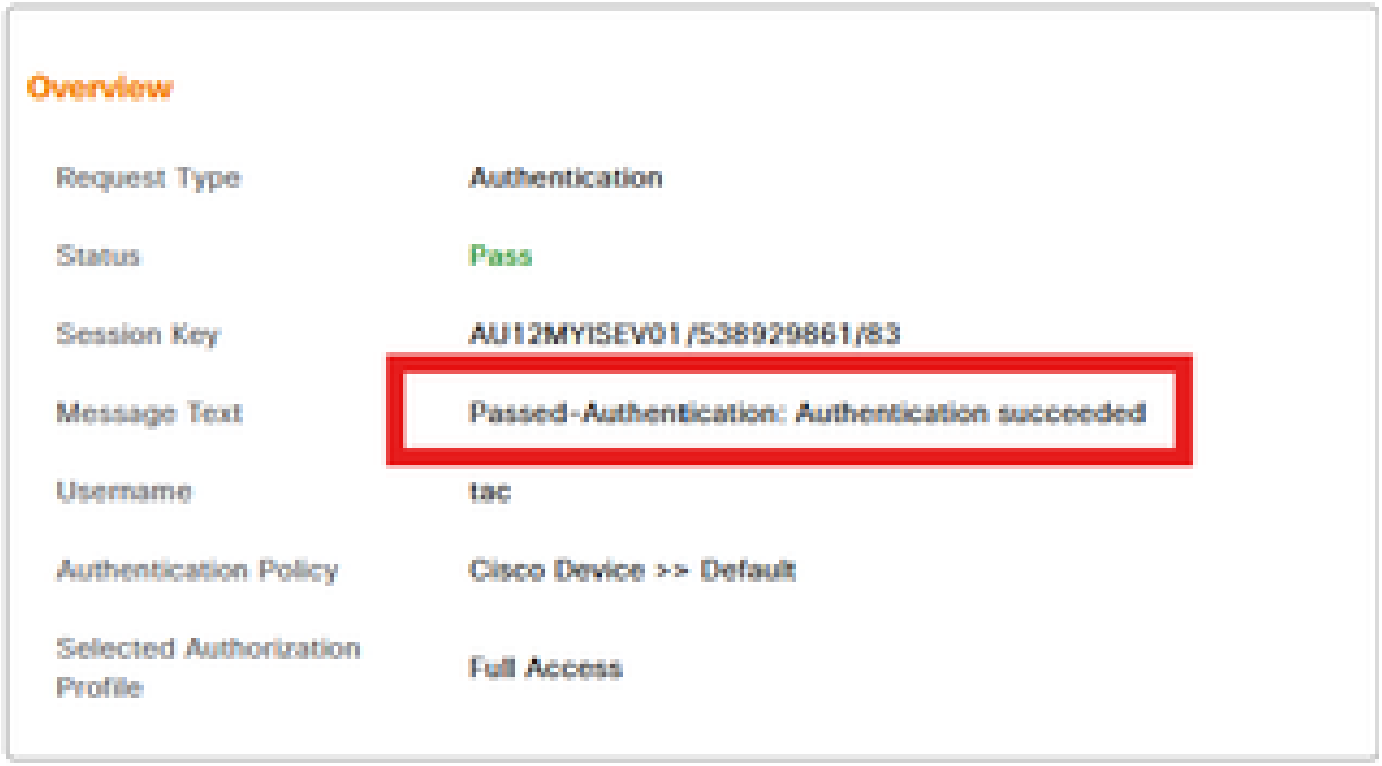
ISE实时日志表示授权失败，因为授权策略中的时间和日期条件不匹配，导致会话命中默认拒绝访问规则。



