

SOPHOS

simple + secure

Sophos NAC Advanced Guida alla risoluzione dei problemi

Versione prodotto: 3.2

Data documento: aprile 2011



Sommario

1 Problemi di installazione.....	3
2 Problemi di Compliance Manager.....	4
3 Problemi di log.....	7
4 Problemi di comunicazione con il server (dall'agente).....	8
5 Problemi del client VPN.....	11
6 Problemi relativi ai criteri.....	12
7 Problemi di registrazione.....	18
8 Problemi di reportistica.....	20
9 Problemi relativi agli allarmi.....	22
10 Problemi del server.....	23
11 Problemi di attuazione.....	25
12 Problemi relativi ad applicazioni prodotte da terzi.....	32
13 Supporto tecnico.....	33
14 Note legali.....	34

1 Problemi di installazione

Questa sezione contiene informazioni sulla risoluzione dei problemi legati all'installazione di Sophos NAC Advanced.

1.1 Installazione dei Compliance Database

Compliance Database L'installazione dei non riesce

Causa: l'account utilizzato per l'installazione non possiede i privilegi di amministratore per il database.

Risoluzione: connettersi con l'account dotato di privilegi di amministratore.

Causa: durante l'installazione, viene visualizzata una finestra che riporta il seguente messaggio di errore: "Failed to load the test rule file" con un nome di file XML e "Cursor operation conflict". Questo messaggio viene visualizzato perché è attivo l'attributo "No count" per le connessioni nel server SQL.

Risoluzione:

1. Aprire Microsoft SQL Server Enterprise Manager e cercare il server SQL in cui l'installazione non è riuscita.
2. Cliccare con il tasto destro del mouse su SQL server e selezionare **Properties**.
3. Cliccare sulla scheda **Connections**.
4. Nell'elenco **Attribute**, cercare l'attributo "No count" e deselezionare la casella.
5. Cliccare su **OK**.

1.2 Distribuzione dell'agente

L'installazione dell'agente non riesce.

Causa: l'account utilizzato per l'installazione non possiede privilegi di amministratore.

Risoluzione: assicurarsi che l'account che installa l'agente possieda privilegi di amministratore.

2 Problemi di Compliance Manager

Questa sezione fornisce informazioni per la risoluzione dei problemi relativi a Compliance Manager.

2.1 Connessione e installazione

Impossibile connettersi a Compliance Manager

Causa: l'amministratore non riesce a connettersi a Compliance Manager.

Risoluzione:

1. accertarsi di poter accedere al Compliance Application Server.
2. Se gli account sono gestiti da Compliance Manager invece che da un archivio utente esterno, assicurarsi che il nome dell'account e la password siano valide.

Nota: La prima volta che ci si connette a Compliance Manager, utilizzare **admin** e una password a propria scelta.

3. Se per la gestione degli account si utilizza un archivio utenti esterno, verificare che l'archivio utilizzato per l'account di Compliance Manager sia dello stesso tipo di quello utilizzato per l'autenticazione dell'agente. Se non sono dello stesso tipo, è necessario innanzitutto creare un Criterio di Richiesta di Connessione cui dare priorità massima. Per ulteriori informazioni, consultare la *Guida all'installazione* di *Sophos NAC Advanced*.
4. Le autorizzazioni potrebbero non essere impostate correttamente per le applicazioni Sophos nei Compliance Database. Per ulteriori informazioni, v. il problema "Nessun componente del Compliance Application Server o del RADIUS server riesce a connettersi ai Compliance Database", nella sezione [Server SQL](#) a pagina 24.

Causa: il servizio ASP.NET non è in esecuzione.

Risoluzione: Impostare il servizio dello stato di ASP.NET su automatico e avviarlo.

2.2 Compliance Manager

Alcune finestre non vengono visualizzate in Compliance Manager

Causa: se il blocco popup è attivato, l'esecuzione di certe operazioni in Compliance Manager, come la stampa di un report e l'apertura della Guida in linea, può essere ostacolata.

Risoluzione: disattivare il blocco popup quando si utilizza Compliance Manager.

Le pagine non vengono visualizzate correttamente in Compliance Manager

Causa: esecuzione di Compliance Manager tramite Internet Explorer 6.x senza avere aggiunto Compliance Manager all'elenco dei siti web affidabili.

Risoluzione: in Internet Explorer, aggiungere Compliance Manager ai siti web attendibili. Questa impostazione non è necessaria in Internet Explorer 7.x.

Le funzioni di creazione, modifica o configurazione non vengono eseguite in Compliance Manager

Causa: i Compliance Database non sono disponibili.

Risoluzione:

1. Accertarsi che i Compliance Database funzionino correttamente.
2. Verificare che il servizio SQL server si sia avviato correttamente e che la password dell'account del servizio Sophos NAC Advanced utilizzato per avviare questa istanza di SQL server sia la stessa password che era stata creata prima dell'installazione di Sophos NAC Advanced.

Causa: l'installazione del Compliance Application Server non è stata completata.

Risoluzione: controllare nel Log eventi del Compliance Application Server l'eventuale presenza di errori di installazione e completare l'installazione del Compliance Application Server.

Nessuna patch disponibile

Causa: se l'elenco della pagina Patches di Compliance Manager non contiene alcuna patch, significa che l'operazione Patch Loader non è riuscita a popolarlo.

Risoluzione: utilizzare il comando Server Task Status nella home page di Compliance Manager per verificare che l'operazione Patch Loader non sia riuscita e visualizzare la causa. La causa più probabile del problema è che il Compliance Application Server non abbia accesso in uscita a Internet (richiesto da Patch Loader) oppure che il server proxy non sia configurato o sia configurato in modo errato. Eseguire manualmente l'operazione Patch Loader nel Compliance Application Server per scaricare e aggiornare le informazioni sulle patch. Configurare il server proxy. Per ulteriori informazioni, consultare la *Guida all'installazione* di *Sophos NAC Advanced*.

Le date del file della firma per le applicazioni antivirus o antispyware risultano obsolete

Causa: il file della firma più recente non è stato recuperato dall'operazione Current Definition Loader.

Risoluzione: utilizzare il comando Server Task Status nella home page di Compliance Manager per verificare che l'operazione Current Definition Loader non sia riuscita e per visualizzarne la causa. La causa più probabile del problema è che il Compliance Application Server non abbia accesso in uscita a Internet (richiesto da Current Definition Loader) oppure che il server proxy non sia configurato o sia configurato in modo errato. Eseguire manualmente l'operazione Current Definition Loader nel Compliance Application Server per scaricare e aggiornare le informazioni sulla data della firma dell'applicazione. Configurare Sophos NAC Advanced come server proxy RADIUS. Per ulteriori informazioni, consultare la *Guida all'installazione* di *Sophos NAC Advanced*.

I nomi delle applicazioni non vengono visualizzati correttamente in Compliance Manager

Causa: il supporto per le lingue orientali non è installato.

Risoluzione: accertarsi di aver installato i file necessari per il supporto delle lingue orientali (tramite Pannello di controllo > Opzioni internazionali e della lingua) nel computer dal quale si visualizza Compliance Manager.

L'utilizzo dei pulsanti del browser produce un errore

Causa: si stanno utilizzando i pulsanti del browser web per la navigazione.

Risoluzione: l'utilizzo dei pulsanti del browser web per muoversi nel Compliance Manager **non** è supportato. La navigazione e le diverse funzioni devono essere svolte utilizzando le voci del menu, i collegamenti e i pulsanti a disposizione in ciascuna pagina.

Non vengono visualizzate tutte le funzioni o le azioni correttive relative a un'applicazione.

Causa: le funzioni o le azioni correttive non sono supportate per la specifica versione dell'applicazione o per tutti i sistemi operativi.

Risoluzione: le funzioni dell'applicazione e le azioni correttive dipendono da come è stato progettato il software dell' applicazione stessa. Alcune funzioni e azioni correttive possono non essere disponibili in determinati sistemi operativi che supportano l'applicazione oppure in tutte le versioni dell'applicazione. Se una funzione non è supportata non verrà visualizzata. Se una funzione è supportata da determinati sistemi operativi, ma non da altri, verrà visualizzata solo da quelli supportati. Se un'azione correttiva è supportata da determinati sistemi operativi, ma non da altri, quelli non supportati verranno visualizzati con una x al loro interno.

Si consiglia di testare il criterio prima di distribuirlo, in modo che l'applicazione, le regole di rilevamento dell'applicazione e le impostazioni del profilo e del criterio siano corrette.

Non vengono visualizzate tutte le funzioni in un profilo.

Causa: non tutte le funzioni possono essere contenute nella pagina di Compliance Manager.

Risoluzione: cliccare sul pulsante di espansione posto accanto all'intestazione per visualizzare le funzioni nella pagina web.

3 Problemi di log

Questa sezione contiene informazioni per la risoluzione dei problemi legati alla registrazione nei log.

3.1 Log dell'agente

I file del log dell'agente non sono presenti nel Quarantine Agent

Causa: la registrazione nel log non è attiva.

Risoluzione: attivare la registrazione spuntando la casella Enable Logging nella finestra di dialogo About. Se non specificato nel modello di configurazione dell'agente applicato al criterio del computer, la registrazione nel log è automaticamente impostata al livello 1 (messaggi di errore e di avviso).

