Configurar o acesso TACACS+ baseado em tempo para dispositivos de rede com ISE

Contents

Introdução

Este documento descreve como configurar a autorização baseada em Data e Hora para a política de Administração de dispositivo no Cisco Identity Services Engine (ISE).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento da configuração do protocolo Tacacs e do Identity Services Engine (ISE).

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Switch Cisco Catalyst 9300 com softwareCisco IOS® XE 17.12.5 e posterior
- Cisco ISE, versão 3.3 e posterior

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

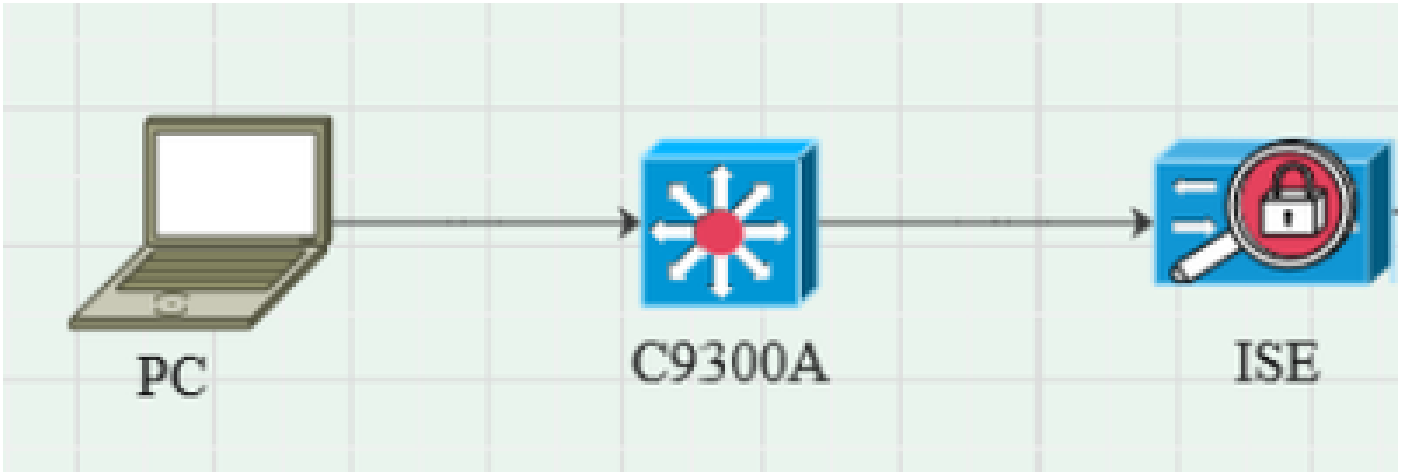
As políticas de autorização são um componente-chave do Cisco Identity Services Engine (ISE), permitindo que você defina regras e configure perfis de autorização para usuários ou grupos específicos que acessam recursos de rede. Essas políticas avaliam as condições para determinar qual perfil aplicar. Quando as condições de uma regra são atendidas, o perfil de autorização correspondente é retornado, concedendo o acesso apropriado à rede.

O Cisco ISE também suporta as condições de data e hora, que permitem que as políticas sejam aplicadas somente durante horários ou dias especificados. Isso é particularmente útil para aplicar controles de acesso com base em requisitos comerciais baseados em tempo.

Este documento descreve a configuração para permitir o acesso administrativo TACACS+ a dispositivos de rede apenas durante o horário comercial (de segunda a sexta-feira, das 08:00 às 17:00) e para negar o acesso fora dessa janela de tempo.

Configurar

Diagrama de Rede



Configurar o ISE

Passo 1: Criar Condição de Data e Hora

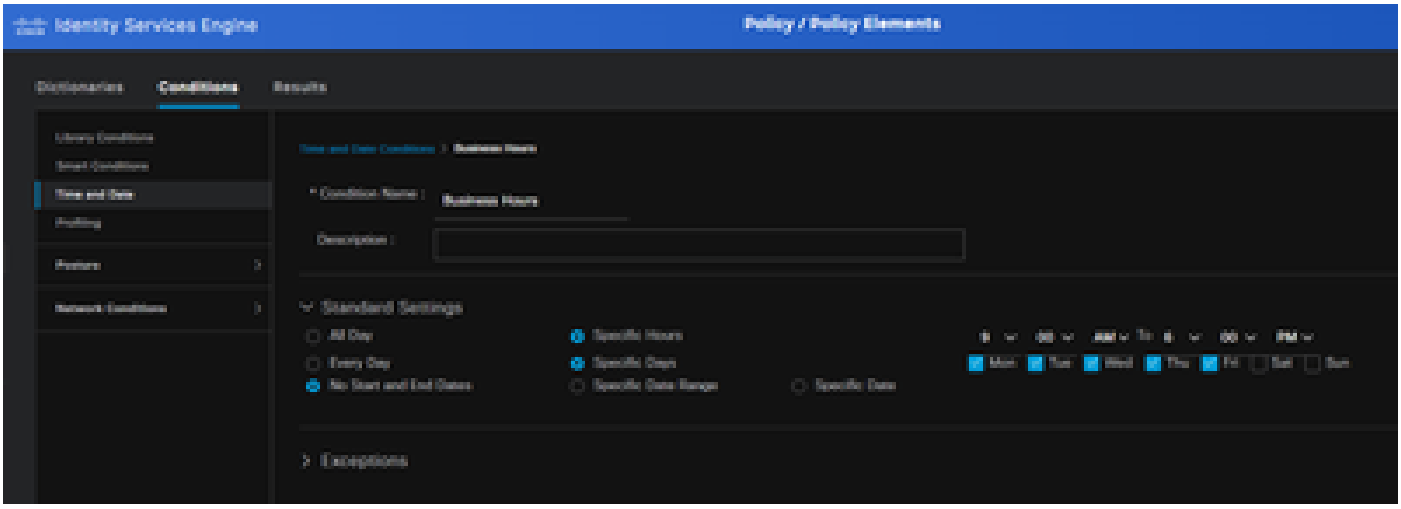
Navegue até Política > Elementos de política > Condições > Hora e data e clique em Adicionar.

