

Como Configurar o Suporte TACACS+ no Cache Engine

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurar o motor do esconderijo para o suporte TACACS+](#)

[Verificar](#)

[Comandos para Troubleshooting](#)

[Informações Relacionadas](#)

[Introdução](#)

Este documento descreve como configurar o apoio do protocolo tacacs+ (TACACS+) a fim alcançar o Cisco Cache Engine. As instruções neste documento permitirão que você valide contra um server remoto/base de dados TACACS+ quando você telnet ao motor do esconderijo. Se o server não inclui uma entrada para seu usuário - identificação, verifica localmente para ver se há a informação de acesso válida.

[Pré-requisitos](#)

[Requisitos](#)

Não existem requisitos específicos para este documento.

[Componentes Utilizados](#)

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

- Cisco Cache Engine 505 em um ambiente de laboratório com configurações esclarecida
- Software Cisco Cache Engine versão 2.3.1
- CiscoSecure para UNIX

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 sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Refira-se às [convenções dos dicas técnicas da Cisco](#) para obter informações sobre as convenções de documento.

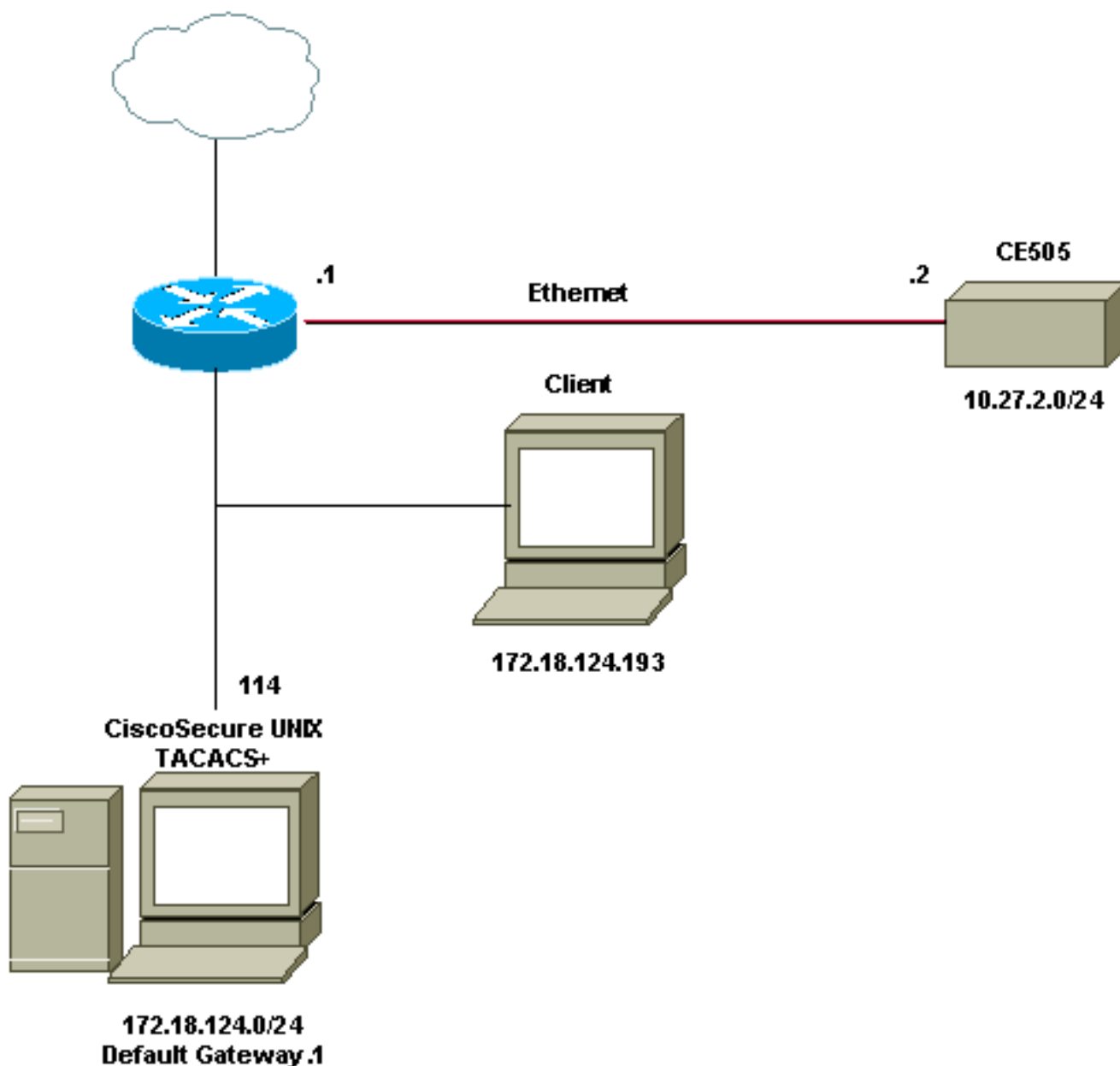
Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Nota: Use a [Command Lookup Tool](#) ([somente clientes registrados](#)) para obter mais informações sobre os comandos usados nesta seção.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Configurar o motor do esconderijo para o suporte TACACS+