Nota: La registrazione ha ripercussioni sulle prestazioni; si consiglia quindi di abilitarla esclusivamente per la risoluzione di un problema e di disabilitarla a problema risolto. I file di log per Windows 2000 e Windows XP si trovano nella directory <unità>:\Documents and Settings\All Users\Application Data\Sophos\Sophos NAC\Logs, mentre i file di log per Windows Vista e Windows 7 si trovano nella directory <unità>:\ProgramData\Sophos\Sophos NAC\Logs.

3.2 Registrazione nel log del Dissolvable Agent

I file del log dell'agente non sono presenti nel Dissolvable Agent

Causa: la registrazione nel log non è attiva.

Risoluzione: attivare la registrazione nel log per il Dissolvable Agent. Spuntare la casella Abilita registrazione nella finestra di dialogo About. Per ulteriori informazioni, consultare la *Sophos NAC Advanced* dell'Agent di *Agente*.

Nota: La registrazione ha ripercussioni sulle prestazioni; si consiglia quindi di abilitarla esclusivamente per la risoluzione di un problema e di disabilitarla a problema risolto. I file di log sono situati nella directory <unità>:\Sophos\SDA<numero casuale>\Logs.

4 Problemi di comunicazione con il server (dall'agente)

Questa sezione contiene informazioni per la risoluzione dei problemi legati alla comunicazione con il server, riscontrati nel o provenienti dall'agente.

4.1 Recupero del criterio, registrazione o reportistica

Recupero del criterio, registrazione o reportistica non riuscito

Importante: per ulteriori problemi relativi a criteri, registrazioni o reportistica, consultare la sezione [Problemi relativi ai criteri](#) a pagina 12, [Problemi di registrazione](#) a pagina 18, o [Problemi di reportistica](#) a pagina 20.

Causa: durante la distribuzione dell'agente l'indirizzo del Compliance Application Server non era corretto oppure è stato modificato successivamente. L'indirizzo del server utilizzato per la connessione al Compliance Application Server viene riportato nel file di log.

Se l'indirizzo IP o il nome DNS **non** è corretto o il Compliance Application Server è inattivo, nella finestra di dialogo o pagina Risultati viene visualizzato il seguente errore: "L'agente non ha potuto eseguire l'operazione <>. Se il problema persiste, segnalarlo al proprio amministratore. (Motivazione: server non trovato. Codice: 700)".

Se l'indirizzo IP o il nome DNS è corretto, ma il percorso URL **non** lo è nella finestra di dialogo o pagina Results viene visualizzato il seguente errore: "L'agente non ha potuto eseguire l'operazione <>. Se il problema persiste, segnalarlo al proprio amministratore. (Motivazione: URL non valida. Codice: 404)".

Risoluzione:

1. fare in modo che il Compliance Application Server non sia raggiungibile, avviando una verifica della conformità che è disponibile tramite l'opzione Check Compliance del menu associato all'icona di Quarantine Agent posta nell'area di notifica.
2. Attivare la registrazione nel log dell'agente spuntando la casella Attiva registrazione nella finestra di dialogo Informazioni su, quindi verificare l'indirizzo del server (indirizzo IP o nome DNS) e la modalità (http/https) del Compliance Application Server, aprendo il file di log dell'API dell'agente con nome <GUID>_trace.log. Per Compliance Agent, questo file di log viene visualizzato se l'impostazione Logging Agent nel modello di configurazione dell'agente è Log All Messages and Brief Trace. Per il Dissolvable Agent, all'attivazione della registrazione nel log questa viene impostata su Log All Messages and Brief Trace. Per il Compliance Agent, i file di log per Windows 2000 e Windows XP si trovano nella directory <unità>:\Documents and Settings\All Users\Application Data\Sophos\Sophos NAC\Log, mentre i file di log per Windows Vista e Windows 7 si trovano nella directory <unità>:\ProgramData\Sophos\Sophos NAC\Log. Per il Dissolvable Agent, i file di log sono situati nella directory <unità>:\Sophos\SDA<numero casuale>\Log.
3. Reinstallare l'agente con il corretto indirizzo del Compliance Application Server. Durante l'installazione, il formato per l'indirizzo del server (< Compliance Application Server> nel quale sono installati i servizi web Registration Interface, Policy Interface e Reporting Interface) deve essere solo il nome DNS o l'indirizzo IP, come "www.sophos.it" o "10.0.0.160".

Importante: se il certificato web nel Compliance Application Server è impostato per utilizzare un indirizzo IP, durante l'installazione dell'agente va utilizzato un indirizzo IP. Allo stesso

modo, se il certificato web è impostato per utilizzare un nome DNS, durante l'installazione dell'agente va utilizzato un nome DNS.

Causa: la registrazione dell'agente è stata cancellata. Nella finestra di dialogo o pagina Risultati viene visualizzato il seguente errore: "L'agente non ha potuto eseguire l'operazione <>. Se il problema persiste, segnalarlo al proprio amministratore. (Motivazione: il server ha rifiutato la richiesta dell'agente. Codice: 500)"

Risoluzione: registrare di nuovo l'agente. Nel computer, cliccare con il tasto destro del mouse sull'icona dell'agente nell'area di notifica e selezionare **Registra**.

Causa: il computer potrebbe non avere accesso a Internet.

Risoluzione: accertarsi che il computer abbia accesso a Internet.

Causa: il certificato SSL non è installato nell'agente o nel Compliance Application Server.

Risoluzione:

1. accertarsi che il certificato digitale rilasciato dall'autorità di certificazione sia installato nell'archivio delle autorità attendibili del computer (non dell'utente). Questa operazione è necessaria per la modalità https.

Nota: per convalidare adeguatamente i certificati nei computer che eseguono i sistemi operativi Microsoft Windows vecchi, compreso Windows 2000, installare l'appropriato "Root Certificate Update" dal sito web di Microsoft.

2. Fare in modo che il Compliance Application Server abbia un certificato digitale installato, emesso da un'autorità di certificazione attendibile come VeriSign. Questa operazione è necessaria per la modalità https.

Nota: se si utilizza HTTP per un test, anche gli URL devono utilizzare HTTP.

Causa: il Compliance Application Server non può essere raggiunto.

Risoluzione:

1. accertarsi che il software firewall nel computer non blocchi il traffico verso il Compliance Application Server e che un firewall non stia bloccando il traffico verso il computer. Se un firewall sta bloccando il traffico, aprirlo per consentirne il passaggio.
2. Accertarsi che l'indirizzo appropriato del Compliance Application Server sia funzionante testando l'URL del Compliance Application Server in un browser web. Se viene visualizzato un errore dei servizi web, l'indirizzo del server è corretto. È possibile testare uno dei seguenti URL:

[http\(s\)://< Compliance Application Server>/RegistrationInterface/RegistrationInterface310.asmx](http(s)://< Compliance Application Server>/RegistrationInterface/RegistrationInterface310.asmx)

[http\(s\)://< Compliance Application Server>/ServerStatusInterface/ServerStatusInterface310.asmx](http(s)://< Compliance Application Server>/ServerStatusInterface/ServerStatusInterface310.asmx)

3. Accertarsi che il Compliance Application Server sia stato aggiunto come risorsa di rete consentita ai modelli di accesso di Compliance Manager appropriati.
4. Nel caso in cui il computer si trovi in una posizione remota, l'utente deve connettersi a VPN ed eseguire una verifica della conformità nel computer tramite l'agente.

Causa: l'agente utilizza un server proxy web per connettersi al e le impostazioni del server proxy web sono errate.

Risoluzione: accedere alle impostazioni del proxy web in Internet Explorer e accertarsi che siano corrette:

1. Cliccare su **Strumenti > Opzioni Internet** .
2. Cliccare sulla scheda **Connections**.
3. Cliccare su **Impostazioni e/o Impostazioni LAN** e specificare le impostazioni proxy appropriate.

Accertarsi che l'indirizzo appropriato del Compliance Application Server sia funzionante testando l'URL del Compliance Application Server in un browser web. Se viene visualizzato un errore dei servizi web, l'indirizzo del server è corretto. È possibile testare uno dei seguenti URL:

[http\(s\)://< Compliance Application Server>/RegistrationInterface/RegistrationInterface310.aspx](http(s)://< Compliance Application Server>/RegistrationInterface/RegistrationInterface310.aspx)

[http\(s\)://< Compliance Application Server>/ServerStatusInterface/ServerStatusInterface310.aspx](http(s)://< Compliance Application Server>/ServerStatusInterface/ServerStatusInterface310.aspx)

Causa: l'agente utilizza un server proxy web per connettersi al Compliance Application Server e le impostazioni del server proxy web non sono impostate per l'utente corrente.

Risoluzione: accertarsi che le impostazioni del proxy web in Internet Explorer siano regolate per l'utente corrente, in quanto sono regolabili separatamente per ciascun utente. Per ulteriori informazioni, v. il problema precedente.

Causa: una voce DNS è cambiata e il computer non è stato riavviato oppure il processo AgentAPI.exe non è stato arrestato e riavviato.

Risoluzione: riavviare ciascun computer oppure uscire dall'agente e quindi arrestare e riavviare AgentAPI.exe in ciascun computer. In questo modo, le voci DNS scadute vengono cancellate.

Causa: le chiavi del server non corrispondono. Nella finestra di dialogo o pagina Risultati viene visualizzato il seguente errore: "Server non convalidato. Codice: 701" (se sono abilitati i messaggi di errore dettagliati).

