Host Access for the Cloud

Documentazione

Agosto 2020

Le sole garanzie valide per prodotti e servizi di Micro Focus, le sue affiliate e i concessori di licenza ("Micro Focus") sono specificate nelle dichiarazioni esplicite di garanzia che accompagnano tali prodotti e servizi. Nulla di quanto riportato nel presente documento deve essere interpretato come garanzia aggiuntiva. Micro Focus non sarà da ritenersi responsabile per errori tecnici o editoriali contenuti nel presente documento né per eventuali omissioni. Le informazioni di questo documento sono soggette a modifiche senza preavviso.

Questo documento contiene informazioni riservate. Salvo diversamente e specificatamente indicato, per il possesso, l'uso o la copia è richiesta una licenza valida. In conformità con il regolamento federale sugli acquisti (Federal Acquisition Regulation, FAR), sezioni 12.211 e 12.212, il software commerciale per computer e la relativa documentazione, nonché i dati tecnici per gli oggetti commerciali, vengono concessi in licenza al governo degli Stati Uniti mediante una licenza commerciale standard del produttore.

Per ulteriori informazioni sulle note legali, i marchi di fabbrica, le dichiarazioni di non responsabilità, le garanzie, le esportazioni e altre limitazioni di utilizzo, i diritti del governo degli Stati Uniti, le policy sui brevetti e la conformità FIPS, consultare https://www.microfocus.com/about/legal/

Sommario

Informazioni su Host Access for the Cloud

Il client Web Host Access for the Cloud consente accesso HTML5 basato su browser ad applicazioni host 3270, 5250, VT, UTS e T27. senza la necessità di toccare il desktop, distribuire software, applicare patch o effettuare configurazioni. È possibile fornire agli utenti un accesso a tutte le applicazioni host, indipendentemente dalla piattaforma.

Il client Web utilizza una protezione delle sessioni completa tramite SSL/TLS, per proteggere la comunicazione con i sistemi mainframe.

1 Note di rilascio

La versione 2.5.1 di Host Access for the Cloud è stata rilasciata ad Agosto 2020. Queste note di rilascio illustrano le funzioni e i problemi noti di questa versione, oltre alle informazioni su come ottenere il prodotto. Host Access for the Cloud fornisce l'emulazione del terminale per i tipi di host 3270, 5250, VT, ALC, UTS e T27, richiedendo soltanto un browser che supporti HTML 5.

Management and Security Server

Host Access for the Cloud 2.5.1 rilasciato con Management and Security Server versione 12.6 SP1 Update 1.

Nota: Il Contratto di licenza utente (EULA) è disponibile in inglese, spagnolo, francese, italiano e tedesco nella directory `<percorso di installazione>\licenses`.

Novità

Host Access for the Cloud (in precedenza Reflection ZFE) supporta i requisiti dei clienti per l'accesso all'host nel nuovo e lungo periodo; evidenziando il passaggio alle tecnologie cloud, sia localmente che non localmente.

Tutte le versioni sono cumulative e questa versione di Host Access for the Cloud contiene tutto ciò che è stato rilasciato in tutte le versioni precedenti di Host Access for the Cloud e Reflection ZFE.

- Funzioni e correzioni includono:
  - Gli utenti di Host Access for the Cloud, Reflection Desktop e InfoConnect Desktop ora possono avviare tutte le sessioni da un nuovo portale consolidato basato su HTML (non è necessario Java). Per ulteriori informazioni, vedere le Note di rilascio di MSS. (2.5.1)
  - In questa versione, Host Access for the Cloud include aggiornamenti di stile. (2.5)
  - Sono state aggiunte funzionalità di stampa sia per i tipi di host UTS che AS/400. Per informazioni, vedere Stampa. (2.5)
  - In questa versione è stata aggiunto il trasferimento file AS/400. Ora è possibile trasferire i dati tra il computer e un host iSeries 5250. Per ulteriori informazioni, vedere la documentazione di Trasferire file. (2.5)
  - Ora è disponibile la funzionalità **Ripristina impostazioni predefinite** per gli amministratori e gli utenti finali. Questa opzione consente di ripristinare lo stato originale delle impostazioni e delle opzioni di visualizzazione. Vedere Impostare le preferenze utente. (2.5)
- Numerose correzioni di bug e aggiornamenti di sicurezza.

Modifiche a comportamento e utilizzo

Queste modifiche possono influenzare l'installazione esistente di Host Access for the Cloud.

- A partire da Chrome versione 80, l'accesso a HACloud mediante l'SDK di JavaScript è limitato a HTTPS. Ciò è dovuto a nuove restrizioni di sicurezza correlate ai cookie di terze parti (Samesite) introdotte dal team del browser Chrome. Inoltre, l'utilizzo di Chrome versione 80 o successiva impedisce l'accesso a HACloud se si utilizza il connettore JavaScript antecedente alla versione 2.4.3 (tramite HTTPS o HTTP).

Problemi noti

Il supporto tecnico Micro Focus è sempre disponibile per assistere l'utente su eventuali problemi che può riscontrare in Host Access for the Cloud.

I problemi irrisolti dalle versioni precedenti sono elencati in Riferimenti tecnici sotto Problemi noti.

Contatti di Micro Focus

Per problemi specifici con il prodotto, contattare il Supporto di Micro Focus (https://www.microfocus.com/support-and-services/).

Ulteriori informazioni tecniche o suggerimenti sono disponibili da diverse origini:

- Documentazione del prodotto, articoli della knowledge base e video. Vedere il sito del supporto per Host Access for the Cloud.
- Pagine della Community Micro Focus, vedere Micro Focus Communities.

Note legali

Per ulteriori informazioni sulle note legali, i marchi di fabbrica, le dichiarazioni di non responsabilità, le garanzie, le esportazioni e altre limitazioni di utilizzo, i diritti del governo degli Stati Uniti, le policy sui brevetti e la conformità FIPS, consultare https://www.microfocus.com/about/legal/.

Le uniche garanzie per questo prodotto e per gli aggiornamenti o servizi correlati sono quelle eventualmente descritte nelle dichiarazioni di garanzia specifiche che accompagnano il prodotto o in un contratto di garanzia applicabile accettato dall'utente. Nulla del presente documento deve essere interpretato come garanzia di prodotto, di aggiornamenti o di servizi. Le informazioni contenute in questo documento sono soggette a modifiche senza preavviso e sono fornite "COME SONO" senza garanzie o condizioni espresse o implicite. Micro Focus non potrà essere ritenuta responsabile per omissioni oppure errori tecnici o di altro tipo contenuti in questo documento. Vedere il contratto di licenza utente applicabile del prodotto per dettagli su termini e condizioni di licenza, garanzie e limitazioni di responsabilità.

I collegamenti a siti Web di terze parti accedono al di fuori dei siti Web di Micro Focus e Micro Focus non ha alcun controllo e non è responsabile per le informazioni contenute nei siti di terze parti.

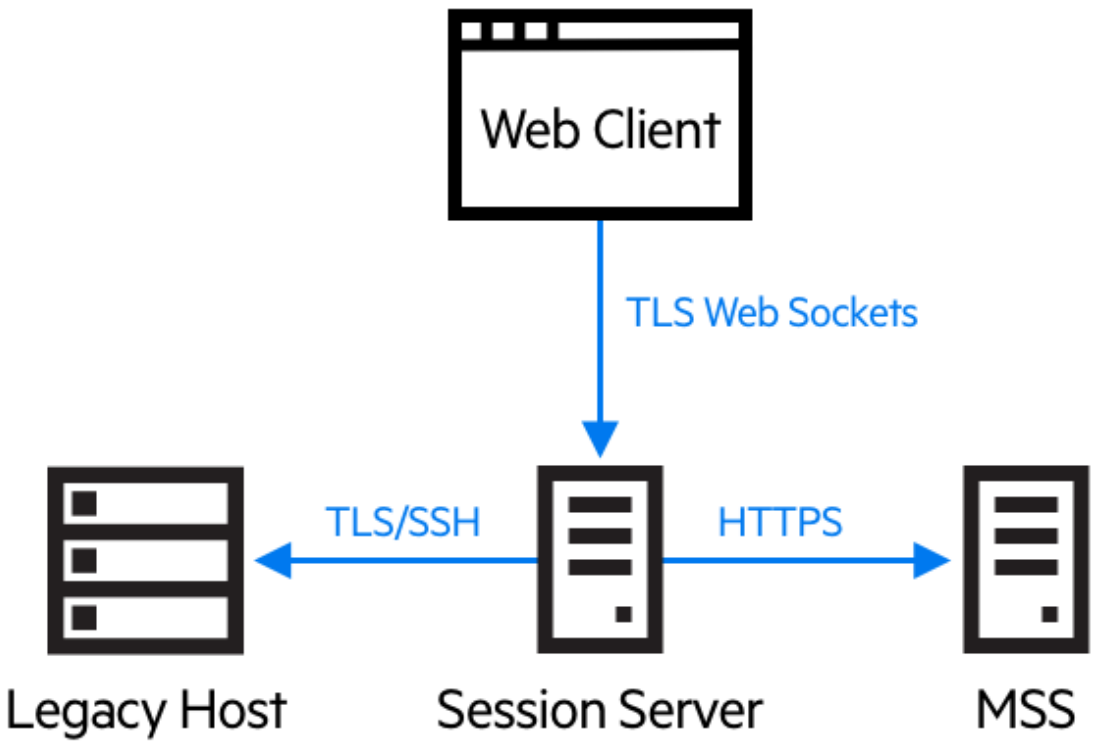
2 Introduzione

Host Access for the Cloud fornisce l'emulazione di terminale a impatto zero che consente l'accesso HTML5 basato su browser ad applicazioni host 3270, 5250, VT, UTS, ALC e T27 senza la necessità di toccare il desktop o installare e gestire ambienti di runtime Java. Una postazione amministrativa centralizzata riduce i costi dell'IT e il tempo di gestione dal desktop, fornendo al contempo un efficiente accesso all'host agli utenti finali. La sicurezza della comunicazione è offerta dalla protezione HTTPS, SSL/TLS e SSH.

Fasi successive

- Come funziona
- Valutazione di Host Access for the Cloud
- Procedura dettagliata di Host Access for the Cloud

Come funziona



Componenti

Acquisire familiarità con questi tre componenti:

- **Host Access Management and Security Server**

  Host Access Management and Security Server (MSS) include Administrative Console, una postazione centralizzata basata sul Web dalla quale è possibile aggiungere, modificare ed eliminare sessioni di terminale. MSS fa parte dell'ampia gamma di prodotti realizzati nel tempo da Micro Focus ed è compatibile con altri prodotti della stessa società. L'icona MSS visualizzata nell'intera documentazione indica le aree in cui sono necessarie configurazioni aggiuntive in MSS Administrative Console.

- **Server di sessione**

  Il server di sessione è un servizio NT o daemon UNIX che fornisce il motore che esegue le sessioni host. Più server di sessione possono servire fino a decine di migliaia di sessioni e fornire un accesso rapido ed efficiente ai dati dell'host.

- **Client Web**

  Il client Web è un emulatore di terminale basato sul Web che gli utenti possono utilizzare facilmente per accedere a sessioni autorizzate da qualsiasi piattaforma e posizione.

  Il client Web mette a disposizione macro, mappatura della tastiera e dei colori, tastiera su schermo, funzionalità di copia e incolla, aggiornamenti di schermate avviati dall'host e capacità di trasferimento file.

Ruoli di amministratore e di utente finale

I ruoli di amministratore e di utente finale sono entrambi descritti nella documentazione e nel workflow. L'amministratore crea le sessioni, assegna gli utenti alle sessioni create e imposta le preferenze dell'utente. L'utente finale accede alle sessioni che gli sono state assegnate, interagisce con il client Web per eseguire la connessione all'host e completa le attività.

Browser e sistemi operativi supportati

Host Access for the Cloud è un prodotto a 64 bit che supporta i browser Google Chrome, Mozilla Firefox, Microsoft Internet Explorer e Microsoft Edge. L'utilizzo dei container di Docker consente il ridimensionamento orizzontale e verticale, permettendo il supporto di tecnologie basate su cloud. Un elenco completo delle piattaforme supportate e di altri requisiti di installazione è disponibile in Requisiti di sistema per la valutazione.

Considerazioni sulla sicurezza

Quando si consente l'accesso ai propri host legacy a utenti che si trovano al di fuori del firewall, ad esempio partner aziendali, utenti remoti e personale commerciale mobile, è necessario schermare le informazioni dalle minacce alla sicurezza note. Con Host Access for the Cloud è possibile fornire accesso sicuro dal Web all'host a tutti gli utenti, vicini o lontani. Insieme a MSS, Host Access for the Cloud fornisce connessioni HTTPS e una vasta gamma di opzioni di autorizzazione e autenticazione.

Host Access for the Cloud supporta i protocolli TLS ed SSH per proteggere i dati di importanza critica. Per proteggere le password e altri dati sensibili, è possibile utilizzare il protocollo HTTPS, il quale include la cifratura TLS.

Host Access for the Cloud può essere connesso in modo sicuro al browser, all'host e al server di gestione. Vedere Protezione delle connessioni per informazioni sulla protezione di tali connessioni.

Valutazione di Host Access for the Cloud

Requisiti di sistema per la valutazione

Per installare e valutare correttamente Host Access for the Cloud, il sistema deve avere:

- 8 GB di memoria
- Un browser e un sistema operativo supportati.

Per un elenco completo degli ambienti supportati, vedere Requisiti di sistema.

Download del software di valutazione

Se ancora non si possiede il software, accedere al relativo sito e compilare il modulo per la richiesta di una copia di valutazione. Si riceverà un messaggio e-mail con istruzioni per il download e l'installazione di una copia di valutazione di Host Access for the Cloud valida per 120 giorni. Utilizzando questa copia di valutazione, è possibile aprire e chiudere sessioni host e mantenere 5 connessioni host attive contemporaneamente. Il sito della versione di prova contiene tutte le informazioni necessarie per intraprendere il passaggio successivo.

Il sito di download di Micro Focus contiene i file compressi necessari a installare tutte le piattaforme, incluso il connettore Windows. File di attivazioni differenti consentiranno di abilitare edizioni/piattaforme di Host Access for the Cloud diverse.

Installazione di base

Le istruzioni seguenti forniscono l'installazione di base predefinita. Questo significa che tutti i componenti vengono installati localmente e utilizzano le porte predefinite. Dopo aver completato questa installazione è possibile seguire la procedura dettagliata e acquisire familiarità con Host Access for the Cloud e MSS.

1. Scaricare dal sito di download di Micro Focus il pacchetto di installazione del prodotto. Il pacchetto include il supporto per tutte le piattaforme supportate.
2. Seguendo le istruzioni del programma di installazione, installare Host Access for the Cloud e Management and Security Server (MSS).

Per abilitare le funzionalità del prodotto, MSS utilizza i file di attivazione (activation.jaw). Il programma di installazione contiene il file di attivazione necessario che viene attivato durante il processo di installazione.

Nota: Durante un'installazione di base, viene utilizzato un certificato firmato da se stessi per assicurare che le connessioni siano sicure. Quando si passa a un ambiente di produzione è possibile utilizzare i propri certificati.

È ora possibile passare alla fase successiva ossia alla procedura dettagliata di Host Access for the Cloud.

Procedura dettagliata

Le seguenti istruzioni si riferiscono a un'installazione predefinita di base. Questo significa che tutti i componenti vengono installati in locale e utilizzano le porte predefinite. Una volta completata l'installazione, sarà possibile completare i passaggi e acquisire familiarità con Host Access for the Cloud e MSS.

Per informazioni sull'installazione negli ambienti di produzione e in scenari di produzione differenti, vedere la sezione Distribuzione.

I passaggi

- ✓ Aprire MSS Administrative Console.
- ✓ Creare e avviare una nuova sessione. Viene aperta una nuova finestra del browser e visualizzato il pannello **Connection** del client Web.
- ✓ Configurare le impostazioni, incluse la mappatura di tasti e colori, l'attivazione di aree sensibili e macro, e altre opzioni di connessione e preferenze dell'utente.
- ✓ Assegnare gli utenti alle sessioni.
- ✓ Fornire accesso alle sessioni.

Aprire Administrative Console

1. In un ambiente Windows, nel menu Start posizionare il cursore del mouse su Micro Focus Host Access for the Cloud e fare clic su Administrative Console oppure fare clic sull'URL della pagina di login dell'amministratore nel browser Web. L'URL utilizza il formato seguente: `https://server.azienda.com:443/adminconsole`.
2. Se ci si connette utilizzando HTTPS e il server dispone di un certificato autofirmato, il browser avviserà l'utente che il certificato è stato creato. Tale comportamento è previsto. È possibile accettare il certificato autofirmato o scegliere di continuare per aprire la pagina di accesso

dell'amministratore. Dopo l'acquisto di un certificato firmato dall'autorità di certificazione (CA) o l'importazione di un certificato autofirmato nell'archivio certificati, gli avvisi non verranno più visualizzati.

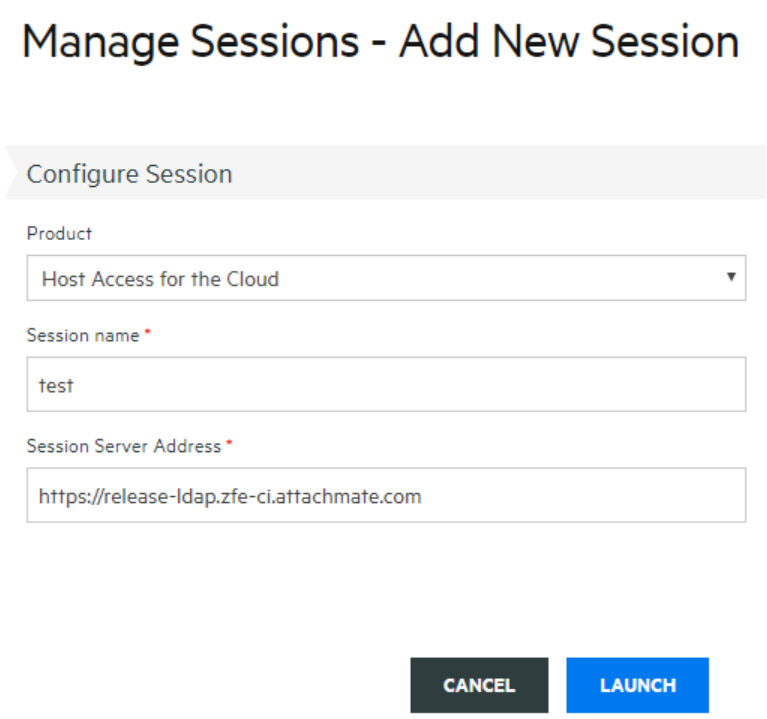
3. L'account dell'amministratore dispone di una password integrata, ***admin.*** Accedere come amministratore utilizzando questa password o immettendo la password specificata durante l'installazione di MSS.

Creare una nuova sessione

Per le istruzioni complete, vedere Add a Session (Aggiunta di una sessione) nella MSS Administrator Guide (Guida dell'amministratore di MSS).

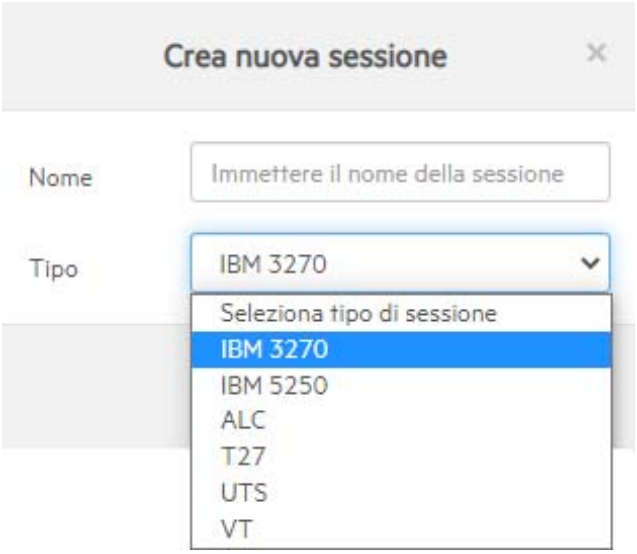
È possibile aggiungere e aggiornare le impostazioni della sessione dal pannello Manage Sessions (Gestisci sessioni) di Administrative Console. Quando si aggiunge una sessione, la nuova sessione diventa disponibile nell'elenco delle sessioni di questo pannello.

1. Nel pannello Manage Sessions (Gestisci sessioni) fare clic su **AGGIUNGI** per creare una nuova sessione.



2. Selezionare Host Access for the Cloud, se non è già selezionato, immettere un nome per la sessione, quindi fare clic su **Launch** (Avvia) per visualizzare una nuova finestra del browser e iniziare la configurazione della sessione per il server specificato all'indirizzo del server di sessione.

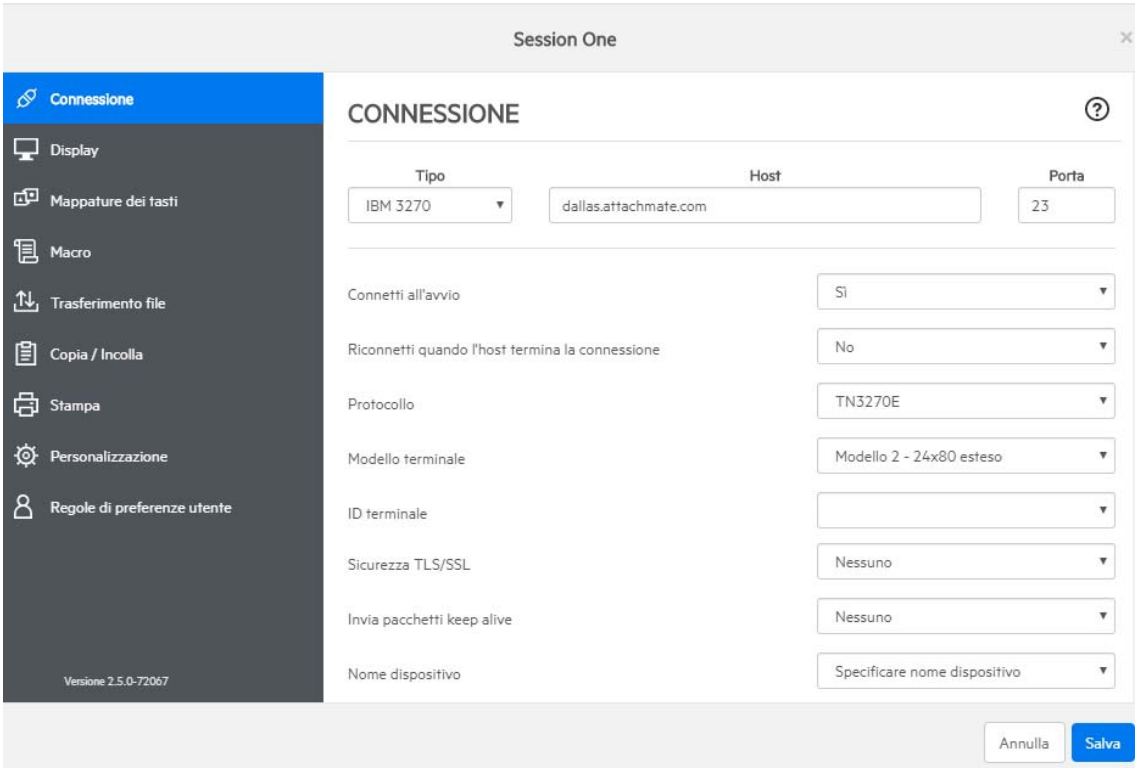
3. Nella finestra di dialogo Crea nuova sessione, selezionare il tipo di host dall'elenco a discesa, quindi fare clic su Successivo.



Configurare le impostazioni e connettersi

Nella finestra del browser del client Web è possibile, oltre che connettersi all'host, configurare diverse impostazioni e opzioni per la sessione.

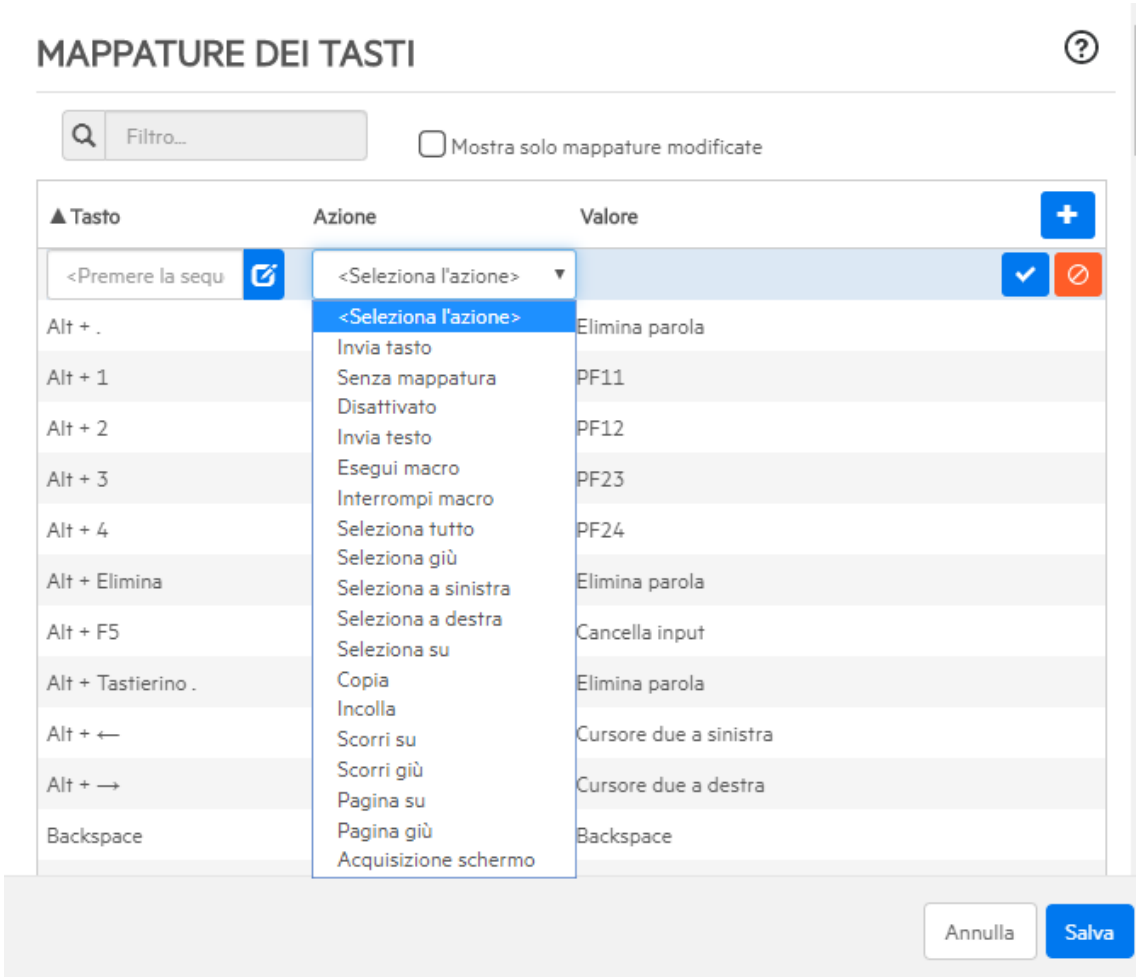
1. Nel pannello **Connessione**, immettere le informazioni di connessione necessarie per la sessione che si desidera creare.



2. Le impostazioni di connessione variano a seconda del tipo di connessione all'host. Per descrizioni dettagliate delle opzioni di impostazione per ogni tipo di host, vedere la guida del client Web. Le opzioni per l'impostazione includono la mappatura delle sequenze di tasti ai tasti selezionati, la mappatura di colori dell'host in base alle preferenze dell'utente e la registrazione delle macro della sessione.

Mappatura dei tasti

3. Per mappare tasti a tasti selezionati, aprire **Mappature dei tasti**.
4. Premere il tasto o la combinazione di tasti da usare per avviare l'azione selezionata.



5. Nell'elenco a discesa **Azione**, selezionare l'azione che si vuole mappare alla sequenza di tasti selezionata. Fare clic su per completare la mappatura dei tasti. È possibile continuare ad aggiungere e mappare altri tasti.
6. Fare clic su **Salva** per completare la mappatura dei tasti.

Modifica dei colori dell'host e altre opzioni

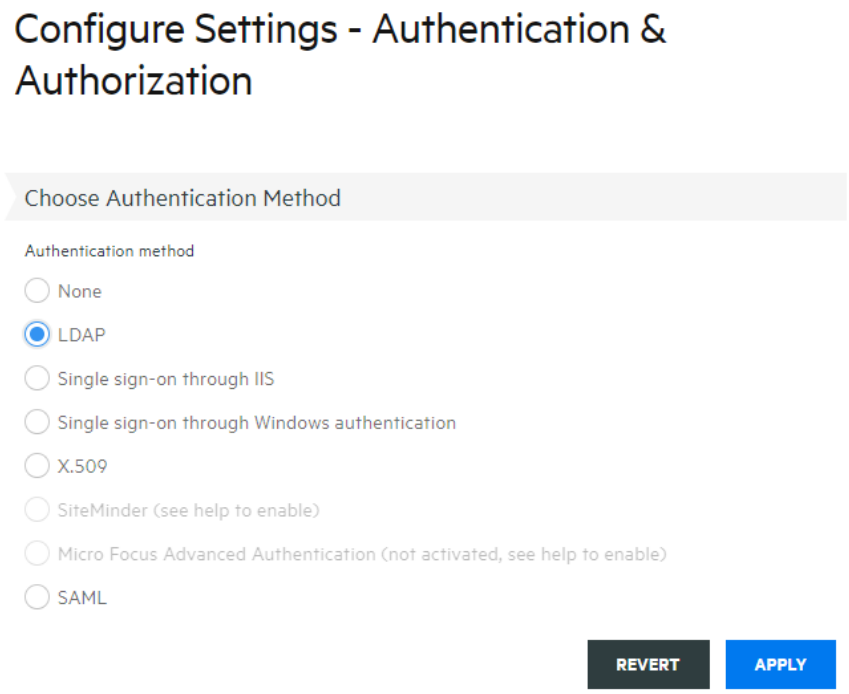
7. Nel riquadro di spostamento a sinistra, è possibile mappare i colori dell'host, impostare le opzioni relative ai caratteri e alla tastiera e attivare le aree sensibili aprendo il pannello **Display**. Le opzioni da scegliere per i colori sono specifiche di ogni sessione.

8. Aprire **Regole di preferenze utente** per estendere le opzioni di configurazione agli utenti finali.
9. Fare clic su **Esci** per tornare alla finestra del browser di Administrative Console per autenticare gli utenti e assegnarli alle sessioni.

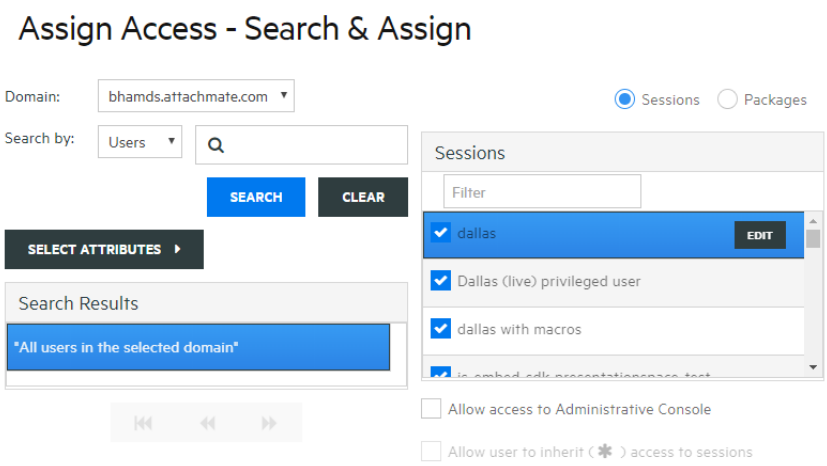
Configurazione dell'autenticazione e assegnazione degli utenti alle sessioni

Ora che le sessioni sono state create, è necessario concedere agli utenti l'accesso a tali sessioni. Gli utenti vengono autenticati e assegnati alle sessioni in MSS Administrative Console. Un utente può essere assegnato a più sessioni.

1. L'autenticazione e l'autorizzazione convalidano l'identità di un utente e il metodo da utilizzare per mappare le sessioni a utenti singoli o gruppi di utenti. Nel riquadro di spostamento a sinistra, selezionare **Configure Authentication**.
2. Scegliere un metodo di autenticazione. Le opzioni variano a seconda della selezione.



3. Nella documentazione di MSS sono disponibili descrizioni per le varie opzioni. Fare clic su ?.
4. Fare clic su **Apply** per completare la procedura.
5. Aprire **Assign Access** per mappare le sessioni a utenti singoli o a gruppi di utenti.



6. Mappare le sessioni agli utenti che devono accedere alle sessioni e fare clic su **Apply.** È anche possibile scegliere di consentire agli utenti di ereditare l'accesso alle sessioni e ad Administrative Console.

MSS Vedere Select a method to authenticate users (Selezione di un metodo per l'autenticazione degli utenti) nella MSS Administrator Guide (Guida dell'amministratore di MSS).

Concessione dell'accesso alle sessioni agli utenti finali

Il passaggio finale consiste nel condividere con gli utenti un URL che consente di accedere al server di sessione. In genere, l'URL ha un aspetto analogo al seguente:

```
https://server.azienda.com:porta
```

Quando accederanno al server di sessione, agli utenti verrà chiesto di eseguire il login, quindi verrà loro concesso l'accesso alle sessioni che sono state loro assegnate.

Nelle distribuzioni più complesse l'URL specificato rimanderà a un sistema di bilanciamento del carico e non al server di sessione. Questo tipo di collegamenti viene spesso incorporato nei portali aziendali o in altri siti Web proprietari.

Argomenti correlati

Fornire accesso alle sessioni
Distribuzione
Gestione

3 Distribuzione

In questa sezione vengono fornite informazioni che vanno oltre la configurazione di base della versione di valutazione. Si presuppone inoltre che l'utente stia passando all'ambiente di produzione. Per informazioni su un'installazione semplice, vedere Valutazione di Host Access for the Cloud.

In questa sezione

Informazioni su MSS

Host Access Management and Security Server (MSS) protegge, gestisce e controlla in modo centralizzato l'accesso dell'utente alle connessioni host. Le operazioni di creazione delle sessioni, impostazione del conteggio e configurazione degli ID dei terminali vengono tutte eseguite con MSS.

Documentazione di MSS:

- Note di rilascio di 12.6 SP1 Update 1
- Evaluation Guide (Guida alla valutazione)
- Installation Guide (Guida all'installazione)
- Guida all'amministrazione
- Automated Sign-On for Mainframe - Administrator Guide (Sign-On automatico per i mainframe - Guida all'amministrazione)

Requisiti di sistema

Queste piattaforme e le rispettive versioni successive sono supportate da Host Access for the Cloud versione 2.5 e successive. I requisiti non tengono conto di altre applicazioni e risorse che possono essere installate nel sistema.

Componente	Versioni del software e hardware supportati
Browser Web	◆ Google Chrome v62 (consigliato) ◆ Mozilla Firefox v57(consigliato) ◆ Microsoft Edge 41 ◆ Microsoft Internet Explorer 11 (non consigliato) Per informazioni sui problemi di prestazioni in caso di utilizzo di Internet Explorer, vedere Problemi relativi al browser. ◆ Apple iOS Safari 11
Server di sessione	**Hardware** ◆ CPU - 2 core (consigliati 4 core) ◆ Memoria libera - 4 GB (consigliati 6 GB) **Sistema operativo (64 bit)** ◆ Windows Server 2012 ◆ SUSE Linux Enterprise Server (SLES) v11 SP4 ◆ Red Hat Enterprise Linux 6 ◆ Linux on z Systems ◆ SUSE Linux Enterprise Server (SLES) v11 ◆ Red Hat Enterprise Linux 6

Ulteriori requisiti

- Per informazioni sui requisiti di sistema per MSS vedere la MSS Installation Guide (Guida all'installazione di MSS).
- I **sistemi di bilanciamento del carico** per MSS e Host Access for the Cloud devono supportare le sessioni permanenti e i Web Socket.

Pianificazione per la distribuzione

Quanti server di sessione è necessario distribuire? Quanti server MSS? Quale metodo di autenticazione si sta utilizzando? Esistono altre considerazioni di cui tenere conto? In questa sezione viene illustrato come ottimizzare la distribuzione del server di sessione e del server MSS.

In questa sezione:

Informazioni sull'autenticazione

Prima di iniziare la distribuzione, è necessario definire la modalità di autenticazione che si desidera utilizzare. L'autenticazione convalida l'identità dell'utente in base ad alcune credenziali, ad esempio una combinazione nome utente/password o un certificato client.

HACloud supporta le seguenti modalità di autenticazione: LDAP, Single Sign-On tramite IIS, Single Sign-On tramite Windows, X.509, SiteMinder e SAML.

È possibile non richiedere agli utenti di eseguire l'autenticazione. Selezionare **Nessuno** per consentire a qualsiasi utente di accedere alle sessioni assegnate senza la richiesta delle credenziali.

Ulteriori informazioni sull'autenticazione sono disponibili in Select a method to authenticate users (Selezione di un metodo per l'autenticazione degli utenti).

Ridimensionamento e alta disponibilità

Determinare il numero server di sessione e di server MSS necessari per soddisfare le proprie esigenze è la prima attività da eseguire per pianificare la distribuzione. Indipendentemente dalle esigenze, Host Access for the Cloud può essere distribuito per fornire capacità e alta disponibilità.

Sebbene ogni soluzione dipenda da esigenze specifiche, è possibile consultare Progetto per una distribuzione ad alta disponibilità per avere indicazioni per una distribuzione scalabile e ad elevata disponibilità.

Le domande principali a cui è necessario rispondere sono:

- Qual è il numero massimo di sessioni host che verranno utilizzate simultaneamente?
- Quanti utenti utilizzeranno il sistema?
- Quale livello di disponibilità del sistema è necessario per far fronte a un eventuale errore nelle diverse aree che lo compongono?

Ridimensionamento

Il ridimensionamento consente a un sistema di gestire carichi di lavoro di varie dimensioni. Per aumentare la capacità, su un sistema può essere utilizzato lo scaling up (ridimensionamento verticale), mediante l'utilizzo di un server più potente, o lo scaling out (ridimensionamento orizzontale) mediante l'aggiunta di più server o nodi.

Ognuna di queste tecniche comporta dei compromessi di cui tener conto:

- Lo **scaling up** è più semplice perché sono presenti meno server, ma aumenta il rischio di un errore di notevole entità nel caso in cui un server non risponda.
- Lo **scaling out** implica l'utilizzo di più server ma, poiché i rischi vengono ripartiti su molti server, la mancata disponibilità di uno di essi avrà effetto su un numero inferiore di utenti.

Per aumentare la capacità, **si consiglia pertanto lo scaling out** mediante l'aggiunta di più server o nodi, in ragione della maggiore resilienza.

Alta disponibilità

L'alta disponibilità (High availability, HA) è la capacità del sistema di continuare a fornire i servizi quando si verifica un errore in un punto qualsiasi dello stesso. L'alta disponibilità viene ottenuta mediante l'aggiunta della ridondanza ai principali componenti del sistema.

Nota: In questa guida viene illustrato come garantire l'alta disponibilità dei principali servizi di Host Access for the Cloud. Tuttavia, poiché l'alta disponibilità si basa sulla ridondanza implementata a molti livelli in tutte le aree dei sistemi, la sua descrizione esula dallo scopo di questo documento.

L'alta disponibilità in Host Access for the Cloud viene ottenuta mediante:

- La distribuzione di un numero di server di sessione e di server MSS sufficiente per fornire la capacità necessaria, implementando inoltre capacità aggiuntiva (libera) per gli errori
- L'implementazione della corretta quantità di capacità aggiuntiva affinché, nel caso di restituzione di errore da parte di un server e di failover del carico di lavoro sui server rimanenti, il funzionamento di questi ultimi non venga compromesso dall'ulteriore carico
- L'utilizzo di sistemi di bilanciamento del carico per distribuire il carico di lavoro e indirizzare gli utenti ad altri server in caso di errore
- Replica dei dati tra i server MSS che viene condotta dalla gestione in cluster MSS

Per una descrizione di come soddisfare questi requisiti, vedere Progetto per una distribuzione ad alta disponibilità.

Dimensionamento dei server di sessione

Il numero di server di sessione necessari è determinato dal **numero di sessioni host simultanee** che si intende eseguire. Le sessioni host generano un maggior carico sul server di sessione rispetto agli utenti, pertanto in questa sezione si farà riferimento a scenari relativi al numero di sessioni host richieste, anziché al numero di utenti.

Numero di sessioni simultanee dell'host	Numero di server di sessione richiesti
Fino a 3.000	2 server di sessione
Oltre 3.000	(Numero di sessioni host richieste)/2.000 + 1 (un minimo di tre)

- Un server a sessione singola supporta 2000 sessioni host simultanee.
- Un server di sessione include capacità aggiuntiva integrata per gestire 1.000 sessioni host aggiuntive in caso di failover.
- Per l'alta disponibilità è necessario un minimo di due server di sessione.

Dimensionamento dei server MSS

Il numero di server MSS richiesto dipende dal numero di **utenti simultanei.**

Numero di utenti simultanei	Numero di server MSS richiesti
Fino a 30.000	3 server MSS
Oltre 30.000	(Numero di utenti necessari)/10.000 +1 (deve essere un numero dispari)

- Un solo server MSS supporta 10.000 utenti simultanei.
- Un server MSS dispone di una capacità aggiuntiva integrata per ospitare ulteriori 5.000 utenti, in caso di failover.
- Per l'alta disponibilità sono necessari almeno 3 server MSS.
- Per l'alta disponibilità è richiesto un numero dispari di server MSS a causa della necessità di un quorum del database.

Opzioni di distribuzione

È possibile distribuire i server di sessione in uno dei modi seguenti:

1. Utilizzando il metodo tradizionale, basato sull'installazione di ciascun server di sessione su un server dedicato
2. Utilizzando Docker per eseguire ciascun server di sessione in un container. Docker offre una serie di vantaggi, inclusa maggiore flessibilità per il numero di server di sessione che è possibile eseguire su un singolo server. Per ulteriori informazioni, vedere Utilizzo di Docker.

Utilizzo dei sistemi di bilanciamento del carico

Sarà necessario implementare sistemi di bilanciamento del carico sia per i server di sessione che per i server MSS. Sono disponibili delle impostazioni comuni che sarà utile conoscere:

- **Algoritmo di bilanciamento del carico** - Questo algoritmo determina a quale server inviare il nuovo traffico. Si consiglia di utilizzare l'impostazione "Least Connections" (Connessioni minime) o un'impostazione analoga. Verificare che questa impostazione consenta di distribuire correttamente il carico è essenziale per la stabilità complessiva del sistema. Se il sistema di bilanciamento del carico non è configurato correttamente o il suo funzionamento non è efficace, si corre il rischio di sovraccaricare i singoli server disponibili.
- **Persistenza della sessione (affinità/sessioni permanenti)** - È la possibilità di inviare lo stesso utente allo stesso server in seguito a più richieste. Il server di sessione e MSS sono applicazioni stateful, che richiedono l'abilitazione delle sessioni permanenti nei propri sistemi di bilanciamento del carico. Questo argomento verrà affrontato di seguito.
- **Endpoint per la verifica dello stato** - Si tratta dell'URL nel servizio di destinazione che viene utilizzato per determinare se l'istanza è integra e deve rimanere in servizio. Ciascun tipo di server fornisce il proprio URL di verifica dello stato.

Nella sezione Progetto per una distribuzione ad alta disponibilità sono riportati i valori delle impostazioni consigliate per ciascun sistema di bilanciamento del carico.

Opzioni TLS/SSL

Per gestire i protocolli TSL/SSL in un sistema di bilanciamento del carico, sono disponibili tre opzioni tipiche. L'opzione prescelta varia in base alle esigenze.

Con le prime due opzioni è necessario installare il proprio certificato nel sistema di bilanciamento del carico. Con la terza opzione, ossia il metodo pass-through TLS, per il sistema di bilanciamento del carico non è richiesto alcun certificato. Il progetto per l'implementazione della disponibilità elevata utilizza il bridging TLS per garantire protezione TLS in tutte le fasi, assicurando al contempo la persistenza basata sui cookie. Le opzioni disponibili includono:

- **Interruzione/offloading TLS** - Questa opzione termina la connessione HTTPS sul sistema di bilanciamento del carico e ristabilisce una nuova connessione HTTP tra il sistema di bilanciamento del carico e il servizio.
- **Bridging TLS (nuova cifratura)** - Questa opzione termina la connessione HTTPS sul sistema di bilanciamento del carico e ristabilisce una nuova connessione HTTPS tra il sistema di bilanciamento del carico e il servizio. In questo modo viene assicurata protezione TLS dall'inizio alla fine, consentendo contemporaneamente al sistema di bilanciamento del carico di utilizzare un cookie per assicurare la persistenza della sessione.
- **Pass-through TLS (obbligatorio per X.509)** - Il sistema di bilanciamento del carico agisce da proxy per la connessione TLS senza decifrarla. Lo svantaggio di questa opzione consiste nel fatto che, poiché non è possibile utilizzare cookie, la persistenza deve essere garantita basandosi sull'indirizzo IP di origine o in modo analogo.

TLS/SSL con Single Sign-On X.509

Quando si utilizza l'autenticazione X.509, i sistemi di bilanciamento del carico di Host Access for the Cloud e di MSS richiedono il pass-through TLS, in quanto i certificati client devono essere inviati ai server nel sistema backend. Poiché il pass-through TLS è obbligatorio, per la persistenza della sessione sarà necessario utilizzare un metodo non basato su cookie, come l'indirizzo IP di origine, sia per il sistema di bilanciamento del carico del server MSS che per quello del server di sessione. Questo è necessario perché con il metodo pass-through di TLS, il sistema di bilanciamento del carico non può decifrare la connessione per impostare o persino visualizzare un cookie.

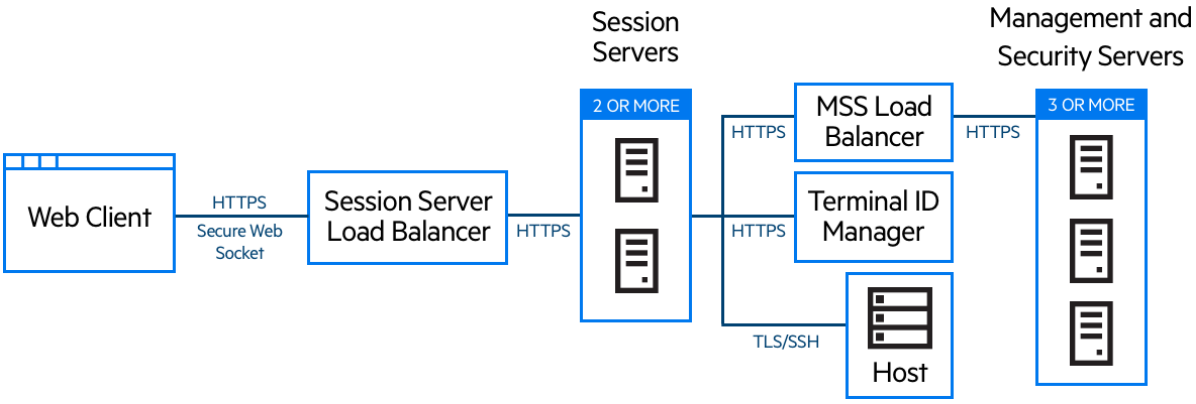
Terminal ID Manager

Attualmente, Terminal ID Manager non supporta l'alta disponibilità. È possibile configurare un server passivo, tuttavia lo stato degli ID non verrà replicato dal server attivo. Se il server attivo non è disponibile, sarà comunque possibile accedere al server passivo, ma gli ID non manterranno il loro stato attuale.

Progetto per una distribuzione ad alta disponibilità

Di seguito è riportato un esempio di come distribuire Host Access for the Cloud in modo scalabile, sicuro e ad alta disponibilità. Anche se i dettagli di ogni implementazione saranno diversi, ad esempio potreste implementare tre o più server di sessione. L'obiettivo è quello di fornire un buon punto di partenza conosciuto e di rispondere alle domande di implementazione più comuni.

Architettura



Questa distribuzione è composta da:

- Un sistema di bilanciamento del carico per il server di sessione
- Due o più server di sessione
- Bilanciamento del carico per MSS
- Tre o più server MSS
- Terminal ID Manager
- Un server LDAP o un server di gestione delle identità
- Un sistema host/mainframe

Vantaggi della distribuzione

In questo esempio viene mostrata una configurazione con le seguenti caratteristiche:

- Capacità per un massimo di 3.000 sessioni host con la possibilità di ridimensionamento in base alle esigenze
- Alta disponibilità dei principali servizi, riduzione del numero dei singoli punti di errore e distribuzione del carico mediante sistemi di bilanciamento del carico
- Possibilità di gestire contemporaneamente errori di un server di sessione e di un server MSS senza una significativa riduzione delle prestazioni del client Web, grazie alla capacità aggiuntiva integrata
- Opzioni di autenticazione e autorizzazione per MSS
- Protezione delle comunicazioni tramite HTTPS

Passaggi per completare la distribuzione

Per effettuare la distribuzione, è necessario completare i passaggi seguenti:

1. Acquisire familiarità con i concetti di base della distribuzione
2. Effettuare il provisioning delle risorse in base ai requisiti di sistema e alle linee guida per il dimensionamento
3. Installare MSS e creare un cluster

4. Configurare il sistema di bilanciamento del carico per MSS
5. Installare i server di sessione
6. Configurare il sistema di bilanciamento del carico per il server di sessione
7. Verificare la distribuzione
8. Configurare il Single Sign-On (facoltativo)
9. Configurare Terminal ID Manager (facoltativo)

I concetti di base della distribuzione, i requisiti di sistema e le linee guida per il dimensionamento sono stati indicati nelle sezioni precedenti.

Installazione di MSS

Installare tre server MSS e configurare ciascuno di essi per la gestione in cluster. È disponibile della documentazione con i dettagli sui passaggi del processo:

1. Aprire le porte sul firewall. Le porte utilizzate da MSS e Host Access for the Cloud sono elencate qui.
2. Installare MSS, quindi i componenti di Host Access for the Cloud per MSS eseguendo il programma di installazione di Host Access for the Cloud su ciascun server MSS.
3. Aggiungere ogni server a un cluster.
4. Su ciascun server MSS configurare le impostazioni generali, le impostazioni di sicurezza e altre impostazioni, in base alle esigenze.

Altre risorse:

- Porte
- Installation Guide (Guida all'installazione)
- MSS Clustering (Gestione in cluster MSS)

Configurazione di un sistema di bilanciamento del carico per MSS

Come descritto nella sezione Utilizzo dei sistemi di bilanciamento del carico di questo manuale, per la configurazione del sistema di bilanciamento del carico per MSS ad elevata disponibilità, è possibile utilizzare questi valori:

- **Algoritmo di bilanciamento del carico:** Least Connections (Connessioni minime) (o un'impostazione analoga)
- **Persistenza della sessione:** Enabled (Abilitata) - Utilizzare il cookie JSESSIONID esistente

  Poiché i cookie non vengono memorizzati nel server di sessione quando funziona come client per MSS, per la persistenza il sistema di bilanciamento del carico di MSS deve utilizzare il cookie JSESSIONID esistente o l'indirizzo IP di origine (o un elemento analogo).
- **Endpoint del controllo integrità:** `https://<server-mss>/mss/`
- **TLS:** configurare TLS e installare i certificati in base alle esigenze.

Installazione dei server di sessione

Installare due o più server di sessione.

Per ciascun server di sessione, effettuare le seguenti operazioni:

1. Aprire le porte sul firewall. Le porte utilizzate da MSS e Host Access for the Cloud sono elencate qui
2. Installare il server di sessione. Durante l'installazione, scegliere di utilizzare un server MSS remoto e immettere l'indirizzo e la porta del sistema di bilanciamento del carico di MSS.
3. Importare il certificato del server di sessione nell'archivio attendibilità di ogni sottosistema attendibile di MSS: `system-trustcerts.bcfks`.

Suggerimento: Questa operazione viene effettuata automaticamente sul server MSS scelto dal sistema di bilanciamento del carico durante l'installazione, ma deve essere eseguita manualmente sugli altri server. È consigliabile importare o verificare la presenza del certificato su ciascun server MSS.

