

SOPHOS

simple + secure

Sophos NAC Advanced Guida all'installazione

Versione prodotto: 3.2

Data documento: settembre 2011



Sommario

| | | |
|----|--|----|
| 1 | Contenuti di questo documento..... | 3 |
| 2 | Requisiti di sistema..... | 5 |
| 3 | Checklist per l'installazione..... | 6 |
| 4 | Checklist per la post installazione..... | 7 |
| 5 | Installazione in un server singolo..... | 13 |
| 6 | Installazione in server multipli..... | 15 |
| 7 | Upgrade del software..... | 19 |
| 8 | Disinstallazione del software..... | 23 |
| 9 | Requisiti di post installazione..... | 24 |
| 10 | Installazione del Dissolvable Agent..... | 52 |
| 11 | Disinstallazione del Dissolvable Agent da un server web..... | 54 |
| 12 | Distribuzione dell'agente..... | 55 |
| 13 | Disinstallazione dell'agente..... | 57 |
| 14 | Impostazioni facoltative | 58 |
| 15 | Supporto tecnico..... | 62 |
| 16 | Note legali..... | 63 |

1 Contenuti di questo documento

Questo documento fornisce supporto per l'installazione e la configurazione di Sophos NAC Advanced. Questa guida tratta dei seguenti argomenti:

- Requisiti di sistema
- Checklist per l'installazione e per la post installazione
- Installazione del Software
- Disinstallazione del software
- Requisiti di post installazione
- Requisiti di sistema per il Dissolvable Agent
- Installazione del Dissolvable Agent
- Disinstallazione del Dissolvable Agent.
- Requisiti di sistema dell'agente
- Distribuzione dell'agente
- Disinstallazione dell'agente
- Impostazioni opzionali (solo per le installazioni su più server).

1.1 Pubblico designato

I destinatari di questa guida sono professionisti del settore informatico non specializzati che operano in aziende di piccole e medie dimensioni o specialisti del settore informatico che operano in imprese con un numero di computer superiore a 25.000. Se si gestiscono più di 1000 computer, si consiglia di avvalersi dei Servizi professionali Sophos. I Servizi professionali Sophos collaborano con i dipendenti che si occupano della sicurezza informatica aziendale al fine di progettare e attuare un piano di distribuzione dei software di protezione.

1.2 Documentazione

La documentazione relativa a Sophos NAC Advanced viene installata insieme a Sophos NAC Advanced ed è reperibile nel **Menu Start > Sophos > Compliance Manager**. Per accedere alla documentazione e utilizzarla, è necessario installare Adobe® Acrobat® Reader.

1.3 Nome e password dell'account di Compliance Manager

Per accedere a Compliance Manager sono necessari un nome account ed una password.

Per accedere per la prima volta a Compliance Manager, utilizzare i seguenti nome account e password:

- **Nome account** = admin
- **Password** = una password a scelta

Memorizzare questa password dal momento che rappresenta l'unico accesso a Compliance Manager finché non vengono creati altri account utente. Per ulteriori informazioni, consultare la sezione [Accesso a Compliance Manager](#) a pagina 27.

2 Requisiti di sistema

L'installazione di Sophos NAC Advanced accompagna nel processo di installazione dei requisiti di sistema di Sophos NAC Advanced. Alcuni requisiti di sistema devono essere installati utilizzando il CD del sistema operativo. È necessario avere a disposizione il CD del sistema operativo adeguato.

Se non già installati nel o nei server, i seguenti requisiti di sistema devono essere installati dal CD del sistema operativo:

- Servizio autenticazione Internet (IAS) (Windows Server 2003) o Server dei criteri di rete (Windows Server 2008)
- Accodamento messaggi Microsoft (MSMQ)
- Gestione servizio Internet (IIS) versione 6.0 o superiore
- ASP.NET

Requisito del controller di dominio

È necessario creare manualmente un account di dominio standard nel controller di dominio, stabilire che la password non abbia scadenza e che l'utente non la possa cambiare. Per poter portare a termine questa procedura è necessario che l'account amministratore di dominio sia presente nel controller del dominio. Durante l'installazione di Sophos NAC Advanced l'account di servizio viene aggiunto al gruppo amministratori locale nel Compliance Agent in modo tale che Sophos NAC Advanced possa accedere ai database di SQL server. Questo account deve avere l'accesso in **lettura** per l'attributo utenti "**membro di**".

Requisiti di certificato web

Policy Interface, Reporting Interface e Registration Interface sono servizi web che richiedono il protocollo HTTPS per comunicare con il Compliance Agent installato in ogni computer. Affinché Sophos NAC Advanced operi correttamente, è necessario installare nel Compliance Application Server un certificato web per tali componenti. Questi componenti possono condividere uno stesso certificato web. Se si crea un certificato web personalizzato, è necessario accertarsi che tutti i computer lo riconoscano come valido. Se si sta testando o valutando Sophos NAC Advanced con HTTPS disattivato, il certificato web non è necessario.

Nota: se si è in possesso di Compliance Application Servers multipli e si desidera utilizzare software di bilanciamento del carico, il certificato web deve corrispondere all'URL del "pool di server" che verrà anche configurato in tutti gli agenti.

Per informazioni relative ai requisiti di sistema, consultare la pagina corrispondente del sito web di Sophos (<http://www.sophos.it/products/all-sysreqs.html>).

3 Checklist per l'installazione

Utilizzare la checklist per l'installazione, in modo tale da verificare di avere completato tutte le operazioni necessarie per l'installazione di Sophos NAC Advanced.

| Op. | Descrizione | Completata |
|-----|--|------------|
| 1. | Inserire i CD del sistema operativo Windows Server. L'installazione di Sophos NAC Advanced accompagna nel processo di installazione dei requisiti di sistema. La procedura di installazione può richiedere che i requisiti di sistema vengano installati utilizzando il CD del sistema operativo. | |
| 2. | Nel controller di dominio, creare un account di servizio per Sophos NAC Advanced. | |
| 3. | Installare un certificato web sul o sui Compliance Application Server. Sophos utilizza HTTPS per proteggere nomi utente, password ed altre informazioni sensibili di un'impresa. Se si desidera condurre un test o una valutazione, è possibile disattivare HTTPS. Per ulteriori informazioni, consultare la sezione <i>Disattivazione di HTTPS per un test in ambienti non di produzione</i> a pagina 60. Se si sta testando o valutando Sophos NAC Advanced con HTTPS disattivato, il certificato web non è necessario. | |
| 4. | Installare il Sophos Compliance Database Server. Per implementazioni e valutazioni di dimensioni ridotte, è possibile installare Sophos NAC Advanced in un server singolo. | |
| 5. | Installare il Sophos Compliance Application Server. Implementazioni più ampie possono richiedere Compliance Application Servers aggiuntivi. | |
| 6. | Installare RADIUS Enforcer nei server corrispondenti (operazione facoltativa). RADIUS Enforcer viene installato automaticamente in quanto parte dell'installazione del Compliance Application Server. In alternativa, è possibile installare RADIUS Enforcer separatamente in server aggiuntivi. | |

4 Checklist per la post installazione

Una volta completata l'installazione, è necessario configurare Sophos NAC Advanced. Utilizzare la checklist per la post installazione, in modo tale da verificare di avere completato tutte le operazioni necessarie per la configurazione di Sophos NAC Advanced. Sophos NAC Advanced La configurazione di DHCP è facoltativa e dipende dall'utilizzo o meno di DHCP.

Checklist per la post installazione se si utilizza Windows Server 2003

| Op. | Descrizione | Completata |
|---|---|------------|
| Sophos NAC Advanced Configurazione | | |
| 1. | Avviare l'agente di SQL server e verificare/modificare le impostazioni predefinite dei report. Per ulteriori informazioni, consultare la sezione Avvio dell'agente di SQL server e verifica/modifica delle impostazioni predefinite dei report a pagina 24. | |
| 2. | Calibrare i Compliance Database ed i log delle transazioni. Per ulteriori informazioni, consultare la sezione Calibrazione dei database di SQL e i log delle transazioni a pagina 25. | |
| 3. | Configurare un archivio utenti esterno per accedere a Compliance Manager. (operazione facoltativa) Per ulteriori informazioni, consultare la sezione Configurazione di un archivio utenti esterno per accedere a Compliance Manager (operazione facoltativa) a pagina 28. | |
| 4. | Accedere a Sophos Compliance Manager. Nota: quando si utilizza Compliance Manager, è necessario creare o utilizzare modelli di accesso, profili, criteri e gruppi predefiniti. Per ulteriori informazioni, consultare la sezione Accesso a Compliance Manager a pagina 27. | |
| 5. | Installare il Dissolvable Agent su un server web. Nota: tale server può essere lo stesso in cui è stato installato Sophos Compliance Manager. Per ulteriori informazioni, consultare la sezione Installazione del Dissolvable Agent in un server web a pagina 52. | |
| Impostazioni (Windows Server 2003) per il Servizio autenticazione Internet (IAS) | | |
| 6. | Fornire accesso IAS a Active Directory. Nota: Per le implementazioni LDAP o se si sta utilizzando Sophos NAC Advanced come proxy RADIUS (configurando Sophos NAC Advanced in modalità proxy in presenza di un altro server RADIUS), non è richiesto il completamento di questa operazione. | |

| Op. | Descrizione | Completata |
|---|--|------------|
| | Per ulteriori informazioni, consultare la sezione <i>Accesso IAS a Active Directory</i> a pagina 30. | |
| 7. | Configurare il criterio di accesso remoto. Per ulteriori informazioni, consultare la sezione <i>Configurazione del criterio di accesso remoto</i> a pagina 31. | |
| 8. | Per la buona riuscita delle richieste di autenticazione, disabilitare il log IAS. (operazione facoltativa) Per ulteriori informazioni, consultare la sezione <i>Disabilitazione del log IAS per la buona riuscita delle richieste di autenticazione (operazione facoltativa)</i> a pagina 33. | |
| 9. | Aggiungere client RADIUS per ogni dispositivo di accesso alla rete. (operazione facoltativa) Nota: completare questa operazione solo se si desidera implementare l'attuazione di RADIUS. L'attuazione di RADIUS viene eseguita con VPN, 802.1x, Cisco NAC e implementazioni estese di RADIUS. Per ciascun concentratore VPN, è necessario aggiungere a IAS una voce relativa al client RADIUS. Per ulteriori informazioni, consultare la sezione <i>Aggiunta di client RADIUS per ogni dispositivo di accesso alla rete (operazione facoltativa)</i> a pagina 33. | |
| Sophos NAC Advanced come proxy RADIUS (Windows Server 2003) (operazione facoltativa) Nota: queste operazioni sono richieste solo se si sta configurando Sophos NAC Advanced in modalità proxy in presenza di un altro server RADIUS. | | |
| 10. | Aggiungere un gruppo di server di accesso remoto. Per ulteriori informazioni, consultare la sezione <i>Aggiunta di un gruppo di server di accesso remoto</i> a pagina 38. | |
| 11. | Creare un criterio di richiesta di connessione. Per ulteriori informazioni, consultare la sezione <i>Creazione di un criterio di richiesta di connessione</i> a pagina 39. | |
| 12. | Verificare le condizioni del criterio. Per ulteriori informazioni, consultare la sezione <i>Verifica delle condizioni del criterio</i> a pagina 40. | |
| 13. | Cambiare le porte di autenticazione di RADIUS. Per ulteriori informazioni, consultare la sezione <i>Modifica delle porte di autenticazione e di accounting di RADIUS</i> a pagina 40. | |

| Op. | Descrizione | Completata |
|--|---|------------|
| 14. | <p>Nell'interfaccia di registrazione di Sophos NAC Advanced, cambiare il protocollo di autenticazione delle registrazioni.</p> <p>Per ulteriori informazioni, consultare la sezione Cambio del protocollo di autenticazione delle registrazioni nell'interfaccia di registrazione a pagina 41.</p> | |
| 15. | <p>Configurare il server RADIUS per i mapping/profilo di gruppo. (operazione facoltativa)</p> <p>Per ulteriori informazioni, consultare la sezione Configurazione del server RADIUS per i mapping/profilo di gruppo (operazione facoltativa) a pagina 41.</p> | |
| <p>Implementazione di LDAP (operazione facoltativa)</p> <p>Nota: questa operazione è obbligatoria solo se si utilizzano, in concomitanza con RADIUS Enforcer, directory LDAP esistenti.</p> | | |
| 16. | Consultare la <i>Guida all'implementazione LDAP</i> di <i>Sophos NAC Advanced</i> per una checklist di tutte le operazioni di LDAP. | |
| <p>Configurazione di Sophos Compliance Application Servers multipli</p> <p>Nota: È necessario configurare tutti i Compliance Application Servers in modo tale che siano identici al Compliance Application Server primario. Nelle implementazioni LDAP, per poter riutilizzare un file di configurazione su server multipli, è necessario utilizzare il tool Password Encryption per poter aggiornare e criptare la password in ogni server. Per ulteriori informazioni, consultare la <i>Sophos NAC Advanced</i> di <i>Sophos NAC Advanced</i>.</p> | | |
| 17. | <p>Esportare la chiave del server dal Compliance Application Server primario ed importarla nei Compliance Application Servers aggiuntivi.</p> <p>Per ulteriori informazioni, consultare la sezione Esportazione e importazione della chiave del server in Compliance Application Server aggiuntivi a pagina 50.</p> | |
| 18. | <p>Configurazione di DNS Round Robin in Windows Server 2003 Portare a termine questa operazione nel server di Windows in cui si esegue il servizio domain name quando altri software di bilanciamento dei carichi o applicazioni non sono in esecuzione.</p> <p>Per ulteriori informazioni, consultare la sezione Configurazione di DNS Round Robin in Windows Server 2003 e superiore a pagina 50.</p> | |
| <p>Implementazione di DHCP (operazione facoltativa)</p> | | |
| 19. | Consultare la <i>Guida all'attuazione dei criteri di sicurezza in DHCP</i> di <i>Sophos NAC Advanced</i> per una checklist di tutte le operazioni di DHCP. | |
| <p>Distribuzione di Sophos Compliance Agent</p> | | |

| Op. | Descrizione | Completata |
|-----|---|------------|
| 20. | Distribuire il Compliance Agent ai computer. Per ulteriori informazioni, consultare la sezione <i>Distribuzione dell'agente</i> a pagina 55. | |

