

配置从 VPN Client 3.5 Solaris 到 VPN 3000 集中器的 IPsec

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[配置](#)

[网络图](#)

[配置](#)

[验证](#)

[连接到 VPN 集中器](#)

[故障排除](#)

[调试](#)

[相关信息](#)

简介

本文说明如何配置Solaris 2.6的VPN Client 3.5能连接到VPN 3000集中器。

先决条件

要求

在尝试此配置前，请保证您满足以下前提条件。

- 此示例使用预先共享密钥组验证。用户名和密码(扩展认证)根据VPN集中器的内部数据库核对。
- VPN客户端必须正确地安装。参考[安装Solaris的VPN客户端](#)关于在安装的详细信息。
- IP连通性必须存在VPN客户端和VPN集中器的公共接口之间。必须适当地设置子网掩码和网关信息。

使用的组件

本文档中的信息基于以下软件和硬件版本。

- Solaris 2.6版本3.5的Cisco VPN Client，3DES镜像。(镜像名称：vpnclient-solaris5.6-3.5.Rel-k9.tar.Z)

- Cisco VPN集中器类型：3005引导代码：Altiga Networks/VPN集中器版本2.2.int_9简19
2000年05:36:41软件：Cisco系统， Inc./VPN 3000集中器系列版本3.1.Rel八月06 2001年
13:47:37

本文档中的信息都是基于特定实验室环境中的设备创建的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您是在真实网络上操作，请确保您在使用任何命令前已经了解其潜在影响。

规则

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

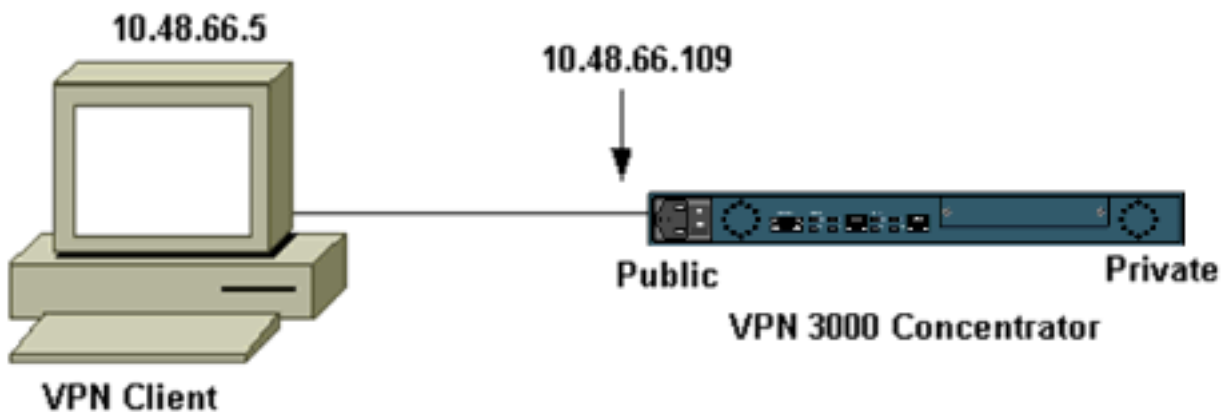
配置

本部分提供有关如何配置本文档所述功能的信息。

注意：要查找本文档所用命令的其他信息，请使用[命令查找工具](#)（[仅限注册用户](#)）。

网络图

本文档使用下图所示的网络设置。



注意：为了使VPN Client 3.5连接对VPN集中器，您需要版本3.0或稍后集中器。

配置

创建连接的用户配置文件

用户配置文件在/etc/CiscoSystemsVPNClient/Profiles目录存储。这些文本文件有一.pcf分机并且包含必要的参数建立了对VPN集中器的连接。您能创建一个新的文件或编辑一存在的一个。您应该查找示例配置文件，sample.pcf，在配置文件目录。此示例跟随使用该文件创建名为toCORPORATE.pcf的新配置文件。

```
[cholera]: ~ > cd /etc/CiscoSystemsVPNClient/Profiles/  
[cholera]: /etc/CiscoSystemsVPNClient/Profiles > cp sample.pcf toCORPORATE.pcf
```

您能使用您偏爱的文本编辑编辑此新的文件，toCORPORATE.pcf。在所有修改前，文件看起来象以下。

注意：如果要使用在网络地址转换(NAT)的IPSec，EnableNat条目在下面配置里必须说"EnableNat=1"而不是"EnableNat=0."

```
[main]
Description=sample user profile
Host=10.7.44.1
AuthType=1
GroupName=monkeys
EnableISPConnect=0
ISPConnectType=0
ISPConnect=
ISPCommand=
Username=chimchim
SaveUserPassword=0
EnableBackup=0
BackupServer=
EnableNat=0
CertStore=0
CertName=
CertPath=
CertSubjectName=
CertSerialHash=00000000000000000000000000000000
DHGroup=2
ForceKeepAlives=0
```

参考用户配置文件关键字的说明的[toUser配置文件](#)。

成功配置您的配置文件，您需要认识，作为最低，您的同等值对于以下信息。

- VPN集中器(10.48.66.109)的主机名或公网IP地址
- 组名(RemoteClient)
- 组密码(cisco)
- 用户名(Joe)