Termine estas etapas a fim configurar o motor do esconderijo para o suporte TACACS+:

1. Configure o Mecanismo de Cache da respectiva versão do protocolo WCCP (Web Cache Communication Protocol).
2. Use estes comandos para a configuração padrão:
`authentication login local enable authentication configuration local enable`
3. Configurar o endereço IP do servidor TACACS+. Se vários servidores especificarem qual endereço é primário, os servidores secundários serão deixados como opções em branco.
4. Configure a autenticação para o servidor TACACS+ como primária. Se o servidor não estiver disponível, o padrão será a autenticação especificada localmente.
5. Configurar a autenticação à informação chave TACACS+ se necessário.

Nota: Você deve permitir o TACACS+ no Cisco Cache Engine porque os motores do Cisco Cache usam o PPP a fim autenticar com o servidor de TACACS, ao contrário do Roteadores que não exige o PPP. A fim permitir o TACACS+ nos motores do Cisco Cache, no Cisco Secure ACS aberto 2.6, clicar a aba da **instalação de grupo**, e verificar a caixa de verificação **IP PPP** situada na área dos ajustes TACACS+.

Suas linhas de comando devem parecer similares a esta saída:

```
cepro(config)#tacacs server 172.18.124.114 cepro(config)#authentication login tacacs ena primary
cepro(config)#authen configuration tacacs enab
```

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

A [Output Interpreter Tool \(apenas para clientes registrados\)](#) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

- **versão da mostra** — Indica o software que é executado no motor do esconderijo, assim como alguns outros componentes como o uptime de sistema (tal como onde o código foi carregado previamente e a data em que foi).
`cepro#show version` Cisco Cache Engine Copyright (c) 1986-2001 by Cisco Systems, Inc. Software Release: CE ver 2.31 (Build: FCS 02/16/01) Compiled: 11:20:14 Feb 22 2001 by bbalagot Image text-base 0x108000, data_base 0x437534 System restarted by Reload The system has been up for 20 hours, 42 minutes, 59 seconds. System booted from "flash"
- **hardware da mostra** — Indicado a mesma informação que o comando `show version`, assim como os componentes de hardware do motor do esconderijo.
`cepro#show hardware` Cisco Cache Engine Copyright (c) 1986-2001 by Cisco Systems, Inc. Software Release: CE ver 2.31 (Build: FCS 02/16/01) Compiled: 11:20:14 Feb 22 2001 by bbalagot Image text-base 0x108000, data_base 0x437534 System restarted by Reload The system has been up for 21 hours, 15 minutes, 16 seconds. System booted from "flash" Cisco Cache Engine CE505 with CPU AMD-K6 (model 8) (rev. 12) AuthenticAMD 2 Ethernet/IEEE 802.3 interfaces 1 Console interface. 134213632 bytes of Physical Memory 131072 bytes of ROM memory. 8388608 bytes of flash memory. List of disk drives: /c0t0d0 (scsi bus 0, unit 0, lun 0)
- **executar-configuração da mostra** — Indica a configuração running no motor do esconderijo.
`cepro#show running-config` Building configuration... Current configuration: ! ! !
user add admin uid 0 password 1 "eeSdy9dcy" capability admin-access user add chbanks uid 5001 password 1 "eeSdy9dcy" capability admin-access ! ! ! hostname cepro ! interface ethernet 0 ip address 10.27.2.2 255.255.255.0 ip broadcast-address 10.27.2.255 exit ! ! interface ethernet 1 exit ! ip default-gateway 10.27.2.1 ip route 0.0.0.0 0.0.0.0 10.27.2.1 cron file /local/etc/crontab ! wccp router-list 1 10.27.2.1 wccp web-cache router-list-num 1

```
! authentication login tacacs enable primary authentication login local enable !--- on by
default ---! authentication configuration tacacs enable authentication configuration local
enable !---- on by default ---! tacacs server 172.18.124.114 primary rule no-cache url-regex
.*cgi-bin.* rule no-cache url-regex .*aw-cgi.* !! end cepro#
```