Risoluzione: se una nuova chiave server viene generata in Compliance Manager, la stessa chiave deve essere importata in tutti i Compliance Application Server, in modo che siano sincronizzati.

Accertarsi di utilizzare l'appropriato file della chiave server ServerKey.xml e che la stessa chiave server sia utilizzata in tutti i Compliance Application Server (se si utilizzano server multipli).

5 Problemi del client VPN

Questa sezione contiene informazioni per la risoluzione dei problemi legati al client VPN.

5.1 VPN

VPN, o altra applicazione prodotta da terzi, non richiama correttamente l'agente

Causa: il Quarantine Agent non è richiamato dal VPN o altra applicazione prodotta da terzi.

Risoluzione: accertarsi che le applicazioni prodotte da terzi stiano richiamando il Compliance Checker (Cmpchk.exe) per far avviare all'agente una completa verifica della conformità. Per ulteriori informazioni, consultare la *Sophos NAC Advanced* dell'Agente di *Agente* .

Causa: l'agente non è in esecuzione.

Risoluzione: prima che venga richiamato da un'applicazione prodotta da terzi, accertarsi che l'agente sia in esecuzione.

VPN non si connette

Causa: l'ultimo criterio recuperato dal computer è obsoleto secondo il Agent Policy Update Threshold.

Risoluzione: accertarsi che l'ultimo recupero del criterio da parte del computer sia avvenuto nell'intervallo di tempo definito nel campo Agent Policy Update Threshold in Compliance Manager (**Configure System > Enforcer Settings**) .

Causa: i codici generati durante la chiamata del Compliance Checker (Cmpchk.exe) non sono corretti.

Risoluzione: accertarsi che durante la chiamata del Compliance Checker (Cmpchk.exe), i codici generati siano corretti e gestiti in modo appropriato. Per ulteriori informazioni relative ai codici generali, consultare la *Guida alla configurazione dell' Agente di Sophos NAC Advanced* .

L'autenticazione VPN non riesce

Causa: il nome utente utilizzato per l'autenticazione RADIUS non coincide con quello utilizzato per l'autenticazione VPN.

Risoluzione: accertarsi che la stringa del nome utente coincida esattamente con quella immessa nell'agente per l'autenticazione RADIUS e nell'applicazione del client VPN (il nome utente non distingue fra maiuscole e minuscole).

Causa: al computer è assegnato un modello di accesso di RADIUS Enforcer che erroneamente nega l'accesso.

Risoluzione: visualizzare il report di RADIUS Enforcer in Compliance Manager per sapere quale modello di accesso è stato assegnato al computer e il motivo dell'assegnazione.

Accertarsi che ai corretti stati di accesso e di conformità nel criterio e nelle impostazioni di Enforcer siano applicati i corretti modelli di accesso di RADIUS Enforcer; verificare che i modelli di accesso contengano le impostazioni o le risorse di rete adeguate.

6 Problemi relativi ai criteri

Questa sezione contiene informazioni per la risoluzione dei problemi legati ai criteri.

6.1 Recupero del criterio

Il recupero del criterio non riesce

Importante: Per ulteriori informazioni, consultare la sezione [Problemi di comunicazione con il server \(dall'agente\)](#) a pagina 8.

Causa: la registrazione dell'utente nell'agente è scaduta. Nella finestra di dialogo o pagina Risultati viene visualizzato il seguente errore: "L'operazione di recupero del criterio non è riuscita perché la registrazione dell'utente è scaduta. È necessario registrare l'agente."

Risoluzione: l'utente deve registrarsi nell'agente utilizzando l'opzione di menu Registra.

6.2 Verifica e attuazione del criterio

L'agente non è in grado di verificare o attuare il criterio

Importante: Per ulteriori informazioni, consultare la sezione [Problemi di comunicazione con il server \(dall'agente\)](#) a pagina 8.

Causa: la registrazione dell'utente nell'agente è scaduta. Nella finestra di dialogo o pagina Risultati viene visualizzato il seguente errore: "L'operazione di attuazione del criterio non è riuscita perché la registrazione dell'utente è scaduta. È necessario registrare l'agente."

Risoluzione: l'utente deve registrarsi nell'agente utilizzando l'opzione di menu Registra.

Il computer non riceve alcun criterio (l'utente si sta autenticando)

Causa: non c'è alcun criterio predefinito e l'utente fa parte di un gruppo che non è associato a un criterio in Compliance Manager, oppure l'utente non può essere mappato a un gruppo.

Risoluzione: tramite Compliance Manager, associare il gruppo a un criterio oppure creare un criterio predefinito.

Causa: il gruppo dell'utente è cambiato nell'arco di tempo fra l'ultima registrazione dell'utente nell'agente e il momento in cui il criterio è stato recuperato.

Risoluzione: far scadere la registrazione dell'utente nell'area **Manage > Endpoints** di Compliance Manager in modo che l'agente possa registrare nuovamente l'utente e recuperare il criterio corretto.

Causa: il gruppo dell'utente non è stato creato in Compliance Manager.

Risoluzione: creare il gruppo in Compliance Manager. Per ulteriori informazioni, consultare la Guida in linea di Compliance Manager.

Causa: se si utilizza il Quarantine Agent, il Policy Refresh Interval non è stato raggiunto e pertanto l'agente non ha recuperato il criterio.

Risoluzione: recuperare il criterio avviando una verifica della conformità, disponibile tramite l'opzione Verifica conformità del menu associato all'icona del Quarantine Agentposta nell'area di notifica.

Il computer non sta ricevendo il criterio corretto

Causa: il gruppo dell'utente è cambiato nell'arco di tempo fra l'ultima registrazione dell'utente nell'agente e il momento in cui il criterio è stato recuperato.

Risoluzione: far scadere la registrazione dell'utente nell'area **Manage > Endpoints** di Compliance Manager in modo che l'agente possa registrare nuovamente l'utente e recuperare il criterio corretto.

Causa: l'utente fa parte di un gruppo, ma il gruppo non è associato al criterio corretto in Compliance Manager.

Risoluzione: accertarsi che il gruppo sia associato al criterio corretto in Compliance Manager.

Causa: i gruppi non sono ordinati correttamente per priorità in Compliance Manager.

Risoluzione: in Compliance Manager, assicurarsi che i gruppi siano nell'ordine di priorità corretto. Se a un particolare computer è associato più di un gruppo, viene utilizzato il primo di essi. Se l'utente sta ricevendo il criterio predefinito, accertarsi inoltre che i nomi dei gruppi siano accurati.

Causa: l'utente non fa parte del gruppo voluto nell'archivio utenti.

Risoluzione: accertarsi che l'utente sia associato al gruppo corretto nell'archivio utenti e che il nome del gruppo sia accurato. Per essere autenticato correttamente, il nome del gruppo in Compliance Manager deve coincidere con un nome di un gruppo di sicurezza nell'archivio utenti (Active Directory o Windows NT) o con un valore generato dal server RADIUS (proxy RADIUS).

Causa: il gruppo dell'utente non è stato creato in Compliance Manager.

Risoluzione: creare il gruppo in Compliance Manager. Per ulteriori informazioni, consultare la Compliance Manager di Guida in linea.

Causa: l'utente riceve il criterio predefinito e non quello corrente.

Risoluzione: accertarsi che l'utente sia associato al gruppo corretto nell'archivio utenti. Verificare che in Compliance Manager il nome del gruppo sia stato creato e sia corretto. accertarsi che il gruppo sia associato al criterio corretto in Compliance Manager.

Se si stanno utilizzando le impostazioni di registrazione Use Computer Logon, gli utenti devono accedere ai loro computer utilizzando le credenziali di dominio; in caso contrario, riceveranno il criterio predefinito.

Il computer non esegue la verifica in base a un criterio aggiornato

Importante: Per ulteriori informazioni, consultare la sezione [Problemi di comunicazione con il server \(dall'agente\)](#) a pagina 8.

Causa: se si utilizza il Quarantine Agent, il Policy Refresh Interval non è stato raggiunto e pertanto l'agente non ha recuperato il criterio.

Risoluzione: recuperare il criterio avviando una verifica della conformità, disponibile tramite l'opzione Verifica conformità del menu associato all'icona del Quarantine Agentposta nell'area di notifica.

Le impostazioni o le funzionalità dell'agente non sono correttamente applicate al computer.

Causa: questo problema può essere un effetto collaterale del problema "Il computer non riceve il criterio corretto" o "Il computer non sta eseguendo la verifica in base a un criterio aggiornato".

Risoluzione: verificare che il computer stia ricevendo il criterio corretto e aggiornato (utilizzare il report Agent Session per conferma). In caso contrario, seguire la procedura di risoluzione di "Il computer non sta ricevendo il criterio corretto" o "Il computer non sta ricevendo il criterio aggiornato". Se il computer sta ricevendo il criterio corretto e aggiornato, continuare con la procedura riportata in questa sezione.

Causa: al criterio del computer è stato applicato un modello di configurazione dell'agente errato oppure sono errate le impostazioni nel modello stesso.

Risoluzione: verificare che il corretto modello di configurazione dell'agente sia applicato al criterio del computer e che il modello stesso contenga le impostazioni corrette.

Causa: l'agente non visualizza la skin con la lingua prevista.

Risoluzione: la skin dell'agente viene visualizzata in modo dinamico secondo la lingua predefinita dell'utente, a prescindere dalla lingua del sistema operativo installato nel computer.

