Configurazione RADIUS con switch gestiti Cisco serie 200/300 e Windows Server 2008

Obiettivo

Il servizio RADIUS (Remote Authorization Dial-in User Service) offre un metodo affidabile di autenticazione degli utenti per consentire l'accesso a un servizio di rete. I server RADIUS offrono pertanto un controllo di accesso centralizzato, in cui l'amministratore del server decide se un segmento specifico viene autenticato o meno utilizzando RADIUS. In questo articolo vengono illustrati i passaggi generali per stabilire un RADIUS in un ambiente client/server, in cui il client è rappresentato dallo switch gestito Cisco serie 200/300 e il server esegue Windows Server 2008 con RADIUS abilitato.

Dispositivi interessati

Cisco serie 200/300 Managed Switch

Procedura dettagliata

La configurazione viene eseguita in due parti. È necessario innanzitutto impostare lo switch come client RADIUS, quindi impostare il server correttamente per RADIUS.

Impostazione di RADIUS sullo switch

Passaggio 1. Nell'utility di configurazione della serie SG200/300, scegliere Sicurezza > RADIUS. Viene visualizzata la pagina RADIUS:

| RADIUS | | | | | | | | |
|------------------|------------------------|-----------|--|----------------------|------------------------|--------------|--------------|---------------|
| Use | Use Default Parameters | | | | | | | |
| IP V | /ersion | : | Version 6 Version 4 | | | | | |
| 🌣 Ret | ries: | | 3 | | (Range: 1 - | 10, Defaul | t 3) | |
| O Tim | neout fo | or Reply: | 3 | | sec. (Range | e: 1 - 30, D | efault: 3) | |
| Oea | ad Tim | e: | 0 min. (Range: 0 - 2000, Default: 0) | | | | | |
| Key | String | : | (0/128 ASCII Alphanumeric Characters Used) | | | | | |
| Apply Cancel | | | | | | | | |
| RADIUS Table | | | | | | | | |
| S | erver | Priority | Key String | Timeout for Reply | Authentication Port | Retries | Dead Time | Usage Type |
| 0 results found. | | | | | | | | |
| Ad | Add Edit Delete | | | | | | | |

Passaggio 2. Immettete le impostazioni RADIUS di default.

- Versione IP visualizza la versione IP supportata.
- Tentativi: in questo campo immettere il numero di richieste trasmesse al server RADIUS prima che si verifichi un errore.
- Timeout per la risposta: in questo campo immettere l'intervallo di tempo, in secondi, durante il quale lo switch attende una risposta dal server RADIUS prima di riprovare a eseguire una query.
- Tempo di inattività: in questo campo immettere il tempo di attesa in minuti dello switch prima di ignorare il server RADIUS.
- Stringa chiave: immettere in questo campo la stringa predefinita utilizzata per l'autenticazione e la crittografia tra lo switch e il server RADIUS. La chiave deve corrispondere a quella configurata nel server RADIUS.

Passaggio 3. Fare clic su Apply (Applica) per aggiornare la configurazione in esecuzione dello switch con le impostazioni RADIUS.



Passaggio 4. È necessario aggiungere il server RADIUS allo switch. Fare clic su Add. Viene visualizzata la pagina Aggiungi server RADIUS in una nuova finestra.

| Server Definition: | By IP address O By name |
|-------------------------|---|
| IP Version: | Version 6 Version 4 |
| IPv6 Address Type: | Global |
| Server IP Address/Name: | |
| Priority: | (Range: 0 - 65535) |
| Key String: | Use Default User Defined Default (0/128 ASCII Alphanumeric Characters Used) |
| Timeout for Reply: | Use Default User Defined Default sec. (Range: 1 - 30, Default: 3) |
| Authentication Port: | 1812 (Range: 0 - 65535, Default: 1812) |
| 🌣 Retries: | Use Default User Defined Default (Range: 1 - 10, Default: 3) |
| 🜣 Dead Time: | Use Default User Defined Default min. (Range: 0 - 2000, Default: 0) |
| Usage Type: | Login 802.1x All |
| Apply Close |) |

Passaggio 5. Immettere i valori nei campi per il server. Se si desidera utilizzare i valori predefiniti, selezionare Utilizza predefiniti nel campo desiderato.