Checklist per la post installazione se si utilizza Windows Server 2008

| Op. | Descrizione | Completata |
|---|--|------------|
| Sophos NAC Advanced Configurazione | | |
| 1. | Avviare l'agente di SQL server e verificare/modificare le impostazioni predefinite dei report. Per ulteriori informazioni, consultare la sezione <i>Avvio dell'agente di SQL server e verifica/modifica delle impostazioni predefinite dei report</i> a pagina 24. | |
| 2. | Calibrare i Compliance Database ed i log delle transazioni. Per ulteriori informazioni, consultare la sezione <i>Calibrazione dei database di SQL e i log delle transazioni</i> a pagina 25. | |
| 3. | Configurare un archivio utenti esterno per accedere a Compliance Manager. (operazione facoltativa) Per ulteriori informazioni, consultare la sezione <i>Configurazione di un archivio utenti esterno per accedere a Compliance Manager (operazione facoltativa)</i> a pagina 28. | |
| 4. | Accedere a Sophos Compliance Manager. Nota: quando si utilizza Compliance Manager, è necessario creare o utilizzare modelli di accesso, profili, criteri e gruppi predefiniti. Per ulteriori informazioni, consultare la sezione <i>Accesso a Compliance Manager</i> a pagina 27. | |
| 5. | Installare il Dissolvable Agent su un server web. Nota: tale server può essere lo stesso in cui è stato installato Sophos Compliance Manager. Per ulteriori informazioni, consultare la sezione <i>Installazione del Dissolvable Agent in un server web</i> a pagina 52. | |
| Impostazioni dei criteri di rete (Windows Server 2008) | | |
| 6. | Garantire al Server dei criteri di rete accesso ad Active Directory. Nota: Per le implementazioni LDAP o se si sta utilizzando Sophos NAC Advanced come proxy RADIUS (configurando Sophos NAC Advanced | |

| Op. | Descrizione | Completata |
|--|---|------------|
| | <p>in modalità proxy in presenza di un altro server RADIUS), non è richiesto il completamento di questa operazione.</p> <p>Per ulteriori informazioni, consultare la sezione <i>Come garantire al Server dei criteri di rete accesso ad Active Directory</i> a pagina 34.</p> | |
| 7. | <p>Configurare un nuovo criterio di rete.</p> <p>Per ulteriori informazioni, consultare la sezione <i>Configurazione di un criterio di rete</i> a pagina 35.</p> | |
| 8. | <p>Disabilitare il log del Server dei criteri di rete, per la buona riuscita delle richieste di autenticazione. (operazione facoltativa)</p> <p>Per ulteriori informazioni, consultare la sezione <i>Disabilitazione del log del Server dei criteri di rete, per la buona riuscita delle richieste di autenticazione (operazione facoltativa)</i> a pagina 37.</p> | |
| 9. | <p>Aggiungere client RADIUS per ogni dispositivo di accesso alla rete. (operazione facoltativa)</p> <p>Nota: completare questa operazione solo se si desidera implementare l'attuazione di RADIUS. L'attuazione di RADIUS viene eseguita con VPN, 802.1x, Cisco NAC e implementazioni estese di RADIUS. Per ciascun concentratore VPN, è necessario aggiungere al Server dei criteri di rete una voce relativa al client RADIUS.</p> <p>Per ulteriori informazioni, consultare la sezione <i>Aggiunta di client RADIUS per ogni dispositivo di accesso alla rete (operazione facoltativa)</i> a pagina 37.</p> | |
| <p>Sophos NAC Advanced come proxy RADIUS (Windows Server 2008) (operazione facoltativa)</p> <p>Nota: queste operazioni sono richieste solo se si sta configurando Sophos NAC Advanced in modalità proxy in presenza di un altro server RADIUS.</p> | | |
| 10. | <p>Aggiungere un gruppo di server di accesso remoto.</p> <p>Per ulteriori informazioni, consultare la sezione <i>Aggiunta di un gruppo di server di accesso remoto</i> a pagina 44.</p> | |
| 11. | <p>Creare un criterio di richiesta di connessione.</p> <p>Per ulteriori informazioni, consultare la sezione <i>Creazione di un criterio di richiesta di connessione</i> a pagina 45.</p> | |
| 12. | <p>Verificare le condizioni del criterio.</p> <p>Per ulteriori informazioni, consultare la sezione <i>Verifica delle condizioni del criterio</i> a pagina 46.</p> | |
| 13. | <p>Nell'interfaccia di registrazione di Sophos NAC Advanced, cambiare il protocollo di autenticazione delle registrazioni.</p> <p>Per ulteriori informazioni, consultare la sezione <i>Cambio del protocollo di autenticazione delle registrazioni nell'interfaccia di registrazione</i> a pagina 46.</p> | |

| Op. | Descrizione | Completata |
|--|---|------------|
| 14. | <p>Configurare il server RADIUS per i mapping/profilo di gruppo. (operazione facoltativa)</p> <p>Per ulteriori informazioni, consultare la sezione Configurazione del server RADIUS per i mapping/profilo di gruppo (operazione facoltativa) a pagina 47.</p> | |
| <p>Implementazione di LDAP (operazione facoltativa)</p> <p>Nota: questa operazione è obbligatoria solo se si utilizzano, in concomitanza con RADIUS Enforcer, directory LDAP esistenti.</p> | | |
| 15. | <p>Consultare la <i>Sophos NAC Advanced</i> di <i>Guida all'implementazione LDAP</i> per una checklist di tutte le operazioni di LDAP.</p> | |
| <p>Configurazione di Sophos Compliance Application Servers multipli</p> <p>Nota: È necessario configurare tutti i Compliance Application Servers in modo tale che siano identici al Compliance Application Server primario. Nelle implementazioni LDAP, per poter riutilizzare un file di configurazione su server multipli, è necessario utilizzare il tool Password Encryption per poter aggiornare e criptare la password in ogni server. Per ulteriori informazioni, consultare la <i>Sophos NAC Advanced</i> di <i>Sophos NAC Advanced</i>.</p> | | |
| 16. | <p>Esportare la chiave del server dal Compliance Application Server primario ed importarla nei Compliance Application Servers aggiuntivi.</p> <p>Per ulteriori informazioni, consultare la sezione Esportazione e importazione della chiave del server in Compliance Application Server aggiuntivi a pagina 50.</p> | |
| 17. | <p>Configurazione di DNS Round Robin in Windows Server 2003 Portare a termine questa operazione nel server di Windows in cui si esegue il servizio domain name quando altri software di bilanciamento dei carichi o applicazioni non sono in esecuzione.</p> <p>Per ulteriori informazioni, consultare la sezione Configurazione di DNS Round Robin in Windows Server 2003 e superiore a pagina 50.</p> | |
| <p>Implementazione di DHCP (operazione facoltativa)</p> | | |
| 18. | <p>Consultare la <i>Guida all'attuazione dei criteri di sicurezza in DHCP</i> di <i>Sophos NAC Advanced</i> per una checklist di tutte le operazioni di DHCP.</p> | |
| <p>Distribuzione di Sophos Compliance Agent</p> | | |
| 19. | <p>Distribuire il Compliance Agent ai computer.</p> <p>Per ulteriori informazioni, consultare la sezione Distribuzione dell'agente a pagina 55.</p> | |

5 Installazione in un server singolo

Quando si esegue l'installazione di Sophos NAC Advanced in un server singolo, prima vengono installati i Sophos Compliance Database e successivamente il Compliance Application Server.

L'installazione di Sophos NAC Advanced richiede l'utilizzo di un account di dominio con privilegi d'amministrazione locali. L'account che installa il NAC deve essere definito come un utente di SQL Server, oppure appartenere ad un gruppo che è definito come utente di Server. Inoltre, quel particolare utente di SQL Server deve anche svolgere il ruolo di server sysadmin in SQL.

1. Nel controller di dominio, creare manualmente un account di dominio standard, stabilire che la password non abbia scadenza e che l'utente non la possa cambiare.

Durante l'installazione di Compliance Server l'account di servizio viene aggiunto al gruppo amministratori locale nel Compliance Server, in modo tale che possa accedere ai database di SQL server. Questo account deve avere l'accesso in **lettura** per l'attributo utenti "**membro di**".

2. Scaricare Sophos NAC Advanced dal sito web di Sophos.
3. Cliccare due volte sul file di installazione per eseguirne l'installazione.

Quando si installa Sophos NAC Advanced, si consiglia di abilitare l'impostazione trace. Dal prompt dei comandi, digitare il nome del file di installazione di Sophos NAC Advanced seguito da uno spazio e dalla dicitura /trace (per es. nac_xx_sfx.exe /trace). Quando viene visualizzato il messaggio di installazione, cliccare su **OK** per eseguire l'installazione. I log di installazione si trova nella cartella %temp%.

4. Cliccare su **Next** per continuare.
5. Leggere il Contratto di Licenza per l'Utente Finale, selezionare il pulsante di opzione **I Accept the terms of the License Agreement**, cliccare poi su **Next** per proseguire.
6. Selezionare il pulsante di opzione **Sophos Compliance Application Server, Compliance Database e RADIUS Enforcer**. Cliccare su **Next** per continuare.
7. Digitare i dati dell'account di servizio nei campi relativi. Cliccare su **Next** per continuare. SQL server e Compliance Application Server richiedono un account di dominio standard. Tale account di servizio è stato creato al passaggio 1.
8. Specificare le impostazioni di proxy per Internet di questo server selezionando la casella **Use Proxy**. Cliccare su **Next** per continuare.

L'indirizzo e il numero di porta del server proxy sono campi obbligatori. Il nome utente, la password e la conferma della password vengono richiesti solo se si utilizza un proxy autenticato.

9. Digitare i dati dell'account di download Sophos nei campi relativi. Cliccare su **Next** per continuare.

I dati dell'account di download Sophos vengono forniti al momento dell'acquisto di Sophos NAC Advanced. Il nome utente e la password sono necessari per eseguire l'aggiornamento delle patch e per ottenere le date più recenti relative alle attuali firme delle applicazioni antivirus e antispyware. Se nome utente e password vengono inseriti in modo errato durante l'installazione, sarà possibile correggerli utilizzando Compliance Manager. Per ulteriori informazioni, consultare la Guida in linea di Compliance Manager.

10. Modificare la directory dei componenti Compliance Manager IIS nel modo appropriato. Cliccare su **Next** per continuare.

11. Per avviare l'installazione, cliccare su **Install**.

I Sophos Compliance Application Server e Compliance Manager vengono così configurati e lo stato dell'installazione visualizzato. Una parte dell'installazione può durare diversi minuti, durante i quali la barra di progresso non si muove. Non cancellare l'installazione perché continuerà ad avanzare.

12. Cliccare su **Finish**.

Nota:

- Se si verificano errori di installazione, utilizzare l'Event Log per visualizzare informazioni aggiuntive. Nei file di installazione dei database, è necessario cancellare i seguenti database, nel caso siano stati creati: AlertStore, AuditStore, GeneralStore, PolicyStore, ReportStore, ReportStoreCache, ReportStoreWH e SecurityStore. Una volta cancellati i database, è possibile ritentare l'installazione.
- Una volta completata l'installazione, è necessario portare a termine i requisiti di post installazione. Per ulteriori informazioni, consultare la sezione [Requisiti di post installazione](#) a pagina 24.

6 Installazione in server multipli

Per installazioni più ampie, Sophos consiglia di installare i database di SQL server e l'applicazione su server separati. È necessario installare i database di SQL server prima dell'applicazione.

6.1 Installazione dei database

Se i database di SQL Server e l'applicazione sono stati installati su server separati, devono essere riuniti sotto lo stesso dominio. L'installazione dei database di SQL server richiede inoltre che si utilizzi un account di dominio con privilegi di amministratore locale. L'account che installa NAC deve essere definito come un utente di SQL Server, oppure appartenere ad un gruppo definito come utente di SQL Server. Tale utente di SQL Server deve anche svolgere il ruolo di server sysadmin in SQL.

1. Nel controller di dominio, creare manualmente un account di dominio standard, stabilire che la password non abbia scadenza e che l'utente non la possa cambiare.

Durante l'installazione di Compliance Application Server l'account di servizio viene aggiunto al gruppo amministratori locale nel Compliance Application Server, in modo tale che Sophos possa accedere ai database di SQL Server. Questo account deve avere accesso in **lettura** per l'attributo utenti "**membro di**".

Nota: Questo passaggio non è necessario per gli upgrade di Sophos NAC Advanced.

2. Scaricare Sophos NAC Advanced dal sito web di Sophos.
3. Cliccare due volte sul file di installazione per eseguirne l'installazione.
Quando si installa Sophos NAC Advanced, si consiglia di abilitare l'impostazione trace. Dal prompt dei comandi, digitare il nome del file di installazione di Sophos NAC Advanced seguito da uno spazio e dalla dicitura /trace (per es. nac_xx_sfx.exe /trace). Quando viene visualizzato il messaggio di installazione, cliccare su **OK** per eseguire l'installazione. I log di installazione si trova nella cartella %temp%.
4. Cliccare su **Next** per continuare.
5. Leggere il Contratto di Licenza per l'Utente Finale, selezionare il pulsante di opzione **I Accept the terms of the License Agreement**, cliccare poi su **Next** per proseguire.
6. Effettuare una delle seguenti operazioni:
 - Se si installano i Compliance Database in Windows Server 2003, selezionare il pulsante di opzione **Sophos Compliance Database Server Only**. Cliccare su **Next** per continuare.
 - Se si installano i Sophos Compliance Database in Windows Server 2000 SP3 o in Windows Server 2003 a 64 bit, quando il programma di installazione indica che è possibile installare solo i database SQL, cliccare sul pulsante **OK**.
7. Digitare i dati dell'account di servizio nei campi relativi. Cliccare su **Next** per continuare. SQL server e Compliance Application Server richiedono un account di dominio standard. Tale account di servizio è stato creato al passaggio 1. Se si sta eseguendo un upgrade, utilizzare gli stessi dati dell'account usati per l'installazione iniziale.

8. Effettuare una delle seguenti operazioni:
 - Se si possiede più di un'istanza del database locale, selezionare quella adeguata. Cliccare su **Next** per continuare.
 - Se non si possiede più di un'istanza del database locale, andare al passaggio successivo.
9. Per avviare l'installazione, cliccare su **Install**.

I Sophos Compliance Database vengono così configurati e lo stato dell'installazione visualizzato. Una parte dell'installazione può durare diversi minuti, durante i quali la barra di progresso non si muove. Non cancellare l'installazione perché continuerà ad avanzare.
10. Cliccare su **Finish**.

Importante: Se si verificano errori di installazione, utilizzare l'Event Log per visualizzare informazioni aggiuntive. Nei file di installazione dei database, è necessario cancellare i seguenti database, nel caso siano stati creati: AlertStore, AuditStore, GeneralStore, PolicyStore, ReportStore, ReportStoreCache, ReportStoreWH e SecurityStore. Una volta cancellati i database, è possibile ritentare l'installazione.

6.2 Installazione dell'applicazione

Se i database e l'applicazione sono stati installati su server separati, devono essere riuniti sotto lo stesso dominio. Inoltre, l'installazione dell'applicazione richiede che si utilizzi un account di dominio con privilegi di amministratore locale.

Importante: i Compliance Application Servers aggiuntivi devono essere installati e configurati adeguatamente, in modo tale da essere identici al Compliance Application Server primario. Per ulteriori informazioni, consultare la sezione [Configurazione di Compliance Application Server multipli \(operazione opzionale\)](#) a pagina 49.

1. Scaricare Sophos NAC Advanced dal sito web di Sophos.
2. Cliccare due volte sul file di installazione per eseguirne l'installazione.

Quando si installa Sophos NAC Advanced, si consiglia di abilitare l'impostazione trace. Dal prompt dei comandi, digitare il nome del file di installazione di Sophos NAC Advanced seguito da uno spazio e dalla dicitura /trace (per es. nac_xx_sfx.exe /trace). Quando viene visualizzato il messaggio di installazione, cliccare su **OK** per eseguire l'installazione. I log di installazione si trova nella cartella %temp%.
3. Cliccare su **Next** per continuare.
4. Leggere il Contratto di Licenza per l'Utente Finale, selezionare il pulsante di opzione **Accept the terms of the License Agreement**, cliccare poi su **Next** per proseguire.
5. Selezionare il pulsante di opzione **Sophos Compliance Application Server and RADIUS Enforcer**. Cliccare su **Next** per continuare.
6. Digitare i dati dell'account di servizio nei campi relativi. Cliccare su **Next** per continuare. SQL server e Compliance Application Server richiedono un account di dominio standard. I dati di tale account di servizio devono corrispondere a quelli inseriti durante l'installazione dei Compliance Database Sophos.

7. Specificare le impostazioni di proxy per Internet di questo server selezionando la casella **Use Proxy**. Cliccare su **Next** per continuare.
L'indirizzo e il numero di porta del server proxy sono campi obbligatori. Il nome utente, la password e la conferma della password vengono richiesti solo se si utilizza un proxy autenticato.
8. Inserire il nome del Sophos Compliance Database Server. Cliccare su **Next** per continuare.
Quando non viene utilizzata l'istanza SQL predefinita, il server e il nome dell'istanza devono avere la forma server\nome istanza. La procedura di installazione permette di verificare la connessione tra il server che si sta installando e quello del Compliance Database Server.
9. Digitare i dati dell'account di download Sophos nei campi relativi. Cliccare su **Next** per continuare.
I dati dell'account di download Sophos vengono forniti al momento dell'acquisto di Sophos NAC Advanced. Il nome utente e la password sono necessari per eseguire l'aggiornamento delle patch e per ottenere le date più recenti relative alle attuali firme delle applicazioni antivirus e antispyware. Se nome utente e password vengono inseriti in modo errato durante l'installazione, sarà possibile correggerli utilizzando Compliance Manager. Per ulteriori informazioni, consultare la Guida in linea di Compliance Manager.
10. Modificare la directory dei componenti Compliance Manager IIS nel modo appropriato. Cliccare su **Next** per continuare.
11. Per avviare l'installazione, cliccare su **Install**.
Il Sophos Compliance Application Server viene così configurata e lo stato dell'installazione visualizzato. Una parte dell'installazione può durare diversi minuti, durante i quali la barra di progresso non si muove. Non cancellare l'installazione perché continuerà ad avanzare.
12. Cliccare su **Finish**.

Nota:

- Se si verificano errori di installazione, utilizzare l'Event Log per visualizzare informazioni aggiuntive.
- Una volta completata l'installazione, è necessario portare a termine i requisiti di post installazione. Per ulteriori informazioni, consultare la sezione [Requisiti di post installazione](#) a pagina 24. Se si sta eseguendo un upgrade, tornare alle istruzioni nella sezione [Upgrade del software](#) a pagina 19 piuttosto che applicare i requisiti di postinstallazione.

6.3 Installazione di RADIUS Enforcer

RADIUS Enforcer viene installato automaticamente in quanto parte dell'installazione del Compliance Application Server. In alternativa, è possibile installare RADIUS Enforcer separatamente in server aggiuntivi. La scalabilità, la configurazione di rete o i requisiti di rete possono richiedere l'installazione di RADIUS Enforcer in uno o più server. Per installazioni più ampie, si consiglia di installare RADIUS Enforcer in un server a parte in modo tale da separare l'attività di correzione da quelle di e dell'agente, posizionati nei Compliance Application Server.

