

Domande & Risposte

Q1. Qual'è l'utilizzo delle risorse degli agenti durante il monitoring?

A1. NETWORK: La massima banda utilizzata dall'agente è tra i 15 ed i 30Kbps durante l'interazione dell'utente. Nei periodi di inattività viene utilizzata una banda minima solo per l'healthcheck tra gli agenti e l'Application Server. Per i server si prevede un utilizzo medio di rete direttamente proporzionale al numero complessivo di amministratori che mediamente accedono simultaneamente ai server monitorati. CPU: l'utilizzo del processore sui server monitorati è stimato intorno al 1% quando l'utente è loggato interattivamente. Nei periodi di idle non c'è nessun impatto significativo. DISCO: L'installazione degli agenti sui server monitorati occupa 10 Mb di spazio disco mentre la registrazione degli eventi di una sessione occupa circa 10MB all'ora di spazio DB. RAM: la memoria occupata dall'agente è di circa 10MB

Q2. Sono necessarie licenze terminal per il monitoring delle sessioni standard di remote administration Windows Server (sessione di console + 2 RDP)?

A2. Le licenze TS/Citrix vengono utilizzate solo in presenza di Windows Server Terminal o Citrix. Le sessioni RDP standard sui server Microsoft di qualsiasi versione essi siano utilizzano la normale licenza agent server. Non è richiesto l'acquisto aggiuntivo di licenze server Agent su sistemi TS/Citrix.

Q3. Qual'è la funzione del menu System Log nella Web Console di ObservelT?

A3. Sì. Nella sezione System Log è possibile visualizzare e scaricare i logs relativi agli eventi/errori dell'Application Server e degli Agenti installati sui server remoti.

Q4. Gli eventi di logon/logoff degli utenti vengono registrati all'interno dei monitor log? E' possibile avere un report delle sole sessioni (data e ora inizio fine, utente, doppia autenticazione se utilizzata, server)?

A4. Sì. Ogni sessione tracciata è aperta identificando il time stamp di logon e il time stamp di logoff sul sistema deve essere attivo l'agent e dove l'utente esegue l'autenticazione. Per ogni sessione registrata può essere visualizzato ed esportato da WEB management console un report che contiene il dettaglio con le applicazioni e le finestre aperte durante la sessione. I timestamp di esecuzione dei login e logoff delle sessioni Win e dell'autenticazione di secondo livello sono anche tracciati ed esportati all'interno del monitor log. In caso di inattività con sessioni lasciate in stato di login (senza eseguire logoff del sistema ma chiudendo solo l'RDP), è possibile all'interno delle policy programmare il time out entro il quale il sistema deve ritenere chiuso il log e generare il time stamp di "end session". Nella versione attuale (4.08) all'interno dei monitor log non vengono evidenziati i timestamp di "timeout end session" che sono evidenziati attraverso la Web Management console. I time stamp di login e logoff Windows sono tuttavia esportati regolarmente all'interno del monitor log. Nella prossima release in rilascio entro fine Ottobre 2009 sarà inclusa una nuova funzionalità avanzata di reportistica ed export log automatico.

Q5. ObservelT fornisce documentazione riguardante l'integrazione con prodotti tipo SCOM di terze parti?

A5. Sì. Sul sito di ObservelT è possibile trovare la documentazione online e il documento PDF relativi all'integrazione di ObservelT con SCOM di Microsoft. All'Appendice A del presente documento sono presenti i link per il download. Più in generale, è possibile utilizzare qualsiasi strumento di terze parti in grado di fare il parse dei file di log generati da ObservelT.

Q6. Come viene distribuito l'agente ai server da monitorare? Richiede il reboot del server?

A6. L'installazione dell'agente prevede un installer .MSI ed un .exe che possono essere eseguiti localmente o remotamente attraverso le policy di dominio o sistemi di software distribution di terze parti. Può essere configurato per un'installazione unattended, silent e non richiede nessun reboot. Inoltre è possibile specificare a priori la policy da assegnare al server target in modo da monitorare le sessioni con le impostazioni corrette.