- Definizione server In questo campo è possibile specificare la modalità di connessione al server, in base all'indirizzo IP o al nome del server.
- Versione IP: se il server verrà identificato dall'indirizzo IP, selezionare Indirizzo IPv4 o IPv6.
- Tipo di indirizzo IPv6: in questo campo viene visualizzato il tipo Globale dell'indirizzo IPv6.
- Indirizzo IP/Nome server: immettere in questo campo l'indirizzo IP o il nome di dominio del server RADIUS.
- Priorità: immettere la priorità del server. Se sono configurati più server, lo switch tenterà di connettersi a ciascun server in base a questo livello di priorità.
- Stringa chiave: immettere in questo campo la stringa predefinita utilizzata per l'autenticazione e la crittografia tra lo switch e il server RADIUS. La chiave deve corrispondere a quella configurata nel server RADIUS.
- Timeout per la risposta: in questo campo immettere l'intervallo di tempo, in secondi, durante il quale lo switch attende una risposta dal server RADIUS prima di riprovare a eseguire una query.
- Porta di autenticazione: in questo campo, immettere il numero di porta UDP impostato per il

server RADIUS per le richieste di autenticazione.

- Tentativi: in questo campo immettere il numero di richieste trasmesse al server RADIUS prima che si verifichi un errore.
- Tempo di inattività: in questo campo immettere il tempo di attesa in minuti dello switch prima di ignorare il server RADIUS.
- Tipo di utilizzo: immettere in questo campo il tipo di autenticazione del server RADIUS. Sono disponibili tre opzioni:

- Accesso: il server RADIUS autentica gli utenti che desiderano amministrare lo switch.

- 802.1X: il server RADIUS viene utilizzato per l'autenticazione 802.1X.

- All - Il server RADIUS viene utilizzato per le autenticazioni di accesso e 802.1X.

Passaggio 6. Fare clic su Apply (Applica) per aggiungere la definizione del server alla configurazione in esecuzione dello switch.

Configurazione di Windows Server 2008 per RADIUS

Passaggio 1. Nel computer Windows Server 2008, scegliere Start > Strumenti di amministrazione > Server dei criteri di rete. Viene visualizzata la finestra Server dei criteri di rete:



Passaggio 2. Per abilitare il server RADIUS per un segmento specifico della rete, è necessario creare un nuovo criterio di rete. Per creare un nuovo criterio di rete, scegliere Criteri > Criterio di rete, quindi fare clic con il pulsante destro del mouse e selezionare Nuovo. Viene visualizzata la finestra Nuovo criterio di rete:

| 🛸 Network Policy Server | |
|--|--|
| File Action View Help | |
| 🗢 🔿 🔰 📅 🔽 🖬 | |
| NPS (Local) RADIUS Clients and Servers Policies Connection Request Policies | Network policies allow you to designate who is authorized to connect to the network and the circumstances under which can or cannot connect. |
| Network Policies | Policy Name |
| Health Policies Network Access Pr Export List | Connections to Microsoft Routing and Remote Access server |
| Accounting View | |
| Refresh | |
| Help | |
| | Connections to other access servers |
| | • |
| | |

Passaggio 3. Nel campo Nome criterio immettere il nome del nuovo criterio. Fare clic su Next (Avanti).

| New Network P | olicy |
|---|---|
| | Specify Network Policy Name and Connection Type You can specify a name for your network policy and the type of connections to which the policy i |
| Policy name SG200/300 S Network conner Select the type type or Vendor Type of ner Unspecifie 0 Vendor specifie 10 | eries ection method e of network access server that sends the connection request to NPS. You can select either the network specific. twork access server: ed ecfic: |
| | Previous Next Finish |