Nota: Sophos collabora direttamente con ogni singola azienda, al fine di stabilire se RADIUS Enforcer debba essere installato su server separati.

1. Scaricare Sophos NAC Advanced dal sito web di Sophos.
2. Cliccare due volte sul file di installazione per eseguirne l'installazione.
Quando si installa Sophos NAC Advanced, si consiglia di abilitare l'impostazione trace. Da un prompt dei comandi, digitare il nome del file di installazione di Sophos NAC Advanced seguito da uno spazio e dalla dicitura /trace (per es. nac_xx_sfx.exe /trace). Quando viene visualizzato il messaggio di installazione, cliccare su **OK** per eseguire l'installazione. I log di installazione si trova nella cartella %temp%.
3. Cliccare su **Next** per continuare.
4. Leggere il Contratto di Licenza per l'Utente Finale, selezionare il pulsante di opzione **I Accept the terms of the License Agreement**, cliccare poi su **Next** per proseguire.
5. Selezionare il pulsante di opzione **Sophos RADIUS Enforcer Only**. Cliccare su **Next** per continuare.
6. Digitare i dati dell'account di servizio nei campi relativi. Cliccare su **Next** per continuare. SQL server e Compliance Application Server richiedono un account di dominio standard. I dati di tale account di servizio devono corrispondere a quelli inseriti durante l'installazione dei Compliance Database Sophos.
7. Inserire il nome del Sophos Compliance Database Server. Cliccare su **Next** per continuare. Quando non viene utilizzata l'istanza SQL predefinita, il server e il nome dell'istanza devono avere la forma server\nome istanza. La procedura di installazione permette di verificare la connessione tra il server che si sta installando e quello del Compliance Database Server.
8. Per avviare l'installazione, cliccare su **Install**.
L'applicazione di RADIUS Enforcer viene così configurata e lo stato dell'installazione visualizzato.
9. Cliccare su **Finish**.
Nota: Se si verificano errori di installazione, utilizzare l'Event Log per visualizzare informazioni aggiuntive.

7 Upgrade del software

Sophos NAC Advanced versione 3.2.x può ricevere l'upgrade da Sophos NAC Advanced versione 3.0.x a 3.2. Sophos NAC per Endpoint Security and Control integrato con Sophos Endpoint Security and Control non può ricevere l'upgrade a Sophos NAC Advanced.

Importante: per eseguire l'upgrade del software, nell'installazione successiva è necessario digitare o selezionare dati identici a quelli digitati o selezionati durante l'installazione originale.

1. Prima di eseguire l'upgrade, accedere a Compliance Manager e configurare un agente di test che utilizzi l'indirizzo IP di uno dei Compliance Application Servers.

Importante: l'indirizzo IP del server del Compliance Application Server utilizzato in questo passaggio deve corrispondere al primo Compliance Application Server in cui verrà eseguito l'upgrade.

2. Eseguire il back up della chiave del Compliance Application Server e di tutti i database di Sophos NAC.

Nota: Back up these databases: AlertStore, AuditStore, GeneralStore, PolicyStore, ReportStore, ReportStoreCache, ReportStoreWH e SecurityStore.

3. Mettere tutti i Compliance Application Servers in modalità di manutenzione tramite il tool Maintenance Mode. Eseguire il tool da prompt dei comandi in ciascun Compliance Application Server.

- Se si sta eseguendo l'upgrading dalla versione 3.0.x, dal prompt dei comandi, andare alla directory Programmi\Endforce\Support Tools e digitare **MaintMode.exe /start**.
- Se si sta eseguendo l'upgrading dalla versione 3.2, dal prompt dei comandi, andare alla directory Programmi\Sophos\NAC\Support Tools e digitare **MaintMode.exe /start**.

Nota: quando il software si trova in modalità di manutenzione, l'agente riconosce tale modalità ed agisce di conseguenza senza commettere errori, interrompersi o inviare avvisi all'utente relativi a tale modalità. L'agente salva localmente tutti i dati relativi alla verifica e ai report fino a quando il software non ritorna in modalità produttiva. Per ulteriori informazioni, consultare la *Sophos NAC Advanced* di *Sophos NAC Advanced*.

4. Installare i database in modo tale che eseguano l'upgrade nel server SQL seguendo le istruzioni nella sezione [Installazione dei database](#) a pagina 15.

Nota: Sophos NAC Advanced ha un solo file di installazione da eseguire sia sul Compliance Database Server che sui Compliance Application Servers. Quando si esegue il file di installazione, è possibile specificare le opzioni di installazione per ciascun server. Per prima cosa è necessario eseguire l'upgrade dei database. Se si verificano errori di installazione, utilizzare l'Event Log per visualizzare informazioni aggiuntive.

Nota: Gli upgrade da SQL Server 2000 sono supportati. È necessario effettuare prima l'upgrade di Sophos NAC Advanced, e successivamente eseguire l'upgrade ad una versione supportata di SQL Server.

Nei file di upgrade dei database, è necessario cancellare i seguenti database, nel caso siano stati creati: AlertStore, AuditStore, GeneralStore, PolicyStore, ReportStore, ReportStoreCache, ReportStoreWH e SecurityStore. Una volta cancellati i database, ricollegare tali database dal back up appena completato. È a questo punto possibile provare ad eseguire nuovamente l'installazione.

5. Nel server SQL, svolgere la seguente procedura:
 - a) Attivare l'agente di SQL Server, se ancora inattivo. Per ulteriori informazioni, consultare la sezione [Avvio dell'agente di SQL server e verifica/modifica delle impostazioni predefinite dei report](#) a pagina 24.
 - b) Verificare/modificare l'orario di esecuzione dell'operazione Report Warehouse Loader. Questa impostazione stabilisce quando i dati correnti di un report debbano essere trasferiti nell'archivio dei report. Per ulteriori informazioni, consultare la sezione [Verifica/Modifica dell'operazione Report Warehouse Loader](#) a pagina 59.
 - c) Verificare/modificare le impostazioni predefinite del report. Per ulteriori informazioni, consultare la sezione [Avvio dell'agente di SQL server e verifica/modifica delle impostazioni predefinite dei report](#) a pagina 24.
6. Per prima cosa rimuovere il Compliance Application Server di cui si desidera eseguire l'upgrade dal gruppo di software di bilanciamento del carico.

Nota: Questo indirizzo IP del server deve corrispondere all'agente di prova configurato al passaggio 1. svolgere questo passaggio solo se Sophos NAC Advanced è installato in un ambiente di bilanciamento del carico.
7. Installare l'upgrade dell'applicazione in questo Compliance Application Server, seguendo le istruzioni della sezione [Installazione dell'applicazione](#) a pagina 16.

Nota: Se si verificano errori di installazione, utilizzare l'Event Log per visualizzare informazioni aggiuntive.
8. Riportare il Compliance Application Server in modalità di produzione tramite il tool Maintenance Mode. Dal prompt dei comandi, andare alla directory Programmi\Sophos\NAC\Support Tools e digitare **MaintMode.exe /stop**.
9. Verificare che l'agente di test appena configurato possa eseguire con successo le operazioni di registrazione, recupero, verifica, attuazione, correzione e reportistica.

10. Mettere tutti i Compliance Application Server in modalità di manutenzione tramite il tool Maintenance Mode. Dal prompt dei comandi, andare alla directory Programmi\Sophos\NAC\Support Tools e digitare **MaintMode.exe /stop**.

11. Ricollocare il Compliance Application Server nel gruppo dei software di bilanciamento del carico.

Nota: svolgere questo passaggio solo se Sophos NAC Advanced è installato in un ambiente di bilanciamento del carico.

12. Installare l'upgrade dell'installazione in tutti i Compliance Application Servers aggiuntivi seguendo le istruzioni della sezione [Installazione dell'applicazione](#) a pagina 16.

13. In tutti i Compliance Application Servers, fare quanto descritto di seguito:

- Verificare/modificare la data di esecuzione dell'operazione Patch Loader in tutti i Compliance Application Servers. Per ulteriori informazioni, consultare la sezione [Verifica/Modifica della procedura Patch Loader](#) a pagina 58.
- Per svolgere test ed utilizzare il software in ambienti non produttivi, disattivare HTTPS. Per ulteriori informazioni, consultare la sezione [Disattivazione di HTTPS per un test in ambienti non di produzione](#) a pagina 60.

14. Riportare il Compliance Application Servers in modalità di produzione tramite il tool Maintenance Mode. Dal prompt dei comandi di tutti i Compliance Application Server, andare alla directory Programmi\Sophos\NAC\Support Tools e digitare **MaintMode.exe /stop**.

15. Installare l'upgrade dell'agente in un computer di test e verificare che possa svolgere con successo le operazioni di registrazione, ritrovamento, verifica, attuazione, correzione e reportistica.

16. Installare l'upgrade dell'agente sui computer interessati.

17. Installare il Dissolvable Agent sull'adeguato server web, utilizzando le istruzioni della sezione [Installazione del Dissolvable Agent in un server web](#) a pagina 52 .

Nota: Il Dissolvable Agent sostituisce il Web Agent in maniera permanente. L'installazione del Dissolvable Agent disinstalla il Web Agent ed installa il Dissolvable Agent.

Nota: quando si esegue l'upgrade del software, vengono rimosse le restrizioni dei diritti di accesso relative alle directory utilizzate da Sophos NAC Advanced. È necessario riapplicare tali restrizioni una volta portato a termine l'upgrade.

L'upgrade di Sophos NAC Advanced dalla versione 3.0.x:

- Configura le nuove funzioni della versione. Per sfruttare al meglio le nuove funzioni del criterio, è necessario eseguire l'aggiornamento dei criteri esistenti.
- Aggiorna Compliance Manager con nuovi profili predefiniti, applicazioni, funzioni e azioni. L'upgrade permette anche di rimuovere profili, applicazioni, funzioni ed azioni non più supportate. Questi cambiamenti possono avere ripercussioni su alcuni dei criteri che sono stati creati.
- Converte i modelli di distribuzione dell'agente in modelli di configurazione. I modelli di configurazione dell'agente comprendono le impostazioni dell'agente simili a quelle dei modelli di distribuzione. I modelli di configurazione dell'agente consentono di aggiornare le impostazioni dell'agente attraverso il criterio.

- Non supporta più Windows 98; tutti i riferimenti a Windows 98 vengono quindi rimossi. I dati dei report di Windows 98 vengono conservati.
- I nomi della vista SQL sono stati aggiornati. Il prefisso per le viste SQL è ora NACVP invece che EFVP. SQL chiede quale utilizzo di EFVP dovrà essere aggiornato.

Nota: Se si sta eseguendo l'upgrade dalla versione 3.2 alla 3.2.x, non è possibile applicare queste modifiche dal momento che riguardano l'upgrade alla versione 3.2.

8 Disinstallazione del software

Quando si effettua la disinstallazione di Sophos NAC Advanced è necessario, per prima cosa, disinstallare l'applicazione e successivamente i database; se non si segue quest'ordine, l'applicazione genererà errori dovuti alla disinstallazione dei database.

8.1 Disinstallazione dell'applicazione

Disinstallare l'applicazione non comporta la cancellazione di nessun elemento creato in Compliance Manager. Tutti gli elementi, quali criteri e informazioni relative all'account utente, sono archiviati nei Compliance Database.

1. Dal menu Start, cliccare su **Pannello di controllo > Installazione applicazioni**.
2. Selezionare **Sophos Compliance Application Server** e cliccare su **Rimuovi**.
3. Cliccare su **Sì** per confermare la rimozione di Compliance Application Server. L'applicazione viene rimossa.

8.2 Disinstallazione del database

La disinstallazione dei database rimuove solo i file utilizzati per crearli e non i database veri e propri.

1. Dal menu Start, cliccare su **Pannello di controllo > Installazione applicazioni**.
2. Selezionare **Sophos Compliance Database Server** e cliccare su **Rimuovi**.
3. Cliccare su **Sì** per confermare la rimozione dei file del server utilizzati per creare i database. I file del server vengono rimossi mentre i database restano intatti.

8.3 Disinstallazione di RADIUS Enforcer

La disinstallazione di RADIUS Enforcer è necessaria solo se è stato installato in un server diverso da quello dell'applicazione di Sophos NAC Advanced.

1. Dal menu Start, cliccare su **Pannello di controllo > Installazione applicazioni**.
2. Selezionare **Sophos RADIUS Enforcer** e cliccare su **Rimuovi**.
3. Per confermare la rimozione del RADIUS Enforcer, cliccare su **Sì**. RADIUS Enforcer viene così rimosso.

9 Requisiti di post installazione

I requisiti di post installazione sono operazioni di configurazione aggiuntive necessarie per il corretto funzionamento di Sophos NAC Advanced.

9.1 Avvio dell'agente di SQL server e verifica/modifica delle impostazioni predefinite dei report

Sophos NAC Advanced genera report di supporto nell'identificazione della conformità ai criteri di protezione e dei computer aziendali a rischio. Questi report forniscono dati utili per la risoluzione di problemi. Perché la creazione dei report avvenga correttamente, è necessario verificare che l'agente di SQL Server sia attivo.

I report devono essere disponibili sia in versione riassunta che dettagliata e devono includere dati correnti ed archiviati. Le impostazioni dei report stabiliscono per quanto tempo debbano essere conservati i dati all'interno di un report corrente e dopo quanto tempo debbano essere archiviati. Si consiglia di non modificare nessun'altra delle impostazioni dei report.

Le impostazioni predefinite per tutti i report sono:

- Cancellazione dei dati dell'audit ogni **90** giorni. Tale impostazione viene rappresentata dal valore `auditStorePurgeDays`. La cancellazione viene disabilitata se si imposta il valore su **-1**.
- La cancellazione dei dati dai report correnti avviene ogni **2** giorni. Si tratta del valore `reportStorePurgeDays`.
- La cancellazione dei dati dall'archivio dei report avviene ogni **30** giorni. Si tratta del valore `reportStoreWHPurgeDays`.

Nota: il valore `reportStoreWHPurgeDays` deve superare quello `reportStorePurgeDays` e quello relativo all'intervallo di tempo di trasferimento dei dati.

- Trasferire i dati di tutti i report in quelli dell'archivio **1** una volta al giorno, alle ore 2:30. Questo valore fa parte dell'operazione Report Warehouse Loader. Per ulteriori informazioni su come modificare questo intervallo di tempo, consultare la sezione [Verifica/Modifica dell'operazione Report Warehouse Loader](#) a pagina 59.

1. Dal menu Start nel server SQL, eseguire una delle seguenti operazioni:

- se si esegue SQL Server 2000, cliccare su **Microsoft SQL Server > Enterprise Manager** . Si apre SQL Enterprise Manager.
- Se si esegue SQL Server 2005 o superiore, cliccare su **Microsoft SQL Server (versione) > SQL Server Management Studio** . Si apre SQL Server Management Studio.

2. Per avviare SQL Server Agent, eseguire una delle seguenti operazioni:
 - Se si esegue SQL Server 2000, nella cartella Management, trovare **SQL Server Agent**, cliccarvi col tasto destro del mouse e selezionare **Avvia**.
 - Se si esegue SQL Server 2005, trovare **SQL Server Agent**, cliccarvi col tasto destro del mouse e selezionare **Avvia**.

Importante: per assicurarsi che SQL Server Agent venga avviato automaticamente quando si riavvia il server SQL, è necessario accedere a Windows Services Control Manager e modificare la modalità di avvio del servizio SQLSERVERAGENT (SQL Server 2000) o di SQL Server Agent (SQL Server 2005) e scegliere l'avvio automatico.
3. Per modificare qualsiasi valore di cancellazione, trovare la tabella **LoadParam** del database **ReportStore**.
4. Per aprire la tabella **LoadParam**, eseguire una delle seguenti operazioni:
 - Se si esegue SQL Server 2000, cliccare col tasto destro del mouse sulla tabella **LoadParam** e selezionare **Apri tabella > Tutte le righe**.
 - Se si esegue SQL Server 2005 o superiore, cliccare col tasto destro del mouse sulla tabella **LoadParam** e selezionare **Apri tabella**.
5. Per modificare il valore di cancellazione dei dati dell'audit, digitare un nuovo valore nella riga **auditStorePurgeDays**, nella colonna **paramValue**.
La cancellazione dei dati dell'audit viene disabilitata, se si imposta tale valore su **-1**.
6. Per modificare il valore dell'intervallo di rimozione dei dati relativo ai report correnti, digitare il nuovo valore nella riga **reportStorePurgeDays** della colonna **paramValue**.
7. Per modificare il valore dell'intervallo di rimozione dei dati relativo ai report archiviati, digitare il nuovo valore nella riga **reportStoreWHPurgeDays** della colonna **paramValue**.
Nota: il valore reportstoreWHPurgeDays deve superare sia quello reportStorePurgeDays che quello relativo all'intervallo di tempo di trasferimento dei dati.
8. Uscire da SQL Enterprise Manager o SQL Server Management Studio.