Nome da condição: Horário comercial

Defina as configurações padrão de intervalo de tempo > Horários específicos: 09:00 AM - 06:00

PM

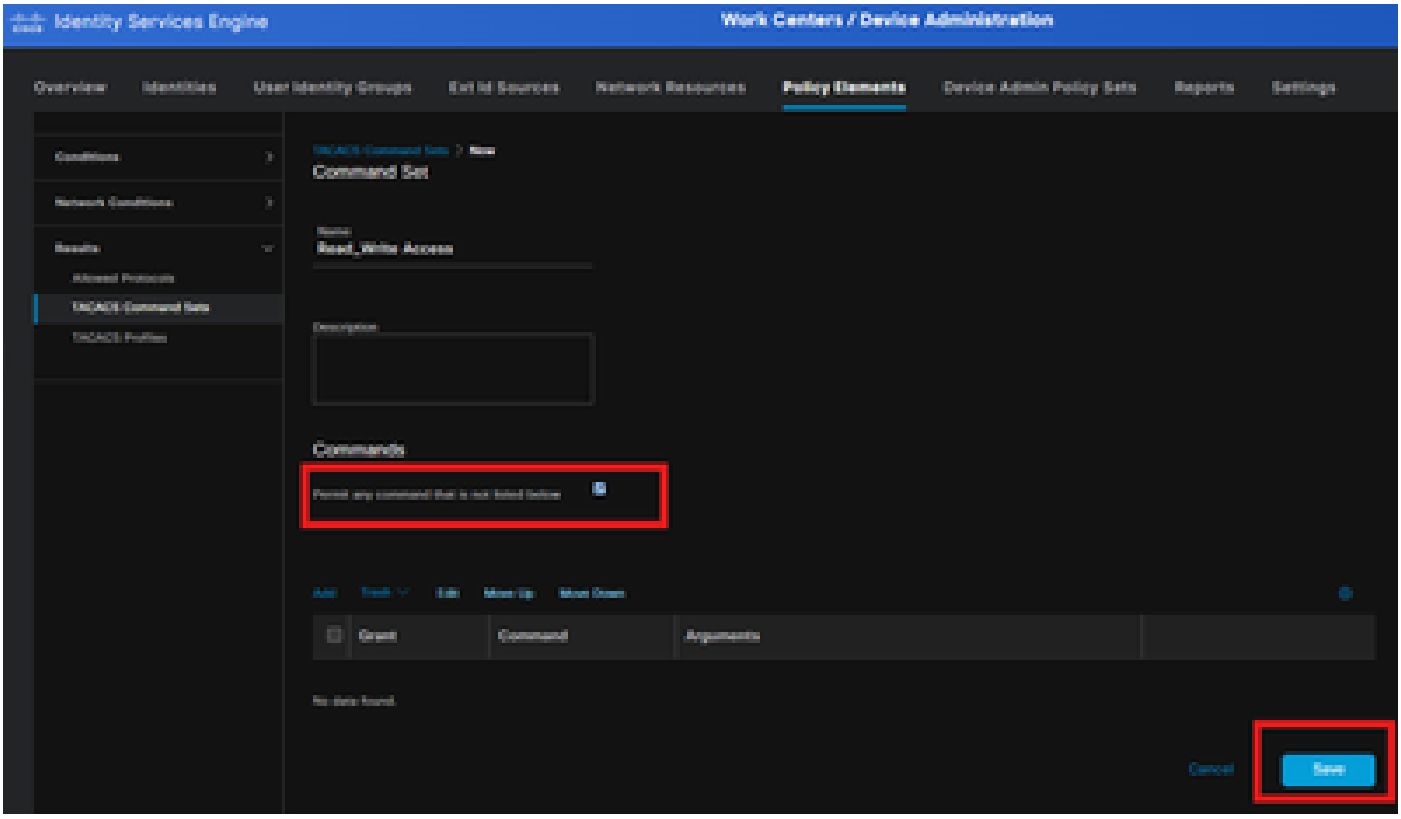
Dias específicos: De segunda a sexta



Passo 2: Criar um conjunto de comandos TACACS+

Navegue até Centros de trabalho > Administração de dispositivo > Elementos de política > Resultados > Conjuntos de comandos Tacacs.