Q7. Sono necessarie licenze specifiche per il cluster MSCS

A7. No, il modello di licenza prevede la distinzione tra Server agent, Terminal Server / Citrix agent e Workstation agent.

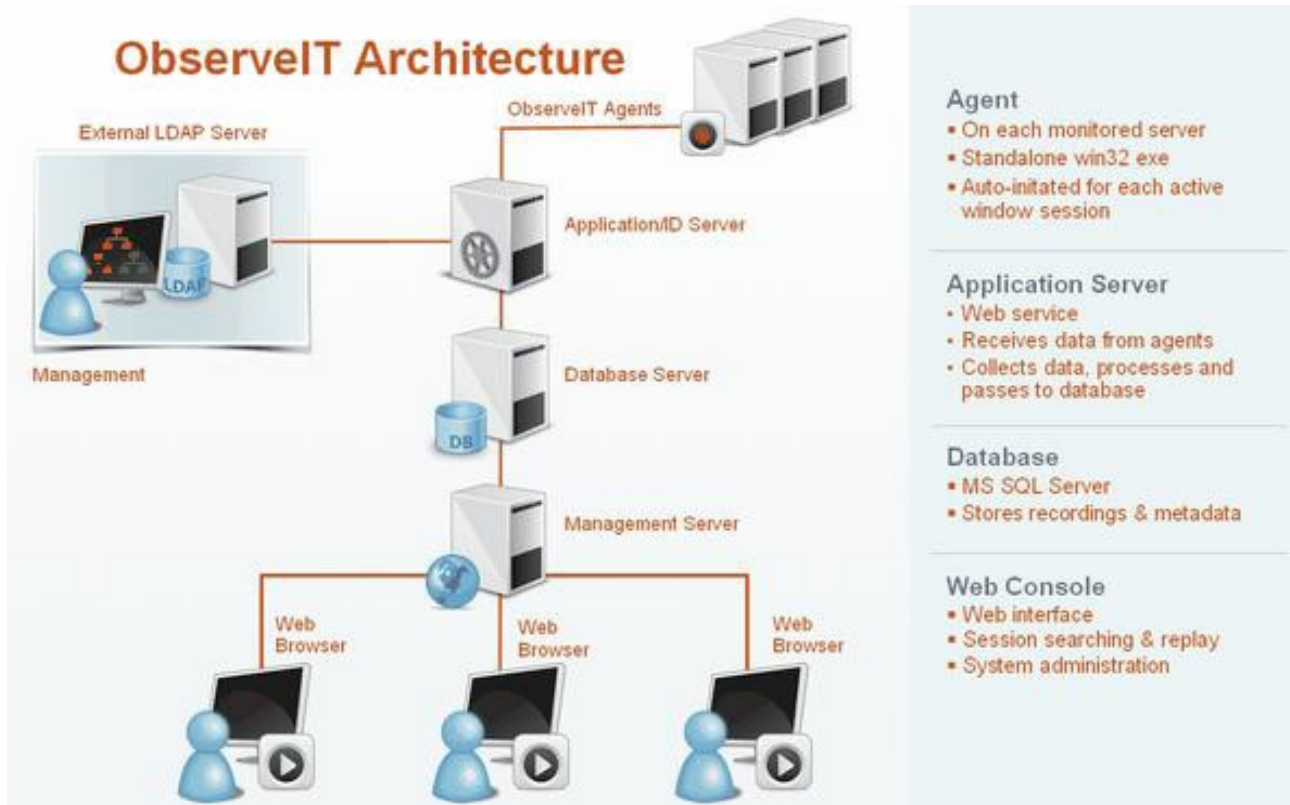
Q8. Esistono best practices per l'utilizzo di ObserveIT all'interno di una VMware-Virtual Infrastructure?