9.2 Calibrazione dei database di SQL e i log delle transazioni

L'installazione crea i database in modo tale che automaticamente le loro dimensioni aumentino, ma non diminuiscano, e che si aggiornino i dati statistici. Si consiglia di non modificare queste proprietà del database.

Per una prestazione del database al meglio delle sue possibilità, si consiglia di:

- calibrare i database ed i relativi log delle transazioni in modo tale che siano abbastanza ampi da non dover espandersi frequentemente.
- Impostare i database ed i relativi log delle transazioni in modo tale che aumentino di una dimensione predefinita e non in percentuale.

9.2.1 Indicazioni per le dimensioni del database

| Nome del database | Dimensioni di riferimento | Crescita fissa di riferimento |
|---|---|-------------------------------|
| ReportStore | .4 KB x (numero di profili nel criterio) x (numero di computer) | 500 MB |
| ReportStoreWH Nota: Per impostazione predefinita, la cancellazione dei valori dei dati avviene entro 30 giorni. | 1.5 KB x (numero di profili nel criterio) x (numero di computer) x (valore "purge data" in giorni) | 500 MB |
| PolicyStore | Per un'impresa che conta migliaia di utenti e un criterio che comprende meno di 100 applicazioni, impostare PolicyStore a 500 MB. | 100 MB |

9.2.2 Istruzioni per la calibrazione dei log di transazione

| Nome del log di transazione | Dimensioni di riferimento | Crescita fissa di riferimento |
|-----------------------------|-------------------------------------|-------------------------------|
| ReportStore | 500 MB | 100 MB |
| ReportStoreWH | 2 GB | 250 MB |
| PolicyStore | Mantenere la dimensione predefinita | 100 MB |

9.2.3 Modifica delle dimensioni del database SQL e del log delle transazioni (SQL Server 2000)

Per stabilire le dimensioni del database di SQL server e del log delle transazioni, consultare le sezioni [Indicazioni per le dimensioni del database](#) a pagina 26 e [Istruzioni per la calibrazione dei log di transazione](#) a pagina 26. Le seguenti istruzioni si riferiscono a SQL Server 2000.

1. Dal menu Start di SQL server, cliccare su **Microsoft SQL Server > Enterprise Manager** .
Si apre SQL Enterprise Manager.
2. Per calibrare il ReportStore, nella cartella dei database, cercare **ReportStore**, cliccarvi col tasto destro del mouse e selezionare **Proprietà**.

3. Cliccare sulla scheda **Data Files**.
4. Selezionare il campo **Space allocated (MB)** e digitare una dimensione appropriata per il ReportStore.
5. Selezionare il pulsante di opzione **In megabytes** e digitare la dimensione appropriata per l'aumento di dimensioni del file ReportStore.
6. Cliccare sulla scheda **Log di transazione**.
7. Selezionare il campo **Space allocated (MB)** e digitare una dimensione appropriata per il ReportStore.
8. Selezionare il pulsante di opzione **In megabytes** e digitare la dimensione appropriata per l'aumento di dimensioni del file ReportStore.
9. Cliccare su **OK**.
10. Ripetere i passaggi dal 2 al 9 per ReportStoreWH e PolicyStore.
11. Uscire da SQL Enterprise Manager.

9.2.4 Modifica delle dimensioni del database SQL e del log delle transazioni (SQL Server 2005 e superiore)

Per stabilire le dimensioni del database di SQL server e del log delle transazioni, consultare le sezioni [Indicazioni per le dimensioni del database](#) a pagina 26 e [Istruzioni per la calibrazione dei log di transazione](#) a pagina 26. Le seguenti istruzioni si riferiscono a SQL Server 2005 e superiore.

1. Dal menu Start di SQL server, cliccare su **Microsoft SQL Server (versione) > SQL Server Management Studio**.
2. Dalla finestra di dialogo SQL Server Management Studio, trovare il database **ReportStore** nella cartella Databases, cliccarvi col tasto destro del mouse e selezionare **Proprietà**.
3. Dalla finestra di dialogo Proprietà, selezionare **Files**.
4. Trovare il file **ReportStore_Data**, selezionare il campo **Initial Size (MB)** ed inserire una dimensione adeguata per il database.
5. Trovare il file **ReportStore_Log**, selezionare il campo **Initial Size (MB)** ed inserire una dimensione adeguata per il file di log.
6. Cliccare su **OK**.
7. Ripetere i passaggi dal 2 al 6 per ReportStoreWH e PolicyStore.
8. Uscire da SQL Server Management Studio.

9.3 Accesso a Compliance Manager

Il Compliance Manager fornisce una posizione centralizzata per la gestione di Sophos NAC Advanced. Il Compliance Manager viene installato come sito web predefinito nella seguente percorso: `<drive locale>\Inetpub\wwwroot\SophosNAC`.

Importante: Per consentire a Compliance Manager di visualizzare e salvare informazioni e grafici correttamente, è necessario:

- in Internet Explorer 7.x, aggiungere Compliance Manager ai siti web affidabili. Questa impostazione non è necessaria in Internet Explorer 7.x.

- Disattivare il blocco dei pop-up quando si accede a Compliance Manager.

Importante: Per consentire il corretto funzionamento di Sophos NAC Advanced tramite HTTPS, è necessario installare un certificato web per i componenti dell'interfaccia web, Policy, Reporting e Registration. I componenti possono condividere uno stesso certificato web. Se si crea un certificato web personalizzato, è necessario accertarsi che tutti i computer lo riconoscano come valido. Se si sta testando o valutando Sophos NAC Advanced con HTTPS disattivato, il certificato web non è necessario.

1. Aprire Internet Explorer.
2. Digitare il seguente indirizzo: `https://<indirizzo ip/nome DNS del server di Sophos>/SophosComplianceManager`. Viene visualizzata la pagina di logon di Compliance Manager.

Nota: Per disattivare HTTPS, consultare la sezione [Disattivazione di HTTPS per un test in ambienti non di produzione](#) a pagina 60. Una volta disattivato HTTPS, è possibile accedere a Compliance Manager utilizzando il seguente indirizzo: `http://<indirizzo ip/nome DNS del server di Sophos>/SophosComplianceManager`.

3. Digitare **Admin** nel campo **Account Name** e la password di propria scelta nel campo **Password**.
4. Cliccare su **OK**.

Nota:

- Memorizzare questa password dal momento che rappresenta l'unico accesso a Compliance Manager finché non vengono creati altri account utente.
- Quando si utilizza Compliance Manager, è necessario creare o utilizzare template di accesso, profili, gruppi e criteri predefiniti.

9.4 Configurazione di un archivio utenti esterno per accedere a Compliance Manager (operazione facoltativa)

Quando si creano account utenti per accedere a Compliance Manager, è possibile specificare che tali account utilizzano un archivio utenti esterno. Se questo archivio utenti è dello stesso tipo di quello utilizzato da Compliance Manager per l'autenticazione, non è richiesta alcuna configurazione aggiuntiva. Se gli account utenti di Compliance Manager sono diversi da quelli dei Compliance Agent, è necessaria la creazione di un criterio di richiesta di connessione.

Nota: Sophos collabora direttamente con le imprese in possesso di account utenti di Compliance Manager che utilizzano un tipo di archivio utenti diverso da quello degli utenti dell'agente. Tale collaborazione garantisce che la configurazione venga installata nel modo corretto.

9.4.1 Creazione di un criterio di richiesta di connessione ad un archivio utenti esterno (Windows Server 2003)

Se gli account utenti di Compliance Manager utilizzeranno tipi di archivio utenti diversi da quelli dei Compliance Agent, è necessario creare un criterio di richiesta di connessione separato

con un tipo di servizio amministrazione. Per prima cosa è necessario stabilire l'ordine di priorità per questo criterio di richiesta di connessione.

1. Dal menu Start del Compliance Application Server, cliccare su **Strumenti di amministrazione > Internet Authentication Service**.

Viene aperto IAS.

2. Cliccare due volte su **Elaborazione richiesta di connessione**.
3. Cliccare col tasto destro del mouse su **Criterio richiesta di connessione** e poi selezionare **Nuovo > Criterio richiesta di connessione**.

Viene visualizzata la finestra di dialogo della procedura guidata del nuovo criterio di richiesta di connessione.

4. Cliccare su **Avanti** per continuare.
5. Selezionare il pulsante di opzione **Criterio personalizzato**. Nel campo adeguato digitare il nome del criterio di richiesta di connessione. Cliccare su **Avanti** per continuare.
6. Cliccare su **Aggiungi** per specificare le condizioni del criterio appropriate.
7. Selezionare la condizione del criterio **Service-Type** e cliccare su **Aggiungi**.
8. Selezionare **Amministrazione** da **Tipi disponibili** e successivamente cliccare su **Aggiungi**. Cliccare su **OK** per continuare.
9. Cliccare su **Avanti** per continuare.
10. Cliccare su **Avanti** per continuare.
11. Verificare i dati relativi al criterio di richiesta di connessione e poi cliccare su **Fine**.

Per prima cosa è necessario stabilire l'ordine di priorità per questo criterio di richiesta di connessione. Per aumentare il livello di priorità del criterio, cliccare col tasto destro del mouse sul nome del criterio e selezionare **Sposta su**.

9.4.2 Creazione di un criterio di richiesta di connessione ad un archivio utenti esterno (Windows Server 2008)

Se gli account utenti di Compliance Manager utilizzeranno tipi di archivio utenti diversi da quelli dei Compliance Agent, è necessario creare un criterio di richiesta di connessione separato con un tipo di servizio amministrazione. Per prima cosa è necessario stabilire l'ordine di priorità per questo criterio di richiesta di connessione.

1. Dal menu Start di Compliance Application Server, cliccare su **Strumenti di amministrazione > Server dei criteri di rete**.

Viene avviato il Server dei criteri di rete.

2. In "Criteri", cliccare con il tasto destro del mouse su **Criterio richiesta di connessione**, e poi cliccare su **Nuovo**.

Viene visualizzata la finestra di dialogo della procedura guidata del nuovo criterio di richiesta di connessione.

3. Digitare un nome per il criterio, e lasciare come metodo di connessione alla rete **Non specificato**.
4. Cliccare su **Avanti** per continuare.

5. Cliccare su **Aggiungi** per specificare le condizioni del criterio appropriate.
6. Selezionare la condizione del criterio **Tipo di servizio** e cliccare su **Aggiungi**.
7. Selezionare **Amministrazione**, e cliccare su **OK**.
8. Cliccare su **Avanti** per continuare.
9. Nella sezione **Autenticazione**, selezionare il pulsante di opzione **Accetta utenti senza la convalida delle credenziali**.
10. Cliccare su **Avanti** per continuare.
11. Cliccare su **Avanti** per continuare. Non è necessario configurare attributi per questo criterio.
12. Verificare i dati relativi al criterio di richiesta di connessione e poi cliccare su **Fine**.
Per prima cosa è necessario stabilire l'ordine di priorità per questo criterio di richiesta di connessione. Per aumentare il livello di priorità del criterio, cliccare col tasto destro del mouse sul nome del criterio e selezionare **Sposta su**.

9.5 Impostazioni (Windows Server 2003) per il Servizio autenticazione Internet (IAS)

IAS viene utilizzato per la ricerca del gruppo, l'autenticazione e l'attuazione RADIUS.

La maggior parte delle implementazioni di Sophos NAC Advanced richiedono la ricerca del gruppo e l'autenticazione. Viene richiesto di:

- Fornire accesso IAS a Active Directory.

Nota: Per le implementazioni LDAP o se si sta utilizzando Sophos NAC Advanced come proxy RADIUS (configurando Sophos NAC Advanced in modalità proxy in presenza di un altro server RADIUS), **non** è richiesto il completamento di questa operazione.

- Creare il criterio di accesso remoto.

Se si esegue RADIUS Enforcement con VPN, 802.1x, Cisco NAC o implementazioni estese di RADIUS, è necessario:

- Fornire accesso IAS a Active Directory.
- Configurare il criterio di accesso remoto.
- Aggiungere i client RADIUS a tutti i dispositivi di accesso alla rete, quali i concentratori VPN.

9.5.1 Accesso IAS a Active Directory

Per impostazione predefinita, il servizio IAS può **non** essere in possesso delle autorizzazioni necessarie per l'autenticazione degli utenti di Active Directory. Il server IAS deve essere in possesso delle autorizzazioni necessarie per l'autenticazione degli utenti di Active Directory.

Importante:

- Per le implementazioni LDAP o se si sta utilizzando Sophos NAC Advanced come proxy RADIUS (configurando Sophos NAC Advanced in modalità proxy in presenza di un altro server RADIUS), **non** è richiesto il completamento di questa operazione.

- Nei Compliance Application Servers, oltre che in tutti i server RADIUS Enforcer, è necessario seguire le istruzioni qui riportate.
1. Accedere al Compliance Application Server o al server RADIUS Enforcer tramite un account con autorizzazioni di amministratore di dominio.
 2. Dal menu Start del Compliance Application Server o del server RADIUS Enforcer, cliccare su **Strumenti di amministrazione > Servizio autenticazione Internet** .
Viene aperto IAS.
 3. Cliccare col tasto destro del mouse su **Servizio autenticazione Internet** e selezionare **Registra server in Active Directory**.
 4. Cliccare su **Sì** per confermare l'accesso IAS a Active Directory.
Se IAS può accedere a Active Directory, si riceverà un messaggio di conferma. Non è richiesta nessun'altra operazione.
 5. Uscire da IAS.
 6. Ripetere questa procedura in tutti i Compliance Application Servers e quelli RADIUS Enforcer.

9.5.2 Configurazione del criterio di accesso remoto

Per la maggior parte delle implementazioni di Sophos NAC Advanced è necessario creare un criterio di accesso remoto. Questo documento fornisce informazioni riguardanti i criteri di accesso remoto più comunemente usati per i VPN. Sophos NAC Advanced Le implementazioni per LAN richiedono un criterio di accesso remoto per la ricerca e l'autenticazione del gruppo.

Importante:

- Se si sta utilizzando Sophos NAC Advanced come proxy RADIUS (configurando Sophos NAC Advanced in modalità proxy in presenza di un altro server RADIUS), **non** è richiesta la configurazione di criteri di accesso remoto.
 - Nei Compliance Application Servers, oltre che in tutti i server RADIUS Enforcer, è necessario seguire le istruzioni qui riportate.
1. Dal menu Start del Compliance Application Server o del server RADIUS Enforcer, cliccare su **Strumenti di amministrazione > Servizio autenticazione Internet** .
Viene aperto IAS.
 2. Cliccare su **Criteri di accesso remoto**.
 3. Cancellare i due criteri incorporati: connessioni ad altri server di accesso remoto e Connessioni al server Routing e Accesso remoto Microsoft. Cliccare col tasto destro del mouse sul nome di ciascun criterio e poi selezionare **Elimina**.
 4. Cliccare col tasto destro del mouse su **Criteri di accesso remoto** e poi selezionare **Nuovo criterio di accesso remoto**.
Viene visualizzata la finestra di dialogo della procedura guidata del nuovo criterio di accesso remoto.
 5. Cliccare su **Avanti** per continuare.

6. Cliccare sul pulsante di opzione **Imposta un criterio personalizzato**. Nel campo adeguato digitare il nome del criterio di accesso remoto. Per esempio, utilizzare Grant VPN Users Access come nome del criterio di accesso remoto. Cliccare su **Avanti** per continuare.
7. Cliccare su **Aggiungi** per specificare le condizioni del criterio appropriate.
8. Effettuare una delle seguenti operazioni:
 - se tutti gli utenti devono poter accedere, a prescindere dal gruppo di appartenenza, andare al passaggio successivo.
 - Se solo specifici gruppi di dominio devono poter accedere andare al passaggio 11.
9. Se l'accesso deve essere concesso a tutti gli utenti, a prescindere dal gruppo di appartenenza, selezionare la condizione del criterio **Day-And-Time Restrictions**. Cliccare su **Aggiungi**.

Nota: La condizione del criterio "Day-And-Time Restrictions" consente l'accesso a tutti gli utenti, mentre la condizione del criterio "Windows-Groups" consente di limitare l'accesso in base al dominio di appartenenza.
10. Selezionare il pulsante di opzione **Consentito** e cliccare su **OK**. Passare al punto 15.
11. Se l'accesso deve essere concesso solo a specifici gruppi di dominio e non a tutti gli utenti, selezionare la condizione del criterio **Windows-Groups**. Cliccare su **Aggiungi**.