L'azione correttiva Enable per i profili Windows Update non funziona.

Causa: il criterio di gruppo non permette l'abilitazione degli aggiornamenti automatici.

Risoluzione: il criterio di gruppo non permette l'abilitazione degli aggiornamenti automatici, impossibile eludere questo problema tramite Compliance Policy. Accertarsi che il criterio di gruppo sia strutturato come previsto e che il criterio NAC sia sincronizzato con Compliance Policy.

L'applicazione non viene rilevata nel computer oppure falsa il rilevamento

Causa: potrebbe esserci un'incongruenza nell'applicazione che si sta di fatto rilevando.

Risoluzione: verificare di aver associato il nome appropriato dell'applicazione al profilo aggiunto al criterio. Le applicazioni sono elencate in Compliance Manager sotto il nome del prodotto principale (o prodotto "core"). A volte l'applicazione è commercializzata con un nome diverso. Per determinare il nome del prodotto principale controllare il prodotto installato oppure rivolgersi al produttore.

Si consiglia di testare il criterio prima di distribuirlo, in modo che l'applicazione, le regole di rilevamento dell'applicazione e le impostazioni del profilo e del criterio siano corrette.

Causa: le regole di rilevamento della funzione Installed per l'applicazione personalizzata sono errate.

Risoluzione: si consiglia di testare il criterio su un gruppo di prova prima di distribuirlo, in modo che l'applicazione, le regole di rilevamento dell'applicazione e le impostazioni del profilo e del criterio siano corrette.

Attivare la registrazione spuntando la casella Abilita registrazione nella finestra di dialogo About e assicurare che il modello di configurazione dell'agente applicato al criterio del computer abbia l'impostazione Logging Agent regolata per messaggi di errore, di avviso, informativi e brief trace. Visualizzare il log dell'API dell'agente (<GUID>_trace.log) per risolvere i problemi di rilevamento.

Nota: La registrazione ha ripercussioni sulle prestazioni; si consiglia quindi di abilitarla esclusivamente per la risoluzione di un problema e di disabilitarla a problema risolto. I file di log per Windows 2000 e Windows XP si trovano nella directory <unità>:\Documents and Settings\All Users\Application Data\Sophos\Sophos NAC\Logs, mentre i file di log per Windows Vista e Windows 7 si trovano nella directory <unità>:\ProgramData\Sophos\Sophos NAC\Logs.

Causa: la data della regola di rilevamento del registro dell'applicazione non è nel formato corretto.

Risoluzione: se si utilizza una data specifica nel rilevamento del registro, assicurarsi che l'applicazione venga rilevata nel computer utilizzando il corretto formato della data. È possibile scegliere System Locale, che determina il formato della data in base alla lingua del sistema, oppure English (U.S.). Per stabilire quale formato utilizzare, si consiglia di installare l'applicazione nel sistema operativo internazionale che si intende supportare, eseguire l'applicazione e determinare il modo in cui le date cambiano o vengono memorizzate per ogni sistema operativo, dal momento che ciò può variare.

Causa: il numero di versione definito nella funzione del profilo oppure la regola di rilevamento dell'applicazione non contiene il numero corretto di cifre significative per la valutazione del computer desiderato.

Risoluzione: la versione viene valutata nel computer utilizzando il numero di cifre significative specificato nella condizione o nella regola di rilevamento. Pertanto, se si definisce una funzione di una versione o si crea una regola di rilevamento con una versione, accertarsi che il numero della versione contenga le cifre significative necessarie per la valutazione del computer desiderato.

Per esempio, se si crea una condizione che specifica == 8 e la versione nel computer è la 8.1, il software confronta 8.1 con 8 (una sola cifra significativa) e la condizione risulta rispettata. Tuttavia, se si crea una condizione che specifica == 8.0 e la versione nel computer è la 8.1, il software confronta 8.1 con 8.0 (due cifre significative) e la condizione risulta non rispettata.

Causa: il formato della data definito nella funzione non corrisponde esattamente a quello generato dalla verifica della conformità.

Risoluzione: se si definisce un profilo per un'applicazione antivirus o antispyware standard, e si specifica una funzione Date (Last Scan Date o Signature Date) tramite l'operatore == (uguale a), accertarsi che la data sia generata dal computer nel formato MM/GG/AAAA. Se l'applicazione genera una data nel formato MM/GG/AAAA HH:MM:SS, il rilevamento può dare esito negativo anche se la data nel computer è identica al valore specificato nella condizione. Per evitare questo problema, durante la definizione delle date si può utilizzare l'operatore >= (maggiore o uguale a) o <= (minore o uguale a) invece di ==, oppure si può testare il criterio prima di distribuirlo, in modo che l'operatore == non falsi il rilevamento.

6.3 Messaggistica e azioni correttive

Nel computer non vengono visualizzati i messaggi e non vengono eseguite le azioni correttive

Causa: agli utenti non vengono visualizzati messaggi.

Risoluzione:

1. Verificare che il criterio sia in modalità Remediate o Enforce. Se si trova in modalità Report Only, i messaggi non vengono visualizzati.
2. Verificare che il messaggio sia stato creato, che sia associato alla corretta condizione del profilo e che la condizione sia soddisfatta nel computer. Utilizzare Compliance Manager per visualizzare il report Agent Session. Il link Assessment Details fornisce i dati del profilo e i messaggi visualizzati agli utenti.

Causa: agli utenti non vengono visualizzati i messaggi nei sistemi operativi in lingue diverse dall'inglese.

Risoluzione: verificare che tutti i profili nel criterio del computer abbiano i messaggi creati in inglese (lingua predefinita) e poi creare messaggi identici nelle altre lingue necessarie.

Causa: nel computer non viene eseguita alcuna azione correttiva.

Risoluzione:

1. Verificare che il criterio sia in modalità Remediate o Enforce. Se si trova in modalità Report Only, le azioni correttive non vengono eseguite.
2. Verificare che un'azione correttiva sia selezionata per la giusta condizione del profilo e che tale condizione sia soddisfatta nel computer. Utilizzare Compliance Manager per visualizzare il report Agent Session. Il link Assessment Details fornisce i dati del profilo e le azioni correttive eseguite nel computer.
3. Se si possiede un criterio che richiede l'aggiornamento automatico, da parte del software, di un file della firma antivirus o antispyware, verificare che il modello di accesso appropriato consenta l'accesso alla posizione del server del file della firma, in modo che l'aggiornamento possa essere implementato.
4. Se sono stati verificati i punti da 1 a 3 e l'azione correttiva non viene ancora eseguita, è possibile che non sia supportata in quel particolare sistema operativo. Se un'azione correttiva è supportata da determinati sistemi operativi, ma non da altri, quelli non supportati verranno visualizzati con una x al loro interno. Accertarsi che l'utente possa correggere l'applicazione in altro modo e che sia stato creato un messaggio per tale funzione dell'applicazione, al fine di dare all'utente le istruzioni per la correzione.

6.4 Patches

L'agente non recupera le patch più recenti

Importante: Per ulteriori informazioni, consultare la sezione [Event Log](#) a pagina 24.

Causa: Sophos NAC Advanced non scarica le patch più recenti.

Risoluzione: utilizzare il comando Server Task Status nella home page di Compliance Manager per verificare che l'operazione Patch Loader non sia riuscita e visualizzarne la causa. La causa più probabile può risiedere nel fatto che il Compliance Application Server non ha accesso in uscita a Internet, necessario per il Patch Loader. Eseguire manualmente l'operazione Patch Loader nel Compliance Application Server per scaricare e aggiornare le informazioni sulle patch. Per ulteriori informazioni, consultare la *Guida all'installazione di Sophos NAC Advanced*.

Causa: patch obsolete per gli agenti meno recenti (3.0.x).

Risoluzione: nel caso in cui il Compliance Application Server non abbia accesso a Internet, accertarsi che il file CAB utilizzato per il rilevamento delle patch venga pubblicato sul Compliance Application Server manualmente. Per ulteriori informazioni, v. il problema "Errori di Patch Loader visualizzati nel Log eventi del Compliance Application Server". Per ulteriori informazioni, consultare la sezione [Event Log](#) a pagina 24.

Causa: un utente con accesso limitato al computer sta utilizzando il Dissolvable Agent.

Risoluzione: il Dissolvable Agent non può svolgere la valutazione delle patch quando eseguito come utente con limitazioni. Cambiare l'utente in modo tale che venga eseguito come amministratore e provare ad utilizzare nuovamente il Dissolvable Agent. Se non è possibile apportare tale cambiamento, Sophos consiglia di creare un criterio a parte per gli utenti del Dissolvable Agent. Tali utenti sono di solito ospiti. 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.

6.5 Date dei file delle firme

Le date dei file delle firme per il software antivirus e antispyware non vengono recuperate dall'agente

Importante: Per ulteriori informazioni, consultare la sezione [Event Log](#) a pagina 24.

Causa: Sophos NAC Advanced non scarica le date più recenti dei file delle firme.

Risoluzione: utilizzare il comando Server Task Status nella home page di Compliance Manager per verificare se l'operazione Patch Loader non è riuscita e visualizzare la causa. La causa più probabile può risiedere nel fatto che il server non ha l'accesso in uscita a Internet necessario per Current Definition Loader. Eseguire manualmente l'operazione Current Definition Loader nel server per scaricare e aggiornare le informazioni sulla data della firma dell'applicazione. Per ulteriori informazioni, consultare la *Guida all'installazione di Sophos NAC Advanced*.