A8. Non sono indicate dal vendor particolari best practices relative all'ambiente virtuale Vmware, tuttavia è disponibile un documento di deployment guide che descrive le Best Practices implementative in ambienti Enterprise sia fisici che virtuali. In fase di definizione della contestualizzazione possono ovviamente essere identificati idonei punti di controllo (VirtualCenter, singole VMs, etc) anche in considerazione delle caratteristiche specifiche dell'ambiente controllato.

Q9. Come funziona nel dettaglio l'agente di ObserveIT?

A9. L'agente di ObserveIT è contenuto all'interno di un pacchetto .MSI , può essere configurato per l'installazione unattended, silent e non richiede reboot. Tra le opzioni di installazione è possibile inoltre specificare la policy da assegnare su quel agente in modo da monitorare le sessioni con le policy corrette ed il percorso del file di log dell'installazione. L'agente è un eseguibile in user-mode che controlla tutte le sessioni avviate dagli utenti. Per ogni sessione, in base alle policy, autorizza, registra ed invia le informazioni all'Application Server. La comunicazione tra l'agente e l'application server avviene attraverso il protocollo http sulla porta configurata in fase di installazione (80 o 4884). In alternativa è possibile utilizzare SSL con il protocollo HTTPS attraverso l'uso di un certificato pubblico. In caso di assenza di connettività tra l'agente e l'application server è possibile configurare un meccanismo di caching attraverso il quale l'agente salverà in locale le registrazioni e si occuperà di inviare le informazioni dinamicamente a connessione ristabilita. L'agente è protetto da un processo watchdog che lo riavvia istantaneamente in caso di kill del processo.

Di seguito un dettaglio dell'architettura:



Q10. E' possibile definire policy differenziate per gruppi di server?

A10. Si. Possono essere create policy differenti da applicare a server o gruppi di server.

Q11. Come vengono applicate e quali sono le tempistiche di deploy delle nuove policy agli agenti già installati?

A11. Ogni agente per controllare le proprie policy interroga l'Application Server all'inizio di ogni nuova sessione monitorata o ogni 15 minuti di inattività

Q12. In caso di disconnessione di una sessione RDP precedentemente doppio-autenticata e di successiva riconnessione alla medesima sessione viene richiesta di nuovo la ri-autenticazione?

A12. Si, verranno registrate due sessioni differenti.

Q13. Quali sono le possibilità di customizzazione nella finestra di doppia-autenticazione e nel banner di segnalazione dell'attività monitorata?

A13. Al momento non è possibile alcuna customizzazione di questi elementi. Questo tipo di personalizzazioni saranno disponibili a partire dalla versione introdotta il prossimo anno.

Q14. In caso di offline dell'Application Server come si comporta l'agente e cosa succede alla Enforce Authentication?

A14. In caso di mancata connessione con l'Application Server, l'Enforce Authentication non è operativa, l'utente quindi può eseguire la login senza ulteriori filtri. Se nelle policy è stato abilitato il meccanismo di caching la sessione verrà comunque registrata ed, appena disponibile la connettività, inviata all'Application Server.

Q15. Come si comporta ObserveIT nel caso in cui l'Application Server sia online e il Database Server offline?

A15. In questo caso l'informazione di down del Database Server viene propagata agli agenti che continuano a registrare le sessioni ed i metadati in locale secondo le policy assegnate (meccanismo di caching).

Q16. Come si comporta l'agente in caso di avvio del server in modalità provvisoria?

A16. In modalità provvisoria l'agente non viene avviato. E' possibile avviarlo manualmente. In questo caso utilizzerà le policy assegnate e se il server è stato avviato con funzionalità network, invierà le informazioni all'Application Server.

Q17. Ci sono anticipazioni sulle nuove funzionalità/ETA/distribuzioni supportate dalla versione Linux/Unix?

