

Cos'è il VRRP?

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Convenzioni](#)

[In che modo VPN 3000 Concentrator implementa il protocollo VRRP?](#)

[Configurazione del VRRP](#)

[Sincronizzare le configurazioni](#)

[Informazioni correlate](#)

Introduzione

Il protocollo VRRP (Virtual Router Redundancy Protocol) elimina il singolo punto di errore nell'ambiente con routing statico predefinito. Il protocollo VRRP assegna dinamicamente il ruolo di router virtuale (un cluster di concentratori VPN serie 3000) a uno dei concentratori VPN di una LAN. Il concentratore VPN VRRP che controlla gli indirizzi IP associati a un router virtuale viene denominato primario e inoltra i pacchetti inviati a tali indirizzi IP. Quando il server primario non è più disponibile, il server primario viene sostituito da un server di backup VPN Concentrator.

Nota: consultare "Configurazione | Sistema | Instradamento IP | Redundancy" (Ridondanza) nella [Guida per l'utente di VPN 3000 Concentrator Series](#) o nella Guida in linea per tale sezione di VPN 3000 Concentrator Manager per informazioni complete sul VRRP e su come configurarlo.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Per la stesura del documento, è stato usato Cisco VPN serie 3000 Concentrator.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

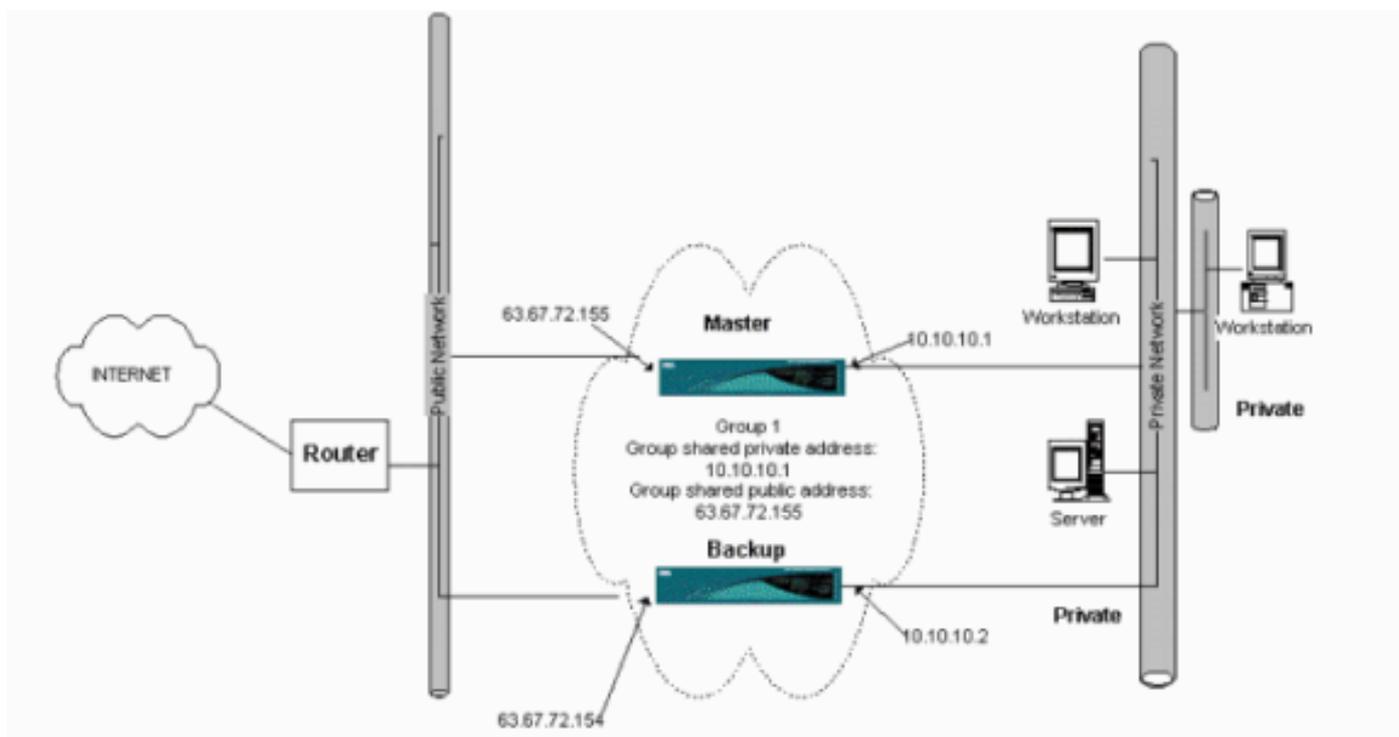
Per ulteriori informazioni sulle convenzioni usate, consultare il documento [Cisco sulle convenzioni nei suggerimenti tecnici](#).

In che modo VPN 3000 Concentrator implementa il protocollo VRRP?