- **tacacs da mostra** — Indica os ajustes para o server TACACS+. `cepro#show tacacs` Login Authentication for Console/Telnet Session: enabled (primary) Configuration Authentication for Console/Telnet Session: enabled TACACS Configuration: ----- Key = Timeout = 5 seconds Retransmit = 2 times Server Status ----- 172.18.124.114 primary
- **mostre tacacs das estatísticas** — Estatísticas dos indicadores TACACS+. `cepro#show statistics tacacs` TACACS+ Statistics ----- Number of access requests: 13 Number of access deny responses: 7 Number of access allow responses: 0
- **autenticação da mostra** — Indica a configuração atual da authentication e autorização TACACS+. `cepro#show authentication` Login Authentication: Console/Telnet Session ----- local enabled tacacs enabled (primary) Configuration Authentication: Console/Telnet Session ----- local enabled tacacs enabled cepro#

Comandos para Troubleshooting

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

A [Output Interpreter Tool \(apenas para clientes registrados\)](#) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

Nota: Consulte [Informações Importantes sobre Comandos de Depuração](#) antes de usar comandos debug.

- **a mostra debuga** — Indica os comandos debug que são permitidos. `cepro#show debug` Authentication debugging is on Tacacs debugging is on
- **monitor terminal** — Indica as saídas de debuga à tela. Esta saída indica os resultados dos comandos debug authentication and debug tacacs. `cepro#terminal monitor`

```
cepro#authenticateUser(): Begin setRemoteIPAddress(): pRemoteAddress 172.18.124.193
bAuthentication(): Begin bAuthenticationIntersection(): Begin bAuthenticationIntersection():
telnet_access 1 setAuthenticatedService(): nServiceToAuthenticate 6
getAuthenticatedService(): Begin getAuthenticatedService(): nServiceToAuthenticate = 6
bAuthenticationIntersection() getAuthenticatedService 6 setErrorDisplayed(): Begin bStatus 0
getLocalLoginAuthEnable(): Begin getLocalLoginAuthEnable(): uiState = 1
getTacacsLoginAuthEnable(): Begin getTacacsLoginAuthEnable(): uiState = 1
getTacacsLoginAuthPrimary(): Begin getTacacsLoginAuthPrimary(): uiState = 1
IncrementTacacsStatRequest(): Begin tacacs_plus_login() Begin isConsole() Begin
getAuthenticatedService(): Begin getAuthenticatedService(): nServiceToAuthenticate = 6
isConsole() nReturn 0 telnet tacacs_plus_login() sWhatService() tty = telnet
getRemoteIPAddress(): Begin getRemoteIPAddress(): pRemoteAddress = 172.18.124.193
tacacs_plus_login() getRemoteIPAddress sHostIp 172.18.124.193 tacacs_malloc() Begin 164
tacacs_malloc() PSkmalloc ptr getUserStruct() malloc_named ustr tacacs_plus_login()
allocated memory for ustruct aaa_update_user() Begin debug_authen_svc() Begin
aaa_update_user(): user='admin' ruser='system' port='telnet' rem_addr='172.18.124.193'
authen_type=1 tacacs_plus_login() updated user getNumTacacsLoginAttempts(): Begin
getNumTacacsLoginAttempts(): ulRetransmit = 2 ##### tacacs_plus_login() num_tries 1
aaa_start_login() Begin debug_start_login() Begin debug_start_login()/AUTHEN/START (0):
port='telnet' list='(null)' action=LOGIN service=LOGIN aaa_randomize_id() Begin
tacacs_plus_start_login() Begin tacacs_parse_server() Begin user_str admin
getTacacsDirectRequestEnable(): Begin getTacacsDirectRequestEnable(): cDirectRequestEnable =
0 printIpAddr() Begin printIpAddr() 0.0.0.0 tacacs_plus_start_login() server.ip_addr 0.0.0.0
server.type 0 server.length 0 choose_version() Begin create_authen_start() Begin