7 Problemi di registrazione

Questa sezione contiene informazioni per la risoluzione dei problemi legati alla registrazione dei computer.

7.1 Registrazione

La registrazione non riesce

Importante: Per ulteriori informazioni, consultare la sezione [Problemi di comunicazione con il server \(dall'agente\)](#) a pagina 8.

L'autenticazione non riesce

Causa: all'agente sono stati passati nome utente o password errati.

Risoluzione: accertarsi che il nome utente e la password utilizzati per eseguire l'agente siano corretti. Il nome utente e la password possono provenire: direttamente dall'utente che li digita nella finestra di dialogo Registrazione o Credenziali oppure dalla riga di comando tramite uno script o altra applicazione, come un dialer.

Causa: l'utente non è configurato nell'archivio utenti del cliente.

Risoluzione: configurare nome utente e password correttamente nell'archivio utenti del cliente (vale a dire AD, NT Domain ecc.).

Causa: mancata corrispondenza con uno shared secret IAS.

Nota: per ulteriori informazioni sull'utilizzo del tool Authentication Test per diagnosticare problemi, consultare la *Guida agli strumenti di Sophos NAC Advanced*.

Risoluzione: per determinare se si sta verificando una mancata corrispondenza con uno shared secret IAS, recuperare il valore shared secret tramite il tool Secret Encryption ed eseguire un test utilizzandolo nel tool Authentication Test. Una mancata corrispondenza dello shared secret genera un errore di risposta non valida simile a:

"Completed Attempt (1): To server 127.0.0.1:1812. Status: InvalidResponse In 2578.1085 mS. Radius request failed after all attempts. Last Reason: InvalidResponse"

Per risolvere questo problema:

Utilizzare il tool Secret Encryption per impostare lo shared secret IAS nell'interfaccia del criterio e nel client RADIUS.

Causa: mancata corrispondenza del tipo di autenticazione.

Nota: per ulteriori informazioni sull'utilizzo del tool Authentication Test per diagnosticare problemi, consultare la *Guida agli strumenti di Sophos NAC Advanced*.

Risoluzione: per determinare se si sta verificando una mancata corrispondenza del tipo di autenticazione, recuperare il valore del tipo di autenticazione dal file Registration Interface Web.config (il predefinito dopo l'installazione è MS-CHAP v2) ed eseguire una prova utilizzandolo nel Tool Authentication Test. In caso di mancata corrispondenza del tipo di autenticazione verrà visualizzato un errore di accesso negato simile a:

"Results: Completed Attempt (1): To server 127.0.0.1:1812. Status: Succeeded Received: AccessReject In 156.249 mS."

Se non si utilizzano dei server proxy RADIUS, nel log degli eventi di sistema verrà riportato un messaggio simile al seguente:

"Resolution/more info - System event log - local authentication method used doesn't match remote access policy. Reason-Code = 66 Reason = The user attempted to use an authentication method that is not enabled on the matching remote access policy."

Per risolvere questo problema:

- Cambiare il tipo di autenticazione nel file Registration Interface Web.config (situato normalmente nella sottodirectory Inetpub\wwwroot\RegistrationInterface del Compliance Application Server) per farlo coincidere con uno di quelli nel server di autenticazione RADIUS.
- Se si utilizzano i server proxy RADIUS, controllare la configurazione o il log del server RADIUS che effettua l'autenticazione per determinare quali sono i metodi di autenticazione utilizzati. Quindi, cambiare il tipo di autenticazione nel file Policy Interface Web.config per farlo coincidere con uno di quelli nel server RADIUS di autenticazione.

Il Log eventi del Compliance Application Server riporta errori relativi all'interfaccia di registrazione

Causa: l'interfaccia di registrazione non riesce a comunicare con RADIUS Enforcer.

Risoluzione: visualizzare l'Event Log del per la presenza di eventuali errori. Se viene visualizzato un errore indicante che nessun tentativo di contattare RADIUS Enforcer è riuscito, verificare l'indirizzo IP, i protocolli e lo shared secret di RADIUS Enforcer nell'interfaccia di registrazione utilizzando il tool Secret Encryption. Per ulteriori informazioni, consultare la *Guida agli strumenti* di *Sophos NAC Advanced*.

8 Problemi di reportistica

Questa sezione contiene informazioni per la risoluzione dei problemi legati ai report.

8.1 Agente

L'agente non crea il report

Importante: Per ulteriori informazioni, consultare la sezione [Problemi di comunicazione con il server \(dall'agente\)](#) a pagina 8.

Causa: la registrazione dell'utente nell'agente è scaduta. Il seguente messaggio di errore viene visualizzato nella finestra di dialogo o pagina Risultati: "The report operation failed due to an expired user registration. You must register the agent".

Risoluzione: l'utente deve registrarsi nell'agente utilizzando l'opzione di menu Registra.

8.2 Compliance Manager

Nel report Agent Session mancano dei dati

Causa: se si utilizza il Quarantine Agent, il Reporting Interval del criterio non è stato raggiunto e pertanto l'agente non ha aggiornato i dati del report.

Risoluzione: aggiornare i dati del report avviando una verifica della conformità, disponibile tramite l'opzione Check Compliance (verifica conformità) del menu associato all'icona del Quarantine Agent posta nell'area di notifica.

I report sono incompleti oppure privi di dettagli

Causa: il servizio Policy Transfer potrebbe non essere in esecuzione.

Risoluzione: avviare Policy Transfer Service nei Compliance Application Server e accertarsi che sia impostato su Automatic.

La creazione di un report con i dati archiviati non produce risultati

Causa: l'operazione Report Warehouse Loader SQL non è mai stata eseguita.

Risoluzione: se questo è vero, il report mostrerà "No Data Available" accanto al nome del report. Utilizzare il comando Server Task Status nella home page di Compliance Manager per verificare che l'operazione Report Warehouse Loader fosse in esecuzione e vedere gli eventuali errori. Confermare che SQL Server Agent è in esecuzione nell'istanza che ospita i Compliance Database. Ogni notte alle 2:30 (a meno che l'orario venga modificato manualmente), SQL Server Agent esegue l'operazione Report Warehouse Loader, che sposta i dati dal database ReportStore al ReportStoreWH. Come migliore pratica, le proprietà di SQL Server Agent devono essere modificate per poter riavviare automaticamente SQL Server Agent nel caso in cui si fermi improvvisamente. Inoltre, il servizio SQLAgent (nome dell'istanza) deve essere in esecuzione. Come migliore pratica, SQLAgent (nome dell'istanza) dev'essere impostato su Automatic.

Per ulteriori informazioni sull'operazione Sophos NAC - Load WH, consultare la *Guida all'installazione* di *Sophos NAC Advanced*.

La creazione di un report con dati archiviati produce risultati obsoleti

Causa: l'operazione Report Warehouse Loader SQL non è stata eseguita di recente.

Risoluzione: se questo è vero, il report mostra "Use Data from the Last Archive (mm/gg/aaaa hh:mm:ss)" accanto al nome del report laddove la data sia più vecchia di 24 ore. Utilizzare il comando Server Task Status nella home page di Compliance Manager per verificare che l'operazione Report Warehouse Loader fosse in esecuzione e vedere gli eventuali errori. Confermare che SQL Server Agent è in esecuzione nell'istanza che ospita i Compliance Database. Ogni notte alle 2:30 (a meno che l'orario venga modificato manualmente), SQL Server Agent esegue l'operazione Report Warehouse Loader SQL, che sposta i dati dal database ReportStore al ReportStoreWH. Come migliore pratica, le proprietà di SQL Server Agent devono essere modificate per poter riavviare automaticamente SQL Server Agent nel caso in cui si fermi improvvisamente. Inoltre, il servizio SQLAgent (nome dell'istanza) deve essere in esecuzione. Come migliore pratica, SQLAgent (nome dell'istanza) dev'essere impostato su Automatic.

Per ulteriori informazioni sull'operazione Sophos NAC - Load WH, consultare la *Guida all'installazione di Sophos NAC Advanced*.

La creazione di un report con dati correnti produce risultati che sembrano obsoleti

Causa: se si utilizza il Quarantine Agent, il Reporting Interval del criterio non è stato raggiunto e pertanto l'agente non ha aggiornato i dati del report.

Risoluzione: aggiornare i dati del report avviando una verifica della conformità, disponibile tramite l'opzione Check Compliance (verifica conformità) del menu associato all'icona del Quarantine Agent posta nell'area di notifica.

Causa: il servizio Agent Report potrebbe non essere in esecuzione.

Risoluzione: avviare Policy Transfer Service nei Compliance Application Server e accertarsi che sia impostato su Automatic.

La creazione di un report con i dati archiviati produce risultati incompleti

Causa: l'operazione Sophos NAC - Load WH SQL non è stata eseguita di recente oppure non è riuscita.