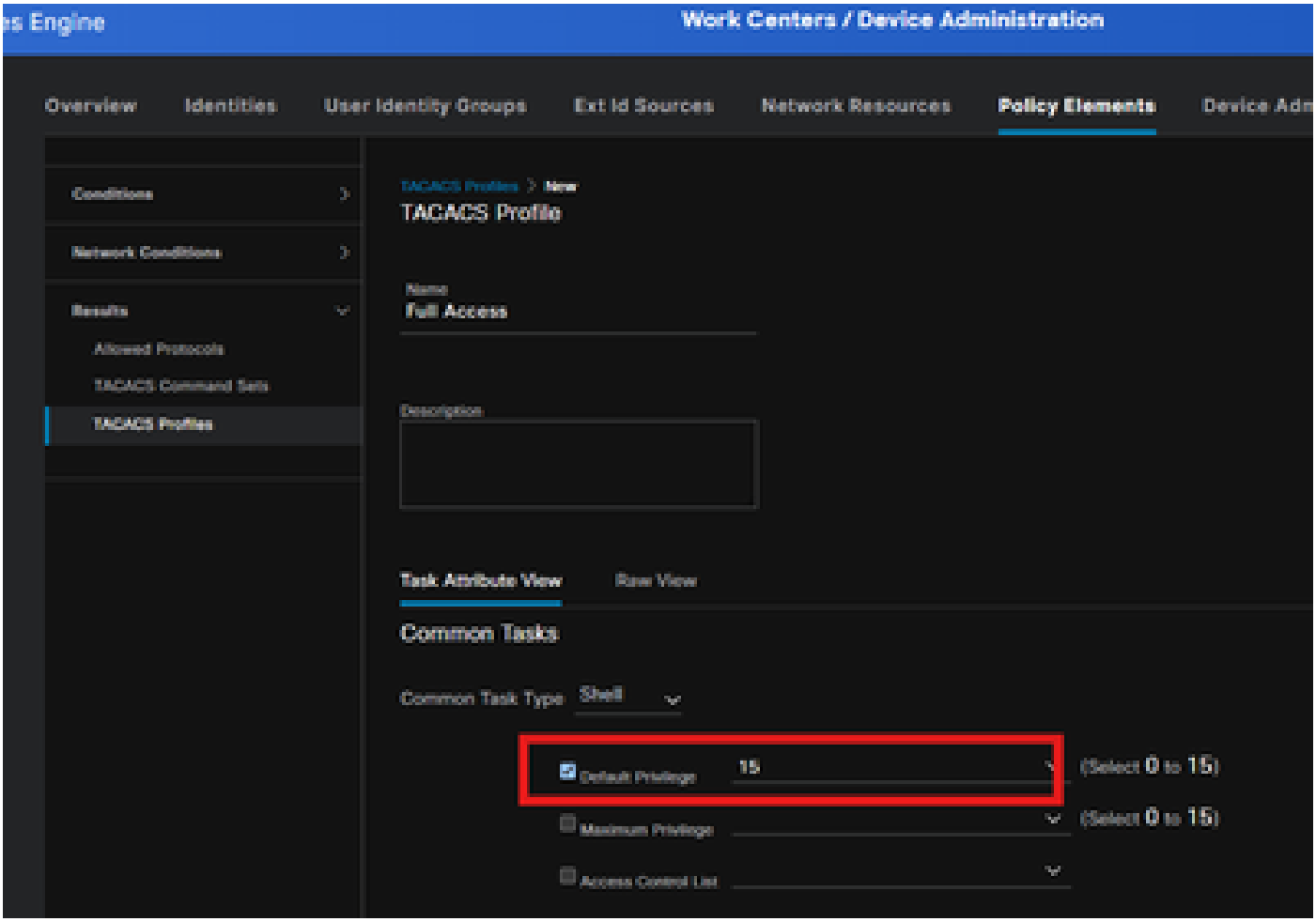
Crie um conjunto de comandos marcando a caixa de seleção Permitir qualquer comando que não esteja listado abaixo e clique em Enviar ou adicione os Comandos limitados se quiser restringir determinados comandos CLI.



Passo 3: Criar um perfil TACACS+

Navegue até Centros de trabalho > Administração de dispositivo > Elementos de política > Resultados > Perfis TACACS. Clique em Add.

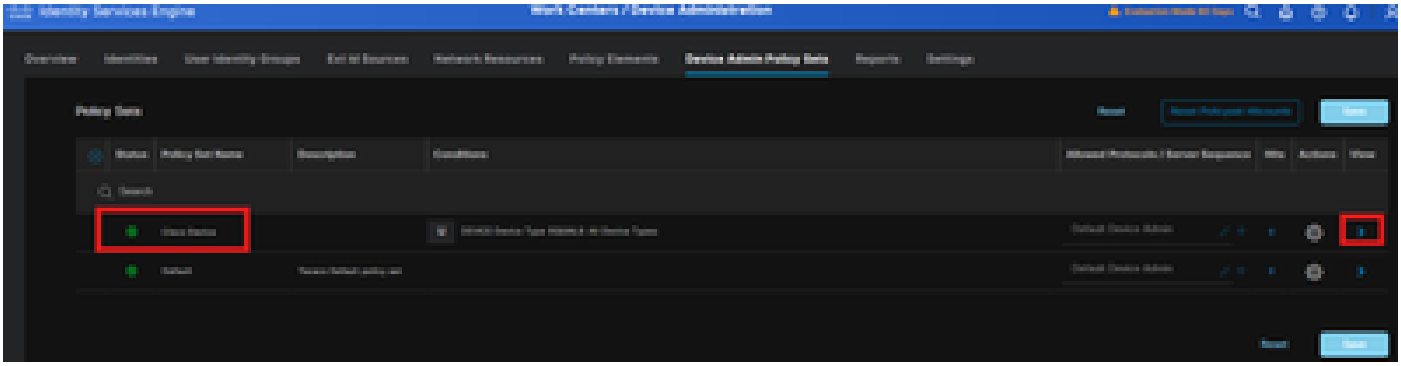
Selecione Tipo de Tarefa de Comando como Shell, depois a caixa de seleção Privilégio Padrão e insira o valor 15. Clique em Enviar.



