Informazioni sulle prestazioni di Active Directory Connector

Sommario

Introduzione

In questo documento vengono descritte le prestazioni del connettore Active Directory per il DNS Umbrella.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sul DNS Umbrella.

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

Panoramica

Il servizio Umbrella Connector viene utilizzato per monitorare gli eventi di accesso utente/computer nell'ambito dell'integrazione di Umbrella con Active Directory. Il servizio OpenDNS Connector legge le informazioni di accesso dal registro eventi di protezione di ogni controller di dominio Active Directory presente nel relativo sito.

Negli ambienti con un'elevata frequenza di eventi di accesso degli utenti è importante rivedere queste linee guida sulle prestazioni. Per un'identificazione accurata dell'utente, il servizio Connettore deve essere in grado di recuperare rapidamente le informazioni di accesso.

Numero massimo di eventi/secondo

Non esiste alcun limite rigido al numero di eventi che è possibile elaborare. Il servizio Umbrella Connector viene testato per supportare 850 eventi continui al secondo in tutti i controller di dominio di un "sito". Si basa su un ambiente lab dedicato senza software di terze parti in esecuzione. I risultati reali possono variare in base alla latenza di rete e ad altri colli di bottiglia.

I clienti possono determinare un numero approssimativo di eventi leggendo la sezione "Eventi al secondo" più avanti in questo articolo.

Nuove caratteristiche

Per i clienti in installazioni più grandi con un'alta frequenza di eventi di accesso, Umbrella ha nuove funzioni orientate alle prestazioni. Oltre alle indicazioni generali sulle prestazioni, leggere le linee guida riportate più avanti in questo articolo sul bilanciamento del carico, la comunicazione parallela e la connessione diretta del lettore di log eventi.

Consigli sulle prestazioni

Dimensionamento dei connettori

Il server su cui è in esecuzione il servizio Active Directory Connector deve disporre delle risorse di CPU e di memoria specificate nella Guida al dimensionamento della documentazione di Umbrella.

Connettore dedicato

Sebbene il servizio Connettore possa essere installato direttamente in un controller di dominio, Cisco Umbrella consiglia di installare il connettore in un server membro dedicato al servizio Connettore. Nel server membro non deve essere installato altro software di terze parti. Ulteriori informazioni sul processo di installazione sono disponibili nella documentazione di Umbrella.

Siti Umbrella

Ove possibile, le distribuzioni Umbrella devono essere suddivise in "Siti" che limitano i componenti che comunicano attraverso la rete. Il servizio Connettore è in grado di comunicare solo con i componenti dello stesso sito Umbrella. Questa funzionalità deve essere sempre utilizzata quando gli utenti dispongono di un'installazione distribuita su aree geografiche di grandi dimensioni.

In genere viene creato un sito Umbrella per ogni ubicazione fisica. I siti Umbrella devono rispettare queste regole nella documentazione Umbrella.

Un utilizzo corretto dei siti Umbrella può migliorare notevolmente l'installazione e impedire la comunicazione dei componenti tramite la rete WAN.

Latenza di rete

Gli eventi di accesso possono essere trasferiti al connettore attraverso la rete. È importante che sia disponibile una connessione ad alta velocità tra il connettore e ciascun controller di dominio per ridurre i ritardi relativi alla rete. Il connettore può essere posizionato il più vicino possibile ai controller di dominio e alle appliance virtuali.

Numero di connettori

È necessario un connettore per ciascun sito Umbrella. È possibile avere più connettori in un sito Umbrella, ma è necessario solo per scopi di ridondanza. La presenza di connettori aggiuntivi aumenta il carico sui controller di dominio in quanto questi duplicano la stessa funzione del primo connettore. Umbrella consiglia un massimo di 2 connettori per ogni sito Umbrella.