Altre risorse:

- Porte
- Installazione e aggiornamento
- Protezione delle connessioni

Configurazione del sistema di bilanciamento del carico del server di sessione

Per configurare il sistema di bilanciamento del carico, utilizzare questi valori:

- **Algoritmo di bilanciamento del carico:** Least Connections (Connessioni minime) (o un'impostazione analoga)
- **Persistenza della sessione:** Enabled (Abilitata) - Utilizzare JSESSIONID o un nuovo cookie. A differenza del sistema di bilanciamento del carico di MSS, non è necessario utilizzare il cookie JSESSIONID esistente.
- **Endpoint per la verifica dello stato:** https://<server di sessione>/actuator/health

  Per il server di sessione, in particolare, prestare attenzione quando si configura la modalità con cui individuare un nodo che ha restituito un errore e le operazioni da eseguire dopo tale evento. Se all'istanza sono ancora connessi degli utenti, è possibile che le loro connessioni all'host vengano interrotte. Per evitare di contrassegnare troppo in anticipo un'istanza come istanza con errore, si consiglia di aumentare il numero di timeout o di tentativi. Alcuni sistemi di bilanciamento del carico forniscono una "modalità di svuotamento", che consente agli utenti esistenti di rimanere connessi, mentre i nuovi utenti vengono indirizzati ad altre istanze.
- **TLS:** configurare TLS e installare i certificati in base alle esigenze.

Configurazione dell'indirizzo di richiamata MSS

In MSS viene fornito un indirizzo di richiamata al server di sessione ogni volta che si crea o si modifica una sessione. Per default, viene utilizzato l'indirizzo specificato in `management.server.url`.

Se il server MSS si trova dietro un proxy e il server di sessione non è in grado di raggiungere l'indirizzo:

- Impostare la proprietà `management.server.callback.address` in ciascun file `container.properties` di MSS su un indirizzo che il server di sessione, di uno specifico MSS, possa raggiungere.

  Nota: Se il server di sessione utilizza HTTP per eseguire la connessione all'indirizzo di richiamata MSS, impostare la proprietà `management.server.callback.address.http` su *True* nel file `container.properties` di ciascun server di sessione.

- Riavviare il server per rendere effettivi i nuovi valori delle proprietà.

Verifica dell'installazione

Dopo l'installazione e la configurazione di tutti i componenti, sarà necessario:

- Eseguire il login a MSS Administrative Console (mediante il sistema di bilanciamento del carico di MSS).
- Accedere a Gestisci sessioni > Aggiungi una nuova sessione e creare una sessione di prova.
- Assegnare la sessione di prova a un utente di prova.
- Eseguire il login al server di sessione come utente di prova, tramite il sistema di bilanciamento del carico del server di sessione.
- Verificare che la sessione assegnata sia disponibile, sia aperta e in grado di connettersi.

Configurazione del Single Sign-On (facoltativa)

Di seguito sono riportate alcune considerazioni da fare quando si configura il Single Sign-On in una distribuzione ad alta disponibilità.

SAML (Security Assertion Markup Language)

1. Importare il certificato del sistema di bilanciamento del carico in ogni `servletcontainer.bcfks` di MSS come certificato attendibile.
2. Aggiornare `management.server.url` in ciascun file `container.properties` di MSS affinché utilizzi l'indirizzo del sistema di bilanciamento del carico di MSS.
3. Impostare la proprietà `management.server.callback.address` in ciascun file `container.properties` di MSS su un indirizzo che il server di sessione, di uno specifico MSS, possa raggiungere.
4. Riavviare i server MSS.

5. Accedere ad Administrative Console del server MSS attivo per configurare l'autenticazione SAML.

   Verificare che nel campo **Assertion consumer service prefix URL** (URL prefisso del servizio consumer di asserzione), sia utilizzato il DNS del sistema di bilanciamento del carico di MSS, quindi aggiungere il DNS del sistema di bilanciamento del carico di MSS e di Host Access for the Cloud alla white list SAML.

La MSS Administrator Guide (Guida dell'amministratore di MSS) fornisce istruzioni per l'autenticazione SAML.

X.509

In ogni caso, il certificato utilizzato deve avere un nome alternativo del soggetto (Subject Alternative Name, SAN) contenente tutti i nomi DNS del server MSS, oltre al nome DNS del sistema di bilanciamento del carico.

1. Verificare che il firewall sul server MSS consenta il traffico HTTP sulla porta di autenticazione reciproca: il valore predefinito è 8003.
2. In ciascun server MSS:
   - Sostituire il certificato della voce servlet-engine nei file `servletcontainer.bcfks`.
   - Sostituire il certificato della voce di sistema nei file `system-keystore.bcfks`.
3. Importare il certificato in ciascun server di sessione:
   - Il file `trustcerts.bcfks` come certificato attendibile.
4. Riavviare i server MSS e di sessione.
5. Configurare i sistemi di bilanciamento del carico di MSS e HACloud per il metodo pass-through di TSL.
6. Configurare l'autenticazione X.509 come mostrato qui: Configurazione dell'autenticazione X.509.

La X.509 Configuration (Configurazione di X.509) nella MSS Administrator Guide (Guida dell'amministratore di MSS) fornisce le istruzioni.

Installazione e aggiornamento

Nella guida di MSS Administrative Console sono riportate informazioni sulla Product Activation (Attivazione del prodotto).

- Installazione su piattaforme differenti
- Utilizzo di un'installazione automatica
- Configurazione di un'installazione incompleta
- Upgrade da versioni precedenti
- Risoluzione dei problemi relativi all'installazione

Quando si esegue l'installazione, tenere in considerazione i seguenti aspetti:

- **File di attivazione**

  I file di attivazione (activation.jaw) vengono utilizzati per abilitare le funzionalità del prodotto. Ad esempio, il pacchetto di installazione contiene il file di attivazione necessario a consentire la comunicazione tra Host Access for the Cloud e MSS. In genere, l'attivazione viene effettuata durante il processo di installazione. I file di attivazione vengono scaricati dal sito di download di Micro Focus e sono specifici per le diverse edizioni e piattaforme supportate da Host Access for the Cloud. Per lavorare in un ambiente di produzione è necessaria l'attivazione.

  In caso contrario, è necessario aprire Administrative Console e completare la procedura di attivazione (Configure Settings (Configura impostazioni > Product Activation (Attivazione del prodotto). Per informazioni su come gestire i file di attivazione quando si esegue l'upgrade, vedere la sezione Upgrading from previous versions (Upgrade dalle versioni precedenti).

- **Utilizzo del proxy inverso IIS con Host Access for the Cloud**

  Se si intende utilizzare il proxy inverso IIS, leggere Accesso a Host Access for the Cloud mediante il proxy inverso IIS per i prerequisiti e le istruzioni di configurazione.

- **Sicurezza**

  Per proteggere i dati di importanza critica, Host Access for the Cloud supporta i protocolli TLS ed SSH. Per proteggere le password e altri dati sensibili, è consigliabile impostare i browser affinché utilizzino il protocollo HTTPS.

Installazione su piattaforme differenti

Host Access for the Cloud e Java

Il server di sessione richiede Java JDK versione 8 o successiva; MSS richiede Java JRE 8 o versione successiva. Questi requisiti per Java vengono soddisfatti nel corso dell'installazione, ad eccezione dei sistemi Linux su System Z che richiedono JDK IBM. Le informazioni sull'utilizzo dell'opzione *nojdk* sono disponibili in Installazione su z/Linux.

Sia Host Access for the Cloud che MSS richiedono che l'installazione Java supporti la cifratura avanzata senza restrizioni. Ulteriori informazioni sono disponibili sul sito Web di Java.

Se necessario, è possibile utilizzare le variabili di ambiente specificate nell'opzione *nojdk* e `INSTALL4J_JAVA_HOME_OVERRIDE` per specificare l'installazione Java specifica.

Windows

Un'installazione di base in Windows è descritta in Valutazione di Host Access for the Cloud.

UNIX

- È necessario eseguire l'installazione come "root" oppure utilizzare un account utente con privilegi root. Dopo che l'installazione è stata completata, l'applicazione installata può essere avviata e gestita da "root" o da un utente con privilegi "root".
- Sulle piattaforme Linux, seguire questi passaggi per impostare l'avvio automatico del server di sessione quando viene avviato il sistema.

- Per aprire qualsiasi porta di applicazione inferiore a 1024 sono necessari privilegi elevati. Host Access for the Cloud può iniziare a utilizzare una porta con numero inferiore solo se l'utente dispone di privilegi di sistema specifici per aprire porte con numeri inferiori.
- È possibile utilizzare il comando `chmod` per assegnare privilegi sulle applicazioni a utenti diversi da root.
- Se si sta eseguendo l'installazione in un sistema Linux headless e non vi sono caratteri installati, è possibile che venga visualizzato il seguente errore: `java.lang.Error: Probable fatal error: No fonts found`. Per proseguire con l'installazione, accertarsi che nel sistema sia installato `fontconfig` o almeno un carattere.

z/Linux (SUSE E11.x e RHEL 6.x)

Per sistemi quali Linux su System Z, che richiedono JDK IBM, è possibile utilizzare il supporto di installazione "*nojdk*", che non include un JDK.

— L'installazione deve poter individuare un eseguibile Java da avviare. Se l'installazione non trova un eseguibile Java, è possibile impostare la variabile di ambiente `INSTALL4J_JAVA_HOME` in modo che faccia riferimento alla directory `bin` di un'installazione Java.

— Dopo l'avvio, il programma di installazione cercherà automaticamente nel sistema JDK con versione compatibile. Se vengono trovati più JDK, verrà visualizzato un elenco dal quale scegliere. Se nel sistema viene individuato un solo JRE, è possibile continuare con l'installazione, ma il server Host Access for the Cloud non verrà eseguito correttamente fino a quando non verrà aggiornata la proprietà `wrapper.java.command` in `sessionserver/container.conf` affinché faccia riferimento all'installazione del JDK.

Se necessario, è possibile utilizzare le variabili di ambiente menzionate sopra e `INSTALL4J_JAVA_HOME_OVERRIDE` per specificare un'installazione Java determinata.

Utilizzo di un'installazione automatica

L'installazione di Host Access for the Cloud si basa sulla tecnologia install4j, che supporta la modalità automatica. L'installazione automatica consente di installare il prodotto allo stesso modo in una serie di computer.

Per utilizzare l'installazione automatica:

1. Installare il server di sessione su un computer tramite il programma di installazione automatico. È possibile utilizzare l'interfaccia grafica o la modalità console (`-c`) per installare il prodotto.

   Durante il processo di installazione viene creato un file di testo `response.varfile`, contenente le opzioni di installazione selezionate. Il file è ubicato in `[sessionserver Install]\.install4j\response.varfile`
2. Copiare `response.varfile` in un altro computer in cui si desidera installare il server di sessione.
3. Individuare il file eseguibile appropriato per l'installazione del prodotto. Avviare il programma di installazione utilizzando l'argomento `-q` e un argomento `-varfile` che specifica l'ubicazione di `response.varfile`.

Ad esempio, per installare il server di sessione su una piattaforma Linux a 64 bit con response.varfile ubicato nella stessa directory, utilizzare questo comando, dove <`2.5.x nnnn`> è la versione del prodotto e il numero di build:

```
hacloud-<2.5.x.nnnnn>-linuxx64.sh –q –varfile response.varfile
```

È inoltre possibile aggiungere l'opzione `–c` per l'installazione in modalità console, in modo da fornire un feedback come "Estrazione del file" e "Completamento dell'installazione".

Configurazione di un'installazione incompleta

Se il server di sessione non è in grado di recuperare un certificato da MSS o non è in grado di completare il processo di registrazione, è possibile che si verifichi un'installazione incompleta. Per completare l'installazione, attenersi alla procedura descritta per l'aggiunta di ulteriori server di sessione.

Se si esegue la connessione a una MSS remota tramite HTTP, completare i seguenti passaggi aggiuntivi:

1. Aprire il file del server di sessione `container.properties` e aggiornare l'indirizzo nelle proprietà riportate di seguito, sostituendo `localhost:80` con un indirizzo risolvibile per il server MSS:
   - `management.server.url`
   - `metering.server.url`
   - `id.manager.server.url`
2. Impostare la proprietà `management.server.callback.address.http` su *True* nel file del server di sessione `container.properties`.

Upgrade da versioni precedenti

Avviso: Se si sta eseguendo un upgrade, rimuovere da MSS eventuali file di attivazione associati a versioni di Host Access for the Cloud precedenti. La conservazione di file di attivazione obsoleti potrebbe determinare un accesso limitato alle sessioni.

---

1. Prima di procedere, eseguire il backup di tutte le modifiche apportate a `hacloud\sessionserver\conf\container.properties` o `hacloud\sessionserver\conf\container.conf`
2. Installare Host Access for the Cloud.
3. Ripristinare i file di cui è stato eseguito il backup nel passaggio uno e riavviare il server di sessione.
4. Installare il nuovo (o i nuovi) file di attivazione in MSS utilizzando Administrative Console > Configure Settings > Product Activation (Administrative Console > Configura impostazioni > Attivazione del prodotto), se questo passaggio non è stato gestito durante la procedura di installazione.

Altre configurazioni

Per continuare a utilizzare gli eventi del lato server creati in Reflection ZFE versione 2.3.2 o precedenti, copiare i file JAR degli eventi sul lato server presenti in `/webapps/zfe/WEB-INF/lib` a `/microservices/sessionserver/extensions/server`, e riabilitare le estensioni.

Risoluzione dei problemi relativi all'installazione

Per completare correttamente l'installazione, accertarsi di aver risolto i seguenti problemi comuni:

I file di attivazione sono stati installati e attivati in Administrative Console?

MSS utilizza file di attivazione per abilitare le funzionalità del prodotto. Con l'installazione viene fornito un file di attivazione associato al tipo di host a cui ci si sta connettendo. Se, ad esempio, si possiede una licenza per la Unisys Edition e il file di attivazione non è stato gestito durante il processo di installazione, è necessario accedere ad Administrative Console, passare a Configure Settings > Product Activation (Administrative Console > Configura impostazioni > Attivazione del prodotto) e verificare che sia presente il file di attivazione per Host Access for the Cloud e Unisys.

MSS è configurato per HTTPS?

Connettersi al sistema in cui è installato Administrative Server e accedere ad Administrative Server. In Administrative Console, aprire la sezione Security Setup e prendere nota del protocollo selezionato.

Verificare che MSS e Host Access for the Cloud stiano entrambi utilizzando certificati attendibili.

MSS importa i certificati e le chiavi private in `C:\ProgramData\Micro Focus\MSS\MSSData\certificates`. Vedere Protezione delle connessioni.

Se non si utilizzano certificati attendibili, controllare di aver configurato Host Access for the Cloud in modo da essere eseguito utilizzando HTTP.

Le proprietà della connessione sono configurate correttamente?

Nell'improbabile eventualità che sia necessario verificare le informazioni di connessione, il file `container.properties` per il componente di gestione e il server di sessione contiene le proprietà necessarie per stabilire la connessione dal server di sessione a MSS e dal browser al server di sessione.

Il file è disponibile nell'installazione di Host Access for the Cloud in `<directory-installazione>/sessionserver/conf/container.properties`.

L'installazione non viene completata in piattaforme UNIX o Linux

Il programma di installazione può bloccarsi in sistemi UNIX o Linus, in particolare se sono headless. Questo blocco può essere causato di una quantità insufficiente di entropia nel sistema, dovuta tipicamente alla mancanza di interazione con l'interfaccia utente del sistema (o alla mancanza di interfaccia utente).

Per risolvere il problema:

1. Interrompere la procedura di installazione.
2. Nella riga di comando del programma di installazione, anteporre –J alla proprietà di sistema Java: `./hacloud-xxxx-linux-x64.sh -J-Djava.security.egd=file:///dev/urandom`
3. Eseguire il programma di installazione contenente l'argomento aggiunto.

Il server su cui si sta eseguendo l'installazione è protetto in modo da impedire l'accesso alla directory temporanea?

Per ulteriori informazioni su questo problema, vedere L'installazione ha esito negativo a causa del server che impedisce l'accesso alla directory TEMP in Problemi noti.

Suggerimento: Per ulteriori informazioni sui problemi noti e la risoluzione dei problemi, vedere Riferimenti tecnici.

Porte

Configurare il firewall per consentire le connessioni sulle porte di attesa TCP seguenti:

Componente	Numeri di porte predefiniti
Server di sessione Host Access for the Cloud	◆ 7443
MSS	◆ 80* - HTTP - Console amministrativa, Terminal ID Management, Gestione conteggio ◆ 443* - HTTPS - Console amministrativa, Terminal ID Management, Gestione conteggio ◆ 7000** - Replica database ◆ 7001** - Replica database TLS ◆ 8003* - Sottosistema attendibile X.509 ◆ 8761* - Registro dei servizi ◆ 8089*** - Server conteggio

* Il server di sessione di Host Access for the Cloud e MSS effettuano richieste su questa porta

** MSS effettua richieste su questa porta

*** Il server di sessione di Host Access for the Cloud effettua richieste su questa porta

È possibile modificare le porte per Host Access for the Cloud e MSS Administrative Server in base alle necessità della propria rete. Per modificare le porte del server di sessione, vedere Come cambiare le porte.

Configurazione della distribuzione

Quando si inizia a configurare una distribuzione di Host Access for the Cloud, è necessario valutare diverse opzioni post-installazione e tenere conto dei problemi di sicurezza.

- Come impostare Terminal ID Manager
- Come impostare il conteggio
- Come impostare Automated Single Sign-On for Mainframe
- Configurazione dell'autenticazione X.509
- Come configurare il Single Sign-On tramite IIS
- Come utilizzare il proxy inverso IIS con Host Access for the Cloud

Come impostare Terminal ID Manager

La procedura Setting up the Terminal ID Manager (Configurazione di Terminal ID Manager) richiede che questa funzione sia abilitata in MSS.

Management and Security Server include Terminal ID Manager per creare pool di ID terminale, tenere traccia dell'utilizzo degli ID e gestire i valori di timeout per inattività per utenti specifici, conservando quindi risorse ID del terminale e riducendo significativamente le spese operative.

L'add-on Terminal ID Manager richiede una licenza separata.

Prima di configurare Terminal ID Manager per Host Access for the Cloud, verificare che questa opzione sia attivata per MSS. Istruzioni complete sono disponibili nella MSS Installation Guide (Guida all'installazione di MSS).

Suggerimento: Se MSS e Host Access for the Cloud sono installati nello stesso computer e utilizzano la porta 80, non sono necessarie ulteriori configurazioni.

Configurazione di Terminal ID Manager per Host Access for the Cloud

Per configurare Terminal ID Manager per Host Access for the Cloud, è necessario fornire l'indirizzo corretto a Terminal ID Manager.

1. Aprire il file `sessionserver/conf/container.properties`.
2. Aggiornare `id.manager.server.url=http://localhost:80/tidm` per riflettere l'indirizzo di Terminal ID Manager configurato in Management and Security Server.
3. Riavviare il server di sessione.

Come impostare il conteggio

MSS offre funzionalità di conteggio per il monitoraggio delle sessioni host. Vedere Metering (Conteggio).

Management and Security Server offre la funzione di conteggio per monitorare le sessioni host.

Prima di configurare il conteggio per Host Access for the Cloud, verificare che questa funzione sia abilitata per MSS. Istruzioni complete sono disponibili nella Installation Guide (Guida all'installazione di MSS).

In Host Access for the Cloud il conteggio viene impostato a livello globale per tutte le sessioni di emulazione create dal server di sessione. Le impostazioni sono specificate nel file `sessionserver/conf/container.properties`.

Tabella 3-1 *Opzioni di analisi*

Proprietà	Descrizione
`metering.enabled`	Attiva o disattiva l'analisi, con un valore "true" o "false". Qualsiasi valore diverso da "true" disattiva l'analisi.
`metering.host.required`	Determina se la sessione può connettersi all'host anche se non è possibile contattare il server di analisi. "True" significa che le connessioni della sessione non riusciranno se l'host di analisi non è disponibile. "False" significa che le connessioni della sessione riusciranno anche se l'host di analisi non è disponibile.
`metering.server.url`	Specifica il nome o l'indirizzo del server di analisi, la porta, il protocollo e il contesto webapp. La sintassi è "`host:port|protocol|context`". La sintassi è la stessa utilizzata dal server MSS nel file `MssData/serverconfig.props` per registrare i server di analisi. Nella sezione host:port dell'URL il carattere ":" deve essere preceduto dal carattere di escape. Ad esempio, `test990.attachmate.com\:8080`.

```
#Example additions to sessionserver/conf/container.properties
   metering.enabled=true
   metering.host.required=false
   metering.server.url=10.10.11.55\:80|http|meter
```

Nota: Nel caso in cui tutte le licenze siano utilizzate e si tenti di stabilire una connessione, la sessione verrà disconnessa. Per determinare se l'host si è disconnesso o se il servizio di conteggio ha interrotto la connessione, vedere il file `<directory-installazione>/sessionserver/logs/sessionserver.log`.

Come impostare Automated Single Sign-On for Mainframe

Automated Sign-On for Mainframe - Administrator Guide (Sign-On automatico per i mainframe - Guida all'amministrazione) contiene le informazioni complete per la configurazione di questa opzione.

Automated Sign-On for Mainframe è un add-on di Management and Security Server che consente all'utente finale di eseguire l'autenticazione a un client di emulazione di terminale e accedere automaticamente a un'applicazione host nel mainframe z/OS.

1. Installare e configurare l'add-on Automated Sign-On for Mainframe per Management and Security Server. È possibile trovare le istruzioni complete qui.
2. Al termine dell'installazione di Management and Security Server, aprire Administrative Console per aggiungere sessioni e mappare gli utenti alle sessioni. Durante questa procedura è possibile completare la configurazione aggiuntiva necessaria per implementare l'accesso automatico.

3 Una macro Host Access for the Cloud invia il nome utente e il pass ticket del mainframe dell'utente all'applicazione host. L'accesso dell'utente viene quindi eseguito automaticamente. Informazioni per la creazione della macro:

- L'API Macro contiene l'oggetto AutoSignon che fornisce i metodi necessari per creare un login a Host Access for the Cloud da utilizzare con la funzione Automated Sign-On for Mainframe (Sign-On automatico per mainframe).
- È anche possibile fare riferimento alla macro di esempio Macro di accesso automatico per mainframe che utilizza l'oggetto AutoSignon per creare una macro che utilizza le credenziali associate a un utente per ottenere un pass ticket da DCAS (Digital Certificate Access Server).

Configurazione dell'autenticazione X.509

L'autenticazione client X.509 consente ai client di autenticarsi con i server utilizzando certificati anziché nome utente e password, sfruttando lo standard dell'infrastruttura a chiave pubblica (PKI) X.509.

In MSS sono disponibili informazioni dettagliate sulla X.509 Configuration (Configurazione X.509).

Quando si abilita l'autenticazione client X.509:

- Quando l'utente accede al client Web mediante TLS, il browser invia un certificato al server di sessione identificando l'utente finale e completando l'handshake TLS.
- Il server di sessione fa riferimento al proprio archivio attendibilità per verificare il certificato del client e la relativa attendibilità.
- Quando la negoziazione TLS è stata completata, ossia l'utente finale è considerato attendibile dal server di sessione, questo invia il certificato pubblico dell'utente finale a MSS per ulteriore convalida.
- Anche MSS conferma l'attendibilità del certificato dell'utente finale confrontandolo con il proprio archivio attendibilità.
- Quando MSS termina la convalida, l'utente finale sarà stato autenticato correttamente.

La catena completa dei certificati del client deve essere presente negli archivi attendibilità del server di sessione e di MSS oppure deve essere firmata da un'autorità di certificazione presente in tali archivi.

Il browser determina il modo in cui inviare il certificato del client in base alla configurazione specifica del browser o della smart card.

Passaggi di base:

1. Confermare l'attendibilità dei certificati nel server di sessione e in MSS se questa operazione non è stata ancora eseguita.
2. Riavviare i server.
3. Configurare X.509 in MSS Administrative Console.

Passaggio 1. Confermare l'attendibilità del certificato in MSS e nel server di sessione

- **Confermare l'attendibilità del certificato in MSS**

  È possibile che l'archivio attendibilità di MSS contenga già il certificato dell'autorità di firma. Questo accade spesso con autorità di firma del certificato note e, in questo caso, ignorare questo passaggio.

  Per verificare:

  Aprire Administrative Console, fare clic su Configure Settings (Configura impostazioni) e aprire la scheda Trusted Certificates (Certificati attendibili). Aprire **Trusted Root Certificate Authorities** (Autorità di certificazione fonti attendibili) per visualizzare un elenco dei certificati disponibili.

  Se il certificato non è presente nell'elenco, è necessario installare l'autorità di certificazione principale di firma in MSS, seguendo le istruzioni e la documentazione seguenti in Administrative Console.

- **Confermare l'attendibilità del certificato nel server di sessione**

  Per installare il certificato nel server di sessione:

  In `<directory di installazione>\sessionserver\etc` importare il certificato:

  ```
  keytool -importcert -file <file certificato> -alias <alias con cui memorizzare il certificato> -keystore trustcerts.bcfks -storetype bcfks -providername BCFIPS -providerclass org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider -providerpath ../lib/bc-fips-*.jar -storepass changeit
  ```

Passaggio 2. Riavviare tutti i server

Per rendere effettiva la configurazione, è necessario riavviare tutti i server.

Passaggio 3. Configurazione di X.509 con failover LDAP in MSS Administrative Console

Una volta importati i certificati, è possibile abilitare X.509 con l'opzione Fallback to LDAP authentication (Fallback all'autenticazione LDAP) in **Management and Security Server Administrative Console | Configure Settings (Configura impostazioni) | Authentication & Authorization (Autenticazione e autorizzazione)**. Per le descrizioni delle opzioni di configurazione vedere la Guida in linea di Administrative Console.

Utilizzo dell'autenticazione X.509 mediante il bilanciamento del carico configurato per l'interruzione TLS

In questa configurazione, il bilanciamento del carico fornisce l'autenticazione dell'utente finale convalidando il certificato client. Tuttavia, il certificato client deve ancora essere inviato a tutti i sistemi MSS per identificare l'utente in entrata.

Se il bilanciamento del carico è configurato per interrompere la connessione TLS, è possibile aggiungere il certificato dell'utente a un'intestazione HTTP, estratta dal server di sessione, quindi passare a MSS per l'autorizzazione. Per trasmettere il certificato in un'intestazione, è necessario innanzitutto impostare il nome dell'intestazione nel file container.properties del server di sessione HACloud:

Per trasmettere il certificato in un'intestazione

1. Impostare il nome dell'intestazione nel file `container.properties` del server di sessione HACloud:

   ```
   x509.header.client.cert=X-SSL-Client-Cert
   ```

2. Impostare il valore dell'intestazione sul certificato dell'utente nella configurazione del bilanciamento del carico. Ad esempio, se si utilizza un BigIP iRule:

   ```
   HTTP::header insert X-SSL-Client-Cert [URI::encode $client_cert]
   ```

   In questo modo si presuppone che `$client _cert` sia stato impostato sul certificato dell'utente in formato PEM. Se il certificato dell'utente è in formato DER, utilizzare la codifica Base64:

   ```
   HTTP::header insert X-SSL-Client-Cert [b64encode $client_cert]
   ```

   La codifica del certificato assicura che il valore dell'intestazione sia una riga di testo ASCII. Questo è necessario affinché il server di sessione di HACloud possa leggere il valore.

   Nota: È necessario che l'autenticazione del certificato client venga effettuata tra il bilanciamento del carico e il server di sessione. È necessario configurare il bilanciamento del carico per inviare il certificato al server di sessione e che la CA del bilanciamento del carico sia presente nell'archivio attendibilità del server di sessione.

   ---

3. Una volta configurato il bilanciamento del carico per inviare il relativo certificato al server di sessione di HACloud e il certificato dell'utente da trasmettere nell'intestazione, riavviare il server di sessione.

La connessione a un certificato o a una smart card tramite il bilanciamento del carico comporterà la corretta autenticazione e l'autorizzazione come l'utente rappresentato dal certificato. Per verificare il corretto funzionamento, impostare il livello di log del server di sessione su DEBUG ed esaminare il file `sessionserver.log` per voci come queste:

```
Attempting to extract certificate from X-SSL-Client-Cert header (Tentativo
di estrazione del certificato dall'intestazione X-SSL-Client-Cert).
  User <DN value> has been preauthenticated from <IP address> (Il <valore
DN> dell'utente è stato preautenticato dall'<indirizzo IP>)
```

Altre configurazioni

Per default, l'archivio attendibilità del server di sessione di HACloud contiene i certificati CA Java. In questo modo, il server di sessione di HACloud accetterà tutti i certificati client firmati dalle CA conosciute. Per assicurare che solo i bilanciamenti del carico desiderati vengano collegati al server di sessione, è necessario rimuovere i certificati CA Java dall'archivio attendibilità e verificare che qui siano installati solo i certificati necessari.

Per filtrare i certificati client consentiti per DN dell'emittente, impostare le seguenti proprietà nel file `container.properties` del server di sessione HACloud:

```
X509.client.cert.issuer=<Valore DN>
   X509.client.cert.subject=<Valore DN del soggetto>
   X509.client.cert.serial=<Numero di serie>
   X509.client.cert.sha1=<Impronta digitale SHA1>
   X509.client.cert.sha256=<Impronta digitale SHA256>
```

I valori DN devono corrispondere esattamente al DN dell'oggetto o all'emittente del certificato del bilanciamento del carico. Il valore del numero di serie deve essere un valore decimale (base 10). È necessario immettere i valori delle impronte digitali SHA1 e SHA256 in formato esadecimale. Se si imposta una di queste proprietà, vengono verificati gli attributi del certificato in entrata per garantire che corrispondano ai valori delle proprietà specificati. L'autorizzazione avrà esito negativo se i valori non corrispondono.

Come configurare il Single Sign-On tramite IIS

Per ulteriori informazioni, vedere Single Sign-on through IIS (Single Sign-On tramite IIS) nella documentazione di MSS Administrative Console.

Questa opzione utilizza il server Web Microsoft IIS.

Per abilitare Host Access for the Cloud affinché possa essere utilizzato con questo metodo di autenticazione, aggiungere la seguente proprietà nel file `<directory di installazione>/sessionserver/conf/container.properties`:

```
management.server.iis.url=<url>
```

Il valore di questa proprietà è l'indirizzo e la porta del server Web IIS insieme al percorso / MSS. Ad esempio: `http://server/mss`. Se l'autenticazione non riesce, potrebbe essere necessario rimuovere il nome del dominio affinché le credenziali del dominio vengano passate a `IIS: http://server/mss`.

Argomenti correlati

Come utilizzare il proxy inverso IIS con Host Access for the Cloud

Come utilizzare il proxy inverso IIS con Host Access for the Cloud

Prima di configurare, leggere Accesso a Host Access for the Cloud mediante il proxy inverso IIS per i prerequisiti e le istruzioni di configurazione.

Utilizzo del proxy inverso IIS con Host Access for the Cloud

Nota: Per garantire la conformità con i requisiti di sicurezza Common Criteria, può essere necessario utilizzare un proxy per il server di sessione, seguendo le istruzioni fornite in Accesso a Host Access for the Cloud mediante il proxy inverso IIS.

Per utilizzare IIS come proxy per Host Access for the Cloud, con il Single Sign-On con IIS, è necessario impostare una proprietà aggiuntiva nello stesso file `container.properties`:

```
servletengine.iis.url=<url>
```

Il valore assume lo stesso formato dell'URL riportato sopra, ma utilizzerà l'indirizzo di Host Access for the Cloud. Ad esempio: `http://server/`. Non è necessario utilizzare il formato di nome host breve in questo URL.

Dopo aver completato questa configurazione, scegliere questa opzione di autenticazione in **Management and Security Server Administrative Console | Assign Access**. Vedere la guida in linea di Administrative Console per le descrizioni delle opzioni di configurazione.

Argomenti correlati

Come configurare il Single Sign-On tramite IIS

Protezione delle connessioni

Host Access for the Cloud utilizza il protocollo TLS (Transport Layer Security) per proteggere, mediante cifratura, la comunicazione tra i browser Web client, il server di sessione, MSS e gli host di backend.

In questa sezione:

Panoramica

Infrastruttura a chiave pubblica (PKI, Public Key Infrastructure)

Per implementare la sicurezza, TSL utilizza l'infrastruttura a chiave pubblica (PKI). L'infrastruttura a chiave pubblica utilizza chiavi pubbliche e private per proteggere la comunicazione tra il client e il server. Le chiavi pubbliche e private sono correlate in modo matematico ma non sono identiche. Questo significa che un messaggio cifrato con una chiave pubblica può essere decifrato solo utilizzando la chiave privata. Insieme, queste chiavi sono denominate coppia di chiavi.

Certificati

I certificati digitali sono credenziali che verificano le identità di utenti, computer e reti. Forniscono il collegamento tra una chiave pubblica e un'azienda che è stata verificata (firmata) da una terza parte attendibile, denominata autorità di certificazione (CA). I certificati digitali rappresentano una comoda soluzione per distribuire chiavi di cifratura pubbliche attendibili.

Archivi chiavi

I certificati e le chiavi private vengono memorizzati negli archivi chiavi Java. Le voci degli archivi chiavi vengono identificate con un identificatore univoco, denominato **alias**. Spesso le chiavi private e i certificati, con la chiave pubblica corrispondente, vengono memorizzati separatamente rispetto ai certificati ricevuti da altre parti che si utilizzano per garantire l'attendibilità. Questo archivio chiavi separato è denominato **archivio attendibilità**. Un archivio attendibilità contiene i certificati provenienti da parti con le quali si prevede di comunicare o da autorità di certificazione considerate attendibili per identificare altre parti.

Installazione sicura predefinita

Durante l'installazione di HACloud e MSS, i certificati firmati da se stessi vengono generati, scambiati e quindi utilizzati per proteggere tutte le comunicazioni tra il server di sessione, i browser Web e MSS. I certificati firmati da se stessi sono certificati di identità che vengono firmati dalla stessa entità di cui certificano l'identità.

I server di sessione e i server MSS utilizzano i certificati firmati da se stessi generati per identificarsi con client remoti, ad esempio browser Web, altri server di sessione e server MSS. Questi certificati firmati da stessi e le loro chiavi private vengono memorizzati nei rispettivi archivi chiavi.

Nella guida di MSS Administrative Console sono disponibili informazioni dettagliate su General Security and Certificates (Sicurezza generale e certificati).

Per la comunicazione sicura tra client (browser Web, server di sessione e server MSS) i client devono considerare attendibile il certificato firmato da se stessi generato. Il server di sessione conferma l'attendibilità del certificato MSS durante l'installazione e lo memorizza nel proprio archivio attendibilità. Allo stesso modo, durante l'installazione MSS recupera e conferma l'attendibilità del certificato del server di sessione e lo memorizza nel proprio archivio attendibilità.

Valori predefiniti:

- Password: **changeit**
- Tipo di archivio chiave - **bcfks (archivio chiavi Bouncy Castle FIPS**)
- Ubicazione del certificato firmato da se stessi MSS: `MSS/server/etc/<nome-computer>.cer`
- Ubicazione del certificato del server di sessione HACloud firmato da se stessi: `HACloud/SessionServer/etc/keystore.cer`

Strumenti

- **KeyStore Explorer** - La utility KeyStore Explorer offre un'interfaccia utente semplice per creare richieste di firma (CSR) e importare certificati firmati da autorità di certificazione in Host Access for the Cloud.
  - Per avviare Keystore Explorer in Windows, eseguire `\HACloud\utilities\keystore-explorer.bat` come amministratore o come utente con diritti amministrativi.
  - Per avviare Keystore Explorer in UNIX, eseguire `hacloud\utilities\keystore-explorer.sh` come amministratore o come utente con diritti amministrativi.

  La utility è dotata di una Guida in linea che illustra l'interfaccia utente.
- **Java Keytool**: Java Key and Certificate Management Tool gestisce un archivio di chiavi di crittografia, catene di certificati X.509 e certificati attendibili. Utilizza un'interfaccia da riga di comando. La documentazione relativa allo strumento di gestione chiavi e certificati di Java è disponibile per le piattaforme Unix e Windows:
  - UNIX (http://docs.oracle.com/javase/8/docs/technotes/tools/unix/keytool.html)
  - Windows (http://docs.oracle.com/javase/8/docs/technotes/tools/windows/keytool.html)

- **Entropia e cifratura** - L'entropia rappresenta la generazione di dati in modo casuale da parte di un sistema operativo per l'utilizzo nella crittografia. La casualità viene spesso raccolta dalle fonti hardware, ad esempio i movimenti del mouse. La mancanza di entropia può avere un impatto negativo sulle prestazioni e la sicurezza e sarà più evidente nelle installazioni basate su server headless.

  Soluzioni per migliorare la generazione di entropia:

  — Parametro Keytool - Per modificare la modalità di generazione dell'entropia, aggiungere un parametro aggiuntivo alla riga di comando keytool di Linux. `-J-Djava.security.egd=file:/dev/urandom`

  — Strumento *Haveged* - È uno strumento che consente di porre rimedio a condizioni di scarsa entropia del generatore di numeri casuali di Linux, che possono verificarsi in presenza di determinati carichi di lavoro, in particolare su server headless. Per ulteriori informazioni su questo strumento, vedere https://wiki.archlinux.org/index.php/Haveged.

Procedure

- Richiesta di un certificato di identità digitale (richiesta di firma del certificato)
- Sostituzione del certificato del server di sessione
- Sostituzione del certificato MSS
- Effettuare una connessione di emulazione sicura a un host attendibile.
- Configurazione dell'autenticazione client X.509 dal browser dell'utente finale nel server di sessione
- Configurazione degli eventi lato server per effettuare chiamate TLS in uscita dal server di sessione
- Aggiunta di più server MSS a un'installazione
- Aggiunta di ulteriori server di sessione all'installazione MSS con più server
- Importazione di un certificato nell'archivio attendibilità del server di sessione

Richiesta di un certificato di identità digitale (richiesta di firma del certificato)

Termini utilizzati

- chiave privata: chiave segreta conosciuta solo dal proprietario, utilizzata con un algoritmo per la cifratura/decifratura dei dati
- coppia di chiavi: chiave privata e la catena di certificati associata
- nome distinto: informazioni di identificazione in un certificato. Un certificato contiene informazioni DN sia per il proprietario/il richiedente del certificato (denominato nome distinto dell'oggetto) che per l'autorità di certificazione che ha rilasciato il certificato (denominata nome distinto dell'emittente)
- Certificato X.509: certificato digitale che utilizza lo standard internazionale PKI (infrastruttura a chiave pubblica) X.509, ampiamente accettato, per verificare che la chiave pubblica appartenga all'utente

Prima di creare una richiesta di firma di un certificato (CSR), il richiedente genera una coppia di chiavi, mantenendo segreta la chiave privata. La CSR contiene informazioni che identificano il richiedente, ad esempio il *nome distinto*, nel caso di un certificato X.509, che devono essere firmate utilizzando la chiave privata del richiedente. La CSR contiene inoltre la chiave pubblica scelta dal richiedente.

Come creare una CSR con KeyStore Explorer

La creazione di una CSR consiste nel creare una coppia di chiavi, quindi generare una richiesta di certificato. Se non è necessario aggiornare le informazioni del certificato, è possibile ignorare la creazione della coppia di chiavi e procedere alla generazione della richiesta di certificato.

- Creare una nuova coppia di chiavi
  - Nel menu Tools (Strumenti) selezionare Generate Key Pair (Genera coppia di chiavi).
  - Nella finestra di dialogo Generate Key Pair (Genera coppia di chiavi) immettere le informazioni dell'algoritmo e i dettagli del certificato. Fare clic su OK.
  - Specificare l'alias pertinente (servlet-engine) e la password predefinita (changeit).
- Generare una richiesta di certificato
  - Selezionare la coppia di chiavi appena creata.
  - Nel menu contestuale selezionare Generate CSR (Genera CSR).
  - Passare alla posizione in cui generare la CSR e immettere il nome file. Fare clic su OK.

Come creare una CSR con Java Keytool

Creare una coppia di chiavi (sostituire il parametro `dname` con il proprio) nella cartella`sessionserver/etc`:

```
..\..\java\bin\keytool.exe -genkeypair -dname "CN=hacloud-
1.microfocus.com, O=Micro Focus, C=US" -alias servlet-engine -keyalg RSA -
keysize 2048 -keystore keystore.bcfks -validity 1095 -storetype bcfks -
storepass changeit -keypass changeit -providername BCFIPS -providerpath ../
lib/bc-fips-*.jar -providerclass
org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider
```

Generare una richiesta di certificato:

```
..\..\java/bin\keytool -certreq -alias servlet-engine -keystore
keystore.bcfks -file cert_request.csr -ext ExtendedkeyUsage=serverAuth -
storetype bcfks -storepass changeit -providername BCFIPS -providerpath ../
lib/bc-fips-*.jar -providerclass
org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider
```

Dopo aver ricevuto il certificato dall'autorità di certificazione, sarà necessario importarlo in Host Access for the Cloud.

Sostituzione del certificato del server di sessione

L'installazione viene protetta mediante i certificati firmati da se stessi. Sebbene siano sicuri quanto i certificati commerciali, i certificati firmati da se stessi non vengono considerati automaticamente attendibili. Pertanto sono difficili da gestire. I certificati commerciali sono necessari quando si desidera che un certificato sia ampiamente supportato e, per fortuna, la maggior parte di browser Web e sistemi operativi già supporta molte autorità di certificazioni commerciali.

Informazioni indispensabili:

- **ubicazione dell'archivio chiavi** - `/etc/keystore.bcfks`
- **formato dell'archivio chiavi** bcfks (Bouncy Castle FIPS)
- **password predefinita** - changeit
- **alias della coppia di chiavi** - servlet-engine

La procedura per sostituire il certificato firmato da se stessi varia a seconda che lo si sostituisca con un certificato ottenuto mediante CSR nell'archivio chiavi predefinito oppure con un archivio chiavi e certificato non predefiniti.

Sostituire certificato firmato da se stessi con risposta di certificato da autorità di certificazione (CA)

1. Creare una richiesta di firma del certificato (CSR) per il server di sessione e inviarla all'autorità di certificazione prescelta. Quando si riceve il certificato firmato dall'autorità di certificazione, procedere nel modo seguente:
2. Importare il certificato/la catena firmato/a nell'archivio chiavi del server di sessione.

   È possibile eseguire questo task utilizzando KeyStore Explorer o le istruzioni da riga di comando di Java Keytool. Indipendentemente dallo strumento prescelto, se CA Reply contiene file separati per il certificato radice e il certificato intermedio, importare nell'archivio chiavi prima il certificato radice, quindi il certificato intermedio.

Strumento utilizzato	Procedura
Keystore Explorer	1. Aprire `keystore.bcfks` in KeyStore Explorer. Utilizzare la password **changeit**. 2. Se sono disponibili file separati per il certificato radice e intermedio, nella barra degli strumenti selezionare **Import Trusted Certificate** per importare i certificati. 3. Selezionare la coppia di chiavi `servlet-engine`. Fare clic con il pulsante destro del mouse e selezionare **Import CA Reply** per importare il file nella coppia di chiavi. 4. Se richiesto, immettere la password **changeit**. 5. Passare alla posizione in cui è memorizzato il file CA Reply, selezionarlo e fare clic su Import.

Strumento utilizzato	Procedura
JavaKeytool	**Windows**

In questi esempi vengono utilizzati i comandi di keytool nella directory `sessionserver\etc`.	**Importare certificati CA radice e certificati intermedi**
	`..\..\java\bin\keytool.exe -importcert -alias rootca -trustcacerts -file <RootCA.cer> -keystore keystore.bcfks –storetype bcfks -storepass changeit`
	`..\..\java\bin\keytool.exe -importcert -alias intermediateca -trustcacerts -file <IntermediateCA.cer> -keystore keystore.bcfks –storetype bcfks -storepass changeit -providername BCFIPS -providerpath ../lib/bc-fips-*.jar -providerclass org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider`
	Importare CA Reply
	`..\..\java\bin\keytool.exe -importcert -alias servlet-engine -trustcacerts -file <CertChainFromCA.p7b> -keystore keystore.bcfks –storetype bcfks -storepass changeit -providername BCFIPS -providerpath ../lib/bc-fips-*.jar -providerclass org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider`

JavaKeytool **UNIX**

Importare certificati CA radice e certificati intermedi

```
../../java/bin/keytool -importcert -alias rootca -
trustcacerts -file <RootCA.cer> -keystore
keystore.bcfks –storetype bcfks -storepass changeit -
providername BCFIPS -providerpath ../lib/bc-fips-*.jar
-providerclass
org.bouncycastle.jcajce.provider.BouncyCastleFipsProvid
er
```

```
../../java/bin/keytool -importcert -alias
intermediateca -trustcacerts -file <IntermediateCA.cer>
-keystore keystore.bcfks –storetype bcfks -storepass
changeit -providername BCFIPS -providerpath ../lib/bc-
fips-*.jar -providerclass
org.bouncycastle.jcajce.provider.BouncyCastleFipsProvid
er
```

Importare CA Reply

```
../../java/bin/keytool -importcert -alias servlet-
engine -trustcacerts -file <CertChainFromCA.p7b> -
keystore keystore.bcfks –storetype bcfks -storepass
changeit -providername BCFIPS -providerpath ../lib/bc-
fips-*.jar -providerclass
org.bouncycastle.jcajce.provider.BouncyCastleFipsProvid
er
```

3 Confermare l'attendibilità del nuovo certificato in MSS.

- Eseguire il login a MSS come amministratore.
- Nel riquadro sinistro fare clic su **Configure Settings (Configura impostazioni) > Trusted Certificates (Certificati attendibili)**.
- Selezionare **Trusted Sub-System (Sottosistema attendibile)**. L'elenco contiene i certificati che MSS considera attendibili.
- Fare clic su **IMPORT** (IMPORTA) per aggiungere il certificato del server di sessione all'elenco.
- Non è necessario ripetere la procedura per ciascun MSS. Le modifiche vengono replicate automaticamente negli altri MSS del cluster.

L'Administrative Console dispone di una guida dettagliata - General Security and Certificates (Sicurezza generale e certificati).

Sostituzione del certificato con l'archivio chiavi non predefinito

È possibile utilizzare un archivio chiavi diverso da quello predefinito (`sessionserver/etc/keystore.bcfks`) per memorizzare i certificati firmati dall'autorità di certificazione.

In `sessionserver/conf/container.properties` specificare le seguenti proprietà:

```
server.ssl.key-store
   server.ssl.key-store-password
```

Dove il percorso dell'archivio chiavi è impostato sul nome file dell'archivio chiavi non predefinito e la password dell'archivio chiavi è impostata sul valore offuscato generato dal comando seguente, dalla directory `sessionserver`:

```
../java/jre/bin/java -cp./lib/jetty-util-<version>.jar
org.eclipse.jetty.util.security.Password passwordToObfuscate
```

Ad esempio:

```
server.ssl.key-store=${server.home}/etc/custom.bcfks
   server.ssl.key-store-password=OBF:1vn21ugu1saj1v9i1v941sar1ugw1vo0
```

Per evitare confusione, eliminare l'archivio chiavi predefinito.

Per evitare che l'archivio chiavi venga generato all'avvio del server, aprire il file `/conf/product-core-ctx.xml` in un editor di testo e rimuovere la sezione `servletEngineKeystoreGenerator` o impostarla come commento. Riavviare il server di sessione.

Sostituzione del certificato MSS

Esaminare la modalità di sostituzione del certificato MSS nell'argomento General Security and Certificates (Sicurezza generale e certificati).

Durante l'installazione, per stabilire una connessione sicura, il server di sessione considera attendibile il certificato MSS esistente. Se il certificato MSS viene aggiornato, deve esserne nuovamente confermata l'attendibilità da tutti i server di sessione HACloud.

Per sostituire il certificato MSS

- Per considerare attendibile il nuovo certificato MSS, importarlo nell'archivio attendibilità del server di sessione utilizzando l'alias **mss**. Vedere Importazione di un certificato nell'archivio attendibilità del server di sessione
- È necessario importare il nuovo certificato attendibile in ciascun server di sessione.

Effettuare una connessione di emulazione sicura a un host attendibile.

Completare questi passaggi per configurare una connessione TLS tra il server di sessione Host Access for the Cloud e un host che supporta TLS:

1. Configurare l'archivio chiavi attendibile in MSS.
2. Configurare la sessione di terminale.

Come configurare l'archivio chiavi in MSS

Aprire MSS Administrative Console > Configure Settings > Trusted Certificates e scegliere **Terminal Emulator Clients**. È possibile accedere alla documentazione su Administrative Console facendo clic sull'icona Guida in alto a destra sulla pagina.

Affinché una sessione consideri attendibile l'host TLS a cui si connette, il certificato pubblico dell'host deve essere aggiunto a un archivio chiavi attendibile tramite Management and Security Server (MSS). La sessione di Host Access for the Cloud recupera questo certificato la prima volta in cui una sessione si connette.

Quando il certificato viene aggiunto al keystore attendibile del server MSS, viene visualizzato nuovamente l'elenco dei certificati contenente il nuovo host.

Come configurare una sessione di terminale di HACloud

A seconda del tipo di host utilizzato, è possibile configurare una sessione di terminale utilizzando protocolli di sicurezza differenti.

Tipo	Procedura
Utilizzo di TLS	Per eseguire la connessione al nuovo host attendibile mediante TLS, configurare una sessione di terminale come di norma quindi, nella finestra di dialogo Impostazioni, specificare TLS come protocollo di sicurezza. Assicurarsi di specificare la porta TLS corretta per la connessione.
Utilizzo di Secure Shell (SSH) con i tipi di host VT	Secure Shell fornisce comunicazioni crittografate fra il client e un host VT. MSS include un elenco di host noti che contiene le chiavi pubbliche degli host ai quali è possibile connettersi tramite SSH. Le connessioni SSH possono essere stabilite solo con host già attendibili da un amministratore. La prima volta che si effettua una connessione SSH da una sessione a un host, viene effettuato il download del file degli host conosciuti da MSS nel server di sessione. Quando si tenta di creare o modificare una sessione mediate SSH nel pannello di gestione delle sessioni, se la chiave non è riconosciuta come attendibile verrà visualizzata una notifica e verrà chiesto se continuare considerando la chiave come attendibile. ◆ Se si sceglie Sì, l'host verrà considerato attendibile e verrà aggiunto all'elenco di host conosciuti, quindi all'utente verrà richiesta la password dell'host SSH. ◆ Se non si sceglie Sì, l'host verrà considerato non attendibile e la sessione verrà disconnessa. È anche possibile configurare manualmente il file degli host conosciuti in SSH effettuando una connessione SSH da una sessione all'host, quindi aggiungendo l'impronta digitale della chiave dell'host remoto all'elenco di host conosciuti in MSS.

Tipo	Procedura
Configurazione del file degli host conosciuti per le connessioni SSH in MSS	1. Connettere il sistema in cui è installato MSS e passare alla cartella dei certificati del server: `C:\ProgramData\Micro Focus\Mss\MssData\certificates` (Windows) o `/var/opt/microfocus/mss/Mssdata/certificates` (UNIX). 2. Copiare il file di certificato pubblico del nuovo host SSH nella cartella `MssData/certificates` (Windows) o `/etc/ssh/ssh_host_rsa_key.pub` (UNIX) descritta sopra. Solo `ssh-rsa` e `ssh-dss` sono validi come tipi di chiavi pubbliche per le voci known_hosts di MMS. Il formato della chiave pubblica dell'host può essere OpenSSH, Base64-encode,.DER, o .PFX. Il file deve avere il formato seguente: nome host, indirizzo IP tipo chiave chiave. Ad esempio, una voce di chiave pubblica potrebbe essere simile alla seguente: `alpsuse132, 10.117.16.232 ssh-rsa AAAAB3NzaC1yc2EAAAADAQABA.....` 3. Accedere a MSS (ad esempio, `http://mycompany.com/adminconsole`). 4. Aprire **Administrative Console**. 5. Fare clic su Configure Settings > Secure Shell. Dopo che la chiave pubblica è stata importata nel file degli host conosciuti, l'utente tornerà alla pagina Secure Shell Known Hosts (Host Secure Shell conosciuti) e il nuovo host sarà presente nell'elenco. 6. Seguire le indicazioni in MSS per importare un host conosciuto. Una volta che la chiave pubblica è stata importata nel file degli host conosciuti, l'utente tornerà alla pagina Secure Shell Known Hosts (Host Secure Shell conosciuti) e il nuovo host sarà presente nell'elenco.