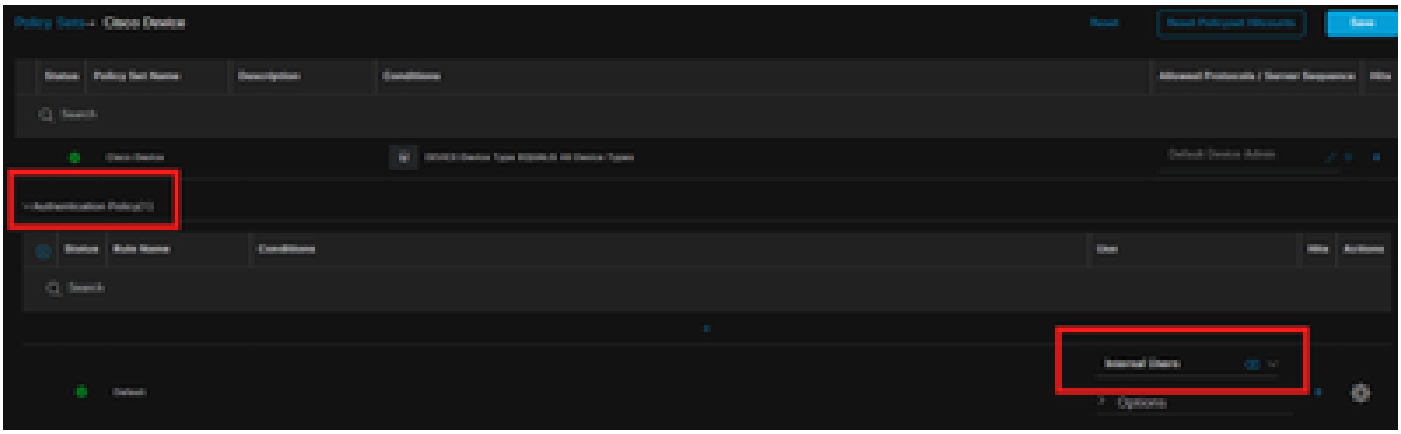
Passo 4: Criar política de autorização TACACS

Navegue até Centros de trabalho > Administração de dispositivos > Conjuntos de políticas de administração de dispositivos.

Selecione seu conjunto de políticas ativo.



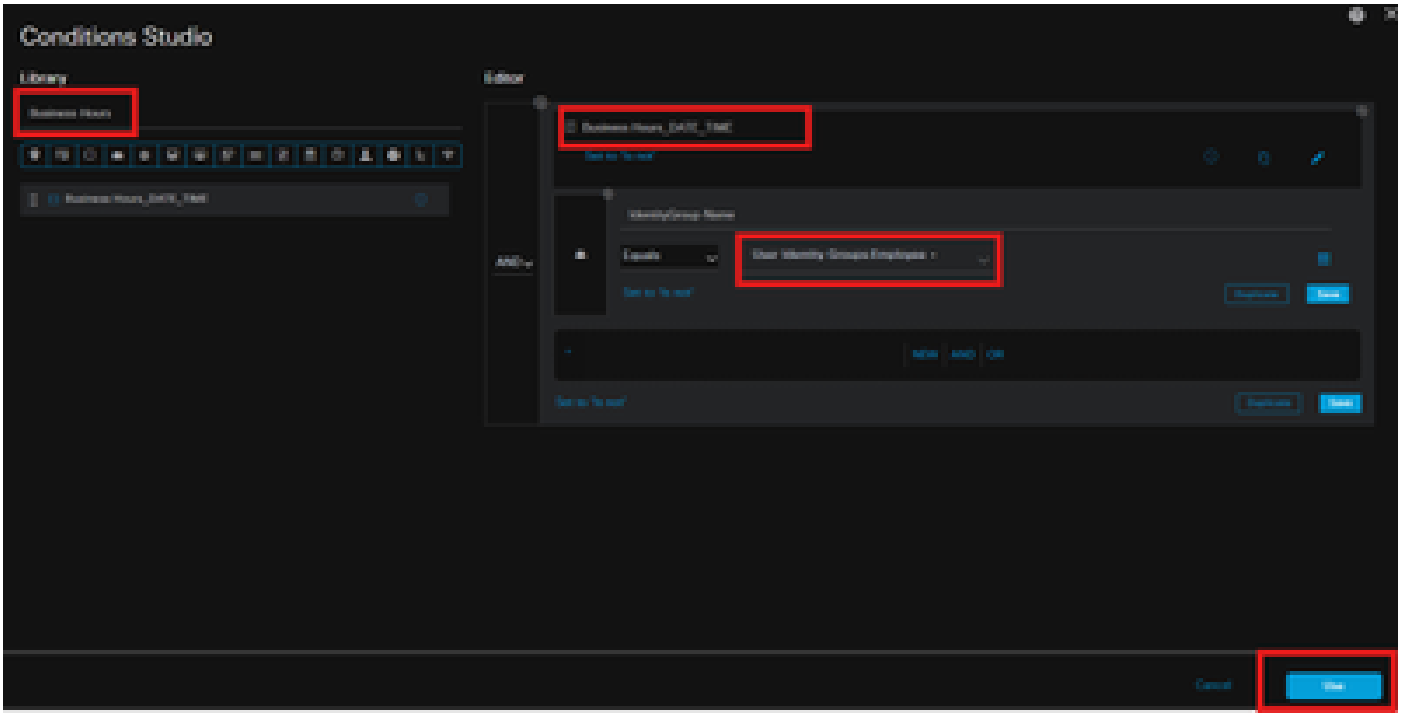
Configure a Diretiva de Autenticação com base nos usuários internos ou do Ative Diretory.