Dimensione registro eventi

Registri eventi di protezione di Windows di grandi dimensioni possono influire negativamente sulle prestazioni di questa operazione WMI. Umbrella consiglia di limitare le dimensioni del registro eventi. Le prestazioni migliori si ottengono con un file di registro < 512 MB, ma è possibile adattarlo ai requisiti di conservazione dei registri. Per regolare le dimensioni del file di log, attenersi alle seguenti istruzioni:

1. Aprire l'applicazione Visualizzatore eventi (eventvwr.msc).

2. Vai a Registri di Windows > Sistema

3. Fare clic con il pulsante destro del mouse sul registro di sistema e selezionare Proprietà.

4. Sintonizzare le dimensioni massime del file di log e selezionare OK.

Software di terze parti

Alcuni altri prodotti software utilizzano inoltre WMI, che può creare un collo di bottiglia in WMI nel controller di dominio. Ciò può includere:

- Software di sicurezza/analisi di terze parti per il monitoraggio dei registri eventi
- Inoltro registro eventi di Windows
- Integrazione SIEM e altro software per il monitoraggio dei registri eventi

Se uno di questi software non è più necessario, si consiglia di disabilitarlo. In alternativa, è possibile risolvere il problema utilizzando il metodo 'Connessione diretta del lettore di registri eventi' descritto nell'Appendice.

Software antivirus

Escludi questa cartella e questi eseguibili dalla scansione antivirus:

```
C:\Program Files (x86)\OpenDNS\OpenDNS Connector
C:\Program Files (x86)\OpenDNS\OpenDNS Connector\OpenDNSAuditService.exe
C:\Program Files (x86)\OpenDNS\OpenDNS Connector\<VERSION>OpenDNSAuditClient.exe
```

Controller di dominio aggiuntivi

Il sistema di notifica WMI nel controller di dominio accoda ed elabora ogni voce del registro eventi e le invia ai sottoscrittori WMI. Si tratta in effetti di un meccanismo di push in cui gli eventi vengono inviati dal controller di dominio. Di conseguenza, è possibile che si verifichi un collo di bottiglia delle prestazioni sul controller di dominio stesso, che determina la velocità di invio degli eventi.

È possibile ridurre questo collo di bottiglia aggiungendo ulteriori controller di dominio all'ambiente AD. Umbrella ha testato un singolo controller di dominio fino a 850 eventi/sec.

Eccezioni account di servizio

Ridurre il numero di accessi AD rilevati da Umbrella escludendo gli account di servizio. Questi account devono essere comunque esclusi per la corretta applicazione dei criteri. È inoltre possibile escludere i server e altri dispositivi che non utilizzano i criteri utente di Active Directory, ma che possono avere un volume elevato di accessi utente.

Patch WMI

Verificare che il controller di dominio e il server di connessione siano aggiornati con le patch Microsoft più recenti. Di seguito sono riportati alcuni esempi di aggiornamenti rapidi per la risoluzione di problemi noti relativi alle prestazioni WMI.

Limiti handle e memoria WMI

WMI presenta limiti interni specifici che possono creare un collo di bottiglia. Ciò è particolarmente vero quando anche altri software eseguono operazioni WMI intensive. Un esempio di come aumentare questi limiti è disponibile nella documentazione di Microsoft.

Il supporto Umbrella non è in grado di comunicare i limiti corretti per l'ambiente. Contattare Microsoft per assistenza.

Load balancing DC

Umbrella ora supporta una funzione di bilanciamento del carico che è utile quando un sito dispone di più controller di dominio e un numero elevato di eventi di accesso. In questo scenario vengono installati ulteriori connettori e i controller di dominio vengono quindi assegnati a un connettore tramite un gruppo di bilanciamento del carico.

In un ambiente semplice, il bilanciamento del carico funziona nel modo seguente:

- DC_A e DC_B sono assegnati al gruppo di bilanciamento del carico Group_1 gestito da Connector_1.
- DC_C e DC_D sono assegnati al gruppo di bilanciamento del carico Group_2 gestito da Connector_2.
- Le appliance virtuali continuano a ricevere eventi da entrambi i connettori, pertanto sono comunque a conoscenza di tutti gli eventi di accesso.
- Se è richiesta la ridondanza, è possibile installare un connettore aggiuntivo in ciascun gruppo di bilanciamento del carico.

Questa funzione offre i seguenti vantaggi:

- Il carico di lavoro di ciascun connettore è notevolmente ridotto. Ogni connettore gestisce un numero inferiore di controller di dominio.
- Ciò è in genere utile in scenari in cui si verifica un ritardo elevato nella ricezione di eventi da un controller di dominio.

Il bilanciamento del carico può essere scalato per l'utilizzo in ambienti multisito complessi con molti controller di dominio. L'utilizzo del bilanciamento del carico non presenta alcun inconveniente se non si installano altri connettori.