编辑有您的信息的文件，以便类似于以下。

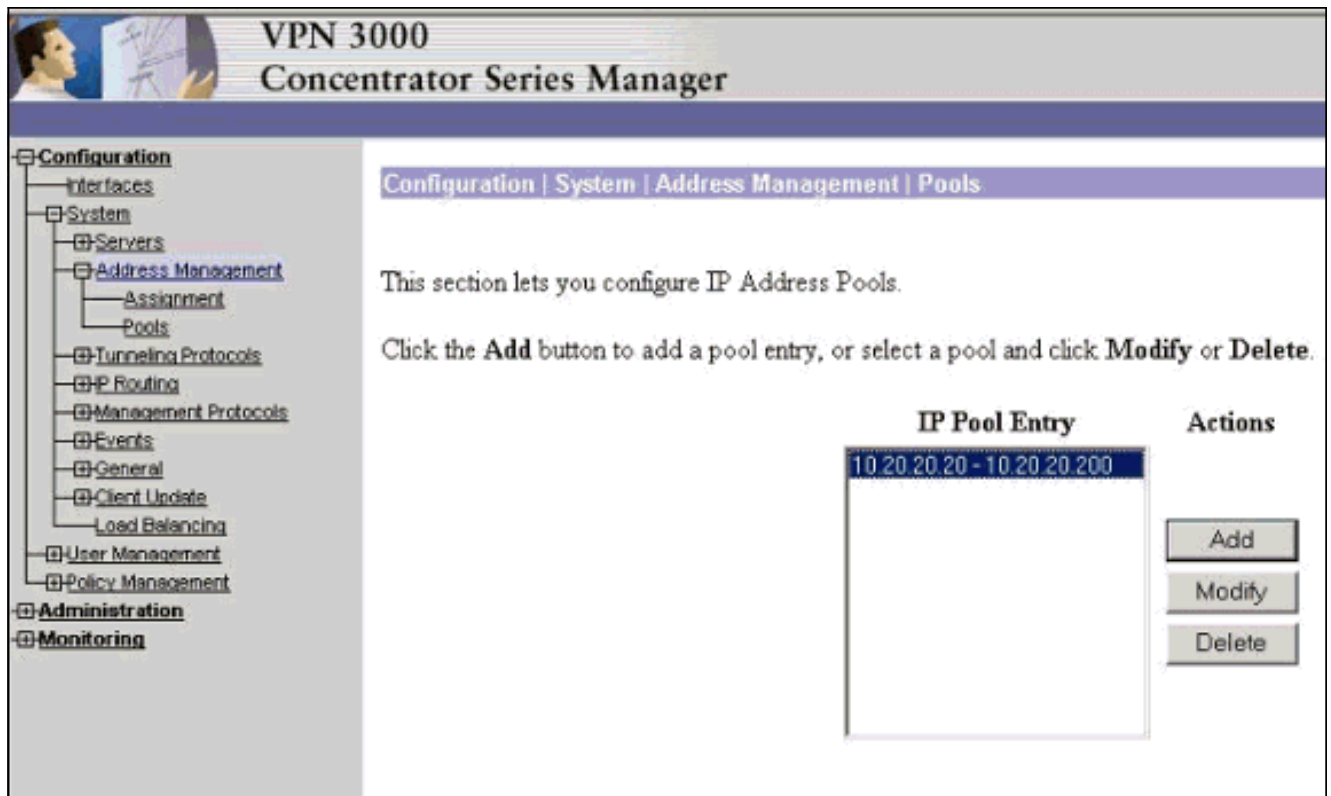
```
[main]
Description=Connection to the corporate
Host=10.48.66.109 AuthType=1 GroupName=RemoteClient GroupPwd=cisco EnableISPConnect=0
ISPConnectType=0 ISPConnect= ISPCommand= Username=joe SaveUserPassword=0 EnableBackup=0
BackupServer= EnableNat=0 CertStore=0 CertName= CertPath= CertSubjectName=
CertSerialHash=00000000000000000000000000000000 DHGroup=2 ForceKeepAlives=0
```

[配置VPN集中器](#)