Passaggio 4. È necessario specificare le condizioni di questo criterio. Sono necessarie due condizioni: il segmento di utenti a cui verrà implementato il server RADIUS e il metodo utilizzato per connettersi a questo segmento. Fare clic su Aggiungi per aggiungere queste condizioni.

| New Network P | olicy | | | | | | |
|----------------|--|-------|--|----------|---|------|--------|
| | Specify Conditions Specify the conditions that determine whether this network policy is evaluated for a connection of one condition is required. | | | | | | |
| Conditions: | | | | | | | |
| Condition | ı | Value | | | | | |
| | | | | | | | |
| Condition desc | ription: | | | | _ | | |
| | | | | | | Add | Edit |
| | | | | Previous | | Next | Finish |

Passaggio 5. In Gruppi sono disponibili tre opzioni: Gruppi di Windows, Gruppi di computer e Gruppi di utenti. Scegliere il gruppo in base all'impostazione della rete e fare clic su Aggiungi. Viene visualizzata una nuova finestra in base al gruppo selezionato. Fare clic su Aggiungi gruppi.

| s | elect co | ondition |
|---|----------|--|
| | Select a | condition, and then click Add. |
| | Group | S |
| | 1 | Windows Groups The Windows Groups condition specifies that the connecting user or computer must belong to one of the s |
| | 1 | Machine Groups The Machine Groups condition specifies that the connecting computer must belong to one of the selected |
| | 88 | User Groups The User Groups condition specifies that the connecting user must belong to one of the selected groups. |
| | HCAP | |
| | | Location Groups The HCAP Location Groups condition specifies the Host Credential Authorization Protocol (HCAP) locatio required to match this policy. The HCAP protocol is used for communication between NPS and some third network access servers (NASs). See your NAS documentation before using this condition. |
| | 00 | HCAP User Groups |
| | | Add Cancel |

Passaggio 6. Selezionare il tipo di oggetto, la posizione e immettere il nome dell'oggetto. Fare clic su Ok, quindi su Ok. Fare clic su Aggiungi per aggiungere la condizione successiva.

| Select Group | | ?× |
|---|----|--------------|
| Select this object type: | | |
| Group | | Object Types |
| From this location: | | |
| Radius.test | | Locations |
| Enter the object name to select (examples): | | |
| Fest Group | | Check Names |
| Advanced | ОК | Cancel |

Passaggio 7. In Client RADIUS, selezionare Indirizzo IPv4 come metodo per connettere il server ai client RADIUS, che in questo caso saranno l'indirizzo IP dello switch. Fare clic su Add.

| Select condition |
|--|
| Select a condition, and then click Add. |
| RADIUS Client |
| Calling Station ID The Calling Station ID condition specifies the network access server telephone number dialed by the ac |
| Client Friendly Name The Client Friendly Name condition specifies the name of the RADIUS client that forwarded the connect |
| Client IPv4 Address The Client IP Address condition specifies the IP address of the RADIUS client that forwarded the conner to NPS. |
| Client IPv6 Address The Client IPv6 Address condition specifies the IPv6 address of the RADIUS client that forwarded the c request to NPS. |
| Client Vendor The Client Vendor Condition specifies the name of the vendor of the RADIUS client that sends connective |
| Add Cancel |

Passaggio 8. Immettere l'indirizzo IP corrispondente, quindi fare clic su Ok. Viene visualizzato un elenco con le condizioni aggiunte. Fare clic su Avanti.

Passaggio 9. Nella pagina Specifica autorizzazione di accesso, selezionare Accesso concesso. Fare clic su Next (Avanti).



Passaggio 10. Nella pagina Autenticazione impostare il metodo di autenticazione più adatto alla rete. Fare clic su Next (Avanti).