A17 L'agent nativo per Unix/Linux sarà disponibile a partire dal Q2 del 2010. Esiste già un preview tecnico delle specifiche funzionali dell'agent linux redatto da ObserveIT. Per maggiori informazioni vedere il documento "Linux – High Level Functional Specifications"

Q18. E' possibile conoscere la dimensione dei dati registrati per ogni singola sessione?

A18. No. Tuttavia l'informazione relativa allo spazio occupato nel DB è dettagliata per singolo agente. E' possibile ottenere una stima di media dello spazio occupato dalle singole sessioni dividendo lo spazio totale occupato per il numero di sessioni.

Q19. E' disponibile un modulo/add-on 'nativo' del prodotto che faccia alerting (smtp, snmp in caso siano intercettati certi eventi)?

A19. Al momento non sono disponibili moduli dedicati. Eventualmente è possibile utilizzare prodotti di terze parti per il monitoring degli events.

Q20. Viene inviata qualche segnalazione in caso di esaurimento dello spazio su file system / Database Server/ Application Server?

A20. No, normalmente il controllo delle quote space viene effettuata attraverso tool di system monitoring di terze parti.

Q21. Quali sono le modalità di gestione del log file utilizzato per il parsing da parte di prodotti di alerting di terze parti? In particolare tale log può essere limitato in dimensioni o tempo, e soggetto a politiche di rollover ?

A21. L'Application e lo User Logs vengono ricreati giornalmente mantenendo lo storico dei giorni precedenti. ObserveIT non integra una politica di rollover per cui è necessario implementare un controllo di terze parti.

Q22. Quali sono le modalità di housekeeping del database?

A22. Nel manuale nella sezione Configuration - Archiving Information and Retention sono indicate le procedure e gli script .SQL per la cancellazione, il backup, l'esportazione ed il rollback dei dati sul DB server.

Q23. Ci sono altre possibilità di esportazione dei dati o la presenza di interfacce con altri prodotti a parte il log file ?

A23. Nella versione che verrà rilasciata a fine anno sarà disponibile un WMI provider.

Q24. E' possibile integrare i report accedendo direttamente ai dati del database?

A24. L'accesso al DB è consentito solo attraverso l'uso dell'Application Server. Nella versione prevista per metà Ottobre sarà ampliata la capacità di reporting avanzato che sarà possibile schedulare automaticamente.

Q25. E' possibile utilizzare i gruppi Active Directory per l'Enforce Authentication?

A25. Nell'attuale versione (v4.08) è possibile selezionare user account di Active Directory. La gestione dei gruppi AD sarà supportata nelle prossime versioni. Questa funzionalità è già presente nella roadmap di sviluppo del prodotto.

Q26. Un utente amministrativo (dba, local admin, etc) a cui non è stato assegnato alcun ruolo nella console di ObserveIT può avere accesso ai dati registrati?

A26. No. I dati relativi alle sessioni registrate sono criptati. Un utente con privilegi di dba o local admin può accedere al DB di ObserveIT per le normali procedure di manutenzione ed eventualmente visualizzare i metadati. Nel caso in cui i metadati fossero oggetto di modifica all'interno del DB il sistema provvederebbe a "macchiare" i video frame relativi con la dicitura "suspected"

Q27. Quali sono le funzionalità di alerting del prodotto in caso di interruzione della registrazione da parte di un agente?

A27. In caso di mancata comunicazione all'interno di una sessione tra l'agente e l'Application Server viene inviata una mail all'amministratore della Web Console. Nel caso in cui, all'interno di una sessione monitorata, venisse attuata un'interruzione forzata dell'Agent un meccanismo di "watchdog" eseguirebbe il suo riavvio.

Q28. E' possibile rimuovere, disinstallare o impedire l'esecuzione dell'agente su un server monitorato?

A28. Un utente con privilegi amministrativi può rimuovere o disinstallare l'agente. Se l'operazione venisse eseguita all'interno della sessione verrebbe monitorata fino alla rimozione. Per impedire la disinstallazione è necessario implementare meccanismi di sicurezza di terze parti.