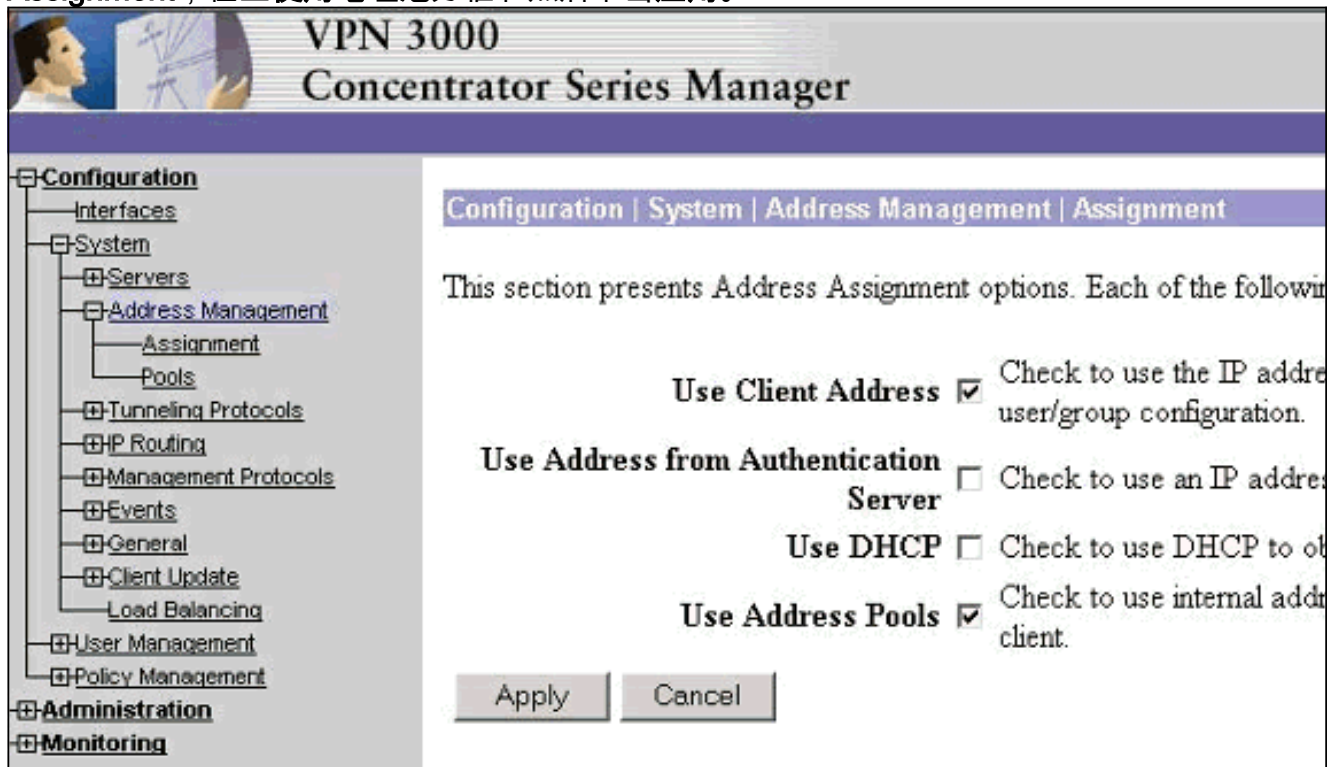
请使用以下步骤配置VPN集中器。

注意： 由于空间限制，屏幕截图只显示部分或相关区域。

1. 分配地址池。分配一可用的IP地址范围，点一个浏览器VPN集中器的内部接口并且选择 **Configuration > System > Address Management > Pools**。单击 **Add**。指定与在网络内部的任何其它设备不相冲突的IP地址范围。



2. 要通知VPN集中器使用池，请选择Configuration > System > Address Management > Assignment，检查使用地址池方框和然后单击应用。



3. 添加一组和一个密码。选择Configuration > User Management > Groups，然后单击添加组。输入正确信息，然后单击添加提交信息。此示例以“cisco密码使用一组名为“RemoteClient””。

Configuration | User Management | Groups | Add

This section lets you add a group. Check the **Inherit?** box to set a field that you want to default to the base group value to override base group values.

Identity General IPSec Client FW PPTP/L2TP

Identity Parameters		
Attribute	Value	Description
Group Name	RemoteClient	Enter a unique name for the group.
Password	*****	Enter the password for the group.
Verify	*****	Verify the group's password.
Type	Internal <input type="checkbox"/>	External groups are configured on an external authentication server and are configured on the VPN 3000 Concentrator Series's Internal Data

Add Cancel

4. 在组的IPSec选项，验证验证设置对内部。

Configuration | User Management | Groups | Modify RemoteClient

Check the **Inherit?** box to set a field that you want to default to the base group value to override base group values.

Identity General **IPSec** Client FW PPTP/L2TP

IPSec Parameters		
Attribute	Value	Inherit?
IPSec SA	ESP-3DES-MD5	<input checked="" type="checkbox"/>
IKE Peer Identity Validation	If supported by certificate	<input checked="" type="checkbox"/>
IKE Keepalives	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Reauthentication on Rekey	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Tunnel Type	Remote Access	<input checked="" type="checkbox"/>

Remote Access Parameter		
Group Lock	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Authentication	Internal	<input checked="" type="checkbox"/>

5. 在组的常规选项卡，请验证IPSec选择作为隧道协议。

General Parameters			
Attribute	Value	Inherit?	
Access Hours	-No Restrictions-	<input checked="" type="checkbox"/>	Select the
Simultaneous Logins	3	<input checked="" type="checkbox"/>	Enter the t
Minimum Password Length	8	<input checked="" type="checkbox"/>	Enter the t
Allow Alphabetic-Only Passwords	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Enter whe be added
Idle Timeout	30	<input checked="" type="checkbox"/>	(minutes) I
Maximum Connect Time	0	<input checked="" type="checkbox"/>	(minutes) I
Filter	-None-	<input checked="" type="checkbox"/>	Enter the f
Primary DNS		<input checked="" type="checkbox"/>	Enter the I
Secondary DNS		<input checked="" type="checkbox"/>	Enter the I
Primary WINS		<input checked="" type="checkbox"/>	Enter the I
Secondary WINS		<input checked="" type="checkbox"/>	Enter the I
Tunneling Protocols	<input type="checkbox"/> PPTP <input type="checkbox"/> L2TP <input checked="" type="checkbox"/> IPsec <input type="checkbox"/> L2TP over IPsec	<input type="checkbox"/>	Select the
			Check to