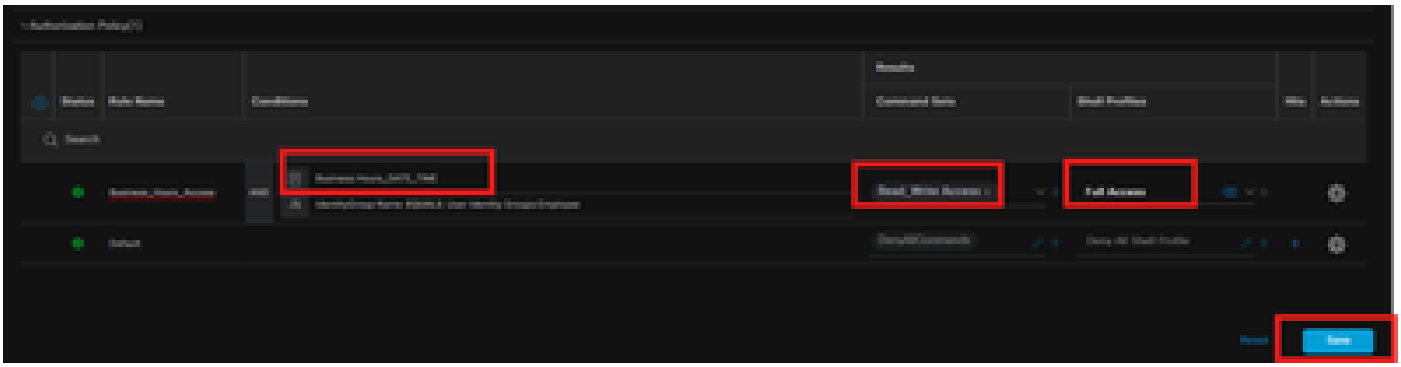
Na seção Authorization Policy, clique em Add Rule para fornecer o nome da regra e clique em + para adicionar condições de autorização.

Uma nova janela Estúdio de condição é exibida, no campo Pesquisar por nome, insira o nome criado na etapa 1 e arraste-o para o Editor.

Adicione outras condições com base no Grupo de usuários e clique em Salvar.



Em Results, selecione o Conjunto de Comandos Tacacs e o Perfil Shell criados nas etapas 2 e 3 e clique em Save.

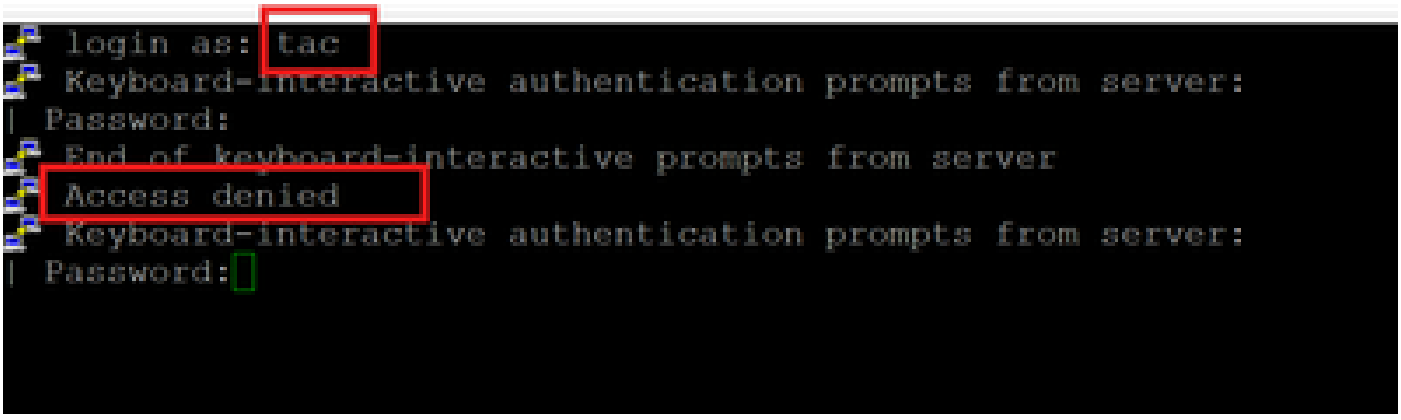


Configurar o switch

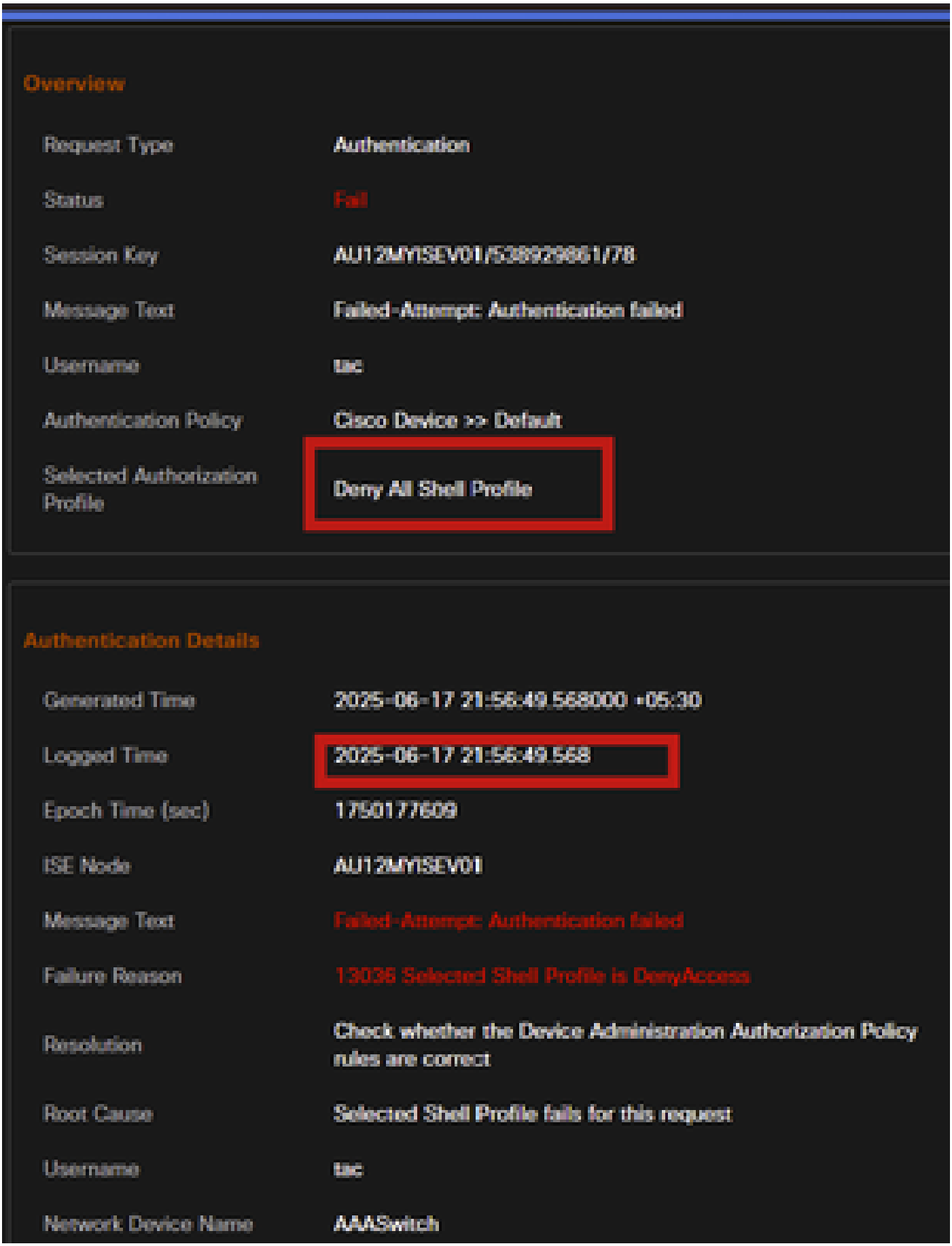
```
aaa new-model

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 command 15 default local group tacacs+

ISE de servidor TACACS
address ipv4 10.127.197.53
key Qwerty123
```