在工作时间尝试通过SSH连接到交换机并获得读写访问的用户：

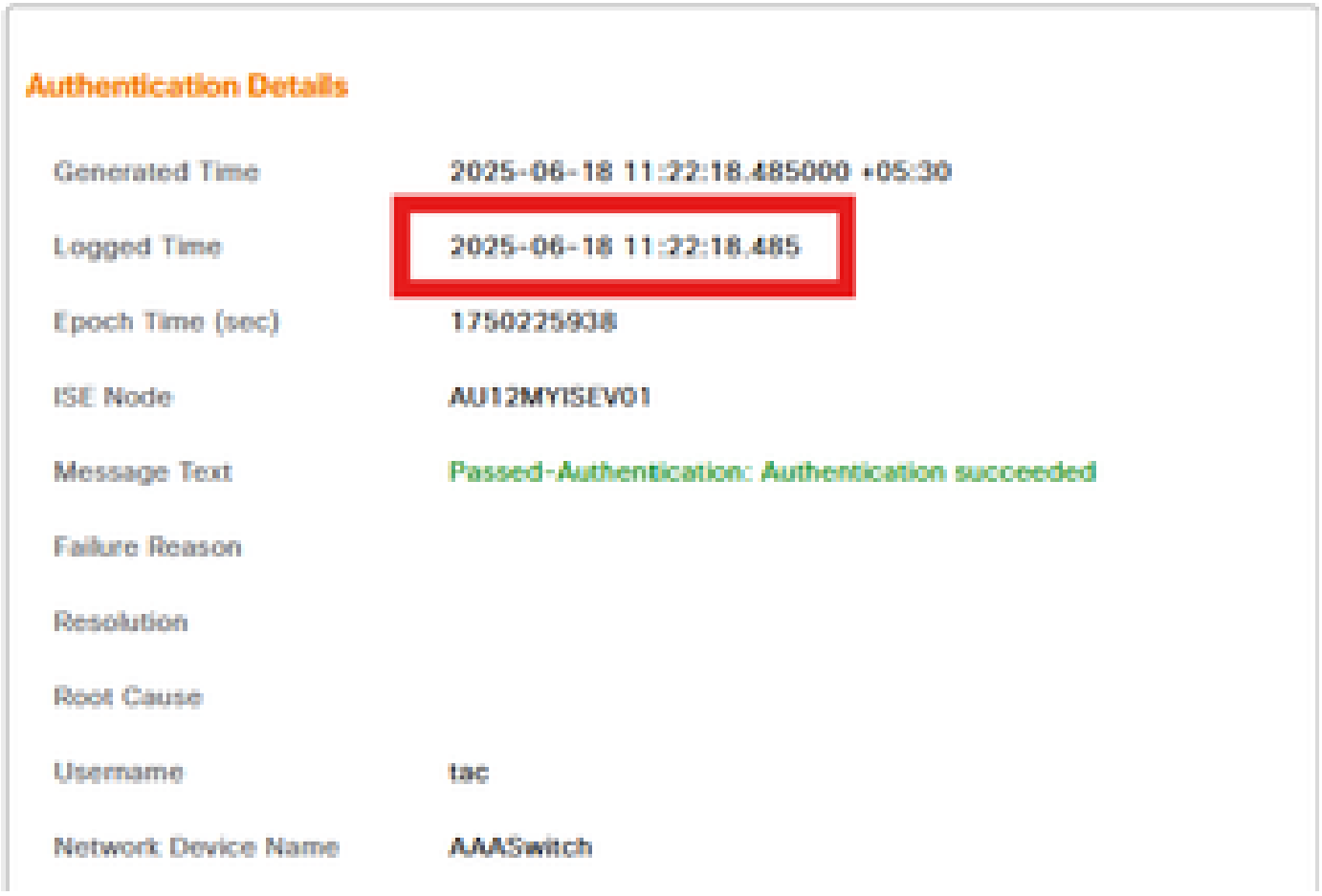


ISE实时日志指示在工作时间登录符合时间和日期条件，并符合正确的策略。



Overview

Request Type	Authentication
Status	Pass
Session Key	AU12MYISEV01/538929861/83
Message Text	Passed-Authentication: Authentication succeeded
Username	tac
Authentication Policy	Cisco Device >> Default
Selected Authorization Profile	Full Access



Authentication Details

Generated Time	2025-06-18 11:22:18.485000 +05:30
Logged Time	2025-06-18 11:22:18.485
Epoch Time (sec)	1750225938
ISE Node	AU12MYISEV01
Message Text	Passed-Authentication: Authentication succeeded
Failure Reason	
Resolution	
Root Cause	
Username	tac
Network Device Name	AAASwitch