6. 添加VPN集中器的用户，选择Configuration > User Management > Users，然后单击添加。

- [-] Configuration
- [-] Interfaces
- [-] System
- [-] User Management
 - [-] Base Group
 - [-] Groups
 - [-] Users
- [-] Policy Management
- [-] Administration
- [-] Monitoring

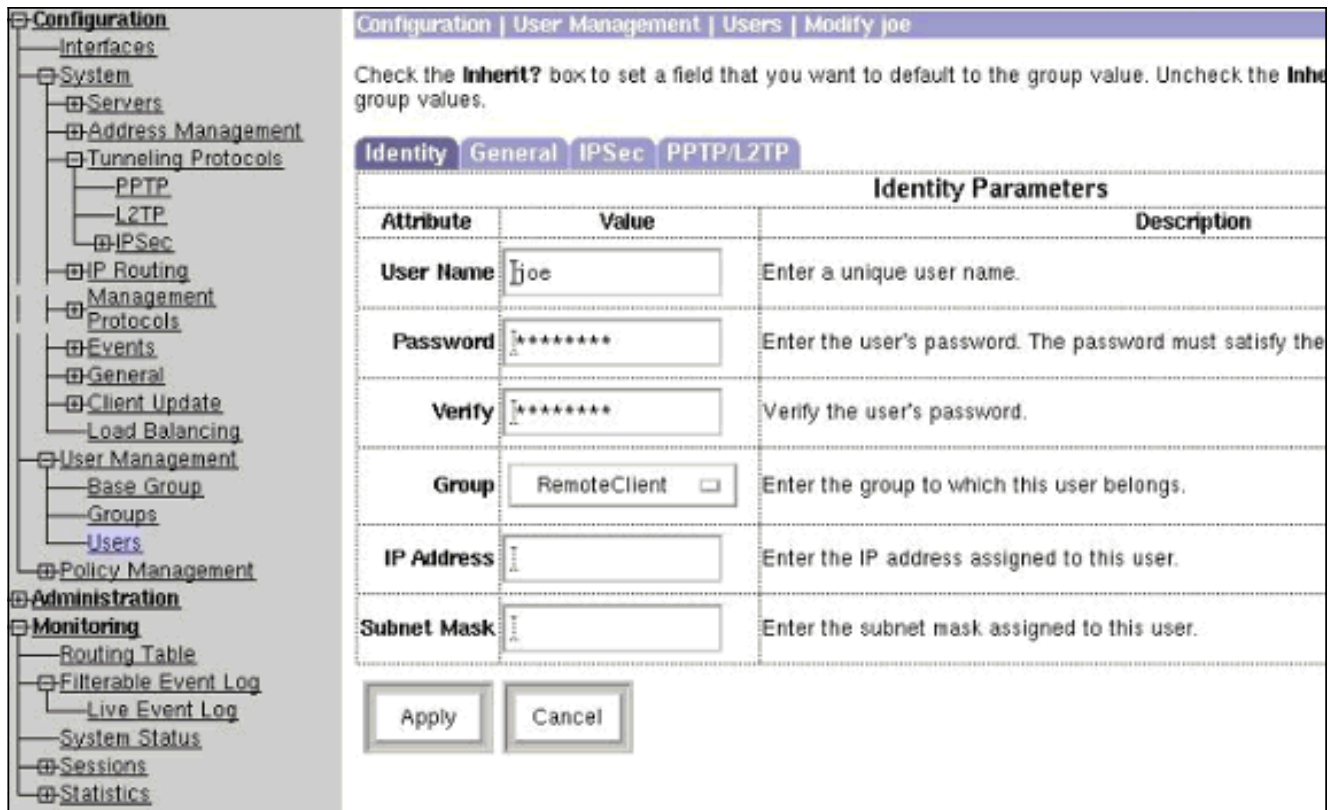
Configuration | User Management | Users

This section lets you configure users.

Click the **Add** button to add a user, or select a user and click **Modify** or **Delete**.

Current Users	Actions
Bredford-3002 itmcs-800	<input type="button" value="Add"/> <input type="button" value="Modify"/> <input type="button" value="Delete"/>