Nota: la condizione del criterio "Windows-Groups" consente di limitare l'accesso in base al dominio di appartenenza, mentre quella "Day-And-Time Restrictions" permette l'accesso a tutti gli utenti.
12. Cliccare su **Aggiungi** per aggiungere i gruppi di dominio a cui applicare questo criterio di accesso remoto.
13. Digitare i nomi dei gruppi di dominio. Per esempio, DOCLAB\VPN Users è un valido gruppo di dominio. Cliccare su **OK**.

Ripetere i passaggi 12 e 13 per aggiungere ulteriori gruppi di dominio.
14. Cliccare su **OK** una volta indicati tutti i gruppi di dominio.

Nella finestra "Gruppi" vengono visualizzati tutti i gruppi di dominio aggiunti.
15. Cliccare su **Avanti** per continuare.

Nota: le condizioni del criterio visualizzate variano a seconda che si sia scelta la condizione del criterio "Day-And-Time Restrictions" o quella "Windows-Groups".
16. Cliccare sul pulsante di opzione **Consenti l'accesso remoto**. Cliccare su **Avanti** per continuare.
17. Cliccare su **Modifica profilo**.

18. Cliccare sulla scheda **Autenticazione**. Selezionare le caselle di spunta relative alle modalità di autenticazione appropriate. Cliccare su **OK**.

Nota:

- Per l'implementazione di LDAP, è necessario selezionare la casella di spunta "Autenticazione non crittografata (PAP, SPAP)".
- Se si seleziona la casella di spunta "Autenticazione crittografata (CHAP)" o "Autenticazione non crittografata (PAP, SPAP)", viene visualizzata una finestra di dialogo in cui si chiede se si desidera accedere alla guida in linea. Per continuare cliccare su **No**.

19. Cliccare sulla scheda **Avanzate**. Cliccare su **Aggiungi**.
20. Selezionare **Ignora le proprietà di composizione dell'utente** dall'elenco attributi. Cliccare su **Aggiungi**.
21. Selezionare il pulsante di opzione **True**. Cliccare su **OK**.
22. Cliccare su **Chiudi**. Cliccare su **OK**.
23. Cliccare su **Avanti** per continuare.
24. Verificare i dati relativi al criterio di accesso remoto e poi cliccare su **Fine**.

9.5.3 Disabilitazione del log IAS per la buona riuscita delle richieste di autenticazione (operazione facoltativa)

Per limitare il numero di messaggi del log eventi, Sophos consiglia di disabilitare il log per la riuscita delle richieste di autenticazione.

Nota: completare questa procedura in tutti i Compliance Application Servers e quelli RADIUS Enforcer.

1. Dal menu Start del Compliance Application Server o del server RADIUS Enforcer, cliccare su **Strumenti di amministrazione > Servizio autenticazione Internet**.

Viene aperto IAS.

2. Cliccare col tasto destro del mouse su **Servizio autenticazione Internet** e successivamente selezionare **Proprietà**.
3. Deselezionare la casella di spunta **Richiesta di autenticazione riuscita** e cliccare su **Applica**.
4. Uscire da IAS.
5. Ripetere questa procedura in tutti i Compliance Application Servers e quelli RADIUS Enforcer.

9.5.4 Aggiunta di client RADIUS per ogni dispositivo di accesso alla rete (operazione facoltativa)

Le seguenti istruzioni riguardano solo l'attuazione RADIUS. L'attuazione di RADIUS viene eseguita con VPN, 802.1x, Cisco NAC e implementazioni estese di RADIUS. Per ciascun concentratore VPN, è necessario aggiungere a IAS una voce relativa al client RADIUS. È necessario completare questa procedura in tutti i Compliance Application Servers e quelli RADIUS Enforcer.

1. Dal menu Start del Compliance Application Server o del server RADIUS Enforcer, cliccare su **Strumenti di amministrazione > Servizio autenticazione Internet**.

Viene aperto IAS.

2. Cliccare col tasto destro del mouse su **Client RADIUS** e selezionare **Nuovo client RADIUS**.

Viene visualizzata la finestra di dialogo "Nuovo client RADIUS".

3. Digitare il nome e l'indirizzo IP, o il nome DNS, utilizzato dal concentratore VPN per contattare il Compliance Application Server. Cliccare su **Avanti** per continuare.
4. Digitare e confermare il segreto condiviso (shared secret) del concentratore VPN nei campi appropriati. Lo shared secret è il medesimo utilizzato nella configurazione del concentratore VPN.

Nota: nell'elenco Fornitore client, lasciare selezionato RADIUS Standard.

5. Verificare che la casella **La richiesta deve contenere l'attributo autenticatore del messaggio non** sia spuntata.

6. Cliccare su **Fine**.

Ripetere questa procedura per tutti i concentratori VPN che si utilizzeranno con Sophos NAC Advanced. Ripetere questa procedura in tutti i Compliance Application Servers e quelli RADIUS Enforcer.

9.6 Impostazioni del Server dei criteri di rete (Windows Server 2008)

Il Server dei criteri di rete viene utilizzato per la ricerca del gruppo, l'autenticazione e l'attuazione RADIUS.

La maggior parte delle implementazioni di Sophos NAC Advanced richiedono la ricerca del gruppo e l'autenticazione. Viene richiesto di:

- Garantire al Server dei criteri di rete accesso ad Active Directory.

Nota: Per le implementazioni LDAP o se si sta utilizzando Sophos NAC Advanced come proxy RADIUS (configurando Sophos NAC Advanced in modalità proxy in presenza di un altro server RADIUS), **non** è richiesto il completamento di questa operazione.

- Creare un nuovo criterio di rete.

Se si esegue RADIUS Enforcement con VPN, 802.1x, Cisco NAC o implementazioni estese di RADIUS, è necessario:

- Garantire al Server dei criteri di rete accesso ad Active Directory.
- Configurare un nuovo criterio di rete.
- Aggiungere i client RADIUS a tutti i dispositivi di accesso alla rete, quali i concentratori VPN.

9.6.1 Come garantire al Server dei criteri di rete accesso ad Active Directory.

Per impostazione predefinita, il Server dei criteri di rete (Network Policy Server) può **non** essere in possesso delle autorizzazioni necessarie per l'autenticazione degli utenti di Active

Directory. Il Server dei criteri di rete deve essere in possesso delle autorizzazioni necessarie per l'autenticazione degli utenti di Active Directory.

Importante:

- Per le implementazioni LDAP o se si sta utilizzando Sophos NAC Advanced come proxy RADIUS (configurando Sophos NAC Advanced in modalità proxy in presenza di un altro server RADIUS), **non** è richiesto il completamento di questa operazione.
- Nei Compliance Application Servers, oltre che in tutti i server RADIUS Enforcer, è necessario seguire le istruzioni qui riportate.

1. Accedere al Compliance Application Server o al server RADIUS Enforcer tramite un account con autorizzazioni di amministratore di dominio.
2. Dal menu Start del Compliance Application Server o del server RADIUS Enforcer, cliccare su **Strumenti di amministrazione > Network Policy Server**.

Viene avviato il Server dei criteri di rete.

3. Cliccare col tasto destro del mouse su **NPS (Local)** e selezionare **Registra server in Active Directory**.
4. Cliccare su **OK** per confermare l'accesso del Server dei criteri di rete ad Active Directory.

Se il Server dei criteri di rete può accedere ad Active Directory, si riceverà un messaggio di conferma. Non è richiesta nessun'altra operazione.

5. Uscire da Network Policy Server.
6. Ripetere questa procedura in tutti i Compliance Application Servers e quelli RADIUS Enforcer.

9.6.2 Configurazione di un criterio di rete

Per la maggior parte delle implementazioni di Sophos NAC Advanced è necessario creare un criterio di rete. Questo documento fornisce informazioni riguardanti il criteri di rete più comunemente usato per VPN. Sophos NAC Advanced Le implementazioni per LAN richiedono un criterio rete per la ricerca e l'autenticazione del gruppo.

Importante:

- Se si sta utilizzando Sophos NAC Advanced come proxy RADIUS (configurando Sophos NAC Advanced in modalità proxy in presenza di un altro server RADIUS), **non** è richiesta la configurazione di criteri di rete.
- Nei Compliance Application Servers, oltre che in tutti i server RADIUS Enforcer, è necessario seguire le istruzioni qui riportate.

1. Dal menu Start del Compliance Application Server o del server RADIUS Enforcer, cliccare su **Strumenti di amministrazione > Network Policy Server**.

Viene avviato il Server dei criteri di rete.

2. In Criteri, cliccare su **Criteri di rete**.
3. Cancellare i due criteri incorporati: connessioni ad altri server di accesso e Connessioni al server Routing e Accesso remoto Microsoft. Cliccare col tasto destro del mouse sul nome di ciascun criterio e poi selezionare **Elimina**.

4. Cliccare col tasto destro del mouse su **Criteri di rete**, e poi selezionare **Nuovo**.
Viene visualizzata la procedura guidata per nuovi criteri di rete.
5. Digitare un nome per il criterio, e lasciare come metodo di connessione alla rete **Non specificato**. Per esempio, utilizzare Grant VPN Users Access come nome del criterio di rete. Cliccare su **Next** per continuare.
6. Cliccare su **Aggiungi** per specificare le condizioni del criterio appropriate.
7. Effettuare una delle seguenti operazioni:
 - se tutti gli utenti devono poter accedere, a prescindere dal gruppo di appartenenza, andare al passaggio successivo.
 - Se solo specifici gruppi di dominio devono poter accedere andare al passaggio 10.
8. Se l'accesso deve essere concesso a tutti gli utenti, a prescindere dal gruppo di appartenenza, selezionare la condizione del criterio **Day And Time Restrictions**. Cliccare su **Aggiungi**.
Nota: La condizione del criterio "Day And Time Restrictions" consente l'accesso a tutti gli utenti, mentre la condizione del criterio "Windows Groups" consente di limitare l'accesso in base al dominio di appartenenza.
9. Selezionare il pulsante di opzione **Consentito** e cliccare su **OK**. Passare al punto 14.
10. Se l'accesso deve essere concesso solo a specifici gruppi di dominio e non a tutti gli utenti, selezionare la condizione del criterio **Windows Groups**. Cliccare su **Aggiungi**.
Nota: la condizione del criterio "Windows Groups" consente di limitare l'accesso in base al dominio di appartenenza, mentre quella "Day And Time Restrictions" permette l'accesso a tutti gli utenti.
11. Cliccare su **Aggiungi gruppi** per aggiungere i gruppi di dominio a cui applicare questo criterio di rete.
12. Digitare i nomi dei gruppi di dominio. Per esempio, DOCLAB\VPN Users è un valido gruppo di dominio. Cliccare su **OK**.
Ripetere i passaggi 11 e 12 per aggiungere ulteriori gruppi di dominio.
13. Cliccare su **OK** una volta indicati tutti i gruppi di dominio.
Nella finestra "Windows Groups" vengono visualizzati tutti i gruppi di dominio aggiunti.
14. Cliccare su **Next** per continuare.
Nota: Le condizioni del criterio visualizzate variano a seconda che si sia scelta la condizione del criterio "Day And Time Restrictions" o quella "Windows Groups".
15. Cliccare il pulsante relativo all'opzione **Accesso consentito**. Cliccare su **Next** per continuare.

16. Selezionare le caselle di spunta relative alle adeguate modalità di autenticazione. Cliccare su **Next** per continuare.

Nota:

- Per l'implementazione di LDAP, è necessario selezionare la casella di spunta "Autenticazione non crittografata (PAP, SPAP)".
- Se si seleziona la casella di spunta "Autenticazione crittografata (CHAP)" o "Autenticazione non crittografata (PAP, SPAP)", viene visualizzata una finestra di dialogo in cui si chiede se si desidera accedere alla guida in linea. Per continuare cliccare su **No**.

17. Cliccare su **Next** per continuare. Non è necessario configurare limitazioni per questo criterio.
18. Cliccare su **Next** per continuare. Non è necessario configurare impostazioni aggiuntive per questo criterio.
19. Verificare i dati relativi al criterio di rete e poi cliccare su **Fine**.

9.6.3 Disabilitazione del log del Server dei criteri di rete, per la buona riuscita delle richieste di autenticazione (operazione facoltativa)

Per limitare il numero di messaggi del log eventi, Sophos consiglia di disabilitare il log per la riuscita delle richieste di autenticazione.

Nota: completare questa procedura in tutti i Compliance Application Servers e quelli RADIUS Enforcer.

1. Dal menu Start del Compliance Application Server o del server RADIUS Enforcer, cliccare su **Strumenti di amministrazione > Network Policy Server** .
Viene avviato il Server dei criteri di rete.
2. Con il tasto destro del mouse, cliccare su **NPS (Local)**, e selezionare **Proprietà**.
3. Deselezionare la casella di spunta **Richiesta di autenticazione riuscita** e cliccare su **Applica**.
4. Uscire da Network Policy Server.
5. Ripetere questa procedura in tutti i Compliance Application Servers e quelli RADIUS Enforcer.

9.6.4 Aggiunta di client RADIUS per ogni dispositivo di accesso alla rete (operazione facoltativa)

Le seguenti istruzioni riguardano solo l'attuazione RADIUS. L'attuazione di RADIUS viene eseguita con VPN, 802.1x, Cisco NAC e implementazioni estese di RADIUS. Per ciascun concentratore VPN, è necessario aggiungere al Server dei criteri di rete una voce relativa al client RADIUS. È necessario completare questa procedura in tutti i Compliance Application Servers e quelli RADIUS Enforcer.

1. Dal menu Start del Compliance Application Server o del server RADIUS Enforcer, cliccare su **Strumenti di amministrazione > Network Policy Server** .
Viene avviato il Server dei criteri di rete.

2. In "RADIUS Clients and Servers", cliccare con il tasto destro del mouse su **Client RADIUS**, e successivamente selezionare **Nuovo client RADIUS**.

Viene visualizzata la finestra di dialogo "Nuovo client RADIUS".

3. Digitare il nome e l'indirizzo IP, o il nome DNS, utilizzato dal concentratore VPN per contattare il Compliance Application Server. Cliccare su **Next** per continuare.
4. Digitare e confermare il segreto condiviso (shared secret) del concentratore VPN nei campi appropriati. Lo shared secret è il medesimo utilizzato nella configurazione del concentratore VPN.

Nota: nell'elenco Nome fornitore, lasciare selezionato RADIUS Standard.

5. Verificare che la casella **I messaggi di richiesta di accesso devono contenere l'attributo autenticatore del messaggio non** sia spuntata.
6. Cliccare su **OK**.

Ripetere questa procedura per tutti i concentratori VPN che si utilizzeranno con Sophos NAC Advanced. Ripetere questa procedura in tutti i Compliance Application Servers e quelli RADIUS Enforcer.

9.7 Sophos NAC Advanced come proxy RADIUS (Windows Server 2003) (operazione facoltativa)

Per utilizzare Sophos NAC Advanced come proxy RADIUS (configurando Sophos NAC Advanced in modalità proxy in presenza di un altro server RADIUS), è necessario apportare modifiche alla configurazione di IAS. L'utilizzo di Sophos NAC Advanced come proxy RADIUS non richiede la creazione di un criterio di accesso remoto. È invece necessario creare un criterio di richiesta di connessione ed utilizzare il gruppo RADIUS server remoto.

Nota: Nei Compliance Application Servers, oltre che in tutti i server RADIUS Enforcer, è necessario seguire le istruzioni qui riportate.

9.7.1 Aggiunta di un gruppo di server di accesso remoto

1. Dal menu Start del Compliance Application Server o del server RADIUS Enforcer, cliccare su **Strumenti di amministrazione > Servizio autenticazione Internet**.

Viene aperto IAS.

2. Selezionare **Elaborazione richiesta di connessione**.
3. Cliccare col tasto destro del mouse su **Gruppi di server RADIUS remoti** e selezionare **Nuovo gruppo server RADIUS remoto**.

Viene visualizzata la finestra di dialogo della procedura guidata del nuovo gruppo RADIUS server remoto.

4. Cliccare su **Avanti** per continuare.
5. Selezionare il pulsante di opzione **Tipico** e quindi digitare il nome del gruppo di server nel campo adeguato.
6. Cliccare su **Avanti** per continuare.

7. Digitare l'indirizzo IP del server primario RADIUS remoto nel campo a disposizione.
8. Digitare l'indirizzo IP del RADIUS server remoto di back up o deselegionare la casella di spunta **Imposta un server di backup per il gruppo**.
9. Digitare e confermare il segreto condiviso (shared secret) del gruppo di server.
10. Cliccare su **Avanti** per continuare.
11. Verificare che la casella di spunta **Avvia Creazione guidata nuovo criterio richiesta di connessione alla chiusura di questa procedura guidata** sia selezionata.
12. Verificare i dati relativi al gruppo di RADIUS server remoti e quindi cliccare su **Fine**.
13. Visitare la pagina web [Creazione di un criterio di richiesta di connessione](#) a pagina 39.