Verificar

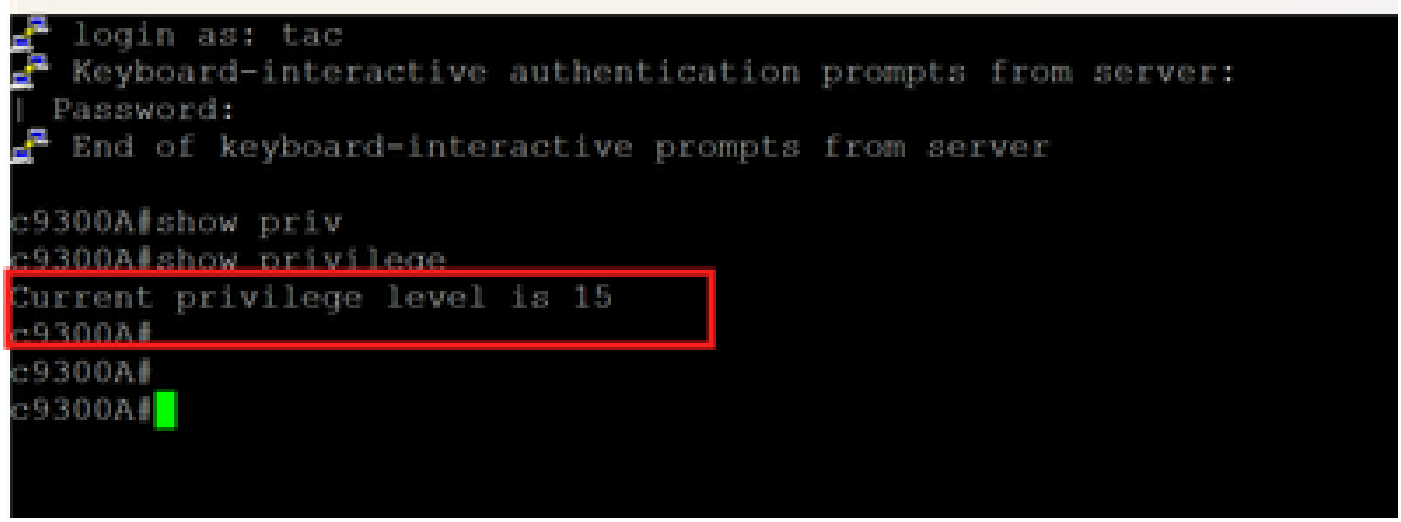
O usuário que está tentando fazer SSH no Switch fora do horário comercial e teve o acesso negado do ISE.