7. 输入组的正确信息，然后单击应用提交信息。



验证

连接到 VPN 集中器

既然VPN客户端和集中器配置，新配置文件应该工作连接到VPN集中器。

```
[cholera]: /etc/CiscoSystemsVPNClient > vpnclient connect toCORPORATE Cisco Systems VPN
Client Version 3.5 (Rel) Copyright (C) 1998-2001 Cisco Systems, Inc. All Rights Reserved. Client
Type(s): Solaris Running on: SunOS 5.6 Generic_105181-11 sun4u Initializing the IPsec link.
Contacting the security gateway at 10.48.66.109 Authenticating user. User Authentication for
toCORPORATE... Enter Username and Password. Username [Joe]: Password []: Contacting the security
gateway at 10.48.66.109 Your link is secure. IPsec tunnel information. Client address:
10.20.20.20 Server address: 10.48.66.109 Encryption: 168-bit 3-DES Authentication: HMAC-MD5 IP
Compression: None NAT passthrough is inactive. Local LAN Access is disabled. ^Z Suspended
[cholera]: /etc/CiscoSystemsVPNClient > bg [1] vpnclient connect toCORPORATE & (The process is
made to run as background process) [cholera]: /etc/CiscoSystemsVPNClient > vpnclient disconnect
Cisco Systems VPN Client Version 3.5 (Rel) Copyright (C) 1998-2001 Cisco Systems, Inc. All
Rights Reserved. Client Type(s): Solaris Running on: SunOS 5.6 Generic_105181-11 sun4u Your
IPsec link has been disconnected. Disconnecting the IPSEC link. [cholera]:
/etc/CiscoSystemsVPNClient > [1] Exit -56 vpnclient connect toCORPORATE [cholera]:
/etc/CiscoSystemsVPNClient >
```

故障排除

本部分提供的信息可用于对配置进行故障排除。

调试

对关闭调试，请使用ipseclog命令。示例如下所示。

```
[cholera]: /etc/CiscoSystemsVPNClient > ipseclog /tmp/clientlog
```