Configurazione dell'autenticazione client X.509 dal browser dell'utente finale nel server di sessione

Sono disponibili le istruzioni complete sulla Configurazione dell'autenticazione X.509 da seguire.

Configurazione degli eventi lato server per effettuare chiamate TLS in uscita dal server di sessione

Quando si scrive codice Java che viene eseguito negli eventi lato server, può essere necessario effettuare chiamate in uscita ai server remoti utilizzando TLS. Se il server remoto è conosciuto, potrebbe già essere considerato attendibile dal server di sessione, quindi non sarà necessario effettuare altre operazioni di configurazione. Tuttavia, spesso il server remoto non è conosciuto, pertanto è necessario confermarne l'attendibilità importandone il certificato nell'archivio attendibilità del server di sessione.

Per confermare l'attendibilità del server remoto

Importarne il certificato pubblico nell'archivio attendibilità del server di sessione, attenendosi alle istruzioni fornite in Importazione di un certificato nell'archivio attendibilità del server di sessione

Aggiunta di più server MSS a un'installazione

Durante l'installazione i server MSS e HACloud si sono scambiati i rispettivi certificati e li hanno considerati attendibili. Quando si aggiungono ulteriori server MSS, devono essere considerati attendibili anche i relativi certificati.

La configurazione è obbligatoria in MSS Administrative Console > Configure Settings (Configura impostazioni) > Trusted Certificates (Certificati attendibili) > Trusted Sub-System (Sottosistema attendibile).

Per configurare l'attendibilità tra il server di sessione e MSS

- Per fare in modo che il server MSS venga considerato attendibile, importare il certificato MSS nell'archivio attendibilità del server di sessione. Vedere Importazione di un certificato nell'archivio attendibilità del server di sessione
- Il nuovo server MSS deve considerare attendibile ciascun server di sessione.
  - Eseguire il login a MSS come amministratore.
  - Nel riquadro sinistro fare clic su **Configure Settings (Configura impostazioni) > Trusted Certificates (Certificati attendibili)**.
  - Selezionare **Trusted Sub-System (Sottosistema attendibile).** L'elenco contiene i certificati che MSS considera attendibili.
  - Fare clic su **IMPORT** (IMPORTA) per aggiungere il certificato del server di sessione all'elenco.
  - Ripetere questa procedura per ciascun server di sessione.

Aggiunta di ulteriori server di sessione all'installazione MSS con più server

Durante l'installazione, il server di sessione e MSS si sono già scambiati e hanno considerato attendibili i relativi certificati, pertanto tutti i server MSS considerano attendibili tutti i server di sessione esistenti. Tuttavia, quando si aggiungono ulteriori server di sessione, è necessario stabilire una relazione di attendibilità tra i nuovi server di sessione e i server MSS esistenti.

Per aggiungere ulteriori server di sessione

1. Importare il certificato del server MSS nell'archivio attendibilità del server di sessione. Vedere Importare un certificato nell'archivio attendibilità del server di sessione.
2. Importare il certificato del server di sessione nell'archivio attendibilità del server MSS. Vedere Certificati attendibili nella documentazione relativa a MSS.
3. Recuperare `service.registry.password` dal file del server MSS `container.properties`.
4. Impostare il `service.registry.password` nel file del server di sessione `container.properties`.

Importazione di un certificato nell'archivio attendibilità del server di sessione

Quando il server di sessione tenta di effettuare connessioni sicure in uscita ai server remoti, verifica l'identità di tali server utilizzando i certificati disponibili nel proprio archivio attendibilità. Tutti i certificati importati in questo archivio verranno considerati attendibili.

Informazioni indispensabili:

- **ubicazione dell'archivio chiavi**: `/etc/keystore.bcfks`
- **formato dell'archivio chiavi** bcfks (Bouncy Castle FIPS)
- **password predefinita** - changeit

Con KeyStore Explorer

1. Aprire `trustcerts.bcfks` utilizzando la password **changeit**.
2. Dalla barra degli strumenti, selezionare **Importa certificato attendibile**.

Con Java Keytool

Dalla directory `sessionserver/etc`:

```
../../java/bin/keytool -importcert -alias <import-cert> -trustcacerts -
file <import-cert.cer> -keystore trustcerts.bcfks –storetype bcfks -
storepass changeit -providername BCFIPS -providerpath ../lib/bc-fips-*.jar
-providerclass org.bouncycastle.jcajce.provider.BouncyCastleFipsProvider
```

Utilizzo di Docker

Docker è una piattaforma open source provvista di una documentazione esauriente da leggere con attenzione.

- Perché Docker?
- Quali sono i vantaggi?
- Terminologia
- Introduzione a Docker e a Host Access for the Cloud
- Esempi

Perché Docker?

Docker è una piattaforma basata su container che consente di sviluppare, distribuire ed eseguire applicazioni all'interno di un container. L'applicazione e tutte le dipendenze che richiede, ad esempio file binari, librerie e informazioni di configurazione, risiedono all'interno del container. È possibile distribuire più container, che vengono tutti eseguiti in Docker e nel sistema operativo.

Utilizzando Docker è possibile ridimensionare le applicazioni in verticale, vale a dire che in un server possono esistere più istanze del server di sessione e che ognuna di essere fornirà esattamente le stesse prestazioni di quando è stata creata e testata.

Quali sono i vantaggi?

L'utilizzo dei container offre diversi vantaggi:

- **Prestazioni**

  Le macchine virtuali rappresentano un'alternativa ai container tuttavia, a differenza di esse, i container non includono un sistema operativo. Questo significa che i container sono più veloci da creare e avviare e hanno un footprint molto inferiore.

- **Flessibilità**

  Poiché i container sono più portabili e forniscono prestazioni superiori, è possibile sfruttare procedure di sviluppo più flessibili e reattive.

- **Isolamento**

  I container di Docker sono indipendenti l'uno dall'altro. Questo aspetto è importante perché un container di Docker che include un'applicazione, comprese le necessarie versioni di eventuale software di supporto, non interferisce con un altro container della stessa applicazione che richiede l'uso di software di supporto differente. È possibile avere la totale certezza che in ogni fase di sviluppo e distribuzione l'immagine creata sarà in grado di fornire esattamente le prestazioni previste.

- **Scalabilità**

  Creare nuovi container è un'operazione rapida e semplice. Nella documentazione di Docker sono disponibili informazioni su come gestire più container.

Terminologia

Esistono termini di base con cui è necessario avere familiarità quando si utilizza Docker. Per ulteriori informazioni, vedere il sito della documentazione di Docker.

Container

Un'istanza runtime di un'immagine. Un container è in genere completamente isolato dall'ambiente host ed è grado di accedere alle porte e i file dell'host solo se è stato configurato per eseguire questa operazione. Per eseguire un'immagine in un container viene utilizzato il comando Run di Docker.

Hub di Docker

Una risorsa per la comunità basata sul cloud per l'utilizzo di Docker. L'hub di Docker viene generalmente utilizzato per l'hosting delle immagini, ma può essere utilizzato anche per l'autenticazione dell'utente e l'automatizzazione delle operazioni di creazione delle immagini. Qualsiasi utente può pubblicare le immagini nell'hub di Docker.

Docker Compose

Compose è uno strumento che utilizza file YAML per configurare i servizi dell'applicazione e quindi per definire ed eseguire applicazioni Docker con più container. Per ulteriori informazioni, visitare la pagina della documentazione di Docker Compose.

Dockerfile

Un documento di testo che contiene i comandi necessari per creare un'immagine Docker. È possibile specificare comandi complessi (ad esempio un'immagine esistente da utilizzare come base) o semplici (come la copia dei file da una directory a un'altra). Per creare un'immagine da un Dockerfile, è necessario utilizzare il comando Build di Docker.

Immagine

Un pacchetto eseguibile autonomo che viene eseguito in un container. Un'immagine Docker è un file binario che include tutto il necessario per eseguire un singolo container di Docker, inclusi i relativi metadati. È possibile creare immagini personali, mediante un Dockerfile, oppure utilizzare le immagini generate da altri utenti che sono state rese disponibili in un registro (ad esempio l'hub di Docker). Per creare un'immagine da un Dockerfile, è necessario utilizzare il comando Build di Docker. Per eseguire un'immagine in un container, è necessario utilizzare il comando Run di Docker.

Introduzione a Docker e a Host Access for the Cloud

Durante l'installazione di HACloud, se si sceglie di utilizzare Docker, il pacchetto di installazione contiene un Dockerfile iniziale e il relativo file jar dell'applicazione per iniziare a utilizzare il server di sessione nei container. Questi file sono disponibili prima dell'installazione.

Alcuni esempi sono disponibili nella cartella `docker/samples`. Per ulteriori istruzioni, vedere Esempi.

La creazione di un'immagine di base richiede il completamento di quattro passaggi:

1. Installare Docker. Seguire le istruzioni disponibili sul sito Web.
   - Installare Docker
2. Estrarre il file del pacchetto di download e individuare `Dockerfile`, `entrypoint.sh` e `sessionserver.jar` nella cartella `Docker`.
3. Creazione dell'immagine Docker
4. Esecuzione dell'immagine Docker

Creazione dell'immagine Docker del server di sessione

Supponendo di aver seguito il primo e il secondo passaggio; installato Docker ed estratto e localizzato Dockerfile e sessionserver.jar, il passaggio successivo è quello di creare l'immagine Docker di base del server di sessione.

1. Eseguire questo comando dalla cartella contenente il Dockerfile:

   ```
   docker build -t hacloud/sessionserver:<versione> .
   ```

   Sostituire <versione> con la versione del server di sessione. Se una versione non è disponibile, il tag predefinito (-t) è `latest`.
2. Verificare che l'immagine sia stata creata correttamente. Eseguire:

   ```
   docker images
   ```

   L'output deve contenere le informazioni sull'immagine appena generata.

Esecuzione dell'immagine

Prima di poter eseguire l'immagine del server di sessione in un container di Docker, è necessario completare i seguenti passaggi:

- Specificare l''indirizzo del server MSS
- Specificare la password di registro dei servizi

- Indicare a MSS l'attendibilità del certificato di identità del server di sessione
- Specificare l'archivio chiavi contenente il certificato di identità del server di sessione
- Fornire l'archivio attendibilità contenente il certificato MSS
- Mappare l'archivio chiavi e archivio attendibilità a quelli del container
- Specificare il nome e la porta dell'host di Docker

Specificare l''indirizzo del server MSS

Per specificare l'ubicazione del server MSS, passare in una variabile di ambiente al server di sessione mediante il Docker. Ad esempio, `--env MSS_SERVER=mss.server.com`

Specificare la password di registro dei servizi

Per specificare la password di registro dei servizi, passare in una variabile di ambiente al server di sessione mediante il Docker. Ad esempio, `--env SERVICE_REGISTRY_PASSWORD=<immettere password>`.

È possibile recuperare la password dalla proprietà `service.registry.password` situata in `./mss/server/conf/container.properties` sul server MSS. Utilizzare la proprietà `service.registry.password` per intero.

Indicare a MSS l'attendibilità del certificato di identità del server di sessione

È possibile eseguire questa operazione utilizzando Administrative Console > Configurare impostazioni > Certificati attendibili. Per aggiungere un certificato del server all'archivio attendibilità MSS, vedere la documentazione relativa ad Administrative Console di MSS. Il certificato del server di sessione è disponibile nella directory `sessionserver/etc/`.

Specificare l'archivio chiavi contenente il certificato di identità del server di sessione

Il server di sessione si identifica utilizzando un certificato. Il certificato dovrebbe essere presente nell'archivio chiavi Java `/sessionserver/etc/keystore.bcfks` situato nel container.

Fornire l'archivio attendibilità contenente il certificato MSS

Quando il server di sessione effettua le connessioni TLS in uscita, verifica l'attendibilità dei server remoti, ad esempio MSS, mediante certificati nell'archivio attendibilità. I certificati presenti nell'archivio chiavi Java `/sessionserver/etc/trustcerts.bcfks` situato nel container saranno considerati attendibili.

Mappare l'archivio chiavi e archivio attendibilità a quelli del container

Sono disponibili due opzioni che consentono di fornire tali archivi chiavi nel container:

- Utilizzare un montaggio di volume
- Estensione di un'immagine Docker esistente

Utilizzare un montaggio di volume

Un montaggio di volume consente di inserire un file o una directory presente nel computer host in un container. Al file o alla directory verrà fatto riferimento mediante il relativo percorso completo o relativo presente nel computer host.

Questo volume inserisce i file dell'archivio chiavi e dell'archivio attendibilità presenti sull'host nel container di Docker.

```
docker run --env MSS_SERVER=localhost \
    --env SERVICE_REGISTRY_PASSWORD=<immettere password qui> \
    --volume ~/demo_keystore.bcfks:/sessionserver/etc/keystore.bcfks \
    --volume ~/demo_truststore.bcfks:/sessionserver/etc/trustcerts.bcfks \
    --publish 7443:7443 \
    sessionserver
```

C'è un lato negativo nell'utilizzare un montaggio di volume. Dal momento che gli archivi chiavi devono essere ubicati su ciascun host di Docker in cui è in esecuzione un container, il container di Docker non sarà molto portatile.

Estensione di un'immagine Docker esistente

Con questo metodo viene creato un nuovo Dockerfile per copiare i file necessari nell'immagine Docker. In questo modo è più portatile l'immagine di Docker.

Per prima cosa, è necessario creare un Dockerfile che venga esteso dall'immagine Docker hacloud/sessionserver.

FROM hacloud/sessionserver:<ad esempio hacloud/sessionserver:latest o hacloud/sessionserver:version>

```
COPY <il-proprio-percorso>/keystore.bcfks //sessionserver/etc/
keystore.bcfks
    COPY <il-proprio-percorso>/truststore.bcfks //sessionserver/etc/
trustcerts.bcfks
```

Successivamente, creare l'immagine estesa Docker e assegnarle il nome **demo**.

```
docker build -t demo .
```

Infine, eseguire l'immagine demo.

```
docker run --env MSS_SERVER=localhost \
    --env SERVICE_REGISTRY_PASSWORD=<immettere la password qui> \
    --publish 7443:7443 \
    demo
```

Specificare il nome e la porta dell'host di Docker

Il server di sessione deve trasmettere il nome host di MSS per trovarlo. Dato che Docker genera un nome univoco casuale che non è raggiungibile all'esterno del container, è necessario specificare il nome dell'host di Docker per MSS. È inoltre necessario indicare al server di sessione la porta che si sta pubblicando sull'host di Docker. I client che accedono al server di sessione finiscono per colpire <nome_host_docker>:<porta_pubblicata_docker>.

```
--env HOST_NAME=docker_host_name
   --env SERVER_PORT=docker_published_port
```

Esempi

Gli esempi, disponibili nella cartella `docker/samples`, illustrano quattro scenari in cui è utilizzato Docker Compose. Compose è uno strumento che utilizza un file YAML per configurare ed eseguire le applicazioni con un singolo comando.

Prerequisiti

Per eseguire gli esempi:

- Installare Docker Compose. Consultare la documentazione di Docker su Docker Compose prima di proseguire.
- Un server MSS in esecuzione
- Un file dell'archivio chiavi per proteggere le connessioni TLS al server di sessione la cui attendibilità è quella di MSS.
- Un file dell'archivio attendibilità contenente il certificato del server MSS in uso
- Per la Creazione dell'immagine Docker del server di sessione

Gli esempi includono:

- Esempio di base - Un esempio di base che fornisce file dimostrativi dell'archivio chiavi e dell'archivio attendibilità in cui è possibile importare un certificato del server MSS.
- Esempio ibrido - Un esempio ibrido che presuppone l'esistenza di un'installazione Host Access for the Cloud locale e monta file dell'archivio chiavi e dell'archivio attendibilità esistenti su disco nel container di Docker.
- Esempio di estensione - Un esempio di estensione che illustra come eseguire l'aggiornamento, la modifica e la personalizzazione del client Web.
- Esempio su un sistema di bilanciamento del carico - Un esempio con un sistema di bilanciamento del carico che illustra come bilanciare il carico tra container collegati.

Esempio di base

In questo esempio di base viene illustrato come eseguire l'immagine Docker del server di sessione in Docker Compose. In questo esempio è necessario importare il certificato del server MSS nell'esempio fornito `./certs/demo_truststore.bcfks` utilizzando un elemento come KeyStore Explorer. Il certificato MSS, per default, si trova in `/mss/server/etc/<nome-computer>.cer`. Vedere Protezione delle connessioni.

Prima di eseguire l'esempio, aggiornare i valori MSS_SERVER, HOST_NAME e SERVICE_REGISTRY_PASSWORD in `docker-compose.yml`.

- Per avviare il servizio del server di sessione, utilizzare il comando:

  ```
  docker-compose up
  ```

- Per eseguire il servizio in un daemon (modalità disconnessa):

  ```
  docker-compose up -d
  ```

- Per esaminare i container in esecuzione, utilizzare il comando:

  ```
  docker ps
  ```

Esempio ibrido

In questo esempio è presente un'installazione locale di Host Access for the Cloud, con file dell'archivio chiavi e dell'archivio attendibilità su disco. Questi file verranno montati, ossia copiati, nel container di Docker.

Prima di eseguire l'esempio, aggiornare i valori MSS_SERVER, HOST_NAME, SERVER_PORT e SERVICE_REGISTRY_PASSWORD nel file `.env`.

Per avviare il servizio del server di sessione:

- Copia `.env` e `docker-compose.yml` in `sessionserver/microservices/sessionserver/`.
- Da questa directory, eseguire: `docker-compose up-d`

Esempio di estensione

Utilizzando le estensioni e il proprio codice HTML, CSS o JavaScript, è possibile aggiornare, modificare e personalizzare l'aspetto del client Web all'interno del browser. Per ulteriori informazioni, vedere Estensione del client Web.

In questo esempio SPRING_PROFILES_ACTIVE viene impostato su **extensions-enabled** e l'ubicazione delle estensioni viene mappata in `docker-compose.yml`.

Prima di eseguire l'esempio, aggiornare i valori MSS_SERVER, HOST_NAME e SERVICE_REGISTRY_PASSWORD nel file `.env`.

Per avviare il servizio del server di sessione, utilizzare il comando:

```
docker-compose up -d
```

È possibile anche scegliere di estendere l'immagine base Docker `hacloud/sessionserver` e copiare i file di estensione nel container Docker:

1. Creare il Dockerfile che si estende dall'immagine di Docker hacloud/sessionserver.

   ```
   FROM hacloud/sessionserver

       COPY ./certs/keystore.bcfks //sessionserver/etc/keystore.bcfks
       COPY ./certs/trustcerts.bcfks //sessionserver/etc/trustcerts.bcfks
       COPY ./extensions /sessionserver/extensions/
   ```

2. Creare l'immagine estesa Docker e assegnare il nome **extensions**.

   ```
   docker build -t extensions
   ```

3. Aggiornare `docker compose.yml` affinché utilizzi la nuova immagine extensions

```
version: '3'
    services:
    sessionserver:
      image: extensions
      environment:
        - LOGGING_FILE=./logs/sessionserver.log
        - LOGGING_FILE_MAXSIZE=10MB
        - LOGGING_FILE_MAXHISTORY=10
        - MSS_SERVER=${MSS_SERVER}
        - SERVICE_REGISTRY_PASSWORD=${SERVICE_REGISTRY_PASSWORD}
        - SPRING_PROFILES_ACTIVE=extensions-enabled
      ports:
        - ${SERVER_PORT}:7443
```

Esempio su un sistema di bilanciamento del carico

HAProxy è un sistema di bilanciamento del carico. Ulteriori informazioni su HAProxy sono disponibili sul relativo sito Web.

In questo esempio, un servizio **haproxy** è incluso nel file `docker-compose.yml`. L'esempio utilizza un'immagine haproxy per bilanciare i container collegati. In questo esempio, per collegare i container, viene utilizzato il bridging SSL

Per garantire una comunicazione sicura tra il client e il sistema di bilanciamento del carico, è necessario aggiornare la proprietà LOAD_BALANCER_CERT nel file `.env` con l'ubicazione del certificato del sistema di bilanciamento del carico.

Per fare una prova, è possibile generare un certificato firmato da se stessi:

1. Generare una chiave privata univoca (KEY):

   ```
   sudo openssl genrsa -out mydomain.key 2048
   ```

2. Generare una richiesta di firma del certificato (CRS).

   ```
   sudo openssl req -new -key mydomain.key -out mydomain.csr
   ```

3. Creare un certificato firmato da se stessi (CRT):

   ```
   sudo openssl x509 -req -days 365 -in mydomain.csr -signkey mydomain.key
   -out mydomain.crt
   ```

4. Aggiungere KEY e CERT a `loadbalancer.pem`:

   ```
   sudo cat mydomain.key mydomain.crt > ./etc/loadbalancer.pem
   ```

Per avviare il server di sessione e i servizi haproxy, utilizzare il comando:

```
docker-compose up -d
```

-oppure-

```
docker-compose up --scale sessionserver=n -d
```

In cui *n* è il numero delle istanze del server di sessione.

È possibile modificare il numero di istanze del server di sessione dopo l'avvio dei servizi:

```
docker-compose scale sessionserver=n
```

Per accedere alla pagina delle statistiche del server di sessione e HAProxy:

- `https://server:7443`
- `http://server:1936/haproxy?stats`

Utilizzo:

- utente: **amministratore**
- password: **password**

4 Gestione

Se si creano e configurano le sessioni e si verifica che tutto funzioni correttamente e senza errori, gli utenti potranno operare senza problemi. Gli argomenti che seguono contengono informazioni per l'amministrazione e la gestione delle sessioni e delle connessioni all'host.

Connessione all'host

Host Access for the Cloud supporta gli host IBM 3270, 5250 e VT, nonché i tipi di host UTS, T27 e ALC.

Nota: Prima di completare i passaggi seguenti, è necessario aggiungere e avviare una sessione da MSS Administrative Console.

Per connettersi all'host:

1. Nella finestra di dialogo **Crea nuova sessione**, selezionare il tipo di host a cui si desidera eseguire la connessione dall'elenco a discesa.
2. Nel pannello Connessione, identificare il nome dell'host a cui si desidera eseguire la connessione. È possibile utilizzare il nome dell'host completo o il relativo indirizzo IP.
3. Digitare il numero della porta da utilizzare.
4. Completare le informazioni necessarie per la connessione all'host.
5. Salvare le impostazioni di connessione.

Gli utenti finali accedono all'host tramite le sessioni create e configurate. Le sessioni vengono create da un amministratore in MSS Administrative Console. Quando si avvia una sessione da Administrative Console, si apre il pannello Connection in una finestra separata del browser. In questo pannello è possibile configurare le opzioni di connessione. Le opzioni variano in base al tipo di host utilizzato.

Impostazioni comuni per le connessioni

Queste opzioni sono comuni a tutti i tipi di host supportati.

- **Connetti all'avvio**

  Per impostazione predefinita, le sessioni sono configurate per connettersi all'host automaticamente quando si crea o si apre una sessione. È comunque possibile impostare una sessione in modo che non si connetta automaticamente all'host. Scegliere **NO** per connettersi manualmente all'host.

- **Riconnetti quando l'host termina la connessione**

  Se si imposta su Sì, Host Access for the Cloud tenta di riconnettersi non appena termina la connessione all'host.

- **Protocollo**

  Nell'elenco a discesa , selezionare il protocollo da utilizzare per comunicare con l'host. Per stabilire la connessione con un host, il client Web e il computer host devono utilizzare lo stesso protocollo di rete. I valori disponibili dipendono dall'host al quale ci si sta connettendo, ovvero:

  Tabella 4-1 *Descrizioni dei protocolli*

Protocollo	Descrizione
TN3270	TN3270 è una variante del protocollo Telnet, che consiste in una serie di specifiche per comunicazioni generiche tra desktop e sistemi host. Utilizza TCP/IP come trasporto tra i desktop e i mainframe IBM.
TN3270E	TN3270E, o Telnet Extended, è dedicato agli utenti di TCP/IP che si connettono a un mainframe IBM tramite un gateway Telnet che implementa RFC 1647. Il protocollo TN3270E consente di specificare il nome del dispositivo di connessione (definito anche unità logica) e fornisce supporto per il tasto ATTN, il tasto SYSREQ e la gestione delle risposte SNA. Se si tenta di utilizzare Telnet Esteso per connettersi a un gateway che non supporta questo protocollo, verrà utilizzato il protocollo TN3270 standard.
TN5250	TN5250 è una variante del protocollo Telnet, che consiste in una serie di specifiche per comunicazioni generiche tra desktop e sistemi host. Utilizza TCP/IP come trasporto tra i computer desktop e i computer AS/400.
Secure Shell (VT)	Quando sono richieste comunicazioni crittografate protette tra un host VT attendibile e il computer attraverso una rete non protetta è possibile configurare le connessioni SSH. Le connessioni SSH garantiscono l'autenticazione sia dell'utente client che del computer host e la crittografia di tutti i dati Sono disponibili due opzioni di autenticazione: ◆ **Interattiva da tastiera** - Questo metodo di autenticazione consente di implementare vari tipi di meccanismi di autenticazione. Qualsiasi metodo di autenticazione attualmente supportato che richieda solo l'input dell'utente può essere realizzato con l'opzione interattiva da tastiera. ◆ **Password** - Questa opzione prevede la richiesta al client di fornire una password all'host dopo aver stabilito la connessione con l'host. La password viene inviata all'host attraverso il canale crittografato.

Protocollo	Descrizione
Telnet (VT)	Telnet è un protocollo della suite di protocolli aperti TCP/IP. In quanto protocollo di flusso di caratteri, Telnet trasmette tramite la rete l'input dell'utente un carattere alla volta da applicazioni in modalità carattere a un host, che lo elabora e lo ritrasmette alla rete.
INT1 (UTS)	Fornisce l'accesso agli host Unisys 1100/1200 tramite il protocollo di rete TCP/IP.
TCPA (T27)	Utilizzare questo protocollo per connettersi agli host Unisys ClearPath serie NX/LX o A. L'autenticazione TCPA è la procedura di verifica delle informazioni di accesso dell'utente. Se è configurato correttamente, è possibile richiedere una credenziale di sicurezza dal server di credenziali dell'applicazione e restituirla al server. Se la credenziale è valida, l'applicazione verrà connessa e non sarà necessario inserire l'ID utente o la password. Tuttavia, se la credenziale non è valida verrà richiesto di specificare ID utente e password.
MATIP (ALC)	MATIP (Mapping of Airline Traffic Over Internet Protocol) utilizza TCP/IP per le prenotazioni aeree, l'emissione di biglietti e i messaggi.

- **Attiva traccia emulazione**

  È possibile scegliere di generare le tracce dell'host per una sessione. Il valore predefinito è **No**. Selezionare **Sì** per creare una nuova traccia dell'host di emulazione ogni volta che viene avviata la sessione. Il file di traccia viene archiviato in `<directory installazione>/sessionserver/logs/hosttraces/<data(aaaammgg>/<file-di-traccia>`. I file di traccia dell'host vengono creati ogni volta che viene avviata una sessione.

Impostazioni delle connessioni 3270 e 5250

Oltre alle impostazioni di configurazione comuni, i tipi di host 3270 e 5250 richiedono le impostazioni specifiche descritte di seguito.

- **Modello terminale**

  Specificare il modello di terminale, noto anche come stazione di visualizzazione, che si desidera far emulare da Host Access for the Cloud. A seconda del tipo di host, sono disponibili modelli di terminale diversi.

  Se si sceglie **Modello personalizzato**, è possibile impostare il numero di colonne e righe per personalizzare il modello di terminale.

- **Utilizzare l'accesso automatico Kerberos (solo 5250)** MSS se impostato su **Sì**, non è necessario che l'utente immetta le credenziali di accesso. L'accesso automatico Kerberos è configurato nella Administrative Console di MSS > Host Access for the Cloud. Nella configurazione di HACloud per l'utilizzo del protocollo di autenticazione Kerberos, sono presenti termini che è necessario comprendere e prerequisiti da rispettare prima della configurazione di questa opzione. Queste opzioni sono descritte in dettaglio nella documentazione del pannello Administrative Console di MSS > Host Access for the Cloud, disponibile tramite il pulsante Guida.
- **ID terminale** (solo 3270)

Quando Host Access for the Cloud si connette a un host Telnet, il protocollo e l'host Telnet negoziano un ID terminale da utilizzare durante la connessione Telnet iniziale. In generale tale negoziazione si conclude con l'uso dell'ID terminale corretto, quindi questa casella deve essere lasciata vuota.

- **Sicurezza TLS/SSL**

  I protocolli SSL e TLS consentono a un client e a un server di stabilire una connessione crittografata protetta su una rete pubblica. Quando ci si connette mediante SSL/TLS, Host Access for the Cloud autentica il server prima di aprire una sessione e tutti i dati trasferiti e l'host vengono cifrati utilizzando il livello di cifratura selezionato. Sono disponibili le seguenti opzioni:

Tabella 4-2 *Descrizioni di TLS/SSL*

Opzioni di sicurezza	Descrizione
Nessuna	Non è necessaria alcuna connessione sicura.
TLS 1.2 - 1.0	Consente la connessione tramite TLS 1.2, TLS 1.1 o TSL 1.0, a seconda delle funzionalità dell'host o del server a cui ci si sta connettendo. Quando **Verifica identità server** è impostata su Sì, il client confronta il nome del server o dell'host con il nome sul certificato del server.
TLS 1.2	Selezionare questo valore per connettersi tramite TLS. Come parte del protocollo TLS, il client confronta il nome del server o dell'host con il nome sul certificato del server quando **Verifica identità server** è impostata su Sì. Questa operazione è fortemente consigliata.

Nota: Vedere la sezione Protezione delle connessioni per informazioni sull'aggiunta di certificati attendibili, sull'archivio di chiavi e sull'utilizzo di SSH, e per altre informazioni sulla sicurezza avanzata.

- **Verifica identità server**

  Quando Sicurezza TLS/SSL è impostata su TLS 1.2 o TLS 1.2-1.0, è possibile confrontare il nome dell'host con il nome sul certificato del server. Si consiglia di abilitare la verifica del nome host per tutte le sessioni.

- **Nome dispositivo**

  Se come protocollo è stato selezionato TN3270, TN3270E o TN5250, specificare il nome del dispositivo da utilizzare quando la sessione si connette all'host Il nome del dispositivo è noto anche come unità logica dell'host o pool. È anche possibile selezionare le opzioni seguenti:

  - **Genera nome dispositivo univoco**. Verrà generato automaticamente un nome di dispositivo univoco.
  - **Utilizza Terminal ID Manager** che visualizza impostazioni aggiuntive da definire.
  - **Richiedi all'utente**. Quando si seleziona questa opzione, all'utente finale verrà richiesto di specificare l'ID dispositivo ogni volta che tenta di stabilire una connessione.

  Se non viene specificato un nome di dispositivo per la sessione, l'host ne assegna dinamicamente uno. Un nome di dispositivo impostato in una macro sostituirà questa impostazione.

Per utilizzare Terminal ID Manager è necessario che sia configurato un server Terminal ID Manager. Vedere Terminal ID Manager nella guida Management and Security Server Installation Guide.

Se è stata selezionata l'opzione **Terminal ID Manager**, è possibile utilizzarla per fornire l'ID alle applicazioni client durante il runtime. È possibile utilizzare Terminal ID Manager per gestire pool di ID per tipi di host diversi. Un ID consiste in dati di connessione univoci per una sessione host singola.

Se si decide di utilizzare Terminal ID Manager ed è stato configurato il server Terminal ID Manager, selezionare le opzioni seguenti per configurare i criteri per acquisire un ID. Per ottenere un ID è necessario che vengano soddisfatti tutti i criteri.

Nota: Tenere presente che specificando un criterio si sta indicando che l'ID deve essere allocato solo quando viene trovato un ID che ha tale attributo specifico. Affinché l'acquisizione dell'ID venga completata, il set di criteri selezionati qui deve corrispondere esattamente al set di criteri specificati in almeno un pool di ID in Terminal ID Manager.

Tabella 4-3 *Criteri di Terminal ID Manager*

Criterio	Descrizione
Nome pool	Includere questo attributo e immettere il nome di un pool per limitare la ricerca di ID al pool specificato.
Indirizzo IP client	L'indirizzo IP del computer client verrà incluso come parte della richiesta di un ID.
Indirizzo host	L'indirizzo dell'host configurato per questa sessione verrà incluso come parte della richiesta di un ID.
Porta host	La porta per l'host configurato per questa sessione verrà inclusa come parte della richiesta di un ID.
Nome sessione	Quando selezionato, richiede che l'ID sia configurato in modo da essere utilizzato solo da questa sessione.
Tipo di sessione	Il tipo di sessione (ad esempio, IBM 3270, IBM 5250, UTS, ALC o T27) viene sempre incluso come parte della richiesta di un ID.

Criterio	Descrizione
Nome utente	Utilizzare questo criterio per garantire che verranno allocati solo gli ID creati per uso esclusivo da parte di utenti specifici. Il nome dell'utente corrente, che deve essere presente in un ID affinché questo possa essere allocato, è il nome dell'utente al quale viene assegnata la sessione durante il runtime. Per configurare una sessione in base ai nomi degli utenti, è disponibile un nome utente segnaposto predefinito: **tidm-setup**. Per la configurazione delle sessioni con **tidm-setup** da parte dell'amministratore, è necessario che in Terminal ID Manager sia stato effettuato il provisioning di ID per tidm-setup. È possibile sostituire il nome predefinito con un nome personalizzato modificando il file `<directory-installazione>/sessionserver/conf/container.properties` nel modo seguente: `id.manager.user.name=nomeutente-personalizzato` Dove nomeutente-personalizzato è da sostituire con il nome che si vuole utilizzare.
Nome applicazione (UTS)	Il nome dell'applicazione host verrà utilizzato come parte della richiesta di un ID.

Per determinare il comportamento del tentativo di connessione se Terminal ID Manager non alloca un ID a questa sessione, utilizzare **Se l'ID non è allocato**:

- **Tentativo di connessione non riuscito** -Se selezionata, la sessione non tenterà di connettersi quando non viene allocato un ID.
- **Consenti tentativo di connessione** -Se selezionata, la sessione tenterà di connettersi quando non viene allocato un ID. Il tentativo può essere rifiutato dall'host. Alcuni tipi di host consentono a un utente di connettersi senza un ID.

Per verificare che Terminal ID Manager sia in grado di fornire un ID utilizzando le selezioni di criterio e valore effettuate, fare clic su Prova.

- **Invia pacchetti keep alive** - Utilizzare questa impostazione per avere un controllo costante della sessione e dell'host in modo che i problemi di connessione vengano evidenziati immediatamente. Scegliere uno dei tipi seguenti di pacchetti keep alive:

Opzione	Azione eseguita
Nessuno	Impostazione predefinita. Non vengono inviati pacchetti.
Sistema	Lo stack TCP/IP tiene traccia della connessione all'host e invia raramente pacchetti keep alive. Questo opzione utilizza risorse di sistema ridotte rispetto a Invia pacchetti NOP o Invia pacchetti di timing mark.
Invia pacchetti NOP	Viene inviato periodicamente un comando No Operation (NOP) all'host. Non è richiesto all'host di rispondere a questi comandi, ma lo stack TCP/IP può rilevare se si è verificato un problema nella consegna del pacchetto.
Invia pacchetti di timing mark	Viene inviato periodicamente un comando Timing Mark all'host per determinare se la connessione è ancora attiva. L'host deve rispondere a questi comandi. Se non viene ricevuta alcuna risposta o viene rilevato un errore nell'invio del pacchetto, la connessione viene chiusa.

Timeout keep alive (secondi) - Se si sceglie di utilizzare l'opzione Invia pacchetti NOP o Invia pacchetti di timing mark, selezionare l'intervallo fra le richieste keep alive impostate. L'intervallo è da 1 a 36000 secondi (1 ora); l'impostazione predefinita è 600 secondi.

Come testare i criteri di Terminal ID Manager

Terminal ID Manager fornisce gli ID alle applicazioni client durante il runtime. Per verificare che Terminal ID Manager può fornire un ID utilizzando le selezioni di criterio e valore effettuate, utilizzare questa opzione di test.

I criteri per la sessione corrente vengono specificati nel pannello Connessione dopo aver selezionato **Utilizza Terminal ID Manager** in Nome dispositivo (tipi di host 3270, 5250), nel campo Terminal ID (UTS) o nel campo ID stazione (T27). Per impostazione predefinita, vengono visualizzati i criteri selezionati per la sessione corrente.

Fare clic su **Prova** per verificare che Terminal ID Manager fornisca un ID corrispondente alle selezioni di criteri e valori configurate. La prova restituisce il nome di un ID disponibile che soddisfa i valori degli attributi selezionati.

Testing for other criteria and values

È possibile utilizzare questo pannello per provare criteri diversi da quelli associati alla sessione corrente.

1. Selezionare un tipo di sessione nell'elenco Tipo sessione e selezionare i criteri da testare. È possibile provare valori alternativi che si desidera utilizzare in una richiesta Terminal ID Manager campione.
2. Fare clic su **Prova** per verificare che Terminal ID Manager fornisca un ID corrispondente alle selezioni di criterio e valore. La prova restituisce il nome di un ID disponibile che soddisfa i valori selezionati.

Impostazioni per le connessioni VT

Oltre alle Impostazioni comuni per le connessioni, gli host VT richiedono impostazioni aggiuntive. Queste impostazioni variano a seconda del protocollo in uso, Telnet o SSH. Salvo diversa indicazione, le impostazioni sono valide per entrambi i protocolli.

Tabella 4-4 *Opzioni di configurazione delle sessioni VT*

Impostazioni VT	Descrizione
ID terminale	Questa impostazione determina la risposta che Host Access for the Cloud invierà all'host in seguito ad una richiesta primaria di identificazione degli attributi del dispositivo (DA). La risposta all'host contiene le informazioni sulle funzioni che il terminale può eseguire. La risposta di Host Access for the Cloud per ogni ID terminale è identica alla risposta del terminale VT, tuttavia alcune applicazioni possono richiedere una risposta DA specifica. Questa impostazione di ID terminale è indipendente dall'impostazione Tipo di terminale. Le opzioni sono: VT220, VT420, VT100, DEC-VT100 e VT52.
Consenti host sconosciuti (SSH)	Questa impostazione consente all'amministratore di decidere se il client Web consentirà l'uso di host sconosciuti. Le opzioni sono: ◆ **Sì**: sono consentiti host sconosciuti e tutte le connessioni SSH. Agli utenti del client Web non viene richiesto se gli host sono considerati attendibili. ◆ **Chiedi**: all'utente del client Web viene chiesto se l'host è attendibile quando eseguono la connessione a un host sconosciuto che non hanno mai visto prima. Se si sceglie di considerare attendibile l'host, la chiave pubblica verrà memorizzata nelle preferenze dell'utente e le connessioni successive non richiederanno un prompt a meno che non venga modificata la chiave dell'host. ◆ **No**: non sono consentiti host sconosciuti. Sono consentiti solo gli host a cui l'amministratore sceglie di concedere l'attendibilità durante la configurazione della sessione. Agli utenti finali non viene mai richiesto nulla e la sessione esegue o non esegue la connessione in base alle scelte dell'amministratore.
Sopprimi messaggi banner (SSH)	Quando è abilitata, l'intestazione SSH non viene visualizzata. Questa opzione è utile per la registrazione di macro di login SSH.
Eco locale (Telnet)	Automatico (impostazione predefinita). Host Access for the Cloud risponde all'eco remoto proveniente da un host Telnet: con l'impostazione Automatico Host Access for the Cloud tenta di negoziare un eco remoto ma esegue i comandi indicati dall'host. Con l'impostazione Sì Host Access for the Cloud negozia l'eco locale con l'host, ma attiva sempre l'eco, con No negozia l'eco remoto con l'host, ma non attiva l'eco.
Rinegozia eco (Telnet)	No (impostazione predefinita). Quando è impostata su Sì, le password non vengono visualizzate sullo schermo locale, ma tutto l'altro testo digitato è visibile. Host Access for the Cloud supporta l'opzione Suppress Local Echo (Sopprimi eco locale) di Telnet quando è connesso a un host in modalità half-duplex. Questo significa che Host Access for the Cloud sopprime l'eco dei caratteri al computer host e, se supporta la funzione Suppress Local Echo (Sopprimi eco locale), può ricevere l'istruzione di sopprimere l'eco a livello locale.

Impostazioni VT	Descrizione
Imposta dimensioni finestra host	Sì (impostazione predefinita). Questa impostazione invia il numero di righe e colonne all'host Telnet tutte le volte che cambiano. In questo modo l'host Telnet può controllare in modo adeguato il cursore quando vengono modificate le dimensioni della finestra.
Richiedi binario (Telnet)	No (impostazione predefinita). Telnet definisce un percorso dati a 7 bit tra l'host e il terminale. Questo tipo di percorso dati non è compatibile con alcuni set di caratteri nazionali. Fortunatamente, molti host consentono dati a 8 bit senza la necessità dello zero per l'ottavo bit evitando così il problema. In alcuni casi, tuttavia, può essere necessario forzare l'host a usare un percorso dati a 8 bit selezionando questa casella di controllo.
Invia LF dopo CR (Telnet)	No (impostazione predefinita). Un "vero" host Telnet si aspetta una sequenza di caratteri CrNu (ritorno a capo/null) come indicatore della fine di una riga inviata da un terminale. Tuttavia, in Internet sono presenti host che non sono veri e propri host Telnet, e questi si aspettano un carattere Lf (Avanzamento riga) dopo Cr al termine di una riga. Se si sta effettuando una connessione a questa tipologia di host Telnet, selezionare Sì.
Ctrl-Interr invia (Telnet)	Consente di scegliere la sequenza inviata all'host quando si preme Ctrl-Interr invia. Le opzioni sono: sequenza Interruzione Telnet (impostazione predefinita), Interrompi processo o Nessuna.
Set di caratteri host	Il valore predefinito per Set di caratteri host dipende dal tipo di terminale che si sta emulando. Questa impostazione riflette lo stato corrente di Set di caratteri host del terminale VT, che può essere modificato dall'host. L'impostazione predefinita associata salvata con il modello è DEC Supplemental.
Identificazione automatica	No (impostazione predefinita). Questa impostazione specifica se il messaggio di identificazione, impostato con la proprietà Answerback, viene inviato automaticamente all'host dopo la connessione della linea di comunicazione.
Stringa di identificazione	Questa impostazione consente di immettere un messaggio di identificazione se l'host si aspetta una risposta all'invio di un carattere ENQ. La stringa di identificazione supporta caratteri con codice minore o uguale a 0xFFFF tramite sequenze di escape Unicode. La sequenza di escape inizia con \u seguito esattamente da quattro cifre esadecimali. È possibile incorporare le sequenze di escape Unicode in qualsiasi stringa. Ad esempio, questa sequenza \u0045 incorporata verrà interpretata come E, poiché 45 è il codice esadecimale per il carattere E. Per passare le sequenze di escape Unicode all'host, aggiungere una barra iniziale alla sequenza di escape. Ad esempio per inviare il valore letterale stringa \u001C all'host, mappare un tasto a \\u001C. Host Access for the Cloud converte il valore nella stringa \u001C quando viene premuto il tasto e invia all'host i 6 caratteri della stringa risultante.

Impostazioni per le connessioni UTS

Oltre alle impostazioni di configurazione comuni, gli host UTS richiedono le impostazioni aggiuntive seguenti:

Tabella 4-5 *Opzioni di configurazione delle sessioni UTS INT1*

Opzioni di UTS INT1	Descrizione
Applicazione	Il nome dell'applicazione host o della modalità operativa dell'host a cui accedere. Si tratta della parola o della frase che il computer locale invia all'host quando si stabilisce la comunicazione iniziale con l'host. Se si utilizza un terminale host, si tratta del nome $$OPEN dell'applicazione. Solitamente il nome dell'applicazione è lo stesso dell'ambiente. Tuttavia è possibile che siano diversi. Ad esempio, il nome dell'ambiente potrebbe essere MAPPER, mentre il nome dell'applicazione potrebbe essere UDSSRC. In questo caso durante la sessione di emulazione del terminale, l'utente digita $$OPEN MAPPER al prompt e, quando la connessione è stabilita, INT1 invia UDSSRC all'host.
TSAP	Il TSAP (Transport Service Access Point) desiderato, fino a 32 caratteri (ad esempio TIPCSU per le connessioni TIP, RSDCSU per le connessioni Demand). TSAP è richiesto solo se ci si connette a un HLC (Host LAN Controller) o a un DCP (Distributed Communications Processor) in modalità router IP. Se non si è certi del valore da utilizzare, contattare l'amministratore dell'host.
Transazione iniziale	Il carattere, la parola o la frase che il computer locale invia all'host quando viene stabilita la comunicazione (fino a 15 caratteri). Questo parametro è facoltativo e viene utilizzato principalmente con TIP. Ad esempio, è possibile digitare ^ per eseguire MAPPER. È possibile utilizzare questo parametro anche per trasmettere password.
Avvia transazione	Quando si configura una transazione iniziale, per impostazione predefinita i dati vengono inviati non appena viene stabilita la connessione. È possibile decidere quando inviare una transazione iniziale utilizzando una stringa particolare per attivarla. Ad esempio, per attendere che venga effettuato l'accesso prima di inviare i dati della transazione iniziale, digitare una stringa da utilizzare per identificare un accesso riuscito. È possibile utilizzare questa impostazione in combinazione con **Invia transazione iniziale**.
Invia transazione iniziale	È possibile determinare quando inviare la transazione iniziale: ◆ **Immediatamente** - Impostazione predefinita. ◆ **Quando viene ricevuto l'inizio del carattere di immissione** - Utile quando devono essere completate le transazioni multiriga prima di inviare la stringa. ◆ **Dopo i millisecondi specificati**
ID terminale	Scegliere se specificare un ID terminale o utilizzare Terminal ID Manager. Per specificare un ID terminale, digitarlo nel campo **Specifica ID terminale**. Se si sceglie **Utilizza Terminal ID Manager**, verrà richiesto di selezionare gli attributi di ID terminale da utilizzare per ottenere un ID. Vedere Attributi di Terminal ID Manager. Per provare gli attributi, fare clic su **Prova**.

Opzioni di UTS INT1	Descrizione
Specifica ID terminale	L'ID terminale, un identificatore di terminale (solitamente composto da un massimo di 8 caratteri alfanumerici) da utilizzare per le sessioni di comunicazione associate al percorso specifico. Ogni ID terminale, noto anche come TID o PID, deve essere univoco per l'host.

Impostazioni per le connessioni T27

Oltre alle impostazioni di configurazione comuni, è possibile configurare le seguenti opzioni di connessione T27 aggiuntive:

Tabella 4-6 *Impostazioni per le connessioni T27*

Opzioni T27	Descrizione
Tipo di terminale	Consente di selezionare il tipo di terminale da emulare durante la sessione. L'emulazione T27 supporta i tipi di terminale Unisys TD830, TD830 ASCII, TD830 INTL e TD830 NDL.
Richiedi binario	Quando si richiede la stampa pass-through è necessario attivare l'opzione Richiedi binario. Il valore di default è No. TCPA definisce un percorso dati a 7 bit tra l'host e il terminale. Questo tipo di percorso dati non è compatibile con alcuni set di caratteri nazionali. Molti host comunque consentono dati a 8 bit senza la necessità dello zero per l'ottavo bit, evitando così il problema. Tuttavia, in alcuni casi, può essere necessario forzare l'host a usare un percorso dati a 8 bit ed è quindi possibile selezionare questa opzione.
Larghezza riga	Selezionare il numero di caratteri che l'host invierà al client. L'impostazione predefinita è 80 caratteri.
Sicurezza TLS/SSL	Vedere Tabella 4-2 Descrizioni di TLS/SSL per una descrizione delle varie opzioni.
ID stazione	Scegliere se specificare un ID stazione o utilizzare Terminal ID Manager. Per specificare un ID stazione, scegliere **Specifica l'ID della stazione** e digitare il nome nel campo ID stazione. Ogni ID stazione deve essere univoco per l'host e solitamente è composto da un massimo di 8 caratteri alfanumerici. Se non viene specificato un ID stazione per la sessione, l'host ne assegna dinamicamente uno. Se si seleziona Terminal ID Manager, verranno visualizzati vari criteri di ID terminale da configurare. Vedere Criteri di Terminal ID Manager per una descrizione delle varie opzioni.

Impostazioni per le connessioni ALC

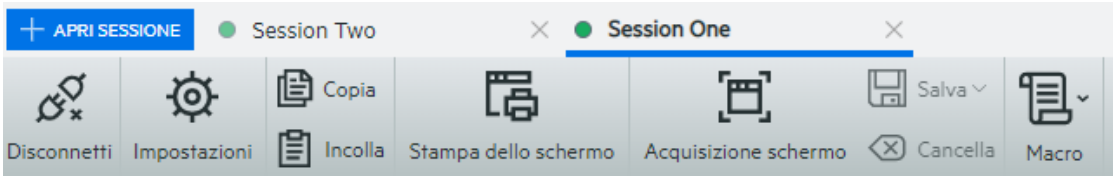
Oltre alle impostazioni di configurazione comuni, gli host ALC richiedono le impostazioni aggiuntive seguenti:

Tabella 4-7 *Impostazioni per le connessioni ALC*

Opzioni di ALC	Descrizione
Sicurezza TLS/SSL	Vedere Tabella 4-2 Descrizioni di TLS/SSL per una descrizione delle varie opzioni.
Codifica caratteri	Scegliere ASCII, EBCDIC o IPARS (predefinito) come set di codifica.
File di configurazione	Immettere il file di configurazione (CNF) che associa le informazioni appropriate per un tipo di host specifico.
Indirizzo del terminale	Scegliere se specificare l'indirizzo del terminale o utilizzare Terminal ID Manager. ◆ Indirizzo del terminale - Specificare se utilizzare la modalità di indirizzamento a 2 byte o a 4 byte. Sebbene sia richiesto un indirizzo a 5 byte univoco quando si specifica l'ID terminale invece di utilizzare Terminal ID Manager, questa opzione specifica quanti byte dell'indirizzo dell'ID terminale vengono inviati con ciascun messaggio per il multiplexing. Se si specifica la modalità di indirizzamento a 2 byte, vengono inviati solo gli ultimi 2 byte (A1, A2) dell'indirizzo del cluster ASCU (Agent Set Control Unit). Se si specifica la modalità di indirizzamento a 4 byte, viene inviato l'indirizzo completo del cluster ASCU (H1, H2, A1, A2). Specificare l'indirizzo univoco a 5 byte del terminale per questa sessione. L'indirizzo del terminale è composto da cinque valori esadecimali a 2 cifre nell'ordine seguente: H1, H2, A1, A2 e TA (indirizzo terminale). Solitamente questo indirizzo univoco viene assegnato dall'amministratore di rete. ◆ **Terminal ID Manager** - Fornisce gli ID alle applicazioni client durante il runtime. Se si sceglie questa opzione è necessario completare ulteriori opzioni di configurazione. Vedere Criteri di Terminal ID Manager per la descrizione di tali opzioni.

Fornire accesso alle sessioni

Gli utenti accedono alle loro sessioni assegnate tramite un URL fornito dall'amministratore (ad esempio, `https://<server di sessione>:7443/`). Da questo URL gli utenti selezionano la sessione da aprire dall'elenco di sessioni disponibili configurate dall'amministratore.

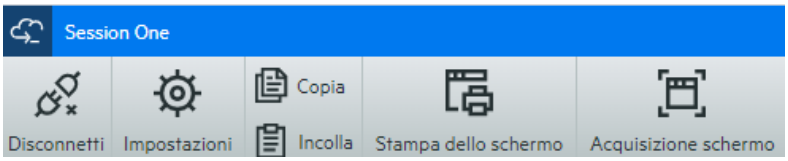


Gli utenti possono passare da una sessione all'altra, aprire sessioni aggiuntive e chiudere le sessioni che non utilizzano più.