A questo punto, la funzionalità di bilanciamento del carico deve essere abilitata dal supporto Umbrella. Contatta l'assistenza Umbrella per discutere le tue esigenze.

Comunicazione parallela appliance virtuale

Il connettore è ora in grado di inviare eventi di accesso a più appliance virtuali in parallelo, anziché utilizzare il metodo seriale predefinito. Ciò è utile quando un sito dispone di più appliance virtuali e di un numero elevato di eventi di accesso.

Questa funzione offre i seguenti vantaggi:

- Riduce al minimo i ritardi nell'invio delle informazioni di accesso quando sono presenti più

appliance. Un evento può essere inviato a tutti gli accessori contemporaneamente.
- Impedisce problemi di comunicazione o interruzioni con un accessorio che influisce su altri accessori. Viene gestita una coda di eventi separata per ciascuna coda.

Questa funzione è ora attivata automaticamente, ma solo quando il server soddisfa i requisiti di CPU e memoria .

Trasmissione accelerata degli eventi di accesso degli utenti

Il connettore è ora in grado di trasmettere gli eventi di accesso utente in batch, aumentando in modo significativo il numero di eventi al secondo che possono essere inviati all'appliance virtuale (al secondo). Ciò è particolarmente importante per i connettori che comunicano con dispositivi virtuali in postazioni remote.

Questa funzionalità può essere abilitata automaticamente, ma presenta i seguenti requisiti:

- È necessario abilitare la comunicazione parallela (sopra). Il server deve soddisfare i requisiti di CPU e memoria.
- ADC versione 1.8+ richiesta
- Connector versione 3.2.0+ richiesto

Connessione diretta lettore registro eventi

La versione 1.4+ di Connettore Active Directory supporta un nuovo metodo per la connessione diretta al registro eventi di sicurezza dei controller di dominio senza utilizzare una query WMI. In questo modo WMI viene eliminato come "intermediario" e le prestazioni risultano notevolmente migliorate nei casi in cui si verifichino colli di bottiglia. Ciò è particolarmente utile negli scenari in cui i singoli controller di dominio elaborano un numero elevato di eventi di accesso.

Questa funzione utilizza un meccanismo di pull nel quale il connettore trascina i nuovi eventi ogni 5 secondi; è quindi possibile identificare l'utente corretto con un breve ritardo, ad esempio 5 secondi.

Questa ottimizzazione è ora attivata per impostazione predefinita. Per ulteriori informazioni su questa funzione, contatta il supporto Umbrella.

Eventi al secondo

È possibile contare il numero di eventi recenti in un controller di dominio per stimare gli eventi al secondo. Umbrella consiglia di farlo nei momenti di massimo traffico:

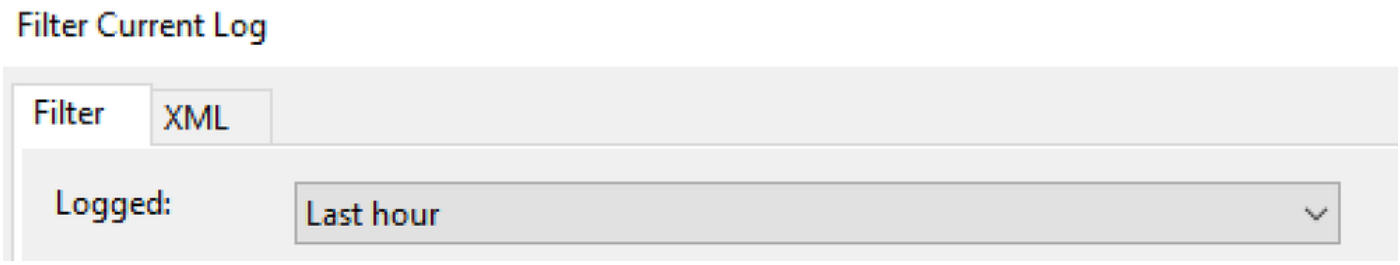
1. Aprire l'applicazione Visualizzatore eventi (eventvwr.msc).

2. Andare a Windows Logs > System.

3. Selezionare Filtra registro corrente e selezionare gli eventi registrati nell'ultima ora.

4. Selezionare OK.

Una volta caricato il filtro, il registro eventi può visualizzare il numero di eventi nell'ultima ora. Questo valore può essere diviso per 3600 per stimare gli eventi al secondo.



360024901511

360024894112

Informazioni su questa traduzione

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