在客户端的调试，当连接对集中器时

```
[cholera]: /etc/CiscoSystemsVPNClient > cat /tmp/clientlog 1 17:08:49.821 01/25/2002 Sev=Info/4
CLI/0x43900002 Started vpnclient: Cisco Systems VPN Client Version 3.5 (Rel) Copyright (C) 1998-
2001 Cisco Systems, Inc. All Rights Reserved. Client Type(s): Solaris Running on: SunOS 5.6
Generic_105181-11 sun4u 2 17:08:49.855 01/25/2002 Sev=Info/4 CVPND/0x4340000F Started cvpnd:
Cisco Systems VPN Client Version 3.5 (Rel) Copyright (C) 1998-2001 Cisco Systems, Inc. All
Rights Reserved. Client Type(s): Solaris Running on: SunOS 5.6 Generic_105181-11 sun4u 3
17:08:49.857 01/25/2002 Sev=Info/4 IPSEC/0x43700013 Delete internal key with SPI=0xb0f0d0c0 4
17:08:49.857 01/25/2002 Sev=Info/4 IPSEC/0x4370000C Key deleted by SPI 0xb0f0d0c0 5 17:08:49.858
01/25/2002 Sev=Info/4 IPSEC/0x43700013 Delete internal key with SPI=0x637377d3 6 17:08:49.858
01/25/2002 Sev=Info/4 IPSEC/0x4370000C Key deleted by SPI 0x637377d3 7 17:08:49.859 01/25/2002
Sev=Info/4 IPSEC/0x43700013 Delete internal key with SPI=0x9d4d2b9d 8 17:08:49.859 01/25/2002
Sev=Info/4 IPSEC/0x4370000C Key deleted by SPI 0x9d4d2b9d 9 17:08:49.859 01/25/2002 Sev=Info/4
IPSEC/0x43700013 Delete internal key with SPI=0x5facd5bf 10 17:08:49.860 01/25/2002 Sev=Info/4
IPSEC/0x4370000C Key deleted by SPI 0x5facd5bf 11 17:08:49.860 01/25/2002 Sev=Info/4
IPSEC/0x43700009 IPsec driver already started 12 17:08:49.861 01/25/2002 Sev=Info/4
IPSEC/0x43700014 Deleted all keys 13 17:08:49.861 01/25/2002 Sev=Info/4 IPSEC/0x43700014 Deleted
all keys 14 17:08:49.862 01/25/2002 Sev=Info/4 IPSEC/0x43700009 IPsec driver already started 15
17:08:49.863 01/25/2002 Sev=Info/4 IPSEC/0x43700009 IPsec driver already started 16 17:08:49.863
01/25/2002 Sev=Info/4 IPSEC/0x43700014 Deleted all keys 17 17:08:50.873 01/25/2002 Sev=Info/4
CM/0x43100002 Begin connection process 18 17:08:50.883 01/25/2002 Sev=Info/4 CM/0x43100004
Establish secure connection using Ethernet 19 17:08:50.883 01/25/2002 Sev=Info/4 CM/0x43100026
Attempt connection with server "10.48.66.109" 20 17:08:50.883 01/25/2002 Sev=Info/6
IKE/0x4300003B Attempting to establish a connection with 10.48.66.109. 21 17:08:51.099
01/25/2002 Sev=Info/4 IKE/0x43000013 SENDING >>> ISAKMP OAK AG (SA, KE, NON, ID, VID, VID, VID)
to 10.48.66.109 22 17:08:51.099 01/25/2002 Sev=Info/4 IPSEC/0x43700009 IPsec driver already
started 23 17:08:51.100 01/25/2002 Sev=Info/4 IPSEC/0x43700014 Deleted all keys 24 17:08:51.400
01/25/2002 Sev=Info/5 IKE/0x4300002F Received ISAKMP packet: peer = 10.48.66.109 25 17:08:51.400
01/25/2002 Sev=Info/4 IKE/0x43000014 RECEIVING <<< ISAKMP OAK AG (SA, KE, NON, ID, HASH, VID,
VID, VID, VID) from 10.48.66.109 26 17:08:51.400 01/25/2002 Sev=Info/5 IKE/0x43000059 Vendor ID
payload = 12F5F28C457168A9702D9FE274CC0100 27 17:08:51.400 01/25/2002 Sev=Info/5 IKE/0x43000001
Peer is a Cisco-Unity compliant peer 28 17:08:51.400 01/25/2002 Sev=Info/5 IKE/0x43000059 Vendor ID
payload = 09002689DFD6B712 29 17:08:51.400 01/25/2002 Sev=Info/5 IKE/0x43000059 Vendor ID
payload = AFCAD71368A1F1C96B8696FC77570100 30 17:08:51.400 01/25/2002 Sev=Info/5 IKE/0x43000001
Peer supports DPD 31 17:08:51.400 01/25/2002 Sev=Info/5 IKE/0x43000059 Vendor ID payload =
1F07F70EAA6514D3B0FA96542A500301 32 17:08:51.505 01/25/2002 Sev=Info/4 IKE/0x43000013 SENDING
>>> ISAKMP OAK AG *(HASH, NOTIFY:STATUS_INITIAL_CONTACT) to 10.48.66.109 33 17:08:51.510
01/25/2002 Sev=Info/5 IKE/0x4300002F Received ISAKMP packet: peer = 10.48.66.109 34 17:08:51.511
01/25/2002 Sev=Info/4 IKE/0x43000014 RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from
10.48.66.109 35 17:08:51.511 01/25/2002 Sev=Info/4 CM/0x43100015 Launch xAuth application 36
17:08:56.333 01/25/2002 Sev=Info/4 CM/0x43100017 xAuth application returned 37 17:08:56.334
01/25/2002 Sev=Info/4 IKE/0x43000013 SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 10.48.66.109
38 17:08:56.636 01/25/2002 Sev=Info/5 IKE/0x4300002F Received ISAKMP packet: peer = 10.48.66.109
39 17:08:56.637 01/25/2002 Sev=Info/4 IKE/0x43000014 RECEIVING <<< ISAKMP OAK TRANS *(HASH,
ATTR) from 10.48.66.109 40 17:08:56.637 01/25/2002 Sev=Info/4 CM/0x4310000E Established Phase 1
SA. 1 Phase 1 SA in the system 41 17:08:56.639 01/25/2002 Sev=Info/4 IKE/0x43000013 SENDING >>>
ISAKMP OAK TRANS *(HASH, ATTR) to 10.48.66.109 42 17:08:56.639 01/25/2002 Sev=Info/4
IKE/0x43000013 SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 10.48.66.109 43 17:08:56.645
01/25/2002 Sev=Info/5 IKE/0x4300002F Received ISAKMP packet: peer = 10.48.66.109 44 17:08:56.646
01/25/2002 Sev=Info/4 IKE/0x43000014 RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from
10.48.66.109 45 17:08:56.646 01/25/2002 Sev=Info/5 IKE/0x43000010 MODE_CFG_REPLY: Attribute =
INTERNAL_IPV4_ADDRESS: , value = 10.20.20.20 46 17:08:56.646 01/25/2002 Sev=Info/5
IKE/0x4300000D MODE_CFG_REPLY: Attribute = MODECFG_UNITY_SAVEPWD: , value = 0x00000000 47
17:08:56.646 01/25/2002 Sev=Info/5 IKE/0x4300000D MODE_CFG_REPLY: Attribute = MODECFG_UNITY_PFS:
, value = 0x00000000 48 17:08:56.646 01/25/2002 Sev=Info/5 IKE/0x4300000E MODE_CFG_REPLY:
Attribute = APPLICATION_VERSION, value = Cisco Systems, Inc./VPN 3000 Concentrator Series
Version 3.1.Rel built by vmurphy on Aug 06 2001 13:47:37 49 17:08:56.648 01/25/2002 Sev=Info/4
CM/0x43100019 Mode Config data received 50 17:08:56.651 01/25/2002 Sev=Info/5 IKE/0x43000055
Received a key request from Driver for IP address 10.48.66.109, GW IP = 10.48.66.109 51
17:08:56.652 01/25/2002 Sev=Info/4 IKE/0x43000013 SENDING >>> ISAKMP OAK QM *(HASH, SA, NON, ID,
ID) to 10.48.66.109 52 17:08:56.653 01/25/2002 Sev=Info/5 IKE/0x43000055 Received a key request
from Driver for IP address 10.10.10.255, GW IP = 10.48.66.109 53 17:08:56.653 01/25/2002
```