Modalità singola sessione

In alternativa, è possibile utilizzare la **modalità a sessione singola** e fornire URL a particolari sessioni che vengono lanciate usando il parametro del nome (ad esempio un collegamento diretto sulla pagina di un portale aziendale). Per abilitare l'avvio di una sessione singola, utilizzare il parametro di query `singleSession`. È possibile utilizzare questo parametro da solo per avviare solamente il client Web in modalità sessione singola, ad esempio `http://<server di sessione>:7443//?singleSession`, oppure è possibile utilizzarlo insieme a un parametro di sessione denominato per avviare una sessione denominata specifica in modalità sessione singola: `http://<server di sessione>:7443//?singleSession&name=HumanResources`. L'ordine dei parametri non ha importanza.

Quando gli utenti finali accedono a una sessione singola, non possono passare da una sessione aperta a un'altra, e non possono aprire nuove sessioni. Non verrà avviata una nuova sessione se la sessione specificata esiste già quando l'utente apre il collegamento.



Se si desidera che tutte le sessioni del server di sessione vengano eseguite in modalità sessione singola:

- Aprire `<directory-installazione>/sessionserver/conf/container.properties`
- Aggiungere `webclient.singlesession=true` al file.

Registrazione

Individuazione dei file di log

Sono disponibili due file di log:

- `<directory-installazione>/sessionserver/sessionserver/sessionserver.log`: il file di log per l'applicazione del server di sessione.
- `<directory_installazione>/sessionserver/container.log`: il file di log del container che ospita l'applicazione Host Access for the Cloud.

Configurazione della rotazione dei log

È possibile configurare la rotazione dei log modificando questi valori in `<directory-installazione>\microservices\microservices\sessionserver\sessionserver\service.yml`:

```
logging.file.max-size
   logging.file.max-history
```

Impostazione dei livelli di log

Sono disponibili diversi tipi di livelli di registrazione che si possono utilizzare per produrre tipi diversi di informazioni. È possibile configurare i livelli di registrazione in `<directory-installazione>\sessionserver\microservices\sessionserver\service.yml`.

Nota: Le righe in `service.yml` devono essere indentate utilizzando spazi.

Per impostare i livelli di log, utilizzare il formato seguente:

```
- name: logging.level.<logger>
   value: "<livello log>"
```

Dove `<logger>` è il nome del logger da regolare e `<livello log>` è uno dei seguenti:

- Trace - indica eventi informativi con granularità più fine di Debug.
- Debug - indica eventi informativi con granularità fine, utili in particolare per eseguire il debug di applicazioni.
- Info - indica messaggi informativi che evidenziano l'avanzamento dell'applicazione con granularità più grossolana.
- Warn - indica situazioni potenzialmente pericolose.
- Error - indica eventi di errore che possono comunque consentire di continuare l'esecuzione dell'applicazione.
- Fatal - indica errori gravi che presumibilmente causeranno l'interruzione dell'applicazione.

Nota: È necessario riavviare il server di sessione dopo le modifiche apportate `service.yml`.

Client Web per la registrazione del server di sessione

Sebbene il browser fornisca un meccanismo di base per registrarsi nella console JavaScript, il client Web viene esteso e, con una certa configurazione, è possibile registrare gli eventi sul server di sessione per la visualizzazione da parte di un amministratore.

Per default, non viene registrato nulla sul server di sessione. Per abilitare questa funzione, è necessario impostare il livello di log seguendo le istruzioni riportate di seguito.

I livelli di log disponibili sono: debug, info, warn, error o off. Il livello di log predefinito è off.

Regolazione del livello di registrazione per tutti gli utenti del client Web

Per modificare il livello di registrazione per tutti i client Web, aggiungere la seguente voce a `<directory-installazione>\sessionserver\microservices\sessionserver\service.yml`

```
- name: <logger>
  value: "<livello di log>"
```

In cui `<logger>` è il seguente:

`logging.level.com.microfocus.zfe.webclient.core.handler.ClientLoggingHandler-webclient`

Nota: Prestare attenzione quando si aumenta il livello di registrazione per tutti gli utenti del client Web in un ambiente di produzione a causa di un potenziale aumento del traffico di rete.

Regolazione del livello di registrazione per un singolo utente

Per modificare il livello di registrazione per i singoli utenti sono disponibili due opzioni:

Per modificare temporaneamente il livello di registrazione per un'istanza del client Web di un utente specifico senza richiedere il riavvio di un server di sessione, indicare all'utente di aggiungere il seguente parametro URL durante il caricamento del client Web nel browser:

`https://mysessionserver.com:7443/`**`?log=<livello di log>`**

Per modificare il livello di registrazione di un singolo utente senza che sia necessario apportare modifiche, aggiungere la seguente voce a `service.yml`:

```
- name: <logger>
  value: "<livello di log>"
```

In cui `<logger>` è il seguente:

`logging.level.com.microfocus.zfe.webclient.core.handler.ClientLoggingHandler-webclient-<nome utente>`

In cui `<nome utente>` è il nome della persona di cui si stanno regolando i livelli di registrazione.

Nota: La registrazione in base a un nome utente richiede una modalità di autenticazione che coinvolga i nomi utente.

---

5 Utilizzo di HACloud

Sono disponibili diverse opzioni di sessione e visualizzazione che permettono di personalizzare la sessione e consentire operazioni efficienti.

- Impostazioni di visualizzazione
- Mappatura dei tasti
- Configurare le macro utente
- Trasferire file
- Specificare le operazioni di copia e incolla
- Operazioni con le sessioni
- Creazione di macro
- Stampa
- Personalizzare le sessioni
- Impostare le preferenze utente

Impostazioni di visualizzazione

Le impostazioni di visualizzazione variano in base al tipo di host e sono specifiche della sessione che si sta configurando.

- Mappatura dei colori
- Configurazione delle aree sensibili
- Configurare le dimensioni dello schermo per host VT, UTS e T27
- Impostare le opzioni del cursore
- Impostare le opzioni dei font
- Impostare le opzioni del buffer di scorrimento indietro di VT
- Impostare le opzioni della tastiera
- Impostazioni del terminale
- Impostare altre opzioni di visualizzazione

Mappatura dei colori

È possibile personalizzare il colore dello schermo e l'aspetto dei diversi attributi dell'host nella finestra del terminale. Per ogni elemento, è possibile selezionare il colore per il primo piano e per lo sfondo di tutte le connessioni host supportate. I colori vengono specificati utilizzando la griglia dei colori o inserendo il formato di codice HEX.

Esistono numerosi siti Web che elencano i colori HEX disponibili, ad esempio w3schools.com HTML Color Picker

Potrebbero essere visualizzate opzioni diverse a seconda del tipo di connessione host.

Opzioni specifiche degli host UTS:

- **Utilizza informazioni di colore dell'host** - Per utilizzare i colori specificati, anziché i colori specificati dall'host, deselezionare questa opzione.
- **Attiva intermittenza** - Per disattivare l'intermittenza, deselezionare questa opzione.
- **Seleziona attributo da modificare** - Nell'emulazione UTS, i colori sono impostati direttamente dall'host. È possibile specificare i colori per il testo associati alle opzioni di visualizzazione dello schermo specifico, incluse le seguenti combinazioni disponibili:

  Normale, Sottolineato (UND), Barrato (STK), Separatore colonna sinistra (LCS), Pagina di controllo e Riga di stato (OIA).
- **Intensità video** - Le intensità del video, Intermittente, Dim, Protetto e Invertito, vengono combinate con gli attributi per creare combinazioni aggiuntive. Ad esempio, è possibile mappare i colori per il primo piano o per lo sfondo a tutte le celle con Dim + Intermittente + Sottolineato oppure Invertito + Protetto + Barrato + Sottolineato.

  Quando si seleziona un'intensità del video (o una combinazione di intensità), queste vengono combinate con il valore dell'elenco a discesa dell'attributo per formare una singola mappatura di colore .

Opzioni specifiche degli host VT e T27:

- **Attiva intermittenza** - Per disattivare l'intermittenza, deselezionare questa opzione.
- **Attiva grassetto** - Visualizza il testo impostato con l'attributo grassetto come testo in grassetto nella finestra del terminale. Per visualizzare i caratteri in grassetto come testo normale, deselezionare questa opzione.
- **Attiva sottolineato** - Visualizza il testo con la sottolineatura.
- **Video inverso** (solo VT) - Questa opzione inverte i colori per il primo piano e per lo sfondo quando l'host VT invia una sequenza di escape di video inverso. Se questa opzione non è attivata, le sequenze di video inverso inviate dall'host vengono ignorate.

Per personalizzare i colori per tutti i tipi di host:

1. Nel riquadro di spostamento a sinistra, fare clic su **Display**.
2. Sotto **Mappature dei colori**, fare clic sul campo del colore per lo sfondo per aprire la griglia dei colori. Nella griglia dei colori, selezionare il colore da utilizzare come colore per lo sfondo dell'host. In alternativa, digitare il numero del colore HEX corrispondente al colore da utilizzare.
3. Nell'elenco a discesa, selezionare il colore predefinito dell'host da cambiare. Ad esempio, se si seleziona **Host rosa** nell'elenco a discesa e il colore in primo piano viene modificato in rosso, ogni volta che si presenta un testo rosa, questo verrà visualizzato in rosso.
4. Aprire la griglia dei colori per il **Primo piano** per scegliere un colore da mappare al nuovo colore per il testo o digitare il codice HEX da utilizzare. Selezionare **Sfondo** per mappare il nuovo colore per lo sfondo.
5. Fare clic su **Salva** per chiudere il pannello Display e continuare a configurare la connessione host.

Ripristina impostazioni predefinite annulla le modifiche apportate e ripristina i colori alle impostazioni predefinite dell'host.

Configurazione delle aree sensibili

Le aree sensibili sono pulsanti che vengono visualizzati sopra i comandi host di uso frequente nelle sessioni del terminale. Quando si utilizzano le aree sensibili è possibile controllare la sessione di terminale utilizzando il mouse o il tocco delle dita anziché la tastiera. L'area sensibile trasmette all'host un tasto del terminale o un comando. Per impostazione predefinita le aree sensibili sono configurate per i comandi 3270, 5250 e VT più comuni.

Le aree sensibili sono attive e visibili per impostazione predefinita, tuttavia è possibile disattivarle per una sessione particolare oppure scegliere di nasconderle.

- **Attiva aree sensibili**

  Scegliere **No** per disattivare le aree sensibili per la sessione alla quale ci si sta connettendo.

- **Mostra aree sensibili**

  Scegliere **No** per nascondere le aree sensibili sullo schermo. Le aree sensibili rimangono funzionali.

Tabella 5-1 *Aree sensibili per host 3270*

Area sensibile	Descrizione
PF1...PF24	Trasmette un tasto PF1...PF24 all'host
PA1, PA2 o PA3	Trasmette un tasto PA1, PA2 o PA3 all'host
invio	Trasmette un tasto Invio all'host
altro	Trasmette un tasto Cancella all'host

Tabella 5-2 *Aree sensibili per host 5250*

Area sensibile	Descrizione
invio	Trasmette un tasto Invio all'host
Ulteriori informazioni...	Trasmette un tasto Sposta su all'host (scorre di una pagina verso il basso)
PF1 - PF24	Trasmette un tasto PF1...PF24 all'host

Tabella 5-3 *Aree sensibili per host VT*

Area sensibile	Descrizione
F1 - F20	Trasmette un tasto F1...F20 all'host

Configurare le dimensioni dello schermo per host VT, UTS e T27

L'amministratore può selezionare il numero di righe e colonne per le sessioni VT, UTS e T27.

1. Aprire il pannello Display.
2. Sotto **Dimensioni**, specificare il numero di righe e colonne desiderato per ogni schermo. I valori predefiniti sono 80 colonne per 24 righe.

   Sono disponibili alcune impostazioni specifiche per il tipo di host:

   - **Pagine** - Se ci si sta connettendo allo schermo di un host T27, è possibile impostare il numero di pagine da visualizzare. Il valore predefinito è 2.
   - **Cancella dopo modifica host** - Se ci si sta connettendo allo schermo di un host VT, selezionare questa opzione per cancellare la finestra del terminale e spostare il contenuto nel buffer di scorrimento indietro quando le dimensioni della colonna cambiano.
3. Fare clic su **Salva**.

Impostare le opzioni del cursore

Utilizzare le opzioni relative al cursore per configurare l'aspetto e il comportamento del cursore e del righello.

Opzione	Azione eseguita
Tipo di cursore	◆ **Sottolineato** visualizza il cursore di testo come sottolineatura. ◆ **Barra verticale** visualizza il cursore come una riga verticale. ◆ **Blocco** visualizza il cursore di testo come un blocco video invertito.
Tipo di righello	◆ **Verticale** visualizza un righello verticale nella posizione del cursore. ◆ **Orizzontale** visualizza un righello orizzontale nella posizione del cursore. ◆ **Mirino** visualizza sia un righello orizzontale sia verticale nella posizione del cursore.
Colore cursore	Fare clic sul campo del colore per aprire la griglia del colori. Nella griglia dei colori, selezionare il colore da utilizzare per il cursore e il righello. In alternativa, digitare il codice HEX corrispondente al colore da utilizzare.
Cursore intermittente	Per impostazione predefinita, il cursore (blocco o sottolineatura) è intermittente. Deselezionare questa opzione per visualizzare un cursore non intermittente.

Impostare le opzioni dei font

Utilizzare queste opzioni dei font per accertarsi che i caratteri di terminale vengano visualizzati con la dimensione e lo stile di carattere desiderati.

Opzione	Azione eseguita
Dimensione carattere	◆ **Automatico** (impostazione predefinita) - il font viene scalato automaticamente in base alle dimensioni della finestra. Con questa opzione selezionata, è possibile scegliere **Mantieni proporzioni** per regolare in modo dinamico la dimensione carattere ma non estendere o ridimensionare il display del terminale per riempire lo spazio disponibile. ◆ **Fisso** - specificare le dimensioni in pixel per la visualizzazione della finestra di terminale.
Carattere zero	Per differenziare il carattere zero predefinito dalla lettera O, selezionare una delle opzioni seguenti: ◆ **Predefinito** ◆ **Zero con una barra** ◆ **Zero con un punto**

Impostare le opzioni del buffer di scorrimento indietro di VT

Il buffer di scorrimento indietro di VT contiene i dati che lo scorrimento ha eliminato dallo schermo e che non sono più accessibili dal computer host. Quando è presente un buffer di scorrimento indietro, è possibile visualizzarlo utilizzando la barra di scorrimento verticale.

Per impostazione predefinita, il buffer di scorrimento indietro è attivo. Se attivo, la sessione conserva in un buffer le righe che lo scorrimento ha eliminato dallo schermo del terminale. Questa opzione è disponibile per tutti gli utenti a cui l'amministratore ha assegnato le autorizzazioni per modificare le **Impostazioni del display del terminale**.

Opzione	Azione eseguita
Limite riga di scorrimento indietro	Imposta il numero di righe da inserire nel buffer di scorrimento indietro. L'impostazione predefinita è 500 righe.
Salva display prima di cancellare	Quando selezionata (impostazione predefinita), i dati sul display del terminale si spostano nel buffer di scorrimento indietro quando l'utente, o l'host, cancella il display del terminale. Se si preferisce che i dati sul display non vengano salvati nel buffer di scorrimento indietro, deselezionare questa opzione. Quando il display del terminale viene cancellato, i dati vengono eliminati.
Salva testo aree di scorrimento	Quando i margini superiore e inferiore dello schermo sono impostati (ad esempio, da un editor di testo come EDT o TPU, o con la funzione DECSTBM) l'area all'interno dei margini viene chiamata area di scorrimento. Quando questa opzione è deselezionata, il testo che scorre nella regione non viene salvato nel buffer di scorrimento indietro. Selezionare questa opzione per salvare le informazioni nelle aree di scorrimento nel buffer di scorrimento indietro. **Nota:** La memoria dello schermo potrebbe riempirsi velocemente.

Opzione	Azione eseguita
Salva prima di cancellare da qualsiasi riga	Questa impostazione specifica se i dati che sono stati cancellati in una parte della finestra del terminale vengono salvati nella memoria dello schermo.
Comprimi righe vuote	Selezionare questa opzione per ottimizzare lo spazio nella memoria dello schermo comprimendo più righe vuote in un'unica riga vuota.

Impostare le opzioni della tastiera

È possibile impostare le opzioni della tastiera seguenti:

Opzioni della tastiera 3270

- **Funzionalità typeahead**

  Quando questa opzione è selezionata, Host Access for the Cloud memorizza nel buffer i caratteri digitati nella finestra del terminale. Typeahead consente di continuare a digitare dopo avere inviato dati all'host. Senza Typeahead i caratteri digitati vengono ignorati finché l'host non è pronto per altri dati.

- **A capo automatico**

  Quando questa opzione è selezionata, viene attivata la funzionalità di a capo automatico in un campo di più righe non protetto. Con la modalità a capo automatico alcuni degli spazi tra le parole vengono sostituiti da interruzioni di riga, in modo che nella finestra del terminale ogni riga sia visibile e possa essere letta senza scorrere orizzontalmente il testo.

- **Tasto Attention invia**

  Consente di specificare il comando inviato quando si preme il tasto ATTN. Le opzioni disponibili sono Interruzione Telnet, Termina output e Sospendi processo.

Opzioni della tastiera 5250

- **Funzionalità typeahead**

  Quando questa opzione è selezionata, Host Access for the Cloud memorizza nel buffer i caratteri digitati nella finestra del terminale. Typeahead consente di continuare a digitare dopo avere inviato dati all'host. Senza Typeahead i caratteri digitati vengono ignorati finché l'host non è pronto per altri dati.

- **Ripristino automatico dopo errore**

  Quando questa opzione è selezionata, la chiave successiva selezionata dopo un errore della tastiera cancella l'errore, ripristina la riga di dati precedente all'errore e tenta di eseguire la sequenza di tasti come segue:

  - Se il cursore si trova in un campo di input valido e il tasto è un tasto dati, i dati vengono immessi se si tratta di dati validi per il campo specifico (ad esempio, un carattere numerico in un campo di input che accetta soltanto numeri).
  - Se il cursore si trova in un campo di input valido e il tasto è un tasto funzione, viene eseguita l'operazione associata al tasto.

- Se la posizione corrente del cursore non è un campo di input valido e il tasto è un tasto dati, il cursore si sposta al successivo campo di input valido e i dati vengono immessi in questo campo, se sono dati validi per il campo specifico.
- Se la posizione corrente del cursore non è un campo di input valido e il tasto è un tasto funzione, il cursore si sposta al successivo campo di input valido e il tasto viene ignorato.
- Se lo schermo corrente non contiene campi di input validi, verrà visualizzato un messaggio di errore a ogni sequenza di tasti premuta e non viene eseguita alcuna sequenza di tasti.

Quando questa opzione è deselezionata, è necessario premere Ripristina per cancellare il messaggio di errore dalla riga di errore prima di poter riprendere l'immissione dei dati.

Per impostazione predefinita, questa opzione non è selezionata.

- **Non eseguire controlli campo per tasto PF**

  Selezionare questa opzione per consentire l'invio di tasti PF all'host da campi con restrizioni. Questa opzione è deselezionata per impostazione predefinita.

Opzioni della tastiera VT

- **Backspace invia**

  Consente di configurare la funzione inviata dal tasto Backspace. Sulla tastiera del terminale VT il tasto freccia indietro (<x) è configurabile: può inviare un carattere di cancellazione (ASCII 127) o backspace (ASCII 8).

- **Eco locale** (VT)

  Se questa opzione è selezionata, qualsiasi carattere digitato sulla tastiera viene immediatamente visualizzato sullo schermo. Per impostazione predefinita questa opzione è deselezionata, perché la maggior parte degli host effettua l'eco dei caratteri ricevuti.

- **Tasti cursore**

  Controlla i caratteri trasmessi dalle quattro frecce (sia sulla tastiera alfanumerica che sul tastierino). L'impostazione di questo valore viene solitamente stabilita dall'host. In generale, è consigliabile impostare l'opzione su **Normale**.

  Se i tasti freccia non funzionano correttamente, l'opzione potrebbe essere rimasta erroneamente impostata sul valore **Applicazione** quando un programma host si è interrotto in modo anomalo. Reimpostare l'opzione su **Normale** per risolvere il problema dei tasti freccia.

- **Tastierino**

  Controlla i caratteri trasmessi dal tastierino numerico. L'impostazione di questo valore viene solitamente stabilita dall'host. In generale, è consigliabile impostare l'opzione su **Numerico**.

  Se i tasti numerici o i tasti PF non funzionano correttamente, l'opzione potrebbe essere rimasta erroneamente impostata sul valore **Applicazione** quando un programma host si è interrotto in modo anomalo. Reimpostare l'opzione su **Numerico** per risolvere il problema del tastierino numerico.

Opzioni della tastiera T27

- **Attiva minuscolo** (T27)

  Attiva la visualizzazione sullo schermo delle lettere minuscole, oltre alle maiuscole. Impostazione predefinita. Se questa opzione è deselezionata, verranno visualizzate solo le lettere maiuscole.

Impostazioni del terminale

Le impostazioni del terminale variano in base al tipo di host utilizzato.

Impostazioni dei terminali 3270 e 5250

- **Set di caratteri host**

  Consente di selezionare il set di caratteri dell'host 3270 o 5250 da utilizzare. Questa impostazione sceglie una tabella di conversione per convertire i caratteri dell'host (EBCDIC) in caratteri per il PC (ANSI). Deve corrispondere al set di caratteri nazionale utilizzato dal sistema host. Se non corrisponde, è possibile che alcuni caratteri, ad esempio gli accenti, non vengano visualizzati correttamente. Per le definizioni dei caratteri di ciascun set, consultare la documentazione dell'host. Il valore predefinito è US English (037).

- **Codice grafica estesa paese** (solo 3270)

  Quando questa opzione è selezionata (impostazione predefinita), sono disponibili caratteri aggiuntivi nel set di caratteri nazionale configurato. Per i dettagli, consultare la documentazione dell'host

Impostazioni del terminale VT

- **Tipo di terminale** (VT)

  Specifica il tipo di terminale da emulare. Queste scelte influenzano i codici generati dal tastierino numerico, l'interpretazione delle funzioni di controllo e la risposta alle richieste di identificazione del terminale.

- **ID terminale** (VT)

  Specifica la risposta che Host Access for the Cloud invia all'host in seguito a una richiesta primaria degli attributi del dispositivo (DA). Nella risposta all'host sono contenute le informazioni sulle funzioni di terminale che può eseguire. È una impostazione indipendente da quella definita per il tipo di terminale. Se impostata sul valore predefinito di Reflection, Host Access for the Cloud risponde alla richiesta primaria degli attributi del dispositivo (DA) primario con l'insieme di funzionalità supportate. Se l'host utilizzato richiede un ID terminale più specifico, selezionare un valore diverso dall'elenco.

- **Nuova riga** (VT)

  Selezionare questa opzione per inviare un ritorno a capo e un avanzamento riga premendo Invio. Quando Host Access for the Cloud riceve un input di avanzamento riga, avanzamento modulo o tabulazione verticale, sposta il cursore alla prima colonna della riga successiva. Quando questa opzione è deselezionata (impostazione predefinita) il tasto Invio produce solo un ritorno a capo. Un comando di avanzamento riga, avanzamento pagina o tabulazione verticale ricevuto dall'host sposta il cursore alla riga sottostante nella colonna corrente.

Selezionare questa opzione se le righe dello schermo si sovrappongono, cioè se l'host non sta inviando un avanzamento riga insieme al ritorno a capo. Se l'opzione Nuova riga è selezionata ma l'host non si aspetta di ricevere un avanzamento riga a ogni ritorno a capo, le righe sullo schermo avranno spaziatura doppia.

Impostazioni del terminale T27

- **Set di caratteri host** (T27)

  Con questa opzione è possibile specificare la conversione da host a schermo. Selezionare la lingua utilizzata per convertire i caratteri ricevuti dall'host prima che vengano visualizzati sul computer locale. Il valore predefinito è Nessuna conversione.

Impostare altre opzioni di visualizzazione

Alcune opzioni di visualizzazione sono specifiche dell'host, come indicato di seguito. Quando il tipo di host non è specificato, le opzioni si applicano a tutti i tipi di host supportato.

Opzione	Azione eseguita
Stile separatore colonna (5250)	Utilizzare questa opzione per specificare il carattere (se presente) da utilizzare per il rendering dei separatori di colonna nelle sessioni di terminale 5250. Le opzioni sono: ◆ **Punti**- Per separare le colonne vengono utilizzati i punti. Impostazione predefinita. ◆ **Barre verticali**- Per separare le colonne vengono utilizzate righe verticali. ◆ **Nessuno** - Per separare le colonne non viene usato alcun carattere.
Sottolineatura campi di input (3270, 5250)	È possibile determinare come viene gestita la sottolineatura dei campi di input dell'host: ◆ **L'host controlla la sottolineatura** (impostazione predefinita) ◆ **Sottolinea sempre i campi di input** ◆ **Non sottolineare i campi di input**
Riga di stato (VT)	Per attivare una riga di stato nella parte inferiore del display. Scegliere: ◆ **Nessuno** per disattivare la riga di stato. (impostazione predefinita) ◆ **Indicatore** per visualizzare la pagina, la posizione del cursore e lo stato della stampante. ◆ **Scrivibile dall'host** per consentire all'applicazione host di visualizzare informazioni nella riga di stato.
Mantieni proporzioni	Selezionare questa opzione per mantenere le proporzioni dello schermo dell'host indipendentemente dalla finestra del browser. Le proporzioni descrivono la relazione fra la larghezza e l'altezza di un'immagine.
Visualizza OIA (3270, 5250)	Selezionare questa opzione per visualizzare i messaggi relativi alle operazioni e allo stato nell'area di informazioni per l'operatore (Operator Information Area, OIA) nella parte inferiore della finestra del terminale. Per impostazione predefinita, questa opzione è selezionata.

Opzione	Azione eseguita
Visualizza riga di stato (ALC)	Attiva una riga di stato nella parte inferiore del display.
Ignora clic del mouse all'attivazione della finestra	Quando un clic del mouse attiva la finestra del terminale, questa opzione specifica se vengono eseguite anche azioni come l'aggiornamento della posizione del cursore del terminale, la deselezione di una selezione o l'esecuzione di un'area sensibile. Per impostazione predefinita, queste azioni non vengono eseguite.
A capo automatico (VT)	Quando questa opzione è selezionata, i caratteri vanno a capo automaticamente quando raggiungono il margine destro e continuano sulla riga successiva. Quando è deselezionata, i caratteri non vanno a capo quando raggiungono il margine destro della visualizzazione. I nuovi caratteri sovrascrivono l'ultimo carattere sul margine destro fino all'immissione di un ritorno a capo.

Mappatura dei tasti

È possibile creare tasti di scelta rapida che eseguono qualsiasi azione assegnabile durante una sessione. La pagina di impostazione Mappature dei tasti fornisce una visualizzazione della mappa della tastiera predefinita per ogni tipo di host e i tasti personalizzati mappati, indicati in grassetto, per la sessione specifica.

Mappatura dei tasti come amministratore e come utente finale

Quando si mappano i tasti, vi sono alcune differenze nel comportamento tra amministratore e utente finale.

- Gli utenti finali possono solo aggiungere o modificare le mappature dei tasti se l'amministratore ha assegnato loro le autorizzazioni nel pannello **Regole di preferenze utente**.
- Eventuali modifiche apportare dall'amministratore sono indistinguibili per l'utente finale dalle mappature dei tasti dell'host predefinite. Una volta assegnate le autorizzazioni, la persona può modificare, aggiungere o eliminare le mappature indipendentemente dalle modifiche dell'amministratore. Tuttavia, il ripristino delle mappature dei tasti le riporta solo allo stato modificato creato dell'amministratore per la sessione corrente.

Aggiunta o modifica dei tasti mappati

1. Nella barra degli strumenti, fare clic su **Impostazioni**.
2. Nel riquadro di spostamento a sinistra, selezionare **Mappatura dei tasti.** Sono visibili i tasti mappati per il tipo di host a cui ci si sta connettendo.
3. Per aggiungere una nuova mappatura dei tasti:
   - Fare clic su  . È possibile scegliere di digitare la sequenza di tasti da utilizzare oppure utilizzare la tastiera per passare  trale due opzioni.
   - Nell'elenco a discesa **Azione**, selezionare l'azione da associare alla selezione di tasti. Se si seleziona **Invia testo**, immettere la stringa da inviare all'host nel campo **Valore**. Analogamente, se si seleziona **Esegui macro**, scegliere la macro che deve essere avviata dal tasto di scelta rapida. È necessario creare la macro prima di mapparla sull'azione Esegui macro.

L'azione Invia testo supporta caratteri con codice minore o uguale a 0xFFFF tramite sequenze di escape Unicode. La sequenza di escape inizia con \u seguito esattamente da quattro cifre esadecimali. È possibile incorporare le sequenze di escape Unicode in qualsiasi stringa. Ad esempio, *questa sequenza \u0045 incorporata* sarà interpretata *questa sequenza E incorporata*, poiché 45 è il codice esadecimale per il carattere *E*.

Per passare le sequenze di escape Unicode all'host, aggiungere una barra iniziale alla sequenza di escape. Ad esempio per inviare il valore letterale stringa *\u001C* all'host, mappare un tasto a *\\u001C*. Host Access for the Cloud lo converte nella stringa *\u001C* quando viene premuto il tasto e invia all'host i 6 caratteri della stringa risultante.

L'azione **Disabilita** rende il tasto inutilizzabile. Quando si preme il tasto non verrà avviata alcuna azione. In questo si differenzia dall'azione **Senza mappatura** che rimuove la mappatura del tasto, ma conserva una scorciatoia del browser se è stata impostata.

- Fare clic sul segno di spunta blu per accettare la mappatura e aggiungere la mappa dei tasti alla sessione.

4 Per modificare una mappatura esistente:

Selezionare la riga che contiene il tasto da modificare.

Seguire i passaggi per l'aggiunta di una nuova mappatura dei tasti, facendo clic su per salvare la nuova mappatura. In alternativa, è possibile fare clic fuori dalla riga modificata per salvare la modifica. Tutte le mappe dei tasti nuove e modificate sono indicate in grassetto. È possibile ripristinare la mappatura dei tasti originale in qualsiasi momento facendo clic su .

Filtro dell'elenco

Il campo Filtro semplifica la visualizzazione delle sole mapature a cui si è interessati. Il filtro si basa su parole chiave e ha effetto su tutte le colonne della tabella. Ad esempio, se si immette **Invia testo** nel campo Filtro, vengono visualizzati solo i tasti mappati sull'azione **Invia testo**.

Utilizzando l'opzione **Mostra solo mappature modificate** è possibile vedere solo le mappature modificate precedentemente dall'utente.

Alcuni punti da ricordare:

- **Mappatura dei tasti modificatore destro e sinistro su azioni singole**

  È possibile mappare i tasti modificatore destro e sinistro ad azioni singole. Tuttavia quando sono combinati con altri tasti, non c'è differenza fra il modificatore destro o sinistro. Ad esempio, Alt-Sinistro può essere mappato ad Azione-A mentre Alt-Destro può essere mappato ad Azione-B, ma Alt-Sinistro+H verrà memorizzato come Alt+H e sia Alt-Sinistro+H e Alt-Destro+H saranno associati a un'unica azione mappata.

- **Combinazioni di tasti e operazioni di copia/incolla**

  Anche per le operazioni di copia/incolla vengono utilizzate combinazioni diverse di tasti. Ad esempio, sullo schermo di un host VT, **Ctrl+ Maiusc + A** avvia l'azione Seleziona tutto. Vedere Operazioni di copia e incolla per un elenco di azioni per i tasti copia/incolla.

- **Tasti di scelta rapida e browser**

  I browser utilizzano i tasti di scelta rapida per risparmiare tempo e clic del mouse. È importante tenere in considerazione questo aspetto quando si mappano i tasti di scelta rapida. Handy Keyboard Shortcuts fornisce una breve panoramica dei tasti di scelta rapida utilizzati da browser diversi. Nella maggior parte dei casi le mappature dei tasti di Host Access for the Cloud hanno la precedenza sulle scelte rapide del browser. Occasionalmente, se non si desidera questo comportamento per una combinazione di tasti specifica, è possibile scegliere **Senza mappatura** dall'elenco di azioni per annullare la mappatura della scorciatoia. Questo consente il passaggio degli eventi chiave attraverso il browser.

Mappatura della tastiera dell'host

Le tabelle seguenti forniscono i tasti predefiniti, il nome dei tasti e le relative descrizioni per le diverse mappature delle tastiere dell'host.

Mappatura della tastiera IBM 3270
Mappatura della tastiera IBM 5250
Mappatura della tastiera VT
Mappatura della tastiera UTS
Mappatura della tastiera T27
Mappatura della tastiera ALC

Tabella 5-4 *Mappatura della tastiera IBM 3270*

Tasto	Mappato a	Descrizione
Ctrl+F1	Attenzione	Invia il tasto ATTENTION all'host
Maiusc+Tab	Backtab	Sposta il cursore sul campo non protetto precedente
Ctrl+F2	Cancella	Cancella lo schermo e invia il tasto CLEAR all'host
Alt+Freccia sinistra	Cursore due a sinistra	Sposta il cursore di due posizioni verso sinistra
Alt+Freccia destra	Cursore due a destra	Sposta il cursore di due posizioni verso destra
Ctrl+F3	Selezione cursore	Simula la selezione di una penna ottica nel campo corrente
Alt+Canc	Elimina parola	Elimina tre caratteri dal campo corrente
Ctrl+5	Duplica	Inserisce il carattere DUP nella posizione del cursore
Invio	Invio	Invia il tasto ENTER all'host
Fine	Cancella fino a fine del campo	Cancella tutti i dati dalla posizione del cursore alla fine del campo corrente
Alt+F5	Cancella input	Cancella tutti i dati in tutti i campi non protetti dello schermo corrente
Ctrl+Alt+F	Delimitatore di campo	Attiva/Disattiva la visualizzazione dei delimitatori di campo sullo schermo
Ctrl+6	Field Mark	Inserisce il carattere Field Mark nella posizione del cursore

Tasto	Mappato a	Descrizione
Home	Home	Sposta il cursore sul primo campo non protetto sullo schermo
Ins	Inserisci	Attiva/Disattiva la modalità inserimento
Maiusc+Invio	Nuova riga	Passa al successivo campo non protetto
Ctrl+1	PA1	Invia il tasto PA1 all'host
PagSu	PA1	Invia il tasto PA1 all'host
Ctrl+2	PA2	Invia il tasto PA2 all'host
PagGiù	PA2	Invia il tasto PA2 all'host
Ctrl+3	PA3	Invia il tasto PA3 all'host
F1 - F10	PF1 - PF10	Invia il tasto PF1, PF2...PF10 all'host
Alt+1	PF11	Invia il tasto PF11 all'host
F11	PF11	Invia il tasto PF11 all'host
Alt+2	PF12	Invia il tasto PF12 all'host
F12	PF12	Invia il tasto PF12 all'host
Maiusc+F1	PF13	Invia il tasto PF13 all'host
Maiusc+F2	PF14	Invia il tasto PF14 all'host
Maiusc+F3	PF15	Invia il tasto PF15 all'host
Maiusc+F4	PF16	Invia il tasto PF16 all'host
Maiusc+F5	PF17	Invia il tasto PF17 all'host
Maiusc+F6	PF18	Invia il tasto PF18 all'host
Maiusc+F7	PF19	Invia il tasto PF19 all'host
Maiusc+F8	PF20	Invia il tasto PF20 all'host
Maiusc+F9	PF21	Invia il tasto PF21 all'host
Maiusc+F10	PF22	Invia il tasto PF22 all'host
Alt3	PF23	Invia il tasto PF23 all'host
Maiusc+F11	PF23	Invia il tasto PF23 all'host
Alt4	PF24	Invia il tasto PF24 all'host
Maiusc+F12	PF24	Invia il tasto PF24 all'host
Ctrl+P	Stampa	Stampa il contenuto dello schermo sulla stampante
Esc	Ripristina	Ripristina le condizioni di errore della tastiera
Ctrl+S	Richiesta di sistema	Invia il tasto SYSTEM REQUEST all'host

Tabella 5-5 *Mappatura della tastiera IBM 5250*

Tasto	Mappato a	Descrizione
Esc	Attenzione	Invia il tasto ATTENTION all'host
Ctrl+F2	Cancella	Cancella lo schermo e invia il tasto CLEAR all'host
Ctrl+F3	Selezione cursore	Simula la selezione di una penna ottica nel campo corrente
Ctrl+Backspace	Backspace distruttivo	Sposta il cursore di una posizione a sinistra
Ctrl+5	Duplica	Inserisce il carattere DUP nella posizione del cursore
Ctrl+Fine	Fine del campo	Sposta il cursore alla fine del campo
Fine	Cancella fino a fine del campo	Cancella tutti i dati dalla posizione del cursore alla fine del campo corrente
Alt+Fine	Cancella input	Cancella tutti i dati in tutti i campi non protetti dello schermo corrente
Alt+F5	Cancella input	Cancella tutti i dati in tutti i campi non protetti dello schermo corrente
Ctrl+Invio	Uscita campo	Sposta il cursore all'esterno di un campo di input
KP + Segno meno	Uscita campo meno	Sposta il cursore all'esterno di un campo numerico con segno o solo numerico
Ctrl+Segno meno	Uscita campo meno	Sposta il cursore all'esterno di un campo numerico con segno o solo numerico
KP + Segno più	Uscita campo più	Sposta il cursore all'esterno di un campo numerico con segno o solo numerico
Ctrl+Segno più	Uscita campo più	Sposta il cursore all'esterno di un campo numerico con segno o solo numerico
Ctrl+6	Field Mark	Inserisce il carattere Field Mark nella posizione del cursore
Ctrl+H	Guida	Invia il tasto Help all'host
Ctrl+X	Modalità esadecimale	Imposta il terminale in modalità di input esadecimale
Home	Home	Sposta il cursore sul primo campo non protetto sullo schermo
Ins	Inserisci	Attiva/Disattiva la modalità inserimento
Maiusc+Invio	Nuova riga	Passa al successivo campo non protetto
Ctrl+1	PA1	Invia il tasto PA1 all'host
Ctrl+2	PA2	Invia il tasto PA2 all'host
Ctrl+3	PA3	Invia il tasto PA3 all'host
F1 - F11	PF1 - PF11	Invia il tasto PF1, PF2....PF11 all'host
Alt+1	PF11	Invia il tasto PF11 all'host

Tasto	Mappato a	Descrizione
Alt+2	PF12	Invia il tasto PF12 all'host
F12	PF12	Invia il tasto PF12 all'host
Maiusc+1	PF13	Invia il tasto PF13 all'host
Maiusc+F2	PF14	Invia il tasto PF14 all'host
Maiusc+F3	PF15	Invia il tasto PF15 all'host
Maiusc+F4	PF16	Invia il tasto PF16 all'host
Maiusc+F5	PF17	Invia il tasto PF17 all'host
Maiusc+F6	PF18	Invia il tasto PF18 all'host
Maiusc+F7	PF19	Invia il tasto PF19 all'host
Maiusc+F8	PF20	Invia il tasto PF20 all'host
Maiusc+F9	PF21	Invia il tasto PF21 all'host
Maiusc+F10	PF22	Invia il tasto PF22 all'host
Alt+3	PF23	Invia il tasto PF23 all'host
Maiusc+F11	PF23	Invia il tasto PF23 all'host
Alt+4	PF24	Invia il tasto PF24 all'host
Maiusc+F12	PF24	Invia il tasto PF24 all'host
Ctrl+P	Stampa	Stampa il contenuto dello schermo sulla stampante
Ctrl	Ripristina	Ripristina le condizioni di errore della tastiera
PagSu	Sposta giù	Invia il tasto RollDown all'host
PagGiù	Sposta su	Invia il tasto RollUp all'host
Ctrl+Home	Inizio del campo	Sposta il cursore all'inizio del campo
Ctrl+S	Richiesta di sistema	Invia il tasto SYSTEM REQUEST all'host

Tabella 5-6 *Mappatura della tastiera VT*

Tasto	Mappato a	Descrizione
Ctrl+Canc	Interruzione	Invia il tasto Break all'host
Ctrl+Invio	Invio	Invia il tasto Enter all'host
Alt+F1	F1	Invia il tasto F1 all'host
Ctrl+F1	F11	Invia il tasto F11 all'host
Ctrl+F2	F12	Invia il tasto F12 all'host
Ctrl+F3	F13	Invia il tasto F13 all'host
Ctrl+F4	F14	Invia il tasto F14 all'host

Tasto	Mappato a	Descrizione
Ctrl+F5	F15	Invia il tasto F15 all'host
Ctrl+F6	F16	Invia il tasto F16 all'host
Ctrl+F7	F17	Invia il tasto F17 all'host
Ctrl+F8	F18	Invia il tasto F18 all'host
Ctrl+F9	F19	Invia il tasto F19 all'host
Ctrl+F10	F20	Invia il tasto F20 all'host
Home	Trova	Invia il tasto Find all'host
F1	In attesa	Invia il tasto Hold Screen all'host
Pausa	In attesa	Invia il tasto Hold Screen all'host
Ins	Inserisci	Invia il tasto Insert all'host
Ctrl+Ins	0 tastierino	Invia il tasto 0 del tastierino numerico all'host
Ctrl+Fine	1 tastierino	Invia il tasto 1 del tastierino numerico all'host
Ctrl+FrecciaGiù	2 tastierino	Invia il tasto 2 del tastierino numerico all'host
Ctrl+PagGiù	3 tastierino	Invia il tasto 3 del tastierino numerico all'host
Ctrl+FrecciaSinistra	4 tastierino	Invia il tasto 4 del tastierino numerico all'host
Ctrl+Canc	5 tastierino	Invia il tasto 5 del tastierino numerico all'host
Ctrl+FrecciaDestra	6 tastierino	Invia il tasto 6 del tastierino numerico all'host
Ctrl+Home	7 tastierino	Invia il tasto 7 del tastierino numerico all'host
Ctrl+FrecciaSu	8 tastierino	Invia il tasto 8 del tastierino numerico all'host
Ctrl+PagSu	9 tastierino	Invia il tasto 9 del tastierino numerico all'host
Ctrl+Alt-Segno più	Virgola tastierino	Invia il tasto Comma del tastierino numerico all'host
Ctrl+Segno più	Meno tastierino	Invia il tasto Minus del tastierino numerico all'host
Ctrl+decimale	Punto tastierino	Invia il tasto Period del tastierino numerico all'host
Ctrl + Canc	Punto tastierino	Invia il tasto Period del tastierino numerico all'host
Ctrl+Alt+FrecciaSu	Riga su	Nel buffer di scorrimento indietro, si sposta di una riga verso l'alto
Ctrl+Alt+FrecciaGiù	Riga giù	Nel buffer di scorrimento indietro, si sposta di una riga verso l'alto
PagGiù	Successivo	Invia il tasto Next Screen all'host
Ctrl+Pausa	PF1	Invia il tasto PF1 all'host
Ctrl+segno diviso	PF2	Invia il tasto PF2 all'host
Ctrl+segno per	PF3	Invia il tasto PF3 all'host

Tasto	Mappato a	Descrizione
Ctrl+Segno meno	PF4	Invia il tasto PF4 all'host
PagSu	Precedente	Invia il tasto Prev Screen all'host
Canc	Rimuovi	Invia il tasto Remove all'host
Fine	Seleziona	Invia il tasto Select all'host
Maiusc+F6	UDK6	Invia il tasto User Defined Key 6 all'host
Maiusc+F7	UDK7	Invia il tasto User Defined Key 7 all'host
Maiusc+F8	UDK8	Invia il tasto User Defined Key 8 all'host
Maiusc+F9	UDK9	Invia il tasto User Defined Key 9 all'host
Maiusc+F10	UDK10	Invia il tasto User Defined Key 10 all'host
Maiusc+Ctrl+F1	UDK11	Invia il tasto User Defined Key 11 all'host
Maiusc+Ctrl+F2	UDK12	Invia il tasto User Defined Key 12 all'host
Maiusc+Ctrl+F3	UDK13	Invia il tasto User Defined Key 13 all'host
Maiusc+Ctrl+F4	UDK14	Invia il tasto User Defined Key 14 all'host
Maiusc+Ctrl+F5	UDK15	Invia il tasto User Defined Key 15 all'host
Maiusc+Ctrl+F6	UDK16	Invia il tasto User Defined Key 16 all'host
Maiusc+Ctrl+F7	UDK17	Invia il tasto User Defined Key 17 all'host
Maiusc+Ctrl+F8	UDK18	Invia il tasto User Defined Key 18 all'host
Maiusc+Ctrl+F9	UDK19	Invia il tasto User Defined Key 19 all'host
Maiusc+Ctrl+F10	UDK20	Invia il tasto User Defined Key 20 all'host

Tabella 5-7 *Mappatura della tastiera UTS*

Tasto	Mappato a	Descrizione
F4	Cancella change bit	Invia il tasto CLEARCHANGEBIT all'host.
Tastierino+Invio	A capo	Invia un ritorno a capo all'host.
Ctrl+PagGiù	Cancella fino a fine display	Cancella tutti i dati dalla posizione del cursore alla fine della visualizzazione.
Ctrl+PagSu	Cancella fino a fine display FCC	Cancella tutti i dati (comprese le informazioni FCC) dalla posizione del cursore alla fine della visualizzazione.
Ctrl+Fine	Cancella fino a fine campo	Cancella tutti i dati dalla posizione del cursore alla fine del campo.
Ctrl+Maiusc+Fine	Cancella fino a fine riga	Cancella tutti i dati dalla posizione del cursore alla fine della riga.
F7	Cancella FCC	Cancella il carattere di controllo del campo.

Tasto	Mappato a	Descrizione
Ctrl+Home	Cancella Home	Invia il tasto CLEAR_HOME all'host.
Ctrl+H	Separatore di colonna destro	Invia il tasto COLUMN_SEP_RIGHT all'host.
Ctrl+F1	Pagina di controllo	Invia il tasto CONTROL_PAGE all'host.
Tastierino+2	Cursore giù	Sposta il cursore in basso di una riga.
Tastierino+4	Cursore a sinistra	Sposta il cursore di una colonna a sinistra.
Tastierino+6	Cursore a destra	Sposta il cursore di una colonna a destra.
Tastierino+8	Cursore su	Sposta il cursore in alto di una riga.
Canc	Elimina nella riga	Invia il tasto DELETE_IN_LINE all'host.
Ctrl+Canc	Elimina nella pagina	Invia il tasto DELETE_IN_PAGE all'host.
Ctrl+Maiusc+Canc	Elimina riga	Elimina la riga nella posizione del cursore.
Ctrl+FrecciaGiù	Duplica riga	Duplica la riga nella posizione del cursore.
F8	Attiva FCC	Attiva il caratteri di controllo del campo.
Tastierino+-	Fine del display e trasmetti	Invia il tasto EOD_AND_TRANSMIT all'host.
Maiusc+Fine	Fine del campo	Sposta il cursore alla fine del campo.
Fine	Fine riga	Sposta il cursore alla fine della riga.
Ctrl+FrecciaDestra	Fine pagina	Sposta il cursore alla fine della pagina.
Shift+Spazio	Cancella carattere	Cancella il carattere nella posizione del cursore.
Ctrl+Maiusc+E	Carattere Euro	Invia il carattere Euro all'host.
Ctrl+1 - Ctrl+9	F1 - F9	Invia il tasto F1 - F9 all'host.
Ctrl+0	F10	Invia il tasto F10 all'host.
Ctrl+-	F11	Invia il tasto F11 all'host.
Ctrl+=	F12	Invia il tasto F12 all'host.
Ctrl+Q	F13	Invia il tasto F13 all'host.
Ctrl+W	F14	Invia il tasto F14 all'host.
Ctrl+E	F15	Invia il tasto F15 all'host.
Ctrl+R	F16	Invia il tasto F16 all'host.
Ctrl+T	F17	Invia il tasto F17 all'host.
Ctrl+Y	F18	Invia il tasto F18 all'host.
Ctrl+U	F19	Invia il tasto F19 all'host.
Ctrl+I	F20	Invia il tasto F20 all'host.

Tasto	Mappato a	Descrizione
Ctrl+O	F21	Invia il tasto F21 all'host.
Ctrl+P	F22	Invia il tasto F22 all'host.
Maiusc+F3	FF	Invia un avanzamento pagina all'host.
F9	Genera FCC	Genera un carattere di controllo del campo.
Home	Home	Sposta il cursore sul primo campo sullo schermo.
Ctrl+Maiusc+Spazio	Inserisci nella riga	Invia il tasto INSERT_IN_LINE all'host.
Ctrl+Spazio	Inserisci nella pagina	Invia il tasto INSERT_IN_PAGE all'host.
Ctrl+Maiusc+Ins	Inserisci riga	Inserisce una nuova riga nella memoria del display.
Ins	Modalità inserimento	Attiva/Disattiva la modalità inserimento carattere.
F5	Individua FCC	Disabilita i caratteri di controllo del campo e passa al primo carattere del campo successivo a destra del cursore.
F3	Attesa messaggio	Invia il tasto MESSAGE_WAIT all'host.
Maiusc+F2	Nuova riga	Sposta il cursore in una nuova riga.
Tastierino+Maiusc+2	Campo successivo	Sposta il cursore sul campo successivo.
Tastierino+Maiusc+4	Campo successivo	Sposta il cursore sul campo successivo.
PagGiù	Pagina giù	Invia il tasto Page Down all'host.
PagSu	Pagina su	Invia il tasto Page Up all'host.
Tastierino+Maiusc+6	Campo precedente	Sposta il cursore sul campo precedente.
Tastierino+Maiusc+8	Campo precedente	Sposta il cursore sul campo precedente.
Clear	Carattere SOE	Invia il carattere SOE all'host.
F12	Carattere SOE	Invia il carattere SOE all'host.
Ctrl+Canc	Imposta tabulazione	Invia il tasto SET_TAB all'host.
Ctrl+Tab	Imposta tabulazione	Invia il tasto SET_TAB all'host.
Maiusc+Home	Inizio del campo	Sposta il cursore all'inizio del campo.
Ctrl+FrecciaSinistra	Inizio della riga	Sposta il cursore all'inizio della riga.
Ctrl+[	Modalità sistema	Invia il tasto SYSTEM_MODE all'host.
Ctrl+J	Attiva/Disattiva separatore colonna	Attiva/Disattiva il separatore di colonna.
Ctrl+F12	Attiva/Disattiva segnale acustico attesa messaggio	Invia il tasto TOGGLEMSGWAITBEEP all'host.

Tasto	Mappato a	Descrizione
Ctrl+L	Attiva/Disattiva barrato	Attiva/Disattiva la modalità barrato.
Ctrl+K	Attiva/Disattiva sottolineato	Attiva/Disattiva la modalità sottolineato.
Ctrl+Invio	Trasmetti	Trasmette il contenuto del display all'host.
ScrollLock	Trasmetti	Trasmette il contenuto del display all'host.
Tastierino++	Trasmetti	Trasmette il contenuto del display all'host.
Tastierino+Ctrl+	Trasmetti	Trasmette il contenuto del display all'host.
Esc	Sblocca	Invia il tasto UNLOCK all'host.
Ctrl+]	Modalità workstation	Invia il tasto WORKSTATION_MODE all'host.

Tabella 5-8 *Mappatura della tastiera T27*

Tasto	Mappato a	Descrizione
Backspace	Backspace	Sposta il cursore di una colonna a sinistra.
Maiusc+Tab	Tab indietro	Sposta il cursore sul campo precedente.
Ctrl + Canc	Cancella fino a fine riga	Cancella tutti i dati dalla posizione del cursore alla fine della riga.
Maiusc+Home	Cancella pagina e Home	Cancella la pagina e riporta il cursore nella posizione iniziale.
Left Ctrl	Pagina di controllo	Imposta la sessione in modalità di controllo.
FrecciaGiù	Cursore giù	Sposta il cursore in basso di una riga.
FrecciaSu	Cursore a sinistra	Sposta il cursore di una colonna a sinistra.
FrecciaDestra	Cursore a destra	Sposta il cursore di una colonna a destra.
FrecciaSu	Cursore su	Sposta il cursore in alto di una riga.
Ctrl+FrecciaSinistra	Cursore una parola a sinistra	Sposta il cursore sulla parola precedente.
Ctrl+ FrecciaDestra	Cursore una parola a destra	Sposta il cursore sulla parola successiva.
Ctrl+D	Elimina riga	Elimina la riga nella posizione del cursore.
Ctrl+Fine	Fine riga	Sposta il cursore alla fine della riga.
Fine	Fine pagina	Sposta il cursore sull'ultimo campo non protetto sulla pagina.
Maiusc+Ctrl+E	Carattere Euro	Invia il carattere Euro all'host.
Home	Home	Sposta il cursore sul primo campo sullo schermo.
Ins	Modalità inserimento	Imposta la sessione in modalità inserimento.