9.7.2 Creazione di un criterio di richiesta di connessione

Quando si utilizza Sophos NAC Advanced come proxy RADIUS è necessario creare un criterio di richiesta di connessione.

1. Effettuare una delle seguenti operazioni:
 - Se si è avviata la procedura guidata da [Aggiunta di un gruppo di server di accesso remoto](#) a pagina 38, andare al passaggio successivo.
 - Dal menu Start del Compliance Application Server o del server RADIUS Enforcer, cliccare su **Strumenti di amministrazione > Servizio autenticazione Internet** . Viene aperto IAS. Cliccare due volte su **Elaborazione richiesta di connessione**. Cliccare col tasto destro del mouse su **Criterio richiesta di connessione** e poi selezionare **Nuovo > Criterio richiesta di connessione** .

Viene visualizzata la finestra di dialogo della procedura guidata del nuovo criterio di richiesta di connessione.

2. Cliccare su **Avanti** per continuare.
3. Selezionare il pulsante di opzione **Criterio tipico per scenari comuni**.
4. Digitare un nome per il criterio di richiesta di connessione.
5. Cliccare su **Avanti** per continuare.
6. Selezionare il pulsante di opzione **Inoltre le richieste di connessione a un server RADIUS remoto per l'autenticazione**.
7. Cliccare su **Avanti** per continuare.
8. Digitare il nome/i di proxy o un carattere jolly .* per tutti i proxy.
9. Deselezionare la casella di spunta **Prima dell'autenticazione, rimuovi il nome area autenticazione dal nome utente**.
10. Selezionare dall'elenco il gruppo di server creato.
11. Cliccare su **Avanti** per continuare.
12. Cliccare su **Fine**.
13. Visitare la pagina web [Verifica delle condizioni del criterio](#) a pagina 40.

9.7.3 Verifica delle condizioni del criterio

1. In IAS, nell'elenco "Criteri richiesta di connessione", cliccare col tasto destro del mouse sul criterio appena creato e selezionare **Proprietà**.

Viene visualizzata la finestra Proprietà.

2. Verificare le condizioni del criterio relative al criterio appena creato.
3. Se errate o incomplete, cliccare su **Aggiungi** o **Modifica** per modificarle.

Nota: se è necessario creare una condizione del criterio per tutti gli utenti di proxy, è possibile utilizzare l'orario come condizione ed impostarla su 24x7.

4. Cliccare su **OK**.
5. Andare alla sezione *Modifica delle porte di autenticazione e di accounting di RADIUS* a pagina 40.

9.7.4 Modifica delle porte di autenticazione e di accounting di RADIUS

Le impostazioni predefinite relative alle porte di autenticazione e di accounting di RADIUS sono impostate su 1812 e 1813. Se si utilizzano altre porte di autenticazione e di accounting, questi valori devono essere cambiati.

Nota: la porta di autenticazione più comunemente utilizzata è la 1645, mentre quella di accounting è la 1646.

1. Nell'elenco relativo al gruppo RADIUS Server remoto in IAS, cliccare col tasto destro del mouse sul gruppo di server appena creato e successivamente selezionare **Proprietà**.

Viene visualizzata la finestra Proprietà.

2. Selezionare il primo server che compare nell'elenco dei server aggiunto a questo gruppo e cliccare su **Proprietà**.
3. Cliccare sulla scheda **Autenticazione/Accounting**.
4. Modificare la porta di autenticazione, lo shared secret e la porta di accounting a seconda delle esigenze.

Nota: la porta di autenticazione più comunemente utilizzata è la 1645, mentre quella di accounting è la 1646.

5. Ripetere i passaggi dal 2 al 5 per impostare le porte di autenticazione e accounting dei server aggiunti al gruppo di server.
6. Cliccare su **OK**.
7. Andare alla sezione *Cambio del protocollo di autenticazione delle registrazioni nell'interfaccia di registrazione* a pagina 41.

9.7.5 Cambio del protocollo di autenticazione delle registrazioni nell'interfaccia di registrazione

Sophos NAC Advanced utilizza MSchapV2 RADIUS come protocollo di autenticazione predefinito. Se non coincide col protocollo di autenticazione utilizzato dal RADIUS server, è necessario cambiare quello di RADIUS utilizzando l'interfaccia di registrazione.

1. Trovare il file Web.config dell'interfaccia di registrazione nel Compliance Application Server oppure nel server RADIUS Enforcer. Se il software Sophos NAC Advanced è stato installato nella posizione predefinita, il file è reperibile in: `<unità locale>\inetpub\wwwroot\RegistrationInterface\web.config`.
2. Aprire il file Web.config nel Blocco note.
3. Trovare la sezione **authInterface** e la sottosezione **radius**.
4. Cambiare il valore **mschapv2** presente in questa riga `<add key="authType" value="mschapv2" />` con quello del protocollo di autenticazione RADIUS utilizzato dal RADIUS server remoto.

La sottosezione radius modificata del file Web.config nell'interfaccia di configurazione è:

```
<radius>
<add key="authType" value="protocollo di autenticazione RADIUS
remoto" /> <add key="serverRetries" value="1" /> <add
key="listRetries" value="1" /> </radius>
```

5. Salvare e chiudere il file.
6. In alternativa, andare alla sezione [Configurazione del server RADIUS per i mapping/profili di gruppo \(operazione facoltativa\)](#) a pagina 41.

9.7.6 Configurazione del server RADIUS per i mapping/profili di gruppo (operazione facoltativa)

È possibile utilizzare Sophos NAC Advanced o il RADIUS server per il mapping di gruppo. Entrambe le configurazioni richiedono la creazione dei gruppi tramite Sophos NAC Advanced. Per ulteriori informazioni, consultare la Guida in linea di Compliance Manager.

Per utilizzare i mapping/profili di gruppo di RADIUS server con Sophos NAC Advanced, è necessario inviare i dati relativi al gruppo tramite un pacchetto RADIUS a Sophos NAC Advanced utilizzando un VSA. Per ulteriori informazioni, consultare la documentazione utente di RADIUS su come recuperare un VSA.

Sophos Vendor-Specific Attribute (VSA)

La sintassi del VSA si basa sulle linee guida descritte alla sezione 5.26 del documento (URL RFC2685) "Remote Authentication Dial In User Service (RADIUS)" (inglese), reperito in Internet all'indirizzo <http://www.rfc-archive.org/getrfc.php?rfc=2865>.

Sophos Vendor ID

La Vendor-Id identifica il produttore. La Vendor ID di Sophos è 5428 (decimale), o 0x00001534 (esadecimale, nell'ordine della rete).

EF-GroupID VSA

EF-GroupID VSA indica quale gruppo viene utilizzato per l'attuazione delle impostazioni della sessione per un utente autenticato.

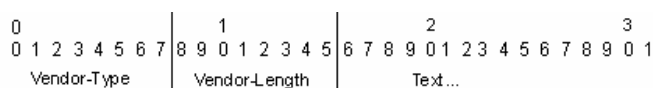
I modelli di accesso del RADIUS Enforcer stabiliscono l'accesso alla rete; le esenzioni sono però le prime ad essere prese in considerazione. Quando la richiesta è esentata, l'accesso alla rete viene consentito a prescindere dal gruppo di appartenenza. La seguente tabella descrive i casi in cui un criterio predefinito è o non è specificato in Compliance Manager:

| Esempi | Criterio predefinito specificato | Criterio predefinito non specificato |
|--|---|--|
| EF-GroupID VSA non presente | Il criterio predefinito è applicato. L'accesso alla rete viene consentito quando un modello di accesso di RADIUS Enforcer coincide con la richiesta. I modelli di accesso di RADIUS Enforcer abbinati al criterio vengono valutati per primi. Se non viene rilevata alcuna corrispondenza, vengono valutati i modelli di accesso predefiniti di RADIUS Enforcer. Se non viene rilevata alcuna corrispondenza, non viene concesso l'accesso alla rete. | L'utente non riceve alcun criterio. L'accesso alla rete viene consentito quando un modello di accesso di RADIUS Enforcer coincide con la richiesta. I modelli di accesso predefiniti di RADIUS Enforcer vengono valutati per primi. Se non viene rilevata alcuna corrispondenza, non viene concesso l'accesso alla rete. |
| EF-GroupID VSA non esistente o non definito. | Il criterio predefinito è applicato. L'accesso alla rete viene consentito quando un modello di accesso di RADIUS Enforcer coincide con la richiesta. I modelli di accesso di RADIUS Enforcer abbinati al criterio vengono valutati per primi. Se non viene rilevata alcuna corrispondenza, vengono valutati i modelli di accesso predefiniti di RADIUS Enforcer. Se non viene rilevata alcuna corrispondenza, non viene concesso l'accesso alla rete. | L'utente non riceve alcun criterio. L'accesso alla rete viene consentito quando un modello di accesso di RADIUS Enforcer coincide con la richiesta. I modelli di accesso predefiniti di RADIUS Enforcer vengono valutati per primi. Se non viene rilevata alcuna corrispondenza, non viene concesso l'accesso alla rete. |
| EF-GroupID VSA non valido | L'utente viene posizionato in un gruppo specifico e gli viene applicato il relativo criterio. L'accesso alla rete viene consentito quando un modello di accesso di RADIUS Enforcer coincide con la richiesta. I modelli di accesso di RADIUS Enforcer abbinati al criterio vengono valutati per primi. Se non viene rilevata alcuna | L'utente viene posizionato in un gruppo specifico e gli viene applicato il relativo criterio. L'accesso alla rete viene consentito quando un modello di accesso di RADIUS Enforcer coincide con la richiesta. I modelli di accesso di RADIUS Enforcer abbinati al criterio vengono valutati per primi. Se non viene rilevata alcuna corrispondenza, vengono valutati i |

| Esempi | Criterio predefinito specificato | Criterio predefinito non specificato |
|--------|--|---|
| | corrispondenza, vengono valutati i modelli di accesso predefiniti di RADIUS Enforcer. Se non viene rilevata alcuna corrispondenza, non viene concesso l'accesso alla rete. | modelli di accesso predefiniti di RADIUS Enforcer. Se non viene rilevata alcuna corrispondenza, non viene concesso l'accesso alla rete. |

EF-GroupID VSA Format

Il formato dei dati relativi al valore EF-GroupID VSA viene mostrato nel diagramma e nella tabella sottostanti. I campi vengono trasmessi da sinistra a destra.



| Vendor-Type | Vendor-Length | Text |
|---------------------------------------|---------------|--|
| 20 (14 esadecimale) per EF-User-Group | >2 | <p>Questo campo di testo è costituito da uno o più ottetti di caratteri leggibili. Non deve essere a terminazione null. Il valore contenuto in questo campo di testo rappresenta un determinato gruppo utenti relativo alla sessione degli utenti autenticati.</p> <p>Parametri di testo relativi all'ID del gruppo utenti:</p> <ul style="list-style-type: none"> ■ massimo 253 caratteri, che possono contenere una combinazione di numeri e lettere. Non è permesso l'utilizzo di nessun altro tipo di carattere. ■ Distingue fra maiuscole e minuscole. ■ Non è consentito l'utilizzo di spazi. |

Esempio relativo a EF-User-Group VSA

Se per esempio il VSA è impostato su EF-User-Group = "WestCoastSales", sarà formato dai numeri esadecimali (ordine della rete) descritti nella tabella seguente:

| Descrizione | Numeri esadecimali |
|---------------------------------------|--------------------|
| Informazioni sull'intestazione | |

| Descrizione | Numeri esadecimali |
|--|---|
| Tipo: RADIUS attributo 26 (dec) | 1A |
| Lunghezza: Inclusi i byte relativi al tipo e alla lunghezza | 16 |
| L'MSB del Vendor-ID è sempre 00 | 00 |
| Sophos Vendor ID | 00 15 34 |
| Vendor-Type: EF-User-Group | 14 |
| Dati relativi al valore | |
| Vendor-Length: Inclusi i byte relativi a Vendor Type e Vendor-Length | 0E |
| Testo: "WestCoastSales" (no virgolette) | 57 65 73 74 43 6F 61 73 74 53 61 6C 65 73 |

9.8 Sophos NAC Advanced come proxy RADIUS (Windows Server 2008) (operazione facoltativa)

Per utilizzare Sophos NAC Advanced come proxy RADIUS (configurando Sophos NAC Advanced in modalità proxy in presenza di un altro server RADIUS), è necessario apportare modifiche alla configurazione del Server dei criteri di rete. L'utilizzo di Sophos NAC Advanced come proxy RADIUS non richiede la creazione di un criterio di rete. È invece necessario creare un criterio di richiesta di connessione ed utilizzare il gruppo RADIUS server remoto.

Nota: Nei Compliance Application Servers, oltre che in tutti i server RADIUS Enforcer, è necessario seguire le istruzioni qui riportate.

9.8.1 Aggiunta di un gruppo di server di accesso remoto

1. Dal menu Start del Compliance Application Server o del server RADIUS Enforcer, cliccare su **Strumenti di amministrazione > Network Policy Server**.

Viene avviato il Server dei criteri di rete.

2. In "Client e Server RADIUS", cliccare con il tasto destro del mouse su **Gruppi di RADIUS server remoti**, e selezionare **Nuovo**.

Viene visualizzata la finestra di dialogo "Nuovo gruppo di RADIUS server remoti".

3. Digitare un nome di gruppo server nell'apposito campo.
4. Cliccare su **Aggiungi**.
5. Digitare l'indirizzo IP del RADIUS server remoto nel campo a disposizione.
6. Cliccare sulla scheda **Autenticazione/Accounting**.
7. Digitare e confermare lo shared secret RADIUS negli appositi campi.

8. Modificare la porta di autenticazione e la porta di accounting a seconda delle esigenze.
Nota: In RADIUS, le porte di autenticazione e accounting predefinite sono la 1812 e la 1813. Se si utilizzano altre porte di autenticazione e di accounting, questi valori devono essere cambiati. la porta di autenticazione più comunemente utilizzata è la 1645, mentre quella di accounting è la 1646.
9. Cliccare sulla scheda **Bilanciamento dei carichi**.
10. Impostare la priorità del proprio RADIUS server remoto nell'apposito campo.
11. Cliccare su **OK**.
12. Ripetere i punti 4 - 11 per creare altri server RADIUS per lo stesso gruppo.
13. Verificare i dati relativi al gruppo di RADIUS server remoti e quindi cliccare su **OK**.
14. Visitare la pagina web [Creazione di un criterio di richiesta di connessione](#) a pagina 45.

9.8.2 Creazione di un criterio di richiesta di connessione

Quando si utilizza Sophos NAC Advanced come proxy RADIUS è necessario creare un criterio di richiesta di connessione.

1. Dal menu Start del Compliance Application Server o del server RADIUS Enforcer, cliccare su **Strumenti di amministrazione > Network Policy Server** .
Viene avviato il Server dei criteri di rete.
2. In "Criteri", cliccare con il tasto destro del mouse su **Criterio richiesta di connessione**, e poi cliccare su **Nuovo** .
Viene visualizzata la finestra di dialogo della procedura guidata del nuovo criterio di richiesta di connessione.
3. Digitare un nome per il criterio, e lasciare come metodo di connessione alla rete **Non specificato**.
4. Cliccare su **Avanti** per continuare.
5. Cliccare su **Aggiungi** per specificare le condizioni del criterio appropriate.
6. Selezionare l'adeguata condizione e poi cliccare su **Aggiungi**.
7. Specificare il valore della condizione, e successivamente cliccare su **OK**.
Nota: Ad esempio, è possibile selezionare "Nome Utente" nella fase precedente, e specificare che contiene "mydomain.com" in questa fase.
8. Cliccare su **Avanti** per continuare.
9. Nella sezione **Autenticazione**, selezionare il pulsante di opzione **Inoltre le richieste a un server RADIUS remoto per l'autenticazione**.
10. Selezionare dall'elenco il gruppo di server RADIUS creato.
11. Cliccare su **Avanti** per continuare.
12. Nella sezione **Attributo**, sotto **Specifica il nome di un'area**, selezionare dall'elenco **Nome-Utente**, e cliccare su **Aggiungi**.
13. Nel campo **Trova**, digitare il nome/i di proxy o un carattere jolly .* per tutti i proxy..
14. Lasciare vuoto il campo **Sostituisci con**.

15. Cliccare su **OK**.
16. Cliccare su **Avanti** per continuare.
17. Cliccare su **Fine**.
18. Visitare la pagina web [Verifica delle condizioni del criterio](#) a pagina 46.

9.8.3 Verifica delle condizioni del criterio

1. In "Server dei criteri di rete", sotto "Criteri", cliccare su **Criterio richiesta di connessione**. Nell'elenco dei criteri, cliccare con il tasto destro del mouse sul criterio appena creato, e selezionare **Proprietà**.

Viene visualizzata la finestra "Proprietà".