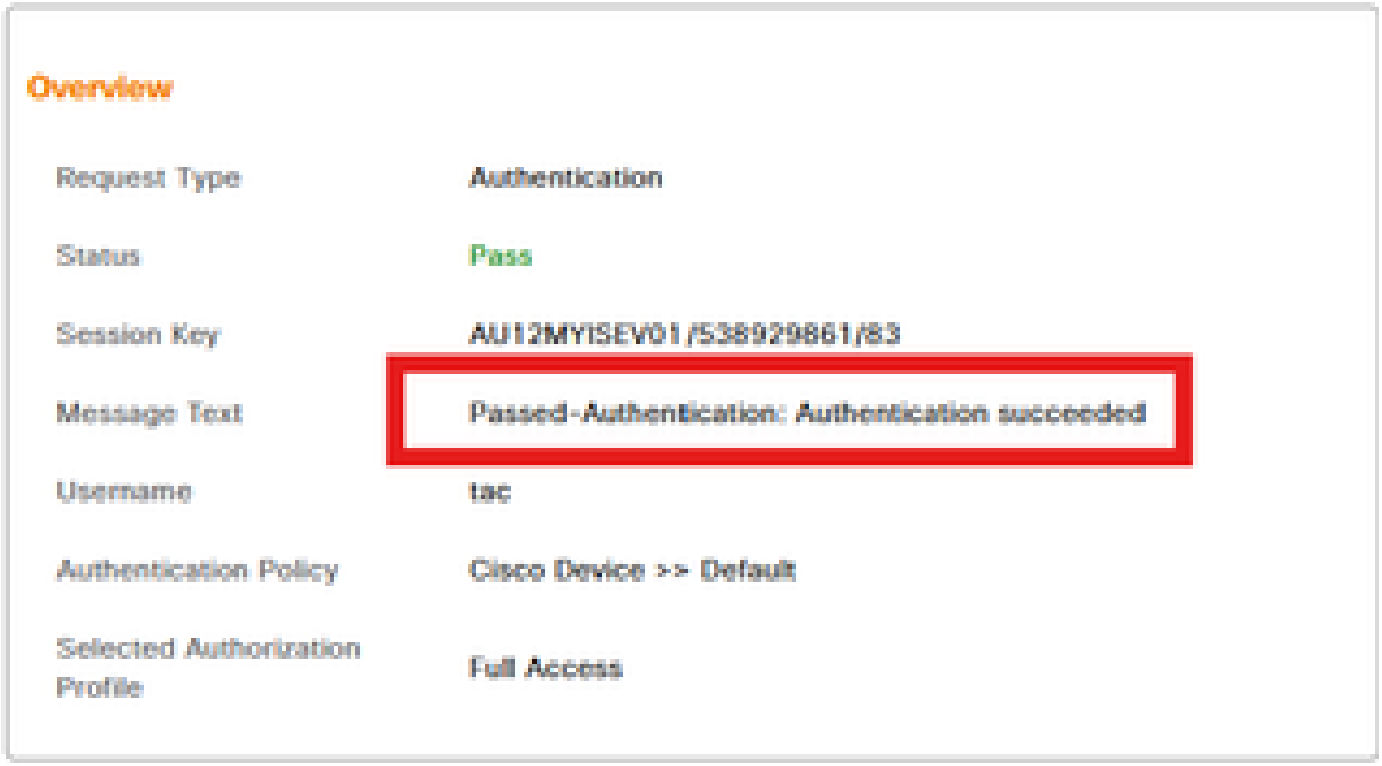
Os registros ao vivo do ISE indicam que a autorização falhou porque a condição de data e hora na política de autorização não correspondeu, fazendo com que a sessão atinja a regra de negação de acesso padrão.



Usuário tentando usar SSH no switch durante o horário comercial e obter acesso de leitura e gravação:

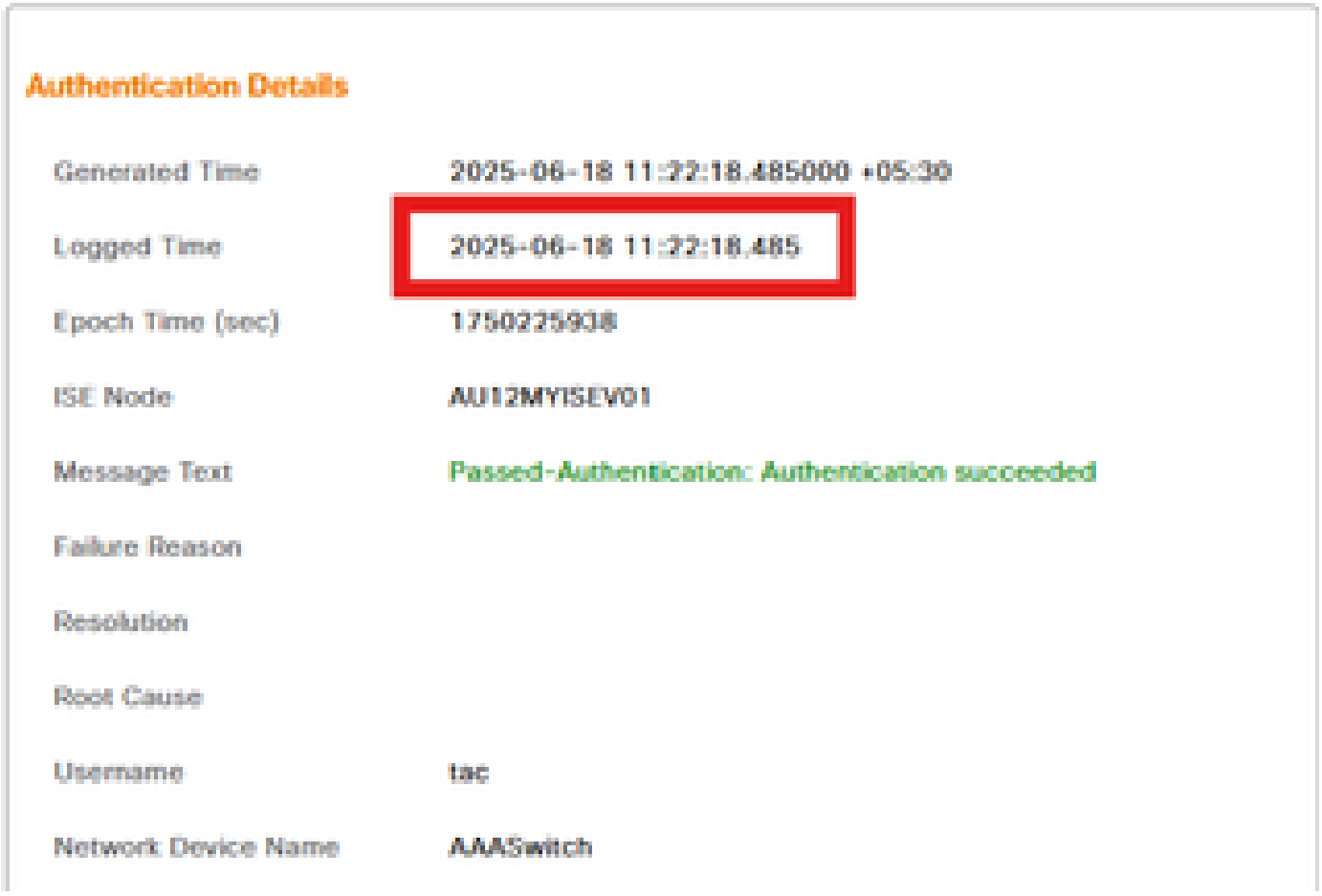


O registro ao vivo do ISE indica que o login durante o horário comercial correspondeu à condição de data e hora e pressiona a política correta.



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

Troubleshooting

Depurações no ISE

Colete o pacote de suporte do ISE com estes atributos para serem definidos no nível de depuração:

- RuleEngine-Policy-IDGroups
- RuleEngine-Atributos
- Mecanismo de política
- epm-pdp
- epm-pip

Quando o usuário tenta usar SSH no switch fora do horário comercial devido à condição de hora e data não correspondida com o horário comercial configurado.

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:
Regra de avaliação - <Rule Id="cdd4e295-6d1b-477b-8ae6-587131770585">
<Condition Lhs-operand="operandId" Operator="DATETIME_MATCHES" Rhs-
operand="rhsoperand"/>
</Regra>
2025-06-17 21:56:49,560 DEBUG [PolicyEngineEvaluationThread-7][[]]
cpm.policy.eval.utils.RuleUtil -::::- 360158683110.127.197.5449306Authentication3601586831:
Condição de Avaliação com id - 72483811-ba39-4cc2-bdac-90a38232b95e - operandId de LHS -
operandId, operador DATETIME_MATCHES, operandId de RHS - rhsoperand
2025-06-17 21:56:49,560 DEBUG [PolicyEngineEvaluationThread-7][[]]
cpm.policy.eval.utils.ConditionUtil -:::::-
360158683110.127.197.5449306Authentication3601586831: Condição lhsoperand Valor -
com.cisco.cpm.policy.DTConstraint@6924136c , rhsoperand Valor -
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:
Resultado da avaliação para Condição - 72483811-ba39-4cc2-bdac-90a38232b95e retornado -
falso
2025-06-17 21:56:49,560 DEBUG [PolicyEngineEvaluationThread-7][[]]
cpm.policy.eval.utils.RuleUtil -::::- 360158683110.127.197.5449306Authentication3601586831:
Definindo resultado para condição: 72483811-ba39-4cc2-bdac-90a38232b95e: falso
```

Quando o usuário que está tentando fazer SSH no Switch durante o horário comercial correspondeu à condição de data e hora.

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:
Regra de avaliação - <Rule Id="cdd4e295-6d1b-477b-8ae6-587131770585">
<Condition Lhs-operand="operandId" Operator="DATETIME_MATCHES" Rhs-
operand="rhsoperand"/>
</Regra>
```

```
2025-06-18 11:22:18,474 DEBUG [PolicyEngineEvaluationThread-11][[]]
cpm.policy.eval.utils.RuleUtil -:::::- 181675991110.127.197.5414126Authentication1816759911:
Condição de Avaliação com id - 72483811-ba39-4cc2-bdac-90a38232b95e - operandId de LHS -
operandId, operador DATETIME_MATCHES, operandId de RHS - rhsoperand
2025-06-18 11:22:18,474 DEBUG [PolicyEngineEvaluationThread-11][[]]
cpm.policy.eval.utils.ConditionUtil -:::::-
181675991110.127.197.5414126Authentication1816759911: Condição lhsoperand Valor -
com.cisco.cpm.policy.DTConstraint@4af10566 , rhsoperand Valor -
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:
Resultado da avaliação para Condição - 72483811-ba39-4cc2-bdac-90a38232b95e retornado -
verdadeiro
2025-06-18 11:22:18,474 DEBUG [PolicyEngineEvaluationThread-11][[]]
cpm.policy.eval.utils.RuleUtil -:::::- 181675991110.127.197.5414126Authentication1816759911:
Definindo resultado para condição: 72483811-ba39-4cc2-bdac-90a38232b95e: verdadeiro
```

Informações Relacionadas

- Guia de implantação prescritiva da administração de dispositivos do Cisco ISE

Perguntas mais freqüentes

- Posso aplicar diferentes níveis de acesso com base no tempo?
  Yes. Você pode criar diferentes políticas de autorização e vinculá-las a condições de tempo.

  Por exemplo:
  Acesso total durante o horário comercial
  Acesso somente leitura após horas
  Sem acesso nos finais de semana

- O que acontece se a hora do sistema estiver incorreta ou não sincronizada?
  O ISE pode aplicar políticas incorretas ou deixar de aplicar regras baseadas em tempo de forma confiável. Certifique-se de que todos os dispositivos e nós do ISE usem uma origem de NTP sincronizada.

- As políticas baseadas em tempo podem ser usadas em conjunto com outras condições (por exemplo, função de usuário, tipo de dispositivo)?
  Yes. As condições de tempo podem ser combinadas com outros atributos em suas regras de política para criar controles de acesso granulares e seguros.

- O acesso baseado em tempo é suportado para o shell e conjuntos de comandos no TACACS+?
  Yes. As condições baseadas em tempo podem controlar o acesso ao shell do dispositivo ou a conjuntos de comandos específicos, dependendo de como a política de autorização e os perfis são estruturados.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.