Configurare utenti, gruppi e computer da Active Directory per la sincronizzazione con il servizio Connettore OpenDNS

Sommario

Introduzione

Panoramica

- Autorizzazioni predefinite
- Visualizza accesso effettivo
- Impostazione delle autorizzazioni LDAP di OpenDNS_Connector
- script userPerms

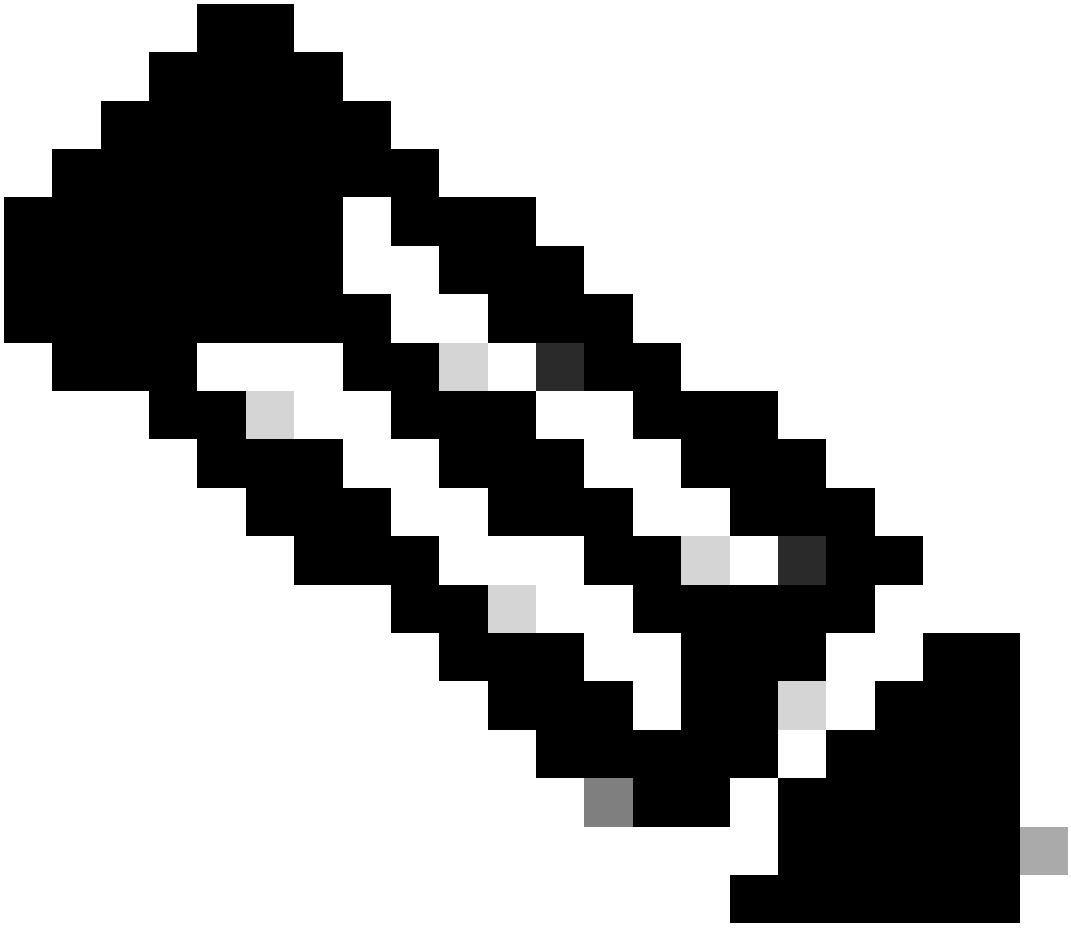
Introduzione

In questo documento viene descritto come sincronizzare utenti, gruppi e computer da Active Directory con il servizio OpenDNS Connector.

Panoramica

Nell'ambito di questa operazione, il servizio OpenDNS Connector sincronizza un elenco di utenti, gruppi e computer da Active Directory utilizzando il protocollo LDAP. In questo articolo viene descritto come verificare che l'account OpenDNS_Connector disponga delle autorizzazioni corrette per leggere tali oggetti.

A ogni oggetto (utenti/gruppi/computer) in Active Directory sono associate autorizzazioni di protezione ACL e ogni oggetto deve consentire all'account utente OpenDNS_Connector di leggere i relativi attributi.



Nota: In questo articolo si presume che i normali prerequisiti per l'account 'OpenDNS_Connector' siano già stati controllati. Se nel dashboard non sono presenti utenti/gruppi di Active Directory, vedere prima questo articolo: [Utenti/gruppi AD mancanti dal dashboard Umbrella.]