2. Cliccare sulla scheda **Condizioni** per rivedere le condizioni del criterio creato.
3. Se errate o incomplete, cliccare su **Aggiungi** o **Modifica** per modificarle.

Nota: Se è necessario creare una condizione di criterio per utilizzare il proxy con tutti gli utenti, è possibile aggiungere una condizione di limitazione data e orario, ed impostarla su 24x7.

4. Cliccare su **OK**.
5. Andare alla sezione [Cambio del protocollo di autenticazione delle registrazioni nell'interfaccia di registrazione](#) a pagina 46.

9.8.4 Cambio del protocollo di autenticazione delle registrazioni nell'interfaccia di registrazione

Sophos NAC Advanced utilizza MSchapV2 RADIUS come protocollo di autenticazione predefinito. Se non coincide col protocollo di autenticazione utilizzato dal RADIUS server, è necessario cambiare quello di RADIUS utilizzando l'interfaccia di registrazione.

1. Trovare il file Web.config dell'interfaccia di registrazione nel Compliance Application Server oppure nel server RADIUS Enforcer. Se il software Sophos NAC Advanced è stato installato nella posizione predefinita, il file è reperibile in: *<unità locale>\inetpub\wwwroot\RegistrationInterface\web.config*.
2. Aprire il file Web.config nel Blocco note.
3. Trovare la sezione **authInterface** e la sottosezione **radius**.
4. Cambiare il valore **mschapv2** presente in questa riga `<add key="authType" value="mschapv2" />` con quello del protocollo di autenticazione RADIUS utilizzato dal RADIUS server remoto.

La sottosezione radius modificata del file Web.config nell'interfaccia di configurazione è:

```
<radius>

<add key="authType" value="protocollo di autenticazione RADIUS
remoto"/> <add key="serverRetries" value="1"/> <add
key="listRetries" value="1"/> </radius>
```

5. Salvare e chiudere il file.
6. In alternativa, andare alla sezione *Configurazione del server RADIUS per i mapping/profilo di gruppo (operazione facoltativa)* a pagina 47.

9.8.5 Configurazione del server RADIUS per i mapping/profilo di gruppo (operazione facoltativa)

È possibile utilizzare Sophos NAC Advanced o il RADIUS server per il mapping di gruppo. Entrambe le configurazioni richiedono la creazione dei gruppi tramite Sophos NAC Advanced. Per ulteriori informazioni, consultare la Guida in linea di Compliance Manager.

Per utilizzare i mapping/profilo di gruppo di RADIUS server con Sophos NAC Advanced, è necessario inviare i dati relativi al gruppo tramite un pacchetto RADIUS a Sophos NAC Advanced utilizzando un VSA. Per ulteriori informazioni, consultare la documentazione utente di RADIUS su come recuperare un VSA.

Sophos Vendor-Specific Attribute (VSA)

La sintassi del VSA si basa sulle linee guida descritte alla sezione 5.26 del documento (URL RFC2685) "Remote Authentication Dial In User Service (RADIUS)" (inglese), reperito in Internet all'indirizzo <http://www.rfc-archive.org/getrfc.php?rfc=2865>.

Sophos Vendor ID

La Vendor-Id identifica il produttore. La Vendor ID di Sophos è 5428 (decimale), o 0x00001534 (esadecimale, nell'ordine della rete).

EF-GroupID VSA

EF-GroupID VSA indica quale gruppo viene utilizzato per l'attuazione delle impostazioni della sessione per un utente autenticato.

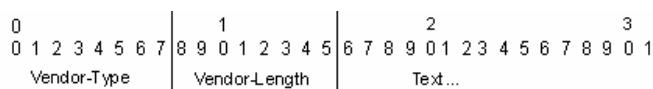
I modelli di accesso del RADIUS Enforcer stabiliscono l'accesso alla rete; le esenzioni sono però le prime ad essere prese in considerazione. Quando la richiesta è esentata, l'accesso alla rete viene consentito a prescindere dal gruppo di appartenenza. La seguente tabella descrive i casi in cui un criterio predefinito è o non è specificato in Compliance Manager:

| Esempi | Criterio predefinito specificato | Criterio predefinito non specificato |
|------------------------------------|---|--|
| EF-GroupID VSA non presente | Il criterio predefinito è applicato. L'accesso alla rete viene consentito quando un modello di accesso di RADIUS Enforcer coincide con la richiesta. I modelli di accesso di RADIUS Enforcer abbinati al criterio vengono valutati per primi. Se non viene rilevata alcuna corrispondenza, vengono valutati i modelli di accesso predefiniti di RADIUS Enforcer. Se non viene rilevata alcuna corrispondenza, non viene concesso l'accesso alla rete. | L'utente non riceve alcun criterio. L'accesso alla rete viene consentito quando un modello di accesso di RADIUS Enforcer coincide con la richiesta. I modelli di accesso predefiniti di RADIUS Enforcer vengono valutati per primi. Se non viene rilevata alcuna corrispondenza, non viene concesso l'accesso alla rete. |

| Esempi | Criterio predefinito specificato | Criterio predefinito non specificato |
|--|--|--|
| EF-GroupID VSA non esistente o non definito. | Il criterio predefinito è applicato. L'accesso alla rete viene consentito quando un modello di accesso di RADIUS Enforcer coincide con la richiesta. I modelli di accesso di RADIUS Enforcer abbinati al criterio vengono valutati per primi. Se non viene rilevata alcuna corrispondenza, vengono valutati i modelli di accesso predefiniti di RADIUS Enforcer. Se non viene rilevata alcuna corrispondenza, non viene concesso l'accesso alla rete. | L'utente non riceve alcun criterio. L'accesso alla rete viene consentito quando un modello di accesso di RADIUS Enforcer coincide con la richiesta. I modelli di accesso predefiniti di RADIUS Enforcer vengono valutati per primi. Se non viene rilevata alcuna corrispondenza, non viene concesso l'accesso alla rete. |
| EF-GroupID VSA non valido | L'utente viene posizionato in un gruppo specifico e gli viene applicato il relativo criterio. L'accesso alla rete viene consentito quando un modello di accesso di RADIUS Enforcer coincide con la richiesta. I modelli di accesso di RADIUS Enforcer abbinati al criterio vengono valutati per primi. Se non viene rilevata alcuna corrispondenza, vengono valutati i modelli di accesso predefiniti di RADIUS Enforcer. Se non viene rilevata alcuna corrispondenza, non viene concesso l'accesso alla rete. | L'utente viene posizionato in un gruppo specifico e gli viene applicato il relativo criterio. L'accesso alla rete viene consentito quando un modello di accesso di RADIUS Enforcer coincide con la richiesta. I modelli di accesso di RADIUS Enforcer abbinati al criterio vengono valutati per primi. Se non viene rilevata alcuna corrispondenza, vengono valutati i modelli di accesso predefiniti di RADIUS Enforcer. Se non viene rilevata alcuna corrispondenza, non viene concesso l'accesso alla rete. |

EF-GroupID VSA Format

Il formato dei dati relativi al valore EF-GroupID VSA viene mostrato nel diagramma e nella tabella sottostanti. I campi vengono trasmessi da sinistra a destra.



| Vendor-Type | Vendor-Length | Text |
|---------------------------------------|---------------|---|
| 20 (14 esadecimale) per EF-User-Group | >2 | Questo campo di testo è costituito da uno o più ottetti di caratteri leggibili. Non deve essere a terminazione null. Il valore contenuto in questo campo di |

| Vendor-Type | Vendor-Length | Text |
|-------------|---------------|--|
| | | <p>testo rappresenta un determinato gruppo utenti relativo alla sessione degli utenti autenticati.</p> <p>Parametri di testo relativi all'ID del gruppo utenti:</p> <ul style="list-style-type: none"> ■ massimo 253 caratteri, che possono contenere una combinazione di numeri e lettere. Non è permesso l'utilizzo di nessun altro tipo di carattere. ■ Distingue fra maiuscole e minuscole. ■ Non è consentito l'utilizzo di spazi. |

Esempio relativo a EF-User-Group VSA

Se per esempio il VSA è impostato su EF-User-Group = "WestCoastSales", sarà formato dai numeri esadecimali (ordine della rete) descritti nella tabella seguente:

| Descrizione | Numeri esadecimali |
|--|---|
| Informazioni sull'intestazione | |
| Tipo: RADIUS attributo 26 (dec) | 1A |
| Lunghezza: Inclusi i byte relativi al tipo e alla lunghezza | 16 |
| L'MSB del Vendor-ID è sempre 00 | 00 |
| Sophos Vendor ID | 00 15 34 |
| Vendor-Type: EF-User-Group | 14 |
| Dati relativi al valore | |
| Vendor-Length: Inclusi i byte relativi a Vendor Type e Vendor-Length | 0E |
| Testo: "WestCoastSales" (no virgolette) | 57 65 73 74 43 6F 61 73 74 53 61 6C 65 73 |

9.9 Configurazione di Compliance Application Server multipli (operazione opzionale)

I Compliance Application Servers multipli consentono la scalabilità di Sophos NAC Advanced . I Compliance Application Servers aggiuntivi devono essere installati e configurati adeguatamente, in modo tale da essere identici al Compliance Application Server primario.

In LDAP, per poter riutilizzare un file di configurazione in più server, è necessario utilizzare il tool Password Encryption che consente di aggiornare e criptare la password in ogni server. La cifratura della password dipende dal server.

Le seguenti operazioni sono obbligatorie quando sono presenti più Compliance Application Servers:

- Esportazione e importazione della chiave del server in Compliance Application Servers aggiuntivi. Per ulteriori informazioni, consultare la sezione [Esportazione e importazione della chiave del server in Compliance Application Server aggiuntivi](#) a pagina 50.
- Configurare DNS Round Robin in Microsoft Windows[®] Server 2003 se altri software o applicazioni di bilanciamento del carico non sono in utilizzo. Per ulteriori informazioni, consultare la sezione [Configurazione di DNS Round Robin in Windows Server 2003 e superiore](#) a pagina 50.

9.9.1 Esportazione e importazione della chiave del server in Compliance Application Server aggiuntivi

Nel caso di Compliance Application Servers multipli viene richiesto che le coppie di chiavi pubblica/privata di tutti i Compliance Application Servers siano sincronizzate. Per ulteriori informazioni, consultare la Compliance Manager di Guida in linea.

1. Nel Compliance Application Server primario, accedere a Compliance Manager.
2. Cliccare su **Configure System > Server Key**.
3. Esportare la coppia di chiavi pubblica/privata
4. In un altro Compliance Application Server, accedere a Compliance Manager e cliccare su **Configure System > Server Key**.
5. Esportare la coppia di chiavi pubblica/privata
6. Ripetere i passaggi 4-5 per tutti i Compliance Application Servers.

9.9.2 Configurazione di DNS Round Robin in Windows Server 2003 e superiore

La configurazione di DNS round robin in Microsoft Windows Server 2003 o superiore consente il bilanciamento della valutazione dei computer in vari server conservando un unico insieme di gruppi, criteri e applicazioni all'interno di Sophos NAC Advanced. DNS round robin è una funzione di bilanciamento del carico dei server DNS che consente a server multipli di distribuire le risorse. Questa sezione fornisce un semplice esempio relativo alla configurazione della funzione round robin del Domain Name Service (DNS) di Microsoft Windows Server. Anche altri server di nome di dominio che supportano round robin operano in modo analogo.

Nota: Questa operazione non è richiesta nel caso in cui vengano utilizzati altri software di bilanciamento del carico.

1. Dal menu Start del server Windows che esegue il servizio di nome di dominio, cliccare su **Strumenti di amministrazione > DNS**.
Viene visualizzata la finestra di gestione di DNS.
2. Espandere l'albero DNS.

3. Cliccare col tasto destro del mouse sul nome del server e poi selezionare **Proprietà**.
4. Cliccare sulla scheda **Avanzate**.
5. Selezionare la casella **Attiva round robin**.
6. Cliccare su **OK** per salvare le modifiche.
7. Espandere la cartella **Zone di ricerca diretta**, cliccare col tasto destro del mouse sul dominio in cui i Compliance Application Servers sono configurati e poi selezionare **Nuovo host (A)...**
8. Digitare il nome dell'host e l'indirizzo IP del Compliance Application Server primario che è stato installato e configurato, poi cliccare su **Aggiungi host**.

Nota: Il nome dell'host inserito diventa la porzione host dell'URL che gli agenti devono utilizzare. Per esempio, se si inserisce sophosapp come host nuovo, il nome di dominio pienamente qualificato diventa sophosapp.endpointsoftware.info.

9. Cliccare su **OK** per confermare il nome dell'host aggiunto e l'indirizzo IP.
10. Ripetere il passaggio 8 per tutti i Compliance Application Server aggiuntivi.

Nota: Affinché DNS round robin operi in modo corretto, il nome dell'host deve essere il medesimo per tutti i Compliance Application Servers. Per esempio, se il nome dell'host del Compliance Application Server primario è sophosapp; ne consegue che anche il nome dell'host di tutti i Compliance Application Servers aggiuntivi deve essere sophosapp.

11. Cliccare su **Finito** per tornare alla finestra di gestione di DNS.

Per esempio, alla richiesta del nome di dominio pienamente qualificato sophosapp.endpointsoftware.info risponde con una dei tre indirizzi IP del Compliance Application Server: 10.0.224.102, 10.0.224.103, or 63.110.105.174. Un agente configurato con questo nome di dominio riuscirà a comunicare con tutti i Compliance Application Servers.

10 Installazione del Dissolvable Agent

Il Dissolvable Agent è progettato per gli utenti, quali collaboratori esterni o ospiti, che non hanno o non possono avere l'agente installato nei loro computer. Per ulteriori informazioni sul Dissolvable Agent, consultare la *Guida alla configurazione dell' Agente di Sophos NAC Advanced*.

10.1 Requisiti di sistema del Dissolvable Agent

Per informazioni relative ai requisiti di sistema, consultare la pagina corrispondente del sito web di Sophos (<http://www.sophos.it/products/all-sysreqs.html>).

10.2 Installazione del Dissolvable Agent in un server web

Per utilizzare il Dissolvable Agent, è necessario innanzitutto installare il componente server del Dissolvable Agent in un server web basato su Windows e accessibile da parte degli utenti. Il Dissolvable Agent può essere installato nello stesso server del Compliance Application Server. Una volta installato, tramite browser l'utente può scaricare il Dissolvable Agent.

1. Scaricare il Sophos Compliance Dissolvable Agent dal sito web di Sophos.
In alternativa, inserire il CD Sophos Network Install. Il CD dovrebbe avviarsi automaticamente.
2. Per eseguire l'installazione del Dissolvable Agent, cliccare due volte sul file di installazione di Sophos Compliance Dissolvable Agent.
3. Cliccare su **Next** per continuare.
4. Leggere il Contratto di Licenza per l'Utente Finale, selezionare il pulsante di opzione **I Accept the terms of the License Agreement**, cliccare poi su **Next** per proseguire.
5. Cliccare su **Change** per selezionare la directory di installazione appropriata oppure mantenere quella predefinita c:\inetpub\wwwroot. Cliccare su **Next** per continuare.
6. Digitare l'indirizzo IP o il nome DNS del Compliance Application Server di Sophos NAC.

Nota: Se Sophos NAC Advanced è installato su più di un server, l'indirizzo del server coincide con l'indirizzo IP o il nome DNS del Compliance Application Server e non del Compliance Database Server. Se in possesso di più di un Compliance Application Server, digitare il nome dell'host rappresentante tutti i Compliance Application Servers. Se si cambia l'indirizzo del server dopo avere eseguito l'installazione del Dissolvable Agent, è necessario reinstallare il componente server del Dissolvable Agent nel server web e, durante la procedura di installazione, indicare il nuovo indirizzo del Compliance Application Server di Sophos.

7. Se si sta testando o valutando Sophos NAC Advanced, deselegionare la casella **Secure Sophos Server (use HTTPS)**.
8. La casella di spunta **Always register agent with server** non è selezionata per impostazione predefinita. Se si desidera che gli utenti si registrino quando utilizzano il Dissolvable Agent, è necessario selezionare tale opzione. Cliccare su **Next** per continuare.

Nota: Se si seleziona la casella "Always register agent with server", è necessario cambiare le impostazioni di registrazioni del Dissolvable Agent in Compliance Manager e scegliere On.

9. Per avviare l'installazione, cliccare su **Install**.
10. Per completare l'installazione cliccare su **Finish**.

Nota:

- Se si verificano errori durante l'installazione, utilizzare il log degli eventi nel server web per visualizzare eventuali informazioni aggiuntive.
- Se il Dissolvable Agent è stato installato nella directory predefinita, i computer possono accedere al Dissolvable Agent tramite il seguente URL `http(s)://<indirizzo ip/nome DNS>/dissolvableagent`. L'indirizzo IP o il nome DNS rappresenta il server web in cui è stato installato il Dissolvable Agent.