create_authen_start() len 45 tacacs_malloc() Begin 45 tacacs_malloc() PSkmalloc ptr
```

```
create_authen_start() malloc_named tac_pak fill_tacacs_plus_hdr() Begin encrypt 1
fill_tacacs_plus_hdr() len 33, tac_pak->length 33 ##### fill_tacacs_plus_hdr() tac_pak-
>encrypted 1 ##### fill_tacacs_plus_hdr() TEST nTestLen 33 create_authen_start() len 33,
tac_pak->length 33 create_authen_start() u->priv_lvl 15 start->priv_lvl 15
create_authen_start() start->action 1 create_authen_start() start->authen_type 1
create_authen_start() start->service 1 create_authen_start() user_len 5
create_authen_start() port_len 6 create_authen_start() addr_len 14 create_authen_start()
out_len 33 tacacs_plus_start_login() TACACS+: send AUTHEN/START packet ver=192 id=1541646967
tacacs_plus_start_login() login to TACACS+ server: printIpAddress() Begin printIpAddress() 0.0.0.0
tacacs_plus_get_conn() Begin server(0) printIpAddress() Begin printIpAddress() 0.0.0.0
tacacs_plus_get_conn() **pSocketHandleIndex 89434348 tacacs_plus_get_conn() Look at server
in the TACACS+ server list tacacs_plus_get_conn() TACACS+: This is a loop through server
list tacacs_plus_openconn() Begin printIpAddress() Begin printIpAddress() 172.18.124.114
open_handle() Begin tacacs_plus_socket() Begin tacacs_plus_socket Socket: return nSocket 784
nSockFdTbl[28] = 784 printIpAddress() Begin printIpAddress() 172.18.124.114 open_handle() TACACS+:
Opening TCP/IP connection to 172.18.124.114 open_handle() nSockFdTbl[28]= 784
setCurrentServer() Begin SaveCurrentServer->ip_addr 172.18.124.114
IncrementTacacsStatPerServerRequest(): Begin ##### IncrementTacacsStatPerServerRequest
Server->ip_addr 1920733868 tacacs_root.ulTacacsServerAddr open_handle() socket(28) 784
tacacs_plus_connect() Begin tacacs_plus_connect() socket(28) 784 tacacs_plus_connect() End
open_handle() is connected open_handle() *connection_handle 28 open_handle()
**pSocketHandleIndex 28 tacacs_plus_openconn() **pSocketHandleIndex 28 get_server() Begin
tacacs_plus_openconn() server->opens++ tacacs_plus_get_conn() **pSocketHandleIndex 28
tacacs_plus_get_conn() oldServerCount: 0, count:0 tacacs_plus_start_login() **pHandleIndex
28 tacacs_plus_send_receive() Begin tacacs_plus_proc_send_receive() Begin
tacacs_plus_proc_send_receive() length 33 copy_tac_plus_packet() Begin tacacs_malloc() Begin
45 tacacs_malloc() Pskmalloc ptr copy_tac_plus_packet() malloc_named copy
tacacs_plus_encrypt() Begin getTacacsKey(): Begin getTacacsKey(): sKey =
tacacs_plus_encrypt() key tacacs_plus_encrypt() sizeof(tacacs_plus_pkt_hdr) 12
tacacs_plus_encrypt() sizeof(uchar) 1 tacacs_plus_encrypt() tac_pak->encrypted 1
tacacs_plus_encrypt() tac_pak->encrypted = TAC_PLUS_CLEAR && key is empty
tacacs_plus_proc_send_receive() out_pak->encrypted 1 tacacs_plus_proc_send_receive()
out_pak->encrypted 1 tacacs_plus_proc_send_receive() Pskfree dump_pak
tacacs_plus_proc_send_receive() ntohl(out_pak->length) 33 dump_start_session() Begin
ntohl(out_pak->length) 33 getTacacsKey(): Begin getTacacsKey(): sKey = 0xc0 0x1 0x1 0x1 0x77
0xaa 0xe3 0x5b 0x0 0x0 0x0 0x21 0x1 0xf 0x1 0x1 0x5 0x6 0xe 0x0 0x61 0x64 0x6d
encrypt_md5_xor() Begin encrypt_md5_xor() no key dump_summarise_incoming_packet_type() Begin
Read AUTHEN/START size=45 dump_nas_pak() Begin dump_header() Begin PACKET: key= version 192
(0xc0), type 1, seq no 1, encrypted 1 session_id 2007688027 (0x77aae35b), Data length 33
(0x21) End header type=AUTHEN/START, priv_lvl = 15action=login authen_type=ascii