Risoluzione: se questo è vero, il report mostra "Use Data from the Last Archive (mm/gg/aaaa hh:mm:ss)" accanto al nome del report laddove la data sia più vecchia di 24 ore. Utilizzare il comando Server Task Status nella home page di Compliance Manager per verificare che l'operazione Report Warehouse Loader non sia riuscita e visualizzarne la causa. Confermare che SQL Server Agent è in esecuzione nell'istanza che ospita i Compliance Database. Ogni notte alle 2:30 (a meno che l'orario venga modificato manualmente), SQL Server Agent esegue l'operazione Report Warehouse Loader, che sposta i dati dal database ReportStore al ReportStoreWH. Come migliore pratica, le proprietà di SQL Server Agent devono essere modificate per poter riavviare automaticamente SQL Server Agent nel caso in cui si fermi improvvisamente. Inoltre, il servizio SQLAgent (nome dell'istanza) deve essere in esecuzione. Come migliore pratica, SQLAgent (nome dell'istanza) dev'essere impostato su Automatic.

Per ulteriori informazioni sull'operazione Report Warehouse Loader, consultare la *Guida all'installazione di Sophos NAC Advanced*.

9 Problemi relativi agli allarmi

Questa sezione contiene informazioni per la risoluzione dei problemi legati agli allarmi.

9.1 Compliance Manager

Non si ricevono allarmi

Causa: l'Event Log del Compliance Application Server è pieno.

Risoluzione: accertarsi che ci sia spazio su disco a sufficienza per il Log eventi del Compliance Application Server.

Causa: il server della posta elettronica non è adeguatamente configurato.

Risoluzione: cercare gli eventuali errori nel Log eventi del Compliance Application Server. Accertarsi che il traffico SMTP (TCP porta 25) sia aperto tra il Compliance Application Server ed il server della posta elettronica. Assicurarsi inoltre che in Compliance Manager sia configurato il server della posta appropriato (**Configure System > Alerts, Alert E-mail Server setting**).

Causa: Alert Service potrebbe non essere in esecuzione.

Risoluzione: avviare Alert Service nel Compliance Application Server e accertarsi che sia impostato su Automatic.

Causa: gli allarmi non sono configurati correttamente in Compliance Manager.

Risoluzione: si consiglia di testare criteri e allarmi su un gruppo di prova prima di distribuirli, al fine di avere le impostazioni corrette.

10 Problemi del server

Questa sezione contiene informazioni per la risoluzione dei problemi legati al server, **non** riscontrati nel o provenienti dall'agente.

10.1 Compliance Application Server

Il computer di SQL Server non è raggiungibile dal Compliance Application Server di Sophos NAC Advanced

Causa: il Compliance Application Server non è connesso correttamente per poter comunicare con i Compliance Database.

Risoluzione: per verificare la connettività, seguire la seguente procedura nel Compliance Application Server, utilizzando un account del servizio di Sophos NAC Advanced che abbia accesso ai Compliance Database:

1. Creare un nuovo file .txt nel desktop del Compliance Application Server.
2. Rinominare il file conn.udl. L'estensione .udl è **necessaria**.
3. Una volta creato, cliccare due volte sul file conn.udl.
4. Nella finestra Data Link Properties, cliccare sulla scheda **Provider**.
5. Selezionare **Microsoft OLE DB Provider for SQL Server** e cliccare su **Avanti**.
6. Selezionare o digitare il nome o l'istanza di SQL server. Questo nome **deve** essere lo stesso utilizzato nell'installazione del Compliance Application Server.
7. Selezionare il pulsante di opzione **Utilizza protezione integrata di Windows**.
8. Selezionare il pulsante di opzione **Seleziona il database sul server**.
9. Dall'elenco selezionare **PolicyStore**.
10. Cliccare su **Verifica connessione**.

Per informazioni sulle possibili cause dei problemi di connettività e le relative soluzioni, consultare la sezione [Installazione dei Compliance Database](#) a pagina 3 e ["Nessun componente del"](#) a pagina 24 nella

10.2 Server RADIUS

SQL server non è raggiungibile dal server RADIUS

Causa: il server RADIUS non è connesso correttamente per comunicare con i Compliance Database.

Risoluzione: per verificare la connettività, seguire la seguente procedura nel server RADIUS, utilizzando un account del servizio Sophos NAC Advanced che abbia accesso ai Compliance Database:

1. Creare un nuovo file .txt nel desktop del server RADIUS.
2. Rinominare il file conn.udl. L'estensione .udl è **necessaria**.
3. Una volta creato, cliccare due volte sul file conn.udl.
4. Nella finestra Data Link Properties, cliccare sulla scheda **Provider**.
5. Selezionare **Microsoft OLE DB Provider for SQL Server** e cliccare su **Avanti**.

6. Selezionare o digitare il nome o l'istanza di SQL server. Questo nome **deve** essere lo stesso utilizzato nell'installazione del RADIUS server.
7. Selezionare il pulsante di opzione **Utilizza protezione integrata di Windows**.
8. Selezionare il pulsante di opzione **Seleziona il database sul server**.
9. Dall'elenco selezionare **PolicyStore**.
10. Cliccare su **Verifica connessione**.

Per informazioni sulle cause potenziali dei problemi di connettività e le relative soluzioni, consultare la sezione [Installazione dei Compliance Database](#) a pagina 3 e "Nessun componente del Compliance Application Server o del RADIUS server riesce a connettersi ai Compliance Database" nella seguente sezione: [Server SQL](#) a pagina 24.

10.3 Server SQL

Nessun componente del Compliance Application Server o del RADIUS Server riesce a connettersi ai Compliance Database

Causa: Le autorizzazioni per le applicazioni di Sophos NAC Advanced nei Compliance Database non sono impostate correttamente.

Risoluzione:

1. aprire lo snap-in Services nel Compliance Application Server.
2. Guardare Sophos NAC Host Service per identificare sotto quale identità di account è in esecuzione il servizio.
3. Verificare che l'identità dell'account possieda le autorizzazioni per i Compliance Database.

10.4 Event Log

Il log eventi del Compliance Application Server riporta errori del Patch Loader o del Current Definition Loader

Causa: il Compliance Application Server potrebbe non avere accesso a Internet.

Risoluzione:

1. Accertarsi che il Compliance Application Server abbia accesso a Internet.
2. Se si utilizza un server proxy, deve essere configurato nel Compliance Manager. Cliccare su **Configure System > Server Settings** . Cliccare sul nome del server e inserire i dettagli del server proxy nel pannello **Dettagli server**.
3. Se continuano a essere rilevati errori del Patch Loader o del Current Definition Loader, contattare il [Supporto tecnico](#) a pagina 33.

Nota: Non esiste alcuna procedura di facile esecuzione per aggiornare manualmente il Current Definition Loader, quando il Compliance Application Server non ha accesso a Internet. Questo file viene aggiornato ogni ora e la data relativa scade molto velocemente. Questo file contiene le date più recenti delle firme correnti per le applicazioni antivirus e antispyware.

11 Problemi di attuazione

Questa sezione contiene informazioni per la risoluzione dei problemi legati all'attuazione dei criteri di sicurezza in rete.

11.1 Accesso alla rete

Al computer viene negato l'accesso quando invece dovrebbe essere concesso (o viceversa), il computer viene messo in quarantena quando non dovrebbe oppure l'utente riceve uno o più messaggi errati nella finestra di dialogo Risultati

Causa: questo problema può essere un effetto collaterale del problema "Il computer non riceve il criterio corretto" o "Il computer non sta eseguendo la verifica in base a un criterio aggiornato". Per ulteriori informazioni, consultare la sezione [Verifica e attuazione del criterio](#) a pagina 12.

Risoluzione: verificare che il computer stia ricevendo il criterio corretto e aggiornato (utilizzare il report Agent Session di Compliance Manager per conferma). In caso contrario, seguire la procedura di risoluzione di "Il computer non sta ricevendo il criterio corretto" o "Il computer non sta ricevendo il criterio aggiornato". Se il computer sta ricevendo il criterio corretto e aggiornato, continuare con la procedura riportata in questa sezione.

Causa: Agent Enforcer, **RADIUS Enforcer**, o DHCP Enforcer nega l'accesso al computer.

Risoluzione: utilizzare Compliance Manager per visualizzare il report di Agent Enforcer, **RADIUS Enforcer**, o DHCP Enforcer e conoscere il motivo per cui Enforcer ha negato l'accesso al computer. RADIUS Enforcer potrebbe non essere riuscito ad autenticare l'utente.

Causa: al criterio sono associati dei modelli di accesso di Agent Enforcer errati o contenenti impostazioni errate.

Risoluzione: utilizzare Compliance Manager per accertarsi che agli stati dell'agente e agli stati di conformità nel criterio siano applicati i corretti modelli di accesso di Agent Enforcer; verificare che i modelli di accesso di Agent Enforcer utilizzati nel criterio includano le adeguate risorse di rete. Inoltre, accertarsi che le risorse di rete abbiano i corretti nomi degli eseguibili, porte/protocolli e indirizzi IP, se necessari.

Il modello di accesso di Agent Enforcer applicato per impostazione predefinita allo stato di conformità Non-Compliant nel criterio permette l'accesso, a tutti i prodotti Sophos e a Internet, alle reti interne che utilizzano indirizzi IP privati e lo nega a tutto il resto del traffico in uscita. È possibile modificare tali impostazioni creando un nuovo modello di accesso di Agent Enforcer e applicandolo allo stato di conformità Non-Compliant nel criterio del computer.

Se si applica un modello di accesso di Enforcer che impedisce l'accesso alla rete nelle modalità Report Only o Remediate, a tutti i computer verrà negato l'accesso a prescindere dal loro effettivo stato di conformità. Per attuare uno stato di conformità, è necessario modificare la modalità del criterio e selezionare Enforce.