Tasto	Mappato a	Descrizione
Ctrl+I	Inserisci riga	Inserisce una nuova riga nella memoria del display.
Ctrl+1	PF1	Invia il tasto PF1 all'host.
Ctrl+10	PF10	Invia il tasto PF10 all'host.
Ctrl+2	PF2	Invia il tasto PF2 all'host.
Ctrl+3	PF3	Invia il tasto PF3 all'host.
Ctrl+4	PF4	Invia il tasto PF4 all'host.
Ctrl+5	PF5	Invia il tasto PF5 all'host.
Ctrl+6	PF6	Invia il tasto PF6 all'host.
Ctrl+7	PF7	Invia il tasto PF7 all'host.
Ctrl+8	PF8	Invia il tasto PF8 all'host.
Ctrl+9	PF9	Invia il tasto PF9 all'host.
PagGiù	Pagina giù	Visualizza la pagina successiva.
PagSu	Pagina su	Visualizza la pagina precedente.
Ctrl+E	Inserisci ETX	Inserisce un carattere di fine testo e riporta il cursore alla posizione iniziale.
Tastierino /	Inserisci modalità locale	Imposta la sessione in modalità locale.
Tastierino *	Inserisci modalità ricezione	Imposta la sessione in modalità ricezione.
Invio	A capo	Invia il tasto Return all'host.
Tastierino+Invio	A capo	Invia il tasto Return all'host.
Ctrl+A	Seleziona tutto	Seleziona tutto il testo.
Maiusc+FrecciaDestra	Seleziona giù	Seleziona il testo in basso.
Maiusc+FrecciaSinistra	Seleziona a sinistra	Seleziona il testo in basso.
Maiusc+FrecciaDestra	Seleziona a destra	Seleziona il testo a destra.
Maiusc+FrecciaSu	Seleziona su	Seleziona il testo in alto.
Maiusc+Ctrl+1	Maiusc F1	Invia il tasto Shift F1 all'host.
Maiusc+Ctrl+0	Maiusc F10	Invia il tasto Shift F10 all'host.
Maiusc+Ctrl+2	Maiusc F2	Invia il tasto Shift F2 all'host.
Maiusc+Ctrl+3	Maiusc F3	Invia il tasto Shift F3 all'host.
Maiusc+Ctrl+4	Maiusc F4	Invia il tasto Shift F4 all'host.
Maiusc+Ctrl+5	Maiusc F5	Invia il tasto Shift F5 all'host.

Tasto	Mappato a	Descrizione
Maiusc+Ctrl+6	Maiusc F6	Invia il tasto Shift F6 all'host.
Maiusc+Ctrl+7	Maiusc F7	Invia il tasto Shift F7 all'host.
Maiusc+Ctrl+8	Maiusc F8	Invia il tasto Shift F8 all'host.
Maiusc+Ctrl+9	Maiusc F9	Invia il tasto Shift F9 all'host.
F5	Specifica	Trasmette la posizione del cursore all'host.
Tab	Tab	Sposta il cursore sul campo successivo.
F2	Trasmetti	Trasmette la pagina all'host.
Tastierino +	Trasmetti	Trasmette la pagina all'host.
Ctrl+F2	Trasmetti riga	Trasmette la riga corrente all'host.
Tastierino -	Trasmetti riga	Trasmette la riga corrente all'host.

Tabella 5-9 *Mappatura della tastiera ALC*

Tasto	Mappato a	Descrizione
Ctrl+M	Sposta giù automatico	Attiva/Disattiva la capacità di ricevere più pagine
Backspace	Backspace	Sposta il cursore di una colonna a sinistra.
Maiusc+Tab	Tab indietro	Sposta il cursore sul campo precedente.
Ctrl+Home	Cancella	Cancella lo schermo e invia il tasto CLEAR all'host
Ctrl+B	Cancella trasmissione	Cancella il messaggio di trasmissione SITA
:	Due punti	Inserisce il carattere due punti nella posizione del cursore.
Ctrl+L	Croce di Lorena	Inserisce il carattere Croce di Lorena nella posizione del cursore
↓	Cursore giù	Sposta il cursore in basso di una riga
Tastierino ↓	Cursore giù	Sposta il cursore in basso di una riga.
←	Cursore a sinistra	Sposta il cursore sulla parola precedente
Tastierino ←	Cursore a sinistra	Sposta il cursore sulla parola precedente
→	Cursore a destra	Sposta il cursore sulla parola successiva
Tastierino →	Cursore a destra	Sposta il cursore sulla parola successiva
↑	Cursore su	Sposta il cursore in alto di una riga
Tastierino ↑	Cursore su	Sposta il cursore in alto di una riga.
Elimina	Elimina carattere	Elimina il carattere nella posizione del cursore.
Ctrl + Canc	Elimina riga	Elimina la riga nella posizione del cursore.

Tasto	Mappato a	Descrizione
=	Visualizza	Inserisce il carattere visualizzato nella posizione del cursore.
Ctrl+N	Visualizza nuova riga	Inserisce il carattere visualizzato in una nuova riga
]	Dollaro	Inserisce il carattere del simbolo di dollaro degli Stati Uniti nella posizione del cursore
.	Fine elemento	Inserisce il carattere di fine elemento nella posizione del cursore
Fine	Fine riga	Sposta il cursore in fondo alla riga
Ctrl+T	Fine transazione	Chiude il PNR
Ctrl+E	Cancella fino a fine del display	Cancella tutti i dati dalla posizione del cursore alla fine del display.
Ctrl+Fine	Cancella fino a fine riga	Cancella tutti i dati dalla posizione del cursore alla fine della riga
Home	Home	Sposta il cursore sul primo campo non protetto sullo schermo
Ctrl+I	Ignora	Annulla le modifiche apportate al PNR corrente
Ctrl+Ins	Inserisci riga	Inserisce una nuova riga nella memoria del display
Ins	Inserisci Spazio	Inserisce uno spazio nella memoria del display
\	Nuova riga	Inserisce il carattere di nuova riga nella posizione del cursore
[	Simbolo generico di valuta	Inserisce il simbolo generico di valuta nella posizione del cursore
Ctrl+G	Sterlina	Inserisce il simbolo di sterlina inglese nella posizione del cursore
Ctrl+Invio	Stampa Invio	Invia la risposta alla stampante
Ctrl+P	Ripristino protetto	Sposta il cursore nel primo campo non protetto
Ctrl+↑	Richiama input successivo	Richiama il successivo input o immissione
Ctrl+↓	Richiama input precedente	Richiama il precedente input o immissione
Ctrl+Z	Immetti di nuovo	Invia di nuovo il messaggio inviato in precedenza all'host
Ctrl+R	Ripeti	Visualizza di nuovo l'ultimo messaggio inviato dall'host
Esc	Ripristina	Ripristina le condizioni di errore della tastiera
Maiusc+Ctrl+↓	Scorri riga giù	Scorre il display in giù di una riga
Maiusc+Ctrl+↑	Scorri riga su	Scorre il display in su di una riga
PagGiù	Scorri pagina giù	Scorre il display in giù di una pagina

Tasto	Mappato a	Descrizione
PagSu	Scorri pagina su	Scorre il display in su di una pagina
Ctrl+A	Seleziona tutto	Seleziona tutto il testo
Maiusc+	Seleziona giù	Seleziona tutto il testo in basso
Maiusc+↑	Seleziona su	Seleziona tutto il testo in alto
Maiusc+←	Seleziona a sinistra	Seleziona tutto il testo a sinistra
Maiusc+→	Seleziona a destra	Seleziona tutto il testo a destra
‘	Inizio del messaggio	Inserisce un carattere di inizio messaggio nella posizione del cursore
F12	Statistiche	Visualizza le statistiche della comunicazione
Tab	Tab	Sposta il cursore nel successivo campo non protetto
Ctrl+F	Attiva/Disattiva CODACOM	Attiva/Disattiva la modalità CODACOM
Invio	Trasmetti	Trasmette la pagina all'host
Tastierino+Invio	Trasmetti	Trasmette la pagina all'host
Maiusc+Invio	Trasmetti	Trasmette la pagina all'host
Maiusc+Esc	Sblocca tastiera	Sblocca la tastiera
Ctrl+U	Messaggio non richiesto	Recupera un messaggio non richiesto dall'host

Configurare le macro utente

Utilizzare il pannello Macro per selezionare le macro da eseguire e quando eseguirle.

- **Esegui macro all'avvio** - Scegliere una macro da eseguire automaticamente quando si apre la sessione.
- **Esegui macro alla connessione** - Scegliere una macro da eseguire automaticamente quando la sessione si connette all'host.
- **Esegui macro alla disconnessione** - Scegliere una macro da eseguire automaticamente quando la sessione si disconnette.

Argomenti correlati

Creazione di macro
Utilizzo dell'API Macro
Macro di esempio

Trasferire file

Host Access for the Cloud supporta tre diversi tipi di protocollo di trasferimento dei file: IND$FILE per i trasferimenti con l'host 3270, AS/400 per i trasferimenti con l'host 5250 e File Transfer Protocol (FTP) che consente a un computer locale di fungere da client FTP. Una volta effettuata la connessione, è possibile visualizzare i file sul server e utilizzare il protocollo FTP per trasferire i file dal computer locale o da qualsiasi altra unità di rete al server FTP.

Per i trasferimenti FTP è disponibile Trasferimento file batch. Utilizzando questa opzione è possibile scaricare e caricare più file con un'unica operazione.

Per poter trasferire o inviare i file, è necessario che l'amministratore abbia attivato le opzioni di trasferimento e invio per la sessione corrente e definito le configurazioni necessarie. Questa operazione viene eseguita nel pannello Trasferimento file.

Le opzioni di configurazione disponibili dipendono dal file system host e dal metodo di trasferimento che si vuole utilizzare. Al termine della configurazione, la finestra di dialogo per il trasferimento file è disponibile tramite la barra degli strumenti.

- IND$FILE
- AS/400
- FTP
- Trasferimenti batch

IND$FILE

IND$FILE è un programma per il trasferimento file di IBM che può essere utilizzato per trasferire informazioni fra il computer dell'utente e un computer host 3270.

Nell'elenco a discesa **File system host** selezionare l'ambiente operativo IBM 3270 in esecuzione sull'host. Host Access for the Cloud supporta TSO (Time Sharing Option), CMS (Conversational Monitor System) e CICS. Il valore predefinito è Nessuno.

È disponibile il supporto per i trasferimenti ASCII o binari e, se si è connessi a un host TSO, è possibile passare direttamente a uno specifico set di dati TSO.

Opzioni generali per tipi di file host CICS, CMS, e TSO

Mostra automaticamente file host - Per impostazione predefinita, l'elenco dei file host contiene tutti i file host disponibili per il trasferimento. Per recuperare i file host solo quando richiesti, disabilitare questa opzione. Nella finestra di dialogo Trasferimento, fare clic su **Mostra file host** per recuperare i file host.

Opzioni di trasferimento per tipi di file host CICS, CMS, e TSO

Opzione	Descrizione
Metodo di trasferimento	◆ Binario Utilizzare questa opzione per i file di programma e altri tipi di file che non devono essere convertiti, ad esempio file che sono già stati formattati per un tipo di stampante particolare o file con formattazione specifica dell'applicazione. I file binari contengono caratteri non stampabili. Con questo metodo, i file non vengono convertiti durante il trasferimento. ◆ ASCII Utilizzare questa opzione per trasferire file di testo privi di una formattazione particolare. I file ASCII sul computer vengono convertiti nel set di caratteri EBCDIC sull'host e i file di testo dell'host vengono convertiti da EBCDIC ad ASCII quando vengono scaricati.
Elaborazione CR/LF	Se questa opzione è selezionata, le coppie di ritorno a capo - avanzamento riga verranno eliminate dai file inviati all'host e aggiunte alla fine di ogni riga nei file ricevuti dall'host.
Comando di avvio	Specifica il programma host utilizzato per avviare il trasferimento file. IND$File, l'impostazione predefinita, è adatto per host CMS e TSO. Per gli host CICS, IND$FILE può essere adeguato, oppure può essere necessario specificare la transazione CICS del sito (ad esempio, CFTR).
Parametri di avvio	Utilizzare questo campo per qualsiasi parametro specifico del programma IND$FILE sul sistema host in uso. I contenuti di questo campo vengono aggiunti alla fine del comando di trasferimento generato da Host Access for the Cloud. Host Access for the Cloud non convalida i parametri.
Dimensioni massime del campo	Selezionare una dimensione campo da utilizzare con il protocollo Write Structured Field. Il valore predefinito è 4 kilobyte. Di norma, a dimensioni più grandi del buffer corrisponde una maggior velocità di trasferimento. La maggior parte dei sistemi supporta 8K; se viene specificato un valore troppo grande per l'host in uso, la sessione in corso sarà disconnessa al primo tentativo di inviare un file sufficientemente grande da riempire il buffer. Questo valore viene di norma fornito dalla persona che installa il software di comunicazione dell'host. Ad esempio, il prodotto host TCP/IP di IBM ottiene questo valore dal parametro DATABUFFERPOOLSIZE, che assume buffer di 8K come impostazione predefinita. Contattare l'amministratore di sistema se non si è certi delle informazioni da immettere.
Tasto iniziale	È possibile specificare determinate azioni prima del trasferimento o dell'elencazione dei file. Le scelte disponibili sono Nessuno, Rilevamento automatico e Cancella. Se impostato su Nessuno, viene emesso automaticamente LISTCAT. Se impostato su Rilevamento automatico, i contenuti della schermata corrente vengono esaminati per determinare se inviare un LISTCAT o TSO LISTCAT. Se impostato su Cancella, il tasto CLEAR viene inviato prima di emettere un comando. Per TSO, Cancella significa inoltre che al comando di richiesta file non viene aggiunto il prefisso "TSO".
Tabella codici PC	Il set di caratteri da utilizzare per la lettura o la scrittura dei file locali durante un trasferimento file. Il valore **Predefinito** utilizza la tabella codici corrispondente alle impostazioni locali del sistema operativo. Se è richiesto un set di caratteri diverso per specificare la tabella codici PC, selezionarlo dall'elenco.

Opzione	Descrizione
Tabella codici dell'host	Il set di caratteri da utilizzare per la traduzione dei caratteri EBCDIC durante il trasferimento di file da o verso l'host. L'impostazione predefinita, **Usa impostazione NCS**, utilizza il set di caratteri nazionale specificato nel pannello Display, sotto Terminale. Se è richiesto un set di caratteri diverso per specificare la tabella codici host, selezionarlo dall'elenco.
Timeout risposta (secondi)	Specifica il numero di secondi che Host Access for the Cloud deve attendere per ricevere una risposta dell'host prima che raggiunga il timeout e che restituisca un errore. Il valore predefinito è 60 secondi.
Timeout avvio (secondi)	Specifica il numero di secondi che Host Access for the Cloud deve attendere per ricevere una risposta dell'host durante un tentativo di connessione a un host. Se il tempo specificato trascorre senza una risposta, Host Access for the Cloud raggiunge il timeout e restituisce un errore. Il valore predefinito è 25 secondi.

Opzioni di invio per tipi di file host CICS, CMS, e TSO

Opzione	Descrizione	Tipo di host interessato
Formato record	Utilizzare questa opzione per specificare il formato record per i file inviati all'host. ◆ Predefinito - l'host stabilisce il formato record. Questa è l'impostazione predefinita. ◆ Fisso - forza l'host a creare record a lunghezza fissa. ◆ Non definito - forza l'host a creare file che non hanno uno specifico formato di record (questa opzione ha rilevanza solo nei sistemi TSO). ◆ Variabile - forza l'host a creare record di lunghezza variabile e conservare il formato di un file binario.	TSO, CMS
Unità di allocazione	Specifica le partizioni del disco per l'allocazione primaria e secondaria di spazio. Se si seleziona Predefinito (impostazione predefinita), l'unità viene stabilita dall'host. Le opzioni disponibili sono Cilindro, Traccia o Blocco. Se si seleziona Blocco, utilizzare la casella Media blocco per specificare la dimensione di un blocco medio (in byte).	TSO
Lunghezza record logici	La dimensione record (in byte) del file creato sull'host. Se il campo viene lasciato vuoto, la dimensione del record viene stabilita dall'host. È possibile impostare qualsiasi valore compreso tra 0 e 32767 per accogliere qualsiasi gamma accettata dall'host. Questa opzione non è disponibile su host CICS. Nel caso di file ASCII, impostare il valore in modo che possa contenere la riga più lunga del file. Se la casella viene lasciata vuota, l'host in genere accetta righe sino a 80 caratteri.	TSO, CMS

Opzione	Descrizione	Tipo di host interessato
Se il file host esiste	Specifica come deve funzionare il trasferimento se esiste già un file con lo stesso nome. ◆ **Aggiungi** - aggiunge i contenuti del file locale al file host esistente. ◆ **Sovrascrivi** - sovrascrive i contenuti del file host. Con i sistemi CICS non è possibile sapere se esiste già un file host, pertanto Sovrascrivi è l'unica opzione disponibile per l'invio di file a un sistema CICS.	TSO, CMS
Dimensione blocco (byte)	Su host TSO, specifica la dimensione blocco del file creato sull'host. Nel caso di file con record a lunghezza fissa, questo valore deve essere un multiplo del valore impostato in Lunghezza record logici (poiché i blocchi sono suddivisi in record logici). È possibile impostare qualsiasi valore compreso tra 0 e 32767 per accogliere qualsiasi gamma accettata dall'host.	TSO
Media blocco (byte)	La dimensione di un blocco medio. Questo valore ha rilevanza solo se si utilizzano i blocchi come unità di allocazione.	TSO
Allocazione primaria (unità di allocazione)	La dimensione dell'allocazione primaria per il file host in corso di creazione.	TSO
Allocazione secondaria (unità di allocazione)	La dimensione di eventuali allocazioni aggiuntive nel caso in cui l'allocazione primaria non sia sufficiente. Sono consentite allocazioni secondarie multiple (chiamate "estensioni") sino a un numero massimo specificato dall'host (normalmente 15).	TSO

Nota: Quando si utilizza CICS come sistema host è necessario immettere manualmente i nomi dei file da trasferire. Non è disponibile un elenco dei file da cui scegliere.

Trasferimento di file

- Download di file
- Caricamento di file
- Risoluzione dei problemi di trasferimento file

Per trasferire i file per la sessione 3270 corrente, è necessario essere connessi e aver effettuato l'accesso all'host.

1. Verificare che lo stato dell'host sia "pronto" per accettare il comando IND$FILE.
2. Nella barra degli strumenti, fare clic sull'icona **IND$File**  .
3. Viene visualizzata la finestra Trasferimento file, che contiene un elenco di file e directory host disponibili per il trasferimento. Quando si seleziona un file, directory e file sono indicati da un'icona. Per gli host CICS, digitare i nomi dei file da trasferire.

4 Selezionare la modalità di trasferimento. Le opzioni sono:

- Binario

  Utilizzare questa opzione per i file di programma e altri tipi di file che non devono essere convertiti, ad esempio file che sono già stati formattati per un tipo di stampante particolare o file con formattazione specifica dell'applicazione. I file binari contengono caratteri non stampabili. Con questo metodo, i file non vengono convertiti durante il trasferimento.

- ASCII

  Utilizzare questa opzione per trasferire file di testo privi di una formattazione particolare. I file ASCII sul computer vengono convertiti nel set di caratteri EBCDIC sull'host e i file di testo dell'host vengono convertiti da EBCDIC ad ASCII quando vengono scaricati.

5 Se si è connessi a un host TSO, fare clic **Livello** per digitare il nuovo set di dati che si desidera visualizzare. Host Access for the Cloud aggiorna il file remoto utilizzando il livello del dataset specificato dall'utente.

Nota: Quando si specificano file utilizzando _Upload As_ o _Download_, i nomi completi di dataset devono essere racchiusi tra singoli apici. Ai nomi di dataset non racchiusi tra singoli apici vine aggiunto un prefisso con un qualificatore di alto livello specificato in TSO PROFILE.

È possibile aggiornare l'elenco di file in qualsiasi momento facendo clic sull'icona **Aggiorna** nell'angolo in alto a sinistra nella finestra di dialogo Trasferimento file.

Download di file

È possibile selezionare i file da scaricare nell'elenco dei file disponibili oppure utilizzare il pulsante **Download** per identificare un file specifico utilizzando il nome file dell'host.

1 Nell'elenco, selezionare il file per avviare il trasferimento facendo clic sul nome del file.

Oppure

2 Fare clic su **Download** e immettere il nome del file host da trasferire. È possibile scaricare da entrambi i tipi di host TSO e CMS. Tuttavia, TSO e CMS rappresentano i file host in modo diverso; questo significa che il formato del nome file immesso nel messasggio di richiesta sarà diverso.

- **TSO** - Racchiudere il nome del percorso host tra singoli apici per specificare il nome completo del dataset. Ad esempio, `'BVTST03.DATA.TXT'`. Per specificare un percorso file relativo al livello di dataset impostato sopra, omettere i singoli apici. Ad esempio, `DATA.TXT`, identifica lo stessso dataset ma relativamente a `BVTST03`.
- **CMS** - Un input CMS tipico potrebbe essere `BVTSTT01 DATA A1`. I singoli apici non sono necessari.

3 Se necessario, è possibile annullare il trasferimento nel pannello di avanzamento del trasferimento.

Caricamento di file

Nota: I sistemi di computer mainframe IBM impongono convenzioni di denominazione specifiche per i file. Per informazioni dettagliare sui requisiti dei nomi, vedere la documentazione IBM.

Sono disponibili due metodi per caricare i file:

1. Nella finestra di dialogo Trasferimento file, fare clic su **Carica**.
2. È possibile specificare un nome diverso per il file caricato. Fare clic su **Carica come**, individuare il file da caricare e, quando richiesto, digitare il nome da utilizzare. Ricordare che quando si è conessi a un host TSO, è necessario racchiudere i nomi completi di dataset tra singoli apici. Vedere il passaggio 5 sotto Trasferimento di file.

Oppure:

1. Trascinare il file da caricare dal percorso in cui si trova alla finestra di dialogo Trasferimento file.
2. Fare clic su **Aggiorna** per verificare che il file sia stato caricato.

Se si annulla il caricamento prima che il file sia trasferito completamente, nell'host rimarrà un file incompleto.

Risoluzione dei problemi di trasferimento file

È possibile che nel trasferimento dei file si verifichino errori. Questi errori possono essere causati da problemi del mainframe o da impostazioni di sicurezza del browser.

Se un trasferimento viene completato ma il file non contiene i dati previsti, verificare che il metodo di trasferimento sia impostato correttamente su Binario o ASCII.

Le operazioni di caricamento di file hanno un limite di dimensione dei file 50 MB. È possibile modificare questo valore.

Per errori specifici dell'host, vedere Messaggi di errore di trasferimento file IBM.

AS/400

Tramite il trasferimento file AS/400 è possibile trasferire i dati tra il computer e un host iSeries.

In genere, i trasferimenti file AS/400 sono intuitivi e non complessi. Tuttavia, poiché i dati dell'host vengono gestiti come database DB2, è possibile utilizzare l'editor SQL per creare query alquanto complesse.

Per configurare il trasferimento file AS/400

1. Creare una sessione di terminale HACloud 5250, immettere un nome o un indirizzo host e assegnare un nome alla sessione.
2. Nel pannello Impostazioni, scegliere **Trasferimento file**.
3. Selezionare **Enable AS/400 (Attiva AS/400)** e procedere con la configurazione.
   - **Host**

     L'indirizzo host fornito per la sessione di terminale è precompilato nel campo host. Se necessario, è possibile utilizzare un altro host. Per specificare un'altra porta, aggiungere il numero di porta all'indirizzo host. Ad esempio, `host.mycompany.com:23`.
   - **Sicurezza TLS/SSL**

Nell'elenco a discesa, selezionare l'opzione di sicurezza TLS che si desidera utilizzare. Per utilizzare questa opzione:

— È necessario aggiungere il certificato del server database AS/400 all'elenco dei certificati attendibili in MSS. Se il certificato non è già stato aggiunto, vedere Certificati attendibili nella documentazione relativa a MSS per istruzioni.

- **Metodo di trasferimento predefinito**

  Impostare il metodo di trasferimento predefinito desiderato; testo a larghezza fissa o CSV (Comma Separated Values). È possibile modificare il metodo di trasferimento durante l'esecuzione di un trasferimento.

4. Fare clic su Salva ed eseguire la connessione alla sessione.

Trasferimento di file

- Download di file
- Download tramite SQL
- Caricamento di file
- Aggiunta di una libreria

Una volta configurata la sessione per l'utilizzo della funzionalità di trasferimento file AS/400, fare clic su  nella barra degli strumenti per aprire la finestra di dialogo di trasferimento file. Questa finestra di dialogo contiene un elenco di file host disponibili per il trasferimento. Se richiesto, potrebbe essere necessario immettere le credenziali di login AS/400.

Download di file

Il file system AS/400 è costituito da librerie, file e membri. Le librerie vengono identificate tramite l'icona  . Sebbene non sia possibile scaricare le librerie, è possibile fare clic sulla libreria per visualizzare i file e i membri contenuti.

1. Aprire la libreria contenente i file ().
2. Espandere il file contenente il membro che si desidera scaricare.
3. Fare clic su un membro per scaricarlo.
4. Aprire la cartella di download del browser per verificare la presenza del file. Aprire il file in un editor di testo.

Download tramite SQL

È possibile creare query SQL per ottenere solo i dati necessari da un membro del file nell'host. In tal modo è possibile selezionare campi specifici e ignorarne altri.

1. Aprire la libreria e il file che si desidera scaricare.
2. Aprire il menu delle opzioni e fare clic su **SQL**.

3. Viene visualizzato l'editor SQL contenente l'istruzione SELECT utilizzata per scaricare l'intero membro. Al membro del file viene fatto riferimento come NOMELIBRERIA/NOMEFILE (NOMEMEMBRO).
4. Fare clic su **Run (Esegui)** per scaricare l'intero membro oppure modificare l'istruzione SQL e fare clic su Run (Esegui) per recuperare un sottoinsieme di dati.

Caricamento di file

È possibile caricare i dati nei file solo come membri nuovi o sostitutivi. Il file AS/400 contiene una specifica che descrive i dati contenuti nei membri e ciascun membro in un file dispone della stessa struttura. In genere, non è possibile (e non è consigliabile) scaricare un membro da un file e caricarlo in un altro file, a meno che entrambi i file non dispongano della stessa specifica. Poiché è possibile caricare i dati solo come membri, è necessario aprire un file e visualizzarne i membri nella finestra di dialogo dell'elenco file affinché venga abilitato il pulsante Carica.

1. Aprire il file che si desidera caricare. Il pulsante Carica è ora disponibile.
2. È possibile effettuare le seguenti operazioni:
   - Fare clic sul pulsante Carica e selezionare un file nel file system locale da caricare.

     oppure
   - Fare clic sulla freccia in basso sul pulsante Carica e selezionare Carica come..., quindi selezionare il file, assegnare un nuovo nome e fare clic su OK.

Aggiunta di una libreria

In genere, in qualità di utente AS/400, sarà possibile accedere a un insieme di librerie assegnato da un amministratore di sistema. Queste librerie vengono visualizzate come voci di primo livello nella finestra di dialogo di trasferimento file. Se è necessario accedere a una libreria non presente nell'elenco, l'amministratore di sistema può aggiornare la configurazione in modo che la nuova libreria venga aggiunta all'elenco. Talvolta potrebbe essere necessario utilizzare una libreria su base temporanea; non è necessario aggiungerla in modo permanente all'elenco di librerie.

Per aggiungere una libreria:

Nella finestra di dialogo di trasferimento file AS/400, fare clic su **Aggiungi libreria**. Questo pulsante è disponibile dal pannello dell'elenco di librerie. L'aggiunta non è permanente e sarà necessario aggiungere nuovamente la libreria se si chiude e si riapre la finestra di dialogo di trasferimento file.

FTP

Con Host Access for the Cloud il computer locale può fungere da client FTP. Con il client FTP è possibile eseguire la connessione a un server FTP in esecuzione in un altro computer. Una volta effettuata la connessione, è possibile visualizzare i file sul server e utilizzare FTP per trasferire i file tra il computer locale (o qualsiasi altra unità di rete) e il server FTP. Utilizzando FTP, un client può

caricare, scaricare, eliminare, rinominare, spostare e copiare file su un server, singolarmente o come trasferimento batch, opzione con cui è possibile creare elenchi di file da trasferire in un unica operazione.

Suggerimento: Se si prevede di usare un trasferimento batch, selezionare e configurare l'opzione **Attiva FTP**.

Per configurare FTP

Selezionare **Attiva FTP** e procedere con la configurazione:

- **Protocollo**

  Utilizzare FTP per avviare una sessione FTP standard. Utilizzare SFTP per avviare una sessione SFTP.

  È possibile configurare un client FTP per utilizzare il protocollo SFTP ed eseguire tutte le operazioni tramite il trasporto Secure Shell crittografato. Per l'autenticazione Host Access for the Cloud utilizza il nome utente e la password.

- **Host**

  Specificare il nome dell'host o l'indirizzo IP del server FTP al quale si desidera connettersi.

- **Porta**

  La porta del server FTP specificato.

- **Se il file remoto esiste quando si carica il file**

  Consente di specificare come gestire il trasferimento se esiste già un file con lo stesso nome. È possibile specificare le opzioni seguenti:

Opzione	Azione eseguita
Aggiungi	Aggiunge il file in corso di invio al file esistente.
Chiedi all'utente (impostazione predefinita)	Richiede una decisione sulla gestione del nome del file duplicato.
Annulla	Annulla il trasferimento del file.
Tralascia	Annulla il trasferimento del file e riceve una notifica dell'errore.
Sovrascrivi	Sovrascrive il file esistente nel computer remoto.
Ignora	Nel caso di una richiesta con più file, il file con un nome corrispondente a un file che esiste già viene ignorato e il trasferimento continua con gli altri file.
Univoco	Crea un nuovo file con un nome file univoco.

- **Directory remota iniziale**

  Consente di specificare il percorso di una home directory, o directory predefinita, per il sito FTP. Quando si stabilisce una connessione con il sito FTP, la directory di lavoro del server viene impostata automaticamente sul percorso della home directory specificato. I file e le cartelle

presenti nella home directory del server vengono visualizzati nella finestra della sessione FTP. Se la directory remota iniziale non è stata trovata, viene emesso un avviso e la connessione continua.

- **Utente Anonimo**

  Selezionare questa opzione per accedere al server FTP specificato come ospite, con il nome utente "Anonimo". Se l'host a cui si sta effettuando la connessione non supporta gli utenti anonimi è necessario fornire le proprie credenziali.

- **Timeout sessione (secondi)**

  Questo valore indica al client FTP il numero massimo di secondi di attesa per il trasferimento dei pacchetti di dati da o verso l'host. Se non si ricevono dati entro il periodo di tempo specificato, viene visualizzato un errore di timeout e il trasferimento termina; in tal caso, tentare nuovamente l'operazione. Se l'errore di timeout si ripete, aumentare il valore di timeout. Immettendo 0 (zero) in questa casella è possibile evitare il timeout del client FTP durante l'attesa di una risposta. Per le sessioni SFTP, il valore predefinito è 0 (zero).

- **Timeout keep alive (secondi)**

  Selezionare questa opzione e immettere un valore in secondi se si desidera continuare la connessione al server oltre il valore automatico di timeout per inattività del server. La maggior parte dei server ha un valore per il tempo di inattività che specifica la durata della sessione FTP di un utente quando non viene rilevata alcuna attività. Quando viene superato questo limite di tempo, la connessione al server viene chiusa.

  Questa impostazione consente di indicare al client FTP di inviare al server un comando NOOP a intervalli periodici per evitare che la connessione venga terminata per inattività. Se si continua la sessione, tuttavia , si potrebbe impedire a un altro utente di effettuare la connessione al server FTP.

- **Codifica host**

  Specifica il set di caratteri utilizzato dall'host per visualizzare i nomi dei file che vengono trasferiti. Di default Host Access for the Cloud utilizza UTF-8 (Unicode). Se si trasferiscono file con l'impostazione predefinita e i nomi dei file non sono riconoscibili, cambiare l'opzione Codifica host con il set di caratteri utilizzato dall'host. Questa opzione non influisce sulla codifica per i contenuti dei file che vengono trasferiti, ma si applica solo ai nomi dei file.

Trasferimento di file

Dopo che l'amministratore ha configurato una sessione per includere la funzionalità FTP, fare clic su  sulla barra degli strumenti per aprire la finestra Trasferimento file FTP che contiene un elenco dei file dell'host disponibili per il trasferimento. Quando si seleziona un file, directory e file sono indicati da un'icona.

1. Selezionare la modalità di trasferimento. Le opzioni sono:

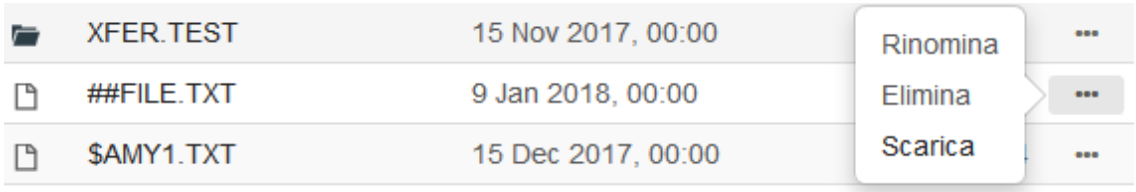
   - Binario

     Utilizzare questa opzione per i file di programma e altri tipi di file che non devono essere convertiti, ad esempio file che sono già stati formattati per un tipo di stampante particolare o file con formattazione specifica dell'applicazione. I file binari contengono caratteri non stampabili. Con questo metodo, i file non vengono convertiti durante il trasferimento.

- ASCII

  Utilizzare questa opzione per trasferire file di testo privi di una formattazione particolare. I file ASCII sul computer vengono convertiti nel set di caratteri EBCDIC sull'host e i file di testo dell'host vengono convertiti da EBCDIC ad ASCII quando vengono scaricati.

2 È possibile rinominare, eliminare o scaricare un file nell'elenco di file.



3 Aggiornare l'elenco di file in qualsiasi momento facendo clic sull'icona **Aggiorna** nell'angolo in alto a sinistra nella finestra di dialogo Trasferimento file.

Download di file

1 Nell'elenco, selezionare il file per avviare il trasferimento.

2 Se necessario, è possibile annullare il trasferimento nel pannello di avanzamento del trasferimento.

Caricamento di file

Sono disponibili due metodi per caricare i file:

1 Nella finestra di dialogo Trasferimento file, fare clic su **Carica**.

2 Scegliere il file da caricare nella finestra Sfoglia.

Oppure:

1 Trascinare il file da caricare dal percorso in cui si trova alla finestra di dialogo Trasferimento file.

2 Fare clic su **Aggiorna** per verificare che il file sia stato caricato.

Fare clic su **Nuova directory** per creare una nuova directory nel server remoto. Viene richiesto di immettere il nome della nuova directory.

Trasferimenti batch

Nota: Prima di configurare i trasferimenti batch è necessario abilitare FTP nel pannello Trasferimento file della scheda FTP.

Per trasferire più file in un'unica operazione, utilizzare l'opzione **Batch**.

1. In Impostazioni > Trasferimento file > pannello FTP, selezionare **Attiva FTP**.
2. Fare clic su FTP **BATCH** per aprire il pannello di trasferimento file **Batch**.
3. Selezionare **Annulla il batch quando si verifica un singolo errore** per arrestare il trasferimento se si verifica un errore durante il trasferimento di un file.

4. Fare clic su  per creare l'elenco di file da trasferire.
   a. Assegnare un nome all'elenco. Come aiuto per la creazione di elenchi simili, è possibile copiare un elenco esistente, ridenominarlo e aggiungere o eliminare i file necessari utilizzando le opzioni disponibili quando è evidenziato l'elenco originale.
   b. Nel pannello a destra, fare clic su  per aprire la finestra di dialogo **Aggiungi richiesta di trasferimento**.
5. Nel pannello **Aggiungi richiesta di trasferimento**, iniziare a creare l'elenco:

Opzione	Descrizione
Trasferimento	Scegliere se il file è da caricare o scaricare.
Nome file locale	Identifica il file da trasferire. È possibile immettere il nome del file da utilizzare o selezionarlo in un percorso.
Percorso file remoto	Fornire un percorso per assegnare un nome al file e archiviarlo dopo il trasferimento. È possibile: ◆ **Mantenere il nome file originale e utilizzare la directoryremota iniziale** - lasciare il campo vuoto ◆ **Utilizzare un nuovo nome file** - immettere `nuovonomefile.txt`. Inserisce il file nella directory remota iniziale utilizzando il nome specificato. ◆ **Mantenere il nome file originale, ma utilizzare un nuovo percorso di directory** - `/cartella/`. Utilizza il nome file originale con il nuovo percorso. ◆ **Utilizzare una nuova directory e un nuovo nome file** - `/cartella/nuovonomefile.txt`.
Metodo di trasferimento	È possibile scegliere il metodo di trasferimento Binario o ASCII.
Se il file remoto esiste	Decidere come gestire il trasferimento file se esiste già un file remoto con lo stesso nome. Le opzioni sono: ◆ Sovrascrivi (predefinita) - Sovrascrive il file esistente nel computer remoto. ◆ Aggiungi - Aggiunge il file in corso di invio al file esistente. ◆ Chiedi all'utente - Richiede una decisione sulla gestione del nome file duplicato. ◆ Annulla - Annulla il trasferimento del file. ◆ Tralascia - Annulla il trasferimento del file e invia una notifica dell'errore. ◆ Ignora - Il file con lo stesso nome di un file esistente viene ignorato, ma il trasferimento continua per gli altri file del batch. ◆ Unico - Crea un nuovo file con un nome file univoco.

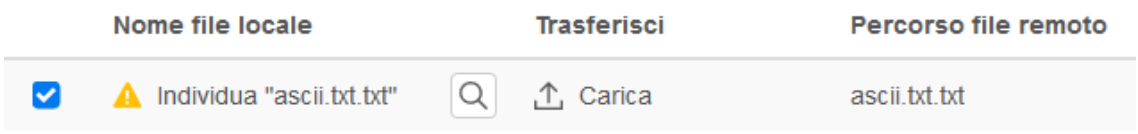
6. Fare clic su **Salva**.

Trasferimento di file

Suggerimento: Gli amministratori concedono l'autorizzazione per il trasferimento file utilizzando l'opzione **Regole di preferenze utente** nel pannello Impostazioni.

Fare clic su  nella barra degli strumenti per aprire l'elenco che contiene i file da trasferire.

1. A causa dei requisiti del browser, è necessario specificare il percorso di tutti i file da caricare. Individuare i file in base alle esigenze utilizzando l'icona Cerca. Questi file sono facilmente identificabili tramite un'icona gialla:



2. I file nell'elenco batch sono selezionati per impostazione predefinita. Per modificare il file prima del trasferimento, è possibile eliminare file dall'operazione di trasferimento deselezionado le rispettive caselle di controllo o selezionando **Tutto** dal menu a discesa. È inoltre possibile filtrare l'elenco dei file trasferibili in base al relativo stato di download o upload.
3. Fare clic su **Avvia** per iniziare il trasferimento.

Specificare le operazioni di copia e incolla

È possibile specificare diverse opzioni da utilizzare nelle operazioni di copia e incolla.

Opzioni di Copia

Selezionare il testo trascinando il mouse. Per impostazione predefinita, tipi di host diversi utilizzano modalità di selezione diverse quando si copia il testo: IBM 3270, 5250 e UTS utilizzano una modalità di selezione a blocco, mentre gli host VT utilizzano una modalità di selezione lineare. Per passare dalla modalità di selezione a blocco a quella lineare e viceversa, tenere premuto il tasto **Alt**, quindi selezionare il testo.

- **Copia solo campi di input** - Selezionare questa opzione per copiare solo i dati dai campi di input. Quando vengono salvati negli Appunti, i dati dei campi protetti vengono sostituiti da spazi.
- **Utilizza l'intero display quando non c'è alcuna selezione** - Questa opzione applica il comando Copia all'intero display del terminale quando non è selezionato testo.

Opzioni di Incolla

Fare clic su Incolla per incollare il contenuto degli Appunti in corrispondenza del cursore.

- **Ripristina la posizione iniziale del cursore dopo incolla**- Per impostazione predefinita, dopo un'operazione Incolla il cursore dell'host è posizionato alla fine dei dati. Selezionare questa opzione per ripristinare il cursore dell'host nella posizione iniziale al termine dell'operazione Incolla.
- **Maschera campi protetti** - Consente di specificare come mappare sullo schermo il testo incollato:

--Se l'opzione non è selezionata (impostazione predefinita), il testo viene interpretato come un flusso lineare che può contenere caratteri di fine riga e delimitatori e come tale viene incollato.

--Se l'opzione è selezionata, il testo viene interpretato come dati dello schermo host e sovrapposto allo schermo corrente iniziando dalla posizione corrente del cursore. Dove lo schermo corrente contiene un campo non protetto, il testo di origine viene incollato, mentre dove è presente un campo protetto il testo di origine viene ignorato.

Combinazioni di tasti

Sono presenti alcune combinazioni di tasti associate ad azioni di copia/incolla diverse.

Combinazione di tasti	Tipo di host	Azione
Ctrl+A	UTS, 3270, 5250	Seleziona tutto
Maiusc+FrecciaSu	UTS, 3270, 5250, VT	Modifica l'estensione della selezione corrente
Ctrl+C	UTS, 3270, 5250	Copia
Ctrl+V	UTS, 3270, 5250	Incolla
Ctrl+Maiusc+A	VT	Seleziona tutto
Ctrl+Maiusc+C	VT	Copia
Ctrl+Shift+V	VT	Incolla

Argomenti correlati

Operazioni di copia e incolla

Operazioni con le sessioni

Tutte le sessioni alle quali l'utente ha accesso sono disponibili nell'elenco **Sessioni disponibili**. Inizialmente, le sessioni vengono create e configurate dall'amministratore di sistema e l'accesso viene eseguito tramite un URL distribuito, ad esempio, https://<server di sessione>:7443.

- “Utilizzo del Tastierino comandi” a pagina 117
- “Operazioni di copia e incolla” a pagina 117
- “Disconnessione” a pagina 118

Per aprire una sessione

1. Selezionare la sessione e fare clic per aprirla.
2. Interagire con l'applicazione host utilizzando la sessione aperta.
3. È possibile creare più istanze di una sessione configurata.

È possibile avere più sessioni aperte contemporaneamente e passare facilmente da una all'altra utilizzando le schede disponibili nella parte superiore dello schermo. La sessione corrente è sempre la prima scheda a sinistra ed è indicata da sfondo bianco e testo in grassetto. Ogni sessione rimane attiva per 30 minuti.

Utilizzare la barra degli strumenti per accedere alle varie opzioni disponibili durante l'interazione con la sessione. È possibile disconnettersi da una sessione, chiudere la sessione, attivare il Tastierino comandi e accedere ad altre impostazioni. Alcune opzioni potrebbero essere disponibili solo dopo che l'amministratore ha concesso l'accesso.

Utilizzo del Tastierino comandi

Il Tastierino comandi è una rappresentazione grafica dei tasti di una tastiera host e fornisce accesso rapido ai tasti del terminale. Fare clic su un tasto del terminale sul Tastierino comando per inviare il tasto all'host. Passando su un tasto con il cursore del mouse viene visualizzata una descrizione della relativa mappatura.

Al Tastierino comandi, disponibile per ogni tipo di host supportato, si accede facendo clic sull'icona  nella barra degli strumenti.

Operazioni di copia e incolla

Nota: Ogni browser gestisce le funzioni di copia e incolla in modo diverso e in alcuni casi non supporta l'uso dei pulsanti copia e incolla della barra degli strumenti oppure del menu contestuale con il pulsante destro del mouse. Si consiglia di utilizzare i comandi da tastiera per queste funzioni. I comandi da tastiera dipendono dal sistema operativo. In Windows i comandi sono: **CTRL+C** per copiare e **CTRL+V** per incollare.

Si tratta di un problema più frequente della funzione incolla anziché copia. Se il pulsante Incolla della barra degli strumenti non è visibile, è probabile che la sicurezza del browser impedisca l'accesso in lettura agli appunti di sistema. I diversi browser si comportano in maniera diversa quando viene fornito l'accesso agli appunti. Tuttavia, incollare è quasi sempre disponibile mediante i comandi da tastiera, (CTRL + V in Windows e Command + V su Mac). Ciò presuppone che le chiavi non siano state rimappate. È inoltre possibile utilizzare il pulsante Incolla o la voce di menu integrata del browser.

Per copiare dal terminale

1. Sullo schermo del terminale, selezionare l'area da copiare.
2. Fare clic su **Copia** dalla barra degli strumenti o selezionare **Copia** dal menu contestuale del tasto destro del mouse disponibile nella schermata del terminale. In alternativa, è possibile utilizzare il comando della tastiera **CTRL + C**.

Per incollare nello schermo del terminale

1. Posizionare il cursore nel punto in cui incollare il contenuto.
2. Se il browser supporta la funzione Incolla, fare clic su **Incolla** dalla barra degli strumenti o selezionare **Incolla** dal menu contestuale del tasto destro del mouse disponibile nella schermata del terminale. Se il browser in uso non supporta questa funzione, queste opzioni non sono disponibili ed è necessario utilizzare il comando tastiera, **CTRL + V**.

Argomenti correlati

Specificare le operazioni di copia e incolla

Disconnessione

Nell'angolo superiore destro dello schermo, aprire l'elenco a discesa associato al nome utente e selezionare **Disconnetti** per interrompere le operazioni con l'applicazione host.

Creazione di macro

Una macro è una serie di azioni della tastiera che è possibile registrare e quindi eseguire. È possibile utilizzare i programmi macro JavaScript per automatizzare le interazioni dell'utente con il terminale. È possibile accedere alle macro ed eseguirle da tutti i dispositivi supportati.

Host Access for the Cloud registra e salva le macro avanzate come JavaScript, semplificando le attività di modifica e miglioramento delle macro registrate. È possibile registrare macro da eseguire in un secondo momento, eseguire macro all'avvio quando la sessione si connette all'host oppure quando si disconnette. È inoltre possibile scrivere macro da zero per eseguire attività complesse che il registratore non è in grado di catturare.

Le macro vengono rese disponibili agli utenti in due modi: create dall'amministratore o registrate dagli utenti stessi per il proprio utilizzo personale. Tutte le macro avanzate sono associate a una sessione e hanno tutte lo stesso obiettivo, ovvero automatizzare l'interazione con l'host. L'unica differenza è costituita semplicemente da quali utenti le possono utilizzare e chi ne gestisce la creazione e la disponibilità:

- **Macro create dagli amministratori**

  Gli amministratori creano le macro quando creano le sessioni. Le macro sono specifiche per una sessione e sono disponibili per tutti gli utenti che hanno accesso alla sessione tramite l'icona Macro nella barra degli strumenti. Gli amministratori possono impostare le macro per essere eseguite all'avvio, quando la sessione si connette all'host oppure quando si sconnette.

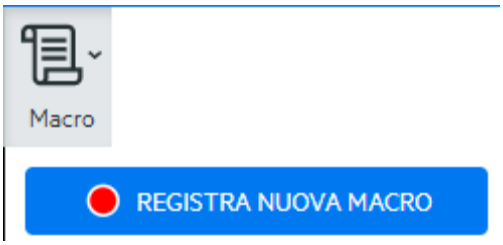
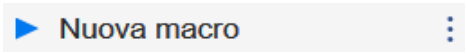
- **Macro create dagli utenti**

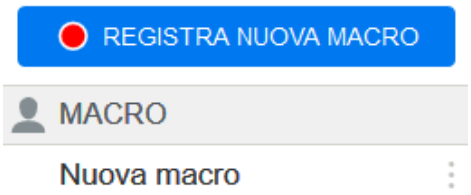
  Le macro degli utenti finali sono create dai singoli utenti per le sessioni alle quali sono autorizzati ad accedere. Gli amministratori concedono le autorizzazioni per creare le macro tramite un'impostazione in Regole di preferenze utente. Gli utenti possono accedere alla sessione con le proprie credenziali o con il ruolo **Guest**. Le macro create dagli utenti Guest sono disponibili per tutti gli utenti Guest. Gli utenti che hanno effettuato l'accesso con le proprie credenziali possono vedere solo le macro create da loro stessi.

Le macro avanzate sono riportate in ordine alfabetico nell'elenco a discesa disponibile nella barra degli strumenti. Le macro create dall'utente finale sono riportate per prime e sono seguite da un indicatore formato da tre punti verticali di colore grigio che, quando selezionato, visualizza le opzioni Modifica ed Elimina. Le macro create dall'amministratore sono riportate senza l'indicatore poiché non possono essere modificate dall'utente finale.

Utilizzo delle macro

Registrazione, modifica e riproduzione delle macro.

Operazione	Procedura
Registrazione	1. Fare clic sull'icona Macro nella barra degli strumenti, quindi fare clic su **Registra nuova macro**.  2. Spostarsi nell'applicazione host per registrare la serie di passaggi da includere nella macro. 3. Fare clic su nella barra degli strumenti per interrompere la registrazione. Il pallino rosso lampeggia per indicare che è in corso la registrazione. 4. Quando richiesto, digitare il nome per la macro.
Modifica	1. Nell'elenco a discesa Macro, selezionare la macro da modificare.  2. Fare clic sui tre punti verticali per espandere il campo. 3. Fare clic su Modifica per aprire l'Editor di macro. L'Editor di macro si apre nel pannello a sinistra. 4. Utilizzare JavaScript per apportare le modifiche necessarie. È possibile eseguire e salvare la macro modificata utilizzando le icone nella barra degli strumenti nel pannello superiore dell'editor.
Esecuzione	Per eseguire una macro, scegliere la macro nell'elenco a discesa e fare clic su . È anche possibile mappare dei tasti che attivano automaticamente una macro già registrata. Nella finestra di dialogo delle impostazioni per la mappatura dei tasti, scegliere **Esegui macro** nell'elenco a discesa **Azione**. Scegliere una macro da associare con la mappatura del tasto nell'elenco **Valore**.
Arresto	È possibile interrompere una macro prima che sia completata nell'Editor di macro o nella barra degli strumenti. Fare clic su per interrompere la macro. Per eseguire nuovamente la macro, tornare alla schermata iniziale delle macro.

Operazione	Procedura
Eliminazione	1. Nell'elenco a discesa Macro, selezionare la macro da eliminare. 2. Espandere il campo facendo clic sull'icona con i tre punti verticali.  3. Fare clic su **Elimina**.
Visualizzazione	L'elenco a discesa Macro è disponibile dalla barra degli strumenti per tutti gli utenti che sono autorizzati a registrare le macro o che accedono a una sessione in cui le macro sono state registrate precedentemente dall'amministratore per essere utilizzate nella sessione. Le macro sono elencate in **MACRO PERSONALI** o **MACRO** in base al tipo di registrazione. Tutti gli utenti, sia che abbiano effettuato l'accesso utilizzando le proprie credenziali o come Guest, possono vedere le macro associate alla sessione. Le macro elencate in MACRO PERSONALI sono riportate in ordine alfabetico in base al nome e sono visibili agli utenti che le hanno registrate. Le macro registrate dall'amministratore e allegate a una sessione sono elencate in ordine alfabetico sotto MACRO.

Debug delle macro

Poiché le macro sono scritte con JavaScript ed eseguite nel browser, il modo migliore per effettuare il debug e risolvere gli errori consiste nell'utilizzare gli strumenti incorporati nel browser Web. I browser più recenti sono dotati di set di strumenti avanzati per il debug di codice JavaScript. È possibile inserire punti di interruzione, eseguire il codice un'istruzione alla volta e visualizzare informazioni sul debug.

Suggerimento: JavaScript distingue tra maiuscole e minuscole. Tenere presente questa informazione quando si modifica codice JavaScript.

Per eseguire il debug di una macro:

1. Aprire la macro per la modifica. Per ulteriori istruzioni, vedere Utilizzo delle macro.
2. Aprire gli strumenti di sviluppo del browser.