故障排除

ISE上的调试

收集具有以下属性的ISE支持捆绑包，在调试级别设置：

- RuleEngine-Policy-IDGroups
- RuleEngine属性
- 策略引擎
- epm-pdp
- epm-pip

当由于时间和日期条件与配置的工作时间不匹配而在工作时间外尝试通过SSH连接到交换机时。

show logging application ise-psc.log

```
2025-06-17 21:56:49,560 DEBUG [PolicyEngineEvaluationThread-7][[]]
cpm.policy.eval.utils.RuleUtil -::::- 360158683110.127.197.5449306Authentication3601586831:评估规则 — <Rule Id="cdd4e295-6d1b-477b-8ae6-587131770585">
<条件Lhs-operand="operandId" Operator="DATETIME_MATCHES" Rhs-operand="rhsproand"/>
</Rule>
2025-06-17 21:56:49,560 DEBUG [PolicyEngineEvaluationThread-7][[]]
cpm.policy.eval.utils.RuleUtil -::::- 360158683110.127.197.5449306Authentication3601586831:使用id评估条件 — 72483811-ba39-4cc2-bdac-90a38232b95e - LHS操作数Id — 操作数Id、运算符DATETIME_MATCHES、RHS操作数Id - rhsoperand
2025-06-17 21:56:49,560 DEBUG [PolicyEngineEvaluationThread-7][[]]
cpm.policy.eval.utils.ConditionUtil -::::-
360158683110.127.197.5449306Authentication3601586831:条件lhsproand值 —
com.cisco.cpm.policy.DTConstraint@6924136c , rhsproand值 —
com.cisco.cpm.policy.DTConstraint@3eeea825
2025-06-17 21:56:49,560 DEBUG [PolicyEngineEvaluationThread-7][[]]
cpm.policy.eval.utils.RuleUtil -::::- 360158683110.127.197.5449306Authentication3601586831:条件评估结果 — 72483811-ba39-4cc2-bdac-90a38232b95e返回 — false
2025-06-17 21:56:49,560 DEBUG [PolicyEngineEvaluationThread-7][[]]
cpm.policy.eval.utils.RuleUtil -::::- 360158683110.127.197.5449306Authentication3601586831:为条件设置结果：72483811-ba39-4cc2-bdac-90a38232b95e:假
```

当用户在营业时间尝试通过SSH连接到交换机时，符合Time and Date Condition（时间和日期条件）。

show logging application ise-psc.log

```
2025-06-18 11:22:18,473 DEBUG [PolicyEngineEvaluationThread-11][[]]
cpm.policy.eval.utils.RuleUtil -::::- 181675991110.127.197.5414126Authentication1816759911:评估规则 — <Rule Id="cdd4e295-6d1b-477b-8ae6-587131770585">
<条件Lhs-operand="operandId" Operator="DATETIME_MATCHES" Rhs-operand="rhsproand"/>
</Rule>

2025-06-18 11:22:18,474 DEBUG [PolicyEngineEvaluationThread-11][[]]
cpm.policy.eval.utils.RuleUtil -::::- 181675991110.127.197.5414126Authentication1816759911:使用id评估条件 — 72483811-ba39-4cc2-bdac-90a38232b95e - LHS操作数Id — 操作数Id、运算符DATETIME_MATCHES、RHS操作数Id - rhsoperand
```

```
2025-06-18 11:22:18,474 DEBUG [PolicyEngineEvaluationThread-11][[]]
cpm.policy.eval.utils.ConditionUtil -::::-
181675991110.127.197.5414126Authentication1816759911:条件lhsproand值 —
com.cisco.cpm.policy.DTConstraint@4af10566，rhsproand值 —
com.cisco.cpm.policy.DTConstraint@2bdb62e9
2025-06-18 11:22:18,474 DEBUG [PolicyEngineEvaluationThread-11][[]]
cpm.policy.eval.utils.RuleUtil -::::- 181675991110.127.197.5414126Authentication1816759911:条
件评估结果 — 72483811-ba39-4cc2-bdac-90a38232b95e返回 — true
2025-06-18 11:22:18,474 DEBUG [PolicyEngineEvaluationThread-11][[]]
cpm.policy.eval.utils.RuleUtil -::::- 181675991110.127.197.5414126Authentication1816759911:为
条件设置结果：72483811-ba39-4cc2-bdac-90a38232b95e:true
```

相关信息

- 思科ISE设备管理规范部署指南

常见问题解答

- 是否可以根据时间应用不同的访问级别？
  Yes.您可以创建不同的授权策略并将其链接到时间条件。

  例如：
  在工作时间完全访问
  数小时后的只读访问
  周末不能访问

- 如果系统时间不正确或不同步，会发生什么情况？
  ISE可能应用不正确的策略或无法可靠地执行基于时间的规则。确保所有设备和ISE节点使用同步的NTP源。

- 基于时间的策略是否可以与其他条件（例如，用户角色、设备类型）结合使用？
  Yes.时间条件可以与策略规则中的其他属性结合使用，以创建精细且安全的访问控制。

- TACACS中的外壳和命令集是否支持基于时间的访问+?
  Yes.基于时间的条件可以控制对设备外壳或特定命令集的访问，具体取决于授权策略和配置文件的构建方式。

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）。