1. I concentratori VPN ridondanti sono identificati per gruppo.
2. Per il gruppo viene scelto un solo database primario.
3. Uno o più concentratori VPN possono essere backup del primario del gruppo.
4. Il server primario comunica il proprio stato ai dispositivi di backup.
5. Se il database primario non comunica il proprio stato, il protocollo VRRP tenta di eseguire ogni backup in ordine di precedenza. Il backup che risponde assume il ruolo di primario. **Nota:** il protocollo VRRP abilita la ridondanza solo per le connessioni tunnel. Pertanto, se si verifica un failover VRRP, il backup resta in ascolto solo dei protocolli e del traffico del tunnel. Il ping di VPN Concentrator non funziona. I concentratori VPN partecipanti devono avere configurazioni identiche. Gli indirizzi virtuali configurati per il protocollo VRRP devono corrispondere a quelli configurati negli indirizzi di interfaccia del server primario.

Configurazione del VRRP

In questa configurazione, il protocollo VRRP è configurato sulle interfacce pubbliche e private. Il protocollo VRRP si applica solo alle configurazioni in cui due o più concentratori VPN operano in parallelo. Tutti i concentratori VPN partecipanti hanno impostazioni identiche per utenti, gruppi e da LAN a LAN. Se si verifica un errore nel server primario, il backup inizierà a gestire il traffico precedentemente gestito dal server primario. Questo passaggio avviene in 3-10 secondi. Mentre le connessioni client IPsec e PPTP (Point-to-Point Tunnel Protocol) vengono disconnesse durante questa transizione, gli utenti devono solo riconnettersi senza modificare l'indirizzo di destinazione del profilo di connessione. In una connessione LAN a LAN, la commutazione è perfetta.



In questa procedura viene illustrato come implementare questa configurazione di esempio.

Sui sistemi principale e di backup:

1. Selezionare **Configurazione > Sistema > Instradamento IP > Ridondanza**. Modificate solo questi parametri. Lasciare tutti gli altri parametri nello stato predefinito: Immettere una password (al massimo 8 caratteri) nel campo Password gruppo. Immettere gli indirizzi IP nel campo Group Shared Addresses (1 Private) of Primary and all Backup systems. Nell'esempio, l'indirizzo è 10.10.10.1. Immettere gli indirizzi IP nel gruppo Indirizzi condivisi (2 pubblici) del sistema principale e di tutti i sistemi di backup. Nell'esempio, l'indirizzo è 63.67.72.155.
2. Tornare alle finestre **Configurazione > Sistema > Instradamento IP > Ridondanza** su tutte le unità e selezionare **Abilita VRRP**. **Nota:** se in precedenza è stato configurato il bilanciamento del carico tra i due concentratori VPN e si sta configurando il protocollo VRRP su di essi, verificare di aver configurato il pool di indirizzi IP. Se si utilizza lo stesso pool IP utilizzato in precedenza, è necessario modificarlo. Questa operazione è necessaria perché il traffico proveniente da un pool IP in uno scenario di bilanciamento del carico viene indirizzato a uno solo dei concentratori VPN.

Sincronizzare le configurazioni

In questa procedura viene illustrato come sincronizzare la configurazione da primaria a secondaria eseguendo il bilanciamento del carico oppure da primaria a secondaria eseguendo il VRRP.

1. In Principale, selezionare **Amministrazione > Gestione file** e dalla riga CONFIG fare clic su **Visualizza**.

Administration | File Management Tuesday, 01 June 2004 15:09:20
Refresh

This screen lets you manage files on the VPN 3000 Concentrator. Select a file from the list and click the appropriate **Action**, or choose an action from the list below.

- [Swap Config File](#) -- swap the backup and boot configuration files.
- [TFTP Transfer](#) -- transfer files via TFTP.
- [File Upload](#) -- send a file via HTTP.
- [XML Export](#) -- export the configuration to an XML file.

Total: 12336KB, Used: 208KB, Free: 12128KB

Filename	Size (bytes)	Date/Time	Actions
CONFIG.BAK	35500	04/23/2004 13:49:24	[View] [Delete] [Copy]
CONFIG	33920	05/27/2004 19:22:46	[View] [Delete] [Copy]
SAVELOG.TXT	8018	05/27/2004 19:21:32	[View] [Delete] [Copy]

2. Quando il browser Web viene aperto con la configurazione, evidenziare e copiare la configurazione (cntrl-a, cntrl-c).
3. Incollare la configurazione in WordPad.
4. Selezionare **Modifica > Sostituisci** e immettere l'indirizzo IP dell'interfaccia pubblica di Principale nel campo Trova. Nel campo Sostituisci con immettere l'indirizzo IP che si desidera assegnare al database secondario o di backup. Eseguire la stessa operazione sull'IP privato e sull'interfaccia esterna, se configurata.