Tabella 5-10 *Supporto del debug tramite browser*

Browser	Aprire il debugger
Mozilla Firefox 40.0.3	◆ Nella barra degli strumenti, aprire il menu e scegliere Sviluppo. ◆ Nel menu Sviluppo web, scegliere Debugger. Il debugger si apre nel pannello inferiore.
Google Chrome 45.0	◆ Nella barra degli strumenti, aprire il menu e scegliere Altri strumenti. ◆ Scegliere Strumenti per sviluppatori per aprire il debugger.
Microsoft Internet Explorer 11	◆ Nella barra degli strumenti, aprire Strumenti e scegliere Strumenti di sviluppo (F12). ◆ Verrà aperta la scheda Debugger.

Queste istruzioni fanno riferimento ai browser supportati e dipendono dalle versioni utilizzate.

3. Utilizzare uno di questi strumenti nel codice delle macro ed eseguire il codice.
   - *debugger*

     L'approccio più accurato per il debug consiste nell'utilizzo dell'istruzione "debugger". Quando si inseriscono queste istruzioni nel codice della macro e la si esegue, quando sono aperti gli strumenti di debug del browser l'esecuzione della macro si interrompe a ognuna delle righe che le contengono. È possibile eseguire la macro un'istruzione alla volta, visualizzare il valore delle variabili locali e altre informazioni che è necessario verificare.

     È consigliabile inserire nel codice più istruzioni debugger; per consentire di raggiungere la riga richiesta. La natura asincrona di JavaScript può rendere difficoltosa l'esecuzione del codice un'istruzione alla volta. Questo aspetto può essere ovviato utilizzando più istruzioni debugger; posizionate opportunamente.

     Example 5-1 *Debugger*

     ```
     ---------------------
     var hostCommand = menuSelection + '[enter]';
     debugger;  // <— Browser's debugger will stop here
     ps.sendKeys(hostCommand);
     ---------------------
     ```

   - `console.log(), alert()`

     Queste due funzioni sono utilizzate comunemente per il debug in JavaScript. Sebbene non offrano la stessa flessibilità dell'istruzione debugger, forniscono un modo veloce per visualizzare le informazioni di debug. Queste funzioni visualizzano le informazioni nella scheda "Console" di JavaScript negli strumenti per sviluppatori del browser.

Example 5-2 *console.log(), alert()*

```
---------------------
var hostCommand = menuSelection + '[enter]';
console.log('Command:' + hostCommand);  // <— Will output the string
to "Console" tab
alert('Command:' + hostCommand); // Will pop up a small window
containing the data
ps.sendKeys(hostCommand);
---------------------
```

- `ui.message()`

  L'API Host Access for the Cloud fornisce una funzione ui.message() molto simile alla funzione alert() di JavaScript. È anche possibile utilizzare ui.message() per visualizzare le informazioni di debug.

Example 5-3 *ui.message()*

```
---------------------
var hostCommand = menuSelection + '[enter]';
ui.message('Command:' + hostCommand);  // <— Will pop up a message
window
ps.sendKeys(hostCommand);
---------------------
```

Tenere presente:

- Esecuzione del codice e istruzioni yield

  Sebbene le istruzioni yield nelle macro rendano le macro più facilmente comprensibili, possono rendere più complessa l'esecuzione del codice un'istruzione alla volta con il debugger. Considerare la possibilità di utilizzare più istruzioni debugger o inserire opportunamente istruzioni debugger di chiamate `console.log()` per visualizzare le informazioni di debug corrette.

- Internet Explorer

  Il debugging in Internet Explorer prevede codice trasformato e può risultare più complesso che con altri browser.

Utilizzo dell'API Macro

In Host Access for the Cloud le macro vengono registrate e scritte utilizzando JavaScript. JavaScript è un linguaggio di programmazione molto comune e diffuso. È disponibile un'ampia gamma di risorse per l'apprendimento e di strumenti.

L'API Macro consiste in un set di oggetti che possono essere utilizzati per interagire con l'host, attendere gli stati delle schermate e interagire con l'utente.

Informazioni su promesse e istruzioni yield

Poiché JavaScript è un linguaggio a thread singolo e utilizza "funzioni di callback" e "promesse" per gestire il flusso di esecuzioni attraverso il codice, spesso seguire il codice può risultare difficile. Host Access for the Cloud unisce il concetto di "promessa" con la parola chiave "yield" affinché il codice delle macro possa essere organizzato in modo più lineare.

- **Promesse**

  Le promesse sono modelli che consentono di semplificare funzioni che, ad un certo punto, restituiscono risultati in modo asincrono. Tutte le funzioni "wait" e "ui" nell'API Macro restituiscono oggetti di tipo promessa.

- **Yield**

  Le macro utilizzano la parola chiave yield per bloccare la loro esecuzione fino a quando non viene risolta o completata una promessa. Quindi anteporre yield alle funzioni "wait" o "ui" mette in pausa l'esecuzione della macro fino a quando la funzione è stata eseguita. È possibile inserire la parola chiave yield prima di qualsiasi funzione che restituisce una promessa, anche davanti alle funzioni personalizzate.

Nota: La capacità di bloccare l'esecuzione della macro combinando yield con la promessa è attivata dalla funzione `createMacro()`.

Errori

Nelle macro gli errori vengono gestiti utilizzando un'istruzione try/catch. Alcune funzioni API possono generare errori se, ad esempio, non è possibile soddisfare le condizioni o se si verifica un timeout. L'errore generato viene rilevato nell'istruzione catch. È possibile eseguire il wrapping di blocchi di codice più piccoli in un'istruzione try/catch per gestire gli errori a un livello più granulare. Gli sviluppatori di macro possono anche generare errori con `'throw new Error('Messaggio di errore utile');`

Argomenti correlati

- “Oggetti dell'API Macro” a pagina 123
- “Macro di esempio” a pagina 153

Oggetti dell'API Macro

È possibile creare macro utilizzando l'API Macro. Per impostazione predefinita sono disponibili quattro oggetti principali da utilizzare nelle macro:

- Session

  Session è il punto di ingresso principale per accedere all'host. L'oggetto Session viene utilizzato per connettere, disconnettere e fornire accesso all'oggetto PresentationSpace.

- PresentationSpace

  L'oggetto PresentationSpace rappresenta lo schermo e fornisce molte capacità comuni, ad esempio ottenimento e impostazione della posizione del cursore, invio di dati all'host e lettura dello schermo. Viene ottenuto chiamando `session.getPresentationSpace()`.

- Wait

Fornisce un modo semplice per attendere che si verifichino i vari stati dell'host prima di continuare a inviare altri dati o a leggere dallo schermo. Ad esempio, è possibile attendere che il cursore si trovi in una determinata posizione, che il testo sia presente in una certa posizione sullo schermo o attendere semplicemente che trascorra un periodo di tempo fissato. Tutte le funzioni "wait" richiedono la parola chiave yield, spiegata più avanti.

- User Interface

  L'oggetto UI è reso disponibile automaticamente nella macro come variabile "ui". Fornisce capacità di interfaccia utente di base. È possibile utilizzare questo oggetto per mostrare i dati all'utente o richiedergli informazioni. Tutte le chiamate alla funzione "UI" richiedono la parola chiave yield.

Altri oggetti disponibili

- Attribute
- AttributeSet
- Colore
- ControlKey
- DataCell
- Dimension
- Field
- FieldList
- FileTransferFactory
- FileTransfer
- HostFile
- Tipo file host
- Opzioni di trasferimento file
- OIA
- OIAStatus
- AutoSignon
- Position
- PresentationSpace
- Session
- SessionType
- StatusSet
- User Interface
- Wait

Attribute

Utilizzare l'oggetto Attribute, insieme ad AttributeSet, per decodificare le informazioni di formattazione presenti nella cella dati.

Tabella 5-11 *Attributi*

Attributo	Descrizione
PROTECTED	Indica una cella dati protetta.
MODIFIED	Indica una cella dati modificata.
NUMERIC_ONLY	Indica l'inizio di una cella dati esclusivamente numerica.
ALPHA_NUMERIC	Indica una cella dati alfanumerica.
HIGH_INTENSITY	Indica se la cella dati contiene testo ad alta intensità.
HIDDEN	Indica se la cella dati contiene testo nascosto.
PEN_DETECTABLE	Indica se la cella dati è rilevabile dalla penna ottica.
ALPHA_ONLY	Indica una cella dati esclusivamente alfabetica.
NUMERIC_SHIFT	Indica l'inizio di un campo di spostamento numerico. con tasto MAIUSC
NUMERIC_SPECIAL	Indica che la cella dati contrassegna l'inizio di un campo numerico speciale.
KATAKANA_SHIFT	Indica una sezione di testo Katakana.
MAGNETIC_STRIPE	Indica che la cella dati contrassegna l'inizio di un campo banda magnetica.
SIGNED_NUMERIC_ONLY	Indica che la cella dati è un campo numerico di tipo signed.
TRANSMIT_ONLY	Indica che la cella dati è un campo di sola trasmissione.
FIELD_END_MARKER	Indica che la cella dati contrassegna la fine di un campo modificato.
FIELD_START_MARKER	Indica che la cella dati contrassegna l'inizio di un campo modificato.
SPECIAL_EMPHASIS_PROTECTED	Indica un campo protetto con enfasi speciale.
TAB_STOP	Indica che la cella dati contiene un arresto di tabulazione.
REVERSE	Indica che la cella dati visualizza in modalità video inverso.
BLINKING	Indica che la cella dati contiene testo intermittente.
RIGHT_JUSTIFIED	Indica che la cella dati contrassegna l'inizio di un campo con giustificazione a destra.
LEFT_JUSTIFIED	Indica che la cella dati contrassegna l'inizio di un campo con giustificazione a sinistra.
LOW_INTENSITY	Indica che la cella dati contiene testo a bassa intensità.
UNDERLINE	Indica che la cella dati contiene testo sottolineato.
DOUBLE_BYTE	Indica che la cella dati contiene testo a doppio byte.
COLUMN_SEPARATOR	Indica che la cella dati contiene un separatore di colonna.
BOLD	Indica che la cella dati contiene testo in grassetto.
DOUBLE_WIDTH	Indica che la cella dati contrassegna un campo a doppia larghezza.

Attributo	Descrizione
DOUBLE_HEIGHT_TOP	Indica una cella dati superiore a doppia altezza.
DOUBLE_HEIGHT_BOTTOM	Indica una cella dati inferiore a doppia altezza.
CONTROL_PAGE_DATA	Indica che la cella dati contiene dati pagina di controllo.
RIGHT_COLUMN_SEPARATOR	Indica che la cella dati contiene un separatore di colonna a destra.
LEFT_COLUMN_SEPARATOR	Indica che la cella dati contiene un separatore di colonna a sinistra.
UPPERSCORE	Indica che la cella dati contiene un sopralineato.
STRIKE_THROUGH	Indica che la cella dati contiene testo barrato.

AttributeSet

L'oggetto AttributeSet consente all'utente di decodificare gli attributi presenti nella cella dati. L'oggetto AttributeSet restituisce i valori definiti nell'oggetto Attribute e, quando utilizzati insieme, è possibile ottenere informazioni sulla formattazione dalla cella dati.

Tabella 5-12 *AttributeSet*

METODI

`contains(attribute)`	Determina se il set contiene l'Attribute specificato.
	Parametri
	`{Number}` attributo da verificare
	Restituisce
	`{Boolean}` True se l'attributo è presente nel set.
`isEmpty()`	Determina se il set di attributi è vuoto.
	Restituisce
	`{Boolean}` True se il set è vuoto.
`size()`	Indica il numero di attributi in un set.
	Restituisce
	`{Number}` Il numero di attributi.
`toArray()`	Converte il set di attributi interno in una matrice.
	Restituisce
	`{Number[]}`Matrice dei valori degli attributi nel set.
`toString()`	Converte il set di attributi interno in una stringa.
	Restituisce
	`{String}` Nomi delimitati da spazi degli attributi nel set.

METODI

`forEach(callback, thisArg)`	Funzione per reiterare ogni elemento nel set di attributi. **Parametri** `{forEachCallback}` Callback per eseguire l'operazione specifica. Chiamato con il nome di ogni attributo nel set. `{Object}` puntatore Arg facoltativo a un oggetto di contesto.
`forEachCallback(string, object)`	Una funzione di callback fornita dall'utente in cui fornire il comportamento, da usare come parametro di callback per forEach. **Parametri** `{String}` `String` nome dell'attributo nel set di attributi. `{Object}` `thisArg` puntatore facoltativo a un oggetto di contesto.

Colore

Costanti di colore da usare per i colori di primo piano e sfondo dell'oggetto DataCell.

Tabella 5-13 *Costanti di colore*

Colore	Descrizione	Valore numerico
BLANK_UNSPECIFIED	Nessun colore specificato	0
BLUE	Blu	1
GREEN	Verde	2
CYAN	Ciano	3
RED	Rosso	4
MAGENTA	Magenta	5
YELLOW	Giallo	6
WHITE_NORMAL_INTENSITY	Bianco con intensità normale	7
GRAY	Grigio	8
LIGHT_BLUE	Blu chiaro	9
LIGHT_GREEN	Verde chiaro	10
LIGHT_CYAN	Ciano chiaro	11
LIGHT_RED	Rosso chiaro	12
LIGHT_MAGENTA	Magenta chiaro	13
BLACK	Nero	14
WHITE_HIGH_INTENSITY	Bianco con intensità alta	15
BROWN	Marrone	16

Colore	Descrizione	Valore numerico
PINK	Rosa	17
TURQUOISE	Turchese	18

ControlKey

L'oggetto ControlKey definisce le costanti per inviare i tasti di controllo del cursore e i comandi dell'host utilizzando il metodo sendKeys. Sono disponibili costanti per i tipi di host seguenti:

- IBM 3270
- IBM 5250
- VT
- UTS

IBM 3270

Tabella 5-14 *IBM 3270*

Parola chiave	Descrizione
ALTVIEW	Alterna visualizzazione
ATTN	Attenzione
BACKSPACE	Backspace
BACKTAB	Tab indietro
CLEAR	Cancella o cancella display
CURSOR_SELECT	Selezione cursore
DELETE_CHAR	Elimina, elimina carattere
DELETE_WORD	Elimina parola
DEST_BACK	Backspace distruttivo
DEV_CANCEL	Annulla dispositivo
DOWN	Cursore giù
DSPSOSI	Visualizza SO/SI
DUP	Duplica campo
END_FILE	Fine del campo
ENTER	Invio
ERASE_EOF	Cancella fino a fine del campo
ERASE_FIELD	Cancella campo
ERASE_INPUT	Cancella input
FIELD_MARK	Field Mark

Parola chiave	Descrizione
HOME	Cursore in posizione Home
IDENT	Identità
INSERT	Inserisci
LEFT_ARROW	Cursore a sinistra
LEFT2	Due posizioni verso sinistra
NEW_LINE	Nuova riga
PA1 - PA3	PA1 - PA3
PF1 - PF24	PF1 - PF24
PAGE_DOWN	Pagina giù
PAGE_UP	Pagina su
RESET	Ripristina, ripristina terminale
RIGHT2	Due posizioni verso destra
RIGHT_ARROW	Cursore a destra, destra
SYSTEM_REQUEST	Richiesta di sistema
TAB	Tasto tabulazione
UP	Cursore su

IBM 5250

Tabella 5-15 *IBM 5250*

Parola chiave	Descrizione
ALTVIEW	Alterna visualizzazione
ATTN	Attenzione
AU1 - AU16	AU1 - AU16
BACKSPACE	Backspace
BACKTAB	Tab indietro
BEGIN_FIELD	Inizio campo
CLEAR	Elimina
DELETE_CHAR	Elimina, elimina carattere
DEST_BACK	Backspace distruttivo
DOWN	Cursore giù
DSPSOSI	Visualizza SO/SI

Parola chiave	Descrizione
DUP	Duplica campo
END_FILE	Fine del campo
ENTER	Invio
ERASE_EOF	Cancella fino a fine del campo
ERASE_FIELD	Cancella campo
ERASE_INPUT	Cancella input
FIELD_EXT	Uscita campo
FIELD_MINUS	Campo meno
FIELD_PLUS	Campo più
FIELD_MARK	Field Mark
HELP	Richiesta guida
HEXMODE	Modalità esadecimale
HOME	Cursore in posizione Home
INSERT	Inserisci
LEFT_ARROW	Cursore a sinistra
NEW_LINE	Nuova riga
PA1 - PA3	PA1 - PA3
[PF1 - PF24	PF1 - PF24
[print]	Stampa
RESET	Ripristina, ripristina terminale
RIGHT_ARROW	Cursore a destra, destra
PAGE_UP	Pagina su
PAGE_DOWN	Pagina giù
SYSTEM_REQUEST	Richiesta di sistema
TAB	Tabulazione
UP	Cursore su

VT

Tabella 5-16 *VT*

Parole chiave	Descrizione
BACKSPACE	Backspace

Parole chiave	Descrizione
BREAK	Interruzione
CLEAR	Cancella o cancella display
CURSOR_SELECT	Selezione cursore
DELETE_CHAR	Elimina, elimina carattere
DOWN	Cursore giù
EK_FIND	Modifica ricerca tastierino
EK_INSERT	Modifica inserimento tastierino
EK_NEXT	Modifica tastierino successivo
EK_PREV	Modifica tastierino precedente
EK_REMOVE	Modifica rimozione tastierino
EK_SELECT	Modifica selezione tastierino
ENTER	Invio
END_FILE	Fine del campo
F1 - F24	F1 - F24
HOLD	In attesa
HOME	Home
INSERT	Ins
KEYPAD_COMMA	Virgola tastierino
KEYPAD_DOT	Decimale tastierino
KEYPAD_MINUS	Meno tastierino
KEYPAD_ENTER	Invio tastierino
KEYPAD0 - KEYPAD9	0 tastierino - 9 tastierino
LEFT_ARROW	Cursore a sinistra
PF1 - PF20	PF1 - PF20
PAGE_DOWN	Pagina giù
PAGE_UP	Pagina su
RESET	Ripristina, ripristina terminale
RETURN	Invio, ritorno a capo
RIGHT_ARROW	Cursore a destra, destra
TAB	Tasto tabulazione
UDK16 - UDK20	Tasto 6 definito dall'utente - Tasto 20 definito dall'utente
UP	Cursore su

UTS

Tabella 5-17 *UTS*

Parola chiave	Descrizione
BACKSPACE	Sposta il cursore alla posizione di tabulazione precedente sullo schermo.
BACKTAB	Tab indietro <Shift> <Tab>
CHAR_ERASE	Cancella il carattere nella posizione del cursore e sposta il cursore in avanti.
CLEAR_DISPLAY	Cancella il display
CLEAR_EOD	Cancella fino a fine display
CLEAR_EOF	Cancella fino a fine campo
CLEAR_EOL	Cancella fino a fine riga
CLEAR_FCC	Cancella il carattere di controllo del campo
CLEAR_HOME	Cancella il contenuto del display e porta il cursore in posizione Home
CONTROL_PAGE	Attiva/Disattiva la pagina di controllo
DELETE_LINE	Elimina la riga che contiene il cursore e sposta di una riga in alto le righe rimanenti
DOWN	Sposta il cursore in basso di una riga. A capo in fondo.
DELIN_LINE	Elimina il carattere nella posizione del cursore e sposta a sinistra i caratteri rimanenti sulla riga.
DELIN_PAGE	Elimina il carattere nella posizione del cursore e sposta a sinistra i caratteri rimanenti sulla pagina.
DUP_LINE	Crea una copia della riga corrente e sovrascrive la riga successiva con il duplicato.
EURO	Inserisce il carattere Euro
END_FIELD	Sposta il cursore alla fine del campo corrente.
END_PAGE	Sposta il cursore alla fine della pagina corrente.
F1 - F22	Tasti funzione F1-F22
HOME	Sposta il cursore all'inizio della pagina corrente (riga 1, colonna 1)
INSERT	Attiva/Disattiva la modalità inserimento/sovrascrittura.
INSERT_IN_LINE	Inserisce uno spazio alla posizione del cursore e sposta a destra i caratteri rimanenti sulla riga. Il carattere nella colonna all'estrema destra della riga viene rimosso.

Parola chiave	Descrizione
INSERT_IN_PAGE	Inserisce uno spazio alla posizione del cursore e sposta a destra i caratteri rimanenti sulla pagina. Il carattere nella colonna all'estrema destra di ogni riga viene rimosso.
INSERT_LINE	Inerisce una nuova riga nella riga del cursore e sposta in basso le righe rimanenti. L'ultima riga nella pagina viene rimossa.
LEFT_ARROW	Sposta il cursore di una posizione a sinistra e sposta a capo se necessario.
LOCATE_FCC	Trova il carattere di controllo del campo successivo sullo schermo.
MSG_WAIT	Recupera i messaggi in coda al terminale.
RETURN	A capo
RIGHT_ARROW	Sposta il cursore di una posizione a destra e sposta a capo se necessario.
SOE	Inserisce il carattere di inizio immissione
START_OF_FIELD	Sposta il cursore all'inizio del campo.
START_OF_LINE	Sposta il cursore alla colonna 1 della riga corrente.
TAB	Sposta il cursore alla posizione di tabulazione successiva sullo schermo.
TOGGLE_COL_SEP	Attiva/Disattiva l'attributo del separatore di colonna.
TOGGLE_STRIKE_THRU	Attiva/Disattiva l'attributo di testo barrato sulla cella dati corrente.
TOGGLE_UNDERLINE	Attiva/Disattiva l'attributo di testo sottolineato sulla cella dati corrente.
TRANSMIT	Trasmette i dati dei campi cambiati all'host.
UNLOCK	Invia il tasto UNLOCK all'host.
UP	Sposta il cursore in alto di una riga, a capo se necessario.

DataCell

L'oggetto DataCell fornisce informazioni su una posizione particolare su uno schermo di terminale.

Tabella 5-18 *DataCell*

METODI

`getPosition()` Restituisce la posizione di questa cella dati sullo schermo.

Restituisce

`{Position}` la posizione della cella dati sullo schermo

METODI	
`getChar()`	Ottiene il carattere associato alla cella. **Restituisce** `{String}` Il carattere associato alla cella.
`getAttributes()`	Restituisce il set di attributi specificato per questa istanza della cella dati. Vedere AttributeSet. **Restituisce** `{AttributeSet}`Di attributi per questa istanza della cella dati.
`getForegroundColor()`	Restituisce il colore del primo piano, come definito nell'oggetto Color, per questa cella dati. **Restituisce** `{Number}`Colore dello sfondo per questa cella dati. Il colore è definito nell'oggetto Colore.
`getBackgroundColor()`	Restituisce il colore dello sfondo, come definito nell'oggetto Color, per questa cella dati. **Restituisce** `{Number}`Colore dello sfondo per questa cella dati. Il colore è definito nell'oggetto Colore.
`toString`	Converte la cella dati interna in una stringa. **Restituisce** `{String}` La rappresentazione sotto forma di stringa di una cella dati.
`isFieldDelimiter()`	Verifica se questa cella rappresenta un delimitatore di campo. **Restituisce** `{Boolean} True se la cella è un delimitatore di campo, altrimenti, false.`

Dimension

Rappresenta le dimensioni dello schermo o l'area dello schermo.

Tabella 5-19 *Dimension*

Metodo	
`Dimension(rows,cols)`	Crea una nuova istanza Dimension. **Parametri** `{Number}` `rows` dimensione delle righe sullo schermo `{Number}` `cols` dimensione delle colonne sullo schermo

Field

Utilizzare l'oggetto Field, insieme a FieldList, per ottenere le informazioni presenti in un campo sullo schermo.

Tabella 5-20 *Field*

Metodo	
`getAttributes()`	Restituisce il set di attributi specificato per questa istanza del campo. Vedere AttributeSet. **Restituisce** `{AttributeSet}` Il set di attributi per questo campo
`getForegroundColor()`	Restituisce il colore del primo piano del campo. **Restituisce** `{Number}` il colore di primo piano per questo campo. Questi valori sono definiti nell'oggetto Colore.
`getBackgroundColor()`	Restituisce il colore dello sfondo del campo. **Restituisce** `{Number}` il colore di sfondo per questo campo. Questi valori sono definiti nell'oggetto Colore.
`getStart()`	Restituisce la posizione iniziale del campo. La posizione iniziale è la posizione del primo carattere del campo. Alcuni tipi di host utilizzano una posizione del carattere per memorizzare attributi a livello di campo. In questo caso la posizione dell'attributo non è considerata la posizione iniziale. **Restituisce** `{Position}` Posizione iniziale del campo. **Genera** `{RangeError}` Per campi con lunghezza pari a zero.
`getEnd()`	Restituisce la posizione finale del campo. La posizione finale è la posizione nello spazio di presentazione che contiene l'ultimo carattere del campo. **Restituisce** `{Position}` Posizione finale del campo. **Genera** `{RangeError}` Per campi con lunghezza pari a zero.

Metodo	
`getLength()`	Restituisce la lunghezza del campo. Per i tipi di host che utilizzano una posizione del carattere per memorizzare gli attributi del campo, la lunghezza del campo non include la posizione dell'attributo del campo. **Restituisce** `{Number}` Lunghezza del campo.
`getDataCells()`	Ottiene le celle dati che compongono questo campo. Vedere DataCell. **Restituisce** `{DataCell[]}`Le celle dati che compongono questo campo.
`getText()`	Ottiene il testo dal campo. **Restituisce** `{String}` testo del campo.
`setText()`	Imposta il testo del campo. Per alcuni tipi di host, ad esempio VT, il testo viene trasmesso immediatamente all'host, ma in altri tipi di host il testo non viene trasmesso all'host fino a quando viene richiamato il tasto AID. Se il testo è più breve del campo, viene inserito nel campo dell'host e il resto del campo viene cancellato. Se il testo è più lungo del campo dell'host, verrà inserito nel campo tutto il testo che può essere contenuto. **Parametri** `{String}`Testo da impostare nel campo. **Genera** `{Error}` Se il campo è protetto.
`clearField()`	Cancella il campo corrente in modo specifico all'emulazione. **Genera** `{Error}` Se il campo è protetto o se la cancellazione non è supportata.
`getPresentationSpace()`	Ottiene l'oggetto PresentationSpace che ha creato questo campo. **Restituisce** `{PresentationSpace}` Padre di questa istanza del campo.
`toString()`	Crea una una descrizione del campo. **Restituisce** `{String}` Una conversione del campo leggibile dall'utente.

FieldList

Utilizzare l'oggetto FieldList, insieme all'oggetto Field, per ottenere informazioni sull'elenco dei campi.

Tabella 5-21 *FieldList*

Metodo	
`getPresentationSpace()`	Ottiene l'oggetto PresentationSpace che ha creato questo elenco dei campi. **Restituisce** `{PresentationSpace}` Padre di questa istanza dell'elenco dei campi.
`findField(position, text, direction)`	Restituisce il campo che contiene il testo specificato. La ricerca inizia nella posizione specificata e continua in avanti o indietro. Se una stringa comprende più campi, viene restituito il campo che contiene la posizione iniziale. Nella ricerca in avanti, la ricerca non andrà a capo all'inizio dello schermo. Nella ricerca all'indietro, la ricerca non andrà a capo alla fine dello schermo. **Parametri** `{Position}` Posizione dalla quale iniziare la ricerca. Vedere l'oggetto Position. `{String}` Il testo da cercare (facoltativo). Se non fornito, restituisce il successivo campo a destra della posizione specificata o sotto di essa. `{Number}` direzione della ricerca (facoltativo). Utilizzare le costanti PresentationSpace. SearchDirection per questo parametro. Ad esempio, `PresentationSpace.SearchDirection.FORWARD` o `PresentationSpace.SearchDirection.BACKWARD`. Se questo parametro non viene fornito, la ricerca è in avanti. **Restituisce** `{Field}` contenente la stringa o null se non viene trovato un campo che soddisfa i criteri specificati. **Genera** `{RangeError}` se la posizione è al di fuori dell'intervallo.

Metodo	
`get(index)`	Ottiene il campo all'indice specificato. **Parametri** `{Number}` indice nell'elenco dei campi. **Restituisce** `{Field}` situato all'indice specificato. **Genera** `{RangeError}` se l'indice è al di fuori dell'intervallo.
`isEmpty()`	Determina se l'elenco dei campi è vuoto. **Restituisce** `{Boolean}` True se l'elenco dei campi è vuoto.
`size()`	Indica il numero di campi nell'elenco. **Restituisce** `{Number}` Il numero di campi
`toString()`	Crea una una descrizione dell'elenco dei campi. **Restituisce** `{String}` Conversione del campo leggibile dall'utente.

FileTransferFactory

Per tutte le macro è disponibile un oggetto fileTransferFactory. Se per la sessione sono configurati dei trasferimenti di file, è possibile usarlo per ottenere un riferimento all'oggetto FileTransfer.

Tabella 5-22 *fileTransferFactory*

Metodo	
`getIND$File()`	Restituisce un oggetto FileTransfer per l'interazione con il tipo Ind$File configurato per la sessione. **Restituisce** `{FileTransfer}` **Genera** `{Error}` Se la sessione non è stata configurata per consentire i trasferimenti IND$File.

FileTransfer

Utilizzare l'oggetto FileTransfer per elencare e trasferire i file fra il sistema host e il client.

L'API di trasferimento dei file di Host Access for the Cloud astrae le convenzioni del percorso del file utilizzate dalle diverse implementazioni di file host. Seguire i formati dei percorsi URL o del file system Linux quando si formattano i percorsi di file utilizzati dall'API. Ad esempio, `/root/directory/file`. È importante attenersi alle regole specifiche dei sistemi host, ad esempio i caratteri consentiti o la lunghezza dei nomi.

Nota: I browser impongono limitazioni di sicurezza considerevoli sulla possibilità di interazione di Javascript con i file system dei client.

Tabella 5-23 *FileTransfer*

Metodo	
`getHostFileListing(remotePath)`	Richiede un elenco di file host. Se viene omesso `remotePath`, viene visualizzato un elenco di file per la directory di lavoro remota corrente. **Parametri** `{String}` (facoltativo) Se specificato si otterrà un elenco di file per il percorso remoto specificato. Se non è specificato, si otterrà un elenco di file per la directory di lavoro remota corrente. **Restituisce** `{Promise}` Si risolve in una matrice di oggetti HostFile contenuti in `remoteName`. Rifiutato se non è possibile leggere il percorso remoto.
`sendFile(localFile, remoteName)`	Invia il file specificato all'host. **Parametri** `{File}` Oggetto file Javascript che punta al file locale da inviare. `{String}` Nome file remoto completo, come consentito dal sistema remoto (Unix, Windows, MVS, VAX). **Restituisce** `{Promise}` completato con un oggetto `HostFile` che rappresenta il file inviato correttamente. Rifiutato se si è verificato un errore nell'invio del file.

Metodo	
`getDownloadURL(remoteName)`	Costruisce un collegamento per scaricare un file dal sistema host. **Parametri** `{String}` Nome file remoto completo, come consentito dal sistema remoto (Unix, Windows, MVS, VAX). **Restituisce** `{URL}` che può essere utilizzato per recuperare il file dal server di sessione di Host Access for the Cloud.
`setTransferOptions(options)`	Imposta le opzioni di trasferimento per la sessione FileTransfer corrente. Le opzioni di trasferimento vengono applicate a tutti i trasferimenti futuri fino a quando la sessione viene chiusa o sostituita da un'altra chiamata a `setTransferOptions`. **Parametri** {JSON} vedere `FileTransferOptions` per i nomi e i valori consentiti. **Restituisce** `{Promise}` completato quando la chiamata viene completata. Rifiutato se si è verificato un errore nell'impostazione delle opzioni.
`cancel()`	Annulla il trasferimento del file in corso. **Restituisce** `{Promise}` completato quando la chiamata viene completata. Rifiutato se si è verificato un errore nell'annullamento del trasferimento.

HostFile

Un oggetto HostFile rappresenta un file nel file system host.

Tabella 5-24 *HostFile*

Metodo	
`getName()`	Ottiene il nome del file **Restituisce** `{String}` il nome del file.

Metodo	
`getParent()`	Ottiene il padre di questo file host. **Restituisce** `{String}` il padre di questo file host. Il risultato dipende dal tipo di host. Ad esempio in TST si tratta del nome del catalogo nel quale risiede il file.
`getSize()`	Le dimensioni in byte del file **Restituisce** `{Number}` le dimensioni del file in byte.
`getType()`	Il tipo di file rappresentato **Restituisce**

Tipo file host

L'oggetto HostFileType definisce le costanti per determinare il tipo di oggetto HostFile.

Tabella 5-25 *HostFileType*

Valore	Descrizione
FILE	Rappresenta un file nel sistema host.
DIR	Rappresenta una directory nel sistema host.
UNKNOWN	Rappresenta un file host di origini sconosciute.

Opzioni di trasferimento file

Specifiche dell'oggetto opzioni di trasferimento file.

Esempio: `fileTransfer.setTransferOptions({ transferMethod : 'ascii' });`

Tabella 5-26 *FileTransferOptions*

Metodo	
`transferMethod`	`{String}`Valori consentiti: ◆ "ascii" ◆ "binary"

OIA

Interfaccia Operator Information Area (OIA). L'oggetto OIA restituisce valori che sono definiti nell'oggetto OIAStatus.

Tabella 5-27 *OIA*

Metodo	
`getStatus` ()	Restituisce il set di flag di stato attivi. Vedere StatusSet. **Parametri** **Restituisce** `{StatusSet}` Contenente le informazioni sullo stato.
`getCommErrorCode()`	Restituisce il codice di errore di comunicazione corrente. **Restituisce** `{Number}` il codice di errore di comunicazione corrente. Se non ne esiste uno, verrà restituito 0.
`getProgErrorCode()`	Restituisce il codice di errore del programma corrente. **Restituisce** `{Number}` il codice di errore del programma corrente. Se non ne esiste uno, verrà restituito 0.

OIAStatus

Tabella 5-28 *OIAStatus*

OIAStatus	Descrizione
CONTROLLER_READY	Controller pronto
A_ONLINE	Online con una connessione non SNA
MY_JOB	Connesso a un'applicazione host
OP_SYS	Connesso a un SSCP (SNA)
UNOWNED	Non connesso
TIME	Tastiera disattivata
SYS_LOCK	Blocco sistema dopo tasto AID
COMM_CHECK	Controllo comunicazione
PROG_CHECK	Controllo programma
ELSEWHERE	Sequenza di tasti non valida nella posizione del cursore.
FN_MINUS	Funzione non disponibile
WHAT_KEY	Sequenza di tasti non valida
MORE_THAN	Troppi caratteri immessi nel campo
SYM_MINUS	Immesso simbolo non disponibile
INPUT_ERROR	Errore di input dell'operatore (solo 5250)

OIAStatus	Descrizione
DO_NOT_ENTER	Non immettere
INSERT	Cursore in modalità inserimento
GR_CURSOR	Cursore in modalità grafica
COMM_ERR_REM	Promemoria errore di comunicazione
MSG_WAITING	Indicatore di messaggio in attesa
ENCRYPT	La sessione è crittografata
NUM_FIELD	Carattere non valido in campo esclusivamente numerico

AutoSignon

Alcuni host mainframe hanno un oggetto DCAS (Digital Certificate Access Server). È possibile richiedere un pass ticket temporaneo monouso a DCAS per accedere all'applicazione host. Utilizzando questo oggetto è possibile scrivere una macro che viene eseguita all'avvio della sessione e che consente di eseguire il login utilizzando le credenziali dell'utente attualmente connesso.

Tabella 5-29 *AutoSignon*

Metodo	
`getPassTicket()`	Ottiene un pass ticket da utilizzare per accedere a un'applicazione mainframe. È possibile richiedere più pass ticket utilizzando ID di applicazioni diversi. **Parametri** `{String}` l'ID applicazione indica all'host a quale applicazione è destinato l'accesso **Restituisce** `{Promise}` completata con la chiave pass ticket o rifiutata se l'operazione non riesce. Il pass ticket ottenuto da DCAS funziona solo per la sessione host corrente ed è valido per dieci minuti.
`sendUserName()`	Applica il nome utente contenuto nel pass ticket al campo nella posizione del cursore corrente sullo schermo host corrente. Il nome utente deve essere inviato prima della password. Se viene inviata prima la password, il pass ticket verrà invalidato e sarà necessario ottenerne un altro. **Parametri** `{String}` passTicketKey ottenuta da getPassTicket **Restituisce** `{Promise}` completata se il nome utente viene inviato correttamente. Rifiutata se l'operazione non riesce.

Metodo	
`sendPassword()`	Applica la password contenuta nel pass ticket al campo nella posizione del cursore corrente sullo schermo host corrente. Il nome utente deve essere inviato prima della password. Se viene inviata prima la password, il pass ticket verrà invalidato e sarà necessario ottenerne un altro. **Parametri** `{String}` passTicketKey ottenuta da getPassTicket **Restituisce** `{Promise}` completata se la password viene inviata correttamente. Rifiutata se l'operazione non riesce.

Position

Rappresenta una riga e una colonna sullo schermo.

Tabella 5-30 *Position*

Metodo	
`Position(row,col)`	Crea una nuova istanza Position. **Parametri** `{Number}` `row` coordinata della riga sullo schermo `{Number}` `col` coordinata della colonna sullo schermo

PresentationSpace

Utilizzare l'oggetto PresentationSpace per interagire con lo schermo del terminale. Le interazioni disponibili includono l'impostazione e l'ottenimento della posizione del cursore, l'invio di chiavi e la lettura del testo.

Tabella 5-31 *PresentationSpace*

METODI	
`getCursorPosition()`	Restituisce un'istanza di Position che rappresenta la posizione corrente del cursore. In una sessione non connessa la posizione del cursore è 0,0. **Restituisce** `{Position}` posizione corrente del cursore

METODI

`setCursorPosition(position)`	Sposta il cursore dell'host alla posizione specificata nella riga e nella colonna. Per alcuni host, ad esempio VT, l'host potrebbe limitare gli spostamenti del cursore. **Parametri** `{Position}` Position nuova posizione del cursore. **Restituisce** Nessun valore **Genera** `{RangeError}` se la posizione non è valida sullo schermo corrente.
`isCursorVisible()`	Verifica che il cursore sia attualmente visibile nello spazio di presentazione. Se la sessione non è connessa il cursore è considerato non visibile. **Restituisce** `{Boolean}` True se il cursore è visibile. False se il cursore non è visibile.
`sendKeys(keys)`	Trasmette una stringa di testo o ControlKey all'host nella posizione corrente del cursore nello spazio di presentazione. Se il cursore non è nella posizione desiderata, utilizzare prima la funzione `setCursorPosition`. La stringa di testo può contenere qualsiasi numero di caratteri e oggetti ControlKey. Ad esempio: `"myname" + ControlKey.TAB + "mypass" + ControlKey.ENTER` trasmetterà un ID utente, il tasto Tab per passare al campo successivo, una password, quindi il tasto Invio. Se è necessario trasmettere una parentesi quadra, raddoppiare le parentesi ([[o]]). **Parametri** `{String}` testo del tasto e/o tasti di controllo da trasmettere

METODI

`getText(start,length)`	Restituisce una stringa che rappresenta un'area lineare dello spazio di presentazione. Se vengono rilevati limiti di riga, non vengono inseriti caratteri di nuova riga. **Parametri** `{Position}` posizione iniziale dalla quale recuperare il testo `{Number} lunghezza del numero massimo di caratteri da restituire. Se il parametro della lunghezza causa il superamento dell'ultima posizione dello spazio di presentazione, verranno restituiti solo i caratteri fino all'ultima posizione.` **Restituisce** `{String)` che rappresenta un'area lineare dello spazio di presentazione che potrebbe essere vuoto se la sessione non è connessa. **Genera** `{RangeError}` se la posizione o la lunghezza non sono valide sullo schermo corrente.
`getSize()`	Ottiene le dimensioni dello schermo come un oggetto Dimension. **Restituisce** `{Dimension}` Contenente il numero di righe e colonne. Le dimensioni dello schermo sono [row:0, col:0] se la sessione non è connessa.
`getDataCells(start, length)`	Restituisce istanze di DataCell in cui il primo membro sarà la posizione specificata dal parametro start. Il numero massimo di istanze di DataCell nell'elenco è specificato dal parametro length. **Parametri** `{Position}` posizione iniziale sullo schermo dell'host in cui recuperare le istanze di DataCell. Vedere Position. `{Number}` lunghezza del numero massimo di istanze di DataCell da recuperare. Se non è specificato, restituisce DataCell dalla posizione iniziale fino alla fine dello schermo. **Restituisce** `{DataCell[]}` Istanze che possono essere vuote se la sessione non è connessa. Se la posizione non è specificata, restituisce tutti i DataCell. Se la lunghezza non è specificata, restituisce i DataCell dalla posizione iniziale alla fine dello schermo. **Genera** `{RangeError}` se l'inizio o la lunghezza sono al di fuori dell'intervallo.

METODI	
`getFields()`	Restituisce un elenco di campi nello spazio di presentazione. Se il tipo di host non supporta i campi o lo schermo corrente non è formattato, il valore restituito sarà sempre un elenco vuoto. Vedere FieldList. **Restituisce** `{FieldList}` di campi definiti dall'host nello spazio di presentazione.

Session

L'oggetto Session è il punto di ingresso principale per l'interazione con l'host. Contiene funzioni per la connessione, la disconnessione e l'ottenimento dell'oggetto PresentationSpace.

Tabella 5-32 *Funzioni dell'oggetto Session*

METODI	
`connect()`	Connette all'host configurato. Se necessario, utilizzare `wait.forConnect()` per bloccare l'esecuzione della macro fino a quando la sessione è connessa. **Restituisce** `Nessuno`
`disconnect()`	Disconnette dall'host configurato. Se necessario, utilizzare `wait.forDisconnect()` per bloccare l'esecuzione della macro fino a quando la sessione è connessa. **Restituisce** `Nessuno`
`isConnected()`	Determina se la connessione all'host è stata stabilita. **Restituisce** `{Boolean}` true se la connessione all'host è stata stabilita; in caso contrario, false.
`getPresentationSpace()`	Fornisce accesso all'istanza di PresentationSpace per questa sessione. **Restituisce** Istanza di `{PresentationSpace}` associata alla sessione.
`getDeviceName()`	Restituisce il nome del dispositivo per una sessione connessa oppure una stringa vuota se la sessione viene disconnessa o non dispone del nome del dispositivo. **Restituisce** `{String}` Il nome del dispositivo connesso.

METODI

`getType()`	Restituisce il tipo di sessione host. Vedere SessionType. **Restituisce** `{String}` Il tipo di sessione host.
`setDeviceName()`	Fornisce un modo per modificare il nome del dispositivo in un'istanza della sessione. **Parametri** `{String}` `name` Nome del dispositivo da utilizzare nella connessione a un host. **Genera** `{Error}` Se viene effettuato un tentativo di impostare il nome del dispositivo mentre la sessione è connessa.
`getOIA()`	Fornisce accesso all'istanza di OIA per questa sessione. **Restituisce** `{OIA}` Associata alla sessione

SessionType

Costanti utilizzate per identificare il tipo di host con il quale viene stabilita la connessione. Vedere l'oggetto Session.

Tabella 5-33 *SessionType*

Tipo host	Descrizione
IBM_3270	Indica una sessione di terminale IBM 3270.
IBM_5250	Indica una sessione di terminale IBM 5250.
VT	Indica una sessione VT.

StatusSet

È possibile utilizzare l'oggetto StatusSet per codificare lo stato di OIA. L'oggetto StatusSet restituisce i valori definiti nell'oggetto OIAStatus e, quando utilizzati insieme, è possibile ottenere informazioni sullo stato da OIA.

Tabella 5-34 *StatusSet*

Metodo	
`contains(statusFlag)`	Determina se il set contiene il flag di stato specificato dalle costanti OIAStatus. **Parametri** `{Number} statusFlag` stato da verificare **Restituisce** `{Boolean}` True se il flag dello stato è presente nel set.
`isEmpty()`	Determina se il set di stati è vuoto. **Restituisce** `{Boolean}` True se il set è vuoto.
`size()`	Indica il numero di flag di stato nel set. **Restituisce** `{Number}` Il numero di stati
`toArray()`	Converte il set di stati interno in una matrice. **Restituisce** `{Object []}` Matrice di flag di stato nel set.
`toString()`	Converte il set di stati interno in una stringa. **Restituisce** `{String}` Nomi delimitati da spazi dei flag di stato nel set.
`forEach(callback, thisArg)`	Funzione per reiterare ogni elemento nel set di stati. **Parametri** `{forEachCallback}` Callback per eseguire l'operazione specifica. Chiamato con il nome di ogni stato nel set. `{Object}`thisArg puntatore facoltativo a un oggetto di contesto.
`forEachCallback(string, thisArg)`	Una funzione di callback fornita dall'utente in cui fornire il comportamento, da usare come parametro di callback per forEach. **Parametri** `{String}` `String` nome dello stato nel set di stati. `{Object}` `thisArg` Puntatore facoltativo a un oggetto di contesto.

User Interface

L'oggetto User Interface fornisce le funzioni per l'interazione con l'utente, la richiesta di informazioni e la visualizzazione di informazioni di base. L'oggetto UI è reso disponibile automaticamente nella macro come variabile "ui".

Nota: Importante! Tutte le funzioni UI devono essere precedute dalla parola chiave "yield". Questo consente alla macro di bloccare l'esecuzione fino a quando sono soddisfatte le condizioni della funzione UI.

`[parameter]` denota un parametro facoltativo.

Tabella 5-35 *Interazione con l'utente*

METODI	
`prompt(message,[defaultAnswer], [mask])`	Richiede all'utente di inserire informazioni nell'interfaccia utente. **Parametri** `{String} titolo del messaggio da visualizzare all'utente.` Impostazione predefinita: stringa vuota. `{String} risposta predefinita da utilizzare non inserisce l'informazione richiesta.` Impostazione predefinita: stringa vuota. `{Boolean} la maschera indica se nascondere il prompt (come con la password).` **Restituisce** `{Promise}` Completata quando l'utente chiude la finestra di dialogo. Restituisce l'input dell'utente quando sceglie "OK", null quando sceglie "Annulla".
`message([message])`	Visualizza un messaggio nell'interfaccia utente. **Parametri** `{String} messaggio da visualizzare all'utente.` Impostazione predefinita: stringa vuota. **Restituisce** `{Promise}` Completata quando l'utente chiude la finestra del messaggio.

Wait

Utilizzare l'oggetto Wait per attendere un particolare stato di una sessione o di uno schermo. Ad esempio, è possibile attendere che il cursore si trovi in una determinata posizione o che in una certa posizione sia presente il testo sia presente un testo prima di continuare l'esecuzione della macro.

Le funzioni Wait sono spesso utilizzare insieme alle funzioni asincrone quali connect() e sendKeys().

Nota: Tutte le funzioni accettano i timeout come parametro facoltativo e hanno un valore di timeout predefinito di 10 secondi (10000ms).

Importante: Tutte le funzioni Wait devono essere precedute dalla parola chiave "yield". Questo consente alla macro di bloccare l'esecuzione fino a quando sono soddisfatte le condizioni della funzione Wait.

`[parameter]` denota un parametro facoltativo.

Tabella 5-36 *In attesa dell'host*

METODI

`setDefaultTimeout(timeout)`	Imposta il valore di timeout per tutte le funzioni. **Parametri** `{Number} timeout predefinito da utilizzare per tutte le funzioni Wait in millisecondi.` **Restituisce** Nessun valore **Genera** `{RangeError}` Se il timeout specificato è minore di zero.
`forConnect([timeout])`	Attende il completamento di una richiesta di connessione. **Parametri** `{Number}` in millisecondi. **Restituisce** `{Promise}` Completata se la sessione è già connessa o quando si verifica la connessione. Rifiutata in caso di timeout.
`forDisconnect([timeout])`	Attende il completamento di una richiesta di disconnessione. **Parametri** `{Number}` timeout in millisecondi. **Restituisce** `{Promise}` Completata se la sessione è già disconnessa o quando si verifica la disconnessione. Rifiutata in caso di timeout.
`forFixedTime([timeout])`	Attende incondizionatamente per il tempo stabilito. Il tempo è stabilito in millisecondi (ms) **Parametri** `{Number}` timeout in millisecondi. **Restituisce** `{Promise}` Completata quando il tempo scade

METODI

`forScreenChange([timeout])`	Attende la modifica della schermata host. Questa funzione restituisce il risultato quando viene rilevato un aggiornamento di schermata. Non fornisce alcuna garanzia in merito al numero di aggiornamenti successivi che possono essere ricevuti prima che la schermata venga completata. Si consiglia di prolungare l'attesa finché il contenuto della schermata soddisfi determinati criteri di interruzione noti. **Parametri** `{Number}` timeout in millisecondi. **Restituisce** `{Promise}` Risolto se la schermata cambia. Rifiutata in caso di timeout.
`forCursor(position, [timeout])`	Attende che il cursore arrivi alla posizione specificata. **Parametri** `{Position}` La posizione che specifica la riga e la colonna `{Number}` timeout in millisecondi **Restituisce** `{Promise}` Completata se il cursore è già posizionato o quando ha raggiunto la posizione. Rifiutata in caso di timeout.
`forText(text, position, [timeout])`	Attende che il testo si trovi in una posizione specifica sullo schermo **Parametri** `{String} testo previsto` `{Position}` posizione che specifica la riga e la colonna `{Number}` timeout in millisecondi **Restituisce** `{Promise}` Completata se il testo è già nella posizione specificata o quando ha raggiunto la posizione. Rifiutata in caso di timeout. **Genera** `{rangeError}` se la posizione non è valida.

METODI

`forHostPrompt(text, column,[timeout])`	Attende un prompt dei comandi posizionato in una colonna specifica sullo schermo.
	
	Parametri
	
	`{String} testo del prompt previsto`
	
	`{Number} colonna in cui è previsto il cursore`
	
	`{Number}` timeout in millisecondi.
	
	Restituisce
	
	`{Promise}` Completata se le condizioni sono già soddisfatte o quando vengono soddisfatte. Rifiutata in caso di timeout.
	
	Genera
	
	`{rangeError}` se la colonna è al di fuori dell'intervallo.

Macro di esempio

Per creare macro utili, che sfruttino tutte le capacità dell'Editor di macro, sono disponibili macro di esempio da utilizzare come punto di partenza.

- "Interazioni di base con l'host" a pagina 153
- "Interazione con l'utente" a pagina 156
- "Spostamento nei dati" a pagina 157
- "Chiamata di un servizio Web" a pagina 159
- "Operazioni con DataCell e Attribute" a pagina 161
- "Utilizzo di Field e FieldList" a pagina 162
- "Macro di accesso automatico per mainframe" a pagina 164
- "Utilizzo di Trasferimento file (IND$File)" a pagina 165

Interazioni di base con l'host

Questo esempio illustra le interazioni di base seguenti:

- Invio di dati all'host
- Attesa della visualizzazione di schermi
- Utilizzo della parola chiave `yield` in attesa delle funzioni asincrone
- Lettura del testo dallo schermo
- Visualizzazione di informazioni di base all'utente
- Gestione di errori di base

Per impostazione predefinita, per tutte le macro sono disponibili gli oggetti seguenti:

1. **session** - Punto di ingresso principale per accedere all'host. Consente di connettersi, disconnettersi e fornisce accesso a PresentationSpace.

L'oggetto PresentationSpace ottenuto da session rappresenta lo schermo e fornisce molte capacità comuni, ad esempio ottenimento e impostazione della posizione del cursore, invio di dati all'host e lettura dello schermo.