Autorizzazioni predefinite

Per impostazione predefinita, tutti gli utenti autenticati possono leggere le proprietà di utenti/gruppi/computer, pertanto l'utente OpenDNS_Connector non richiede autorizzazioni aggiuntive per eseguire la sincronizzazione LDAP.

Le autorizzazioni predefinite sono generalmente impostate come segue:

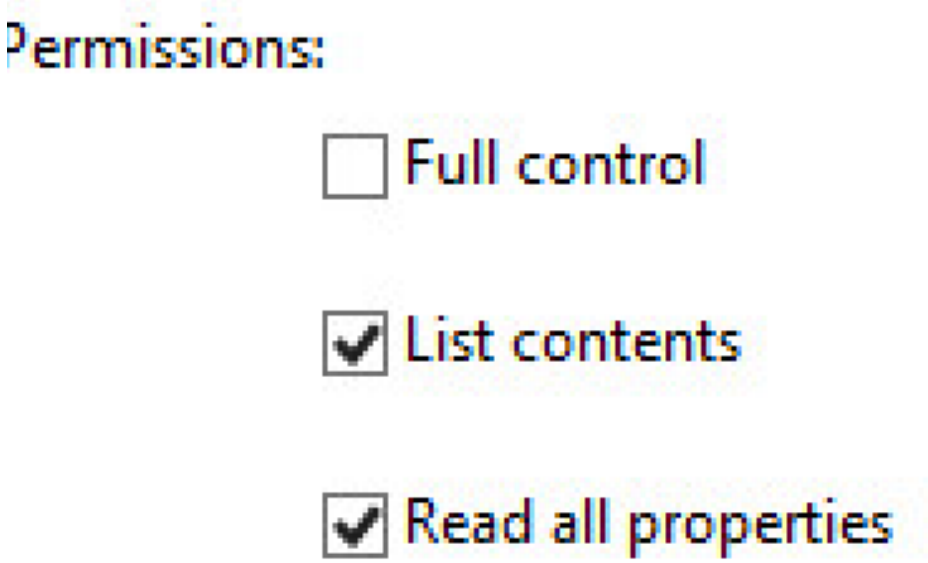
1) Al gruppo 'Accesso compatibile precedente a Windows 2000' vengono assegnate autorizzazioni di lettura (lettura di tutte le proprietà) nel dominio per 'Oggetti utente discendenti', 'Oggetti gruppo discendente' e 'Oggetti computer discendenti'.

È possibile effettuare un doppio controllo come indicato di seguito:

- Apri Utenti e computer di Active Directory
- Fare clic su 'Visualizza' e selezionare l'opzione 'Caratteristiche avanzate'.
- Fare clic con il pulsante destro del mouse sull'oggetto Domain e selezionare 'Proprietà', quindi 'Protezione > Avanzate'
- Selezionare la voce 'Accesso compatibile precedente a Windows 2000' con autorizzazioni 'Speciali':

115011616667

- Fare clic su 'Modifica' per visualizzare i dettagli di queste autorizzazioni.
- Selezionare 'Oggetti utente discendenti' nella sezione Si applica a
- Cercare le autorizzazioni seguenti:

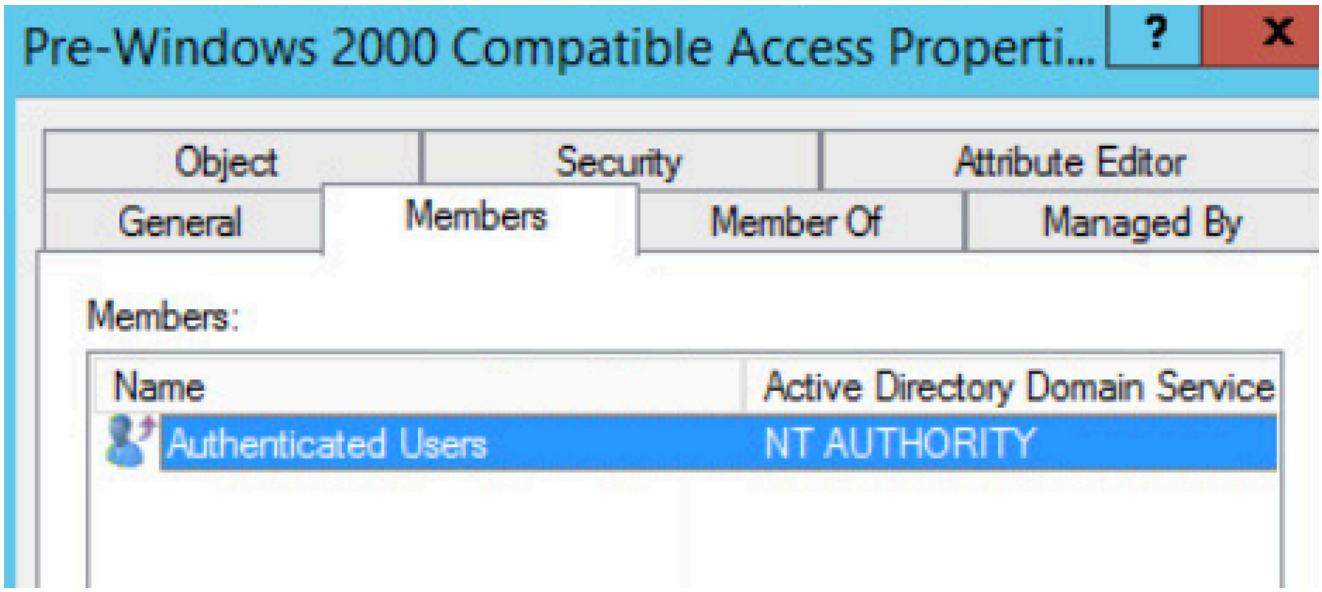


115011616687

- Ripetere questi passaggi per 'Oggetti gruppo discendente' e 'Oggetti computer discendenti'

2) Il gruppo All 'Authenticated Users' è membro del gruppo 'Accesso compatibile precedente a Windows 2000' che fornisce queste impostazioni a tutti gli utenti.

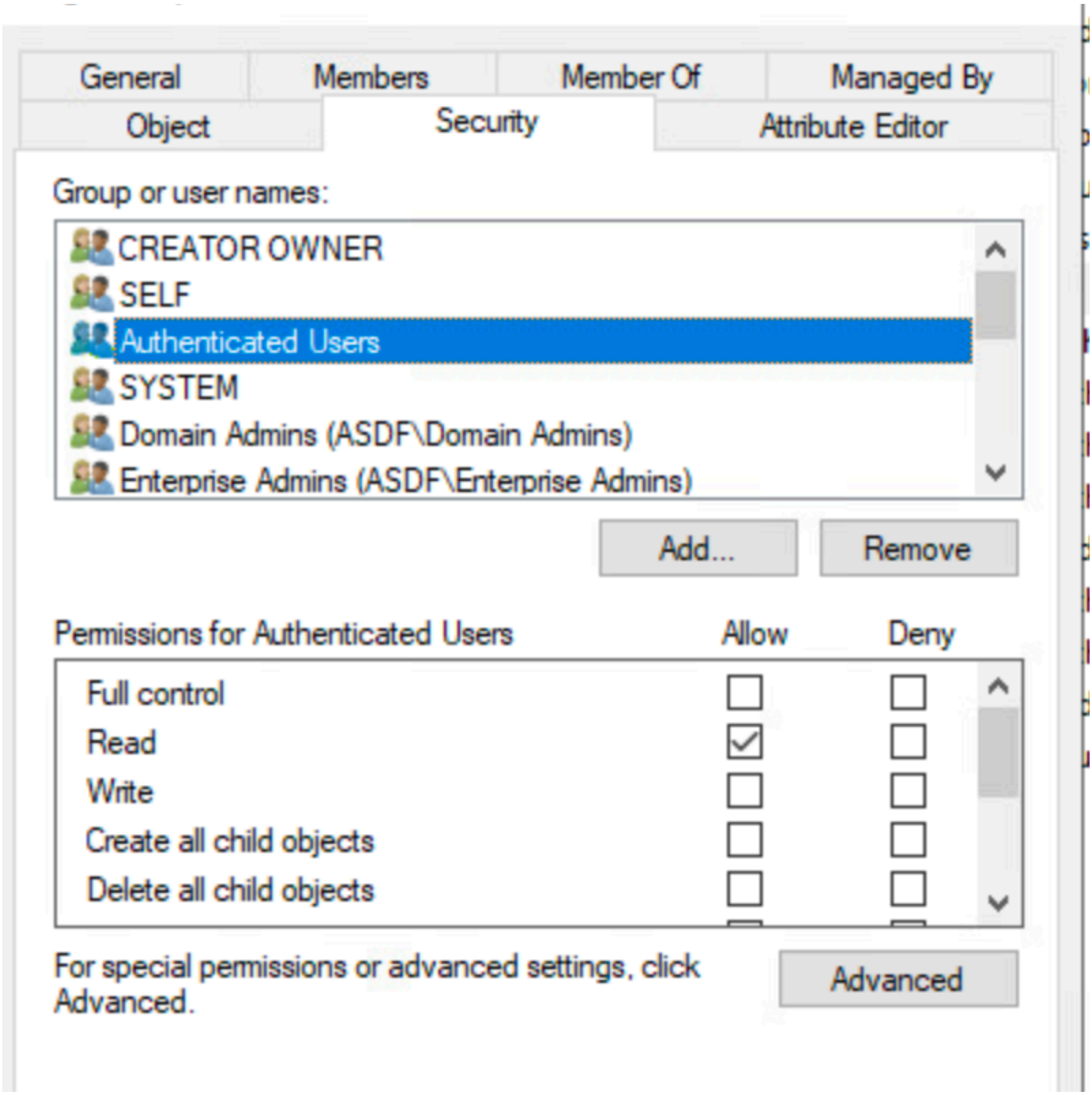
- Fare clic con il pulsante destro del mouse sul gruppo Accesso compatibile precedente a Windows 2000, che in genere si trova nel contenitore Active Directory predefinito.
- Selezionare 'Proprietà' e passare alla scheda 'Membri'.
- Verificare se è elencato 'Utenti autenticati'.