Causa: al criterio o alle impostazioni di Enforcer sono associati dei modelli di accesso di RADIUS Enforcer, DHCP Enforcer, RADIUS Enforcer o DHCP Enforcer errati o contenenti impostazioni errate.

Risoluzione: utilizzare Compliance Manager per accertarsi che ai corretti stati di accesso e di conformità nel criterio e nelle impostazioni di Enforcer siano applicati i corretti modelli di

accesso di RADIUS Enforcer o DHCP Enforcer; verificare che i modelli di accesso di RADIUS Enforcer o DHCP Enforcer contengano le impostazioni corrette.

Se si applica un modello di accesso di Enforcer che impedisce l'accesso alla rete nelle modalità Report Only o Remediate, a tutti i computer verrà negato l'accesso a prescindere dal loro effettivo stato di conformità. Per attuare uno stato di conformità, è necessario modificare la modalità del criterio e selezionare Enforce.

Causa: i modelli di accesso di RADIUS Enforcer o DHCP Enforcer hanno un ordine di priorità errato.

Risoluzione: utilizzare Compliance Manager per accertarsi che l'ordine di priorità dei modelli di accesso di RADIUS Enforcer o DHCP Enforcer nel criterio o nelle impostazioni di Enforcer sia corretto. Dare maggiore priorità ai modelli di accesso più specifici/rigidi e minore priorità a quelli meno specifici/rigidi. I modelli di accesso più specifici/rigidi forniscono un indirizzo IP specifico o un intervallo IP più limitato, mentre quelli meno specifici/rigidi forniscono un intervallo più ampio.

Causa: una risorsa di rete eseguibile non viene rilevata dal software.

Risoluzione: il nome del processo dell'eseguibile deve essere lo stesso visualizzato in Windows Task Manager, scheda Processi.

Il software rileva solo gli eseguibili che girano al livello Winsock. Se l'applicazione non è in esecuzione al livello Winsock, non viene rilevata.

Causa: l'ordine di priorità delle risorse di rete è errato.

Risoluzione: utilizzare Compliance Manager per accertarsi che l'ordine di priorità delle risorse di rete nel modello di accesso di Agent Enforcer sia corretto. Dare maggiore priorità alle risorse di rete più specifiche/rigide e minore priorità a quelle meno specifiche/rigide. Se un computer ha più di una risorsa di rete, la prima di tali risorse determina l'accesso alla rete per la sessione del computer. Le risorse di rete eseguibili vengono valutate prima delle risorse di rete porta/protocollo.

Causa: il computer è esente quando non dovrebbe esserlo o viceversa.

Risoluzione: utilizzare Compliance Manager per accertarsi che il computer **non** costituisca un'esenzione se dev'essere valutato ai fini della conformità. Parimenti, accertarsi che il computer costituisca un'esenzione se **non** dev'essere valutato ai fini della conformità.

Accertarsi che alle esenzioni siano applicati gli appropriati modelli di accesso di RADIUS Enforcer o DHCP Enforcer.

Inoltre, assicurarsi che nell'elenco della pagina Exemptions l'ordine di priorità delle esenzioni sia corretto. Dare maggiore priorità alle esenzioni più specifiche/rigide e minore priorità a quelle meno specifiche/rigide. Se a un computer si applica più di un'esenzione, la prima di tali esenzioni determina l'accesso alla rete per la sessione del computer. Inoltre, se una particolare esenzione contiene più di un modello di accesso, verrà utilizzato il primo modello contenente l'indirizzo IP del RADIUS client, DHCP server o del DHCP relay.

Causa: le regole di rilevamento dell'applicazione sono definite in modo errato in Compliance Manager.

Risoluzione:

1. verificare che le regole di rilevamento dell'applicazione siano definite correttamente in Compliance Manager. Per ulteriori informazioni, v. il problema "L'applicazione non viene rilevata nel computer oppure falsa il rilevamento" nella seguente sezione: [Verifica e attuazione del criterio](#) a pagina 12.
2. Attivare la registrazione spuntando la casella Abilita registrazione nella finestra di dialogo About e assicurare che il modello di configurazione dell'agente applicato al criterio del computer abbia l'impostazione Logging Agent regolata per messaggi di errore, di avviso, informativi e brief trace. Visualizzare il log dell'API dell'agente (<GUID>_trace.log) per risolvere i problemi di rilevamento.

Nota: La registrazione ha ripercussioni sulle prestazioni; si consiglia quindi di abilitarla esclusivamente per la risoluzione di un problema e di disabilitarla a problema risolto. I file di log per Windows 2000 e Windows XP si trovano nella directory <unità>:\Documents and Settings\All Users\Application Data\Sophos\Sophos NAC\Log, mentre i file di log per Windows Vista e Windows 7 si trovano nella directory <unità>:\ProgramData\Sophos\Sophos NAC\Log.

Causa: i profili o le applicazioni personalizzate associati al criterio possono non contenere il sistema operativo del computer e pertanto non essere valutati in modo appropriato.

Risoluzione:

1. Utilizzando Compliance Manager, accertarsi che il sistema operativo del computer sia stato aggiunto come profilo di sistema operativo nel criterio assegnato e che le eventuali applicazioni personalizzate associate al criterio (tramite i profili delle applicazioni) contengano anche il sistema operativo del computer.
2. Utilizzare Compliance Manager per visualizzare il report Non-Compliance Detail o Agent Session, cliccare sul collegamento Assessment Details, per accertarsi che l'agente stia valutando le applicazioni.

Causa: l'ultimo criterio recuperato dal computer è obsoleto secondo il Agent Policy Update Threshold.

Risoluzione: accertarsi che l'ultimo recupero del criterio da parte del computer sia avvenuto nell'intervallo di tempo definito nel campo Agent Policy Update Threshold in **(Configure System > Enforcer Settings)** . Aggiornare i dati del report avviando una verifica della conformità, disponibile tramite l'opzione Verifica conformità del menu associato all'icona del posta nell'area di notifica del Quarantine Agent.

Causa: la casella Override **Enforcers** in Compliance Manager **(Configure System > Enforcer Settings)** è spuntata.

Risoluzione: deselezionare la casella di spunta Override Enforcers e accertarsi che lo stato di accesso predefinito abbia i corretti modelli di accesso assegnati per il tipo di attuazione RADIUS o DHCP.

Causa: il Compliance Agent potrebbe non essere in esecuzione nel computer.

Nota: Questo problema riguarda solo il Quarantine Agent.

Risoluzione:

1. accertarsi che il Compliance Agent sia in esecuzione.
2. Assicurarsi che il servizio Agent API sia in esecuzione.

Causa: l'impostazione Agent Enforcement Action nel criterio (sezione DHCP Agent Settings) è impostata su None e il computer sta ancora utilizzando un indirizzo IP non conforme.

Nota: questo problema riguarda l'attuazione DHCP.

Risoluzione: se l'impostazione DHCP Agent Enforcement Action nel criterio è None e il computer è passato da uno stato non conforme a uno conforme, può non ricevere un indirizzo IP conforme. Modificare l'impostazione Agent Enforcement Action in Release Renew, salvare il criterio ed eseguire una verifica della conformità nel computer.

Causa: l'impostazione Agent Enforcement Action nel criterio (sezione 802.1x Agent Settings) è impostata su None e il computer è ancora assegnato a una VLAN in quarantena.

Nota: questo problema riguarda l'attuazione 802.1x.

Risoluzione: se l'impostazione 802.1x Agent Enforcement Action nel criterio è None e il computer è passato dallo stato non conforme al conforme, può non venire autenticato nuovamente e assegnato a una VLAN conforme. Modificare l'impostazione Agent Enforcement Action in Reauthentication, salvare il criterio ed eseguire una verifica della conformità nel computer.

Causa: l'utente non ha ricevuto alcun messaggio, nonostante che al computer sia stato negato l'accesso o sia stato messo in quarantena.

Risoluzione:

1. Verificare che il messaggio sia stato creato, che sia associato alla corretta condizione del profilo e che la condizione sia soddisfatta nel computer. Utilizzare Compliance Manager per visualizzare il report Non-Compliance Detail o Agent Session. Cliccare sul collegamento Assessment Details per avere i dati del profilo e i messaggi visualizzati agli utenti e capire perché al computer è stato negato l'accesso o è stato messo in quarantena e l'utente non ha ricevuto alcun messaggio.
2. Verificare che il criterio sia in modalità Remediate o Enforce. Se si trova in modalità Report Only, i messaggi non vengono visualizzati. Se si applica il modello di accesso di Enforcer che impedisce l'accesso alla rete nella modalità Report Only, a tutti i computer verrà negato l'accesso a prescindere dal loro effettivo stato di conformità.
3. Accertarsi che i corretti modelli di accesso siano applicati ai corretti stati di conformità e di accesso del criterio; verificare che i modelli di accesso contengano le impostazioni o risorse di rete corrette.

Causa: può esserci un problema con l'installazione nel computer di una o più applicazioni di sicurezza.

Risoluzione:

1. utilizzare Compliance Manager per visualizzare il report Non-Compliance Detail o Agent Session, cliccare sul collegamento Assessment Details per vedere i dettagli della verifica di conformità e determinare i problemi che sta avendo l'agente.
2. Verificare di aver associato il nome appropriato dell'applicazione al profilo aggiunto al criterio. Le applicazioni sono elencate in Compliance Manager sotto il nome del prodotto principale (o prodotto "core"). A volte l'applicazione è commercializzata con un nome diverso. Per determinare il nome del prodotto principale controllare il prodotto installato oppure rivolgersi al produttore.