2. **wait** - Fornisce un modo semplice per attendere che si verifichino i vari stati dell'host prima di continuare a inviare altri dati o a leggere dallo schermo.
3. **UI** - Fornisce capacità di interfaccia utente di base. Mostra i dati o richiede informazioni all'utente.

```
// Creare una nuova funzione macro
var macro = createMacro(function*(){
  'use strict';

  // Per impostazione predefinita, per tutte le macro sono disponibili gli
oggetti seguenti:
  // 1. session - Punto di ingresso principale per accedere all'host.
Consente di connettersi, disconnettersi e fornisce accesso a
PresentationSpace.
  //  L'oggetto PresentationSpace ottenuto da session rappresenta lo
schermo e fornisce molte capacità comuni, ad esempio ottenimento e
impostazione della
  //  posizione del cursore, invio di dati all'host e lettura dello
schermo.
  // 2. wait - Fornisce un modo semplice per attendere che si verifichino i
vari stati dell'host prima di continuare a inviare altri dati o a leggere
dallo schermo.
  // 3. ui - Fornisce capacità di base di interazione con l'utente. Mostra
i dati o richiede informazioni all'utente.

  // Dichiarare una variabile per la lettura e la visualizzazione di alcuni
dati dello schermo.
  // La procedura consigliata è dichiarare tutte le variabili all'inizio di
una funzione.
  var numberOfAccounts = 0;

  // Iniziare ottenendo l'oggetto PresentationSpace, che fornisce molte
operazioni comuni dello schermo.
  var ps = session.getPresentationSpace();

  try {
    // Può impostare e ottenere la posizione del cursore
    ps.setCursorPosition(new Position(24, 2));

    // Utilizzare la funzione sendKeys per inviare caratteri all'host
    ps.sendKeys('cics');

    // SendKeys viene utilizzata anche per inviare all'host tasti quali PA
e PF.
    // Vedere tutte le opzioni disponibili in "Tasti di controllo" nella
documentazione
    ps.sendKeys(ControlKey.ENTER);

    // Attendere che il cursore si trovi nella posizione corretta.
    // L'oggetto wait fornisce numerose funzioni per attendere che si
verifichino determinati stati
```

```
    // in modo che sia possibile inviare altri tasti o leggere i dati dello
schermo.
    yield wait.forCursor(new Position(24, 2));

    // È possibile combinare caratteri e tasti di controllo in una chiamata
sendKeys.
    ps.sendKeys('data' + ControlKey.TAB + ControlKey.TAB + 'more data' +
ControlKey.ENTER);

    // La parola chiave "yield" deve essere utilizzata prima di tutte le
chiamate alle funzioni "wait" e "ui".
    // Indica al browser di interrompere l'esecuzione della macro fino a
quando la
    // funzione wait (asincrona) restituisce il risultato. Consultare la
documentazione per informazioni sulle funzioni
    // che richiedono la parola chiave yield.
    yield wait.forCursor(new Position(10, 26));
    ps.sendKeys('accounts' + ControlKey.ENTER);

    // È possibile anche attendere che il testo venga visualizzato in aree
specifiche dello schermo
    yield wait.forText('ACCOUNTS', new Position(3, 36)) ;
    ps.sendKeys('1' + ControlKey.ENTER);

    // Tutte le funzioni wait scadranno se i criteri non vengono
soddisfatti entro il limite di tempo definito.
    // È possibile aumentare i timeout con un parametro aggiuntivo nelle
funzioni wait (in millisecondi)
    // Tutti i timeout sono specificati in millisecondi e il valore
predefinito è 10 secondi (10000ms).
    yield wait.forCursor(new Position(1, 1), 15000);
    ps.sendKeys('A' + ControlKey.ENTER);

    // PS fornisce la funzione getText per leggere il testo dalla schermata
    numberOfAccounts = ps.getText(new Position(12, 3), 5);

    // Utilizzare l'oggetto ui per visualizzare alcuni dati dalla schermata
    ui.message('Numero di account attivi: ' + numberOfAccounts);

    // try/catch consente di rilevare gli errori e segnalarli in
un'ubicazione centrale
  } catch (error) {
    // Utilizzare di nuovo l'oggetto ui per visualizzare un messaggio che
informa che si è verificato un errore
    yield ui.message('Error: ' + error.message);
  }
  //Fine della macro generata
});

// Eseguire la macro e restituire i risultati a Macro Runner
// L'istruzione return è necessaria poiché l'applicazione la utilizza
// per sapere se la macro è stata eseguita correttamente e se è terminata
return macro();
```

Interazione con l'utente

Questo esempio illustra come utilizzare i metodi API forniti per richiedere input o fornire informazioni all'utente tramite un messaggio.

```
var macro = createMacro(function*(){
  'use strict';

  // L'oggetto "ui" fornisce funzioni per richiedere informazioni
all'utente e visualizzare informazioni

  // Dichiarare variabili da utilizzare successivamente
  var username;
  var password;
  var flavor;
  var scoops;

  //Begin Generated Macro
  var ps = session.getPresentationSpace();

  try {
    // Richiedere all'utente di immettere il proprio nome e memorizzarlo in
una variabile.
    // Notare che la parola chiave 'yield' è necessaria per bloccare
l'esecuzione in attesa dell'input dell'utente.
    username = yield ui.prompt('Please enter your username');

    // Richiedere all'utente di immettere un valore, proponendo una
risposta predefinita.
    flavor = yield ui.prompt('What is your favorite flavor of ice cream?',
'Chocolate');

    // Richiedere all'utente di immettere informazioni riservate
utilizzando l'opzione 'mask'. Durante l'immissione il testo sarà nascosto.
    // Se un parametro non viene utilizzato, è possibile usare 'null' per
specificare che non deve essere usato.
    // Qui lo illustriamo specificando che non è necessario mostrare un
valore predefinito.
    password = yield ui.prompt('Please enter your password', null, true);

   // La funzione prompt restituisce null se l'utente fa clic sul pulsante
'Cancel' anziché sul pulsante 'OK'.
    // Un modo per gestire questo caso consiste nell'eseguire il wrapping
della chiamata in un blocco try/catch.
    scoops = yield ui.prompt('How many scoops would you like?');
    if (scoops === null) {
      // Termina la macro.
      return;
      // In alternativa potrebbe generare un Error che potrebbe essere
catturato nel "catch" sotto
    }
    // Utilizzare i valori raccolti per ordinare il gelato
    ps.sendKeys(username + ControlKey.TAB + password + ControlKey.ENTER);
    yield wait.forCursor(new Position(5, 1));
    ps.sendKeys(flavor + ControlKey.TAB + scoops + ControlKey.ENTER);
```

```
    // Visualizzare un messaggio all'utente. Utilizzando la parola chiave
'yield' davanti alla chiamata,
    // l'esecuzione della macro verrà bloccata fino a quando l'utente
sceglie il pulsante 'OK'.
    yield ui.message('Order successful. Enjoy your ' + scoops + ' scoops of
' + flavor + ' ice cream ' + username + '!');
  } catch (error) {
    // Qui abbiamo usato l'oggetto ui per visualizzare un messaggio che
informa che si è verificato un errore
    yield ui.message(error.message);
  }
  //Fine della macro generata

});

return macro();
```

Spostamento nei dati

Questo esempio illustra come spostarsi in un numero variabile di schermi ed elaborare i dati di ogni schermo.

```
 // Creare una nuova funzione macro.
var macro = createMacro(function*(){
  'use strict';

  // Creare una o più variabili da utilizzare successivamente
  var password;
  var accountNumber;
  var transactionCount = 0;
  var row = 0;

  // Ottenere un riferimento all'oggetto PresentationSpace.
  var ps = session.getPresentationSpace();

  try {
    // Immettere nome utente e password per accedere all'applicazione.
    yield wait.forCursor(new Position(19, 48));
    ps.sendKeys('bjones' + ControlKey.TAB);

    yield wait.forCursor(new Position(20, 48));
    password = yield ui.prompt('Password:', null, true);
    ps.sendKeys(password);
    ps.sendKeys(ControlKey.ENTER);

    // Immettere un comando dell'applicazione.
    yield wait.forCursor(new Position(20, 38));
    ps.sendKeys('4');
    ps.sendKeys(ControlKey.ENTER);

    // Creare l'elenco delle transazioni per un conto.
    yield wait.forCursor(new Position(13, 25));
    ps.sendKeys('2');
    // Immettere un numero di conto. In questo esempio ne è stato inserito uno per
maggior chiarezza.
    yield wait.forCursor(new Position(15, 25));
    accountNumber = yield ui.prompt('Account Number:', '167439459');
    ps.sendKeys(accountNumber);
    ps.sendKeys(ControlKey.ENTER);

    // Attendere fino a quando raggiunge lo schermo del profilo del conto
```

```
    yield wait.forText('ACCOUNT PROFILE', new Position(3, 33));

    // Cercare il testo che indica che è stata raggiunta l'ultima pagina del record
    while (ps.getText(new Position(22, 12), 9) !== 'LAST PAGE') {

      // Quando non è ancora stata raggiunta l'ultima pagina del record, passare
alla pagina successiva di record.
      ps.sendKeys(ControlKey.PF2);
      yield wait.forCursor(new Position(1, 1));

      // Se la posizione del cursore non cambia da uno schermo di record all'altro
e non è presente testo sullo schermo,
      // è possibile attendere che uno schermo venga aggiornato. È possibile
specificare
     // il periodo di tempo di attesa dopo che è stato inviato un tasto AID per il
completo aggiornamento dello schermo.
      // Ad esempio:
      // yield wait.forFixedTime(1000);

      // Per ogni riga, incrementare la variabile count se contiene dati.
      for (row = 5; row <= 21; row++) {

       // Sullo schermo sono presenti 2 colonne. Verificare i dati nella colonna 1.
       // In questo esempio, sappiamo che se è presente uno spazio in una posizione
        // particolare, esiste una transazione.
        if (ps.getText(new Position(row, 8), 1) !== ' ') {
          transactionCount++;
        }
        // Verificare i dati nella colonna 2.
        if (ps.getText(new Position(row, 49), 1) !== ' ') {
          transactionCount++;
        }
      }
    }

    // Dopo essere passati in tutte le pagine di record, visualizzare il numero di
record in una casella di messaggio.
    yield ui.message('There are ' + transactionCount + ' records found for account
' + accountNumber + '.');

    // Disconnettersi dall'applicazione
    ps.sendKeys(ControlKey.PF13);
    ps.sendKeys(ControlKey.PF12);

    // try/catch consente di rilevare gli errori e segnalarli in un'ubicazione
centrale
  } catch (error) {
    // Qui viene utilizzato l'oggetto ui per visualizzare un messaggio che informa
che si è verificato un errore
    yield ui.message(error.message);
  }
});

// Qui viene eseguita la macro e i risultati vengono restituiti a Macro Runner
// L'istruzione return è necessaria poiché l'applicazione la utilizza
// per sapere se la macro è stata eseguita correttamente
return macro();
```

Chiamata di un servizio Web

Questo esempio illustra come effettuare una chiamata AJAX / REST direttamente da una macro a un servizio Web. È possibile integrare i dati dall'applicazione host alla chiamata al servizio Web o dal servizio Web all'applicazione host.

In questo esempio, viene chiamato il servizio REST CICSAcctsDemo di Verastream Host Integrator (VHI). È però possibile adattare facilmente il codice per chiamare qualsiasi servizio Web. Non si è limitati a VHI.

Nell'esempio, la chiamata passa attraverso un proxy configurato nel server di sessione (mostrato sotto) per evitare la complicazione "Same Origin Policy". Se si utilizza un servizio Web che supporta Cross-origin Resource Sharing (CORS) e si utilizza un browser recente, il proxy non è necessario.

Poiché la libreria jQuery è disponibile nelle macro, è possibile utilizzare direttamente la funzione $.post() per richiamare i servizi REST.

Questo esempio dimostra anche come eseguire il wrapping di una chiamata REST jQuery in una nuova promessa. La promessa restituita dalla funzione personalizzata sotto consente di utilizzare "yield" nel codice macro principale. Questo consente all'esecuzione della macro principale di attendere fino al completamento della chiamata del servizio prima di continuare.

```
 var macro = createMacro(function*() {
  'use strict';

  // Creare alcune variabili da utilizzare successivamente
  var username;
  var password;
  var accountNumber;
  var accountDetails;

  // Creare una funzione che effettuerà una chiamata AJAX / REST al servizio Web
VHI.
  // Può essere modificata per chiamare qualsiasi servizio, non solo VHI.
  // Se non si utilizza CORS, è probabile che la richiesta debba passare
  // attraverso un proxy nel server di sessione. Per ulteriori informazioni, vedere
le note dell'esempio.
  /**
   * Funzione helper codificata manualmente per incapsulare i parametri AJAX /
REST, richiamare il
   * servizio REST e restituire i risultati in un oggetto Promise.
   * @param {Number} acctNum per inviare la query REST.
   * @param {String} username per accedere al servizio REST.
   * @param {String} password per accedere al servizio REST.
   * @return {Promise} contenente i risultati di $.post() compatibili con yield.
  */
  var getAccountDetails = function (acctNum, username, password) {
    var url = "proxy1/model/CICSAcctsDemo/GetAccountDetail";
    var args = {"filters": {"AcctNum": acctNum}, "envVars": {"Username": username,
"Password": password}};

    // Eseguire il wrapping di una chiamata jQuery AJAX / HTTP POST in un nuovo
oggetto Promise.
    // L'oggetto Promise restituito qui consente alla macro di eseguire yield /
wait
    // per il completamento.
    return Promise.resolve($.post(url, JSON.stringify(args)))
      .catch(function (error) {
      // Mappare gli errori che si verificano nella chiamata jQuery all'oggetto
Promise.
      throw new Error('REST API Error: ' + error.statusText);
    });
```

```
  };

  // Inizio della macro generata
  var ps = session.getPresentationSpace();
  try {
    // Qui è possibile interagire con l'host, accedere all'app host ecc.
    // Raccogliere nome utente e password
    username = yield ui.prompt('Username:');
    password = yield ui.prompt('Password:', null, true);
    accountNumber = yield ui.prompt('Account Number:');
    if (!username || !password || !accountNumber) {
      throw new Error('Username or password not specified');
    }

   // Richiamare il servizio REST esterno e utilizzare yield / wait per completare
la chiamata.
    accountDetails = yield getAccountDetails(accountNumber, username, password);

    // Sono ora disponibili i dati del servizio esterno.
    // È possibile integrare i dati nell'app host locale o semplicemente mostrarli
all'utente.
    // Per questo esempio, verranno semplicemente visualizzati i dettagli del
conto.
    if (accountDetails.result && accountDetails.result.length > 0) {
      yield ui.message(accountDetails.result[0].FirstName + ' $' +
accountDetails.result[0].AcctBalance);
    } else {
      yield ui.message('No records found for account: ' + accountNumber);
    }
  } catch (error) {
    // Se si è verificato un errore durante la chiamata AJAX / REST
    // o nella raccolta di nomeutente / password, l'operazione terminerà qui.
    yield ui.message(error.message);
  }
});

// Eseguire la macro
return macro();
```

Supporto di scripting proxy tra origini

Se sono presenti servizi Web che non supportano CORS, le chiamate AJAX/REST avranno esito negativo se tentano di accedere a un server diverso da quello in cui è stata originata l'applicazione Host Access for the Cloud. Si tratta di una funzione di sicurezza del browser.

Il server Host Access for the Cloud fornisce un modo esplicito per agire da proxy per i server remoti attendibili.

- Aprire `..\<directory-installazione>\sessionserver\microservice\sessionserver\service.yml` per effettuare modifiche.
- Nella sezione `env`, aggiungere:

  ```
  name: zfe.proxy.mappings
       value: percorso-proxy=indirizzo-destinazione-proxy
  ```

  Dove percorso-proxy si riferisce alla mappatura URL desiderata e indirizzo-proxy=indirizzo-destinazione-proxy si riferisce all'URL dove la chiamata verrà trasferita tramite proxy.
- In questo esempio:

  ```
  name: zfe.proxy.mappings
       value: percorso-proxy=indirizzo-destinazione-proxy
  ```

Le chiamate effettuate a `<server:port>/proxy1` saranno delegate a `http://remote-vhi-server:9680/vhi-rs/`

- È possibile specificare più mappature proxy utilizzando una virgola per separare le singole mappature
- Tenere presente che anche quando un server REST supporta intestazioni CORS, alcuni browser meno recenti potrebbero non supportarle, perciò questi esempio potrebbe comunque essere rilevante.

Suggerimento: Il file `service.yml` può essere sostituito quando si distribuisce nuovamente Host Access for the Cloud. Creare sempre una copia di backup dei file.

Operazioni con DataCell e Attribute

Questa macro illustra come utilizzare DataCell e AttributeSet per ispezionare testo e attributi in una determinata riga/colonna sullo schermo. In questo esempio si può vedere:

- Come ottenere una raccolta di DataCell per una determinata posizione e lunghezza.
- Come eseguire l'iterazione sui DataCell per creare una stringa di testo
- Come, per confronto, è possibile eseguire un'operazione simile anche utilizzando getText().
- E infine, come eseguire operazioni con gli attributi, ottenere un elenco di stringhe o determinare se stringhe specifiche sono impostate in una determinata posizione dello schermo.

```
var macro = createMacro(function*() {
  'use strict';

  // Ottenere PresentationSpace per interagire con l'host
  var ps = session.getPresentationSpace();

  // Dichiarare le variabili da utilizzare successivamente
  var cells;
  var text;
  var attrs;

  // Impostare il valore di timeout predefinito per le funzioni "wait"
  wait.setDefaultTimeout(10000);

  // Macro di esempio per operazioni con DataCell e Attributi
  try {
    yield wait.forCursor(new Position(24, 2));

    // Ottenere DataCell dallo spazio di presentazione.
    // Riga 19, col 3 è il prompt, lunghezza 35 caratteri
    // "Choose from the following commands:"
    cells = ps.getDataCells({row:19, col:3}, 35);
    text = '';

    // È possibile visualizzare il testo utilizzando getText
    yield ui.message("Screen text: " + ps.getText({row:19, col:3}, 35));

    // Oppure è possibile assemblare il testo da DataCell a ogni posizione
    for(var index = 0; index < cells.length; index++) {
      text = text.concat(cells[index].getChar());
    }
    // E visualizzare il testo
    yield ui.message("Cells text: " + text);

    // Ottenere gli attributi per la prima DataCell (cell[0])
```

```
    attrs = cells[0].getAttributes();

    // Visualizzare se sono presenti attributi nella cella dati
    yield ui.message("Attribute set is empty: " + attrs.isEmpty());

    // Visualizzare il numero di attributi impostato set
    yield ui.message("Number of attributes: " + attrs.size());

    // Visualizzare quali attributi sono impostati
    yield ui.message("Attributes: " + attrs.toString());

    // Ora visualizzare se l'attributo high intensity è impostato
    yield ui.message("Is high intensity: "
             + attrs.contains(Attribute.HIGH_INTENSITY));

    // Ora visualizzare se l'attributo underline è impostato
    yield ui.message("Is underline: "
             + attrs.contains(Attribute.UNDERLINE));

   // Ora visualizzare se sono impostati gli attributi alphanumeric, intensified e
pen-detectable
    yield ui.message("Is alphanumeric, intensified and pen-detectable: "
             + attrs.containsAll([Attribute.ALPHA_NUMERIC,
Attribute.HIGH_INTENSITY, Attribute.PEN_DETECTABLE]));

    // Ora visualizzare se sono impostati gli attributi underline, intensified e
pen-detectable
    yield ui.message("Is underline, intensified and pen-detectable: "
             + attrs.containsAll([Attribute.UNDERLINE, Attribute.HIGH_INTENSITY,
Attribute.PEN_DETECTABLE]));
  } catch (error) {
    yield ui.message(error);
  }
  //Fine della macro generata
});

// Eseguire la macro
return macro();
```

Utilizzo di Field e FieldList

Questa macro di esempio illustra come utilizzare funzioni comuni per interagire con i campi nell'API Macro. Ad esempio, come ottenere il testo dei campi, visualizzare informazioni sui campi e come utilizzare field.setText come alternativa a sendKeys per interagire con l'host.

Nota: A causa delle considerazioni sul browser ui.message comprime stringhe di spazi in un solo spazio. Gli spazi vengono mantenuti nel codice JavaScript effettivo.

```
var macro = createMacro(function*() {
  'use strict';

  // Ottenere PresentationSpace per interagire con l'host
  var ps = session.getPresentationSpace();

  // Dichiarare variabili da utilizzare successivamente use
  var fields;
  var field;
  var searchString = 'z/VM';

  // Impostare il valore di timeout predefinito per le funzioni "wait"
  wait.setDefaultTimeout(10000);

  // Macro di esempio per operazioni con FieldList e Field
```

```
  try {
    yield wait.forCursor(new Position(24, 2));

    // Ottenere l'elenco di campi.
    fields = ps.getFields();

    // Scorrere l'intero elenco di campi e visualizzare le informazioni sul campo.
    for(var index = 0; index < fields.size(); index++) {
      field = fields.get(index);

      yield ui.message("Field " + index + " info: " + field.toString());
    }

    yield ui.message("Now, find a field containing the text '" + searchString +
"'");
    field = fields.findField(new Position(1, 1), searchString);

    if(field !== null) {
      yield ui.message("Found field info: " + field.toString());
      yield ui.message("Found field foreground is green? " + (Color.GREEN ===
field.getForegroundColor()));
      yield ui.message("Found field background is default? " +
(Color.BLANK_UNSPECIFIED === field.getBackgroundColor()));
    }

    // Cercare ora un campo comando e modificarlo.
    field = fields.findField(new Position(23, 80));
    if(field !== null) {
      field.setText("cics");
    }

    yield ui.message("Click to send 'cics' to host.");
    ps.sendKeys(ControlKey.ENTER);

    // Attendere il nuovo schermo; ottenere nuovi campi.
    yield wait.forCursor(new Position(10, 26));
    fields = ps.getFields();

    // Trovare il campo utente e impostarlo.
    field = fields.findField(new Position(10, 24));
    if(field !== null) {
      field.setText("myusername");
    }

    // Trovare il campo della password e impostarlo.
    field = fields.findField(new Position(11, 24));
    if(field !== null) {
      field.setText("mypassword");
    }

    yield ui.message("Click to send login to host.");
    ps.sendKeys(ControlKey.ENTER);

    // Attendere il nuovo schermo; ottenere nuovi campi.
    yield wait.forCursor(new Position(1, 1));
    fields = ps.getFields();

    // Trovare il campo comando e impostare il comando di disconnessione.
    field = fields.findField(new Position(24, 45));
    if(field !== null) {
```

```
      field.setText("cesf logoff");
    }

    yield ui.message("Click to send logoff to host.");
    ps.sendKeys(ControlKey.ENTER);

  } catch (error) {
    yield ui.message(error);
  }
  //Fine della macro generata
});

// Eseguire la macro
return macro();
```

Macro di accesso automatico per mainframe

In questo esempio l'oggetto Autosignon viene utilizzato per creare una macro che usa le credenziali associate a un utente per ottenere un pass ticket da DCAS (Digital Certificate Access Server).

```
var macro = createMacro(function*() {
  'use strict';

  // Ottenere PresentationSpace per interagire con l'host
  var ps = session.getPresentationSpace();

  // Variabile per il pass ticket di accesso
  var passTicket;

  // ID applicazione di accesso
  var appId = 'CICSV41A';

  // Impostare il timeout predefinito per le funzioni "wait"
  wait.setDefaultTimeout(10000);

  // Inizio della macro generata
  try {
    yield wait.forCursor(new Position(24, 2));

    // Ottenere un pass ticket da DCAS.
    passTicket = yield autoSignon.getPassTicket(appId);

    ps.sendKeys('cics');
    ps.sendKeys(ControlKey.ENTER);

    yield wait.forCursor(new Position(10, 26));

    // Sostituire il nome utente generato con sendUserName(passTicket) ...
    yield autoSignon.sendUserName(passTicket);

    // ps.sendKeys('bvtst01' + ControlKey.TAB + ControlKey.TAB);
    ps.sendKeys(ControlKey.TAB + ControlKey.TAB);

    yield wait.forCursor(new Position(11, 26));

    // Sostituire la password generata con sendPassword(passTicket) ...
    yield autoSignon.sendPassword(passTicket);

    // var userInput3 = yield ui.prompt('Password:', '', true);
    // if (userInput3 === null) {
      // throw new Error('Password not provided');
    // }
    // ps.sendKeys(userInput3);
```

```
    ps.sendKeys(ControlKey.ENTER);

    yield wait.forCursor(new Position(1, 1));
    yield ui.message('Logged in. Log me off.');
    ps.sendKeys('cesf logoff');
    ps.sendKeys(ControlKey.ENTER);
  } catch (error) {
    yield ui.message(error);
  }
  //Fine della macro generata
});

// Eseguire la macro
return macro();
```

Utilizzo di Trasferimento file (IND$File)

Questa serie di macro di esempio illustra come utilizzare l'API Trasferimento file per richiamare un elenco di file, scaricare un file e caricare un file in un host 3270.

Nota: Per poter eseguire queste macro, effettuare l'accesso e passare al prompt dei comandi.

Elenco di file

Questa macro illustra come utilizzare l'API Trasferimento file per richiamare un elenco di file in un host 3270 tramite il trasferimento IND$File. L'oggetto di trasferimento IND$File viene richiamato dalla factory trasferimento file, quindi utilizzato per ottenere una matrice di oggetti HostFile da TSO o CMS.

```
var macro = createMacro(function*() {
  'use strict';

  try {
    var fileTransfer = fileTransferFactory.getInd$File();
    var hostFiles = yield fileTransfer.getHostFileListing();

    yield ui.message('Found ' + hostFiles.length + ' files');
    if (hostFiles.length > 0) {
      var firstFile = hostFiles[0];
      var msg1 = 'The catalog name is ' + firstFile.getParent() + '. ';
      var msg2 = 'The first file is ' + firstFile.getName();
      yield ui.message(msg1 + msg2);
    }
  } catch (error) {
    yield ui.message(error);
  }
});

// Eseguire la macro
return macro();
```

Download di file

Questa macro illustra come utilizzare l'API Trasferimento file per scaricare un file da un host 3270 tramite il trasferimento IND$File. L'oggetto di trasferimento IND$FILE viene richiamato dalla factory trasferimento file. In questo esempio il metodo di trasferimento è impostato su ASCII per dimostrare l'utilizzo della funzione setTransferOptions. La macro di esempio scarica il primo file restituito da una chiamata a getHostFileListing creando un URI di download tramite una chiamata alla funzione

getDownloadUrl. La macro può essere utilizzata sia in ambiente CMS che TSO ma è necessario specificare la scelta nella prima riga oppure modificare leggermente il codice per il sistema desiderato.

```
var hostEnvironment = 'CMS'; // 'TSO'
// Costruire il percorso file, ad esempio catalog/file.name o catalog/partition/
file
function getPath (fileNode) {
  var prefix = fileNode.getParent() ? fileNode.getParent() + '/' : '';
  return prefix + fileNode.getName();
}

var macro = createMacro(function*() {
  'use strict';

  try {
    var fileTransfer = fileTransferFactory.getInd$File();

    // Le opzioni di transferMethod sono 'binary' e 'ascii'
    fileTransfer.setTransferOptions({transferMethod: 'ascii'});

    // Questo esempio recupera il primo file restituito nell'elenco
    var hostFiles = yield fileTransfer.getHostFileListing();
    var firstHostFile = hostFiles[0];

    if (hostEnvironment === 'CMS') {
      yield wait.forText('Ready', new Position(1,1), 5000);
    }

    // Download
    // Se si conosce già il percorso del file desiderato, passare il percorso a
getDownloadURL()
    var downloadUrl = fileTransfer.getDownloadURL(getPath(firstHostFile));

    // Questo modifica la posizione del browser. I risultati potrebbero essere
diversi a seconda del browser
    window.location = downloadUrl;

    // Per leggere il contenuto del file in una variabile anziché scaricarlo,
    // è possibile utilizzare jQuery
    // var fileContents = yield $.get(downloadUrl);

  } catch (error) {
    yield ui.message(error);
  }
});

// Eseguire la macro
return macro();
```

Caricamento di file

Questa macro illustra come utilizzare l'API Trasferimento file per caricare un file in un host 3270 tramite il trasferimento IND$File. La macro di esempio richiede all'utente di scegliere un file dal file system locale attivando la finestra di selezione dei file del browser. Richiama poi il catalogo corrente su TSO o l'identificatore di unità su CMS chiamando getHostFileListing. Infine viene chiamata la funzione sendFile per consegnare all'host il file locale selezionato. La macro può essere utilizzata sia in ambiente CMS che TSO ma è necessario specificare la scelta nella prima riga. In questo esempio il metodo di trasferimento è impostato su **ascii**, ma è possibile impostarlo su **binary**.

```
var hostEnvironment = 'CMS'; // 'TSO'
// Apre la finestra di selezione file del browser a livello di codice
function promptForFileToUpload () {
  return new Promise(function (resolve, reject) {
    // Non si ricevono notifiche se l'utente annulla la finestra di selezione file,
quindi rifiutare dopo 30 secondi
    var timerId = setTimeout(reject.bind(null, 'Timed out waiting for file
selection'), 30000);
    var fileSelector = document.createElement('input');
    fileSelector.setAttribute('type', 'file');
    fileSelector.onchange = function (evt) {
      var file = evt.target.files[0];
      clearTimeout(timerId);
      resolve(file);
    };
    fileSelector.click();
  });
}

var macro = createMacro(function*() {
  'use strict';

  try {
    var fileTransfer = fileTransferFactory.getInd$File();

    // Le opzioni di transferMethod sono 'binary' e 'ascii'
    fileTransfer.setTransferOptions({transferMethod: 'ascii'});

    var localFile = yield promptForFileToUpload();

    // Richiamare il nome del catalogo corrente e aggiungervi il nome del file
selezionato
    var hostFiles = yield fileTransfer.getHostFileListing();
    var destination = hostFiles[0].getParent() + '/' + localFile.name;

    if (hostEnvironment === 'CMS') {
      yield wait.forText('Ready', new Position(1,1), 5000);
    }

    var result = yield fileTransfer.sendFile(localFile, destination);

  } catch (error) {
    yield ui.message(error);
  }
});

// Eseguire la macro
return macro();
```

Stampa

Sono disponibili diverse opzioni di stampa per gli host 3270, 5250 e UTS. È possibile effettuare catture di schermate, stampare una schermata selezionata, abilitare e configurare le funzionalità di stampa host:

- Acquisire uno schermo
- Stampare uno schermo
- Stampa host

Le impostazioni disponibili per l'impostazione della pagina e l'orientamento dipendono dalle opzioni del browser.

Acquisire uno schermo

Utilizzare la funzione di acquisizione dello schermo per acquisire più schermi e salvarli in un file per la stampa o la condivisione. Questa opzione è disponibile per tutti gli utenti dopo che l'amministratore l'ha selezionata in **Preferenze utente**.

1. Passare allo schermo che si vuole acquisire.
2. Fare clic su  per acquisire lo schermo. Il contatore visualizza il numero di acquisizioni effettuate. Ogni acquisizione verrà stampata su una pagina separata.
3. Fare clic su Salva per passare al percorso in cui salvare gli schermi acquisiti. Il browser determina il funzionamento dell'opzione di salvataggio. Ad esempio, in Chrome, in base alle impostazioni del browser, il file verrà salvato nella directory di download oppure verrà visualizzata una finestra di dialogo Salva con nome per selezionare il percorso in cui salvare il file acquisito.
4. Per aggiungere gli schermi appena salvati a un file di acquisizione dello schermo esistente, fare clic su **Aggiungi e salva**. Quando si stampa il file a cui sono stati aggiunti gli schermi, ogni acquisizione viene stampata su una pagina separata.
5. È possibile cancellare le acquisizioni in qualsiasi momento facendo clic su Cancella.

Stampare uno schermo

L'opzione Stampa dello schermo stampa il contenuto dello schermo del terminale. Non stampa la barra degli strumenti o altre informazioni sul display.

1. Passare allo schermo da stampare.
2. Fare clic su Stampa dello schermo sulla barra degli strumenti.
3. Utilizzare la finestra di stampa del browser per selezionare la stampante e le opzioni di impostazione della pagina.

Stampa host

Questa funzione è disponibile per le sessioni host 3270, 5250 e UTS. È possibile creare una o più sessioni della stampante e associarle alla sessione di terminale corrente. Ogni sessione della stampante è associata a un ID dispositivo nel sistema host e ogni lavoro di stampa successivo inviato a tale ID dispositivo sarà indirizzato al client Web Host Access for the Cloud.

La sessione host crea un file PDF contente il file da stampare e lo invia al client Web. Dopo aver ricevuto il file, il client Web ne effettua il download in base alle opzioni di download configurate nel browser in uso. Browser diversi offrono opzioni diverse per la gestione dei file scaricati. Quando si riceve il file PDF, è possibile stamparlo su qualsiasi stampante a cui si ha accesso.

Nota: Un amministratore può consentire agli utenti finali di stampare i file impostando l'opzione **Stampa host** nelle preferenze dell'utente.

Argomenti correlati

Impostazioni di connessione

Impostazioni in Impostazioni pagina
Impostazioni avanzate
Per stampare la sessione della stampante host

Per configurare la stampa host

1. Da una sessione host, fare clic su **Impostazioni** nella barra degli strumenti per aprire il riquadro di spostamento a sinistra.
2. Nel riquadro a sinistra, fare clic su **Stampa**.
3. Fare clic su **Aggiungi** per aprire la finestra di dialogo di configurazione. Sono presenti tre schede: Impostazioni di connessione, Impostazioni in Impostazioni pagina e Impostazioni avanzate. Ogni scheda contiene impostazioni diverse per personalizzare la sessione stampante.
4. Fare clic su **Salva** per tornare alla sessione. L'impostazione avrà effetto quando viene riaperta la sessione.

Argomenti correlati

Impostazioni di connessione
Impostazioni in Impostazioni pagina
Impostazioni avanzate

Impostazioni di connessione

Per impostazione predefinita, le sessioni stampante sono disponibili dall'icona della stampante sulla barra degli strumenti della sessione di terminale. Per impedire agli utenti finali di accedere a questa sessione stampante, deselezionare **Attiva questa sessione stampante** nella scheda Connessione.

Le impostazioni variano in base al tipo di host utilizzato.

Impostazioni di connessione 3270
Impostazioni di connessione 5250
Impostazioni per le connessioni UTS

Impostazioni di connessione 3270

Impostazione	Descrizione
Nome	Fornire un nome facilmente identificabile per la sessione della stampante. Obbligatorio.
Protocollo	Selezionare il protocollo da utilizzare. Le opzioni sono: ◆ **TN3270E** - TN3270E di Telnet Extended è dedicato agli utenti di software TCP/IP che si collegano a un mainframe IBM tramite un gateway Telnet che implementa RFC 1647. ◆ **TN3287** - TN3287 è dedicato agli utenti di software TCP/IP che si collegano a un mainframe IBM tramite un gateway Telnet che implementa RFC 1646.

Impostazione	Descrizione
ID dispositivo	Specificare se si vuole utilizzare un ID dispositivo, richiedere il nome del dispositivo o un'associazione TN (se si seleziona TN3270E), per collegare la sessione di terminale alla sessione della stampante. Obbligatoria. Selezionare una delle seguenti opzioni: ◆ **Specifica ID dispositivo** - Specificare l'ID dispositivo da utilizzare quando la sessione della stampante si connette all'host. ◆ **Utilizza associazione TN** - (TN3270E) Se si sceglie di utilizzare un'associazione TN, per collegare le sessioni 3270 e 3287, Host Access for the Cloud utilizzerà il nome del dispositivo specificato nelle impostazioni di connessione. L'associazione TN è disponibile solo se si seleziona TN3270E come protocollo. ◆ **Chiedi all'utente** - Quando la sessione stampante stabilisce la connessione, all'utente viene richiesto di fornire l'ID dispositivo per la sessione della stampante.

Impostazioni di connessione 5250

Impostazione	Descrizione
Nome	Fornire un nome facilmente identificabile per la sessione della stampante. Obbligatorio.
ID dispositivo	Specificare se si desidera utilizzare un ID dispositivo o richiedere un ID dispositivo: ◆ **Specifica ID dispositivo** - Specificare l'ID dispositivo da utilizzare quando la sessione della stampante si connette all'host. ◆ **Chiedi all'utente** - Quando la sessione stampante stabilisce la connessione, all'utente viene richiesto di fornire l'ID dispositivo per la sessione della stampante.

Impostazioni per le connessioni UTS

Impostazione	Descrizione
Nome	Fornire un nome facilmente identificabile per la sessione della stampante. Obbligatorio.
Protocollo	La scelta dei protocolli DEMAND o MAPPER dipende dal tipo di sessione UTS creata. I tipi di sessione UTS vengono determinati in base ai valori specificati per le opzioni di TSAP e di applicazione nel pannello Connessione. Ad esempio, se si immettono valori che creano una sessione MAPPER o DEMAND UTS, è necessario selezionare MAPPER o DEMAND come protocollo. Specificare il protocollo che si desidera utilizzare: ◆ **MAPPER** - È possibile scegliere di specificare l'ID dispositivo da utilizzare quando la sessione della stampante si connette all'host o di richiedere all'utente di fornire l'ID dispositivo per la sessione della stampante, quindi continuare con la configurazione della sessione. ◆ **DEMAND** - Dopo aver fornito un nome per la sessione, è possibile continuare con la configurazione della sessione utilizzando le schede Impostazioni pagina e Avanzate.

Impostazioni in Impostazioni pagina

La scheda Impostazioni pagina contiene opzioni per impostare il formato carta e l'orientamento, oltre a dimensioni, margini e valori di ridimensionamento.

Impostazione	Descrizione
Formato carta	Selezionare il formato della carta utilizzata nella stampante.
Orientamento	È possibile scegliere tre modalità: **Verticale**, **Orizzontale** o **Automatico**, l'impostazione predefinita. Se viene selezionato Automatico, la stampante valuta il lavoro di stampa e utilizza il formato più adeguato.
Unità di misura	Selezionare l'unità di misura da utilizzare per margini e formati di pagina. I valori sono Pollici o Millimetri.
Dimensioni	Immettere il numero di righe e colonne da mostrare su ogni pagina stampata. 60 è il valore predefinito per le righe, 80 per le colonne.
Margini	Imposta i margini sinistro, destro, superiore e inferiore della pagina.
Ridimensionamento	Imposta il ridimensionamento orizzontale e verticale per l'output stampato. Aumentare la percentuale per aumentare lo spazio orizzontale o verticale utilizzato dalla stampa.

Argomenti correlati

Impostazioni di connessione
Impostazioni avanzate
Per stampare la sessione della stampante host

Impostazioni avanzate

Sono disponibili tre opzioni relative a quando scaricare il file PDF.

- **In automatico** - (impostazione predefinita) il PDF viene scaricato automaticamente al completamento del lavoro di stampa. Quando è selezionata questa opzione, l'impostazione di timeout di inattività non è disponibile.
- **Manualmente** - una volta che il lavoro di stampa è iniziato, è possibile avviare un download in qualsiasi momento individuando il lavoro nell'elenco di download disponibile dall'icona Stampa sulla barra degli strumenti e facendo clic su **Svuota**. Il lavoro di stampa viene aggregato in un singolo file PDF e può essere scaricato.
- **Dopo timeout inattività** - utilizzando questa opzione è possibile eseguire lavori di stampa multipli, aggregarli in un unico PDF, quindi scaricarlo automaticamente al momento specificato.

  Se viene scelto un valore maggiore di 0 (ad esempio 5 secondi), qualsiasi lavoro di stampa assegnato a una stampante che arrivi entro 5 secondi dal precedente verrà aggiunto allo stesso PDF. Dopo 5 secondi e in assenza di lavori di stampa rimanenti, il PDF viene scaricato. Se per il timeout di inattività viene specificato 0, ogni lavoro di stampa viene scaricato immediatamente appena completato. È sempre possibile interrompere un lavoro di stampa facendo clic su **Svuota**.

Argomenti correlati

Impostazioni di connessione
Impostazioni in Impostazioni pagina
Per stampare la sessione della stampante host

Per stampare la sessione della stampante host

Quando si apre la sessione del terminale è possibile:

1. Selezionare la stampante da utilizzare. Sono disponibili tutte le stampanti associate alla sessione terminale aperta. Fare clic su  nella barra degli strumenti per visualizzare un elenco delle stampanti.
2. La sessione host riceve i dati di stampa dall'host e genera un file PDF da stampare. Al client Web viene inviato un collegamento per indicare che il file è disponibile per il download.

   È possibile monitorare i vari lavori di stampa utilizzando il contatore pagine della barra degli strumenti o il contatore associato con le diverse stampanti nell'elenco a discesa di stampa.

   Il contatore pagine sulla barra degli strumenti riflette il numero totale di pagine attualmente in corso di stampa o completate ma in attesa del download del file dal server. È possibile avviare un download selezionando **Svuota** dall'elenco della stampante.

   Il contatore pagine associato alle stampanti nell'elenco a discesa mostra lo stesso valore, ma suddiviso per ogni stampante. La somma dei diversi lavori di stampa si riflette nel conteggio sulla barra degli strumenti. Il conteggio viene azzerato dopo il download dei lavori di stampa.
3. Una volta che il file PDF è disponibile, viene avviato il download oppure viene attesa l'attivazione da parte dell'utente mediante l'opzione Svuota, a seconda delle opzioni configurate.

Se necessario, quando l'esecuzione di un lavoro di stampa richiede troppo tempo, è possibile svuotare il lavoro di stampa corrente. L'opzione **Svuota** è disponibile nell'elenco di sessioni di stampa accessibile tramite l'icona stampanti sulla barra degli strumenti. Quando un lavoro di stampa viene svuotato, vengono stampate tutte le informazioni accumulate fino a quel momento e l'elaborazione dei dati di stampa continua.

Personalizzare le sessioni

È possibile utilizzare queste funzionalità per personalizzare le sessioni per gli utenti finali:

- **Plus** - Attiva i controlli personalizzati per consentire un flusso di lavoro più efficiente e un'interfaccia più semplice e moderna. Vedere Utilizzare Plus per personalizzare gli schermi.

  Utilizzando questa opzione, è possibile aggiungere descrizioni ai campi, sostituire gli elenchi numerati vecchio stile con i più moderni elenchi a discesa, aggiungere tasti all'interfaccia dell'host e programmarli per l'avvio di macro o l'esecuzione di altre azioni, e sostituire l'immissione manuale della data con un calendario grafico da cui selezionarla.

- **Eventi lato server** - Fornisce codice Java procedurale che estende e migliora la presentazione dei dati dell'host.

  Quando si utilizzano gli eventi lato server, è possibile definire eventi specifici e sospendere l'applicazione host, sostituendola o interrompendola con il codice che è stato fornito per quella sessione, oltre che estendere le opzioni di gestione degli errori. Ad esempio è possibile aggiungere un evento che riconosce quando si verifica un errore e quindi implementa il codice per intercettarlo, assumere il controllo e correggere l'errore. Vedere Utilizzare gli eventi lato server.

- **Avanzate** - Utilizzare solo seguendo le indicazioni del supporto tecnico Micro Focus.

Queste opzioni sono configurate nel riquadro Personalizzazione.

1. Fare clic su Impostazioni nella barra degli strumenti per aprire il riquadro di spostamento a sinistra.
2. Fare clic su Personalizzazione.

Argomenti correlati

Utilizzare Plus per personalizzare gli schermi
Utilizzare gli eventi lato server

Utilizzare Plus per personalizzare gli schermi

Nota: La funzione Plus richiede i file di archivio (.rdar) prodotti da Micro Focus Screen Designer versione 9.5 o successiva. Screen Designer è disponibile in Micro Focus Rumba Desktop 9.5. Reflection Desktop 16.1 include una versione limitata di Screen Designer. Per ottenere più controlli e l'accesso alla versione completa di Plus e Screen Designer, è possibile acquistare e installare l'add-on Micro Focus Reflection Desktop Plus.

---

1. Nel pannello **Personalizzazione**, fare clic su **Attiva Plus**.
2. Selezionare il file di archivio Plus da utilizzare dall'elenco a discesa o caricare il file da un percorso diverso. I file di archivio Plus sono identificati dall'estensione `rdar`.

   I file di archiviazione sono l'output di un progetto Screen Designer e vengono utilizzati per fornire criteri di controllo personalizzati.

   Se si aggiorna il file di archivio Plus (.rdar) associato alla sessione attiva di Plus, è necessario eliminare per prima cosa la cartella contenente il file .rdar precedente dal server di sessione. Dopo aver eliminato la cartella, è possibile aprire la sessione attiva di Plus e il nuovo file rdar file verrà scaricato sul server di sessione.
3. Verificare che il numero di millisecondi per il ritardo della risoluzione dell'host sia accurato. Si tratta del tempo di attesa del server per una connessione sincrona prima di decidere che l'invio di dati da parte dell'host è terminato.
4. Quando si torna alla sessione, Plus è disponibile. Fare clic su  nella barra degli strumenti per disattivare i controlli personalizzati.

Quando si attiva Plus per una sessione, tutti gli utenti finali della sessione vedono l'icona Plus sulla barra degli strumenti e tutti i controlli resi disponibili tramite i file di personalizzazione di Screen Designer.

Argomenti correlati

Personalizzare le sessioni

Utilizzare gli eventi lato server

Utilizzando gli eventi lato server è possibile fornire codice Java procedurale in grado di estendere e migliorare la presentazione dei dati dell'host.

Il riquadro **Personalizzazione** indica al client Web dove trovare l'evento dopo averlo configurato. Vedere Utilizzo di Java SDK per istruzioni sull'utilizzo di SDK e per gli esempi disponibili.

1. Aprire il riquadro **Personalizzazione**.
2. In **Eventi lato server** digitare il nome completo della classe dell'evento.
3. Avviare la sessione e verificare l'evento.

Accedere alla documentazione dell'API e a esempi di eventi

Argomenti correlati

Personalizzare le sessioni
Utilizzo di Java SDK
Sviluppo

Impostare le preferenze utente

L'amministratore può scegliere le opzioni che gli utenti possono configurare per le proprie sessioni. Queste opzioni sono impostate per singola sessione e tutti gli utenti che hanno accesso alla sessione specifica possono configurare la propria istanza della sessione.

1. Nel riquadro di spostamento a sinistra, scegliere **Regole di preferenze utente**.
2. Selezionare le opzioni che gli utenti potranno configurare.
3. Fare clic su Salva.

Le configurazioni di ogni utente sono specifiche all'istanza della sessione dell'utente e non entreranno in conflitto con le configurazioni di altri utenti.

È disponibile un'opzione **Ripristina impostazioni predefinite** nelle diverse impostazioni e nei riquadri di visualizzazione. Come amministratore, questa opzione consente di ripristinare le impostazioni predefinite del client Web. Per gli utenti finali questa opzione consente di ripristinare i valori impostati dall'amministratore al momento della creazione della sessione.

Argomenti correlati

Impostazioni di visualizzazione
Specificare le operazioni di copia e incolla
Trasferire file
Configurare le macro utente

6 Sviluppo

Host Access for the Cloud include una raccolta di API e librerie che consentono di sviluppare applicazioni client/server e Web efficienti che integrano i dati dell'host in diversi ambienti di sviluppo.

È anche possibile estendere il client Web senza modificare i file installati. Questa funzionalità fornisce con un'ampia gamma di opzioni per personalizzare il client Web in base alle proprie esigenze.

- Utilizzo di Java SDK è possibile utilizzare l'API Java fornita per migliorare la presentazione dei dati dell'host utilizzando gli eventi lato server.
- Utilizzo di Connector for Windows è possibile interagire con le sessioni host nella propria applicazione .NET o all'interno di Visual Basic for Applications utilizzando l'API e gli esempi forniti.
- Utilizzo dell'API JavaScript è possibile incorporare il client Web nel proprio sito Web.
- Estensione del client Web è possibile migliorare e ampliare l'ambito del client Web utilizzando codice personalizzato, come CSS o JavaScript.

Visualizza la documentazione dell'API

Argomenti correlati

Personalizzare le sessioni
Registrazione

Utilizzo di Java SDK

Lavorando con gli eventi lato server e con Host Access for the Cloud SDK è possibile creare codice Java procedurale in grado di estendere e migliorare la presentazione dei dati dell'host. Per facilitare la creazione di eventi lato server, Host Access for the Cloud contiene un SDK ed esempi che forniscono un punto di partenza.

I Javadoc sono disponibili nella directory di installazione (`<directory di installazione>\sessionserver\sdk\java\javadocs\index.html`) e online.

1. Rendere Host Access for the Cloud SDK disponibile per il proprio ambiente di sviluppo. L'SDK si trova in `directory-installazione\sessionserver\sdk`.
2. Scrivere il codice Java necessario per svolgere il task e compilare il codice in una classe Java all'interno di un file JAR (Java Archive).
3. Copiare il file JAR in `directory-installazione\sessionserver\microservices\extensions\server` e riavviare il server di sessione.

Se si dispone di più server di sessione sui quali si desidera eseguire l'evento, è necessario copiare il file JAR in questo percorso in ogni server.

4 Aggiungere la sessione da associare all'evento in Administrative Console.

5 Mentre si configura la sessione nel client Web, aprire il riquadro **Personalizzazione** e digitare il nome di classe completo dell'evento.

6 Avviare la sessione e verificare l'evento.

Esempi e documentazione

Per accedere all'SDK per visualizzarlo direttamente e importarlo nell'IDE:

1 Accedere a `<directory-installazione>\\sessionserver\sdk\java`.

2 Nella directory dell'SDK accedere a:

- `\javadoc`. Questa directory contiene i file javadoc per la visualizzazione diretta.
- `\samples` - Questa directory contiene le origini Java per la visualizzazione diretta.
- `\zfe-sdk.jar` - Il file JAR contiene le classi Java da importare nell'IDE.
- `\zfe-sdk-javadoc.jar` - Il file JAR contiene i file JavaDoc da importare nell'IDE.

Utilizzo di Connector for Windows

Connector for Windows di Host Access for the Cloud è un'installazione separata disponibile sul sito di download di Micro Focus. Con Connector for Windows è possibile interagire con le sessioni host nell'applicazione .NET o nell'ambito di Visual Basic for Applications.

La documentazione dell'API è disponibile nella directory di installazione (`<directory di installazione>\sessionserver\sdk\csharp\apidocs\index.html`) e online.

Ecco alcuni aspetti da considerare nella preparazione all'installazione:

- Sono disponibili due piattaforme di installazione: versione a 32 bit e versione a 64 bit. A seconda della piattaforma installata, il percorso di base predefinito dell'installazione sarà `C:\Program Files (x86)\Micro Focus\HACloud\Connector for Windows` o `C:\Program Files\Micro Focus\HACloud\Connector for Windows`.
- La piattaforma di installazione scelta determina anche la piattaforma della soluzione in cui è possibile sviluppare. Se, ad esempio, è stata installata la versione a 32 bit di Microsoft Office® e si desidera utilizzare Visual Basic for Applications con il connettore, è necessario installare la versione a 32 bit di Connector for Windows di Host Access for the Cloud.
- La documentazione dell'API è disponibile qui: `< directory di installazione >\sessionserver\sdk\csharp\apidocs\index.html`.
- È richiesto .NET 4.5.2.

Esempi e documentazione del connettore

La documentazione è disponibile come riferimento dall'IDE. Sono inoltre disponibili alcuni esempi per sfruttare il connettore. Le risorse si trovano qui:

1. Accedere alla directory di installazione. In un'installazione predefinita, `C:\Program Files (x86)\Micro Focus\HACloud\Connector for Windows` o `C:\Program Files\Micro Focus\HACloud\Connector for Windows` in base alla piattaforma.
2. Nella directory `Connector for Windows` sono disponibili:
   - `MicroFocus.ZFE.Connector.dll` - un assembly .NET Framework a cui fare riferimento nel progetto C# o .NET.
   - `MicroFocus.ZFE.Connector.tlb` - una libreria dei tipi da usare nel progetto COM o Visual Basic for Applications.
   - `\help` - questa directory contiene informazioni utili per l'utilizzo del connettore.
   - `\samples` - questa directory contiene gli esempi di codice che forniscono un punto di partenza per lo sviluppo delle applicazioni.

Utilizzo del connettore con Microsoft Visual Studio

Se si utilizza Microsoft Visual Studio per lo sviluppo di applicazioni, tenere in considerazione gli elementi seguenti:

- Quando si utilizza Microsoft Visual Studio con Connector for Windows, assicurarsi che la piattaforma della soluzione sia impostata su x86 o x64, a seconda dell'installazione. A causa dei componenti nativi utilizzati nell'ambito di Connector for Windows SDK, la piattaforma **Qualsiasi CPU** non è supportata. Utilizzare Gestione configurazione per la soluzione Visual Studio per creare una piattaforma per x86 o x64.
- Quando si aggiunge un riferimento alla libreria Connector for Windows, è possibile che Visual Studio imposti la proprietà di riferimento **Copia localmente** su **True**. Questa proprietà deve invece essere impostata su **False** affinché la libreria e le relative dipendenze siano eseguite dalla directory di installazione dell'SDK.