New Network Policy



Configure Authentication Methods

Configure one or more authentication methods required for the connection reques authentication, you must configure an EAP type. If you deploy NAP with 802.1X or Protected EAP in connection request policy, which overrides network policy authen

EAP types are negotiated between NPS and the client in the order in which they are listed.



Passaggio 11. Nella finestra Configura vincoli utilizzare i valori predefiniti. Fare clic su Next (Avanti).

Passaggio 12. Nella pagina Configura impostazioni, in Attributi RADIUS, fare clic su Specifiche del fornitore, quindi su Aggiungi.

Nota: le restanti impostazioni di questa pagina vengono impostate sui valori predefiniti. È necessario controllare solo le impostazioni specifiche del fornitore.

New Network Policy



Configure Settings

NPS applies settings to the connection request if all of the network policy condition are matched.

| Settings: | | | | |
|---|---|---------------------------------------|--|--|
| RADIUS Attributes | To send additional attributes to RADIUS clients, select a Vend then click Edit. If you do not configure an attribute, it is not sen your RADIUS client documentation for required attributes. | | | |
| 🗾 Vendor Specific | | | | |
| Network Access Protection | | | | |
| NAP Enforcement | Attributes: | · · · · · · · · · · · · · · · · · · · | | |
| Extended State | Name | Vendor Val | | |
| Routing and Remote Access | | | | |
| Multilink and Bandwidth Allocation Protocol (BAP) | | | | |
| IP Filters | | | | |
| A Encryption | Add Edit | Remove | | |
| TP Settings | | | | |
| | | | | |
| | | Previous Next | | |

In Fornitore, Selezionare Cisco. Fare clic su Add. Viene visualizzata la finestra Informazioni attributo.

| Add Vendor Specific Attribute | × |
|---|-------|
| To add an attribute to the settings, select the attribute, and then click Add. | |
| To add a Vendor Specific attribute that is not listed, select Custom, and then click Add. | |
| Cisco | |
| Attributes: | |
| Name Vendor | |
| Cisco-AV-Pair Cisco | |
| | |
| | |
| Description: | |
| Specifies the Cisco AV Pair VSA. | |
| Add | Close |

Nella finestra Informazioni attributo, fare clic su Aggiungi e immettere il valore shell:privlvl:15. Fare clic su OK.

| А | ttri | bute | Infor | mation |
|---|------|------|-------|--------|
| | | | | |

| Attribute name: Cisco-AV-Pair | |
|----------------------------------|-----------|
| Attribute number: 5000 | |
| Attribute format: String | |
| Attribute values: | |
| Vendor Value | (Add |
| Cisco shell:priv-lvl:15 | Edit |
| | E916 |
| | Remove |
| | |
| | Move Up |
| | Move Down |
| | |
| ОК | Cancel |

Nota:questo è il valore assegnato da Cisco per consentire al server RADIUS di concedere l'accesso all'utility di configurazione dello switch basata sul Web.

Fare clic su OK per chiudere la finestra Informazioni attributo, quindi fare clic su Chiudi per chiudere la finestra Aggiungi attributo specifico del fornitore. Fare clic su Next (Avanti).

Passaggio 13. Viene visualizzato un riepilogo delle impostazioni per questo criterio. Fare clic su Fine. Il criterio di rete è stato creato.

X



Completing New Network Policy

You have successfully created the following network policy:

SG200/300 Series

Policy conditions:

| Condition | Value |
|---------------------|-------------------|
| Windows Groups | RADIUS\Test Group |
| Client IPv4 Address | 192.168.1.10 |

Policy settings:

| Condition | Value |
|-----------------------------|---|
| Authentication Method | MS-CHAP v1 OR MS-CHAP v1 (User can change password after it has expired) OF |
| Access Permission | Grant Access |
| Update Noncompliant Clients | True |
| NAP Enforcement | Allow full network access |
| Framed-Protocol | PPP |
| Service-Type | Framed |
| | |

To close this wizard, click Finish.

| - . |
|------------|
| Previous |

Finish

Next

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).