service=login user_len=5 port_len=6 (0x6), rem_addr_len=14 (0xe) data_len=0 User: port:
rem_addr: data: End packet dump_start_session() Pskfree test getTacacsTimeout(): Begin
getTacacsTimeout(): ulTimeout = 5 tacacs_plus_sockwrite() Begin
tacacs_plus_proc_send_receive() Pskfree out_pak getTacacsTimeout(): Begin
getTacacsTimeout(): ulTimeout = 5 sockread() Begin tacacs_plus_proc_send_receive() read
tacacs_malloc() Begin 18 tacacs_malloc() Pskmalloc ptr tacacs_plus_proc_send_receive()
malloc_named *in tacacs_plus_proc_send_receive() allocated memory getTacacsTimeout(): Begin
getTacacsTimeout(): ulTimeout = 5 sockread() Begin tacacs_plus_proc_send_receive() OK
tacacs_plus_decrypt() Begin getTacacsKey(): Begin getTacacsKey(): sKey =
tacacs_plus_decrypt() key tacacs_plus_decrypt() tac_pak->encrypted = TAC_PLUS_CLEAR && key
is empty authen_resp_sanity_check() Begin tacacs_plus_hdr_sanity_check() Begin
authen_debug_response() Begin authen_debug_response() TACACS+: ver=192 id=1541646967
received AUTHEN status = FAIL tacacs_plus_start_login() Pskfree out_tac_pak
unload_authen_resp() Begin tacacs_plus_start_login() Pskfree in_tac_pak
debug_authen_status() Begin TACACS+/AUTHEN (2007688027): status = FAIL tacacs_plus_login()
Authentication failed. tacacs_plus_login() labell aaa_cleanup_login() Begin
aaa_close_connection() Begin tacacs_plus_closeconn() Begin get_server() Begin close_handle()
Begin close_handle() nHandleIndex 28 nSockFdTbl[**handle] 784 aaa_set_password() Begin
aaa_free_user() Begin debug_authen_svc() Begin aaa_close_connection() Begin TACACS+/AUTHEN:
free user admin system telnet 172.18.124.193 authen_type=ASCII service=LOGIN priv_lv
aaa_free_user() Pskfree ustr ##### tacacs_plus_login() num_tries 2 aaa_start_login() Begin
debug_start_login() Begin debug_start_login()/AUTHEN/START (0): port='unknown' list='(null)'
action=LOGIN service=LOGIN TACACS+/AUTHEN/START aaa_start_login() (0): ERROR (no ustruct)
tacacs_plus_login() TACACS+: aaa_start aaa_free_user() Begin tacacs_plus_login()
```

```
try_local_login AUTHENTICATION_INTERNAL_ERROR IncrementTacacsStatDenyAccess(): Begin
localAuthentication(): Begin localAuthentication() usrName admin localAuthentication()
passwd system localAuthentication() pUId 89435294 localAuthentication() telnet_access
localAuthentication() rc == TRUE AuthenticationIntersection(): bTacacsLogin 0
IncrementLocalLoginStat(): Begin getLocalConfigAuthEnable(): Begin
getLocalConfigAuthEnable(): uiState = 1 getTacacsConfigAuthEnable(): Begin
getTacacsConfigAuthEnable(): uiState = 1 getTacacsConfigAuthPrimary(): Begin
getTacacsConfigAuthPrimary(): uiState = 0 localAuthentication(): Begin localAuthentication()
usrName admin localAuthentication() passwd system localAuthentication() pUId 89435294
localAuthentication() telnet_access localAuthentication() rc == TRUE
AuthenticationIntersection(): bTacacsConfig 0 AuthenticationIntersection():= Local Database
Authentication == IncrementLocalConfigStat(): Begin AuthenticationIntersection(): user has
been found AuthenticationIntersection(): bTacacsLogin pUId 89435294
AuthenticationIntersection(): GOT ACCESS capab 0 Admin 0 Ftp 0 Http 0 Telnet 0
authenticateUser() AUTHENTICATION IS OK authenticateUser() AUTHENTICATION #2
```

Informações Relacionadas

- [Release Note para o Software Cisco Cache, liberação 2.3.0 - Cache de FTP](#)
- [Produtos & serviços do motor do esconderijo do Cisco 500 Series](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)