Sev=Info/4 IKE/0x43000013 SENDING >>> ISAKMP OAK QM *(HASH, SA, NON, ID, ID) to 10.48.66.109 54
17:08:56.663 01/25/2002 Sev=Info/5 IKE/0x4300002F Received ISAKMP packet: peer = 10.48.66.109 55
17:08:56.663 01/25/2002 Sev=Info/4 IKE/0x43000014 RECEIVING <<< ISAKMP OAK INFO *(HASH,
NOTIFY:STATUS_RESP_LIFETIME) from 10.48.66.109 56 17:08:56.663 01/25/2002 Sev=Info/5
IKE/0x43000044 RESPONDER-LIFETIME notify has value of 86400 seconds 57 17:08:56.663 01/25/2002
Sev=Info/5 IKE/0x43000046 This SA has already been alive for 6 seconds, setting expiry to 86394
seconds from now 58 17:08:56.666 01/25/2002 Sev=Info/5 IKE/0x4300002F Received ISAKMP packet:
peer = 10.48.66.109 59 17:08:56.666 01/25/2002 Sev=Info/4 IKE/0x43000014 RECEIVING <<< ISAKMP
OAK QM *(HASH, SA, NON, ID, ID, NOTIFY:STATUS_RESP_LIFETIME) from 10.48.66.109 60 17:08:56.667
01/25/2002 Sev=Info/5 IKE/0x43000044 RESPONDER-LIFETIME notify has value of 28800 seconds 61
17:08:56.667 01/25/2002 Sev=Info/4 IKE/0x43000013 SENDING >>> ISAKMP OAK QM *(HASH) to
10.48.66.109 62 17:08:56.667 01/25/2002 Sev=Info/5 IKE/0x43000058 Loading IPsec SA (Message ID =
0x4CEF4B32 OUTBOUND SPI = 0x5EAD41F5 INBOUND SPI = 0xE66C759A) 63 17:08:56.668 01/25/2002
Sev=Info/5 IKE/0x43000025 Loaded OUTBOUND ESP SPI: 0x5EAD41F5 64 17:08:56.669 01/25/2002
Sev=Info/5 IKE/0x43000026 Loaded INBOUND ESP SPI: 0xE66C759A 65 17:08:56.669 01/25/2002
Sev=Info/4 CM/0x4310001A One secure connection established 66 17:08:56.674 01/25/2002 Sev=Info/5
IKE/0x4300002F Received ISAKMP packet: peer = 10.48.66.109 67 17:08:56.675 01/25/2002 Sev=Info/4
IKE/0x43000014 RECEIVING <<< ISAKMP OAK QM *(HASH, SA, NON, ID, ID, NOTIFY:STATUS_RESP_LIFETIME)
from 10.48.66.109 68 17:08:56.675 01/25/2002 Sev=Info/5 IKE/0x43000044 RESPONDER-LIFETIME notify
has value of 28800 seconds 69 17:08:56.675 01/25/2002 Sev=Info/4 IKE/0x43000013 SENDING >>>
ISAKMP OAK QM *(HASH) to 10.48.66.109 70 17:08:56.675 01/25/2002 Sev=Info/5 IKE/0x43000058
Loading IPsec SA (Message ID = 0x88E9321A OUTBOUND SPI = 0x333B4239 INBOUND SPI = 0x6B040746) 71
17:08:56.677 01/25/2002 Sev=Info/5 IKE/0x43000025 Loaded OUTBOUND ESP SPI: 0x333B4239 72
17:08:56.677 01/25/2002 Sev=Info/5 IKE/0x43000026 Loaded INBOUND ESP SPI: 0x6B040746 73
17:08:56.678 01/25/2002 Sev=Info/4 CM/0x43100022 Additional Phase 2 SA established. 74
17:08:57.752 01/25/2002 Sev=Info/4 IPSEC/0x43700014 Deleted all keys 75 17:08:57.752 01/25/2002
Sev=Info/4 IPSEC/0x43700010 Created a new key structure 76 17:08:57.752 01/25/2002 Sev=Info/4
IPSEC/0x4370000F Added key with SPI=0x5ead41f5 into key list 77 17:08:57.753 01/25/2002
Sev=Info/4 IPSEC/0x43700010 Created a new key structure 78 17:08:57.753 01/25/2002 Sev=Info/4
IPSEC/0x4370000F Added key with SPI=0xe66c759a into key list 79 17:08:57.754 01/25/2002
Sev=Info/4 IPSEC/0x43700010 Created a new key structure 80 17:08:57.754 01/25/2002 Sev=Info/4
IPSEC/0x4370000F Added key with SPI=0x333b4239 into key list 81 17:08:57.754 01/25/2002
Sev=Info/4 IPSEC/0x43700010 Created a new key structure 82 17:08:57.755 01/25/2002 Sev=Info/4
IPSEC/0x4370000F Added key with SPI=0x6b040746 into key list 83 17:09:13.752 01/25/2002
Sev=Info/6 IKE/0x4300003D Sending DPD request to 10.48.66.109, seq# = 2948297981 84 17:09:13.752
01/25/2002 Sev=Info/4 IKE/0x43000013 SENDING >>> ISAKMP OAK INFO *(HASH, NOTIFY:DPD_REQUEST) to
10.48.66.109 85 17:09:13.758 01/25/2002 Sev=Info/5 IKE/0x4300002F Received ISAKMP packet: peer =
10.48.66.109 86 17:09:13.758 01/25/2002 Sev=Info/4 IKE/0x43000014 RECEIVING <<< ISAKMP OAK INFO
*(HASH, NOTIFY:DPD_ACK) from 10.48.66.109 87 17:09:13.759 01/25/2002 Sev=Info/5 IKE/0x4300003F
Received DPD ACK from 10.48.66.109, seq# received = 2948297981, seq# expected = 2948297981 debug
on the client when disconnecting 88 17:09:16.366 01/25/2002 Sev=Info/4 CLI/0x43900002 Started
vpnclient: Cisco Systems VPN Client Version 3.5 (Rel) Copyright (C) 1998-2001 Cisco Systems,
Inc. All Rights Reserved. Client Type(s): Solaris Running on: SunOS 5.6 Generic_105181-11 sun4u
89 17:09:16.367 01/25/2002 Sev=Info/4 CM/0x4310000A Secure connections terminated 90
17:09:16.367 01/25/2002 Sev=Info/5 IKE/0x43000018 Deleting IPsec SA: (OUTBOUND SPI = 333B4239
INBOUND SPI = 6B040746) 91 17:09:16.368 01/25/2002 Sev=Info/4 IKE/0x43000013 SENDING >>> ISAKMP
OAK INFO *(HASH, DEL) to 10.48.66.109 92 17:09:16.369 01/25/2002 Sev=Info/5 IKE/0x43000018
Deleting IPsec SA: (OUTBOUND SPI = 5EAD41F5 INBOUND SPI = E66C759A) 93 17:09:16.369 01/25/2002
Sev=Info/4 IKE/0x43000013 SENDING >>> ISAKMP OAK INFO *(HASH, DEL) to 10.48.66.109 94
17:09:16.370 01/25/2002 Sev=Info/4 IKE/0x43000013 SENDING >>> ISAKMP OAK INFO *(HASH, DEL) to
10.48.66.109 95 17:09:16.371 01/25/2002 Sev=Info/4 CM/0x43100013 Phase 1 SA deleted cause by
DEL_REASON_RESET_SADB. 0 Phase 1 SA currently in the system 96 17:09:16.371 01/25/2002
Sev=Info/5 CM/0x43100029 Initializing CVPNDrv 97 17:09:16.371 01/25/2002 Sev=Info/6
CM/0x43100035 Tunnel to headend device 10.48.66.109 disconnected: duration: 0 days 0:0:20 98
17:09:16.375 01/25/2002 Sev=Info/5 CM/0x43100029 Initializing CVPNDrv 99 17:09:16.377 01/25/2002
Sev=Info/5 IKE/0x4300002F Received ISAKMP packet: peer = 10.48.66.109 100 17:09:16.377
01/25/2002 Sev=Warning/2 IKE/0x83000061 Attempted incoming connection from 10.48.66.109. Inbound
connections are not allowed. 101 17:09:17.372 01/25/2002 Sev=Info/4 IPSEC/0x43700013 Delete
internal key with SPI=0x6b040746 102 17:09:17.372 01/25/2002 Sev=Info/4 IPSEC/0x43700013 Delete
internal key with SPI=0x333b4239 103 17:09:17.373 01/25/2002 Sev=Info/4 IPSEC/0x43700013 Delete
internal key with SPI=0xe66c759a 104 17:09:17.373 01/25/2002 Sev=Info/4 IPSEC/0x43700013 Delete
internal key with SPI=0x5ead41f5 105 17:09:17.373 01/25/2002 Sev=Info/4 IPSEC/0x43700014 Deleted
all keys 106 17:09:17.374 01/25/2002 Sev=Info/4 IPSEC/0x43700009 IPsec driver already started
107 17:09:17.374 01/25/2002 Sev=Info/4 IPSEC/0x43700014 Deleted all keys 108 17:09:17.375