115011616707

Tuttavia, in alcuni ambienti AD questo modello di autorizzazioni potrebbe essere stato modificato e gli utenti autenticati sono stati rimossi. Questo potrebbe rivelarsi come un caso di utenti mancanti dal dashboard Umbrella o di appartenenza a gruppi non corretta. In questo caso, aggiungere l'utente OpenDNS_Connector a questo gruppo, riavviare il servizio di connessione e gli elementi mancanti verranno visualizzati in Umbrella.

In alcuni rari casi, questo non risolve ancora il problema. In questo caso, controllare la scheda Protezione gruppi in Active Directory e verificare che gli utenti autenticati siano elencati con l'opzione Archivia accesso in lettura. Se l'opzione non è selezionata, disattivarla e riavviare il servizio connettore per verificare se i membri del gruppo sono visualizzati. Inoltre, se riscontrano che questa impostazione di protezione non è presente in tutti i gruppi, devono applicare le modifiche a tutti i gruppi in blocco.



28728163336852

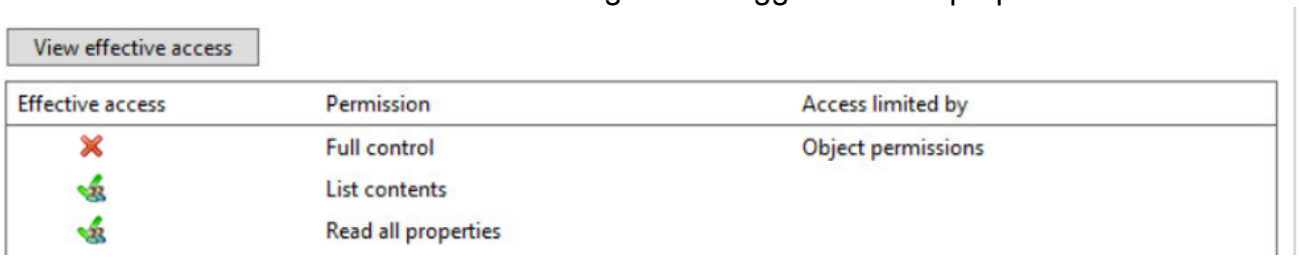
Visualizza accesso effettivo

È possibile utilizzare lo strumento 'Accesso effettivo' di Windows per verificare se l'utente OpenDNS_Connector è in grado di leggere un particolare oggetto mancante o con appartenenza a un gruppo non corretta.

- Apri Utenti e computer di Active Directory
- Fare clic su 'Visualizza' e selezionare l'opzione 'Caratteristiche avanzate'.
- Individuare l'oggetto utente e fare clic con il pulsante destro del mouse per selezionare

'Proprietà'

- Andare alla pagina 'Protezione > Avanzate > Accesso effettivo' (può dire 'Autorizzazioni valide')
- Fare clic su 'Seleziona un utente', quindi selezionare l'account utente 'OpenDNS_Connector'.
- Fare clic su 'OK', quindi su 'Visualizza accesso effettivo'
- Verificare che l'utente del connettore sia in grado di leggere tutte le proprietà:

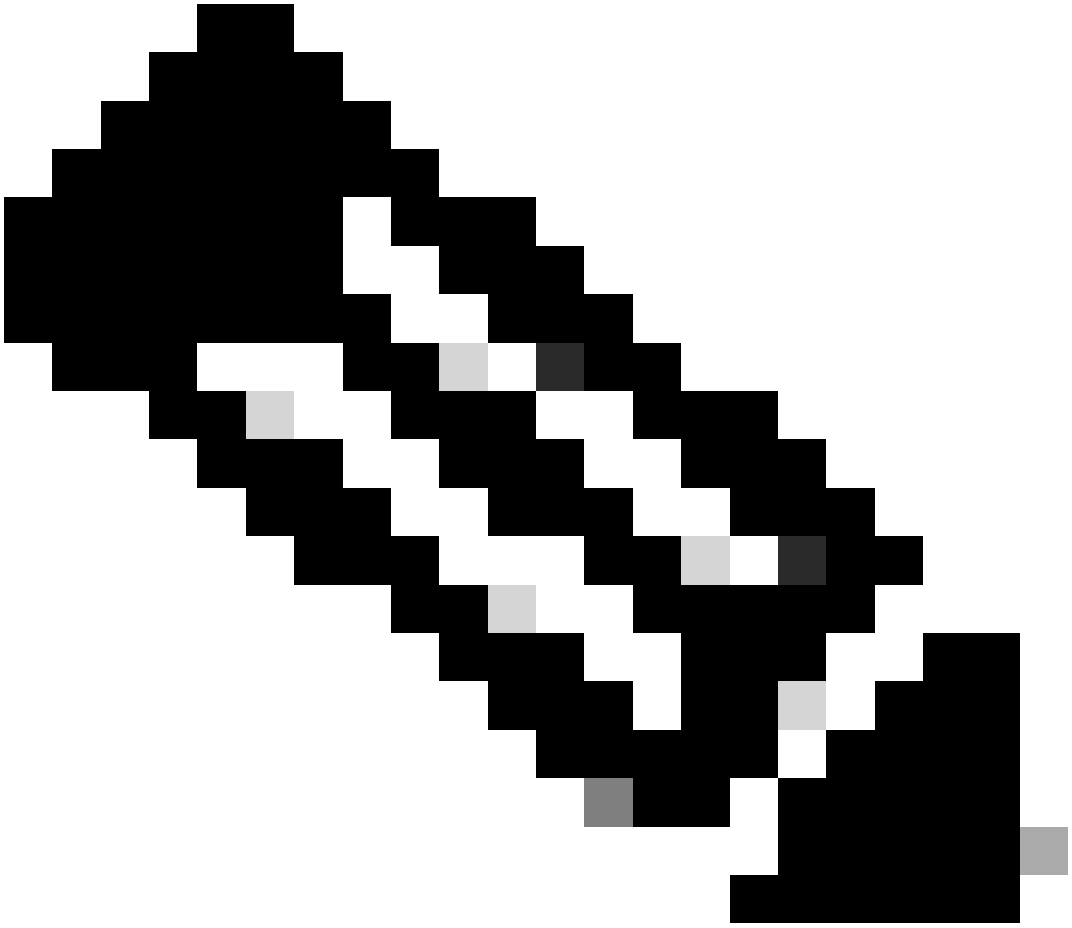


115011616727

Impostazione delle autorizzazioni LDAP di OpenDNS_Connector

La procedura guidata 'Controllo delegato' in Active Directory consente di assegnare rapidamente le autorizzazioni necessarie all'utente 'OpenDNS_Connector':

1) Passare a Strumenti di amministrazione e aprire lo snap-in Utenti e computer di Active Directory.
2) Fare clic con il pulsante destro del mouse sul dominio che include OpenDNS_Connector e selezionare "Delegate Control...", quindi fare clic su Avanti.
3) Aggiungere l'utente OpenDNS_Connector, quindi fare clic su Avanti.
4) Selezionare "Read all user information" (Leggi tutte le informazioni utente) e fare clic su Next (Avanti). [Vedi figura 3.]
7) Fare clic su Fine. [Vedi figura 6.]



Nota: Questi passaggi possono avere esito negativo se l'ereditarietà è disabilitata su alcuni oggetti. Per questi oggetti è necessario impostare le autorizzazioni manualmente.

script userPerms

Lo script PowerShell associato è un altro metodo per ottenere le autorizzazioni di un oggetto specifico, ad esempio utente) in Active Directory. Includere l'output di questo script quando si contatta il supporto tecnico Umbrella.

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).