Importante: il Dissolvable Agent non può svolgere la valutazione delle patch quando eseguito come utente con limitazioni. È necessario cambiare l'utente in modo tale che venga eseguito come amministratore. Se non è possibile apportare tale cambiamento, si consiglia di creare un criterio a parte per gli utenti del Dissolvable Agent. Questo criterio non dovrà contenere patch; potrà invece contenere il Profilo di Windows Update. Tale profilo garantisce che il tool di Windows Update sia installato e che gli Aggiornamenti automatici siano attivati.

11 Disinstallazione del Dissolvable Agent da un server web

Utilizzare queste istruzioni per disinstallare il componente lato server del Dissolvable Agent da un server Web. Se si disinstalla il Dissolvable Agent dal server web, gli utenti non potranno scaricare il Dissolvable Agent.

1. Dal menu Start, selezionare **Pannello di controllo > Installazione applicazioni** .
2. Selezionare **Sophos Compliance Dissolvable Agent** e cliccare su **Rimuovi**.
3. Cliccare su **Sì** per confermare la rimozione di Dissolvable Agent.

12 Distribuzione dell'agente

Una volta completata la sezione *Requisiti di post installazione* di questo documento, è possibile installare i Compliance Agent sui computer.

12.1 Requisiti di sistema

Per informazioni relative ai requisiti di sistema, consultare la pagina corrispondente del sito web di Sophos (<http://www.sophos.it/products/all-sysreqs.html>).

12.2 Installazione dell'agente

L'installazione dell'agente utilizza tutti i valori ricavati dall'installazione precedente, nel caso sia stata eseguita. Per poter installare l'agente i computer devono essere in possesso dei diritti di amministrazione. Comunque, dopo l'installazione, l'interfaccia dell'agente opera in tutte le modalità utente, compresa quella limitata. Dopo l'installazione, l'agente viene visualizzato nel pannello di controllo di Microsoft Windows Installazione applicazioni, ma non nel menu Start di Microsoft Windows.

Opzioni di configurazione dell'installazione dell'agente

È possibile configurare l'installazione dell'agente con opzioni della riga di comando specifiche.

- Per installare l'Quarantine Agent e specificare la modalità di registrazione, utilizzare il seguente comando "*<fp Percorso completo del file di installazione dell'agente>*"
AGENT_SETTINGS="Register=<rmodalità di registrazione>". Se la modalità di registrazione non viene specificata, allora viene utilizzata, per impostazione predefinita, quella su richiesta.

Nota: le modalità di registrazione dell'agente disponibili sono always, demand, nopassword e usecomputerlogon. Per ulteriori informazioni, consultare la *Guida alle migliori pratiche di Sophos NAC Advanced*.

- Per configurare l'indirizzo IP o il nome DNS, e la modalità (HTTP o HTTPS) del Compliance Application Server con cui l'agente comunica, utilizzare il seguente comando: msiexec /i "*<percorso completo del file di installazione dell'agente>*" AGENT_SERVER=<indirizzo IP o nome DNS> AGENT_SERVERMODE=<http o https>. Se la modalità non viene specificata, allora viene utilizzata, per impostazione predefinita, quella HTTPS.
- Per configurare la classe utente DHCP, utilizzare il seguente comando: msiexec /i "*<percorso completo del file di installazione dell'agente>*" AGENT_DHCPCLASS= <classe utente>. La classe utente DHCP viene utilizzata per attuare DHCP, quando non si esegue NAC DHCP Enforcer.

Per esempio, il comando: msiexec /i "c:\SophosComplianceAgent.msi"
AGENT_INSTALLTYPE=quarantine AGENT_SETTINGS="Register=usecomputerlogon"
AGENT_SERVER=appserver AGENT_SERVERMODE=https esegue l'installazione del Quarantine Agent, con l'impostazione di registrazione Use Computer Logon presa da un file di installazione dell'agente posizionato nell'unità C e in cui si indica che l'agente comunicherà con il Compliance Application Server, il cui nome DNS è "appserver", tramite HTTPS.

Per installare l'agente:

1. Scaricare Sophos Compliance Agent dal sito web di Sophos.
In alternativa, inserire il CD Sophos Network Install. Il CD dovrebbe avviarsi automaticamente.
2. Cliccare due volte sul file di installazione di Sophos Compliance Agent.
3. Cliccare su **Next** per dare inizio alla procedura guidata.
4. Leggere il Contratto di Licenza per l'Utente Finale, selezionare il pulsante di opzione **I Accept the terms of the License Agreement**, cliccare poi su **Next** per proseguire.
5. Digitare l'indirizzo IP o il nome DNS del Compliance Application Server.
6. Se si sta testando o valutando Sophos NAC Advanced, deselezionare la casella **Secure Sophos Server (use HTTPS)**. Cliccare su **Next** per continuare.

Nota: Se Sophos NAC Advanced è installato su più di un server, l'indirizzo del server coincide con l'indirizzo IP o il nome DNS del Compliance Application Server e non del Compliance Database Server. Se in possesso di più di un Compliance Application Server, è necessario digitare il nome dell'host rappresentante tutti i Compliance Application Servers.

7. Cliccare su **Change** per selezionare la directory di installazione appropriata oppure mantenere quella predefinita e successivamente cliccare su **Next** per continuare.
8. Per avviare l'installazione, cliccare su **Install**. Per annullare l'installazione, cliccare su **Cancel**.

Nota: nelle installazioni di Windows 2000, se il Service Pack 3 o superiore non è stato installato, viene visualizzata la finestra di dialogo Driver Unsigned. Tale comportamento è dovuto alla modalità in cui Windows Hardware Quality Lab (WHQL) genera la firma. Nelle installazioni di Windows XP, se il Service Pack 1 è stato installato, viene visualizzata la finestra di dialogo Driver Unsigned; mentre se Service Pack 1a, Service Pack 2 o se nessun service pack è stato installato ciò non dovrebbe verificarsi.

9. Per completare l'installazione cliccare su **Finish**.
Una volta completata l'installazione dell'agente può essere richiesto il riavvio del computer per le seguenti ragioni:
 - Durante l'installazione è stato richiesta la chiusura di applicazioni che utilizzano risorse condivise, quali XMLDOM, ma ciò non è stato fatto.
 - Si sta eseguendo l'upgrade del Quarantine Agent e tale upgrade esegue una nuova versione driver kernel dell'Agent Quarantine Manager.

13 Disinstallazione dell'agente

Importante: durante la disinstallazione di un agente, prima che questo venga effettivamente disinstallato, può venire visualizzata la finestra di dialogo di Windows Explorer che richiede di chiudere determinate applicazioni, quali il client di posta elettronica. Perché la disinstallazione abbia esito positivo, si consiglia di chiudere tutte le applicazioni. La disinstallazione dell'agente richiede anche il riavvio del computer.

1. Dal menu Start, selezionare **Pannello di controllo > Installazione applicazioni** .
2. Selezionare **Sophos Compliance Agent** e cliccare su **Rimuovi**.
3. Cliccare su **Sì** per confermare la rimozione dell'agente.

14 Impostazioni facoltative

Questa sezione contiene informazioni relative alle impostazioni facoltative per Sophos NAC Advanced. L'implementazione di Sophos NAC Advanced può richiedere il completamento di alcune o di tutte queste operazioni.

14.1 Verifica/Modifica della procedura Patch Loader

Per impostazione predefinita, l'operazione Patch Loader è programmata in modo tale da essere eseguita casualmente ogni giorno. Questa operazione consente di recuperare le ultime definizioni delle patch da Sophos e richiedere accesso a Internet.

1. Dal menu Start del Compliance Application Server, cliccare su **Pannello di controllo > Operazioni pianificate** .
Viene visualizzata la finestra delle operazioni pianificate.
2. Cliccare due volte su **Sophos NAC PatchLoader**. Viene visualizzata la finestra Proprietà.
3. Cliccare sulla scheda **Pianificazione**
4. A seconda delle esigenze, cambiare l'ora in cui è stata programmata la procedura e cliccare su **OK**.
5. Cliccare su **OK** per salvare le modifiche.
6. Uscire dalla finestra delle operazioni pianificate.

14.2 Esecuzione manuale dell'operazione Patch Loader

Per impostazione predefinita, l'operazione Patch Loader è programmata in modo tale da essere eseguita casualmente ogni giorno; è tuttavia possibile eseguirla manualmente. Questa operazione consente di recuperare le ultime definizioni delle patch da Sophos e richiedere accesso a Internet.

1. Dal menu Start del Compliance Application Server, cliccare su **Pannello di controllo > Operazioni pianificate** .
Viene visualizzata la finestra delle operazioni pianificate.
2. Cliccare col tasto destro del mouse su **Sophos NAC PatchLoader**, e selezionare **Esegui**.
3. Uscire dalla finestra delle operazioni pianificate.

14.3 Verifica/modifica dell'operazione Current Definition Loader

L'operazione Current Definition Loader è programmata per essere eseguita ogni ora. L'installazione di Sophos NAC Advanced pianifica l'esecuzione casuale di questa procedura, che impiega pochi minuti per completarsi e richiede l'accesso a Internet. Questa operazione consente di recuperare da Sophos le date più recenti relative alle firme correnti delle applicazioni antivirus e antispyware.

1. Dal menu Start del Compliance Application Server, cliccare su **Pannello di controllo > Operazioni pianificate** .
Viene visualizzata la finestra delle operazioni pianificate.

2. Cliccare due volte su **Sophos NAC CurrentDefsLoader**. Viene visualizzata la finestra Proprietà.
3. Cliccare sulla scheda **Pianificazione**
4. Cliccare su **Avanzate**.
5. Cambiare l'ora in cui è stata programmata la procedura e cliccare su **OK**.
6. Cliccare su **OK** per salvare le modifiche.
7. Uscire dalla finestra delle operazioni pianificate.

14.4 Esecuzione manuale dell'operazione Current Definition Loader

L'operazione Current Definition Loader è programmata per essere eseguita ogni ora; è comunque possibile eseguirla manualmente. L'installazione di Sophos NAC Advanced pianifica l'esecuzione casuale di questa procedura, che impiega pochi minuti per completarsi e richiede l'accesso a Internet. Questa operazione consente di recuperare da Sophos le date più recenti relative alle firme correnti delle applicazioni antivirus e antispyware.

1. Dal menu Start del Compliance Application Server, cliccare su **Pannello di controllo > Operazioni pianificate** .
Viene visualizzata la finestra delle operazioni pianificate.
2. Cliccare col tasto destro del mouse su **Sophos NAC CurrentDefsLoader**, e selezionare **Esegui**.
3. Uscire dalla finestra delle operazioni pianificate.

14.5 Verifica/Modifica dell'operazione Report Warehouse Loader

Per impostazione predefinita, l'operazione Report Warehouse Loader è programmata per essere eseguita giornalmente alle 02:30; è tuttavia possibile eseguirla manualmente. Questa operazione consente di verificare quando i dati dei report vengono archiviati e eliminati.

1. Dal menu Start del server SQL, eseguire una delle seguenti operazioni:
 - se si esegue SQL Server 2000, cliccare su **Microsoft SQL Server > Enterprise Manager** . Si apre SQL Enterprise Manager.
 - Se si esegue SQL Server 2005 o superiore, cliccare su **Microsoft SQL Server (versione) > SQL Server Management Studio** . Si apre SQL Server Management Studio.
2. Trovare l'**agente di SQL Server**.
Nota: se si esegue SQL Server 2000, l'agente di SQL Server si trova nella cartella Management.
3. In SQL Server Agent, selezionare **Operazioni**.
4. Cliccare due volte sul nome della procedura **Sophos NAC - LoadWH**. Viene visualizzata la finestra "Proprietà".
5. Effettuare una delle seguenti operazioni:
 - Se si esegue SQL Server 2000, cliccare sulla scheda **Pianificazioni**.
 - Se si esegue SQL Server 2005 o superiore, cliccare su **Pianificazioni**.

6. Effettuare una delle seguenti operazioni:
 - Cliccare su **Nuove pianificazioni** (SQL Server 2000) o **Nuova** (SQL Server 2005 o superiore) per aggiungere nuove operazioni pianificate, aggiungere le pianificazioni aggiuntive e cliccare su **OK**.
 - Cliccare su **Modifica** per modificare le pianificazioni esistenti, modificarle e poi cliccare su **OK**.

Nota: è possibile modificare l'orario in cui i dati vengono trasferiti nei report archiviati e/o è possibile specificare operazioni aggiuntive per trasferire i dati dei report negli archivi più di una volta al giorno.
7. Cliccare su **OK** per salvare le modifiche.
8. Uscire da SQL Enterprise Manager o SQL Server Management Studio.

14.6 Esecuzione manuale dell'operazione Report Warehouse Loader

L'operazione Report Warehouse Loader consente di verificare quando i dati dei report vengono archiviati e eliminati. Per impostazione predefinita viene eseguita una volta al giorno alle ore 2:30; è tuttavia possibile eseguire il Report Warehouse Loader manualmente.

1. Dal menu Start del server SQL, eseguire una delle seguenti operazioni:
 - se si esegue SQL Server 2000, cliccare su **Microsoft SQL Server > Enterprise Manager** . Si apre SQL Enterprise Manager.
 - Se si esegue SQL Server 2005 o superiore, cliccare su **Microsoft SQL Server (versione) > SQL Server Management Studio** . Si apre SQL Server Management Studio.
2. Trovare l'**agente di SQL Server**.

Nota: se si esegue SQL Server 2000, l'agente di SQL Server si trova nella cartella Management.
3. In SQL Server Agent, selezionare **Operazioni**.
4. Cliccare col tasto destro del mouse su **Sophos NAC - LoadWH** e selezionare **Avvia operazione**.

Nota: il tempo necessario per l'esecuzione manuale di Sophos NAC - LoadWH è identico a quello per la sua esecuzione automatica svolta tutte le notti.
5. Uscire da SQL Enterprise Manager o SQL Server Management Studio.

14.7 Disattivazione di HTTPS per un test in ambienti non di produzione

Sophos NAC Advanced utilizza HTTPS per proteggere nomi utente, password ed altre informazioni sensibili di un'impresa. In alcuni casi, nello specifico per test e valutazioni, può essere necessaria la disattivazione di HTTPS.

1. Dal menu start del Compliance Application Server, cliccare su **Strumenti di amministrazione > Gestione Internet information services (IIS)** .

Viene aperto IIS.

2. Aprire la cartella **Siti web** e successivamente quella **Sito web predefinito**.
3. Cliccare con il tasto destro del mouse su **RegistrationInterface** e selezionare **Proprietà**.
Viene visualizzata la finestra delle proprietà di RegistrationInterface.
4. Cliccare sulla scheda **Protezione directory**.
5. Nell'area **Comunicazioni protette**, cliccare su **Modifica**.
Viene visualizzata la finestra delle Comunicazioni protette.
6. Deselezionare la casella **Richiedi un canale protetto (SSL)**.
7. Cliccare su **OK** per tornare alla finestra di RegistrationInterface ed ancora su **OK** per tornare a IIS.
8. Ripetere i passaggi dal 2 al 6 per PolicyInterface, ReportInterface e ServerStatusInterface.
9. Uscire da IIS.

15 Supporto tecnico

È possibile ricevere supporto tecnico per i prodotti Sophos in uno dei seguenti modi:

- Visitando la community SophosTalk su <http://community.sophos.com/> e cercando altri utenti con lo stesso problema.
- Visitando la knowledge base del supporto Sophos su <http://www.sophos.it/support/>.
- Scaricando la documentazione del prodotto su <http://www.sophos.it/support/docs/>.
- Inviando un'e-mail a support@sophos.com, indicando il o i numeri di versione del software Sophos in vostro possesso, i sistemi operativi e relativi livelli di patch, ed il testo di ogni messaggio di errore.

16 Note legali

Copyright © 2011 Sophos Limited. Tutti i diritti riservati. Nessuna parte di questa pubblicazione può essere riprodotta, memorizzata in un sistema di recupero informazioni, o trasmessa, in qualsiasi forma o con qualsiasi mezzo, elettronico o meccanico, inclusi le fotocopie, la registrazione e altri mezzi, salvo che da un licenziatario autorizzato a riprodurre la documentazione in conformità con i termini della licenza, oppure previa autorizzazione scritta del titolare dei diritti d'autore.

Sophos e Sophos Anti-Virus sono marchi registrati di Sophos Limited. Tutti gli altri nomi citati di società e prodotti sono marchi o marchi registrati dei rispettivi titolari.

OpenSSL cryptographic toolkit

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL license

Copyright © 1998-2011 The OpenSSL Project. Tutti i diritti riservati.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR

PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay license

Copyright © 1995–1998 Eric Young (eay@cryptsoft.com) All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscape's SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

"This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"

The word "cryptographic" can be left out if the routines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

"This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR

OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License.]