01/25/2002 Sev=Info/4 IPSEC/0x43700009 IPsec driver already started 109 17:09:17.375 01/25/2002
Sev=Info/4 IPSEC/0x43700014 Deleted all keys 110 17:09:17.375 01/25/2002 Sev=Info/4
IPSEC/0x43700009 IPsec driver already started 111 17:09:17.376 01/25/2002 Sev=Info/4
IPSEC/0x43700014 Deleted all keys

在VPN集中器的调试

如果有事件连接故障，请选择**Configuration > System > Events > Classes**打开以下调试。

- 验证-记录1-13的严重性
- IKE -记录1-6的严重性
- IPSEC-记录1-6的严重性

The screenshot shows the configuration interface for the 'Classes' page. On the left is a navigation tree with 'Events' expanded to 'Classes'. The main content area has a breadcrumb 'Configuration | System | Events | Classes' and a title bar. Below the breadcrumb, there is instructional text: 'This section lets you configure special handling of specific event classes. Click the **Add** button to add an event class, or select an event class and click **Mod**. [Click here to configure general event parameters.](#)'

Configured Event Classes	Actions
AUTH	<input type="button" value="Add"/> <input type="button" value="Modify"/> <input type="button" value="Delete"/>
IKE	
IPSEC	

您能通过选择**Monitoring > Event Log**查看日志。

相关信息

- [Cisco VPN 3000 系列集中器支持页](#)
- [Cisco VPN 3000 系列客户端支持页](#)
- [IPSec 支持页面](#)
- [技术支持 - Cisco Systems](#)