Utilizzo dell'API JavaScript

Utilizzando JavaScript in un browser è possibile incorporare il client Web in una pagina Web. Accedendo a una pagina Web comune, gli utenti finali possono interagire con il client Web ed eseguire la connessione all'applicazione host, con la possibilità di:

- Interagire con le sessioni host a livello di programmazione.
- Eseguire l'applicazione "in modalità headless", ossia accedendo a tutte le sue funzionalità senza un'interfaccia visibile incorporata nella pagina Web.

È possibile consultare una guida introduttiva e altre esercitazioni. La documentazione dell'API e altre esercitazioni sono disponibili online e in `<directory di installazione>\sessionserver\sdk\javascript`.

Argomenti correlati

Estensione del client Web

È possibile aggiornare, modificare e personalizzare l'aspetto del client Web utilizzando il proprio codice HTML, CSS o JavaScript dall'interno del browser.

È possibile usufruire delle estensioni per apportare modifiche visive al client Web e personalizzare l'applicazione. Il client Web ospita il codice HTML o CSS personalizzato, rendendo più semplice modificarlo e supportarlo.

È possibile ottenere ulteriori informazioni su:

- Aggiunta di un'estensione
- Esempio di estensione
- Come è possibile utilizzare le estensioni all'interno di Docker

Aggiunta di un'estensione

Prima di procedere, tenere presente che sebbene Host Access for the Cloud offra la possibilità di pianificare e utilizzare codice personalizzato, il supporto per tale codice deve essere fornito dal team che lo ha prodotto.

Avviso: Durante un upgrade del prodotto le estensioni vengono disabilitate. Questo significa che, dopo questa operazione, è necessario verificare che il prodotto funzioni come previsto senza estensioni, quindi sarà possibile abilitare nuovamente le estensioni utilizzano la procedura per l'aggiunta di codice personalizzato.

Quando si aggiungono le estensioni al client Web, le modifiche apportate sono visibili a tutti gli utenti e vengono applicate a tutte le sessioni.

Per aggiungere un'estensione

1. Aprire `<directory-installazione>/sessionserver/microservices/sessionserver/service.yml`.
2. Aggiungere `extensions-enabled` al valore esistente della proprietà `SPRING_PROFILES_ACTIVE`. Utilizzare una virgola per separare i valori.

   Ad esempio:

   ```
   env:
      - name: SPRING_PROFILES_ACTIVE
      value: tls,extensions-enabled
   ```

3 Riavviare il server di sessione.

4 Creare <directory-installazione>/sessionserver/microservices/sessionserver/extensions/client/index.html come punto di entrata. Questo è il momento in cui deve essere aggiunto eventuale codice HTML, CSS o JavaScript (inclusi i riferimenti agli script esterni).

Come rendere le estensioni disponibili senza l'autenticazione client

I file all'interno della directory /client sono protetti con il livello di autenticazione selezionato in MSS.

Per condividere i file, senza necessità dell'autenticazione:

Creare <directory-installazione>/sessionserver/microservices/sessionserver/extensions/public/. Inserire il codice nella directory, chiamandola utilizzando l'URL /public /*.

Esempio di estensione

In questo esempio, una volta che le estensioni sono state abilitate (vedere il passaggio 2 riportato sopra), è possibile aggiungere codice JavaScript e CSS personalizzato per modificare il colore dei caratteri del titolo dei menu e stampare il testo nella console JavaScript.

Verranno creati tre file; custom.css, custom.js e index.html.

Passaggio 1.

Individuare il file index.html creato nel passaggio 4. Nella stessa posizione andranno inseriti i file delle estensioni, creando in tal modo un punto di entrata:

```
<!-- Define the link to the external style sheet -->
   <link href="client/custom.css" rel="stylesheet">
   <!-- Define the external JavaScript file -->
   <script src="client/custom.js"></script>
```

Passaggio 2.

Modificare le etichette nere predefinite del menu applicando il colore arancione:

Creare custom.css per modificare il colore in arancione:

```
/* Change link text to Orange */
   a span {
  color: #ff5d28;
   }
```

Passaggio 3.

Creare il file custom.js per inviare il testo alla console JavaScript:

```
//Print message to the JavaScript console
   console.log('Hello World!');
```

Passaggio 4.

Quando i file sono a posto, `<directory-installazione>/sessionserver/microservices/sessionserver/extensions/client/index.html`, i risultati dovrebbero avere il seguente aspetto:

E nella console di JavaScript sarà visibile il testo "Hello World":

Argomenti correlati

Documentazione dell'API
Utilizzo dell'API JavaScript
Utilizzo di Connector for Windows
Utilizzo di Java SDK

7 Riferimenti tecnici

In questa sezione sono disponibili informazioni su problemi specifici che possono insorgere. Il Micro Focus Technical Support Handbook contiene informazioni su come ottenere supporto tecnico per i prodotti installati, accedere alle risorse online e contattare e interagire con la nostra organizzazione mondiale di supporto tecnico.

Monitoraggio dei server di sessione mediante Prometheus e Grafana

È possibile monitorare i server di sessione di Host Access for the Cloud utilizzando Prometheus e Grafana. Entrambi questi strumenti sono gratuiti, open source ed eseguibili nei container di Docker, caratteristiche che ne rendono semplice la distribuzione. Ciascun server di sessione fornisce un endpoint Prometheus che espone le metriche su tale server. Prometheus può essere configurato per recuperare i dati da questo endpoint e memorizzare regolarmente le metriche anche se provengono da più server di sessione. Grafana quindi fornisce un dashboard in cui è possibile eseguire query e visualizzare questi dati con una configurazione minima.

Prerequisiti:

Docker e Docker Compose devono essere installati.

Passaggi:

1. Creare un file Docker Compose (.yml) che contenga entrambe le immagini di Grafana e Prometheus.
2. Collegare Prometheus all'endpoint Prometheus del server di sessione.

3. Configurare l'origine dati di Grafana affinché comunichi con Prometheus e importare i dashboard preconfigurati.
4. Configurare i dashboard Grafana.
5. Accedere a Grafana.

Passaggio 1. Creare un file Docker Compose

Creare un file docker-compose.yml contenente le immagini di Grafana e Prometheus.

docker-compose.yml

```
versione: "3.1"
  servizi:
  grafana:
    build: grafana
    porte:
      - '3000:3000'
    prometheus:
      immagine: prom/prometheus:v2.6.1
      porte:
        - '9090:9090'
      volumi:
        - ./config/prometheus.yml:/etc/prometheus/prometheus.yml
        - ./prometheus:/prometheus
      networks:
        monitoring:
          aliases:
            - prometheus
  networks:
    monitoring:
```

Passaggio 2. Collegare Prometheus al proprio endpoint Prometheus di HACloud

Per collegare Prometheus al proprio endpoint, generare un file prometheus.yml.

- Nel nostro esempio il file prometheus.yml viene salvato nella directory config.
- In questo esempio config consente di recuperare l'endpoint di Prometheus utilizzando il protocollo HTTP o HTTPS (TLS).

  Se TLS è disabilitato sul server di sessione, rimuovere tls_config e modificare lo schema a http nella configurazione di esempio.
- Configurare session-server-hostname.

  Nota: A causa della networking di Docker, questo deve essere l'indirizzo IP o il nome host effettivo del computer host del server di sessione. Questo indirizzo IP può essere in genere ottenuto utilizzando ifconfig/ipconfig.
- Modificare le porte, se necessario.

config/prometheus.yml

```
scrape_configs:
  - job_name: 'HACloud Session Server with TLS'
  scrape_interval: 15s
  scheme: https
  tls_config:
  insecure_skip_verify: true
  metrics_path: actuator/prometheus
  static_configs:
  - targets: ['session-server-hostname:7443']
```

Passaggio 3. Configurare la comunicazione tra Prometheus e l'origine dati

La comunicazione può essere configurata nell'immagine Docker di Grafana tra l'istanza locale di Prometheus e l'origine dati di Grafana. All'avvio sono anche disponibili dashboard pre-caricati.

grafana/Dockerfile

```
FROM grafana/grafana:5.3.2
  ADD ./provisioning /etc/grafana/provisioning
  ADD ./config.ini /etc/grafana/config.ini
  ADD ./dashboards /var/lib/grafana/dashboards
```

grafana/config.ini

```
[paths]
  provisioning = /etc/grafana/provisioning
```

grafana/provisioning/datasources/all.yml

```
origini dati:
  - nome: 'Prometheus'
  tipo: 'prometheus'
  accesso: 'browser'
  url: 'http://localhost:9090'
  is_default: true
  editable: false
```

grafana/provisioning/dashboards/all.yml

```
- nome: 'default'
  org_id: 1
  folder: ''
  tipo: 'file'
  opzioni :
  cartella: '/var/lib/grafana/dashboards'
```

Passaggio 4. Configurazione dei dashboard Grafana

È disponibile un esempio di file JSON che consente di iniziare a configurare i dashboard Grafana.

Per fare in modo che il container di Docker carichi il dashboard all'avvio:

- Individuare HACloudSessionservers.json nella directory hac`loud/utilities/grafana`.
- Copiare HACloudSessionservers.json nella directory grafana/dashboard.

Passaggio 5. Accedere a Grafana

- Avviare il container di Docker con il comando docker-compose up -d.

- Verificare che le destinazioni di Prometheus recuperino correttamente i server di sessione utilizzando `http://localhost:9090/targets`.
- Accedere a Grafana utilizzando `http://localhost:3000`.
- Entrambi nome utente e password = admin. Il nome utente e la password possono essere configurati utilizzando le variabili di ambiente di Docker.
- Utilizzare il comando docker-compose down per arrestare il container di Docker.

Modifica del limite delle dimensioni dei file durante le operazioni di caricamento

Le operazioni di caricamento di file hanno un limite di dimensione dei file 50 MB. Per modificare il limite delle dimensioni dei file, impostare `spring.servlet.multipart.maxfilesize` e `spring.servlet.multipart.maxrequestsize` in `HACloud/sessionserver/microservices/sessionserver/service.yml` e riavviare il server di sessione.

Ad esempio:

```
- name: spring.servlet.multipart.maxfilesize
value: "100MB"
- name: spring.servlet.multipart.maxrequestsize
value: "100MB"
```

Copia delle sessioni tra istanze di Management and Security Server

È possibile copiare e convertire le sessioni di Reflection for the Web e renderle disponibili per un'altra istanza di Management and Security Server (MSS) e per Host Access for the Cloud.

Nota: Nella procedura seguente l'istanza di Management and Security Server da cui si copiano le sessioni è l'**origine** e l'istanza di Management and Security Server nella quale si sta copiando è la **destinazione**.

Per copiare sessioni dal server di origine al server di destinazione, seguire questi passaggi:

1. Arrestare il server MSS di destinazione, se necessario.
2. Sul server di origine e di destinazione MSS, aprire *SessionDS.xml* nel percorso seguente:
   - In Windows: `C:\ProgramData\Micro Focus\MSS\MSSData`
   - In Linux: `/var/opt/microfocus/mss/mssdata`
3. Nel file XML di origine, individuare l'elemento OBJECT_ARRAY.
4. Sempre nel file XML di origine, sotto OBJECT_ARRAY, identificare e copiare gli elementi *Session* figli di Reflection for the Web.
5. Aprire il file XML di destinazione e incollarli sotto l'elemento OBJECT_ARRAY del file di destinazione.

6. Sempre nel file di destinazione, identificare l'attributo size di OBJECT_ARRAY che corrisponde al numero di sessioni. Aumentare il valore in base al numero di elementi di sessione aggiunti. Ad esempio, se sono stati incollati sei elementi *Session* nel file di destinazione e il valore esistente dell'attributo size di OBJECT_ARRAY è 4, aumentare il valore di 6 unità. Il valore dell'attributo size sarà quindi dieci. A questo punto ci saranno 10 elementi *Session* elencati sotto l'elemento OBJECT_ARRAY.
7. I nomi delle sessioni devono essere univoci. Verificare la presenza di eventuali nomi di sessione duplicati. I nomi delle sessioni si trovano nell'elemento figlio *Session* , *SessionName*.
8. Copiare i file di configurazione per ogni sessione aggiunta a *SessionDS.xml* dal server di origine a quello di destinazione. I nomi dei file di configurazione si trovano sotto l'elemento *Session* nell'elemento figlio, *configuration*. Percorso dei file:
   - In Windows: `C:\ProgramData\Micro Focus\MSS\MSSData\deploy\dyncfgs`
   - In Linux: `/var/opt/microfocus/mss/mssdata/deploy/dyncfgs`
9. Se il server MSS di destinazione è stato arrestato, riavviarlo. Aprire Administrative Console. Tutte le voci Reflection copiate per le sessioni Web dovrebbero essere presenti nell'elenco **Manage Sessions**.
10. Il passaggio successivo consiste nel salvare la sessione di Reflection for the Web come sessione di Host Access for the Cloud. In Manage Sessions, fare clic con il pulsante destro del mouse sulla sessione da esportare. I tipi di sessione sono identificati da un'icona nella colonna Tipo.
11. Vedere Export a Reflection for the Web session (Esportazione di una sessione di Reflection for the Web) per informazioni su come salvare una sessione di Reflection for the Web in una sessione di Host Access for the Cloud in Administrative Console.

Come cambiare le porte

Vedere Porte per ottenere l'elenco delle porte di default utilizzate da Host Access for the Cloud.

Per modificare le porte predefinite:

Componente	Istruzioni

Server di sessione Host Access for the Cloud	Aprire `sessionserver/microservices/sessionserver/service.yml` da modificare:
	`- nome: SERVER_PORT`
	`valore: "7443"`

Management and Security Server	La porta SSL utilizzata da MSS per stabilire la connessione HTTPS è impostata su 443 per impostazione predefinita. Se è necessario modificare il numero della porta, avviare Management Server. Verrà creato il file PropertyDS.xml. Aprire quindi PropertyDS.xml nella directory MssData. Modificare il valore da 443 al numero di porta appropriato nella sezione sotto e riavviare Management Server. `<CORE_PROPERTY NAME="sslport"> <STRING>443</STRING>`

Come avviare e interrompere i servizi automaticamente

Tutti i componenti server sono installati come servizi ed è possibile configurarli durante l'installazione.

Se si utilizza una piattaforma Linux, seguire questi passaggi per impostare l'avvio automatico del server di sessione quando viene avviato il sistema.

Creare un file chiamato `sessionserver` contenente i seguenti elementi e usando la directory di installazione:

```
#!/bin/sh
  #
  #This script manages the service needed to run the session server
  #chkconfig:235 19 08
  #description: Manage the Host Access for the Cloud session server

  ###BEGIN INIT INFO
  # Provides: sessionserver
  # Required-Start: $all
  # Required-Stop: $all #
  Default-Start: 2 3 4 5
  # Default-Stop: 0 1 6
  # Description: Start the Host Access for the Cloud Session Server
  ### END INIT INFO

  INSTALL_DIR=<immettere directory d'installazione>
  BIN_DIR=$INSTALL_DIR/sessionserver/bin
  case "$1" in
  start)
  echo "Starting Host Access for the Cloud Session Server"
  $BIN_DIR/server start

  RETVAL=0
  ;;
  stop)
  echo "Stopping Host Access for the Cloud Session Server"
  $BIN_DIR/server stop

  RETVAL=0
  ;;
  status) echo "Current Host Access for the Cloud Session Server status"
  $BIN_DIR/server status
```

```
  RETVAL=0
  ;;
  restart) echo "Restart Host Access for the Cloud Session Server"
  $BIN_DIR/server restart

  RETVAL=0
  ;;
  *)
  echo "Usage: $0 (start|stop|status|restart)"

  RETVAL=1
  ;;
  esac
  exit $RETVAL
```

Quindi completare i passaggi pertinenti.

Piattaforma	Seguire questi passaggi
Linux	1. Copiare il file nella directory `/etc/init.d`. 2. Impostare l'autorizzazione del file. Eseguire `chmod` utilizzando il valore 755. Ad esempio, `chmod 755 sessionserver` 3. Eseguire `chkconfig` per aggiungere lo script di inizializzazione. Ad esempio, `/sbin/chkconfig --add sessionserver`

Accesso al server di sessione mediante HTTP

Per default, HACloud utilizza TLS (HTTPS) per la comunicazione tra il client Web e il server di sessione. È possibile modificare questa opzione durante il processo di installazione. Tuttavia, potrebbe essere necessario apportare la modifica dopo l'installazione.

Per modificare il protocollo (HTTPS o HTTP) successivo all'installazione:

1. Aprire e modificare `<server di sessione>/microservices/sessionserver/service.yml`.
2. Modificare la variabile di ambiente SPRING_PROFILES_ACTIVE.
   - Per utilizzare HTTP: impostare la variabile su `no-tls`.
   - Per utilizzare HTTPS: impostare la variabile su `tls`.
3. Riavviare il server di sessione.

Ad esempio:

```
ENV:
  - nome: SPRING_PROFILES_ACTIVE
  valore: No-TLS
```

Nota: La modifica del protocollo da HTTPS a HTTP non ha effetto sulla porta del server. HACloud utilizza la porta 7443 come porta di default. Per modificare la porta utilizzata, vedere Come cambiare le porte.

Connessione a MSS mediante HTTP

Per l'installazione di HACloud è necessario che tutti i componenti siano attendibili tramite lo scambio dei certificati. Tuttavia, in alcuni casi è possibile che alcune connessioni debbano esssere pronte per l'ispezione del pacchetto. Vedere Installazione sicura predefinita.

Nota: L'utilizzo di HTTP non elimina la necessità di stabilire l'attendibilità. Altri componenti utilizzeranno sempre TLS dietro le quinte per registrarsi e rilevarne i servizi.

Per abilitare l'interazione del server di sessione con MSS mediante HTTP anziché HTTPS per la maggior parte delle comunicazioni:

Connessione a...	Procedere nel modo seguente...
MSS Administrative Server remoto esistente	1. Durante l'installazione, dopo aver accettato il contratto di licenza e scelto la directory di destinazione, selezionare Use remotely hosted MSS (Usa MSS ospitato in remoto). Fare clic su Avanti. 2. Immettere il nome dell'host, il nome DNS o l'indirizzo IP. 3. Modificare la porta con la porta HTTP del server MSS (ad esempio, 80). 4. Selezionare HTTP e completare la procedura di installazione.
L'MSS Administrative Server installato con Host Access for the Cloud	1. Al termine dell'installazione, aprire `<directory di installazione>\sessionserver\conf\container.properties` in un editor di testo e aggiornare la proprietà `management.server.url`. Ad esempio, `management.server.url=http://yourmachine:80/mss` 2. Riavviare il servizio del server di sessione.

Regolazione del percorso URL del server di sessione

È possibile modificare il percorso URL utilizzato per accedere al server di sessione.

È, ad esempio, possibile modificare `https://myserver:7443/` in `https://myserver.com:7443/hacloud/`

1. Aprire `<directory-installazione>/sessionserver/microservices/sessionserver/service.yml`.
2. Aggiungere la seguente voce (mantenere formattazione) in cui *percorso* viene sostituito con il valore che si desidera utilizzare.

   ```
   - nome:SERVER_SERVLET_CONTEXTPATH
     valore:"/<percorso>"
   ```

3. Riavviare il server di sessione.
4. Accedere al server di sessione a `https://<server di sessione>:7443/<percorso specificato>/`

Configurazione di nomi utente quando si utilizza il controllo di accesso Anonimo

Gli utenti necessitano dell'accesso alle macro che hanno creato, alle configurazioni utente e ad altre impostazioni personalizzate indipendentemente dal fatto che vengano autenticati o meno tramite in Management and Security Server. Queste impostazioni vengono definite collettivamente 'preferenze utente'.

Quando MSS è configurato per l'autenticazione, ad esempio utilizzando LDAP o SAML, il nome utente viene determinato quando l'utente esegue il login. Le impostazioni dell'utente vengono salvate centralmente in MSS e tale nome utente viene utilizzato per tutti i login successivi.

Tuttavia, se il metodo di autenticazione MSS è impostato su Nessuno, noto anche come modalità anonima, il sistema non dispone di alcun nome utente univoco che consenta di identificare l'utente specifico al suo ritorno. In questa configurazione, tutti gli utenti condividono le stesse impostazioni. Se un utente modifica un'impostazione, quest'ultima verrà modificata per tutti gli altri utenti.

Dato che questo potrebbe non essere sempre il comportamento desiderato, Host Access for the Cloud supporta numerosi metodi che, in qualità di amministratore, consentono di configurare un identificatore univoco per ciascun utente, in modo da poter memorizzare e recuperare le rispettive impostazioni personalizzate durante i login successivi.

Nota: Queste modifiche della configurazione non incidono sulle considerazioni sulla sicurezza relative all'utilizzo di Management and Security Server in modalità anonima.

Opzioni di configurazione

Sono disponibili quattro opzioni diverse di configurazione fra le quali scegliere quando si configurano gli identificatori dei nomi utente. È necessario riavviare il server di sessione per rendere effettive le impostazioni.

- **Per utilizzare un valore del cookie della richiesta HTTP come nome utente**

  Aggiungere le righe seguenti a `<session-server>/conf/container.properties`:

  ```
  zfe.principal.name.provider=com.microfocus.zfe.webclient.security.mss.
    CookieKeyAnonymousPrincipalNameProvider
  zfe.principal.name.identifier=<la chiave del cookie da utilizzare>
  ```

- **Per utilizzare un valore dell'intestazione della richiesta HTTP come nome utente**

  Aggiungere le righe seguenti a: `<session-server>/conf/container.properties`:

  ```
  zfe.principal.name.provider=com.microfocus.zfe.webclient.security.mss.
    HeaderKeyAnonymousPrincipalNameProvider
  zfe.principal.name.identifier=<la chiave dell'intestazione da
    utilizzare>
  ```

- **Per utilizzare un parametro URL della richiesta HTTP come nome utente**

  Aggiungere le righe seguenti a: `<session-server>/conf/container.properties`

  ```
  zfe.principal.name.provider=com.microfocus.zfe.webclient.security.mss.
    UrlParameterAnonymousPrincipalNameProvider
  ```

```
zfe.principal.name.identifier=<la chiave del parametro dell'url da
  utilizzare>
```

- **Per utilizzare l'indirizzo IP del client come nome utente**

  Aggiungere la riga seguente a: `<session-server>/conf/container.properties`

  ```
  zfe.principal.name.provider=com.microfocus.zfe.webclient.security.mss.
    RemoteAddrAnonymousPrincipalNameProvider
  ```

Risoluzione dei problemi relativi alla configurazione

Se dopo aver apportato modifiche alla configurazione, un utente riscontra problemi durante la connessione a un'applicazione Web di Host Access for the Cloud, verificare quanto riportato di seguito:

- Viene visualizzato un messaggio **503 Service Unavailable** (503 Servizio non disponibile) quando gli utenti si connettono all'applicazione Web di Host Access for the Cloud. Prima controllare il file di log (`<server di sessione>/logs/sessionserver.log`), quindi:

  -- Se il file di log contiene il messaggio seguente: **"Unable to create AnonymousPrincipalNameProvider instance for class..."**, è probabile che la proprietà `zfe.principal.name.provider` contenga un errore di ortografia. Verificare l'ortografia e l'utilizzo delle lettere maiuscole/minuscole per correggere l'errore.

  --Se il file di log contiene il messaggio:**"zfe.principal.name.identifier is not defined"**, la proprietà è mancante. Per correggere l'errore, assicurarsi che la proprietà sia definita.

- Gli utenti non riescono ad autenticarsi.

  Gli utenti ricevono un messaggio di errore indicante che la richiesta HTTP iniziale all'applicazione Web di Host Access for the Cloud non contiene le informazioni richieste.

Accesso a Host Access for the Cloud mediante il proxy inverso IIS

In questa sezione viene descritto come utilizzare il proxy inverso IIS con Host Access for the Cloud. Per rispettare la conformità con i requisiti di sicurezza Common Criteria, è necessario collocare il server Host Access for the Cloud dietro a un proxy nel modo seguente.

Prerequisiti

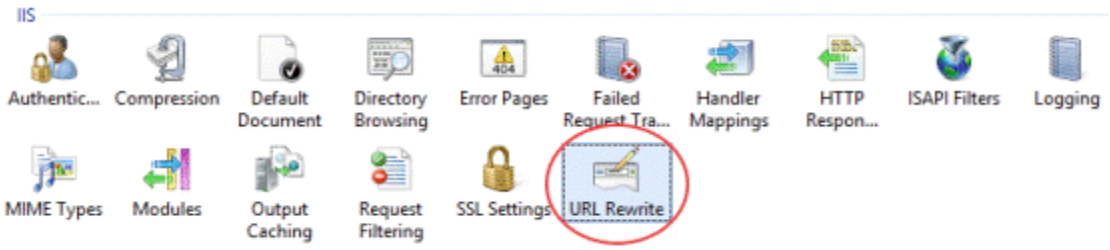
- È richiesto Internet Information Services (IIS) 8.0 o versione successiva.
- Il **protocollo WebSockets** IIS deve essere attivato. Vedere IIS 8.0 WebSocket Protocol Support per informazioni su come attivare il protocollo.
- È richiesto IIS **Application Request Routing (ARR) 3.0** o versione successiva.
- Il modulo IIS **URL Rewrite** deve essere installato.

Configurazione del proxy inverso IIS per Host Access for the Cloud

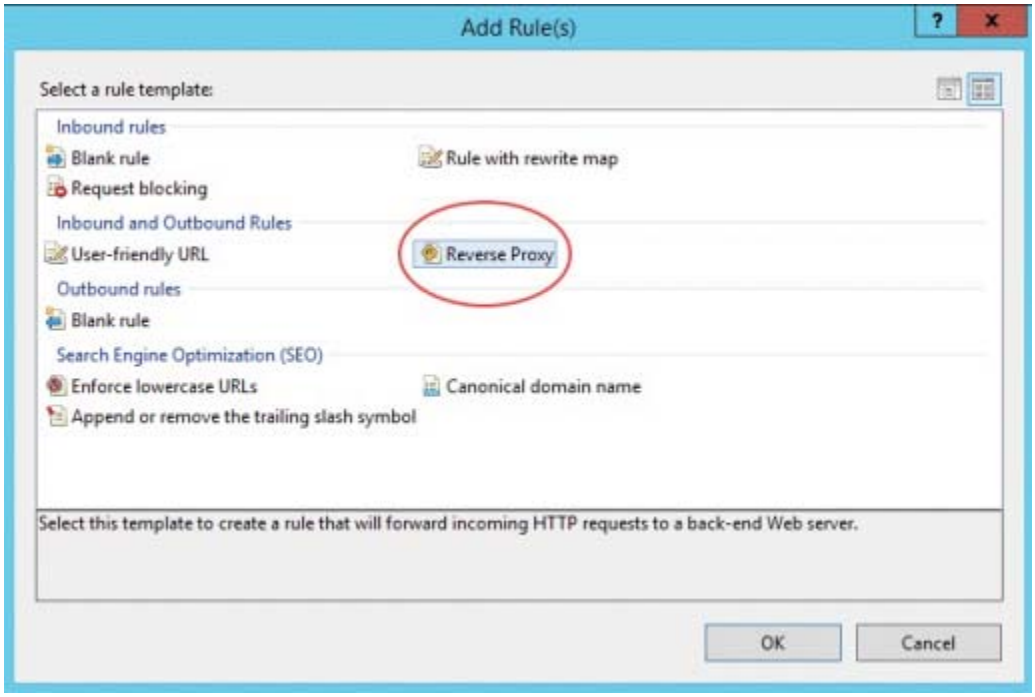
Questo esempio illustra la configurazione di un server IIS con l'indirizzo IP 192.168.1.1 per creare un proxy per le connessioni al server di sessione Host Access for the Cloud all'indirizzo http://10.10.10.1:7070.

Configurazione di IIS

1 Avviare Internet Information Services (IIS) Manager, passare al sito Web da utilizzare e aprire la funzione **URL Rewrite**.



2 Scegliere l'azione **Add Rule(s)** e aggiungere la regola Proxy inverso.



3 Per la regola in entrata, immettere l'indirizzo IP o il nome host e la porta del server Host Access for the Cloud. Ad esempio, se il server di sessione si trova nello stesso computer di IIS e utilizza la porta predefinita, immettere `localhost:7443`.

4 Selezionare la regola in uscita **Riscrivi i nomi dei domini** e immettere il nome host o l'indirizzo IP del server nella casella A:

5 Fare clic su OK per creare la nuova regola Proxy inverso.

Configurazione di Host Access for the Cloud

Per usare un proxy per le connessioni, il modulo IIS **URL Rewrite** deve ispezionare e riscrivere le pagine Web e le connessioni WebSocket che passano attraverso il proxy. Affinché la riscrittura venga completata, questi elementi devono essere inviati in forma non compressa. Notare che, se configurata, la compressione si verificherà comunque dal server IIS al browser del client. Il server di sessione deve essere configurato anche per consentire che le connessioni WebSocket abbiano origine dal proxy.

1. Aprire `container.properties` in un editor di testo. Il percorso predefinito di questo file è: `<directory installazione dir>/sessionserver/conf`.
2. Aggiungere le righe seguenti a container.properties:

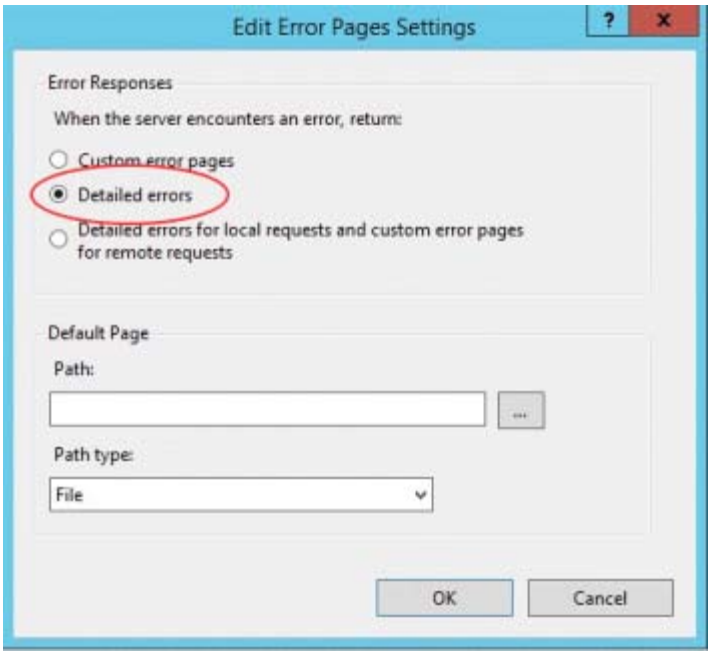
   ```
   websocket.compression.enable=false
   server.compression.enabled=false
   websocket.allowed.origins=http://<nome server IIS o indirizzo IP>
   ```

   . Ad esempio: `192.168.1.1`.

   Salvare le modifiche al file. La proprietà **Allowed Origins** è un elenco di URL delimitato da virgole. Se client Web si connetteranno al sito Web utilizzando una connessione HTTPS, modificare l'URL di conseguenza. Se verranno utilizzate sia connessioni sicure che non sicure, utilizzare entrambi gli URL come valore: `websocket.allowed.origins=http://192.168.1.1,https://192.168.1.1`. Per evitare errori, verificare che tutti i possibili formati indirizzo siano inclusi nell'elenco Allowed Origins.
3. Riavviare il sito Web, quindi riavviare il server di sessione e verificare il proxy connettendosi a: `http(s)://192.168.1.1`.

Risoluzione dei problemi

Se si ricevono errori dal server Web, attivare gli errori dettagliati può contribuire a diagnosticare il problema. In Gestione IIS Manager, aprire la funzione **Pagine errori** e selezionare **Errori dettagliati**:



Solitamente gli errori nell'intervallo 5XX sono causati da problemi di attivazione della compressione o errori nel valore **Allowed Origins**.

Se il proxy IIS si connette al server di sessione con HTTPS, il certificato utilizzato con il server di sessione deve essere considerato attendibile dal server IIS. Se il server di sessione utilizza un certificato firmato da se stessi, questo certificato deve essere aggiunto all'archivio attendibilità di Windows. Se il server di sessione utilizza un certificato firmato, il firmatario deve essere un'autorità di certificazione attendibile.

Miglioramento dei tempi di connessione in piattaforme non Windows

Per migliorare i tempi di connessione in piattaforme non Windows, completare i seguenti passaggi prima di installare il server di sessione Host Access for the Cloud, in particolare se il sistema è virtualizzato o comunque è headless:

1. Arrestare il servizio del server di sessione.
2. Aprire il file `<cartella di installazione >/sessionserver/conf/container.conf` in un editor di testo.
3. Individuare questa riga e modificare come segue:

   `#wrapper.java.additional.x=-Djava.security.egd=file:///dev/urandom`

   - Rimuove il carattere # per eliminare il commento dalla riga.
   - Sostituire x con <n+1>, dove <n> è il numero più grande indicato nelle altre righe `wrapper.java.additional.<n>`.
   - Salvare il file.
4. Riavviare il servizio del server di sessione.

impostazioni avanzate

Di seguito sono riportate alcune configurazioni post-installazione che possono risultare utili.

- Come modificare il timeout della sessione HTTP
- Per abilitare la sicurezza di livello FIPS

Come modificare il timeout della sessione HTTP

Il valore di timeout predefinito per una sessione di utente inattiva è di 30 minuti. Questo significa che quando un utente chiude il browser senza prima eseguire il logout, la sessione dell'utente e tutte le sessioni dell'host aperte verranno chiuse dopo 30 minuti. È possibile configurare questa impostazione sul server.

1. Aprire `<installare directory>/sessionserver/microservices/sessionserver/service.yml`.
2. Modificare il valore del timeout di sessione nella sezione env del file:

```
- nome: server.servlet.session.timeout
   valore: <tempo-desiderato-in-secondi>
```

Suggerimento: La formattazione, con i corretti rientri, è importante.

3 Riavviare il server.

Per abilitare la sicurezza di livello FIPS

I moduli di cifratura convalidati dallo standard FIPS (Federal Information Processing Standards) 140-2 sono lo standard normativo per la sicurezza utilizzato dal governo federale degli Stati Uniti. Host Access for the Cloud supporta questo standard, pertanto è possibile abilitare facilmente la modalità FIPS modificando un file nel server di sessione.

- Aprire `<directory-installazione>\sessionserver\microservice\sessionserver\service.yml`.
- Aggiungere il flag `-Dcom.attachmate.integration.container.FIPS.enabled=true` al comando Java appropriato per il sistema operativo specifico: per Unix - `start-command`, per Windows - `start-command-win`.
- Riavviare il server.
- Per accertarsi che la modalità FIPS sia abilitata, aprire `<directory_di_installazione>\sessionserver\logs\sessionserver.log` e verificare che la modalità FIPS sia impostata su true; `FIPS mode: true`.

Problemi noti

Questi problemi sono stati identificati nelle versioni precedenti e sono noti.

- Problemi relativi al browser
- Problemi specifici degli host
- Problemi di installazione

Problemi relativi al browser

Le note seguenti sono specifiche per i diversi browser Web.

- Browser consigliati
- Problemi di mappatura dei tasti con browser diversi

Browser consigliati

Si consiglia di utilizzare Google Chrome o Mozilla Firefox. Sebbene Host Access for the Cloud supporti Microsoft Internet Explorer (IE) 11, esistono problemi noti delle prestazioni causati dal motore JavaScript di Internet Explorer che possono incidere negativamente sull'utilizzo di Host Access for the Cloud da parte dell'utente finale.

Questi problemi sono stati identificati e hanno una soluzione, tuttavia il modo più semplice per evitarli consiste nell'utilizzare un browser diverso.

Non è possibile eseguire macro registrate con Internet Explorer

Quando si utilizzano determinate versioni precedenti del browser Web Microsoft Internet Explorer (IE) con Host Access for the Cloud, i tentativi di riprodurre le macro possono restituire un errore. Messaggio di errore: *Macro Error: Error transpiling macro code: TypeError: unknown: Circular reference in value argument not supported.*

Si tratta di un problema con questa versione di Internet Explorer e JavaScript. Potrebbe essere possibile evitare questo errore se si elimina la funzione createMacro() e la si sostituisce utilizzando promesse JavaScript (ad esempio, then()).

Poiché questo problema è specifico di versioni precedenti di Internet Explorer, la soluzione più semplice a questo problema consiste nell'utilizzare un browser diverso (Chrome o Firefox) o una versione più recente di Internet Explorer. È possibile riprodurre correttamente le macro utilizzando Internet Explorer versione 11.0.9600.18161, versione aggiornamento 11.0.27. Eseguire Windows Update per aggiornare Internet Explorer.

Connessioni HTTPS tra dispositivi mobili con Apple iOS e il server di sessione

Gli utenti di Host Access for the Cloud non possono eseguire la connessione a un server di sessione tramite HTTPS con l'iPad di Apple quando utilizzano un certificato firmato da se stessi. Se possibile, la soluzione più veloce consiste nell'utilizzare HTTP anziché HTTPS.

Se HTTPS è necessario, sono disponibili le opzioni seguenti:

- Ottenere un certificato valido firmato da una CA attendibile e installarlo nel server di sessione.
- Trovare un browser alternativo che accetti il certificato autofirmato. Vedere Browser e sistemi operativi supportati per un elenco di browser supportati.
- Utilizzare un'autorità di certificazione personalizzata:
  1. Creare una CA personalizzata, un certificato radice della CA e un certificato del server firmato dal certificato radice della CA.
  2. Installare il certificato del server nel server di sessione.
  3. Installare il certificato radice della CA personalizzata sull'iPad mediante un profilo. A questo punto l'iPad dovrebbe accettare il certificato del server come se fosse stato firmato da una "CA attendibile".

  Per un elenco di CA considerate attendibili da Apple iOS, vedere Elenchi dei certificati root attendibili disponibili in iOS (https://support.apple.com/en-us/HT204132).

Internet Explorer visualizza schermi vuoti

Quando si utilizza il browser Web Microsoft Internet Explorer (IE) con Host Access for the Cloud o Access Management and Security Server (MSS), potrebbe essere visualizzata una schermata vuota anziché la sessione prevista.

Quando si utilizza Microsoft Internet Explorer per accedere alle sessioni di Host Access for the Cloud o a Management & Security Server, si potrebbero riscontrare dei problemi, quali:

- Host Access for the Cloud esegue correttamente il rendering per alcuni URL e non per altri (viene visualizzata una schermata vuota). Il comportamento varia a seconda che la sessione utilizzi l'indirizzo IP, il nome host breve o il nome completo.
- In MSS non è possibile creare o aprire una sessione di Host Access for the Cloud a meno che la sessione non si trovi nello stesso server in cui è installato MSS. Viene visualizzato uno schermo vuoto laddove si prevede di vedere una sessione.

Spiegazione

Questo problema è specifico del modo in cui Internet Explorer attiva e disattiva varie impostazioni in base all'interpretazione della sicurezza del sito Web. Le impostazioni in questione sono Visualizzazione Compatibilità e Cookie di terze parti. In base all'area in cui secondo Internet Explorer si trova il sito Web, è necessario attivare o disattivare tali impostazioni. La determinazione di Internet Explorer è basata sull'URL del sito. Ad esempio, se il nome del server nell'URL non contiene punti (ad esempio, http://serveraziendale/mss/AdminStart.html), Internet Explorer suppone che l'indirizzo appartenga all'area Intranet locale. In questo caso, il sito viene assegnato all'area Internet.

Area	Impostazioni predefinite di Internet Explorer
Area Internet locale	Visualizzazione Compatibilità attivata (non desiderata)
	Cookie di terze parti attivata (desiderata)
Area Internet	Visualizzazione Compatibilità disattivata (desiderata)
	Cookie di terze parti disattivata (non desiderata)

Sebbene sia possibile che un sito Web ignori l'impostazione Visualizzazione Compatibilità mediante la specifica di Modalità documento con un metatag HTML X-UA-Compatible e Host Access for the Cloud utilizza tale modalità specifica, lo stesso non accade con MSS. Quindi, se un server Host Access for the Cloud e un'istanza di Management and Security Server si trovano nella stessa zona Intranet locale (con l'impostazione Visualizzazione Compatibilità predefinita attiva), è probabile che Host Access for the Cloud funzioni correttamente mentre MSS no.

Soluzione

Per utilizzare Internet Explorer 10 o 11 con i server Host Access for the Cloud e MSS, è necessario:

- Visualizzazione Compatibilità disattivata
- Cookie di terze parti attivata

È necessario determinare in quale area si trova il sito Web, quindi apportare le modifiche necessarie alle impostazioni di Internet Explorer. Poiché, a seconda della situazione, Internet Explorer può essere configurato in molti modi differenti, è difficile fornire una singola soluzione che consenta di utilizzare Internet Explorer con Host Access for the Cloud e MSS. Ecco alcune configurazioni che è possibile seguire:

- Se Host Access for the Cloud e MSS si trovano entrambi nella stessa zona Internet, aggiungere manualmente il server Host Access for the Cloud in Intranet locale o Siti attendibili (Opzioni Internet > Sicurezza > Intranet locale > Siti). Utilizzare i nomi host completi o gli indirizzi IP.
- Se entrambi i server si trovano nell'area Internet, modificare il comportamento predefinito per quell'area e attivare Cookie di terze parti (Opzioni Internet > Privacy > Avanzate > Sostituisci gestione automatica cookie).
- Se entrambi i server si trovano nell'area Intranet locale, modificare il comportamento predefinito per quell'area e disattivare Visualizzazione Compatibilità (Strumenti > Impostazioni Visualizzazione Compatibilità).

Problemi di mappatura dei tasti con browser diversi

Non è possibile mappare alcuni tasti su un tastierino numerico e alcuni tasti specifici del browser. Ad esempio, in Chrome non è possibile mappare Ctrl+n e Ctrl+w.

Problemi specifici degli host

I problemi seguenti sono specifici per tipi di host diversi.

Visualizzazione del carattere Euro

Se il carattere Euro non viene visualizzato correttamente sullo schermo del terminale, verificare con l'amministratore di sistema che il set di caratteri dell'host per la sessione sia impostato correttamente. Di default, Host Access for the Cloud utilizza un set di caratteri che non supporta il carattere euro (€). Per visualizzare il carattere Euro, passare a un set di caratteri che lo supporta.

Problemi riscontrati con gli host VT

Tipo	Descrizione
Problemi relativi alle prestazioni	◆ Un output di testo complesso, ad esempio un modulo "Is-IR" può causare un rallentamento delle prestazioni ◆ Le aree di scorrimento possono apparire rallentate o incostanti ◆ I movimenti del cursore possono essere rallentati o incostanti ◆ Internet Explorer è particolarmente lento e le prestazioni si riducono quando viene utilizzato per righe e colonne.
Set di caratteri	◆ I caratteri grafici e alcuni set di caratteri non sono supportati. ◆ Alcuni caratteri non inglesi possono causare il blocco del display del terminale.
Altri problemi di VT	◆ L'inserimento e/o l'eliminazione di colonne (DECIC, DECDC) potrebbe non riuscire. ◆ VT400 non riconosce DECSCL.

Contorni dei campi nelle sessioni 3270

Gli attributi di 3270 per i contorni dei campi non sono supportati completamente. Attualmente Host Access for the Cloud supporta il carattere sottolineato e sopralineato, ma la riga verticale sinistra, la riga verticale destra e le combinazioni dei quattro tipi di riga non sono ancora supportate.

Problemi di installazione

Gli argomenti Installazione e aggiornamento includono una sezione per la risoluzione dei problemi che può aiutare a diagnosticare e risolvere problemi specifici di installazione.

L'installazione ha esito negativo a causa del server che impedisce l'accesso alla directory TEMP

È necessario che HACloud disponga dell'accesso a una directory temporanea affinché l'installazione venga eseguita correttamente. In precedenza, se la directory temporanea predefinita non era disponibile, ad esempio in un ambiente server bloccato, l'installazione veniva compromessa.

Impostazione di una directory TEMP per il programma di installazione

Il programma di installazione richiede una directory temporanea scrivibile. Se la directory temporanea predefinita non è adatta, è possibile eseguire il programma di installazione con una directory temporanea alternativa.

- **Windows**

  Se la directory temporanea predefinita non è scrivibile, impostare temporaneamente le variabili di ambiente TMP o TEMP in un'ubicazione alternativa durante l'esecuzione del programma di installazione. Ripristinare le variabili al termine dell'installazione.

- **Linux/Unix**

La variabile di ambiente `INSTALL4J_TEMP` determina la directory di base utilizzata dal programma di installazione per l'autoestrazione. Durante l'estrazione dei file da parte del programma di installazione e l'avvio di Java per l'esecuzione di altre attività, viene utilizzata l'ubicazione temporanea `/tmp` di Java.

Per eseguire i programmi di installazione Linux con una directory temporanea alternativa:

- Definire la variabile `INSTALL4J_TEMP` specificandone il valore come ubicazione temporanea desiderata.
- Creare la directory temporanea specificata per il programma di installazione. Il programma di installazione richiede che la directory sia stata già creata.
- Aggiungere lo switch della riga di comando `–J-Djava.io.tmpdir={tempdir}` all'avvio del programma di installazione. Ad esempio:

```
abcd@linux:~$ INSTALL4J_TEMP=/home/abcd/i4jtemp
     abcd@linux:~$ export INSTALL4J_TEMP
     abcd@linux:~$ sudo ./hacloud-2.4.2.12345-linux-x64.sh -J-
Djava.io.tmpdir=/home/abcd/i4jtemp
```

- Il programma di installazione deve essere eseguito con autorizzazioni amministrative.

Installazioni concatenate di HACloud e MSS

In **Windows**, l'installazione concatenata di HACloud e MSS non richiede altre modifiche se si impostano temporaneamente le variabili di ambiente TMP o TEMP descritte in precedenza.

In **Linux/UNIX** - Non è possibile eseguire un'installazione concatenata su questa piattaforma; eseguirle separatamente, ognuna con autorizzazioni amministrative, con la variabile `INSTALL4J_TEMP` impostata e con lo switch `-J-Djava.io.tmpdir`.

Nota: Se vengono installati sia MSS che HACloud in modo "non concatenato", è necessario installare prima MSS e successivamente HACloud.

Impostazione di una directory TEMP per il prodotto

HACloud utilizza una directory temporanea interna che dovrebbe essere idonea in tutti i casi. Se necessario, è tuttavia possibile modificare questa directory modificando il file `container.conf`.

Modifica dell'ubicazione TMP

È possibile configurare questa ubicazione:

1. Aprire `<cartella di installazione>/sessionserver/conf/container.conf` in un editor di testo.
2. Modificare la proprietà `wrapper.java.additional` per specificare la nuova ubicazione. Se il percorso contiene spazi, racchiuderlo tra virgolette in Windows o usare la sintassi appropriata per le piattaforme Linux/Unix. Ad esempio, `wrapper.java.additional.9=-Djava.io.tmpdir=../tmp`
3. Se necessario, è possibile impostare una proprietà aggiuntiva per cancellare la directory temporanea all'arresto del server.
4. Riavviare il server.

Riferimento per MSS Administrative Console

Host Access Management and Security Server (MSS) fornisce una Administrative Console, una postazione centralizzata basata sul Web dalla quale è possibile gestire le sessioni, assegnare sessioni agli utenti, configurare l'autenticazione e molto altro ancora. I flussi di lavoro che includono la configurazione di impostazioni aggiuntive in MSS Administrative Console sono contrassegnati da questa icona.

nella documentazione di HACloud.

Questo elenco comprende la funzionalità MSS Administrative Console utilizzata da HACloud, inclusi i collegamenti diretti alle sezioni associate nella documentazione MSS. È possibile reperire queste impostazioni nel pannello di navigazione di sinistra di MSS Administrative Console.

- **Manage Sessions** (Gestisci sessioni)

  In questo pannello, Add and configure a Host Access for the Cloud session (Aggiunta e configurazione di una sessione Host Access for the Cloud).

- **Assign Access** (Assegna accesso)

  Utilizzare Assign Access (Assegna accesso) per specificare le sessioni alle quali ha accesso ciascun utente. Se è abilitata l'autorizzazione LDAP, è possibile assegnare diverse sessioni a utenti e gruppi specifici. Con altri tipi di autorizzazione, tutti gli utenti ricevono tutte le sessioni autorizzate. Vedere Assign Access (Assegna accesso)

- **Configure Settings - Authentication and Authorization** (Configura impostazioni - Autenticazione e autorizzazione)

  Consente di configurare il metodo di autenticazione degli utenti durante l'accesso al sistema e il metodo da utilizzare per autorizzare l'accesso alle sessioni. Vedere Select a method to authenticate users (Selezione di un metodo per l'autenticazione degli utenti).

- **Configure Settings - Automated Sign-on** (Configura impostazioni - Sign-On automatico)

  Questa funzione consente a un utente finale di accedere automaticamente a un'applicazione host mainframe mediante un client di emulazione del terminale. Le impostazioni devono essere configurate in MSS Administrative Console, nel client HACloud e su z/OS. Consultare i seguenti riferimenti.

  — Automated Sign-on for Mainframe (Sign-On automatico per i mainframe) nella guida di MSS Administrative Console.

  — Automated Sign-On for Mainframe - Administrator Guide (Sign-On automatico per i mainframe - Guida all'amministrazione)

  — Come impostare Automated Single Sign-On for Mainframe.

- **Conteggio**

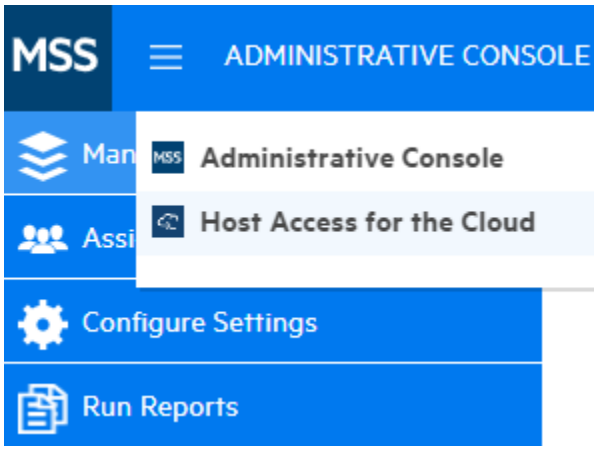
  MSS offre funzionalità di conteggio per il monitoraggio delle sessioni host. Vedere: .

  — Metering (Conteggio) nella MSS Administrator Guide (Guida dell'amministratore di MSS).

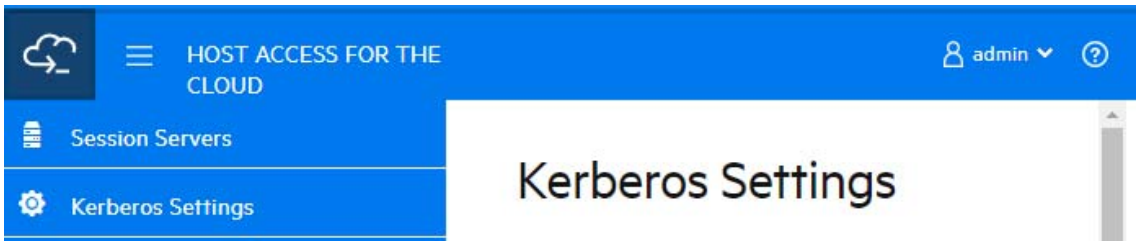
  — Come impostare il conteggio.

- **Accesso automatico Kerberos (solo IBM 5250)**

  Kerberos è un protocollo di autenticazione che utilizza i ticket crittografici per evitare la trasmissione di password come testo normale. Per configurare Kerberos, aprire MSS Administrative Console e selezionare Host Access for the Cloud dall'elenco a discesa:



Nella configurazione di HACloud per l'utilizzo del protocollo di autenticazione Kerberos, sono presenti termini che è necessario comprendere e prerequisiti da rispettare prima della configurazione di questa opzione. Queste opzioni sono descritte in dettaglio nella documentazione del pannello MSS Administrative Console > Host Access for the Cloud. Scegliere Host Access for the Cloud dall'elenco a discesa, quindi selezionare Kerberos Settings (Impostazioni Kerberos) e fare clic sul pulsante Guida.



- **Terminal ID Manager**

  MSS include Terminal ID Manager per creare pool di ID terminale, tenere traccia dell'utilizzo degli ID e gestire i valori di timeout per inattività per utenti specifici, conservando quindi risorse ID del terminale e riducendo significativamente le spese operative. È necessaria una licenza aggiuntiva. Consultare i seguenti riferimenti:

  — Setting up the Terminal ID Manager (Configurazione di Terminal ID Manager)

  — Terminal ID Manager Guide (Guida di Terminal ID Manager)

  — Come impostare Terminal ID Manager