3. Accertarsi che nel computer le applicazioni di sicurezza previste stiano funzionando normalmente. Per ulteriori informazioni, consultare le informazioni per la risoluzione dei problemi nel sito web dell'applicazione di sicurezza oppure rivolgersi al supporto tecnico.

Causa: problema di accesso alla rete indeterminato.

Risoluzione:

1. accertarsi che il criterio sia corretto.
2. Utilizzare Compliance Manager per visualizzare il report Non-Compliance Detail o Agent Session e cliccare sul collegamento Assessment Details per vedere i dettagli della verifica di conformità.
3. Utilizzare Compliance Manager per visualizzare il report Agent Session e accertarsi che l'agente stia ricevendo il criterio e relativa versione corretti.
4. Utilizzare Compliance Manager per visualizzare i report di Agent Enforcer, RADIUS Enforcer, DHCP Enforcer, RADIUS Exemption o DHCP Exemption e ottenere ulteriori informazioni per risolvere i problemi legati ad accesso alla rete ed esenzioni.

11.2 802.1x

Impossibile autenticarsi all'autenticatore/switch 802.1X

Risoluzione: cercare nel Log eventi di sistema del Compliance Application Server la voce IAS relativa all'utente interessato. Se viene visualizzato il seguente errore, l'utente potrebbe avere un problema di accesso alla rete: " The request was rejected by a third-party extension DLL file".

Importante: Per ulteriori informazioni, consultare la sezione [Accesso alla rete](#) a pagina 25.

Risoluzione: cercare nel Log eventi di sistema del Compliance Application Server la voce IAS relativa all'utente interessato. Se viene visualizzato uno dei seguenti errori, l'utente potrebbe avere un problema di autenticazione: "The connection attempt did not match any remote access policy" o "The remote RADIUS (Remote Authentication Dial-In User Service) server did not process the authentication request".

Importante: Per ulteriori informazioni, consultare la sezione [Impostazioni di configurazione di RADIUS Enforcer](#) a pagina 30.

IAS non può autenticare il computer

Causa: un errore di sistema nel server dell'applicazione NAC informa che EAP è un protocollo non valido; pertanto, il criterio di accesso remoto di IAS non è configurato per il protocollo EAP.

Risoluzione: cercare gli eventuali errori nel Log eventi di sistema del server dell'applicazione NAC. Se viene rilevato un errore per cui AuthenticationEAP è un protocollo non valido, modificare il profilo del criterio di accesso remoto del Compliance Application Server e aggiungere i tipi EAP adeguati per quel determinato computer (**Authentication > EAP Methods**) .

L'autenticatore/switch 802.1x assegna una VLAN non corretta

Causa: l'impostazione Agent Enforcement Action nel criterio (sezione 802.1x Agent Settings) è impostata su None e il computer è ancora assegnato a una VLAN in quarantena.

Risoluzione: se l'impostazione 802.1x Agent Enforcement Action nel criterio è None e il computer è passato dallo stato non conforme al conforme, può non venire autenticato nuovamente e assegnato a una VLAN conforme. Modificare l'impostazione Agent Enforcement Action in Reauthentication, salvare il criterio ed eseguire una verifica della conformità nel computer.

Causa: le impostazioni del modello di accesso RADIUS nel Compliance Manager non sono corrette.

Risoluzione: gli attributi RADIUS sono specifici del produttore del dispositivo. Per informazioni sugli attributi RADIUS necessari per un particolare dispositivo, consultare la documentazione di quest'ultimo.

Causa: le impostazioni del modello di accesso RADIUS in NAC Manager non includono un indirizzo IP che corrisponde all'autenticatore/switch 802.1X.

Risoluzione: fare in modo che le impostazioni del modello di accesso RADIUS includano un indirizzo IP nell'elenco degli indirizzi IP corrispondente all'autenticatore/switch 802.1X.

Causa: le VLAN configurate tramite Compliance Manager non esistono nell'autenticatore/switch 802.1X.

Risoluzione: aggiungere l'adeguata VLAN all'autenticatore/switch 802.1X.

Impossibile utilizzare l'agente quando ci si trova in una VLAN Guest di un autenticatore/switch 802.1X

Causa: la VLAN Guest dell'autenticatore/switch 802.1X potrebbe non consentire l'accesso al server dell'applicazione NAC.

Risoluzione: verificare che la VLAN Guest dell'autenticatore/switch 802.1X consenta l'accesso al Compliance Application Server.

11.3 Impostazioni di configurazione di RADIUS Enforcer

L'utente non può autenticarsi al dispositivo di rete (VPN)

Causa: al computer è assegnato un modello di accesso di RADIUS Enforcer che erroneamente nega l'accesso.

Risoluzione: visualizzare il report di RADIUS Enforcer per sapere quale modello di accesso è stato assegnato al computer e il motivo dell'assegnazione.

Accertarsi che ai corretti stati di accesso e di conformità nel criterio e nelle impostazioni di Enforcer siano applicati i corretti modelli di accesso di RADIUS Enforcer; verificare che i modelli di accesso contengano le impostazioni o le risorse di rete adeguate.

Causa: il criterio di accesso remoto potrebbe essere impostato in modo errato oppure è impostato correttamente ma l'utente non è stato aggiunto all'archivio utenti.

Risoluzione:

1. Utilizzare Compliance Manager per visualizzare il report di RADIUS Enforcer e conoscere il motivo per cui RADIUS Enforcer non ha autenticato l'utente.
2. Rivedere i criteri di accesso remoto. Questa causa può essere verificata cercando nel Log eventi di sistema la voce IAS Event Log per l'utente interessato e il seguente motivo: "The

connection attempt did not match any remote access policy." Per avere un esempio di criterio di accesso remoto, consultare la *Guida all'installazione di Sophos NAC Advanced*.

Causa: il server RADIUS remoto (proxy) ha rifiutato la richiesta.

Risoluzione:

1. Utilizzare Compliance Manager per visualizzare il report di RADIUS Enforcer e conoscere il motivo per cui RADIUS Enforcer non ha autenticato l'utente.
2. Accertarsi che tutte le impostazioni nel server RADIUS di autenticazione siano corrette. Questa causa può essere verificata cercando nel Log eventi di sistema la voce IAS Event Log per l'utente interessato e il seguente motivo: "The remote RADIUS (Remote Authentication Dial-In User Service) server did not process the authentication request". L'indirizzo IP del server di autenticazione elencato sarà quello del server RADIUS remoto che ha rifiutato la richiesta di autenticazione dell'utente. Se è così, per ulteriori informazioni visualizzare i log del server RADIUS remoto.

Causa: i tipi di autenticazione del criterio di accesso remoto IAS e del dispositivo di rete non corrispondono.

Per dispositivo di rete si intende un RAC, un concentratore VPN o altro dispositivo che fa richiesta di autenticazione.

Nota: per ulteriori informazioni sull'utilizzo del tool Authentication Test per diagnosticare problemi, consultare la *Guida agli strumenti di Sophos NAC Advanced*.

Risoluzione: eseguire un test utilizzando il tool del test di autenticazione. Scegliere il metodo di autenticazione utilizzato dal dispositivo di rete. In caso di mancata corrispondenza del tipo di autenticazione verrà visualizzato un errore di accesso negato simile a:

"Results: Completed Attempt (1): To server 127.0.0.1:1812. Status: Succeeded Received: AccessReject In 156.249 mS."

Se non si utilizzano dei server proxy RADIUS, nel log degli eventi di sistema verrà riportato un messaggio simile al seguente:

"Resolution/more info - System event log - local authentication method used doesn't match remote access policy. Reason-Code = 66 Reason = The user attempted to use an authentication method that is not enabled on the matching remote access policy."

Per risolvere questo problema:

- Modificare la configurazione del dispositivo di rete in modo da supportare il tipo di autenticazione oppure modificare il criterio di accesso remoto IAS in modo da supportare il tipo di autenticazione per il dispositivo di rete
- Se si utilizzano dei server RADIUS proxy, modificare la configurazione del dispositivo di rete in modo da supportare il tipo di autenticazione utilizzato dal server RADIUS remoto oppure modificare la configurazione nel server RADIUS remoto per supportare il metodo di autenticazione utilizzato dal dispositivo di rete.

12 Problemi relativi ad applicazioni prodotte da terzi

Questa sezione contiene informazioni sulla risoluzione di problemi legati ad applicazioni prodotte da terzi.

12.1 Applicazioni prodotte da terzi

Un'altra applicazione non funziona

Causa: il modello di accesso di Agent Enforcer impedisce il funzionamento di un'altra applicazione.

Risoluzione: accertarsi che il modello di accesso di Agent Enforcer associato al criterio del computer sia corretto. Tentare di ignorare la quarantena nel computer. Se l'applicazione funziona quando la quarantena è ignorata nel computer, accertarsi che le risorse di rete dell'applicazione siano incluse nel modello di accesso di Agent Enforcer associato al criterio del computer. Inoltre, accertarsi che le risorse di rete abbiano i corretti nomi degli eseguibili, porte/protocolli e indirizzi IP, se necessari.

13 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.com/support/>.
- Scaricando la documentazione del prodotto su <http://www.sophos.com/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.

14 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.