5. Salvate il file e assegnategli un nome che scegliete. Tuttavia, accertarsi di salvarlo come "documento di testo" (ad esempio, synconfig.txt). *Non è possibile* salvare come file con estensione doc (impostazione predefinita) e quindi modificare l'estensione in un secondo momento. Il motivo è che salva il formato e VPN Concentrator accetta solo testo.
6. Andare al database secondario e selezionare **Amministrazione > Gestione file > Caricamento file**.

The screenshot shows a web-based interface for file upload. At the top, there is a navigation bar with the text "Administration | File Management | File Upload". Below this, a paragraph of text reads: "This section lets you upload files to your VPN 3000 Concentrator. Type in the name of the destination file on the VPN 3000 Concentrator, and the name of the file on your workstation. **Please wait for the operation to finish.**"

There are two input fields: "File on the VPN 3000 Concentrator" and "Local File". The "Local File" field has a "Browse..." button next to it. At the bottom of the form, there are two buttons: "Upload" and "Cancel".

7. Immettere **config.bak** nel campo File su VPN 3000 Concentrator e individuare il file salvato sul PC (synconfig.txt). Quindi fare clic su **Upload**. VPN Concentrator lo carica e modifica automaticamente il file synconfig.txt in config.bak.
8. Selezionare **Amministrazione > Gestione file > Scambia file di configurazione** e fare clic su **OK** per avviare VPN Concentrator con il file di configurazione caricato.

The screenshot shows a dialog box titled "Administration | File Management | Swap Configuration Files". The text inside reads: "Every time the active configuration is saved, a backup is made of the config file. By clicking OK, you can swap the backup config file with the boot config file. To reload the boot configuration, you must then reboot the device. **You will be sent to the System Reboot screen after the config files have been swapped.**"

At the bottom of the dialog, there are two buttons: "OK" and "Cancel".

9. Dopo essere stati reindirizzati alla finestra Riavvio del sistema, lasciare le impostazioni predefinite e fare clic su **Applica**.

This section presents reboot options.



If you reboot, the browser may appear to hang as the device is rebooted.

- Action**
- Reboot
 - Shutdown without automatic reboot
 - Cancel a scheduled reboot/shutdown

- Configuration**
- Save the active configuration at time of reboot
 - Reboot without saving the active configuration
 - Reboot ignoring the configuration file

- When to Reboot/Shutdown**
- Now
 - Delayed by minutes
 - At time (24 hour clock)
 - Wait for sessions to terminate (don't allow new sessions)

Dopo l'accensione, avrà la stessa configurazione del database primario, ad eccezione degli indirizzi modificati in precedenza. **Nota:** non dimenticare di modificare i parametri nella finestra Bilanciamento del carico o Ridondanza (VRRP). Selezionare **Configurazione > Sistema > Instradamento IP > Ridondanza.**

Configure the Virtual Router Redundancy Protocol (VRRP) for your system. **All interfaces that you want to configure VRRP on should already be configured.** If you later configure an additional interface, you need to revisit this screen.

Enable VRRP <input type="checkbox"/>	Check to enable VRRP.
Group ID <input type="text" value="1"/>	Enter the Group ID for this set of redundant routers.
Group Password <input type="text"/>	Enter the shared group password, or leave blank for no password.
Role <input type="text" value="Master"/>	Select the Role for this system within the group.
Advertisement Interval <input type="text" value="1"/>	Enter the Advertisement interval (seconds).
Group Shared Addresses	
1 (Private) <input type="text" value="192.168.12.10"/>	
2 (Public) <input type="text" value="172.18.124.130"/>	
3 (External) <input type="text"/>	

Nota: in alternativa, selezionare **Configurazione > Sistema > Bilanciamento del carico.**

Configure Load Balancing. All devices in the cluster must share an identical **Cluster Configuration**. **Note: the public and private filters need to have the *VCA In* and *VCA Out* filter rules added. These filter rules may need to be modified if the *VPN Virtual Cluster UDP Port* is modified.**

Cluster Configuration

- VPN Virtual Cluster IP Address Enter the cluster's virtual IP address.
- VPN Virtual Cluster UDP Port Enter the cluster's UDP port.
- Encryption Check to enable IPsec encryption between cluster devices.
- IPsec Shared Secret Enter the IPsec Shared secret in the cluster.
- Verify Shared Secret Re-enter the IPsec Shared secret in the cluster.

Device Configuration

- Load Balancing Enable Check to enable load balancing for this device.
- Priority Enter the priority of this device. The range is from 1 to 10.
- NAT Assigned IP Address Enter the IP address that this device's IP address is translated to by NAT. Enter 0.0.0.0 if NAT is not being used, or the device is not behind a firewall using NAT.

Informazioni correlate

- [Cisco VPN serie 3000 Concentrator Support Page](#)
- [Negoziazione IPsec/protocolli IKE](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)